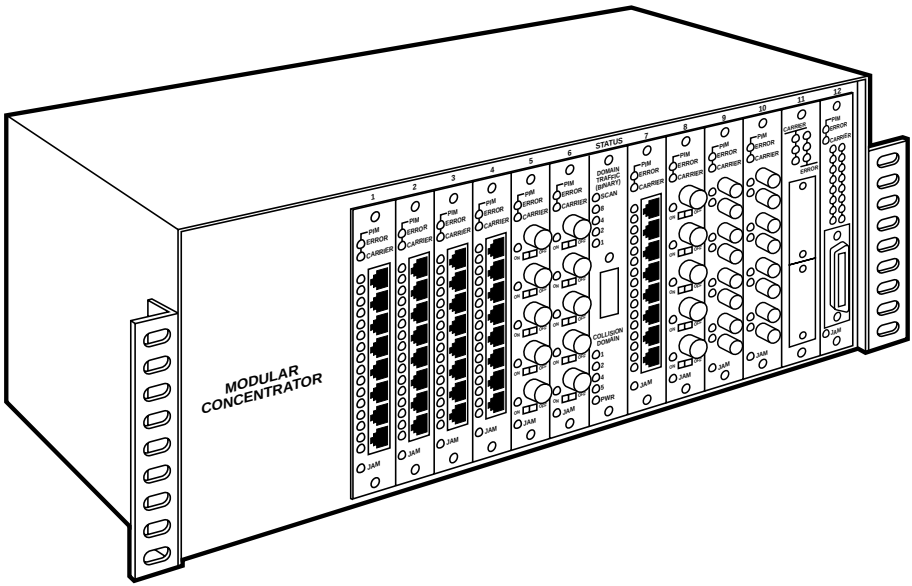
BLACK BOX®
NETWORK SERVICES

JULY 2000

LE6402A	LE6413A	LE6424
LE6403A	LE6420	LE6425
LE6405A	LE6421	LE6426
LE6406A	LE6422	LE6427
LE6412A	LE6423	RM6400

Modular Concentrator



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S. 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION
AND
INDUSTRY CANADA
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart 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 classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

NORMAS OFICIALES MEXICANAS (NOM)
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.

TRADEMARKS

3Com® is a registered trademark of 3Com Corporation.
ARCNET® is a registered trademark of DATAPOINT CORPORATION.
AT&T® and ST® are registered trademarks of AT&T.
dBASE® is a registered trademark of Inprise Corporation.
Digital™ and VAX™ are trademarks of Compaq Corporation.
Fujitsu® is a registered trademark of Fujitsu Limited.
HP®, EtherTwist®, and Open View® are registered trademarks of Hewlett-Packard.
IBM®, Micro Channel®, and ThinkPad® are registered trademarks of International Business Machines Corporation.
Intel® is a registered trademark of Intel Corporation.
MICOM® is a registered trademark of Nortel Networks.
MultiTech® is a registered trademark of Multi-Tech Systems, Inc.
Mylar® is a registered trademark of E.I. du Pont de Nemours and Company.
NCR® is a registered trademark of NCR Corporation.
Novell®, LAN WorkPlace®, and NetWare® are registered trademarks of Novell Incorporated.
PCnet® is a registered trademark of S3, Inc.
Ungermann-Bass® is a registered trademark of Alcatel.
WANG® is a registered trademark of Getronics NV.
Microsoft® and Windows™ are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Zenith® is a registered trademark of Zenith Electronics Corporation.

All applied-for and registered trademarks are the property of their respective owners.

Contents

Chapter **Page**

Chapter **Page**

1. Specifications

Standards — IEEE 802.3 10BASE-T, 10BASE2, 10BASE5, FOIRL

Indicators — LE6402A, LE6403A, LE6425: (1) Power, (2) Collision Domain; LE6405A, LE6406A, LE6412A, LE6413A, LE6426, LE6427: (1) Power, (3) Collision Domain; LE6420, LE6421: (1) Error, (1) Carrier, (1) Jam (8) Link, (8) Error, LE6422: (1) PIM, (1) PIM Carrier, (1) Jam, (5) Error; LE6423, LE6424: (1) Carrier, (1) Jam, (8) Link, (9) Error; LE6427: (1) Power, (3) Collision Domain, (5) Domain Traffic

Connectors — LE6402A, LE6403A: (1) IEC 320, (2) Hub Module slots, (2) PIM slots; LE6405A, LE6406A: (I) IEC 320, (5) Hub Module slots, (5) PIM slots; LE6412A, LE6413A: (1) IEC 320, (12) Hub Module slots, (12) PIM slots; LE6420: (8)RJ-45, (1) card edge, (1) PIM slot; LE6421: (1) 50-pin telco female, (1) card edge, (1) PIM slot; LE6422: (5) BNC female, (1) card edge, (1) PIM slot; LE6423: (8) ST female, (1) card edge, (1) PIM slot; LE6424: (8) SMA female, (1) card edge, (1) PIM slot; LE6425, LE6426, LE6427: (1) card edge, (1) PIM slot

Temperature — *Operating*: 32° to 122° F (0° to 50° C), *Storage*: 22° to 160° F (-6° to 71° C)

Power — 115/230 V, 60/50 Hz, internal switching

Size — LE6402A, LE6403A: 1.8"H x 17.5"W x 6.8"D (4.6 x 44.5 x 17.3 cm); LE6405A, LE6406A: 3.5"H x 17.5"W x 6.8" D (8.9 x 44.5 x 17.3 cm); LE6412A, LE6413A: 5.3"H x 17.5"W x 6.8"D (13.5 x 44.5 x 17.3 cm)

Weight — LE6402A, LE6403A: 8.5 lb. (3.8 kg); LE6405A, LE6406A: 11 lb. (5 kg), LE6412A, LE6413A: 15.5 lb. (7 kg)

2. Introduction

The modular, IEEE 802.3 (ISO/IEC 8802-3) compliant Ethernet hubs/repeaters include the following models:

- Modular Concentrator/2 (Unmanaged) (LE6402A)
- Modular Concentrator/2 (w/SNMP Module) (LE6403A)
- Modular Concentrator/5 (Unmanaged) (LE6405A)
- Modular Concentrator/5 (w/SNMP Module) (LE6406A)
- Modular Concentrator/12 (Unmanaged) (LE6412A)
- Modular Concentrator/12 (w/SNMP Module) (LE6413A)
- TP/8 Module (LE6420)
- TP/8—Telco Module (LE6421)
- BNC/5 Module (LE6422)
- FO/4—STII Module (LE6423)
- FO/4—SMA Module (LE6424)
- SNMP Module—Modular Concentrator/2 (LE6425)
- SNMP Module—Modular Concentrator/5 (LE6426)
- SNMP Module—Modular Concentrator/12 (LE6427)
- Rackmount Brackets/Modular Concentrator (RM6400)

The Concentrators are user-configurable using Hub Modules (HMs) for twisted-pair, fiberoptic, and thin coaxial cabling. Each version can be purchased with an SNMP Hub Management Module already installed, or you can get the Concentrator unmanaged and add SNMP management later.

Each may be configured with more than one Collision Domain (refer to **Section 3.2, Multiple Collision Domains,** for details). The internal power supply works with standard AC voltages worldwide (the Concentrator comes with the right power cord for your country). Every model is UL®, CSA, and TUV certified.

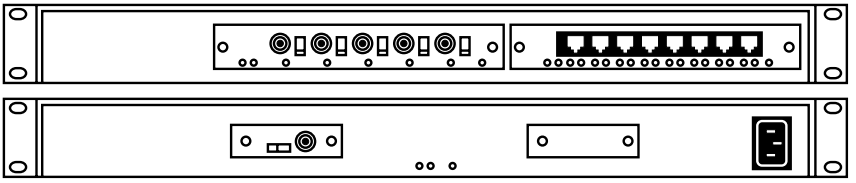
Each concentrator can be installed in a standard 19" rack, using the rackmount brackets (RM6400); hung on a wall, using wallmount brackets; or set on a desk or table-top.

For detailed installation information on SNMP management options, please refer to **Chapter 4, Software Installation**.

2.1 Base Units

Base Units are modular, low-profile Ethernet concentrators. They can be configured with 1, 2, or 4 collision domains, depending on model. LEDs indicating Collision Domain and Power are located on the back of the unit.

The Modular Concentrator/2 is a low-profile (1.8"H x 17.5"W x 6.8"D [4.6 x 44.5 x 17.3 cm]) Ethernet concentrator that has two slots for installing one (minimum) or two HMs in any combination. It is available with an SNMP Concentrator Management Module already installed (LE6403A), or it can be purchased unmanaged (LE6402A) and SNMP management can be added later. The Concentrator can function as a single collision domain or can be configured with two domains. LEDs indicating Collision Domain 1, Collision Domain 2, and Power are located on the back of the unit.



The Modular Concentrator/5, measuring 3.5"H x 17.5"W x 6.8"D (8.9 x 44.5 x 17.3 cm), is the same as the Modular Concentrator/2, but has 5 slots for installing 1 (minimum) to 5 HMs in any combination. It can be configured with 1, 2, or 4 collision domains. A DB9 modem connector for out-of-band SNMP management, an 8-position switch for concentrator configuration, and an ON/OFF power switch are located on the back of the unit.

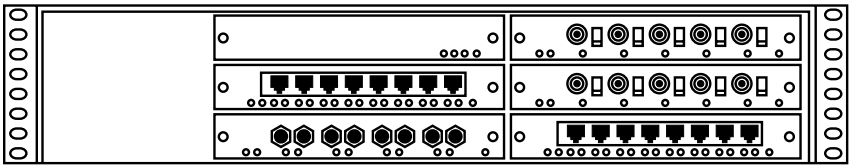


Figure 2-2. Modular Concentrator/5—Front Panel.

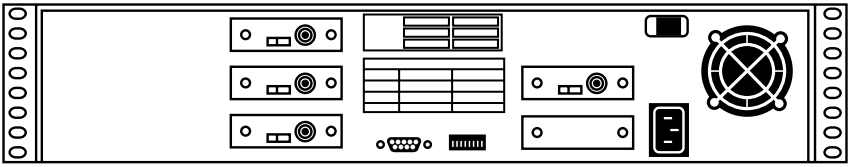


Figure 2-3. Modular Concentrator/5—Rear Panel.

The Modular Concentrator/12, measuring 5.3"H x 17.5"W x 6.8"D (13.5 x 44.5 x 17.3 cm), is the same as the Modular Concentrator/5, but has 12 slots for installing 1 (minimum) to 12 HMs in any combination. It can be configured with 1, 2, or 4 collision domains. A DB9 modem connector for out-of-band SNMP management, an 8-position switch for concentrator configuration, and an ON/OFF power switch are located on the back of the unit.

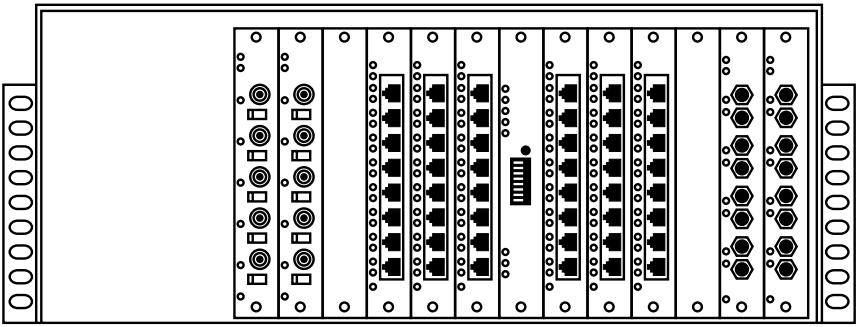


Figure 2-4. Modular Concentrator/12—Front Panel.

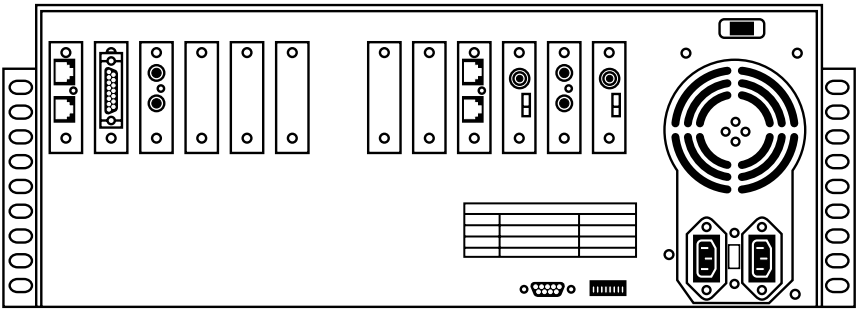


Figure 2-5. Modular Concentrator/12—Rear Panel.

2.2 SNMP Hub Management Modules (HMMs)

Each Modular Concentrator can be purchased with an SNMP Module already installed, or it can be purchased unmanaged and SNMP management can be added later. SNMP Modules are installed with no loss of media slots. The SNMP Module—Modular Concentrator/2 is installed internally to the concentrator; it comes with everything required for installation. The Modular Concentrator/5 and the Modular Concentrator/12 each feature an external slot for the installation of the SNMP Module, which also comes with everything required for installation. Refer to **Section 3.1.3**, **Installing SNMP Modules,** for details.

2.3 Hub Modules (HMs)

The basic building blocks for the modularity of the network concentrators are the Hub Modules (HMs). HMs are available in the following versions:

- TP/8 Module (LE6420) includes eight RJ-45 connectors for 1 to 8 10BASE-T unshielded twisted-pair link segments. Shielded twisted-pair cable may also be used.

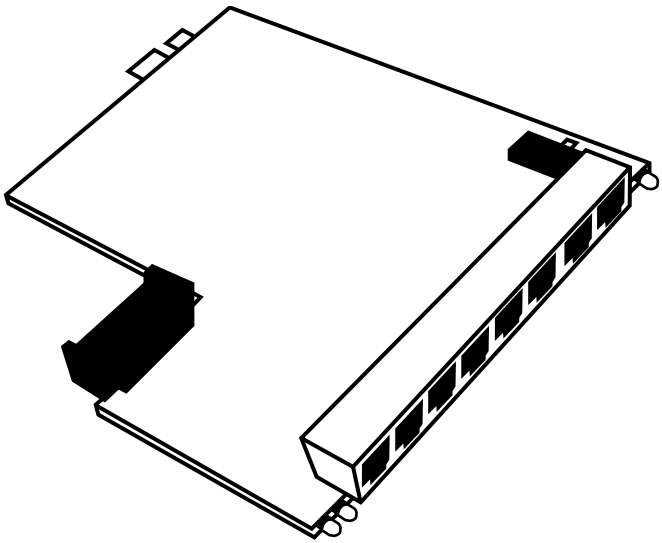


Figure 2-6. TP/8 Module.

- TP/8—Telco Module (LE6421) includes a 50-pin Telco connector for 1 to 8 10BASE-T unshielded twisted-pair link segments.

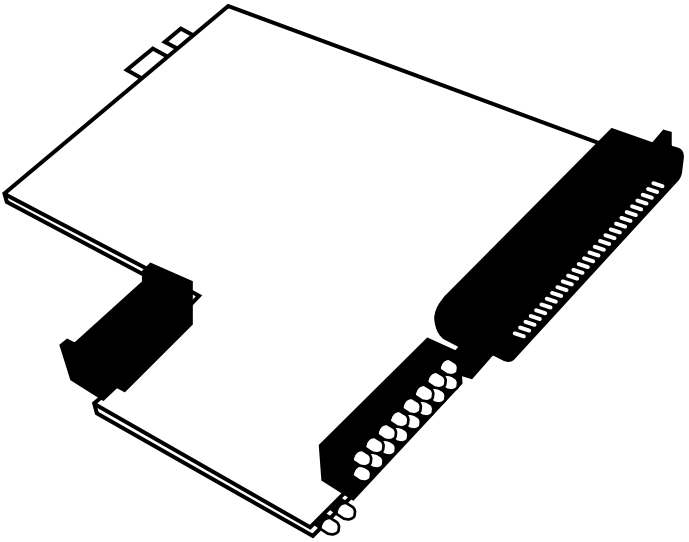


Figure 2-7. TP/8—Telco Module.

- BNC/5 Module (LE6422) includes five BNC connectors for 1 to 5 10BASE2 “thin” and optional 75- or 93-Ohm coaxial segments.

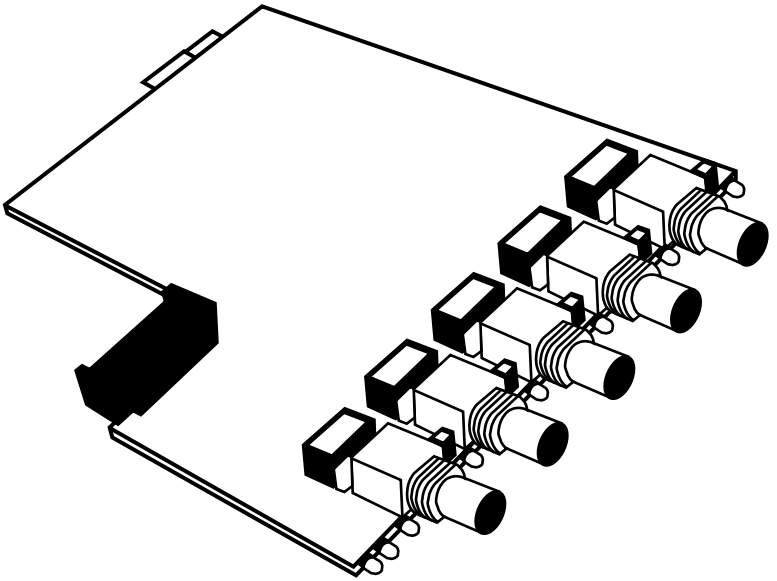


Figure 2-8. BNC/5 Concentrator Module.

- FO/4-STII Module (LE6423) includes four pair (transmit/ receive) STII connectors for 1 to 4 10BASE-FL/FOIRL fiberoptic link segments.

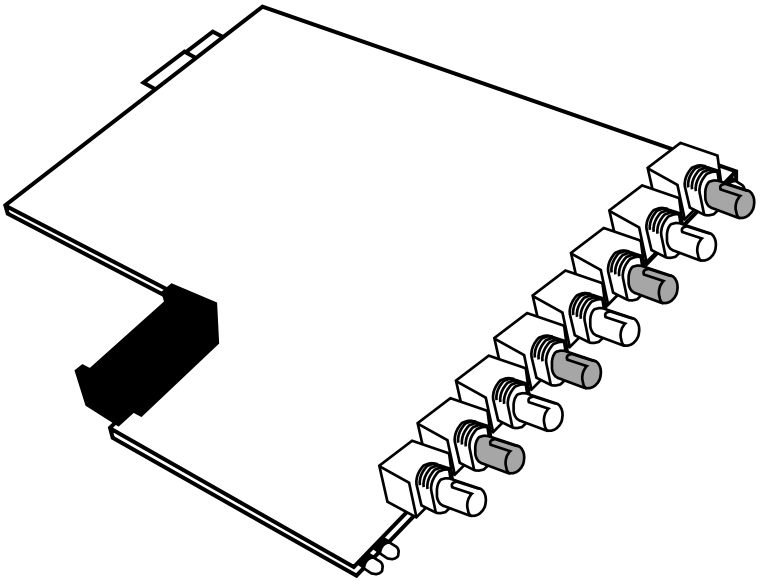


Figure 2-9. FO/4-STII Module.

- FO/4-SMA Module (LE6424) includes four pair (transmit/ receive) SMA connectors for 1 to 4 10BASE-FL/FOIRL fiberoptic link segments.

The concentrators are shipped from the factory with no HMs installed. HMs can be installed in any combination. In the Modular Concentrator/12, for example, HMs of the same type could be configured to total up to 96 twisted-pair link segments, 60 “thin” coaxial segments, or 48 fiberoptic link segments. If cabling requirements change, concentrators can be reconfigured at any time without bringing the entire unit down. Refer to **Section 3.1.2**, **Installing Hub Modules,** for details.

Front-panel LEDs on each HM indicate JAM for the module, ERROR for each BNC segment, and ERROR and LINK for each twisted-pair or fiberoptic link segment.

3. Hardware Installation

3.1 Installation

The design of the multiple domain, modular Ethernet concentrators allows for easy network expansion at any time. Hub Modules (HMs) support a variety of configuration options that may be implemented as the LAN grows. Modular Concentrators are configured by combining HMs.

NOTE

If you install rack-mounted units in a closed or multi-rack assembly, consider the following items:

1. The ambient temperature within the rack may be greater than room ambient. The maximum temperature for the equipment in this environment is 122° F (50° C).

2. Allow enough air flow for safe operation, and do not load the unit unevenly.

Input Supply

Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.

Grounding

Maintain reliable earthing of this equipment. Pay attention to supply connections when connecting to power strips, rather than direct connections to the branch circuit.

3.1.1 Opening the Case

The concentrator cases have been designed for effective RFI shielding. Under most circumstances, you don't need to open the case. If you must open the case, instructions have been included here.

CAUTION

Hazardous voltages that could cause serious injury are present in these concentrators. Before opening the case, have all users log out from the network and remove the power cable from the unit. Opening the case before disconnecting from electrical power could result in damage.

Once the power is off, disconnect the power cord from the back of the unit. To open the case, use a Phillips-head screwdriver to remove all the screws on the sides and the top of the unit, then remove the cover.

NOTE

If the concentrator has been mounted in a rack, remove the unit from the rack and remove the rackmount brackets.

3.1.2 Installing the Hub Modules (HMs)

Each HM includes an edge connector for attaching to the backplane PCB. A minimum of one HM must be installed to have a functional concentrator.

The concentrator can be reconfigured at any time. HMs are "hot-swappable," so you don't need to power the concentrator down before configuration. Installed HMs will continue to operate without interruption during configuration.

NOTE

Make sure that all BNC ports are properly terminated before "hot-swapping" a BNC/5 Module.

Before installing HMs, you might need to adjust the coaxial cable impedance selection on the BNC/5 Module (refer to **Section 3.1.6**).

BNC connections may also require adjustments for termination, which is externally accessible from the front of the unit and can be done after installation (refer to **Section 3.1.5**).

Each concentrator is shipped with "blank" brackets covering the unused HM slots. Each HM is shipped with the appropriate bracket. Using a Phillips-head screwdriver, simply remove the two screws holding the "blank" bracket over the slot where you will install the HM.

To install an HM in the Modular Concentrator/12, insert the HM into the card guides on the top and bottom of the slot and slide the HM forward until it fits securely in the connector on the backplane PCB (**Figure 3-1**).

