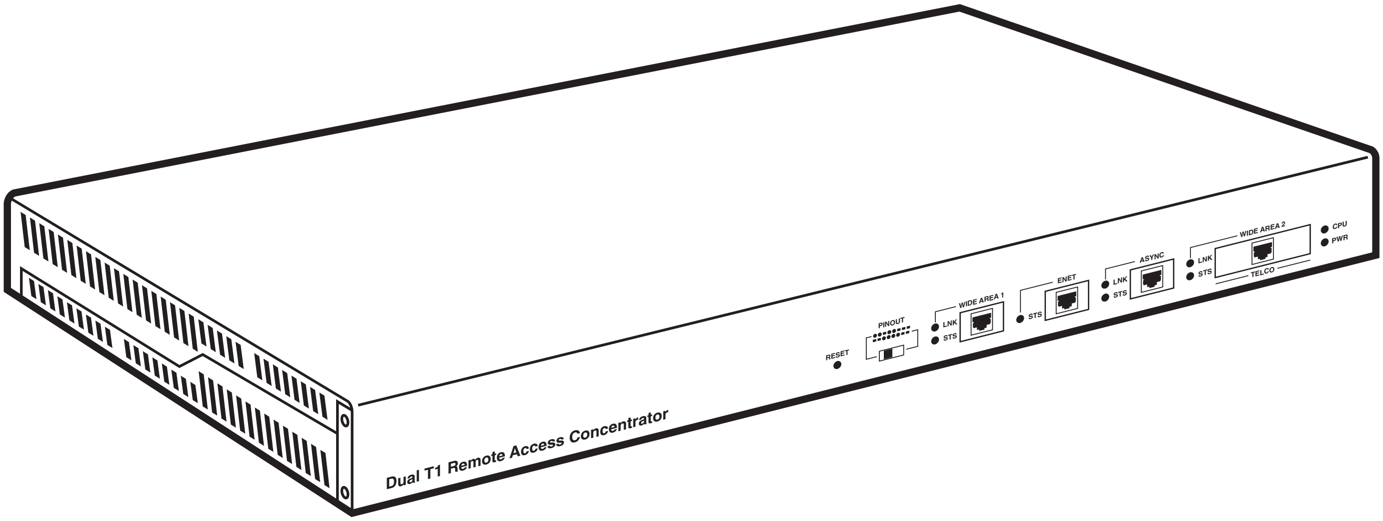
BLACK BOX®
NETWORK SERVICES

MAY 2000
LRA3000A
LRA3001A
LRA3002A
LRA3003A

T1 and E1 Remote Access Concentrators



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 (FCC), INDUSTRY CANADA (IC), AND VOLUNTARY CONTROL COUNCIL FOR INTERFERENCE (VCCI) 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 J 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.

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

EUROPEAN UNION DECLARATION OF CONFORMITY

This equipment has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in the European standard EN 55022. These limits are designed to provide reasonable protection against harmful interference. This equipment generates, uses and can radiate radio-frequency energy, and if not installed and used in accordance with the instructions, might cause harmful interference to radio or television reception. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, you can correct the interference with one or more of the following measures:

(a) Reorient or relocate the receiving antenna.

(b) Increase the separation between the equipment and the receiver.

(c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

(d) Consult the supplier or an experienced radio/TV technician for help.

This equipment has also been tested and found to comply with European standard EN 50082-1:1992.

NORMAS OFICIALES MEXICANAS ELECTRICAL-SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

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.

FCC REQUIREMENTS FOR TELEPHONE-LINE EQUIPMENT

1. The Federal Communications Commission (FCC) has established rules which permit this device to be directly connected to the telephone network with standardized jacks. This equipment should not be used on party lines or coin lines.

2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until the repair has been made. If this is not done, the telephone company may temporarily disconnect service.

3. If you have problems with your telephone equipment after installing this device, disconnect this device from the line to see if it is causing the problem. If it is, contact Black Box.

4. The telephone company may make changes in its technical operations and procedures. If any such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You'll also be advised of your right to file an FCC complaint.

5. If the telephone company requests information on what equipment is connected to their lines, inform them of:

   a. The telephone number that this unit is connected to.

   b. The ringer equivalence number.

   c. The USOC jack required: RJ-11C.

   d. The FCC registration number.

   Items (b) and (d) can be found on the unit's FCC label. The ringer equivalence number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the RENs of all devices on any one line should not exceed five (5). If too many devices are attached, they may not ring properly.

6. In the event of an equipment malfunction, all repairs should be performed by Black Box. It is your responsibility to tell us that your equipment needs to be serviced.

CERTIFICATION NOTICE FOR TELEPHONE-LINE EQUIPMENT USED IN CANADA

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications-network protective, operational, and safety requirements. Industry Canada does not guarantee the equipment will operate to your satisfaction.

Before installing this equipment, you should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (extension cord). Be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized maintenance facility—in this case, Black Box. Any equipment malfunctions, or any repairs or alterations you make to this equipment, may give the telecommunications company cause to ask you to disconnect the equipment.

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

CAUTION!

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

The LOAD NUMBER (LN) assigned to each terminal device denotes what percentage of the total load to be connected to a telephone loop is caused by the device. In order to prevent overloading, the termination on a loop may consist of any combination of devices, subject only to the requirement that the sum of the load numbers of all the devices does not exceed 100.

AFFIDAVIT FOR THE CONNECTION OF CUSTOMER EQUIPMENT TO 1.544-MBPS AND/OR SUBRATE DIGITAL SERVICES

For the work to be performed in the certified territory of

Telco's name: ______________________________,

State/province of: ____________________________,

Country of : _________________________________,

I, ____________________, of _________________,
(Name of Authorized Representative and Customer Name)

____, __________________,
(Customer's Address and Telephone Number)

being duly sworn, state:

I have responsibility for the operation and maintenance of the terminal equipment to be connected to ____________________ 1.544-Mbps and/or _______________ Subrate digital services. The terminal equipment to be connected complies with Part 68 of the Commission's rules except for the encoded analog content and billing-protection specifications. With respect to encoded analog content and billing protection:

- I attest that all operations associated with the establishment, maintenance, and adjustment of the digital CPE with respect to encoded analog content and encoded billing information continuously complies with Part 68 of the FCC's Rules and Regulations.
- The encoded analog and billing protection is factory-set and is not under the control of the customer.

I attest that the operator(s)/maintainer(s) of the digital CPE responsible for the establishment, maintenance, and adjustment of the encoded analog content and billing information has (have) been trained to perform these functions by successfully completing at least one of the following (check all that apply):

a. A training course provided by the manufacturer/grantee of the equipment used to encode analog signals; or

b. A training course provided by the customer or authorized representative, using training materials and instructions provided by the manufacturer/grantee of the equipment used to encode analog signals; or

c. An independent training course (at a trade school, technical institution, etc.) recognized by the manufacturer/grantee of the equipment used to encode analog signals; or

d. In lieu of the proceeding training requirements, the operator(s)/maintainer(s) is (are) under the control of a supervisor trained in accordance with letter ___ above.

I agree to provide ________________________ (Telco's Name) with proper documentation to demonstrate compliance with the information provided in the preceding paragraph, if so requested.

______________________________ (Signature)

______________________________ (Title)

______________________________ (Date)

Subscribed and sworn to me this ____ day of ______________ (month), ________ (year).

____
(Notary Public)

My commission expires:

DISCLAIMER

In no event shall the manufacturer or its suppliers or agents be liable for any damages whatsoever (including, without limitation, damages for loss of business or profits; damages for business interruption; damages for loss of business information; special, incidental, consequential, or reliance damages; or damages for other loss) arising out of the use or inability to use this product, even if the manufacturer or its suppliers or agents have been advised of the possibility of such damages. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, or on the duration or limitation of implied warranties, in some instances the above limitations and exclusions might not apply to you.

TRADEMARKS USED IN THIS MANUAL

BLACK BOX and the logo are registered trademarks of Black Box Corporation.

AT&T is a registered trademark, and Definity is a trademark, of AT&T.

VT100 is a trademark of Compaq Computer Corporation.

K56flex is a trademark of Rockwell Telecommunications and Lucent Technologies.

MNP is a registered trademark of Microcom Systems, Inc.

Microsoft, Windows, and Windows NT are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Telnet is a trademark of Telnet Communications, Inc.

UL is a registered trademark of Underwriters Laboratories Incorporated.

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

Contents

Chapter **Page**

Contents (cont'd)

Chapter **Page**

1. Specifications

Compliance —
EMI/RFI:
USA: FCC (47CFR) Part 15 Subpart J Class A;
Canada: IC Class/classe A, CSA C108.8;
EU: CE (EN 55022 class A, EN 50082:1-1992, 89/336/EEC);
Australia/New Zealand: AS/NZ 3548;
Japan: VCCI V-3 93.01;
PSTN connection: FCC Part 68/IC-03;
Electrical safety:
USA: UL® 1950;
Canada: CSA C22.2 No. 950;
EU: IEC 950, EN 60950, 73/23/EEC;
Australia/New Zealand: TS 001

Standards —
LAN: IEEE 802.3 Ethernet v. 2;
Modem:
Main data interchange: ITU-T V.90, V.34, V.32 bis, V.32, V.22 bis, V.22 A/B, V.23, and V.21; proprietary K56flex™ and V.34+; Bell 212A and 103;
Error correction: ITU-T V.42 LAP-M, MNP® 1 through 4 and 10;
Data compression: ITU-T V.42 bis and MNP 5;
RFCs: 768 (UDP), 791 (IP), 793 (TCP), 1157 (SNMP), 1213 (MIB-II/UDP, DS0, SNMP), 1321 (MD5 Message Digest), 1332 (IPCP), 1406 (DSX1 MIB), 1638 (BCP), 1650 (Ethernet), 1661 (PPP), 1676 (PPP/HDLC framing), 1696 (modem MIB), 1757 (RMON), 1877 (DNS and NBNS address negotiation), 1990 (MLP), 1994 (PPP authentication/ PPP-CHAP), 2011 (SNMP v2 MIB for IP using SMI v2), 2013 (SNMP v2 MIB for UDP using SMI v2), 2021 (RMON v2 for SMI v2), 2127 (ISDN), 2138 (RADIUS authentication), 2139 (RADIUS accounting), 2233 (interfaces MIB);
MIBs: Modem MIB, MIB-II, DSX1 MIB, DS0 MIB, SNMP MIBs, RMON MIBs, interfaces MIB

Interfaces —
WAN:
LRA3000A, LRA3002A: ISDN T1 PRI (including CT1 if CAS is enabled) through integral CSU and digital modems;
LRA3001A, LRA3003A: ISDN E1 PRI (including R2 if CAS is enabled) through digital modems;
LAN: 10BASE-T;
Console: EIA/TIA RS-232 (proprietarily pinned on RJ-45)

Protocols —
WAN: Unnumbered IP WAN, HDLC, ISDN, R2 (for E1) or RBS (for T1/CT1), digital modem, PPP, Multilink PPP, Async-PPP, Sync-PPP, PPP-IPCP, PPP-BCP, PPP trace;
Console: Asynchronous

T1 Characteristics (LRA3000A, LRA3002A) — ISDN PRI Signaling (switch types): N1-2, AT&T® 4ESS/5ESS/Definity™; DMS500/250/100, SL100, INS1500 (Japan);
Framing: D4/SF, ESF;
Line coding: B8ZS;
Channel-associated signaling: Robbed-bit signaling (RBS) including E&M Wink Start (B8ZS)

E1 Characteristics (LRA3001A, LRA3003A) — ISDN PRI Signaling (switch types): ETSI - CTR4/NET5 (Euro-ISDN), 1TR6 (Germany); TS014/TS038 (Australia/New Zealand); for other countries, call Black Box Technical Support;
Framing: Multi-framing with CRC4, double framing;
Line coding: HDB3;
R2 channel-associated signaling: ITU, Mexico (Telmex™), Brazil, Indonesia, or India (for other countries, call Black Box Tech Support)

Routing — IP: Default route, static routes, RIP v1 and v2;
All other routing protocols are supported for bridging only

Authentication — RADIUS authentication, PAP, CHAP, CLID, PPP Call Back (CBCP), basic IP-address pooling; with proprietary CSM software, also supports proxy to NT domains and proxy to RADIUS

Authorization — All authorization options require CSM;
IP Layer 4 policy controls (per TCP/UDP port) based on remote user and/or device; time-of-day, bandwidth, and maximum connect-time restrictions; priority port reservation; policy violation logging; and dynamic profile updates

Accounting — RADIUS accounting; with proprietary CSM software, also supports PPP connection statistics, connection accounting, and IP Layer 4 flow accounting based on TCP/UDP port

Advanced Connection Management — Modem-inactivity timer;
All other connection-management options require CSM:
Advanced IP-address pooling, static IP addresses, dial-out (calling out), device connection history, connection-problem logging, connection accounting, and SQL-based reporting and statistics

Device Management — In-band: SNMP;
Out-of band: RS-232 console, Telnet™ server, TFTP client

Number of Internal Modems — LRA3000A: (48);
LRA3001A: (30);
LRA3002A: (24);
LRA3003A: (60)

User Controls — All models: (1) Front-mounted recessed RESET switch;
LRA3000A, LRA3002A only: (1) Front-mounted PINOUT switch
(affects pinout of WIDE AREA 1 port);
Firmware-resident terminal-based Local Management utility
for configuration and system management;
All advanced functions are software-controlled

Indicators — Front-mounted LEDs:
(1) for main power, labeled PWR;
(1) for self-test, labeled CPU;
(2) for the console (ASYNC) port, labeled LNK and STS;
(1) for the LAN (ENET) port, labeled STS;
(2) for each WAN (WIDE AREA) port, labeled LNK and STS;
All other indications are firmware- and software-based

Connectors — All front-mounted:
(1) RJ-45 female console port, labeled ASYNC;
(1) RJ-45 female LAN port, labeled ENET;
(1) RJ-48C female WAN port, labeled WIDE AREA 1;
LRA3000A, LRA3003A only: (1) RJ-48C female WAN port,
labeled WIDE AREA 2

MTBF — 50,000 hours (calculated estimate)

Temperature Tolerance — Operating: 32 to 104˚F (0 to 40˚C);
Storage: –22 to +194˚F (–30 to +90˚C)

Humidity Tolerance — 5 to 95% noncondensing

Power — From utility-power (mains) outlet(s), through included detachable power cord(s), rear-mounted IEC 320 inlet(s), and internal transformer(s):
Input: 100 to 125 VAC (~300 mA) or 200 to 240 VAC (~150 mA) at 50 or 60 Hz (autosensing);
Current: Rated for 55 watts;
Inlets: Dual (redundant) IEC 320 male;
Consumption: 35 watts maximum

Size — 1.8"H (1U) x 15.5"W x 17"D (43.2 x 39.4 x 4.5 cm)

Weight — 13 lb. (5.9 kg)

2. Introduction

NOTE

This manual is intended to help you get your Remote Access Concentrator up and running. It isn't a detailed reference on the Concentrator's operation; for more complete information, use a standard browser to page through the HTML documentation included on CD with the Concentrator. Also, you might want to check our Black Box Web site (www.blackbox.com) for material that might be more up-to-date than what you received, including software or firmware updates, updated MIBs, and revised HTML documentation.

Enterprises seeking increased productivity and communication are extending dial-up access to their telecommuting employees and business partners, and service providers are searching for ways to differentiate their dial-up services to retain existing customers and attract new ones.

But this expansion in access is creating new challenges in the areas of security, accounting, and network management. Our T1 and E1 Remote Access Concentrators (the LRA3000 series of product codes) directly address these challenges by delivering the lowest-cost dial solutions with support built in for using RADIUS for remote device authentication.

The Concentrators support high-density ISDN/V.90 concentration of dial-up traffic in a compact, rack-mountable form factor. The Concentrators' architecture supports universal dial access (ISDN or modem) on every port, yielding excellent price/performance in a slender design that's only 1U (1.8", 4.4 cm) high. Both T1 and E1 versions are available, supporting two ISDN Primary Rate Interfaces (PRIs) and either 48 (T1) or 60 (E1) DS0 connections; the DS0s can be any combination of V.90 (56K) modem and ISDN calls. All Concentrators have redundant power supplies for added protection in mission-critical applications.

We also offer Connection Services Manager (CSM) software (our product code LRA300SW) for use with the Concentrators. It performs remote device authentication, supports robust connection management, and gives you real-time control over remote user authentication, policy definitions, and accounting from a centralized server. More information about CSM is available in the HTML documentation on the CD that came with your Concentrator.

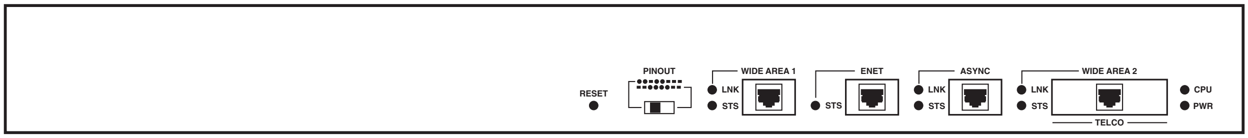
The table below summarizes each Concentrator model's options.

Model	WAN Access	Telco Interface(s)	Number of V.90 Digital Modem Ports
LRA3000A	T1	Dual ISDN T1/PRI	48
LRA3001A	E1	Single ISDN E1/PRI	30
LRA3002A	T1	Single ISDN T1/PRI	24
LRA3003A	E1	Dual ISDN E1/PRI	60

NOTE

The T1 models support ISDN Primary Rate Interface (PRI) in Canada, the United States, and Japan. The E1 models support ISDN Primary Rate Interface (PRI) in Europe, the Asia-Pacific region (excluding Japan), and Latin America.

The figure below shows the Concentrator's front panel, where most of its connectors and indicators are. The connectors are discussed in more detail in the next chapter of this manual, and the LED indicators are discussed in the Concentrator's HTML documentation.



3. Installation

CAUTION!

Only qualified personnel should attempt to install this equipment.

3.1 The Complete Concentrator Package

You should have received these things with your Remote Access Concentrator:

- The Concentrator itself.
- (1) Console cable for connections to the Concentrator's ASYNC port.
- (1) RJ-45 M to DB9 F adapter for use with the console cable.
- (1) or (2) Cross-pinned WAN cable(s) for connections to the Concentrator's WIDE AREA port(s).
- (1) Standard 10BASE-T cable for connections to the Concentrator's ENET port.
- A grounding wrist strap for installers and maintenance people to wear, to prevent static discharges that might damage the Concentrator.
- (4) Adhesive rubber feet for placing the Concentrator on a desk, counter, etc.
- A rackmount kit for mounting the Concentrator in a 19" rack.
- (2) Power cords.
- (1) CD of HTML documentation.
- This manual.

If anything is missing or arrives damaged, please call Black Box right away.

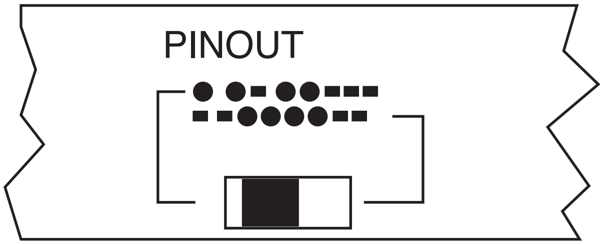
3.2 Arranging ISDN Service

Before you install your Remote Access Concentrator, we recommend that you contact your telco or service provider and arrange for ISDN service compatible with the Concentrator:

1. Make sure that they use a type of ISDN central-office switch that the Concentrator supports.
2. Order an ISDN PRI line if you haven't done so already.
3. Ask them for the ISDN line's phone number, any prefix necessary for dialing, and the specs for line encoding, framing, and (for T1 models) the T1 LBO.

For more details, see the "ISDN Line Ordering," "ISDN PRI Line Information," and "Telephone Switch Support" sections in the Concentrator's HTML documentation.

3.3 Setting the Pinout Switch for Your WAN Interface (T1 Models Only)



The T1 models of the Remote Access Concentrator have a PINOUT switch on their front panels. This switch allows you to make WAN-interface adjustments based upon country of usage for the Concentrator's WIDE AREA 1 port. (For instructions on connecting cables to this port, see **Section 3.6.3**.) For North American installations, this switch should be set to the *left* (the default setting). For use in Japan, this switch should be set to the *right*. The switch positions translate to the following WAN-connector pinout settings:

Switch set to the **left** for use in North America:

pin number	1	2	4	5
polarity	+	–	+	–
direction	receive	receive	transmit	transmit

Switch set to the **right** for use in Japan:

pin number	3	4	5	6
polarity	+	+	–	–
direction	transmit	receive	receive	transmit

NOTE

As stated above, the PINOUT switch adjusts the pinout setting for the WIDE AREA 1 port *only*. The default pinout for both ports (WIDE AREA 1 and WIDE AREA 2) is for North American use. If the LRA3000A or LRA3002A is used in Japan, a ModTap™ adapter is required for the WIDE AREA 2 port to have a correct pinout.

E1 models of the Concentrator don't have a PINOUT switch; they use this unchangeable, international-standard WAN-connector pinout:

pin number	1	2	4	5
polarity	+	–	+	–
direction	receive	receive	transmit	transmit

3.4 Placement

Installation sites must be within reach of the network cabling and must meet the following requirements:

- A properly grounded AC power receptacle must be within 7 feet (2.1 m) of the location.
- Temperatures at the installation site must remain between 32 and 104°F (0 and 40°C), with fluctuations of less than 18°F (10°C) per hour.
- If you are placing the Concentrator on a shelf, the shelf must be able to firmly support 13 lb. (5.9 kg) of static weight for each Concentrator on the shelf.
- If you are placing the Concentrator in a rack, there must be at least two inches (5 cm) of clearance on each side of and behind the Concentrator for adequate ventilation.

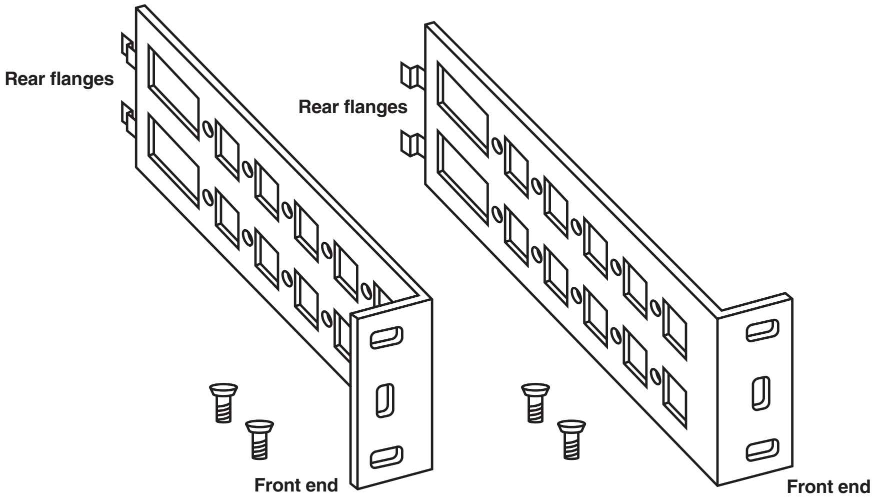
3.5 Rackmounting (Optional)

CAUTION!

Before installing the Concentrator in a rack, make sure that the rack can hold the Concentrator securely without toppling, warping, breaking, etc. Otherwise, personal injury and equipment damage might result.

Do *not* use screws other than those included with the Concentrator's Rackmount Kit to attach the Kit's rackmount brackets to the Concentrator's chassis. Wrong-sized screws can cause electrical shorts and can physically damage the Concentrator.

To mount a Remote Access Concentrator in a 19" rack, you'll need to attach the brackets from its included rackmount kit to the Concentrator, then attach the bracketed assembly to your rack. You'll need both a flathead and a Phillips screwdriver to do this.

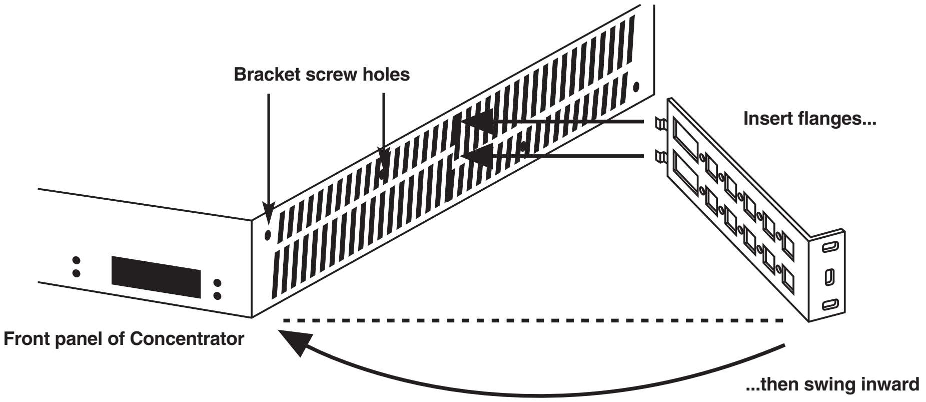


Take these steps:

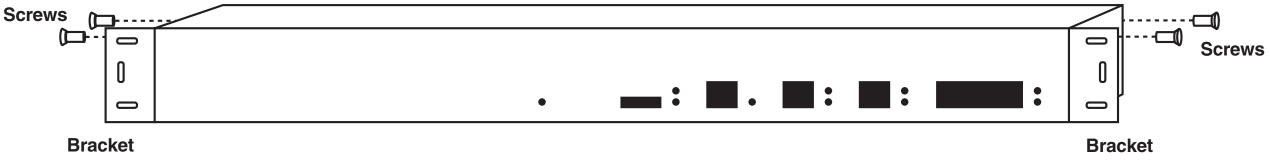
1. Decide which way you want the Concentrator to face. The standard installation is with the front of the Concentrator facing the front of the rack; the rest of the directions in this section assume that orientation. But you can install the Concentrator with its rear panel facing the front of the rack instead. If you do so, you'll have to install the brackets upside down, so that they screw onto the *bottom* edge of the Concentrator's side. You'll also have to substitute "rear of the Concentrator" for "front of the Concentrator" in the following steps.

2. With the Concentrator's faceplate (the front of the unit) towards you, take the Rackmount Kit's brackets and place one on either side of the Concentrator, so that the front end of each bracket lines up with the faceplate.

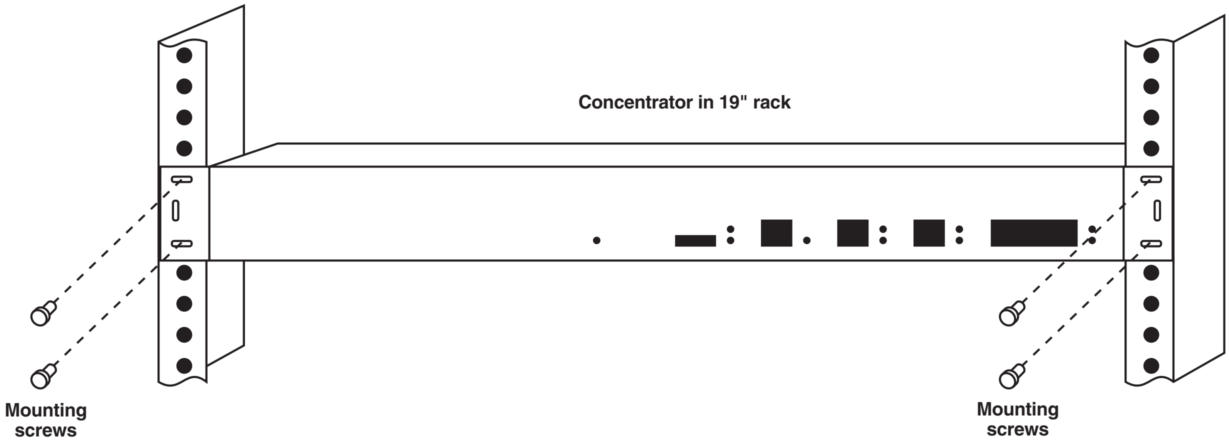
3. There are slots in each side of the Concentrator that are made to accept the brackets' rear flanges, as shown below. Swing the front of each bracket outward, insert the flanges in these slots, and swing the front back in. (If, after you do this, the front of a bracket doesn't line up with the Concentrator's faceplate, or the screwholes along the top of the side a bracket don't line up with the screwholes on the side of the Concentrator's chassis, swing the bracket back out and adjust how the flanges are seated in the slots.)



4. Using the four included $\frac{6}{32}$ x $\frac{1}{4}$-inch flathead screws, attach each bracket to the Concentrator along the top of the Concentrator's chassis, as shown below.

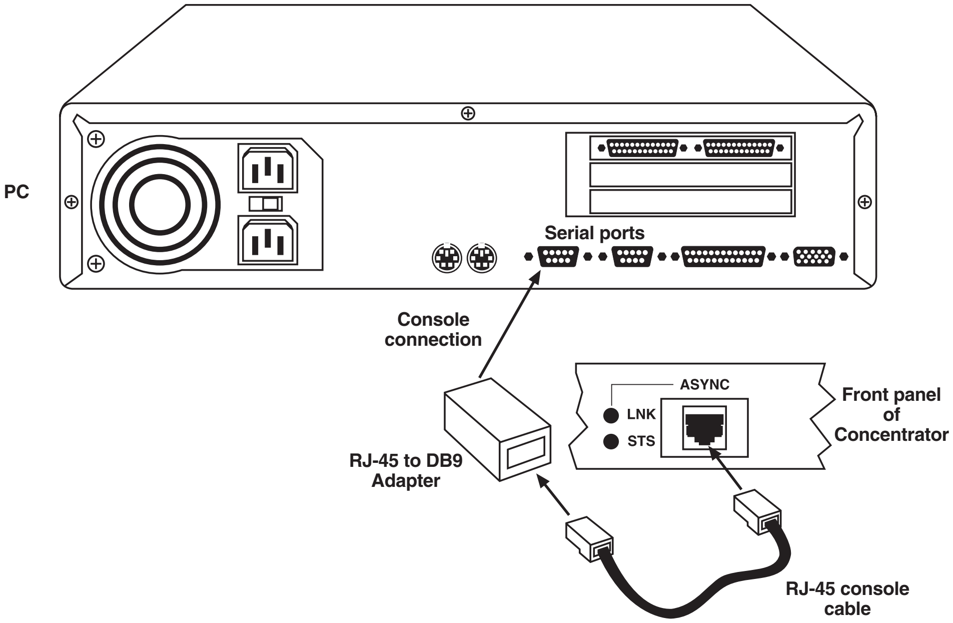


5. Fasten the bracketed Concentrator assembly to the vertical frame of a 19" rack using your own mounting screws, bolts, cage nuts, etc., as shown below.



