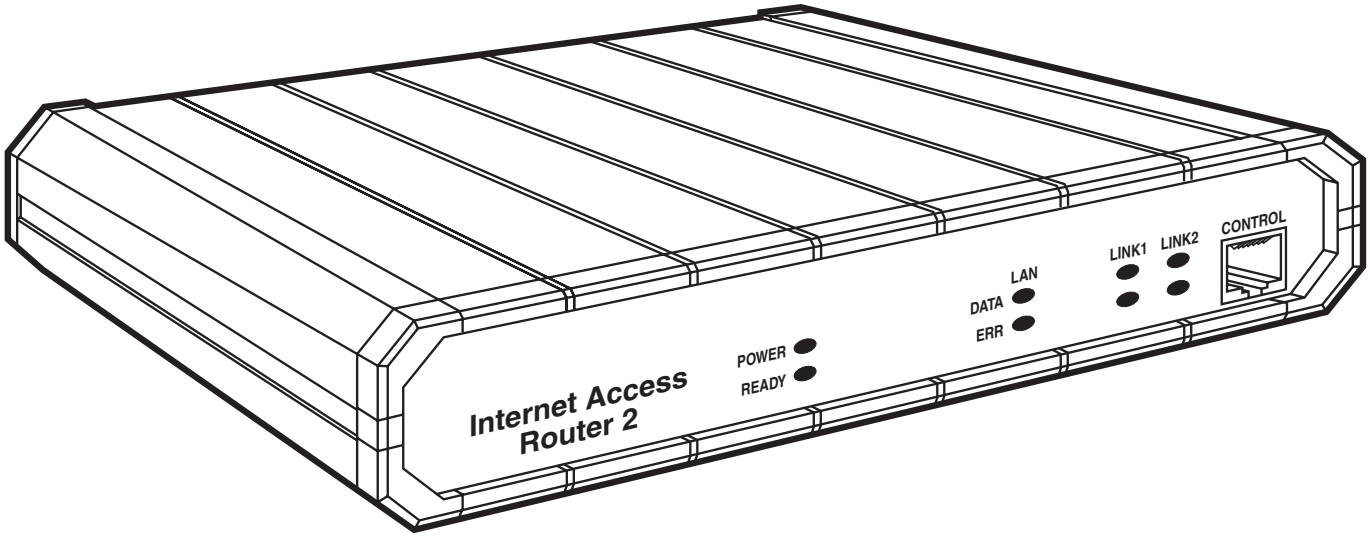
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

BLACK BOX®
NETWORK SERVICES

JUNE 1999

LR0003A-UE1
LR0003A-UBE1
LR0003A-2UE1
LR0003A-UT1-R2
LR0003A-UT1S
LR0003A-U35
LR0003A-2U35
LR0003A-U21
LR0003A-2U21

Internet Access Router 2



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S.: Call **877-877-BBOX** (outside U.S. call **724-746-5500**)
FREE technical support 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mailing address: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION
AND
INDUSTRY CANADA
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

INSTRUCCIONES DE SEGURIDAD (Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    - A: El cable de poder o el contacto ha sido dañado; u
    - B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    - C: El aparato ha sido expuesto a la lluvia; o
    - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    - E: El aparato ha sido tirado o su cubierta ha sido dañada.

TRADEMARKS USED IN THIS MANUAL

BLACK BOX and the ◆ logo are registered trademarks, and "The World's Source for Cabling and Network Connectivity" is a service mark, of Black Box Corporation.

AT&T is a registered trademark of American Telephone & Telegraph Co.

AppleTalk and Mac are registered trademarks of Apple Computer, Inc.

DECnet is a trademark of Compaq Computer Corporation.

IBM, LAN Server, and OS/400 are registered trademarks of Inetrnational Business Machines Corporation.

Microsoft, Exchange, and Internet Explorer are registered trademarks, and HyperTerminal is a trademark, of Microsoft Corporation.

Netscape and Navigator are registered trademarks of Netscape Corporation.

Novell, NCP, NetWare, and Netware Core Protocol are registered trademarks of Novell, Inc.

RealAudio is a registered trademark of RealNetworks, Inc.

UNIX is a registered trademark of UNIX System Laboratories, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Contents

Contents (cont'd)

Chapter **Page**

Chapter **Page**

Contents (cont'd)

Chapter **Page**

Chapter **Page**

1. Specifications

Compliance — FCC Part 15 Class A, DOC Class/MDC classe A

Standards — LAN: IEEE 802.3 Ethernet v. 2;
E1: ITU-T G.703, G.704, G.706, G.732

Interfaces — Control: EIA/TIA RS-232 proprietarily pinned on RJ-45, DCE;
LAN:
- All models: 10BASE-T;
- -UBE1 model only: 10BASE2;

LINK:
- –UE1, -UBE1, and -2UE1 models only: E1;
- –UT1 and UT1S models only: T1;
- –U35 and -2U35 models only: ITU-T V.35;
- –U21 and -2U21 models only: EIA/TIA RS-530 patched to ITU-T X.21

Protocols — On LINK interface: Synchronous PPP, Frame Relay (RFC 1490), HDLC

Data Format — Control interface: 8 data bits, no parity, 1 stop bit (fixed);
E1:
- Framing: D4 or ESF;
- Line coding: AMI;
- Zero suppression: Transparent, B7ZS, B8ZS;

T1:
- Framing: 256N (no MF, CCS) with or without CRC-4, 256S (TS16 MF, CAS) with or without CRC-4
- Line Coding: AMI;
- Zero suppression: HDB3

E1 Line — Impedance: 120 ohms (balanced) or 75 ohms (unbalanced);
Signal Levels:
- Receive: 0 to –30 dB with LTU, 0 to –12 dB without LTU;
- Transmit: 2.7 to 3.3 volts balanced or 2.133 to 2.607 volts unbalanced;

Jitter Performance: As per ITU-T G.823

T1 Line — Impedance: 100 ohms (balanced);
Signal Levels:
- Receive: 0 to –36 dB with CSU, 0 to –10 dB without CSU;
- Transmit: 0, –7.5, –15, –22.5 dB with CSU, user-adjustable at up to 655 ft. (200 m) without CSU;

Jitter Performance: As per AT&T Pub. TR-62411

Data Rate — Control interface: 9600 bps (fixed);
E1: 2.048 Mbps (fixed);
T1: 1.544 Mbps (fixed)

User Controls — On-screen menus;
(1) Rear-mounted rocker switch for power

Indicators —

All front-mounted LEDs;
All models:
- (1) POWER,
- (1) READY,
- (2) LINK1:
  - (1) DATA (activity), (1) ERR (error);
- (2) LINK2:
  - (1) DATA (activity), (1) ERR (error);

-UE1, -UT1, -UT1S, -U35, and -U21 models only:
- (2) LAN:
  - (1) DATA (activity), (1) ERR (error);

-2UE1, -UBE1, -2U35, and -2U21 models only:
- (2) LAN1:
  - (1) DATA (activity), (1) ERR (error);
- (2) LAN2:
  - (1) DATA (activity), (1) ERR (error);

-UE1, -UBE1 models only:
- (2) SYNC LOSS:
  - (1) LOC (local), (1) REM (remote);

-2UE1 model only:
- (4) SYNC LOSS:
  - (2) LINK1 (main channel):
    - (1) LOC (local), (1) REM (remote);
  - (2) SUB (subchannel):
    - (1) LOC (local), (1) REM (remote);

-UT1 model only:
- (2) ALARM:
  - (1) RED, (1) YEL (yellow);

-UT1S model only:
- (4) ALARM:
  - (2) LINK1 (main channel):
    - (1) RED, (1) YEL (yellow);
  - (2) SUB (subchannel):
    - (1) RED, (1) YEL (yellow)

Connectors —

(1) Front-mounted RJ-45control port;
All others rear-mounted;
All models: (1) IEC 320 male power inlet;
LR0003A-UE1:
- (1) RJ-45 female 10BASE-T port,
- (1) RJ-48C female balanced E1 port,
- (2) BNC female unbalanced alternative E1 port:
  - (1) TX, (1) RX;

LR0003A-2UE1:
- (2) RJ-45 female 10BASE-T ports,
- (2) RJ-48C female E1 ports:
  - (1) main channel, (1) subchannel;

LR0003A-UBE1:
- (1) RJ-45 female 10BASE-T port,

(1) BNC female 10BASE2 port,
(1) RJ-48C female E1 port;
LR0003A-UT1:
(1) RJ-45 female 10BASE-T port,
(1) RJ-48C female T1 port;
LR0003A-UT1S:
(1) RJ-45 female 10BASE-T port,
(2) RJ-48C female T1 ports:
(1) main channel, (1) subchannel;
LR0003A-U35:
(1) RJ-45 female 10BASE-T port,
(1) M/34 female V.35 port;
LR0003A-2U35:
(2) RJ-45 female 10BASE-T ports,
(1) M/34 female V.35 port;
LR0003A-U21:
(1) RJ-45 female 10BASE-T port,
(1) DB25 female RS-530 port patched to (1) DB15 female X.21 port;
LR0003A-2U21:
(2) RJ-45 female 10BASE-T ports,
(1) DB25 female RS-530 port patched to (1) DB15 female X.21 port

Power — Input: 100 to 230 VAC, 50 or 60 Hz;
Consumption: Up to 10 VA

Temperature Tolerance — 32 to 122˚F(0 to 50˚C)

Humidity Tolerance — 0 to 90% noncondensing

Size — 1.8" (1U) H x 8.5"W x 9.6"D (4.4 x 21.6 x 24 cm)

Weight — 2.5 lb. (1.2 kg)

2. Introduction

The Internet Access Router 2 (IAR2) connects an Ethernet LAN to the Internet or an Intranet. The connection is made via Frame Relay, synchronous, Digital Data Service (DDS), or E1/T1 links, operating at data rates up to 2.048 Mbps.

The IAR2 includes a feature called Single IP, which allows users in a small office to connect to the Internet/Intranet quickly and transparently. The connection can be made via PSTN, Frame Relay, or leased lines. A description of Single IP features can be found later in this chapter.

The IAR2 also supports two Ethernet LAN connections.

2.1 Overview

The Internet Access Router 2 is a standalone access router that connects small-to-medium-sized networks to the Internet or an intranet. The IAR2 supports IP, IPX routing, and bridging. Quick setup and configuration menus provide on-screen instructions which guide you through installation and configuration procedures.

These are some of the IAR2's most important features:

- IP Routing.
- IPX Routing.
- Bridging.
- Address Translation.
- Solid Firewall.

2.1.1 IP Routing

The Internet Access Router 2 as an IP router supports:

- Static IP net configuration.
- Dynamic IP net learning using the RIP and RIP-2 protocols.
- CIDR topologies.
- Multiple IP nets on the LAN interfaces.
- Numbered and unnumbered interfaces.
- IP fragmentation.

2.1.2 IPX Routing

In addition to IP routing, the Internet Access Router 2 also supports standard IPX routing and includes support for RIP and SAP.

2.1.3 Bridging

The Internet Access Router 2 supports bridging. The bridge function is used to interconnect a number of LANs, by accessing layer 2 (the MAC layer). The IAR2 automatically extends the scope of any interface, allowing the interface to interconnect several networks—if all supported interfaces are set to "bridge mode."

The IAR2 interconnects:

- Any attached LAN to the WAN link.
- Both attached LANs to each other (on two-LAN models).
- Both attached LANs and the WAN link to each other (on two-LAN models).

The IAR2 interconnects all its interfaces to one extended LAN.

The IAR2 supports standard bridging, as specified in IEEE 802.1D, and can operate opposite any other third-party bridge. Spanning Tree Algorithm is not supported. Bridging works over PPP, RFC-1490 Frame Relay, and also a "native" protocol. MAC frames pass in an HDLC format.

2.1.4 Address Translation (Single IP)

The Internet Access Router 2 includes a feature called "Single IP." Single IP allows users in a small-office LAN to connect to the Internet or an intranet quickly and transparently using a single assigned IP address. For more information, see **Section 2.2** and **Appendix C**.

2.1.5 Solid Firewall

The "Solid Firewall" feature prevents access from the Internet or an intranet into the small-office LAN. This feature makes the small-office LAN invisible to outside users. The Solid Firewall feature is a simple and foolproof way of protecting security-sensitive small offices (for example, those of doctors and lawyers) from Internet hackers. For more information, see **Section 6.4**.

2.2 Single IP

Single IP is an Internet Access Router 2 feature that involves the translation of IP addresses. Single IP can be enabled or disabled; when it's enabled, the IAR2 allows users in a small office to connect to the Internet or an intranet quickly and transparently, as shown in Figure 2-1 below. Connection is via PSTN, Frame Relay, or leased lines. Single IP also protects all small office users from hackers on the Internet or intranet.

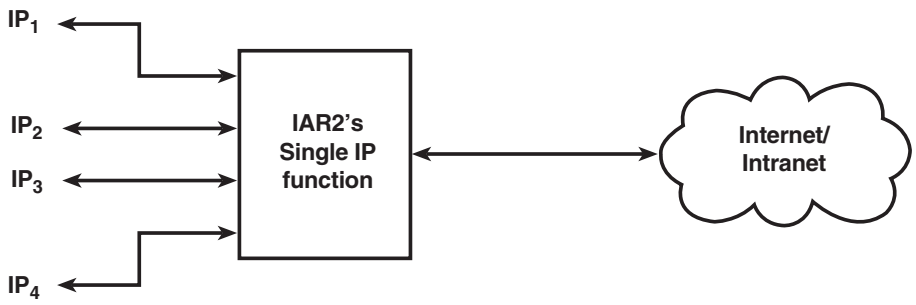


Figure 2-1. IP connections to an IAR2.

Normally, a LAN requires a complete, statically assigned, unique, legal subnet in order to connect to the Internet or to an intranet. Single IP allows an entire small office to connect to the Internet or corporate intranet using only one dynamically or statically assigned IP address received from the ISP via a dial-up modem, leased line, DDS, or Frame Relay line, as shown in Figure 2-2 below. Single IP is recommended for small-office LANs.

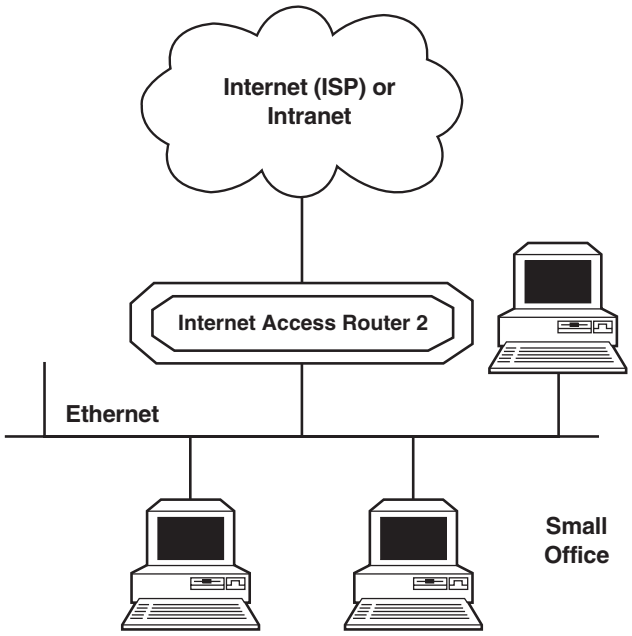


Figure 2-2. An IAR2 with Single IP enabled.

2.2.1 Single IP Features

The Internet Access Router 2's Single IP features include:

- Allows a small office to connect to the Internetor an intranet in the same way as a single PC would.
- Requires only one legal IP address.
- Obtains a single legal IP address from the higher-level Internet or intranet router(s) it communicates with using standard IPCP.
- Allows a small office to access any public IP subnet.
- Allows Web browsing, FTP, Telnet, e-mail, newgroups, and other IP applications using any TCP/IP stack on any type of station in the small office.
- Provides security against Internet hackers using the Solid Firewall feature.
- Allows automatic connection and disconnection of either of the links based on actual or specific use of the Internet or intranet.
- Allows filtering of traffic on the links to reduce bandwidth waste and to improve security.

2.2.2 Small-Office Internet Access vs. Single-PC Internet Access

You can configure the Internet Access Router 2 to make an Internet or intranet connection to a higher-level router and to receive a user name and password over PPP. The higher-level router automatically supplies the IAR2 with a single temporary IP address using the IPCP protocol—the same way that a single PC would connect directly to the ISP.

You can connect a complete small-office LAN with a private subnet to the IAR2. Through the IAR2 the LAN users can access the Internet or an intranet. The Internet or intranet provider does not need to specially coordinate with the office or allocate subnets.

The IAR2 is even designed to support multiple concurrent users on the LAN. Refer to Figure 2-3 below.

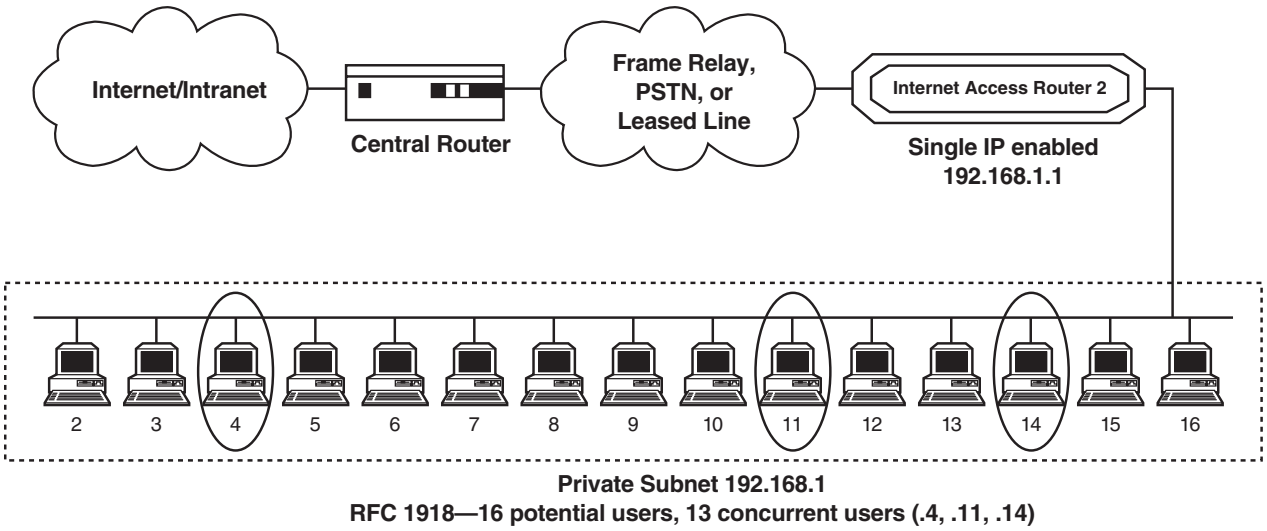


Figure 2-3. An IAR2 in Single IP mode.

2.2.3 IP Applications

Single IP allows the use of any Web browser, such as Netscape® Navigator® or Microsoft® Internet Explorer®, to access the World Wide Web. The list below shows some of the types of Internet and intranet access supported by Single IP:

- World Wide Web browsing.
- E-mail.
- FTP client.
- News reader.
- TELNET client.
- Ping (outbound).

Single IP supports any SOCKS-compatible client application (for example, Netscape Navigator). The IAR2 also supports access to FTP within browsers, Gopher access, and access to secure servers. POP3 clients (such as Eudora®, Pegasus® mail, Microsoft Exchange®) and other e-mail packages and news readers are allowed access to e-mail servers through Single IP e-mail support.

Single IP allows use of FTP client applications that support the "username@hostname" method of firewall crossing (for example, WS_FTP®, CuteFTP®, and command-line FTP clients). Connection through another firewall using the same mechanism is also allowed.

2.3 Features and Where in This Manual to Find Them

Routing:

- Supports bridging, IP routing, IPX routing, and any combination of these.
- Supports the Single IP feature (IP Address Translation) which allows multiple users to use a single Internet or intranet connection. Refer to **Section 2.2** and **Appendix B**.
- Supports static nets and multinets. Refer to **Section 7.4.2**.
- Supports IP fragmentation. Refer to **Section 7.4.3.C**.

Protocols:

- Supports PPP. Refer to **Section 7.4.1.E**.
- Integral Frame Relay operating at data rates up to T1. Refer to **Sections 7.5.1** and **7.5.2**.

Interfaces:

- Supports synchronous and E1/T1 WAN interfaces. Refer to **Section 7.5.1.B**.
- Supports 10BASE2 or 10BASE-T LAN interfaces. Refer to **Section 3.4.3**.

Configuration and Control:

- Supports TELNET. This feature allows configuration and control over WAN and LAN of the IAR2. Refer to **Section 6.2**.
- Supports RADIUS. Refer to RADIUS in **Section 7.3.5**.
- Fast initial configuration can be performed from a terminal emulator or via TELNET. Refer to **Chapter 5**.
- An SNMP agent for management at a standard SNMP station. Refer to **Section 7.3.3**.
- Software (firmware) downloading is available using XMODEM or TFTP. And dual-image flash enables downloading two software versions. Refer to **Section 7.9.1**.

Security:

- PAP/CHAP provides access authentication. Refer to **Section 7.6.1.B**.
- Solid Firewall feature allows the user to block all access from the outside into the LAN. Refer to **Section 6.4**.
- Undesired access to the IAR2 via TELNET or SNMP can also be blocked or password-protected. Refer to **Section 7.3**.

2.4 Applications Illustrated

The Internet Access Router 2 connects your Ethernet LAN to the Internet or an intranet. The connection is made via Frame Relay or leased line.

WAN Interfaces:

- **E1** and **T1** are digital line services which provide high-speed connections.
- **V.35** and **X.21** are synchronous interfaces which provides efficient connections. This interface can provide connection to one or two LANs.

Protocols:

- **PPP** is the Point to Point Protocol. This protocol supports a variety of links and connection options.
- **Frame Relay** is a network interface which provides high-speed frame or packet transmission with minimum delay and maximum bandwidth utilization.

Application Options:

The following three figures illustrate three application options for the IAR2.

In the application shown in Figure 2-4 below, an IAR2 supports a single LAN connection to the Internet using the V.35 WAN interface and the PPP or Frame Relay protocol:

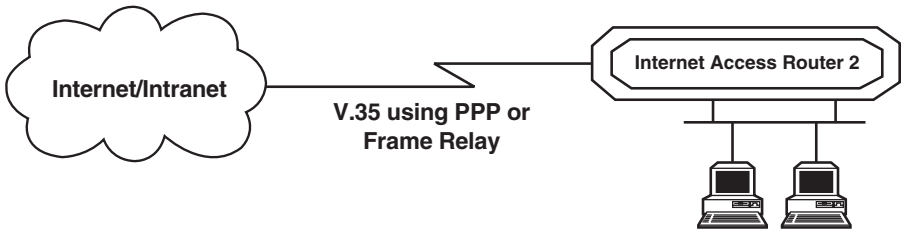


Figure 2-4. An IAR2 with a V.35 WAN interface and a single LAN interface.

In the application shown in Figure 2-5 below, an IAR2 supports two separate LAN configurations. The IAR2 connects these networks to the Internet with a V.35 interface, again using the PPP or Frame Relay protocols.

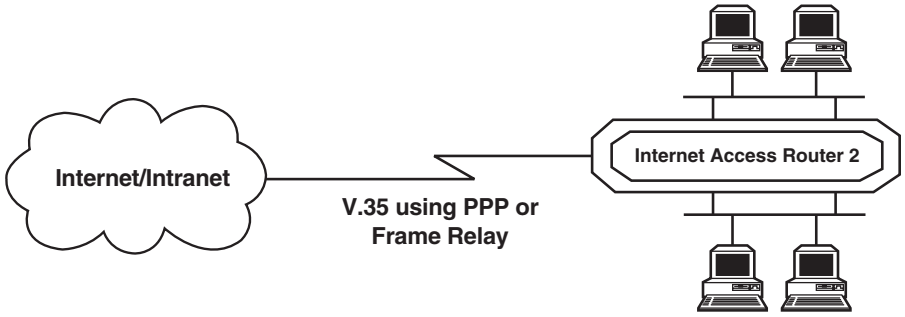


Figure 2-5. An IAR2 with a V.35 WAN interface and dual LAN interfaces.

In the application shown in Figure 2-6 below, an IAR2 uses the E1 or T1 interface to connect to both Internet services and voice (telephone) services. E1 and T1 sublinks are for carrying voice lines *only*.

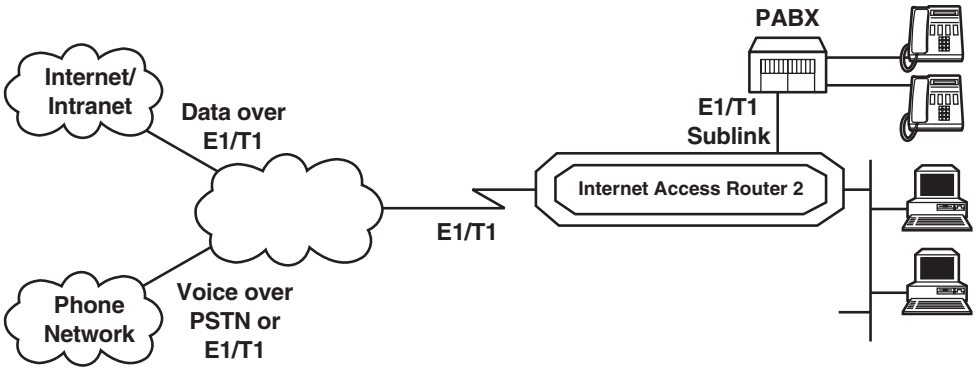


Figure 2-6. An IAR2 with an E1 or T1 WAN interface, a LAN interface, and a sublink to a PABX.

3. Installation

This chapter provides information on installing and initially operating the Internet Access Router 2. The IAR2 is delivered completely assembled; installing it involves these procedures:

- Unpacking, placing, and hardware-configuring the unit.
- Connecting it to a power source.
- Connecting it to your LAN(s).
- Connect it to your WAN link(s).
- Connecting it to a terminal emulator.

After installing the IAR2, refer to **Chapter 4** for configuration instructions. If you have any problems, refer to **Chapter 10** for fault-isolation and troubleshooting instructions.

3.1 The Complete Package

The complete Internet Access Router 2 package includes the IAR2 itself, its power cord, and an adapter cable to connect to its control port. The X.21 models also come with a DB25 male to DB15 female patch cable. If you didn't receive everything, or if anything arrived damaged, call Black Box right away.

3.2 Site Requirements

Before installing the Internet Access Router 2, make sure that these conditions are met:

- The IAR2 unit should be installed within 1.5 m (5 feet) of a grounded AC outlet furnishing the appropriate voltage (115 VAC for "A" models, 230 VAC for "AE" models).

CAUTION!

Do not attempt to adjust, repair, or maintain an open device while it is plugged in. All repairs should be carried out by competent technicians who are aware of the hazards involved.

- Allow at least 10 cm (4 inches) clearance in front of and behind the unit for interface-cable connections.
- The temperature should be between 0 and 50°C (32 and 122°F) with not more than 90% relative humidity noncondensing.
- The IAR2 is designed for installation on top of a bench or shelf, or secured to a 19" rack. A rackmount kit for the IAR2 is available as a special quote; call Black Box Technical Support if you'd like one.

3.3 Hardware Configuration

CAUTION!

In most cases, there is no need to do hardware configuration. It is only necessary when you need to set the V.35 interface to DCE, when you need to enable the unbalanced E1 interface, or when you need to decouple frame ground from the E1 or T1 reference grounds.

To avoid accidental electric shock, disconnect the Internet Access Router 2's power cord before opening the unit's top cover.

1. Disconnect the Internet Access Router 2's power cord from the wall socket. (Turning OFF the POWER switch on the IAR 2's rear panel is *not* sufficient!)
2. Remove the unit's cover by loosening the screw located on the bottom of the unit.
3. Set the desired jumpers; see **Sections 3.3.1** and **3.3.2**. Although there are other jumpers on the IAR2's circuit boards than those described in these sections, do *not* change the settings of any of the other jumpers.
4. Refit the cover.

3.3.1 V.35 DTE/DCE Jumpers

The WAN-link interface of V.35 models of the IAR2 can be configured as DTE or DCE. The factory setting is DTE. To set it to DCE, you'll have to move a jumper block; refer to Figure 3-1 below.

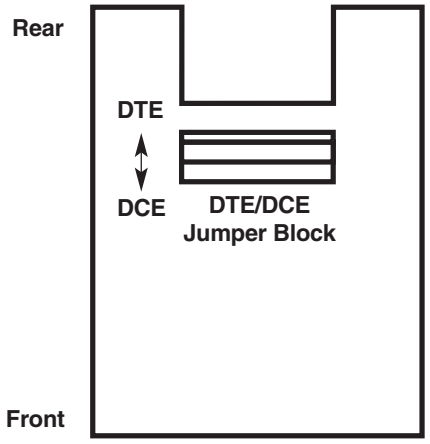


Figure 3-1. Location of DTE/DCE jumpers on the IAR2's V.35 daughterboard.

3.3.2 E1/T1 Jumpers

Using the E1/T1 jumpers (see Figure 3-2 on the next page), the WAN-link interfaces of E1 and T1 models of the IAR2 can be set for several options:

Jumpers	Description
Balanced/Unbalanced Jumpers	On E1 models *only,* use jumpers J2, J3, J6, J7, and J8, all designated "BAL/UN," to choose whether the unit uses the balanced or unbalanced E1 interface. Set all of these jumpers to "BAL" to select the balanced interface (the RJ-48 connector) or all of them to "UN" to choose the unbalanced interface (the two BNC connectors). (All of these jumpers must be set the same way in order for the unit to work at all.) The factory-default setting is "BAL."
Receive/Frame Ground Jumper (J1)	On E1 models set for the unbalanced interface *only,* use jumper J1 to control whether or not the WAN link's unbalanced E1 receive-ground reference is connected to the IAR2's frame (chassis) ground. Set this jumper to "YES" to connect the grounds or "NO" to let the receive ground float (that is, to isolate the grounds from each other). The factory-default setting is "YES."
Signal/Frame Ground Jumper (J4)	On T1 models and on E1 models set for the balanced interface *only*, use jumper J4 to control whether or not the WAN link's signal-ground leads (pins 3 and 6 of the RJ-48 connector) are connected to the IAR2's frame (chassis) ground. Set this jumper to "YES" to connect the grounds or "NO" to let the signal ground float (that is, to isolate the grounds from each other). The factory-default setting is "YES."

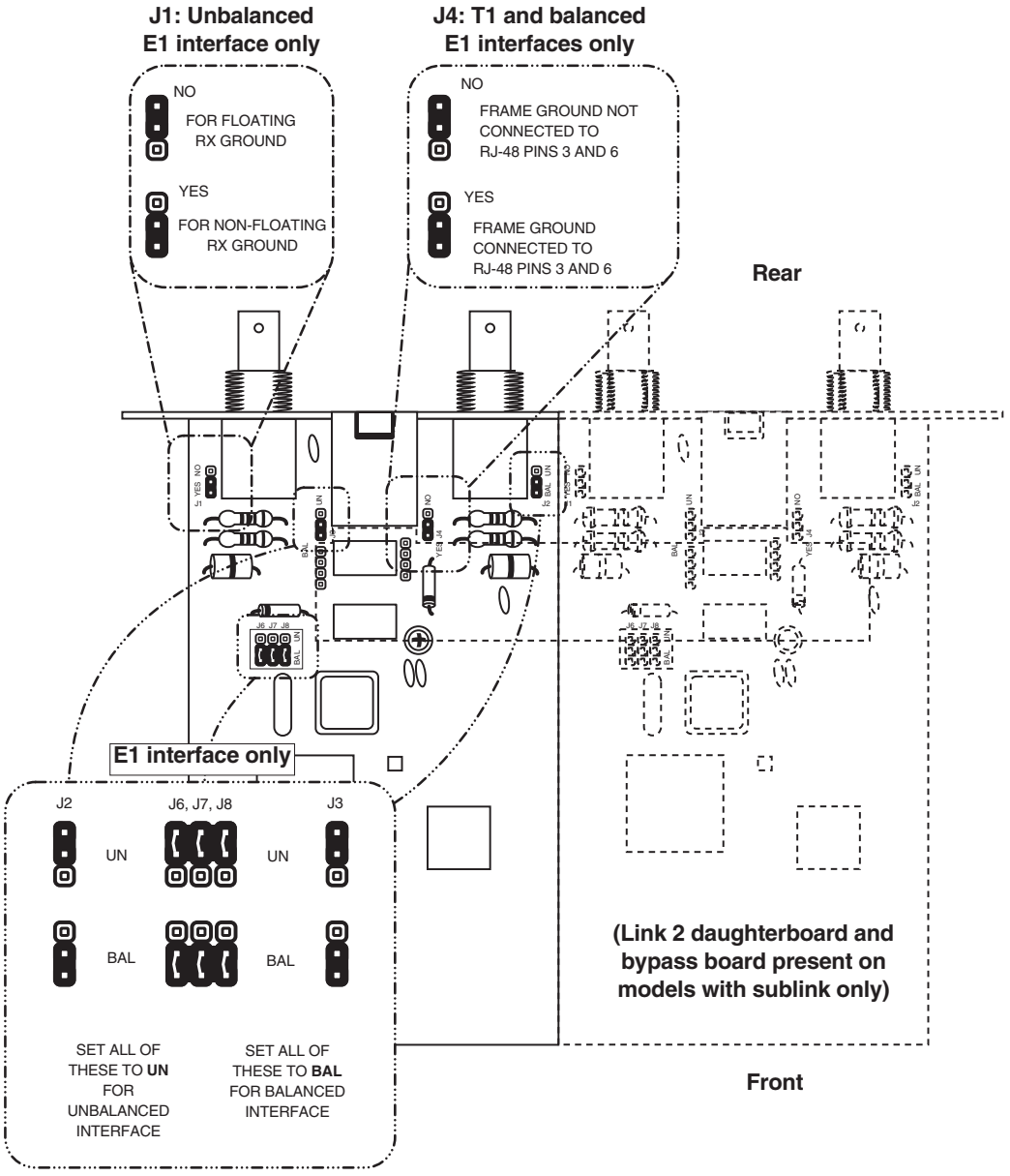


Figure 3-2. The E1/T1 jumpers.

3.4 Power and Cable Connections

3.4.1 AC Power Connection

AC power should be supplied to the Internet Access Router 2 through a power cord terminated by a standard three-prong plug, such as the 175-cm (6.7-ft.) cord provided with the unit. Connect the cord's outlet to the IAR2's rear-panel IEC 320 male power inlet, then attach the cord's plug to a standard grounded AC outlet.

CAUTION!

When you apply power to the IAR2, make sure that it is properly connected to the site's grounding (earth) system. Make sure to always use a power cord with a ground lead running from the ground terminal of the IAR2's power inlet to the ground contact of a utility-power (mains) outlet. Do not leave the IAR2 ungrounded by using a power cord, power strip, extension cord, BPS/UPS, or outlet without a ground conductor.

In the course of normal operation under normal conditions, your IAR2's one-amp fuse (located in the unit's rear panel above the unit's power inlet) should never blow. But if it ever does, make sure that you replace it only with a new fuse rated for the same current. Do not use repaired fuses or short-circuit the IAR2's fuse holders. If you ever suspect that the IAR2's fuse might have blown or been damaged, unplug the unit and make sure it is not powered up again until the problem can be checked and fixed.

