WIRELESS COMMUNICATIONS

PINNACLE LINK 2/E IP Router

The Pinnacle LINK 2/E wireless ethernet IP Router is capable of connecting two or more remote Ethernet LANs at speeds of 2MBPS at distances up to 10 miles. With 2MBPS speeds Pinnacle LINK 2/E obsoletes traditional slower telco T1 wireline solutions. Pinnacle LINK 2/E provides higher performance, without the expense of recurring monthly line charges! Pinnacle LINK 2/E works in conjunction with all wired ethernet networks, including BNC coaxial and twisted pair 10BaseT, making it the ideal solution for metropolitan area networking.

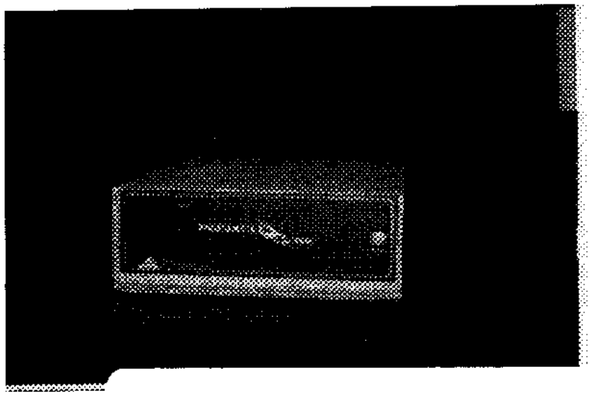
Pinnacle LINK 2/E uses proven spread spectrum radio technology that provides reliable data transmission, evidenced by the thousands of installed units using this technology. Pinnacle LINK 2/E uses the 902-928 MHz or 2.4 GHz spread spectrum radio frequency for transmission which means there are NO FCC licensing requirements to be concerned with. The Pinnacle LINK 2/E supports all ethernet and ethernet like protocols making the Pinnacle LINK 2/E easy to integrate into your existing network.

Pinnacle LINK 2/E supports point-to-point or multipoint configurations. In multipoint configurations a centrally located "hub" station communicates with multiple satellite buildings to form a cell. Each location within that cell has the capability of communicating with the hub site. Multiple cells can be interconnected utilizing any of the Pinnacle wireless solutions yielding infinite wireless networking possibilities.

Installation is easy with the Pinnacle LINK 2/E wireless ethernet IP Router. Install the antenna outside and run the coax cable to the Pinnacle LINK unit located inside. The indoor unit is then connected to your LAN via BNC, AUI, or 10BaseT cable.

Pinnacle LINK 2/E IP Router Features

- *Wireless data rates up to 2 MBPS*
- *Point-to point wireless links up to 10 miles*
- *Multipoint configurations using hub station for campus area networks*
- *Industry standard 902-928 MHz or 2.4 GHz spread spectrum radio*
- *NO FCC license required*
- *Immune to environmental interface like rain or snow*
- *DES encryption*
- *SNMP management*
- *Supports all major ethernet protocols*
- *NO monthly recurring line charges*
- *Supports IEEE 802.3 Ethernet Protocols, IEEE 802.1 d transparent MAC layer bridging and RFC compliant IP routing*
- *Directional or OMNI directional antenna kit. (Antenna, Cable, Lighting Arrestor)*
- *One year warranty with free telephone support*



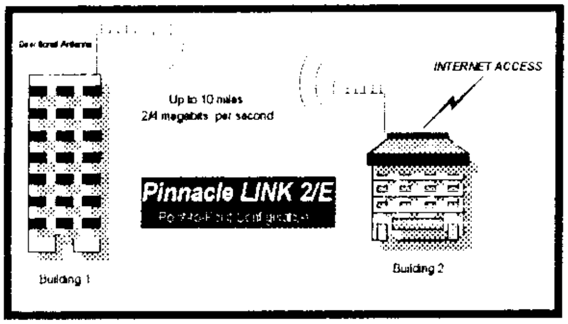
FCC ID: NSU EIPRTR

PINNACLE
COMMUNICATIONS
INCORPORATED

1403 Business Center Court • Dayton, Ohio 45410
Voice: 937.254.0141 • Fax 937.254.0156

OPTIONAL FEATURES

- *Antenna Mounting hardware*
- *Full featured installation and set-up utility*
- *Fiber optic ethernet interface*
- *Low loss Antenna Extensions*
- *4 MB full duplex upgrade kit*
- *14 dBi Yagi Directional Antenna*
- *23 dBi Parabolic Directional Antenna*
- *6 dBi OMNI Directional Antenna*
- *15 dBi Quad Array High Gain Antenna*
- *LINKamp Amplifier card*



SPECIFICATIONS

- ***Power 90 - 132 vac 200-235 vac 47-63 Hz***
  100 Watts Minimum
- ***Temperature: 5° to 40°C / 40° to 105° F***
- ***Humidity: 20%-80%***
- ***Dimensions: 6" H x 16" x 14.25" W***
- ***Frequencies:***
  902 - 928 MHz Spread Spectrum
  2.4 - 2.45 GHz Spread Spectrum
- ***MAX Power output: <4 watts ERP***
- ***Ethernet Connections: AUI, BNC, 10BaseT***
- ***Power Cord Connector: NEMA 515***

ORDERING INFORMATION

Product Code	***Product Description***
PL2RTR-0001	***Pinnacle LINK 2/E (915 MHz, Dir)*** ***2 Mbps Ethernet IP Router Kit***
PL2RTR-0002	***Pinnacle LINK 2/E (915 MHz, OMNI*** ***2 Mbps Ethernet IP Router Kit***
PL2RTR-0003	***Pinnacle LINK 2/E (2.4 GHz, Dir)*** ***2 Mbps Ethernet IP Router Kit***
PL2RTR-0004	***Pinnacle LINK 2/E (2.4 GHz, OMNI)*** ***2 Mbps Ethernet IP Router Kit***
PL2/RB-0001	***Pinnacle LINK 2/E*** ***2 Mbps Ethernet Roaming Bridge Kit***

This manual covers
Pinnacle Link Bridge and Pinnacle Link Router
Software Version 2.0

PUBLISHED BY
Pinnacle Communications, Inc
1403 Business Center Ct.
Dayton, OH 45410
(937) 254-0141

Revised 1-13-97

FCC Statement (For U.S.A. Only)
Federal Communications Commission Radio
Frequency Interference Statement

Warning: This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when 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 required to correct the interference.

If this equipment causes interference to radio reception (which can be determined by unplugging the power cord from the equipment) try these measures: Re-orient the receiving antenna. Relocate the equipment with respect to the receiver. Plug the equipment and receiver into different branch circuits. Consult your dealer or an experienced technician for additional suggestions.

Software License Agreement

Introduction: It is important for Users of Pinnacle Link Software to take time to read this License Agreement associated with this software PRIOR TO ITS USE. The End User has paid a License fee to Pinnacle Communications, Inc. for the use of this software on one computer. This License does not extend to any copyrights to the program nor does it License use of the program on more than one computer no to make copies of the program for distribution or resale. A software registration card is located in the front of this manual. Please complete the card within 10 days of receipt of the software and return it to Pinnacle Communications, Inc. hereafter in this License Agreement, Pinnacle. Registration is required for warranty service and notification of software updates and revisions.

License Agreement: The End User is granted a non-exclusive License to use the Licensed program on a single computer subject to the terms and conditions as set forth in this agreement. The End User may not copy, modify or transfer the reference manual or other documentation or any copy thereof except as expressly provided in this agreement.

The copyright and all intellectual / industrial rights of this program and associated material remain the property of Pinnacle Communications, Inc. THE END USER MAY NOT USE, COPY, SUBLICENSE, ASSIGN OR TRANSFER THE LICENSED MATERIALS OR ANY COPIES THEREOF IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS LICENSE AGREEMENT. The End User shall not reverse assemble or reverse compile the Licensed product or any copy thereof in whole or in part.

Upgrades and Revisions: At its sole option and discretion, Pinnacle may from time to time make available for licensing to the End User, in consideration for the payment of an additional fee specified by Pinnacle, future updated versions of the Licensed product. Also, at its sole discretion, Pinnacle may from time to time make available for licensing to End Users, free of charge, revisions to the Licensed product.

Warranty and Liability: Pinnacle warrants to the end user/purchaser, that this product will be free from defects, under normal use, in materials and workmanship under normal user and service for a period of one year from the date of original purchase. Pinnacle agrees under this warranty, at its sole option, to repair, replace, or refund the purchase price of any product discovered to be defective during the warranty period. Any such replacement may be, at the sole option of Pinnacle, a new or a re-manufactured product.

Pinnacle has made a good-faith effort to ensure that the firewall security filters are implemented in the best way possible. The user/purchaser is solely responsible for ensuring that all firewall security filters are setup correctly and functioning correctly.

This warranty shall not apply to any product that has been modified without written approval of Pinnacle, abused, misused, tampered with, damaged by other equipment or systems, or operated or stored under adverse environmental conditions.

EXCEPT AS EXPRESSLY SET FORTH ABOVE, PINNACLE MAKES NO OTHER WARRANTIES OR REPRESENTATIONS, EITHER EXPRESSED OR IMPLIED (INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE). PINNACLE EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED HEREIN. YOU ASSUME THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PRODUCT. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS WHICH MAY VARY FROM STATE TO STATE.

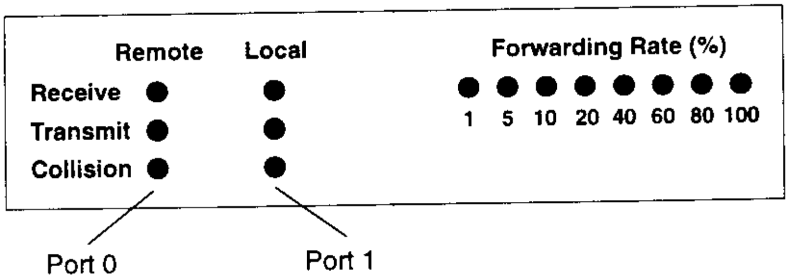
LIMITATION OF LIABILITY

YOUR SOLE REMEDIES AND PINNACLE'S AND ITS SUPPLIERS, DISTRIBUTORS, RESELLERS, AND AGENTS ENTIRE LIABILITY ARE SET FORTH ABOVE, IN NO EVENT SHALL PINNACLE OR ITS SUPPLIERS, DISTRIBUTORS, RESELLERS, AND AGENTS BE LIABLE TO YOU, OR ANY OTHER PERSON, FOR ANY DAMAGES, INCLUDING ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, LOST SAVINGS, COST OF REPLACEMENT, OR OTHER EXPENSES ARISING OUT OF THE USE OR INABILITY TO USE THIS PRODUCT, EVEN IF KARLNET HAS BEEN ADVISED OF SUCH POSSIBLE DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. SOME STATES DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

For product returns, please call Pinnacle Communicatons, Inc. (937) 254-0141.

Hardware Information

FRONT PANEL (ETHERNET-TO-ETHERNET)



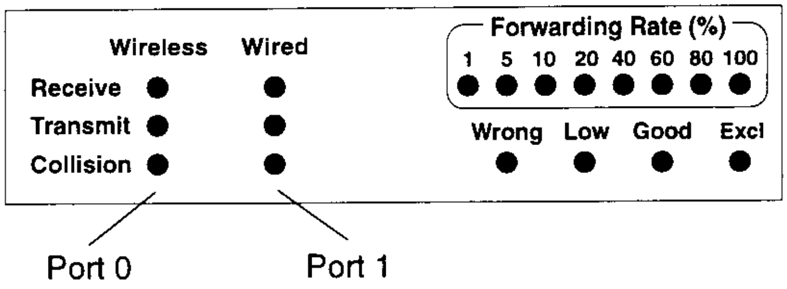
Receive: This light will blink whenever a packet is received.

Transmit: This light will blink whenever a packet is transmitted.

Collision: This light will blink whenever a collision or error is detected on the LAN.

Forwarding Rate: This will display the forwarding rate of the bridge/brouter in percent of the full theoretical Ethernet rate of 10 megabits per second.

FRONT PANEL (ETHERNET-TO-WAVELAN)



Wired Receive: This light will blink whenever a packet is received.

Wired Transmit: This light will blink whenever a packet is transmitted.

Wired Collision: This light will blink whenever a collision or error is detected on the LAN.

Wireless Receive: This light will blink whenever a packet is correctly received.

Wireless Transmit: This light will blink whenever a packet is transmitted

Wireless Collision: This light will blink whenever a packet is retransmitted (packets will only be retransmitted if the CellWave algorithm is being used).

Forwarding Rate: This will display the forwarding rate of the bridge/brouter in percent of the full theoretical Ethernet rate of 10 mega bits per second.

Wrong: This light will blink whenever a packet from another WaveLAN network is detected.

Low: This light will blink whenever a CellWave "hello" packet is received with a low signal to Noise Ratio.

Good: This light will blink whenever a CellWave "hello" packet is received with a good signal to Noise Ratio.

Excl: This light will blink whenever a CellWave "hello" packet is received with a high signal to Noise Ratio.

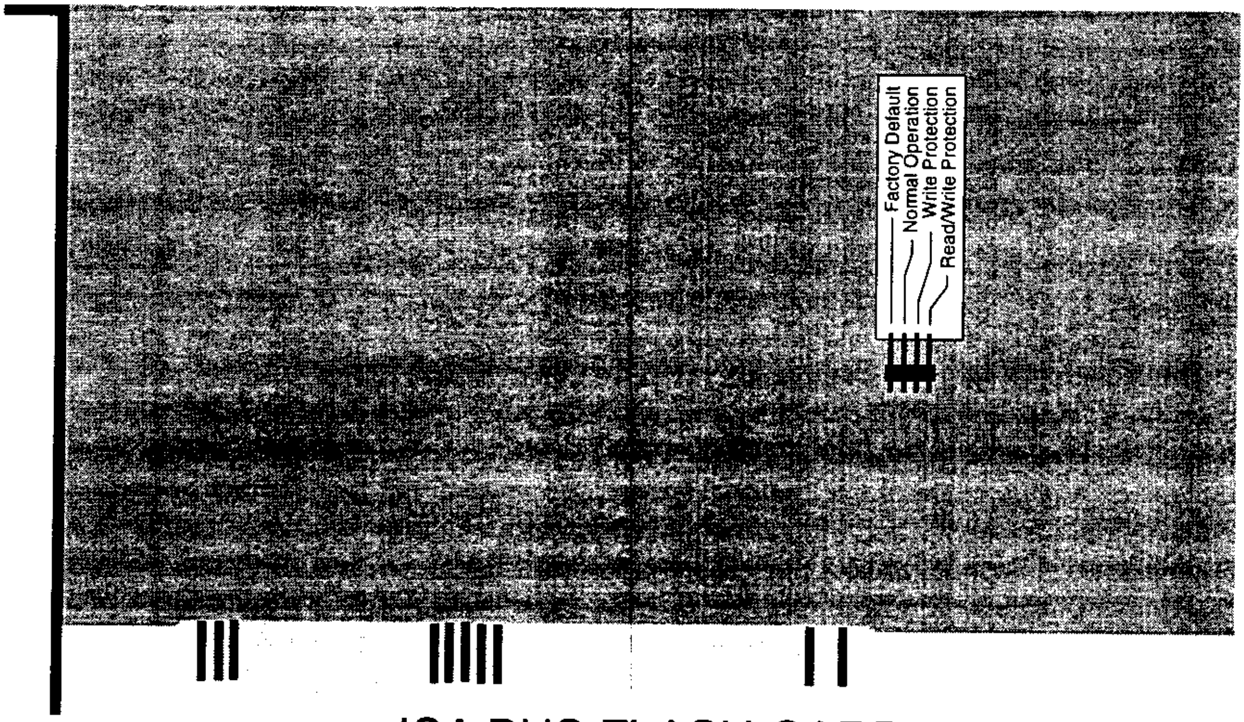
HARDWARE REMOTE CONFIGURATION PROTECTION

The Flash ROM version of the Pinnacle Link Bridge/Pinnacle Link Router is configured remotely through the network using KBCONFIG via IP/SNMP. This leaves open the remote possibility that someone on the Internet could guess your SNMP read/write password and use their version of KBCONFIG to reconfigure your Pinnacle Link Bridge/ Pinnacle Link Router. This loophole can be completely closed by use of the SNMP Access Lists (described later in this manual) or jumpers on the Flash ROM card located inside the case. These jumpers positions are as follows:

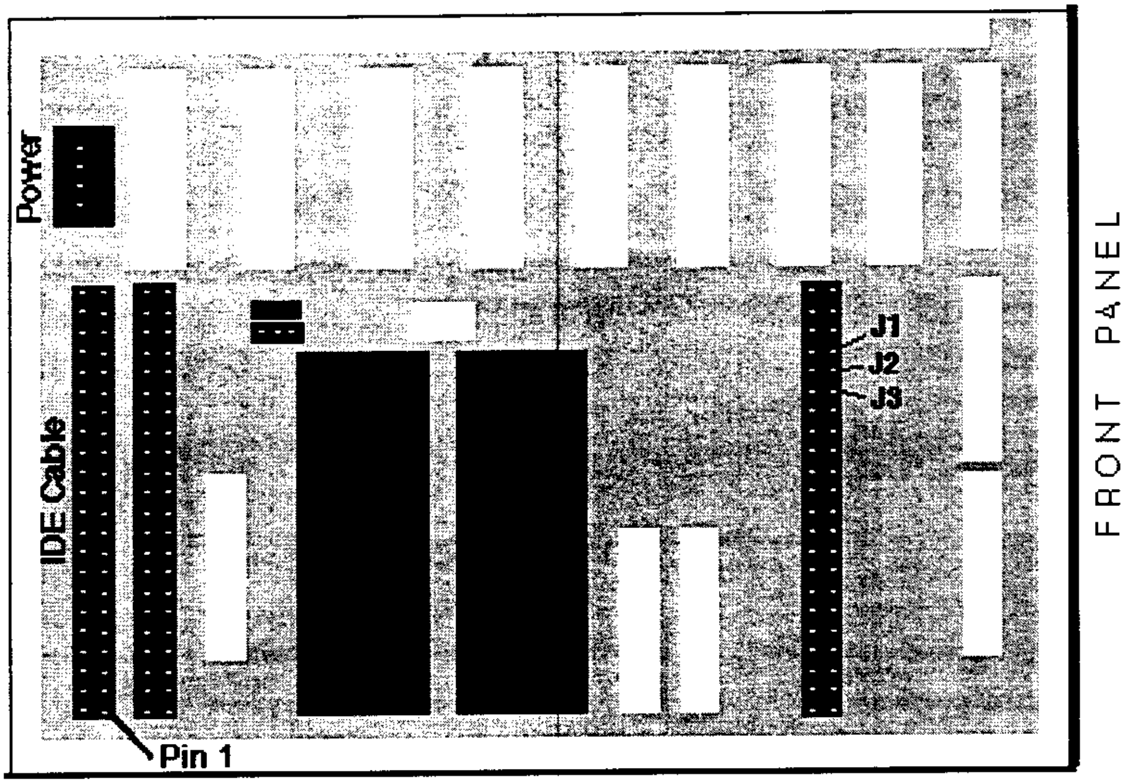
Normal Operation — The only protection is through passwords and the SNMP Access Lists, there is no special hardware protection.

