IntraPort Carrier-8 Chassis
Administrator's Guide

Compatible Systems Corporation
4730 Walnut Street
Suite 102
Boulder, Colorado 80301

303-444-9532
800-356-0283
http://www.compatible.com

IntraPort Carrier-8 Chassis Administrator's Guide
Version 1

Part number: A00-1855

FCC Notice: This product has been certified to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules. It is designed to provide reasonable protection against radio or television communication interference in a commercial environment. Operation of this equipment in a residential area could cause interference with radio or television communication.

Table of Contents

Table of Contents

Introduction to the IntraPort Carrier-8

The IntraPort Carrier-8 (IPC) is a Layer 3 to Layer 2 gateway designed to let Network Service Providers (NSPs) sell services that provide secure access to traditional networks such as Frame Relay via IPSec-based Virtual Private Network (VPN) client sessions.

The IPC terminates Layer 3 IPSec sessions which were initiated by PCs running VPN Client software. Client PCs may be connected to the IP infrastructure (on or off a particular NSP's network) via dial-up or direct Ethernet attachment. The IPC administrator determines whether these sessions are encrypted and/or digitally signed.

Traffic from client sessions is typically decrypted and authenticated by the IPC, and then switched into pre-specified Layer 2 virtual circuits (VCs), if a WAN interface is in use, or routed onto the Ethernet at the POP. The process also works in reverse, with traffic received from a specific VC or POP network typically being encrypted and digitally signed before being routed to the appropriate client session.

RADIUS authentication can be used to provide general access control to the IPC, along with returning information regarding which set of pre-configured parameters a client session should be assigned.

IPC systems are based on a two-slot chassis that can hold one or two I/O cards. Currently available I/O cards include 3DES - DS3, 3DES - HSSI and DES - 10/100 Ethernet. These can be used in any combination desired.

IntraPort Carrier-8 Manual Overview

The manual is divided into several sections that should provide you with the basic information you will need to use the IntraPort Carrier-8 on your network. For the latest documentation on Compatible Systems products, including the most current version of this manual, visit the Technical Support section of our Web site.

Chapter 1 - Getting Started

This part of the manual describes the contents of the IntraPort Carrier-8 package and emphasizes the preparation and equipment you will need to install the server.

Chapter 2 - Mounting Instructions

This part of the manual includes detailed instructions for mounting the IntraPort Carrier-8 in a variety of equipment racks.

Chapter 3 - Powering Up the Server

This part of the manual includes information on the voltage switch and instructions for powering up the device.

Chapter 4 - CompatiView Software Installation

This part of the manual describes how to install CompatiView, Compatible Systems' GUI (Graphical User Interface) management software which is included with your server.

Chapter 5 - Command Line Preparation

This part of the manual provides basic instructions for using command line management and text-based configuration to configure a server.

Chapter 6 - Functionality and Configuration Overview

This part of the manual provides a minimal list of parameters that must be entered into a server for proper operation.

Chapter 7 - Test Switch Settings

This part of the manual describes the test switch settings.

Appendices

This part of the manual includes additional information that might be of interest to you such as technical specifications, some maintenance procedures and instructions for downloading current software.

Chapter 1 - Getting Started

A Few Notes

Please Read the Manuals

The manuals included with your IntraPort Carrier-8 VPN Access Server contain very important information about installing and operating the IntraPort Carrier-8. Please read this manual, and refer to the management reference guides as required. It's worth the few minutes it will take.

Also, please fill out the warranty registration card and return it to us today. This will help us keep you informed about updates to the IntraPort Carrier-8 and future products available from Compatible Systems.

You can also register on the Web at http://www.compatible.com. If you'd like to be notified via e-mail about new products and receive important news from Compatible Systems, please join our e-mail list on the Web.

Warranty and Service

The IntraPort Carrier-8 is covered by the Compatible Systems Integrated Support Package, which includes a lifetime comprehensive warranty, a twenty-four hour advance replacement program, unlimited phone support and software upgrades for the life of the product. A 24 x 7 support plan is also available.

Compatible Systems maintains copies of current software updates on the Internet. You may download product software from the Internet at any time. For more information on downloading current product software, see Appendix B.

Getting Help with the IntraPort Carrier-8

If you have a question about the IntraPort Carrier-8 and can't find the answer in one of the manuals included with the product, please visit the technical support section of our Web site (http://www.compatible.com). This site includes extensive technical resources which may answer many of your questions. You can also request technical support by filling out a brief form. Technical support requests received via the Web form will receive expedited treatment. You may also call Compatible Systems Corporation or send support questions via e-mail to support@compatible.com. Compatible Systems' phone number is listed on the front of this guide. We will be happy to help you.

What You Will Need to Get Started

Before connecting the IntraPort Carrier-8 VPN Access Server, please check the list below to make sure that you have received all of the items that are supplied with the shipping package(s).

You should also make sure you have any additional items that are necessary to connect the server to your network.

Supplied with the IntraPort Carrier-8

Please check your shipping package(s) for the following items:

- IntraPort Carrier-8 unit
- 2 power cords
- One left rack-mount bracket
- One right rack-mount bracket
- Two mounting ears
- Two handles
- Two handle spacers
- 14 mounting screws (10-32 undercut flat head)
- One DB-25 male to DB-25 female console cable
- One reusable replacement air filter
- CD-ROM including:
  - CompatiView software for Windows
  - Operating software
  - VPN Client software
  - HTML version of product documentation (which can be viewed with your favorite Web browser)
- *VPN Client Reference Guide*
- *CompatiView Management Software Reference Guide*
- *Text-Based Configuration and Command Line Management Reference Guide*
- Warranty registration card

Additional Items Needed for Installation

- If you choose to rack-mount the IntraPort Carrier-8, you will need to provide your own screws or clips to secure the mounting brackets to the equipment rack. A more detailed list of the items needed for mounting the server is in Chapter 2 - Mounting Instructions.
- Before connecting the IntraPort Carrier-8 to your network, you need to make sure that you have the necessary interface cabling equipment. See each I/O card's Network Installation section for details.

Chapter 2 - Mounting Instructions

The IntraPort Carrier-8 VPN Access Server is designed to be mounted in a 19-inch equipment rack or in a Telco rack. Compatible Systems provides all the parts necessary for securing the supplied mounting brackets and ears to the device; however, due to the variety of equipment racks and mounting techniques, you will need to provide your own screws or clips to secure the mounting brackets and ears to the equipment rack.

Placement Considerations

There are several things to consider when preparing to install the IntraPort Carrier-8 VPN Access Server.

- Do not place the server on the floor, since it will more quickly accumulate dust. As alternatives to rack-mounting, it can be placed on a sturdy table or solid platform.
- A clean, air-conditioned environment is ideal.
- An open equipment rack (i.e., one without side enclosures or doors) is recommended for adequate ventilation.
- The chassis requires 13.5 shelf positions (23.5 vertical inches) of rack space.
- While no rear clearance is required, the front of the server needs adequate clearance for air circulation, RIOP card addition or replacement, cable connections, etc. At least two feet of front clearance and one inch of top clearance are recommended.
- Load the equipment rack from the bottom. For stability, it is strongly recommended that the IntraPort Carrier-8 VPN Access Server be placed in the bottom half of an equipment rack.

❖ **Note:** *When stacking other equipment on the IntraPort Carrier-8 VPN Access Server, do not exceed 35 pounds of evenly distributed weight on top of the server. Additional weight may bend the case.*

Safety Guidelines

To help ensure your safety and minimize potential damage to equipment, read and follow these guidelines before attempting to move or work on the IntraPort Carrier-8 VPN Access Server. These guidelines do not encompass all potential hazards. You must use good judgment and due caution when working with this or any other electrical device.

- The default setting for the voltage switch on the power supplies for the Carrier-8 is for a low input voltage (marked 115V on the switch). If your electrical system requires a high input voltage on the power supplies, you must change the settings before plugging in the server (for instructions, see Changing the Power Supply Voltage Settings).
- Never attempt to move the server using the RIOP card handles or the filter cover opening. They will not support the weight of the device. Use the built-in side handles and either the large mounting handles, if you have installed them, or the very bottom of the chassis to move it (see Figures 2 and 2.1).
- The IntraPort Carrier-8 VPN Access Server weighs approximately 110 pounds. Moving the server requires at least two people, able to bear 55 pounds of weight apiece. If your union or company policy outlines a lower maximum weight load per person, use the appropriate number of people.
- Make sure you have a clear path between the server and the equipment rack, platform or table before attempting to move it into place.