Operating the IAR2 when it's not properly grounded or does not have proper fuse protection could damage the IAR2 and any attached equipment, and could also pose a potentially fatal shock hazard.

3.4.2 WAN-Link Connection(s)

The Internet Access Router 2 has one of these different sets of WAN-interface connectors on its rear panel depending on which model it is (refer to Figure 3-3 on the next page and to the illustrations in **Section 3.5**):

- The -UT1 model has one RJ-48C female connector for its T1 interface.
- The -UT1S model has one RJ-48C female connector for its main T1 interface and a second RJ-48C female connector for its T1 sublink interface.
- The -UE1 and -UBE1 models have one RJ-48C female connector for their balanced E1 interface and two BNC female connectors for their unbalanced E1 interface. To use the unbalanced interface, you need to set the IAR2's balanced/unbalanced jumpers to the "unbalanced" setting (see **Section 3.3.2**).
- The -2UE1 models have one RJ-48C female connector for their balanced main E1 interface and two BNC female connectors for their unbalanced main E1 interface. They have another set of these three connectors for their balanced and unbalanced E1 sublink interface. To use the unbalanced interfaces, you need to set the IAR2's balanced/unbalanced jumpers to the "unbalanced" setting (see **Section 3.3.2**).
- The -U35 and -2U35 models have one M/34 female connector for their V.35 interface. This interface is normally DTE; to make it DCE, you need to set the IAR2's DTE/DCE jumpers to the "DCE" setting (see **Section 3.3.1**). Refer to **Appendix A** for the pinout of this connector.
- The -U21 and -2U21 models have one DB25 female connector for an RS-530 interface. These models come with a DB25-male-to-DB15-female patch cable that you should plug into this port; the cable's DB15 female connector is the IAR2's X.21 interface. This interface is normally DTE; to make it DCE, you need to set the IAR2's DTE/DCE jumpers to the "DCE" setting (see **Section 3.3.1**). Refer to **Appendix A** for the pinout of both the DB25 and DB15 connectors.

Run cable from each WAN interface to a WAN device (modem, CSU/DSU, FRAD, etc.) or WAN wall outlet.

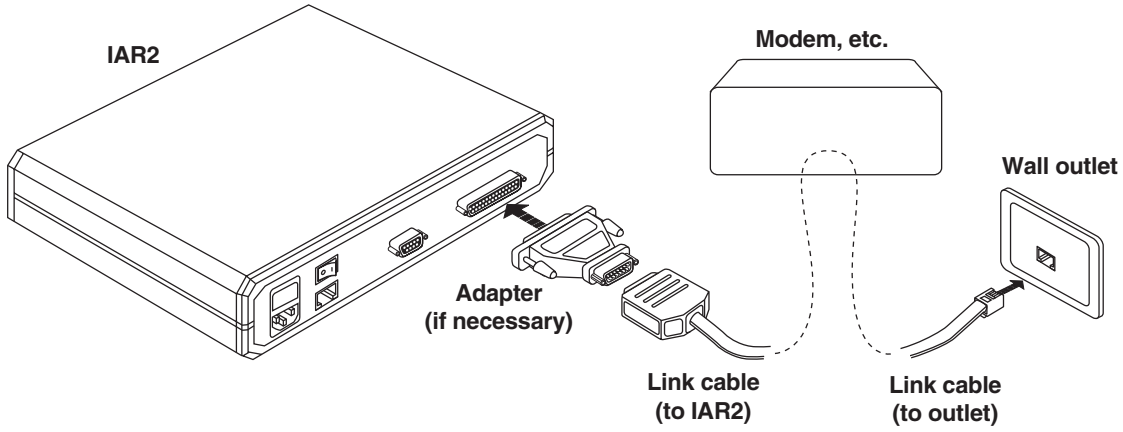


Figure 3-3. A sample WAN-link connection.

3.4.3 LAN Connection(s)

The Internet Access Router 2 has one of these different sets of Ethernet LAN-interface connectors on its rear panel depending on which model it is (refer to Figure 3-4 on the next page and to the illustrations in **Section 3.5**):

- The -UE1, -UBE1, -UT1, -UT1S, -U35, and -U21 models both have one RJ-45 female connector for their 10BASE-T interface.
- The -2UE1, -2U35, and -2U21 models have two RJ-45 female connectors for their 10BASE-T interfaces, one for each of two LAN segments you can connect.
- -UBE1 models have one BNC female connector for their 10BASE2 interface.

Run cable from each of these interfaces to a LAN or LAN device (hub, repeater, router, switch, etc.).

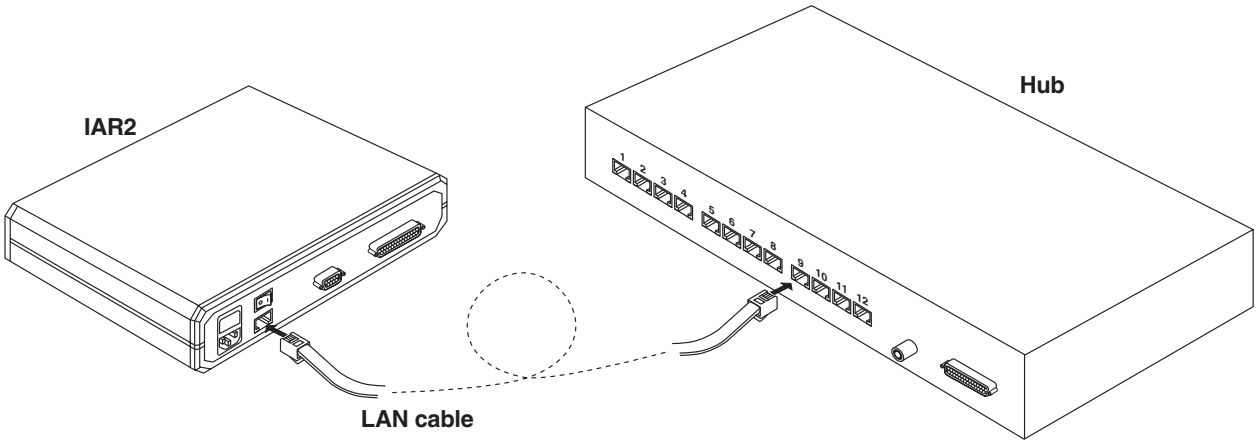


Figure 3-4. A sample LAN connection.

3.4.4 Control-Interface Connection

The Internet Access Router 2 has an RS-232 DCE control interface (a proprietarily pinned RJ-45 female connector) on its front panel. Through this interface, you can soft-configure the IAR2 with an ASCII terminal or a computer running a terminal emulation program. To make this connection, you should run the adapter cable included with your unit from the IAR2's CONTROL port to one of the CPU's serial ports, as shown in Figure 3-5 below. This cable has an RJ-45 male connector at one end and a DB9 female (or sometimes a DB25 female) connector at the other; see **Section A.3** of **Appendix A** for pinouts of these connectors. (If the DB9 or DB25 connector on the cable can't be plugged into any of the serial ports on your computer, you might need a serial-port adapter such as our product code FA520A-R2 for DB25 male to DB9 female or FA521A for DB9 male to DB25 female.)

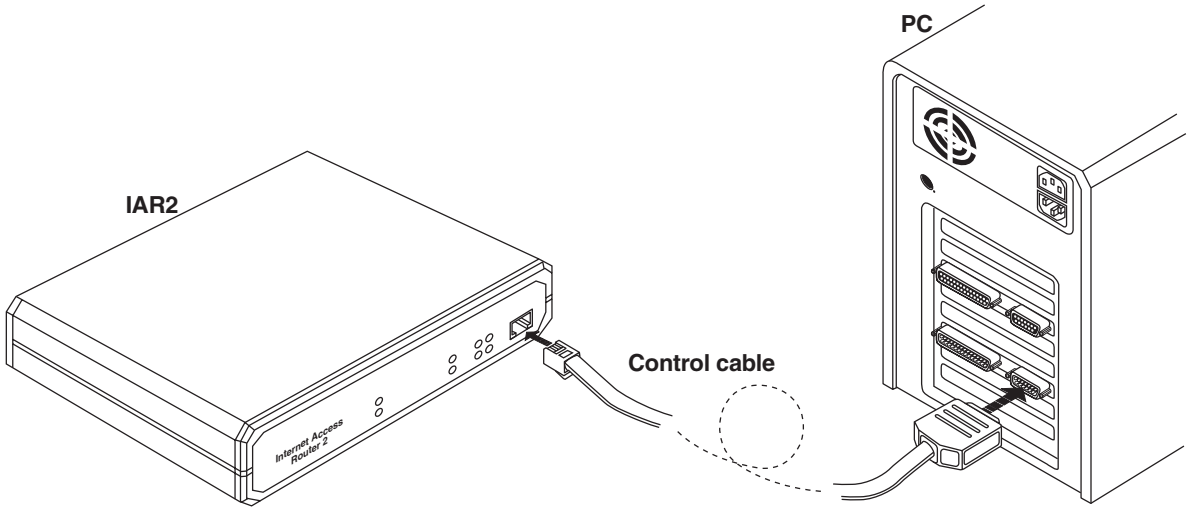


Figure 3-5. A sample control connection.

3.5 The Front Panels Illustrated

Figures 3-6 through 3-11 below and on the next page show the front panels of the various Internet Access Router 2 models. The CONTROL port on each model is an RJ-45 female connector that functions as a proprietarily pinnned RS-232 DCE port for terminal-based management. Table 3-1 on page 27 describes what each of the LEDs indicates.

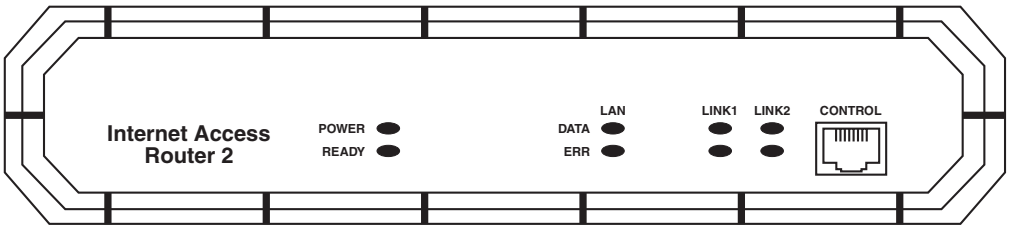


Figure 3-6. The front panel of the -U35 and -U21 models.

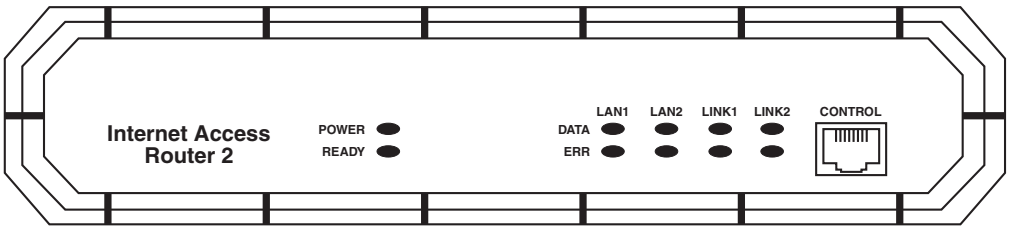


Figure 3-7. The front panel of the -2U35 and -2U21 models.

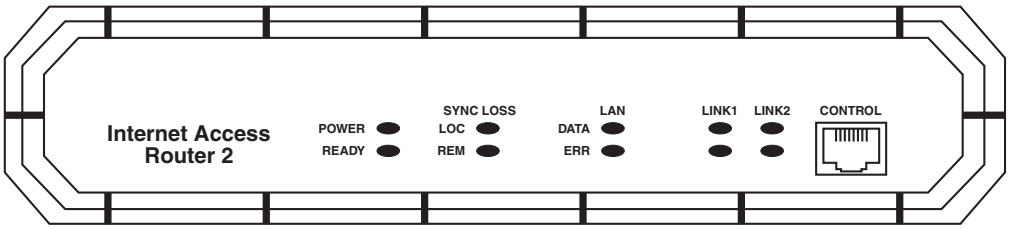


Figure 3-8. The front panel of the -UE1 and -UBE1 models.

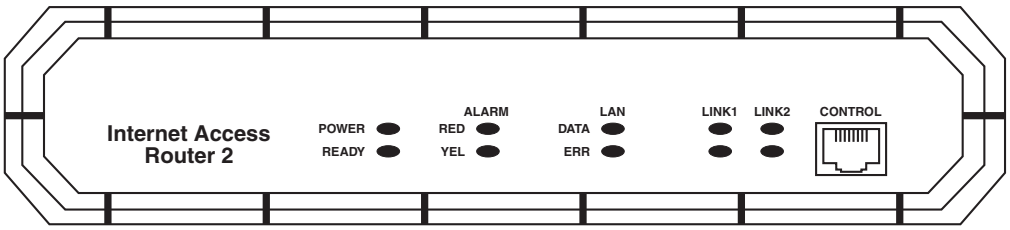


Figure 3-9. The front panel of the -UT1 model.

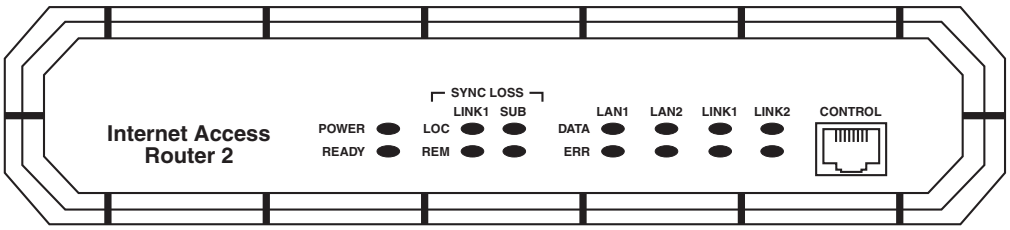


Figure 3-10. The front panel of the -2UE1 model.

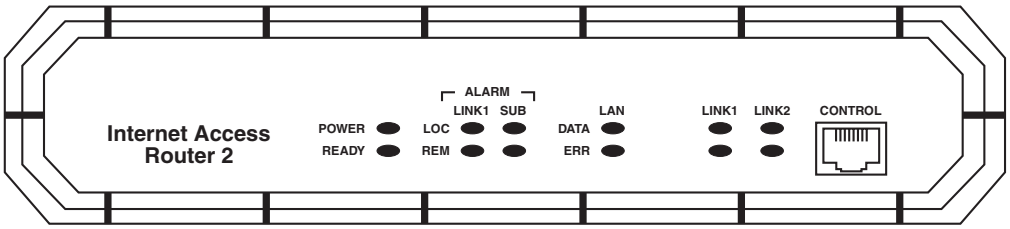


Figure 3-11. The front panel of the -UT1S model.

Table 3-1. The IAR2's LEDs

Label	Color	Function
POWER	Green	Lights when IAR2 is powered ON.
READY	Green	Lights when packets can be transferred (that is, when at least two interfaces are connected at the physical layer).
LAN 1 DATA	Yellow	Lights when a packet is sent or received on the LAN1 side.
LAN 2 DATA	Yellow	Lights when a packet is sent or received on the LAN2 side.
LAN 1 ERR	Red	Lights when an error is detected on LAN1.
LAN 2 ERR	Red	Lights when an error is detected on LAN2.
LINK 1 DATA	Yellow	Lights briefly when a packet is sent or received on the main WAN link (LINK1).
LINK 2 DATA	Yellow	Lights when a packet is sent or received on the WAN sublink (LINK2/SUB). Has no function on units with no sublink ports.
LINK 1 ERR	Red	Lights briefly when an error is detected on the main link (LINK1); lights continuously if there is a physical failure on the main link (connector disconnected, cable broken, etc.).
LINK 2 ERR	Red	Lights briefly when an error is detected on the WAN sublink (LINK2/SUB); lights continuously if there is a physical failure on the sublink (connector disconnected, cable broken, etc.). Has no function on units with no sublink ports.
LINK 1 LOC SYNC LOSS	Red	Lights when E1 main link is in "local sync loss alarm" (local IAR2 has lost frame synchronization on main link for more than 2.5 consecutive seconds).
SUB LOC SYNC LOSS	Red	Lights when E1 sublink is in "local sync loss alarm" (local IAR2 has lost frame synchronization on sublink for more than 2.5 consecutive seconds).
LINK 1 REM SYNC LOSS	Red	Lights when E1 main link is in "remote sync loss alarm" (local IAR2 has received a "sync loss" signal from the remote IAR2).
SUB REM SYNC LOSS	Red	Lights when E1 sublink is in "remote sync loss alarm" (local IAR2 has received a "sync loss" signal from the remote IAR2).
LINK 1 RED ALARM	Red	Lights when T1 main link is in "red alarm" (local IAR2 has lost frame synchronization on main link for more than 2.5 consecutive seconds).
SUB RED ALARM	Red	Lights when T1 sublink is in "red alarm" (local IAR2 has lost frame synchronization on sublink for more than 2.5 consecutive seconds).
LINK 1 YELLOW ALARM	Red	Lights when T1 main link is in "yellow alarm" (local IAR2 has received a "red alarm" signal from the remote IAR2).
SUB YELLOW ALARM	Red	Lights when T1 sublink is in "yellow alarm" (local IAR2 has received a "red alarm" signal from the remote IAR2).

3.6 The Rear Panels Illustrated

Figures 3-12 through 3-20 below and on the next page show the rear panels of the various Internet Access Router 2 models. Table 3-2 on page 30 describes what each of the connectors is for.

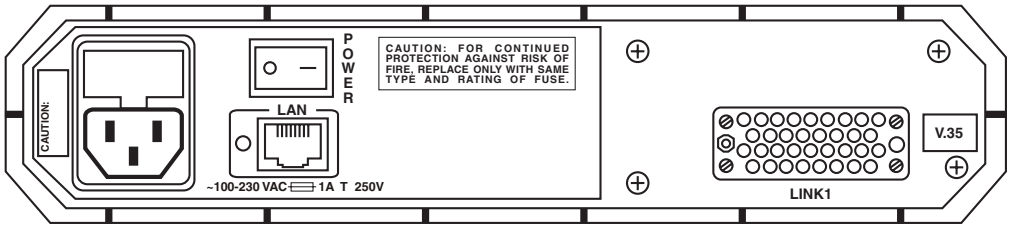


Figure 3-12. The rear panel of the -U35 model.

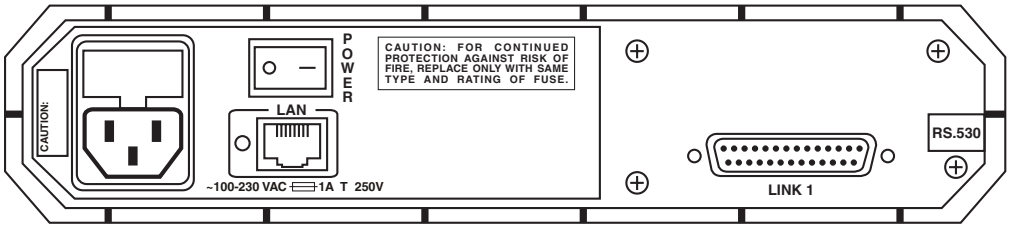


Figure 3-13. The rear panel of the -U21 model (patch cable from RS-530 DB25 to X.21 DB15 not shown).

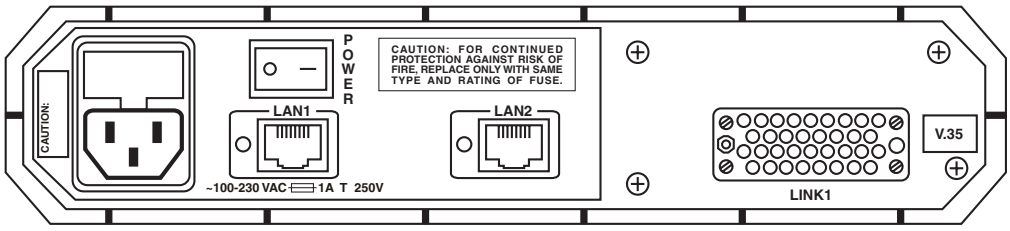


Figure 3-14. The rear panel of the -2U35 model.

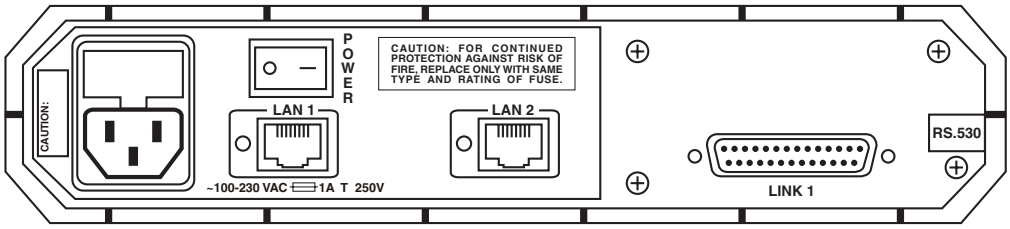


Figure 3-15. The rear panel of the -2U21 model (patch cable from RS-530 DB25 to X.21 DB15 not shown).

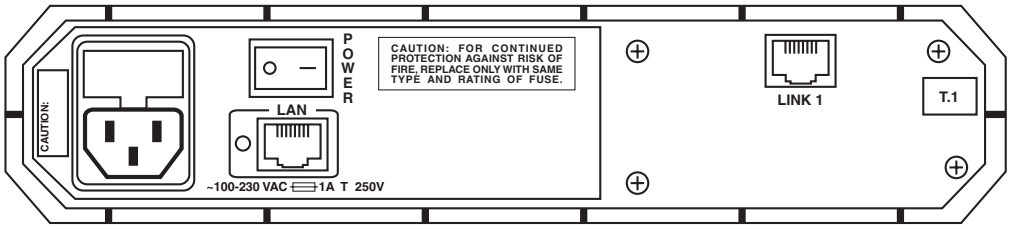


Figure 3-16. The rear panel of the -UT1 model.

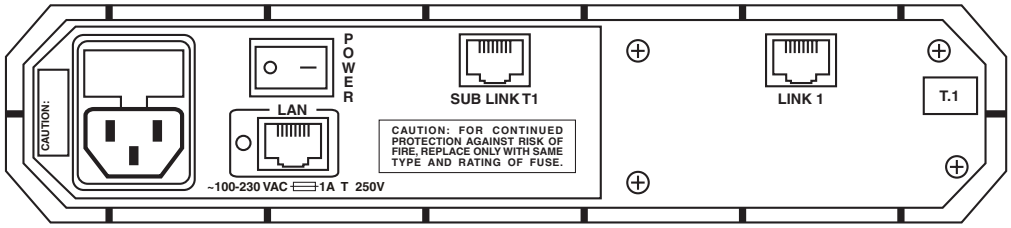


Figure 3-17. The rear panel of the -UT1S model.

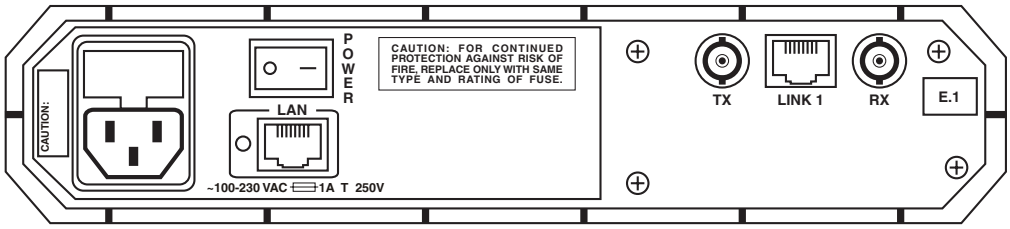


Figure 3-18. The rear panel of the -UE1 model.

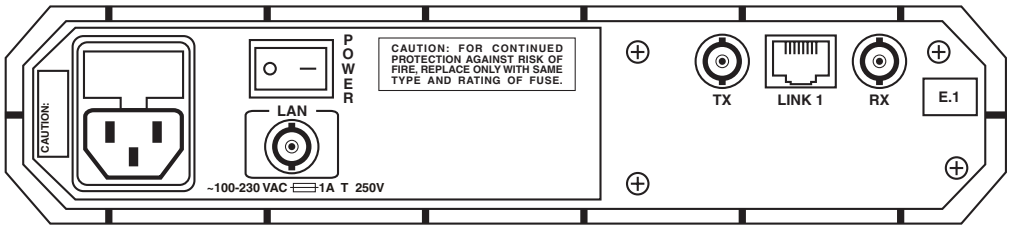


Figure 3-19. The rear panel of the -UBE1 model.

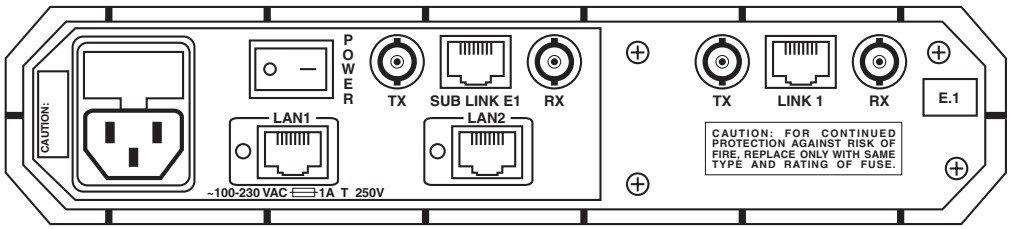


Figure 3-20. The rear panel of the -2UE1 model.

Table 3-1. The IAR2's Rear-Panel Connectors

Label	Function
LAN	The sole LAN interface for this model.
LAN1	The first of two LAN interfaces for this model.
LAN2	The second of two LAN interfaces for this model.
LINK1	The main T1, V.35, or X.21 WAN link for this model.
LINK1 + TX, RX	The main E1 WAN link for this model. LINK1 is the balanced interface, TX and RX are the unbalanced interface.
SUB LINK T1	The T1 WAN sublink for this model.
SUB LINK E1 + TX, RX	The E1 WAN sublink for this model. SUB LINK E1 is the balanced interface, TX and RX are the unbalanced interface.

3.7 Initial Operation

Once you have the Internet Access Router 2 fully installed, you can turn it ON by moving its rear-mounted POWER switch to the ON position. The front-panel POWER LED should light. Before attempting to operate the unit any further, you should soft-configure it for your application as described in **Chapter 4**. Once this is done and the system is operating normally (remote stations are active), the IAR2's READY LED should remain continuously lit, its LAN DATA and LINK DATA LEDs should blink, and its LAN ERR, LINK ERR, and (if present) SYNC LOSS or ALARM LEDs should stay dark. To turn the IAR2 OFF, move its POWER switch back to the OFF position.

4. Configuration

This chapter tells you how to software-configure your Internet Access Router 2. (Some WAN-link options must be configured by manipulating the hardware, but this is not usually necessary; see **Section 3.3**.)

4.1 Starting Your Configuration

4.1.1 Connecting to the Internet or an Intranet as a Public IP Net

Use the following check list to make sure you are ready to connect to the Internet or an intranet:

- Subscribe to the Internet Service Provider (ISP) and request a static IP subnet.
- Disable Single IP in the IAR2's Quick Setup option.
- Make sure the line (Frame Relay or leased line) to the ISP is working properly.
- Use the static IP subnet you have obtained to configure the IAR2's LAN IP host addresses.

Use this one to make sure that your PCs are prepared:

- Make sure your PCs have a correctly installed a TCP/IP stack such as WinSock or Chameleon.
- Assign an IP address, from the static IP subnet to each PC.
- Ensure that each PC has the correct subnet mask.
- Configure each PC with the IAR2 as the Default Gateway.
- Configure each PC with the ISP's DNS IP address.
- Check that your small-office LAN is correctly set up to work with IP.

4.1.2 Connecting to the Internet or an Intranet as a Private IP Net Using Single IP

Use the following check list to make sure you are ready to connect to the Internet or an intranet.

- Subscribe to the Internet Service Provider (ISP) and request a single subscription connection.
- Decide on a private IP net for your small office LAN (Reference RFC 1918).
- Enable the Single IP in the IAR2 Setup option.
- Make sure the line (Frame Relay or leased line) to the ISP is working properly.
- Use the private IP subnet you have obtained to configure the private host addresses of the IAR2.
- Check that your small-office LAN is correctly set up to work with IP.

Use this one to make sure that your PCs are prepared:

- Make sure your PCs have a correctly installed TCP/IP stack such as WinSock or Chameleon.
- Assign an IP address, unique to the LAN, to each PC.
- Configure each PC with the IAR2 as the Default Gateway.
- Ensure that each PC has a correct subnet mask.
- Configure each PC with the ISP's DNS IP address.
- Check that your small-office LAN is correctly set up to work with IP.

4.2 Initial Setup

The Internet Access Router 2 has a setup program in its firmware that you can invoke and run from an ASCII terminal or a PC (running a terminal emulator) attached to the IAR2's RJ-45 CONTROL port. Refer to **Section 3.4.4** for instructions on making this connection.

4.2.1 Accessing the Configuration Program's Main Menu

Once your PC or terminal is attached to the IAR2, set the terminal or terminal emulator to communicate at any data rate from 9.6 Kbps, using 8 data bits, no parity, and 1 stop bit. Set hardware flow control to OFF. Turn on the IAR2. The operational status screen should appear. Press ENTER several times to invoke the password message.

4.2.2 Setting a Password

The password protects entry to the configuration module, preventing unauthorized personnel from changing setup and configuration parameters. For first-time operation, or if no configuration password has been specified, the following message appears:

```
WARNING: No configuration password exists.
Define configuration password? (Y/N):
```

To set a configuration password:

1. Type **Y**. A message appears, prompting you to enter a new configuration password.
2. Type a password. The password can be up to twelve characters. Press the ENTER key. A message appears, prompting you to retype the password for verification.
3. Retype the password and press ENTER. The Main menu screen appears (refer to **Section 4.3**).

NOTE

All IAR2 password-verification routines are CASE-SENSITIVE. Once a password has been set, always use the same case as in the original when typing the password.

4.2.3 Changing the Password

To change the password during normal operation:

1. From the Main Menu, select option 0, Exit, to return to the Operational Status Messages screen.
2. Press ENTER several times; you will then be prompted to enter the current password.
3. Enter the current password. A message appears, asking if you want to update the current password. Type **Y**; you will then be prompted to re-enter the current password.
4. Re-enter the current password. A message appears prompting you to enter the new password.
5. Enter the new password, then re-enter the same password for verification. The Main Menu appears.

4.2.4 Deleting the Password

To delete the current password:

1. Follow steps 1 through 5 in **Section 4.2.3** to change the password. But when you're prompted to enter a new password, press ENTER without typing a new password. This deletes the current password and removes password protection.

2. Press ENTER again when prompted for verification. The Main Menu appears. (If the unit doesn't have an IP address, the Quick Setup menu appears instead.)

NOTE

We recommend that you use password protection for the configuration module Always use the Exit option in the Main Menu once the unit has been configured; this will force personnel requiring access to the configuration module to enter the password.

4.3 Menus and Screens

This section provides a brief description of the Internet Acccess Router 2's available menus and screens.

The Main Menu
The Internet Access Router 2's product name ("IAR2") is listed at the top of the screen, as shown below. The Main Menu has five options. To choose an option, type the number preceding the option.

```
      MAIN MENU  ( Device name - IAR2 )
      ---------

  1.  Quick setup
  2.  Secutity setup
  3.  Advanced setup
  4.  View
  5.  Diagnostic mode


  0.  Exit

    ESC - Returns to previous menu


Choose one of the above:
```

The Quick Setup Menu
The Quick Setup menu allows you to adjust the setup and link-configuration parameters of your Internet Access Router 2 (including those involving security and economy features, the WAN interface, and IP configuration) while the IAR2 is in operation. Line-by-line prompting simplifies the setup. On-screen instructions and explanations guide you through the setup procedure. For a complete description of the Quick Setup menu, refer to **Chapter 5**.

The Security Setup Menu
Use the options in the Security Setup menu to control IAR2 management and entry to your LAN by unauthorized users.

The Advanced Menu
The Advanced Menu lists IAR2 configuration parameters and their current values. You can change these parameters and perform advanced configuration operations, not available through the Quick Setup menu. Resetting the device and software downloads are also performed via the Advanced Menu.

The View Menu
Use the options in the View menu to view configuration screens and information on interface connections, routing tables and statistics.

The Diagnostic Tools Menu
Use the Diagnostic Tools menu to verify WAN and LAN connectivity. The Ping feature allows you to dial (Ping) another user on the LAN or WAN. If the remote user replies, WAN connectivity is confirmed up to and including the IP level.

Exit
Select this option to return to the Operational Status Messages screen. From the Operational Status Messages screen you can remove or change the password.

5. The Quick Setup Menu

The Quick Setup Menu allows you to enter the minimum number of parameters needed to operate your Internet Access Router 2. The Quick Setup menu is designed for ease of use. You can access it with an ASCII terminal, a terminal emulator, or TELNET.

For more extensive control of your IAR2, refer to **Chapters 5** and **6**.

The Quick Setup screen presents messages, prompting you to accept or modify the current parameters. To accept the current parameter, press ENTER. The parameter options (possible settings) are enclosed in brackets ("[ ]"). To view the options, toggle with the space bar and press ENTER. To enter new information, type in the new parameters and press ENTER. After all parameters have been accepted or changed, you can view them on the screen. A confirmation message appears requesting that you confirm all the setup changes. The IAR2 will reset after saving these changes.

To configure the setup parameters:

1. From the Main Menu, select option 1, Quick Setup.
2. Follow the on-screen instructions to accept or modify the setup parameters.
3. Press "Y" to save the setup parameters.

The Quick Setup menu automatically adapts itself to the built-in link interface. The final screen for each interface, and a description of the options in the Quick Setup menu, can be found in the sections that follow. Refer to the section which applies to the interface you ordered.

The following sections contain descriptions of the Quick Setup menu for the following WAN interfaces:

- **Section 5.1** deals with V.35 and X.21 models.
- **Section 5.2** deals with E1 and T1 models.

5.1 Settings for V.35 and X.21 Models

```
     QUICK SETUP
     -----------
WARNING: This device automatically exits to Operational
          Messages 10 minutes after last keyboard action without
          saving parameters

  'ENTER' - Accept parameter , 'SPACE' - Change parameter.

  WAN interface #1 - V.35
    Connection type: [Uplink  ]
    Link mode: [Frame Relay    ]
    Routing: [IP & IPX ROUTER ], Protocol: [RFC 1490   ]
    Number of DLCIs to configure: 2
    Enter DLCI id number (16-991): 16
    WAN IP address: 10.0.0.1 , enter new : 10.0.0.1
    WAN IP mask   : 255.255.255.252 , enter new : 255.255.255.252
    Do you want to enable SINGLE IP option (Y/N)? : [N]
    Enter DLCI id number (16-991): 18
    WAN IP address: 10.1.1.5 , enter new : 10.1.1.5
    WAN IP mask   : 255.255.255.252 , enter new : 255.255.255.252
    Do you want to enable SINGLE IP option (Y/N)? : [N]

  LAN 1 settings:
    Routing: [IP & IPX ROUTER ]
    IP address : 192.168.2.1 , enter new : 192.168.2.1
    IP mask    : 255.255.255.0 , enter new : 255.255.255.0
  LAN 2 settings:
    Routing: [IP & IPX ROUTER ]
    IP address : 192.168.3.1 , enter new : 192.168.3.1
    IP mask    : 255.255.255.0 , enter new : 255.255.255.0
  Default gateway setting by: [Interface ]
    Default gateway interface: 1 DLCI: 18


  Saving the changes might cause RESET the unit.
  Do you want to save QUICK SETUP (Y/N) ? Y
```

Figure 5-1. Quick Setup screen for -2U35 model (V.35 WAN link + 2 LANs).