Write Protection — The configuration can be read but not written unless the hardware protections are lowered by use of the front panel protection button.

Read/Write Protection — The configuration cannot be read or written unless the hardware protections are lowered by the use of the front panel protection button.



ISA BUS FLASH CARD



Pinnacle Link Bridge/Pinnacle Link Router Flash ROM Module

FUNCTION	J 1	J 2	J 3	J4*
Normal operation	ON	ON	ON	OFF
Factory Default	OFF	ON	ON	OFF
Write Protection	ON	OFF	ON	OFF
Read/Write Protection	OFF	OFF	ON	OFF
Boot on PROM	ON	ON	OFF	OFF

RESETTING TO THE FACTORY DEFAULT CONFIGURATION

The Flash ROM version of the Pinnacle Link Bridge/Router is configured remotely through the network using KBCONFIG via IP/SNMP. In order for KBCONFIG to communicate through the network two things must be known; the IP Address and the read/write SNMP password (sometimes called the community name) of the Pinnacle Link Bridge/Router. When shipped from the factory the IP Address is 198.17.74.254 and the read only and read/write passwords are set to *public* and *public.* If you forget what you have changed these to you can restore them to the factory default by placing the jumper on the Flash ROM board located inside the case to the Factory Default position. You must then reboot the Pinnacle Link Bridge/Router and configure it with KBCONFIG using the factory default address and passwords. Once you have changed the address and password and saved them with KBCONFIG and the Pinnacle Link Bridge/Router has rebooted itself it is ready for use. You should then shut off the Pinnacle Link Bridge/ Router move the jumper back to Normal Operation, or one of the protection settings, and start it back up to verify that your changes have taken effect.

REMOTE AND LOCAL PORTS

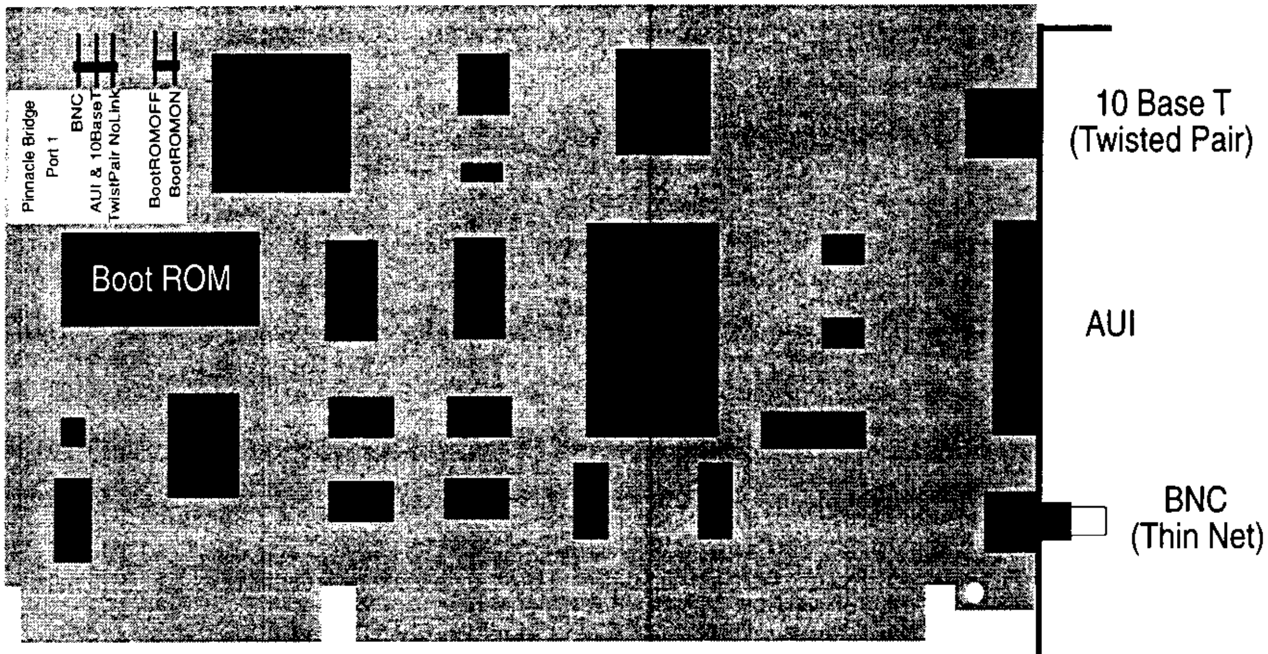
The Pinnacle Link Bridge and Pinnacle Link Router's security filters provide isolation between one or more local networks and one or more remote networks. The ports on the standard 2 port Pinnacle Link Bridge and Pinnacle Link Router are labeled Port 0 Remote and Port 1 Local. The work group or computer lab that you wish to isolate should be connected to the Local Port and the external network should be connected to the Remote Port. NOTE: If you have a Pinnacle Link Bridge/Router that supports mixed media or more than 2 ports you will have the option in the Setup-Ports menu to change which port(s) are considered "local" and which port(s) are considered "remote".

115/230 VOLT SETTING

The Non-Auto switch Pinnacle Link Bridge/Router is shipped with 115V selected. If your country uses 230V this setting should be changed. The Auto switch version of the Pinnacle Link Bridge/Router automatically detects and adjusts for the proper voltage setting and no manual switch is needed or provided.

ETHERNET INTERFACE (BNC OR AUI CONNECTIONS)

The 10Base2 (Thin Wire) Pinnacle Link Bridge/Router is shipped with both Ethernet cards setup for BNC (Thin Wire Ethernet). If you wish to use the AUI (transceiver) port you must open the case and change the jumpers located on the appropriate Ethernet card. These Ethernet cards have been customized for use in the commercial Pinnacle Link Bridge/Router and are not interchangeable with the standard Ethernet cards by the same manufacturer.



SMC Elite 16 Ethernet Card

BNC

Use this setting if you are connecting your LAN to the BNC connection.

AUI & 10BaseT

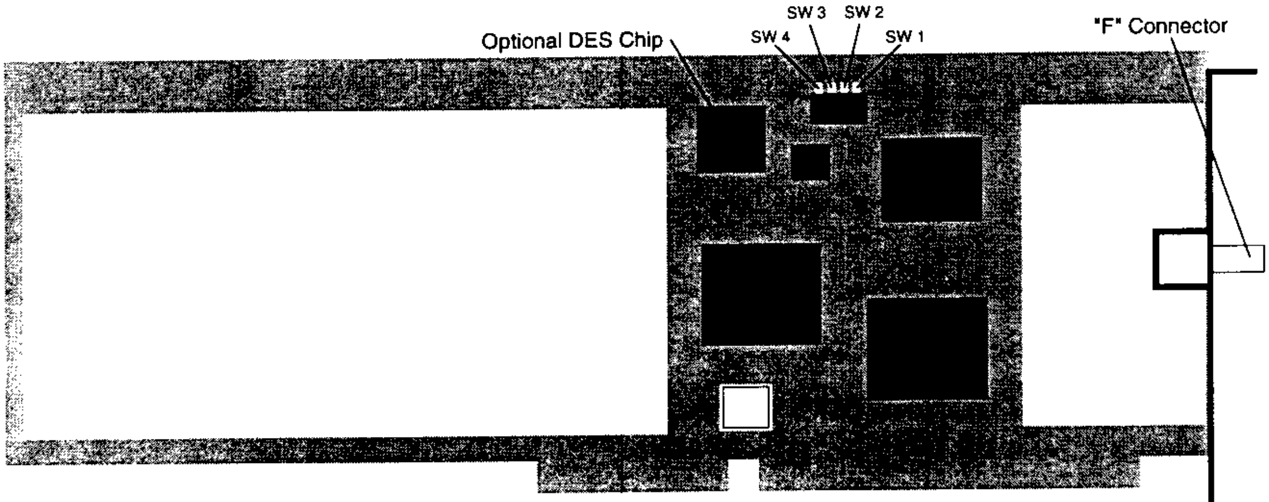
Use this setting if you are connecting your LAN to either the AUI or the 10BaseT (Twisted Pair) connector.

Twisted Pair No Link

Use this setting if you are connecting your LAN to the 10BaseT (Tiwsted Pair) connector and wish to have No Link Integrity signal active - (This setting is not normally used).

WAVELAN INTERFACE

The commercial version of the Pinnacle Link Bridge/Router supports a standard ATT/ NCR or DEC WaveLAN wireless interface card. The card is configured in "factory default" mode (all switches in the up position). It provides a wireless link to other WaveLAN wireless cards within a building. The Omni directional antenna supplied has a range of 800 feet. With the addition of a directional antenna, (wireless network) connections can be made between buildings that are several miles apart.



ATT/NCR DEC Style WaveLAN Card

	SW1	SW2	SW3	SW4
* Port 0	off	off	off	off
Port 1	off	on	off	off
Port 2	on	on	off	off

***NOTE**: It is highly recommended that you install the WaveLAN card as Pinnacle Link Bridge Port 0.

CONFIGURATION

The Pinnacle Link Bridge/Pinnacle Link Router has been designed to provide several layers of isolation and firewall security protection for many types of local area networks. You will most likely not need to use all of the features and filters provided.

RUNNING THE KBCONFIG PROGRAM

(on a floppy based Pinnacle Link Bridge/Pinnacle Link Router)

Remove the Pinnacle Link Bridge/Router floppy from the floppy drive and insert it into any standard PC compatible computer that is running DOS version 3 or higher with an EGA or VGA monitor. For this example it is assumed your floppy drive is drive A.

1. Copy the files KBCONFIG.EXE, KBC.EXE, KBHELP.HLP, and KBCONFIG.CFG from the "Flash ROM Remote Configuration" diskette into a directory on your hard disk.

2. Issue the command: KBCONFIG A:KBRIDGE.BIN

3. Set-up the Pinnacle Link Bridge/Pinnacle Link Router features and filters by use of the menus as described in the sections later in this manual.

4. Save your new configuration back into the KBRIDGE.BIN file on the floppy by issuing the Save command under the File menu.

The KBCONFIG program modifies the KBRIDGE.BIN file which contains the bridge/ router program and your filter settings. When the floppy is inserted into the Pinnacle Link Bridge/Pinnacle Link Router floppy drive and the box is powered up the program KBRIDGE.BIN will boot and execute.

<u>WARNING</u>: The Pinnacle Link Bridge/Pinnacle Link Router floppy disk boot block program will only boot the KBRIDGE.BIN file if it is contiguous. The only way to guarantee that the KBRIDGE.BIN file is contiguous is to copy it to a blank newly formatted disk with a Pinnacle Link Bridge boot block on it. If you copy the KBRIDGE.BIN file to a hard disk and then back to a non-blank floppy it may not be contiguous and thus will not boot properly. NOTE: When the KBCONFIG program modifies the KBRIDGE.BIN file on the floppy it does not move the KBRIDGE.BIN file and therefore will boot properly. Therefore whenever you change the configuration of the KBRIDGE.BIN file on the boot floppy always open the file on the floppy directly from KBCONFIG.

RUNNING THE KBCONFIG PROGRAM

(remotely on Flash ROM Pinnacle Link Bridge/Pinnacle Link Routers)

1. Ensure that a standard "Packet" driver is installed on your MS-DOS computer. It came with the software you received when you pourchased your Ethernet card. If you do not have a packet driver you can use one of the drivers that are included on the "Flash ROM Remote Configuration" diskette provided with your Flash ROM Pinnacle Link Bridge or Pinnacle Link Router.

2. Copy the files KBCONFIG.EXE, KBC.EXE, KBHELP.HLP, and KBCONFIG.CFG from the "Flash ROM Remote Configuration" diskette into a directory on your hard disk.

3. If you are connected to an existing IP network then setup the KBCONFIG.CFG file to reflect your IP address, IP mask, default router, etc.

4. Issue the command: KBCONFIG.

5. Under the File menu issue an Open Remote then specify the IP address of the network connected remote Pinnacle Link Bridge/Pinnacle Link Router. The factory default for the Pinnacle Link Bridge/Pinnacle Link Router IP address and the IP address as shipped is 198.17.74.254.

6. Set-up the Pinnacle Link Bridge/Pinnacle Link Router features and filters by use of the menus as described later in this manual.

7. Save your new configuration by issuing the Save command under the File menu.

The KBCONFIG program modifies the configuration section of the Pinnacle Link Bridge/ Pinnacle Link Router Flash ROM and then the remote bridge/router will reboot.

KBCONFIG's File Menu

KBCONFIG will configure either an executable Pinnacle Link Bridge/Pinnacle Link Router file or configure a remote FlashROM based Pinnacle Link Bridge or Pinnacle Link Router.

CONFIGURING AN EXECUTABLE FILE

To configure an executable file you can use the Open and Save functions. The file can be either a .EXE or .BIN file. EXE files can be run under DOS and are usually the shareware demo version. BIN files can either be loaded into FlashROM or booted off of the special Pinnacle Link Bridge/Pinnacle Link Router boot diskette. You must have a file open before any other KBCONFIG functions can be performed. After you have made your configuration choices you should then Save them back to the open file.

CONFIGURING A REMOTE Pinnacle Link Bridge or Pinnacle Link Router

To configure a remote (network attached) Pinnacle Link Bridge or Pinnacle Link Router you can use the Open Remote and Save functions. You must have a remote bridge or brouter open before any other KBCONFIG functions can be performed. After you have opened the remote device and configured it you can then Save your configuration back to the open device. When you Save back to the remote device its FlashROM will be erased and then reprogrammed with the new configuration.

ets will take up a small amount of RF air time. If you only have a few wireless stations this is inconsequential. If you have hundreds of wireless stations in your wireless cell and all of these stations are transmitting hello/test packets the wireless LAN will be slowed down.

[X] Enable Directional Antenna Support

The WaveLAN card is designed to connect to either a special omni-directional antenna or a directional antenna. If you are using a directional antenna you should enable directional antenna support. With directional antenna support enabled, the WaveLAN card stops sending out the 10 Volt, 1 MHz square wave signal needed only by the special omni-directional antenna. Note: A DC blocking device should be connected to the WaveLAN cards antenna port if the WaveLAN card is connected to a DC grounded directional antenna such as the loop yagi.

[X] Enable Signal Quality Front Panel Display

This function will enable WaveLAN signal quality statistics on the CRT monitor or LCD front panel display.

[X] Enable Data Encryption on All Packets

Some Pinnacle Link Bridges and Pinnacle Link Routers contain a special software encryption algorithm that is distinct from the optional WaveLAN DES encryption chip. If Data Encryption is enabled on the General Setup menu and if an Encryption Key is setup in the Data Encryption menu then enabling encryption here will cause all packets transmitted over the WaveLAN wireless network to be software encrypted.

(•) WaveLAN Compatibility Mode

KarlNet, ATT/NCR, DEC, Persoft, Solectek and others can transmit and receive data over WaveLAN wireless networks in an industry compatible way. This setting will enable the Pinnacle Link Bridge/Pinnacle Link Router to transmit and receive its WaveLAN wireless packets in this compatible way.

(•) CellWave Mode (No Base Station)

The industry compatible way of transmitting and receiving data over WaveLAN (and many other) wireless networks cause data packets to be frequently lost. This is due to the fact that a wireless network does not have the ability to detect collisions like an Ethernet network has. In an Ethernet network collisions can be detected by the hardware (Ethernet chip) and are automatically retransmitted. Ethernet is referred to as CSMA/CD (Carrier Sense Multiple Access with Collision Detect). Wireless networks are CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The reason that collisions cannot be detected is because with radio you cannot receive and transmit at the same time hence you cannot detect the collisions. In practice a properly operating WaveLAN point-to-point network will loose, due to collisions, approximately 1% of the transmitted packets. This packet loss is not normally a problem with protocols such as Novell IPX (without the burst mode NLM) but will cause networks using most other protocols to experience poor performance.

If all of the wireless Pinnacle Link Bridge/Pinnacle Link Routers in your wireless cell can "hear" each other and if you are running a non-Novell IPX protocol or Novell IPX with burst mode NLM then this setting will greatly improve the performance of your wireless network.

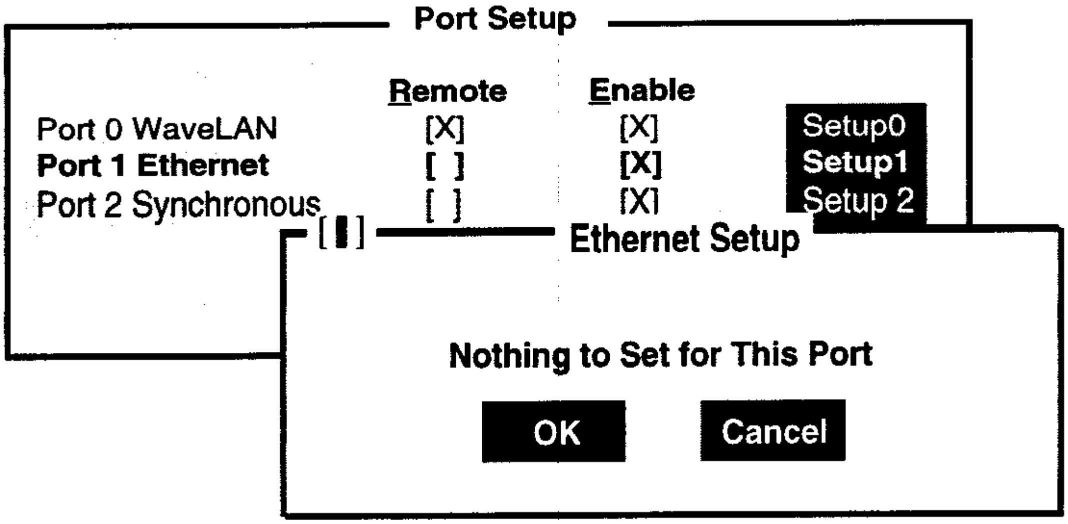
(•) CellWave Base Station Mode (This is a base station)
This setting should be used if this wireless Pinnacle Link Bridge/Pinnacle Link Router is the one and only base station in the wireless network (i.e. a WaveLAN network with the same Network ID, NWID). With the previously mentioned CellWave Mode (No Base Station) setting there is a requirement that all wireless stations be able to transmit to and receive from ALL other stations in the wireless network. This is not always possible due to the particular topology and terrain. The Wireless Pinnacle Link Bridge/Pinnacle Link Router has a special mode where one of the wireless nodes can be setup as a "base" station and all others can be setup as "satellite" stations. In this configuration the only requirement is that each satellite station be able to communicate with the one base station. The base station is responsible for "repeating" packets that need to travel between satellite stations.