Warning: *All power cords and interface cables must be disconnected before you attempt to move or work on the IntraPort Carrier-8 VPN Access Server. Even the interface cables can deliver lethal doses of electricity.*

Parts and Tools

The following items are needed to install the mounting ears and handles on the IntraPort Carrier-8 VPN Access Server.

- IntraPort Carrier-8 unit
- Two mounting ears
- Two handles
- Two handle spacers
- 14 mounting screws (10-32 undercut flat head)
- Phillip's head screwdriver

In addition to the above items, the following items are needed to install the IntraPort Carrier-8 VPN Access Server in an equipment rack.

- One left rack-mount bracket
- One right rack-mount bracket
- One DB-25 male to DB-25 female console cable
- Tape measure (optional)
- Level (optional)
- Your own screws or clips, for fastening the brackets to the rack
- At least two people to lift the device into place. Do not attempt to move the device into the rack or onto a table or platform by yourself.

Changing the Power Supply Voltage Settings

The default setting for the voltage switches on the server's power supplies is for a low input voltage (marked 115V on the switch). If your electrical system requires a high input voltage on the power supplies, you must change it manually on the device before plugging the device in.

To change the settings:

1. Make sure the server is powered down and not connected to any power source.
2. Using a small screw driver, change the voltage switches to the desired setting (230V for high input voltage, 115V for low input voltage).

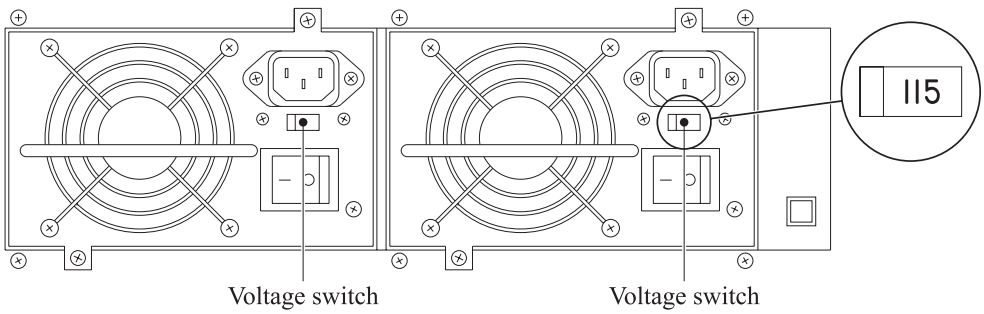

Figure 1. Location of Voltage Switch on the Power Supply

Rack-Mounting Instructions

Installing Mounting Ears and Handles

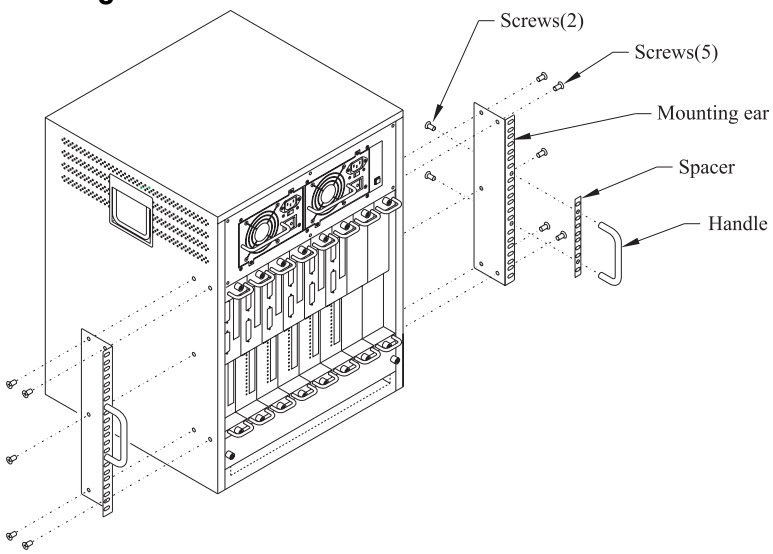

Figure 2. Installing Mounting Ears and Handles for a Standard Equipment Rack

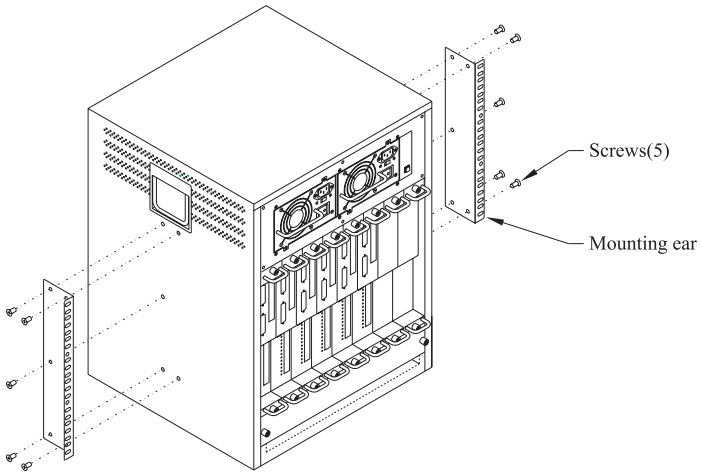

Figure 2.1. Installing Mounting Ears for a Telco Rack

The mounting ears should be installed on the IntraPort Carrier-8 VPN Access Server whether you are planning to rack-mount it or not. The handles need not be installed for Telco rack mounts because there is not enough finger room to use them, but the handles are recommended for all other installations.

If you are not going to rack-mount the IntraPort Carrier-8, it is recommended that you install the mounting ears and handles using the Standard Equipment Rack position (as shown in Figure 2).

1. Use the supplied screws and fasten the mounting ears to the sides of the device using 5 screws on each side as shown in Figure 2 (for a standard equipment rack) or in Figure 2.1 (for a Telco rack).
2. Use the supplied screws and fasten the handles and spacers to the center of the mounting ears as shown in Figure 2.

Rack-Mount Brackets

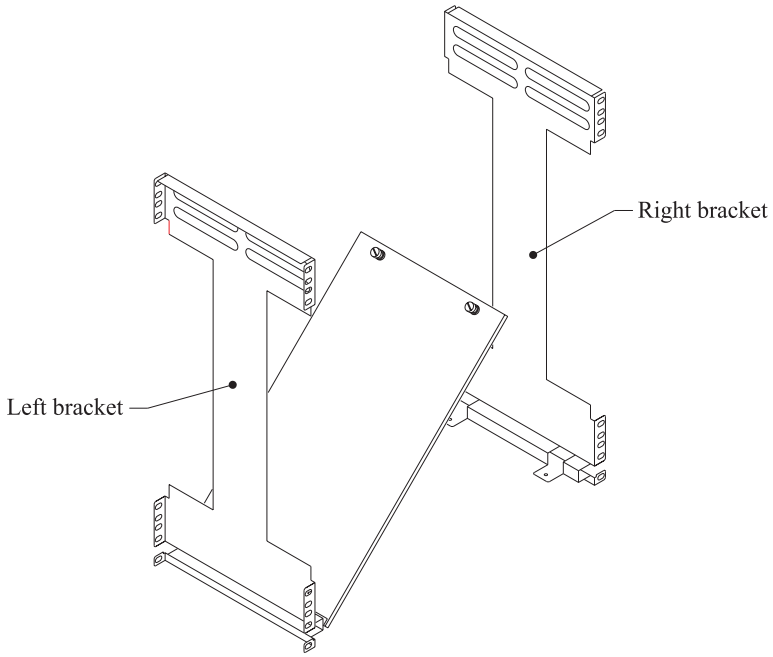

Figure 3. Rack-Mount Brackets

Brackets (shown in Figure 3) are provided for mounting the IntraPort Carrier-8 in a standard 19-inch equipment rack or a Telco rack. Note that the left bracket features a fold-down shelf which maintains the proper alignment of the brackets in the rack, but does not bear the weight of the unit. The ledges at the bottom of the brackets bear the weight of the unit until it is securely attached to the equipment rack. You will need to provide your own screws or clips to fasten the brackets and mounting ears to the equipment rack.

