Private Internet Exchange

Network Translation, Inc.

Network Translation, Inc.

1901 Embarcadero Road
Palo Alto, California 94303
Telephone 415 494-6387
Fax 415 424-9110
Email info@translation.com

Table of Contents

Overview of the Private Internet Exchange

DESCRIPTION

The Private Internet Exchange (PIX) from Network Translation, Inc. allows the creation of a private secure network for your organization. This is done with a process known as Network Address Translation. The dynamic translation algorithm in the PIX assigns addresses from a global pool to the hosts in your private network as needed. The Adaptive Security algorithm in the PIX provides the bulletproof security needed in today's public Internet environment.

PACKING LIST

The PIX shipping carton should contain:

- The black rack-mountable PIX unit
- Keys for the front panel lock
- Power cord
- DB-9 to DB-25 serial cable (null modem)
- DB25 gender adapter
- PIX system diskette
- This manual
- Software support information sheet
- Release Notes with bug fixes and known bugs

In order to set up and configure the unit, you will also need an ASCII terminal or PC/workstation with serial communication software installed and running.

SETUP PROCEDURE

1. Unpack the PIX and place it in a convenient location.
2. Connect the power cable to the unit and plug it in.
3. Use the provided null modem serial cable to connect the PIX DB-9 console port to a terminal or the RS-232 of a PC/workstation running serial communication software. Make sure the communications settings on the console device are: 9600 8-N-1.
4. Turn on the power switch. Since your PIX was shipped with the system already installed on the flash RAM, it is **not** necessary to boot from the floppy diskette. As the system boots, you should see the messages shown below on your terminal screen.

   NOTE: The actual Ethernet addresses displayed will be different for each PIX unit.

```
PIX Bios V2.7

Booting Floppy

Loading from Flash
unit outside enet is 00:20:af:ed:f9:08
unit inside enet is 00:20:af:ed:f9:3d

              N e t w o r k     T r a n s l a t i o n     I n c.
  -----------------------------------------------------------------------
                      ppppppp     iiiii  xxx    xxx
                      p      p      i     x      x
                      p       p     i      x    x
                      p       p     i       x  x
                      p       p     i        xx
                      p      p      i        xx
                      ppppppp       i       x  x
                      p             i      x    x
                      p             i     x      x
                      p           iiiii  xxx     xxx
  -----------------------------------------------------------------------
                        Private Internet Exchange
Version 2.6.2
Hit return to login
```

5. Now you are ready to begin configuring your PIX. Here's a typical set of configuration commands (see figure 1):

```
$
$ ifconfig outside 207.39.25.1 netmask 255.255.255.0 link bnc up
$ route outside 207.39.25.2
$ ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
$ route inside 192.168.1.2
$ global -a 207.39.26.0
$
```

NOTE: If you will be using the syslog feature (which is enabled by the **loghost** command, please read *Appendix A: Syslog Configuration* for more information. If your inside hosts and routers are running RIP, you may wish to enable certain RIP functions of the PIX. See the **rip** manual page for more information.

6. Save the configuration to the flash RAM, then display it to the console to make sure you have entered all the information correctly.

```
$ save
$ save -s
: Saved Config
ifconfig outside 207.39.25.1 netmask 255.255.255.0 link bnc up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
global -a 207.39.26.1-207.39.26.254
route outside 207.39.25.2
route inside 192.168.1.2
timeout xlate 24:00:00 conn 12:00:00
rip inside nodefault nopassive
rip outside nopassive
loghost 0.0.0.0
arp -t 600
: version 2.6.2
$
```

7. Connect the inside and outside networks to the PIX Ethernet interfaces.
8. Perform tests (ping, etc.) to make sure the PIX is correctly configured to perform the translation you desire.
9. Set the password and resave the config using the **save** command.
10. **IMPORTANT NOTE:** Once the PIX is configured and running, remove the diskette from the floppy drive and put it in a safe place.