The fields in the Quick Setup screens are described in the following subsections.

5.1.1 WAN Interface

5.1.1.A Connection Type

Select this parameter to specify the type of connection:

- **Uplink -** if the link is to be used to connect to the Internet or intranet, or if the link is to be used for both incoming and out going connections (not simultaneously).
- **Answer -** if the link is to be used for receiving remote-access connections.

5.1.1.B Link Mode

Select this parameter to determine how data is transmitted across the link. When the mode is **synchronous**, data bits are transmitted at a fixed rate; the sender and the receiver are synchronized at this rate. When the mode is **Frame Relay**, data is transmitted using a packet-switching protocol; a hardware setup using Frame Relay is shown in Figure 5-2 below. And when the mode is **E1** or **T1**, data is transmitted according to that standard.

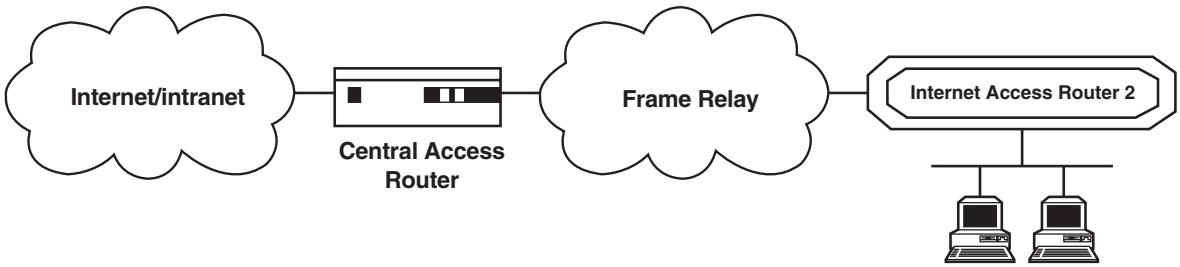


Figure 5-2. Frame Relay hardware setup.

5.1.1.C Routing

Select this parameter to assign the link type. Use the space bar to toggle between **bridge**, **IP**, and **IPX** link types or any combination of these link types.

Selecting the IPX link type disables the Single IP and WAN IP Address features, and eliminates the corresponding parameters from the screen.

5.1.1.D Protocol

The default value of this parameter is PPP.

- **PPP -** Point to Point Protocol. PPP consists of 3 components:
  - A way to encapsulate IP datagrams on a serial link. PPP supports either HDLC synchronous links or async links with 8 data bits, no parity, and 1 stop bit.
  - A link-control procedure (LCP) to establish, configure, and test the data-link connection. Having an LCP allows each end to negotiate various options.
  - A family of network-control protocols (NCPs) specific to different network-layer protocols. The NCPs allow each end to configure network-control parameters.

  PPP is often used across slow serial lines. It is therefore important to reduce the number of bytes per frame to reduce the latency time. Using the LCP, most implementations negotiate to omit the constant address and control fields and to reduce the size of the protocol fields from 2 bytes to 1 byte. In addition, when using the IP NCP, most implementations use Van Jacobson header compression to reduce the size of the IP and TCP headers.

- RFC-1490 - Encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. RFC-1490 also supports a simple fragmentation procedure for carrying large frames over a frame relay network with a smaller MTU. There is some very important information that goes with this setting:

  – DLCI - Every network interface card (NIC) has a Data Link Communication Identifier (DLCI) that uniquely identifies the node on the network. DLCI enables connection to the Frame Relay network *without configuring Frame Relay parameters.*

    DLCI executes congestion control when an explicit congestion notification is received for the DLCI from the Frame Relay network. The unit reduces the transmitted information rate of the DLCI and increases it when the congestion condition is cleared.

5.1.1.E Number of DLCI

Select this parameter to set the number of DLCIs to configure. This number reflects the number of active DLCIs in the Frame Relay port.

5.1.1.F DLCI ID

Select this parameter to set the DLCI identification number.

5.1.1.G WAN IP Address

Select this parameter to enter the IP address for the WAN interface (as opposed to the IP address for the LAN interface, as shown in Figure 5-3 below):

- **Regular Router Mode (Unnumbered):** Set WAN IP Address to 0.0.0.0 (with Single IP OFF).
- **Regular Router Mode (Numbered):** Set WAN IP Address to a.b.c.d (with Single IP OFF).
- **Single IP Mode (Fixed IP address):** Set WAN IP Address to a.b.c.d (with Single IP ON).
- **Single IP Mode (Dynamic IP address):** Set WAN IP Address to 0.0.0.0 (with Single IP ON; IP address is received dynamically over the WAN using IPCP).

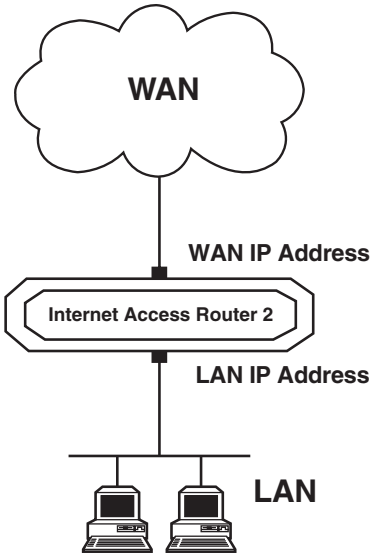


Figure 5-3. The WAN and LAN IP addresses.

5.1.1.H WAN IP Mask
Select this parameter to statically enter the IP mask for the WAN interface; for example 255.255.255.0. Refer to **Section 3.1.1.G** on the previous page for more information.

5.1.1.J Single IP Option
Single IP is a IAR2 feature which allows users in a small-office LAN to connect to the Internet or an intranet quickly and transparently. Single IP uses a single dynamically or statically assigned IP address for all users. Select this parameter to enable or disable Single IP. For more information about Single IP, refer to **Section 2.2**.

5.1.2 LAN Settings

Set these parameters for each LAN connection.

5.1.2.A Routing
Select this parameter to set the routing option. Refer to **Section 5.1.1.C** for more information.

5.1.2.B LAN IP Address
Select this parameter to enter the IP address. Every device on a TCP/IP network must have an address to identify it; see Figure 5-4 on the next page. The IP address is a value consisting of the network address and the host address on that network. The value assigned to a network depends on the number of computers on that network.

The IP address is a 32-bit number. The number is made up of 4 parts, with each part consisting of 3 digits. One part of the address identifies the network and another part of the address identifies the host. The numbers in the address which identify the host depend on the class.

There are 5 classes of IP addresses. Each class represents a network having a certain number of computers. For example, a Class C address is given to a network having up to 255 computers. Table 5-1 below gives the ranges for different classes of IP addresses.

Table 5-1. IP Address Classes

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

The numbers in each part of the code are translated into binary. The binary code identifies the network and the host.

IP addresses are currently assigned by Network Solutions, Inc. Network Solutions also assigns the network ID. Host IDs are assigned by the network administrator.

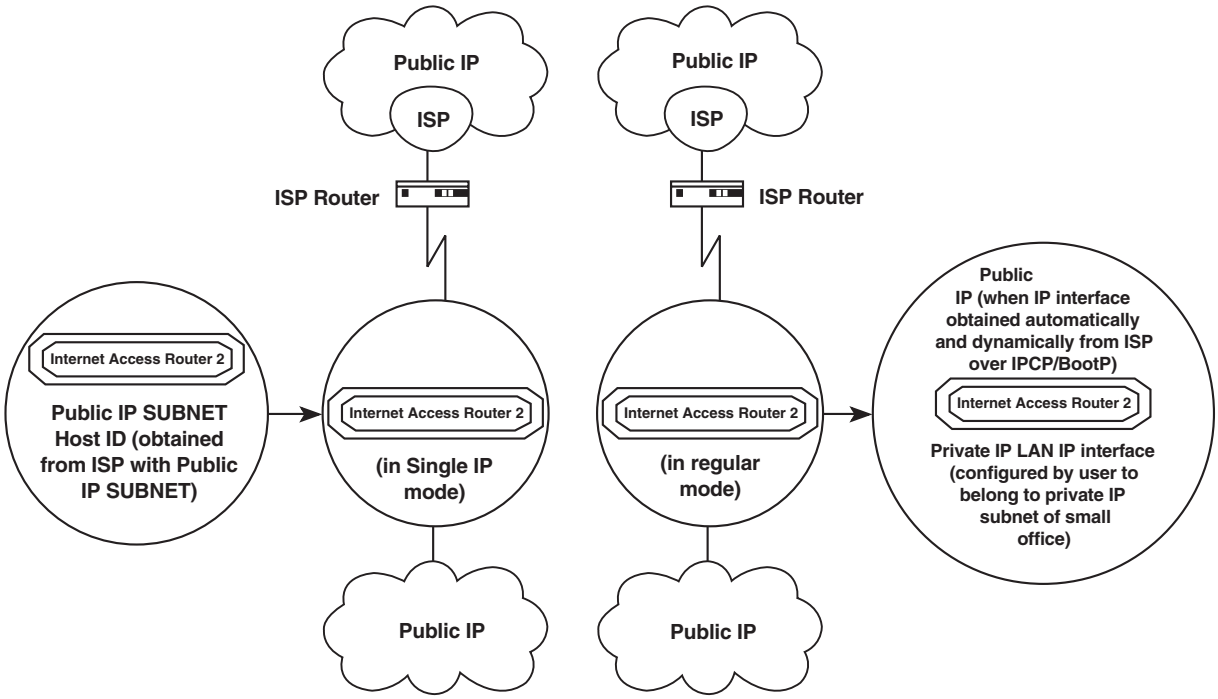


Figure 5-4. Choosing LAN IP addresses in Single IP (left) or regular routing mode (right).

5.1.2.C LAN IP Mask

Select this parameter to enter the IP mask. The mask is configured automatically from the IP-address class. If you want to change the default mask, enter a new mask. For example, the IP mask is usually 255.255.255.0. A mask like this would allow 254 hosts on the LAN. If you want to create a subnet which allows 6 users, including the IAR2, configure the mask as 225.225.225.248 on the IAR2 and each host that is included on the subnet. Refer to Figure 5-5 below.

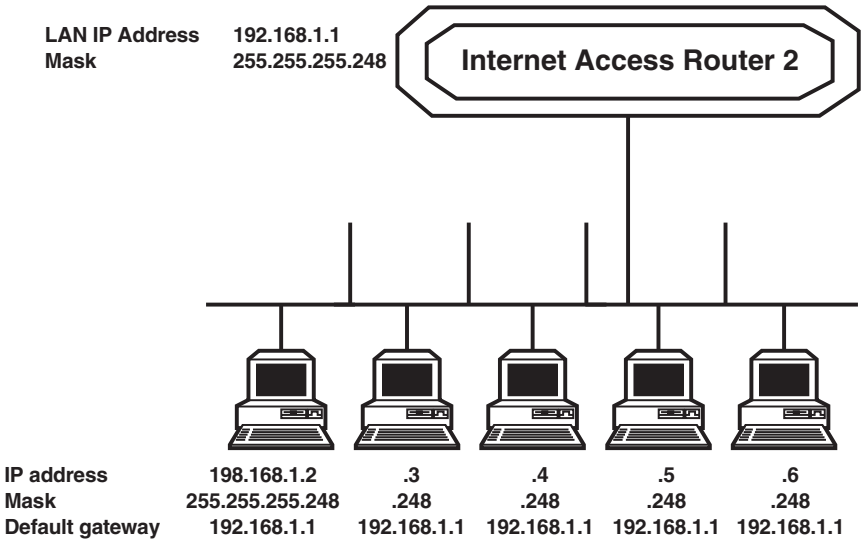


Figure 5-5. Setting up the IP mask.

5.1.2.D Default Gateway Setting

Select this parameter to set the default gateway settings. The default gateway is the address to which frames are sent if no other address is defined in the routing table.

The default gateway can be an IP address or a WAN interface. If you choose to use an IP address, enter the address of the router which will deliver the frames. Specifying an IP address for the default gateway is done with shared media, such as the LAN interface.

If you choose to use a WAN interface, the connection to the router is point-to-point. Choose by interface and enter the interface or, for Frame Relay, the DLCI number.

NOTE

It is very important to obtain the correct parameters from the system administrator or ISP. The most common problem when establishing an IP connection is incorrect configuration of the IP parameters and Default Gateway. Do *not* try to guess these parameters.

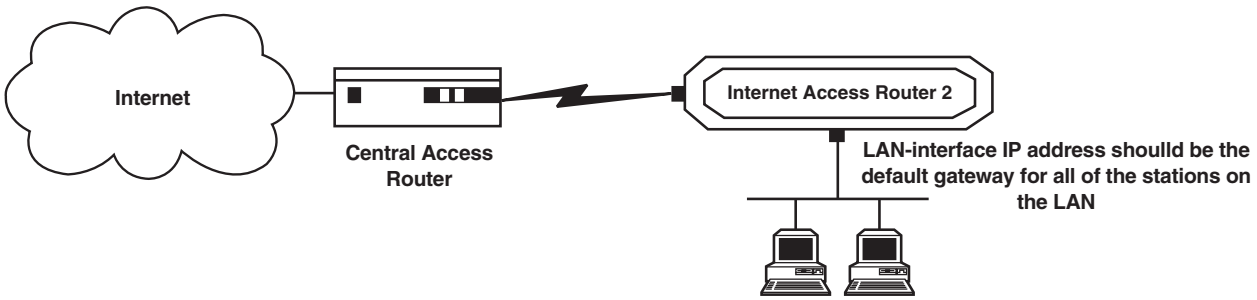


Figure 5-6. Default gateway.

5.2 Settings for E1 and T1 Models

```
    QUICK SETUP
    -----------
WARNING: This device automatically exits to Operational
         Messages 10 minutes after last keyboard action without
         saving parameters

'ENTER' - Accept parameter , 'SPACE' - Change parameter.

WAN interface #1 - T1
 Connection type: [Uplink  ]
 Link mode: [Frame Relay    ]
 Routing: [IP ROUTER    ], Protocol: [RFC 1490  ]
 Number of DLCIs to configure: 1
 Enter DLCI id number (16-991): 100
 WAN IP address: 10.1.1.2, enter new : 10.1.1.2
 WAN IP mask   : 255.255.255.252, enter new: 255.255.255.252
 Do you want to enable SINGLE IP option (Y/N)? : [N]
 Do you want to configure the T1 Interface parameters (Y/N)?:[N]
 Host IP setup:
 LAN IP address : 192.168.1.1, enter new : 192.168.1.1
 LAN IP mask    : 255.255.255.000, enter new : 255.255.255.000
 Default gateway setting by: [Interface ]
 Default gateway interface: 1 DLCI: 100


Saving the changes might cause RESET the unit.
Do you want to save QUICK SETUP (Y/N) ? Y
```

Figure 5-7. Quick Setup screen for -UT1 model (T1 WAN link + 1 LAN).

The fields in the Quick Setup screens are described in the following subsections.

5.2.1 WAN Interface

Connection Type
Toggle this parameter to set the connection type, just as described in **Section 5.1.1.A**.

Link Mode
Toggle this parameter to set the link mode, just as described in **Section 5.1.1.B**.

Routing
Toggle this parameter to set the routing option, just as described in **Section 5.1.1.C**.

Protocol
Toggle this parameter to set the protocol, just as described in **Section 5.1.1.D**.

DLCI
Toggle this parameter to set the DLCI address, just as described in **Section 5.1.1.F**.

IP Address
Toggle this parameter to set the IP address, just as described in **Section 5.1.1.G**.

IP Mask
Toggle this parameter to set the IP mask, just as described in **Section 5.1.1.H**.

Single IP Option
Toggle this parameter to set this option, just as described in **Section 5.1.1.J**.

E1/T1 Parameters
Toggle this parameter to determine if the hardware interface detected is E1 or T1. When an E1 or T1 interface is detected, the IAR2 enables the user to setup the E1/T1 parameters. These parameters are described in **Chapter 7**.

5.2.2 Host IP

LAN IP Address
Toggle this parameter to set the LAN IP address, just as described in **Section 5.1.2.B**.

LAN IP Mask
Toggle this parameter to set the LAN IP Mask, just as described in **Section 5.1.2.C**.

Default Gateway Setting
Toggle this parameter to set the Default Gateway, just as described in **Section 5.1.2.D**.

5.3 How to Proceed

Depending on what you need to do with the Internet Access Router 2, you'll want to go from here to one of the next four chapters of this manual:

- If you want to prevent unauthorized users from trying to manage your IAR2 or trying to get into your LAN, refer to **Chapter 6**.
- If you want to change the IAR2's configuration parameters to perform advanced configuration operations, or if you want to reset the IAR2 or download firmware to it, refer to **Chapter 7**.
- If you want to view the configuration screens and information on interface connections, routing tables, and statistics, refer to **Chapter 8**.
- If you want to verify WAN and LAN connectivity, refer to **Chapter 9**.

6. The Security Setup Menu

Topics covered in this chapter include:

- Enabling Telnet access.
- Enabling SMNP access.
- Enabling/disabling the Solid Firewall.
- Configuring Network Address Translation (NAT).

6.1 Overview

The Security Setup menu, shown in Figure 6-1 below, allows you to control access to the Internet Access Router 2 and the attached LAN(s). IAR2 is protected against access by unauthorized users by disabling access via SNMP and TELNET. The Solid Firewall is used to protect the LAN against undesired entry.

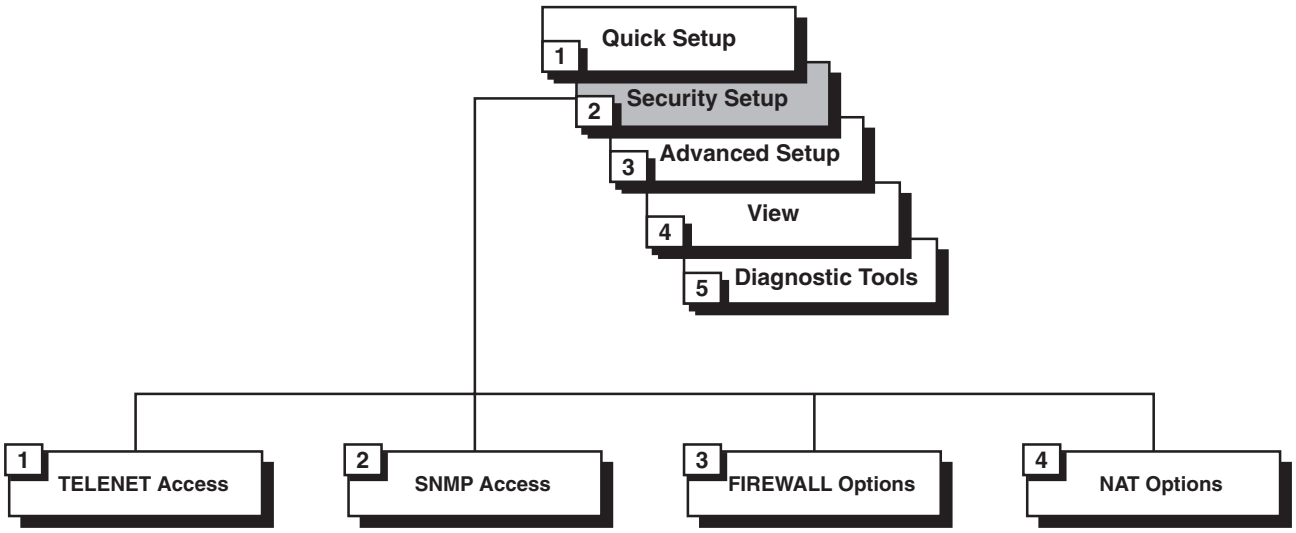


Figure 6-1. Outline of the Security Setup menu.

To access the Security Setup menu, press **2** at the Main menu. The following screen appears:

```
        SECURITY SETUP  ( Device name - IAR2 )


    1.  TELNET access     -  Disabled
    2.  SNMP access       -  Disabled
    3.  FIREWALL options  -  Disabled

    ESC - Return to previous menu


    Choose one of the above:
```

Figure 6-2. Security Setup screen.

The Security Setup options are described in the following subsections.

6.2 Enabling TELNET Access

The Internet Access Router 2 supports TELNET. This allows IAR2 to be configured and controlled over the WAN and LAN using TCP/IP. Access to TELNET requires authentication by the IAR2, using a username and password. By default, TELNET access to IAR2 is disabled to prevent changes being made to the unit's configuration parameters.

To enable TELNET access:

1. From the Main menu, select option **2**, Security Setup.
2. From the Security Setup menu, select option **1**, TELNET access. This screen appears:

```
   TELNET access setup

'ENTER' - Accept parameter , 'SPACE' - Change parameter .

Do you want to permit TELNET management of the device? [ N ]Y

TELNET user name : lan
Do you want to change TELNET password ? [ N ]Y
Current password : ***
Enter new password : ***
Enter new password verification : ***

Do you want to save TELNET parameters (Y/N) ? Y
```

3. Toggle "Do you want to permit TELNET management?" to **Y**.
4. Press **ENTER**.
5. Follow the on-screen instructions to allocate a user name and password. Save the new setup.

IAR2 can now be accessed using your TELNET username and password.

6.3 Enabling SNMP Access

By default, access to the Internet Access Router 2 via SNMP is disabled. Blocking SNMP access prevents changes being made to the unit's configuration parameters. Enabling SNMP access prompts the user to define SNMP management parameters.

To enable SNMP access:

1. From the Main menu, select option **2**, Security Setup.
2. From the Security Setup menu, select option **2**, SNMP access. This screen appears:

```
   SNMP access setup

'ENTER' - Accept parameter , 'SPACE' - Change parameter .

 Do you want to permit SNMP management of the device ? [ N ]Y

  SNMP read community : public
  SNMP write community : private
  SNMP trap community : public

  Do you want to save SNMP parameters (Y/N) ? Y
```

3. Toggle "Do you want to permit SNMP management?" to **Y**.
4. Press **ENTER**.
5. Enter the read, write and trap communities. Save the new setup.

The IAR2 can now be accessed for SNMP operation using the appropriate communities.

6.4 Enabling/Disabling the Solid Firewall

Solid Firewall, when enabled, prevents all access from the WAN or Internet/intranet into the small-office LAN(s) attached to the Internet Access Router 2. Outgoing traffic from the LAN will be forwarded to the WAN, but incoming traffic from the WAN—except for those applications that are enabled via the Firewall Forward Application List (such as WWW, FTP, e-mail servers, etc.)—will be blocked from entering the LAN.

By default, the Solid Firewall is disabled. In Single IP mode, Solid Firewall is always enabled by default and cannot be disabled. To enable the Solid Firewall feature (in regular router mode):

1. From the Main menu, select option **2**, Security Setup.
2. From the Security Setup menu, select option **3**, Firewall Options. This screen appears:

```
FIREWALL options setup


Enabling FIREWALL will forward outgoing sessions
from LAN to WAN and block incoming sessions from
entering the LAN except for applications that are
enabled by the FIREWALL FORWARD APPLICATION LIST.

Do you want to enable firewall options ? [ N ]Y
Enter link from which to be protected by FIREWALL: 1
```

3. Toggle "Do you want to enable firewall options?" to **Y** and press ENTER to enable the Solid Firewall and open the Firewall Forward Application List screen.
4. Press ESC and save the Firewall setup to block all incoming traffic from the WAN.

To enable a specific application to enter the Solid Firewall (both in regular router and Single IP modes):

1. In the Firewall Forward Application List screen shown here, press **A** to add an application.

```
      FIREWALL FORWARD APPLICATION LIST  ( Device name - IAR2 )

      List of applications which may pass the FIREWALL.

   APPLICATION             ADVANCED SETUP   IP ADDRESS

 1. TELNET server               NO          192.168.182.040
 2. PING request                NO          192.168.182.040

Telnet server, Ping request, DNS server, E_Mail POP3, E-Mail SMTP,
FTP server, WWW server, TFTP server, SNMP, User defined
Application type: [E-MAIL POP3   ]   [Default ] Advanced
```

2. To select a different application, use the SPACE bar to toggle to the desired application. When the application name appears, press **ENTER**. The word `DEFAULT` appears.
3. If a specific application has a specific IP destination on the LAN, press ENTER and when DEFAULT appears, type the IP destination address.

4. The advanced option includes the following possibilities for forwarding an IP session to the secured LAN:

```
Host IP address interval: [SINGLE  ]
Host IP Address: 192.168.182.39
Guest IP address interval: [INTERVAL ]
Guest start IP Address: 192.168.182.30
Guest end IP Address: 192.168.182.40
Host port interval: [SINGLE  ]
Host port: 110
Guest port interval: [ALL     ]
Frame type: [TCP ]
```

Select Single, All or Interval and type the IP address for each of these options:

- Host IP address interval - range of destination addresses on the LAN (only one address for Single IP).
- Guest IP address interval - range of source addresses in the Internet or intranet .
- Host port interval - range of UDP or TCP destination ports of the applications.
- Guest port - range of UDP or TCP source ports of the applications.
- Frame type - UDP, TCP, or ICMP protocol.

5. Press ESC and save the Firewall setup.

NOTES

In Single IP mode, for each application, only one FTP server can be used. The FTP server is represented by the Single IP address.

Incoming traffic from the WAN should be sent to the Single IP address. IAR2 forwards the application to the destination address on the LAN, as listed in the Firewall Forward Application List.

6.5 Enabling the NAT Option (Single IP Mode Only)

NOTE

NAT should be fully implemented in future software revisions. At the time of this writing, however, the NAT menu might not be available or active in some IAR2 units.

Ordinarily the Internet Access Router 2, when it's operating in Single IP mode, will automatically detect attached devices and build its own network-address translation (NAT) table based on the devices' IP addresses and the IP address(es), either statically or dynamically allocated, that it receives across the WAN link(s). However, if you need to make sure that certain static addresses are always translated the same way—if, for example, you make several different WAN connections at different times during the day to different corporate facilities with different security/access levels—you can enable the NAT option (if it is available and active in your unit) and build your own "NAT Static List" of static translations:

1. From the Main menu, select option **2**, Security Setup.
2. From the Security Setup menu, select option **4**, NAT Options. You are prompted with the message: `Do you want to enable the NAT option?` Press **Y**; a screen headed "NAT Static List" appears. Press **A** to add an entry; type the "Real IP" address (the static address received across the WAN) in that left-hand column, then type the "Translated IP" addresses (the IP addresses you use internally on the LAN) in that right-hand column. (To delete an entry later, press **D** instead of **A**.)
3. Press ESC and save the NAT-list setup for translation control.

7. The Advanced Menu

The Advanced Menu, shown in Figure 7-1 below, contains the majority of the Internet Access Router 2's configuration parameters and their current values. These parameters can be used to configure the IAR2 in great detail. You can change these parameters and to perform advanced configuration operations not available through the Quick Setup menu. Resetting the IAR2 and downloading firmware are also performed via the Advanced Menu.

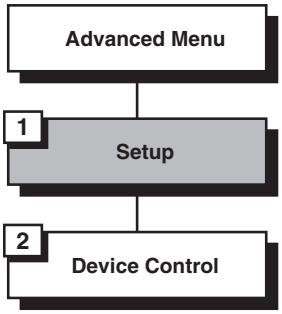


Figure 7-1. Outline of the Advanced menu.

7.1 Overview of the Advanced Menu

To access the Advanced menu, press **3** at the Main menu. This screen appears:

```
      ADVANCED  MENU  ( Device name - IAR2  )
      --------------

  1.  Setup
  2.  Device control

  ESC - Return to previous menu

  Choose one of the above:
```

- Setup - Select this option to modify setup parameters. See **Section 7.2** for an overview of this menu and **Sections 7.3** through **7.8** for descriptions of its submenus and their options.
- Device Control - Select this option to download the software, perform reset operations, and choose a terminal type. See **Section 7.9** for descriptions of this menu, its submenus, and their options.

7.2 Overview of the Setup Menu

To access the Setup menu, shown in Figure 7-2 below, press **3** at the Main menu, then press **1** at the Advanced menu. This screen appears:

```
      SETUP  ( Device name - IAR2  )
      -----

  1.  Host parameters
  2.  Routing
  3.  Interface parameters
  4.  Access control (Security)
  5.  WAN economy
  6.  Factory default options

  ESC - Return to previous menu

  Choose one of the above:
```

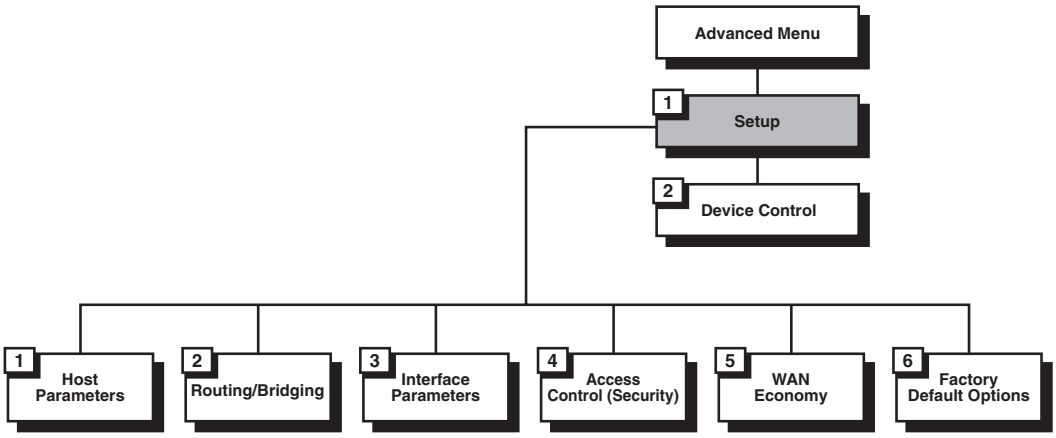


Figure 7-2. Outline of the Setup menu.

The Setup menu's options are:

- Host Parameters - Select this option to enter reference information about the IAR2, the IP Host, the SNMP agent, and TFTP. See **Section 7.3**.
- Routing - Select this option to enter IAR2 routing information. See **Section 7.4**.
- Interface Parameters - Select this option to set link, Frame Relay, or E1/T1 parameters. See **Section 7.5**.
- Access Control (Security) - Select this option to perform security operations. See **Section 7.6**.
- WAN Economy - Select this option to reduce traffic over the WAN and to keep the link up only when necessary. See **Section 7.7**.
- Factory Default Options - Select this option to return settings to the factory default. See **Section 7.8**.

7.3 The Host Parameters Menu

To access the Host Parameters menu, shown in Figure 7-3 below, press **3** at the Main menu, then press **1** at the Advanced menu, then press **1** in the Setup menu. This screen appears:

```
      HOST PARAMETERS  ( Device name - IAR2  )
      --------------

  1.  Device ID
  2.  IP host
  3.  SNMP manager table
  4.  TFTP
  5.  RADIUS

  ESC - Return to previous menu

  Choose one of the above:
```

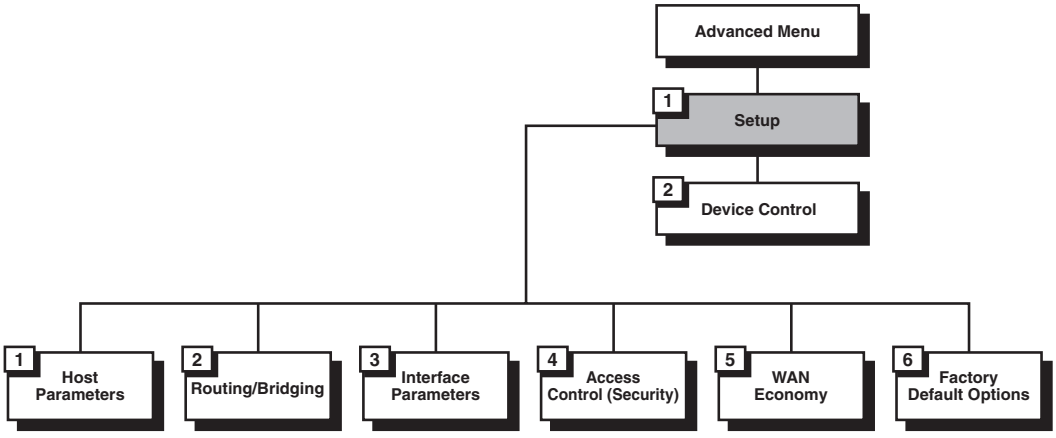


Figure 7-3. Outline of the Setup menu.

The options in the Host Parameters menu are described in the following subsections.

7.3.1 Device ID

Select this option to view and/or modify these "device identity" parameters:

Device Name
Select this parameter to assign an arbitrary name to the IAR2 for identification by the system manager; for example, "accounting."

Contact Person
Select this parameter to enter the name of the person to be contacted with matters pertaining to the system; for example, "John Doe."

System Location
Select this parameter to enter the physical location of the device; for example, "Building 3 Floor 4."

MAC Address
Select this parameter to assign a MAC address locally. This allows you additional control of the devices in the LAN. The IAR2 can be used with the burned-in (default) address provided by the manufacturer or with athe locally administered address; for example, "40 20 2D 16 12 34". Locally administered addresses are very useful for managing large networks.

7.3.2 IP Host

Select this option to configure the Internet Access Router 2's IP parameters.

NOTE

It is very important to obtain the correct parameters from the system administrator or ISP. The most common problem when establishing an IP connection is incorrect configuration of the IP parameters and default gateway. Do *not* try to guess these parameters.

7.3.2.A IP Address
Every device on a TCP/IP network must have an address to identify it. The IP address is a value consisting of the network address and the host address on that network. The value assigned to a network depends on the number of computers on that network.

The IP address is a 32-bit number. The number is made up of 4 parts, with each part consisting of 3 digits. One part of the address identifies the network and another part of the address identifies the host. Which numbers in the address identify the host is dependent on the address class.

There are 5 classes of IP addresses. Each class represents a network having a certain number of computers. For example, a Class C address is given to a network having up to 255 computers. Table 7-1 below gives the ranges for different classes of IP addresses.

Table 7-1. IP Address Classes

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

The numbers in each part of the code are translated into binary. The binary code identifies the network and the host.

IP addresses are assigned by Network Solutions, Inc. Network Solutions also assigns the network ID. Host IDs are assigned by the network administrator.

7.3.2.B IP Mask

A subnet is a portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 133.100.100. would be part of the same subnet. An IP mask allows filtering of IP addresses on a subnet.

The IP mask is a unique 4-byte (32-bit) value that allows the recipient of IP packets to distinguish between different host IDs. When an IP address is configured, the IP mask is automatically configured according to Table 7-2 below, but you can edit the mask as you see fit.

Table 7-2 IP Masks

IP Network Class	IP Address Range	Default IP Mask
A	0.0.0.0 to 127.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	255.255.255.225

7.3.2.C Default Gateway

The default gateway is the address to which frames are sent if no other address is defined in the routing table.

The default gateway can be an IP address or a WAN interface. If you choose an IP address as your gateway (as is often done with shared media such as the LAN interface), enter the address of the router which will deliver the frames. If you choose a WAN interface as your gateway, the connection to the router is point-to-point. Making very sure to select the correct interface, enter the interface/DLCI number.