3.6 Making Cable Connections

3.6.1 Console (ASYNC) Connections



The Remote Access Concentrator's RJ-45 female RS-232 console port (labeled ASYNC) is the gateway to the Concentrator's local management (configuration) utility. It's proprietarily pinned out this way:

Pin	Function
1	Transmit Data (TD)
2	Carrier Detect (CD)
3	Data Set Ready (DSR)
4	Receive Data (RD)
5	Signal Ground (SGND)
6	Data Terminal Ready (DTR)
7	Request To Send (RTS)
8	Clear to Send (CTS)

(Refer to the Concentrator's HTML documentation for complete information about this port and its two associated LEDs.)

To attach a console to this port, use the included RJ-45 male-to-male console cable to make the following connection:

1. Plug one end of the cable into the Concentrator's console (ASYNC) port.
2. Plug the other end of the cable into the RJ-45 to DB9 adapter that's included with the Concentrator in its "console cabling kit."
3. Plug the adapter into the serial port of a terminal or of a PC running a communications package that can do VT100™ emulation.

In certain unusual circumstances, you might need to connect an analog modem to the Concentrator's console port. (This type of connection would allow you to remotely administer the Concentrator by dialing in to the modem.) To do this, you'll need a special cable cross-pinned like this:

Signal	Concentrator End	Modem End	Signal
TD	1	2	TD
CD	2		
DSR	3	8	CD
CTS	8		
RD	4	3	RD
SGND	5	7	SGND
DTR	6	N/C	—
RTS	7	20	DTR

The modem *must* be configured as follows:

- 9600 bps, 8 data bits, 1 stop bit, no parity.
- Auto-answer enabled.
- Drop CD (Carrier Detect) when calls drop. (This setting helps prevent security breaches.)
- Ignore DTR and RTS.

NOTES

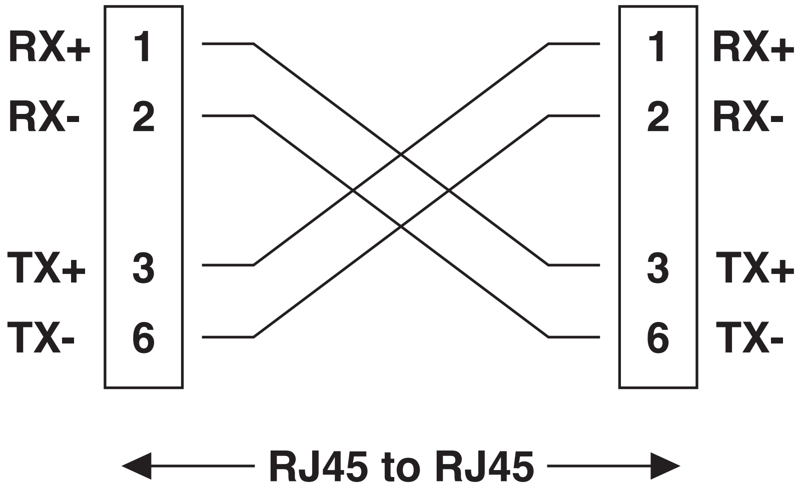
CD, DTR, and RTS settings may be changed by sending your modem "AT commands" or, sometimes, by setting DIP switches. Refer to its manual.

When the modem is connected to the Concentrator and no call is up, none of the Concentrator's LNK and STS LEDs are lit. Once the call is connected, these LEDs function the same way as if it were a local connection. Refer to the LEDs section of the Concentrator's HTML documentation.

3.6.2 LAN (ENET) Connections

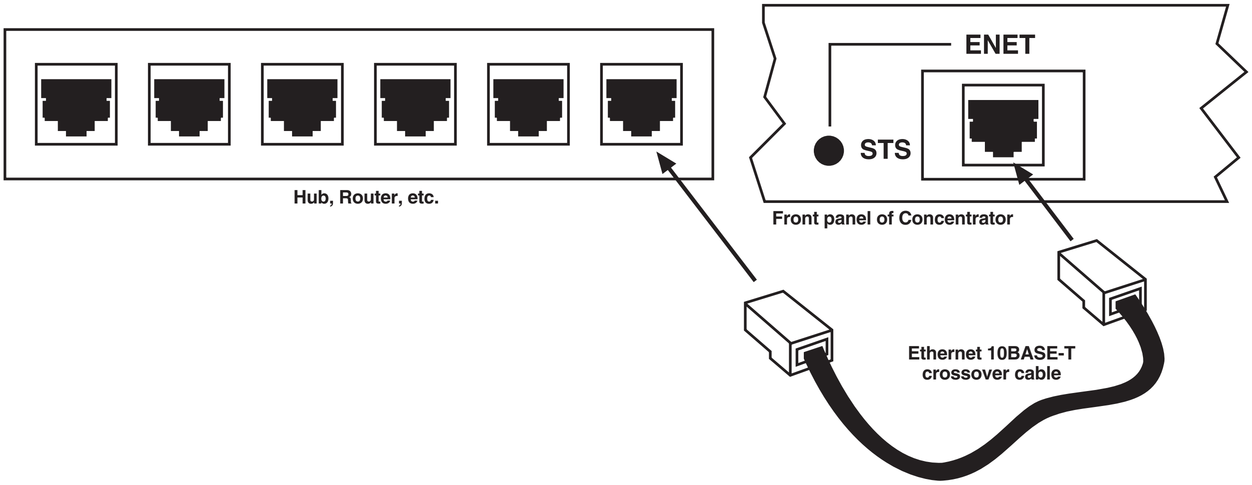
The Concentrator's Ethernet port (labeled ENET) is an RJ-45 socket configured as a 10BASE-T hub port. (Refer to the Concentrator's HTML documentation for complete information about this port and its associated STS LED.)

When connecting the Concentrator to another hub (a common scenario), you'll need a crossover cable. A standard-length RJ-45 crossover cable is included with your Concentrator (pinout illustrated below).



Using this included cable, make a LAN connection this way:

1. Plug one end of the cable into the Concentrator's LAN (ENET) port.
2. Plug the other end of the cable into the hub or other LAN device.



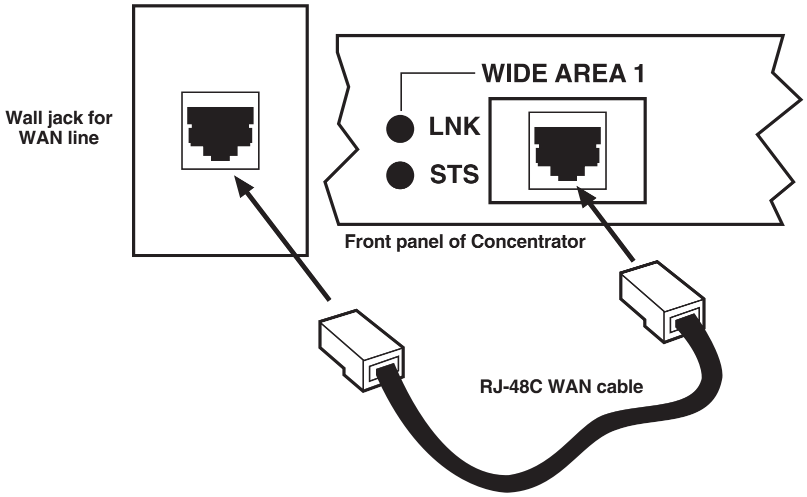
3.6.3 WAN (WIDE AREA) CONNECTIONS

CAUTION!

Do *not* plug a WAN cable into either of the Concentrator's WIDE AREA ports until you are sure that the encoding, framing, T1 LBO, and switch type that the Concentrator is configured for match the line's actual values. If you plug in this cable when there's a discrepancy between the line's actual values and the line values that the Concentrator is configured for, you might actually temporarily disable the WAN line.

Refer to the "ISDN Line Ordering," "ISDN PRI Line Information," and "Telephone Switch Support" sections in the Concentrator's HTML documentation for more information about these values, and see Section 4.4 **in this manual for the Concentrator's default settings for these values and how to change those settings.**

To connect the Concentrator's WIDE AREA 1 or WIDE AREA 2 WAN port to a WAN line, plug one end of the included RJ-48C (RJ-45 style) WAN cable into the Concentrator's WAN port, then plug the other end of the cable into the WAN line's wall jack, as shown below. (Refer to the Concentrator's HTML documentation for complete information about these ports and their two associated LEDs.)



NOTES

If you're installing the Concentrator at a Japanese site, you'll need to set the Concentrator's WAN-pinout switch and/or use a ModTap adapter; see Section 3.3**.**

Some Canadian service providers use DB15 male connectors for their WAN-line interface. So if you're installing the Concentrator at a Canadian site, you might need an RJ-48C female to DB15 female adapter that's pinned out this way (available on a special-quote basis):

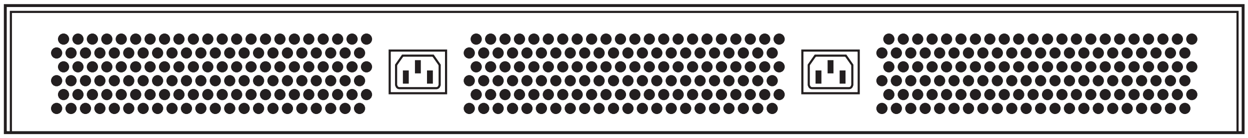
Signal	RJ-48C F Pin		DB15 F Pin	Signal
RCV+	1	———	11	RCV+
RCV–	2	———	3	RCV–
XMT+	4	———	9	XMT+
XMT–	5	———	1	XMT–

3.7 Connecting to AC Power

As shown below, there are two power inlets on the rear panel of the Remote Access Concentrator. This is because the Concentrator has two internal power supplies. You don't have to plug in both of them; the unit will run with just one plugged in. But when both power supplies are plugged in, one is redundant: If the transformer in use fails, the other will supply power to the unit to keep it in operation.

These power supplies are autosensing: You can plug them into power outlets providing either 100 to 125 VAC or 200 to 240 VAC, at a frequency of 50 or 60 Hz.

It might be possible to plug the two transformers into two different electrical circuits, so that the Concentrator is less likely to go down if a particular circuit fails. However, the two circuits would have to be regulated very strictly, so that no difference of ground potential could build up between them; otherwise, an electrical "ground loop" from one circuit to the other could pass through the Concentrator and damage it. In general, we recommend that you plug the two transformers into the same circuit, and use uninterruptible power supplies (UPSes) to guard against failures of site power.



To connect the Concentrator to AC power, take these steps:

1. Plug the "outlet end" of one of the included detachable power cords into one of the Concentrator's inlets.
2. Plug the "plug end" of the cord into a grounded wall outlet.
3. Verify that the PWR LED on the front of the Concentrator is lit solid green, indicating that the Concentrator is receiving power from that outlet. After the Concentrator runs a self-test, the CPU LED on the front of the Concentrator should be flashing green, indicating normal operation. If a minute passes and the CPU LED is still not flashing green, contact Black Box Tech Support.
4. *If you're using both power supplies:* Unplug the first power cord, then repeat steps 1 through 3 for the other cord. Once you've verified that the Concentrator can run normally from the power on either outlet, plug the first cord back in.

The Concentrator is now ready to be configured.

4. Configuration

4.1 The Information You'll Need

Before you configure the Remote Access Concentrator, you'll need to gather the following information and write it down on a copy of the worksheet printed on the next page:

- Establish an IP address for the Concentrator. You will need this address to configure both the Concentrator and the application you are using for authentication (either RADIUS or CSM).
- If the RADIUS server or CSM is not on the same subnet as the Concentrator, you must know the gateway address to the RADIUS server or the device running CSM.
- *If you're using CSM:* Establish a CSM secret for CHAP Authentication, as well as a Concentrator name, secret, and password. You will need to configure these values on both the Concentrator and CSM.
- Assign names to the remote devices that will access the Concentrator.
- Establish authentication information (secrets or passwords) for remote devices. You will need to configure the same values on the RADIUS or CSM device and on the remote devices themselves.
- Establish either permanent IP addresses or an IP-pool name and a range of IP addresses for these remote devices.
- Determine the telephone number for the Concentrator network.
- Determine telephone numbers for remote devices (if you're configuring the Concentrator for outbound calling).
- For security purposes, we advise you to change the Concentrator's default passwords (which control access to its Local Management and SNMP) as soon as possible.
- Establish new SNMP community names for *read-only*, *read-write*, and *superuser* access.
- The Concentrator requires line information for its WAN (WIDE AREA) ports. Determine the switch type, framing, and line coding you will be using. For T1* models, determine whether you will be using a short- or long-haul Line Build Out (LBO). If your installation's required values differ from the Concentrator's factory-default values, you'll need to make configuration adjustments to the Concentrator.

*The T1 models of the Concentrator support both short- and long-haul capabilities. When configuring your system, you must match the Concentrator's Line Build Out and that of the device (short haul) or network (long haul) to which it is attached. Its factory-default value is 0.0 dB (long haul). (Line Build Out is not configurable on the E1 models of the Concentrator; they are preset to operate with standard 120-ohm termination and line impedance.)

Table 4-1. Configuration Worksheet

Record some of the most important Remote Access Concentrator configuration settings here.

Concentrator information:

1. IP address: ____
2. Phone number: ____
3. RADIUS or CSM on same subnet as Concentrator? **Yes** **No**

    If not, provide gateway: ____________________________

4. Authentication Information:

    CSM secret: _______________________________________

    Concentrator name: _________________________________

    Concentrator secret: ________________________________

    Concentrator password: _____________________________

5. IP-address pool name: ____________________________________

    Range of IP addresses in pool: _______________________

6. SNMP community names:

    Read only (default=public): ___________________________

    Read/write (default=public): ___________________________

    Superuser (default=public): ___________________________

Device information:

1. Remote device name: _____________________________________
2. IP Address: ____

    Permanent or **From IP address pool** (circle one)

3. Secret/password: ____
4. Phone number: ____

Line information:

1. Encoding (T1 default=B8ZS, E1 default=HDB3): ____________
2. Framing (T1 default=ESF, E1 default=E1-CRC): ____________
3. Switch type (T1 default=NI-2, E1 default=ETSI): ____________
4. LBO (T1 default=0.0 dB, N/A for E1): ______________________

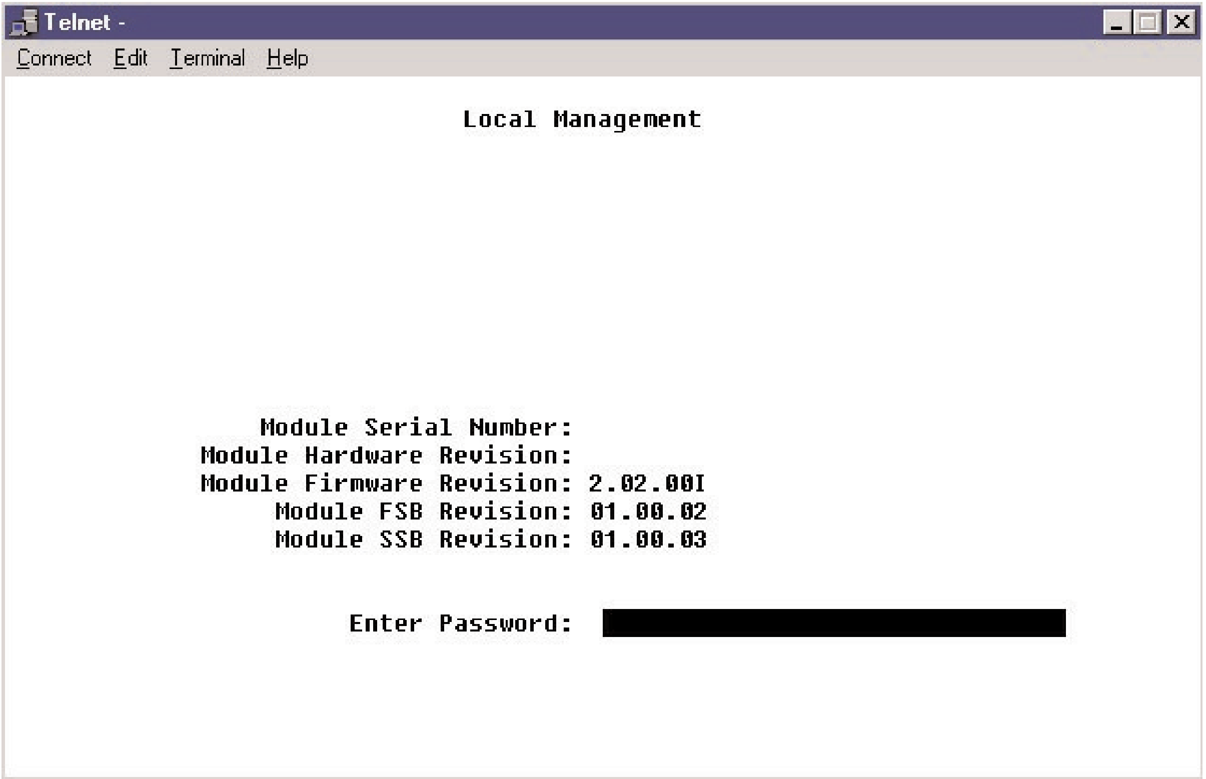
4.2 The Local Management Utility

You'll configure the Remote Access Concentrator with its Local Management utility. This utility is accessible through the Concentrator's local console (ASYNC) port or through a remote (Telnet) connection. For initial configuration, you must use the local console port to access Local Management. After initial configuration, you can use the remote connection to verify the initial configuration, and/or make updates to existing configurations.

Here are some pointers for navigating the utility:

- The Local Management utility doesn't support mice; use your keyboard's **tab** key and/or its **up-** and **down-arrow** keys to navigate through the menus.
- If a menu item gives you a choice between set values, use your keyboard's **space bar** to toggle between choices.
- If you do not need to save any changes once you are done viewing a menu, you may find it quicker to press your keyboard's **Esc** (escape) key twice to return to the previous menu instead of tabbing through the entire menu to get to the **RETURN** option.

When you access the utility through (a) the local console port (just plug in the cable as directed in **Section 3.6.1** and attach the other end of the cable to a PC running a terminal emulator) or (b) a remote Telnet connection, your terminal will display the main Local Management screen:

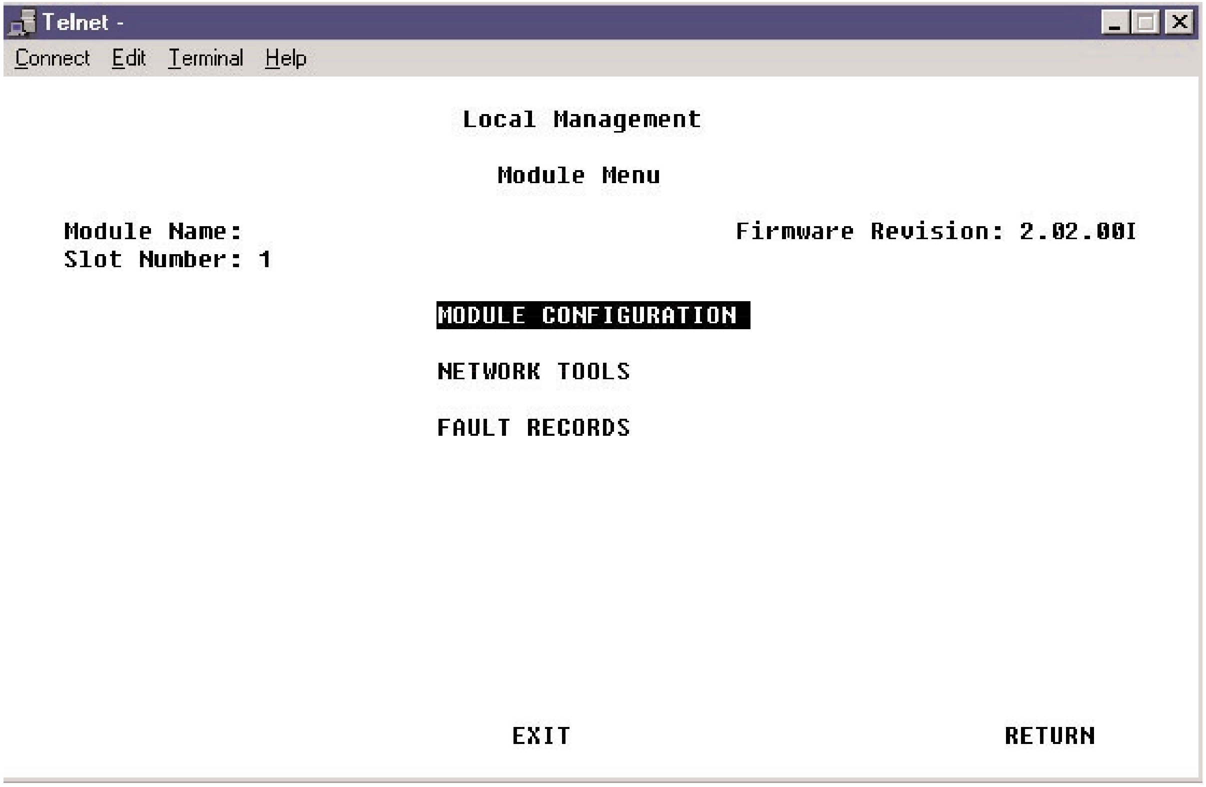


```
                         Local Management




          Module Serial Number:
        Module Hardware Revision:
        Module Firmware Revision: 2.02.00I
             Module FSB Revision: 01.00.02
             Module SSB Revision: 01.00.03


                  Enter Password:
```

The default password for initial configuration is the word "public". Your Concentrator might be configured with this password already typed in and displayed here, in which case all you have to do is tab through this field. Otherwise, enter the password here. (To change the initial default password values—you can assign a different password to each of the three levels of access— select "SNMP Community Names" from the Module

Configuration menu; see **Section 4.3.2**. For security reasons, we suggest making this change at the time of the initial installation.)

The next screen presented is the Module Menu:



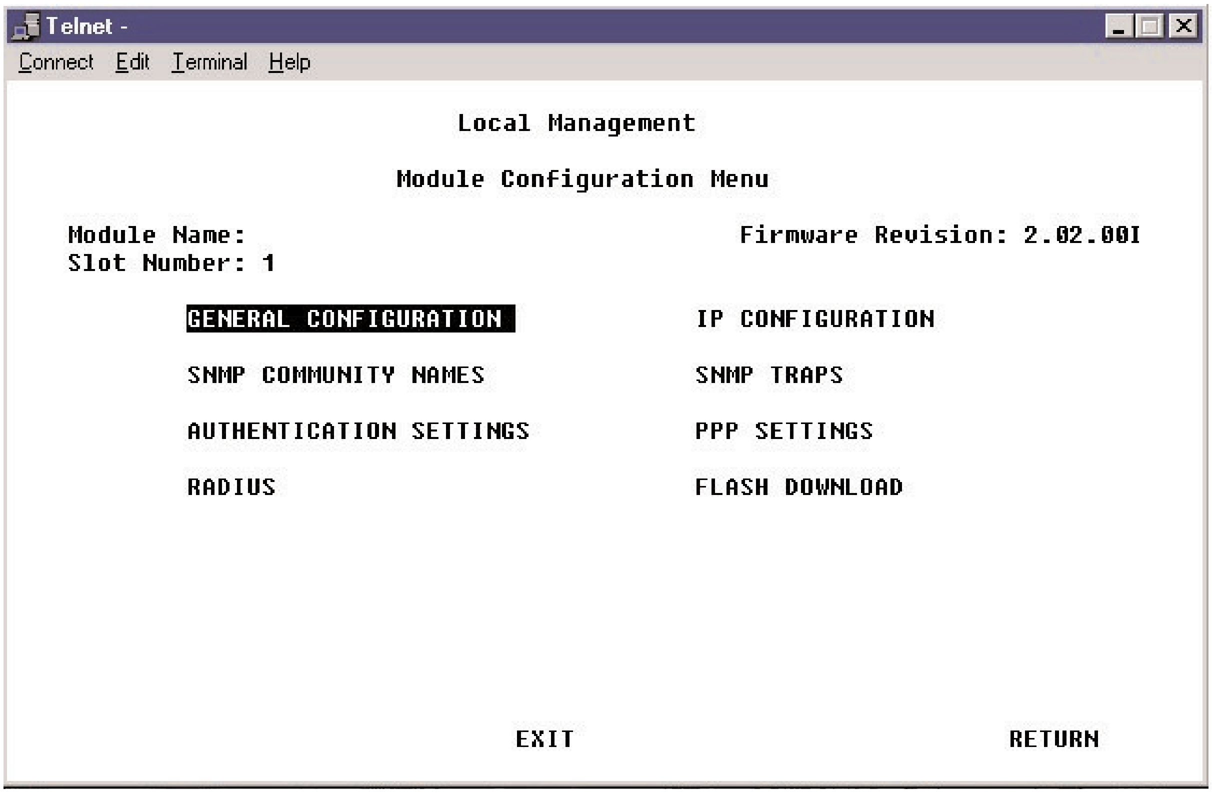
```
                              Local Management

                                Module Menu

    Module Name:                                  Firmware Revision: 2.02.00I
    Slot Number: 1

                             MODULE CONFIGURATION

                             NETWORK TOOLS

                             FAULT RECORDS




                                 EXIT                        RETURN
```

Select Module Configuration (see **Section 4.3**) for menus of options for setting up your Concentrator. Select Network Tools (see **Section 4.4**) for a prompt at which you can enter a number of commands to control the Concentrator's configuration and operation.

You can also select Fault Records here; it's not really a configuration option, but it can provide valuable troubleshooting information for Customer Support personnel. If you're continually experiencing system problems, specific log messages may point you to the Fault Records log; please get screen captures of this log and give them to our tech support technicians if they ask you to do so. For more details about the Fault Records features, see **Section 4.5**.

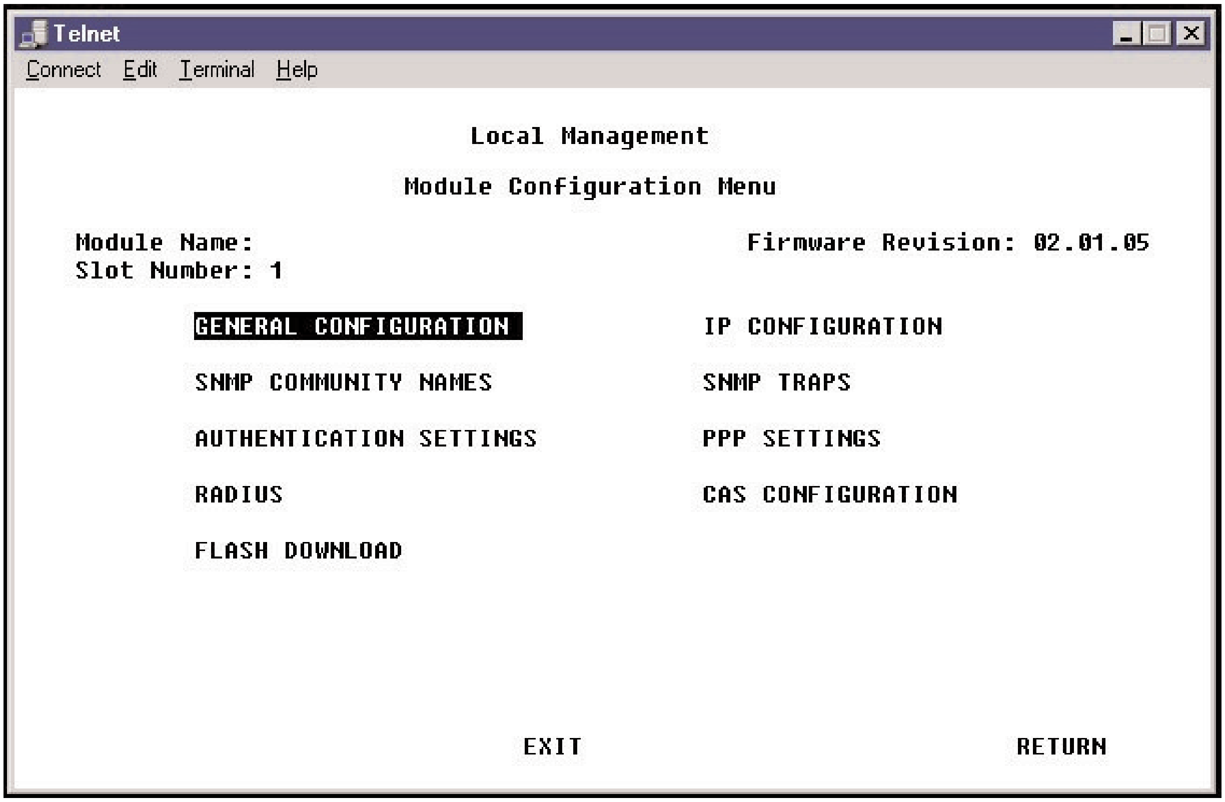
4.3 Module Configuration

When you select Module Configuration from the main Local Management menu (see **Section 4.2**), you'll see this screen if the Remote Access Concentrator is set to its default values:



```
                         Local Management

                     Module Configuration Menu

   Module Name:                                Firmware Revision: 2.02.00I
   Slot Number: 1

           GENERAL CONFIGURATION              IP CONFIGURATION

           SNMP COMMUNITY NAMES               SNMP TRAPS

           AUTHENTICATION SETTINGS            PPP SETTINGS

           RADIUS                             FLASH DOWNLOAD




                           EXIT                             RETURN
```

If Channel Associated Signaling (CAS) has been enabled in the Network Tools menu (see **Section 4.3.6**), you'll see *this* version of the screen:



```
                          Local Management

                      Module Configuration Menu

  Module Name:                                 Firmware Revision: 02.01.05
  Slot Number: 1

          GENERAL CONFIGURATION              IP CONFIGURATION

          SNMP COMMUNITY NAMES               SNMP TRAPS

          AUTHENTICATION SETTINGS            PPP SETTINGS

          RADIUS                             CAS CONFIGURATION

          FLASH DOWNLOAD




                            EXIT                               RETURN
```

Select any of the Module Configuration options to set up a wide variety of features:

- ***Required:*** **General Configuration**
  Set the date and time and the Concentrator's IP address. *Wait until last to set these options;* as soon as you enter an IP address for the Concentrator, the Concentrator will automatically reboot. See **Section 4.3.7**.