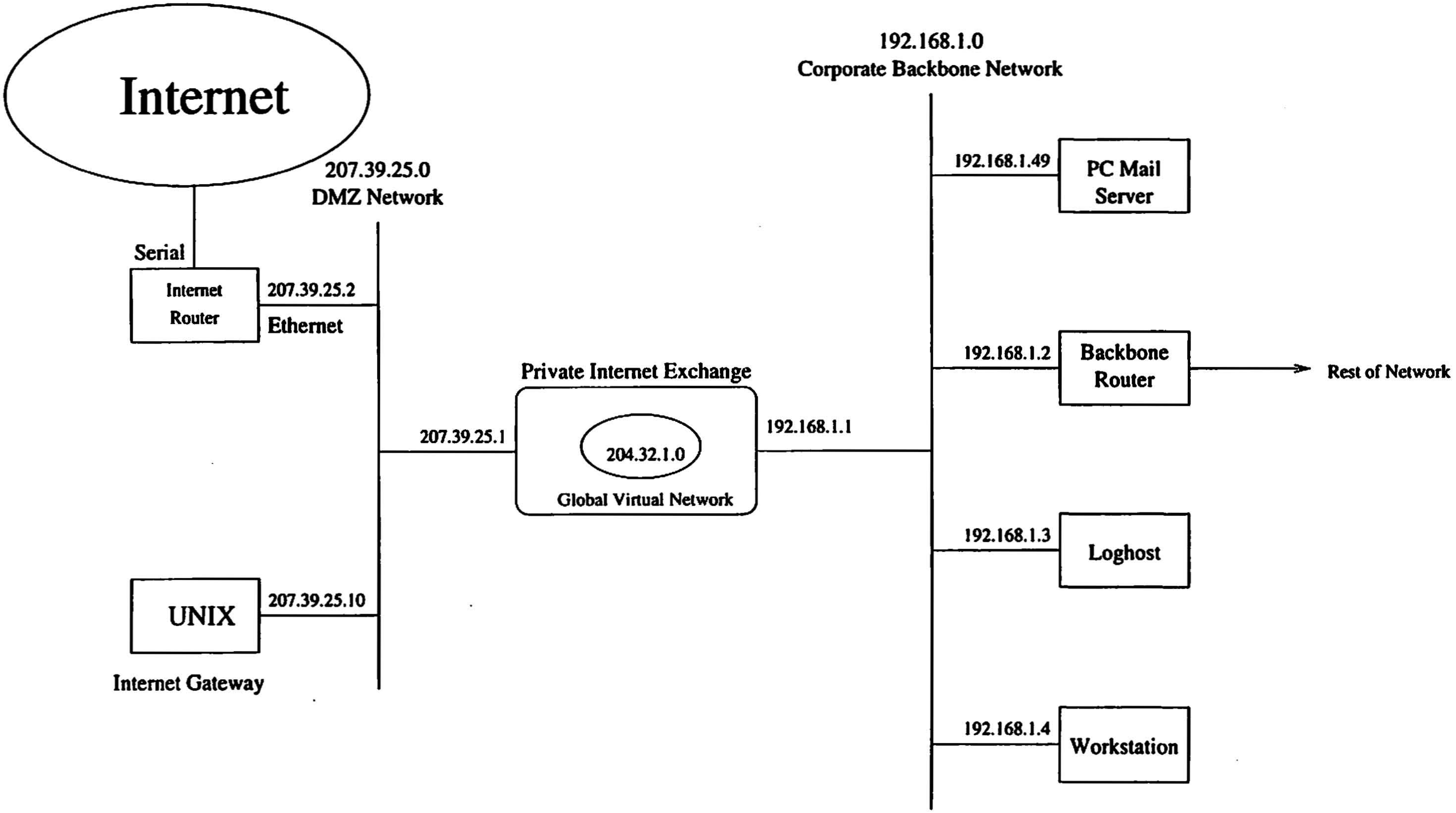

Internet
207.39.25.0
DMZ Network
Serial
Internet
Router
207.39.25.2
Ethernet
207.39.25.1
UNIX
207.39.25.10
Internet Gateway
Private Internet Exchange
204.32.1.0
Global Virtual Network
192.168.1.1
192.168.1.0
Corporate Backbone Network
192.168.1.49
PC Mail
Server
192.168.1.2
Backbone
Router
Rest of Network
192.168.1.3
Loghost
192.168.1.4
Workstation

Figure 1

NAME

: – insert comment; null operation

SYNOPSIS

: [*comment_line*]

DESCRIPTION

Use the : command to add remarks to the system configuration when storing it in a file on a remote system. Comment lines are ignored by the PIX. *comment_line* may be any text string, terminated by a carriage return.

EXAMPLES

For a configuration file containing the following lines:

```
: My Simple Configuration
: Here's the outside network
ifconfig outside 207.39.25.1 netmask 255.255.255.0 link bnc up
route outside 207.39.25.2
: Here's the inside network
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link aui up
route inside 192.168.1.2
: And here's the virtual network
global -a 207.39.26.0
: Save this config
save
: End of My Simple Configuration
```

Pasting the contents of this file into the PIX console results in the configuration shown below:

```
$ save -s
: Saved Config
ifconfig outside 207.39.25.1 netmask 255.255.255.0 link bnc up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
global -a 207.39.26.1-207.39.26.254
route outside 207.39.25.2
route inside 192.168.1.2
timeout xlate 24:00:00 conn 12:00:00
rip inside default passive
rip outside nopassive
loghost 192.168.1.3
telnet 192.168.1.3
arp -t 600
: version 2.6
$

$
```

NAME

arp – display and adjust ARP cache parameters

SYNOPSIS

arp ?
arp [-tl] [*num*]

DESCRIPTION

The **arp** command displays PIX ARP cache entries for each interface and allows the administrator to adjust and display ARP cache timeouts.

? Displays the usage statement.

-t Change the ARP cache persistence timer. The entries in the ARP cache will remain in the PIX for the number of seconds specified by the [*num*] parameter.

-l Display the ARP cache persistence timer value.

num Value in seconds of the ARP cache persistence timer. This parameter accompanies the [-t] parameter. The minimum timer value is 30, the maximum is 4000000.

EXAMPLES

```
$ arp
Inside:
192.168.1.2 at 08:00:20:0b:3a:32
192.168.1.3 at 08:00:20:1d:5b:43
Outside:
207.39.25.2 at 08:00:20:09:6f:71
207.39.25.3 at 08:00:20:0a:5e:64
207.39.25.4 at 08:00:20:0b:3c:71
$

$ arp -l
arp -t 600
$

$ arp -t 60
$ arp -l
arp -t 60
```

NAME

clear_config – erase current flash configuration

SYNOPSIS

clear_config

DESCRIPTION

The **clear_config** command erases the configuration information stored in the flash RAM.

EXAMPLES

```
$ clear_config
Cleared saved config;  interfaces down
You must now reboot to clear ram config
$
```

SEE ALSO

restore

save

NAME

conduit – add and remove conduits to static translations

SYNOPSIS

conduit ?

[*no*] **conduit** *global_ip protocol:ip-addr/bits-port*

DESCRIPTION

The **conduit** command creates a path through a **secure** static translation slot. This allows the administrator to permit connections from outside the PIX to hosts on the inside network.

? Displays the usage statement.

global_ip The IP address from the global pool to associate this conduit with.

protocol:ip-addr/bits-port

On secure static translations, permit incoming connections as follows:

protocol **tcp** or **udp**

ip-addr IP address (host or network) from which to permit incoming connections (0.0.0.0 is any host)

bits Number of bits to apply as netmask for address comparisons (24 for a Class C network, 32 for a single host, 0 for no comparison, etc.)

port Destination port number into which connections are permitted on the inside machine (if using tcp, 25 for smtp, 80 for http, etc.)

The conduit command has the effect of creating an exception to the PIX Adaptive Security mechanism. The conduits exist on the static translation slots and can be added with the conduit command or through the last parameter of the static command. The conduit command is the recommended method. The **no** prefix to the conduit command has the effect of removing the specified conduit.

