



TCP/IP Reference Information

This appendix includes the following sections:

- [IP Addresses](#)
- [Ports](#)
- [Protocols and Applications](#)
- [Using Subnet Masks](#)

IP Addresses

- IP address classes are defined as follows:
 - Class A—If the first octet is between 1 and 127 (inclusive), the address is a Class A address. In a Class A address, the first octet is the one-byte net address and the last three octets are the host address. The network mask for Class A addresses is 255.0.0.0.
 - Class B—If the first octet is between 128 and 191 (inclusive), the address is a Class B address. In a Class B address, the first two octets are the net address and the last two octets are the host address. The network mask for Class B addresses is 255.255.0.0.
 - Class C—If the first octet is 192 or higher, the address is a Class C address. In a Class C address, the first three octets are the net address and the last octet is the host address. The network mask for Class C addresses is 255.255.255.0.
 - Class D—These addresses are used for multicast transmissions and within the range from 224.0.0.0 to 239.255.255.255. Some of these addresses are assigned to multicasts used by specific TCP/IP protocols. Other Class D addresses are assigned to applications, such as streaming video, that send data to many recipients simultaneously. For information about enabling the PIX Firewall to transmit multicast traffic, refer to “[Enabling Stub Multicast Routing](#)” in *Chapter 2, “Establishing Connectivity.”*
- We recommend that you use RFC 1918 IP addresses for inside and perimeter addresses. These addresses follow:
 - Class A: 10.0.0.0 to 10.255.255.255
 - Class B: 172.16.0.0 to 172.31.255.255
 - Class C: 192.168.0.0 to 192.168.255.255
 - Class D: 224.0.0.0 to 239.255.255.255
- PIX Firewall requires that IP addresses in the **ip address**, **static**, **global**, **failover**, and **virtual** commands be unique. These IP addresses cannot be the same as your router IP addresses.

- In this guide, the use of “address” and “IP address” are synonymous.
- IP addresses are primarily one of these values:
 - *local_ip*—An untranslated IP address on the internal, protected network. In an outbound connection originated from *local_ip*, the *local_ip* is translated to the *global_ip*. On the return path, the *global_ip* is translated to the *local_ip*. The *local_ip* to *global_ip* translation can be disabled with the **nat 0 0 0** command. In syslog messages, this address is referenced as *laddr*.
 - *global_ip*—A translated global IP address in the pool or those addresses declared with the **global** or **static** commands. In syslog messages, this address is referenced as *gaddr*.
 - *foreign_ip*—An untranslated IP address on an external network. *foreign_ip* is an address for hosts on the external network. If the **alias** command is in use, an inbound message originating for the *foreign_ip* source address is translated to *dnat_ip* by PIX Firewall.
 - *dnat_ip*—(dual NAT) A translated (by the **alias** command) IP address on an external network. In an outbound connection destined to *dnat_ip*, it will be untranslated to *foreign_ip*. In syslog messages, this address is referenced as *faddr*.
 - *virtual_ip*—(used with the **virtual** command) A fictitious public or private IP address that is not the address of a real web server on the interface you are accessing. We recommend that you use an RFC 1918 address or one you make up.

Ports

The following literal names can be used instead of a numerical port value in command lines:

PIX Firewall permits the following TCP literal names: **bgp**, **chargen**, **cmd**, **daytime**, **discard**, **domain**, **echo**, **exec**, **finger**, **ftp**, **ftp-data**, **gopher**, **h323**, **hostname**, **http**, **ident**, **irc**, **klogin**, **kshell**, **lpd**, **nntp**, **pop2**, **pop3**, **pptp**, **rpc**, **smtp**, **sqlnet**, **sunrpc**, **tacacs**, **talk**, **telnet**, **time**, **uucp**, **whois**, and **www**.

PIX Firewall uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net. This value, however, does not agree with IANA port assignments.

PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you will need to reconfigure it to listen on ports 1645 and 1646.

Permitted UDP literal names are **biff**, **bootpc**, **bootps**, **discard**, **dnsix**, **echo**, **mobile-ip**, **nameserver**, **netbios-dgm**, **netbios-ns**, **ntp**, **rip**, **snmp**, **snmptrap**, **sunrpc**, **syslog**, **tacacs**, **talk**, **tftp**, **time**, **who**, and **xmcp**.



Note

To assign a port for DNS access, use **domain**, not **dns**. The **dns** keyword translates into the port value for **dnsix**.

Port numbers can be viewed online at the IANA website:

<http://www.iana.org/assignments/port-numbers>

Table D-1 lists the literal values.