- *Optional:* **IP Configuration**
  Configure an IP LAN interface, a default LAN route, and up to 10 static LAN routes. Configuring these elements allows the Concentrator to function more efficiently in a network containing routers. See **Section 4.3.1**.

- *Optional:* **SNMP Community Names**
  Change your Concentrator's initial default passwords for increased security. See **Section 4.3.2**.

- ***Required:*** **Authentication Settings**
  Select the device database and configure authentication information such as system name, password, and secret. See **Section 4.3.3**.

- *Optional:* **PPP Settings**
  Configure primary and secondary DNS and NBNS addresses for remote devices using Windows dialup. See **Section 4.3.4**.

- *If you select RADIUS as the device database:* **RADIUS**
  See **Section 4.3.5**.

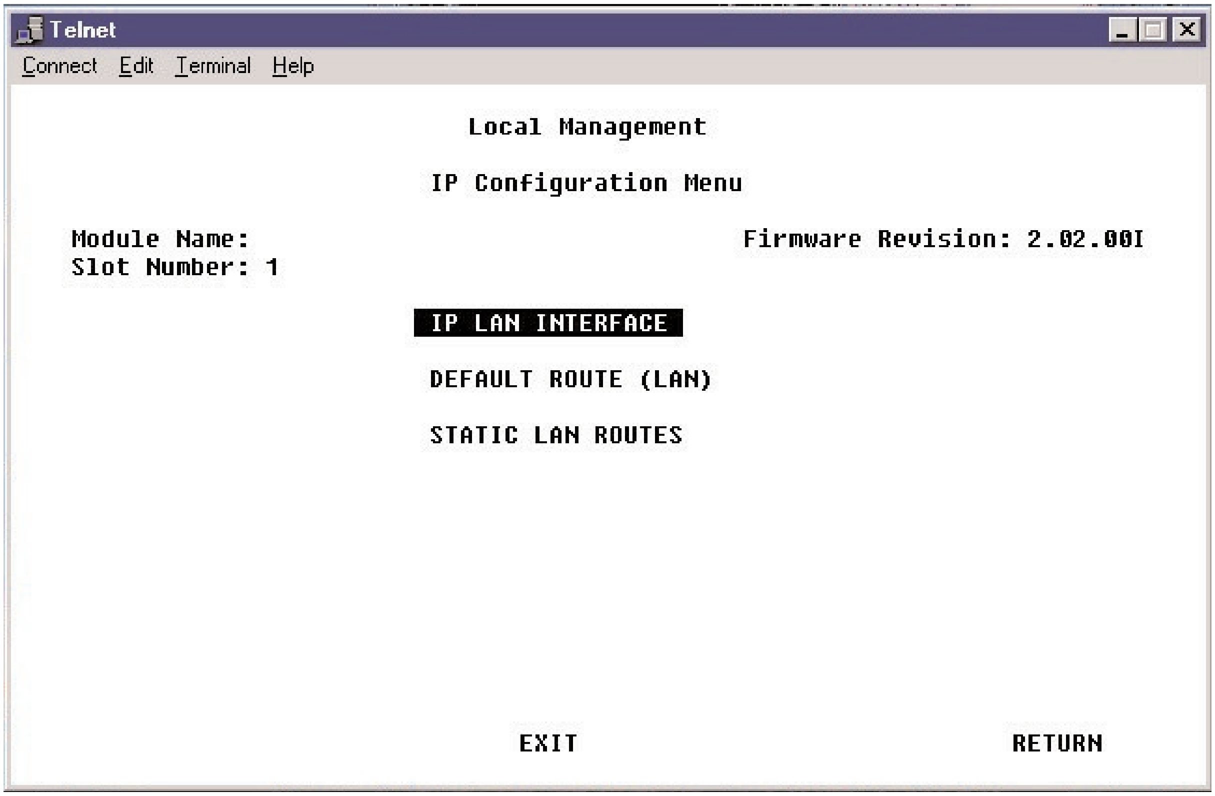
- *If you enable CAS:* **CAS Configuration**
  Configure the Concentrator to provide channel associated signaling (CAS) for specified lines; select R2 signaling (for E1 lines) or Robbed Bit Signaling (for T1 lines) if desired.

You can also select **Flash Download** from this menu if you want to upgrade the Concentrator's firmware. See **Section 4.3.8**. (Call Black Box Tech Support if you're not sure whether you need an upgrade or not.)

The other option on this menu, **SNMP Traps**, is not supported at this time.

4.3.1 IP Configuration

Configuring IP information for the Remote Access Concentrator allows it to function efficiently in a network that includes routers. To enter the Concentrator's IP-configuration information, select IP Configuration from the Module Configuration menu. This screen will appear:



```
                         Local Management

                       IP Configuration Menu

  Module Name:                                   Firmware Revision: 2.02.00I
  Slot Number: 1

                        IP LAN INTERFACE

                        DEFAULT ROUTE (LAN)

                        STATIC LAN ROUTES




                            EXIT                               RETURN
```

From this menu you can define these parameters for the Concentrator:

- **IP LAN Interface**
  Configuring the LAN interface allows the Concentrator to route IP data. See **Section 4.3.1.A**.

- **Default LAN Route**
  All IP packets received having a destination IP address without an explicit routing-table entry will be sent to the defined default route. See **Section 4.3.1.B**.

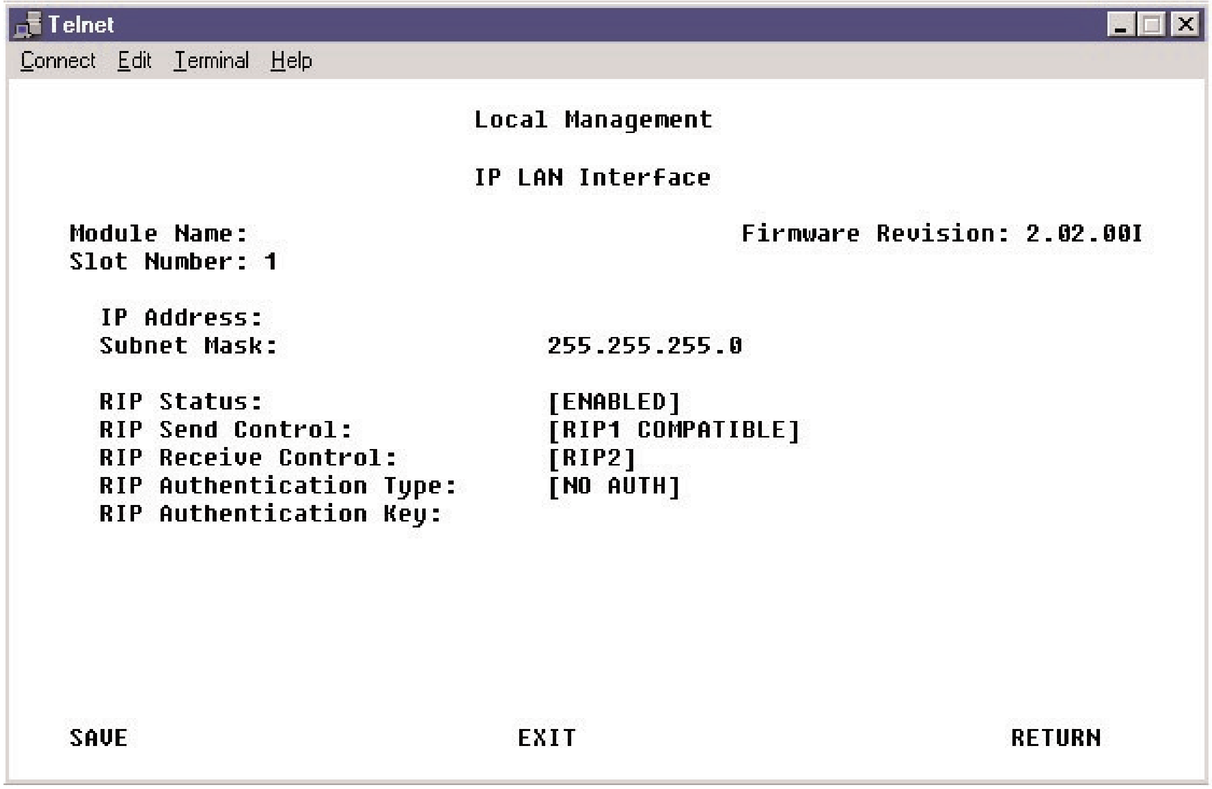
- **Static LAN Routes**
  Although most routes are automatically entered in the Concentrator's routing table, there are cases where it is necessary to manually enter static routes. See **Section 4.3.1.C**.

4.3.1.A IP LAN Interface

Configuring its LAN interface allows the Remote Access Concentrator to route IP data. Routing Information Protocol (RIP) can be enabled on the interface to allow the exchange of routing information among IP devices, automating the maintenance of routing tables.

To configure the IP LAN Interface, take these steps:

1. Select IP LAN Interface from the IP Configuration Menu. This screen will appear:



```
                         Local Management

                         IP LAN Interface

Module Name:                                    Firmware Revision: 2.02.00I
Slot Number: 1

  IP Address:
  Subnet Mask:                     255.255.255.0

  RIP Status:                      [ENABLED]
  RIP Send Control:                [RIP1 COMPATIBLE]
  RIP Receive Control:             [RIP2]
  RIP Authentication Type:         [NO AUTH]
  RIP Authentication Key:







SAVE                           EXIT                                RETURN
```

2. Enter the Concentrator's IP Address. Note that this address can also be configured through the General Configuration menu, and that if you change the address here, the change will also be reflected in the General Configuration menu—see **Section 4.3.7**.

3. Enter the Subnet Mask associated with the IP Address. The mask bits start at the most significant bit of the IP address and proceed to the least significant bit. The mask identifies the LAN subnet to which the Concentrator is directly connected. Note that this mask can also be configured through the General Configuration menu, and that if you change the mask here, the change will also be reflected in the General Configuration menu—see **Section 4.3.7**.

4. Select the RIP Status (either ENABLED or DISABLED) for the LAN interface. Use the space bar to toggle between the selections. Enabling RIP allows the Concentrator to automatically learn LAN routes.

5. Select the RIP Send Control. This determines how RIP update messages are sent on the interface. Choices are:

   - **RIP1 COMPATIBLE**
     RIP V2 version packets are sent using RFC 1058 subsumption rules with standard broadcast addressing. This choice allows RIP-1 routers to receive RIP update messages from the Concentrator.
   - **RIP2**
     RIP V2 version packets are sent. Compliant with RFC 1723. Uses standard multicast addressing.
   - **DO NOT SEND**
     No RIP packets are sent.

6. Select the RIP Receive Control. This determines how the Concentrator receives RIP updates. Choices are:

   - **RIP2**
     Only accepts RIP V2 updates compliant with RFC 1723.
   - **DO NOT RECEIVE**
     No RIP packets are received.

7. Select the RIP Authentication Type. This determines the type of authentication the Concentrator uses on the interface. Choices are:

   - **NO AUTH**
     Unauthenticated RIP updates are accepted. RIP advertisements are sent without passwords.
   - **SIMPLE PASSWORD**
     RIP updates that pass an authentication test are accepted. The authentication test is done using a simple password. RIP advertisements include the password.

8. If you have selected SIMPLE PASSWORD as the RIP Authentication Type, enter a RIP Authentication Key. The authentication key is a user-defined password, 1 to 16 characters in length.

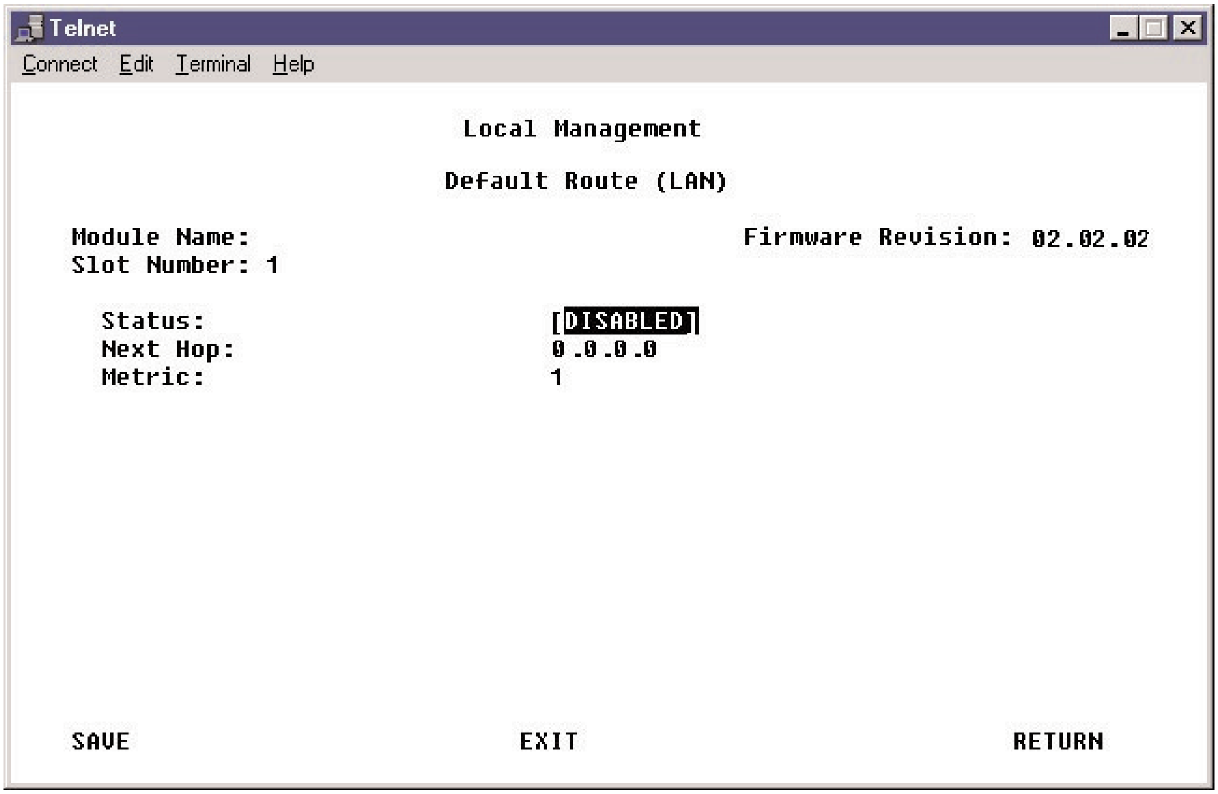
9. Select SAVE and then RETURN to return to the IP Configuration menu.

4.3.1.B Default LAN Route

The Default LAN Route is a special static route that can be useful when there are a large number of networks accessible through a gateway. All IP packets received having a destination IP address without an explicit routing-table entry will be sent to the default route.

To define the Concentrator's default LAN route:

1. Select Default Route (LAN) from the IP Configuration Menu. For a Concentrator right out of the box, this screen will appear:



```
                         Local Management

                        Default Route (LAN)

  Module Name:                                Firmware Revision: 02.02.02
  Slot Number: 1

    Status:                     [DISABLED]
    Next Hop:                   0.0.0.0
    Metric:                     1










  SAVE                         EXIT                              RETURN
```

2. To enable a default route, you will need to change the Status from **DISABLED** to one of the following:
   - **SET TO NEXT HOP**
     With this setting, you will need to specify a Next Hop IP address for your default route (you'll do this in step 3).
   - **SET TO SELF**
     With this setting, the Concentrator will ARP directly for all IP addresses for which it does not have a route. This requires routers on the Concentrator's LAN segment to have proxy ARP enabled in order for the Concentrator to reach subnets behind the routers. If you select Set to Self, no additional screen changes are needed here. Proceed to step 5.
3. If you have changed the status to Set to Next Hop, enter the IP address of the Next Hop gateway that provides access to the target default network. The Next Hop must be on the network connected to the defined LAN interface.

4. Enter the Metric value. This is the administrative distance to the destination. The administrative distance is typically measured by the hop count (the number of routers) between the Concentrator and the destination. If multiple routes exist to the same destination, the route with the lowest metric value will be chosen as its primary route. A metric value of 0 is interpreted as the destination being reachable directly (no intermediate routers between the Concentrator and the destination). The range of metric values for static routes is from 0 to 15.

5. Select SAVE and then RETURN to return to the IP Configuration menu.

You can configure both a default route (as described above) and static routes (see **Section 4.3.1.C**) through the Concentrator itself, and you can configure routes on a per-device basis through CSM (see the CSM documentation) or RADIUS. A route that designates a different next hop to the same subnet with the same metric as another route is considered “conflicting.” The Concentrator records conflicting routes in log messages (see **Section 4.5**). Check the log for conflicting-route messages, and make changes to the routes as necessary.

4.3.1.C Static LAN Routes

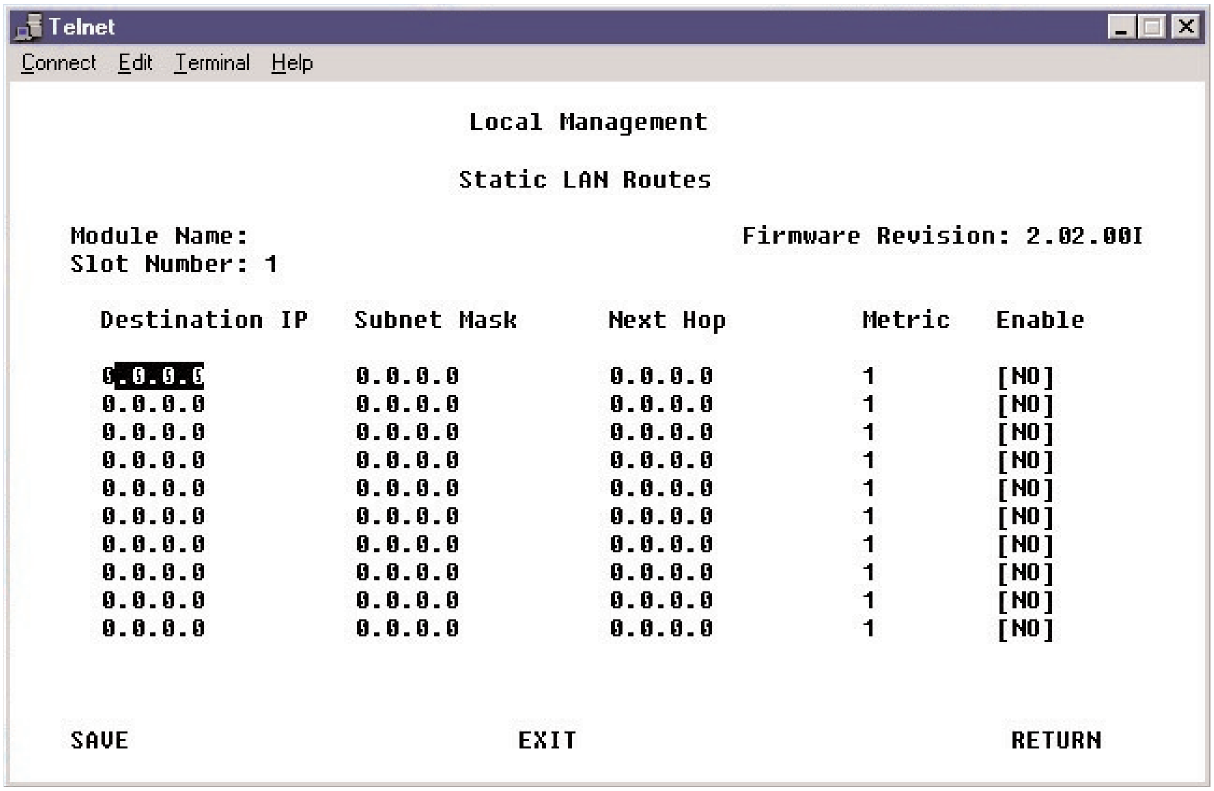
The LAN routes that the Remote Access Concentrator uses to get to subnets reachable through a WAN device are configured using CSM or RADIUS. Routes behind LAN-attached routers are discovered with RIP. And the Concentrator's LAN-interface configuration specifies its LAN subnet. Although all of these routes are automatically entered in the Concentrator's routing table, there are cases where it is necessary to manually enter routes. For example, manually entered static routes are required if:

- There are routers on the LAN that do not support RIP.
- The Concentrator's LAN has more than one subnet. In this case, a route for a subnet that is not the same as that of the LAN interface needs to be manually entered with the LAN interface as the Next Hop and a metric of 0 (direct delivery).

A maximum of 10 static LAN routes may be defined.

To define the Concentrator's static LAN routes:

1. Select Static LAN Routes from the IP Configuration Menu. This screen will appear:



```
                          Local Management

                          Static LAN Routes

  Module Name:                                 Firmware Revision: 2.02.00I
  Slot Number: 1

    Destination IP   Subnet Mask     Next Hop        Metric   Enable

    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]
    0.0.0.0          0.0.0.0         0.0.0.0         1        [NO]


  SAVE                         EXIT                              RETURN
```

2. Enter the route's Destination IP Address. This address specifies the destination subnet or host.
3. Enter the Subnet Mask associated with the Destination IP Address. The mask bits start at the most significant bit of the IP address and proceed to the least significant bit. The mask identifies the static route's subnet. A subnet mask of 255.255.255.255 implies that this static route entry is for a host rather than a subnet.

4. Enter the Next Hop Address. This is the address for the next-hop gateway that provides access to the target subnet or host. The IP address of the Next Hop must be on the subnet connected to the Concentrator's LAN interface.

5. Enter the Metric value. This is the administrative distance to the destination. The administrative distance is typically measured by the hop count (the number of routers) between the Concentrator and the destination. If multiple routes exist to the same destination, the route with the lowest metric value will be chosen as its primary route. A metric value of 0 is interpreted as the destination being reachable directly (no intermediate routers between the Concentrator and the destination). The range of metric values for static routes is from 0 to 15.

6. Select to either enable or disable the static route. Use the space bar to toggle between selections. If you disable the route, the other fields on the screen will remain unchanged, allowing you to easily reactivate the route later.

7. Repeat steps 2 through 6 for each static LAN route (up to 10 routes).

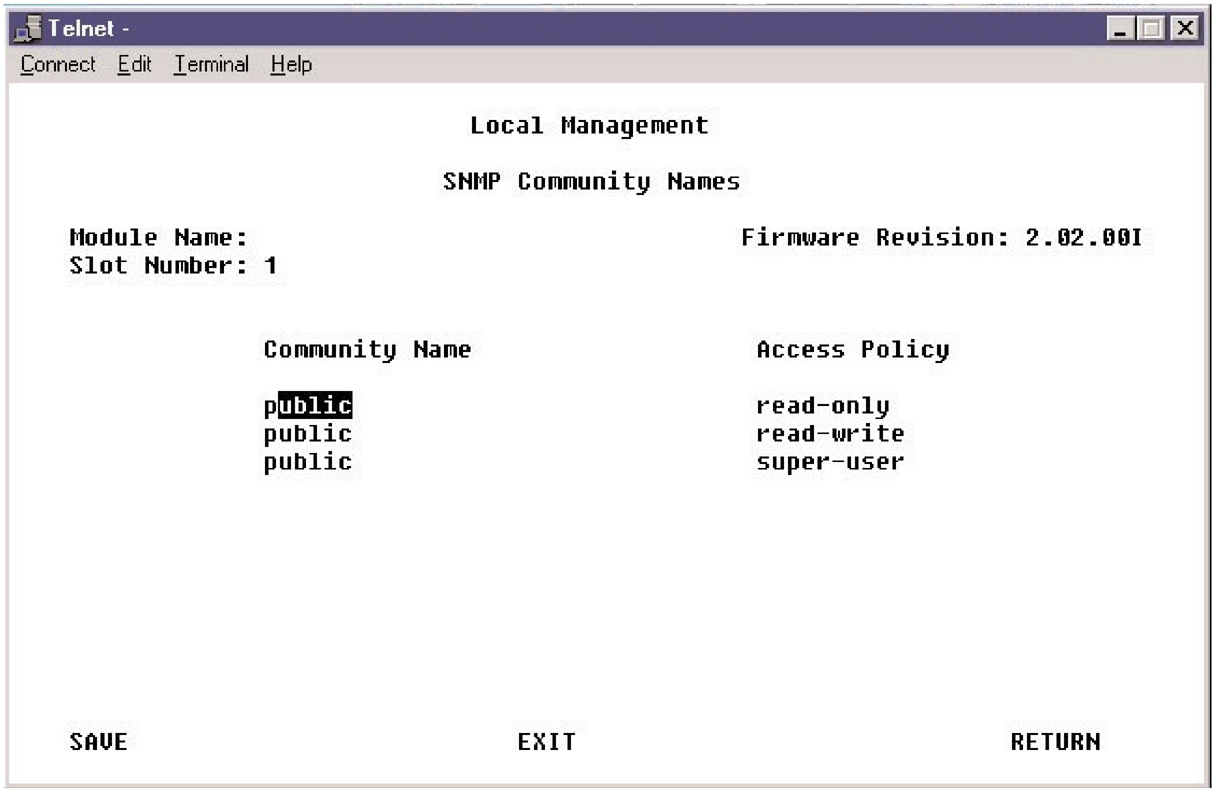
8. Select SAVE and then RETURN to return to the IP Configuration menu.

You can configure both static routes (as described above) and a default route (see **Section 4.3.1.B**) through the Concentrator itself, and you can configure routes on a per-device basis through CSM (see the CSM documentation) or RADIUS. A route that designates a different next hop to the same subnet with the same metric as another route is considered "conflicting." The Concentrator records conflicting routes in log messages (see **Section 4.5**). Check the log for conflicting-route messages, and make changes to the routes as necessary.

4.3.2 SNMP Community Names

Use this menu to change the Remote Access Concentrator's passwords from their initial factory-default values. For security reasons, we suggest making this change at the time of your initial Concentrator installation. Take these steps:

1. From the Local Management utility's Module Menu, select Module Configuration.
2. From the Module Configuration menu, select SNMP Community Names. This screen will appear:



```
                              Local Management

                             SNMP Community Names

  Module Name:                                     Firmware Revision: 2.02.00I
  Slot Number: 1


               Community Name                        Access Policy

               public                                read-only
               public                                read-write
               public                                super-user









  SAVE                         EXIT                                 RETURN
```

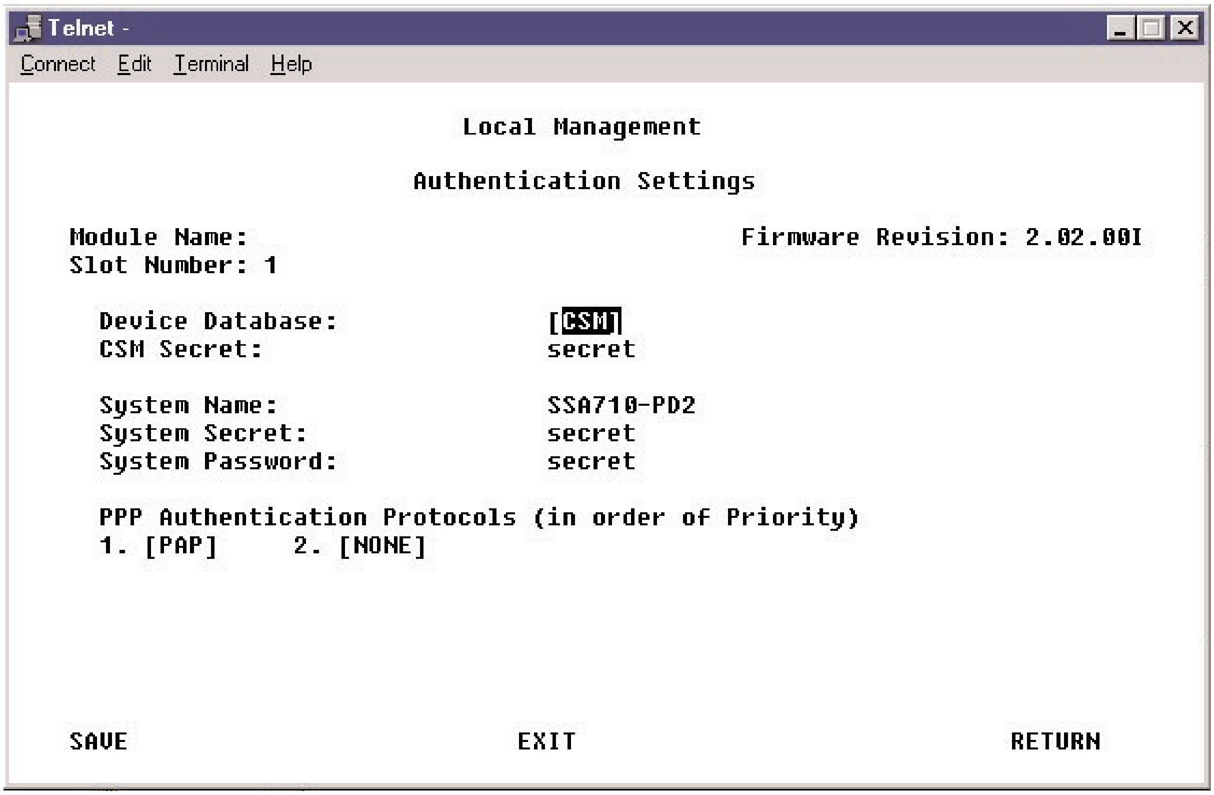
The community names correspond to the passwords you enter to access the Concentrator's local management utility and SNMP. Note that there are three levels of access: read-only, read-write, and super-user.