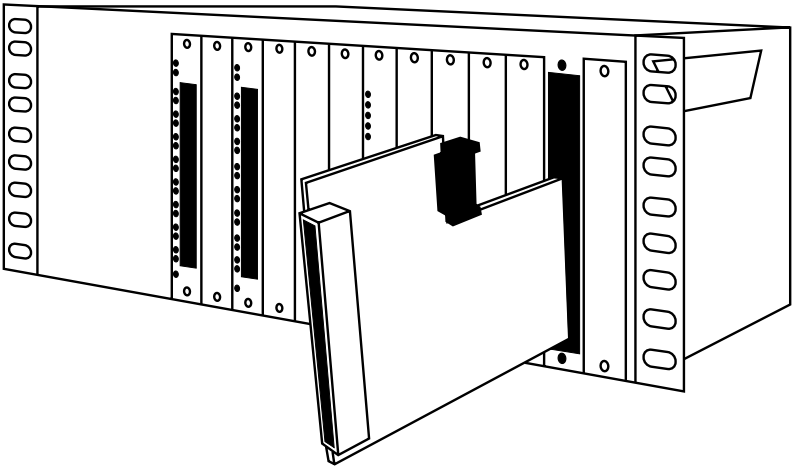


Figure 3-1. Installing the TP/8 Module in the Modular Concentrator/12.

To install an HM in the Modular Concentrator/2 or the Modular Concentrator/5, insert the HM into the card guides on the left and right sides of the slot and slide the HM forward until it fits securely into the connector on the backplane PCB (**Figure 3-2**).

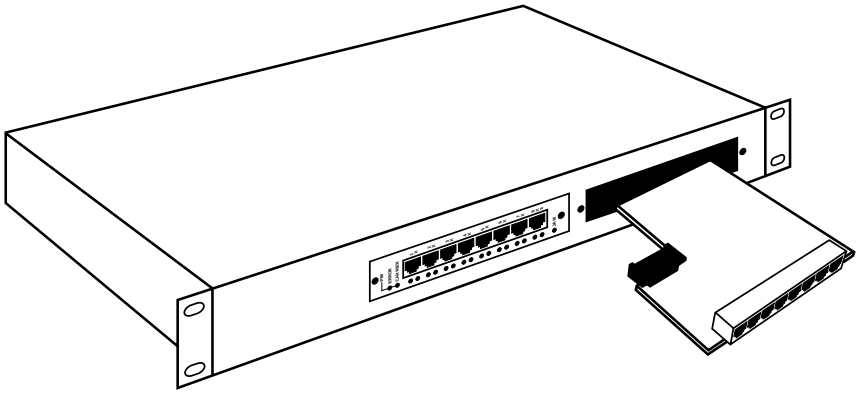


Figure 3-2. Installing the TP/8 Module into the Modular Concentrator/2.

After inserting the HM, secure it in place with the bracket supplied and connect the cables.

3.1.3 Installing SNMP Concentrator Management Modules

You can purchase Modular Concentrators unmanaged and you can add the SNMP Concentrator Management Module (HMM) when needed. This section discusses the hardware installation only. Refer to **Chapter 4**, **Software Installation,** for details on software installation and configuration.

NOTE

We recommend that all users log off the network and the unit be powered down before installing HMMs.

Installing in Modular Concentrator/5 and Modular Concentrator/12

The SNMP Module—Modular Concentrator/5 (LE6426) and the SNMP Module—Modular Concentrator/12 (LE6427) include the Concentrator Management Module, bracket, and two software diskettes.

NOTE

A DB9 modem connector for out-of-band management is pre-installed on both these concentrators.

Each concentrator features a slot which, when shipped unmanaged, contains a dumb controller module. To install the SNMP Concentrator Management Module, the dumb controller module must be removed.

Using a Phillips-head screwdriver, remove the two screws holding the bracket over the controller module. Take the bracket away and gently pull the module forward until it is completely out of the slot.

To install the HMM in the Modular Concentrator/12, insert the HMM into the card guides on the top and bottom of the slot and slide the HMM forward until it fits securely in the connector on the backplane PCB (**Figure 3-1**). Secure the HMM in place using the bracket supplied.

To install an HMM in the Modular Concentrator/5, insert the HMM into the card guides on the left and right sides of the slot and slide the HMM forward until it fits securely into the connector on the backplane PCB (**Figure 3-2**). Secure the HMM in place using the bracket supplied.

Installing in Modular Concentrator/2

The SNMP Module—Modular Concentrator/2 (LE6425) includes the Management Module, a DB9 connector assembly with ribbon cable and bracket and two software diskettes.

NOTE

The DB9 connector assembly is for optional out-of-band management.

To install an HMM in the Modular Concentrator/2, the cover of the concentrator must removed. Please refer to **Section 3.1.1**.

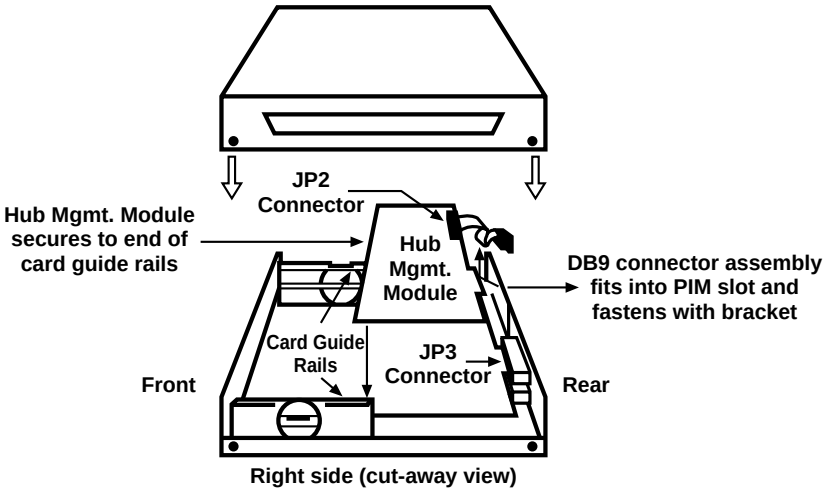


Figure 3-3. Installing the SNMP Module in the Modular Concentrator/2.

Once the cover is removed, remove the two screws located on the rear portion of the two card guide rails on the right side of the concentrator (with the front of the concentrator facing forward). Set them aside for later use.

With the connector toward the rear, position the HMM over the card guide rails. Slide the HMM into the connector at position JP3 on the main board until it fits securely into place. Secure the module to the card guide rails using the two screws that you previously removed.

If you require out-of-band management, you need to install the DB9 connector assembly in the PIM slot on the right rear side of the concentrator (while the cover is removed).

Using a Phillips-head screwdriver, simply remove the two screws holding the "blank" bracket over the PIM slot where the DB9 connector is to be installed. To install the DB9 connector assembly, pull the ribbon cable through the PIM slot to the inside of the concentrator until the DB9 connector is flush with the slot. Secure the connector with the bracket supplied. Attach the ribbon cable connector to the pins located at position JP2 on the HMM, making sure the red stripe on the ribbon cable lines up with Pin 1 on the JP2 pin block (**Figure 3-4**).

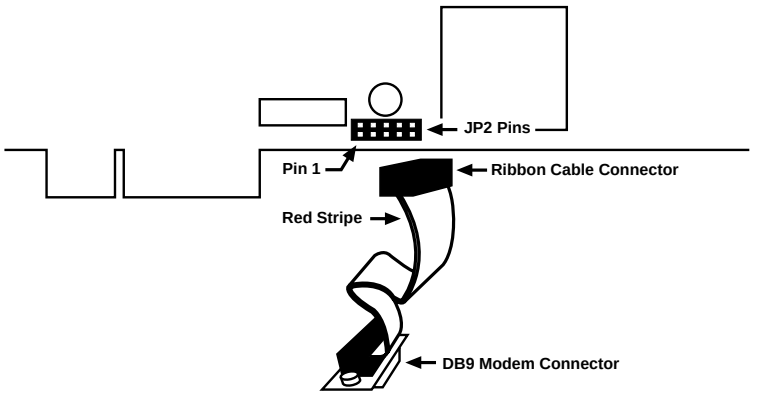


Figure 3-4. Modular Concentrator/2 DB9 Modem Ribbon Cable Installation.

When the hardware installation is completed, replace the cover and power the unit on.

3.1.4 Port Termination

BNC/5 Modules feature a termination switch next to each BNC connector. This switch lets you terminate a "thin" coaxial segment at the repeater without a "T" connector and terminator. If you will terminate a "thin" Ethernet segment at the HM, attach the cable directly to the BNC connector with the termination switch in the ON (enabled) position (**Figure 3-5**).

If the HM is attached to a midpoint of a "thin" Ethernet segment, attach a "T" connector to the BNC connector. The termination switch must be set to the OFF (disabled) position when this configuration is used (**Figure 3-5**). **Table 3-1** summarizes BNC termination switch settings.

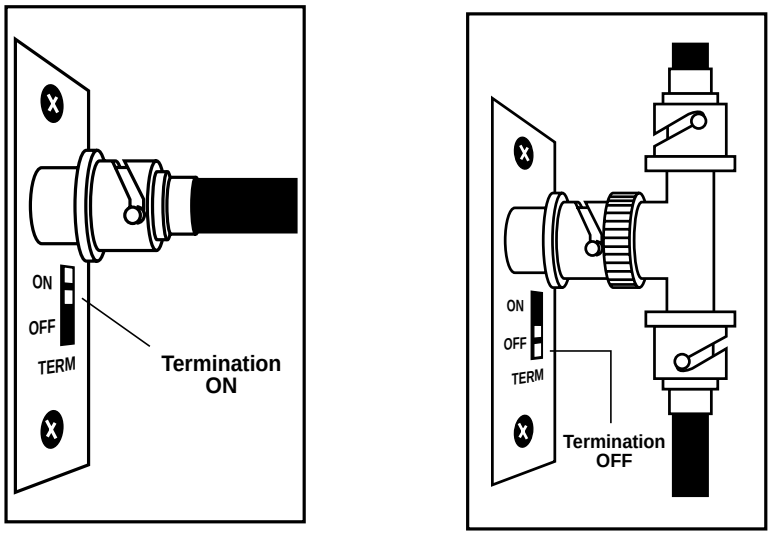


Figure 3-5. Termination ON and Termination OFF.

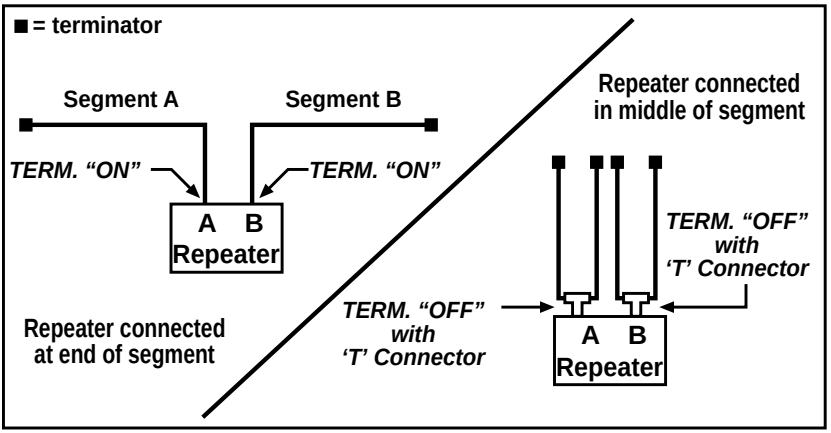


Figure 3-6. BNC Port Termination.

Table 3-1. BNC Port Termination

Location of Concentrator/Repeater	TERM Switch Setting	"T" Connector
At end of segment	ON	Not needed, attach cable directly to BNC port
At end of segment	OFF	Use a "T" connector with terminator
In middle of segment	OFF	Use a "T" connector

NOTE

"Thin" Ethernet segments must be properly terminated at both ends and grounded at one end. If the BNC segment is not terminated correctly, the ERROR LED on the front panel will glow.

3.1.5 Coaxial Cabling Impedance Selection

The BNC/5 Module can run Ethernet over 93-ohm (ARCNET®, IBM® 3270) or 75-ohm (WANG®, PCnet®, G/Net) coaxial cable. This provides a low-cost link between existing cabling systems and modern Ethernet LANs. Different cabling impedances can be freely intermixed in a single concentrator to join 93-ohm or 75-ohm cable to standard 50-ohm Ethernet LANs. The BNC connectors are factory-set for RG-58U 50-Ohm cabling in compliance with 10BASE-2 specifications.

3.1.9 Connecting Twisted Pair Cabling

TP/8 Modules support both shielded and unshielded twisted-pair cable. No adjustments are necessary. All RJ-45 connectors on TP/8 Modules are internally crossed, complying with 10BASE-T specifications. This is indicated by an "X" by each port.

You can interconnect TP/8 Modules by running twisted-pair cable from an RJ-45 port on one to an RJ-45 port on another. If both ports contain internal crossover functions, you need an additional external crossover.

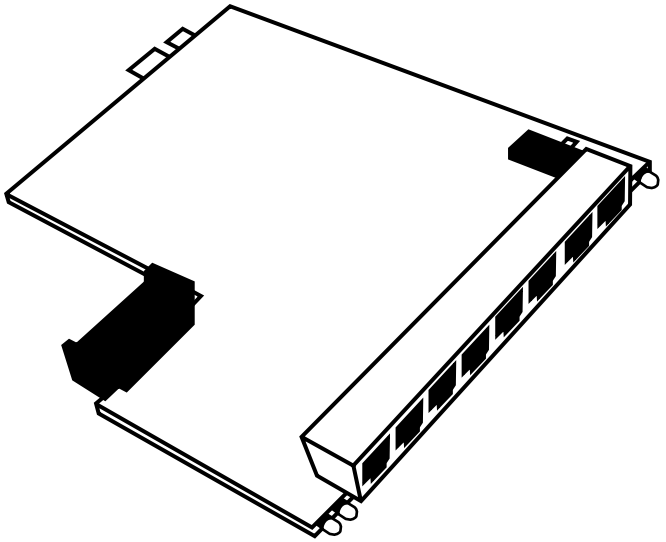


Figure 3-7. TP/8 Module.

To eliminate the need for external crossover wires, TP/8 Modules feature an internal cascading switch at port 8 (labeled "X/II") that lets you select either crossover "X" (factory default) or pass-through "II" (parallel) connections.

To access the cascading switch, remove the TP/8 Module from the concentrator. The switch is located at position S1 near Port 8 (**Figure 3-8**) on the TP/8 Module. To select the pass-through capability, simply move the switch to the "II" position (away from the RJ-45 connector).

You can also interconnect TP/8 Modules by running twisted-pair cables from any of the RJ-45 connectors on one module to an AUI connector on another concentrator by using a miniature twisted-pair transceiver (part number LE2040A) and a PIM module. Once the TP/8 Module is successfully connected to the MAU and both devices are powered on, the link LEDs on the TP/8 Module and the MAU should light.

Connecting TP/8 Modules using twisted-pair cabling limits the cascading distance to 335 feet (100 meters), the 10BASE-T specification.

3.1.6 Wiring TP/8-Telco Modules

The TP/8-Telco Module provides 8 twisted-pair link-segment connections. **Table 3-3** details the pin-out specifications for wiring the 50-pin telco connector.

Table 3-3. Wiring the 50-pin Telco Connector.

50-Pin Telco Pin Numbers	Port	Concentrator Designation Pin Numbers	10BASE-T RJ-45 (8-pin)
26	1	RCV POS (TIP)	1
1	1	RCV NEG (RING)	2
27	1	XMT POS (TIP)	3
2	1	XMT NEG (RING)	6
28	2	RCV POS (TIP)	1
3	2	RCV NEG (RING)	2
29	2	XMT POS (TIP)	3
4	2	XMT NEG (RING)	6
30	3	RCV POS (TIP)	1
5	3	RCV NEG (RING)	2
31	3	XMT POS (TIP)	3

Table 3-3 (continued). Wiring the 50-pin Telco Connector.

50-Pin Telco Pin Numbers	Port	Concentrator Designation Pin Numbers	10BASE-T RJ-45 (8-pin)
6	3	XMT NEG (RING)	6
32	4	RCV POS (TIP)	1
7	4	RCV NEG (RING)	2
33	4	XMT POS (TIP)	3
8	4	XMT NEG (RING)	6
34	5	RCV POS (TIP)	1
9	5	RCV NEG (RING)	2
35	5	XMT POS (TIP)	3
10	5	XMT NEG (RING)	6
36	6	RCV POS (TIP)	1
11	6	RCV NEG (RING)	2
37	6	XMT POS (TIP)	3
12	6	XMT NEG (RING)	6
38	7	RCV POS (TIP)	1
13	7	RCV NEG (RING)	2

Table 3-3 (continued). Wiring the 50-pin Telco Connector.

50-Pin Telco Pin Numbers	Port	Concentrator Designation Pin Numbers	10BASE-T RJ-45 (8-pin)
39	7	XMT POS (TIP)	3
14	7	XMT NEG (RING)	6
40	8	RCV POS (TIP)	1
15	8	RCV NEG (RING)	2
41	8	XMT POS (TIP)	3
16	8	XMT NEG (RING)	6

3.1.7 Cabling the 10BASEFL/ FOIRL Link Segment

FO/4-STII Modules come with STII connectors; FO/4-SMA Modules come with SMA connectors. Each fiber connection consists of two (one pair) STII or SMA connectors, one for transmit and one for receive, for a single fiberoptic link segment. A concentrator can be connected to any other 10BASE-FL or FOIRL device (repeater, network interface card, or FO MAU) by running a fiberoptic cable from the transmit connector on one device to the receive connector on the other device, and vice versa (**Figure 3-9)**.

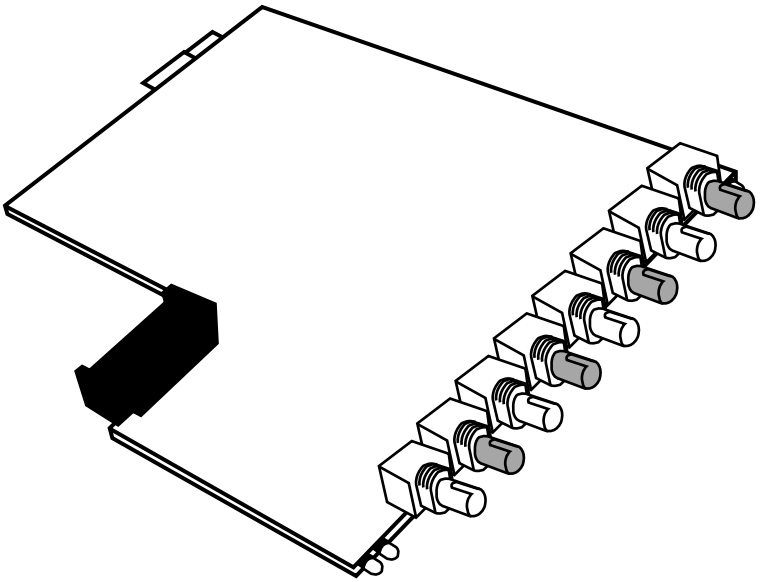


Figure 3-8. FO/4 Module.

Once the concentrator is successfully connected to another 10BASE-FL/FOIRL device, and both devices are powered on, the LINK LED for each link segment should remain lit during normal LAN operation. The LINK LED acts as a link integrity check and low-light indicator. If it does not light, or goes out, there is a physical problem with the fiberoptic link segment.

3.1.8 Cabling Configurations

You can use Modular Concentrators for a wide variety of cabling configurations and distances. If connecting to "thick" or "thin" coaxial cabling, you can place the concentrator anywhere on the segment. If connecting to twisted-pair or fiberoptic cabling, you can place the concentrator only at the end of the segment.

You may install HMs in any combination, depending upon the network requirements. The flexibility of the Concentrator is limited only by the IEEE 802.3 configuration and distance specifications for each cabling type.

Figure 3-11 shows a configuration example using Modular Concentrator/12. The Concentrator is connected to twisted-pair concentrators using "thin" coaxial cable for connections in Building 1 and using fiberoptic cable for connections in Buildings 2 and 3, which are farther away. This is only one example of the many possible configurations available with the Concentrators.

For additional information on IEEE 802.3 repeater and cabling configuration specifications, refer to **Section 3.4**.

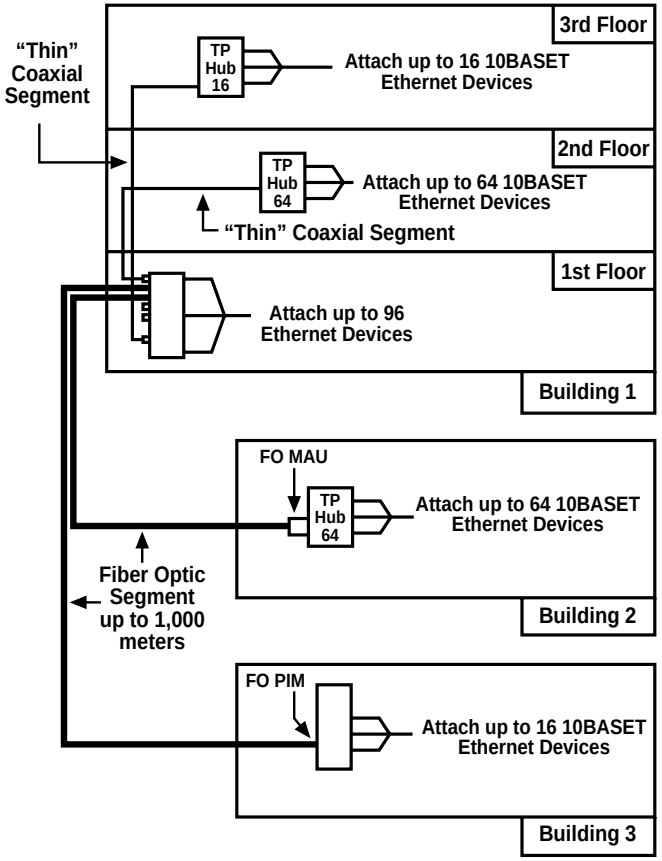


Figure 3-9. Example of Modular Concentrator/12 Configuration.

3.2 Multiple Collision Domains

A single Ethernet LAN is made up of one or more segments connected together. This single LAN can also be thought of as one logical unit or, more accurately, a collision domain. “LAN,” “logical unit,” and “collision domain” are used interchangeably in this manual.

A Modular Concentrator, whether managed or unmanaged, can be configured with two or more collision domains. You configure the Concentrator by setting an externally accessible switch. Which slots fall within which collision domain are preset. Refer to **Section 3.2** for details.

The following examples show variations on applications for using this capability. These examples use the Modular Concentrator/2 (with the exception of **Figure 3-15**, which uses the Modular Concentrator/5) and are very simple in their scope. The Modular Concentrator/5 and the Modular Concentrator/12 can each be configured with multiple collision domains providing many more configuration possibilities. If in doubt as to how to use this capability to its full advantage, contact technical support.

Configuring the concentrator with two domains and connecting both collision domains to a single fileserver with two network interface cards (NICs), using the server as an internal bridge, broadens the bandwidth, which increases the throughput and can dramatically decrease the number of collisions.

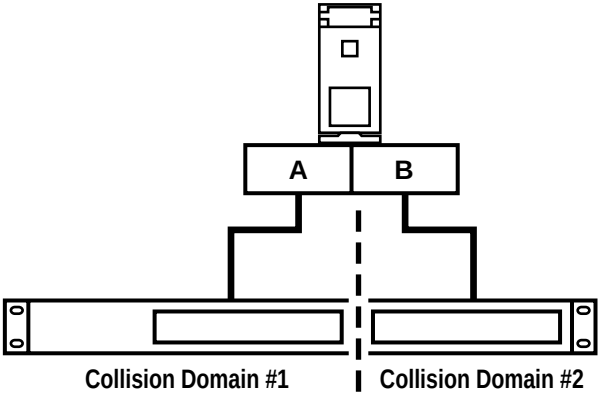


Figure 3-10. Server Internal Bridging.