EXAMPLES

The following pair of commands will enable only SMTP communication between the UNIX gateway host (207.39.25.10) and an SMTP server on the inside network (192.168.1.49):

```
$ static -a 207.39.26.147 192.168.1.49 secure
$ conduit 207.39.26.147 tcp:207.39.25.10/32-25
```

To remove the conduit above, just issue the following command:

```
$ no conduit 207.39.26.147 tcp:207.39.25.10/32-25
```

SEE ALSO

static

NAME

exit – logout of PIX system

SYNOPSIS

exit

DESCRIPTION

The **exit** command is used to close a PIX session. After issuing the **exit** command on the serial console, a `password:` prompt will appear. No further PIX commands will be accepted until the system password is correctly entered. If the **exit** command is used on a telnet session to the PIX, the telnet session is closed.

EXAMPLES

```
$ exit
password:
```

SEE ALSO

passwd

NAME

global – enter global network addresses

SYNOPSIS

global ?
global [**-ar**] *ip*[-*ip*]

DESCRIPTION

The **global** command is a mandatory configuration command for the PIX. It sets up the global pool of registered IP addresses to which private network addresses are mapped. If the PIX will be connecting a private network to the Internet, each IP network added to the global address space must be a registered network obtained from an Internet service provider or directly from the NIC. The phrases *global network* and *virtual network* are synonymous in this manual.

The following options are available for the **global** command:

? Displays the usage statement.

-a Add IP addresses to the PIX virtual network.

-r Remove IP addresses from the PIX virtual network.

ip[-*ip*] Virtual network IP address(es) to add or remove. Ranges of IP addresses are also supported and are expressed by indicating the upper and lower bounds of the address range, separated by a hyphen. Note that *207.39.26.0* is exactly equivalent to *207.39.26.1-207.39.26.254* in this context and will show up in the **save -s** output with the range form. Note that the minimum number of IP addresses to add to the global pool is 2 *(i.e. 207.39.26.10-207.39.26.11)*. The maximum is 1 class B network worth of IP addresses. It is not valid to add 1 address *(i.e. global -a 207.39.26.20)*.

If you are using 1 class C network and sharing it between the outside network and the PIX virtual network, the PIX will proxy-arp for the global pool on the outside network. If you are using global networks that are disjoint from the outside network address, be certain that the networking equipment and computers have a routing table entry for the global network with a next hop of the outside interface of the PIX.

EXAMPLES

```
$ global -a 207.39.26.0
$

$ global -a 207.39.26.5-207.39.26.254
$
```

SEE ALSO

static

NAME

help – list available commands

SYNOPSIS

help

DESCRIPTION

help displays a brief description of each user command.

EXAMPLES

```
$ help
arp           - show arp tables         clear_config  - erase flash config
conduit       - modify static conduits  exit          - logout
global        - enter global addresses  help          - this listing
ifconfig      - configure interface     ifstat        - show interface status
kill          - terminate login session link          - establish private link
link_stat     - show link status        list_rip      - show PIX RIP table
loghost       - enter addr for loghost  mem           - PIX memory information
passwd        - assign password         reboot        - reboot PIX
restore       - reload configuration    rip           - adjust RIP behavior
route         - enter default routes    save          - save configuration
static        - make static translation tcpstat       - show tcp connections
telnet        - assign telnet host      timeout       - adjust resource timeout
trace         - icmp packet trace       version       - show software version
who           - show PIX users          xlate         - show xlate/conn tables
$
```

NAME

ifconfig – configure interface

SYNOPSIS

ifconfig
ifconfig[*interface*] [*ip_address*] [**netmask** *mask*] [**link** *type*] [**up**|**down**]

DESCRIPTION

ifconfig with no arguments displays the current configuration of both network interfaces.

interface Indicates which network interface is being configured. Must be either **inside** or **outside** depending on which interface is being configured.

ip_address Initializes the interface's IP address.

netmask *mask* Sets the netmask for the interface being configured.

link *type* Specifies the *type* of network cabling for the interface. Must be one of the following: **bnc** (Thin Ethernet), **rj** (10BASE-T), or **aui** (Thick Ethernet or transceiver).

up Marks the interface as up, enabling it for use.

down Marks the interface as down, disabling it.

IP addresses and netmasks must be specified in dotted decimal notation.

EXAMPLES

```
$ ifconfig inside 192.168.1.1 netmask 255.255.255.0 link aui up
$ ifconfig outside 207.39.1.1 netmask 255.255.255.0 link bnc up
$ ifconfig
ifconfig outside 207.39.1.1 netmask 255.255.255.0 link aui up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link bnc up
$

$ ifconfig outside down
$ ifconfig
ifconfig outside 207.39.1.1 netmask 255.255.255.0 link aui down
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link bnc up
$
```

NAME

ifstat – display interface statistics

SYNOPSIS

ifstat

DESCRIPTION

The **ifstat** command displays cumulative statistics for the inside and outside Ethernet interfaces of the PIX.

dropped	Packets discarded because of a lack of resources
incomplete	Sender of the packet never completed the transmission
crc	Bad CRC on the end of the Ethernet frame
overrun	Packet discarded because of a lack of Ethernet interface resources
oversized	Packet larger than the legal Ethernet limit
runt	Packet was legal, but less than the Ethernet minimum packet size
framing	Problems with the Ethernet header or trailer of the packet

EXAMPLES

```
$ ifstat

unit      dropped  incomplete  crc  overrun  oversized  runt  framing
outside:  0        0           0    0        0          0     0
inside:   0        0           0    0        0          0     0

$
```

NAME

kill – terminate login sessions to the PIX

SYNOPSIS

kill ?
kill *tty_id*

DESCRIPTION

kill terminates PIX administration sessions that are established via the console and through telnet.

? Displays the usage statement.

tty_id The tty_id is the session number shown in the output of the **who** command.