The performance of this approach is slightly improved if the base station is connected to the most heavily loaded file server or wired network access point. This is due to the fact that data flowing from one satellite to another satellite station must be repeated (retransmitted) by the base station using more of the wireless bandwidth. Data packets flowing from a satellite station to the base station are transmitted directly without the need to be repeated.

(•) CellWave Base Station Mode (This is a satellite station)
Set this if this wireless Pinnacle Link Bridge/Pinnacle Link Router is one of the satellite stations in the wireless network. (i.e. a WaveLAN network with the same Network ID, NWID).

Ethernet Interface

There are no special hardware setups needed for Ethernet ports.



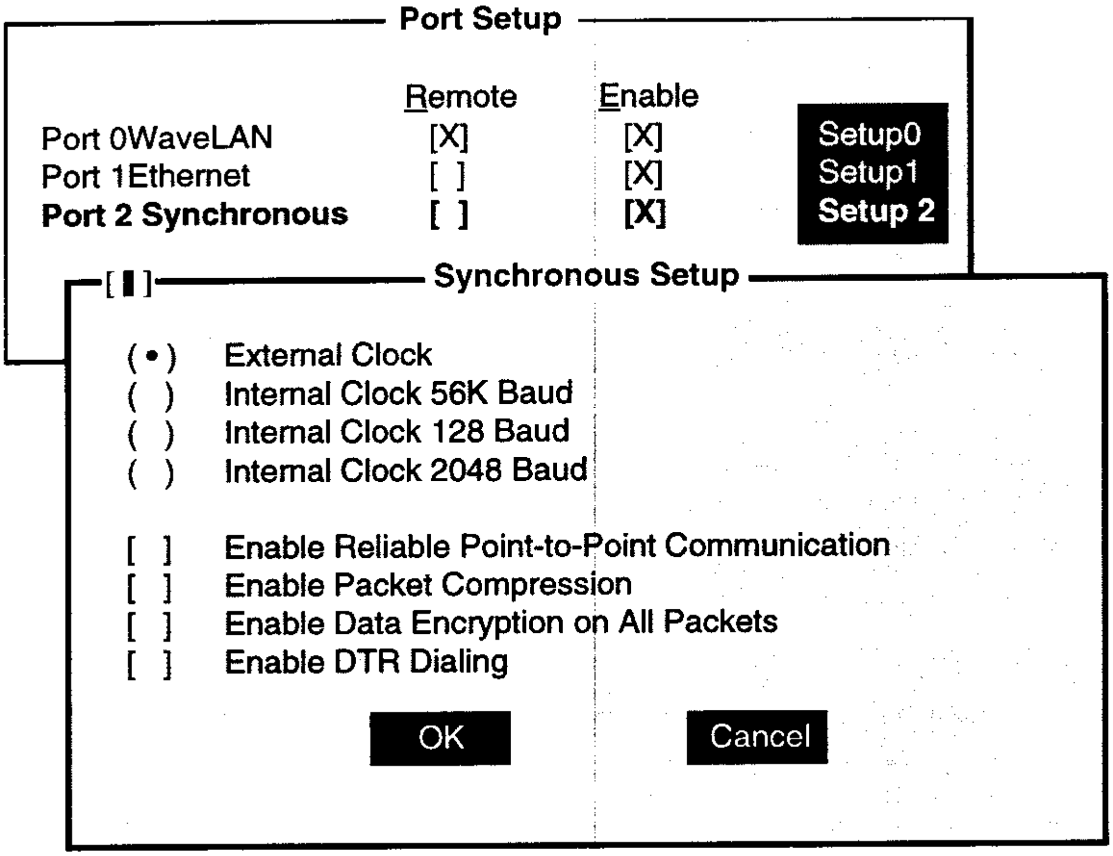
Port Setup

	Remote	Enable	
Port 0 WaveLAN	[X]	[X]	Setup0
Port 1 Ethernet	[ ]	[X]	Setup1
Port 2 Synchronous	[ ]	[X]	Setup 2

Ethernet Setup

Nothing to Set for This Port

Synchronus Interface



Port Setup

	Remote	Enable
Port 0WaveLAN	[X]	[X]
Port 1Ethernet	[ ]	[X]
Port 2 Synchronous	**[ ]**	**[X]**

[▮] Synchronous Setup

(•) External Clock
( ) Internal Clock 56K Baud
( ) Internal Clock 128 Baud
( ) Internal Clock 2048 Baud

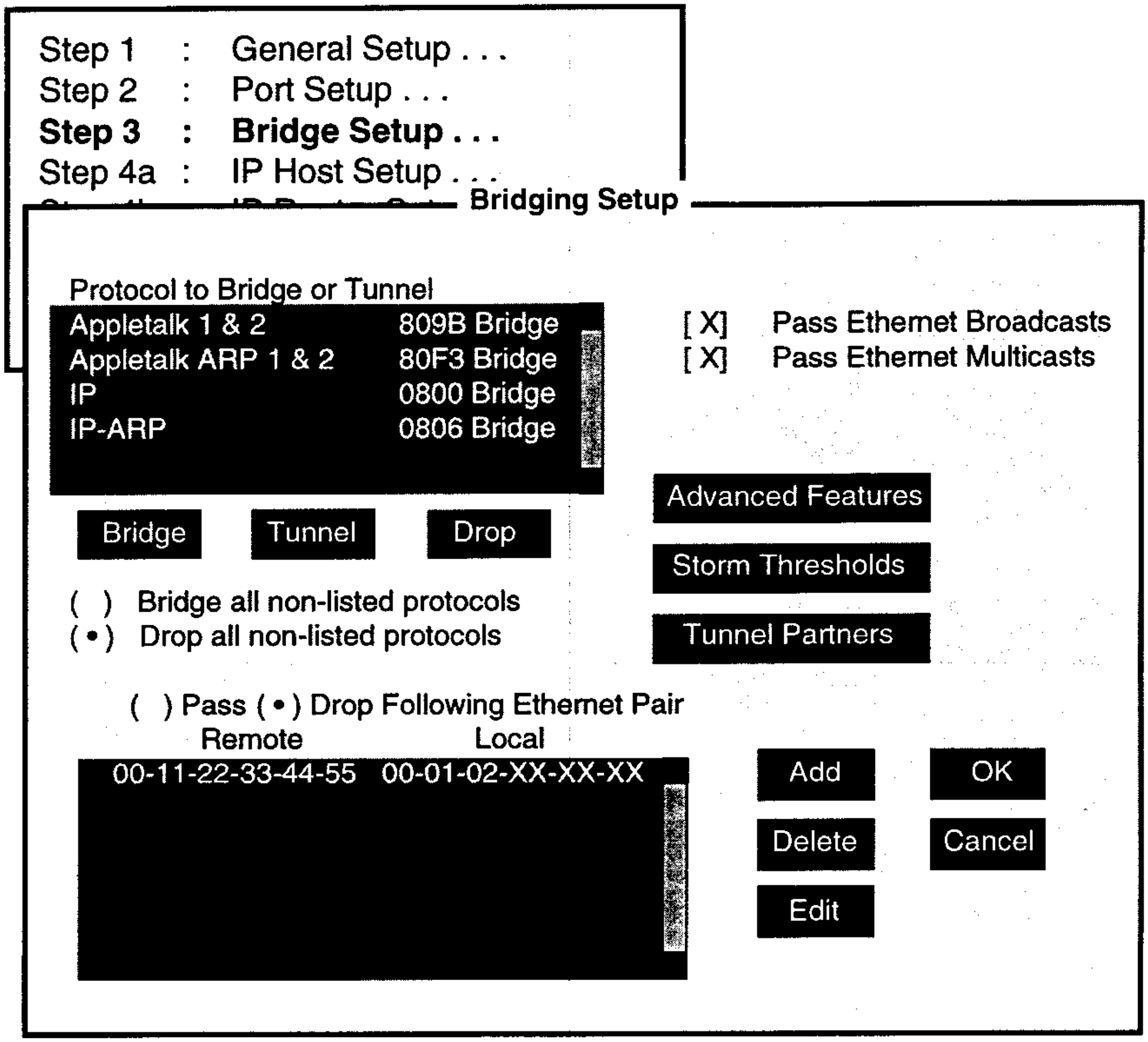
[ ] Enable Reliable Point-to-Point Communication
[ ] Enable Packet Compression
[ ] Enable Data Encryption on All Packets
[ ] Enable DTR Dialing

(•) External Clock
This setting will enable the external clock inputs and disable the internal clock source.

(•) Internal Clock
One of these settings will enable the internal clock generator to the specified bit rate.

[X] Enable Date Encryption on All Packets
Some Pinnacle Link Bridges and Pinnacle Link Routers contain a special software encryption algorithm that is distinct from the optional WaveLAN DES encryption chip. If Data Encryption is enabled on the General Setup menu and if an Encryption Key is setup in the Data Encryption menu then enabling encryption here will cause all packets transmitted over the synchronous port to be encrypted.

STEP 3: BRIDGE SETUP



Step 1 : General Setup . . .
Step 2 : Port Setup . . .
Step 3 : Bridge Setup . . .
Step 4a : IP Host Setup . . .
Bridging Setup
Bridge
Tunnel
Drop
Advanced Features
Storm Thresholds
Tunnel Partners
Add
Delete
Edit
OK
Cancel

Protocol to Bridge or Tunnel

```
Appletalk 1 & 2        809B Bridge
Appletalk ARP 1 & 2    80F3 Bridge
IP                     0800 Bridge
IP-ARP                 0806 Bridge
```

☒ Pass Ethernet Broadcasts

☒ Pass Ethernet Multicasts

○ Bridge all non-listed protocols

● Drop all non-listed protocols

○ Pass ● Drop Following Ethernet Pair

```
      Remote              Local
00-11-22-33-44-55   00-01-02-XX-XX-XX
```

NOTE: The Tunnel and Tunnel Partners Buttons will not appear unless "Remote Bridging using IP Tunnels" is enabled in the General Setup Menu.

Protocol to Bridge or Tunnel

This menu specifies the Ethernet protocols to Bridge, Drop or optionally Tunnel. Each protocol can be bridged (a synonym for passed) or can be dropped as selected with the Bridge or Drop button. All other protocols not specified in the menu are then either bridged or dropped depending upon the mode selected by the radio buttons labeled "Bridge all non-listed protocols" or "Drop all non-listed protocols".

It is recommended that you bridge only the protocols that you absolutely need and drop all non-listed protocols. If you elect to bridge IP, DECNET, Novell, or AppleTalk then you will have the opportunity to setup additional filters under the Setup - Security menus. You will be given the opportunity to specify in more detail the types of services you wish to promote (pass) or restrict (drop) for the particular protocols selected.

Tunneling is a method of encapsulating Ethernet packets, received from the "Local" port in a IP/UPD packet and sending them to one or more tunnel partners. Tunneling can be used to setup virtual Ethernet networks. You can tunnel some protocols, bridge other protocols and drop other protocols all simultaneously.

(•) Bridge ( ) Drop all non-listed protocols
This setting will determine what is to happen to packets that are not listed in the "Protocol to Bridge or Tunnel" menu.

[X] Pass Ethernet Broadcast
Standard Ethernet bridges will always forward broadcast packets. Many protocols do not use broadcasts (e.g. AppleTalk Phase II, DECNET and others). However, IP/ARP does use broadcasts. If you do not use IP or any other protocol that requires broadcasts then you can drop them. Shutting off broadcast packets will reduce the traffic on your network and will also greatly reduce the number of interrupts that each computer connected to your network experiences. Networks with a high number of broadcasts will slow down the processing of each attached computer even if it is not using the network.

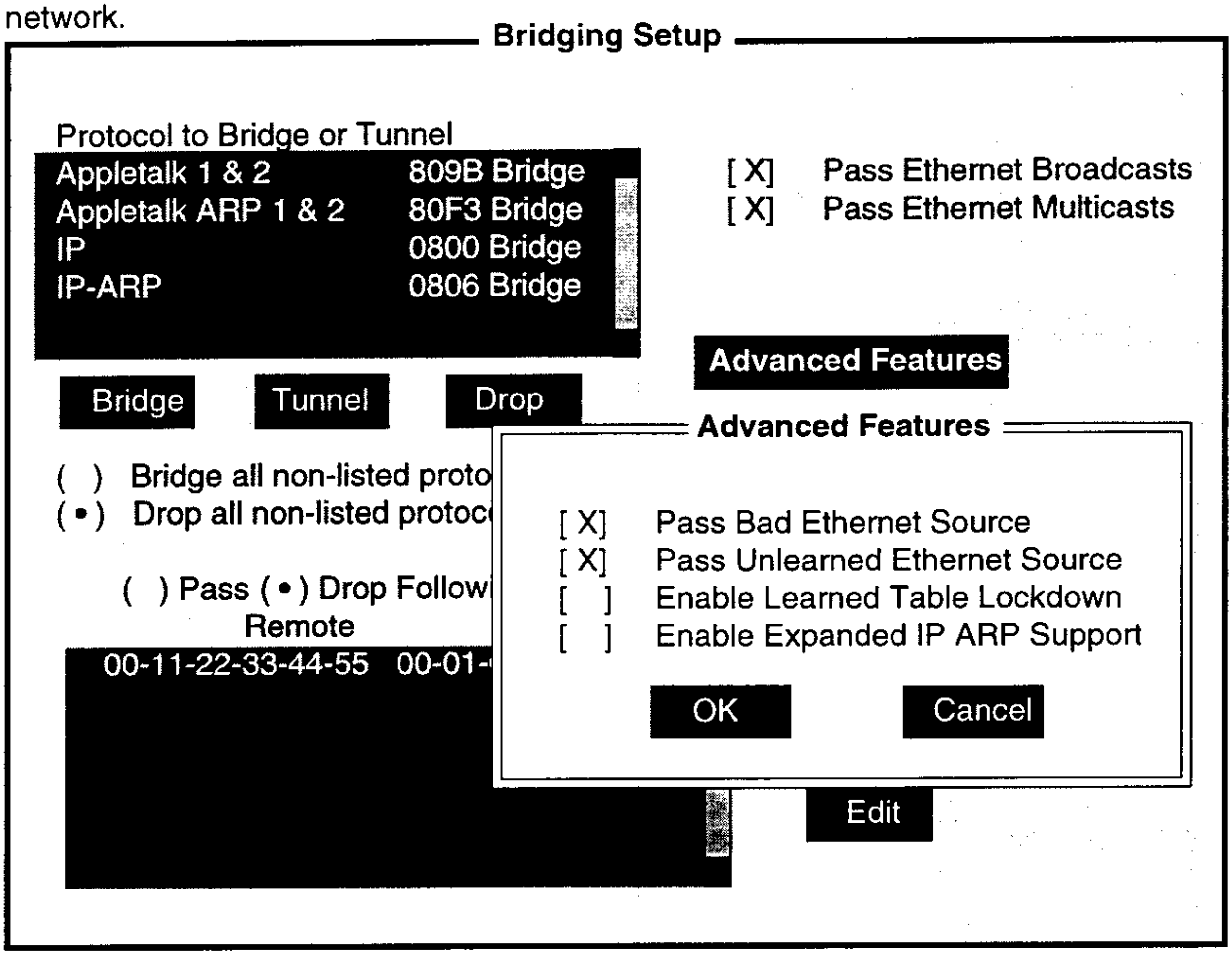
[X] Pass Ethernet Multicasts
Standard Ethernet bridges will always forward multicast packets. Some protocols do not use multicast packets, such as IP and Novell IPX. If you do not use protocols that use multicast packets then you can drop them by shutting off multicasts on the Pinnacle Link Bridge. Shutting off multicast packets will reduce the traffic on your network and will also reduce the number of interrupts that each computer connected to your network experiences.

(•) Pass ( ) Drop Following Address Pair
This menu specifies the Ethernet addresses that should be either Passed or Dropped both the source and destination address are checked against this filter. An entire 6 byte Ethernet address can be filtered or just portions of it. This menu can be used to inhibit or promote communication with a several particular Ethernet addresses or groups of Ethernet addresses. This approach of specifying Ethernet addresses is similar to a standard bridge that supports Ethernet address filtering. We have found this approach to not be very useful, however, support it for completeness.

As an example if the menu is set to "Drop following Pair" and an address pair of: 00-11-22-33-44-55 & 00-01-02-XX-XX-XX is specified then data packets from the address 00-11-22-33-44-55 to any addresses that start with 00-01-02 will be dropped.

Advanced Features

This menu contains advanced bridging options. These options should be changed from their default only if you clearly understand their functions and how they may impact your network.



Bridging Setup

Protocol to Bridge or Tunnel

Appletalk 1 & 2	809B Bridge
Appletalk ARP 1 & 2	80F3 Bridge
IP	0800 Bridge
IP-ARP	0806 Bridge

☒ Pass Ethernet Broadcasts
☒ Pass Ethernet Multicasts

( ) Bridge all non-listed proto
(•) Drop all non-listed protoc

( ) Pass (•) Drop Follow
Remote
00-11-22-33-44-55 00-01-

Advanced Features

☒ Pass Bad Ethernet Source
☒ Pass Unlearned Ethernet Source
☐ Enable Learned Table Lockdown
☐ Enable Expanded IP ARP Support

[X] Pass Bad Ethernet Source

The standard Ethernet bridges we have tested will pass Ethernet packets with a broadcast or multicast address as their source (i.e. the first bit set to 1). The Ethernet specification for Transparent (i.e. Non-Source Routing) bridges does not allow these types of packets and are considered as "bad" packets. Our studies have shown that a common failure mode of many Ethernet interfaces and networking software is to transmit packets like these. If you do not need the Pinnacle Link Bridge to pass Source Routing packets it is suggested that you set it to drop these packets. Default: Pass

[X] Pass Unseen Ethernet Source

Standard Ethernet bridges will always forward packets with destination addresses that have not been "learned" (i.e. not been seen as a source address of a packet). This characteristic is needed for the proper operation of an Ethernet bridge. The down side to this is that our studies have shown that the failure mode of many Ethernet interface cards is to send out erroneous packets with good CRC's but with random Ethernet destination and source addresses. Standard bridges will pass these erroneous packets since they have not "learned" the random destination address and then add this packets random source address to their finite "learned" table. This situation is not uncommon and can greatly hinder the operation of standard bridges. If you chose to Drop unlearned packets then the Pinnacle Link Bridge will not forward unicast packets to Ethernet addresses that have not already been seen as a source address. This scheme works for most protocols because it relies on the characteristics of most upper-layer protocol to transmit ARP requests or Hello packets. It should be set to Drop with care by a qualified network engineer. Default: Pass

[X] Enable Learned Table Lock down

A standard bridge watches the source addresses of each packet it receives on any of its ports. As new addresses are seen, entries are added in the "learned table" that contain the particular source address and the port number that address was received on. If that source address is later seen on a different port the bridge will immediately change the port number in the learned table entry. This condition could happen in a correctly functioning network if someone moved the computer to a different part of the network. This could also happen if someone was trying to capture network packets by spoofing the bridge. Enabling learned table lock down will prevent the port number from being changed once the source address has been seen.