3. Replace the default password ("public") with your own secure selection.
   Provide passwords for all three categories of access.
4. Select SAVE and then RETURN to go back to the Module Configuration menu.

4.3.3 Authentication Settings

To configure the Remote Access Concentrator's Authentication Settings, take these steps:

1. Select Module Configuration from the Local Management utility's Module Menu.
2. Select Authentication Settings from the Module Configuration menu. This screen will appear:



```
                         Local Management

                      Authentication Settings

  Module Name:                                 Firmware Revision: 2.02.00I
  Slot Number: 1

    Device Database:             [CSM]
    CSM Secret:                  secret

    System Name:                 SSA710-PD2
    System Secret:               secret
    System Password:             secret

    PPP Authentication Protocols (in order of Priority)
    1. [PAP]     2. [NONE]



  SAVE                          EXIT                             RETURN
```

3. Select the type of Device Database you'll be using. The device database stores remote-device data used for device authentication. Use the space bar to toggle your selection between either RADIUS (if you'll be using an RFC-2138-compliant RADIUS server) or CSM (if you'll be using CSM for device authentication). Note that CSM not only performs traditional authentication tasks, it also allows for more advanced policy management and flow accounting.

Steps 4 through 7 concern CSM and call-out functions only; if you've chosen RADIUS as your device database, skip to step 8. (You'll use the Local Management utility's RADIUS menu to configure the authentication information—a shared secret—required for the Concentrator to interact with RADIUS; see **Section 4.3.5**.)

NOTE

The CSM Secret, System Name, and System Secret you'll set in steps 4 through 6 must match those configured through CSM (under the Properties tab of CSM's Access Server option). Refer to CSM's HTML documentation.

4. Enter the CSM Secret. This is the CHAP secret shared between CSM and the Concentrator and used for authentication negotiation.
5. Enter a unique System Name for the Concentrator.

6. Enter the System Secret. This is the Concentrator's own CHAP secret, used in authentication negotiation not only with CSM but also whenever the Concentrator calls out to remote devices that use CHAP.

7. Enter the System Password. This is the Concentrator's PAP secret, used for authentication negotiation when the Concentrator calls out to a remote device that uses PAP.

8. Prioritize the PPP Authentication Protocols to be used for authenticating remote devices. By default, the Concentrator will authenticate remote devices using CHAP first and PAP second (as shown in the example screen). You may change the defaults to meet your network's requirements. For example, if the Concentrator's remote devices only use PAP, you will need to change the priority to PAP first, and either CHAP or NONE second. Choices for the preferred authentication protocol are CHAP or PAP. Choices for the second protocol are CHAP, PAP, or NONE. Use the space bar to toggle the selection.

9. Select SAVE and then RETURN to return to the Module Configuration menu.

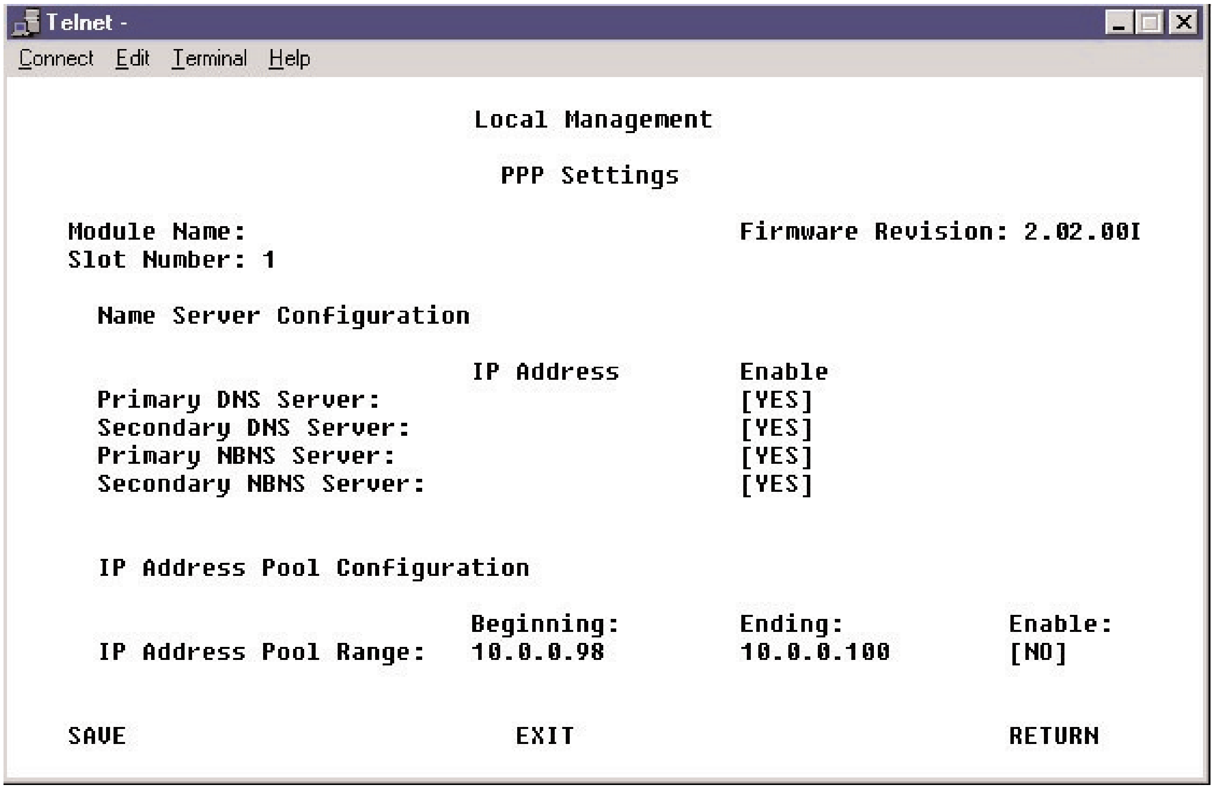
4.3.4 PPP Settings

Through the Concentrator's PPP settings, you can:

- **Configure name server information**
  This feature implements RFC 1877—PPP Internet Protocol Control Protocol Extensions for Name Server Addresses—which allows the Concentrator to supply remote devices with primary and secondary Domain Name System (DNS) and NetBIOS Name Server (NBNS) addresses when they dial in to the Concentrator using Windows dialup. When this feature is configured, dialup users no longer need to manually configure DNS and NBNS server addresses on their Windows PCs; the server addresses are automatically configured when they dial in to the Concentrator.
- **Define an IP-address pool**
  This allows you to define a simple IP-address pool, which allows the Concentrator to dynamically allocate IP addresses to remote devices as they dial in. The pool is mainly used when the Concentrator's authentication database is a RADIUS server. If you're using CSM instead, we recommend that you use CSM's own IP address pool; see CSM's HTML documentation.

To use these features:

1. Select Module Configuration from the Local Management utility's Module Menu.
2. Select PPP Settings from the Module Configuration menu. This screen will appear:



```
                        Local Management

                          PPP Settings

  Module Name:                              Firmware Revision: 2.02.00I
  Slot Number: 1

    Name Server Configuration

                             IP Address        Enable
    Primary DNS Server:                        [YES]
    Secondary DNS Server:                      [YES]
    Primary NBNS Server:                       [YES]
    Secondary NBNS Server:                     [YES]


    IP Address Pool Configuration

                             Beginning:        Ending:           Enable:
    IP Address Pool Range:   10.0.0.98         10.0.0.100        [NO]


  SAVE                           EXIT                            RETURN
```

3. To complete the Name Server Configuration, tab to the appropriate row, enter the server's IP Address, and toggle the Enable value to YES.

4. To complete the IP Address Pool Configuration, enter a Beginning and Ending address for the IP Address Pool Range and toggle the Enable value to YES.

5. Select SAVE and then RETURN to return to the Module Configuration menu.

4.3.5 Using a RADIUS Server as a Device Database

You may use a RADIUS server with a Remote Access Concentrator both for remote device authentication and to maintain accounting information.

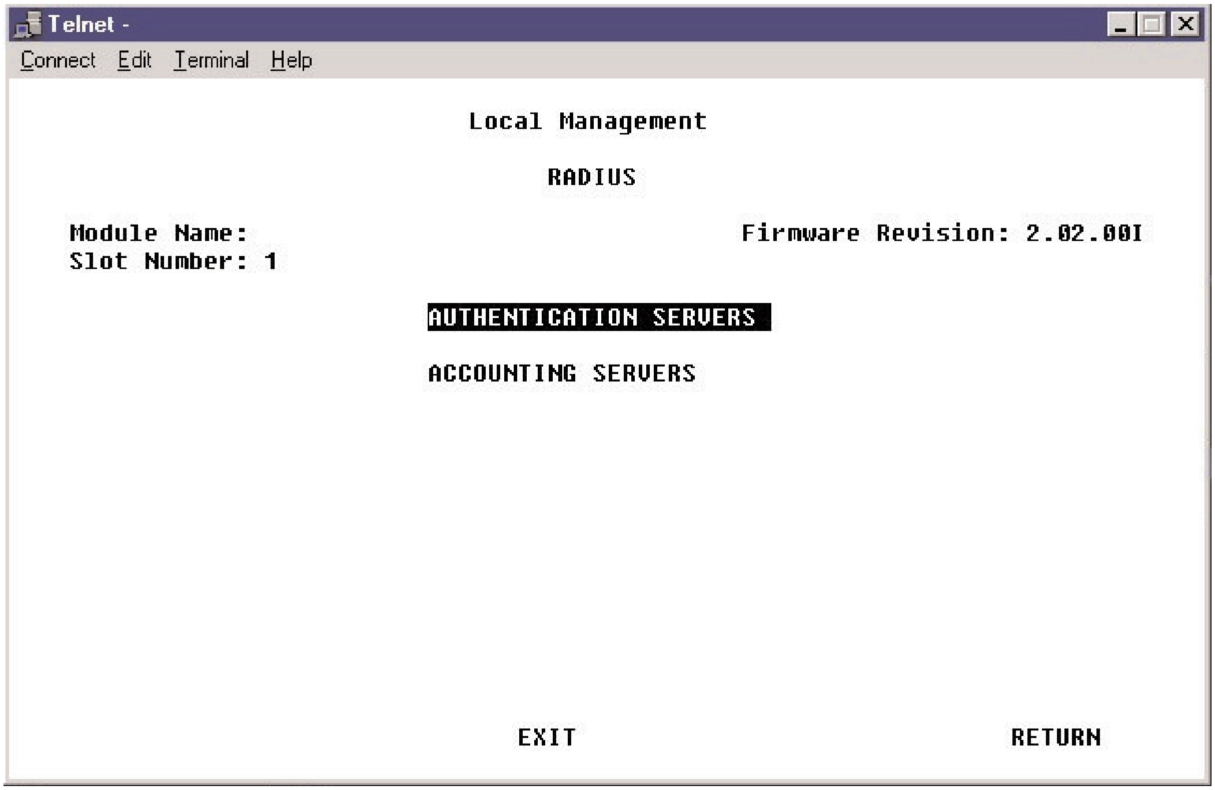
NOTE

If the RADIUS device is not on the same subnet as the Concentrator, you will need to define either a default LAN route (see Section 4.3.1.B**) or a static LAN route (see** Section 4.3.1.C**) to the RADIUS device, and add a matching route on that device (that is, a route from the device to the Concentrator) by issuing a route command at the device's command prompt.**

For information regarding RADIUS Client features supported by the Concentrator's software, see Section 4.3.5.C**.**

To configure RADIUS information on the Concentrator:

1. Select Module Configuration from the Local Management utility's Module Menu.
2. Select RADIUS from the Module Configuration menu. This screen will appear:



```
                         Local Management

                              RADIUS

  Module Name:                                 Firmware Revision: 2.02.00I
  Slot Number: 1

                       AUTHENTICATION SERVERS

                       ACCOUNTING SERVERS




                           EXIT                                 RETURN
```

3. If you'll be using a RADIUS server as an authentication server for remote devices, you *must* configure the Authentication Servers settings; see **Section 4.3.5.A**. You don't need to configure the Accounting Servers settings unless you're also using a RADIUS server for accounting information; if you are, see **Section 4.3.5.B**.

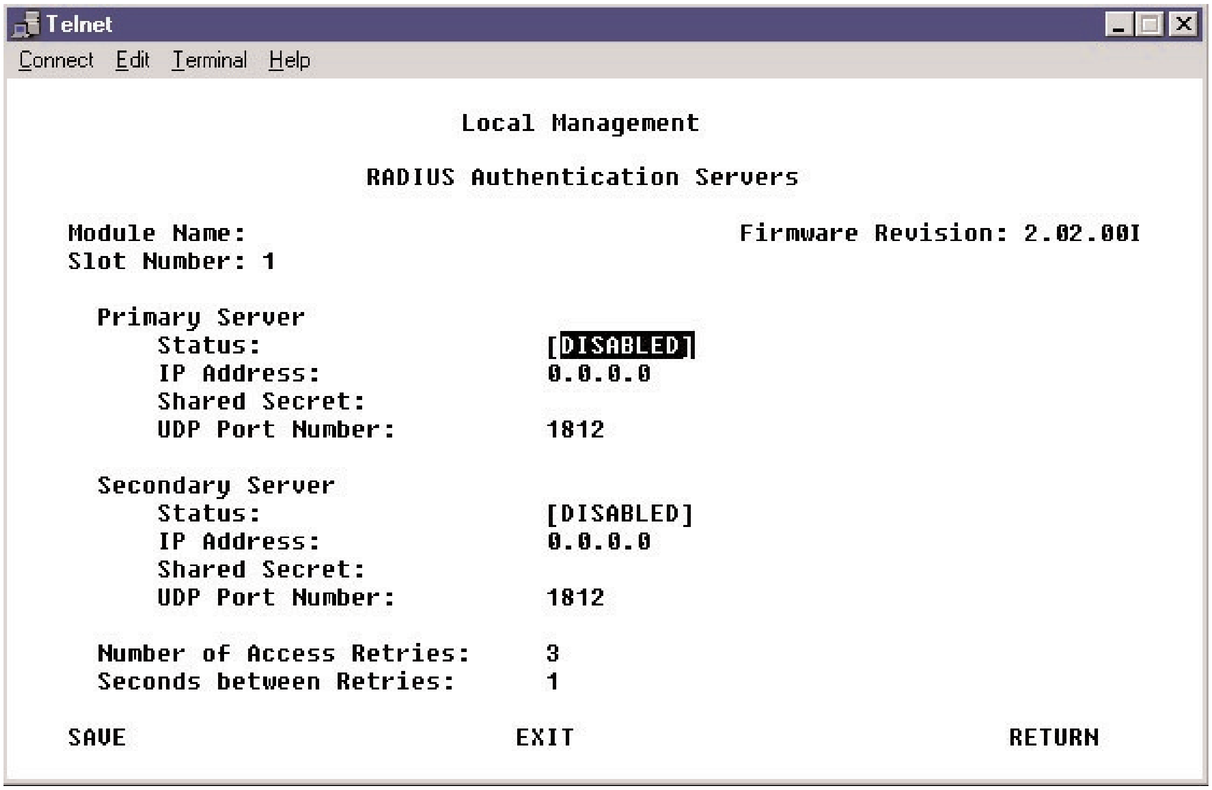
4.3.5.A RADIUS Authentication Servers

If you want to, you can use the Remote Access Concentrator's software implementation of a RADIUS authentication client with a RADIUS authentication server acting as your device database. As a client, the Concentrator sends access-request packets to designated RADIUS authentication servers to authenticate remote devices.

If you are using RADIUS as your device database, you *must* configure information for a Primary RADIUS Authentication Server. Configuring a Secondary Server is optional; in the event that the primary server does not respond to system requests, the secondary server will be queried for device authentication information.

To enter information for RADIUS authentication servers, take these steps:

1. Select Authentication Servers from the RADIUS menu. This menu will appear:



```
                          Local Management

                    RADIUS Authentication Servers

    Module Name:                                  Firmware Revision: 2.02.00I
    Slot Number: 1

      Primary Server
          Status:                 [DISABLED]
          IP Address:             0.0.0.0
          Shared Secret:
          UDP Port Number:        1812

      Secondary Server
          Status:                 [DISABLED]
          IP Address:             0.0.0.0
          Shared Secret:
          UDP Port Number:        1812

      Number of Access Retries:   3
      Seconds between Retries:    1

    SAVE                        EXIT                              RETURN
```

2. Use the space bar to toggle the Primary Server's Status to ENABLED.

3. Enter the IP Address of the primary server.

4. Enter the Shared Secret between the Concentrator and the primary server.

5. Enter the UDP Port Number used by the server. The UDP port number defaults to 1812 because this is the port number assigned for RADIUS authentication in RFC 2138. However, many RADIUS servers use UDP port number 1645 for authentication instead.

6. *If you're using a secondary RADIUS authentication server:* Repeat steps 2 through 5 for the Secondary Server. (In most cases, the address of the secondary server will not be the same as that of the primary server. If, however, you have two RADIUS servers running on the same PC but using different UDP ports, the two servers *would* have the same IP address.)

7. Specify the Number of Access Retries that the system will send to the RADIUS authentication server. When a remote device needs to be authenticated, the Concentrator will send an access request to the server. After a set wait-for-response interval elapses—you'll configure the length of this interval in the next step—the system will send an access-request retry if the server does not respond. Once the configured number of access-request retries has been reached, the Concentrator will request authentication information from the secondary server if one is configured. If there is no secondary server configured or if the secondary server also fails to respond to the access requests, the connection will be released.

8. Specify the Seconds between Retries. This is the time in seconds between access-request retries sent from the Concentrator to the RADIUS authentication server.

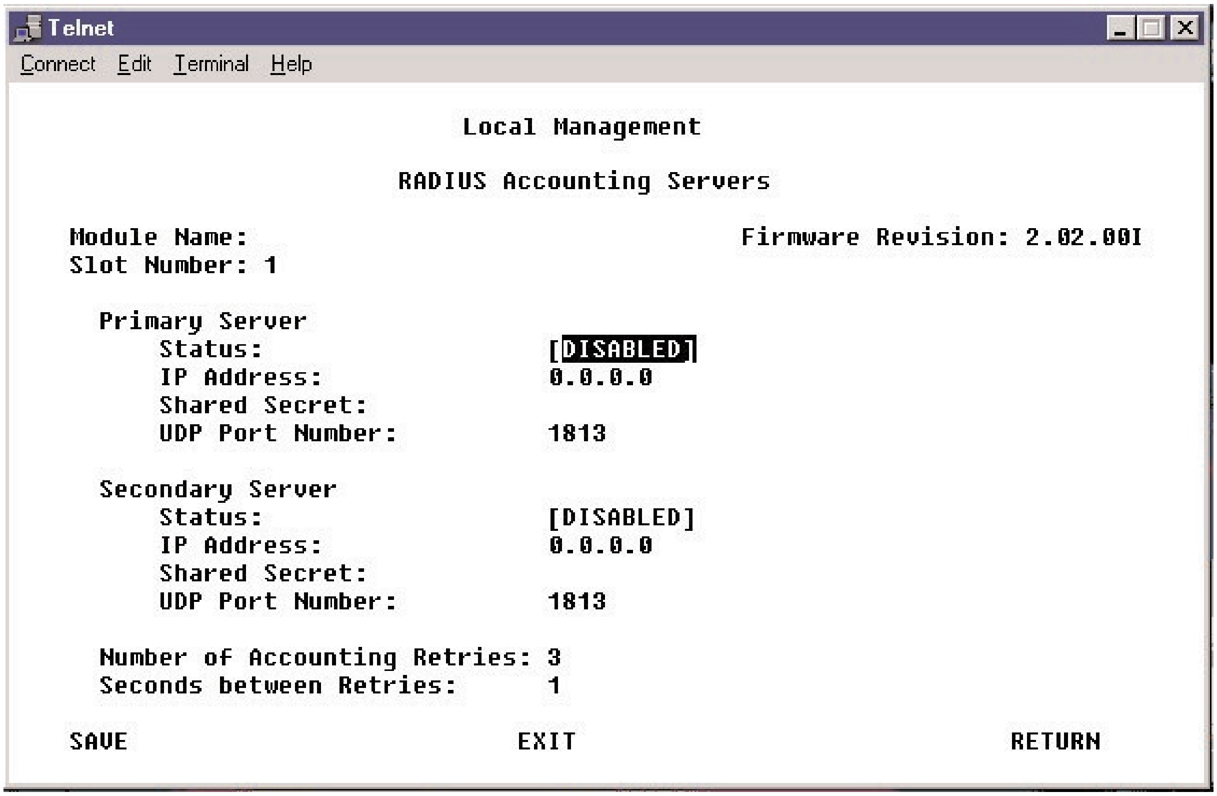
9. Select SAVE and then RETURN to go back to the RADIUS menu.

4.3.5.B RADIUS Accounting Servers

If you want to, you can use the Remote Access Concentrator's software implementation of a RADIUS accounting client. As a client, the Concentrator sends accounting packets to designated RADIUS accounting servers. When a call is initiated and authenticated successfully, the Concentrator will send an accounting-request "START" packet to flag the start of a call. When the call is terminated, the Concentrator will send a corresponding accounting-request "STOP" packet. This packet exchange provides a means of determining the session time for the call (that is, the number of seconds the call has been active).

To enter information for RADIUS accounting servers, take these steps:

1. Select Accounting Servers from the RADIUS menu. This screen will appear:



```
                          Local Management

                       RADIUS Accounting Servers

   Module Name:                                  Firmware Revision: 2.02.00I
   Slot Number: 1

     Primary Server
         Status:                 [DISABLED]
         IP Address:             0.0.0.0
         Shared Secret:
         UDP Port Number:        1813

     Secondary Server
         Status:                 [DISABLED]
         IP Address:             0.0.0.0
         Shared Secret:
         UDP Port Number:        1813

     Number of Accounting Retries: 3
     Seconds between Retries:      1

   SAVE                         EXIT                            RETURN
```

2. Use the space bar to toggle the Primary Server's Status to ENABLED.

3. Enter the IP Address of the primary server.

4. Enter the Shared Secret between the Concentrator and the primary server.

5. Enter the UDP Port Number used by the server. The UDP port number defaults to 1813 because this is the port number assigned for RADIUS accounting in RFC 2139. However, many RADIUS servers use UDP port number 1646 for accounting instead.

6. *If you're using a secondary RADIUS authentication server:* Repeat steps 2 through 5 for the Secondary Server. (In most cases, the address of the secondary server will not be the same as that of the primary server. If, however, you have two RADIUS servers running on the same PC but using different UDP ports, the two servers *would* have the same IP address.)

7. Specify the Number of Access Retries that the system will send to the RADIUS accounting server. When a call is initiated, the Concentrator will send an accounting request to the server. After a set wait-for-response interval elapses—you'll configure the length of this interval in the next step—the system will send an accounting-request retry if the server does not respond. Once the configured number of accounting-request retries has been reached, the Concentrator will start sending accounting requests to the secondary server if one is configured. If there is no secondary server configured or if the secondary server also fails to respond to the accounting requests, no accounting data will be logged.

8. Specify the Seconds between Retries. This is the time in seconds between accounting-request retries sent from the Concentrator to the RADIUS authentication server.

9. Select SAVE and then RETURN to go back to the RADIUS menu.

4.3.5.C RADIUS Client Support

The Remote Access Concentrator's RADIUS Client supports these features:

- **Device-level authentication** for inbound PPP-IP and PPP-bridge devices.
- **CHAP** or **PAP authentication** (one or the other is required).
- **Remote-device IP addresses:** Assigned by the RADIUS server or selected by the remote device itself.
- **Call accounting:** Records the number of "in" octets, "in" packets, "out" octets, and "out" packets; the multi-session ID; and the number of seconds a B-channel is in service. (If desired, the number of calls can be calculated by counting records with the same multi-session ID.)

Table 4-2 below and on the following pages describes supported attributes for the Access-Request, Access-Accept, Access-Reject, Accounting-Request, and Accounting-Response packet types. Each of the attribute types in the table are more fully described in RFC 2138 and RFC 2139.

Table 4-2. Supported RADIUS-Packet Attributes

ID	Attribute Name	Comments
1	User-Name	In Access-Request and Accounting-Request. Currently, this is always the device name.
2	User-Password	In Access-Request.
3	CHAP-Password	In Access-Request.
4	NAS-IP-Address	In Access-Request and Accounting-Request.
5	NAS-Port	In Access-Request and Accounting-Request. The NAS-Port attribute can be useful for determining physical resources used by a connection. It's a 5-digit number with the format: *<type> <wide area port> <channel>* *<type>* is "1" for a digital call or "2" for an analog call. *<wide area port>* uses two digits to specify the port that the call is using. *<channel>* uses two digits to represent the channel on the line that the call is using. For example, an analog call on port 1, channel 0 would have a NAS-Port attribute of "20100".
6	Service-Type	In Access-Request and Access-Accept. The only supported Service-Type is Framed (Framed protocol PPP).
7	Framed-Protocol	In Access-Request and Access-Accept. The only supported Framed Protocol is PPP.

Table 4-2. Supported RADIUS-Packet Attributes (continued)

ID	Attribute Name	Comments
8	Framed-IP-Address	Access-Accept may contain this attribute, which indicates the IP address assigned to the remote device. If the attribute is 255.255.255.255, the NAS (Network Access Server—the Concentrator in this case) should allow the user to select an address. If it is 255.255.255.254, the NAS should select an address for the user. Accounting-Request will also contain this attribute. If the Framed-IP-Address attribute is not specified in an Access-Accept message, or if it is specified as being 255.255.255.255, the Concentrator will attempt to establish a WAN Unnumbered connection with the remote device. If the Framed-IP-Address attribute is specified in an Access-Accept message as something other than 255.255.255.255, the Concentrator will attempt to establish a WAN Direct Host connection with the remote device. When establishing the WAN Direct Host connection, the Concentrator will only allow the remote device to use the IP address specified in the Framed-IP-Address attribute. A WAN Direct Host remote device must be assigned an IP address by either CSM or a RADIUS server.
22	Framed-Route	Up to five routes can be specified for a remote device. This attribute contains a destination prefix in dotted quad form, optionally followed by a slash and a decimal length specifier stating how many high-order bits of the prefix should be used. That is followed by a space, a gateway address in dotted quad form, another space, and a metric. An example of this full form would be “192.168.1.0/24 0.0.0.0 2”. The length specifier may be omitted, in which case it defaults to 8 bits for class-A prefixes, 16 bits for class-B prefixes, and 24 bits for class-C prefixes. An example of this shortened form would be “192.168.1.0 0.0.0.0 2”. When the gateway address is specified as “0.0.0.0”, the IP address of the device is used as the gateway address. “0.0.0.0” is the only gateway address we support. If any other gateway address is encountered, it is ignored, and the gateway address is treated as if it had been configured as “0.0.0.0”.
25	Class	Used for accounting. Allows for different classes of users. If the Class attribute is returned to the Concentrator in an Access-Accept message for a call, it will be reported in Accounting-Request messages that pertain to the call.
30	Called-Station-Id	In Access-Request and Accounting-Request.
31	Calling-Station-Id	In Access-Request and Accounting-Request. This attribute is only reported when the Calling-Station-Id is reported to the Concentrator by the ISDN switch.

Table 4-2. Supported RADIUS-Packet Attributes (continued)

ID	Attribute Name	Comments
40	Acct-Status-Type	In Accounting-Request packet. Indicates whether this is the beginning of the user service (Start) or the end (Stop).
42	Acct-Input-Octets	In Accounting-Request packet. Number of octets received from the port over the course of this service being provided.
43	Acct-Output-Octets	In Accounting-Request packet. Number of octets sent to the port in the course of delivering this service.
44	Acct-Session-Id	This attribute is a unique Accounting ID to make it easy to match start and stop records in a log file.
45	Acct-Authentic	Indicates how the user was authenticated: whether by RADIUS, the Concentrator itself, or CSM.
46	Acct-Session-Time	This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type (ID 40) is set to Stop.
47	Acct-Input-Packets	In Accounting-Request packet. Number of packets received on the port.
48	Acct-Output-Packets	In Accounting-Request packet. Number of packets sent on port.
49	Acct-Terminate-Case	May be sent in Accounting-Request messages when a session terminates. Specifies the cause of session termination.
50	Acct-Multi-Session-Id	In Accounting-Request packet. This attribute is a unique Accounting ID to make it easy to link together multiple related sessions in a log file. Sessions (B-channel calls) with the same Acct-Multi-Session-Id are part of the same PPP multilink connection to a remote device.
61	NAS-Port-Type	In Access-Request and Accounting-Request packets. Digital Modem calls are Async; ISDN calls are ISDN Sync; other NAS-Port-Type values are not used.

4.3.6 CAS Configuration

You may configure the Remote Access Concentrator to provide channel associated signaling (CAS). Similar to ISDN signaling, CAS signaling methods provide an interface for the telco switch to signal incoming calls (or, with the R2 protocol, both incoming and outgoing calls).