Table D-1 Port Literal Values

Literal	Value	Description
bgp	179	Border Gateway Protocol, RFC 1163
biff	512	Used by mail system to notify users that new mail is received

Table D-1 Port Literal Values (continued)

Literal	Value	Description
bootpc	68	Bootstrap Protocol Client
bootps	67	Bootstrap Protocol Server
chargen	19	Character Generator
cmd	514	Similar to exec except that cmd has automatic authentication
daytime	13	Day time, RFC 867
discard	9	Discard
domain	53	DNS (Domain Name System)
dnsix	195	DNSIX Session Management Module Audit Redirector
echo	7	Echo
exec	512	Remote process execution
finger	79	Finger
ftp	21	File Transfer Protocol (control port)
ftp-data	20	File Transfer Protocol (data port)
gopher	70	Gopher
hostname	101	NIC Host Name Server
nameserver	42	Host Name Server
ident	113	Ident authentication service
irc	194	Internet Relay Chat protocol
isakmp	500	ISAKMP
klogin	543	KLOGIN
kshell	544	Korn Shell
lpd	515	Line Printer Daemon - printer spooler
login	513	Remote login
mobile-ip	434	MobileIP-Agent
netbios-ns	137	NetBIOS Name Service
netbios-dgm	138	NetBIOS Datagram Service
nntp	119	Network News Transfer Protocol
ntp	123	Network Time Protocol
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode
pop2	109	Post Office Protocol - Version 2
pop3	110	Post Office Protocol - Version 3
radius	1645, 1646	Remote Authentication Dial-In User Service
rip	520	Routing Information Protocol
smtp	25	Simple Mail Transport Protocol
snmp	161	Simple Network Management Protocol
snmptrap	162	Simple Network Management Protocol - Trap

Table D-1 Port Literal Values (continued)

Literal	Value	Description
sqlnet	1521	Structured Query Language Network
sunrpc	111	Sun RPC (Remote Procedure Call)
syslog	514	System Log
tacacs	49	TACACS+ (Terminal Access Controller Access Control System Plus)
talk	517	Talk
telnet	23	RFC 854 Telnet
tftp	69	Trivial File Transfer Protocol
time	37	Time
uucp	540	UNIX-to-UNIX Copy Program
who	513	Who
whois	43	Who Is
www	80	World Wide Web
xdmcp	177	X Display Manager Control Protocol, used to communicate between X terminals and workstations running UNIX

Protocols and Applications

This section provides information about the protocols and applications with which you may need to work when configuring PIX Firewall. It includes the following topics:

- [Supported Multimedia Applications](#)
- [Supported Protocols and Applications](#)

Possible literal values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **ipsec**, **nos**, **ospf**, **pcp**, **snp**, **tcp**, and **udp**. You can also specify any protocol by number. The **esp** and **ah** protocols only work in conjunction with Private Link.



Note

PIX Firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their data. If you need to send routing protocols across the PIX Firewall, configure the routers with the Cisco IOS software **neighbor** command. We consider it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.

[Table D-2](#) lists the numeric values for the protocol literals.

Table D-2 Protocol Literal Values

Literal	Value	Description
ah	51	Authentication Header for IPv6, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	Encapsulated Security Payload for IPv6, RFC 1827

Table D-2 Protocol Literal Values (continued)

Literal	Value	Description
gre	47	General Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
igmp	2	Internet Group Management Protocol, RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	IP-in-IP encapsulation
nos	94	Network Operating System (Novell's NetWare)
ospf	89	Open Shortest Path First routing protocol, RFC 1247
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768

Protocol numbers can be viewed online at the IANA website:

<http://www.iana.org/assignments/protocol-numbers>

Supported Multimedia Applications

PIX Firewall supports the following multimedia and video conferencing applications:

- CUseeMe Networks CU-SeeMe
- CUseeMe Networks CU-SeeMe Pro
- CUseeMe Networks MeetingPoint
- Intel Internet Video Phone
- Microsoft NetMeeting
- Microsoft NetShow
- NetMeeting
- RealNetworks RealAudio and RealVideo
- Point-to-Point Protocol over Ethernet (PPPoE)
- VDOnet VDOLive
- VocalTec Internet Phone
- VXtreme WebTheater
- Xing StreamWorks

Supported Protocols and Applications

PIX Firewall supports the following TCP/IP protocols and applications:

- Address Resolution Protocol (ARP)
- Archie
- Berkeley Standard Distribution (BSD)-rcmnds
- Bootstrap Protocol (BOOTP)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Generic Route Encapsulation (GRE)
- Gopher
- HyperText Transport Protocol (HTTP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol (IP)
- NetBIOS over IP (Microsoft Networking)
- Point-to-Point Tunneling Protocol (PPTP)
- Simple Network Management Protocol (SNMP)
- Sitara Networks Protocol (SNP)
- SQL*Net (Oracle client/server protocol)
- Sun Remote Procedure Call (RPC) services, including Network File System (NFS)
- Telnet
- Transmission Control Protocol (TCP)
- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)

Using Subnet Masks

This section lists information by subnet mask and identifies which masks are for networks, hosts, and broadcast addresses.