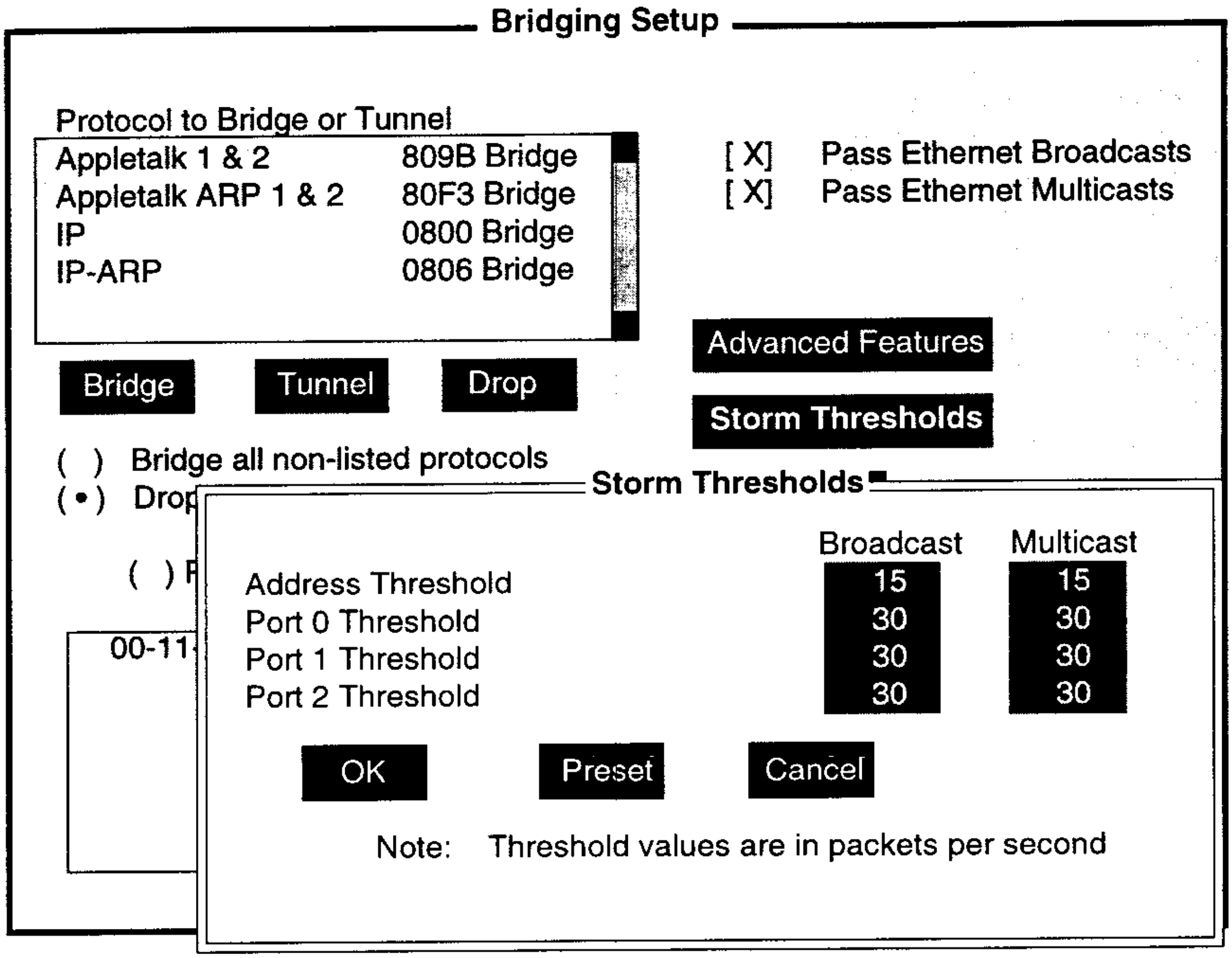
A standard bridge will also time-out the learned table records every 10 minutes. If learned table lock down is enabled then these records will not be timed out, once a record is learned it will not change or be deleted until either the bridge reboots or the learned table becomes completely filled and needs to be reset. Note: A typical Pinnacle Link Bridge learned table can contain over 12,000 records. Default: Disabled

[X] Enable Expanded IP ARP Support

Enabling this feature will cause the bridge to also watch the IP/ARP packets that occur on the network. No action is taken in response to an IP/ARP packet (since that is the role of an IP router) other than the bridge will add the IP address to it's IP/ARP table. This feature is helpful on an IP network because it will build a database of MAC layer address to IP address pairs. An SNMP monitoring program such as KBCONFIG can at any time extract this information. NOTE: 1) The IP/ARP table is never timed out in this mode. 2) This feature is not available if the Pinnacle Link Router is routing IP. Default: Disabled

Storm Thresholds

One of the unique and very useful features of the Pinnacle Link Bridge/Pinnacle Link Router is its ability to keep Broadcast and Multicast storms from spreading throughout a network. Network storms are common and can cause bridges, routers, workstations, servers and PC's to slow down or crash. Storms occur if network equipment is configured incorrectly, if network software is not functioning correctly, or if poorly designed programs such as network games are used.



Bridging Setup

Protocol to Bridge or Tunnel

```
Appletalk 1 & 2        809B Bridge
Appletalk ARP 1 & 2    80F3 Bridge
IP                     0800 Bridge
IP-ARP                 0806 Bridge
```

[X] Pass Ethernet Broadcasts
[X] Pass Ethernet Multicasts

( ) Bridge all non-listed protocols
(•) Drop
( ) F
00-11

Storm Thresholds

	Broadcast	Multicast
Address Threshold	15	15
Port 0 Threshold	30	30
Port 1 Threshold	30	30
Port 2 Threshold	30	30

Note: Threshold values are in packets per second

Address Threshold > Broadcast

This setting determines the maximum number of broadcast packets that can occur each one second period before a storm condition is declared for a particular Ethernet address (host). Once it is determined that a storm is occurring then any additional broadcast packets from that host address will be dropped until the storm is determined to be over. The storm will be determined to be over when 30 seconds has passed where every 1 second period has less then the stated threshold in broadcast packets.

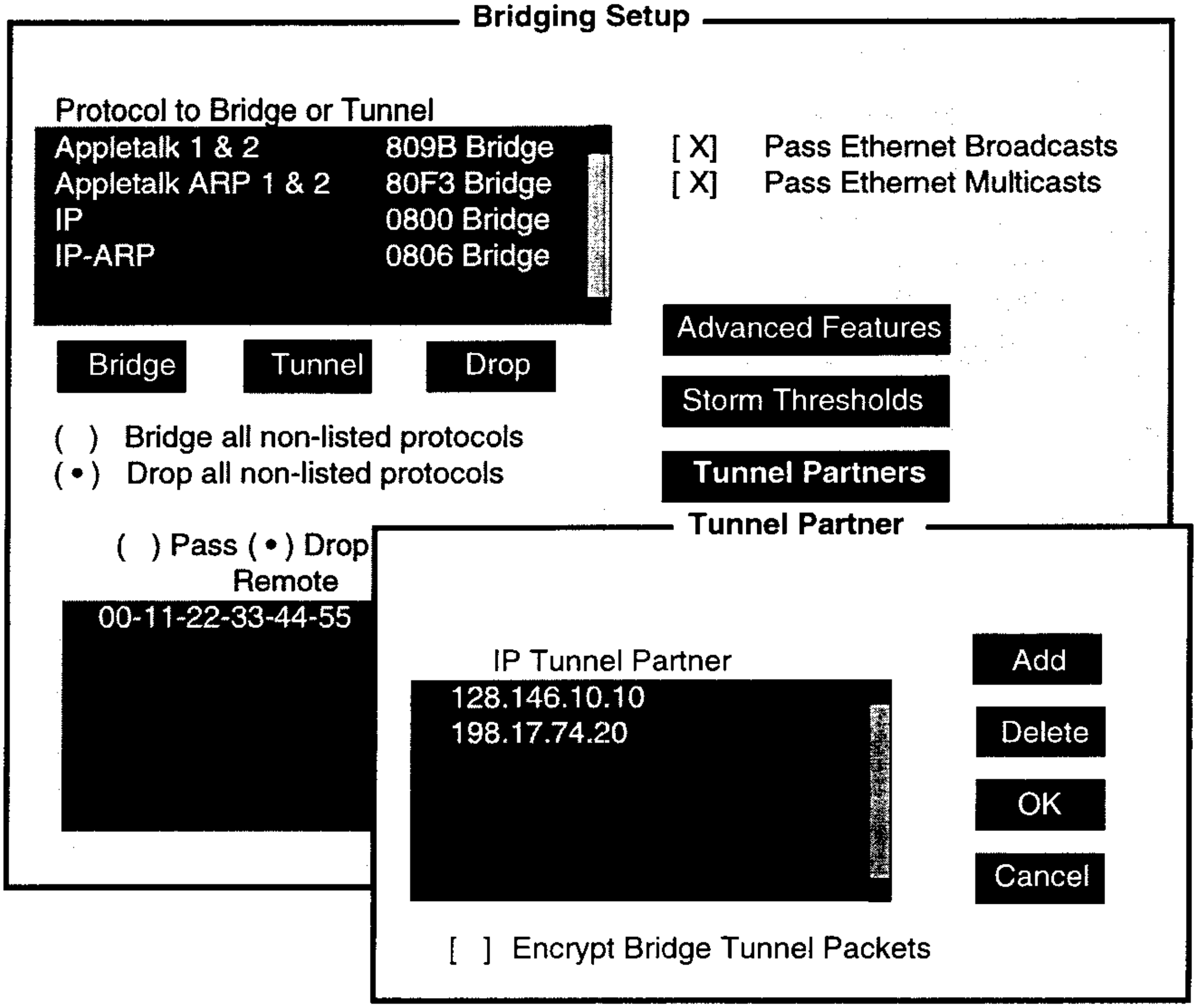
Address Threshold > Multicast
This setting determines the maximum number of multicast packets that can occur each one second period before a storm condition is declared for a particular Ethernet address (host). Once it is determined that a storm is occurring then any additional multicast packets from that host address will be dropped until the storm is determined to be over. The storm will be determined to be over once 30 seconds has passed where every 1 second period has less then the stated threshold in multicast packets.

Port Threshold > Broadcast
This setting determines the maximum number of broadcast packets that can occur each 1 second period before a storm condition is declared for a particular port. Once it is determined that a storm is occurring then any additional broadcast packets received on that port will be dropped until the storm is determined to be over. The storm will be determined to be over once a 1 second period has occurred with no broadcast packets received on that port.

Port Threshold > Multicast
This setting determines the maximum number of multicast packets that can occur each 1 second period before a storm condition is declared for a particular port. Once it is determined that a storm is occurring then any additional multicast packets received on that port will be dropped until the storm is determined to be over. The storm will be determined to be over once a 1 second period has occurred with no multicast packets received on that port.

Preset Button
This button sets the Broadcast and Multicast storm thresholds to the recommended values. These values have been determined to offer good protection without interfering with the operation of the typical network. These values may need to be tuned for your particular network.

Tunnel Partners



```
Protocol to Bridge or Tunnel
Appletalk 1 & 2        809B Bridge
Appletalk ARP 1 & 2    80F3 Bridge
IP                     0800 Bridge
IP-ARP                 0806 Bridge

[X]  Pass Ethernet Broadcasts
[X]  Pass Ethernet Multicasts

( )  Bridge all non-listed protocols
(•)  Drop all non-listed protocols

( ) Pass (•) Drop
Remote
00-11-22-33-44-55

IP Tunnel Partner
128.146.10.10
198.17.74.20

[ ]  Encrypt Bridge Tunnel Packets
```

Tunneling is a method of encapsulating Ethernet packets, received from the "Local" port in an IP/UPD packet and sending them to one or more tunnel partners. Tunneling can be used to setup virtual Ethernet networks.

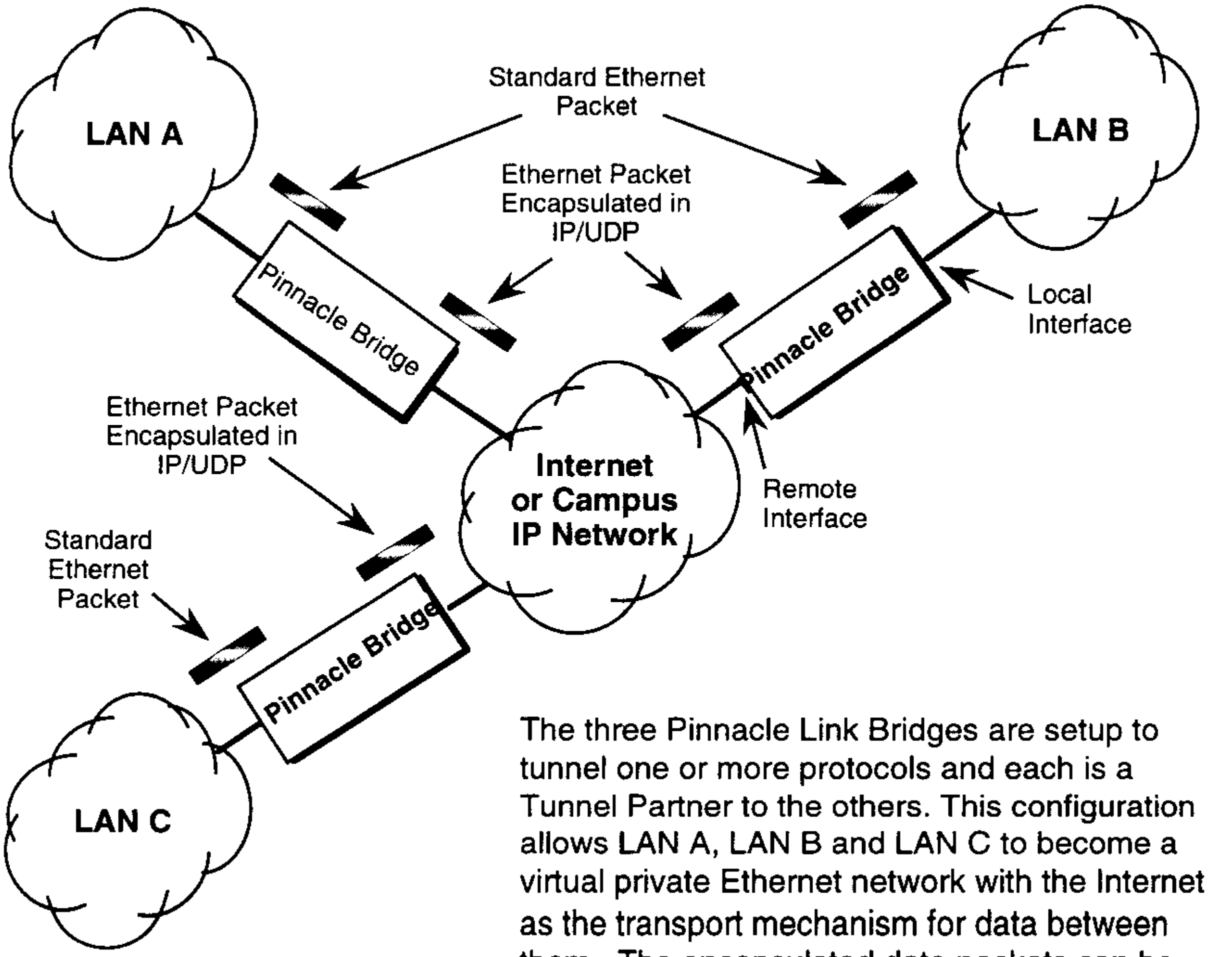
Tunnel Partners

In the General Setup menu if the "Remote Bridging using IP Tunnels" is enabled then Tunnel Partners can be setup. This menu specifies the IP addresses of each of the Pinnacle Link Bridge/Pinnacle Link Routers that are setup to participate in the tunnel group. Specify the addresses of all the bridges that are participating in the tunnel group but DO NOT specify the IP address of this bridge.

[X] Encrypt Bridge Tunnel Packets

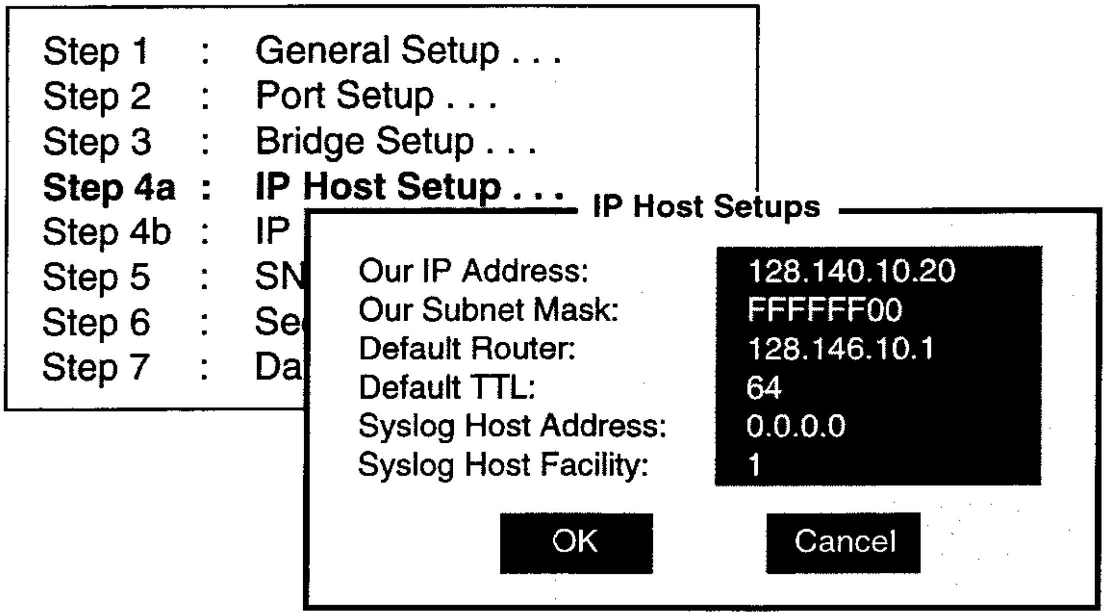
Some Pinnacle Link Bridges and Pinnacle Link Routers contain a special software encryption algorithm that is distinct from the optional WaveLAN DES encryption chip on Wireless Pinnacle Link Bridge/Pinnacle Link Routers. If Data Encryption is enabled on the General Setup menu and if an Encryption Key is setup in the Data Encryption menu then enabling encryption here will cause all packets transmitted to tunnel partners to be encrypted and any packets received from tunnel partners to be decrypted.