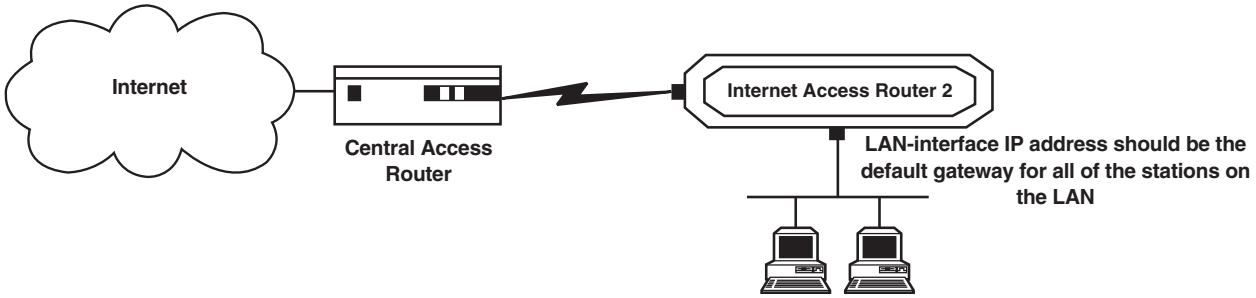


Figure 7-4. A default gateway.

7.3.3 SNMP Manager Table

Select this option to add, clear or delete parameters from the manager table. The manager table lists the SNMP manager's IP addresses and masks.

Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP to access management information (such as packets per second and network-error rates), network administrators can more easily manage network performance and find and solve network problems.

7.3.4 TFTP (Trivial File Transfer Protocol)

TFTP is a file-transfer protocol used for downloading boot code to diskless workstations, as shown in Figure 7-5 below. It's used in a server designated as the TFTP server. The server needs to provide concurrency to allow multiple users to boot up simultaneously. To do this, TFTP creates a UDP port for each client. By creating a UDP port, the different clients' input datagrams can be demultiplexed by the server's UDP module. Demultiplexing in the module increases the server efficiency.

However, one characteristic of TFTP is that it is not secure. There is no password or firewall associated with TFTP. Anyone with the IP address of the TFTP server can enter the server and download files. Security can be provided by creating a directory which contains only those files which you want to be downloaded. This prevents access to any other files.

Select this option to configure the following parameters in a TFTP server:

File Server IP Address
Select this parameter to enter the IP address of the TFTP server; for example, "192.168.10.11".

File Name
Select this parameter to enter the name and path of the file to be transferred; for example, "c:\booting\boot.exe".

Retransmitting Timeout
Select this parameter to enter the amount of time that is allowed to pass before a file is retransmitted; for example, 30 seconds.

Total Timeout
Select this parameter to enter the amount of time the IAR2 should wait for an acknowledgment from the TFTP server; for example, 60 seconds.

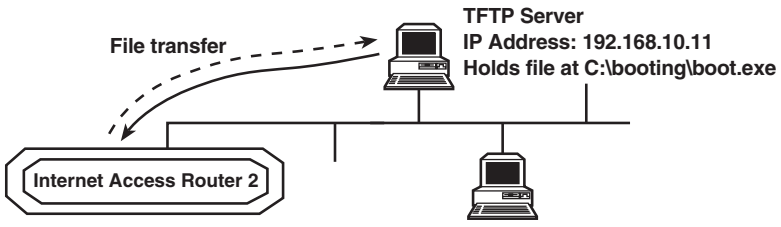


Figure 7-5. Transfer to and from a TFTP server.

7.3.5 RADIUS Authentication and Billing

RADIUS (Remote Authentication Dial-In User Service) is a client/server security protocol. Security information is stored in a central location, known as the RADIUS server. RADIUS clients, such as the IAR2, communicate with the RADIUS server to authenticate users, as shown in Figure 7-6 below. Although the term RADIUS refers to the network protocol that the client and server use to communicate, it is often used to refer to the entire client/server system.

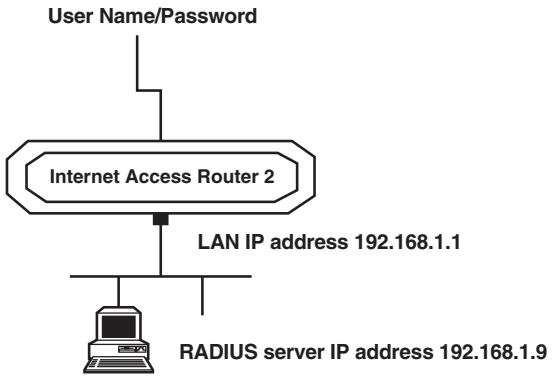


Figure 7-6. Setting up the RADIUS server.

The three main functions of RADIUS are authentication, authorization, and accounting. To perform these functions, you must configure the following parameters:

RADIUS Server IP Address
Select this parameter to enter the IP address of the RADIUS server; for example, 192.168.1.9.

RADIUS Authenticator
Select this parameter to enter the shared secret. The shared secret is a password used by RADIUS to authenticate the client. It is important to remember that the client is the IAR2; make sure to use the same value in the IAR2 and the RADIUS server. The user is not requested to supply the shared secret.

RADIUS Accounting System Type
Select this parameter to track when the link is up and when it's down. This information is often used for billing purposes. Use the space bar to toggle between **ON** and **OFF**.

RADIUS Authentication Port
Select the UDP port number to be used for the RADIUS authentication application. Confirm that the same value is defined in the RADIUS server.

RADIUS Accounting Port
Select the UDP port number to be used by the RADIUS accounting application. Confirm that the same value is defined in the RADIUS server.

Retransmission Timeout
Select this parameter to enter the maximum time the IAR2 will wait for a response from the RADIUS server; for example, 30 seconds.

Total Timeout
Select this parameter to enter the total time the IAR2 will try to communicate with the RADIUS server.

7.4 The Routing/Bridging Menu

To access the Routing/Bridging menu, shown in Figure 7-7 on the next page, press **3** at the Main menu, then press **1** at the Advanced menu, then press **2** in the Setup menu. This screen appears:

```
    ROUTING/BRIDGING ( Device name - IAR2  )
    ----------------

         Link 1 - IP & IPX ROUTER  PPP


    Setup Menu
    ----------
1. Interface Routing Bridging Mode
2. Static stations & nets
3. IP routing settings
4. IPX routing settings
5. Station ageing (minutes): 30

 ESC - Return to previous menu

 Choose one of the above :
```

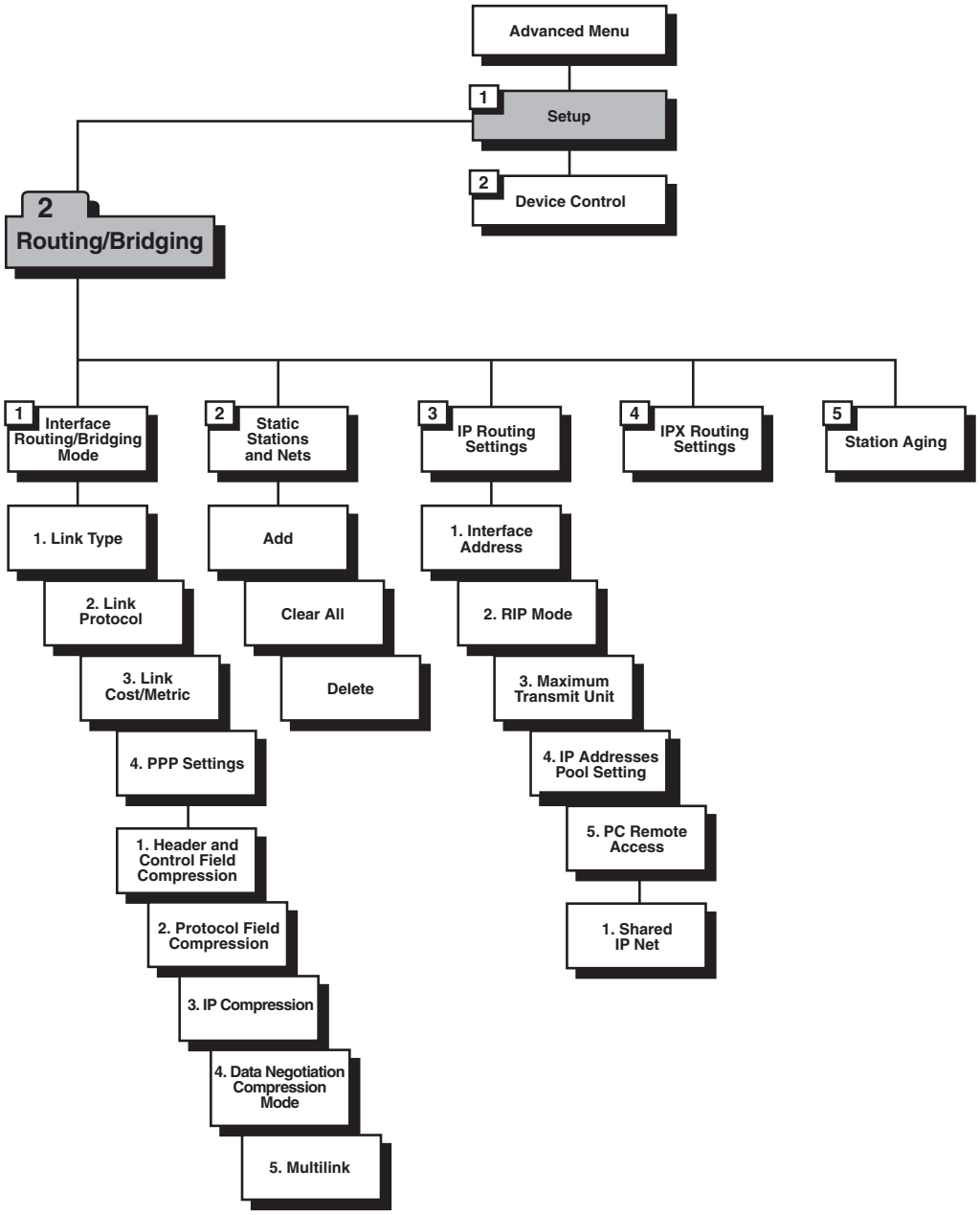


Figure 7-7. Outline of the Routing/Bridging menu.

7.4.1 Interface Routing Bridging Mode

When you press **1** at the Routing/Bridging menu, you will be prompted with a message like this:

```
Choose Interface number
(link number for Link, L for LAN 1, S for LAN 2) :
```

When you select a LAN port, a screen like this appears (see **Section 7.4.1.A**):

```
    TYPE: LAN 1  ( Device name - IAR2  )
    -----------

1. Bridge:     [Enabled]
2. IP Router:  [Disabled]
3. IPX Router: [Disabled]

 ESC - Return to previous menu

 Choose one of the above :
```

When you select a LAN port, this screen appears (see **Sections 7.4.1.A**, **74.1.B**, and **7.4.1.C**):

```
    ROUTING/BRIDGING MODE: LINK 1  ( Device name - IAR2  )
    ----------------------------

1. Link type        - IP Router
2. Link protocol    - PPP
3. PPP settings

 ESC - Return to previous menu

 Choose one of the above :
```

7.4.1.A LAN Routing/Bridging (for LAN on Dual-LAN Models) or Link Type (for WAN Link)

Select one of the Internet Access Router 2's LAN ports when prompted to do so after selecting "Interface Routing Bridging Mode," or select a Link port and then select "Link type" at the Routing/Bridging Mode menu, to assign the link type for each interface. Use the space bar to toggle between **Bridge**, **IP router**, **IPX router**, or any combination of these types, as shown in Figure 7-8 below.

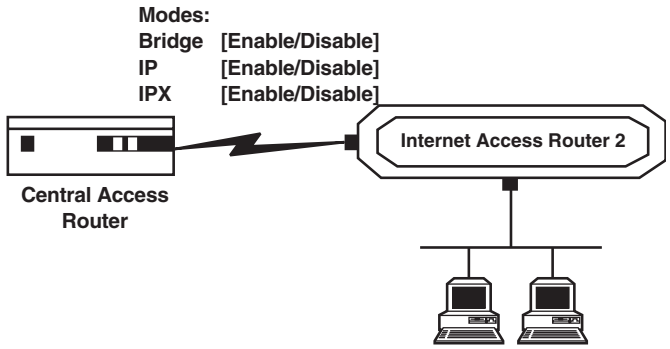


Figure 7-8. Link-routing types.

The IAR2 uses a standard bridging setup, as shown in Figure 7-9 below. Bridging allows one IAR2 to be set up opposite another IAR2 or any other standard bridge. Figure 6-9 shows two IAR2s set up opposite each other, interconnecting two LANs to an extended LAN.

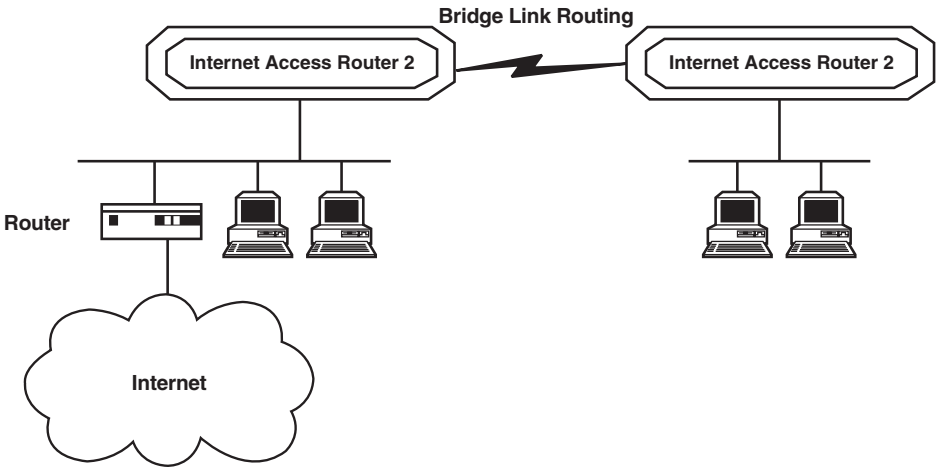


Figure 7-9. Standard bridging application.

7.4.1.C Link Protocol

Select this parameter to assign the link protocol. Available protocols for synchronous links are **PPP** and **Native**, as shown in Figure 7-10 below. The "native" setting uses HDLC—for protocol packets when the IAR2 is configured as a router, for MAC frames when the IAR2 is configured as a bridge.

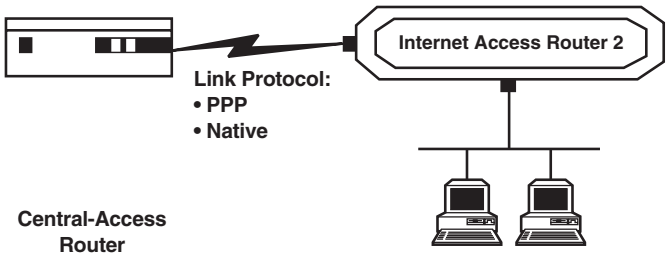


Figure 7-10. Link protocols.

7.4.1.D Link Cost/Metric

Select this parameter to assign a cost to each WAN link for routing purposes.

Metrics are hop counts. Hop counts are the number of routers through which a packet must go to get to its destination. Adjacent interfaces have a hop count of 1. If a packet must go through 2 routers to get to its destination, the hop count is 2. The higher the hop count, the longer the route.

A router such as the IAR2 will automatically send packets using the lowest possible metric. The IAR2 will send the packets through an interface with a higher metric only if it detects that a router somehere along the optimum route is not functioning.

7.4.1.E PPP Settings

This option is only available when the Link Protocol (see the previous page) is set to PPP.

The PPP Setting screen has the following options:

- **Header and Control Field Compression -** This parameter is used for troubleshooting only. Change the Header and Control Field Compression setting only if there is a problem with PPP negotiation (if you notice initial-connection problems, etc.).
- **Protocol Field Compression -** This parameter is used for troubleshooting only. Change the Protocol Field Compression setting only if there is a problem with PPP negotiation (if you notice initial-connection problems, etc.).
- **IP Compression -** This parameter activates Van Jacobson TCP Header Compression on a specified link. PPP is normally used on devices with low bandwidths, such as modems. To quicken the transmission, certain parts of the data packets can be compressed. In Van Jacobson TCP Header Compression, the packet header is compressed. Every IP data packet contains a header. The header contains the source address, destination address and other information. Because PPP is used for point-to-point transmissions, both the local and remote devices must have Van Jacobson TCP Header Compression enabled for compression to be performed. To verify that Van Jacobson TCP Header Compression is being performed, open the Interface Connections Screen (refer to **Chapter 8**).
- **Data Compression Negotiation Mode -** The IAR2 supports IP and IPX data compression according to RFC 1974 using the STAC Compression Method, as shown in Figure 7-11 on the next page. The following modes are supported:

  – Disabled.

  – No History.

  – LCB.

  – Sequence.

  – Extended.

  When the IAR2 attempts to negotiate with another device, a message is sent stating in which mode the data will be sent. If the mode is acceptable to the receiving unit, data transmission begins. If the mode is not acceptable (meaning that the second unit does not support this mode), another mode is tried, until an acceptable mode is found. This process is called auto-negotiation. When you choose a mode with this option, you are choosing the first mode that the IAR2 will use during auto-negotiation. Do not change this parameter unless a problem arises with autonegotiation (data transfers take longer, etc.). If a problem does arise, refer to the manual of the device the IAR2 is negotiating with to find out which mode(s) that device is looking for.

For example, in Figure 7-11 below, the IAR2's data compression is set to LCB. In the remote unit the data compression is set to Extended. Messages are sent between the two units, until a common data compression mode is found.

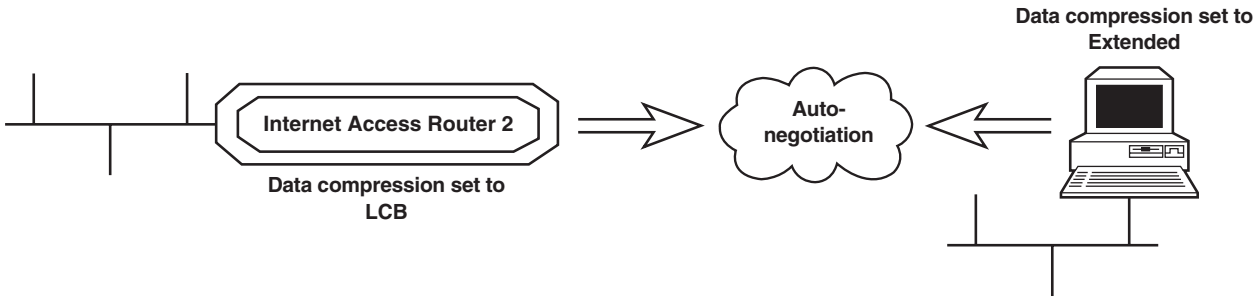


Figure 7-11. Auto-negotiation.

- **Multilink -** This parameter is included to support future capabilities of the IAR2. It has no function in current models; do not change its setting.

7.4.2 Static Stations and Nets

When you press **2** at the Routing/Bridging menu, a screen like this appears:

```
STATIC STATIONS AND NETS (MAC, IP, IPX)  ( Device name - IAR2)
---------------------------------------

1. IP  - 192.168.182.056  mask-255.255.255.248

2. IPX - 25490880



   A - Add , C - Clear all , D - Delete
   ESC - Return to previous menu.
```

Select this option to add, delete, or clear static stations or nets/subnets from the network. When setting a static net (subnet) for a link, you define all nets over which the link will perform routing. You can set more than one routing net for the same link. Also, more than one link can perform routing to the same net (in this case, the device will learn the IP addresses of the stations connected to each link and will route the frames to the appropriate link according to this information).

When setting a static station for a link, you define which stations are set in the remote net. A station can be set only once. By setting a static station, the device can transmit frames to the station even though it hasn't been learned yet (that is, even though the station hasn't sent any frames yet). Select this parameter to add, delete, or clear static entries in the IP/IPX Routing table or Bridge Routing table. If the Internet Access Router 2 is attached to more than one LAN, then select this parameter for each LAN interface, if necessary. Static entries are not removed from the routing tables by the Ageing Mechanism. When you add them, static entries can be defined in four ways:

- **MAC Station -** MAC Station defines a single static entry in the Bridge routing table. The entry is a single MAC Address (6 bytes) entered in hexadecimal format, and the interface that is the frame pathway.
- **IP Net -** IP Net defines a network as the destination. IP Net consists of 2 parts:
  - *Frame pathway* - The frame pathway is specified either as an interface (i.e. port) number or as Next Hop IP address. In Next Hop IP the frames are sent to another router; from there they will be sent to their final destination, as shown in Figure 7-12 on the next page.
  - *Destination* - The destination is defined by entering the subnet IP address and IP mask. For example, 192.168.182.32 is a subnet IP address and 255.255.255.240 is the IP mask.
- **IP Station -** IP Station defines a single host as the destination. IP Station consists of 2 parts:
  - *Frame pathway* - The frame pathway is specified as in IP Net, above.
  - *Destination* - The destination is defined by entering the host IP address; for example, "192.168.182.11".
- **IPX Net -** IPX Net is used for IPX routing. Define the IPX Net in hexadecimal, then the interface number ("1" for Link 1, "2" [on sublink units only] for Link 2).

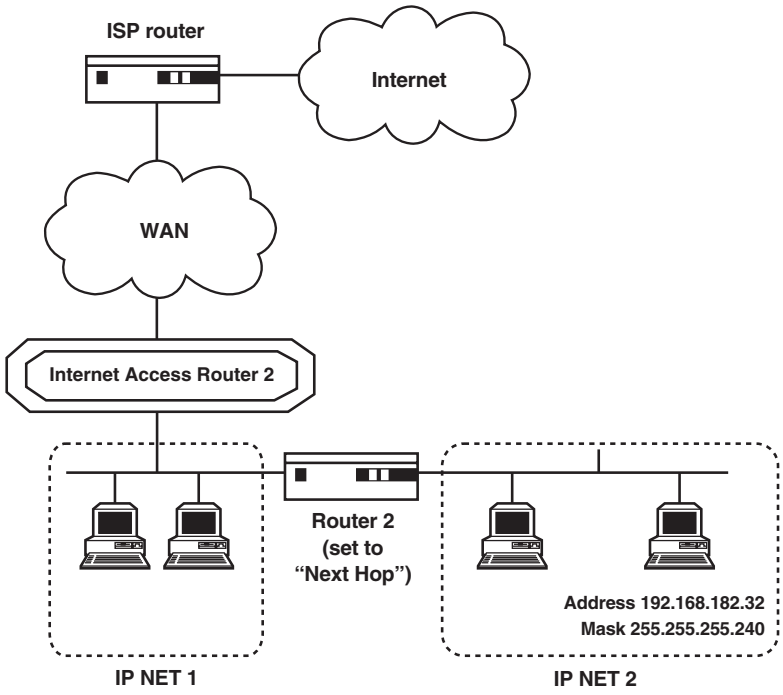


Figure 7-12. The IAR2 used in an application with another router set to "Next Hop."

7.4.3 IP Routing Settings

When you press **3** at the Routing/Bridging menu, this screen appears:

```
IP ROUTING SETTINGS ( Device name - IAR2  )
-------------------

1. Interface address
2. RIP mode
3. Maximum transmit unit
4. IP address pool setting
5. PC remote access

 ESC - Return to previous menu

 Choose one of the above:
```

7.4.3.A Interface Address

Select this parameter to enter an IP address for one or both of a unit's WAN interfaces and one or more IP addresses for one or both of its LAN interfaces. Multiple IP addresses on the LAN are useful in environments with multiple IP nets on the LAN (refer to Figure 7-13 below). If your IAR2 has two LAN interfaces, use this screen to enter one or more IP addresses for the second LAN. Depending on how you set the WAN IP address, the IAR2 will be configured for one of these operating modes:

- **Regular Router Mode (Unnumbered):** Set WAN IP Address to 0.0.0.0 (with Single IP OFF).
- **Regular Router Mode (Numbered):** Set WAN IP Address to a.b.c.d (with Single IP OFF).
- **Single IP Mode (Fixed IP address):** Set WAN IP Address to a.b.c.d (with Single IP ON).
- **Single IP Mode (Dynamic IP address):** Set WAN IP Address to 0.0.0.0 (with Single IP ON; IP address is received dynamically over the WAN using IPCP).

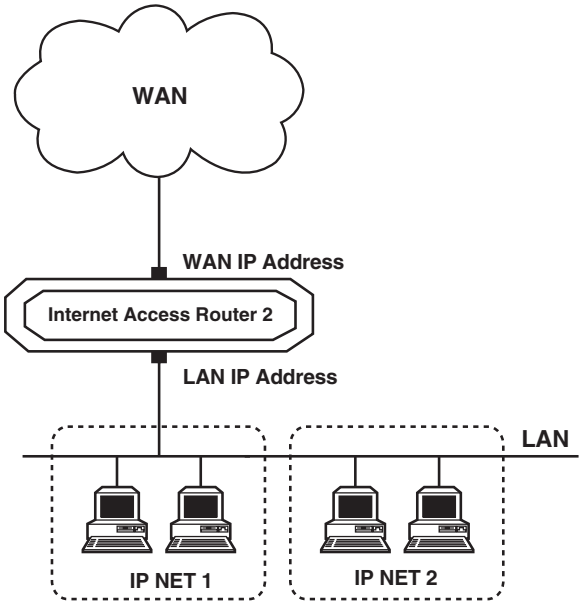


Figure 7-13. WAN and LAN interface addresses.

7.4.3.B RIP Mode

Select this parameter to set the type of RIP to be sent for each of the Internet Access Router 2's interface (LANs and WANs). Use the space bar to toggle **RIP1**, **RIP2**, **RIP1+2**, or **No RIP** for each interface.

RIP stands for Routing Information Protocol. Every router has a routing table which directs packets. A router uses the routing table to send the packets through a designated gateway (if the packet was sent to another network) or directly to a host. The routing table is built when the host is booted up. RIP sends a request to all active interfaces, asking for the others' routing table. Using the information received, the host builds its own routing table in which the packet destinations are entered. Refer to Figure 7-14 below.

By sending requests for information, RIP both builds the table and updates the entries. RIP updates the table using the responses received every 30 seconds.

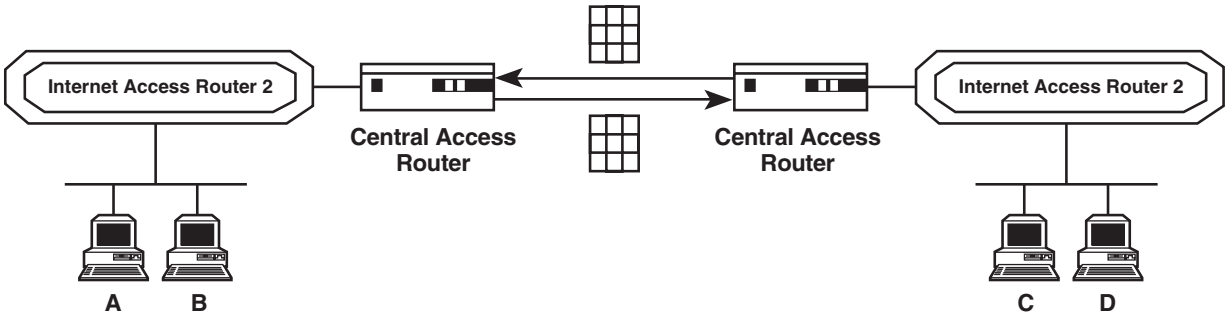


Figure 7-14. Routers exchanging routing tables.

7.4.3.C Maximum Transmit Unit

Select this parameter to set the maximum transmit unit (MTU) for IP fragmentation. The MTU must be set for each interface (LANs and WANs). If a frame is larger than the MTU, IP fragments the frame into smaller units.

7.4.3.D IP Address Pool Setting

Select this parameter to determine how the Internet Access Router 2 dynamically assigns IP addresses to connected workstations. The IAR2 can use any of the following mechanisms (or all of them simultaneously) to assign IP addresses dynamically to workstations:

- **IPCP Negotiations -** This is a mechanism where the remote router or a workstation connected to the IAR2 across a WAN link requests an IP address. This request is made by specifying zero for the IP address in the IPCP configure request (PPP).
- **BOOTP -** This is a method whereby another router or workstation sends an affirmation for an IP address. The IAR2 uses BOOTP to confirm the IP address by sending a BOOTP reply packet across a WAN link or an attached LAN. The IAR2 supports basic BOOTP options only.
- **DHCP -** This protocol is an extension to BOOTP and permits the IAR2 to supply not only an IP address but also additional parameters, such as Default Gateway, DNS server addresses etc. The IAR2 supplies these parameters to the client's workstation. In contrast to BOOTP, DHCP supplies these parameters on a temporary basis. When it's using DHCP, the IAR2 checks on the workstation periodically. If the workstation is not using the IP address, the address can be supplied to other workstations later.

7.4.3.E IP Address Pool

Select this option to define IP-address information. You can define up to five entries. Each entry contains the following parameters:

- **Low IP Address -** Defines the lower boundary of the IP-address range.
- **High IP Address -** Defines the upper boundary of the IP-address range.
- **IP Mask -** Defines the IP mask for the IP-address range.
- **Default Gateway -** This is the Default Gateway IP address for workstations which receive IP addresses from the range defined by the Low IP Address and High IP Address. The Default Gateway IP address must be within this IP address range (used by DHCP only).
- **Primary DNS -** This is the IP address of the DNS server which can be used by the workstation. The workstation receives an IP address from the range defined by the Low IP Address and High IP Address (for DHCP and IPCP).
- **Secondary DNS -** Additional DNS server address that is an alternative to the Primary DNS (for DHCP and IPCP).
- **Interface -** This interface determines which requests to the IP address can be accepted. You can determine the interface by toggling between **WAN**, **LAN**, and **ALL** (both WAN and LAN).

7.4.3.F PC Remote Access

Select this parameter to define the remote access. (This option is important if the IAR2 is going to be used as a remote access server for remote PCs accessing the LAN.) When you select it, this screen appears:

```
    PC Remote Access ( Device name - IAR2  )
    ----------------

1. Shared IP net - 192.168.1.1    mask - 255.255.255.240

 ESC - Return to previous menu

 Choose one of the above:
```

As you can see, “Shared IP Net” is the only parameter currently available in this menu. Select it to enter the Shared IP net address. The Shared IP net address is used by all remote workstations connecting to the remote access server on the WAN links.

7.4.4 IPX Routing Settings

When you press **4** at the Routing/Bridging menu, this screen appears:

```
IPX ROUTING SETTINGS (  Device name - IAR2   )
--------------------

1.  LAN IPX net for frame type 802.3        - 00000000
2.  LAN IPX net for frame type Ethernet II  - 00000000
3.  LAN IPX net for frame type 802.2        - 00000000
4.  LAN IPX net for frame type SNAP         - 00000000
5.  Dial-in IPX net                         - D2162747
6.  Autolearn of zero LAN IPX nets          - [Enable ]
7.  RIP/SAP mode

ESC - Return to previous menu

Choose one of the above:
```

Select this parameter to specify how the Internet Access Router 2 learns IPX Nets. IAR2 can learn IPX Nets in several ways:

- **LAN IPX Net for Frame Type -** Each of these parameters specifies the IPX Nets associated with a particular frame type. (Each of the frame types shown is supported by the IAR2's LAN port[s].) If the IAR2 is in Autolearn enable mode, then non-zero values point to learned Nets. The IAR2 supplies default values for these frame types which can be added to PCs operating on LANs without other IPX routing.
- **Dial-in IPX Net -** This parameter specifies the IPX Net definition for a WAN interface.
- **Autolearn Zero LAN IPX Nets -** By setting this parameter to **Enable**, IAR2 learns IPX Nets from RIP/SAP frames sent by other IPX routers on the same LAN. Refer to Figure 7-15 below. If there are no other IPX routers on the IAR2's LAN(s), this parameter must be set to **Disable**, and you must configure the IPX Nets for each frame type.

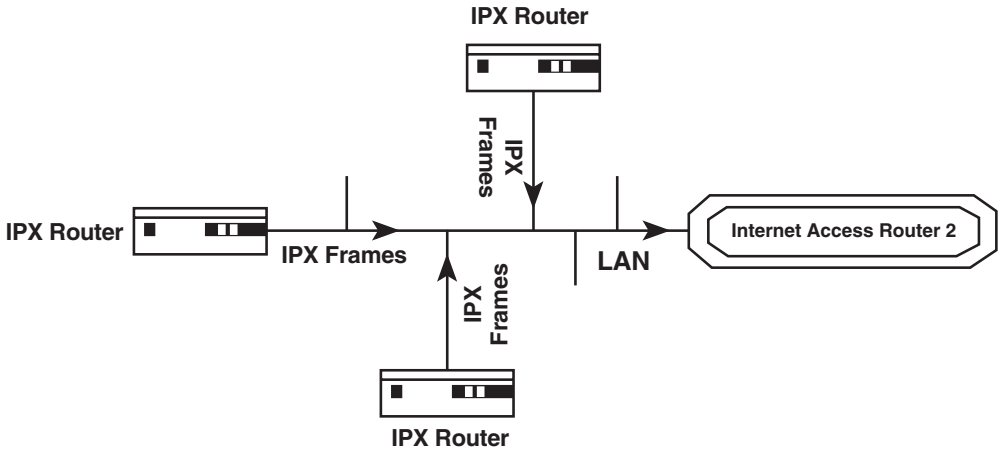


Figure 7-15. Automatic learning from IPX frames.

Also, when you press **7** at the IPX Routing Settings menu to select RIP/SAP Mode, this screen appears:

```
RIP / SAP MODE SETUP ( Device name - IAR2  )
--------------------

1. Link 1 RIP/SAP mode: [Enabled ]
2. LAN    RIP/SAP mode: [Enabled ]

 ESC - Return to previous menu

 Choose one of the above:
```

Select this parameter to enable or disable the RIP/SAP mode for WAN links or LAN connections. The default setting enables sending RIP and SAP tables for all updates and interfaces (Link and LAN). To disable/enable RIP/SAP for an interface, select that interface and use the space bar to toggle between **Enabled** and **Disabled**.

When RIP/SAP mode is disabled, the IAR2 does not send RIP/SAP frames, although IAR2 always receives and processes RIP/SAP frames sent from other routers.

7.4.5 Station Ageing

Station ageing determines the amount of time a station is allowed to be inactive before it is removed from the network. A station is inactive when no IP traffic is forwarded or received to the IAR2's LAN interface. For example, in Figure 7-16 below, IP address 192.168.1.1 has an ageing time of 120 seconds. If no frames are received from IP address 192.168.1.1 within 120 seconds, the station will be removed from the IAR2's IP-net table. The ageing mechanism is active in both the IAR2's IP router and Bridge functions. Both the IP router and Bridge use the same ageing-time parameter. Static stations are not removed by the ageing mechanism. The default ageing time is 60 minutes.

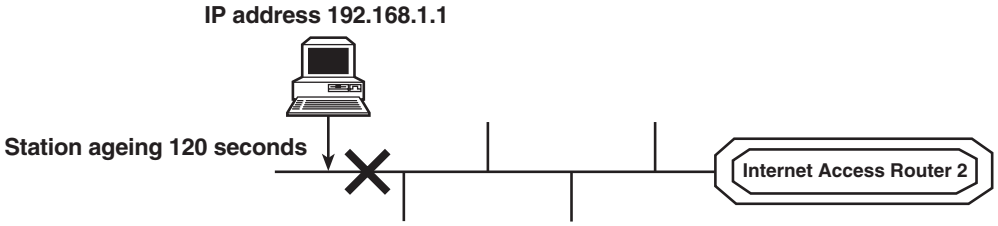


Figure 7-16. Station ageing.