EXAMPLES

```
$ who
1: From 192.168.1.3
0: On console
$ kill 1
$ who
0: On console
$
```

SEE ALSO

who
telnet

NAME

link – establish an encrypted PIX Private Link

SYNOPSIS

```
link ?
[no] link local_global remote_global key
```

DESCRIPTION

The **link** command creates an encrypted path between Private Link equipped PIX units.

? Displays the usage statement.

no Removes the specified link entry from the local PIX.

local_global The IP address from the global pool that is associated with the link command. The encrypted packet will be encapsulated in a UDP frame with a source IP of *local_global*.

remote_global This is the IP address associated with the far end PIX and is the global address on that PIX to send UDP frames to. The encrypted packet will be encapsulated in a UDP frame with a destination IP address of *remote_global*.

key This is the key to seed the encryption chip. This key must be the same at each end of an encrypted **link**.

The PIX Private Link is a hardware encryption mechanism for creating private channels across a public network. The encryption hardware is an option on the PIX and is not shipped unless explicitly ordered.

The Private Link feature allows up to 64 PIX units to communicate in a secure fashion across a public network (usually the Internet). At least 2 PIX units are required along with the hardware/software option to use this feature. Packets that arrive at the PIX inside interface will have their destination address examined. If a **route link** exists that matches the destination network address, the packet is encrypted and encapsulated in a UDP frame. The UDP frame will have a destination address of *remote_global* and a source address of *local_global* and will have a destination port of 1123. When the packet arrives at the remote PIX unit, the data in the packet is decrypted and then sent through the inside interface to the original IP address specified. No translation takes place on packets that traverse the PIX Private Link. The addressing and data remains completely unchanged.

EXAMPLES

Please see *Appendix C: Private Link Configuration Examples* for further information.

SEE ALSO

route
link_stat

NAME

link_stat – show status of PIX Private Links

SYNOPSIS

link_stat

DESCRIPTION

link_stat shows the number of frames passed through a PIX Private Link since the boot time.

EXAMPLES

```
$ link_stat
147.3.0.1->147.4.0.1 15043904 out, 7948217 in
```

SEE ALSO

link
route

NAME

list_rip – display the current RIP table

SYNOPSIS

list_rip

DESCRIPTION

The RIP table is displayed in the following format:

destination gateway hop_count seconds

The rightmost field in each line of the display indicates the number of seconds until expiration of the routing information in that RIP table entry.

EXAMPLES

```
$ list_rip
192.168.2.0 192.168.1.2 1 249
$
```

SEE ALSO

rip

NAME

loghost – set the IP address of the logging system

SYNOPSIS

loghost ?
loghost [*ip_address*]

DESCRIPTION

loghost with no arguments displays the current loghost IP address.

? Displays the usage statement.

ip_address The IP address of the logging host machine.

PIX generates syslog messages for a number of reasons, including security alerts and resource depletion. These syslog messages may be used to generate email alerts, create log files, or get redirected to the console of a designated host using UNIX syslog conventions. The loghost machine must be on the internal network.

Please see *Appendix A: Syslog Configuration* for further details of the logging features of the PIX.

EXAMPLES

```
$ loghost 192.168.1.3
$ loghost
loghost 192.168.1.3
$
```

NAME

mem – display the current PIX system memory usage

SYNOPSIS

mem

DESCRIPTION

The **mem** command displays the current PIX system memory usage, showing the current resources in use, remaining, and mose used since reboot. The following information is displayed:

Memory	RAM utilization of PIX system
Xlate	translation slots utilization - addresses from **global** pool
Conn	connection slots utilization - a count of TCP connections through PIX
Block	system memory blocks utilization
Conduit	conduit resource utilization
Link	PIX Private Link utilization
Path	count of *route link* commands in the system
Uptime	Hours:Minutes:Seconds of time since PIX has booted

EXAMPLES

```
$ mem
           in use       remain        most used
Memory  :   3830K        3338K         3830K
Xlate   :      1          253             1
Conn    :   5244         4996          6322
Block   :      5          324            18
Conduit :      8         4088             8
Link    :      1           63             1
Path    :      1          255             1
Uptime  :  432:29:05
$
```

NAME

passwd – assign a password to the PIX system

SYNOPSIS

passwd ?
passwd [*password*] [-]

DESCRIPTION

passwd is used to assign or change the password for future PIX logins. The *password* can be no longer than 14 printable characters. **passwd** with no arguments will display the current system password on the console.

?	Displays the usage statement.
password	Assigns *password* for all future logins to PIX.
-	Removes *password*. The PIX now requires no password for login.

EXAMPLES

```
$ passwd xyzzy
$ passwd
passwd xyzzy
$ passwd -
$ passwd
$
```

SEE ALSO

exit

NAME

reboot – reboot system

SYNOPSIS

reboot

DESCRIPTION

The **reboot** command shuts down the PIX system and restarts it. If there is a PIX system disk in the floppy drive, the system will reboot from the disk. If there is no disk in the floppy drive, the system will boot from the flash RAM. The PIX will ask if you want to load from floppy to flash after loading the floppy image. If you want to upgrade the system software, press *y* within 15 seconds. The PIX will then automatically upgrade the system software. If you type nothing, the PIX will boot from flash and operate normally.

EXAMPLES

```
$ reboot
Rebooting....

PIX Bios V2.6

Booting Floppy

..................................
```

NAME

restore – restore system configuration from flash card or floppy disk

SYNOPSIS

restore ?
restore [**-fs**]

DESCRIPTION

restore without any arguments restores the system configuration from the flash card.

? Displays the usage statement.

-f Restores the system configuration from the floppy disk.

-s Displays the system configuration currently stored in the flash RAM.