**Note**

In some networks, broadcasts are also sent on the network address.

This section includes the following topics:

- [Masks](#)
- [Uses for Subnet Information](#)
- [With Limited IP Addresses](#)
- [Addresses in the .128 Mask](#)
- [Addresses in the .192 Mask](#)
- [Addresses in the .224 Mask](#)

- [Addresses in the .240 Mask](#)
- [Addresses in the .248 Mask](#)
- [Addresses in the .252 Mask](#)

Masks

For the PIX Firewall commands that accept network masks, specify the correct mask for a network address. For hosts, use 255.255.255.255. However, for the **ip address** command, use a network mask, and for the **global** command, use a network address for both Port Address Translation (PAT) addresses and when specifying a pool of global addresses.

For the **conduit** and **access-list** commands, precede host addresses with the **host** parameter and without specifying a mask.

The following are examples of commands in which a mask can be specified:

```
ip address inside 10.1.1.1 255.255.255.0
ip address outside 209.165.201.1 255.255.255.224
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 209.165.201.2 netmask 255.255.255.224
static (inside,outside) 209.165.201.3 10.1.1.3 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.3 eq www
aaa authentication include http outside 209.165.201.3 255.255.255.255 0 0 TACACS+
route outside 0 0 209.165.201.4 1
telnet 10.1.1.2 255.255.255.255
```

In these examples, the **ip address** commands specify addresses for the inside and outside network interfaces. The **ip address** command only uses network masks. The inside interface is a Class A address, but only the last octet is used in the example network and therefore has a Class C mask. The outside interface is part of a subnet so the mask reflects the .224 subnet value.

The **nat** command lets users start connections from the inside network. Because a network address is specified, the class mask specified by the **ip address inside** command is used.

The **global** command provides a PAT address to handle the translated connections from the inside. The global address is also part of the subnet and contains the same mask specified in the **ip address outside** command.

The **static** command maps an inside host to a global address for access by outside users. Host masks are always specified as 255.255.255.255.

The **access-list** command permits any outside host to access the global address specified by the **static** command. The **host** parameter is the same as if you specified 209.165.201.3 255.255.255.255.

The **aaa** command indicates that any users wishing to access the global address must be authenticated. Because authentication only occurs when users access the specified global which is mapped to a host, the mask is for a host. The “0 0” entry indicates any host and its respective mask.

The **route** statement specifies the address of the default router. The “0 0” entry indicates any host and its respective mask.

The **telnet** command specifies a host that can access the PIX Firewall unit’s console using Telnet. Because it is a single host, a host mask is used.

If you are using subnet masks, refer to “[Using Subnet Masks](#),” to be sure that each IP address you choose for global or static addresses is in the correct subnet.

The subnet masks are also identified by the number of bits in the mask. [Table D-3](#) lists subnet masks by the number of bits in the network ID.

Table D-3 Masks Listed by Number of Bit

Network ID Bits	Host ID Bits	Subnet	Example Notation	# of Subnets	# of Hosts on Each Subnet
24	8	.0	192.168.1.1/24	1	254
25	7	.128	192.168.1.1/25	2	126
26	6	.192	192.168.1.1/26	4	62
27	5	.224	192.168.1.1/27	8	30
28	4	.240	192.168.1.1/28	16	14
29	3	.248	192.168.1.1/29	32	6
30	2	.252	192.168.1.1/30	64	2

The .255 mask indicates a single host in a network.

Uses for Subnet Information

Use subnet information to ensure that your host addresses are in the same subnet and that you are not accidentally using a network or broadcast address for a host.

The network address provides a way to reference all the addresses in a subnet, which you can use in the **global**, **outbound**, and **static** commands. For example, you can use the following net **static** command statement to map global addresses 192.168.1.65 through 192.168.1.126 to local addresses 192.168.2.65 through 192.168.2.126:

```
static (dmz1,dmz2) 192.168.1.64 192.168.2.64 netmask 255.255.255.192.
```

Subnet mask information is especially valuable when you have disabled Network Address Translation (NAT) using the **nat 0** command. PIX Firewall requires that IP addresses on each interface be in different subnets.