Generic Ethernet Tunneling
(Through an IP Network)



The three Pinnacle Link Bridges are setup to tunnel one or more protocols and each is a Tunnel Partner to the others. This configuration allows LAN A, LAN B and LAN C to become a virtual private Ethernet network with the Internet as the transport mechanism for data between them. The encapsulated data packets can be optionally encrypted to make the virtual private network more secure.

STEP 4a: IP HOST SETUP


Step 1 : General Setup . . .
Step 2 : Port Setup . . .
Step 3 : Bridge Setup . . .
Step 4a : IP Host Setup . . .
Step 4b : IP
Step 5 : SN
Step 6 : Se
Step 7 : Da
IP Host Setups
OK
Cancel

Our IP Address: 128.140.10.20
Our Subnet Mask: FFFFFF00
Default Router: 128.146.10.1
Default TTL: 64
Syslog Host Address: 0.0.0.0
Syslog Host Facility: 1

NOTE: IP Routing in the General Setup Menu must be disabled for this menu to be used.

Our IP Address
This is the IP address of the Pinnacle Link Bridge itself. If you wish to configure or monitor your Pinnacle Link Bridge or if your network supports IP and you wish to enable the Ping support and IP/SNMP support of the Pinnacle Link Bridge set this to a valid IP address. Setting this address to 0.0.0.0 will disable bridges Ping and IP/SNMP support. Please note that unless you enable IP Routing the Pinnacle Link Bridge is not an IP router. It has only one IP address and that address applies to both the Remote and Local networks (i.e. both sides of the bridge). Having two Ethernet interfaces with the same IP address is different than a standard IP host, but is appropriate for a Transparent Bridge. It is interesting to note that the Ethernet address of both ports is also the same.

Our Subnet Mask
Every IP network has what is referred to as a Subnet mask. This should be set to the appropriate mask for your network. Note that this is a hex number, hence the mask 255.255.255.0 should be specified as FFFFFF00.

Default Router
Most every IP network has a default IP router and that address should be specified here.

Default TTL
IP hosts on the Internet send out packets with a default time to live parameter. If you wish to override the factory default of 64 you can specify your new default here.

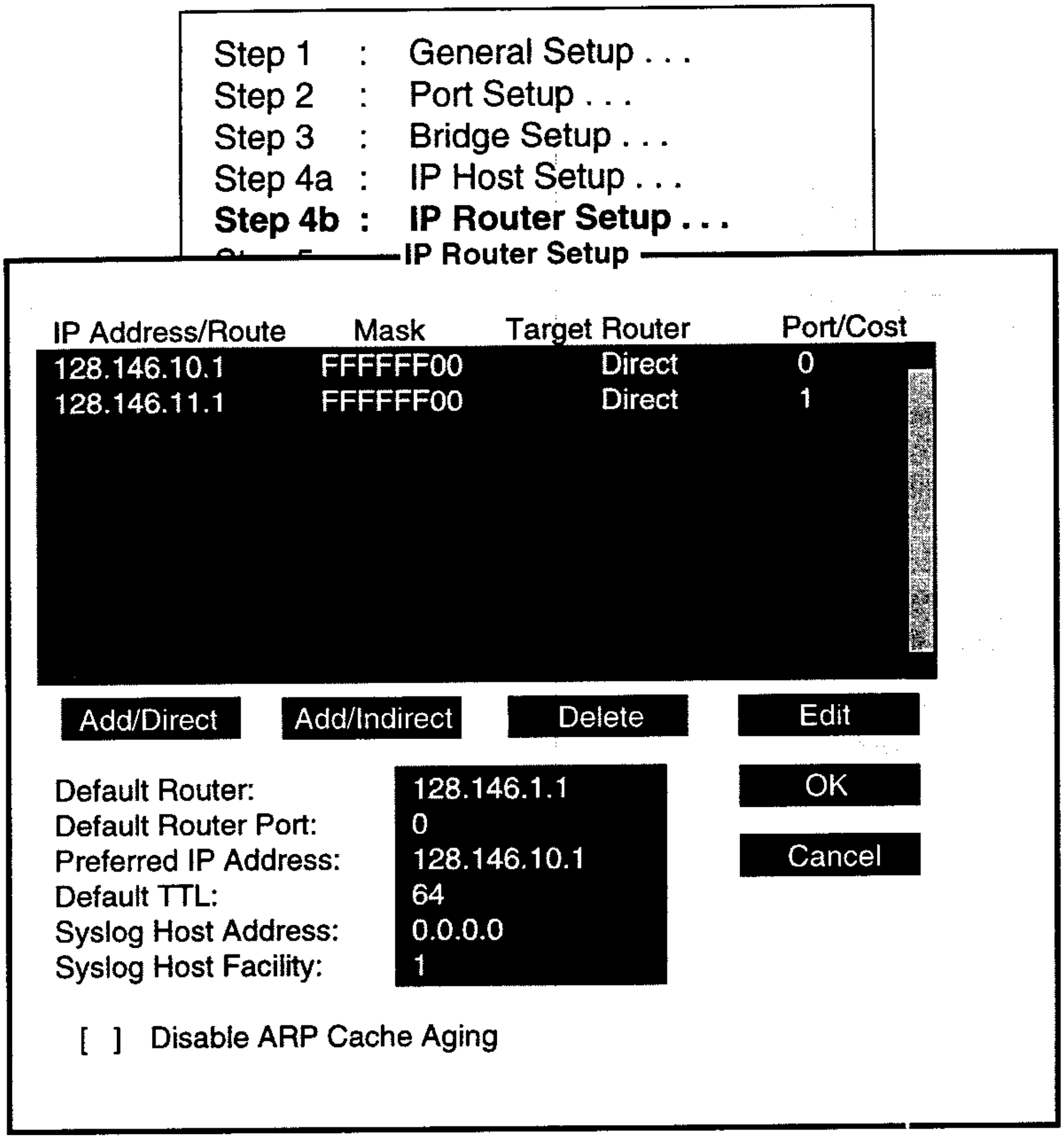
Syslog Host Address

There are many events that the Pinnacle Link Bridge/Pinnacle Link Router can log. One of the places these events can be logged is on a computer equipped with the standard UNIX Syslog facility. If you want logs of this type to be kept then the IP address of the host that will take the logs must be entered here.

Syslog Host Facility

On Unix computers that you are using to log Pinnacle Link Bridge/Pinnacle Link Router events there are 7 categories of syslog messages available to you. This number specifies which category will be used. If this number is set to "1", then the facility used is local1, so the line in the syslog.conf file should be: " local1.debug filename". On most computers there must be exactly one tab between the word "debug" and the filename.

STEP 4b: IP ROUTER SETUP


Step 1 : General Setup . . .
Step 2 : Port Setup . . .
Step 3 : Bridge Setup . . .
Step 4a : IP Host Setup . . .
Step 4b : IP Router Setup . . .
IP Router Setup
Add/Direct
Add/Indirect
Delete
Edit
OK
Cancel

IP Address/Route	Mask	Target Router	Port/Cost
128.146.10.1	FFFFFF00	Direct	0
128.146.11.1	FFFFFF00	Direct	1

Default Router:	128.146.1.1
Default Router Port:	0
Preferred IP Address:	128.146.10.1
Default TTL:	64
Syslog Host Address:	0.0.0.0
Syslog Host Facility:	1

[ ] Disable ARP Cache Aging

NOTE: IP Routing in the General Setup Menu must be enabled for this menu to be used.

Default Router (IP Address)
This entry should be set to the IP Address of the default router that this Pinnacle Link Router is to use when it does not know where to route a particular IP packet. If the port that the default router is connected to is a serial port then this entry is ignored.

Default Router Port

This entry should be set to the port that the default router is connected to. If the port that the default router is connected to is a serial port then this defines the port that is used for the default router.

Preferred IP Address

From time to time the Pinnacle Link Router will transmit unsolicited IP packets such as SNMP Traps, Syslog, RIP or IP ARP packets. Most routers randomly use one of the IP addresses from one of the router ports as the source IP address for these packets. On the Pinnacle Link Router you can specify the source IP address that you prefer to use for these packets.

Default TTL

IP hosts on the Internet send out packets with a default time to live parameter. If you wish to override the factory default of 64 you can specify your new default here.

Syslog Host Address

There are many events that the Pinnacle Link Bridge/Pinnacle Link Router can log. One of the places these events can be logged is on a computer equipped with the standard UNIX Syslog facility. If you want logs of this type to be kept then the IP address of the host that will take the logs must be entered here.

Syslog Host Facility

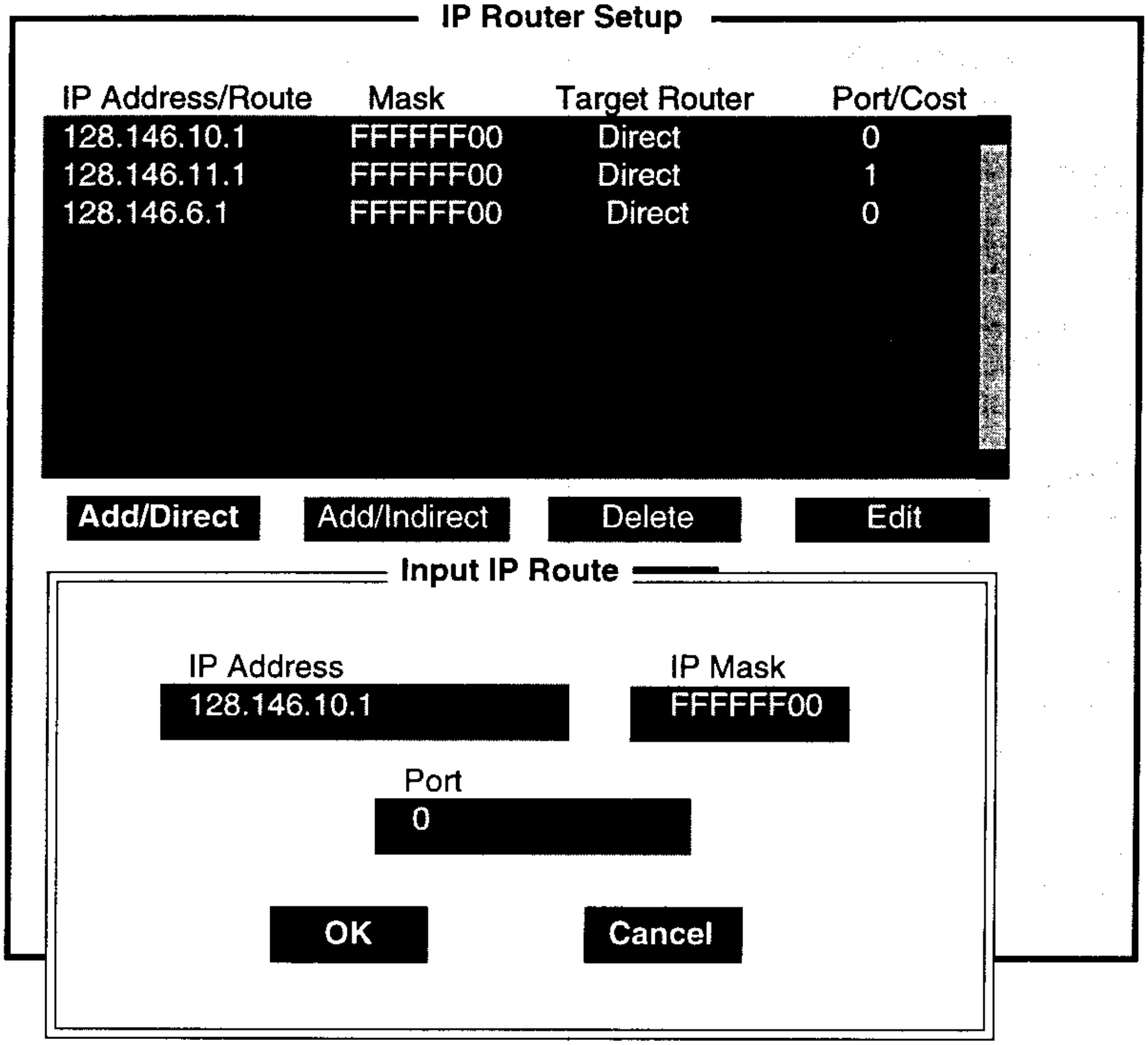
On Unix computers that you are using to log Pinnacle Link Bridge/Pinnacle Link Router events there are 7 categories of syslog messages available to you. This number specifies which category will be used. If this number is set to "1", then the facility used is local1, so the line in the syslog.conf file should be: " local1.debug filename". On most computers there must be exactly one tab between the word "debug" and the filename.

[X] Disable ARP Cache Aging

Use this option if you want to keep a permanent record of the IP to Ethernet addresses table for each computer directly connected to a port on this Pinnacle Link Router. This feature is helpful when used in conjunction with a corporate wide SNMP monitoring tool to create a database of all Ethernet to IP address combinations on your network. A standard IP router and the Pinnacle Link Router will age it's ARP cache entries. It will time-out and delete the ARP entries after a certain specified period (usually 10 minutes). The Pinnacle Link Router has the option of not aging (deleting) any ARP cache entries. This will not normally cause any IP network problems but could result in a large ARP cache table. Since the typical Pinnacle Link Router can hold over 10,000 ARP entries this is not normally a problem.

Add/Direct

This button activates a menu which is used to specify the "direct" routes for each of the ports on the Pinnacle Link Router. Direct routes are those that are directly connected to the ports. As an example if port 0 is to have subnet 128.146.6.X connected to it and an IP address of 128.146.6.1 with a subnet mask of 255.255.255.0 then an entry in this menu should be setup as: IP Address = 128.146.6.1; IP Mask = FFFFFF00; and Port = 0.



IP Address/Route	Mask	Target Router	Port/Cost
128.146.10.1	FFFFFF00	Direct	0
128.146.11.1	FFFFFF00	Direct	1
128.146.6.1	FFFFFF00	Direct	0

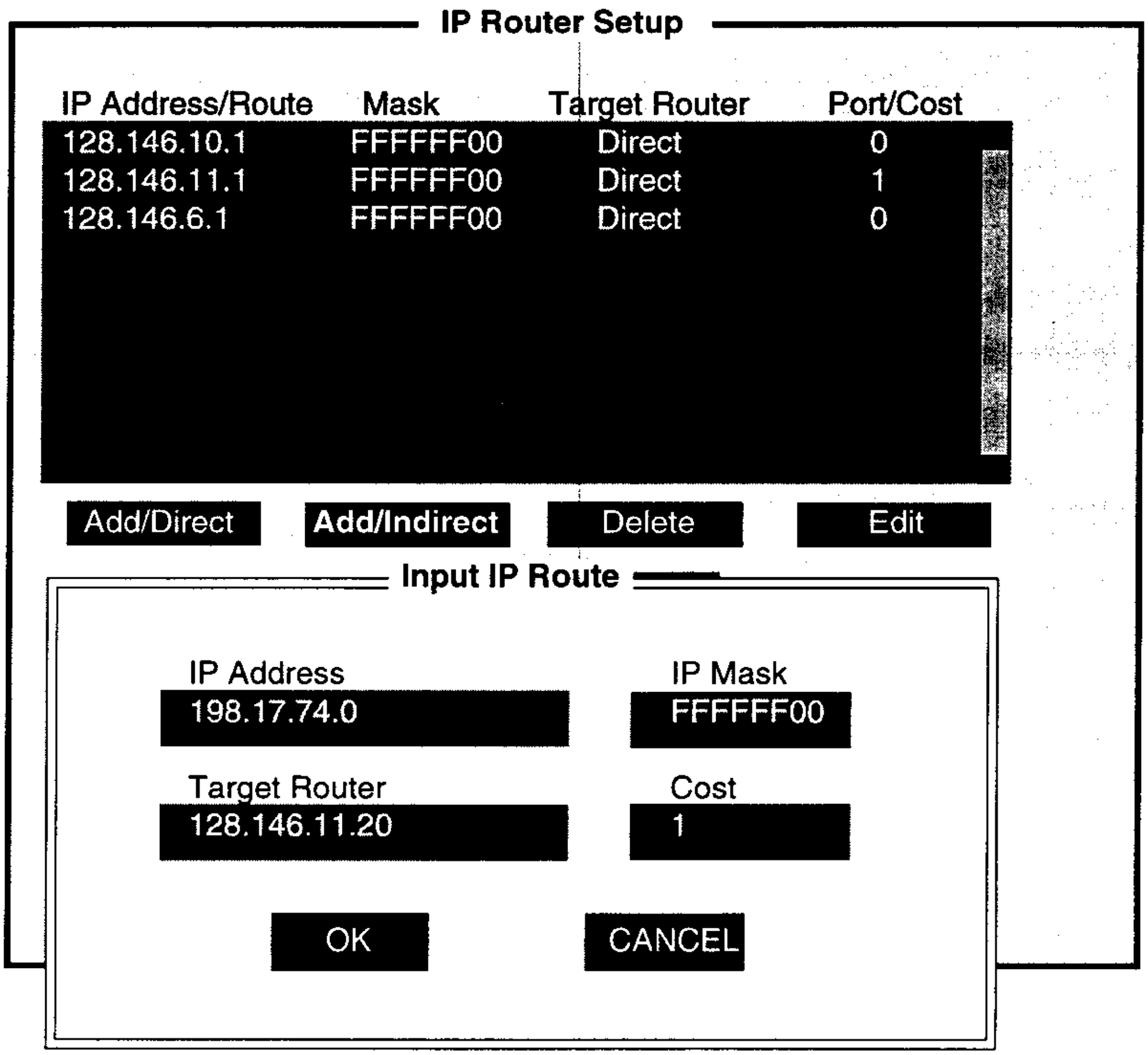
IP Address: 128.146.10.1

IP Mask: FFFFFF00

Port: 0

Add/Indirect

This button activates a menu which is used to specify the "indirect" routes for this Pinnacle Link Router. These routes are sometime referred to as static routes. You can use indirect routes to define the way to get to subnets that are attached to other routers in your network. As an example, if subnet 198.17.74.0 is attached to a router 128.146.11.20 in order for this Pinnacle Link Router to route packets to 198.17.74.1 you should specify an entry that is setup as: IP Address = 198.17.74.0;
IP Mask = FFFFFF00; Next Hop = 128.146.11.20 with a Cost = 1.