CAS must be both enabled and configured on the Concentrator in order to be operational. On E1 models of the Concentrator, take the steps described in **Section 4.3.6.A** to enable and configure the R2 CAS protocol; on T1 models, take the steps described in **Section 4.3.6.B** to enable and configure the RBS CAS protocol.

4.3.6.A R2 (for E1)

Because the E1 models of the Remote Access Concentrator support R2, they can accept incoming calls and place outgoing calls over E1 lines provisioned for R2 signaling. R2 signaling uses data in the E1 multiframe to perform line signaling (line seizure and clearing), then uses in-band signaling (forward and backward compelled tones) to exchange call-setup information.

To activate R2 signaling, you must enable Channel Associated Signaling (CAS) through the Concentrator's Network Tools interface (see **Section 4.4**), and then configure CAS through the Module Configuration menu. Take these steps:

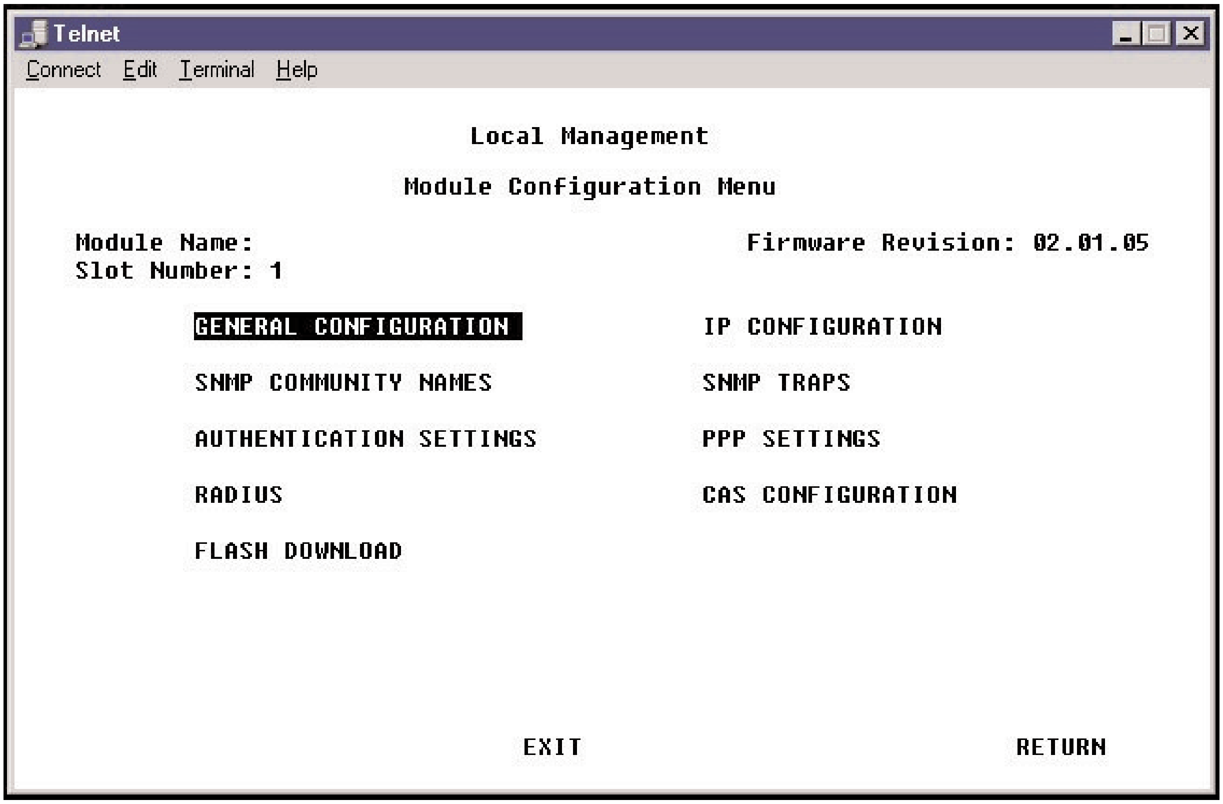
1. From Local Management's Module Menu, select Network Tools. The Network Tools command prompt appears. (Network Tools is command-line-driven.)
2. At the Network Tools prompt, set the line's signal mode to bit-oriented by typing in the command

   ```
   wanl1p signalmode bitOriented <port#>
   ```

   replacing the variable <port#> with the actual port number (that is, the line number) you want reserved for R2 signaling. For example, to reserve both ports on the LRA3003A for R2 signaling, enter the following two commands:

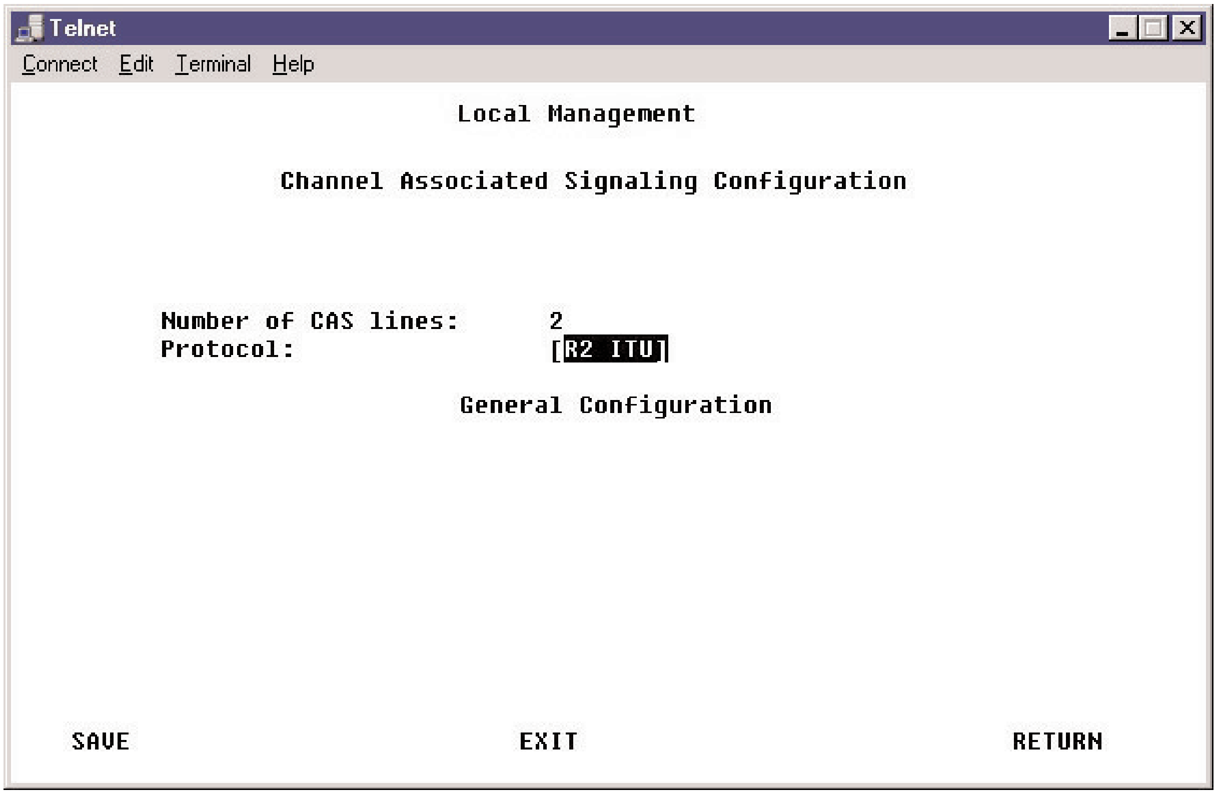
   ```
   wanl1p signalmode bitOriented 1
   wanl1p signalmode bitOriented 2
   ```
3. Reboot the system. (You can perform a soft reboot by typing in Network Tools' `soft_reset` command.)

4. Select Module Configuration from the Local Management utility's Module Menu. The screen below will appear.



```
                              Local Management

                          Module Configuration Menu

  Module Name:                                         Firmware Revision: 02.01.05
  Slot Number: 1

          GENERAL CONFIGURATION             IP CONFIGURATION

          SNMP COMMUNITY NAMES              SNMP TRAPS

          AUTHENTICATION SETTINGS           PPP SETTINGS

          RADIUS                            CAS CONFIGURATION

          FLASH DOWNLOAD




                              EXIT                                RETURN
```

5. You'll notice that the Module Configuration menu now includes an option—CAS Configuration—that it didn't before. (This option only appears after CAS has been enabled in Network Tools and the system has been rebooted.) Select CAS Configuration. This screen will appear:



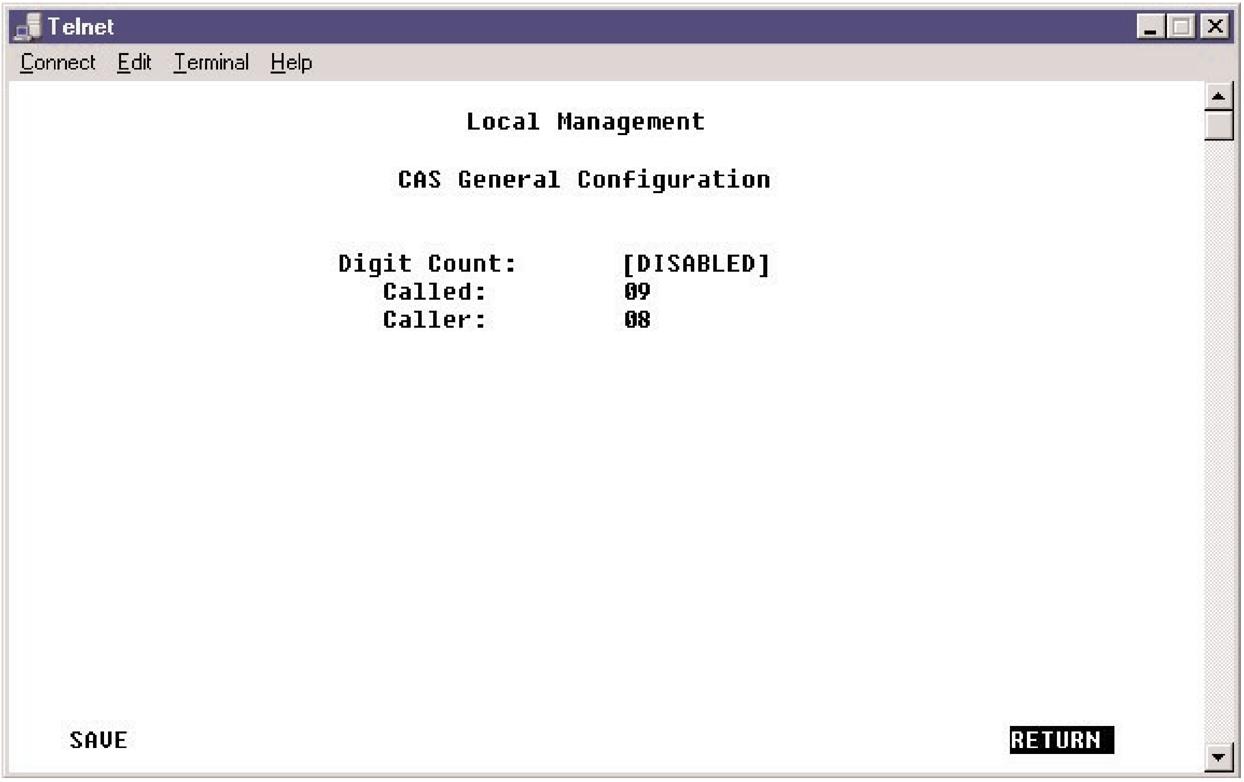
```
                         Local Management

                 Channel Associated Signaling Configuration



         Number of CAS lines:      2
         Protocol:                 [R2 ITU]

                         General Configuration









   SAVE                           EXIT                           RETURN
```

Note that the Number of CAS Lines is not changeable through this menu. Its value is equal to the number of lines you set for bit-oriented signaling in step 2.

6. Press the space bar as necessary to toggle Protocol to your desired R2 setting ("R2 ITU", for example).

7. Save any changes before proceeding.

8. There are some CAS protocols (such as R2 Mexico) for which you may designate the number of digits used for the telephone number. To set the digit count, select the General Configuration option by using the arrow keys to move the highlight onto it and pressing Enter. This screen will appear:



```
                    Local Management

                 CAS General Configuration


               Digit Count:       [DISABLED]
                  Called:         09
                  Caller:         08









  SAVE                                              RETURN
```

If Digit Count appears as ENABLED in this menu, you may change the count's value. If it appears as DISABLED, digit counting is not enforced for the protocol you've selected; other mechanisms are used to know when the phone number is complete.

9. Save any changes you have made and return to the previous menu.

Note that a channel-associated signaling resource does not have an ISDN Layer 2; so you will not see a "Data link up" log message. Instead, once the R2 line is operational, you should see a "Channel Associated Signaling Up" log message.

4.3.6.B RBS (for T1)

The T1 models of the Remote Access Concentrator are capable of accepting incoming calls over a channelized T1 (CT1) line provisioned for Robbed Bit Signaling (RBS). RBS is a framing pattern that allows signaling bits to be "robbed" every sixth frame. The least significant bit of a channel's time slot is preempted in selected frames.

To activate RBS signaling, you must enable Channel Associated Signaling (CAS) through the Concentrator's Network Tools interface (see **Section 4.4**), and then configure CAS through the Module Configuration menu. Take these steps:

1. From Local Management's Module Menu, select Network Tools. The Network Tools command prompt appears. (Network Tools is command-line-driven.)
2. At the Network Tools prompt, set the line's signal mode to robbed bit by typing in the command

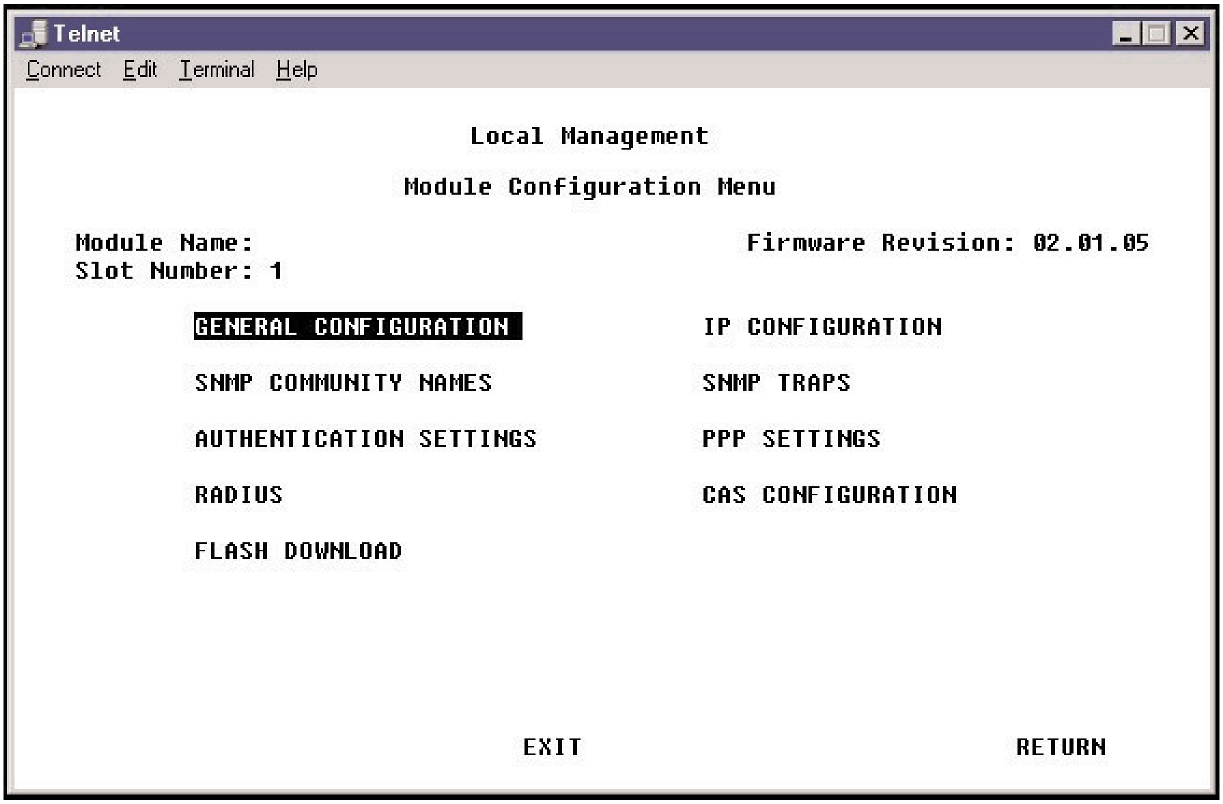
   ```
   wanl1p signalmode robbedBit <port#>
   ```

   replacing the variable <port#> with the actual port number (that is, the line number) you want reserved for RBS. For example, to reserve both ports on the Concentrator for RBS, enter the following two commands:

   ```
   wanl1p signalmode robbedBit 1
   wanl1p signalmode robbedBit 2
   ```

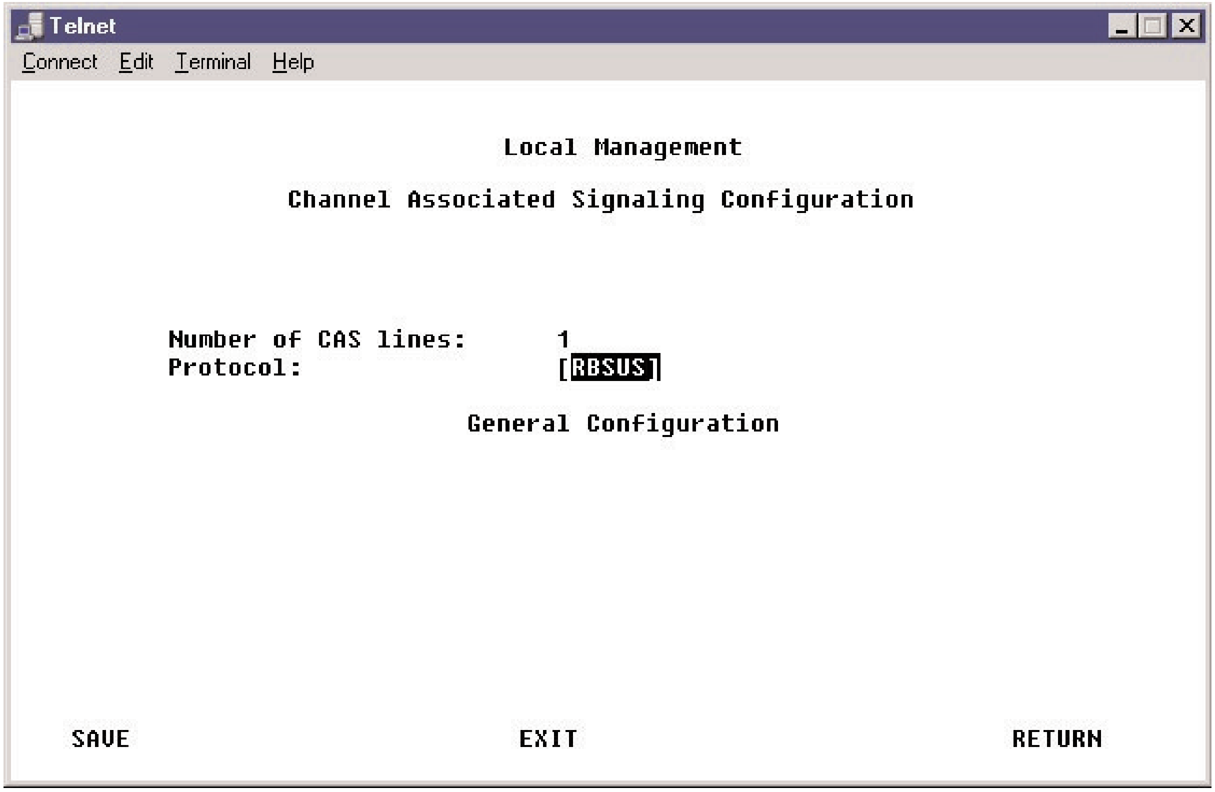
3. Reboot the system. (You can perform a soft reboot by typing in Network Tools' `soft_reset` command.)

4. Select Module Configuration from the Local Management utility's Module Menu. The screen below will appear.



```
                         Local Management

                      Module Configuration Menu

 Module Name:                               Firmware Revision: 02.01.05
 Slot Number: 1

        GENERAL CONFIGURATION              IP CONFIGURATION

        SNMP COMMUNITY NAMES               SNMP TRAPS

        AUTHENTICATION SETTINGS            PPP SETTINGS

        RADIUS                             CAS CONFIGURATION

        FLASH DOWNLOAD




                       EXIT                              RETURN
```

5. You'll notice that the Module Configuration menu now includes an option—CAS Configuration—that it didn't before. (This option only appears after CAS has been enabled in Network Tools and the system has been rebooted.) Select CAS Configuration. This screen will appear:



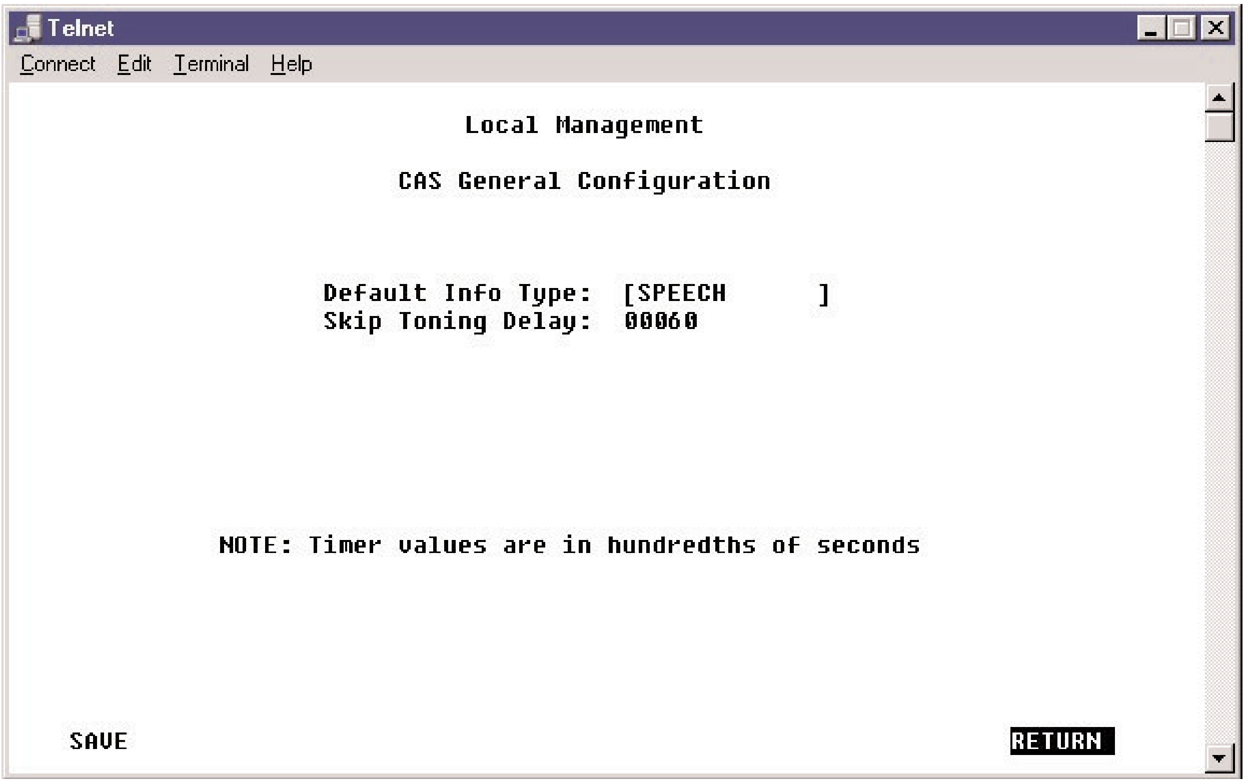
```
                         Local Management

              Channel Associated Signaling Configuration



        Number of CAS lines:        1
        Protocol:                   [RBSUS]

                        General Configuration









    SAVE                        EXIT                          RETURN
```

Note that the Number of CAS Lines is not changeable through this menu. Its value is equal to the number of lines you set for bit-oriented signaling in step 2.

6. Press the space bar as necessary to toggle Protocol to your desired RBS setting ("RBSUS", for example).

7. Save any changes before proceeding.

8. Select the General Configuration option by using the arrow keys to move the highlight onto it and pressing Enter. This screen will appear:



```
                         Local Management

                      CAS General Configuration


                 Default Info Type:  [SPEECH      ]
                 Skip Toning Delay:  00060




             NOTE: Timer values are in hundreds of seconds



    SAVE                                                    RETURN
```

This screen displays Default Info Type and Skip Toning Delay information. Note that the Skip Toning Delay is measured in hundredths of seconds (in this example, 00060 =0.6 seconds).

9. Specify your Default Info Type. This field indicates the type of data that the Concentrator should expect calls to carry, so it affects how every call is connected on this line. As it's shipped from the factory, the Concentrator's Default Info Type is SPEECH. We don't recommend selecting anything other than SPEECH unless you know that your configuration requires a different selection (if every single one of your calls will be data calls, for example).

10. Save any changes you have made and return to the previous menu.

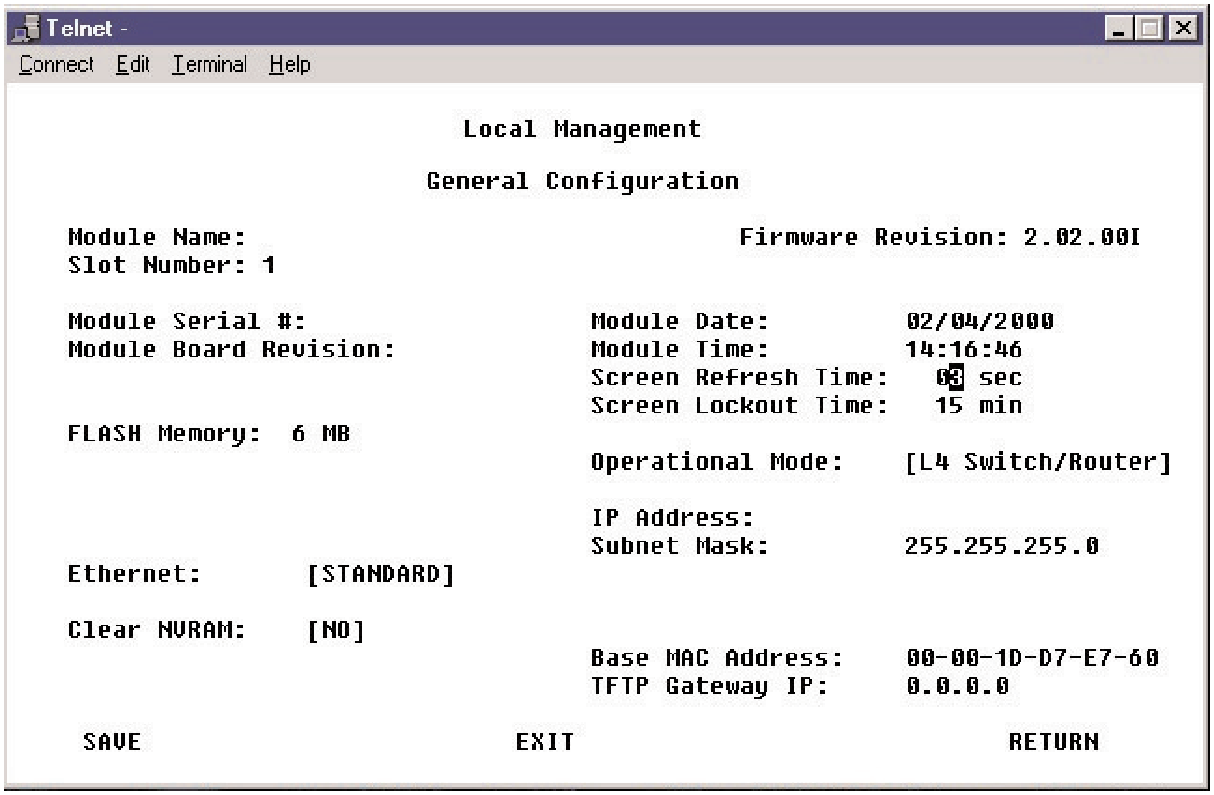
Note that a channel-associated signaling resource does not have an ISDN Layer 2; so you will not see a "Data link up" log message. Instead, once the RBS line is operational, you should see a "Channel Associated Signaling Up" log message.

4.3.7 General Configuration

Use the General Configuration menu of the Remote Access Concentrator's Local Management utility to set date and time information, as well as to establish the Concentrator's IP address. Also, if you ever need to restore your Concentrator to its factory-default settings (including its password), select Clear NVRAM from this menu to purge the Concentrator's nonvolatile RAM.

To enter general configuration information for the Concentrator, take these steps:

1. Select Module Configuration from the Local Management utility's Module Menu.
2. Select General Configuration from the Module Configuration menu. This screen will appear:



```
                          Local Management

                        General Configuration

 Module Name:                              Firmware Revision: 2.02.00I
 Slot Number: 1

 Module Serial #:                  Module Date:         02/04/2000
 Module Board Revision:            Module Time:         14:16:46
                                   Screen Refresh Time:   03 sec
                                   Screen Lockout Time:   15 min
 FLASH Memory:  6 MB
                                   Operational Mode:    [L4 Switch/Router]

                                   IP Address:
                                   Subnet Mask:         255.255.255.0
 Ethernet:        [STANDARD]

 Clear NVRAM:     [NO]
                                   Base MAC Address:    00-00-1D-D7-E7-60
                                   TFTP Gateway IP:     0.0.0.0

  SAVE                        EXIT                              RETURN
```

3. Enter Module Date and Time information.
4. Enter the Concentrator's IP Address; if you're using CSM, you'll need to enter this in CSM as well (see **Section 5.2.2**). Note that you can also set the address in the Concentrator's IP LAN Interface screen (see **Section 4.3.1.A**); if you change the address here, the change will be automatically reflected in that screen, and vice versa.
5. Enter the Subnet Mask for the IP address. Note that you can also set the subnet mask in the Concentrator's IP LAN Interface screen (see **Section 4.3.1.A**); if you change the mask here, the change will be automatically reflected in that screen, and vice versa.