Right Bracket Installation

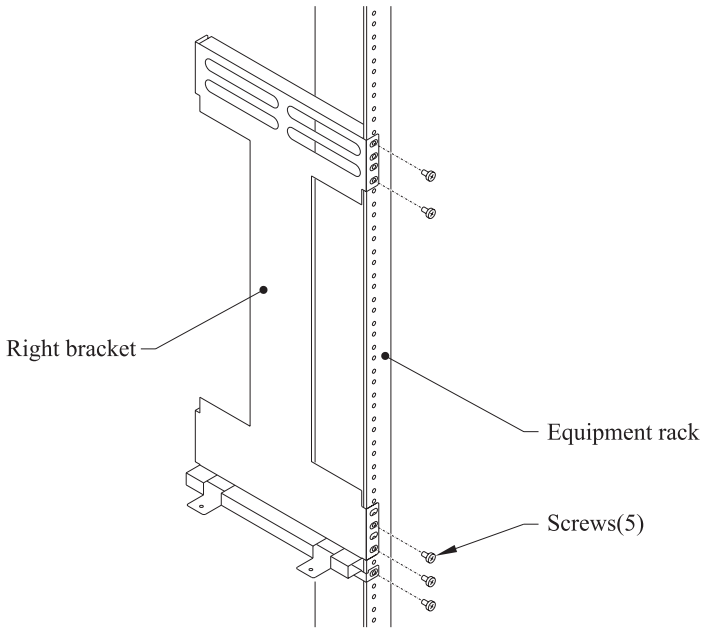

Figure 4. Fastening the Right Bracket to the Rack

1. It is recommended that you mark on the equipment rack exactly where you want the top of the two mounting brackets to go on the device in order to make sure that they are level with each other (using a level if necessary). Once you have determined the desired location, fasten the right bracket to the rack using your own screws or clips, as shown in Figure 4.

•At least 2 screws must be used to fasten the top of the bracket to the rack (using any two holes on the rack tab).

•At least 3 screws must be used to fasten the bottom of the bracket to the rack. One of the screws must be used to fasten the very bottom hole in the rack tab.

Left Bracket Installation

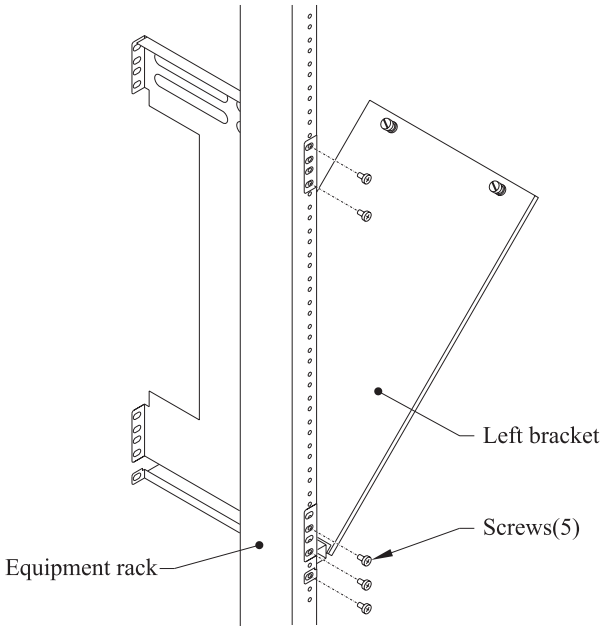

Figure 5. Fastening the Left Bracket to the Rack

1. It is recommended that you mark on the equipment rack exactly where you want the top of the two mounting brackets to go on the device in order to make sure that they are level with each other. Once you have determined the desired location, fasten the left bracket to the rack using your own screws or clips, as shown in Figure 5.

•2 screws must be used to fasten the top of the bracket to the rack (using any two holes on the rack tab).

•At least 3 screws must be used to fasten the bottom of the bracket to the rack. One of the screws must be used to fasten the very bottom hole in the rack tab.

Securing the Shelf

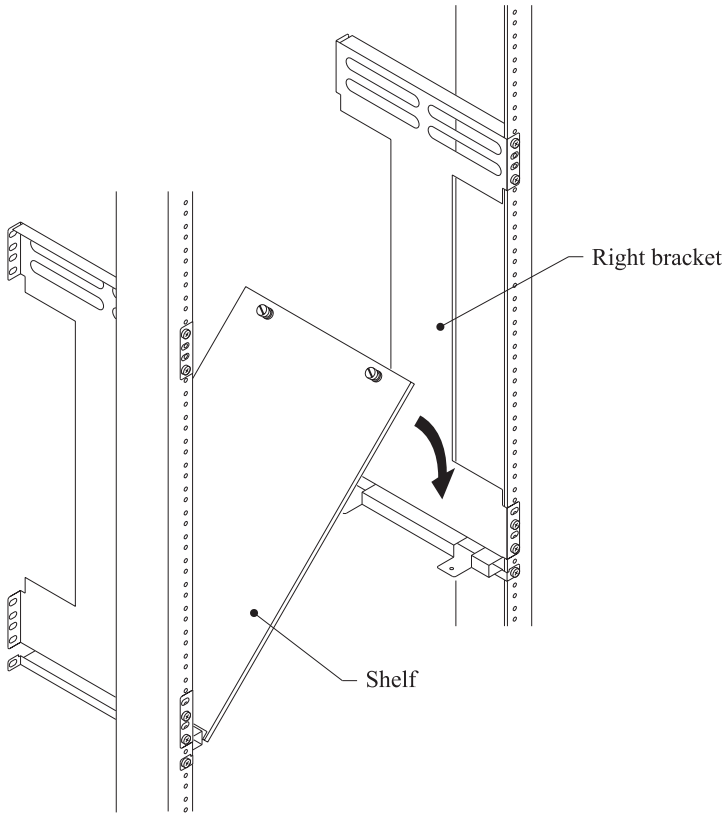

Figure 6. Lowering the Shelf

1. Lower the shelf onto the tabs protruding from the right bracket as shown in Figure 6 and use the thumb screws to fasten the shelf to the bracket. The brackets and shelf should look like Figure 6.1 when fully installed.

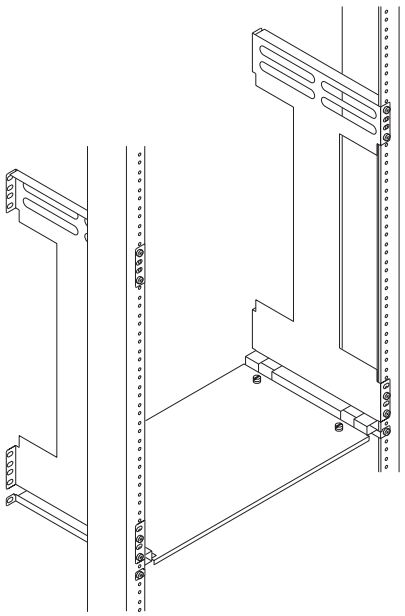

Figure 6.1. Securing the Shelf

Moving the Unit into the Rack

Never attempt to move the server using the RIOP card handles or the filter cover opening. They will not support the weight of the device. Use the built-in side handles and either the large mounting handles, if you have installed them, or the very bottom of the chassis to move it.

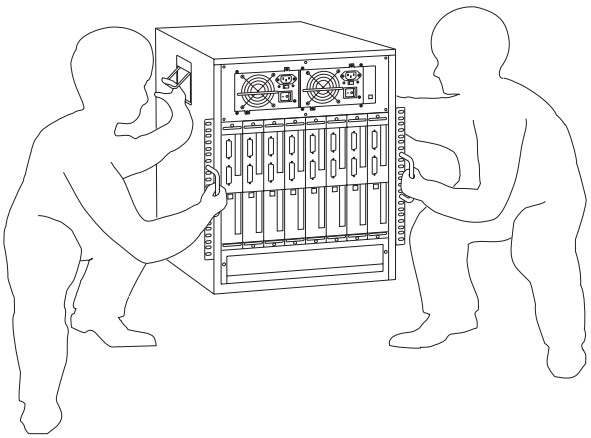

Figure 7. Moving the Unit into a Standard Equipment Rack

1. Two people are needed to move the unit into the rack. Do not attempt to move the unit by yourself. Holding the unit by the front and side handles as shown in Figure 7, carefully lift the unit and place it into the brackets.