IP Router Setup

IP Address/Route	Mask	Target Router	Port/Cost
128.146.10.1	FFFFFF00	Direct	0
128.146.11.1	FFFFFF00	Direct	1
128.146.6.1	FFFFFF00	Direct	0

Input IP Route

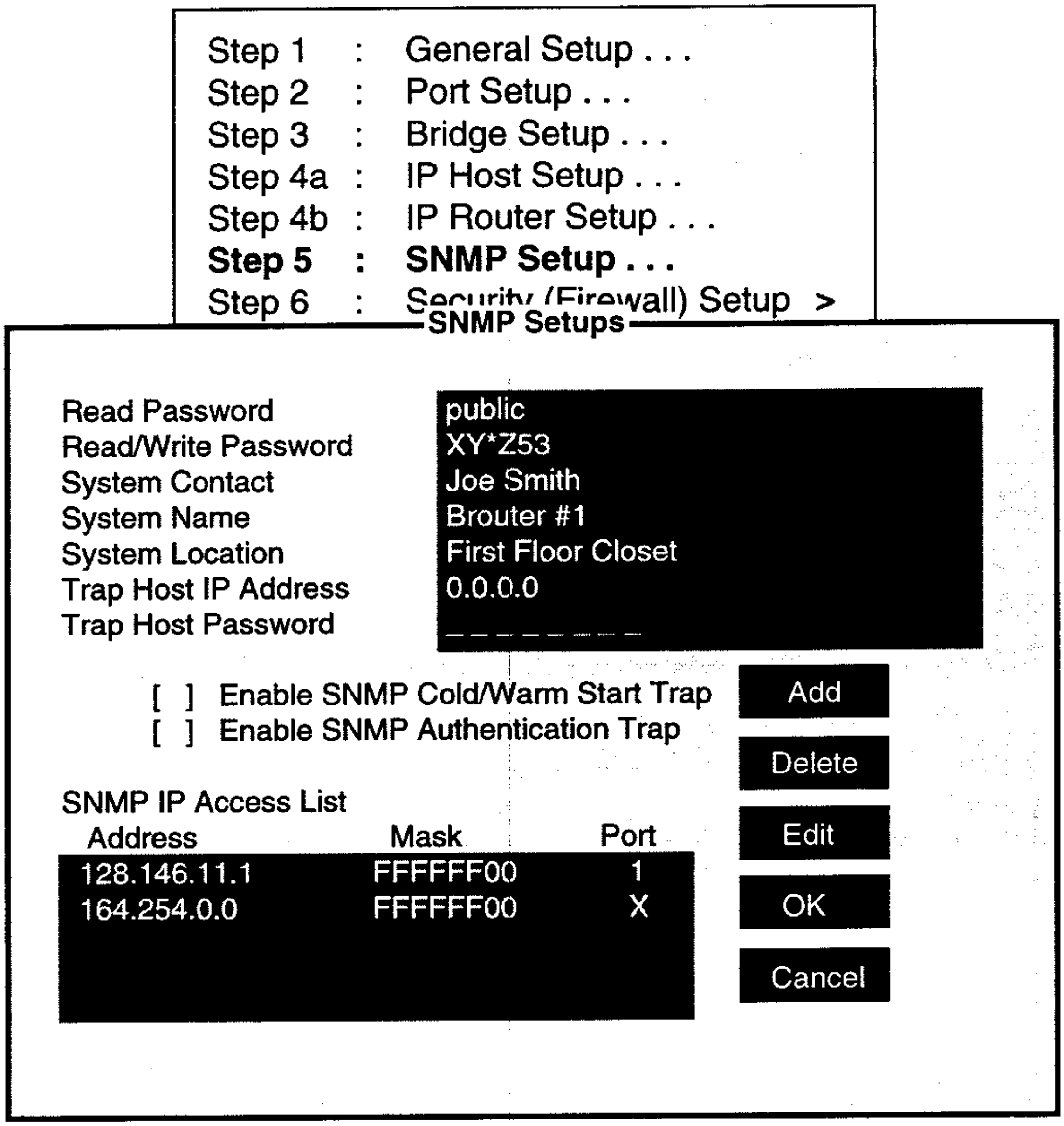
IP Address: 198.17.74.0

IP Mask: FFFFFF00

Target Router: 128.146.11.20

Cost: 1

Step 5: SNMP SETUP



Step 1 : General Setup . . .
Step 2 : Port Setup . . .
Step 3 : Bridge Setup . . .
Step 4a : IP Host Setup . . .
Step 4b : IP Router Setup . . .
Step 5 : SNMP Setup . . .
Step 6 : Security (Firewall) Setup >

SNMP Setups

Read Password: public
Read/Write Password: XY*Z53
System Contact: Joe Smith
System Name: Brouter #1
System Location: First Floor Closet
Trap Host IP Address: 0.0.0.0
Trap Host Password: _ _ _ _ _ _ _ _

[ ] Enable SNMP Cold/Warm Start Trap
[ ] Enable SNMP Authentication Trap

SNMP IP Access List

Address	Mask	Port
128.146.11.1	FFFFFF00	1
164.254.0.0	FFFFFF00	X

Read Password
This is the read only password used for SNMP support. It is the SNMP password needed to read the Flash ROM Configuration and SNMP MIB Variables. The factory default value for this variable is the string *public.*

Read/Write Password
This is the read/write password used for SNMP support. It is the SNMP password needed to write the Flash ROM configuration and SNMP MIB variables in to the bridge/ router. The string should be set to a value that is known only by you. The factory default value for this variable is the string *public* and should be changed to a string known only to you.

System Contact

This field should contain the identification of the contact person for this SNMP managed node, (i.i., this bridge/router) together with information on how to contact this person.

System Name

This field should contain the administratively assigned name for this managed node. By convention, this is the node's fully-qualified Internet domain name(ex: bridge20.karlnet.com).

System Location

This field should contain the physical location of this node (e.g.,`telephone closet, 3'rd floor').

Trap Host IP Address

This is the IP address of a network connected host that is setup to receive SNMP Trap messages from this bridge/router. If you do not have an SNMP Trap host then set this to 0.0.0.0.

Trap Host Password

This is the SNMP read/write password (community name) of the host that is setup to receive SNMP Trap messages. This field is ignored if the Trap Host IP Address described above is 0.0.0.0.

[X] Enable SNMP Cold/Warm Start Trap

If Cold/Warm Start traps are enabled then an SNMP Trap will be sent to the trap host whenever this bridge/router powers up, is restarted because of an internal software error, has just completed a Flash ROM reprogram and restart cycle, or reboots because the watchdog timer expired. Please see "Enable Watchdog Reboot Timer" under the General Setup Menu.

[X] Enable SNMP Authentication Traps

If SNMP authentication Traps are enabled adn a Trap Host is setup properly then an SNMP Trap will be sent to the to the trap host whenever an SNMP request is made of the bridge/router where the password (community name) is wrong.

SNMP IP Access List

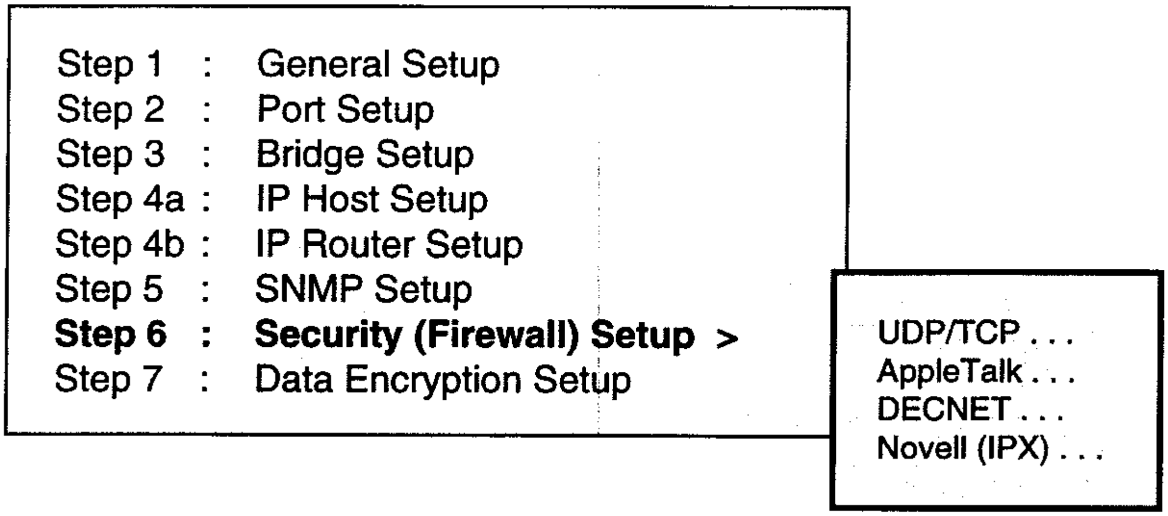
You can optionally setup a list of networks, subnets and hosts that are authorized to access the Pinnacle Link Bridge/Pinnacle Link Router via SNMP. SNMP access lists are used in conjunction with well picked SNMP passwords and the special SNMP hardware protection jumpers to prohibit unauthorized access into the Flash ROM configuration database of this bridge/router.

Examples:

1. IP Address: 128.146.11.0 Mask: FFFFFF00 Port: 1 will only allow SNMP access from the Network 128.146.11.x and only if the SNMP request was made from the portion of the network attached to Port 1.

2. IP Address: 164.254.0.0 Mask: FFFF0000 Port: X will only allow SNMP access from the network 164.254.x.x received from any port.

STEP 6: SECURITY (FIREWALL) SETUP



Security firewalls are enabled in the "General Setup" menu. If Security Filters are enabled and if the protocols that have security firewall capability (i.e. IP/UDP/TCP, AppleTalk, DECNET, or Novell IPX) are enabled to be passed through the bridge/ brouter then additional protection is added with these protocols. Security filters will cause the Pinnacle Link Bridge/Pinnacle Link Router to analyze on the application level each packet to determine if it should be passed or dropped.

Remote & Local Menus

Some of these menus are marked "Remote" and some are marked "Local". Remote menus configure filters that pertain to networks, subnets, and/or hosts that are connected to the Remote network (i.e. the Remote port of the Pinnacle Link Bridge/Pinnacle Link Router). Local menus configure filters that pertain to network, subnets, and/ or hosts that are connected to the Local network (i.e. the Local port of the Pinnacle Link Bridge/Pinnacle Link Router).

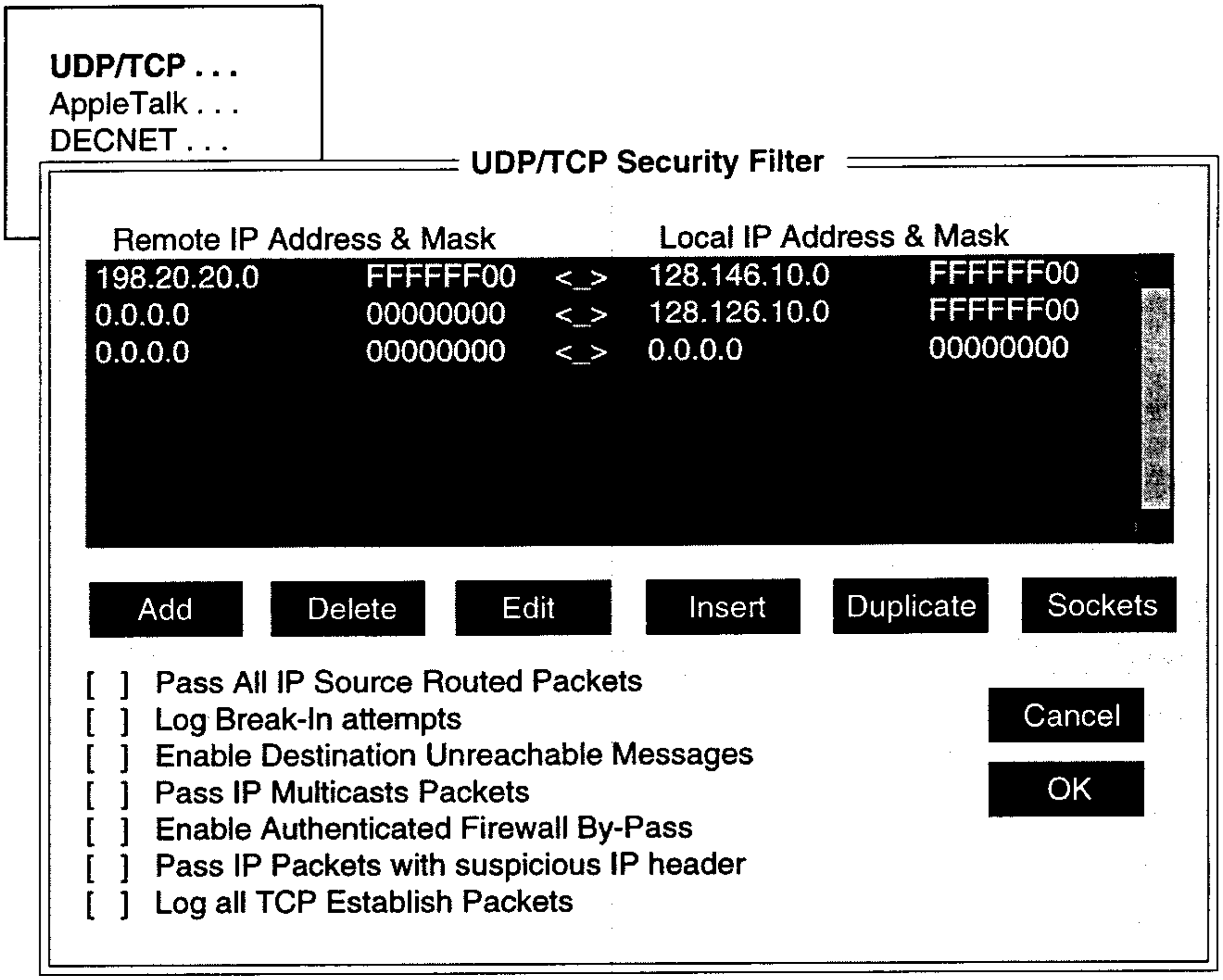
You can determine weather a port is remote and local by looking at the Port Setup Menu.

Pass or Drop Menu modes:

The menus can be in a mode to either pass (permit) or drop (deny) their items. The concept is that in most situations one wants to either drop a few selected items or to pass a few selected items of each type. If the menu is EMPTY and is set-up to "Pass Following..." then all packets of that type will be dropped. This is because you are passing an empty menu therefore nothing will be passed. If the menu is EMPTY and is set-up to "Drop Following..." then all packets of that type will be passed.

IP/UDP/TCP Security Filter

(This will only appear if IP is being bridged or routed)



Remote IP Address & Mask			Local IP Address & Mask	
198.20.20.0	FFFFFF00	<_>	128.146.10.0	FFFFFF00
0.0.0.0	00000000	<_>	128.126.10.0	FFFFFF00
0.0.0.0	00000000	<_>	0.0.0.0	00000000

[ ] Pass All IP Source Routed Packets
[ ] Log Break-In attempts
[ ] Enable Destination Unreachable Messages
[ ] Pass IP Multicasts Packets
[ ] Enable Authenticated Firewall By-Pass
[ ] Pass IP Packets with suspicious IP header
[ ] Log all TCP Establish Packets

Remote/Local IP Address Menu & Mask

This menu specifies the IP network, subnet, and/or single machine that is to have its IP packets passed, dropped, logged, or encrypted. Each packet's IP source and destination address is checked against each entry in the list to determine what action should be performed on the packet. *Matching is performed on the first entry first* and then goes down the list looking for the first match. When a match is found the action specified by the socket menus for that line is performed immediately. The packet's IP addresses are logically "anded" with the mask and then compared with the IP address to determine if a match has occurred.

NOTE: This menu specifies the IP networks, IP subnets and IP Hosts on the remote network that hosts on the local network can communicate with. This menu does not specify IP routes and is not used to setup IP Routing.

[X] Pass All IP Source Routed Packets

Source routed packets are special IP packets that are rarely used. There are certain situations where they can also be used by hackers to spoof firewalls. You should set this to *drop* unless you know you need to pass source routed packets.

[X] Log Break-In Attempts

Enabling the logging of break-in attempts will cause a Syslog packet to be sent to the Syslog server each time the security filter module detects and drops a packet.

[X] Enable Destination Unreachable Messages

Destination unreachable messages are normally sent by routers when a packet is unable to be delivered to it's final destination due to one of several reasons. If the dropped packet is a UDP packet then usually an ICMP Destination Unreachable packet is sent to the originator of the dropped IP packet. If the packet is a TCP packet then a TCP Reset packet is usually sent. If you enable this feature then the Pinnacle Link Bridge/Pinnacle Link Router's security module will send either an ICMP destination unreachable packet or a TCP Reset packet to the originator of the dropped packet. This feature is helpful because software such as telnet will quickly detect that a connection cannot be made. This feature is helpful but can also tip off a potential hacker that a security firewall is being used.

[X] Pass IP Multicast Packets

IP multicast packets are normally used for M-Bone audio and video data transmissions on a local network. IP multicast packets will penetrate through bridges and can cause abnormal behavior on some network attached computers. It is recommended that you Drop IP multicast packets unless you know you need them.