7.5 The Interface Parameters Menu

To access the Interface Parameters menu, one version of which is shown in Figure 7-17 below, press **3** at the Main menu, then press **1** at the Advanced menu, then press **3** in the Setup menu. This screen appears:

```
      INTERFACE PARAMETERS    ( Device name - IAR2  )
      --------------------

1.  Link settings
2.  Frame relay DLCI settings
3.  E1/T1 settings

ESC - return to previous menu


Choose one of the above:
```

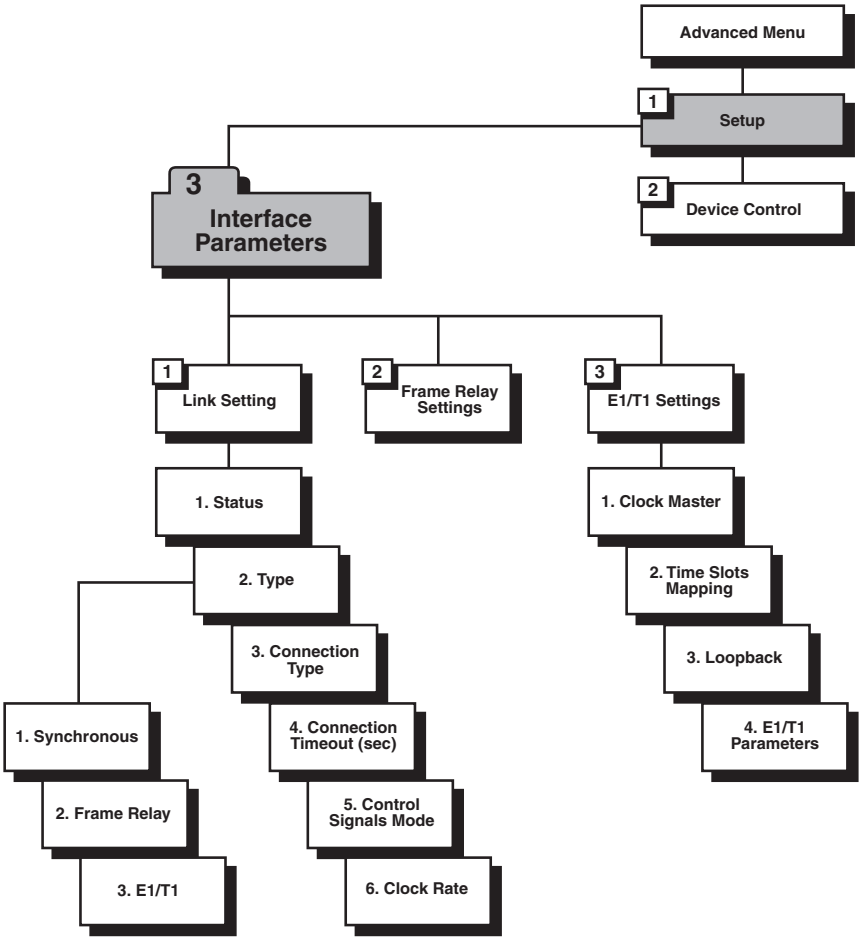


Figure 7-17. One outline of the Interface Parameters menu (submenus and parameters will vary).

7.5.1 Link Settings

This menu's parameters involve the Internet Access Router 2's WAN link(s), as shown in Figure 7-18 below.

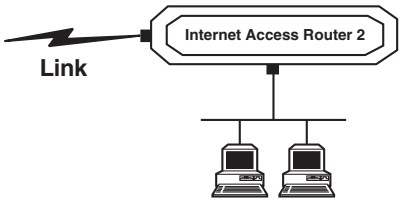


Figure 7-18. The WAN link.

7.5.1.A Status

Select this parameter to specify the status of a link (either **enabled** or **disabled**). An enabled link transmits frames. Normally you want all links in enabled status. However, if another router is not working, the link to that router should be disabled. The IAR2 will then reroute all frames.

7.5.1.B Type

Select this parameter to specify the type of interface. On V.35 and X.21 models, the only choices available here will be **Synchronous** and **Frame Relay**; E1 and T1 models will also have an **E1/T1** setting. Note that **Frame Relay** *must* be chosen here in order for further options in this menu to become available (see **Sections 7.5.1.H** through **7.5.1.P**), as well as for the Frame Relay Settings menu to become available in the Interface Parameters Menu (see **Section 7.5.2**).

7.5.1.C Connection Type

Select this parameter to specify the type of connection:

- **Originate only -** If the link is to be used to connect to the Internet or an intranet.
- **Answer only -** If the link is to be used for receiving remote-access connections.
- **Answer&Originate -** If the link is to be used for both incoming and outgoing connections (not simultaneously).

7.5.1.D Connection Timeout (sec) [PPP only]

Select this parameter to specify the connection timeout in seconds. The remote side has that long to answer; if within that time there is no response, you will be informed that the remote side is no longer active. The connection-timeout parameter is always visible and configurable, but it is only meaningful and active when the PPP protocol is used. This timeout can range from 1 to 255 seconds; factory default is 30 seconds.

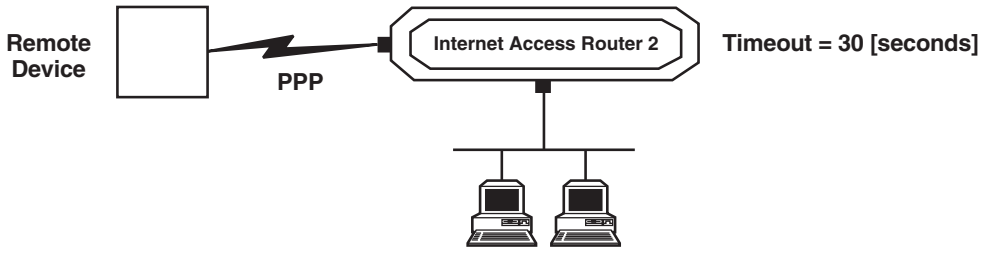


Figure 7-19. The connection timeout.

7.5.1.E Control Signals Mode

As shown in Figure 7-20 below, the Internet Access Router 2 can be set to **ignore** or **acknowledge** the RS-232 control signals RTS (Request to send), CTS (Clear to send), and CD (Carrier Detect).

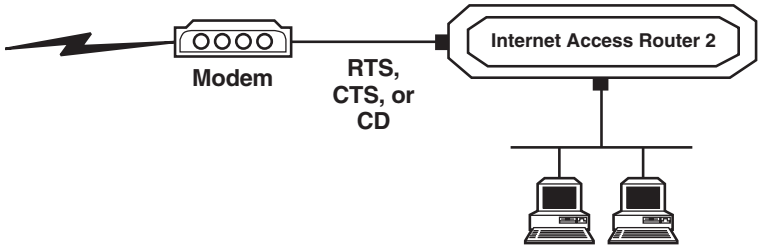


Figure 7-20. Control signals mode.

7.5.1.F Clock Type [V.35 Models Only]

This parameter appears in the Link Settings menu of V.35 and X.21 models only, and it has no effect in X.21 models (which are always DTE and *must* receive their clock from the attached DCE), so it's only actually useable in V.35 models. Select it to specify whether the IAR2 uses its own **internal** clock or the **external** clock (receive/recovered clock) from the attached WAN device. The factory-default setting is **external**. If you set Clock Type to **internal**, the Clock Rate (Kbps) parameter becomes enabled (see **Section 7.5.1.G**) and you'll have to set it.

7.5.1.G Clock Rate (Kbps) [V.35 Models Only]

This parameter appears in the Link Settings menu of V.35 and X.21 models only, and only if it has been enabled by setting Clock Type to "internal" (see **Section 7.5.1.F**). But it has no effect in X.21 models, so it's only actually useable in V.35 models. Select this parameter to specify the data rate that the IAR2 will get from its internal clock for synchronous WAN operation. Possible choices are **2.4**, **4.8**, **9.6**, **14.4**, **19.2**, **38.4**, **48**, **56**, **64**, **112**, **128**, **256**, **384**, **512**, **768**, **1024**, or **2048** Kbps.

7.5.1.H Self Learn DLCI/Maintenance [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify whether the Internet Access Router 2 will self-learn the maintenance protocol on the Frame Relay link and the existing DLCIs with their status (UP or DOWN). When this parameter is disabled (OFF), you'll need to configure the maintenance protocol and the DLCIs manually.

7.5.1.J CLLM Status [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify whether CLLM frames, used for congestion indication, will be supported (**ON**) or not (**OFF**).

7.5.1.K Maintenance Protocol [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify the maintenance protocol of the Frame Relay link: **T1.617/ANNEX D**, **Q.933/ANNEX A**, **LMI**, or **None**. This parameter can only be configured if the Self Learn DLCI/Maintenance parameter(see above) is disabled (**OFF**).

7.5.1.L Polling Interval [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify the number of seconds between transmission of two successive status-inquiry frames. Refer to Figure 7-21 on the next page.

7.5.1.M Full Enquiry Interval [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify the number of polling intervals after which a full-status-inquiry frame is transmitted. Refer to Figure 7-21 below.

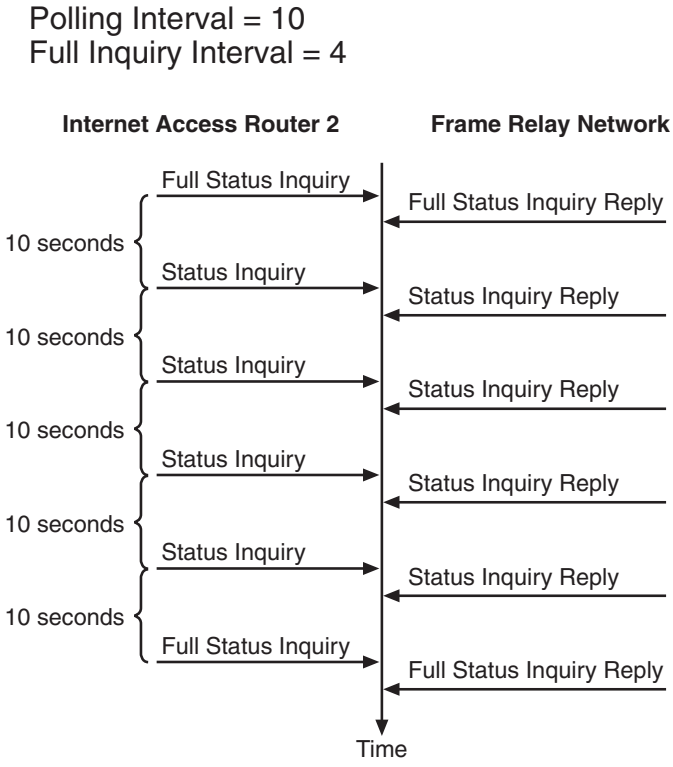


Figure 7-21. Polling intervals.

7.5.1.N Error Threshold [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify the number of unacknowledged monitored events (status-inquiry frames and full-status-inquiry frames) that can occur in a sliding monitored-events window before the link is declared DOWN. Refer to Figure 7-22 below.

7.5.1.P Monitored Events [Frame Relay Only]

This parameter appears in the Link Settings menu only when "Frame Relay" has been selected for Type in the Link Settings menu (see **Section 7.5.1.B**). Select this parameter to specify the number of monitored events (status-inquiry frames and full-status-inquiry frames) in a sliding monitored events window. Refer to Figure 7-22 below.

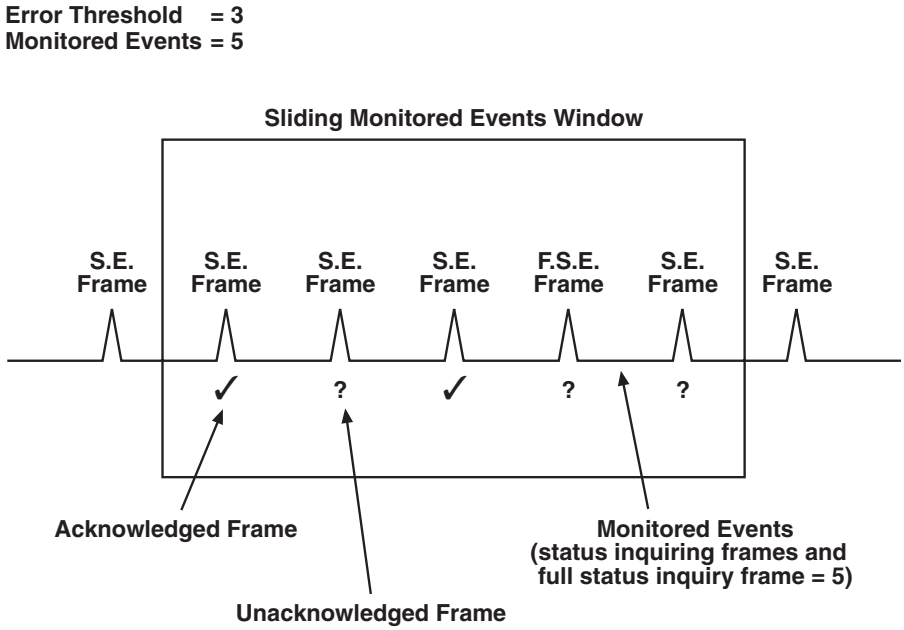


Figure 7-22. Monitored events.

After the link is declared DOWN, it can only be declared UP again when the sliding monitored events window contains only successfully monitored events, as shown in Figure 7-23 below.

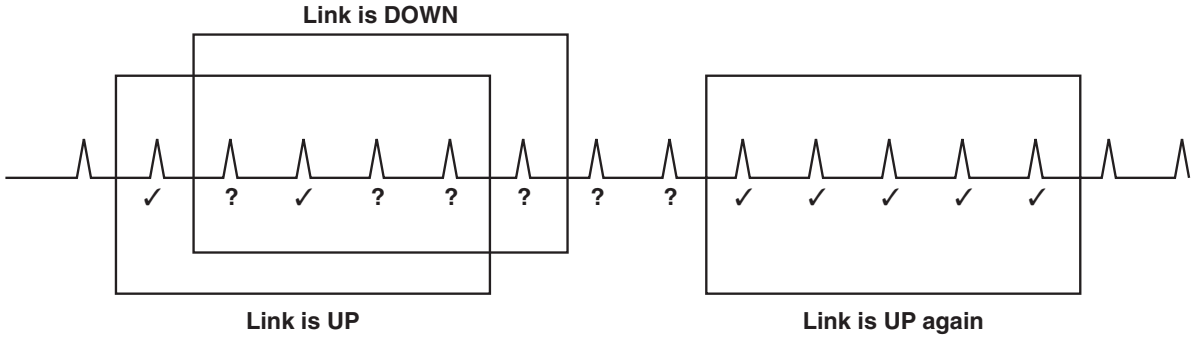


Figure 7-23. Monitored events—link is down.

7.5.2 Frame Relay DLCI Setings

Frame Relay is a form of wide-area networking which is designed to maximize throughput and minimize cost by simplifying network processing. Refer to Figure 7-24 below.

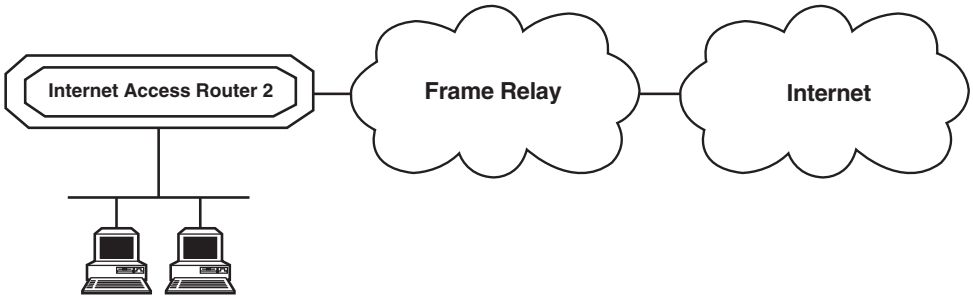


Figure 7-24. Connection to the Internet over Frame Relay.

The important features of Internet Access Router 2's Frame Relay implementation include:

- Supports permanent virtual circuits (PVC).
- Supports Frame Relay (IP/IPX/Bridge) encapsulation based on RFC 1490.
- Supports different maintenance protocols: T1.617/Annex D, Q.933/Annex A, and LMI.
- Supports self-learning of the maintenance protocol and the DLCI, which enables connection to the Frame Relay network without configuring Frame Relay parameters.
- Executes congestion control when an explicit congestion notification is received for the DLCI from the Frame Relay network. The unit reduces the transmitted information rate of the DLCI and increases it when the congestion condition is cleared.
- Supports the Frame Relay SNMP MIB.

Figure 7-25 below maps the options in the Advanced Menu which are used to configure the IAR2 for operation over a Frame Relay network.

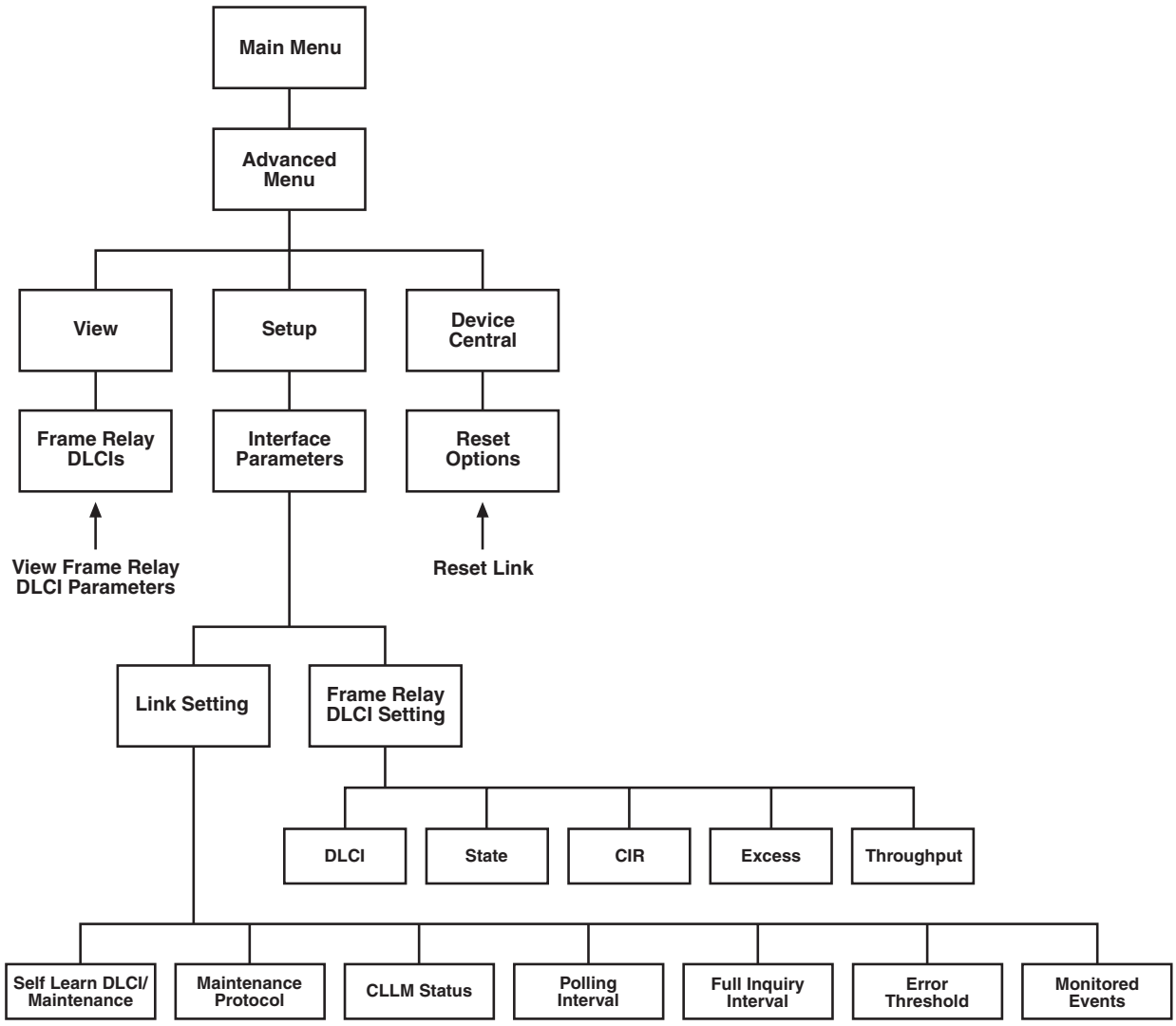


Figure 7-25. Frame Relay options in the Advanced menu.

The Frame Relay DLCI Settings menu is available only when "Frame Relay" has been selected as the Type in the Link Settings menu (see **Section 7.5.1.B**). The parameters in the Frame Relay DLCI Settings menu are described below.

7.5.2.A DLCI
Select this parameter to specify the DLCI number.

7.5.2.B State
Select this parameter to specify whether the DLCI is **Enabled** or **Disabled** (for receive/transmit).

7.5.2.C CIR
Select this parameter to specify the maximum amount of data in bits which the network guarantees to transfer during the measurement interval (the measurement interval is usually one second). The value of this parameter is *obtained from your Frame Relay provider.*

7.5.2.D Excess
Select this parameter to specify the maximum amount of uncommitted data bits that the network will attempt to deliver during the measurement interval. The value of this parameter *should be received from your Frame Relay provider.*

7.5.2.E Throughput
Select this parameter to specify the average number of data bits per second transferred by the network. When a measurement interval of one second is assigned to the CIR, the throughput value *should equal the CIR value.*

7.5.3 E1/T1 Settings (E1/T1 Models Only)

Select this option to configure the E1 or T1 parameters of E1 or T1 models of the Internet Access Router 2. In T1 models, the T1 Setup Menu should appear when you select this option; in E1 models, the E1 Setup Menu should appear. After you read the rest of this section, see **Section 7.5.3.A** for the T1 parameters or **Section 7.5.3.B** for the E1 parameters.

Each model of the IAR2 that has an E1 or T1 interface is an integrated router/bridge with E1/T1 and fractional E1/T1 services (see Figures 7-26 and 7-27 below). Different models of the IAR2 have different E1/T1-interface configurations:

- Main T1 link only ("-UT1" model).
- Main T1 link and T1 sublink ("-UT1S" model).
- Main E1 link only ("-UE1" and "-UBE1" models).
- Main E1 link and E1 sublink ("-2UE1" model).

Each model of the IAR2 with an E1 or T1 sublink has "drop & insert" capability, which means that it can multiplex data from the local router/bridge together with the voice signal from the local PABX and carry both streams across the E1 or T1 main link at the same time.

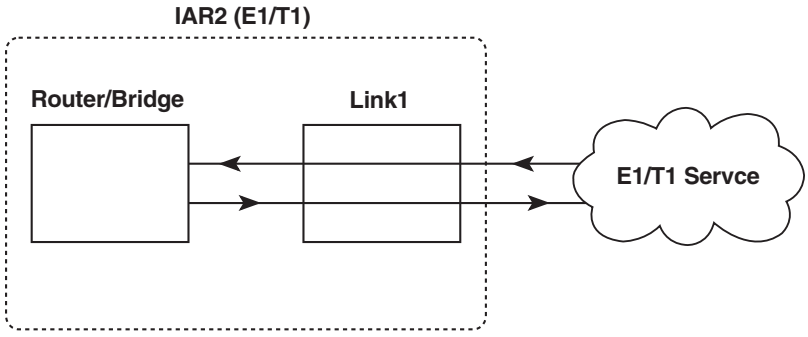


Figure 7-26. An IAR2 with an E1 or T1 interface for its main link only.

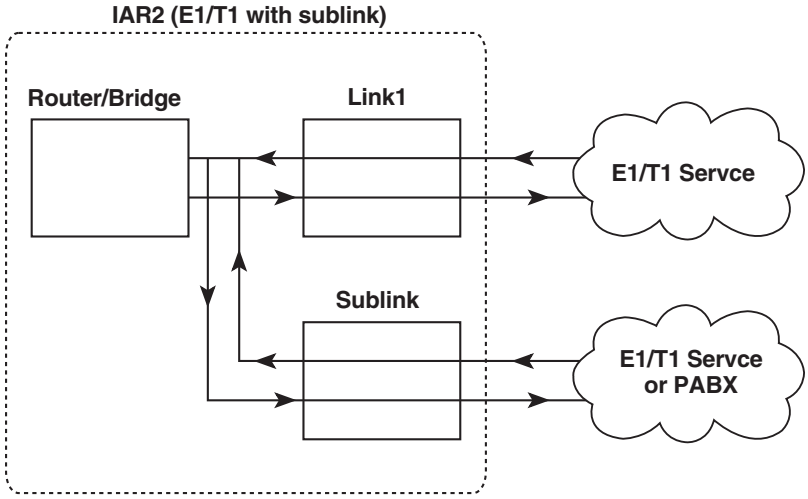


Figure 7-27. An IAR2 with E1 or T1 interfaces for both its main link and sublink.

Features of the **T1 interface** include:

- Nominal rate - 1.544 Mbps.
- Data rates are multiples of 56 Kbps or 64 Kbps (N x 56 Kbps or N x 64 Kbps, N = 1 to 24).
- Time-slot assignment is user selectable.
- Link interface includes integral CSU/DSU depending on user configuration of the transmit level, 0 to –22.5 dB for the Channel Service Unit (CSU) or 0 to 655 feet for the Data Service Unit (DSU).
- Framing modes: Super Frame (SF [D4]) or Extended Super Frame (ESF).
- Line code: Alternate Mark Inversion (AMI).
- Zero suppression modes: B8ZS, B7ZS or transparent.
- Master system clock:
  - Internal oscillator.
  - Recovered from the link 1 received data.
  - Recovered from the sublink received data (for the model with a sublink).
- Variety of Loopback possibilities:
  - Network activated loopbacks (PLB, LLB).
  - Facility Data Link (FDL) loopbacks.
  - User-configurable local or remote loopbacks.
- Extended Super Frame (ESF) diagnostic for previous 24 hours collected in 15-minute intervals (according to AT&T® PUB 54016).

Features of the **E1 interface** include:

- Nominal rate - 2.048 Mbps.
- Data rates are multiples of 56 Kbps or 64 Kbps (N x 56 kbps or N x 64 kbps, N = 1 to 31).
- Time-slot assignment is user-selectable.
- E1 interface with or without LTU.
- Interfaces: balanced or unbalanced.
- Framing modes: G732N and G732S.
- Optional Cyclic Redundancy Check (CRC-4).
- Line code: HDB3.
- Master system clock:
  - Internal oscillator.
  - Recovered from the link 1 received data.
  - Recovered from the sublink received data (for the model with a sublink).
- Loopback: User-configurable local or remote loopbacks.
- When CRC-4 is enabled, diagnostics for the last 24 hours collected in 15-minute intervals (similar to AT&T PUB 54016).

The following sections describes the parameters in the T1 Setup and E1 Setup menus.

7.5.3.A Clock Master

Select this parameter to set the source clock that synchronizes the whole T1 or E1 network. Timing source options are:

- **Internal** - The IAR2 generates the system source clock from an internal clock oscillator.
- **Link 1** - The IAR2 recovers the clock from the data received from the T1 link1.
- **Sub link T1** or **Sub link E1** (for models of the IAR2 with a sublink) - The IAR2 recovers the clock from the data received from the T1 or E1 sublink.

7.5.3.B Multiplier

Select this parameter to set the data rate of each DATA time slot. The multiplier value can be **56** or **64** Kbps.

7.5.3.C Time Slots Mapping

Select this parameter to configure the routing and the type of individual time slots for the link. Figure 7-28 below shows the type of time slots entering the multiplexor (for models of the IAR2 with a T1or E1 sublink). The time-slot mapping options are:

- **NC -** Time slot not connected.
- **DATA -** Time slot used for data from the router/bridge.
- **VOICE (for models of the IAR2 with a sublink) -** Time slot used for voice from the sublink.
- **DATA_SUB (for models of the IAR2 with a sublink)** - Time slot used for data from the sublink.

NOTES

For a multiplier of 64 kbps all time slots can be configured to DATA. But, for a multiplier of 56 kbps, a maximum of 15 (E1) or 16 (T1) time slots can be configured to DATA.

For models of the IAR2 with a sublink, this limitation does not exist for time slots configured to the VOICE or DATA_SUB type.

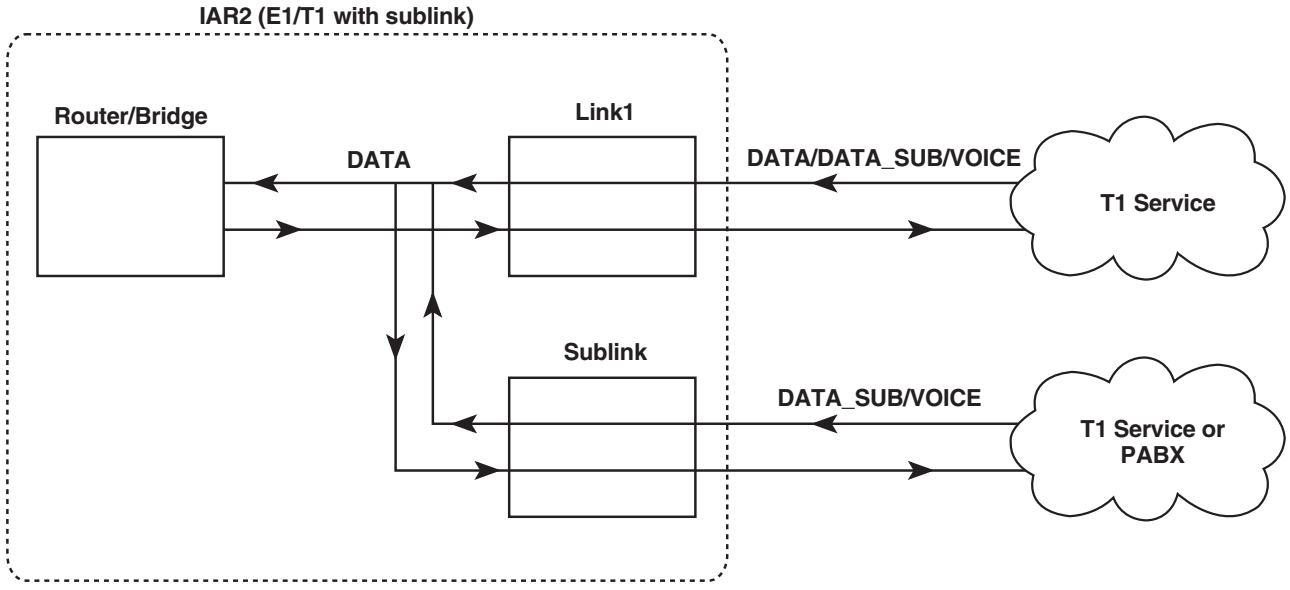


Figure 7-28. Time slots mapping (for the IAR2 models with a sublink).

7.5.3.D Loopback

Select this parameter to test the Internet Access Router 2's T1 or E1 interface. Loopback options are:

- **Disabled**
- **Remote Analog Loopback (for models without a sublink)**
  In this mode, the IAR2 performs an analog loopback and transmits back the data that was received from the T1 or E1 line, as shown in Figure 7-29 below.

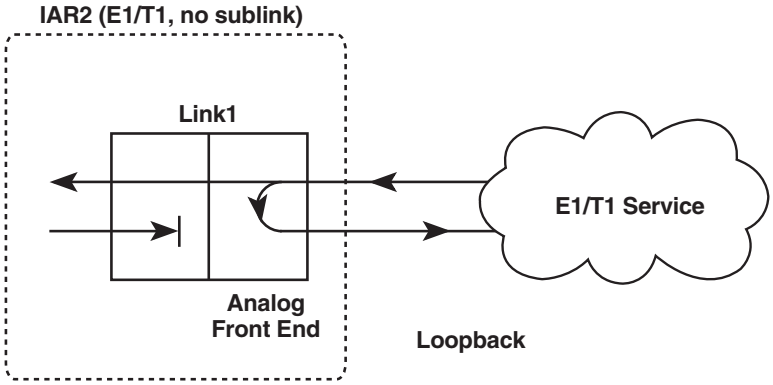


Figure 7-29. Remote analog loopback (main link only).

- **Remote Analog Loopback (for models with a sublink)**
  In this mode, the IAR2 performs an analog loopback and transmits back the data that was received from both the main link (Link1) and the sublink, as shown in Figure 7-30 below.

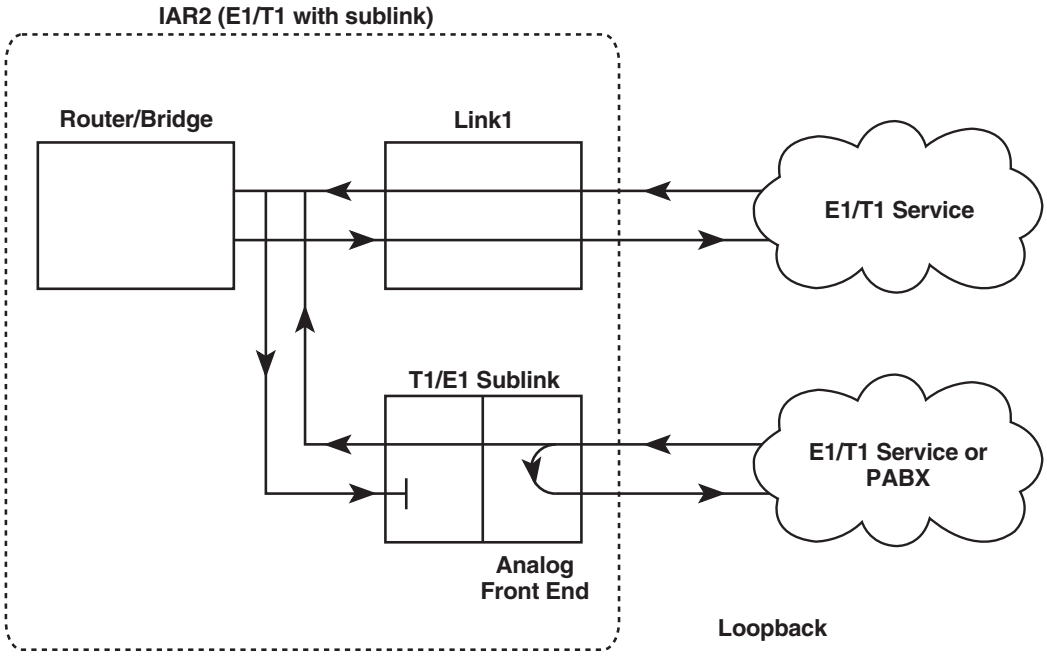


Figure 7-30. Remote analog loopback (main link and sublink).

- **Remote Digital Loopback (T1 models only, no sublink)**
  In this mode the IAR2 performs a digital loopback and transmits back the signal that was received from the T1 line, as shown in Figure 7-31 below.

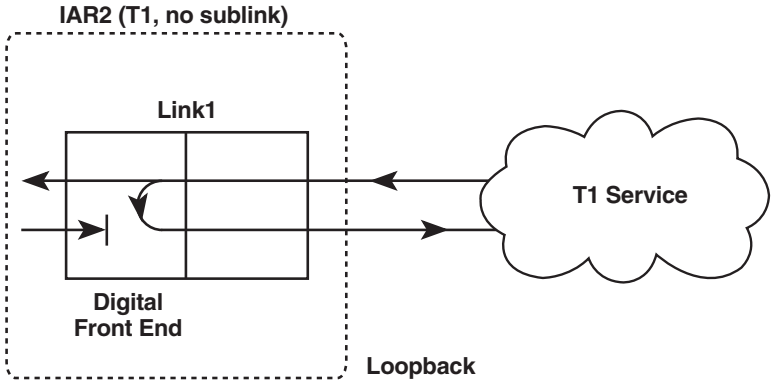


Figure 7-31. Remote digital loopback (T1 models, main link only).