6. TFTP is used for uploading firmware upgrades to the Concentrator. If your TFTP server is not on the same physical/logical subnet as the Concentrator, you will need to enter its IP address in the TFTP Gateway IP field. Note that you can also set this address in the Concentrator's Flash Download screen (see **Section 4.3.8**); if you change this address here, the change will be automatically reflected in that screen, and vice versa.

7. Verify the entered information, then select SAVE. The Concentrator will automatically reboot so that the changes take effect immediately.

4.3.8 Flash Download (Upgrading the Firmware)

There are several methods available for upgrading your Remote Access Concentrator's firmware. The first time you do so—and each subsequent time you upgrade a single Concentrator, or every time you upgrade if you aren't using CSM—you'll probably want to use the Concentrator's Local Management utility as described in this section. (For this upgrade method, a TFTP server is required.) If you're using CSM in a multiple-Concentrator system, however, it will probably be easier to use other methods available through CSM to simultaneously upgrade your Concentrators; see **Section 5.3**.

To use the Local Management utility to upgrade a Concentrator's firmware, take these steps:

1. Check your TFTP-server setup. The TFTP server must be "available" to the Concentrator, meaning it must either *be* on the same LAN as the Concentrator, or *appear to be* on the same LAN. Specifically, one of these conditions needs to be true:

   - The Concentrator and the TFTP server are on the same physical and logical LAN subnet. (This is the recommended case.)

   - The Concentrator and TFTP server are on the same logical LAN subnet and "appear to be" on the same physical LAN subnet (there's some sort of bridge between them).

   - The Concentrator and the TFTP server are on different logical subnets (even if they're on the same physical subnet). In this case, a gateway (router) is required, and you'll have to configure a TFTP Gateway Server IP address (refer to step 5e). Note that you can also set this address in the Concentrator's General Configuration screen (see **Section 4.3.6**); if you change the address here, the change will be automatically reflected in that screen, and vice versa.

     You should also be aware that if you use a BootP server located on a different physical subnet, the router between the Concentrator and the BootP server must be configured as a DHCP Relay Agent; see your router's documentation for instructions on how to do this.

2. Make sure the TFTP server is up and running.

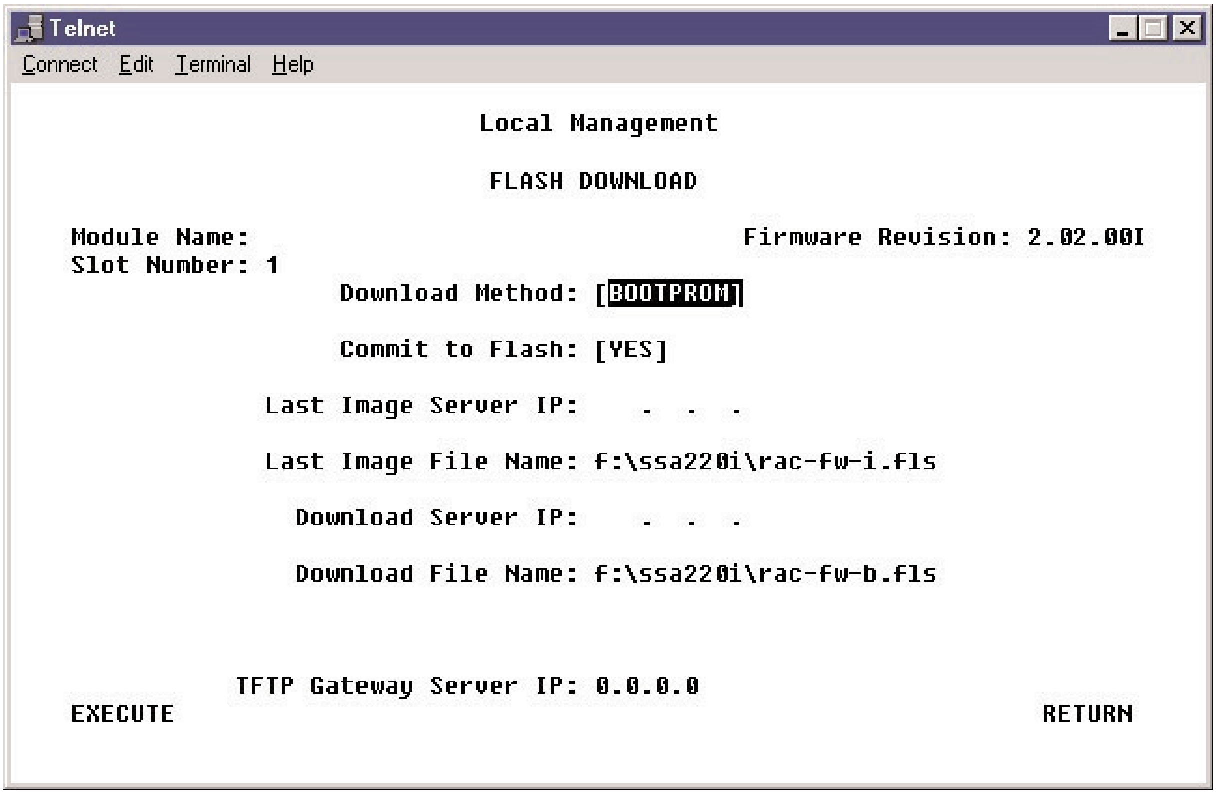
3. If you haven't done so already, download the archive file that contains the latest version of the Concentrator's firmware. This should be on the Black Box Web site; if you can't find it, call Black Box Tech Support.

4. Copy the firmware-upgrade archive file onto the TFTP server. If this file is zipped, unzip it; if it's a self-extracting executable (that is, if it has a ".EXE" file extension), run it to extract the firmware file(s) it contains. Make sure that all of the unzipped/extracted files are in the same folder or directory.

5. Access the Concentrator's Local Management utility. You may do so locally through the local console connection or remotely using Telnet.

6. Select the Module Configuration from the utility's Module Menu.

7. Select Flash Download from the Module Configuration menu. A screen like this will appear:



```
                         Local Management

                          FLASH DOWNLOAD

Module Name:                                Firmware Revision: 2.02.00I
Slot Number: 1
                  Download Method: [BOOTPROM]

                  Commit to Flash: [YES]

              Last Image Server IP:    .  .  .

              Last Image File Name: f:\ssa220i\rac-fw-i.fls

                Download Server IP:    .  .  .

                Download File Name: f:\ssa220i\rac-fw-b.fls


           TFTP Gateway Server IP: 0.0.0.0
EXECUTE                                                     RETURN
```

8. In the Download Server IP field, enter the IP address of the TFTP server to which the firmware upgrade has been copied.

9. In the Download File Name field, enter the full pathname of the upgrade file (upgrade files have ".FLS" extensions).

10. If the TFTP server is not on the same LAN as your Concentrator, you will need to provide its gateway IP address in the TFTP Gateway Server field.

11. After verifying the information you've provided, click Execute. The Concentrator will immediately reboot and perform an off-line upgrade. This will take about four minutes. (The exact time might vary due to differences in network speed.)

12. When the process is complete, use the Concentrator's Network Tools interface to examine the Concentrator's log. Verify the upgrade by checking log messages for upgrade-status information.

4.4 Network Tools

Network Tools (accessible from the Local Management utility's Module Menu) is command-line driven. It allows you to enter commands in order to gather information, change system parameters, and/or perform diagnostic procedures. For a listing of all of its available commands, type "help" at its command prompt, or refer to the "LRA3000 Console Commands" section in the Concentrator's online documentation.

One of the most important uses of the Network Tools commands is to configure the Remote Access Concentrator to interoperate properly with your ISDN line. If you haven't done so already, get the vital specifications for your line from your ISDN service provider; see **Section 3.2**. If your line's specs are different from the default ones listed in Table 4-3 below, use the Network Tools commands listed in the table to configure your Concentrator for the line. You *must* make any necessary changes to these settings *before* plugging the Concentrator's WAN cable into the WAN line.

Table 4-3. Line Specifications and Their Network Tools Commands

Line Specification	T1 Default Value	E1 Default Value	Corresponding Network Tools Command
Encoding	B8ZS	HDB3	`wanl1p linecode*`
Framing	ESF	E1-CRC	`wanl1p linetype*`
Line Build Out (T1 only)	0.0dB loss (long haul)	N/A†	`wanl1p linebuildout*`
Switch Type	NI-2	ETSI	`isdn switchtype`

*It is easy to misread the "wanl1p" command. Spelled out in uppercase, it would read "WANL1P".

†Line Build Out does not apply to the E1 interface. The E1 network is preconfigured to operate with 120 ohm termination and line impedance.

Here's an example of using these commands:

To adjust the switch-type value from the T1 default of NI-2 to 5ESS, enter the command:

```
isdn switchtype ESS5
```

Next, check the log to verify system integrity. Issue the command:

```
log start
```

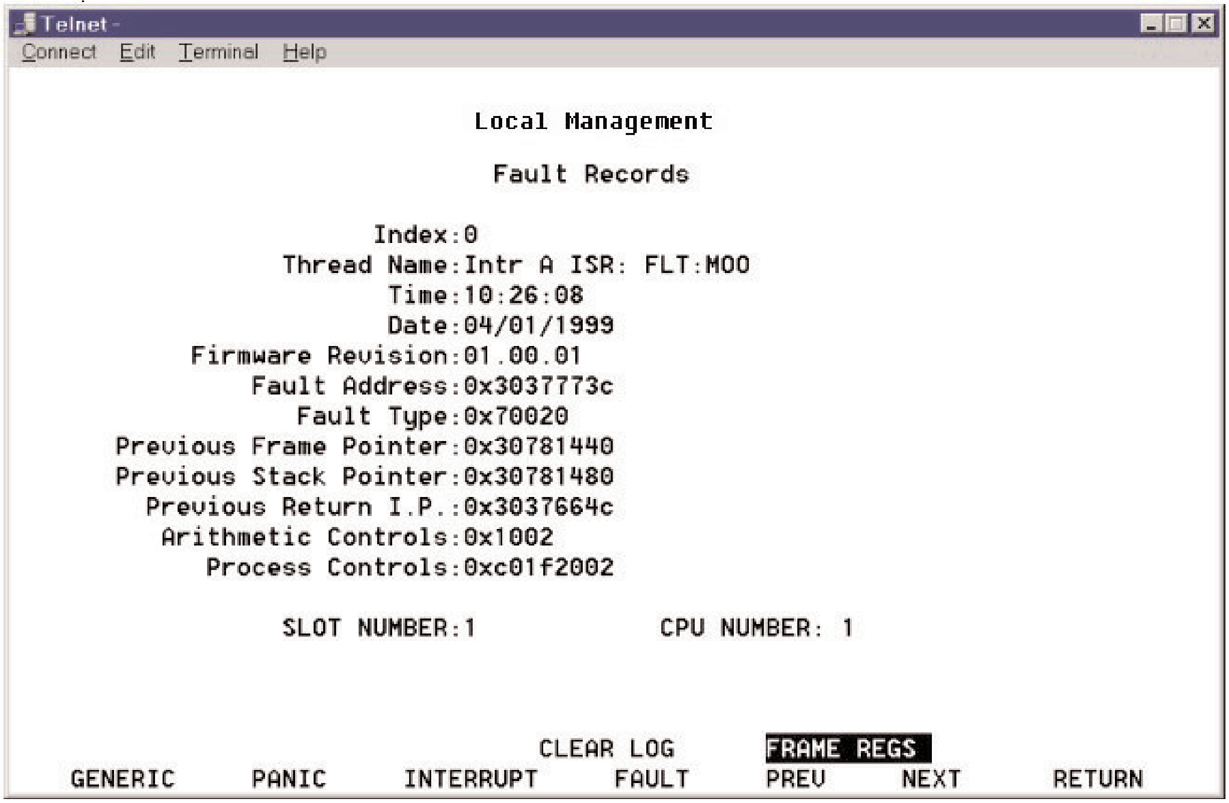
The log should contain at least two messages stating that Layer 1 is OK and the data link is OK.

4.5 Fault Records

You can review the Remote Access Concentrator's regular log messages by typing in the `log start` command at the Local Management utility's Network Tools command prompt; see **Section 4.4**. These messages might refer you to the Fault Records log for additional information. To access the Fault Records log, select Fault Records from the Local Management utility's Module Menu. Under normal Concentrator operating conditions, the Fault Records screen will display a message stating:

```
No Records Stored. NO ENTRIES ARE CONTAINED IN THE MESSAGE QUEUE.
```

If problems exist, however, the No Records message may be replaced with a screen display like this:

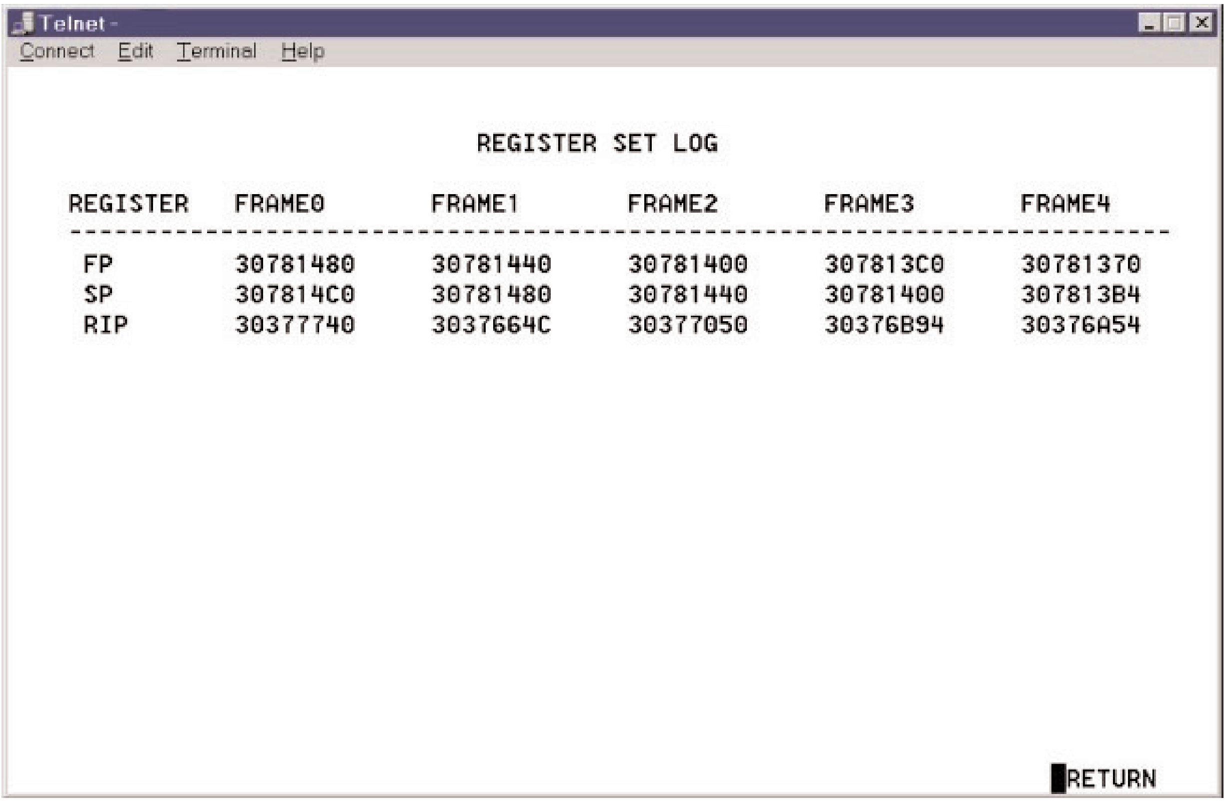


```
                        Local Management

                         Fault Records

                   Index:0
             Thread Name:Intr A ISR: FLT:MOO
                    Time:10:26:08
                    Date:04/01/1999
       Firmware Revision:01.00.01
           Fault Address:0x3037773c
              Fault Type:0x70020
  Previous Frame Pointer:0x30781440
  Previous Stack Pointer:0x30781480
    Previous Return I.P.:0x3037664c
     Arithmetic Controls:0x1002
        Process Controls:0xc01f2002

             SLOT NUMBER:1            CPU NUMBER: 1
```

There are several things to note about this screen:

- Each fault record is identified by an index number. In our example, the index number is zero (Index: 0).
- The latest fault is always displayed when this screen is initially accessed. To view previous fault records, select the PREV screen option; to move forward in the Fault Records log, select the NEXT screen option. You can also display the fault records by type (GENERIC, PANIC, and INTERRUPT screen options).

- Each fault record has a corresponding set of frame registers. Display these registers by selecting the FRAME REGS screen option. A screen like this will appear:



```
                          REGISTER SET LOG

 REGISTER   FRAME0       FRAME1       FRAME2       FRAME3       FRAME4
-------------------------------------------------------------------------
  FP        30781480     30781440     30781400     307813C0     30781370
  SP        307814C0     30781480     30781440     30781400     307813B4
  RIP       30377740     3037664C     30377050     30376B94     30376A54









                                                                RETURN
```

When problems arise with the Concentrator, take these steps:

1. Get screen captures of both the main screen (Fault Records) and the Frame Logs (Register Set Log) for each entry.
2. Get screen captures of the results of the initial log-in screen and `inv` command output.
3. Forward this information to Black Box Tech Support.

When you no longer need the current set of Fault Records, use the CLEAR LOG screen option to empty the log.

4.6 Integrating the Concentrator Into Your Network

There are special configuration considerations you need to keep in mind if you want to integrate the Remote Access Concentrator into a network containing routers.

First, you should disable outbound authentication on routers that connect to a Concentrator. This is because leaving outbound authentication enabled on routers that connect to the Concentrator creates a security gap. Someone could “assume the identity” of the Concentrator by using information captured during outbound authentication. (This is not a concern with PCs and other types of devices that use Windows Dialup to connect to the Concentrator, because—unlike routers—they don’t request the Concentrator’s authentication information for outbound communication.)

For instructions on, and illustrated examples of, specific applications:

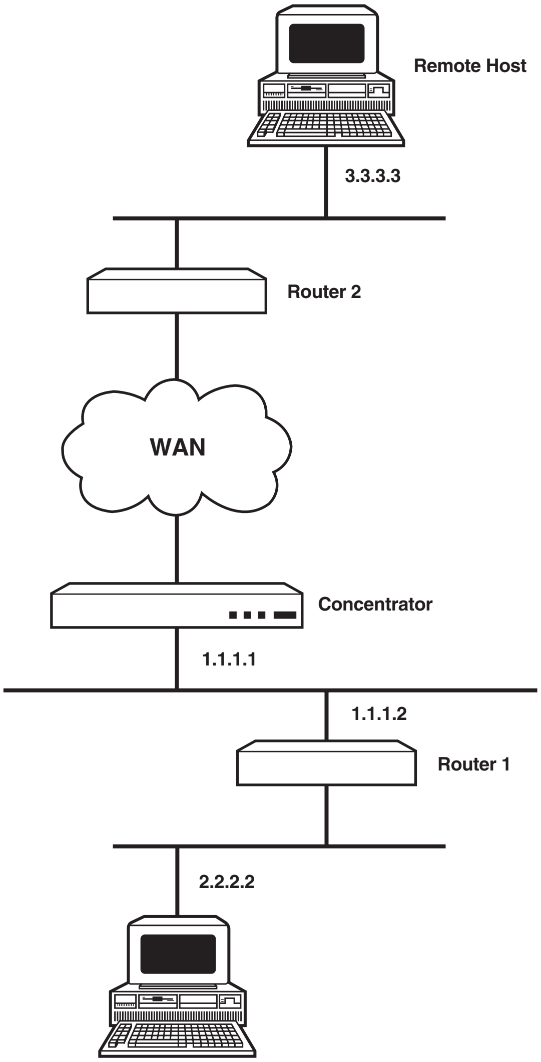
- Refer to **Section 4.6.1** for instructions on using static routes for connecting to subnets reachable through WAN devices.
- Refer to **Section 4.6.2** for instructions on integrating the Concentrator into a standard IP network.
- Refer to **Section 4.6.3** for instructions on integrating the Concentrator into an IP network in which the Concentrator is the gateway to the Internet.
- Refer to **Section 4.6.4** for instructions on integrating the Concentrator into an IP network with multiple LAN subnets.

4.6.1 Using Static Routes to Reach Subnets Through WAN Devices

Some remote devices connecting to the Remote Access Concentrator may actually be routers and not simply dial-up clients. These routers across the WAN are added to either RADIUS or CSM as remote devices. If the routers have one or more subnets reachable behind them, static routes must be configured to those subnets. In the example network shown below, you would have to configure a static route to allow the Concentrator to reach the 3.3.3.x subnet. Assuming that you're using CSM, configure the static route in CSM under Router 2's IP information. Note that this static route does not include a next hop because CSM's static routes assume that the remote device *is* the next hop.

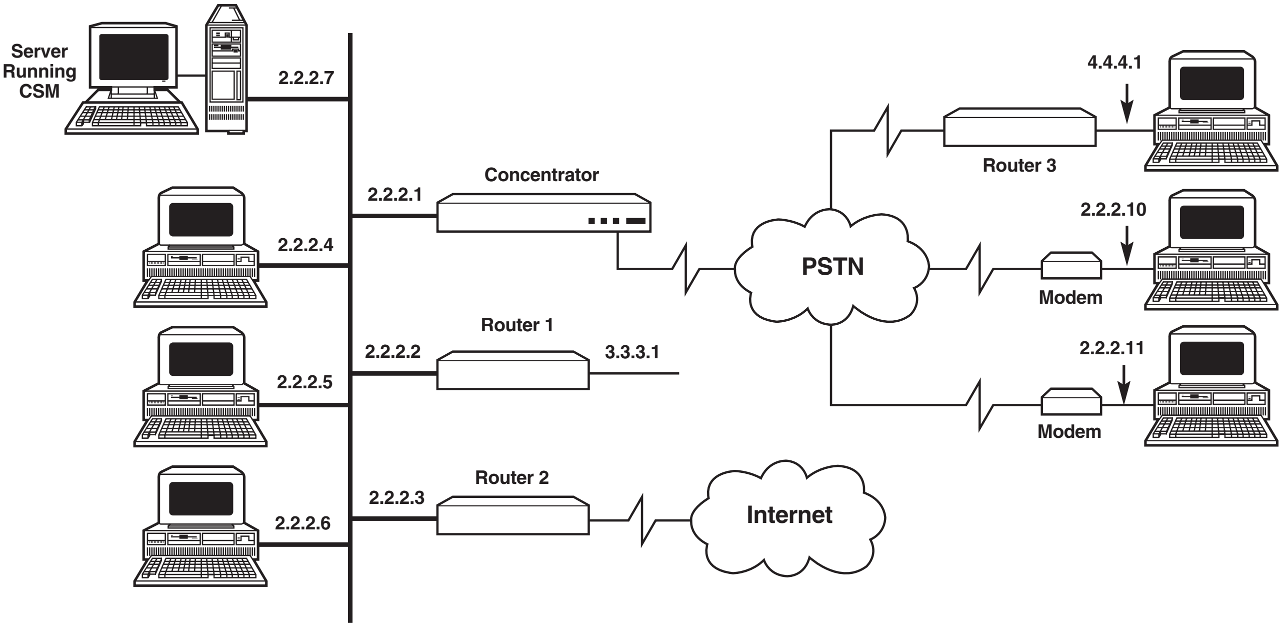
The Concentrator advertises routes locally, so unless Router 1 does not support RIP or has RIP disabled, no static routes should be needed for Router 1 to reach the 3.3.3.x subnet.

Any routers across the WAN from the Concentrator will need static routes to any subnets on the other side of the WAN. For example, Router 2 would need static routes to the 1.1.1.x subnet and the 2.2.2.x subnet, with the Concentrator designated as the Next Hop for both static routes.



4.6.2 Integrating the Concentrator Into a Standard IP Network

The illustration below shows how to integrate your Remote Access Concentrator into a standard IP network. Refer to this example as you set up your network, substituting your network's specifics where applicable.



Below we describe the configuration needed for connectivity between devices. (In our example, the "authentication database" and "authentication application" can be either CSM or RADIUS.)

Remote host 2.2.2.10 to local host 2.2.2.4:

Configure the remote host as a device in the authentication database. The device may be configured to have a specific IP address, or an IP address from one of the authentication application's IP-address pools.

Remote host 2.2.2.10 to device behind local router 3.3.3.1:

1. Configure the remote host as a device in the authentication database.
2. Enable RIP on the Concentrator and on Router 1 on the 2.2.2.x interface.

Remote host 2.2.2.10 to Internet through locally attached router:

1. Configure the remote host as a device in the authentication database.
2. Enable RIP on the Concentrator and on Router 2's 2.2.2.x interface. Router 2 should have a default route to the Internet that it advertises to the Concentrator.

Remote host 2.2.2.10 to remote host 2.2.2.11:

Configure both remote hosts as devices in the authentication database.

Remote host 2.2.2.10 to device 4.4.4.1 behind remote router:

1. Configure remote host 2.2.2.10 as a device in the authentication database.
2. Configure Router 3 as a device in the authentication database.
3. Configure a static route to subnet 4.4.4.x through Router 3 in the authentication database.
4. Configure Router 3 with a WAN Unnumbered interface to the Concentrator.
5. On Router 3, configure a static route to the 2.2.2.x subnet with the Concentrator listed as the next hop device.

Device 4.4.4.1 behind remote router to local host 2.2.2.4:

1. Configure Router 3 as a device in the authentication database.
2. Configure a static route to subnet 4.4.4.x through Router 3 in the authentication database.
3. Configure Router 3 with a WAN Unnumbered interface to the Concentrator.
4. On Router 3, configure a static route to the 2.2.2.x subnet with the Concentrator listed as the next hop device.

Device 4.4.4.1 behind remote router to device 3.3.3.1 behind local router:

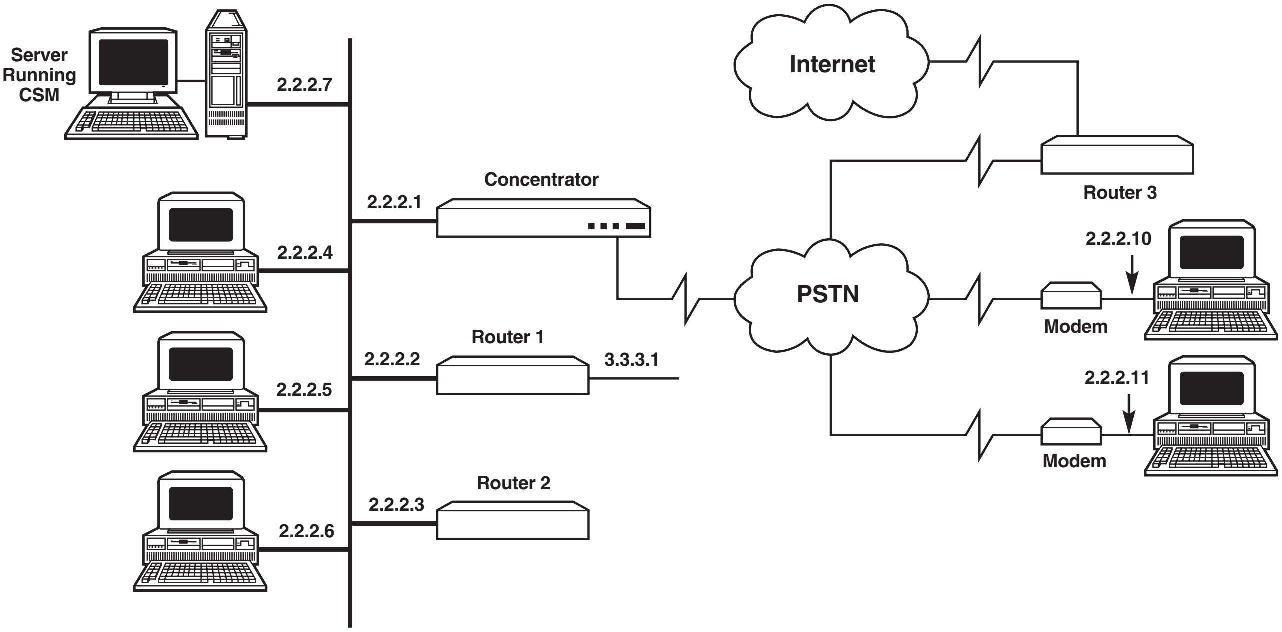
1. Configure Router 3 as a device in the authentication database.
2. Configure a static route to subnet 4.4.4.x through Router 3 in the authentication database.
3. Configure Router 3 with a WAN Unnumbered interface to the Concentrator.
4. On Router 3, configure a static route to the 3.3.3.x subnet with the Concentrator listed as the next hop device.
5. Configure Router 1 and the Concentrator to RIP on the 2.2.2.x subnet.

Device 4.4.4.1 behind remote router to Internet through locally attached router:

1. Configure Router 3 as a device in the authentication database.
2. Configure a static route to subnet 4.4.4.x through Router 3 in the authentication database.
3. Configure Router 3 with a WAN Unnumbered interface to the Concentrator.
4. On Router 3, configure the default route with the Concentrator listed as the next hop device.
5. Configure Router 2 and the Concentrator to RIP to each other. Router 2 should advertise a default route to the Internet.

4.6.3 Integrating the Concentrator into an IP Network as an Internet Gateway

The illustration below shows how to integrate your Remote Access Concentrator into an IP network in which the Concentrator is configured as a gateway to the Internet. Refer to this example as you set up your network, substituting your network's specifics where applicable.