EXAMPLES

```
$ restore -s
: Saved Config
ifconfig outside 207.39.25.1 netmask 255.255.255.0 link bnc up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
route outside 207.39.25.2
route inside 192.168.1.2
timeout xlate 24:00:00 conn 12:00:00
rip inside default passive
rip outside nopassive
loghost 192.168.1.3
telnet 192.168.1.3
arp -t 600
: version 2.6
$
```

SEE ALSO

save
clear_config

NAME

rip – change or display RIP settings

SYNOPSIS

rip ?

rip [**inside**|**outside**] [**nodefault**|**default**] [**passive**|**nopassive**]

DESCRIPTION

rip with no arguments displays the current RIP settings.

? Displays the usage statement.

inside The following arguments modify RIP behavior on the inside interface.

outside The following arguments modify RIP behavior on the outside interface.

nodefault Disables the default route broadcast on the inside interface.

default Causes the PIX to broadcast a default route to the inside network.

passive (enable) Enables passive RIP on either the inside or outside interface. The PIX will listen for RIP routing broadcasts and use that information to populate its routing tables.

nopassive (disable) Disables passive RIP on either the inside or outside interface.

RIP default broadcast is only possible on the inside interface.

EXAMPLES

```
$ rip
rip inside nodefault passive
rip outside nopassive
$ rip inside default
$ rip
rip inside default passive
rip outside nopassive
$
```

SEE ALSO

list_rip

NAME

route – set the network default router and paths for Private Links

SYNOPSIS

```
route ?
[no] route interface ip_address
[no] route link dest_net net_mask remote_global
```

DESCRIPTION

route with no arguments displays the IP addresses of the default routers for both inside and outside networks and any paths for link commands.

? Displays the usage statement.

no Removes the specified route entry.

interface Either **inside** or **outside**

ip_address IP address of the default router for the network attached to that interface.

link This keyword means the following arguments affect packets destined for a PIX Private Link.

dest_net The destination network on the inside interface of the remote PIX of a Private Link.

net_mask Specifies a subnet mask to apply to the *dest_net* documented above.

remote_global IP address in the global pool of the remote PIX in a Private Link environment.

Please see *Appendix C: Private Link Configuration Examples* for further information.

EXAMPLES

```
$ route outside 204.39.25.2
$ route inside 192.168.1.2
$ route link 192.168.100.0 255.255.255.0 207.39.27.1

$ route
route outside 204.39.25.2
route inside 192.168.1.2
route link 192.168.100.0 255.255.255.0 207.39.27.1
$

$ no route link 192.168.100.0 255.255.255.0 207.39.27.1
$ route
route outside 204.39.25.2
route inside 192.168.1.2
```

Only get one route when
using statics! unless
your using Private Link

SEE ALSO

link
link_stat

NAME

save – save or display current configuration

SYNOPSIS

```
save ?
save [-sf]
```

DESCRIPTION

save with no arguments saves the configuration data to the flash RAM.

?	Displays the usage statement.
-f	Saves the current configuration to the floppy disk.
-s	Displays the current configuration to the console screen.

EXAMPLES

```
$ save -s
: Saved Config
ifconfig outside 207.39.25.1 netmask 255.255.255.0 link bnc up
ifconfig inside 192.168.1.1 netmask 255.255.255.0 link rj up
global -a 207.39.26.1-207.39.26.254
route outside 207.39.25.2
route inside 192.168.1.2
timeout xlate 24:00:00 conn 12:00:00
rip inside default passive
rip outside nopassive
telnet 192.168.33.4
loghost 192.168.1.3
arp -t 600
: version 2.6.2
$
```

SEE ALSO

restore
clear_config

NAME

static – reserve a local to global address translation table entry

SYNOPSIS

```
static ?
static [-ar] global_ip local_ip [secure][protocol:ip-addr/bits-port]
```

DESCRIPTION

The **static** command creates a permanent mapping (static translation slot) between a local IP address and a global IP address in the virtual pool.

? Displays the usage statement.

-a Add a static IP address to the system configuration.

-r Remove a static address from the system configuration.

global_ip The registered IP address to be used from the global pool.

local_ip The local IP address from the inside network.

secure Enable Adaptive Security (AS) for this translation entry.

protocol:ip-addr/bits-port

On secure static translations, you may permit incoming connections by creating a conduit as follows:

protocol **tcp** or **udp**

ip-addr IP address (host or network) from which to permit incoming connections (0.0.0.0 is any host)

bits Number of bits to apply as netmask for address comparisons (24 for a Class C network, 32 for a single host, 0 for no comparison, etc.)

port Destination port number into which connections are permitted on the inside machine (if using tcp, 25 for smtp, 80 for http, etc.)

A static address is a permanent mapping from one of the global, registered IP addresses to a local IP address inside the private network. Static addresses are recommended for internal network service hosts, such as an SMTP server. Note that Adaptive Security is not enabled unless the **secure** flag is explicitly specified. Although it is possible to add conduits to the static translation on the **static** command line, it is recommended to add and remove conduits using the **conduit** command.

EXAMPLES

The following pair of commands will enable TCP SMTP communication between the UNIX gateway host (207.39.25.10) on the outside network and an SMTP gateway on the inside network (192.168.1.49):

```
$ static -a 207.39.26.147 192.168.1.49 secure
$ conduit 207.39.26.147 tcp:207.39.25.10/32-25
```

For backward compatibility only, the following static command will also work:

```
$ static -a 207.39.26.147 192.168.1.49 secure tcp:207.39.25.10/32-25
```

To remove the above static:

```
$ static -r 207.39.26.147 192.168.1.49 secure tcp:207.39.25.10/32-25
```

SEE ALSO

conduit
global

NAME

tcpstat – display TCP statistics for telnet sessions

SYNOPSIS

tcpstat

DESCRIPTION

The **tcpstat** command displays the PIX unit's notion of TCP state for all telnet sessions.

EXAMPLES

```
$ tcpstat
0:192.168.1.1:23 -> 0.0.0.0:0 listen
        snd(0, 0, 0), rcv(0, 1000),
        Flags:
        rto 6000, rt_timer 0, tw_timer 0, cl_timer 0, per_timer 0
        |in| 0, |out| 0
        cwnd 1024
$
```

SEE ALSO

telnet

NAME

telnet – add authorized IP addresses for telnet access to PIX

SYNOPSIS

telnet ?