- **Remote Digital Loopback (T1 model with a sublink only)**
  In this mode the IAR2 performs a digital loopback and transmits back the signal that was received from the T1 line, as shown in Figure 7-32 below.

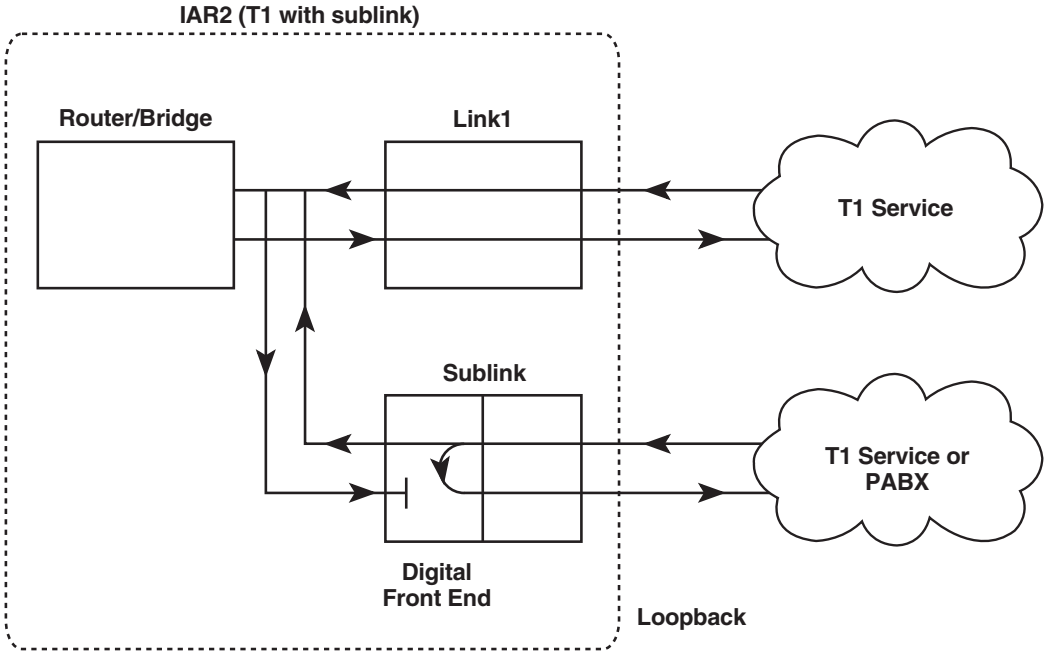


Figure 7-32. Remote digital loopback (T1 model, main link and sublink).

- **Local Analog Loopback (for models without a sublink)**
  In this mode the data transmitted from the IAR2 to the T1 or E1 line is sent back to the IAR2 instead of the data received from the line, as shown in Figure 7-33 below.

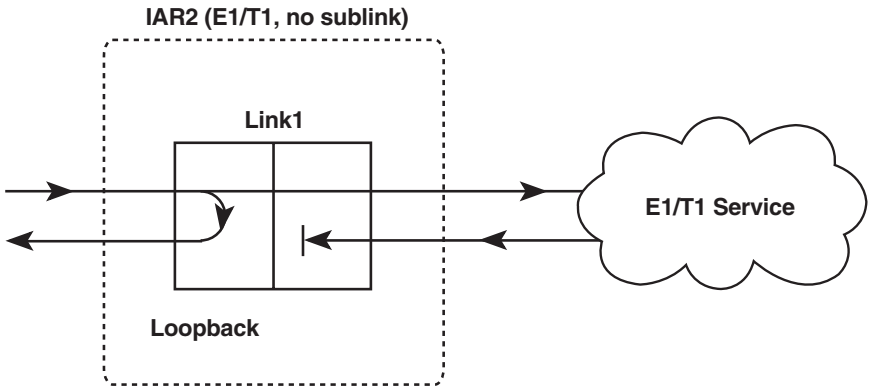


Figure 7-33. Local analog loopback (main link only).

- **Local Analog Loopback (for modesls with a sublink)**
  In this mode the data transmitted from the IAR2 to the T1 or E1 line is sent back to the IAR2 instead of the data received data from the line, as shown in Figure 7-34 below.

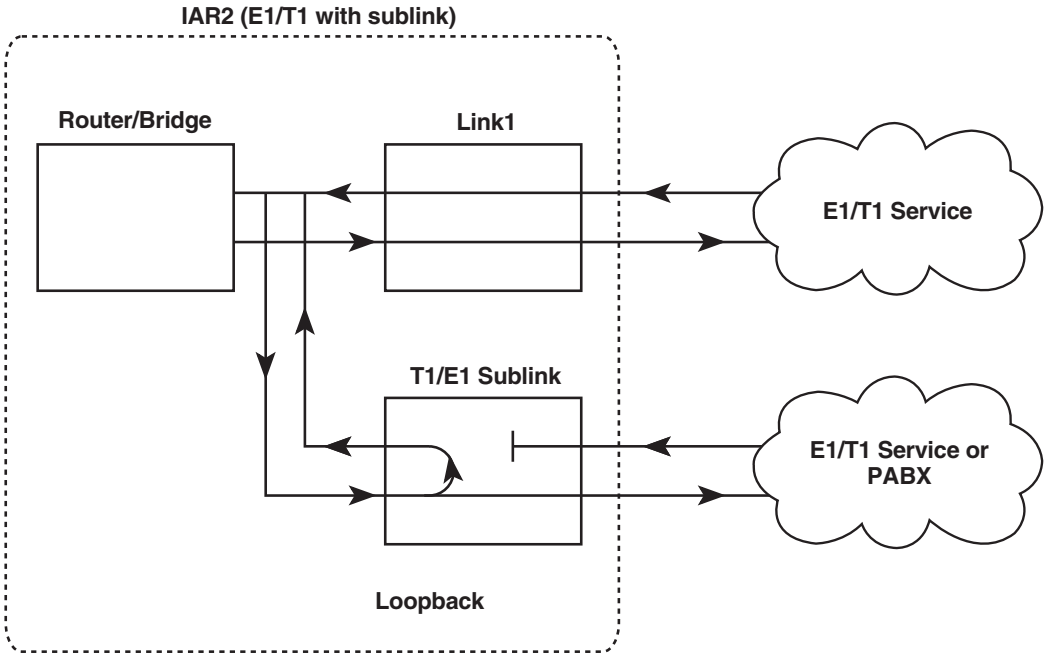


Figure 7-34. Local analog loopback (main link and sublink).

7.5.3.E T1 Link Parameters and T1 Sublink Parameters (T1 Models Only)
Select this option to configure any of the following parameters:

- **Frame Type**
  Select this parameter to set the T1 framing type. Available types are:
  – **ESF -** Extended SuperFrame. 24 frames per multiframe.
  – **SF -** SuperFrame. 12 frames per multiframe.

- **Line Code**
  Select this parameter to set the line coding method used for zero suppression. The zero-suppression method is used to avoid long strings of "0" bits, because these strings do not carry timing information. The available zero-suppression methods are **B7ZS**, **B8ZS**, and **Transparent** (AMI only).

- **Tx Line Mask**
  Select this parameter to control the link's transmit-signal characteristics. Options depend on whether the link should be configured with a CSU or not. When the link is configured without a CSU, the transmit-signal mask is selected according to the transmit-line length (0 to 655 ft. [0 to 200 m]), to meet DSX-1 requirements. When the link is configured with a CSU, the transmit signal can be attenuated by **7.5**, **15**, or **22.5** dB.

- **Sync**
  Select this parameter to define the time required for the link to return to normal operation after a red-alarm event has terminated. Choose **FAST** for one second or **AT&T 62411** for ten seconds.

- **Idle Code**
  Select this parameter to set the value to be transmitted on the NC time slots.

- **Rx Gain**
  Select this parameter to set the maximum receive sensitivity for the T1 interface.

- **Remote Alarm Indication (sublink model only)**
  From the T1 Link Parameters menu, select this parameter to determine whether to transmit a yellow-alarm indication on the sublink when Link1 is in yellow alarm state.
  From the T1 Sublink Parameters menu, select this parameter to determine whether to transmit a yellow-alarm indication on Link1 when the sublink is in either a yellow- or red-alarm state.
  (Note that when Link1 is in a red-alarm state, an "all ones" indication is *always* sent to the sublink.)

- **Out-Of-Service Signaling (sublink model only)**
  Select this parameter to determine the value of the A and B signaling bits sent to Link1 when the sublink is in the Out-Of-Service state. The C and D signaling bits are not affected.
  – **MARK -** Both A and B signaling bits are forced to "1" during out-of-service period.
  – **SPACE -** Both A and B signaling bits are forced to "0" during out-of-service period.
  – **MARK-SPACE -** The A and B signaling bits are forced to "1" for 2.5 seconds, then shift to the "0" state until the out-of-service period ends.
  – **SPACE-MARK -** The A and B signaling bits are forced to "0" for 2.5 seconds, then shift to the "1" state until the out-of-service period ends.

7.5.3.F E1 Link Parameters and E1 Sublink Parameters (E1 Models Only)
Select this option to configure any of the following parameters:

- **Frame Type**
  Select this parameter to set the E1 framing type. Available types are:
  – **G732N -** 2 frames per multiframe. Time slot 16 can be used for user data.
  – **G732S -** 16 frames per multiframe. Time slot 16 is used for Channel Associated Signaling (CAS).

- **CRC-4 (Cyclic Redundancy Check)**
  Select this parameter to **enable** or **disable** calculation of a 4-bit checksum in order to detect errors in frames.

- **Sync**
  Select this parameter to define the time required for the link to return to normal operation after a local sync-loss alarm event has terminated. Choose **FAST** for one second, **AT&T 62411** for ten seconds, or **CCITT** for 100 milliseconds.

- **Idle Code**
  Select this parameter to set the value to be transmitted on the NC time slots.

- **Rx Gain**
  Select this parameter to set the maximum receive sensitivity for the E1 interface.

- **Remote Alarm Indication (sublink model only)**
  From the E1 Link Parameters menu, select this parameter to determine whether to transmit a remote sync-loss alarm indication on the sublink when Link1 is in a remote sync-loss alarm state.
  From the E1 Sublink Parameters menu, select this parameter to determine whether to transmit a remote sync-loss alarm indication on Link1 when the sublink is in either a local or remote sync-loss alarm state.
  (Note that when Link1 is in a local sync-loss alarm state, an “all ones” indication is *always* sent to the sublink.)

- **Out-Of-Service Signaling (sublink model only)**
  Select this parameter to determine the value of the A and B signaling bits sent to Link1 when the sublink is in the Out-Of-Service state. The C and D signaling bits are not affected.
  – **MARK -** Both A and B signaling bits are forced to “1” during out-of-service period.
  – **SPACE -** Both A and B signaling bits are forced to “0” during out-of-service period.
  – **MARK-SPACE -** The A and B signaling bits are forced to “1” for 2.5 seconds, then shift to the “0” state until the out-of-service period ends.
  – **SPACE-MARK -** The A and B signaling bits are forced to “0” for 2.5 seconds, then shift to the “1” state until the out-of-service period ends.

7.6 The Access Control (Security) Menu

To access the Access Control (Security) menu, shown in Figure 7-35 below, press **3** at the Main menu, then press **1** at the Advanced menu, then press **4** in the Setup menu. This screen appears:

```
    ACCESS CONTROL  ( Device name - IAR2  )
    --------------

1. External access security
2. Device security identity
3. Security Host/Guest
4. Script Setup

 ESC - Return to previous menu

 Choose one of the above :
```

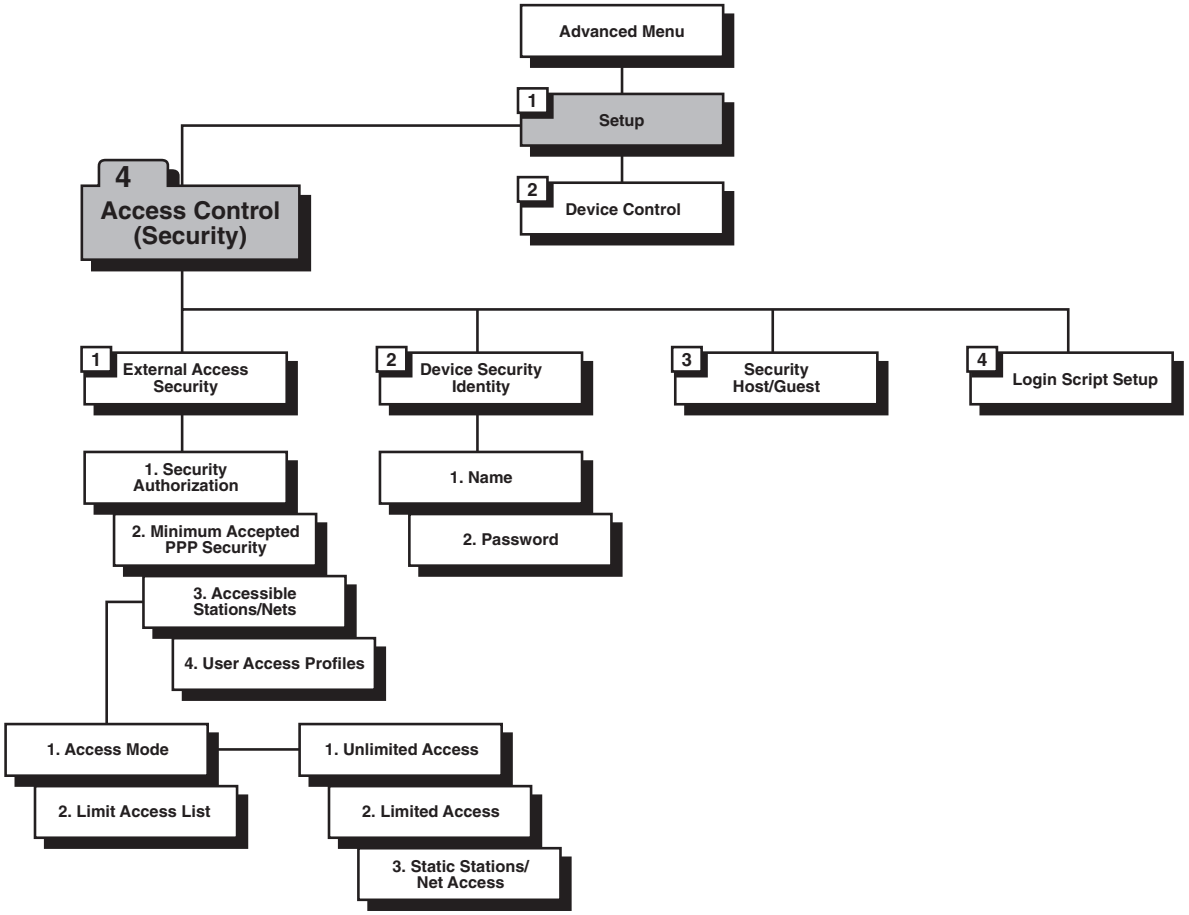


Figure 7-35. Outline of the Access Control (Security) menu.

7.6.1 External Access Security

7.6.1.A Security Authorization

Select this parameter to protect your LAN against unwanted entry by outside users. Toggle between the following options:

- **None -** Access denied to all users.
- **User Access Profile -** Allow/deny access according to the User Access Profile (see **Section 7.6.1.D**).
- **RADIUS -** Allow/deny access according to any parameters you've configured for the RADIUS Authenticator (see **Section 7.3.5**).
- **User Access Profile + RADIUS -** Access is allowed if the User Access Profile allows it *or* if the User Access Profile does not have an entry for the user but the RADIUS Authenticator allows it.

7.6.1.B Minimum Accepted PPP Security

Select this parameter to specify the minimum security as **none**, **PAP**, or **CHAP**. CHAP and PAP are the two types of security systems that PPP supports:

- **CHAP (Challenge Handshake Authentication Protocol) -** CHAP is a type of authentication in which the authentication agent (typically a network server) sends the client program a key to be used to encrypt the username and password. This enables the username and password to be transmitted in an encrypted form to protect them against hackers.
- **PAP (Password Authentication Protocol) -** PAP is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The main weakness of PAP is that both the username and password are transmitted in an unencrypted form.

7.6.1.C Accessible Stations/Nets

Select this parameter to define the limits of public access to the network. Access can be allowed for all stations/nets, for only certain stations/nets, or for only static stations/nets. When the access mode is "limited," create an access list here that define which stations/nets have access.

7.6.1.D User Access Profiles

Select this parameter to view and modify user-access profiles in the access-control users list. The list contains user names, security parameters, and dialback options.

7.6.2 Device Security Identity

7.6.2.A Name

Select this parameter to assign a a name to the Internet Access Router 2 for access to your ISP's central access router. The maximum name length is 30 characters.

7.6.2.B Password

Select this parameter to assign a password to the IAR2 for access to the ISP's Internet Service Provider's central access router. The maximum length is 30 characters.

7.6.3 Security Host/Guest

Select this parameter to define a link's security status. When a link is defined as a Host, users are approved according to your profile list (see **Section 7.6.1.D**). When link is defined as a Guest, the device sends its name and password to be approved by the host. The Guest mode is the default.

7.6.4 Login Script Setup

The Internet Access Router 2's scripting tool allows you to negotiate an initial login, required by some Internet Service Providers (ISPs). The initial login usually consists of a username, password, and possibly some other information, which has to be entered to gain access to the ISP.

The IAR2's script is a sequence of commands, with a maximum of 20 commands in the script. As soon as a physical connection to the remote host is achieved (and the script is enabled), the IAR2 begins to forward the script. Script processing ends when the last script command has been forwarded.

The IAR2's script comprises one or more command lines. Each command line consists of a command code, as shown in Table 7-3 below, followed by an argument. The *pattern* arguments can be any string without apostrophes, quotation marks, or unsigned integers. In addition to printable/displayable ASCII symbols, these arguments can contain any control characters with ASCII codes from 1 to 31 decimal (0x01 to 0x1F hex). While editing scripting commands, use the "control" mode to enter these characters; that is, type in each character as "^" followed by the ASCII character (from "A" to "[") whose code is 64 decimal greater than the control character's. For example, if you want the code to wait for or send the hex code 0x0A (an ASCII line feed), type it in as "^J". Likewise, specify 0x0D hex (a carriage return) with "^M" and 0x1B hex (an escape character) with "^[".

Table 7-3. The Command Codes

Command Code	Description
waitcase *pattern*	Waits until the specified case-sensitive *pattern* is received from the remote host and forwards the next command. The maximum pattern length is 24 characters. If the speicifed pattern is not received within the timeout period (default is 15 seconds, see "timeout" below), the link then disconnects and the IAR2 performs the same actions as required during authentication failure.
waitnocase *pattern*	Same as "waitcase *pattern*" above, except not case-sensitive.
send *pattern*	Transmits specified *pattern* to remote host. The pattern can contain any recognized control symbols. The maximum pattern length is 24 characters.
sendhide *pattern*	As above. However, the *pattern* is displayed on the screen as asterisks. The control symbol is displayed as two asterisks when editing and as one when viewing.
timeout *number*	Changes the timeout for the "waitcase," "waitnocase," and "getip" commands. The *number* is the timeout value, in seconds. This value can be any number from 1 to 99 and will be used until the next timeout command.
delay *number*	The delay in seconds between sending commands. All symbols received during this time will be ignored. This value can be any number from 1 to 99.
getip *address*	This command waits for an IP address from the remote host. If the remote host returns several IP addresses in a string, the *address* specified with this command will determine which one should be used. If an IP address is received successfully from the host, and the Single IP feature is enabled, the IP address will be used on the IAR2's WAN interface. If an IP address is not received successfully within the specified timeout period, the link disconnects.

7.7 The WAN Economy Menu

To access the WAN Economy menu, shown in Figure 7-36 below, press **3** at the Main menu, then press **1** at the Advanced menu, then press **5** in the Setup menu. This screen appears:

```
      WAN ECONOMY  ( Device name - IAR2 )
      -----------

Use these features:
- to reduce traffic over the WAN to a minimum and increase throughput
- to keep the link up only when it is required

  1.  Filters
  2.  Connection on demand
  3.  Spoofing
  4.  Fast retransmission frame limit: 2

  ESC - Return to previous menu

  Choose one of the above:
```

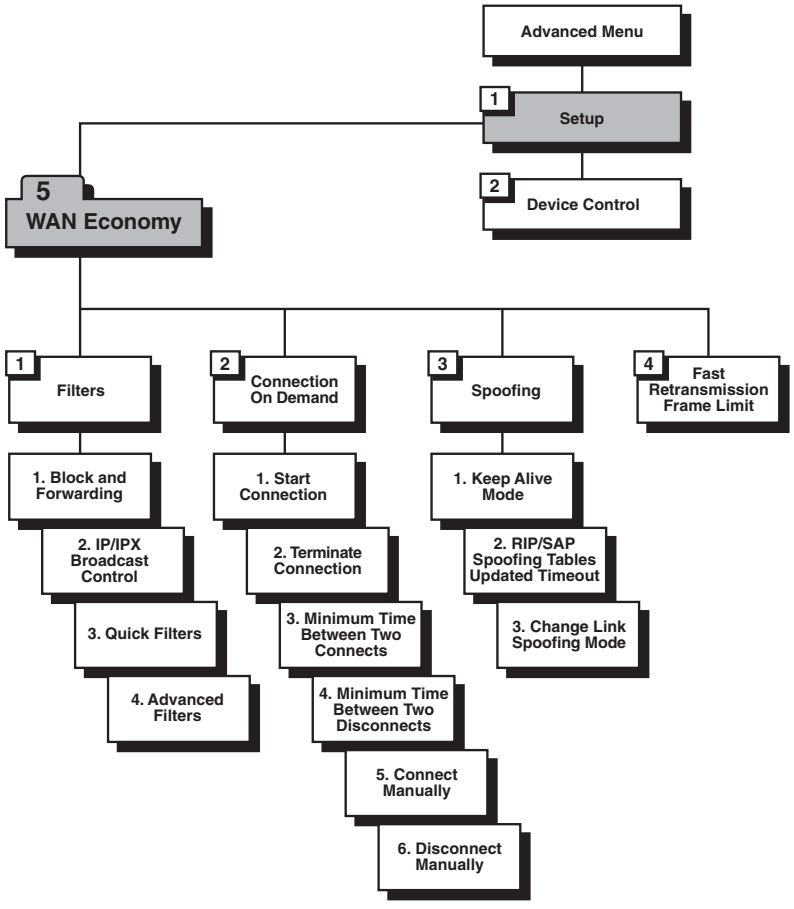


Figure 7-36. Outline of the WAN Economy menu (CoD and Spoofing menus have no effect).

7.7.1 Filters: An Overview

Filtering allows you to limit the amount of traffic which enters and exits the small-office LAN via the Internet Access Router 2. If the IAR2 is attached to more than one LAN, then select this option for each LAN interface. Filtering is used to increase security and reduce traffic to the link. The IAR2 features two types of filters: "Quick" and "Advanced." **Quick Filters** can be used to regulate specific protocols:

- IP.
- IPX.
- SNA.
- NetBIOS.
- AppleTalk®.
- DECnet™.

A Quick Filter can neutralize these protocols by blocking all traffic of that protocol from the link inwards. Refer to Figure 7-37 below.

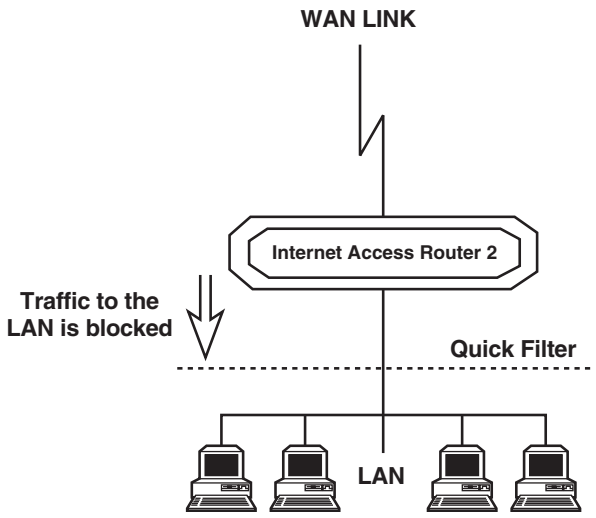


Figure 7-37. Action of a Quick Filter.

Advanced Filters can be used to regulate traffic in both directions (refer to Figure 7-38 on the next page):

- From the LAN to the WAN link. Using filters here will forward or block traffic from the LAN outwards.
- From the WAN link to the LAN. Using filters here will forward or block traffic from the link inwards.

Using a variety of parameters, Advanced Filters can be used to regulate different protocols, to totally or partially block traffic, and to control traffic between links.

NOTE

On dual-LAN models, use Quick Filters for LAN1 and Advanced Filters for LAN2.

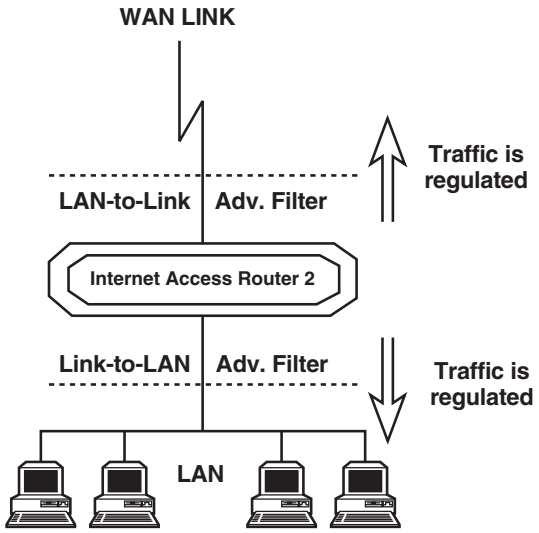


Figure 7-38. Action of an Advanced Filter.

There are two modes through which filtering can be implemented: **blocking** and **forwarding**.

The blocking command causes the IAR2 to test every packet of data that is sent to or from the LAN; if the packet meets the blocking criteria, passage is denied. For example, perhaps you want to ensure that IP/UDP packets do not go onto the link in the direction of the Internet or intranet. Thus, you design a filter which tests each packet to see if it is an IP/UDP packet. If the packet tests positive, it is automatically blocked.

The forwarding command works roughly the same way, but in reverse: If the packet meets the forwarding criteria, it is allowed to pass to or from the LAN. For example, to allow a certain user on the LAN to access the Internet for FTP purposes, create a filter to test each packet for the IP host address of the specified user and the FTP socket of the packet. If the packet passes the test, the packet is forwarded to or from the Internet.

Up to 18 filters can be defined (although, to avoid killing the IAR2's performance, we recommend that you keep the number of active filters to a minimum). If there are two filters which have contradictory operations, forwarding takes precedence over blocking. Once again, an example: Let's say you want to allow *only one* particular LAN user to access the Internet. To ensure that no one else is able to access the Internet, create a blocking filter for all traffic going to the link. To do this, select "Filters" from the WAN Economy menu, then select "Block and Forwarding," then select **Block all traffic for Link1**. Then create a filter to test each packet for the IP host address of the specified user and the FTP socket of the packet. Since forwarding takes precedence over blocking, that user's frames are forwarded even though traffic to and from all other users is blocked.

You can use any combination of the following parameters when you define filtering tests:

- Protocol.
- Operation (block, forward, etc.).
- Interface (LAN, Link).
- Destination and/or source IP address of the packet.
- Destination and/or source MAC address of the packet (layer 2).
- IP socket (upper and lower level).
- IP packet type (broadcast, multicast).

Filters can be defined through the control port, TELNET, or SNMP. First decide on the mode and conditions for a filter, then follow the instructions in **Section 7.7.2** or **7.7.3** to set filter parameters.

7.7.2 Defining Quick Filters (The Quick Filters Menu)

There are four steps in defining a Quick Filter:

1. From the Advanced menu, choose Setup ➔ WAN Economy ➔ Filters. This screen will appear:

```
     FILTERS  ( Device name - IAR2  )
     -------

  1. Block and Forwarding
  2. IP / IPX broadcast control - [Full Propagation]
  3. Quick filters
  4. Advanced filters

  Esc - Return to main menu


  Choose one of the above:
```

2. Set the filter type (block or forward).
3. Set the broadcast control.
4. Set the Quick Filter parameters.

To set the filter type:

1. At the Filters menu, choose **Block and Forwarding**.
2. Toggle between **Block** and **Forward**.

To set the broadcast control:

1. The broadcast-control filter manages special frames which are normally propagated throughout the network. The frames managed are:
   - **IP -** Local broadcast propagation.
   - **IPX -** Zero destination propagation and IPX Type 20 frames propagation.
   - **NETBIOS over IP -** Propagation of IP frames with TCP/UDP ports 137, 138, and 139.
2. From the Filters menu, press **2** to toggle between **Full Propagation** and **Block Propagation**. The default is **Block Propagation**.

To set the Quick Filter parameters:

1. From the Filters menu, choose **3**, Quick Filters. This screen will appear:

```
     QUICK  FILTERS  ( Device name - IAR2 )
     --------------

     Choose the protocols you want to block or forward!!:
     (The Blocking or forwarding is to interface LAN 1 only)

  1. IP          NO FILTERS
  2. IPX         NO FILTERS
  3. SNA         NO FILTERS
  4. NetBIOS     NO FILTERS
  5. AppleTalk   NO FILTERS
  6. DECnet      NO FILTERS
  7. Others      NO FILTERS


  ESC - Return to previous menu


  Choose one of the above:
```

2. To toggle between Forward and Block (and No Filters), press the number of the protocol that you want to filter. (Quick Filters are defined protocol-by-protocol; set blocking or forwarding independently for each protocol.)

7.7.3 Defining Advanced Filters (The Advanced Filters Menu)

There are four steps in defining a Advanced Filter:

1. From the Advanced menu, choose Setup ➔ WAN Economy ➔ Filters. The screen shown on the previous page will appear.

2. Choose **4**, Advanced Filters.

3. If you are defining a new filter, choose **Add**. (The screen shown below will appear.) If you are editing an existing filter, choose **Edit** and enter the filter number.

```
   ADD  FILTERS ( Device name - IAR2 )
   ------------

     ENTER     -  Enter data
     T         -  Toggle (parameters inside [] )
     N         -  Next line (skip this one)
     SPACE     -  Move right
     BACKSPACE -  Move left
     ESC       -  Return to previous menu

Filter Id -  1
```

4. Set the desired parameters. The available parameters are discussed in the following subsections.

NOTE

Many of the Advanced Filter parameters can be configured according to what are called "True-False Menus." This means that they can be configured so that either frames *with* the parameter (parameter = "true") pass or frames *without* the parameter (parameter = "false") pass. For example, if you choose "BroadCast - True," any frame which *is* BroadCast will pass; if you choose "BroadCast - False," any frame which *is not* BroadCast will pass.

7.7.3.A Filter ID
The system automatically assigns a new number to each filter. This Filter ID number must be entered to view, edit, or delete a filter.

7.7.3.B Protocol
The protocol on which the filter operates (IP, IPX, SNA, etc.). You can also choose to filter for protocols which are not defined in the system.

7.7.3.C Operation
What the filter does with a frame that passes the filtering test: **Forward** or **Block**. These operations are listed in their order of priority. For example, if the forward and block commands are both applied to a frame, the forward command takes precedence.

7.7.3.D Interface
The interface on which the filters will be applied. If you want to filter traffic going to the LAN, choose **LAN**. If you want to filter traffic going to the WAN link, choose **Link**.

7.7.3.E Source Address
The "source address" of any given frame is the address from which that frame was sent. Input a source address (or a range of source addresses) here if you want the IAR2 to filter frames based on their source addresses.

Once you select this parameter, toggle to the desired address type (**MAC** or **NET**). The address format (hexadecimal or binary) appears. Type in the complete source address. If you want to include a group of addresses, type "x" for a given digit to indicate "this can be any number—I don't care." For example, a filter with the MAC source address "4020.D2FE.xxxx" will pass any address beginning with "4020.D2FE." You can also select **IP RANGE** to filter a group of sequential IP addresses. Finally, choose **True** or **False** if you want the frame to be filtered because it *has* or *doesn't have* the specified source address respectively.

7.7.3.F Destination Address
The "destination address" of any given frame is the address to which that frame is being sent. Input a destination address (or a range of destination addresses) here if you want the IAR2 to filter frames based on their destination addresses.

Once you select this parameter, toggle to the desired address type (**MAC**, **NET**, **All**, **BroadCast**, or **MultiCast—**see the next paragraph). The address format (hexadecimal or binary) appears. Type in the complete destination address. You can also select **IP RANGE** to filter a group of sequential IP addresses. Finally, choose **True** or **False** if you want the frame to be filtered because it *has* or *doesn't have* the specified destination address respectively.

Select the "All" address type if you want to filter *all* frames no matter what their destination address is. Select "BroadCast" to filter frames intended for all stations; if you do so, don't specify a mask pattern (see **Section 7.7.3.K**). Select "MultiCast" to filter frames intended for all stations of a certain type.

7.7.3.G High Level (IP Only)
Whether or not you want the IAR2 to filter IP frames based on their high-level protocol, and if so, which protocols. When you choose this parameter, the two choices **Yes** and **No** appear. If you select **Yes**, you need to select which of these high-level protocols you want to filter:

- **FTP**.
- **WWW**.
- **TELNET**.
- **Email**.
- **TFTP**.
- **SNMP**.
- **DNS**.
- **RIP**.

Finally, choose **True** or **False** if you want the frame to be filtered because it *uses* or *doesn't use* the specified destination address respectively.

7.7.3.H Source/Destination Ports/Sockets (IP or IPX Only)
Whether or not you want the IAR2 to filter IP frames based on their port number or IPX frames based on their socket address or number. The behavior of this parameter differs for IP and IPX:

- **IP -** The Destination Port is enabled when no High Level protocol is specified (see **Section 7.7.3.G**). If you define a port number in decimal numbers, be sure to define the Low Level protocol (see **Section 7.7.3.H**) as **UTP** or **TCP**. If no port number is defined, be sure to define the Low Level protocol as **UTP**, **TCP**, or **ICMP**.
- **IPX -** If a socket address or low level protocol is not defined, a socket number may be specified.

Finally, either way, choose **True** or **False** if you want the frame to be filtered because it *uses* or *doesn't use* the specified source/destination port/socket respectively.

7.7.3.J Low Level (IP or IPX Only)
Whether or not you want the IAR2 to filter IP or IPX frames based on their low-level protocol. The behavior of this parameter also differs for IP and IPX:

- **IP -** Toggle to the required low-level protocol for the filter. If the port number is defined in decimal format (see **Section 7.7.3.H**), specify the low level protocol as **UTP** or **TCP**. If the no port number is defined, specify the low level protocol as **UTP**, **TCP**, or **ICMP**.
- **IPX -** Toggle to the required low-level protocol for the filter. If a socket is defined in the destination address, a low level protocol or socket number may not be specified. Conversely, if a socket address or low level is not defined, a socket number may be specified.