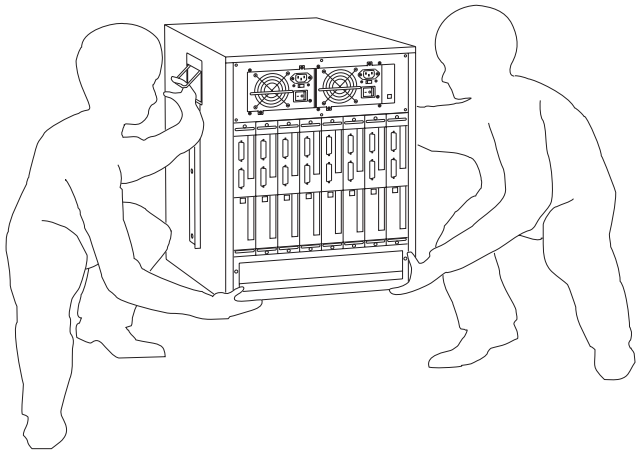

Figure 7.1. Moving the Unit into a Telco Rack

1. Two people are needed to move the unit into the rack. Do not attempt to move the unit by yourself. Holding the unit from the bottom and by the side handles as shown in Figure 7.1, carefully lift the unit and place it into the brackets.

Placing the Unit in an Equipment Rack

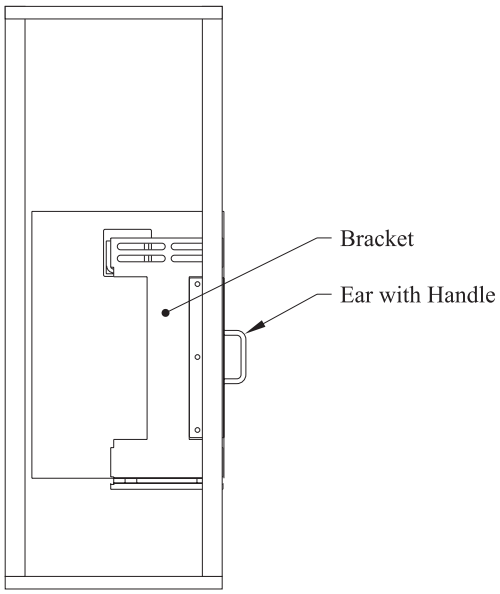

Figure 8. Placing the Unit in a Standard Equipment Rack

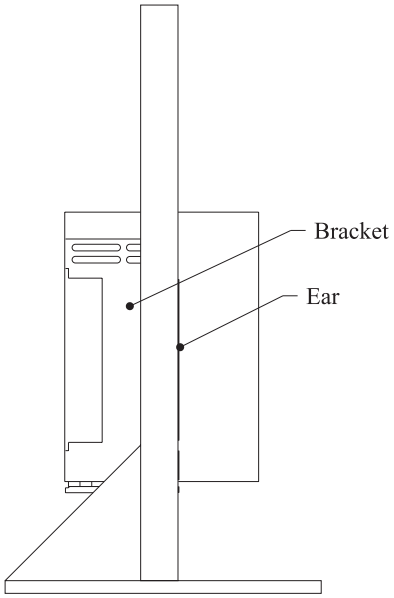

Figure 8.1. Placing the Unit in a Telco Rack

1. Slide the unit back into the rack until the mounting ears are flush with the sides of the rack.

   Proper placement in a standard equipment rack should look like Figure 8.

   Proper placement in a Telco rack should look like Figure 8.1.

Securing the Unit to the Rack

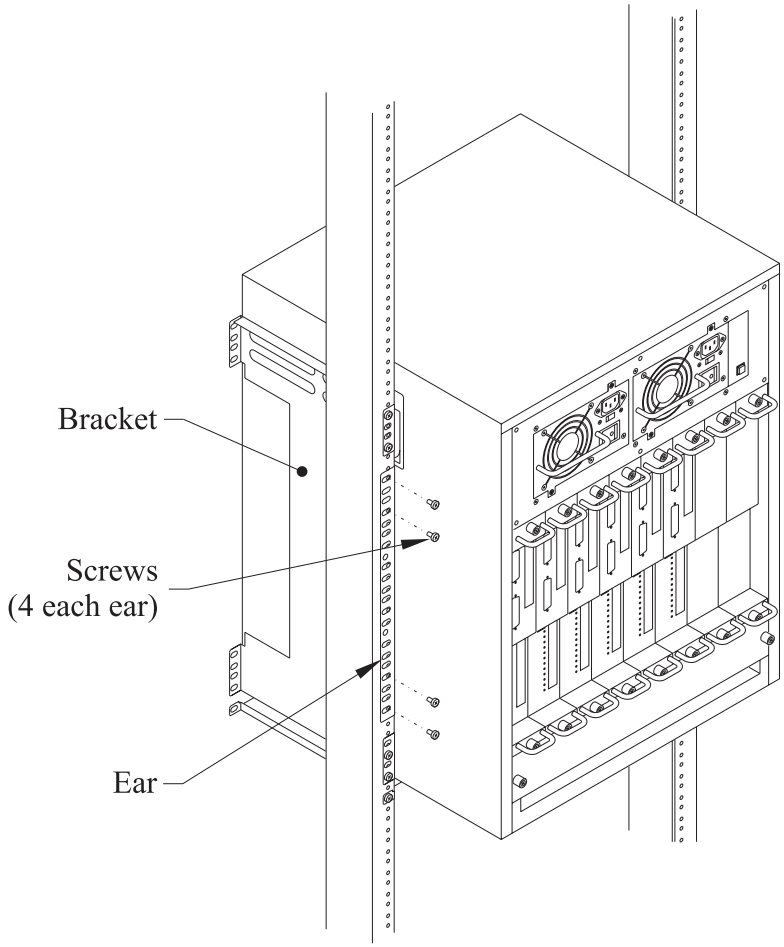

Figure 9. Securing the Unit to the Rack

1. Using your own screws or clips, secure the mounting ears to the rack as shown in Figure 9, using two screws at the top of each mounting ear and two screws at the bottom of each mounting ear.

Chapter 3 - Powering Up the Server

Powering Up the Server

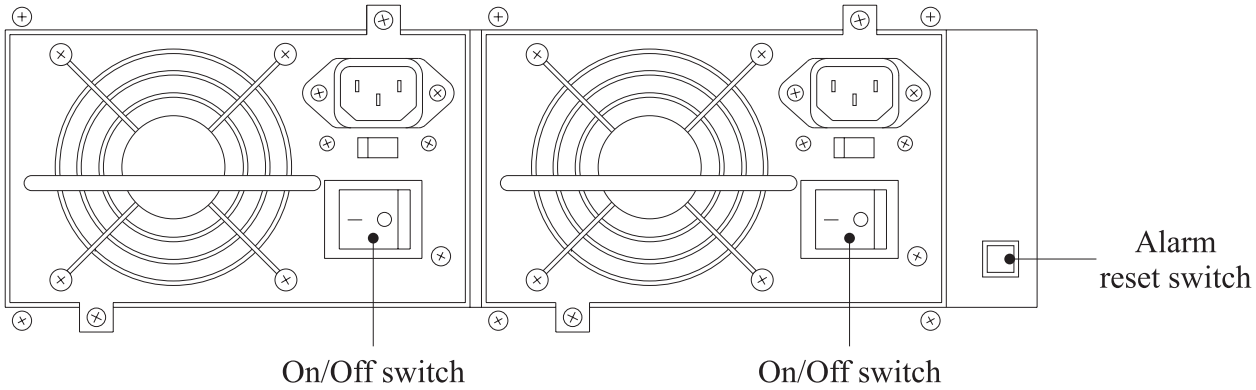

Figure 10. Detail of Power Units

❖ **Note:** *The default setting for the voltage switch on the power supplies for the Carrier-8 is for a low input voltage (marked 115V on the switch). If your electrical system requires a high input voltage on the power supplies, you must change the settings before plugging in the server (for instructions, see* Changing the Power Supply Voltage Settings*).*

The IntraPort Carrier-8 VPN Access Server features dual redundant 400 Watt power supplies. Operation using both power supplies is recommended, but not required.