If the concentrator has not been configured with two or more domains but two cables from the concentrator have been attached to two NICs in a single fileserver, an illegal Ethernet loop will have been created (**Figure 3-12**). This will cause router errors at the fileserver.

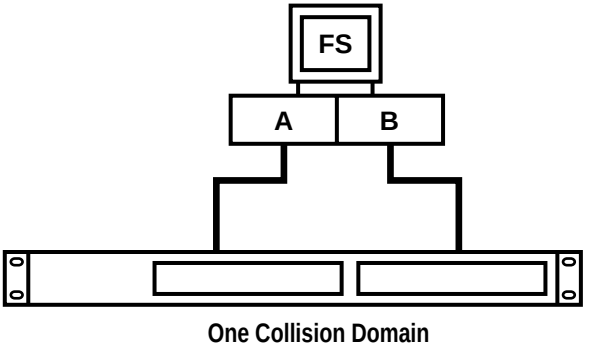


Figure 3-11. Illegal Ethernet Loop.

If the concentrator has been attached to two independent fileservers but has not been configured with two collision domains, the LANs are not separated, resulting in a single LAN with two fileservers.

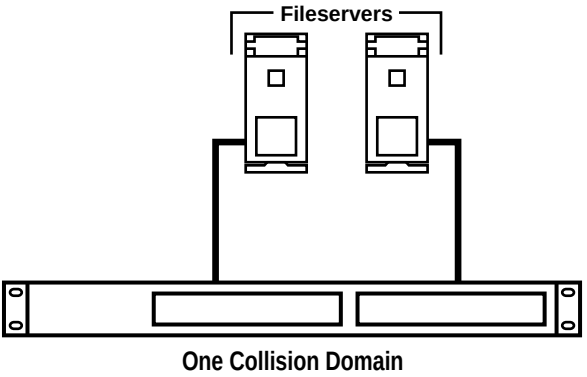


Figure 3-12. One LAN with Two Fileservers.

Configuring the concentrator with two collision domains and connecting each domain to a separate fileserver will create two independent LANs (**Figure 3-14**).

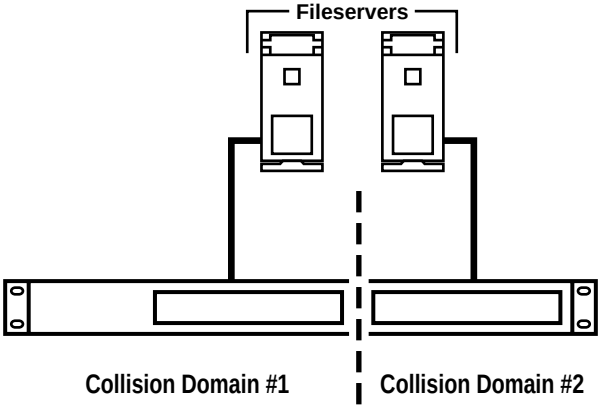


Figure 3-13. Two Independent LANs.

Configuring a Modular Concentrator/5 with four collision domains and connecting each domain to a separate fileserver will create four independent LANs (**Figure 3-15**).

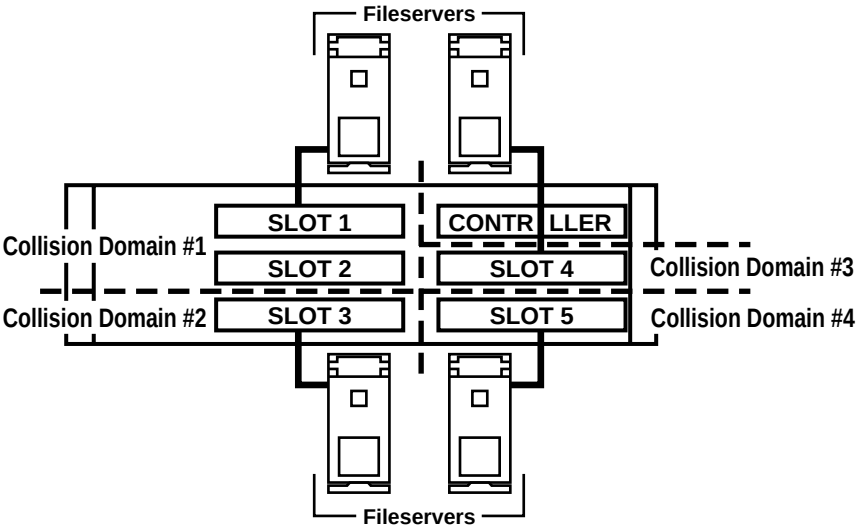


Figure 3-14. Four Independent LANs.

Configuring Multiple Collision Domains

You can configure Modular Concentrators with multiple collision domains, creating separate workgroups. You can then connect a cable from each domain to multiple network interface cards installed in the fileserver, dedicated bridge, or router. This optional multiple domain capability takes advantage of the server's internal bridging function to provide logical, as well as physical, LAN segmentation and increased performance.

The Modular Concentrator is factory-set as one collision domain, but it can be configured with two collision domains by setting a two-position switch located on the backplane of the PCB. You can access this switch through the left PIM slot (**Figure 3-16**) by removing the "blank" PIM bracket covering the PIM slot, or removing the PIM.

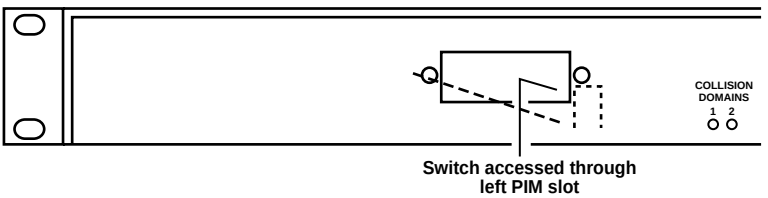


Figure 3-15. Modular Concentrator/2 Collision Domain Switch.

If the switch is up (Position 2), the Concentrator is configured as two collision domains. If the switch is down (Position 1), the concentrator is configured as a single collision domain. After setting the collision-domain switch to the desired setting, replace the blank PIM bracket.

The Modular Concentrator/5 and the Modular Concentrator/12 are also factory-set as one collision domain. The Modular Concentrator/5 may be configured with one, two, or four collision domains and the Modular Concentrator/12 with one, two, or four, collision domains. **Figures 3-17** and **3-18** show which slots fall within each collision domain. To configure the concentrators, set switches 1 and 2 on the 8-position DIP switch located on the back of the unit as follows:

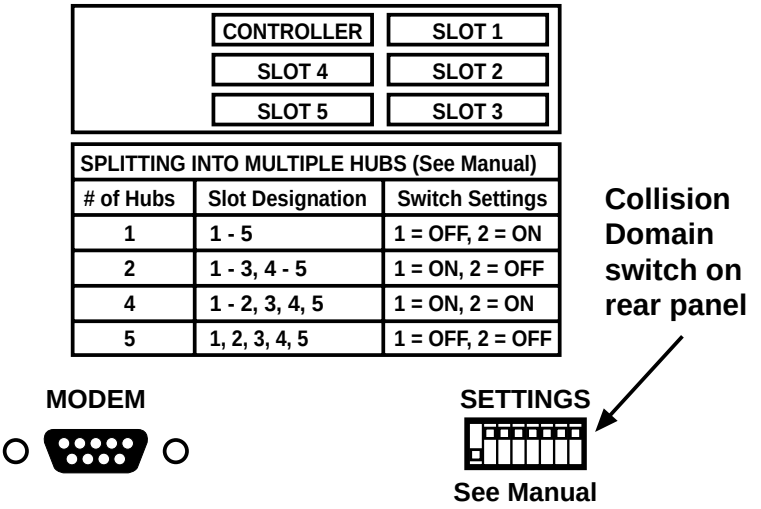


Figure 3-16. Modular Concentrator/5 Collision Domain Switch Settings.

SPLITTING INTO MULTIPLE HUBS (See Manual)		
# of Hubs	Slot Designation	Switch Settings
1	1 - 12	1 = OFF, 2 = ON
2	1 - 6, 7 - 12	1 = ON, 2 = OFF
4	1 - 3, 4 - 6, 7 - 9, 10 - 12	1 = ON, 2 = ON
12	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1 = OFF, 2 = OFF

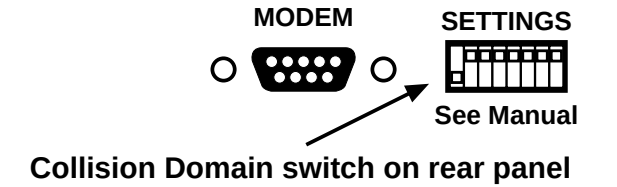


Figure 3-17. Modular Concentrator/12 Collision Domain Switch Settings.

3.3 Indicator LEDs

3.3.1 Concentrator Modules

Each Concentrator Module (HM) features LEDs for troubleshooting and monitoring connection status. Located on the front panel of each HM are the following LEDs (shown in **Figure 3-19**):

- JAM—Flickers amber occasionally in normal operation. This signifies collisions on the network, a common occurrence in Ethernet networks.
- CARRIER—Not used.
- ERROR—Not used.

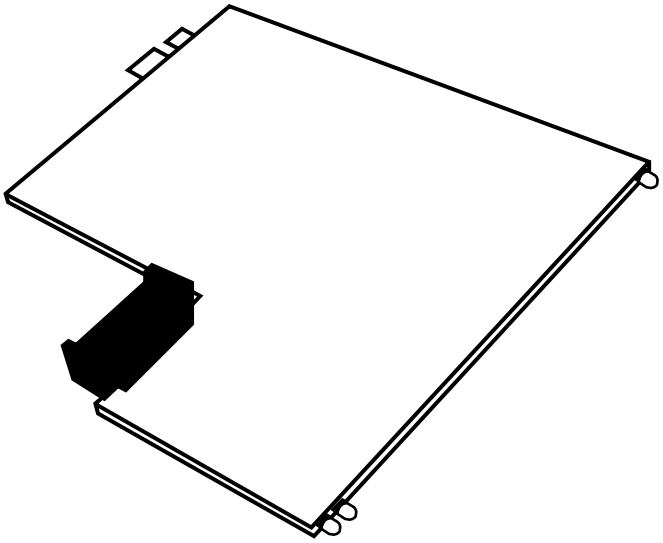


Figure 3-18. Concentrator Module JAM LED.

Also located on the front panel of each HM are LEDs for each port. They are:

- LINK—Glows green if a good twisted-pair or fiberoptic connection has been established. This LED should glow constantly during normal operation. If it does not glow, or goes out, there is a problem with the link segment.
- ERROR—Flickers red indicating an error condition. If this LED stays on, it indicates the segment has been partitioned from the network (usually indicating a termination problem or link failure). Reconnection is automatic when the error condition has been corrected.

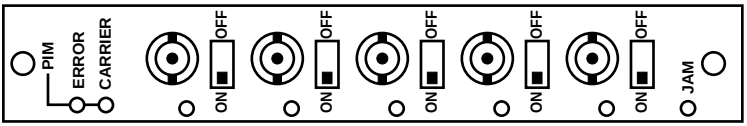


Figure 3-19. BNC/5 Module LEDs.

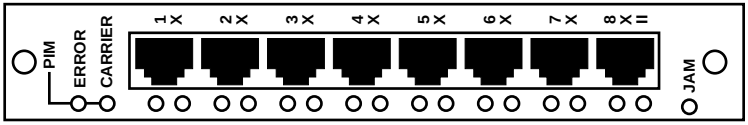


Figure 3-20. TP/8 Module LEDs.

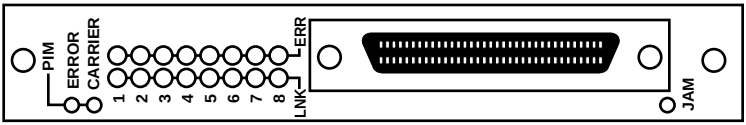


Figure 3-21. TP/8 Telco LEDs.

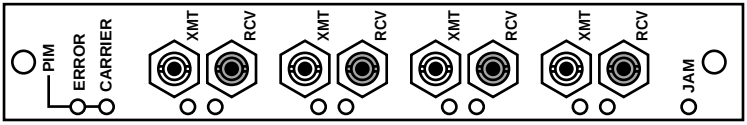


Figure 3-22. FO/4 Module LEDs.

If any red ERROR LED glows constantly, it indicates that a segment has been partitioned from the network. Reconnection is automatic when the error condition has been corrected. If constant ERROR or JAM conditions exist, refer to **Section 3.5** for possible solutions. If the problem persists, contact Technical Support for assistance.

3.3.2 Concentrator Controller Modules

Each controller module features LEDs for troubleshooting and monitoring connection status. The front panel of the "dumb" concentrator controller module features the following LEDs:

- POWER—Glows green if the module is receiving power.
- COLLISION DOMAINS—There are LEDs to indicate how many collision domains the concentrator has been configured with. (For example, on the Modular Concentrator/5, these LEDs are labeled 1, 2, and 4.) If the concentrator has not been configured with more than one collision domain, the Collision Domain 1 LED will glow green. If the concentrator has been configured with more than one collision domain, the appropriate LED will glow green.

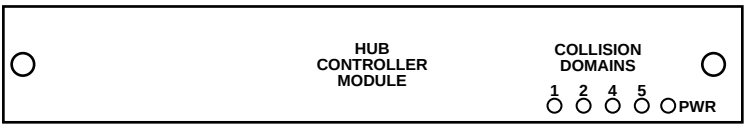


Figure 3-23. Modular Concentrator/5 "Dumb" Concentrator Controller Module LEDs.

NOTE

The Hub Controller Module on the Modular Concentrator/12 is in a vertical orientation. Collision LEDs are labeled 1, 2, 4 and 12.

3.3.3 SNMP Modules

The front panel of the SNMP Module features the following LEDs:

NOTE

The SNMP Concentrator Management Module on the Modular Concentrator/12 is in a vertical orientation. Collision LEDs are labeled 1, 2, and 4.

- POWER—Glows green if the module is receiving power.
- COLLISION DOMAINS—There are LEDs to indicate how many collision domains the concentrator has been configured with. (For example, on the Modular Concentrator/5, these LEDs are labeled 1, 2, and 4. If the concentrator has not been configured with more than one collision domain, the Collision Domain 1 LED will glow green. If the concentrator has been configured with more than one collision domain, the appropriate LED will glow green.

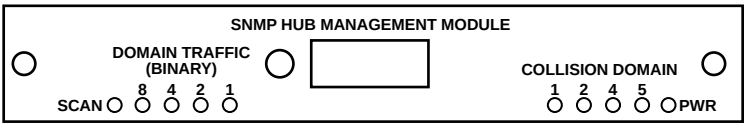


Figure 3-24. Modular Concentrator/5 SNMP Module LEDs.

The front panel of the SNMP Module features a switch button, which is located between the Bargraph LEDs and the Domain Traffic LEDs. This button lets you select which collision domain is to be monitored. If you select SCAN, each domain is monitored, in turn, for 5 seconds.

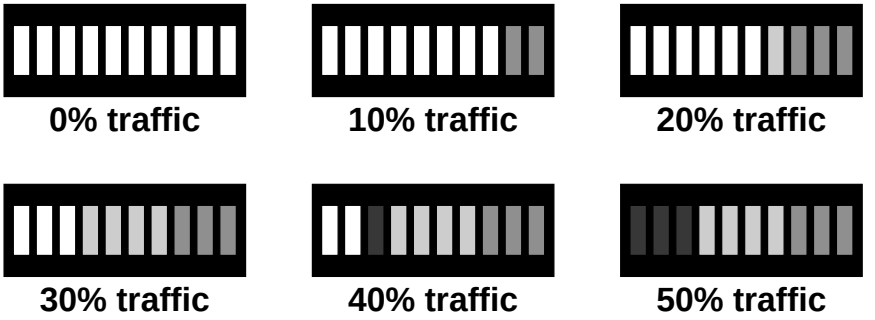


Figure 3-25. LED Bargraph—Domain Use (Modular Concentrator—5).

- DOMAIN TRAFFIC—The LED Bargraph monitors Ethernet use from 0 to 50% on whichever collision domain is selected. The DOMAIN TRAFFIC LEDs will glow green to indicate which domain is being monitored on the Bargraph.

NOTE

The LED Bargraph on the Modular Concentrator/12 is in a vertical orientation reading from bottom to top (for example, If there is 10% traffic, the bottom two LEDs would glow). The Modular Concen-trator/2 does not feature these LEDs, but, if the concentrators are managed, status is displayed in the SNMP software.

3.4 Network Installation Guidelines

To aid network installers, this section contains network-configuration information and IEEE 802.3 specifications for Ethernet networks. While most office LANs are easy for experienced computer users to install and support, we recommend that you call a reputable cable-installation contractor for larger or more complex networks.

3.4.1 The 5-4-3 Rule

The IEEE defines how many repeaters can be used as well as how many coaxial segments vs. link segments between any two nodes on a LAN. This definition is referred to as the 5-4-3 Rule. It has been designed to get the maximum performance out of a LAN. If you do not follow this rule, your network performance might degrade.

Very simply, this rule means:

5: There should be no more than 5 segments between any two nodes.

4: There should be no more than 4 repeaters between any two nodes.

NOTE

An Ethernet concentrator qualifies as a repeater.

3: There should be no more than 3 coaxial segments between any two nodes. The rest must be link segments.

This rule is documented in IEEE Std-802.3i-1990, in the “System Considerations for Multisegment 10Mbps Baseband Network” section.

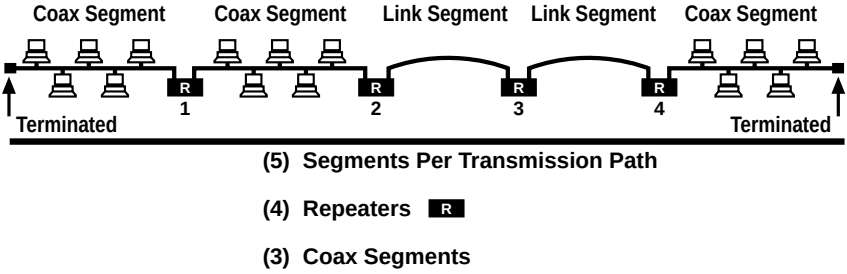


Figure 3-26. The 5-4-3 Rule.

3.4.2 Creating Multi-Media Networks

The physical size of a network is restricted by the limits of individual network components. You may combine segments of various types using repeaters for more versatility in larger LAN installations. In planning a network layout and installation, refer to **Table 3-4** and the examples on the following pages.

Table 3-4. Ethernet Specification Summary.

Characteristic	"Thick" Ethernet	"Thin" Ethernet	Unshielded Twisted Pair	Shielded Twisted Pair[1]	Fiber Optic[3]		
IEEE specification	802.3 10BASE5	802.3 10BASE2	802.3 10BASE-T	N/A	10BASE-FL	FOIRL	Single-mode
Topology	Linear bus	Linear bus	Star	Star	Star	Star	Star
Max. segment length	1,640 ft (500 m)	607 ft[2] (185 m)	328 ft (100 m)	492 ft (150 m)	6,560 ft (2,000m)	3,280 ft (1,000 m)	6,560 ft (2,000 m)
Max. MAUs per segment	100	30	2	2	2	2	2
Min. cable length between MAUs	8.2 ft (2.5m)	1.64 ft (0.5 m)	1 ft (0.3 m)	1.5 ft (0.45 m)	8.2 ft (2.5 m)	8.2 ft (2.5 m)	8.2 ft (2.5 m)
Connector type	AUI (DB15) N-series	BNC	RJ-45 (ISO 8877)	RJ-45 (ISO 8877)	STII bayonet mount	STII bayonet mount	STII bayonet mount

NOTES

[1]Specification based on tests done with Modular Concentrator series only.

[2] The Modular Concentrator series supports "thin'' cable segment lengths of up to 1,000 feet (305 meters), exceeding the IEEE 802.3 specification. If they are used in conjunction with other manufacturers' Ethernet products which only support the IEEE 802.3 standard of 607 feet (185 meters), the Modular Concentrator series is restricted to the same distance limitations.

[3]If using 4 repeaters with 5 fiberoptic link segments, the maximum fiber segment length is 1140 feet (500 meters).

The following are IEEE 802.3 specifications for network configuration:

1. If a MAU is attached to a repeater, you must disable Heartbeat (SQE) Test on the MAU.

2. The transmission path between any two DTEs may consist of a maximum of five segments and four repeaters (**Figure 3-29**).

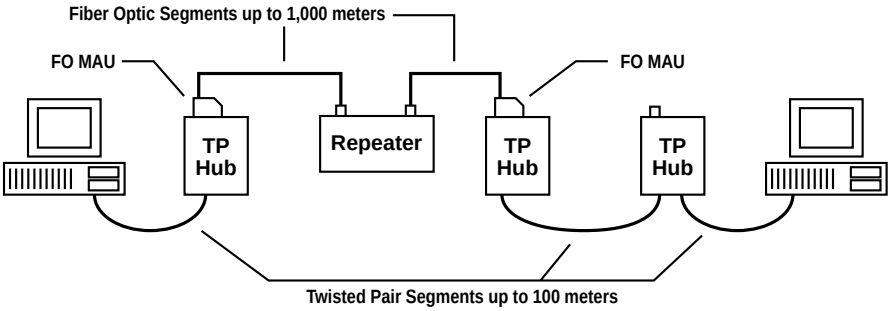


Figure 3-27. Example of Transmission Path Between Two DTEs.

3. When a network path consists of five segments and four repeaters, up to three of the segments may be coaxial and the remainder must be either twisted-pair or fiberoptic cable (link segments) (**Figure 3-30**).

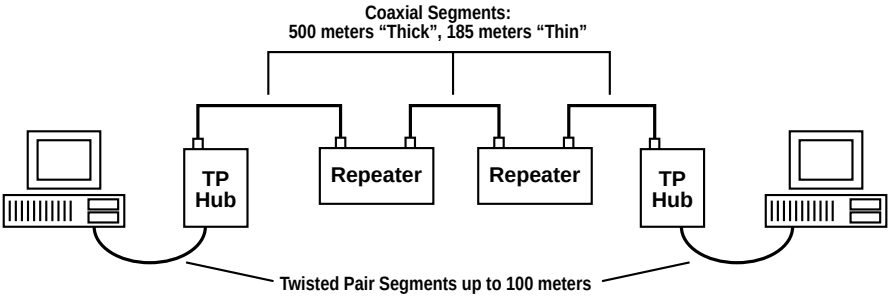


Figure 3-28. Maximum Transmission with Three Coaxial Segments.

4. When a network path consists of five fiberoptic cable segments, each segment should not exceed 1640 feet (500 meters). With four fiber optic cable segments, the maximum allowable length per segment is 3,280 feet (1,000 m) (**Figure 3-31**).