Finally, either way, choose **True** or **False** if you want the frame to be filtered because it *uses* or *doesn't use* the specified low-level protocol respectively.

7.7.3.K Mask

A mask is a test pattern that is used to allow certain frame patterns only. You define a code against which the frame is compared. To create a mask, toggle to **Yes**. Three pairs of codes and offsets must be created. The offset defines the point in the frame at which the comparison is made. For example, an offset of **8** means that the 8th byte is compared to the code. The offset can be from the 7th byte onwards.

Each frame has 3 different main portions that you might want to build codes to test for:

- The MAC (Media Access Control) info is at the beginning of the frame.
- The LLC (Logical Link Control) info is after the source address in the frame.
- Data follows the LLC section in the frame.

For each code-offset pair, select the code format:

- **Binary -** specify 48 address bits to be either 0, 1, or X (can be either value).
- **Hexadecimal -** specify 12 hex digits to be 0 through F or X (can be any value).

Finally, choose **True** or **False** if you want the frame to be filtered because it *contains* or *doesn't contain* each specified code-offset pair respectively.

While the IAR2 operates, it compares every frame to the three codes in the mask at the designated offsets. If all three codes and the True-False condition match the values in a given frame, that frame is filtered.

NOTE

Only 1 mask can be defined per filter.

7.7.3.L Status

Whether the filter is currently active or not. Toggle between:

- **Active -** The filter will be applied when the IAR2 is operating.
- **Not Active -** The filter won't be applied right now, but can be saved for later use.

7.7.4 Saving Filter Parameters

All filters are stored in the Internet Access Router 2's Flash memory, thereby preserving them if the power goes down. When filtering is selected, all of the filters are copied into the RAM. The RAM copy is then used to activate the software filtering process. Any filter which is modified goes into effect immediately. The previous filter also remains in effect until the system is rebooted.

To exit the Filters menu and return to the main Setup menu, press Esc. The following prompt appears: 'Do you want to save and apply new setup' (Y/N)? Press **Y** to save changes in the Flash memory. Press **N** to cancel your changes; the system will load the previously existing set of masks the next time the system is rebooted.

7.7.5 Connection on Demand and Spoofing

Although these menus appear on your screen, and you can change and save the settings of their options, they have no effect on current models of the Internet Access Router 2.

7.7.6 Fast Retransmission Frame Limit

This option allows you to set the maximum number of "request for acknowledgement" frames that the Internet Access Router 2 will keep in its buffer. Keeping these frames to a minimum will prevent unnecessary retransmissions on the WAN. The factory-default value is "2."

7.8 Restoring Factory Default Options

The Factory Default Options parameter, shown in Figure 7-39 below, allows you to restore all of the Internet Access Router 2's configuration parameters back to their factory defaults.

Figure 7-39. Outline of the Factory Default Options parameter.

To select this parameter, press **3** at the Main menu, then press **1** at the Advanced menu, then press **6** in the Setup menu. A string of text will appear, prompting you to reset certain parameters (MONITOR, DEVICE ID, MASKS, etc.). Press **Y** to reset those parameters to their factory-default values, or press **N** to leave that set of parameters unchanged. The next prompt string will appear, and so on. Here is the full list:

```
Reset MONITOR parameters to factory default ? (Y/N): Y
Reset DEVICE ID parameters to factory default ? (Y/N): Y
Reset MASKS parameters to factory default ? (Y/N): Y
Reset FORWARDING parameters to factory default ? (Y/N): Y
Reset SPOOFING parameters to factory default ? (Y/N): Y
Reset SNMP parameters to factory default ? (Y/N): Y
Reset LINKS parameters to factory default ? (Y/N): Y
Reset DOWNLOAD parameters to factory default ? (Y/N): Y
Reset COD parameters to factory default ? (Y/N): Y
Reset MODEMS parameters to factory default ? (Y/N): Y
Reset ISDN parameters to factory default ? (Y/N): Y
Reset FRAME RELAY parameters to factory default ? (Y/N): Y
Reset PPP parameters to factory default ? (Y/N): Y
Reset E1T1 parameters to factory default ? (Y/N): Y
Reset HOST IP parameters to factory default ? (Y/N): Y
Reset TELNET parameters to factory default ? (Y/N): Y
Reset RADIUS parameters to factory default ? (Y/N): Y
Reset SECURITY parameters to factory default ? (Y/N): Y
```

Note that although all of these prompt messages will appear for all models of the IAR2, not all of the corresponding parameters are actually available in all models; some, such as the MODEMS and ISDN parameters, are not supported by any models.

Finally you will see these three lines:

```
RESETTING TO FACTORY DEFAULT
On completion the unit will reset automatically
Do you really want to set to factory default ? (Y/N):
```

Press **Y** to complete the factory reset, or press **N** to abort.

7.9 The Device Control Menu

To access the Device Control menu, shown in Figure 7-40 below, press **3** at the Main menu, then press **2** at the Advanced menu. This screen appears:

```
      DEVICE CONTROL  ( Device name - IAR2  )
      --------------

  1.  Software download
  2.  Upload device parameters to TFTP server
  3.  Download device parameters from TFTP server
  4.  Reset options
  5.  Control other device (bridge link only)
  6.  Terminal type

  ESC - Return to previous menu

  Choose one of the above :
```

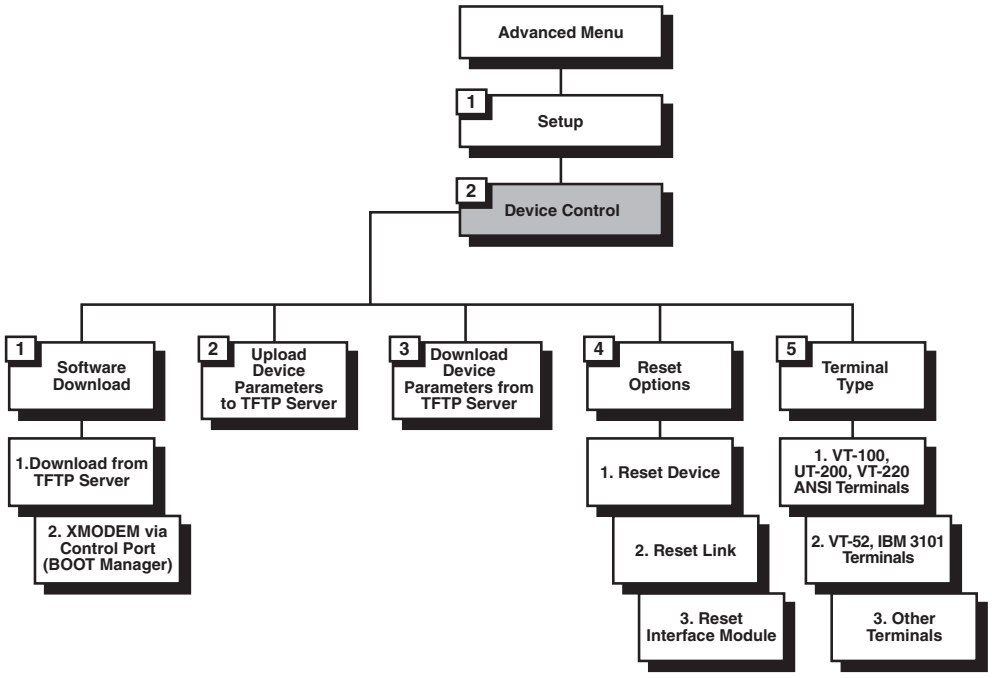


Figure 7-40. Outline of the Device Control menu.

The options in this menu are described in the following subsections.

7.9.1 Software Download

Select this option to download a new software (firmware) version for the Internet Access Router 2. A screen like this appears:

```
      SOFTWARE PARAMETERS IN THE DOWNLOAD (Device name - IAR2 )
      ---------------------------------

  1.  The parameters in the download from TFTP Server
  2.  The parameters in the XMODEM via control port (BOOT Manager)

  ESC - Return to previous menu

  Choose one of the above :
```

The IAR2 has a Dual Image Flash, capable of storing two different versions of its software in two different partitions. Upon reset (or boot, refer to **Appendix B**), the IAR2 automatically runs the program stored in the **active** partition. New software versions are loaded into the **backup** partition. If loading succeeds, the **backup** partition becomes **active** and reset is automatically performed, running the new software version. If loading fails, however, the device will still be capable of working, since the Flash partition storing the old version is still **active**. Refer to Figure 7-41 below.

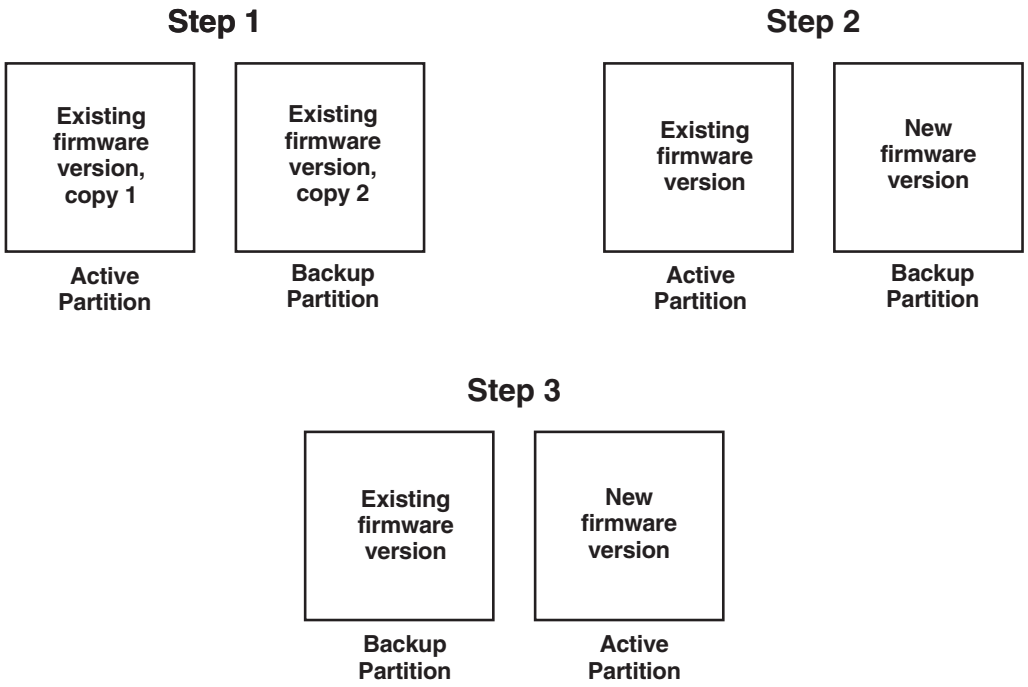


Figure 7-41. Using the Dual Image Flash.

Dual Image Flash can be controlled by the BOOT Manager. You use the BOOT Manager to manually define which is the active and which is the backup partition, to run from the backup partition, to erase some or all information from Flash memory, etc. The BOOT Manager is accessible by choosing option **2** in this menu or immediately after resetting the IAR2. Refer to **Appendix B** for a detailed description of the BOOT Manager.

The two options in the Software Download menu are described in the following pair of subsections.

7.9.1.A Download from TFTP Server

TFTP is an IP/UDP client-server application. The unit is a TFTP client Operating opposite the client, you need a TFTP server connected to the LAN or WAN interface by an IP network, as shown in Figure 7-42 below.

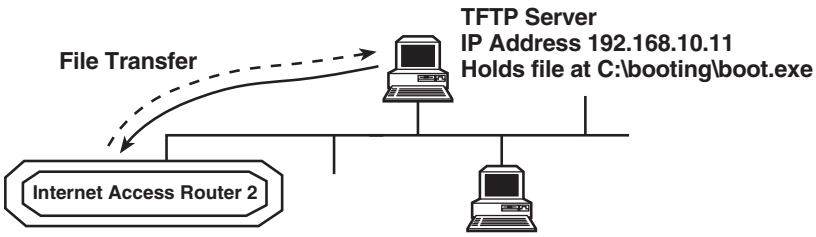


Figure 7-42. Downloading from a TFTP server.

To download a new software version from a TFTP server:

1. Select option **1** from the Software Download menu. This text appears on the screen:

```
Do you want to download new software version? (y/n): Y

TFTP server IP address: 192.168.182.34
New software file name: webebraseb.mbi

Download process will erase the program code
in the second partition of the device.

Upon completion of the download,
the device will be reset automatically.

Press 'S' to start the download process
or
ESC to return to previous menu:
```

2. Make sure that the answer to "Do you want to download new software version? (y/n)" is set to **Y**.
3. In the TFTP Server IP Address field, type the IP address of the TFTP server.
4. In the New Software File Name field, type the path and file name of the new software version.

NOTE

The IP address and the new software version's file name can also be defined through the Advanced → Setup → Host Parameters → TFTP menu. Refer to Section 7.3.4**.**

5. Press **S** to start the download process. During the process, the new program code is downloaded to the Flash **backup** partition, thus erasing its previous contents.

   Upon completion, the newly downloaded Flash partition becomes **active**, while the old version's partition becomes the **backup**. The device automatically resets, running the new program stored in the **active** partition.

   During the download process, a counter shows the number of packets that have passed. Downloading can be interrupted at any time by pressing the ESC key, but this leaves the **backup** partition with destroyed firmware. So you'll need to go into BOOT Manager right away (see **Appendix B**) and choose option **5** to duplicate the **active** partition (thus overwriting the bad **backup** partition—see **Section B.7**).

7.9.1.B Download with XMODEM via Control Port (BOOT Manager)
Use this option to access the BOOT Manager through the Internet Access Router 2's CONTROL port. Refer to **Appendix B** for more information on the Boot Manager.

7.9.2 Upload Device Parameters to TFTP Server

Select this option to save device-configuration parameters to a file by uploading them to a TFTP server, as shown in Figure 7-43 below This operation sends all of the Internet Access Router 2's parameters to the TFTP server, where they are saved under a filename that you specify.

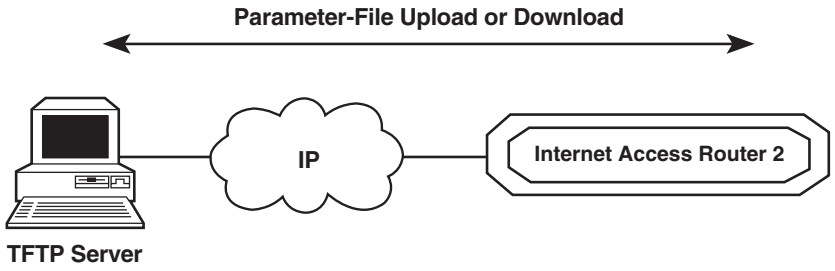


Figure 7-42. Uploading or downloading parameters.

To upload device parameters:

1. Activate the TFTP server application connected to the IAR2 via an IP network.
2. Configure the following IP parameters: IP address, IP mask, and IP default gateway.
3. Select the "Upload device parameters..." option.
4. Enter the TFTP server's IP address.
5. Assign a name to the configuration file you want to save on the server (for example, "iarparam.cfg").
6. Press **S** to start the upload process.

7.9.3 Download Device Parameters from TFTP Server

Select this option to download device-configuration parameters from a file on the TFTP server, as shown in Figure 7-43 above. To download these parameters:

1. Activate the TFTP server application connected to the IAR2 via an IP network.
2. Configure the following IP parameters: IP address, IP mask, and IP default gateway.
3. Select the "Download device parameters..." option.
4. Enter the TFTP server's IP address.
5. Enter the name of the configuration file you want to download from the server.
6. Press **S** to start the download process.

Upon completion of the download process, the IAR2 will reset itself. The new parameters only come into effect after this reset.

7.9.4 Reset Options

Select this option to reset the entire Internet Access Router 2, to reset just the link, or to reset just the interface-module daughterboard.

7.9.5 Terminal Type

Select this option to choose a terminal type. Since each terminal type uses different ASCII control codes for cursor control, the IAR2 requires this information to clearly display the screens clearly on your terminal's or terminal emulator's screen.

8. The View Menu

Use the View Menu, one version of which is shown in Figure 8-1 below, to view the Internet Access Router 2's configuration screens and information on interface connections, routing tables, and statistics. To access the View menu, press **4** at the Main menu. This screen appears:

```
      VIEW  MENU  ( Device name - IAR2  )
      ----------

  1.  Configuration
  2.  Interface connections
  3.  Routing tables
  4.  Statistics
  5.  E1/T1 Diagnostics
  6.  Frame relay DLCIs

  ESC - return to previous menu
```

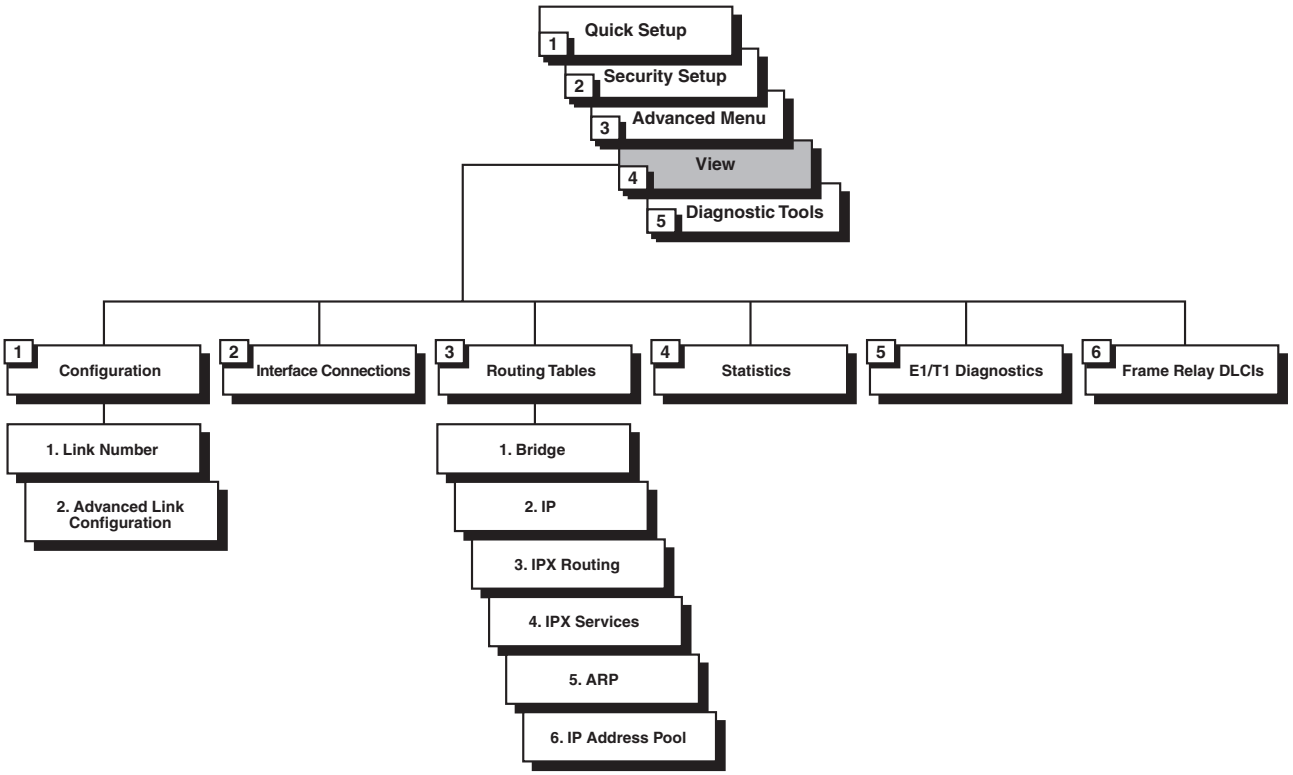


Figure 8-1. Outline of the View menu.

The options in the View menu are described in the following subsections.

8.1 Configuration

Select this option to view the configuration parameters for the Internet Access Router 2 and the WAN links (the parameters that can be entered through the Setup menu—see **Chapter 7**). The Advanced Link Configuration screen displays configuration parameters for a specific link. Since these screens are "display only," you cannot use them to adjust parameters.

8.2 Interface Connections

Select this option to display information about the devices connected to the Internet Access Router 2. The Interface Connections screen includes information about the type of router connected to a specific interface, the name of the router (if available), and the state of the connection.

8.3 Routing Tables

Select this option to display the Internet Access Router 2's various routing tables. When you do, the Routing Tables menu appears:

```
ROUTING TABLES  ( Device name - IAR2  )
--------------

   1.  Bridge
   2.  IP
   3.  IPX Routing
   4.  IPX Services
   5.  ARP
   6.  IP Address Pool

   ESC - Return to previous screen
```

These routing tables are described in the following subsections:

8.3.1 Bridge

Select this option to display a table that contains information on Bridge MAC addresses:

```
     BRIDGE TABLE  (Page-1) ( Device name - IAR2  )
     ------------

   MAC ADDRESS         TYPE                INTERFACE
   ------------        ----                ---------
   0020D2FD5153        Web RANger-II       LAN

   ESC - Return to previous menu
```

8.3.2 IP

Select this option to display a table that contains information on IP routing:

```
       IP TABLE  (Page-1) ( Device name - IAR2  )
       --------

   IP ADDRESS        IP MASK       TYPE  COST      NEXT HOP      AGEING  INTRF
---------------  ---------------  ------ ----  ---------------  -------- ------
192.168.  1. 32  255.255.255.240  INTRF    0   192.168.  2. 33  00:00:00 LAN
192.168.  2. 33  255.255.255.255  INTRF    0   ---------------  00:00:00 LAN
 10. 10. 10.  0  255.255.255.252  INTRF    0    10. 10. 10.  1  00:00:00 1/18
 10. 10. 10.  1  255.255.255.255  INTRF    0   ---------------  00:00:00 1/18

ESC - Return to previous menu
```

8.3.3 IPX Routing

Select this option to display a table that contains information on IPX routing:

```
         IPX ROUTING TABLE (Page-1) ( Device name - IAR2  )
         -----------------

 IPX NET     IPX NODE       TYPE     HOPS  TICKS   AGEING   INTERFACE
 --------  ------------  ----------  ----  -----  --------  -----------
 0000000A  0000C0F5D899  NET (RIP)     1      2   00:00:50  LAN
 0000001B  0000C0F5D899  NET (RIP)     4      5   00:00:50  LAN
 0000001C  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000001D  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000001E  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000001F  0000C0F5D899  NET (RIP)     1      2   00:00:50  LAN
 0000001G  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000001H  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000002I  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000002J  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000003K  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000006L  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000009M  0000C0F5D899  NET (RIP)     2      3   00:00:50  LAN
 0000012N  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000067O  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
 0000083P  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN

 ESC - Return to previous menu
```

8.3.4 IPX Services

Select this option to display a table that contains information on IPX services (SAP table):

```
    IPX SERVICES TABLE  (Page-1) ( Device name - IAR2  )
    ------------------

SERVER  NAME    TYPE IPX NET  HOPS INTERFACE
-------------------------------------------
ACCESS          0004 3381AFCA   2  LAN
ACCOUNTING      0004 0000AAAB   2  LAN
BACKUP          0004 0001267C   2  LAN
ENG             0004 ACE1111D   3  LAN
EXPORT          0004 00AA110E   2  LAN
FDD_EYE         0004 0032142F   1  LAN


  ESC - Return to previous menu , N - next screen
```

8.3.5 ARP Table

Select this option to display a table that shows the correlation between the IP address and the MAC address of each station on the LAN:

```
      ARP TABLE  (Page-1) ( Device name - IAR2)
      ---------

   IP ADDRESS     MAC ADDRESS   AGEING
   ----------     -----------   ------
 192.168.1.33    0020D2FD9F16   00:00:00
 192.168.1.35    0000B431CBD6   00:00:50
 192.168.1.36    0000B471B335   00:02:15
 192.168.1.38    0020D2FD51F0   00:02:15

 ESC - Return to previous menu
```

8.3.6 IP Address Pool

Select this option to display the IP address pool, the group of IP addresses that the Internet Access Router 2 can dynamically allocate, or has allocated, to remote workstations connected to the attached LANs or WANs. This screen will display the time to ready the DHCP server, then these six columns below that:

- **IP Address –** Each IP address in the pool.
- **IP Mask –** The mask that will be applied to each IP address.
- **MAC –** The MAC address corresponding to each IP address.
- **Lease –** The time remaining on the "lease" (station ownership) of each IP address.
- **Status –** Whether each IP address is currently active or not.
- **Interface –** Which of the IAR2's interfaces the device using each IP address is attached to.

8.4 Statistics

Select this option to display information on the traffic between the networks connected by the Internet Access Router 2. These statistics will help you gauge how well the network is performing. (The headline of the screen shown below is not a typo; it actually *does* say, "STATISTICS FOR THE LAST.")

```
 STATISTICS  FOR  THE  LAST            ( Device name - IAR2 )

        LAN 1 STATISTICS (per second)      CURRENT    MAX   AVG
        ----------------
     1) Total network frames
     2) Received good frames
     3) Received good broadcast/multicast
     4) Received masked frames
     5) Transmitted frames
     6) Memory overflow errors
     7) LAN errors
     8) Received missed frames errors
     9) LAN buffers overflow


C - Clear statistics, U - Update average, L - LAN , Link number
     ESC - Return to previous menu
```

8.5 E1/T1 Diagnostics (E1/T1 Models Only)

Select this option to display error information for the Internet Access Router 2's E1/T1 link (if it has one). This information enables you to evaluate the line quality of the E1/T1 line. The errors are accumulated in 15-minute intervals. The IAR2 keeps up to 96 intervals (all of the intervals for the most recent 24-hour period).

In addition, there is a rolling 24-hour total of each error parameter. The rolling total is displayed in the interval parameter called TOTAL. The interval parameter called CURRENT is the open interval (the current 15-minute one). The errors counted in the CURRENT interval are not included in the TOTAL interval. The amount of time that has elapsed in the open interval is displayed on the right of the CURRENT parameter line. T1 diagnostics are available only when frame mode is ESF. E1 diagnostics are available only when CRC-4 is enabled.

```
 Choose link number:

        T1 DIAGNOSTIC - LINK 1 ( Device name - IAR2 )
        ----------------------
INTERVAL    ES    UAS    SES    BES   LOFC    CSS    DM
--------   ----  -----  -----  -----  ----   -----  ----
CURRENT      0     0      0      0      0       0        03.33min
      1      1     0      0      1      0       0
      2      1     0      0      1      0       0
 TOTAL       2     0      0      2      0       0     0



ESC - Return to previous menu | N - Next page |
P - Previous page  |  R - Refresh | C - Clear diagnostics
```

The interval parameters reported in this screen include:

- **Current Errored Seconds (ES)**
  An errored second is any second containing one or more CRC error events, or one or more OOF events, or one or more controlled slip events.
- **Unavailable Seconds Out-Of-Frame (UAS)**
  An unavailable second out-of-frame is any second in which a failed signal state exists. A failed signal state is declared when 10 consecutive severely errored seconds (SES) occur, and is cleared after 10 consecutive seconds of data are processed without a SES.
- **Severely Errored Seconds (SES)**
  A SES is a second with 832 or more CRC error events, or one or more OOF events.
- **Bursty Errored Seconds Out-Of-Frame (BES)**
  A BES is a second with 2 to 831 CRC error events.
- **Current Loss of Frame Counter (LOFC)**
  The loss of frame (LOF) counter counts the "loss of frame alignment" events.
- **Current Slip Second Counter (CSS)**
  A CSS is a second with one or more controlled slip events.
- **Degraded Minutes (DM)**
  The total number of degraded minutes in the current 24-hour interval. A degraded minute is a minute in which the bit error rate (BER) exceeded 1x10-6. This number is updated every minute.

8.6 Frame Relay DLCIs

Select this option to display the Internet Access Router 2's Frame Relay DLCI settings:

```
FRAME RELAY DLCI SETTINGS ( Device name - IAR2  )
-------------------------

 LINK   DLCI   STATE    CIR   EXCESS  THROUGHPUT STATUS
 ----   ----   -----    ---   ------  ----------------
LINK-1   16    Enabled   0    64000        0 UP
LINK-1   17    Enabled   0    64000        0 UP
LINK-1   18    Enabled   0    64000        0 UP




ESC - Return to previous menu
```

9. The Diagnostic Tools Menu

The Internet Access Router 2's Diagnostic Tools menu, whose outline is shown in Figure 9-1 below, currently has one tool in it: a "Ping terminal" function. To access this menu, press **5** at the Main menu. This screen appears:

```
      DIAGNOSTIC TOOLS   ( Device name - IAR2 )
      ----------------

  1.  Ping terminal

   ESC - Return to previous menu


    Choose one of the above:
```

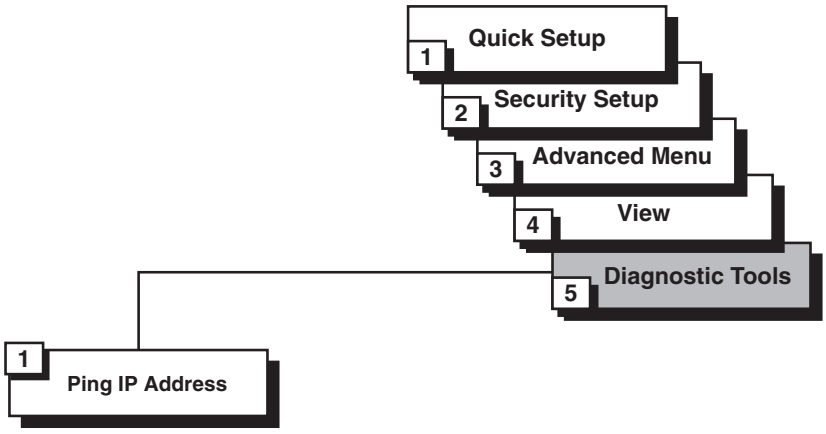


Figure 9-1. Outline of the Diagnostic Tools menu.

This menu's Ping option allows you to confirm IP connectivity by "pinging" (dialing) other IP hosts, as shown in Figure 9-2 below. If there is a reply from the remote IP host, WAN connectivity is confirmed.

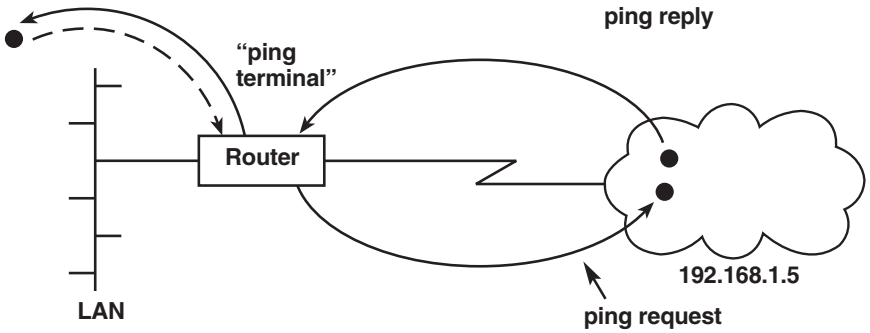


Figure 9-2. Pinging an IP host.

To Ping another host:

1. From the Main Menu, select option **4**. The Diagnostic Tools menu appears.
2. From the Diagnostic Tools menu, select option **1**. You are prompted to enter the IP address of the host.
3. Enter the host's IP address. The IAR2 pings the destination host. A message appears showing the result of the request, as shown below. The IAR2 continues pinging the host until you press ESCAPE.

```
      PING TERMINAL  ( Device name - IAR2  )
      -------------

  Insert the target IP address in the format : xxx.xxx.xxx.xxx

  ESC - Return to previous menu

  Ping IP address: 10.10.10.10



  Pinging 10.10.10.10


  Reply from 10.10.10.10:   time = 0.100 sec
  Reply from 10.10.10.10:   time = 0.050 sec
  Reply from 10.10.10.10:   time = 0.050 sec
  Reply from 10.10.10.10:   time = 0.050 sec


  ESC - Return to previous menu
```

10. Troubleshooting

10.1 Common Problems

Here are some common problems you might encounter with the Internet Access Router 2, along with their possible causes and solutions. If the trouble is chronic, confirm that the IAR2 is configured properly. Also be aware that link errors are sometimes caused by loose contact between connectors or lack of cable continuity. Check that all connectors are plugged in properly and that cable quality is good.

Problem #1: All front-panel indicators are OFF.
Possible Cause: The unit is not receiving power.
Recommended Actions: Check that power is supplied to the unit. Check the fuse and have a qualified technician replace it if necessary.

Problem #2: Red LINK ERROR indicator is blinking.
Possible Causes: In synchronous operation: Corrupted frames are being received, or the physical connection is unstable.
Recommended Action: Check the modem configuration and cables.

Problem #3: Red LINK ERROR indicator is ON.
Possible Cause: The LINK ERROR indicator will be ON if the link is configured in Synchronous mode and no clock signal is being received.
Recommended Actions: Check configuration settings. Check the link-side cables and the configurations of any link-side devices.

Problem #4: Red LAN ERROR indicator is blinking.
Possible Cause: There is a temporary transmission problem.
Recommended Actions: Check cable connections and make sure that the proper cable type is being used.

Problem #5: Red LAN ERROR indicator is ON.
Possible Cause: There is a problem with the LAN connection.
Recommended Action: Check that the LAN is connected properly.

Problem #6: READY indicator is OFF.
Possible Cause: If LAN ERROR indicator is ON, or all LINK ERROR indicators are ON, there is a possible connection problem with the LAN or Link.
Recommended Action: Check LAN and Link connections.

10.2 Calling Black Box

If you determine that your Internet Access Router 2 is malfunctioning, *do not attempt to alter or repair the unit.* It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.
- the results of any testing you've already done.

10.3 Shipping and Packaging

If you need to transport or ship your Internet Access Router 2:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the IAR2 for repair, make sure you include its power cord and the adapter cable(s) you're using with it. If you are returning the IAR2, make sure you include everything you received with it. Before you ship, contact Black Box to get a Return Authorization (RA) number.

Appendix A: Pinouts

This appendix lists the pinouts of the Internet Access Router 2's WAN-link interfaces and its CONTROL interface.

A.1 The Regular Serial Interfaces: V.35, RS-530, X.21

The WAN links of -U35 and -2U35 models of the Internet Access Router 2 are native V.35 interfaces, expressed as M/34 female connectors. The WAN links of -U21 and -2U21 models are native RS-530 interfaces expressed as DB25 female connectors; these are patched with an included adapter cable (whose pinout is shown in Table A-2 on the next page) to X.21 interfaces expressed as DB15 female connectors. The signals supported by these interfaces are shown in Table A-1 below, cross-referenced to their ITU-T V.24 circuit numbers.