1. Make sure the power switches are set to the “Off” position.
2. Connect the supplied power cords to the plug on each power unit on the front of the IntraPort Carrier-8.
3. Set each power switch to “On.”

At power-up, the server will take approximately one minute to become visible to CompatiView (see Chapter 4 - CompatiView Software Installation for more information).

Power Alarm Information

The power unit alarm will sound whenever a unit is unplugged or turned off. To reset the alarm, simply press the alarm reset switch.

Chapter 4 - CompatiView Software Installation

All of the products in Compatible Systems' internetworking and VPN families, including the IntraPort Carrier-8, can be managed from a single GUI management platform called CompatiView. CompatiView for Windows is included on the CD-ROM which was shipped with your IntraPort Carrier-8 VPN Access Server.

❖ **Note:** *An older version of CompatiView for Mac OS is also included on the CD-ROM shipped with your server. The Mac OS version can be used with other Compatible products such as MicroRouters and RISC Routers; however, it is not compatible with the IntraPort Carrier-8 VPN Access Server software. You must use CompatiView for Windows, versions 5.2.1 or later, to manage your server with CompatiView.*

CompatiView for Windows

CompatiView for Windows allows you to manage the server from an IBM-compatible PC running Windows 95/98 or Windows NT. The PC can either be configured as an IPX client on a Novell NetWare internet, or as an IP WinSock client on an IP internet.

System Requirements

In order to successfully run CompatiView for Windows, you need:

- IBM PC or compatible w/ 486 or later processor
- Microsoft Windows 95/98 or Windows NT installed
- VGA or better monitor
- IP - A WinSock-compatible transport stack

  and/or
- IPX - A Netware or Microsoft Client installation

❖ **Note:** *To choose the active transport protocol on a Windows machine which has both IPX and IP installed, select "Options" from the Database menu and click the General tab. Then select the appropriate radio button under "Transport."*

Installation and Operation

The Windows version of the CompatiView program can be found in the Network Management/CompatiView/Windows directory on the CD-ROM that was included with your IntraPort Carrier-8 VPN Access Server.

Run the auto-installation program (CV5x file) by double-clicking on it. The installation program will ask you to select (or create) a directory in which it should locate CompatiView and its associated files and database subdirectory.

Once the installation is complete, double click on the CompatiView icon to open the program. For further information on using CompatiView, see the *CompatiView Management Software Reference Guide* included with your server.

❖ **Note:** *For an up-to-date description of the changes (if any) made to Windows system files by the installation program, see the README.TXT file located in the CompatiView installation directory.*

Transport Protocols and CompatiView

CompatiView will be able to use the transport protocol (IP or IPX) you have selected to access Compatible Systems products anywhere on your internetwork. Depending on your security setup, you may also be able to use the IP transport option to manage devices across the Internet.

The IP protocol does not provide a method for CompatiView to automatically discover the IntraPort Carrier-8 VPN Access Server. To initially contact the server over IP using CompatiView, you must first enter a valid IP address into the server in one of two ways:

1. Use a console directly connected to the server.
2. If an Ethernet interface is installed on your Carrier-8, set a workstation's IP address to 198.41.12.2 with a Class C subnet mask (255.255.255.0) so that it can communicate over Ethernet with 198.41.12.1 (the shipping default of Ethernet 0:0).

After setting the server's IP address, be sure to change the workstation's configuration back to its original settings.

The IPX protocol does allow CompatiView to automatically discover the server. Compatible Systems devices are configured to autoseed the two most common IPX frame types upon startup (802.2 and 802.3 (raw)). If CompatiView has the IPX/SPX protocol selected as its transport, it will be necessary to either powerup the server before powering up the workstation, or reboot the workstation after the server has completed its boot sequence. This process will ensure that the workstation and the server have the proper IPX network bindings for communication.

Chapter 5 - Command Line Preparation

The command line interface allows you to configure and monitor the IntraPort Carrier-8 VPN Access Server in-band via Telnet or out-of-band with a terminal connected to the server's Console interface.

❖ **Note:** *Proper syntax is vital to effective operation of command line management. Case is not significant – you may enter commands in upper case, lower case, or a combination of the two.*

Out-of-Band Command Line Management

You can use command line management and text-based configuration out-of-band as a permanent management tool, or only temporarily in order to set the server's IP parameters to allow in-band Telnet access.

In order to access the command line out-of-band, do the following:

1. Set a terminal or a PC equipped with VT100 terminal emulation to a baud rate of 9600, 8 bits, no parity, 1 stop bit and no Flow Control.
2. Connect it to the server's Console interface using the cable which was supplied with the IntraPort Carrier-8.
3. Press the <Return> key one or two times.
4. Enter the default password ***letmein*** at the password prompt. The command line interface prompt will appear on the screen.

If you plan to use out-of-band access for ongoing management of your server, you can find further information on configuring your server in the documentation for the I/O card. Otherwise, see the section later in this chapter on Setting Up Telnet Operation for information on setting the server to allow Telnet access from hosts on its network.

Temporarily Reconfiguring a Host for Command Line Management

If no LAN-accessible interface (i.e., Ethernet) is installed in your IntraPort Carrier-8 VPN Access Server, then you can only use the Console port for command line management. If an Ethernet interface is installed, you can temporarily reconfigure an IP host in order to set the server's IP parameters to allow in-band Telnet access.

If you wish to set the server's basic IP parameters in this fashion, the host must be on the same Ethernet segment as one of the server's Ethernet interfaces. You can then do the following:

1. Set the host's IP address to 198.41.12.2, with a Class C subnet mask (255.255.255.0) and then Telnet to 198.41.12.1.
2. Enter the default password ***letmein*** at the password prompt. The command line interface prompt will appear on the screen.
3. Use the **configure** command and set the **IPAddress**, **SubnetMask**, and **IPBroadcast** keywords in the **IP Ethernet 0:0** section.
4. Use the **save** command to save the changes to the device's Flash ROM.
5. Change the host's configuration back to its original settings.

See the next section (Setting Up Telnet Operation) for information on setting the server to allow Telnet access from hosts on its network.

Setting Up Telnet Operation

Telnet is a remote terminal communications protocol based on TCP/IP. With Telnet you can log into and manage the IntraPort Carrier-8 from anywhere on your IP internetwork, including across the Internet if your security setup allows it. To manage the server with Telnet, you must:

1. Run Telnet client software on your local computer, which will communicate with the Telnet server built into the IntraPort Carrier-8.
2. You must also set some basic IP parameters in the server. The required parameters for Telnet access to an interface are the IP address, IP subnet mask, and IP broadcast address. There are several ways to set them.

•You may set them using text-based configuration either out-of-band via the Console interface or in-band via a reconfigured IP host. Instructions for setting up these two methods were given earlier in this chapter. Once you have set up the command line interface, do the following:

A. Use the **configure** command and set the **IPAddress**, **SubnetMask**, and **IPBroadcast** keywords in the **IP Ethernet 0:0** section.

B. Use the **save** command to save the changes to the device's Flash ROM.

•You may also use CompatiView from a reconfigured IP host (if using the IP transport protocol), or anywhere on your network (if using the IPX transport protocol). Instructions for these two methods are given in Chapter 4 - CompatiView Software Installation.

With CompatiView, basic IP parameters can be set using the TCP/IP Routing: Ethernet 0:0 Dialog Box. Use the Save to/Device option under the File menu to save the changes.

After you have set these IP parameters and saved the changes, you can use Telnet to access the server from any node on your IP network. Invoke the Telnet client on your local host with the IP address of the server you wish to manage.

Chapter 6 - Functionality and Configuration Overview

IntraPort Carrier-8 Functionality

This is a brief description of the IntraPort Carrier-8 functionality in terms of packet flows.

Routing From/To the Public Internet

VPN packets from the public Internet will be forwarded to and from the IPC via one or more PVCs. Depending on routing requirements, multiple PVCs can be used. A default route is required to forward wrapped VPN packets to the public Internet. The default route can be learned through either a routing protocol such as RIP or OSPF or can be configured manually.

Routing To/From a Corporate Intranet

Once a VPN packet is received via the public Internet, the IPC will perform the normal VPN sequence: decrypt, authenticate and translate source address. The source address will be translated from the pool of addresses assigned to the VPN Group through the configuration.