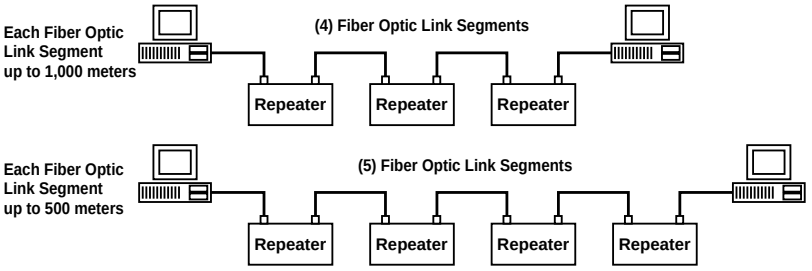


Figure 3-29. Fiberoptic Link Segment Distance Limitation.

5. For greater flexibility with coaxial cable, DTEs or repeaters (up to 100 for "thick" Ethernet, up to 30 for "thin" Ethernet) may be attached via the AUI or BNC ports to a single Ethernet backbone (**Figure 3-32**).

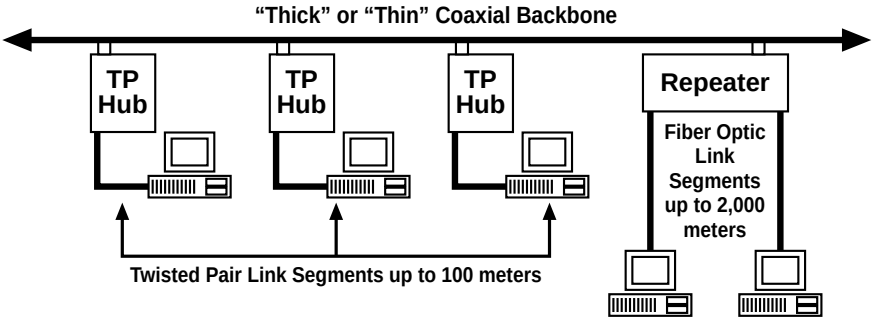


Figure 3-30. Backbone Structure.

Additional requirements for each type of cabling are given in the following sections. We recommend that you thoroughly inspect and test the cabling system before you call technical support.

3.4.3 Coaxial Ethernet Cabling

Both ends of a coaxial segment must be properly terminated. Refer to **Section 3.1.4** for more details. The terminator must match the impedance of the coaxial segment.

The coaxial cable segment must be properly grounded using grounded terminators (ordinary terminators with grounding wires attached). To use these, make sure only one of the two terminators of any LAN segment is a grounding terminator and attach the grounding wire to the grounding screw of any AC power outlet.

If grounding terminators are not available, you can ground the cable by soldering a 16 or 18 gauge insulated wire to the shield conductor on a BNC "T" connector and connecting the opposite end of the wire to the grounding screw of an AC power outlet.

3.4.4 Twisted Pair Ethernet Cabling

The TP/8 Modules with RJ-45 and Telco ports support both shielded and unshielded twisted pair cabling. No adjustments to the ports are necessary.

Twisted-pair Ethernet systems are unusually sensitive to improper cabling. You must combine high-quality wire and connectors into a cabling system meeting or exceeding the 10BASE-T specification.

The recommended twisted pair wire for the link segment is a 100-ohm unshielded 24 AWG wire or 150-ohm shielded 26 AWG. DIW is available in several sizes: 3, 4, 6, 12, 16, and 25 pairs. The cable must have at least two twists per foot.

The 10BASE-T specification does not allow the use of silver-satin flat wire (commonly found between the wall and the phone device in modular home or office telephone systems), straight patch wires, or any other cable that is not made up of at least two twisted copper pairs.

If there is unshielded twisted-pair cable already installed in offices, typically phone cabling, you may be able to use it. The existing cable must meet or exceed the IEEE 802.3 specification. In addition, it must be thoroughly tested for continuity and attenuation (no more than 10 dB at 10 MHz), visually inspected along as much of its length as possible, must not be routed near sources of electrical noise such as radio transmitters, amplifiers, motors, or fluorescent lighting fixtures, and must not run alongside power lines for great distances. These are also good recommendations for routing new cable.

3.4.5 Twisted Pair Cable Connectors

The 10BASE-T specification stipulates that the link segment terminate with a male 8-pin RJ-45 (ISO 8877) modular connector. This is different from the 6-pin RJ-11 connector commonly used in telephone applications. The corresponding female connector is defined for use at the medium-dependent interface (MDI) on the MAU itself, and is also used on many 10BASE-T repeaters.

Only two of the twisted pairs in the cable are used per link. **Table 3-5** provides the most common wire colors for pin assignments needed for straight-through link segment cables with DIW wire and RJ-45 connectors (the pin numbers correspond to those in **Figure 3-33**, and colors may vary depending on the cable manufacturer).

Table 3-5. Common Wire Colors for RJ-45 Cable.

Pin	Pair	Common Wire Colors	Function
1	2	White insulation with orange band or solid blue	Transmit +
2	2	Orange insulation with white band or solid orange	Transmit -
3	3	White insulation with green band or solid black	Receive +
4	1	Blue insulation with white band or solid red	Not used
5	1	White insulation with blue band or solid green	Not used
6	3	Green insulation with white band or solid yellow	Receive -
7	4	White insulation with brown band or solid brown	Not used
8	4	Brown insulation with white band or solid gray	Not used

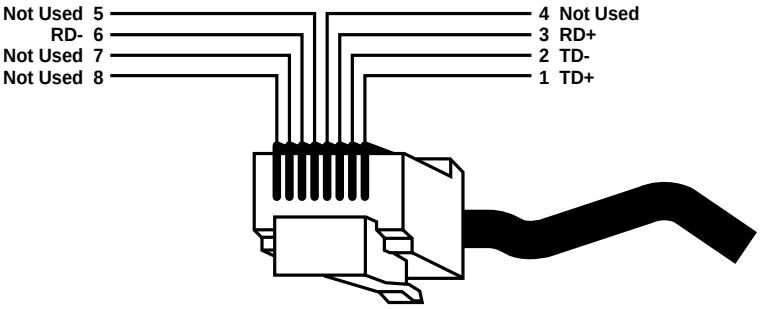


Figure 3-31. RJ-45 Connector Pin Assignments.

Most cable faults appear at the RJ-45 connector itself. Use caution when building these cables, or have them assembled by experienced professional cable installers.

Use only the highest quality connectors from reputable manufacturers. If the LAN operates erratically, wiggling the cables where they attach to RJ-45 connectors may often restore or reduce network performance, in which case you should replace the connectors.

3.4.6 Fiberoptic Cabling

You can use fiberoptic cabling to expand the reach of Ethernet LANs. 10BASE-FL/FOIRL supports cable lengths that would require repeaters or bridges with coaxial or twisted-pair cable. Because digital signals transmitted over unbroken lengths of fiberoptic cable are completely immune to RF interference, avoiding electronically noisy environments is not a factor when planning the cable installation.

Fiberoptic cable is vulnerable to signal loss and distortion from low light levels caused by excessive splices, so keep these splices to a minimum during LAN installation planning. Fiberoptic cable splicing requires special splicing equipment used by trained personnel. For these reasons, we recommend that you consult professionals experienced with fiberoptic LANs when planning and installing fiberoptic networks.

You need a fiberoptic concentrator or multiport repeater to carry the signal to multiple devices. Connect 10BASE-FL/FOIRL devices by running a fiberoptic cable from the transmit connector on one device to the receive connector of the other, and vice versa. Though not required, we recommend duplex cable (cable with one of the pair of cables marked along its length) to make installation and maintenance easier and more convenient.

The fiberoptic specifications require each fiberoptic cable segment, as installed (including splices, etc.), to have an attenuation (weakening of signal) less than or equal to 10 dB/km and a bandwidth greater than or equal to 150 MHz (referred to 1 km at a wavelength of 850 nm). You can check this using specialized fiberoptic measuring and test equipment.

The following gauges are compatible with 10BASE-FL/FOIRL:

- 50/125 µm
- 62.5/125 µm (most common)
- 85/125 µm
- 100/140 µm

The FO/4 Modules come with STII bayonet-mount connectors or SMA screw-on connectors.

3.5 Troubleshooting

The following troubleshooting suggestions may help you locate problem areas and correct difficulties. This guide assumes that the workstations and fileserver are on the same collision domain, or that a bridge, an internal fileserver bridge, and/or a router is installed for communication between different domains.

I. During initial installation, if the unit does not seem to be working properly:

A. Make sure *all* modules are correctly fitted into the concentrator. The Hub Module (HM) should slide into the slot and "click" into place (refer to **Section 3.1.2**).

B. Check that the power LED is on.

C. Make sure that the software, both for the server and workstation, is correctly installed. Making sure that communication exists between a PC and the fileserver will speed up troubleshooting procedures.

II. If the workstation will not connect to the fileserver:

A. If the LAN is running on BNC coaxial cabling:

1. Can other workstations on the *same* coaxial segment connect to the fileserver?

a. If yes, the problem is at the workstation. Refer to the documentation for the PC and Ethernet LAN card.

b. If no, and other workstations on different coaxial segments can connect to the fileserver, check the termination on the faulty segment. Both ends *must* be terminated. If the coaxial cable is connected *directly* to the BNC port, make sure the termination is ON. If the cable is connected via a "T" connector, the termination should be OFF.

If termination is set correctly, check the BNC connectors on the cable. If the connectors are not fitted correctly, the segment will not operate. Refer to **Sections 3.1.5** and **3.4** for further information on coaxial cabling.

2. Can other workstations connected to a *different* cable and *different* BNC port on the same HM connect to the fileserver?

a. If yes, the problem may be the port or the segment. Try connecting a working segment to the port in question. If it works, the problem is in the segment cable.

b. If "a" doesn't work, either the termination is set wrong, or the port is bad.

C. If the LAN is running on twisted-pair or fiberoptic cabling:

1. Is the link integrity LED for that port glowing?

a. If yes, the problem is with the workstation. Refer to the documentation for the PC and Ethernet LAN card.

Some 10BASE-T LAN cards also have a link integrity test LED. If this LED is not glowing, there is a problem with the PC or LAN card.

b. If no, the cabling could be at fault. Refer to **Sections 3.4.4** and **3.4.6** for more information on twisted-pair or fiberoptic cabling.

2. Can other workstations connected to a *different* TP or FO port on the same HM connect to the fileserver?

a. If yes, the problem may be the port or the segment. Try connecting a working segment to the port in question. If it works, the problem is in the segment cable.

b. If "a" doesn't work, either the termination is set wrong, or the port is bad.

III. General Errors:

A. Collision Domains—The number of collision domains is indicated by LEDs either on the front of the unit (Modular Concentrator/5 and Modular Concentrator/12) or the rear of the unit (Modular Concentrator/2). You set the number of domains with a DIP switch (refer to **Section 3.2**).

1. Is the concentrator configured with multiple collision domains?

a. If yes, make sure that the workstation's collision domain is connected via a bridge/router to the fileserver's collision domain.

b. If no, check the configuration as indicated in sections I and II in this chapter. If the problem persists, contact Technical Support.

B. LEDs

1. The red ERROR LED is glowing constantly.

a. This may indicate a cabling fault. Check the configuration as indicated in sections I and II in this chapter. If the problem persists, contact Technical Support.

2. The amber JAM LED is glowing constantly.

a. When the JAM LED flickers, this signifies collisions on the network. This is a common occurrence in Ethernet networks. As nodes and traffic increase on an Ethernet network, so will the number of collisions. This does not automatically mean the concentrator or the network has a problem.

If the network seems to be experiencing too many JAMs (collisions) and the performance is deteriorating, there may be too many nodes on the network, or the fileserver may be getting overloaded. There are many ways to fix this; splitting the network with bridges (internal/external) is one solution. If you need more technical advice, contact Technical Support.

4. Software Installation

4.1 HUBCTRL

4.1.1 What is HUBCTRL?

HUBCTRL (Hub Control) is a powerful, easy-to-use configuration tool that is included with SNMP-manageable Modular Concentrators.

HUBCTRL is an in-band configuration utility that lets you quickly and easily complete the first stages of SNMP configuration (setting the IP address, the subnet mask and default gateway, defining the community strings and SNMP traps).

In addition to the above functions, HUBCTRL offers an authorized IP address system and access restriction to MIB groups supported by Modular Concentrators. These extra layers of security are optional and do not affect SNMP compatibility in any way.

You can also use HUBCTRL to upload new versions of the system software and new MIB information. It also offers diagnostic capabilities so you can quickly resolve technical-support issues.

4.1.2 Hardware Requirements

HUBCTRL requires the following hardware:

- 8086 with 640K RAM (minimum)
- 3-1/2" floppy disk drive
- Ethernet NIC with Packet Driver Specification (PDS) driver
- DOS 5.0 or higher

NOTE

A CRYNWR public-domain packet driver set is supplied with all manageable Modular Concentrators. Please refer to Section 4.3 **for more details.**

4.1.3 Software Requirements

HUBCTRL is mapped directly to an Ethernet II frame, so you must load a PDS-compatible packet driver. This packet driver *must* conform to the PDS specifications.

The CRYNWR public-domain packet driver set is included on SNMP Support Disk 2 (supplied with the managed Modular Concentrator). You can use these drivers in conjunction with most Ethernet Network Interface Cards (NICs). Please refer to **Section 4.3** for further information on which NICs are supported and how to install the corresponding packet driver.

If a specific NIC is *not* listed, consult the card's documentation, or your supplier, for information on how to obtain a packet driver.

4.1.4 Transport Protocols for the Management PC

HUBCTRL does *not* use the TCP/IP transport protocol or the SNMP management protocol—it is mapped directly to an Ethernet II-type frame. Therefore, to run HUBCTRL, you do not need NMS or a TCP/IP protocol stack.

Since HUBCTRL is not reliant on a protocol (such as TCP/IP or IPX), HUBCTRL frames *cannot* be passed through a router. However, HUBCTRL frames *can* pass through a bridge, or a bridge/router (brouter). We strongly recommend that you connect the HUBCTRL PC directly to an Ethernet port within the first collision domain of the managed device.

4.1.5 HUBCTRL Overview

Transport Protocol Variables

SNMP is purely a management protocol. SNMP does *not* have a transport component. SNMP uses TCP/IP as the transport protocol for SNMP.

For TCP/IP to function correctly within the Modular Concentrator, you must correctly configure certain variables associated with the protocol:

1. You must assign a unique IP address.
2. You must set the subnet mask.
3. You must set a default TCP/IP gateway address must be set.

HUBCTRL lets you set these variables in-band, across the Ethernet cable, from *any* PC running a packet driver and HUBCTRL.

HUBCTRL Transport Protocol

HUBCTRL is a unique product that will only work with Modular Concentrators. As mentioned earlier, HUBCTRL is directly mapped to an Ethernet II frame and uses its own protocol, Hub Management Protocol (HMP).

HUBCTRL does *not* rely upon TCP/IP, so it a useful first line tool for troubleshooting. If HUBCTRL can connect to the manageable device, it proves that the manageable device is operational and that the PC and Ethernet card are also functioning correctly.

Community Definitions

After setting the variables for the transport protocol, you might need to create community strings. The community database and the community access right are always resident within the managed device. As standard, the manageable device is shipped with the community string PUBLIC pre-defined with READ/WRITE (GET, GET-NEXT, and SET) rights access to all MIB groups.

In addition to the standard GET, GET-NEXT or GET, GET-NEXT, and SET, there are three extra levels of security associated with community strings: Community View Group Assignments, IP Authentication, and IP Authentication directly related to a community string.

- MIB VIEW (Community View Group Assignments)—This limits the MIB groups that can be seen by a specific community. For example, a certain community may be disallowed access to the agent information. This would prevent the members of this community from viewing or re-configuring agent information.

- IP AUTHENTICATION—Certain IP addresses, when using a specific community string, may be given more, or less, access than other users of this community from other IP addresses. For example, members of the community EVERYONE may be given READ ONLY (r/o) rights (equivalent to the GET and GET NEXT commands). However, the IP address 192.92.192.10 may be given READ WRITE (r/w) permission (equivalent to GET, GET NEXT and SET).

- IP AUTHENTICATION AND COMMUNITIES—A community can be created that can ONLY be used by certain IP addresses. In other words, you could create the community PRIVATE that can only be used by IP address 192.92.191.1. This ties the SNMP SET command to a specific community (PRIVATE) *and* a specific IP address (192.92.191.1).

NOTE

These functions are not required to manage devices, but they do add extra security and functionality that some installations might need.

As with the community definitions, the MIB VIEW and IP Authentications are resident within the managed device. **Table 4-1** summarizes some of the possibilities associated with these commands.

Table 4-1. MIBVIEW and IP Commands.

Option	Comments	Example
Community String	Any SNMP command must be preceded by a community string. If the string is incorrect (i.e., the managed device does *not* have that community string configured), the SNMP command is rejected by the managed device.	A managed device has two community strings defined: PUBLIC and MANAGERS. If a management PC tries to manage this device using the community string GLOBAL, the command is rejected.
Access Mode	READ ONLY (R/O): GET and GET-NEXT READ WRITE (R/W): GET, GET-NEXT and SET	A community with R/O can view information from the managed device but *cannot* set information (e.g. disable a port). A community with R/W can read information and SET information. The community PUBLIC may be R/O; the community MANAGERS may be R/W (SET).

Table 4-1. MIBVIEW and IP Commands.

Option	Comments	Example
MIB VIEW	Enables/disables access to certain MIB groups.	A community EVERYONE could be setup so that access to the RMON statistics group (Ethernet statistics for the entire collision domain) is disabled.
IP Authentication	Assigns a different access mode to a community string, dependent on IP address	If a community string is used by a management station with a certain IP address, this management station may have *more* or *less* permission than another station using this management address. The community MANAGERS may be R/O, but if IP address 192.92.191.1 is used with the community MANAGERS, it will receive R/W.
IP Authentication and Communities	A community can *only* be used by a certain IP address	A certain community string can *only* be used from a pre-defined IP address. The community MANAGERS may *only* be used by the IP address 192.92.191.2.

4.1.6 HUBCTRL Installation and Set-up

After installing the packet driver, and before installing HUBCTRL, check the collision-domain setting on the hardware. If the manageable device has been configured with more than one collision domain, the PC running HUBCTRL must be attached to any Ethernet port in the *first* collision domain. For further details, or if there is uncertainty as to how the hardware is configured, refer to **Section 3.2**. Once the hardware settings are confirmed, copy HUBCTRL.EXE from the sub-directory IMC on SNMP Support Disk 1, included with the device, to the hard disk or to a working floppy disk. At the DOS prompt, type:

HUBCTRL<CR>

HUBCTRL is now installed, and the main screen will appear (**Figure 4-1**).

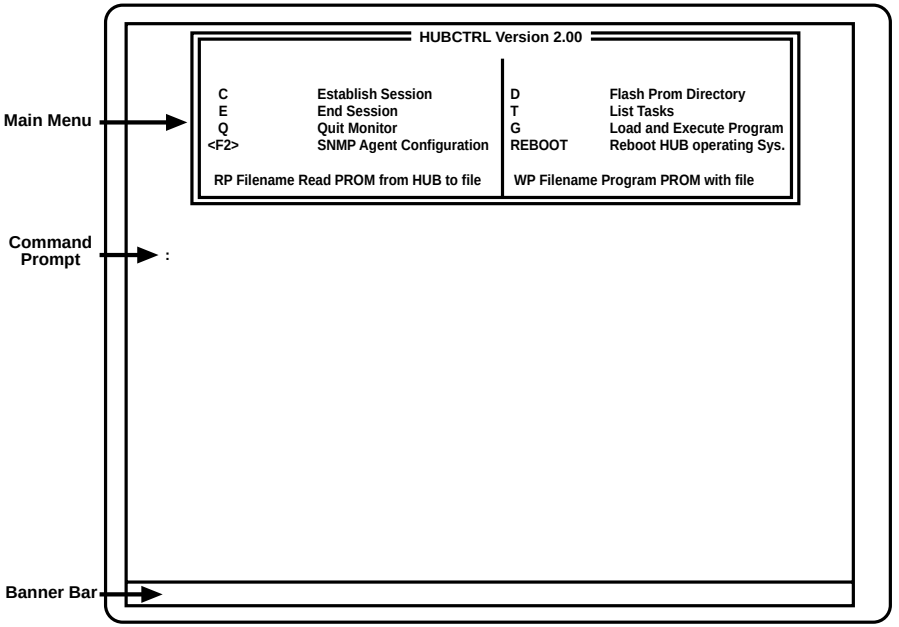


Figure 4-1. Main Menu—HUBCTRL.

4.1.7 Connecting to Manageable Devices

Once HUBCTRL is installed, and before you can configure the SNMP agent, you must establish a connection to a manageable Modular Concentrator.

When you press <C><CR>, the network will be scanned for all manageable Modular Concentrators. If only one manageable Modular Concentrator exists on the network, HUBCTRL automatically connects to this Concentrator. The message "Session Established" and the node address (MAC address) of the Concentrator will appear.

If multiple manageable Modular Concentrators exist on the network, the Connection Selection screen will appear (**Figure 4-2**). This screen lists the MAC addresses of all manageable Concentrators currently active on the LAN.

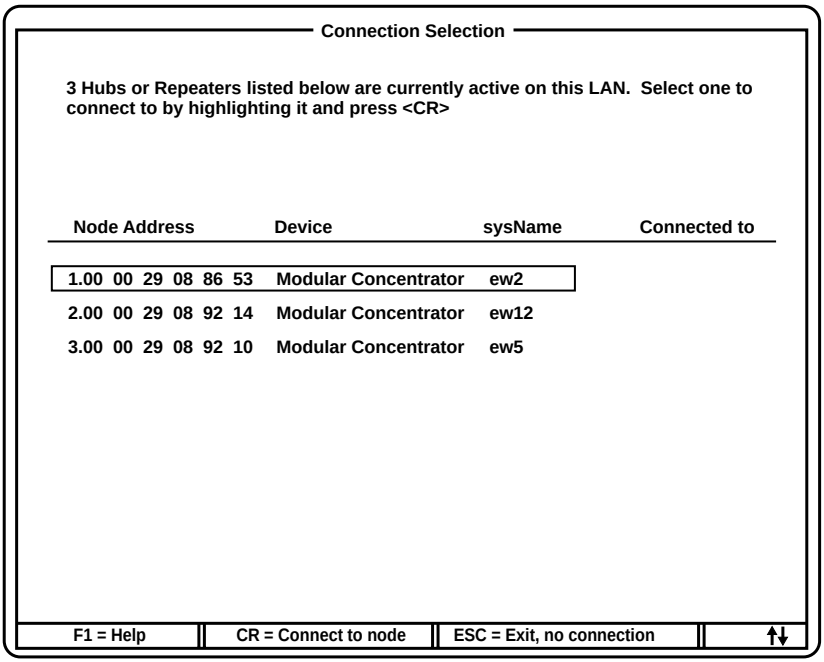


Figure 4-2. Connection Selection Screen.

Using the <ARROW KEYS>, highlight the desired device. Press <CR> to select or <ESC> to abort.

When you select a device, the main menu will appear. The message "Session Established," together with the node address (MAC address) of the selected device, will appear (**Figure 4-3**).