Below we describe the configuration needed for connectivity between devices. (In our example, the "authentication database" can be either CSM or RADIUS.)

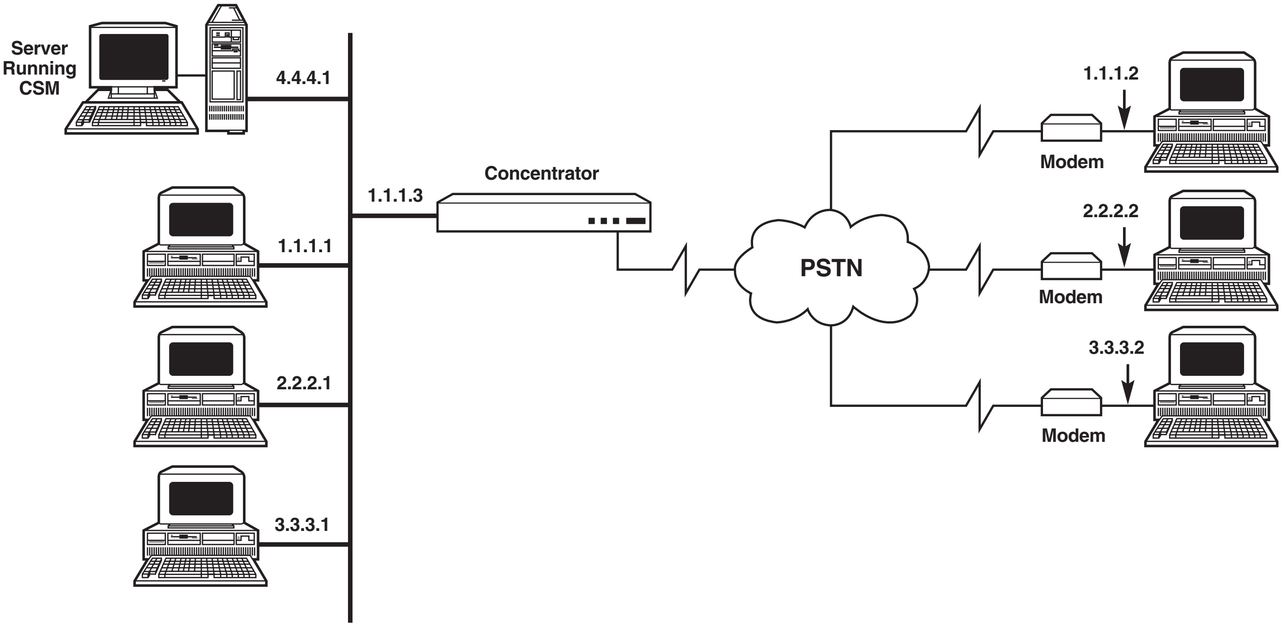
Remote Host 2.2.2.10 to the Internet through Router 3

1. Configure Router 3 as a device in the authentication database.
2. Configure a static route to subnet 0.0.0.0 through Router 3 in the authentication database. This will act as the default route for the Concentrator when Router 3 is connected.
3. Configure Router 3 with a WAN Unnumbered interface to the Concentrator.
4. On Router 3, configure a static route to the 2.2.2.x subnet with the Concentrator listed as the next hop device.
5. Configure remote host 2.2.2.10 as a device in the authentication database.
6. Either configure the Concentrator to RIP on the LAN interface or configure static LAN routes.

If a device such as 3.3.3.1 needs access to the Internet, you'll need to either configure the Concentrator to RIP on the LAN interface or configure static LAN routes.

4.6.4 Integrating the Concentrator Into an IP Network with Multiple Subnets

The illustration below shows how to integrate your Remote Access Concentrator into an IP network with multiple LAN subnets. Refer to this example as you set up your network, substituting your network's specifics where applicable.



Below we describe the configuration needed for connectivity between devices. (In our example, the "authentication database" can be either CSM or RADIUS.)

1. Configure the Concentrator with an IP address of 1.1.1.3 and a subnet mask of 255.0.0.0.
2. Configure remote hosts 1.1.1.2, 2.2.2.2, and 3.3.3.2 as devices in the authentication database.
3. Configure a static LAN route with a destination IP address of 2.0.0.0, a subnet mask of 255.0.0.0, a next hop address of 1.1.1.3, and a metric of 0.
4. Configure a static LAN route with a destination IP address of 3.0.0.0, a subnet mask of 255.0.0.0, a next hop address of 1.1.1.3, and a metric of 0.

The Concentrator will ARP on the LAN for all devices on the 2.0.0.0 and 3.0.0.0 subnets.

5. Basic CSM

This chapter is intended as a brief guide to some important functions of the Remote Access Concentrator's Connection Services Manager (CSM) software (sold separately as product code LRA300SW). (If you aren't using CSM, this chapter is irrelevant.) For much more complete information about CSM, see its HTML documentation.

For a very basic overview of CSM installation, see **Section 5.1**. For highlights of CSM configuration, see **Section 5.2**. And for how to use CSM to upgrade the Concentrator's firmware, see **Section 5.3**. Keep in mind that, for all of these functions, CSM's HTML documentation will provide more information.

5.1 Overview of Installing CSM

Connection Services Manager (CSM) is an authentication application and database specifically designed for use with the Remote Access Concentrator. To install it, you'll need to do these things:

- Install Microsoft® SQL Server software.
- *If you're using Windows® 95:* Install DCOM95. (The function of this software is already built into Windows 98, 2000, and NT.)
- Set up the ODBC driver.
- Install the CSM software.
- Install the CSM database.
- *If you're using Windows NT® 4.0 or higher:* Install the NDIS driver.

If the computer that you install CSM on isn't on the same subnet as the Concentrator, you'll need to either define a default LAN route or a static LAN route to the CSM from the Concentrator and vice versa. To define default LAN routes and static routes for the Concentrator, see **Sections 4.3.1.B** and **4.3.1.C** respectively. To define these in CSM, issue a "route" command at the Microsoft command prompt; see the CSM's documentation.

For full details about CSM installation—and all other aspects of using CSM—refer to CSM's HTML documentation.

5.2 CSM Configuration

To configure CSM, these prerequisites need to be in place:

1. The CSM software should be properly installed and running.
2. Make sure that these critical authentication values for the Concentrator have been configured in the Concentrator's Local Management utility (see **Sections 4.3.1.A**, **4.3.3**, and **4.3.7**) and that you set them to match in CSM:
   - The Concentrator's IP address, name, and secret.
   - The CSM secret.

   These values should be readily available if you recorded them on a copy of the Concentrator's Worksheet; see **Section 4.1**.
3. Determine whether or not you will use the Concentrator to initiate calls:
   - If the Concentrator *will* initiate calls, you must assign permanent IP addresses to all remote devices receiving calls.
   - If the Concentrator does *not* need to initiate calls, you may use an IP-address pool for remote devices.

When these things are ready/decided, you can configure CSM for your application. Full configuration information is in CSM's HTML documentation, but the basic CSM-configuration elements consist of:

- Establishing IP-pool information (optional); see **Section 5.2.1**.
- Setting up CSM to work with the Access Server (that is, the Concentrator); see **Section 5.2.2**.
- Setting up CSM to work with your remote devices; see **Section 5.2.3**.

5.2.1 Establishing an IP-Address Pool

To simplify remote-device management, consider using an IP-address pool to dynamically assign IP addresses to remote devices as they connect to the Remote Access Concentrator. In order to use an IP address pool, you must first determine whether or not the Concentrator needs to initiate calls.

- If the Concentrator does not need to initiate calls, establish an IP-address pool rather than assign permanent IP addresses to all remote devices. Assign as many IP addresses as the number of available ISDN connections. When a remote device calls in, it will be assigned one of the IP addresses available in the pool.
- If the Concentrator does need to initiate calls, you cannot use an IP pool. You'll need to provide permanent IP addresses for all remote devices instead. Skip ahead to **Section 5.2.2**.

To establish a pool in CSM, take these steps:

1. From the CSM Connection Manager, select Configure on the menu bar.
2. Select IP Information.
3. Enter a unique user-defined IP Pool Name.
4. Enter a Start IP Address. The Start IP Address field designates the beginning of a range of IP addresses used by this "Access Server" (the Concentrator). The Concentrator, in turn, will assign IP addresses from this range to any remote device not already having an IP address configured. Specify the address in dotted decimal notation: "XXX.XXX.XXX.XXX".
5. Enter an End IP Address. The End IP Address field designates the end of a range of IP addresses used by the Concentrator. Specify the address in dotted decimal notation: "XXX.XXX.XXX.XXX". The addresses should be limited to the same subnet, and the number of addresses should not exceed the number of available ISDN connections.
6. Click "Create New Pool".
7. Click "Close".

Refer to CSM's HTML User Documentation if you need more detailed instructions.

5.2.2 Setting Up the Concentrator as an Access Server

Take these steps to configure CSM to recognize the Concentrator as its Access Server:

1. From the CSM Connection Manager, select Configure on the menu bar.
2. Select Access Servers.
3. Select Add. This will place you in the Properties window; in the following steps, you will set options here to add the Concentrator as an Access Server for CSM.
4. Under Name, provide the unique name you've established for the Concentrator.
5. Provide the IP address you've established for the Concentrator. Specify it in dotted decimal notation. This must be the same IP address you've configured through the Concentrator's Local Management utility; see **Sections 4.3.1.A** and **4.3.7**.
6. In the Access Server Type field, select "LRA3000".
7. Provide authentication information: Supply both a CSM Secret—which applies to CSM only—and a System Secret unique to the Concentrator. These values must be the same as those you've configured through the Concentrator's Local Management utility; see **Section 4.3.3**.
8. Select the Access tab and change these settings as necessary or desired:

   If you plan to use an IP address pool, provide IP Pool information here. Under Default IP Pool, select the IP pool name. If you have established Groups, select a group name.

   If you plan to assign permanent IP addresses to remote devices and to configure the Concentrator for calling out, provide channel information here. You must specify the total number of ISDN or Digital Modem channels available. Currently, these values are "23" for ISDN and "24" for Digital Modem.

   The Priority Devices and Service Management selections are optional.
9. Click "Add".

Refer to CSM's HTML User Documentation if you need more detailed instructions.

5.2.3 Setting Up CSM for Your Remote Devices

To configure CSM to recognize your remote devices, these prerequisites need to be in place:

1. The Concentrator should be properly installed and configured through its Local Management utility.
2. The CSM software should be properly installed and configured to recognize the Concentrator (see **Section 5.2.2**).
3. The remote devices should be properly installed and configured, and make sure that their configuration settings match the settings for them in CSM:
   - The names of the remote devices that will access the Concentrator.
   - The authentication information (secret and/or password) for these devices.
   - An IP-pool name and a range of IP addresses for these remote devices, or permanent addresses for them if you can't use an IP-address pool.
   - If you've configured the Concentrator for calling out and/or callback, phone numbers for these devices.

   These values should be readily available if you recorded them on a copy of the Concentrator's Worksheet; see **Section 4.1**.

Take these steps to perform remote-device configuration in CSM:

1. From the CSM Connection Manager, select Configure on the menu bar.
2. Select Devices.
3. Select Add to add a device.
4. Under the Address tab, specify a name for the remote device.
5. Under the Protocols tab:
   a. enable IP;
   b. provide a permanent IP address, or check the Dynamic Address Assignment box; and
   c. if you have selected Dynamic Address Assignment, select the IP pool you created from the pull-down list.
6. Under the Access tab (Authentication):
   a. select PPP as Layer 2 Protocol;
   b. enable authentication; and
   c. enter a PAP Password and/or CHAP Secret (enter both if you are not sure of the type of authentication the Concentrator uses).
7. Press Add to add the device:
   - If you plan to call out from the Concentrator to a remote device, continue with the remaining steps.
   - If you do *not* plan to call out from the Concentrator, the configuration process is complete.

8. Select the Telephone tab:
   - Specify whether the connection is ISDN or Digital Modem.
   - Enter the telephone number of the remote device.

   Two things to be aware of:
   - You cannot call out from the Concentrator if you plan to use IP address pooling for this device.
   - You may configure multiple telephone numbers for a remote device; the Concentrator will call these numbers in the order they were configured.
9. Return to the Protocols tab and enable “Callable.” (You may check the Callable box only after you’ve provided the telephone number for the device in step 8.)
10. Click “Update”.

Refer to the CSM User Documentation if you need more detailed instructions regarding adding devices to the CSM configuration.

5.3 Upgrading the Concentrator's Firmware Through CSM

There are several methods available for upgrading your Remote Access Concentrator's firmware. The first time you do so—and each subsequent time you upgrade a single Concentrator—you'll probably want to use the Concentrator's Local Management utility as described in **Section 4.3.7**. If you're using CSM in a multiple-Concentrator system, however, it will probably be easier to use the methods available through CSM, described in this section, to simultaneously upgrade your Concentrators.

To use CSM to upgrade the Concentrator's firmware, the Concentrator must be configured, running, and able to communicate with the CSM machine. If it is, there are two main ways to upgrade the firmware using CSM:

1. **With a TFTP server.** This upgrade method requires the least amount of configuration and should be used under normal circumstances—although, to protect against the rare occurrence of the Concentrator going down, you may want to leave a TFTP/BootP server running in the background (see #2 below) for complete reliability. This method is described in **Section 5.3.1**.
2. **With a TFTP/BootP server.** This upgrade method requires more configuration, and is needed only in unusual circumstances. An example of such a circumstance would be if your site has an unreliable power source that causes upgrade files to become corrupted by interrupting the file-transfer process. Use a TFTP/BootP server in these kinds of situations to do a reliable upgrade: If something happens to interrupt the firmware-transfer process, the process restarts repeatedly until the upgrade is successful. This method is described in **Section 5.3.2**.

5.3.1 Using a TFTP Server

If you have some type of TFTP-server software installed, take these steps to use a TFTP server and CSM to upgrade Concentrator firmware:

1. Check your TFTP-server setup. The TFTP server must be “available” to the Concentrator, meaning it must either *be* on the same LAN as the Concentrator, or *appear to be* on the same LAN. For a more complete explanation, see **Section 4.3.8**.

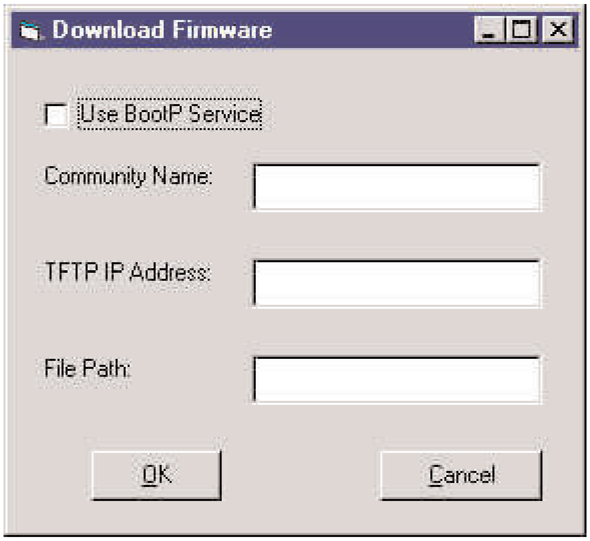
2. Make sure the TFTP server is up and running.

3. If you haven’t done so already, download the archive file that contains the latest version of the Concentrator’s firmware. This should be on the Black Box Web site, **www.blackbox.com**; if you can’t find it, call Black Box Tech Support.

4. Copy the firmware-upgrade archive file onto the TFTP server. If this file is zipped, unzip it; if it’s a self-extracting executable (that is, if it has a “.EXE” file extension), run it to extract the firmware file(s) it contains. Make sure that all of the unzipped/extracted files are in the same folder or directory.

5. On the CSM Connection Manager, click the Configure menu, then select Access Server.

6. Double-click the entry for the first Concentrator whose firmware you want to upgrade, then click the HW/FW tab. Click the “Upgrade firmware” button. You’ll see this dialog box:



7. Leave “Use BootP Service” disabled (checkbox empty).

8. Enter the SNMP Community Name assigned to the Concentrator you’re upgrading (see **Section 4.3.2**). If you haven’t assigned a community name to it, then enter “public”.

9. Enter the IP address of the TFTP server to which the firmware upgrade has been copied.

10. Enter the full pathname of the upgrade file (upgrade files have “.FLS” extensions).

11. Click “OK.”

12. You should see a message asking you to wait for the Concentrator to reboot. This does not necessarily mean that the download was successful. This only means that the SNMP parameters have been successfully set for a download. After waiting several minutes, click “Refresh”, then check the entry in the Currently Running box to see if the release number for the new firmware upgrade is displayed.

    If the new release is not what is currently running, check the information you entered for correctness. Make sure the new firmware upgrade was indeed copied successfully to the TFTP server.

13. Verify the process by checking the TFTP log to see if all files were downloaded properly. You may ignore invalid TID errors as long as the log indicates that five files were successfully downloaded.

5.3.2 Using a TFTP/BootP Server

NOTES

If you do not already have a TFTP/BootP server installed, freeware servers are available. We suggest you use a Web search engine to locate available freeware TFTP/BootP servers on the Internet.

For the upgrade to be successful, the device that the TFTP/BootP server is running on *must* have *only one* IP address.

Take these steps to use a TFTP/BootP server and CSM to upgrade Concentrator firmware:

1. Check your TFTP/BootP-server setup. The TFTP server must be "available" to the Concentrator, meaning it must either *be* on the same LAN as the Concentrator, or *appear to be* on the same LAN. For a more complete explanation, see **Section 4.3.8**.

2. Make sure the TFTP/BootP server is up and running.

3. If you haven't done so already, download the archive file that contains the latest version of the Concentrator's firmware. This should be on the Black Box Web site, **www.blackbox.com**; if you can't find it, call Black Box Tech Support.

4. Copy the firmware-upgrade archive file onto the TFTP/BootP server. If this file is zipped, unzip it; if it's a self-extracting executable (that is, if it has a ".EXE" file extension), run it to extract the firmware file(s) it contains. Make sure that all of the unzipped/extracted files are in the same folder or directory.

5. Get the Concentrator's MAC address from the General Configuration menu of the Concentrator's Local Management utility; see **Section 4.3.7**. You'll need this address in step 7.

For steps 6 through 9, you might want to consult the documentation for your TFTP/BootP server:

6. Start up the TFTP/BootP service.

7. Add an entry for each Concentrator using this BootP server for upgrades. For each entry you may need to enter the Concentrator's MAC address and IP address and the full pathname of the upgrade file (upgrade files have ".FLS" extensions). If an option is available to set the ARP, enable it. If the option is not available, you may want to manually configure each device into your ARP table.

8. If you can select a BootP reply method, select to receive "direct replies to BootP requests."

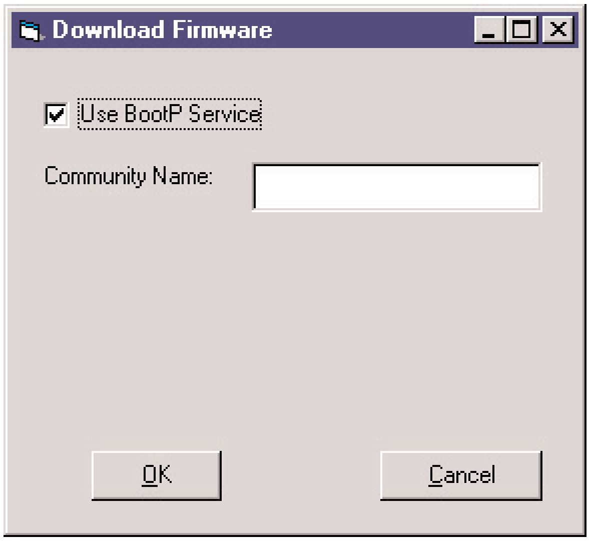
9. Continue with the following steps involving CSM; do *not* close the BootP service until the upgrade is complete.

Finish the process by triggering the upgrade with CSM (consult CSM's HTML documentation as necessary):

10. In the CSM Connection Manager, click the Configure menu, then select Access Server.

11. Double-click the entry for the first Concentrator whose firmware you want to upgrade, then click the HW/FW tab. Click the "Upgrade firmware" button.

12. Check the "Use BootP Service" checkbox to enable BootP, so that the dialog box looks like this:



☑ Use BootP Service

Community Name:

13. Enter the SNMP Community Name assigned to the Concentrator you're upgrading (see **Section 4.3.2**). If you haven't assigned a community name to it, then enter "public".

14. Click "OK".

15. You should see a message asking you to wait for the Concentrator to reboot. This does not necessarily mean that the download was successful. This only means that the SNMP parameters have been successfully set for a download. After waiting several minutes, click Refresh, then check the entry in the Currently Running box to see if the release number for the new firmware upgrade is displayed.

    If the new release is not what is currently running, check the information you entered for correctness. Make sure the new firmware upgrade was indeed copied successfully to the TFTP server.

16. Verify the process by checking the TFTP log to see if all files were downloaded properly. You may ignore invalid TID errors as long as the log indicates that five files were successfully downloaded.

17. After determining that the upgrade was successful, close the BootP Server in use.

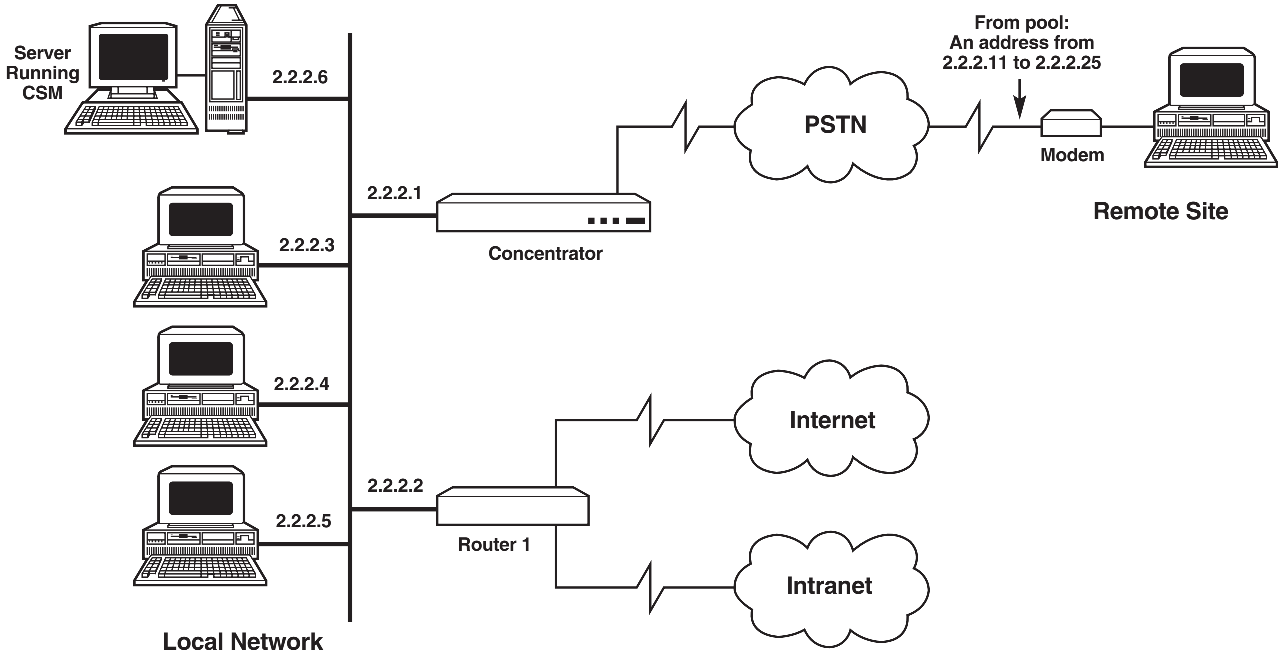
For subsequent upgrades—as long as you do not add any new Concentrator's to the network—you only need to copy the new firmware to the device running the BootP server, then trigger the upgrade through the Connection Manager. If you *do* add additional Concentrator's that you want to include in the BootP upgrade process, you also need to add those devices' information to the BootP server configuration.

6. Applications

There are several ways to establish a remote connection to the Remote Access Concentrator. This chapter describes these four remote-access applications, including illustrations and examples of configuration parameters:

- Windows Dial-up Networking and a modem (in **Section 6.1**)
- ISDN IP router running NAT (example includes switch-type and LBO changes; see **Section 6.2**)
- ISDN IP router not running NAT (in **Section 6.3**)
- ISDN bridge (in **Section 6.4**)

6.1 Windows 95/98/2000/NT Dial-up Networking



In this example, a single PC end station (that is, a "remote user") needs to connect to the local network using IP protocol through an analog modem or an ISDN terminal adapter (a "remote device"). This configuration is commonly used by telecommuters with a Windows Dial-up Networking client and is often referred to as IP Host mode. The remote device has no Layer 2 address. Rather, it is a Layer-3-only device connected to the end station typically through a serial port. The Remote Access Concentrator and the IP Host share a common IP address range; the Concentrator uses Layer 3 intelligence to determine what packets to send to the remote device. The Concentrator provides a proxy ARP to the local network for any remote devices connected this way.

Perhaps this is what the Configuration Worksheet for our example network looks like:

Configuration Option	Setting
IP address for Concentrator	2.2.2.1
Phone number for Concentrator	(555) 555-1234
RADIUS or CSM on same subnet as Concentrator?	Yes
Authentication:	
CSM secret	CSM_sec
Concentrator name	Conc_LRA3
Concentrator secret	LRA3_sec
Concentrator password	LRA3_pw
IP-address pool name	LRA3_ip_pool
Range of IP addresses in pool	2.2.2.11 through 2.2.2.25
Remote Device Name	Rem_PC
Secret/password for Device	secret1
Phone Number for Device	N/A

The Concentrator handles Windows 95, Windows 98, Windows 2000, or Windows NT Dial-Up Networking connections through its digital modems. This particular example illustrates Win95 Dial-Up Networking; however, the same setup principles apply to Windows 98, Windows 2000, and Windows NT as well. If you're using Windows 95 Dial-Up Networking, it must be release 1.2 or higher. For best results, we recommend using V.90-compatible modems with the latest modem drivers from your modem manufacturer.

This example requires proper setup of:

- The Concentrator (see **Section 6.1.1**),
- CSM (see **Section 6.1.2**), and
- Windows Dial-up Networking (see **Section 6.1.3**).

Standard Windows 95 client and modem configurations apply; standard PAP/CHAP/CLID authentication options are supported. The remote device uses an IP-address pool to obtain an IP address for its connection. The Concentrator is not configured to call out.

6.1.1 Concentrator Configuration for Windows Dial-up Networking

This section describes using the Remote Access Concentrator's Local Management utility to configure the Concentrator for the example Windows Dial-up application shown earlier in **Section 6.1**. Because we're using the Concentrator's default values for Line Build Out and switch type, configuration involves only the utility's Module Configuration menu, not Network Tools. Note that the Local Management utility doesn't support mice; use the keyboard's up- and down-arrows or its tab key to navigate through the utility's fields.

Here's what the procedure would be for our hypothetical network:

1. From Local Management utility's Module Menu, select Module Configuration; from the Module Configuration menu, first select Authentication Settings.
2. Provide the CSM Secret ("CSM_sec") for the CSM service.
3. Provide the Concentrator's System Name ("Conc_LRA3"), System Secret ("LRA3_sec"), and System Password ("LRA3_pw"). These values correspond to the values we will enter on the CSM.
4. Select Save, and then Return, to go back to the Module Configuration menu.
5. Next, select PPP Settings.
6. Provide primary and secondary DNS and NBNS addresses. This will allow the Concentrator to supply the Windows dial-up clients with DNS and NBNS addresses, so that the users of remote devices running Windows dial-up won't need to manually configure their DNS and NBNS server addresses.
7. Select Save, and then Return, to go back to the Module Configuration menu again.
8. Next, select General Configuration.
9. Provide date and time information.
10. Provide the Concentrator's host IP address (2.2.2.1) and subnet mask (255.0.0.0), which correspond to the values we'll enter on the CSM. We do not need to enter a default gateway, since the CSM is on the same subnet as the Concentrator.
11. Verify information, then press Save.

At this point, the Concentrator will automatically reboot.

6.1.2 CSM Configuration for Windows Dial-up Networking (CSM Only)

This section describes configuring the Connection Services Manager (CSM) software for the example Windows Dial-up application shown earlier in **Section 6.1**. This would include:

- Establishing a pool of IP addresses to be temporarily assigned to remote devices. The PC using Windows 95 dial-up networking will be one of these remote devices.
- Defining the Concentrator as an access server and establish authentication parameters. We will identify the IP-address pool we wish to use with the Concentrator.
- Identifying the remote PC (the one using Windows Dial-up Networking) as a remote device.

(If we were using RADIUS rather than CSM, the values we would need to set would be the same, but the procedures would be different—consult the RADIUS documentation.)

Here's what the procedure would be for our hypothetical network. To begin, we'd start up the CSM Connection Manager and make a connection (File/Connect). Then we'd proceed with the following steps:

1. From Configure on the CSM Connection Manager menu bar, select IP Information.
2. Enter the user-defined IP pool name ("LRA3_ip_pool").
3. Enter a Start IP Address of 2.2.2.11.
4. Enter an End IP Address of 2.2.2.25. Note that this range of addresses is limited to the same subnet, and that the number of addresses (15) does not exceed the number of available ISDN connections (23).
5. Click Create New Pool.
6. From Configure on the menu bar, select Access Servers.
7. Click Add to configure CSM for the Concentrator. This will place you in the Properties window:
   a. Under Name, enter "Conc_LRA3".
   b. Provide the Concentrator's IP address (2.2.2.1).
   c. In the Access Server Type field, select "LRA3000".
   d. Provide authentication information: the CSM Secret ("CSM_sec") and System Secret ("LRA3_sec"). These values correspond to the values we already entered on the Concentrator (see **Section 6.1.1**).
8. Select the Demand Access tab. Since we plan to use an IP address pool, select the IP Pool name of "LRA3_ip_pool" from the pull-down list. We do not need to change the Group field since we did not set up groups.
9. Click Add.
10. From Configure on the menu bar, select Devices.
11. Click Add to add the remote PC.
12. Under the Address tab, specify the device name of "Rem_PC".
13. Under the Protocols tab:
    a. Enable IP;
    b. Check the Dynamic Address Assignment box (since we will be using the IP-address pool for this device);
    c. Select "LRA3_ip_pool" from the pull-down box in the IP pool field.