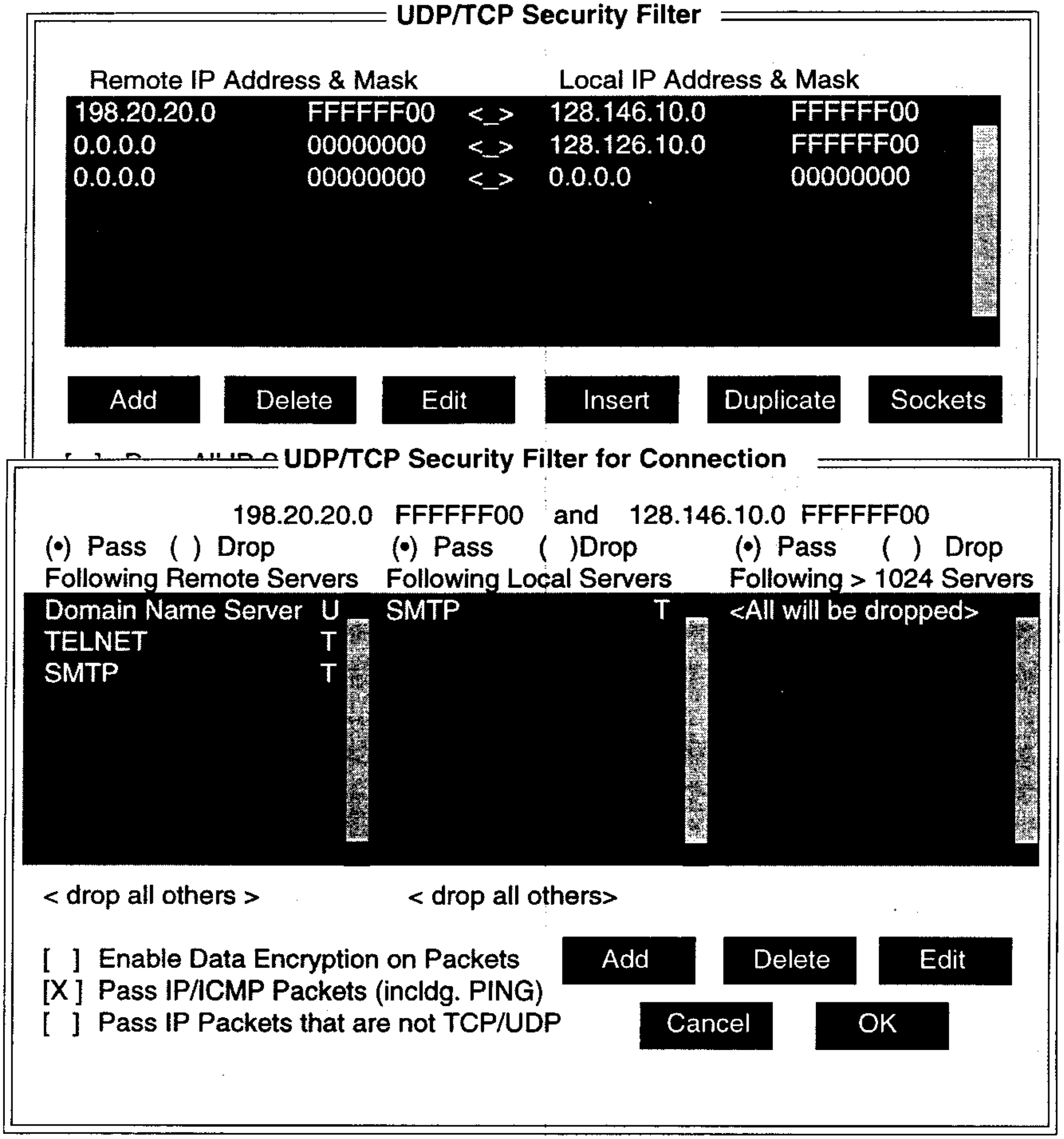
[X] Enable Authenticated Firewall By-Pass

The Pinnacle Link Bridge/Pinnacle Link Router's UDP/TCP firewall filters can be dynamically bypassed. This feature enables data between particular subnets or hosts to flow through the firewall untouched by any security filters. This feature is very powerful and can be used to create a way to authenticate access by logging into a particular network or host. If enabled this feature can also be used by a hacker to gain unauthorized access to your network. If you enable this feature you must take great care to setup SNMP passwords and access lists to prevent such unauthorized tampering with your firewall.

[X] Pass IP Packets with suspicious IP header

If you set this to "drop" then each IP packet that passes through the Pinnacle Link Bridge/Pinnacle Link Router is checked for inconsistencies in its IP header. If an anomaly is found the packet is dropped.

[X] Log all TCP Establish Packets
Each IP/TCP packet that travels through the bridge/router is checked to see if it is the special TCP/IP SYN packet. This type of packet is always sent in a TCP/IP network to initiate a TCP connection. As an example when the Telnet client attempts to connect to a Telnet server it sends a TCP SYN packet. If you enable this setting a SYSLOG message will be sent to the SYSLOG server each time a TCP program attempts to connect to another TCP program such as the Telnet or FTP server.



UDP/TCP Security Filter

Remote IP Address & Mask			Local IP Address & Mask	
198.20.20.0	FFFFFF00	<_>	128.146.10.0	FFFFFF00
0.0.0.0	00000000	<_>	128.126.10.0	FFFFFF00
0.0.0.0	00000000	<_>	0.0.0.0	00000000

UDP/TCP Security Filter for Connection

198.20.20.0 FFFFFF00 and 128.146.10.0 FFFFFF00

(•) Pass ( ) Drop Following Remote Servers		(•) Pass ( )Drop Following Local Servers		(•) Pass ( ) Drop Following > 1024 Servers
Domain Name Server	U	SMTP	T	<All will be dropped>
TELNET	T			
SMTP	T			
< drop all others >		< drop all others>		

[ ] Enable Data Encryption on Packets
[X] Pass IP/ICMP Packets (incldg. PING)
[ ] Pass IP Packets that are not TCP/UDP

Once a packets source and destination IP address matches an entry in the Remote/ Local IP Address Menu the UDP/TCP sockets are tested against this menu to determine if the packet is to be passed or dropped.

Following Remote Servers

This menu specifies which sockets with values less then 1024 on computers connected to the remote port are to be passed and which are to be dropped.

Following Local Servers

This menu specifies which sockets with values less then 1024 on computers connected to the local port are to be passed and which are to be dropped.

Following > 1024 Servers

This menu specifies which sockets with values greater then or equal to 1024 on computers connected to either the local or remote port are to be passed and which are to be dropped.

[X] Enable Data Encryption on Packets

After a packets source and destination IP address matches an entry in the Remote/ Local IP Address Menu then he data portion of the UDP or TCP packet can be optionally encrypted (if received on the local port and destined for the remote port) or decrypted (if received on the remote port and destined for the local port). You can specify the encryption/decryption key on the Setup - Data Encryption Menu.

[X] Pass IP/ICMP Packets (including Ping)

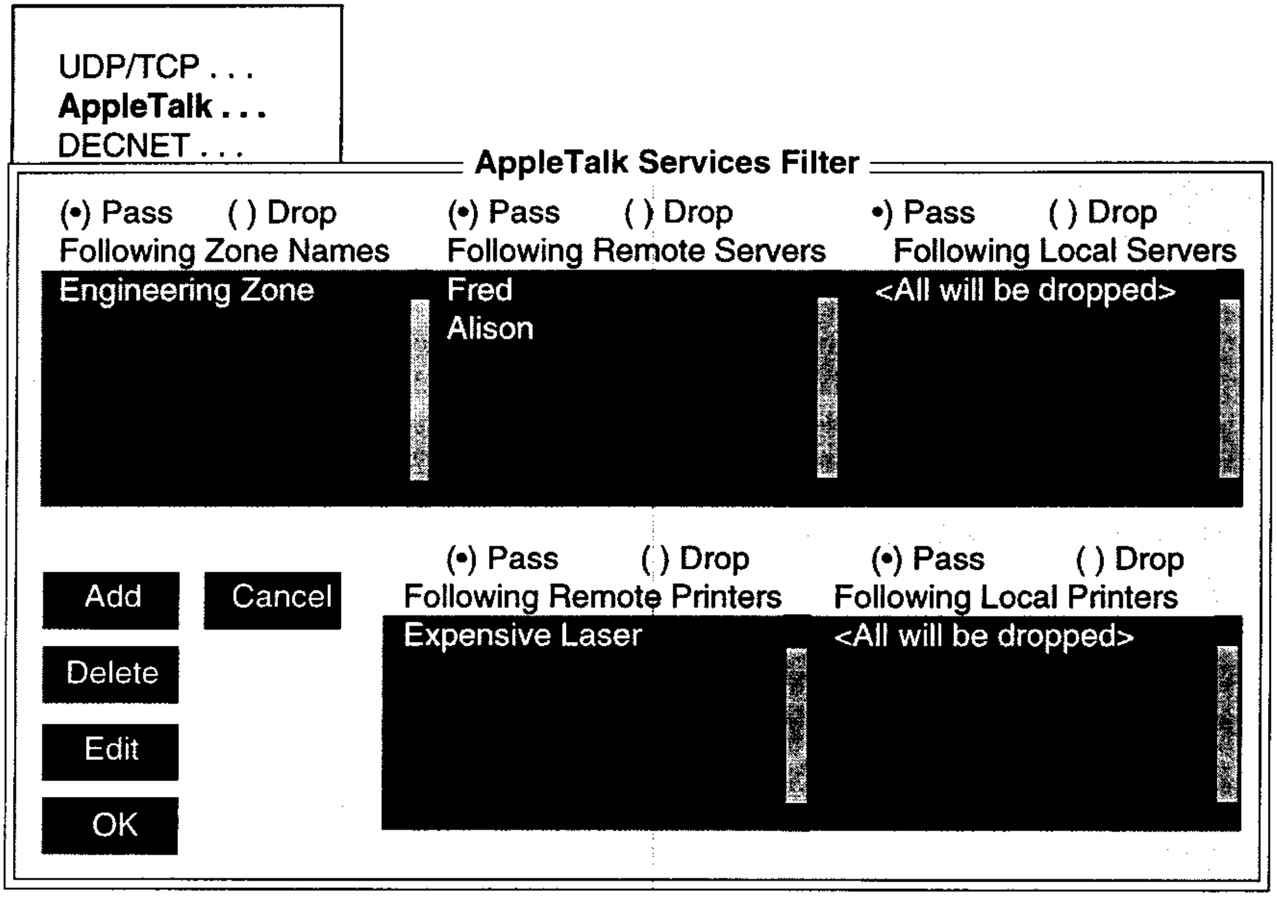
After a packets source and destination IP address matches an entry in the Remote/ Local IP Address Menu then it can be tested to see if it is an ICMP packet. You can optionally drop any ICMP packets to/from the matched IP addresses. This is helpful if you wish to allow ping packets to pass through the firewall. You can drop all ICMP (including Ping) packets if you wish to hide the computers on the other side of the firewall from potential hackers using ping to discover their existence.

[X] Pass IP Packets that are not TCP/UDP

If a packets source and destination IP address matches an entry in the Remote/Local IP Address Menu and if it is either TCP or UDP its socket number will be tested to see if it should be passed or dropped. If the packet is not UDP nor TCP then a decision must be made what to do with the packet since it does not have a socket number. Most IP packets are UDP or TCP with the exception of IGP. Since most LANs do not use IGP it is best to drop packets that are not UDP/TCP. This is helpful so keep hackers from sending non-UDP and non-TCP packets through the firewall.

APPLETALK FILTERS

(Will only appear if AppleTalk is being bridged)



AppleTalk Services Filter

(•) Pass ( ) Drop
Following Zone Names
Engineering Zone

(•) Pass ( ) Drop
Following Remote Servers
Fred
Alison

•) Pass ( ) Drop
Following Local Servers
<All will be dropped>

(•) Pass ( ) Drop
Following Remote Printers
Expensive Laser

(•) Pass ( ) Drop
Following Local Printers
<All will be dropped>

When Macintosh's are networked together, one of the undesirable side effects is that all Macintosh's can "see" in their Choosers all servers and all printers that are connected to the network. If multiple zones are specified then there is some form of protection but a user needs to only specify a zone and then can choose a printer to print to anywhere in the network. These menus will configure the Pinnacle Link Bridge to selectively restrict access to specified Apple servers and/or Apple printers. The Pinnacle Link Bridge is not an AppleTalk router. It does not have any of the characteristics of an AppleTalk router. The Pinnacle Link Bridge is simply a bridge that for AppleTalk can promote or prohibit the appearance of server and/or printer names in the chooser.

CAUTION: It is common characteristic of AppleTalk networks with multiple routers to have configuration problems if all of the routers do not agree on zone names and networks numbers. The Pinnacle Link Bridge is not an AppleTalk Router, it does not contribute to this problem. These menus will not, however, remedy this problem. If you wish to isolate a local AppleTalk network from a remote AppleTalk network you must be sure to drop AppleTalk and AppleTalk ARP in the "Ethernet Protocol Menu".

(•) Pass ( ) Drop Apple Zone Name Menu:
This menu specifies the AppleTalk Zone names that are to be passed or dropped. Each of the Apple Zones can be named in this menu. The menu entry * (single asterisk) is the standard AppleTalk code that means "my Zone". As an example; if the Local LAN's Zone name is Tiger and if you wish to see in your chooser printers and servers from a Remote LAN with the Zone name Tiger, then two entries must appear in this menu, the string Tiger and on the next line an *. This is because sometimes AppleTalk explicitly asks for printers and servers in the Zone Tiger and sometimes it uses the * as shorthand for Tiger (i.e. "my Zone").

(•) Pass ( ) Drop Apple Remote Servers Menu:
This menu specifies the Remote file servers that are to appear in the Local LAN's Macintosh Choosers, regardless of Zone. If the Local LAN's Macintoshes are not to see any Remote file servers then this menu should be set to "Pass Apple Remote Servers" with no entries in it. This will force the Pinnacle Link Bridge to pass none of the Remote file server names to the Local LAN. If all Remote file servers are to be seen by the Local LAN then this menu should be empty and set to "Drop Apple Remote Servers".

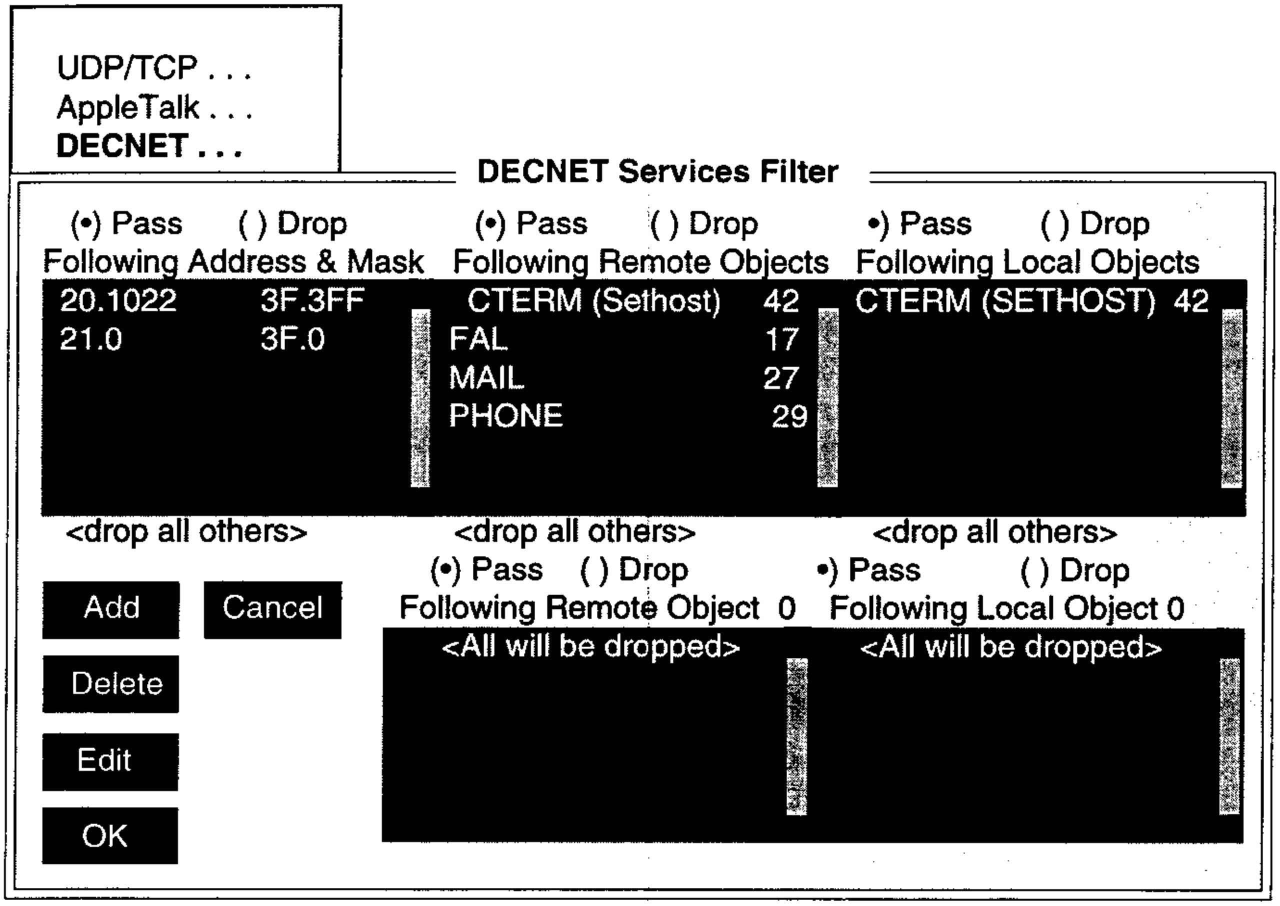
(•) Pass ( ) Drop Apple Local Servers Menu:
This menu specifies the Local file servers that are to appear in the Remote LAN's Macintosh Choosers, regardless of Zone. If the Remote Macintoshes are not to see any Local file servers then this menu should be set to "Pass Apple Local Servers" with no entries in it. This will force the Pinnacle Link Bridge to pass none of the Local LAN's file server names to the Remote network. If all of the Local file servers are to be seen by the Remote network then this menu should be empty and set to "Drop Apple Local Servers".

(•) Pass ( ) Drop Apple Remote Printers Menu:
This menu specifies the Remote printers that are to appear in the Local LAN's Macintosh Choosers, regardless of Zone. If the Local LAN's Macintoshes are not to see any Remote printers then this menu should be set to "Pass Apple Remote Printers" with no entries in it. This will force the Pinnacle Link Bridge to pass none of the Remote printer names to the Local LAN. If all Remote printers are to be seen by the Local LAN then this menu should be empty and set to "Drop Apple Remote Printers".

(•) Pass ( ) Drop Apple Local Printers Menu:
This menu specifies the Local printers that are to appear in the Remote LAN's Macintosh Choosers, regardless of Zone. If the Remote Macintoshes are not to see any Local printers then this menu should be set to "Pass Apple Local Printers" with no entries in it. This will force the Pinnacle Link Bridge to pass none of the Local LAN's printer names to the Remote network. If all of the Local printers are to be seen by the Remote network then this menu should be empty and set to "Drop Apple Local Printers".

DECNET FILTERS

(Will only appear if DECNET is being bridged)



UDP/TCP . . .
AppleTalk . . .
DECNET . . .

DECNET Services Filter

(•) Pass ( ) Drop
Following Address & Mask

20.1022	3F.3FF
21.0	3F.0

<drop all others>

(•) Pass ( ) Drop
Following Remote Objects

CTERM (Sethost)	42
FAL	17
MAIL	27
PHONE	29

<drop all others>

•) Pass ( ) Drop
Following Local Objects

CTERM (SETHOST)	42

<drop all others>

(•) Pass ( ) Drop
Following Remote Object 0

<All will be dropped>

•) Pass ( ) Drop
Following Local Object 0

<All will be dropped>

(•) Pass ( ) Drop Following Address & Mask Menu:
This menu specifies the DECNET Areas and Hosts that are to be passed or dropped. Each entry consists of a DECNET Address and an special Mask; a packet that matches is then either passed or dropped as specified. Each DECNET packet's source and destination address is checked against each entry in the list to determine if the packet is to be passed or dropped. Matching is performed on the first entry first and then goes down the list. When a match is found the action specified on that line is performed immediately. The packet's DECNET addresses are logically "anded" with the mask and then compared with the IP address to determine if a match has occurred. Addresses are specified in the standard DECNET syntax: Area.Host. The special mask is a hexadecimal number that specifies a bit mask to be "anded" with the packet's DECNET address prior to being comparing with the specified DECNET address.