NOTE

The banner bar at the bottom of the screen indicates what device HUBCTRL is managing, as well as the Repeater ID (MAC address) for that device.

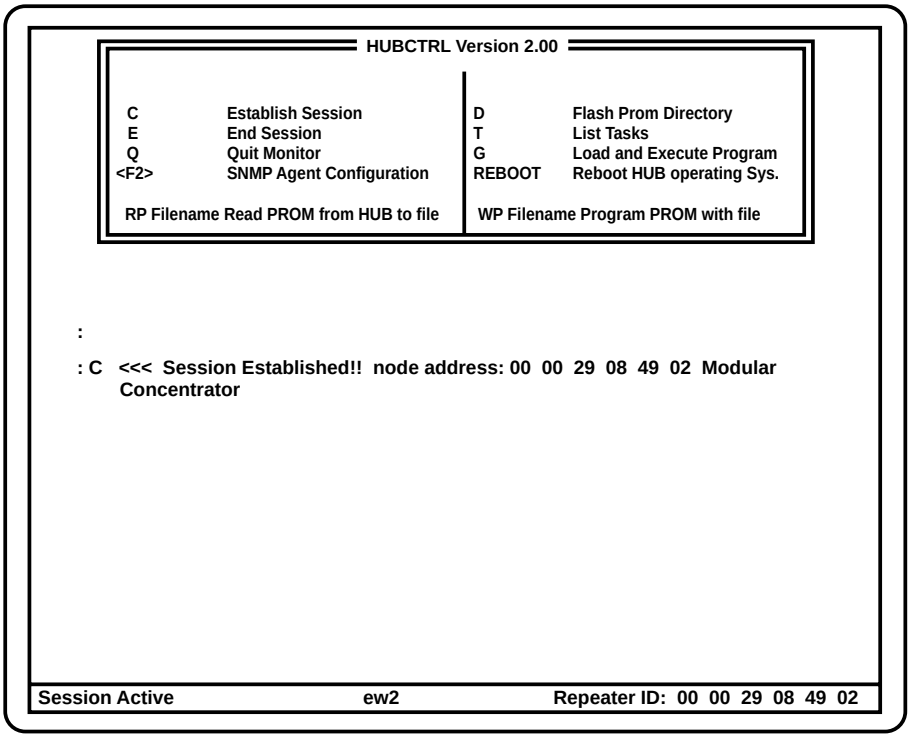


Figure 4-3. Main Menu—Session Established.

4.1.8 SNMP Agent Configuration

Once the device to be configured has been selected, press <F2>. This will access the SNMP Agent Configuration Screen (**Figure 4-4**).

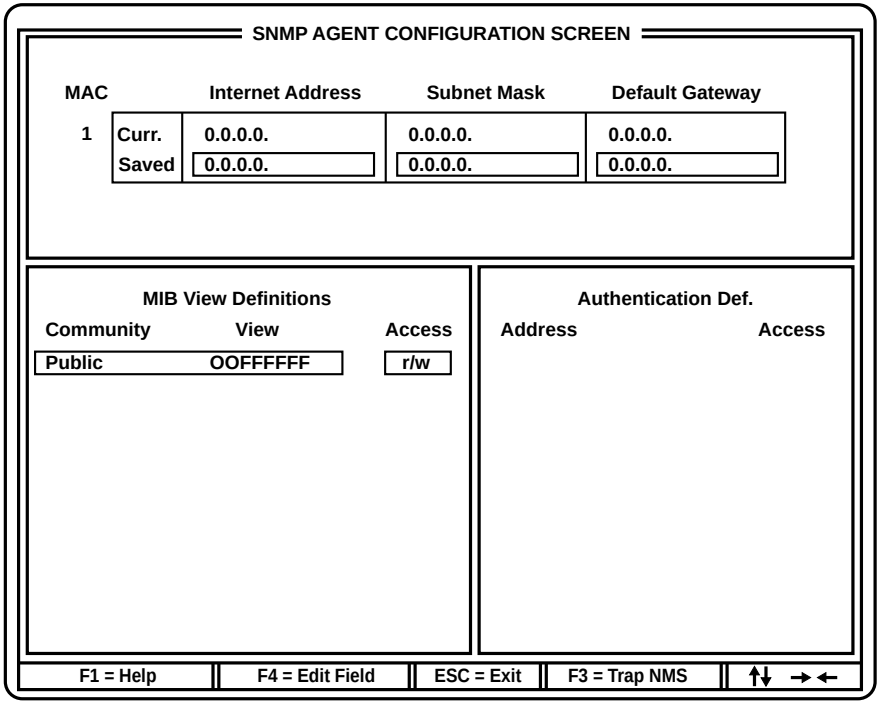


Figure 4-4. SNMP Agent Configuration Screen.

This screen is divided into three sections:

- MAC settings
- MIB View Definitions
- IP Authentication Definitions

MAC Settings

The MAC Settings section of the SNMP Agent Configuration Screen is where you set the IP address, subnet mask, and default gateway information.

The IP address, subnet mask and default gateway each have two independent fields. They are labeled:

- CURR—This lists the IP addresses which are currently in use.
- SAVED—This lists the IP addresses that are held in non-volatile RAM.

With the cursor on the Internet Address section of the screen, set the IP address by pressing <F4>. Enter the new IP address in the banner bar on the bottom of the screen. Press <CR> to enter the information, or <ESC> to cancel the operation. Once you enter the information, HUBCTRL will automatically update the SAVED list.

The procedure for setting the subnet mask and default gateway is exactly the same as setting the IP Address. Use the <ARROW KEYS> to move from field to field.

Once you complete the new settings, you must reboot the managed device for these changes to take effect.

Quit the SNMP Agent Configuration Screen by pressing <ESC>. Press <CR> to confirm the changes made to the IP information, or <ESC> to abort.

Use the REBOOT option from the main menu to reboot the managed device. Within 30 to 40 seconds, the device will be active.

Use <C><CR> to re-establish the session.

4.1.9 TRAP NMS

Traps are sent by the managed device to a management PC when a certain event takes place. To configure traps, first make sure that the SNMP Agent Configuration Screen is loaded. If not, press <F2> to load. Next, make sure the cursor is in the MAC settings section of the screen. Press <F3> and the Trap NMS Configuration Screen will appear (**Figure 4-5**).

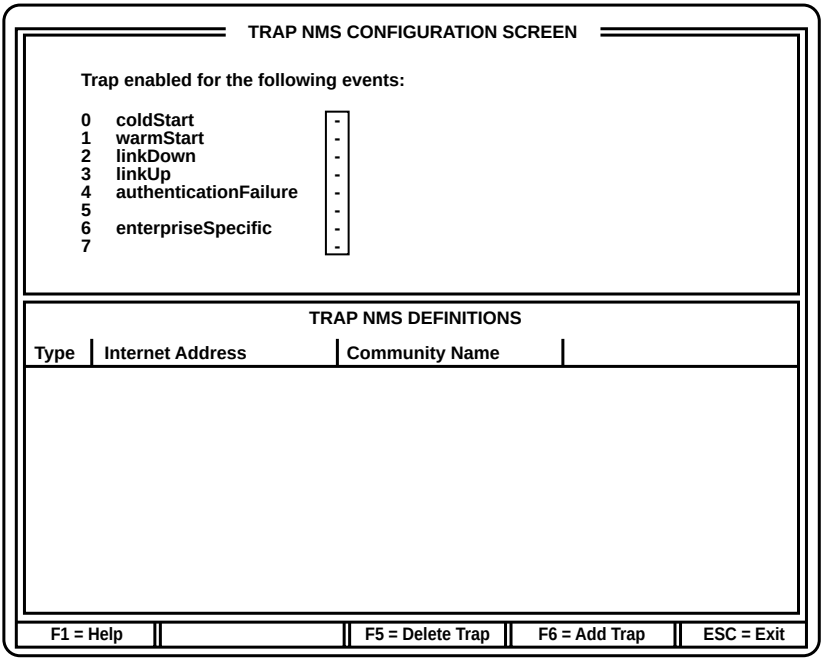


Figure 4-5. TRAP NMS Configuration Screen.

This screen has two sections. The top section lists the traps currently available, as shown below.

- 0 coldStart—If the device is cold-booted, a trap will be sent
- 1 warmStart—If the device is warm-booted, a trap will be sent
- 2 linkDown—Currently not implemented
- 3 linkUp—Currently not implemented
- 4 authenticationFailure—If an incorrect community string is used to manage the device, a trap will be sent.
- 5—Not in use
- 6 enterpriseSpecific—Traps unique to IMC Networks manageable devices. Currently not implemented
- 7—Not in use

The bottom screen, Trap NMS Definitions, is where traps are defined. The cursor will already be in this section.

To add a trap, press <F6>. A prompt for the IP address of the PC running the management software that will receive the traps will appear in the banner bar. Enter the IP address, then press <CR> to enter.

The cursor will then move to the top section of this screen. To select which traps are to be received, use the <ARROW KEYS> to move from one trap to another. Use the <SPACE BAR> to toggle between enable (+) and disable (-). When completed, press <CR> to confirm selections.

Next, a prompt will ask for the community string the managed device will use when sending a trap. Enter the community string and press <CR> to update the information.

To delete a trap, highlight the trap using the <ARROW KEYS> and press <F5> (delete trap).

4.1.10 Community Strings

Creating a new community is similar to the MAC address settings described above.

Using the <ARROW KEYS>, move to the MIB View Definitions section (**Figure 4-6**). As mentioned previously, HUBCTRL automatically sets the community as PUBLIC with READ WRITE (GET, GET-NEXT and SET) rights.

When you press <F6>, a prompt for the new community name will appear on the banner bar. Type in the new community name and press <CR>. The community name is now accepted.

NOTE

Take care when entering the community name. Community names are case-sensitive.

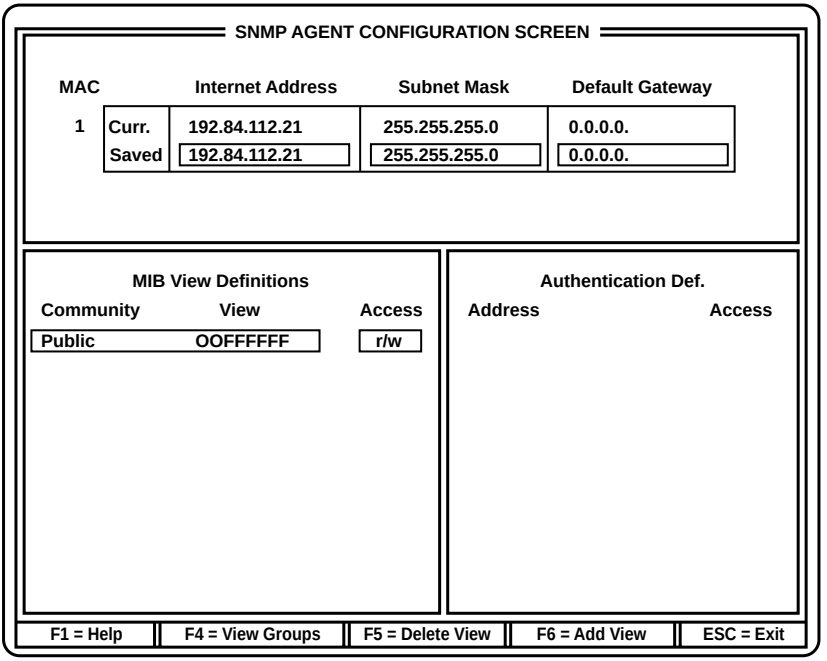


Figure 4-6. MIB View Definitions Screen.

The View Group Assignments screen will appear next (**Figure 4-7**).

This screen lists all MIB Groups available that can be viewed and edited. A (-) next to the MIB Group denotes that the community's access to this group is disabled (the default setting). A (+) denotes that the community's access is enabled.

To enable (+) or disable (-) a group use <SPACEBAR>. Using the <ARROW KEYS>, move to the next MIB Group and select +/-.

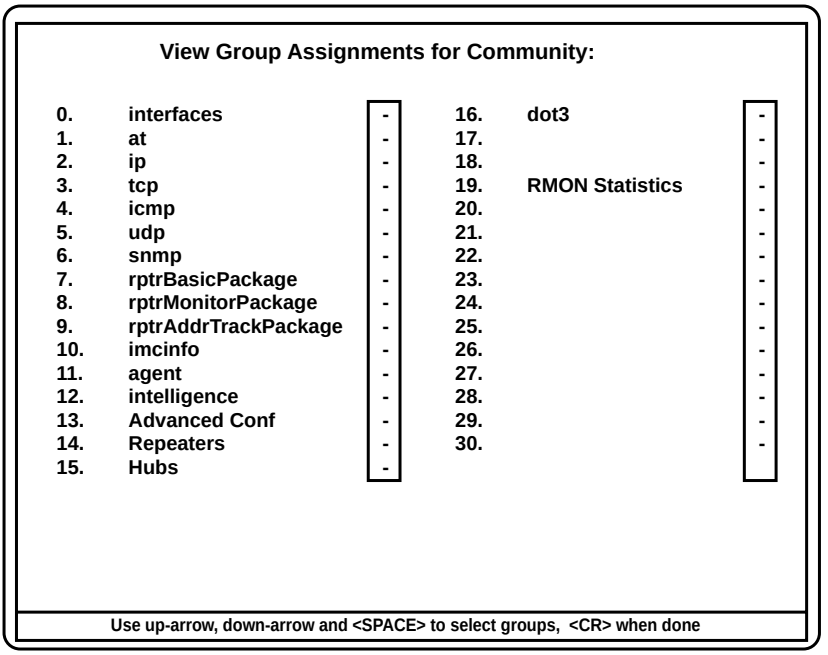


Figure 4-7. View Group Assignments Screen.

All MIB Groups that are enabled (+) will be highlighted. When completed, press <CR> to update the group assignment(s) for the community.

Once the group assignments are completed, the SNMP Agent Configuration Screen will reappear. A banner bar for selecting the Access Mode will appear at the bottom of the screen. At the prompt, select either READ ONLY (r/o) (GET, GET NEXT), READ WRITE (r/w) (GET, GET NEXT, SET), or AUTHENTICATION ENTRY (Aut.) (this community may be used only by certain IP addresses). The <SPACEBAR> toggles between the selections. To confirm the selection, press <CR>.

Next, confirm the addition of the new community by pressing <CR> to confirm, or <ESC> to abort.

On completion, the new community, its View Group Assignment (an eight digit hex number), and the access rights: r/o (GET, GET-NEXT), r/w (GET, GET-NEXT, SET), or Aut. (Authentication entry required), will be listed (**Figure 4-6**).

4.1.11 IP Authentication Definition

Certain IP addresses within a community can have different access rights. To set IP Authentication Addresses, move the cursor to the community to be changed, then press <RIGHT ARROW> (**Figure 4-8**).

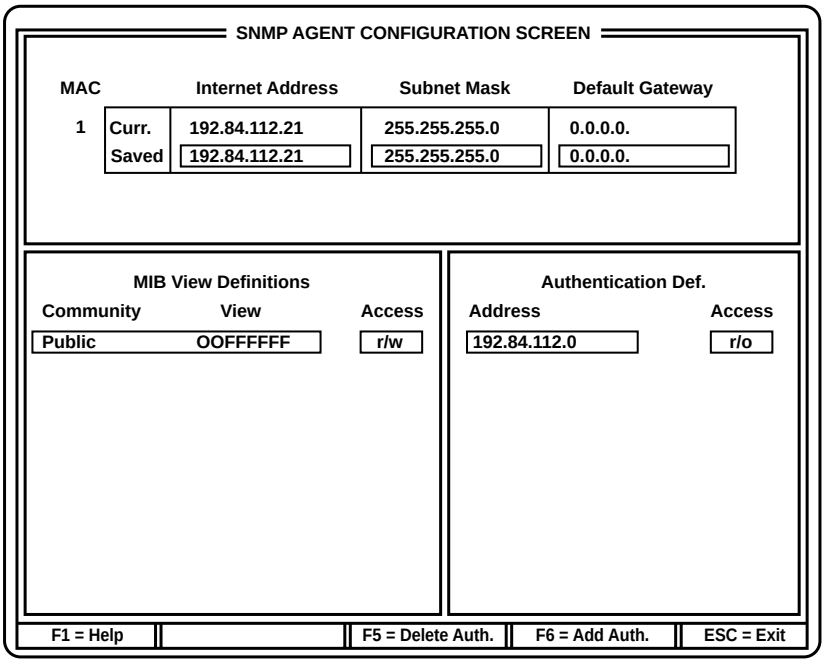


Figure 4-8. Authentication Definition Screen.

Press <F6> to add an entry. The banner bar at the bottom of the screen will ask for the community name to be added. Enter the community name and confirm by pressing <CR>, or <ESC> to abort.

The banner bar will now ask for the IP address. Enter the IP address and confirm by pressing <CR>, or <ESC> to abort.

Next, define the Access Mode using the <SPACEBAR> bar to toggle between READ ONLY, READ WRITE, and NO ACCESS. Confirm selection by pressing <CR>.

Once you complete the above steps, press <CR> to add the new entry to the hub database, or <ESC> to abort.

Repeat this process to add other IP addresses. When finished, press <ESC> to return to the main screen.

4.1.12 Other HUBCTRL Commands

You can use the remaining HUBCTRL options for these reasons:

- Uploading new releases of the SNMP Agent or MIB information, or
- Diagnostics to aid in solving problems

A brief review of these commands follows:

- **G Progname—**Loads a program from the PC into the manageable Concentrator and executes the program. This command is commonly used for loading different versions of the MIB information into the managed device. The syntax is:

  G [program name] <CR>

  For example:

  G NEWFILE.HUB <CR>

- **T List tasks—**Shows the current tasks running within the managed Concentrator, along with the task ID, priority, and size.

Task ID	Priority	Size	Task Name
37BC	02	00A1	imctask
31AB	02	00C1	mibtask

- **D (FLASH PROM Directory)—** This displays the contents of the FLASH PROM, the file name, its size, and the date/time it was created. In addition, the FLASH PROM checksum is displayed.

- **M (List Memory Blocks)—**This lists the various tasks and the memory blocks in use by these tasks.

- **RP Filenam (Read PROM)—** Makes an image on disk of the FLASH PROM in the manageable Concentrator. Once the device is configured, make a backup of the FLASH PROM information by running this option.

NOTE

Keep this file somewhere safe! *Always* run RP before using the option WP.

- **WP Filenam (Write PROM)—** Reprograms the FLASH PROM within the manageable Concentrator with a new image. As you make changes to the agent software, updates in the form of a file called PROMALL.BIN will be made available. *Do not* use this option with a new PROM image unless instructed to do so by Technical Support.

- **E (End session)—**Disconnect from the current active managed device.

- **Q (Quit Monitor)—**Exits to DOS.

- **REBOOT (Reboot the managed device)—**If you made changes to the SNMP Agent and/or MIB information, you must reboot. When you type REBOOT, the managed Concentrator goes through a cold start. After rebooting, you may re-connect the Concentrator with the ESTABLISH SESSION (<C><CR>) command.

4.1.13 Troubleshooting HUBCTRL

If HUBCTRL *cannot* load, the PDS driver is probably incorrectly installed. Please refer to **Section 4.3** for more information on troubleshooting the PDS drivers.

If HUBCTRL *can* load, but *c annot* connect to an manageable Concentrator, please check the following:

1. Make sure all cabling is correct between the PC running HUBCTRL and the manageable device. If the cable is not connected, faulty, or not terminated properly, no communication can take place between the PC and the manageable device. If using 10BASE-T or 10BASE-FL, make sure that the link LEDs are on.

2. Make sure that the PC running HUBCTRL is *not* connected to the manageable device via a router. HUBCTRL uses its own unique protocol, Hub Management Protocol (HMP), which may not be supported by the router.

3. If the manageable device is configured with multiple domains, the PC running HUBCTRL *must* be connected to the first collision domain (slot 1 on all Modular Concentrators).

4.1.14 Troubleshooting the Protocol Stack

If the CRYNWR PDS fails to load, please refer to **Section 4.3** for complete information on loading and troubleshooting the PDS.

4.2 Quick Start

4.2.1 What Is Quick Start?

Quick Start is intended to give the installer an overview of what is required to set up and manage a Modular Concentrator.

NOTE

This section deals primarily with managing a Modular Concentrator using Castle Rock Computing's SNMPc Network Management Software (NMS). Refer to Section 4.2.14 **for information on integrating the network agent with other software.**

Before you start, there are two things you must already have done:

- You must have completed th hardware installation of the Modular Concentrator. Refer to **Chapter 3** for further details.

- You must have run HUBCTRL on the Management PC to set the TCP/IP information in the Modular Concentrator (IP address, subnet mask, and default gateway). Refer to **Section 4.1** for complete information.

In addition to the above, you may need to configure extra community and trap information. Although they are not required, we recommend that you complete these stages. Refer to **Section 4.1** for details.

NOTE

"Management PC" refers to the PC that will run HUBCTRL for the initial configuration and/or where the SNMP network-management software will be installed.

To manage the Modular Concentrator, complete the following stages in the Management PC:

- Install a TCP/IP stack compatible with the SNMP network management software (NMS) you are using.
- Install the SNMP network-management software.
- Integrate the MIB into the SNMP management software.
- If using SNMPc NMS, integrate the device graphics into SNMPc.

NOTE

The PC intended for use as the Management PC must conform to the *minimum* hardware and software requirements of the management software being used.

The *minimum* requirements for SNMPc are:

Hardware:

- Intel® based 80386, 33MHz (or higher), IBM compatible PC
- 20-MB hard drive
- 8-MB RAM
- VGA color monitor and adapter
- 3.5" high-density floppy-disk drive
- Parallel port
- Ethernet NIC
- Mouse

Software:

- MS-DOS Version 3.0 or higher
- MS-Windows Version 3.1 or higher
- A TCP/IP stack compatible with the Ethernet NIC being used and with Windows 3.1 (examples: FTP, TCP/IP, Novell® LAN WorkPlace® for DOS, Beame & Whiteside)

If you are not using SNMPc, refer to the NMS supplier's documentation for the minimum system requirements.

4.2.2 Using MIB

The Modular Concentrator uses the following MIBs, which can be found in the directory \MIBFILES on SNMP Support Disk 1 (included):

- MIB-I/MIB-II—SNMP statistics, transport protocol orientated statistics (IP, ICMP, UDP, TCP), information collected on frames sent to/from the MAC interface inside the Modular Concentrator. The MAC interface is always connected to Collision Domain 1.
- RFC1398—Ethernet-specific statistics collected on traffic directed to/from the MAC interface inside the Modular Concentrator.
- RMON—Ethernet Statistics Group. Information on the Ethernet traffic (packet types, errors, packet sizes, etc.) being transmitted within Collision Domain 1. RMON provides advanced troubleshooting information.
- IEEE REPEATER—Ethernet-specific statistics collected on traffic for each repeater port as well as repeater concentrator module.
- MIB—Enterprise specific information for the Modular Concentrator. For example: port types, Hub Module types, BNC port termination settings, etc.