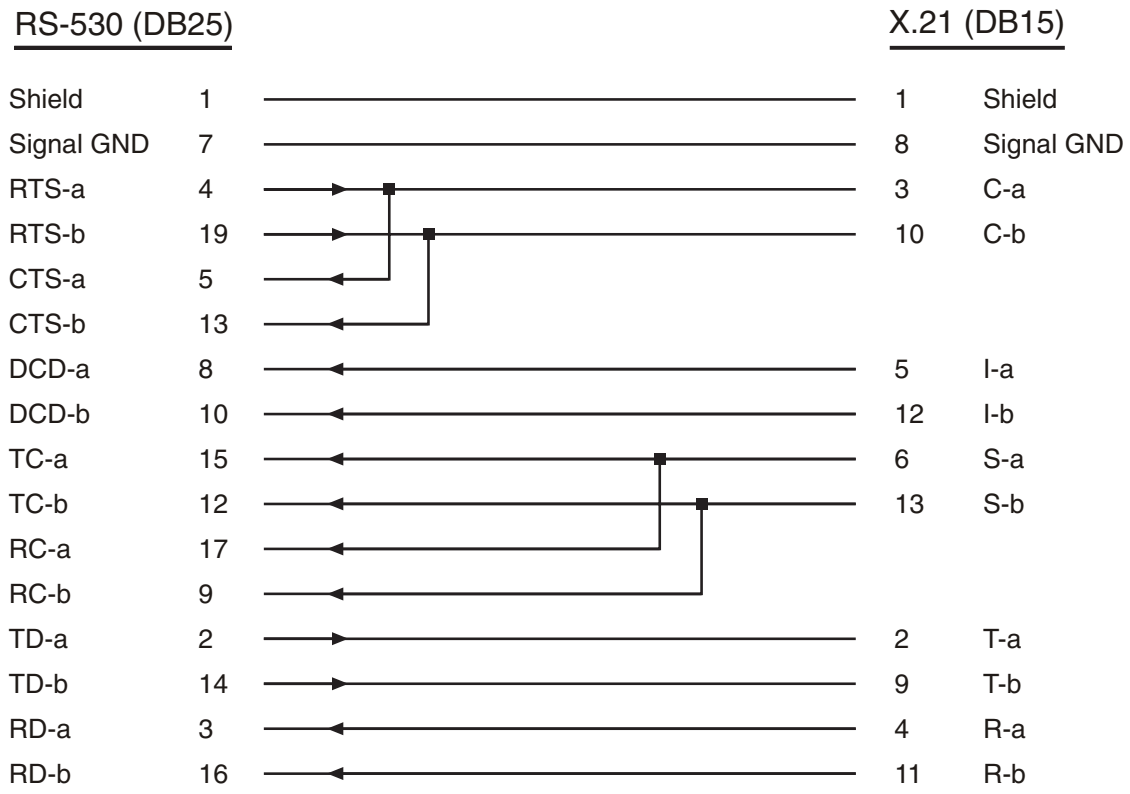
Table A-1. The Supported V.35, RS-530, and X.21 Signals

ITU-T V.24	ITU-T V.35 (M/34 F)			EIA/TIA RS-530 (DB25 F)			ITU-T X.21 (DB15 F)		
CIRC. REF.	PIN	ABBR.	NAME	PIN	ABBR.	NAME	PIN	ABBR.	NAME
101	A	FGND	Frame Ground	1	SHD	Shield	1	—	Shield
102	B	SGND	Signal Ground	7	SGND	Signal Ground	8	G	Signal Ground
103	P	SD (A)	Send Data A	2	TD (A)	Transmitted Data A	2	T (A)	Transmit A
	S	SD (B)	Send Data B	14	TD (B)	Transmitted Data B	9	T (B)	Transmit B
104	R	RD (A)	Receive Data A	3	RD (A)	Received Data A	3	R (A)	Receive A
	T	RD (B)	Receive Data B	16	RD (B)	Received Data B	10	R (B)	Receive B
105	C	RTS	Request to Send	4	RTS (A)	Request to Send A	4	C (A)	Control A*
				19	RTS (B)	Request to Send B	11	C (B)	Control B*
106	D	CTS	Clear to Send	5	CTS (A)	Clear to Send A	4	C (A)	Control A*
				13	CTS (B)	Clear to Send B	11	C (B)	Control B*
107	E	DSR	Data Set Ready	6	DSR (A)	Data Set Ready A	—	—	—
				22	DSR (B)	Data Set Ready B			
108.2	H	DTR	Data Terminal Ready	20	DTR (A)	Data Terminal Ready A	—	—	—
				23	DTR (B)	Data Terminal Ready B			
109	F	CD	Carrier Detect	8	CD (A)	Carrier Detect A	5	I (A)	Indication A
				10	CD (B)	Carrier Detect B	12	I (A)	Indication B
114	Y	SCT (A)	Serial Clock Tmit. A	15	TC (A)	Transmit Clock A	6	S (A)	Signal Timing A†
	AA	SCT (B)	Serial Clock Tmit. B	12	TC (B)	Transmit Clock B	13	S (B)	Signal Timing B†
115	V	SCR (A)	Serial Clock Rcv. A	17	RC (A)	Receive Clock A	6	S (A)	Signal Timing A†
	X	SCR (B)	Serial Clock Rcv. B	9	RC (B)	Receive Clock B	13	S (B)	Signal Timing B†

* In X.21 models of the IAR2, the X.21 Control leads are used for flow-control signaling in both directions; they carry RS-530 Ready to Send signals sent *from* the IAR2 as well as RS-530 Clear to Send signals sent *to* the IAR2. See Table A-2 on the next page.

† In X.21 models of the IAR2, which must be DTE, the X.21 Signal Timing leads are used *only to receive clock signaling* from an attached DCE, even though the adapter cable patches them to both the Receive Clock *and* Transmit Clock leads on the IAR2's native RS-530 connector. See Table A-2 on the next page.

Table A-2. Pinout of the RS-530 to X.21 Adapter Cable



A.2 E1/T1 Connectors

On E1 models of the Internet Access Router 2, the unbalanced interface of the E1 main link and sublink are terminated with two BNC female connectors. The connectors are designated RX-IN and TX-OUT.

The balanced interfaces of the E1 and T1 main links and sublinks are terminated with an RJ-48C connector, wired in accordance with Table A-3 below. (Note that in order to connect a PABX to a sublink you should use a cross-pinned cable.)

Table A-3. Pinout of the E1/T1 Main-Link and Sublink Connectors

Pin	Designation	Direction	Function
1	RX (T)	Input	Receive data (tip)
2	RX (R)	Input	Receive data (ring)
3	FGND	N/A	Frame ground
4	TX (T)	Output	Transmit data (tip)
5	TX (R)	Output	Transmit data (ring)
6	FGND	N/A	Frame ground
7,8			(Not connected)

A.3 The CONTROL Port and Its Adapter Cables

The Internet Access Router 2's front-mounted CONTROL port is an RS-232 DCE interface proprietarily pinned on an RJ-45 female connector. The pinout of this connector, as well as that of the adapter cables (RJ-45-to-DB9 and RJ-45-to-DB25) that can come with the IAR2 for connection to this port, are shown in Table A-4 below. Note that the CONTROL port itself is pinned as a DTE, while the connector at the other end of the adapter cable is pinned as DCE.

Table A-4. Pinout of the CONTROL Port and Its Associated Cables

RJ-45 Pin	Signal Abbrev.	Signal Name		To DB25 Pin	To DB9 Pin	Signal Abbrev.
4	SGND	Signal Ground	———	7	5	SGND
5	TD	Transmitted Data	→	3	2	RD
6	RD	Received Data	←	2	3	TD
7	RTS	Request to Send	→	5	8	CTS
8	CTS	Clear to Send	←	4	7	RTS

Appendix B: BOOT Manager

B.1 Introduction

The Internet Access Router has a Dual Image Flash memory capable of storing two different versions of its software (firmware) in two different partitions. When it's reset, the IAR2 automatically runs the program stored in the **active** partition. When new software versions become available, you can download them into the **backup** partition. If a download succeeds, the **backup** partition becomes the **active** partition and the IAR2 is reset automatically and begins running the new software version. If loading fails, the device is still capable of working, since the Flash partition storing the old version remains active.

This is where the IAR2's BOOT Manager comes in: You can use it to control the Dual Image Flash. With the BOOT Manager, you can:

- Download new software.
- Manually define the active and backup partitions.
- Run the backup partition.
- Erase some or all information from Flash.

B.2 Accessing BOOT Manager

You can access BOOT Manager in either of two ways:

1. The normal procedure works like this: From the Internet Access Router 2's Advanced menu, press **3** to bring up the Device Control menu, then press **4** to bring up the Software Download menu, then press **2** for the BOOT Manager menu (shown below).
2. If the IAR2 is not functioning properly, or if for whatever other reason you can't get to the BOOT Manager menu, make sure your terminal or terminal emulator is running and is connected to the IAR2, then switch the IAR2 off and back ON again, then immediately press "R" on your keyboard. This should trigger "Rescue" mode, which should cause the BOOT Manager menu to appear:

```
BOOT 302 Version 1.04 (Jan 27 1998)
Active : 1998 Apr 16 14:56 WEBEB.X
Backup : 1998 Apr 16 14:56 WEBEB.X

1) Load new software
2) Partitions status
3) Run backup partition
4) Reactivate backup partition
5) Duplicate active partition
6) Erase configuration
7) Erase all FLASH
8) Set baud rate

0) Exit

   ESC - Return to previous menu

   Choose one of the above:
```

B.3 Load New Software

Select this option to download new software to the Internet Access Router 2 through its the control port using the XMODEM protocol. During the download process, the new program code is downloaded to the Flash backup partition, thus erasing its previous contents.

Upon completion, the newly downloaded Flash partition becomes the active partition, while the old version's partition becomes the backup partition. The device automatically resets, running the new program stored in the active partition, as shown in Figure B-1 below.

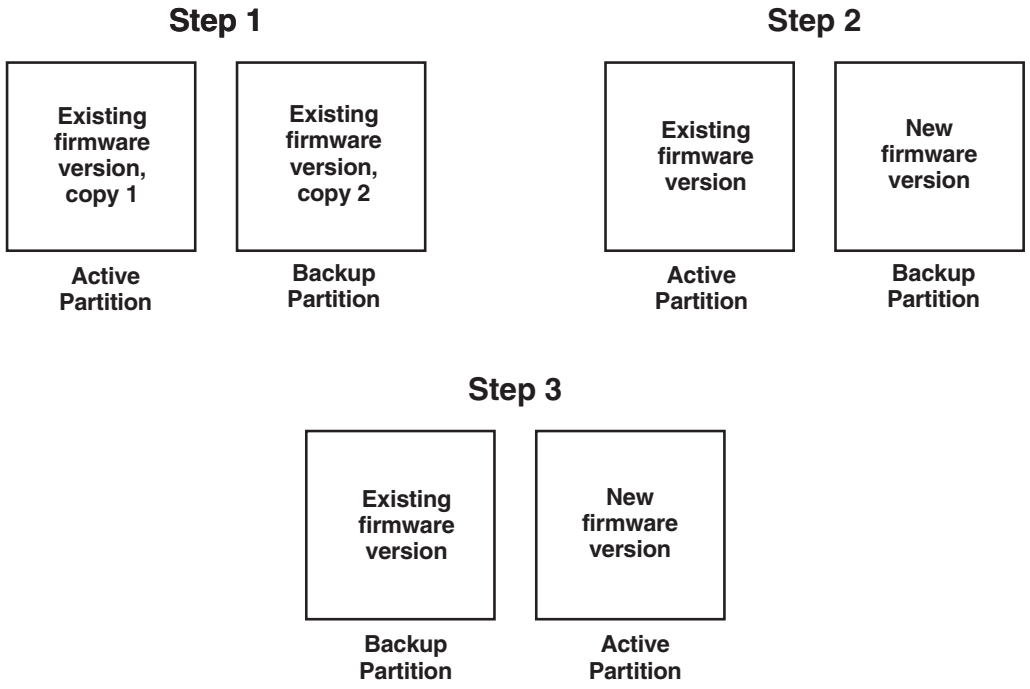


Figure B-1. Using the Dual Image Flash.

B.4 Partitions Status

Select this option to display information about the status of the active and backup Flash partitions (note that the top of the BOOT Manager menu also displays a partial status):

```
Active : 1998 Apr 16 14:56 WEBEB.X
Backup : 1998 Apr 16 14:56 WEBEB.X
```

B.5 Run Backup Partition

Select this option to run the program stored in the backup partition of the Flash memory. Normally that program is the previous software version. This "backup" program runs once. After the next hardware reset or reboot, the IAR2 will run the program stored in the active partition.

B.6 Reactivate Backup Partition

Select this option to turn the backup partition into the active partition (and vice versa). In this way you can return to the previous software version permanently. This command may be executed up to 16 times, after which you *must* download new software. Therefore avoid using this option for a one-time run of the old version (use the Run Backup Partition option for that purpose—see **Section B.5**).

B.7 Duplicate Active Partition

Select this option to copy the program stored in the active partition into the backup partition.

B.8 Erase Configuration

Select this option to erase the IAR2's configuration parameters, which are also stored in the flash memory. Sometimes these configuration parameters are needed after downloading a new version of BOOT Manager. When the new version's parameter set is not fully compatible with the previous version's parameters, then you need to erase the previous version's parameters. You can also use this command to set the IAR2 to its default settings, and it will also come in very handy if you forget the IAR2's password.

B.9 Erase All FLASH

Select this option to erase everything in the IAR2's Flash memory: the IAR2's configuration parameters and the programs stored in both partitions. After doing this, you *must* download new software before attempting to operate the device.

B.10 Set Baud Rate

Select this option to set the IAR2's CONTROL-port baud rate (data rate) to either **9.6**, **19.2**, **38.4**, **57.6**, or **115.2 kbps**. For software downloads, the rate *must* be set higher than 9.6 kbps; we recommend that you use the highest rate your computer is capable of.

Once you change the IAR2's baud rate, you must change your computer's rate to match. Once you do so, ppress Enter several times to make sure that the computer and the IAR2 are communicating properly at the new rate.

CAUTION!

If you're using the Windows® 95 version of HyperTerminal™, be aware that it might have a bug that affects this process. After changing the baud rate for HyperTerminal, its status line will show the new value, but the new rate might not come into effect unless you perform the disconnect and connect commands immediately after making the change.

B.11 Exit

Select this option to exit the BOOT Manager menu and reboot the IAR2. (If the BOOT Manager is idle for more than two minutes, exit is performed automatically.)

Appendix C: How Single IP Works

C.1 Overview

In order to set up your small-office LAN connection to your IP provider quickly and easily, read this section to understand how Single IP works.

A typical Internet Access Router 2 system like the one shown in Figure C-1 below is made up of:

- A LAN.
- An IAR2.
- An optional CSU/DSU or other intermediary device.
- A public access service such as PSTN or Frame Relay.
- An Internet Service Provider or intranet access point.

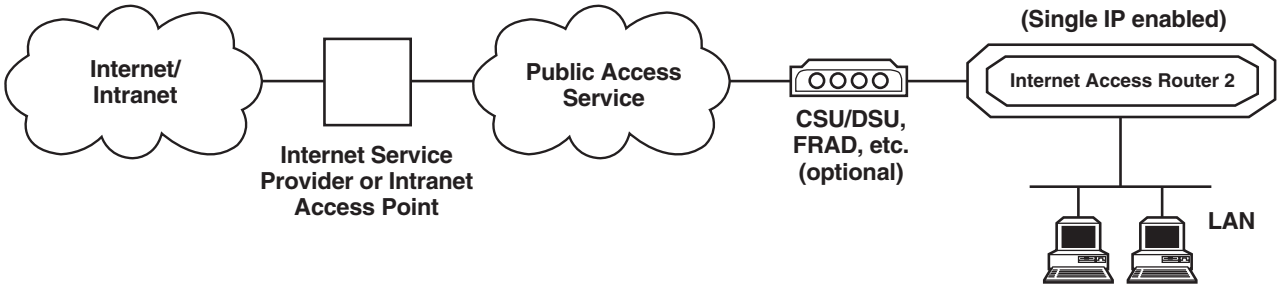


Figure C-1. Setup of sample system using Single IP.

LAN

The user stations are connected to the LAN. Each user station requires its own unique host IP address.

IAR2

IAR2 is connected to the small-office LAN via its LAN port(s). It has its own local IP address which you configure. The local IP host address of the IAR2 must belong to the same IP subnet as the other stations on the LAN. The IAR2's subnet mask must also be the same as that of the other stations on the LAN.

PUBLIC ACCESS SERVICE

The IAR2 can be used over a wide variety of WAN links, including DDS and Frame Relay. You may require a CSU/DSU, FRAD, etc., to make this connection, depending on the type of link used.

INTERNET SERVICE PROVIDER OR INTRANET ACCESS POINT

The IAR2 is designed to access an Internet or intranet router on the other side of the Public Access Service. This remote router can be any router that supports standard PPP and IPCP. When the IAR2 establishes a connection to the remote router, the IAR2 dynamically obtains a single IP address from it using the IPCP

protocol. The IAR2 releases this temporary IP address when it disconnects. The temporarily assigned IP address is not the same as the locally assigned host IP address which you assigned to IAR2 during the first installation, as shown in Figure C-2 below.

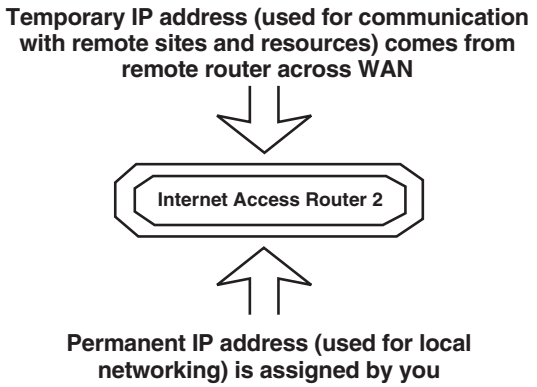


Figure C-2. IP addressing in Single IP mode.

C.2 IP Functionality

The Internet Access Router 2 is a dedicated IP access router for the small office. Familiarization with the following terms will assist you in gaining the most benefit from your IAR2 installation.

TCP is the most common transport layer protocol used on Ethernet and the Internet. TCP is built on top of Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication, flow-control, multiplexing, and connection-oriented communication. It provides full-duplex, process-to-process connections. TCP is defined in STD 7, the Internet Engineering Task Force (IETF)'s RFC 793 document.

UDP is an Internet standard for network-layer, transport-layer, and session-layer protocols. These components provide simple but unreliable datagram services. UDP adds a checksum and additional process-to-process addressing information; it's a connectionless protocol which, like TCP, is layered on top of IP. It's defined in STD 6, RFC 768.

Each **IP Address** is a 32-bit host address. It is usually represented in dotted decimal notation, for example "128.121.4.5." The address can be split into a network number (or network address) and a host number unique to each host on the network, plus sometimes also a subnet address. IP Addressing is defined in RFC 791.

IP Ports are logical ports on a computer used to connect the computer with a server.

DNS is a general-purpose distributed, replicated data-query service chiefly used on the Internet for translating hostnames into Internet IP addresses. DNS is defined in STD 13, RFCs 1034 and 1035.

C.3 Implementing Single IP

C.3.1 IP Provider Concerns

The Internet Access Router 2 must first be configured to connect to the IP provider over the link layer (Frame Relay, DDS, etc.). Refer to **Chapter 5** for instructions on connecting the IAR2 to your link.

The IAR2 has a built-in utility called Ping Terminal (see **Chapter 9**). After configuring Single IP, we recommend that you use Ping Terminal to confirm that IP connectivity between the IAR2 and the rest of the Internet or intranet is correct, as shown Figure C-3 below. Pinging should be done before configuring the LAN.

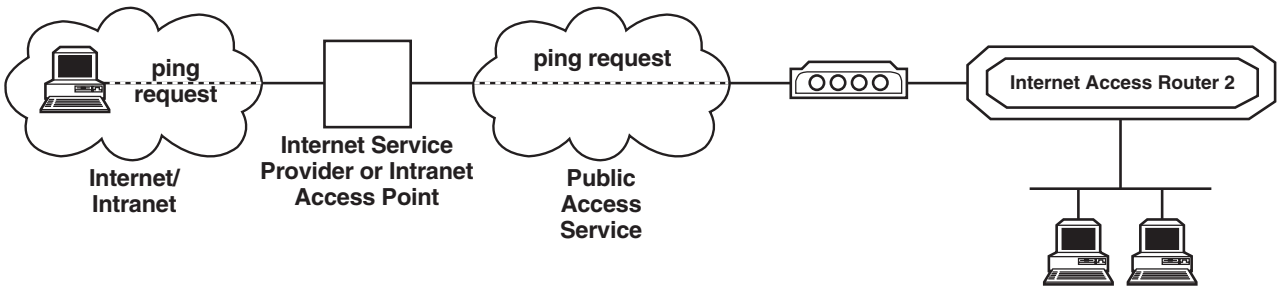


Figure C-3. Pinging an IP host on the Internet/intranet.

C.3.2 LAN and IP addresses

Although Single IP operation is almost completely independent of the LAN, you need to make sure that each station on the LAN has an IP address assigned to its LAN port. Each station should have its own unique IP address within the LAN.

Any IP address can be used as a host IP address for the stations on the LAN, provided that it follows the rules in this section. However, if the same IP subnet is used on the small-office LAN and also somewhere else in the Internet, and if you try to start an IP session between one of your LAN stations and a station on that other same-numbered subnet, that specific traffic will not get past the IAR2.

The reason for this is that the IAR2 inspects the source and destination subnet of every IP packet sent from the small-office LAN. If the source and destination subnets are the same, the Single IP will not transfer the packet to the IP provider.

To solve this problem, you can use subnets which are called Private Addresses. These addresses are guaranteed by the IP standard in RFC 1918 not to be used by "legal" IP stations on the Internet. Private Addresses are reserved for stations which "hide" behind gateways such as the IAR2.

Private Addresses exist in the range from 192.168.0.0 through to 192.168.255.255. For a small-office LAN, you can use the subnet mask 255.255.255.0 to allow up to 256 stations on the LAN. Because the IAR2 is the "first" device in the LAN, we recommend that you give the IAR2 a host IP address of 1 during Quick Setup.

For example (refer to Figure C-4 below): Three PCs want to connect to the Internet using Single IP. Assign 192.168.1.1 as the Single IP host IP address. For the first PC, allocate an address of 192.168.1.2; use 192.168.1.3 for the second PC's address and 192.168.1.4 as the third PC's address. Set the subnet mask for the Single IP and all the PCs to 255.255.255.0.

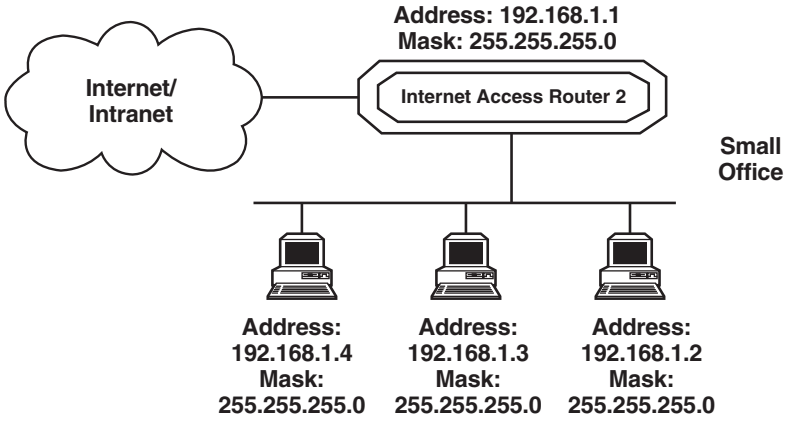


Figure C-4. Setting up Single IP addressing.

C.3.3 The LAN and DNSs

When a user on the small-office LAN generates IP traffic, the Internet Access Router 2 automatically checks whether the traffic is destined for a station outside the small office. If it is, the IAR2 automatically dials up the IP provider and transfers the traffic to the IP provider's router.

If you generate traffic for a named destination, such as http://www.blackbox.com (our Web site), a DNS server somewhere on the Internet needs to translate the specific destination name into an IP address which is used in all subsequent packets. Small offices with Single IP will usually utilize the DNS server of the IP provider to do this. Therefore we recommend that you configure the DNS address for all users on the small-office LAN with the IP address of the DNS server at the IP provider's site, as shown in Figure C-5 on the next page.

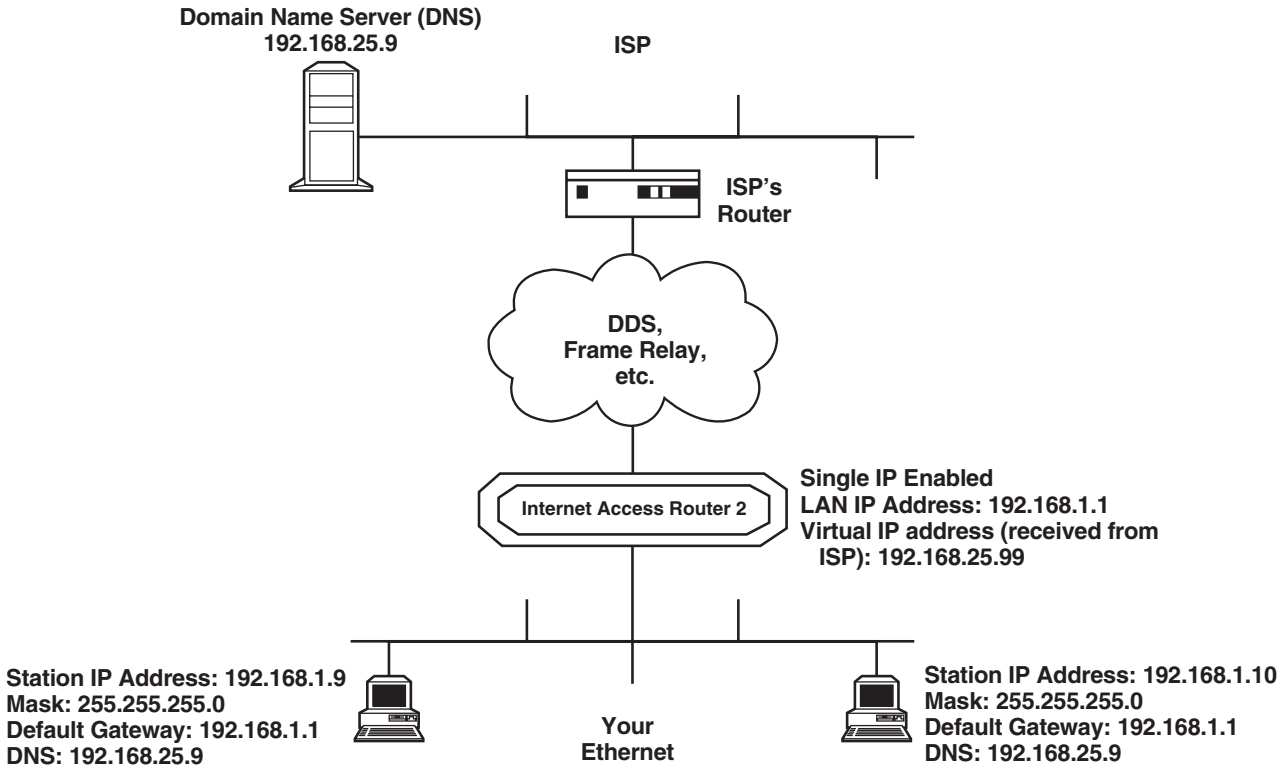


Figure 7-5. Typical office setup with Single IP.

C.4 Frequently Asked Questions About Single IP

Can I use computers running Windows, UNIX®, Mac® OS, or OS/400® on my LAN?
Yes, you can. In fact, you can use any operating system that supports TCP/IP.

Can I run other protocols such as IPX/SPX on my LAN as well?
Yes, you can. If you are running Microsoft networking software, it supports multiple simultaneous protocols. You may find that you get better response on your LAN if you enable NetBEUI and set it as your default protocol. (The default protocol is the first protocol that Microsoft Windows networking will try to connect with, except for sockets applications, which only support TCP/IP. The default protocol will be used for your local LAN traffic and is slightly more efficient than TCP/IP.)

If you are running Novell® NetWare®, you will probably want to enable IPX/SPX.

Can I ping anything on the Internet from my LAN?
Yes, you can. However, you cannot ping from the Internet into the LAN when using Single IP.

When I use Single IP, why does the IAR2 sometimes dial out apparently with no reason?
The IAR2 only dials out when it is trying to connect to something. If the IAR2 seems to dial out for no reason, it's because the unit is trying to perform DNS forwarding. To solve this problem, place an entry in the host file of every LAN station which points to a local DNS on the LAN.

Why can't I ping anything on my small-office LAN from the Internet?
When Single IP is enabled, pinging your units is not possible. Your small-office LAN does not exist as far as the global Internet is concerned. The Single IP feature blocks all access initiated from outside the small office towards the LAN.

Why can't I get RealAudio® and some UDP clients to work?
Make sure that your RealAudio application is configured to work in TCP mode and not in UDP mode.

Glossary

10BASE-T - An Ethernet LAN interface that allows stations to be attached with twisted-pair cable.

ARP (Address Resolution Protocol) - A method for finding a host's Ethernet address from its Internet address. The sender broadcasts an ARP packet containing the Internet address of another host and waits for the second host to send back its Ethernet address. Defined in RFC 826.

Bandwidth - The total data-carrying capacity of a WAN link. The greater the bandwidth, the more information can be sent through the link at a particular time.

Bridging - The forwarding of traffic between network segments based on data-link-layer information. These segments have a common network-layer address.

Broadcast - A transmission to multiple, unspecified recipients. On an Ethernet network, a broadcast packet is a special type of multicast packet which all nodes on the network are always willing to receive.

Default Gateway - A routing-table entry which is used to direct packets addressed to hosts or networks not explicitly listed in the routing table.

DLCI (Data Link Control Identifier) - A channel number which is attached to data frames to tell the network how to route the data in Frame Relay Networks.

DNS (Domain Name System) - A general-purpose, distributed, replicated data-query service chiefly used on the Internet for translating hostnames into Internet IP addresses. Defined in STD 13, RFCs 1034 and 1035.

Dynamic Station - A host which is added automatically to an ARP or LAN table.

E1/T1 - Two services that provide high-speed WAN connections. E1, widely used in Europe, has a top speed of 2.048 Mbps; T1, used in North America, has a top speed of 1.544 Mbps. E1 and T1 support Frame Relay, PPP, and HDLC, providing the flexibility to support high-performance point-to-point or multipoint WAN topologies.

Firewall - A system that controls access to or from a protected local network. It implements a network-access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

Frame Relay - A packet-switching protocol for connecting devices on a WAN.

IP Address - The 32-bit address assigned to a host on an IP network. It is usually represented in dotted decimal notation, for example "128.121.4.5". The address can be split into a network number (or network address) and a host number unique to each host on that network, as well as sometimes a subnet address also. Defined in RFC 791.

IP Mask - A unique 4-byte (32-bit) value that allow the recipient of IP packets to distinguish between different host IDs.

IP/IPX Routing - The process, performed by a router, of selecting the correct interface and next hop for a packet being forwarded. Routing is done in order to send a packet to a specific destination.

IPX (Internetwork Packet Exchange) - A network-layer protocol used in the Novell NetWare file-server operating system. A router with IPX routing can interconnect LANs so that NetWare clients and servers can communicate.

Leased Line - A private telephone circuit permanently connecting two points, normally provided on a lease basis by a local telephone company.

MAC (Media Access Control) - The lower sublayer of the data-link layer. MAC is the interface between a node's Logical Link Control and the network's physical layer. The MAC differs for various physical media.

MAC Address - The hardware address of a device connected to a shared network medium.

Mask - A filtering aid used to define classes of addresses. By defining classes, any packet can be judged as to whether it should pass the filter or not.

MTU (Maximum Transmit Unit) - The largest frame length which may be sent on a physical medium.

Multicast - An Ethernet addressing scheme used to send packets to devices of a certain type or for broadcasting to all nodes.

NCP® (NetWare Core Protocol®) - A Novell trademark for the protocol used to access Novell NetWare file- and print-service functions. NCP uses an underlying IPX or IP transport protocol.

NetBEUI (NetBIOS Extended User Interface) - The network-transport protocol used by all Microsoft network systems and IBM® LAN Server® based systems.

Parity Bit - An extra bit added to a byte or word to reveal errors in storage (in RAM or disk) or transmission. "Even parity" means that the parity bit is set to maintain an even number of one bits in the word, including the parity bit. "Odd parity" means that the parity bit is set to maintain an odd number of one bits in the word, including the parity bit.

PPP (Point to Point Protocol) - The Internet standard protocol for transmitting network-layer datagrams such as IP packets over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems; it can configure connections to a remote network dynamically, and test that the link is usable. PPP can be configured to encapsulate different network-layer protocols (such as IP, IPX, or AppleTalk). Defined in RFC 1661.

Protocol - A set of formal rules describing how to transmit data across a network. Low-level protocols define the electrical and physical standards to be observed; bit and byte ordering; and the transmission, error detection, and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, terminal-to-computer-dialogue, character sets, sequencing of messages, etc.

PSTN (Public Switched Telephone Network) - The collection of interconnected systems operated by the various telephone companies and administrations around the world.

RFC (Request for Comment) - One of many numbered Internet informational documents and standards widely followed and adopted by commercial software and freeware developers in the Internet and UNIX communities.

RIP (Routing Information Protocol) - The companion protocol to IPX for exchange of routing information in a NetWare network. It is not related to the Internet protocol of the same name.

SAP (Service Access Point) - The OSI term for the component of a network address which identifies the individual application on a host which is sending or receiving a packet.

SNMP (Simple Network Management Protocol) - The Internet standard protocol developed to manage nodes across an IP network. Defined in STD 15, RFC 1157.

SOCKS - A security package that allows a host behind a firewall to use browsers, FTP, Telnet, and other Internet applications to access resources outside the firewall while maintaining the security requirements.

Spoofing - A technique used to reduce network overhead, especially in a WAN, that works this way: Some network protocols send frequent packets for management purposes. These can be routing updates or keep-alive messages. In a WAN this can introduce significant overhead, due to the typically smaller bandwidth of WAN connections. Spoofing reduces the required bandwidth by having devices, such as bridges or routers, answer for the remote devices. This fools (spoofs) the LAN device into thinking the remote LAN is still connected, even though it's not. The spoofing saves WAN bandwidth, because the extra management packets are not sent out on the WAN.

SPX (Sequenced Packet Exchange) - A transport-layer protocol built on top of IPX. It's used in Novell NetWare systems for communications in client/server application programs such as the BTRIEVE ISAM manager.

Static Station - A static station is a host which is added manually to an ARP or LAN table.

Stop Bit - A bit that marks the end of a unit of transmission (normally a byte or character) in asynchronous communication. In serial communications, where each bit of the message is transmitted in sequence, stop bits are extra "1" bits which follow the data bits and any parity bit.

Synchronous Transmission - Transmission of data bits at fixed, clocked rate. The sender and the receiver are synchronized to the same clock signal.

TCP (Transmission Control Protocol) - The most common transport-layer protocol used on Ethernet networks and on the Internet. TCP is built on top of Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication, flow-control, multiplexing and connection-oriented communication. It provides full-duplex, process-to-process connections. Defined in STD 7, RFC 793.

TCP/IP (Transmission Control Protocol over Internet Protocol) stack - The standard Ethernet protocols originally incorporated into 4.2 BSD UNIX. While TCP and IP specify two protocols at specific layers, TCP/IP is often used to refer to the entire Internet protocol suite based upon these, including Telnet, FTP, UDP and RDP.

TFTP (Trivial File Transfer Protocol) - A simple file-transfer protocol used for downloading boot code to diskless workstations.

Throughput - The amount of data a communications channel can actually deliver from one end of the channel to the other, often measured in bytes per second.

UDP (User Datagram Protocol) - An Internet standard network-layer, transport-layer, and session-layer protocol which provides simple but unreliable datagram services. It adds a checksum and additional process-to-process addressing information. UDP is a connectionless protocol which, like TCP, is layered on top of IP. Defined in STD 6, RFC 768.

WAN (Wide Area Network) - A network not confined within a single site, extending over distances greater than one kilometer.