NOTE: The Pinnacle Link Bridge is not a DECNET Router. This menu specifies the DECNET hosts and/or DECNET areas that hosts on either the local or remote network can communicate with.

(•) Pass ( ) Drop Remote Objects Menu:
This menu specifies the DECNET Objects on remote DECNET hosts that are to be passed or dropped. Each DECNET connect packet is checked against each entry in the list to determine if the packet is to be passed or dropped.

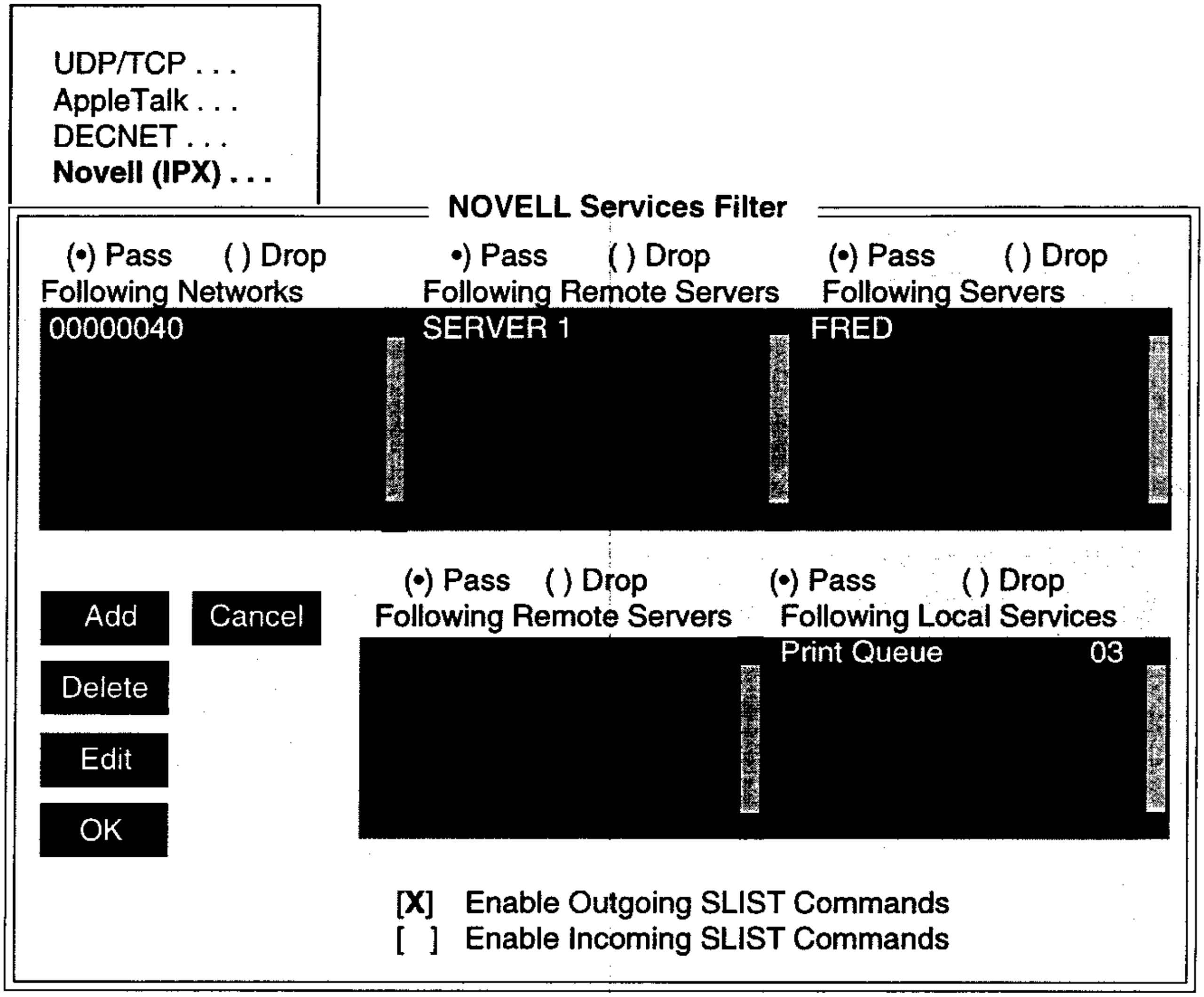
(•) Pass ( ) Drop Remote Object 0 Menu:
This menu specifies the DECNET Object 0 names on remote hosts that are to be passed or dropped. Each DECNET connect packet to DECNET Object 0 is checked against each entry in the list to determine if the packet is to be passed or dropped.

(•) Pass ( ) Drop Local Objects Menu:
This menu specifies the DECNET Objects on the local hosts that are to be passed or dropped. Each DECNET connect packet is checked against each entry in the list to determine if the packet is to be passed or dropped.

(•) Pass ( ) Drop Local Object 0 Menu:
This menu specifies the DECNET Object 0 names that are to be passed or dropped. Each DECNET connect packet to DECNET Object 0 is checked against each entry in the list to determine if the packet is to be passed or dropped.

NOVELL (IPX) FILTERS

(Will only appear if Novell is being bridged)



NOVELL Services Filter

(•) Pass ( ) Drop Following Networks: 00000040

•) Pass ( ) Drop Following Remote Servers: SERVER 1

(•) Pass ( ) Drop Following Servers: FRED

(•) Pass ( ) Drop Following Remote Servers

(•) Pass ( ) Drop Following Local Services: Print Queue 03

[X] Enable Outgoing SLIST Commands

[ ] Enable Incoming SLIST Commands

When Novell systems are networked together, one of the undesirable side effects is that all Novell servers can be seen by all other Novell servers and clients that are connected to the network. These menus will configure the Pinnacle Link Bridge/Pinnacle Link Router to selectively restrict access to specific Novell networks, servers and/or services. The Pinnacle Link Bridge/Pinnacle Link Router is not a Novell router. It does not have any of the characteristics of a Novell router. The Pinnacle Link Bridge/Pinnacle Link Router is simply a bridge that for Novell IPX can promote or prohibit specific services.

Following Networks

This menu specifies the Novell networks that will be passed (permitted) or dropped (denied) through the Pinnacle Link Bridge/Pinnacle Link Router. You can use it to firewall off specific Novell networks from other Novell networks.

Following Remote Servers

This menu specifies the Remote Novell servers that are to be accessible by the Local LAN's.

Following Local Servers

This menu specifies the Local Novell servers that are to be accessible by the Remote LAN's.

Following Remote Services

This menu specifies the Remote Novell services that are to be accessible by the Local LAN's.

Following Local Services

This menu specifies the Local Novell services that are to be accessible by the Remote LAN's.

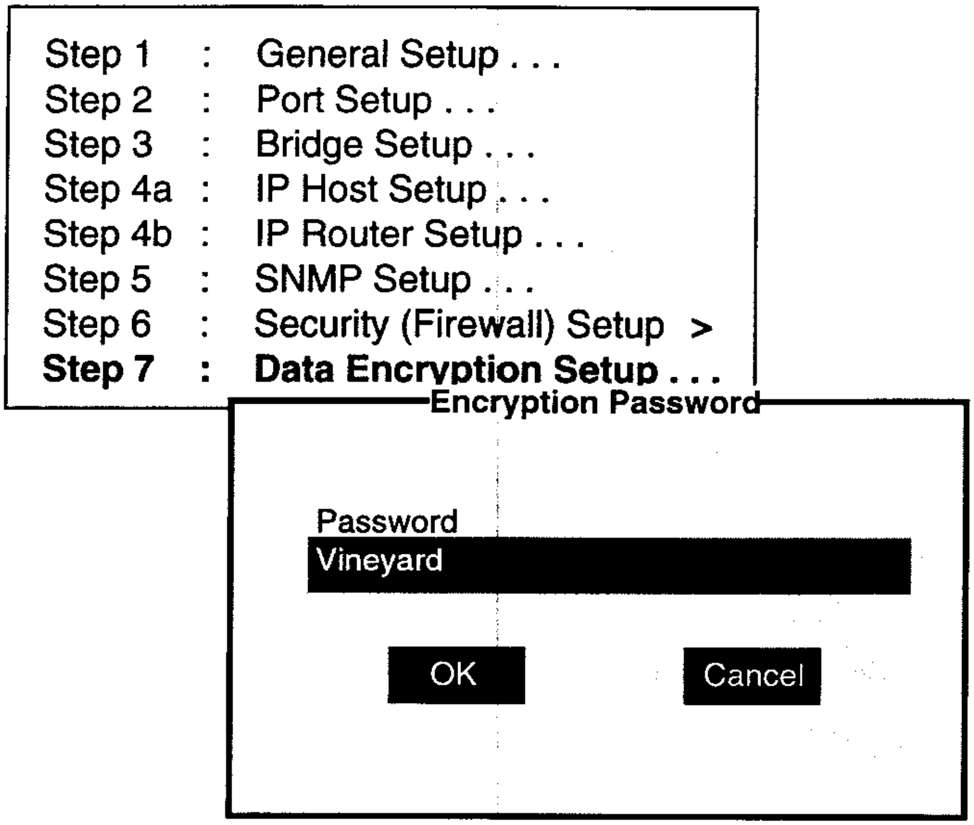
[X] Enable Outgoing SLIST Commands

The Novell SLIST and related commands bypass the normal Novell Remote Server Pinnacle Link Bridge/Pinnacle Link Router filters. This is a special filter that enables or disables the Novell server listing commands from local clients to remote servers.

[X] Enable Incoming SLIST Commands

The Novell SLIST and related commands bypass the normal Novell Remote Server Pinnacle Link Bridge/Pinnacle Link Router filters. This is a special filter that enables or disables the Novell server listing commands from remote clients to local servers.

STEP 7: DATA ENCRYPTION SETUP

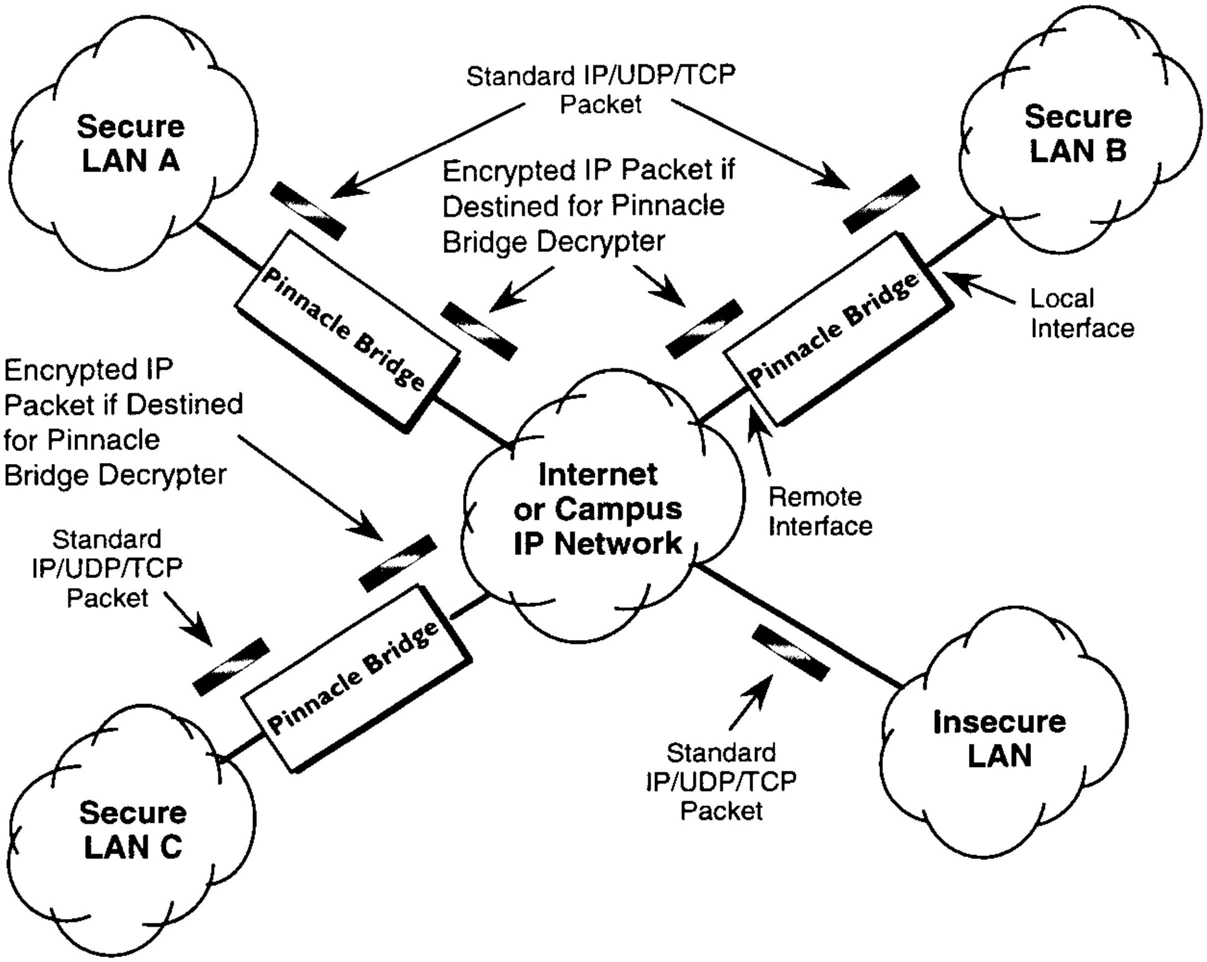

Step 1 : General Setup . . .
Step 2 : Port Setup . . .
Step 3 : Bridge Setup . . .
Step 4a : IP Host Setup . . .
Step 4b : IP Router Setup . . .
Step 5 : SNMP Setup . . .
Step 6 : Security (Firewall) Setup >
Step 7 : Data Encryption Setup . . .
Encryption Password
OK
Cancel

Password
Vineyard

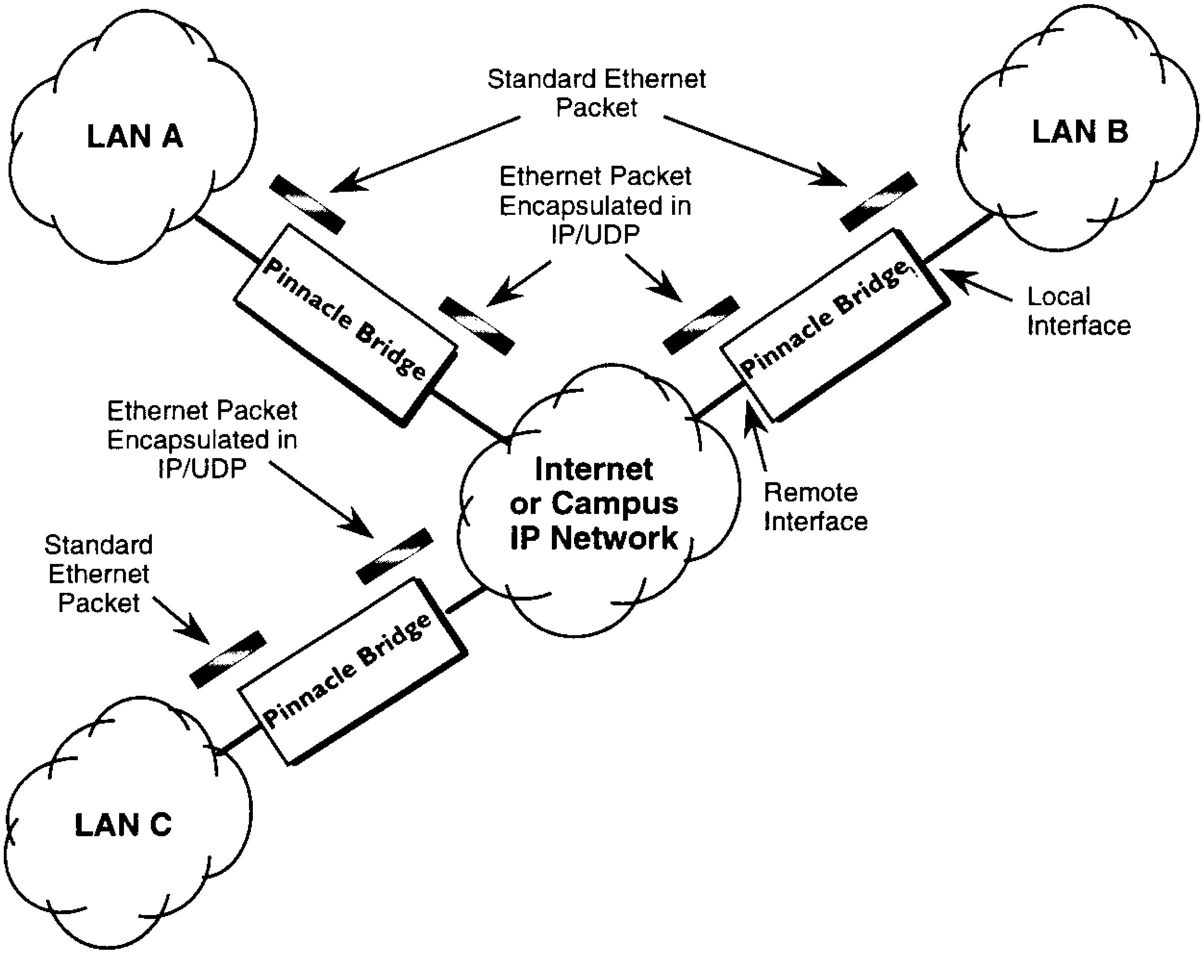
Data Encryption

The Pinnacle Link Bridge/Pinnacle Link Router contains a proprietary software encryption algorithm developed in the United Kingdom. This encryption algorithm can be applied to Pinnacle Link Bridge Tunneled packets, IP UDP/TCP packets or all packets sent to or received from a particular non-Ethernet port.

Adding Data Encryption
(To IP/UDP/TCP Packets)


Secure LAN A
Standard IP/UDP/TCP Packet
Secure LAN B
Encrypted IP Packet if Destined for Pinnacle Bridge Decrypter
Pinnacle Bridge
Pinnacle Bridge
Local Interface
Encrypted IP Packet if Destined for Pinnacle Bridge Decrypter
Internet or Campus IP Network
Remote Interface
Standard IP/UDP/TCP Packet
Pinnacle Bridge
Insecure LAN
Standard IP/UDP/TCP Packet
Secure LAN C

Generic Ethernet Tunneling
(Through an IP Network)


LAN A
Standard Ethernet Packet
LAN B
Ethernet Packet Encapsulated in IP/UDP
Pinnacle Bridge
Pinnacle Bridge
Local Interface
Ethernet Packet Encapsulated in IP/UDP
Internet or Campus IP Network
Remote Interface
Standard Ethernet Packet
Pinnacle Bridge
LAN C