4.2.3 If You Are Using SNMPc

Assuming that:

- IP address, subnet mask, etc., have been set using HUBCTRL,
- the TCP/IP stack for the Management PC is installed correctly (refer to the TCP/IP documentation for information on installing the stack), and
- SNMPc has been installed (refer to Castle Rock documentation for information on installing SNMPc),

you must complete the following stages before the Modular Concentrator can be fully managed.

4.2.4 Directory Structure

Before installing any files, it is worth noting the directories used by SNMPc and Modular Concentrator devices:

- \SNMPC\HUBVIEW—This directory holds the descriptor files (*.BIT) used by BITVIEW. In addition, the file HUBNAMES.TXT is resident in this directory.
- \SNMPC\MIBFILES—This directory holds the MIB files that SNMPc uses. In addition, the file NAMES.TXT, which holds the names of the MIBs in use, is resident in this directory.
- \SNMPC\APIEXEC—The SNMPc GUI, BITVIEW.EXE, is resident in this directory.
- \SNMPC\BITMAPS—Icons associated with SNMPc.

4.2.5 Installing Networks Files

To simplify the installation of the Networks specific files within SNMPc, an automatic installation routine is provided on SNMP Support Disk 1 (shipped with the Modular Concentrator). Loading the automatic installation is as follows:

1. Go to the MS-DOS prompt.
2. Insert Disk 1 into any floppy drive, make that drive the current drive, and type the following command:

IMCINST {source_drive} {destination_directory}

For example:

IMCINST A: C:\SNMPC

The procedure should take approximately five minutes. All the necessary files for the Modular Concentrator have now been installed.

IMCINST also creates an extra sub-directory:

\SNMPC\HUBVIEW\ETHERWAY

This directory holds the bit-mapped files used by BITVIEW.EXE

4.2.6 SNMPc—First-Time Loading

From within Windows, double click on the SNMPc icon (usually in the program group Network Manager). A prompt for a password will appear. The default password is PUBLIC. You can change this password after installation. Refer to the SNMPc documentation for details.

After SNMPc is loaded, a network map appears. On the title bar of this map the legend NO-OBJECT in NOMAP should appear (**Figure 4-9**).

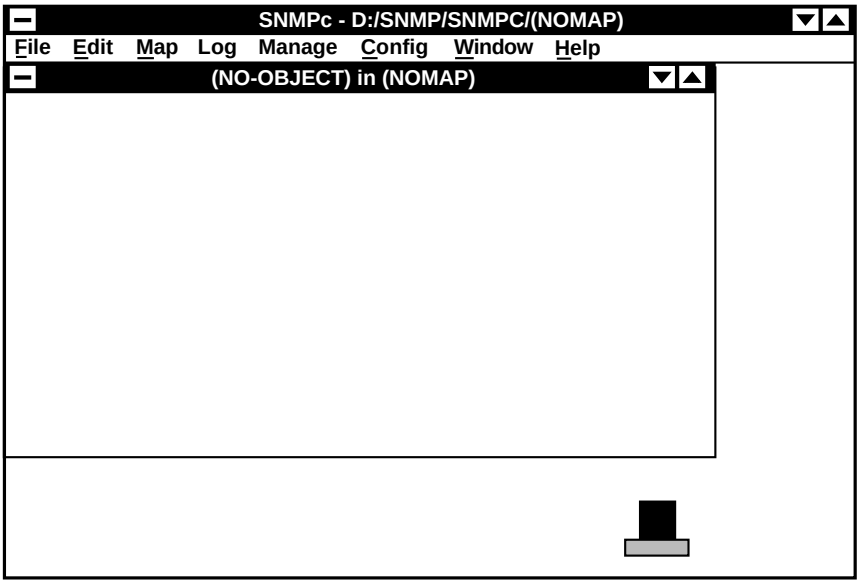


Figure 4-9. NOMAP Screen.

4.2.7 SNMPc—Compile MIB

The automatic installation routine has updated the MIB file information that SNMPc uses. For these changes to take effect, you need to recompile the MIB information.

If devices from other manufacturers are also in use, you may need to add the MIB files relevant to these devices. The names of the MIB files to be used are held in the file NAMES.TXT (\SNMPC\MIBFILES).

You can edit NAMES.TXT via Windows Notepad and add the extra MIB names. If you don't know what MIBs the other devices support, check the documentation supplied with the device, or contact the supplier.

From the menu bar, select the option Config, then the sub-option Compile MIB. At the prompt "Recompile SNMP MIB," click on the YES box.

SNMPc will now use the entries in the NAMES.TXT file to recompile the MIB information. This process should take a few minutes. On completion, the screen in **Figure 4-10** will appear.

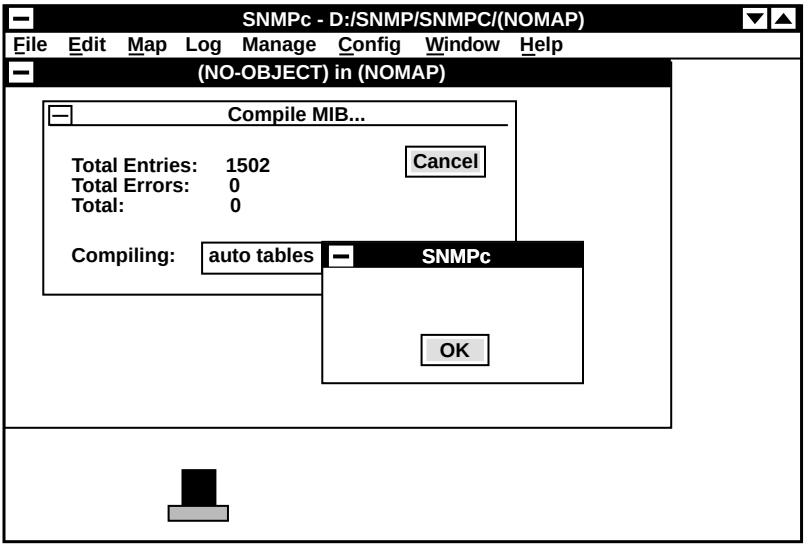


Figure 4-10. Compile MIB Window.

If the compile fails, or there are any errors, the Total Errors Field in the Compile MIB window will indicate the number of errors/ failures. A full description of what caused the error(s) will be entered in the SNMPc log called NOMAP.LOG.

To open this file, select the menu option File, then the sub-option Open Log. Select the log named NOMAP.LOG to see the error(s).

NOTE

This file is in ASCII format and can be opened and printed using Windows Notepad.

4.2.8 SNMPc—Discovering Modular Concentrators

After the above has been completed successfully, select the menu option Edit then the option Discover Nodes (**Figure 4-11**). The Auto Discovery window will open.

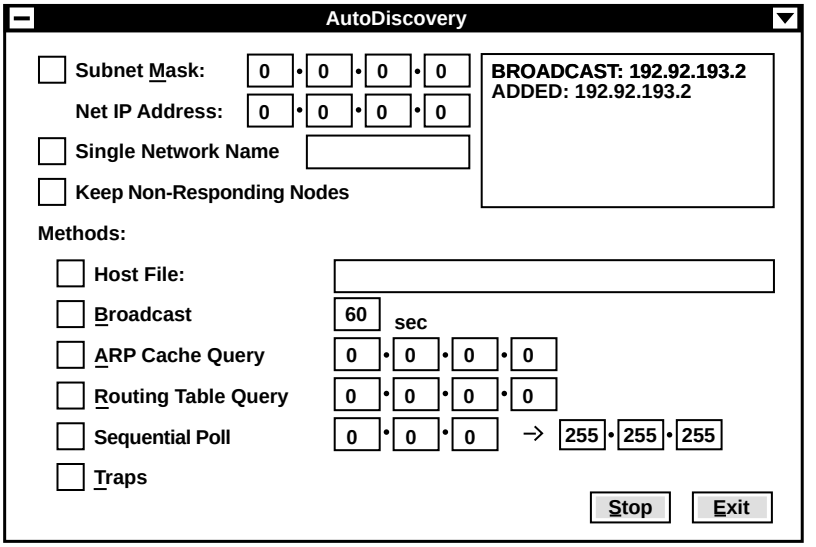


Figure 4-11. Auto Discovery Window.

Click on the Start option. SNMPc will now attempt to auto discover ALL Modular Concentrators on the network.

A small sub-window on the upper right side of the Auto Discovery window will be updated as to what devices have been discovered by SNMPc by showing the IP address of the device(s) it has found. If just a few managed devices are being used, the auto discover will take no longer than one or two minutes. The IP addresses of the Modular Concentrators should appear in the sub-window.

After all of the IP addresses of the Modular Concentrators appear in the window, click on STOP, then EXIT. An icon, or icons, with the IP address(s) of the Modular Concentrator(s) should appear on the network map (**Figure 4-12**).

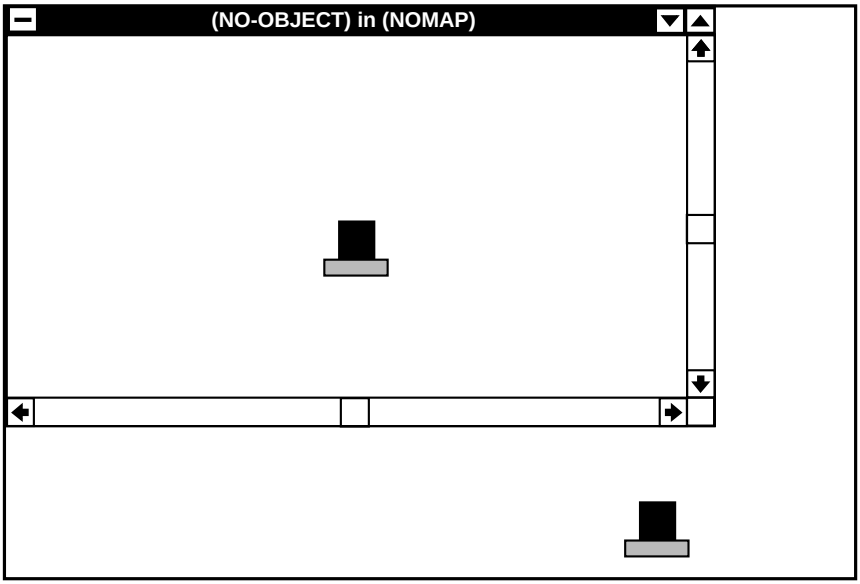


Figure 4-12. Modular Concentrator Icon with IP Address.

4.2.9 SNMPc—Edit Node

To edit a Modular Concentrator, click *once* on the icon/IP address of the device within the map to highlight it. Select the menu option EDIT. Next, select the Edit Object option (**Figure 4-13**).

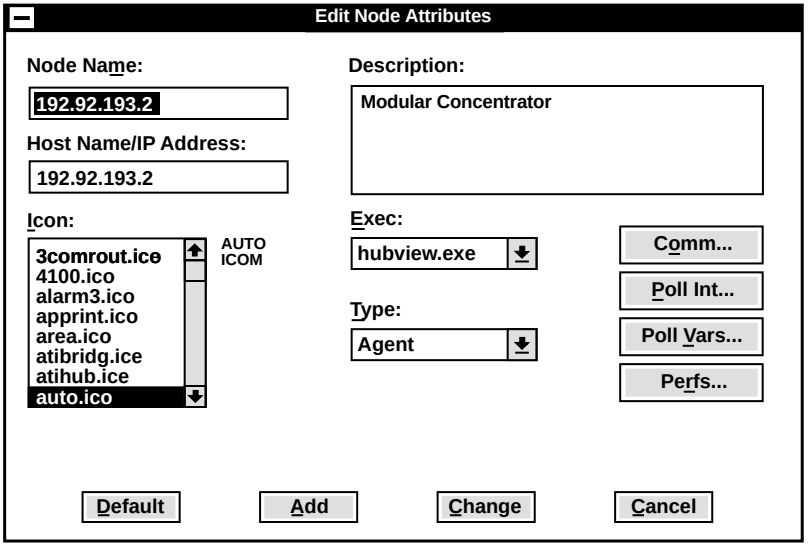


Figure 4-13. Edit Node Attributes Window.

The Edit Node Attributes window will appear. The following options need to be set:

- Node Name—This is a symbolic name within this map for the managed Concentrator, which can be set to anything desired. For example: "ModularConcentrator/12_ Main_Office" or "ModularConcentrator_5."

NOTE

No spaces are allowed.

- Icon—The icon can be changed to any one desired. For example: HUB.ICO or IMC.ICO.
- Exec—This should be changed to BITVIEW.EXE. Either type in the name or use the pull-down box.
- Comm—When you select this option, the SNMP Community Names window appears. Make sure that the communities in use for GET, SET, and TRAP are the same as were configured in the Modular Concentrator. Once the names are set, click on the OK box.
- Poll Vars—When you select Poll Vars, the Poll Variables window appears. Set the NODE IDENTIFY object to sysName.0 (**Figure 4-14**).

NOTE

"sysName.0" is case-sensitive.

Once the NODE IDENTIFY is set, click on OK.

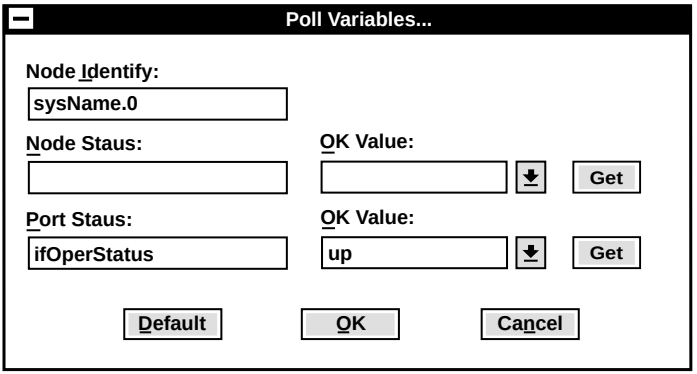


Figure 4-14. Poll Variables Window.

This will return to the Edit Node Attributes window. Click on Change. If the name has been changed, a "Change Node Name" box will appear. Click on YES to confirm the change or NO to abort.

Repeat the procedure above for all Modular Concentrators on the network.

4.2.10 SNMPc—Setting sysName.0

The poll variable sysName.0 is used by BITVIEW to load the correct graphic for the device. The sysName.0 variable and its associated graphics file are defined, and can be edited, in the HUBNAMES.TXT file.

For the GUI to work correctly, the sysName.0 variable needs to be set. For example:

sysName.0	Device
EtherWay/2	Modular Conc/2
EtherWay/5	Modular Conc/5
EtherWay/12	Modular Conc/12

To set sysName.0, highlight the Modular Concentrator to be changed. Select the menu option MANAGE, then the option **edit mib vars**. The Edit MIB Variables screen will appear.

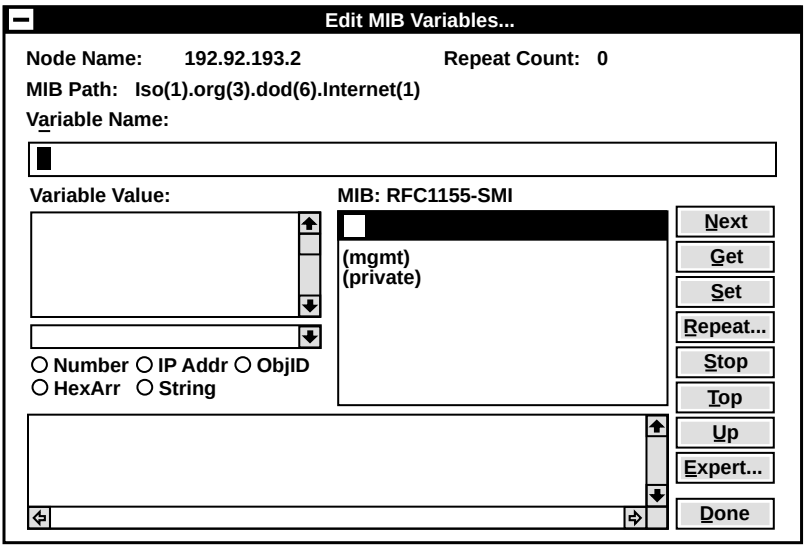


Figure 4-15. Edit MIB Variables Screen.

A sub-window on the right, entitled MIB: RFC1155-SMI, will appear (**Figure 4-15**). Double-click on the option "mgmt."

Next, double click on the option "system." A list of the managed objects within the system group of MIB-II will appear.

Click *once* on sysName, then click on the GET button.

Click once on the "Variable Value" window to activate it and enter the appropriate string. For example: If you are configuring a Modular Concentrator/5, enter the value ew5 (case sensitive). If an entry already exists and needs to be changed, delete it and enter the correct value.

Finally, click on the SET button (**Figure 4-16**).

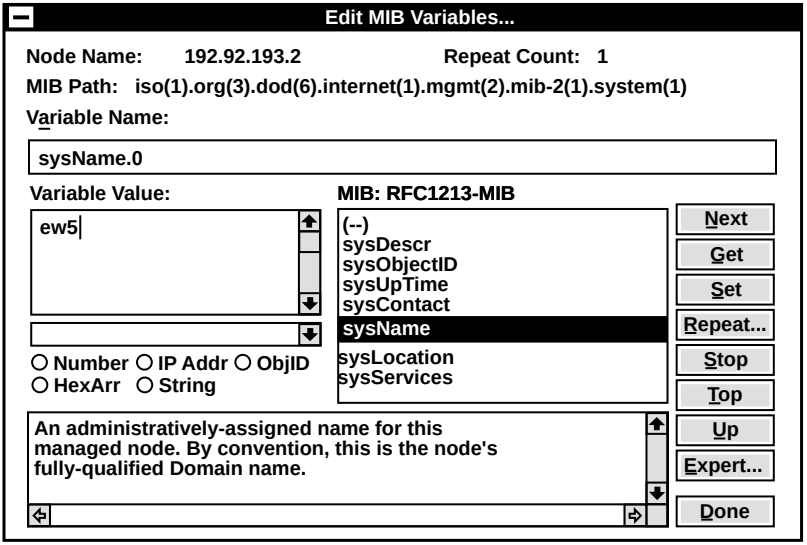


Figure 4-16. Edit MIB Variables Window.

Once the above is completed, click on the DONE button to return to the network map.

4.2.11 SNMPc—Calling the GUI

From the menu option MANAGE, click on the option "SNMP Poll." A window should open giving the following information:

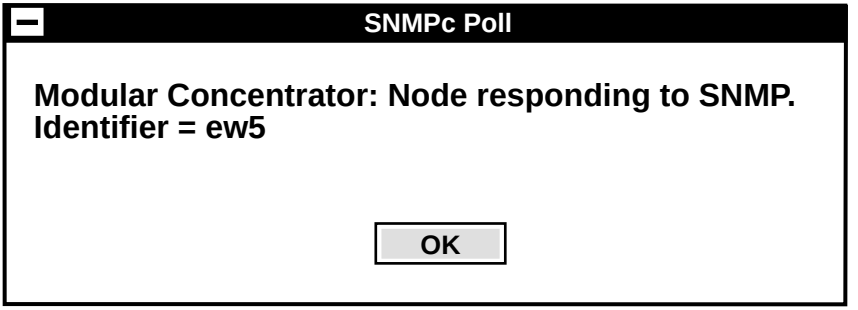


Figure 4-17. SNMPc Poll Window.

NOTE

"Identifier" should equal the value set in sysName.0.

Once you complete all of the above, double-click on the Modular Concentrator icon. BITVIEW loads and a graphic of the Modular Concentrator will appear (**Figure 4-18**).

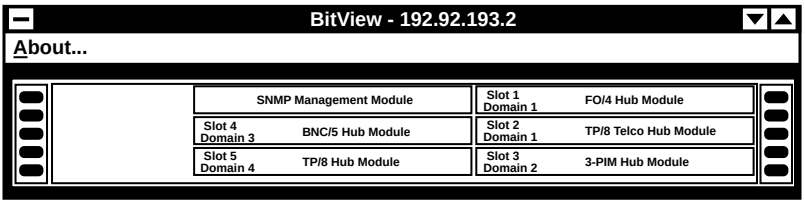


Figure 4-18. BitView Screen.

4.2.12 Check List

To ensure that the above stages have been completed, a Configuration Checklist is included in **Section 4.2.15**.

4.2.13 Troubleshooting

The following are some of the more common errors that may occur. Please review this section before contacting Technical Support.

Auto Discovery Fails

Is the Management PC connected to the *first* collision domain of the Modular Concentrator to be managed? If not, auto discovery will fail. Try to enter the IP address manually from the edit object option, then try an SNMP poll. If this fails, check which collision domain the Management PC is connected to on the Modular Concentrator.

If the TCP/IP stack on the Management PC is incorrectly configured, Auto Discovery will *not* work.

Check that the TCP/IP information held within the Modular Concentrator is correct. The IP address and subnet mask are set by using the HUBCTRL utility.

Try to enter the IP address manually from the edit object option then try an SNMP poll.

If the network portion of the IP address of the Modular Concentrator differs from the network portion of the IP address assigned to the Management PC, either you need a router or you must correct one of the two addresses for the two devices to communicate. If you use a router, make sure that the Modular Concentrator default gateway is set to reference the appropriate default router.

If Auto Discovery still fails, the TCP/IP stack may be incorrectly installed. Refer to the TCP/IP documentation for assistance.

Bitview Errors

ERROR: \SNMPC\HUBVIEW\{filename} Bad Token {path}{filename} Could not process bitmap

Are the *.BMPs in the directory \SNMPC\HUBVIEW\ MODCONC? If not, the BMPs cannot be loaded.

ERROR: Can't Open \SNMPC\HUBVIEW\{filename}

Are the IMC*.BITs copied into the directory \SNMPC\ HUBVIEW? If not, BITVIEW cannot open the file.

ERROR: \SNMPC\HUBVIEW\ default.concentrator - bad token 'MENUDEFS' on line 1

Is the Poll Var set to sysName.0? Are the entries for the Modular Concentrators in the file HUBNAMES.TXT correct?

Graphics loads, but NO Concentrator Module Information

Has the NAMES.TXT file been edited to include the correct MIB names? If not, the graphic will load, but information may be missing. Edit NAMES.TXT to read correctly then re-compile the SNMP MIB.

Re-compile of SNMP MIB Fails

Check that the entries in NAMES.TXT (\SNMPC\ MIBFILES) are CORRECT. If the compile fails with an error referencing Unresolved Object Identifier, the MIB may be corrupt. Reinstall the relevant MIB files.

TCP/IP Errors

If auto discovery fails or error messages appear referring to the TCP/IP stack when initially loading Windows, the TCP/IP stack may not be installed correctly.

Try PINGing your own IP address. If this fails, the stack may be incorrectly installed. Refer to the TCP/IP documentation for further information.

If you *can* **ping** your own IP address, try PINGing the IP address of the Modular Concentrator. If this fails, the TCP/IP information in the Modular Concentrator may be incorrect. Use HUBCTRL to check the settings.

Also, check the subnet mask in use. If this is set incorrectly, the TCP/IP stack on the Management PC or in the Modular Concentrator may be on a different subnet.

4.2.1 If SNMPc is NOT Being Used

NOTE

Installation of non-SNMPc software differs from one package to another. This section describes the steps required to integrate the Networks agent with other management software. For installation details on the management software being used, refer to the manufacturer's documentation.