14. Under the Access tab (Authentication):
    a. Select PPP as Layer 2 Protocol.
    b. Enable Authentication.
    c. Enter the CHAP secret (“secret1”).
15. Click Add to add the device.

6.1.3 Remote-Device Configuration for Windows Dial-up Networking

This section describes configuring the remote device (a PC, in this case) for the example Windows Dial-up application shown earlier in **Section 6.1**. This would include:

- Identifying the new connection;
- Defining the server type; and then
- Attempting to dial out.

These directions apply to Windows 95; we'd set the same values in Windows 98, Windows 2000, or Windows NT, but the menus and their options would be different.

Here's what the procedure would be for our hypothetical network, on the remote PC running Windows 95 software:

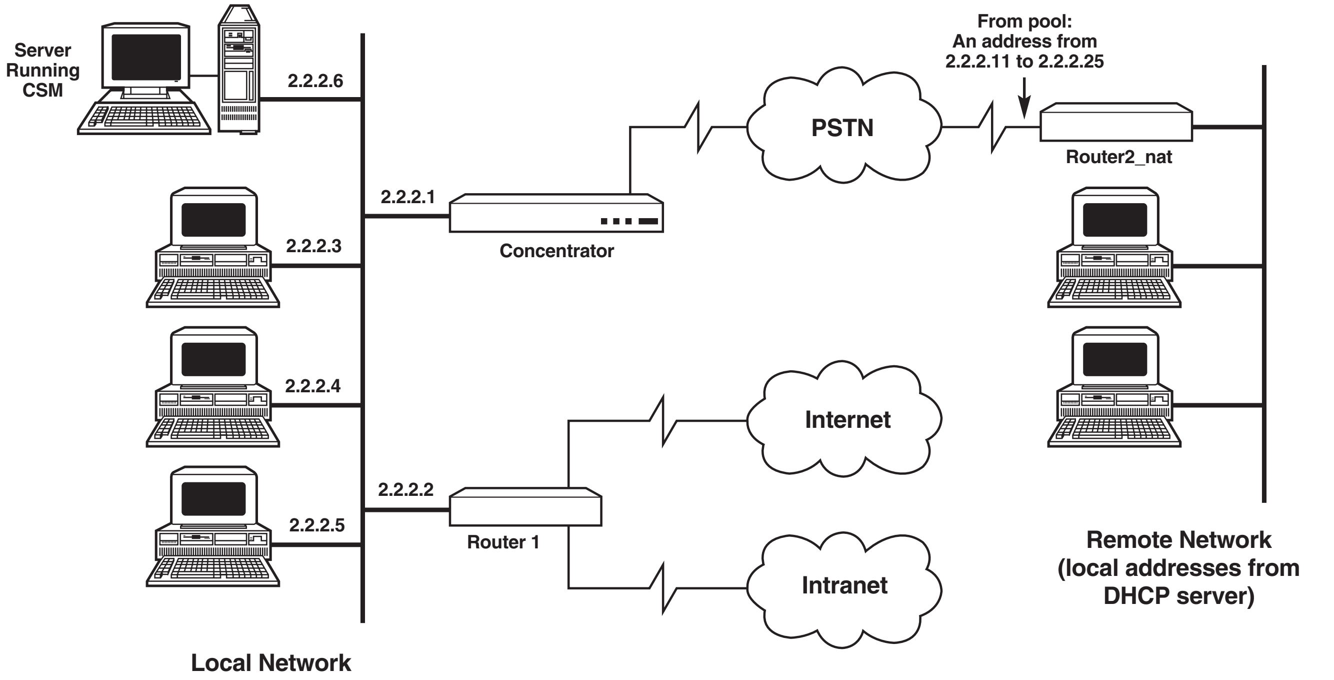
1. Click Start, select Programs, select Accessories, and then Dial-Up Networking. (You can get to the same location by clicking My Computer, then double clicking on Dial-Up Networking.)
2. Double-click Make New Connection: Provide the name of the Concentrator ("Conc_LRA3"), then select the modem type.
3. Click Configure. The following tabs are displayed:
   - Under the General tab, select (a) the COM port the modem is using and (b) the modem's maximum speed.
   - Under the Connection tab, in Connection Preferences, set Data Bits to 8, Parity to None, and Stop Bits to 1. (Port Settings and Advanced may remain at their default values.)
   - Also under the Connection tab, the Call Preferences may remain at their default values.
   - The Options tab should remain at its default values for PPP connections.
4. Click OK to accept these values and return you to the modem name/type screen. Click Next.
5. Provide the area code and phone number of the Concentrator's network (along with any other prefixes needed to obtain an external connection): If it were necessary to dial "9" to make an outbound call from the PC, we'd enter "9-1-555-555-1234" here. Also identify the country of the network. Click Next.
6. Confirm your choices. Click Finish to proceed, or Cancel to abort the new number shortcut.
7. After setting up a new number, a new dialing icon named "Conc_LRA3" is displayed under Dial-Up Networking. Select this item, click File, and then Properties.
8. Click Server Type. Select TCP/IP.
9. If you have not configured primary and secondary DNS or WINS (NBNS) addresses on the Concentrator (through PPP settings), you will need to manually enter them here. To do so:
   - Click TCP/IP Settings. Select "Server assigned IP address". Provide any additional DNS or WINS information provided by your administrator.
   - Click OK when you're finished.
10. Double-click your new dialing icon to bring up the "Connect To" screen.
11. Enter your user name and password. These values must correspond to the CSM values: name "Rem_PC", password "secret1".

12. *Optional:* If necessary, change the settings of any dialing properties for this connection by clicking the box labeled “Dialing Properties”.

13. Double-click “Connect”.

This should place the call.

6.2 ISDN IP Router Running NAT



In this example, multiple PC end stations on a remote subnet need to connect to the local network using an ISDN IP router. This example assumes Network Address Translation (NAT) is configured on the IP router. Note that, in many ways, this configuration behaves like an IP Host environment (see **Section 6.1**). NAT is an IP address-conversion feature managed by the remote router that allows one-to-many one or more end stations to share a single IP address to the Internet, thus reducing connection costs and address-management hassles. NAT effectively allows an entire subnet to connect to the Internet as a single remote user.

Perhaps this is what the Configuration Worksheet for our example network looks like:

Configuration Option	**Setting**
IP address for Concentrator	2.2.2.1
Phone number for Concentrator	(555) 555-1234
RADIUS or CSM on same subnet as Concentrator?	Yes
Authentication:	
CSM secret	CSM_sec
Concentrator name	Conc_LRA3
Concentrator secret	LRA3_sec
Concentrator password	LRA3_pw
IP-address pool name	LRA3_ip_pool
Range of IP addresses in pool	2.2.2.11 through 2.2.2.25
Switch type	5ESS
Line Build Out	–15.0 dB
Remote Device Name	Router2_nat
Secret/password for Device	secreta
Phone Number for Device	N/A

This example requires proper setup of:

- The Concentrator (see **Section 6.2.1**),
- CSM (see **Section 6.2.2**), and
- The IP Router ("Router2_nat"; see **Section 6.2.3**).

Standard PAP/CHAP/CLID authentication options are supported. The remote router ("Router2_nat") will use an IP address pool to obtain an IP address for its connection. The remote end stations will have "local" IP addresses (on the subnet) assigned by Router2's DHCP server. The Concentrator will not be configured to call out.

The Concentrator will use a switch type different than the default; it will be configured to use a 5ESS. In addition, the telephone company provided a decibel attenuation value of -15.0 dB when they installed the lines. This is different than the default Line Build Out value of 0.0 dB, so you will need to adjust this value as well. These adjustment will require Network Tools commands to be entered.

6.2.1 Concentrator Configuration for NAT

This section describes using the Remote Access Concentrator's Local Management utility to configure the Concentrator for the example NAT application shown earlier in **Section 6.2**. Because we're using values other than the Concentrator's defaults for Line Build Out and switch type, configuration involves both the utility's Module Configuration menu *and* its Network Tools interface. Note that the Local Management utility doesn't support mice; use the keyboard's up- and down-arrows or its tab key to navigate through the utility's fields.

Here's what the procedure would be for our hypothetical network:

1. From Local Management utility's Module Menu, select Network Tools. The Network Tools command prompt will appear.

2. To set the switch type from NI-2 (the Concentrator's default) to 5ESS, enter the command

   ```
   isdn switchtype ESS5
   ```

3. To set the Line Build Out value from 0.0 dB (the Concentrator's default) to -15.0 dB on both of the WAN (WIDE AREA) ports, enter the commands

   ```
   wan11p linebuildout -15.0dB 1
   wan11p linebuildout -15.0dB 2
   ```

   where "1" at the end of the first command represents the WIDE AREA 1 port and the "2" at the end of the second command represents the WIDE AREA 2 port. Both commands *must* be entered in order to make the change on both interfaces.

4. Because the Concentrator's defaults for the other line-information values are acceptable for this application, we can enter the `exit` command to return to the Module Menu.

5. From the Module Menu, select Module Configuration.

6. From the Module Configuration menu, first select Authentication Settings.

7. Provide the CSM Secret ("CSM_sec") for the CSM service.

8. Provide the Concentrator's System Name ("Conc_LRA3"), System Secret ("LRA3_sec"), and System Password ("LRA3_pw"). These values correspond to the values we will enter on the CSM.

9. Select Save, and then Return, to go back to the Module Configuration menu.

10. Next, select General Configuration.

11. Provide date and time information.

12. Provide the Concentrator's host IP address (2.2.2.1) and subnet mask (255.0.0.0), which correspond to the values we'll enter on the CSM. We do not need to enter a default gateway, since the CSM is on the same subnet as the Concentrator.

11. Verify information, then click Save.

At this point, the Concentrator will automatically reboot.

6.2.2 CSM Configuration for NAT (CSM Only)

This section describes configuring the Connection Services Manager (CSM) software for the example NAT application shown earlier in **Section 6.2**. This would include:

- Establishing a pool of IP addresses to be temporarily assigned to remote devices. The IP router using NAT will be one of these remote devices.
- Defining the Concentrator as an access server and establish authentication parameters. We will identify the IP-address pool we wish to use with the Concentrator.
- Identifying the remote router using NAT as a remote device.

(If we were using RADIUS rather than CSM, the values we would need to set would be the same, but the procedures would be different—consult the RADIUS documentation.)

Here's what the procedure would be for our hypothetical network. To begin, we'd start up the CSM Connection Manager and make a connection (File/Connect). Then we'd proceed with the following steps:

1. From Configure on the CSM Connection Manager menu bar, select IP Information.
2. Enter the user-defined IP pool name ("LRA3_ip_pool").
3. Enter a Start IP Address of 2.2.2.11.
4. Enter an End IP Address of 2.2.2.25. Note that this range of addresses is limited to the same subnet, and that the number of addresses (15) does not exceed the number of available ISDN connections (23).
5. Click Create New Pool.
6. From Configure on the menu bar, select Access Servers.
7. Click Add to configure CSM for the Concentrator. This will place you in the Properties window:
   a. Under Name, enter "Conc_LRA3".
   b. Provide the Concentrator's IP address of (2.2.2.1).
   c. In the Access Server Type field, select "LRA3000".
   d. Provide authentication information: the CSM Secret ("CSM_sec") and System Secret ("LRA3_sec"). These values correspond to the values we already entered on the Concentrator (see **Section 6.1.1**).
8. Select the Demand Access tab. Since we plan to use an IP address pool, select the IP Pool name of "LRA3_ip_pool" from the pull-down list. We do not need to change the Group field since we did not set up groups.
9. Click Add.
10. From Configure on the menu bar, select Devices.
11. Click Add to add the remote router.
12. Under the Address tab, specify the device name of "Router2_nat".
13. Under the Protocols tab:
    a. Enable IP;
    b. Check the Dynamic Address Assignment box (since we will be using the IP-address pool for this device);
    c. Select "LRA3_ip_pool" from the pull-down box in the IP pool field.

14. Under the Access tab (Authentication):
    a. Select PPP as Layer 2 Protocol.
    b. Enable Authentication.
    c. Enter the CHAP secret (“secret1”).
15. Click Add to add the device.

6.2.3 Remote-Router Configuration for NAT

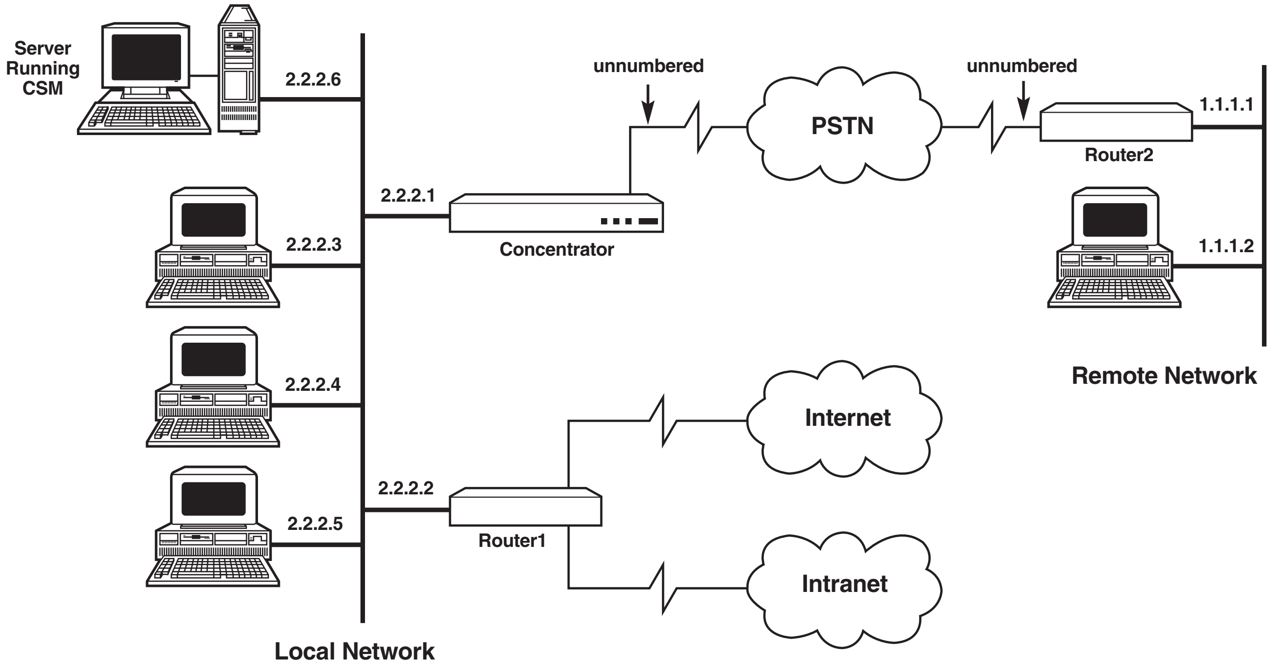
This section describes configuring the remote router for the example NAT application shown earlier in **Section 6.2**. This would include:

- Enabling IP routing on the router.
- Providing authentication information: Configure the router's name ("Router2_nat") and secret ("secreta"), which must match the remote-device configuration in CSM.
- Disabling outbound authentication. (Leaving outbound authentication enabled creates a security gap: Someone could "assume the identity" of the Concentrator by using information captured during outbound authentication.)
- Defining a remote connection to the Concentrator.

The last item—defining a remote connection—consists of these separate tasks:

- Adding a remote connection: Provide the Concentrator's name (Conc_LRA3) and password (LRA3_pw).
- Entering the Concentrator's phone number. Be sure to enter any necessary prefixes, such as "9" for external calls, or "1 + area code" for long-distance calls (9-1-555-5551234).
- Configuring a default route to the Concentrator (IP address 2.2.2.1, subnet mask 255.0.0.0).

6.3 Standard ISDN IP Router



In this example, a single PC end station on a remote subnet needs to connect to the local network using an ISDN IP router. The scenario assumes you will have fixed IP addresses assigned to the remote end station and the remote device (router). In this configuration, the Concentrator will have dial-out capabilities. DHCP relay and proxy are not supported.

Perhaps this is what the Configuration Worksheet for our example network looks like:

Configuration Option	Setting 1	Setting 2
IP address for Concentrator	2.2.2.1	
Phone number for Concentrator	(555) 555-1234	
RADIUS or CSM on same subnet as Concentrator?	Yes	
Authentication:		
CSM secret	CSM_sec	
Concentrator name	Conc_LRA3	
Concentrator secret	LRA3_sec	
Concentrator password	LRA3_pw	
Remote Device Name	Router1	Router2
Secret/password for Device	secret2	secret3
IP address for Device	2.2.2.2	1.1.1.1
Phone Number for Device	N/A	(888) 555-4321

This example requires proper setup of:

- The Concentrator (see **Section 6.3.1**),
- CSM (see **Section 6.3.2**), and
- The remote IP Router (“Router2”; see **Section 6.3.3**).

The Concentrator must have a static IP address. The remote router Router2 must have a static IP address and a static route configured to the Concentrator. Its default gateway must be set equal to Router1 (which is “local” to the Concentrator). The remote end station must have a static address. Its default gateway must be equal to Router2.

Standard PAP/CHAP/CLID authentication options are supported. The Concentrator will be configured to call out.

6.3.1 Concentrator Configuration for Standard IP

This section describes using the Remote Access Concentrator's Local Management utility to configure the Concentrator for the example standard IP application shown earlier in **Section 6.3**. Because we're using the Concentrator's default values for Line Build Out and switch type, configuration involves only the utility's Module Configuration menu, not Network Tools. Note that the Local Management utility doesn't support mice; use the keyboard's up- and down-arrows or its tab key to navigate through the utility's fields.

Here's what the procedure would be for our hypothetical network:

1. From the Module Menu, select Module Configuration.
2. From the Module Configuration menu, first select Authentication Settings.
3. Provide the CSM Secret ("CSM_sec") for the CSM service.
4. Provide the Concentrator's System Name ("Conc_LRA3"), System Secret ("LRA3_sec"), and System Password ("LRA3_pw"). These values correspond to the values we will enter on the CSM.
5. Select Save, and then Return, to go back to the Module Configuration menu.
6. Next, select General Configuration.
7. Provide date and time information.
8. Provide the Concentrator's host IP address (2.2.2.1) and subnet mask (255.0.0.0), which correspond to the values we'll enter on the CSM. We do not need to enter a default gateway, since the CSM is on the same subnet as the Concentrator.
9. Verify information, then click Save.

At this point, the Concentrator will automatically reboot.

6.3.2 CSM Configuration for Standard IP (CSM Only)

This section describes configuring the Connection Services Manager (CSM) software for the example NAT application shown earlier in **Section 6.3**. This would include:

- Defining the Concentrator as an access server and establish authentication parameters.
- Identifying the remote PC as a remote device and providing its authentication parameters and IP address.
- Identifying the remote router as a remote device and providing its authentication parameters, IP address, and phone number.

(If we were using RADIUS rather than CSM, the values we would need to set would be the same, but the procedures would be different—consult the RADIUS documentation.)

Here's what the procedure would be for our hypothetical network. To begin, we'd start up the CSM Connection Manager and make a connection (File/Connect). Then we'd proceed with the following steps:

1. From Configure on the CSM Connection Manager menu bar, select Access Servers.
2. Click Add to configure CSM for the Concentrator. This will place you in the Properties window:
   a. Under Name, enter "Conc_LRA3".
   b. Provide the Concentrator's IP address (2.2.2.1).
   c. In the Access Server Type field, select "LRA3000".
   d. Provide authentication information: the CSM Secret ("CSM_sec") and System Secret ("LRA3_sec"). These values correspond to the values we already entered on the Concentrator (see **Section 6.1.1**).
3. Select the Demand Access tab. Skip the IP Pool section, because we're assigning specific IP addresses to remote devices. Instead, provide channel information. In order to support the call-out feature, we must specify the total number of ISDN channels available. On the Concentrator, this value is "23".
4. Click Add.
5. From Configure on the menu bar, select Devices.
6. Click Add to add the remote router ("Router2").
7. Under the Address tab, specify the device name of "Router2".
8. Under the Protocols tab:
   a. Enable IP;
   b. Because this is an unnumbered interface, provide Router2's IP address as 0.0.0.0.
9. Click Add.
10. Continue with IP Protocols configuration:
    a. Click "Add Static Route".
    b. Provide the Destination Subnet of the Concentrator (1.0.0.0). The system calculates the subnet mask, which is 255.0.0.0.
    c. Provide the Metric value. This value corresponds to the number of routers we use to make this connection. In our example, this number is 2.

11. Under the Access tab (Authentication):
    a. Select PPP as Layer 2 Protocol.
    b. Enable Authentication.
    c. Enter the CHAP secret ("secret3").

12. Under the Telephone tab, specify ISDN as the Connect Type.

13. Provide Router2's telephone number: Click Add, and then enter the number (9-1-888-555-4321).

14. Return to the Protocols tab and enable Callable. (We may check the Callable box only after we've provided the telephone number for the device in the previous step.)

15. Click Update, and then Close to exit.

6.3.3 Remote-Router Configuration for Standard IP

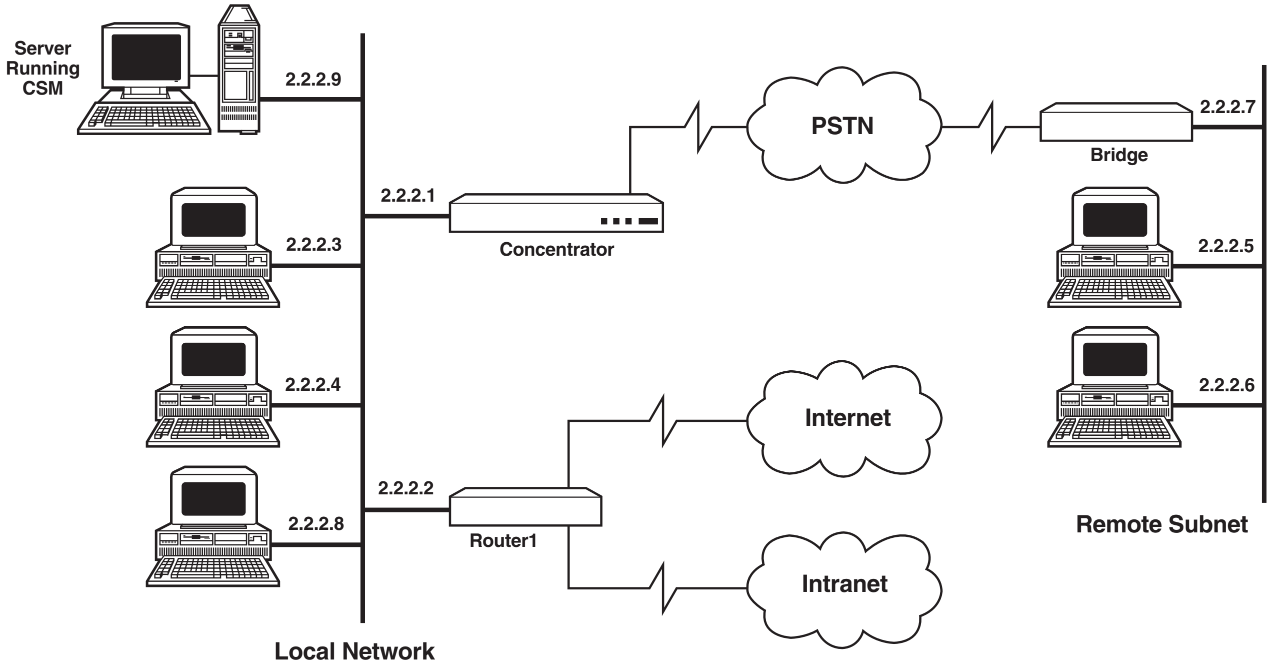
This section describes configuring the remote router for the example standard IP application shown earlier in **Section 6.3**. This would include:

- Enabling IP routing on the router.
- Providing authentication information: Configure the router's name ("Router2") and secret ("secret3"), which must match the remote-device configuration in CSM.
- Disabling outbound authentication. (Leaving outbound authentication enabled creates a security gap: Someone could "assume the identity" of the Concentrator by using information captured during outbound authentication.)
- Defining a remote connection to the Concentrator.

The last item—defining a remote connection—consists of these separate tasks:

- Adding a remote connection: Provide the Concentrator's name (Conc_LRA3) and password (LRA3_pw).
- Entering the Concentrator's phone number. Be sure to enter any necessary prefixes, such as "9" for external calls, or "1 + area code" for long-distance calls (9-1-555-555-1234).
- Configuring a default route to the Concentrator (IP address 2.2.2.1, subnet mask 255.0.0.0).

6.4 ISDN Bridge



In this example, multiple PC end stations on a remote subnet need to connect to the local network using an ISDN bridge.

Perhaps this is what the Configuration Worksheet for our example network looks like:

Configuration Option	**Setting**
IP address for Concentrator	2.2.2.1
Phone number for Concentrator	(555) 555-1234
RADIUS or CSM on same subnet as Concentrator?	Yes
Authentication:	
CSM secret	CSM_sec
Concentrator name	Conc_LRA3
Concentrator secret	LRA3_sec
Concentrator password	LRA3_pw
Remote Device Name	RBridge
Secret/password for Device	secretbr
IP Address for Device	N/A
Phone Number for Device	N/A

This example requires proper setup of:

- The Concentrator (see **Section 6.4.1**),
- CSM (see **Section 6.4.2**), and
- The ISDN bridge. This part is very simple: Configure the device as a simple bridge and provide the Concentrator network’s phone number: (555) 555-1234.

Standard PAP/CHAP/CLID authentication options are supported. There is no IP address assignment. The Concentrator is not configured to call out (which is not supported anyway for this type of application).

6.4.1 Concentrator Configuration for ISDN Bridging

This section describes using the Remote Access Concentrator's Local Management utility to configure the Concentrator for the example ISDN-bridging application shown earlier in **Section 6.4**. Because we're using the Concentrator's default values for Line Build Out and switch type, configuration involves only the utility's Module Configuration menu, not Network Tools. Note that the Local Management utility doesn't support mice; use the keyboard's up- and down-arrows or its tab key to navigate through the utility's fields.

Here's what the procedure would be for our hypothetical network:

1. From the Module Menu, select Module Configuration.
2. From the Module Configuration menu, first select Authentication Settings.
3. Provide the CSM Secret ("CSM_sec") for the CSM service.
4. Provide the Concentrator's System Name ("Conc_LRA3"), System Secret ("LRA3_sec"), and System Password ("LRA3_pw"). These values correspond to the values we will enter on the CSM.
5. Select Save, and then Return, to go back to the Module Configuration menu.
6. Next, select General Configuration.
7. Provide date and time information.
8. Provide the Concentrator's host IP address (2.2.2.1) and subnet mask (255.0.0.0), which correspond to the values we'll enter on the CSM. We do not need to enter a default gateway, since the CSM is on the same subnet as the Concentrator.
9. Verify information, then click Save.

At this point, the Concentrator will automatically reboot.

6.4.2 CSM Configuration for ISDN Bridging (CSM Only)

This section describes configuring the Connection Services Manager (CSM) software for the example ISDN-bridging application shown earlier in **Section 6.4**. This would include:

- Defining the Concentrator as an access server and establish authentication parameters.
- Identifying the bridge as a remote device.

(If we were using RADIUS rather than CSM, the values we would need to set would be the same, but the procedures would be different—consult the RADIUS documentation.)

Here's what the procedure would be for our hypothetical network. To begin, we'd start up the CSM Connection Manager and make a connection (File/Connect). Then we'd proceed with the following steps:

1. From Configure on the CSM Connection Manager menu bar, select Access Servers.
2. Click Add to configure CSM for the Concentrator. This will place you in the Properties window:
   a. Under Name, enter "Conc_LRA3".
   b. Provide the Concentrator's IP address (2.2.2.1).
   c. In the Access Server Type field, select "LRA3000".
   d. Provide authentication information: the CSM Secret ("CSM_sec") and System Secret ("LRA3_sec"). These values correspond to the values we already entered on the Concentrator (see **Section 6.1.1**).
3. Click Add.
4. From Configure on the menu bar, select Devices.
5. Click Add to add the bridge as a remote device.
6. Under the Address tab, specify the device name of "RBridge".
7. Under the Protocols tab, check the box to Enable IP.
8. Under the Bridging tab, check the box to Enable Bridging.
9. Under the Access tab (Authentication):
   a. Select PPP as Layer 2 Protocol.
   b. Enable Authentication.
   c. Enter the CHAP secret ("secretbr").
10. Click Add to add the device.

7. Troubleshooting

The first thing to do if you're having problems with the Remote Access Concentrator is to check its LEDs and its cable connections. If all of its cables are securely attached and its LEDs don't tell you what you need to know, check the system log for any error messages that might be recorded there. Consult the "Log Messages" section of the Concentrator's HTML documentation for directions on retrieving the log and interpreting any error messages it contains. Also consult the logs of any routers, bridges, etc., that the Concentrator was communicating with when the trouble happened.

If this doesn't help, proceed with the rest of this section.

7.1 Calling Black Box

If you determine that your Remote Access Concentrator 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;
- a screen capture of the Concentrator's log; and
- the results of any testing you've already done.

7.2 Shipping and Packaging

If you need to transport or ship your Remote Access Concentrator:

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

NOTES

NOTES

NOTES

BLACK BOX®
NETWORK SERVICES

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