[*no*] **telnet** [*ip_address*]

DESCRIPTION

telnet with no arguments displays the current list of IP addresses that are authorized to access the PIX via the *inside* network. Up to 16 hosts are allowed access to the PIX, 4 simultaneously.

?	Displays the usage statement.
no	Removes the specified host from the list of those allowed.
ip_address	The IP address of a host that is authorized to access the PIX telnet management interface.

The PIX allows telnet access to configure the PIX from the *inside* network only. Having no telnet hosts set implies that no hosts on the inside network can telnet to the PIX.

EXAMPLES

```
$ telnet 192.168.1.3
$ telnet 192.168.1.4
$ telnet
telnet 192.168.1.3
telnet 192.168.1.4
$ no telnet 192.168.1.3
$ telnet
telnet 192.168.1.4
```

SEE ALSO

kill
tcpstat
passwd

NAME

timeout – set the maximum idle time for translation and connection slots

SYNOPSIS

timeout ?

timeout [**xlate** *hh:mm:ss*] [**conn** *hh:mm:ss*]

DESCRIPTION

timeout with no arguments displays the current timeout settings.

?	Display the usage statement.
xlate *hh:mm:ss*	Idle time until a translation slot is cleared (default value is 24 hours).
conn *hh:mm:ss*	Idle time until a connection slot is cleared (default value is 12 hours).

TCP connection slots are freed within 30 seconds after a normal connection close sequence. The timeout value sets an idle time for connection and translation slots. If the connection or translation slot has not been used for the idle time specified, the resource is put back in the free pool. The minimum idle times for both xlate and conns is 5 minutes.

EXAMPLES

```
$ timeout
timeout xlate 24:00:00 conn 12:00:00
$ timeout xlate 5:0:0
$ timeout conn 2:0:0
$ timeout
timeout xlate 5:00:00 conn 2:00:00
$ timeout xlate 0:10:0 conn 0:5:0
$ timeout
timeout xlate 0:10:00 conn 0:05:00
$
```

NAME

trace – trace ICMP packets traversing the PIX

SYNOPSIS

trace ?
trace [**on**|**off**]

DESCRIPTION

The **trace** command by itself shows the status of tracing on the PIX (either on or off).

? Displays the usage statement.

on Enables tracing of ICMP packets on the PIX.

off Disables tracing of ICMP packets on the PIX.

When **trace** is on ICMP packets that traverse the PIX are displayed on the terminal in real-time. The first IP address shown in each line of the display is that of the outside world host being communicated with, followed by an arrow indicating the direction of packet flow, then the registered IP address which has been dynamically assigned to the private network host by the PIX. The final address in parenthesis is the IP address on the private network. Be sure to turn the trace option off during normal operation because it will impair performance if left on.

EXAMPLES

```
$ trace on
$
16.1.0.2 <- 207.39.26.5 (192.168.1.49)
16.1.0.2 -> 207.39.26.5 (192.168.1.49)
192.48.96.9 -> 207.39.26.251 (192.168.1.2)
192.48.96.9 <- 207.39.26.251 (192.168.1.2)
trace off
$
```

NAME

version – display PIX system software version

SYNOPSIS

version

DESCRIPTION

The **version** command displays the current version of PIX software.

EXAMPLES

```
$ version
: version 2.6.2
$
```

NAME

who – show active administration sessions on PIX

SYNOPSIS

who

DESCRIPTION

The **who** command shows the active users on the PIX and from where they have logged in. The number before the colon indicates the tty_id on the PIX. The IP address is shown for all telnet sessions. Note that telnet sessions can only be initiated from the inside network.

EXAMPLES

```
$ who
2: From 192.168.2.2
1: From 192.168.1.3
0: On console
$
```

SEE ALSO

kill
telnet

NAME

xlate – display current translation and connection slot information

SYNOPSIS

xlate ?
xlate [**-x** | **-1 local_ip** | **-g global_ip**]

DESCRIPTION

xlate displays the current translation and connection slot information.

? Displays the usage statement.

-x Show just the translation slot information.

-1 local_ip Show the translation and connection slot information for a particular [**local_ip**] address.

-g global_ip Show the translation and connection slot information for a particular [**global_ip**] address.

The lines that are flush on the left margin are the translation slots. The translation slot information contains both the Global and Local addresses (Global addresses are from the virtual pool added using the *global* command. The Local address is the address from the inside LAN). The indented lines display information about connection slots that are associated with the above mentioned translation slot. The information includes the outside IP address and port number, the inside IP address and port number, idle time and number of bytes transferred on a per TCP connection basis. The *xlate* command is simply a snapshot of system resources at the time the command is executed.

EXAMPLES

```
$ xlate
$ xlate
Global 207.39.26.3 Local 192.168.1.2
  out 16.1.0.2-23 in 192.168.1.2-3538 idle 0:00:21 Bytes 96
Global 207.39.26.254 Local 192.168.1.4
  out 192.100.81.100-23 in 192.168.1.4-1182 idle 0:00:42 Bytes 1032
$ xlate -x
Global 207.39.26.3 Local 192.168.1.2
Global 207.39.26.254 Local 192.168.1.4
$ xlate -1 192.168.1.4
Global 207.39.26.254 Local 192.168.1.4
  out 192.100.81.100-23 in 192.168.1.4-1182 idle 0:00:44 Bytes 1032
$ xlate -g 207.39.26.3
Global 207.39.26.3 Local 192.168.1.2
  out 16.1.0.2-23 in 192.168.1.2-3538 idle 0:00:24 Bytes 96
```

Appendix A: Syslog Configuration

Introduction

Informative messages from the PIX may be redirected into email, written into log files, or displayed on the console of a designated UNIX host on the inside network by using the built-in Berkeley syslog facility. Logging is enabled by configuring the PIX with the IP address of the loghost, and produces four different categories of messages relating to different aspects of PIX operation. A PC winsock version of syslogd also will work, but it logs everything to one file, not separate files like the UNIX model.