The SNMP management protocol is an industry standard. Any management software that is 100% compatible with the SNMP standard can manage any device that is also 100% compatible with the same standard.

The only area where incompatibilities may occur is with the device graphics. As discussed earlier in this chapter, SNMPc provides a Graphical User Inter-face (GUI) for which we have developed graphical interface files. Other management software packages, such as HP® OpenView® for Windows, are not compatible with the SNMPc graphical files, so the Modular Concentrator's graphical files will *not* function with these other packages. The graphical files are purely a function of the User Interface provided with the software.

NOTE

This incompatibility may also occur with the same management software running on different platforms.

Although graphics are a desirable feature for viewing concentrator information, such as which concentrator modules are installed and the status of ports, you can "see" this same information by browsing the MIB information to which the management software has access.

To successfully manage a Modular Concentrator, you must integrate *all* of the MIBs mentioned in the **Section 4.2.2** into the management software. The MIBs are included on SNMP Support Disk 1 (supplied with the Modular Concentrator).

The majority of management packages have a function known as a MIB compiler. This function reads in the MIB information and converts it to machine-readable format. Refer to the management software documentation about how MIBs are integrated into the software.

You can retrieve the information held within the Modular Concentrator by using the MIB browser function of the management software. MIB browser is a generic term that applies to the function that lets you view MIB information.

In addition to integrating the MIB information, please make sure that the community strings configured in the Modular Concentrator are also the ones used by the management software. If you do not, you won't be able to SET, or retrieve, MIB variables.

Once the MIB compile is complete and the management software has "discovered" the Modular Concentrator, complete the following stages using the MIB BROWSER to ensure that the MIBs are installed correctly and the Modular Concentrator is responding to the SNMP.

1. From the SYSTEM group of MIB-I/MIB-II, GET the variable sysDescr.0. This should return the following information:

Modular Concentrator

2. From the SYSTEM group of MIB-I/MIB-II, SET the variable sysContact.0 to your name.

3. From the rptrMonitorPackage group of the IEEE repeater MIB, GET the variable rptrMonitorGroupTotalFrames.1 (within the rptrMonitorGroupInfo table). The number of frames received by the Concentrator Module in Slot 1 should appear.

4. From the Statistics group of the RMON MIB, GET the variable etherStatsPkts.1. The number of frames transmitted within the collision domain should appear.

If any of the above fails, please note the error message and the type of management software you are using, and call Technical Support for assistance.

The following files are copied from SNMP Support Disk 1 during automatic installation:

Table 4-1. Files Copied from SNMP Support Disk 1.

File Name	Destination Directory	Comment
A:\MIBFILES*.MIB	\SNMPC\MIBFILES	MIB Information
A:\HUBVIEW*.BIT	\SNMPC\HUBVIEW	Bitview definition scripts
A:\HUBVIEW\ ETHERWAY*.BMP	\SNMPC\HUBVIEW\ ETHERWAY	Bit-mapped graphics
A:\LIBS*.*	\SNMPC\LIBS	Default files
A:\BITMAPS*.*	\SNMPC\BITMAPS	Icon files

4.2.15 Configuration Checklist

Certain SNMPc specific files are modified by the installation routine. You can find backup copies of the original files in the relevant directories with the file extension .OLD. The modified files have the file extension .IMC. The files modified by the installation routine are:

Table 4-2. Files Modified by the Installation Routine.

File Name	Description
\SNMPC\MIBFILES\NAMES.TXT	Contains the names of the MIBs SNMPc will compile
\SNMPC\MIBFILES\AUTOICO.TXT	Default icons used by node discovery
\SNMPC\MIBFILES\BASIC.MEN	Basic menu accessed from the Manage menu of SNMPc
\SNMPC\HUBVIEW\HUBNAMES.TXT	Lists which .BIT is used, depending on the Poll Var
\SNMPC\LIBS\DEFAULT.TXT	Default node attributes for Auto Discover

Table 4-3. Configuration Checklist—Actions Within HUBCTRL/DOS.

Action	Comments/Examples	Completed
Modular Concentrator TCP/IP information	Refer to HUBCTRL	
Installation of PC's TCP/IP stack	Refer to manufacturer's documentation	
Installation of SNMP software	Refer to manufacturer's documentation	
Installation of IMC files	Run IMCINST from Disk #1	

Table 4-4. Configuration Checklist—Actions Within SNMPc.

Action	Comments/Examples	Completed
Load SNMPc		
Select DISCOVER NODES		
Edit Object	Set Concentrator-specific information	
Node Name	e.g. Concentrator/5_Main_Office	
Change Icon	e.g. HUB.ICO, IMC.ICO	
EXEC	Change to BITVIEW	
COMM	GET/SET & TRAP community names	
POLL VARS	Set to sysName.0	
Edit MIB VARs		
SET sysName.0	Set correct value, e.g. mc5 for Modular Concentrator/5	
SNMP Poll	Return identifier should be as above	

4.3 Packet Driver Specification (PDS)

As mentioned in **Section 4.1**, a driver compliant with the Packet Driver Specification (PDS) is required for HUBCTRL to operate. This section discusses the CRYNWR public-domain packet-driver set that is included with each Modular Concentrator.

4.3.1 CRYNWR Packet Driver Set

Included with each Modular Concentrator is a set of public-domain packet drivers: the CRYNWR packet-driver set (included on SNMP Support Disk 2). Most Ethernet NICs have a PDS driver available. Please consult the NIC documentation or manufacturer for specifics.

The CRYNWR drivers are shipped in three different files:

- PKTD11.ZIP—Executable code and information files
- PKTD11A.ZIP—The source files of the drivers
- PKTD11B.ZIP—Continuation of sources

The CRYNWR packet driver set is also available from other sources. These sources are listed in the document HOWTOGET.IT in the file PKTD11.ZIP.

Please refer to the README.PDS file on SNMP Support Disk 2 for the latest information of the CRYNWR packet driver set.

NOTE

Contact technical support for information about where to get the latest revisions of the CRYNWR packet driver set.

4.3.2 Installing the CRYNWR Packet Driver Set

Document conventions

All numbers in this document are given in C-style representation. Decimal is expressed as 11, hexadecimal is expressed as 0x0B, octal is expressed as 013. All reference to network hardware I/O addresses (source, destination and multicast) and demultiplexing information for the packet headers assumes the numbers are represented as they would be in a MAC-level packet header being passed to the send_pkt() function. Any numbers that the packet driver prints will be in the same notation.

Loading the Packet Drivers

Before installing the packet driver, you must choose an entry point (software interrupt) number, in the range from 0x60 to 0x7e inclusive.

NOTE

Some installers have reported trouble with dBase when using interrupts in the low 60's. These problems go away when they switch to an interrupt in the high 70s (e.g.: 0x7E).

Interrupt 0x67 is unavailable, because it is used by the EMS interface interrupt. Interrupts 0x70 through 0x77 are unavailable, because the second interrupt controller uses them for IRQ 8 through IRQ 15. Interrupts 0x7F and 0x80 are unavailable, because at least one package, when locating a packet driver, stops searching before 0x7F.

Running a packet driver with no specifications will give a usage message. The parameters for each packet driver are listed below.

Options

- -d—Most drivers can also be used in a PROM boot environment (see PROMBOOT.NOT in PKTD11.ZIP for how to use -d and -n options for that purpose). This switch delays the NIC's initialization until the first time you access the packet driver.
- -n—NetWare can use two different framing types on Ethernet: IEEE 802.3 and Ethernet II. The BYU packet driver shell requires Ethernet II. However, the CRYNWR packet drivers can convert Ethernet II into the Novell version of IEEE 802.3 (and back) when you use the -n switch is used.
- -p—You can achieve a certain small level of security by disabling promiscuous mode with the -p switch. Do not mistake this for real security, however.
- -w—A switch used with Windows, made obsolete by the creation of WINPKT.

NOTE

If you think you need the -w switch, or you are using it, consider using WINPKT instead. WINPKT actually solves the problem that -w only attempts to solve. You only need WINPKT (and -w) for non-resident DOS TCP stacks (e.g. NCSA Telnet, PC-Gopher, etc.).

- -i—A switch used with client software that expects to find an IEEE 802.3 packet driver. Many CRYNWR Ethernet packet drivers implement both IEEE 802.3 (class 11) and Ethernet II, aka Bluebook (class 1), framing. The packet driver specification only allows a driver to report one class. The default is to report Ethernet II. Using -i switches the reported class to IEEE 802.3.

4.3.3 Loading a Driver

- 3Com 3C501—usage: 3C501 [options] packet_int_no [hardware_irq [io_addr]]

  The 3c501 driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 3 and 0x300.

- 3Com 3C503—usage: 3C503 [options] packet_int_no [int_level(2-5) [io_addr [cable_type]]]

  The 3c503 driver requires up to three additional parameters: the hardware interrupt number, the I/O address, and the cable type. The 3c503 can be attached to thick or thin Ethernet cables, and the selection is made in software. The cable type is automatically determined at start-up, but may be forced to an external transceiver (AUI/Thickwire) by specifying zero or internal transceiver (Thinwire, 10BASE-T, or 10BASE2) or one for thin. The defaults are 2, 0x300, and 65535 (automatic). The 3c503 can use shared memory, but the driver automatically determines that parameter from the hardware.

- 3Com 3c505—usage: 3c505 [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The 3c505 driver requires three additional parameters: the hardware interrupt number, the I/O address and the memory base address. The defaults are 2, 0x300, and 0xd000.

- 3Com 3c507—usage: 3c507 [options] packet_int_no io_addr
  The 3c507 will determine its parameters by reading the NIC. The only time the parameters need to be specified is when there are multiple 3c507s in the same machine. The 3c507 driver will use three additional parameters: the hardware interrupt number, the I/O address and the memory base address.

- 3Com 3c509—usage: 3c509 [options] packet_int_no [id_port]|[io_port]| [board_num]

  The 3c509 will determine its parameters by reading the board. The only time the parameters need to be specified is when there are multiple 3c509s in the same machine, or if there is an I/O conflict with the default id_port (0x110). The 3c509 driver will use three additional parameters: the id port, the I/O address, or the board number. If the number is between 0 and 0xFF, it is the board number. If between 0x100 and 0x1FF, it is an ID port. Otherwise it is an I/O address number.

- 3Com 3c523—usage: 3c523 [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The 3c523 driver requires no additional parameters. It gets the NIC's parameters from the Micro Channel® POS registers.

- AQUILA—usage: aquila [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The AQUILA driver requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The defaults are 3, 0x360, and 0xd000.

- AT1500—usage: at1500 [options] packet_int_no [io_addr]

  The Allied Telesis AT1500 packet driver will automatically search for the NIC's I/O address. If there are two NICs being used, or the automatic search fails, the proper I/O address should be specified.

- AT1700—usage: at1700 [options] packet_int_no [io_addr]

  The Allied Telesis AT1700 packet driver will automatically search for the NIC's I/O address. If there are two NICs being used, or the automatic search fails, then the proper I/O address should be specified.

- AT&T—usage: at&t [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The AT&T® driver requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The defaults are 2, 0x360, and 0xd000. This driver supports the StarLAN 1, StarLAN 10 NAU, EN100, and StarLAN Fiber NAU.

- AT&T_LP 0x62 2 0x360 0xd000 0 0—usage: at&t_lp [options] <packet_int_no> [<hardware_irq> [<io_addr> [<base_addr> [<media_sel> [<li_enabl>]]]]]

  The AT&T_LP driver requires five additional parameters: the hardware interrupt number, the I/O address, the memory base address, media select and link integrity. The defaults are 2, 0x360 and 0xd000. This driver supports the ATStarStation, ATStarLAN 10 LanPACER+ NAU, ATStarLAN 10, LanPACER NAU, and AT Microelectronics T7231 evaluation board.

  The final two numbers are new attributes, listed below:

  0 0: This is for AUI setting

  0 1: This is also for AUI setting

  1 0: This is for TP setting, no link integrity

  1 1: This is for TP setting, link integrity enabled

  The LP NAU has no AUI port, thus 0 0 and 0 1 are invalid.

- David Systems Inc (DSI)—usage: davidsys [options] <packet_int_no> <hardware_irq> <io_addr> <delay_mult>

The DSI driver requires three additional parameters: the hardware interrupt number, the I/O address, and the delay multiplier. Delay_mult is a system-dependent timing loop used for I/O to the NIC. A reasonable value is calculated during initialization, but on some fast systems it may need to be somewhat larger. The multiplier is divided by ten, then multiplied by the calculated delay. The default multiplier is 10 (actually 1.0).

- D-Link DE-600 —usage: de600 [options] packet_int_no

  The D-Link Pocket LAN Adapter packet driver requires no additional parameters.

- Digital Equipment Corporation DEPCA—usage: depca [options] <packet_int_no> [<hardware_irq> [<io_addr> [<mem_addr>]]]

  The DEPCA packet driver requires three additional parameters: the hardware interrupt number, the I/O address and the memory base address. The defaults are 5, 0x300 and 0xd000.

  The packet driver will resolve the io_addr automatically if io_addr is set to ?' (e.g.: depca 0x7e 5 ? 0xd000). The driver requires that the jumpers be set to enable the boot PROM.

- Digital Equipment Corporation VAXMATE—usage: vaxmate [options] <packet_int_no> [<hardware_irq> [<io_addr> [<mem_addr>]]]

  The VAXMATE packet driver requires three additional parameters: the hardware interrupt number, the I/O address and the memory base address. The defaults are 2 and 0x300 and 0xd000.

  The packet driver will resolve the io_addr automatically if io_addr is set to ?' (e.g.: depca 0x7e 2 ? 0xd000).

- EtherSLIP—usage: ethersl [options] packet_int_no [-h] [hardware_irq] [io_addr] [baud_rate] [send_buf_size] [recv_buf_size]

  The EtherSLIP driver is a simulated Ethernet NIC. It appears to the application software to be an Ethernet driver, but it transmits and receives SLIP packets on the serial line.

  The parameters are as follows:

  The -h flag is included for using the hardware handshaking (the packet driver will then suspend the transmission of characters while CTS is low).

  The hardware_irq is the hardware interrupt number (defaults to 4 (COM1)).

The io_addr is the hardware I/O address (defaults to 0x3F8 (COM1)).

The baud_rate defaults to 4800 baud.

The send_buf_size and recv_buf_size default to 3000 each.

- Fujitsu® dk86960.com—usage: dk86960 [options] packet_int_no [hardware_irq [io_addr]]

  The dk86960 driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 3 and 0x300.

- Fujitsu dk86965.com—usage: dk86965 [options] packet_int_no

  The dk86965 driver requires no additional parameters. It always searches for the proper I/O address.

- HP EtherTwist®—usage: hppclan [options] packet_int_no [hardware_irq [io_addr]]

  The hppclan driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 3 and 0x300.

- IBM Token Ring—usage: ibmtoken [options] packet_int_no [adapter_no]

  The IBM Token Ring packet driver requires one additional parameter: the adapter number. The default is zero. See IBMTOKEN.DOC for more information.

- ICL EtherTeam16—usage: ETHIIE [options] packet_int_no [int_level [io_addr [cable_type]]]

  The ETHIIE driver requires three additional parameters: the hardware interrupt number, the I/O address, and cable type. The interrupt levels supported by the NIC are 5, 9 (2), 12, and 15.

  The Ethernet IIe can be attached to thick or thin Ethernet cables and the selection is made in software. The cable type parameter should be zero (0) for thick and one (1) for thin. On the Twisted Pair (TP) version of the adapter, the interface value should be set to 1 (thin).

  The defaults are 9 (2), 0x300, and 1 (thin).

NOTE

This NIC can be used only in a 16-bit slot.

- Intel® EtherExpress—usage: exp16 [options] <packet_int_no> [<io_addr>] The Intel EtherExpress packet driver has one optional parameter. The <io_addr> is only needed if there is more than one EtherExpress NIC in the computer. Otherwise, the driver will search for the NIC and get its parameters from it.

- BICC Data Networks' ISOLAN 4110 Ethernet—usage: isolan [options] packet_int_no [hardware_irq [base_addr]]

  The BICC Isolan requires two additional parameters: the hardware interrupt number and the memory base address. The defaults are 2 and 0xb800h.

- BICC Data Networks' ISOLAN 4112/3 Ethernet—usage: isolink [options] packet_int_no [hardware_irq [dma_no [io_addr]]]

  The BICC Isolan requires three additional parameters: the hardware interrupt number, the DMA channel number, and the I/O address. The defaults are 10, 0 and auto-search.

- Kodiak Raven and Kombo—usage: kodiak8 [options] packet_int_no [hardware_irq [io_addr]]

  usage: kodiak16 [options] packet_int_no [hardware_irq [io_addr]]

  usage: kodiakk [options] packet_int_no [hardware_irq [io_addr]]

  The Kodiak drivers require two additional parameters: the hardware interrupt number and the I/O address. The defaults are 2 and 0x300.

- Microdyne EXOS205T—usage: exos205 [options] <packet_int_no> [hardware_irq] [io_addr] [base_addr]

  This Packet Driver supports the EXOS205T with 256KB or 512KB RAM. It has not been tested with the old EXOS205E with 128 KB.

  The last three arguments are optional. If these are not supplied, the driver uses 0x02 0x310 0xcc00, the EXOS defaults.

  The interrupt must be set by a jumper on the NIC. The Packet Driver does not check for a valid setting. Possible values are 2 (default), 3, 4, 5, 6, 7, 10, 11, 12, 13 and 14.

Five bytes of I/O address space are used by the EXOS205. A jumper on the EXOS205 NIC sets the starting address. Possible values are 0x300, 0x310 (default), 0x320 and 0x330. The Packet Driver will fail if it does not find an EXOS205 NIC at the specified address.

The EXOS205 uses shared memory to interface the Intel 82586 Ethernet chip to the host's address space. The EXOS205 memory can be 256 KB or 512 KB. The Packet Driver uses a 16-KB window to access the EXOS205 memory. The location of this window is set by software. The following segments are possible:

0xA000 0xC000 0xC400 0xC800 0xCC00 (default) 0xD000 0xD400 0xD800 0xDC00

If a BOOT PROM is installed on the EXOS205, care should be taken to ensure that the same address is not used for the PROM and for the shared memory.

The SQE check jumper is ignored by the EXOS205 Packet Driver.

- Mitel Express—usage: express [options] <packet_int_no> [-n] [<driver_class> [<hardware_irq>]]

  The Mitel Express packet driver has one optional switch and two optional parameters. The <driver_class> defaults to SLIP and the <hardware_irq> defaults to 7.

  The -n switch instructs the NIC to be an NT. The <driver_class> should be SLIP or a number.

- MultiTech EN-301—usage: en301 [options] packet_int_no [hardware_irq [io_addr]]

  The MultiTech® driver runs the EN-301 NICs. The MultiTech driver requires two additional parameters: the hardware interrupt number and the I/O address.

- Mylex LNE-390B—usage: mylex [options] packet_int_no [int_level [io_addr [mem_base]]]
  The Mylex driver requires three additional parameters: the hardware interrupt number, the I/O address and the memory base address. The defaults are pulled out of the EISA configuration registers for the first NIC found.

- NCR ET-105—usage: ncret105 [options] <packet_int_no> <hardware_irq> <base_addr> <Ethernet_address>

The NCR® ET-105 driver requires four additional parameters: the hardware interrupt number, the I/O address, the memory base address, and the Ethernet address. The Ethernet address assigned to any particular NIC is printed on sticky labels that come with the NIC.

- NetBIOS—usage: nb [options] packet_int_no ip.ad.dr.ess [receive queue size]

  The NetBIOS packet driver transports IP packets over NetBIOS.

- Novell IPX—usage: ipxpkt [options] packet_int_no [-n [no_bytes]]

  The ipxpkt packet driver simulates Ethernet on Novell IPX protocol.

- Novell ne/2—usage: ne2 [options] <packet_int_no>

  The ne/2 driver requires no additional parameters.

- Novell ne1000—usage: ne1000 [options] packet_int_no [hardware_irq [io_addr]]

  The ne1000 driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 3 and 0x300.

- Novell ne2000—usage: ne2000 [options] packet_int_no [hardware_irq [io_addr]]

  The ne2000 driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 2 and 0x300.

- Novell ne2100 and ne1500 — usage: ne2100 [options] packet_int_no [hardware_irq [io_addr [dma_no]]]

  The ne2100 Ethernet NIC is software compatible with the ne1500 NIC. The ne2100 driver requires three additional parameters: the hardware interrupt number, the I/O address, and the DMA channel number. The defaults are 3, 0x300, and 5.

- Racal-Interlan (formerly Interlan) ES3210—usage: es3210 [options] packet_int_no [int_level [io_addr [mem_base]]]
  The es3210 driver requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. There are no defaults.

- Racal-Interlan (formerly Interlan) NI5010—usage: NI5010 [options] packet_int_no [hardware_irq [io_addr]]

The NI5010 driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 3 and 0x300.

- Racal-Interlan (formerly MICOM-Interlan) NI5210 — usage: ni5210 [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The NI5210 driver requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The defaults are 2, 0x360, and 0xd000.

- Racal-Interlan NI6510—usage: ni6510 [options] packet_int_no [hardware_irq [io_addr]]

  The ni6510 driver has two additional parameters: the hardware interrupt number and the I/O address. The defaults are 2 and auto-sense. These parameters do not need to be set unless the auto-sense routine fails or otherwise disrupts operation of the PC.

- Racal-Interlan (formerly MICOM-Interlan) NI9210—usage: ni9210 [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The ni9210 driver requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The defaults are 2, 0x360, and 0xd000.

- NTI 16—usage: nti16 [options] packet_int_no [hardware_irq [io_addr [base_addr]]]

  The nti16 driver requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The defaults are 3, 0x338, and 0xd000.

- SLIP8250—usage: SLIP8250 [options] packet_int_no [-h] [driver_class] [hardware_irq] [io_addr] [baud_rate] [recv_buf_size]

  The driver_class should be SLIP, KISS, AX.25, or a number.

  The SLIP8250 driver is not strictly an Ethernet adapter. However, some software packages (such as KA9Q's NET and NCSA Telnet) support Serial Line IP (SLIP). SLIP must be specially supported because it doesn't use ARP and has no hardware addresses assigned to its packets. The PDS is not clear on this, but the packet driver does the SLIP encoding.

The parameters are as follows:

The -h flag is included for using hardware handshaking (the packet driver will then suspend the transmission of characters while CTS is low).

The driver_class is the class that is returned to a client of the packet driver spec in the driver_info call.

The hardware_irq is the hardware interrupt number (defaults to 4 (COM1)).

The io_addr is the hardware I/O address (defaults to 0x3f8 (COM1)).

The baud_rate defaults to 4800 baud.

The recv_buf_size defaults to 3000.

- SMC (formerly Western Digital) (also IBM) SMCWD—usage: smc_wd [options] packet_int_no [-o] [int_level [io_addr [mem_base]]]

  The SMC_WD driver runs the SMC (formerly Western Digital) E, EBT, EB, ET/A, and E/A Ethernet NICs (but not the Ultra), and also runs on the IBM Micro Channel® Ethernet NICs with POS ID's 0xEFE5, 0xEFD4 and 0xEFD5.