These unwrapped, normal IP packets will be forwarded to the corporation through a PVC that is associated with them. This can be accomplished through a route learned through a dynamic protocol (RIP or OSPF) or through a manually configured static route. The destination address in the static route is the corporate IP network and the gateway is the PVC. This can also be done by forwarding the Layer 3 tunnel to a Layer 2 PVC by mapping network traffic to a DLCI.

The router at the corporate site will need to be able to forward packets with the translated address back to the IPC so it can then do a VPN encapsulation to forward back to the public Internet.

Routing in General

The IPC will absolutely not allow routing between the private Frame Relay PVCs that are connected to the corporations that are used to deliver unwrapped VPN IP packets.

Sample Configuration

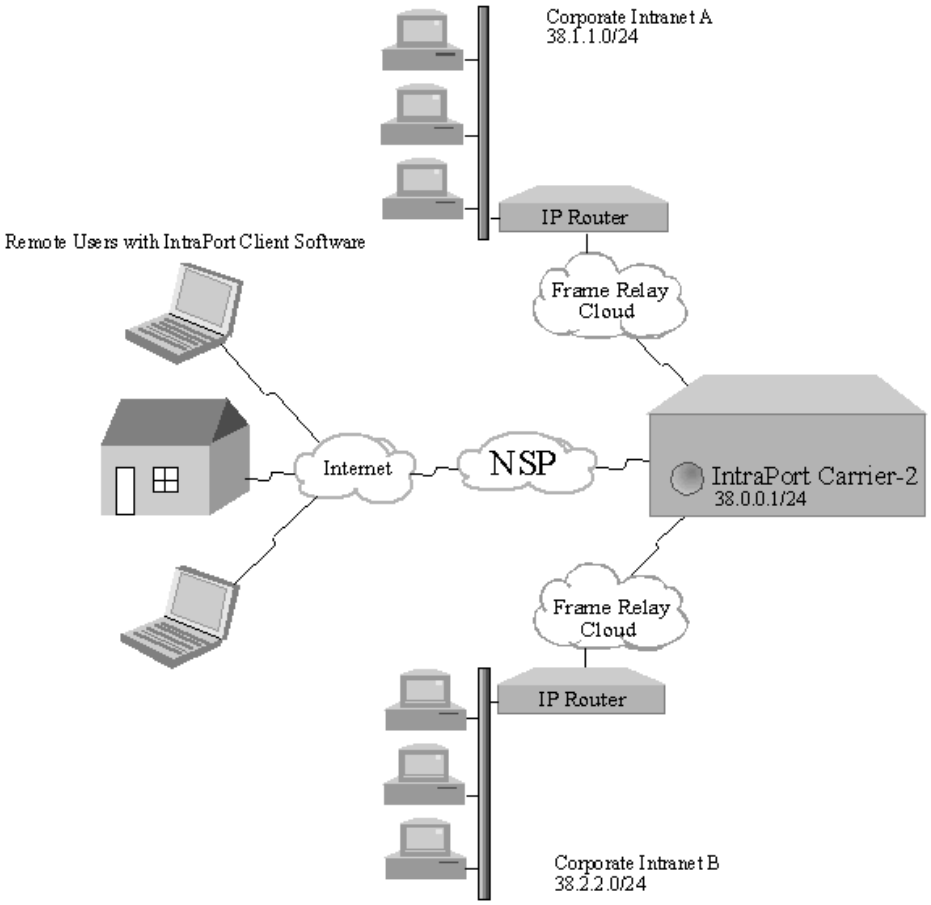

Figure 11. IntraPort Carrier-8 Configuration Example

The following text-based configuration would be for the IPC shown in Figure 11. Some sections include a detailed text description to help explain the VPN features. For details on the syntax or command line configuration reference, see the *Text-Based Configuration and Command Line Reference Guide*.

```
[ IP Wan 0 ]
Numbered                = On
Mode                    = Routed
RIPVersion              = V2
SubnetMask              = 255.255.255.0
IPAddress               = 38.0.0.1

[ Link Config Wan 0 ]
Mode                    = FrameRelay

[ Frame Relay Wan 0 ]
MaintProtocol           = AnnexD

[ General ]
SoftwareVersion         = IntraPortCarrier
DeviceType              = IntraPortCarrier


[ VPN Users ]
corpauser Config="Corporate A" SharedKey="corporatea"
```

```
corpbuser Config="Corporate B" SharedKey="corporateb"

# This is a sample user configuration for each of the corporations.
# This is the IPCs internal authentication database. These users
# may be stored in a RADIUS database and are only show here for
# for the example.

[ SNMP ]
AdminName                = IntraPortCarrier
Domain                   = ipc.pci.com
Location                 =

[ Logging ]
LogToAuxPort             = Off
Level                    = Debug
Enabled                  = Off

[ Bridging Global ]
Mode                     = Off

[ RADIUS ]
PrimAddress              = 38.100.100.1
Authentication           = TRUE
Accounting               = TRUE
Secret                   = Radius
[ VPN Group "Corporate A" ]
ipnet                    = 38.1.1.0/24
bindto                   = "Wan 0"
maxconnections           = 32
transform                = ESP(MD5,DES)
localipnet               = 38.0.0.100/27
vpngroupdlci             = 16

# This is the VPN configuration for Corporate A.
# The ’ipnet’ keyword specifies the IP address of the corporate LAN. These
# are the addresses that the client will get when a connection is established
# and used by it to create VPN packets to be forwarded to the corporate net.
# The ’localipnet’ specifies the pool of addresses that the IPC
# will use to translate the source address of the unwrapped IP packet
# being forwarded to the corporate intranet. This pool must be reserved
# for use by the IPC and should include as many addresses as specified
# in the 'maxconnections' keyword. The ‘vpngroupdlci’ maps this group’s
# tunnel traffic to a PVC.

[ VPN Group "Corporate B" ]
ipnet                    = 38.2.2.0/24
ipnet                    = 38.2.8.0/22
ipnet                    = 38.3.3.0/24
bindto                   = "Wan 0"
maxconnections           = 32
transform                = ESP(MD5,DES)
localipnet               = 38.0.0.132/27
vpngroupdlci             = 17

# This is the VPN configuration for Corporate B.
# This is similar to Corporation A's configuration. The main difference
# is that Corporation B has more IP addresses assigned to its intranet.
```

A more complicated configuration, showing two different VPN groups for Company A, and requiring all of Company B's VPN clients to tunnel all traffic back through the company intranet (and by extension through the company firewall for traffic which is bound for outside destinations) is shown below.

```
[ IP Wan 0 ]
Numbered                = On
Mode                    = Routed
RIPVersion              = V2
SubnetMask              = 255.255.255.0
IPAddress               = 38.0.0.1

[ Link Config Wan 0 ]
Mode                    = FrameRelay

[ Frame Relay Wan 0 ]
MaintProtocol           = AnnexD

[ General ]
SoftwareVersion         = IntraPortCarrier
DeviceType              = IntraPortCarrier
[ VPN Users ]
corpauser-den Config="Corporate A-Denver" SharedKey="corporatea"
corpauser-sf Config="Corporate A-SFrancisco" SharedKey="corporatea"
corpbuser Config="Corporate B-San Francisco" SharedKey="corporateb"

# This is a sample user configuration for each of the corporations.
# This is the IPCs internal authentication database. These users
# may be stored in a RADIUS database and are only shown here for
# for the example.

[ SNMP ]
AdminName               = IntraPortCarrier
Domain                  = ipc.pci.com
Location                =

[ Logging ]
LogToAuxPort            = Off
Level                   = Debug
Enabled                 = Off

[ Bridging Global ]
Mode                    = Off

[ RADIUS ]
PrimAddress             = 38.100.100.1
Authentication          = TRUE
Accounting              = TRUE
Secret                  = yourRadiusPW


[ VPN Group "Corporate A-Denver" ]
ipnet                   = 38.1.1.0/24
bindto                  = "Wan 0"
maxconnections          = 32
transform               = ESP(MD5,DES)
localipnet              = 38.0.0.100/27
vpngroupdlci            = 16

# This is the VPN configuration for the Denver office of Corporate A.
# The 'ipnet' keyword specifies the IP address of the corporate LAN. These
# are the addresses that the client will get when a connection is established
# and used by it to create VPN packets to be forwarded to the corporate net.
# The 'localipnet' specifies the pool of addresses that the IPC
# will use to translate the source address of the unwrapped IP packet
# being forwarded to the corporate intranet. This pool must be reserved
# for use by the IPC and should include as many addresses as specified
# in the 'maxconnections' keyword. The 'vpngroupdlci' maps this group's
```

```
# tunnel traffic to a PVC.

[ VPN Group "Corporate A-SFrancisco" ]
ipnet                    = 38.3.3.0/24
bindto                   = "Wan 0"
maxconnections           = 32
transform                = ESP(MD5,DES)
localipnet               = 38.0.0.200/27
vpngroupdlci             = 17

# This is the VPN configuration for the San Francisco office of Corporate A.
# It requires the same features configured as for the Denver office but
# the values will be different since it is has a different geographic
# location.

[ VPN Group "Corporate B" ]
ipnet                    = 0.0.0.0
bindto                   = "Wan 0"
maxconnections           = 32
transform                = ESP(MD5,DES)
localipnet               = 38.0.0.132/27
vpngroupdlci             = 18


# This is the VPN configuration for Corporate B.
# This is similar to Corporation A's configuration. The main difference
# is that Corporation B has more IP addresses assigned to its intranet
# and that all packets from Corporate B clients will be tunneled
# to the IntraPort. This is possible by specifying the wild card
# parameter 0.0.0.0 for the ipnet keyword.
```