PIX Syslog Message Categories	
Category	*Logged Events*
Security	UDP packets dropped, TCP connections denied
Resource	Notification of 80% and 100% conn/xlate slot depletion
System	Console logins and logouts from console and telnet, PIX reboots
Accounting	Bytes transferred per conn, xlate/conn counts each 10 minutes

Syslog Configuration

In order to take advantage of the logging capabilities of the PIX, you will need to set up a UNIX host on your inside network to accept syslog messages from the PIX and process them appropriately. The following example is for a loghost system running SunOS 4.1.4, but syslog configuration should be nearly identical on any modern UNIX-based operating system.

Step 1. Configure the PIX to send syslog messages to the desired host with the **loghost** command.

Step 2. As **root** on the loghost machine, execute the following sequence of commands:

```
# mkdir /var/log/pix
# touch /var/log/pix/system
# touch /var/log/pix/resource
# touch /var/log/pix/security
# touch /var/log/pix/acct
```

Step 3. Again as **root** on the loghost machine, edit the */etc/syslog.conf* file with your favorite editor, adding the following *selector/action* pairs:

```
# A.S. violations
local4.crit     /var/log/pix/security
# resource depletion
local5.err      /var/log/pix/resource
# boot/login messages
local6.notice   /var/log/pix/system
# accounting information
local7.info     /var/log/pix/acct
```

Please note that entries in the */etc/syslog.conf* file must obey the following rules:

- Comments are only allowed on separate lines, which must begin with the '#' character.
- The *selector/action* pairs must be separated with a tab character. Blanks will not work.
- Make sure there are no trailing blanks after the filenames.

The configuration shown below will direct PIX syslog messages to four separate files, one for each category. If you desire to send these messages to the loghost console or have them emailed to a system administrator, check the syslog.conf(5) manual page on your loghost system for further instructions. The *acct* log file can grow to several megabytes per day on a busy PIX. Logging is disabled by issuing the *loghost 0.0.0.0* command on the PIX.

Once the logging files have been created and the /etc/syslog.conf file has been edited, you must tell syslogd to reread its configuration file by sending it a HUP signal:

```
# cat /etc/syslog.pid
92
# kill -HUP 92
```

Examples of PIX Syslog Messages

```
Jan 15 12:55:03 pix-in  PIX out of connections!

Jan 15 12:54:28 pix-in  conn end faddr 204.31.33.1 fport 4457 gaddr 204.30.204.3 laddr 204.30.204

Jan 15 13:04:02 pix-in  deny tcp out 192.48.96.14 25 in 204.30.204.3 3507  flags SYN ACK

Jan 15 13:37:44 pix-in  conns 10240 conns_used 0 xlate 254 xlate_used 1

Jan 15 13:47:21 pix-in  PIX logged in from 204.30.204.112
```

Appendix B: PIX Operation Summary and Security Policy

Overview

The Private Internet Exchange (PIX) is a Network Address Translation unit that provides the capability of your private (possibly unregistered or RFC-1597) IP network to directly access the Internet. The PIX has inside and outside Ethernet interfaces. The inside Ethernet has the capability of listening to RIP routing updates and broadcasting a RIP default route. When packets arrive at the inside Ethernet, the PIX checks to see if it has ever seen a packet from this inside host. If not, the PIX creates a translation slot which includes in its state table the inside IP address and the new globally unique IP address drawn from the virtual network of up to 64K host addresses. The PIX then changes the IP address in the packet and fixes all the checksums and other aspects of the packet that need changing. The packet is then forwarded to the outside Ethernet interface on its way to the Internet.

When a packet arrives at the outside interface, it must first pass the Adaptive Security criteria described below. If the packet passes the security tests, it has its destination IP address removed, and the internal IP address is inserted in its place. The packet is again fixed and forwarded to the inside interface. This dynamic translation slot notion-is useful for desk top machines that do not need a constant address on the Internet. Unregistered hosts can directly access the Internet with standard TCP/IP software on the desktop. No special client side software is needed, as is required for the use of application-layer gateway schemes.

Another class of address translation on the PIX is the static translation. The static translation effectively moves an internal unregistered host into the virtual network in the PIX. This is useful for internal machines that need to be addressed from the outside Internet gateways (i.e. an SMTP server). Unless Adaptive Security is enabled on a static translation slot, that inside host is effectively part of the outside network.

Adaptive Security

The Adaptive Security (AS) feature applies to the dynamic translation slots and can be applied to static translation slots via the **secure** flag to the **static** command. The Adaptive Security algorithm is a very stateful approach to security. Every inbound packet is checked exhaustively against the Adaptive Security algorithm and against connection state information in memory. This stateful approach to security is regarded in the industry as being far more secure than a stateless packet screening approach. Adaptive Security follows these rules:

- Allow any TCP connections that originate from the inside network.
- Ensure that if an FTP data connection is initiated to a translation slot, there is already an FTP control connection between that translation slot and the remote host. If not, the attempt to initiate an FTP data connection is dropped and logged.
- Prevent the initiation of a TCP connection to a translation slot from the outside. The offending packet is dropped and logged.
- Allow inbound UDP packets only from DNS, and archie. NFS is explicitly denied.
- Drop and log source routed IP packets sent to any translation slot on the PIX.
- Allow ICMP of types 0, 3, 4, 8, 11, 12, 17 and 18. This implies that ICMP redirects (type 5) and others are denied.
- Ping requests to dynamic translation slots are silently dropped.
- Ping requests to static translation slots are answered.

Static translation slots can be secured via AS, and can have exceptions (called conduits) to the AS rules described above. These conduits are in the format **protocol:address/mask-port**. Multiple exceptions may be applied to a single static translation slot (via multiple **conduit** commands). This allows the administrator to permit access from an arbitrary machine, network, or any host on the Internet to the inside host defined by the static translation slot.