  The ISA SMC_WD requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The ISA defaults are 3, 0x280, and 0xd000.

  The MCA SMC_WD picks up its default parameters from the POS registers, so they only need to be specified when there are multiple NICs.

  The SMC_WD NICs do not enable their memory until configuration time. Some 386 memory mappers will map memory into the area that the NIC intends to use. The software should be configurable so this area of memory will be left alone. Also, the driver will refuse to map memory into occupied memory. The occupied memory test fails on some machines. The optional switch -o disables the check.

  If the error "PROM ADDRESS Invalid" occurs, use EZSETUP to reset all the parameters (to the same values). Occasionally wayward programs will write to locations that don't belong to them. This can corrupt the EEPROM checksum on the NIC. EZSETUP will restore the correct checksum.

- Thomas-Conrad tcenet—usage: tcenet [options] packet_int_no [int_no [io_addr]]

The tcenet driver requires two additional parameters: the hardware interrupt number and the I/O address. The defaults are 3 and auto-sense.

- Tiara LANcard—usage: tiara [options] packet_int_no [hardware_irq [io_addr]]

  The Tiara driver runs both the 8- and 16-bit Tiara LANCARD/E NICs. The Tiara driver requires two additional parameters: the hardware interrupt number and the I/O address.

- Ungermann-Bass NIC-PC—usage: ubnicpc [options] <packet_int_no> <hardware_irq> <base_addr> The UB NIC-PC driver requires two additional parameters: the hardware interrupt number and the memory base address.

- Ungermann-Bass NIC-PS/2—usage: ubnicps2 [options] <packet_int_no> <hardware_irq> <io_addr> <base_addr>

  The UB NIC-PS/2 requires three additional parameters: the hardware interrupt number, the I/O address, and the memory base address. The defaults are the contents of the POS registers, so the only time the parameters would need to be used is if there are two NIC-PS/2 NICs in one machine.

- Zenith Data Systems Z-Note—usage: znote [options] packet_int_no

  The Z-Note packet driver also works on the IBM Thinkpad 300. The Z-Note packet driver has no parameters beyond the packet driver software interrupt number. It picks up its parameters from the BIOS. This driver also turns the hardware on when it starts, and off when it exits so the NIC does not need to be enabled. In fact, it should be left disabled so the power is saved when the driver is not installed.

4.3.4 Error Levels

Some of the packet drivers return error codes. Some of these error codes indicate fatal errors, and some are merely warnings. For the moment, you must consult the source to see what the error codes mean. For example, pktchk returns 0 if a packet driver exists at a given address, and 1 if not.

4.3.5 Utility Programs

CRYNWR also includes several utility programs for packet drivers:

- PKTADDR—usage: pktaddr packet_int_no [Ethernet_addr]

  If the second argument is given, the Ethernet address of the given packet driver is set. The Ethernet address is printed out.

- PKTALL—usage: pktall packet_int_no [-v] [-p] [-a et:he:rn:et:ad:dr]

  All packets are received and discarded from the given packet driver. This program is most useful with PKTMODE and TRACE.

  The -v switch causes the packet contents to be printed.

  The -p switch causes the driver to enter promiscuous mode (receives all packets regardless of destination address).

  The -a switch can filter out all but a specific address.

- PKTCHK—usage: pktchk packet_int_no [packet_int_no]

  Test for existence of a packet driver. Returns with errorlevel 0 if the specified interrupt has a packet driver. If the second argument is given, all interrupts in the range are checked for a packet driver. If no packet driver is found at all, errorlevel 1 is returned.

- PKTMODE—usage: pktmode packet_int_no [receive_mode]

  If the second argument is given, the receive mode of the given packet driver is set. A decimal number from the list of modes should be used. All the possible modes are printed out. Unimplemented modes are marked with "xx", and the current mode is marked with "->".

- PKTMULTI—usage: pktmulti packet_int_no [-f filename | address ...]

  The specified addresses are set as allowed multicast addresses. If no list of addresses is given, the current list of addresses is printed. The addresses may either be specified on the command line or in a file using the -f option. When a file is used, any white-space in the file is ignored.

- PKTSTAT—usage: pktstat first_int_no [last_int_no]

  The statistics for all packet drivers in the given range are printed. The default range is 0x60 through 0x80. The meanings of the columns are:

  pkt_in—The number of packets ever received by this driver

pkt_out—The number of packets ever transmitted by this driver

byt_in—The number of bytes ever received by this driver

byt_out—The number of bytes ever transmitted by this driver

pk_drop—Packets dropped because there was no handler for that Ethernet packet type

err_in—Dependent upon the packet driver

err_outa—Dependent upon the packet driver

- PKTSEND—usage: pktsend packet_int_no [-r] [-d delay] [-f filename | packet]

  The specified packet is sent using the specified packet driver. The -r option says to repeat sending as fast as possible. This option should not be used very often. The -d option inserts a system-dependent delay between sending packets. Without -r, the program waits for a key before sending a packet. The packet may either be specified on the command line, or in a file using the -f option. When a file is used, any white-space in the file is ignored.

- PKTTRAF—usage: pkttraf packet_int_no

  Graphically display traffic on an EGA or VGA screen. The first twenty Ethernet addresses encountered are assigned a node number. The traffic between each pair of nodes is displayed as a line of varying intensity. When any line reaches maximum intensity, the intensities of all lines are halved. A cursor highlights one of the nodes. The Ethernet address of the highlighted node is printed in the lower-right corner. The cursor is moved using space and backspace.

- PKTWATCH—usage: pktwatch packet_int_no [-a et:he:rn:et:ad:dr]

  PKTWATCH runs the driver in promiscuous mode and prints all packets received on the screen. The a- switch filters out all but a specific address.

- TERMIN—usage: termin [-s] packet_int_no

  The specified packet driver is terminated, and its memory recovered.

The s-option (stop) is used to prepare for termination. The in-use flag for all handles is cleared. This prevents upcalls to handlers that are to be removed and also makes it possible to later terminate the packet driver even though handles are not released.

- TRACE—usage: trace packet_int_no [buffer_size]

  TRACE is very useful for debugging packet driver troubles. TRACE can trace all transactions between a user program and the packet driver. The transactions are stored in a memory buffer whose size is set with buffer_size. The default size is 10,000 bytes.

  When TRACE is run, it sets itself up and then spawns COMMAND.COM, so a network program can run that uses the packet driver. After quitting the network session, issue an EXIT command. This returns to TRACE, which writes the transaction log to TRACE.OUT. The following program, DUMP, interprets TRACE.OUT.

- DUMP—usage: dump

  Interprets the contents of TRACE.OUT as written by TRACE.

- WINPKT—usage: winpkt <packet_int_no>

  Provides a packet driver interface between Windows 3 Enhanced Mode applications and a real packet driver. This attempts to solve the problem of Windows moving DOS applications around in memory "willy-nilly." It replaces the -w flag hack. WINPKT and -w are only needed for non-resident DOS TCP stacks (e.g. NCSA Telnet, PC-Gopher, etc.).

  Previous versions of WINPKT had two parameters and required different interrupts for the virtual packet driver and the real packet driver. This caused confusion when the software used the wrong packet driver. This version requires that the same packet_int_no as the existing packet driver be used.

  Install WINPKT after the packet driver and before starting Windows.

5. General Information

5.1 Technical Support

If problems occur with the Modular Concentrator, please re-check the configuration, then call for technical support. Please have the following information ready when calling:

- The product name
- A description of the problem
- A list of the corrective actions already taken

5.2 Glossary of Terms

10BASE2—The implementation of the 802.3 standard also known as ThinNet. 10BASE2 networks operate over thin coaxial cable at 10 megabits per second baseband.

10BASE5—The implementation of the 802.3 standard also known as standard Ethernet or thicknet. 10BASE5 networks run on thick coaxial cable at 10 megabits per second baseband.

10BASE-FL—The implementation of the 802.3 standard designed to operate over fiberoptic cable at 10 megabits per second baseband.

10BASE-T—The implementation of the 802.3 standard designed to operate over Unshielded Twisted-Pair (UTP) cable at 10 megabits per second baseband.

100BASE-T—A proposed update to the 802.3 standard which preserves the CSMA/CD protocol; Also known as Fast Ethernet; Designed to operate over Unshielded Twisted Pair (UTP) cable at 100 megabits per second baseband.

802.3—The numerical designation for the IEEE standard governing the use of the CSMA/CD media-access method.

Agent—All software components running within a Modular Concentrator (e.g.: the SNMP tasks, TCP/IP tasks).

ASN.1 (Abstract Syntax Notation One)—An OSI programming/description language used by SNMP to define managed objects.

Attenuation—The weakening of the signal being transmitted. It is a crucial factor in LAN design and the lengths of cable being used.

Authentication—Confirmation that a message has been transmitted correctly. For example: Is the community string, and, optionally, the IP address, correct? If one or both is incorrect, an Authentication Failure occurs.

Backbone—The primary connectivity mechanism of a hierarchical distributed system. For example, the main coaxial cable in a 10BASE5 Ethernet network.

Backplane—The bus in the back of a concentrator chassis that connects interface modules.

Bandwidth—The data-carrying capacity of a transmission medium, measured in bits per second (bps) or in cycles per second or Hertz (Hz).

Baseband—A data-transmission technique that uses the entire bandwidth of a medium without modulating a digital signal. Ethernet, Token Ring, and ARCNET use baseband transmission. The opposite is “broadband.”

BNC—A bayonet-locking connector used on 10BASE2 thinnet coaxial cabling. BNC is an acronym for Bayonet-Neill-Concelman.

Bridge—A networking device, often referred to as a MAC-level bridge, that connects local or wide-area networks using the same or different data-link layer, or Layer 2 of the OSI model, protocol. Two LANs connected in this manner effectively become one LAN.

Broadband—A data-transmission technique that allows multiple signals to share the bandwidth of a transmission media. Cable TV is a broadband transmission in that signals for multiple TV stations are carried over separate channels. The opposite is "baseband."

Bus Topology—A network architecture in which all the nodes are connected to a single cable that is terminated at each end.

Cascading—The term used to describe the connection of twisted-pair concentrators by running twisted-pair cable from one concentrator to another.

Collision—The term used when the electrical signals from two network devices run into each other, triggering a retransmission. When this is detected, retransmission is timed so a second collision is not likely.

Collision Domain—A LAN is network that spans a limited geographical area. It is further described by the IEEE as a collision domain. A collision domain is a single CSMA/CD network that may consist of two or more Medium-Access Control (MAC) sublayers. MAC sublayers separated by a repeater are in the same collision domain. MAC sublayers separated by a bridge are within different collision domains. Configuring a concentrator or repeater with separate or multiple collision domains is often incorrectly referred to as "segmentation."

Community String—A name associated with a group of SNMP-managed objects.

Concentrator—See Repeater.

Connection-less mode (CL)—A transport service that includes ALL information required. (e.g.: addressing, data transfer and control [error checking]). CL is often termed "robust."

Connection-orientated (CO)—A transport protocol with 3 distinct phases: Establish session, Transfer data, Release session.

Converter—A device that converts one media type to another (BNC to twisted pair, for example). These devices do not retime data as required by the IEEE 802.3 standard for repeater performance. Using these devices on a heavy-traffic LAN may result in excessive collisions.

CRC (Cyclical Redundancy Check)—The mathematical calculation for checking the number of errors in a message.

Crossover Wiring—A special twisted-pair cable with the transmit and receive functions of the two twisted pairs transposed on one end for connecting (cascading) twisted-pair concentrators through RJ-45 ports without the ability to disable the internal crossover function.

CRYNWR Packet Drivers—A family of public domain PDS's. The Crynwr PDS's are based on the Clarkson Packet Drivers.

CSMA/CD (Carrier-Sense Multiple Access with Collision Detection)—The network-access method used by Ethernet networks.

DCE (Data Communications Equipment)—The equipment that sits between end devices (DTE) and the network, establishing, maintaining, and terminating the connection in a data conversation. It also provides any encoding or conversion necessary via transceiver/MAU.

Default Gateway—The IP address of a gateway (usually a router) on the network.

DTE (Data Terminal Equipment)—The end point of a communications link (e.g., workstations, repeater, fileservers, printers). A DTE must connect with a DCE for data conversation.

EIA (Electronic Industries Association)—A professional organization that formulates computer and communications standards in the U.S.

EMI (Electromagnetic Interference)—Unwanted noise created by current-producing devices such as electric motors and fluorescent lights. EMI affects the quality of the signal passing through data transmission medium.

Ethernet—A 10-megabit-per-second (Mbps) baseband-type network that uses the contention-based CSMA/CD media-access method. Invented by Robert Metcalfe at the Xerox Palo Alto Research Center in the mid-1970s.

Ethernet II Frame—An Ethernet frame format defined by the IEEE. Ethernet II frames are usually associated with the TCP/IP protocol.

Fast Ethernet—A 100-megabit-per-second (Mbps) baseband-type network that uses the contention-based CSMA/CD media access method. The new method was presented to the IEEE committee for review in 1994.

Fault Tolerance—A method of making a LAN resistant to cable or hardware problems. In reference to a LAN, fault tolerance is accomplished by using a transceiver/MAU, concentrator, or multiport repeater where each segment can be isolated from others and the rest of the LAN remains up and running with no loss of data.

FOIRL (Fiber Optic Inter Repeater Link)—An early implementation of a subset of the 802.3 10BASE-FL standard designed to connect fiberoptic repeaters at 10 Mbps. This specification has been used by various Ethernet manufacturers, to produce network and port interface cards and MAUs/ transceivers.

Frame—A term applied to an Ethernet packet.

Hot-swapping—Removing and replacing a network-device interface without taking the network out of service or powering down the network device.

Heartbeat—Also known as SQE (Signal Quality Error); a test between the transceiver/MAU and the DTE to ensure that the collision-detection circuit in the transceiver/MAU is working. The heartbeat function must be disabled when a transceiver/MAU is attached to a repeater. Every time a transceiver/MAU has successfully completed a transmission, it must send the SQE to the DTE to which it is connected to confirm that the collision-detect circuit is functioning properly. This continual "pulsing" is referred to as heartbeat.

HM (Hub Module)—The basic building blocks for the modularity of the Modular Concentrator. HMs are available for 10BASE2 thin coax, 10BASE-T twisted pair, and 10BASE-FL/FOIRL fiberoptic cabling.

HMP (Hub Management Protocol)—A unique protocol that allows a PC running HUBCTRL to connect to a Modular Concentrator without using TCP/IP or SNMP.

Hub—A wiring hub or repeater that brings together the connections from multiple network nodes in a star topology. See Repeater.

HUBCTRL—In-band configuration and diagnostics software. HUBCTRL does not rely upon TCP/IP or SNMP and can be used to configure the TCP/IP and SNMP information in Modular Concentrator.

IAB (Internet Architecture Board)—The top committee of the Internet. Responsible for overseeing the IETF and IESG.

IANA (Internet Assigned Numbers Authority)—A committee responsible for assigning numbers for the Internet suit of protocol (IP addresses, enterprise specific MIBs, etc).

ICMP (Internet Control Message Protocol)—A reporting protocol for the IP component of TCP/IP. ICMP relays messages as to the status of an IP connection.

IEEE (Institute of Electrical and Electronics Engineers)—A professional organization that formulates computer and communications standards in the U.S. and works with other standards-setting bodies, including the International Standards Organization (ISO).

IEEE 802.3 Repeater MIB—The IEEE MIB for repeaters and concentrators.

IESG (Internet Engineering Steering Group)—The coordinators of IETF and standard setters for the Internet.

IETF (Internet Engineering Task Force)—A task force under supervision of the IAB responsible for answering the short-term needs of the Internet.

In-band—The technique of transmitting controlling information over the same LAN the information is controlling.

Internet—A collection of computer networks all running the Internet suite of protocols. The Internet is the basic foundation for the "information super highway." With a small "i," "internet" is a term applied to a group of interconnected networks.

Inter-Repeater Link—See "Link Segment."

IP (Internet Protocol)—A connectionless orientated protocol, offering network services.

IP Address—A unique address assigned to any device running TCP/IP.

ISO (International Standards Organisation)—An internationally recognised standards body.

Jabber—An error condition that occurs when an Ethernet network device transmits packets that are larger than the maximum allowable size.

LAN (Local Area Network)—See "Collision Domain."

Link Segment—Electronically continuous piece of a bus, consisting of the same cable with only two devices in a point-to-point configuration.

MAC (Medium Access Control)—The lower half of OSI Layer 2 that governs access to the transmission media (e.g. coaxial, fiberoptic, or twisted-pair cable); the method of determining which device has access to the Ethernet collision domain at any given time.

MAC Interface—The Ethernet interface used by the intelligence (specifically the SNMP agent) in the Modular Concentrator for communications to/from the Ethernet cable. The MAC interface in Modular Concentrators is always connected to Collision Domain 1.

Managed Object—A term applied to a unit of management information (e.g. the status of Board 1 Port 1 is a managed object).

MAU (Medium Attachment Unit)—See "Transceiver.

MDI (Medium-Dependent Interface)—The mechanical and electrical interface between the segment and the MAU.

MIB (Management Information Base)—The general term for the database of objects managed within a network.

MIB Variable—See "Managed object."

Netmask—Used by the TCP/IP protocol to decide how the network is broken up into subnetworks.

NIC (Network Interface Card)—An adapter card providing the physical connection between a computer and the network medium.

NMS (Network Management Software)—A term applied to any SNMP-compliant management software. Not to be confused with NetWare Management Services from Novell.

Node—A point in a network where service is provided, service is used, or communications channels are interconnected (e.g. a workstation, a fileserver, etc).

Nonvolatile RAM—Memory that holds its information even when main power is turned off. Usually, nonvolatile RAM is backed up via a battery.

Octet—Eight bytes make an octet. Many MIBs have a managed object for counting the number of octets received by the MAC, the port, or the index.

Out-of-band—The technique of transmitting controlling information over a separate channel to the LAN the information is controlling. This allows access to network devices even when the network is not functioning.

Packet—A collection of bits comprising data and control information, including source and destination node addresses, formatted for transmission from one node to another.

PDS (Packet Driver Specification)—A defined driver structure usually used in conjunction with a higher-level protocol (e.g. TCP/IP, HMP)

PDU (Protocol Data Unit)—A term applied to the user data and control information transmitted by an SNMP Modular Concentrator or SNMP management station.

Port—The entrance and exit point for information going into and out of a network device.

Promiscuous Mode—The MAC interface on the device will record/capture *all* packets on the collision domain, regardless to the fact that the packet may not be destined to this MAC.

Protocol—A standardized set of rules specifying the packet format, timing, sequencing and/or error checking for data transmission.

Protocol Stack—Several protocols that are stacked on top of each other to form a layered structure in which each protocol utilizes the services provided by the layer below and provides services to the layer above.

Repeater—A device that regenerates and amplifies signals to extend transmission distance. It also links multiple segments of an Ethernet network in either a bus or star topology. Fully 802.3-compliant repeaters regenerate and retime the signal of each packet of information and automatically partition and isolate faulty segments when collisions occur on the network. Repeaters, concentrators, and concentrator all technically perform the same basic function.

RFC (Request For Comment)—A document describing an Internet protocol (e.g., RFC1155 is the core document for SNMP).

RFC1155 SMI—Structure and identification of Management Information. The core RFC for SNMP compliant devices.

RFC1157 SNMP—Definition of the SNMP command set and PDU.

RFC1212 Concise MIB definition—The RFC outlining how MIBs should be structured.

RFC1213 Management Information Base II—The Internet Standard MIB. The minimum MIB requirement in order to be called SNMP-compatible.

RFC1271 RMON MIB—Remote MONitor MIB. A MIB designed for monitoring and diagnosing traffic on a collision domain.

RFC1398—MIB for Ethernet-like interfaces.

RFI (Radio Frequency Interference)—Unwanted noise created by current-producing devices such as electric motors and fluorescent lights. RFI affects the quality of the signal passing through some data transmission medium.

Router—A device that provides intelligent connections between networks. Routers operate at the network (Layer 3) layer of the OSI model and are responsible for making decisions about which paths through a network the transmitted data will use.

RS-232C—An EIA standard definition for the 25-pin interface linking DTEs and DCEs. RS-232C is suitable for both synchronous and asynchronous communications.

RS-422—An EIA recommended standard definition for extending the RS-232C interface beyond the 50-foot limit.

RS-485—Similar to RS-422 but used in multipoint applications where up to 64 network devices may be interconnected.

Segment—An electronically continuous portion of a network, usually consisting of the same coaxial cable with multiple devices attached.

SGMP (Simple Gateway Monitoring Protocol)—The forerunner of SNMP. SGMP was developed by the Internet community to manage the gateways which provide access to the Internet.

SNMP (Simple Network Management Protocol)—The protocol governing network management and monitoring of network devices and their functions.

SNMPv2—Version 2 of the SNMP Protocol. The next release of SNMPv2 adds extra security, commands, and statistics.

Socket—A unique number defined by the TCP/IP protocol indicating what type of services or packet the frame is composed of (e.g., socket 161 is a UDP/SNMP socket).

SQE (Signal Quality Error)—Also know as heartbeat, a test between the transceiver/MAU and the DTE to ensure that the collision detection circuit in the transceiver/MAU is working. The heartbeat function must be disabled when a transceiver/MAU is attached to a repeater. If a transceiver/MAU, while transmitting, detects a collision, the transceiver/MAU sends the SQE signal to the repeater, or node, to which it is connected.

Star Topology—A network architecture in which nodes are connected to a central device such as a concentrator or concentrator.

STP (Shielded Twisted Pair)—Twisted-pair cable with metal-backed Mylar, plastic, or PVC covering to protect the cable from EMI and RFI. STP cable offers better noise protection than UTP (Unshielded Twisted Pair) cabling.

Subnet—A physically distinct network identified by its IP address.

Subnet-mask—A 32-bit number used by IP to identify subnets.

Subnet-number—The part of the IP address which identifies a certain subnet.

TCP (Transmission Control Protocol)—A connection-oriented transport protocol.

TCP/IP (Transmission Control Program/Internet Protocol)—A general term applied to the transport suite developed by the Internet.

Transceiver—Also known as a MAU (Medium Attachment Unit), and not to be confused with a Token Ring MAU (Media Access Unit). An Ethernet device for transmitting and receiving data that provides data packet collision detection as well. It can either be an internal or external feature of a network device such as network interface card, repeater, concentrator or concentrator. Internal transceivers are built into the device; external transceivers usually plug directly onto the AUI port of the device. A multiport transceiver allows a number of computers or workstations to be attached to a single connection on the Ethernet bus, and each port performs the standard transceiver functions.

UDP (User Datagram Protocol)—A connectionless-oriented transport protocol. UDP is the transport protocol used by SNMP.

UTP (Unshielded Twisted Pair)—Cabling with insulation material like that commonly used with telephone cabling but without a covering to protect it from EMI and RFI. The cable consists of at least two conductors twisted together six twists per inch to minimize the effects of electromagnetic radiation.

Wiring Closet—Central location for terminating and routing onsite wiring systems.

NOTES

NOTES

NOTES

NOTES

NOTES

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