Configuration Details

Frame Relay

The PVCs as shown are assumed to be through a Frame Switch, which isn't shown.

Routing

The default route for the IPC should be pointed to the public Internet to allow VPN packets to be forwarded. The default route can be learned through either a routing protocol such as RIP or OSPF or can be configured manually.

Clients

Clients can be anywhere on the NSP's network or the public Internet. They can be connected to a LAN or dialed-in to an Internet Access Provider. The client configuration involves specifying the IntraPort Carrier's IP address in the 'Primary IP Address' field of the Client UI. The client uses this address to forward VPN packets intended for the corporate intranet that the user wishes to reach.

The client will only VPN encapsulate and forward packets intended for the corporate intranet to the IPC. All other IP traffic from the client to other Internet sites will be forwarded without a VPN wrapper as it normally would. The clients learn about the IP networks from the IPC when it establishes a connection. These IP networks are specified as part of the IPC configuration.

Chapter 7 - Test Switch Settings

The switch for Slot 0 controls the entire device. For example, if you set the switch for Slot 0 to "3" and download new software to the device, all the other interfaces will automatically receive the software update from Slot 0 via the backplane. In general, the only time you should use an individual RIOP card's switch is when the card is unable to communicate with the backplane for some reason.

0	Normal Operation
1	Unused*
2	Unused*
3	Run Boot ROM Downloader
4	Unused*
5	Erase Flash ROM (OS and Configuration)
6	Erase Flash ROM (Configuration Only)
7	Unused*
8	Unused*
9	Allow letmein password for 5 minutes after powerup

Caution: *Settings marked with an asterisk may erase your Flash ROM. Please do not use these settings without first contacting Compatible Systems Technical Support.*

Appendix A - Connector and Cable Pin Outs

Pin Outs for DB-25 Male to DB-25 Female Console Cable

The cable supplied with the IntraPort Carrier-8 is twenty-five conductors, straight through. Connections on the console interface follow the standard RS-232C pin outs.

Appendix B - Downloading Software

From Compatible Systems

The latest versions of operating software for all Compatible Systems products are available at our Web site. The latest version of CompatiView management software is also available.

To download software, follow the instructions below:

1. Use your browser to access http://www.compatible.com/, and find the link on our home page to "Software Downloads."
2. Select the product and software version you want, and click on the appropriate file to download it.

❖ **Note**: *These files are also accessible directly via Anonymous FTP at* **ftp.compatible.com/files/**.

To the Device

Depending on which I/O cards are installed in your IntraPort Carrier-8 VPN Access Server, it may not have a LAN-accessible interface (i.e., Ethernet.) If this is the case, then new software versions must be downloaded to the device either through a WAN interface or through the RS-232 Console port.

If the WAN interface is not accessible for remote software image downloads, the download must be performed through the Console.

This can be done from a workstation running terminal emulation software (TERM) that supports Xmodem file transfers over a standard RS-232 serial asynchronous communications port (COM).

To download software to the device through the Console, follow the instructions below:

1. Make sure the software image file is accessible to the workstation.
2. Connect the IntraPort Carrier-8's Console port to the workstation's COM port using the Console cable which was included with your shipping package.
3. Launch the workstation's TERM application using a COM port rate of 9600 baud.
4. At the IntraPort Carrier-8 command line prompt enter: `set baud rate 115200 <Return>` (or the highest standard rate supported by the TERM application below 115,200).
5. The IntraPort Carrier-8 will prompt you to set the workstation's TERM application baud rate to match the entered value. Set the TERM application to the corresponding rate (115,200, ideally). Hit any key.
6. If the rates were set correctly, you will see a readable confirmation string. At the IntraPort Carrier-8 command line prompt enter the **sys rxmodem** command.
7. Press the Enter key.
8. Ensure that the TERM file transfer method is set for: Xmodem-1K, binary, and 16-bit CRC mode.
9. Initiate the transfer.
10. The TERM application will display the file transfer progress. When finished, the IntraPort Carrier-8 will reboot automatically. For access to the IntraPort Carrier command line, remember to return the TERM application to: 9600, 8 bits, no parity, 1 stop bit and no Flow Control.

Appendix C - Adding or Replacing RIOP Cards

The modular design of the IntraPort Carrier-8 VPN Access Server allows you to add, remove or replace the RIOP cards without disconnecting the device. Be sure to keep a cover plate over any empty slots to maintain proper air ventilation and minimize dust accumulation. The following instructions apply to adding or removing an RIOP card or cover plate.

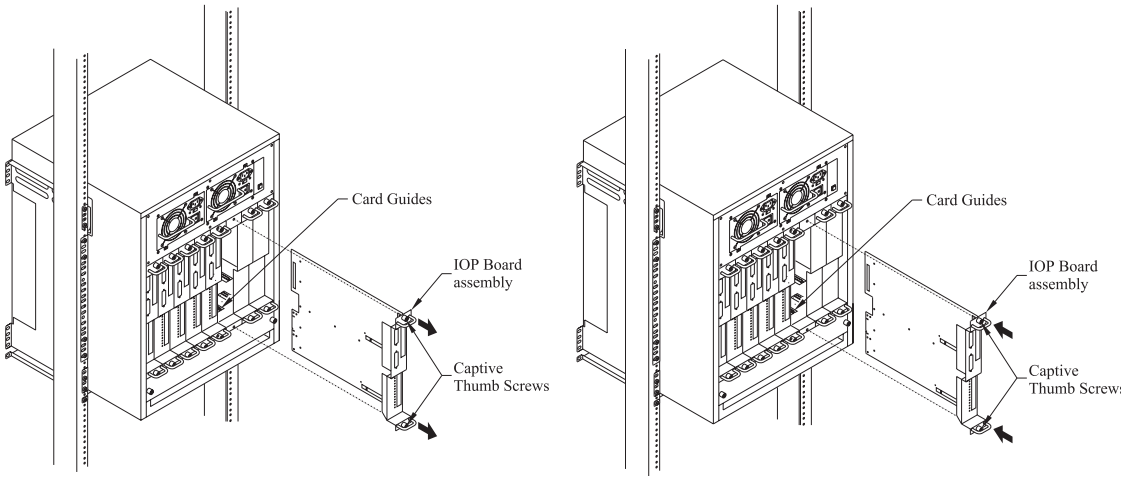

Figure 12. Removing and Replacing an RIOP Card or Cover Plate

1. Loosen the captive thumb screws on either end of the RIOP card you wish to remove.
2. Grasping only the handles on either end of the card, gently remove it from its slot. Place the card in a board rack or other safe place.
3. To add a card to an empty slot, grasp only the handles of the RIOP card and gently move the card along the guides into the slot.
4. Securely tighten the thumb screws.