Appendix C: Private Link Configuration Examples

Overview

The PIX Private Link option provides the capability of secure links between PIX units across a public network like the Internet. The minimum configuration for using the PIX Private Link is 2 PIX units with the PIX Private Link hardware/software option.

The Private Link hardware uses 56 bit hardware DES encryption. The linking of 2 PIX units is a 2 command process beyond the normal configuration. Examine the *Private Link Configuration Example 1* diagram. Note the private networks are 147.3.0.0 and 147.4.0.0. It is not important that these networks are registered. Configure *PIX A* as you would normally. For example:

```
ifconfig inside 147.3.1.1 netmask 255.255.255.0 link rj up
ifconfig outside 204.31.35.1 netmask 255.255.255.0 link rj up
global -a 204.31.34.0
route outside 204.31.35.2
route inside 147.3.1.2
```

Configure *PIX B* normally as follows:

```
ifconfig inside 147.4.1.1 netmask 255.255.255.0 link rj up
ifconfig outside 204.32.2.1 netmask 255.255.255.0 link rj up
global -a 204.32.1.0
route outside 204.32.2.2
route inside 147.4.1.2
```

You need to select a local global address to use for our encrypted link. The PIX uses the last address entered first for dynamic translation slots. It is a good policy to use the address from the other end of the selection pool. In the examples above, for *PIX A* you should choose *204.31.34.1*. For *PIX B*, choose *204.32.1.1*. Next you need to agree on a key between the 2 PIX units. For the example, *1234567890* will be used. We need to first add a link command to create the encrypted link, then create a *route link* to tell the PIX to send packets for the destination network across the link, rather than translating and forwarding them. On *PIX A*, you would then enter the following 2 commands:

```
link 204.31.34.1 204.32.1.1 1234567890
route link 147.4.0.0 255.255.0.0 204.32.1.1
```

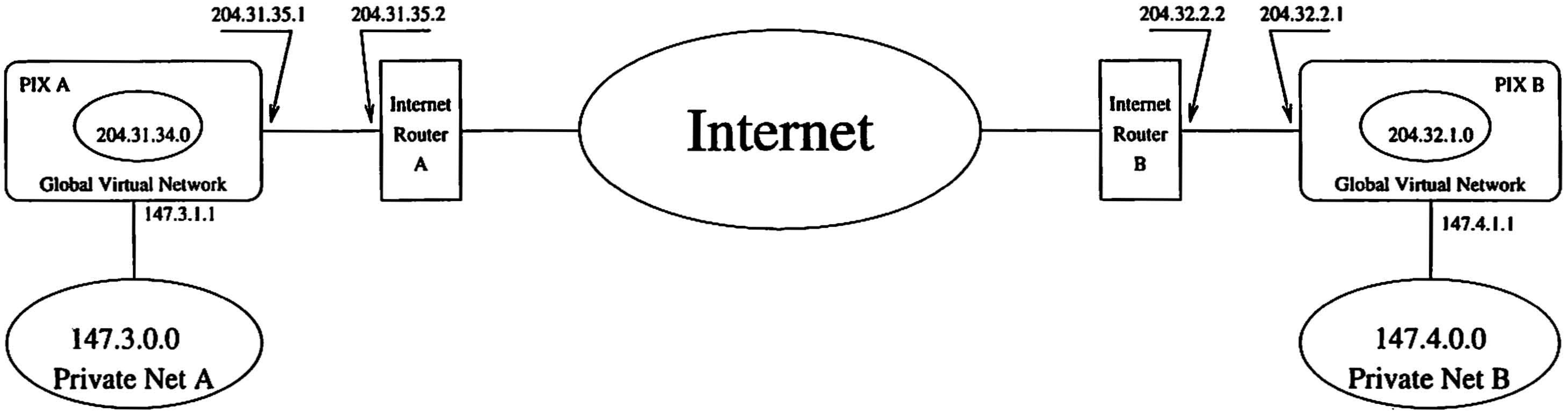
Examine the previous 2 commands. The first argument of the link command tells the PIX to use *204.31.34.1* as the source address for all encrypted packets. The second argument is the destination of this link command. The third argument to the link command is the encryption key which has to be the same on both ends of the private link.

The second command has 4 arguments. The first tells the PIX that this route statement pertains to a Private Link. The second argument is the network address you are trying to reach using the PIX Private Link. The third argument is a netmask. In the example above, the PIX will send all packets for the 147.4.0.0 network through this route. The last argument is a *next host* for these encrypted packets. This maps to the second argument of the link command. Note that if you have more than one IP network on the far end of the Private Link, you will need multiple *route link* commands to ensure that all packets for those networks are encrypted and sent properly.

The 2 commands needed for *PIX B* are:

```
link 204.32.1.1 204.31.34.1 1234567890
route link 147.3.0.0 255.255.0.0 204.31.34.1
```

All packets flowing between PIX units that are linked are UDP and will have a source and destination port of 1123.



PIX Private Link Configuration Example

Appendix D: PIX Specifications

Product Models

PIX-32
PIX-256
PIX-1024
PIX-4096
PIX-10240

Hardware Specifications

19" Rack Mount Enclosure
2 Ethernet interfaces
1 DB-9 RS-232 console interface port
3.5" floppy disk drive
Lockable front panel
250 watt power supply with 29 CFM cooling fan

Network Interfaces

Connector	Cable Type	Standard
DB-15 AUI	RG-11 50Ω coax (Thick Ethernet)	Ethernet 10BASE-5
BNC	RG-58 50Ω coax (Thin Ethernet)	Ethernet 10BASE-2
RJ-45	Unshielded Twisted Pair	Ethernet 10BASE-T

Physical Dimensions

Height:	7"
Width:	19"
Depth:	19"
Weight:	25 lb.

Power Requirements

115 VAC ±10%, 47-63 Hz, 2.5A
230 VAC ±10%, 47-63 Hz, 1.3A