Warning: *Do not place your hand or any object other than an RIOP card into a slot. Contact with any interior part could lead to a potentially fatal shock of electricity.*

Appendix D - When the “Over Temp” Light Comes On

The Intraport Carrier-8 is designed to operate reliably in a normal computer room, and requires no special environmental control. If operating within its published temperature and humidity specifications (0° to 45° C, up to 95% relative humidity, non-condensing, at 40° C) in a normal computer room, no periodic maintenance is required. If, however, an “Over Temp” light illuminates, it indicates that the internal circuitry is operating above its specified temperature range. If this happens, perform the following check sequence:

1. Verify that the server is installed properly in an environment in which the air temperature around the server is within the specified limits.
2. Verify that air flow to the front of the server is unrestricted.
3. If the above checks do not indicate a problem, it is probable that the air filter inside the chassis is clogged and must be cleaned or replaced. Follow the procedure outlined next to clean and replace the dust filter.

Replacing or Cleaning the Intraport Carrier-8 Air Filter

Under normal operation, the air filter does not require periodic maintenance. The filter should be replaced only when an excessive amount of dirt and dust has collected over an extended period of time. A replacement filter is supplied with the unit to minimize the unit’s down time when the filter is replaced.

Before attempting to change or clean the filter, the unit must be removed from its mounting in an equipment rack or on a wall. Changing or cleaning the filter is a simple process.

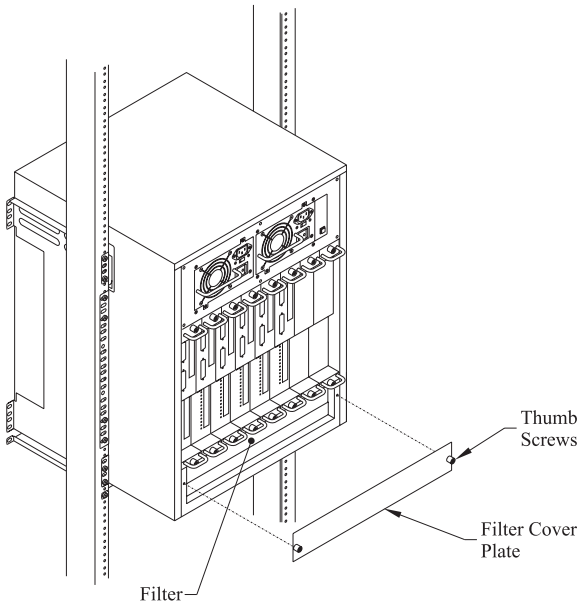

Figure 13. Removing the Filter Cover Plate

1. Remove the filter cover plate by loosening the two captive thumb screws.
2. Remove the filter from its slot.
3. Put the supplied replacement filter in the slot. The used filter may be washed in warm, soapy water and used again once it is completely dry.
4. Replace the filter cover plate and securely tighten the captive thumb screws.

❖ **Note:** *If either of the supplied filters is worn out or cannot be thoroughly cleaned, you may order a replacement filter from Compatible Systems Corporation at the number in the front of this manual.*

Appendix E - Terms and Conditions

Compatible Systems Corporation (Compatible Systems) offers to sell only on the condition that Customer's acceptance is expressly limited to Compatible Systems' terms and conditions of sale. Compatible Systems' acceptance of any order from Customer is expressly made conditional on assent to these terms and conditions of sale unless otherwise specifically agreed to in writing by Compatible Systems. In the absence of such an agreement, commencement of performance or delivery shall be for Customer's convenience only and shall not be construed as an acceptance of Compatible Systems' terms and conditions. If a contract is not earlier formed by mutual agreement in writing, Customer's acceptance of any goods or services shall be deemed acceptance of the terms and conditions stated herein.

1. Warranty. Compatible Systems warrants to the Customer and to all persons who purchase Products from the Customer during the Warranty terms ("subsequent purchasers"), that, for an unlimited period from the date (the "shipping date") on which Compatible Systems ships the Products to the Customer: (a) the Product meets, in all material respects, all specifications published by Compatible Systems for such Products as of the shipping date; (b) the Products are free from all material defects in materials and workmanship under normal use and service; and (c) that as a result of the purchase of the Products from Compatible Systems, the Customer will have good title to the Products, free and clear of all liens and encumbrances.

Compatible Systems' obligations pursuant to this Warranty, and the sole remedies of the Customer and of any subsequent purchaser, shall be limited to the repair or replacement, in Compatible Systems' sole discretion, of any of the Products that do not conform to this Warranty.

This Warranty shall be invalidated if the Products (a) have not been installed, handled, or used in accordance with Compatible Systems' recommended procedures; (b) have been damaged through the negligence or abuse of the Customer or of any subsequent purchasers; (c) are damaged by causes external to the Products, including (without limitation) shipping damage, power or air conditioning failure, or accident or catastrophe of any nature; and (d) have been subjected to repairs or attempted repairs by any person other than Compatible Systems (or an authorized Compatible Systems service technician).

To obtain service under this Warranty, the Customer (or subsequent purchaser, if applicable) must follow the procedures outlined below, under "Product Return Policy."

THE WARRANTIES SET FORTH IN THESE TERMS AND CONDITIONS ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED. WITHOUT LIMITATION ON THE GENERALITY OF THE FOREGOING SENTENCE, COMPATIBLE SYSTEMS EXPRESSLY DISCLAIMS AND EXCLUDES ALL IMPLIED WARRANTIES OF MERCHANTIBILITY AND OF FITNESS (GENERALLY OR FOR A PARTICULAR PURPOSE).

2. Shipments. All delivery indications are estimated and are dependent in part upon prompt receipt of all necessary information to service an order. Compatible Systems shall not be liable for any premium transportation or other costs or losses incurred by Customer as a result of Compatible Systems' inability to deliver Product in accordance with Customer's requested delivery dates. All shipments by Compatible Systems are made F.O.B. factory (Boulder, Colorado); risk of loss shall pass to Customer at point of shipment. Unless specified by the Customer, Compatible Systems will select the mode of transportation for each order. Compatible Systems reserves the right to make deliveries in installments. Partial shipments are subject to the terms of payment noted below. Compatible Systems reserves the right to allocate inventory and production if such allocation becomes necessary.

3. Payment Terms. Payment shall be made prior to shipment or upon delivery, unless otherwise agreed to in writing. Payment shall not constitute acceptance of the goods.

4. Force Majeure. All orders accepted by Compatible Systems are subject to postponement or cancellation for any cause beyond the reasonable control of Compatible Systems, including without limitation: inability to obtain necessary materials and components; strikes, labor disturbances, and other unavailability of workers; fire, flood, and other acts of God; war, riot, civil insurrection, and other disturbances; production or engineering difficulties; and governmental regulations, orders, directives, and restrictions.

5. Product Return Policy. Prior to shipping any Product to Compatible Systems, the Customer must contact Compatible Systems Technical Support (by letter or telephone) with the following information: (a) reason for return; (b) quantity, description, and model number, and (if applicable) serial number of each item being returned; (c) original Compatible Systems Sales Agreement number; and (d) any special instructions. Upon receipt of this information, Compatible Systems will issue an RMA ("Return Material Authorization") number and any required U.S. Customs identification to assure correct identification of the Customer and to insure prompt and accurate processing.

6. Limitation of Remedies. Compatible Systems' liability for all claims brought pursuant to or in connection with this agreement, including the purported breach hereof, shall be limited: (a) in the case of claims for breach of warranty, to compliance with the repair or replacement provisions of the warranty, and (b) in all other cases (including any claim that the warranty failed of its essential purpose), to actual damages of the Customer (or, if appropriate, of the subsequent purchaser). IN NO EVENT SHALL COMPATIBLE SYSTEMS BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE SALE, USE, INSTALLATION OR OPERATION OF THE PRODUCTS, WHETHER A CLAIM IS BASED ON STRICT LIABILITY, BREACH OF WARRANTY, NEGLIGENCE, OR ANY OTHER CAUSE WHATSOEVER, WHETHER OR NOT SIMILAR. This limitation on remedies shall apply even if Compatible Systems is advised of the possibility and nature of any special, consequential, or incidental damages.

7. Governing Law; Merger. This agreement and all Terms and Conditions hereof shall be governed by, and construed in accordance with the internal laws of the State of Colorado. Except as superseded by a separate written contract signed by both Compatible Systems and the Customer, superseding all prior negotiations or offers, written or oral, this agreement may be amended only in writing, signed by an authorized officer of Compatible Systems.