However all the hosts on a PIX Firewall interface between the PIX Firewall and the router must be in the same subnet as well. For example, if you have an address such as 192.168.17.0 and you are not using NAT, you could use the 255.255.255.192 subnet mask for all three interfaces and use addresses 192.168.17.1 through 192.168.17.62 for the outside interface, 192.168.17.65 through 192.168.17.126 for the perimeter interface, and 192.168.17.129 through 192.168.17.190 for the inside interface.

With Limited IP Addresses

Another use for subnet mask information is for network planning when an Internet service provider (ISP) gives you a limited number of IP addresses and requires you to use a specific subnet mask. Use the information in this appendix to ensure that the outside addresses you choose are in the subnet for the appropriate subnet mask.

For example, if your ISP assigns you 192.168.17.176 with a subnet mask of .240, you can see in [Table D-7](#), Subnet Number 12 for the .240 mask, that hosts can have IP addresses of 192.168.17.177 through 192.168.17.190. Because this only yields 14 hosts, you will probably use one for your router, another for the outside interface of the PIX Firewall, one for a static for a web server, if you have it, one for a static for your mail server, and the remaining 10 for global addresses. One of these addresses should be a PAT address so that you do not run out of global addresses.

Addresses in the .128 Mask

Table D-4 lists valid addresses for the .128 subnet mask. This mask permits up to 2 subnets with enough host addresses for 126 hosts per subnet.

Table D-4 .128 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.126	.127
2	.128	.129	.254	.255

Addresses in the .192 Mask

Table D-5 lists valid addresses for the .192 subnet mask. This mask permits up to 4 subnets with enough host addresses for 62 hosts per subnet.

Table D-5 .192 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.62	.63
2	.64	.65	.126	.127
3	.128	.129	.190	.191
4	.192	.193	.254	.255

Addresses in the .224 Mask

Table D-6 lists valid addresses for the .224 subnet mask. This mask permits up to 8 subnets with enough host addresses for 30 hosts per subnet.

Table D-6 .224 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.30	.31
2	.32	.33	.62	.63
3	.64	.65	.94	.95
4	.96	.97	.126	.127
5	.128	.129	.158	.159
6	.160	.161	.190	.191
7	.192	.193	.222	.223
8	.224	.225	.254	.255

Addresses in the .240 Mask

Table D-7 lists valid addresses for the .240 subnet mask. This mask permits up to 16 subnets with enough host addresses for 14 hosts per subnet.

Table D-7 .240 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.14	.15
2	.16	.17	.30	.31
3	.32	.33	.46	.47
4	.48	.49	.62	.63
5	.64	.65	.78	.79
6	.80	.81	.94	.95
7	.96	.97	.110	.111
8	.112	.113	.126	.127
9	.128	.129	.142	.143
10	.144	.145	.158	.159
11	.160	.161	.174	.175
12	.176	.177	.190	.191
13	.192	.193	.206	.207
14	.208	.209	.222	.223
15	.224	.225	.238	.239
16	.240	.241	.254	.255

Addresses in the .248 Mask

Table D-8 lists valid addresses for the .248 subnet mask. This mask permits up to 32 subnets with enough host addresses for 6 hosts per subnet.

Table D-8 .248 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.6	.7
2	.8	.9	.14	.15
3	.16	.17	.22	.23
4	.24	.25	.30	.31
5	.32	.33	.38	.39
6	.40	.41	.46	.47
7	.48	.49	.54	.55

Table D-8 .248 Network Mask Addresses (continued)

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
8	.56	.57	.62	.63
9	.64	.65	.70	.71
10	.72	.73	.78	.79
11	.80	.81	.86	.87
12	.88	.89	.94	.95
13	.96	.97	.102	.103
14	.104	.105	.110	.111
15	.112	.113	.118	.119
16	.120	.121	.126	.127
17	.128	.129	.134	.135
18	.136	.137	.142	.143
19	.144	.145	.150	.151
20	.152	.153	.158	.159
21	.160	.161	.166	.167
22	.168	.169	.174	.175
23	.176	.177	.182	.183
24	.184	.185	.190	.191
25	.192	.193	.198	.199
26	.200	.201	.206	.207
27	.208	.209	.214	.215
28	.216	.217	.222	.223
29	.224	.225	.230	.231
30	.232	.233	.238	.239
31	.240	.241	.246	.247
32	.248	.249	.254	.255

Addresses in the .252 Mask

Table D-9 lists valid addresses for the .252 subnet mask. This mask permits up to 64 subnets with enough host addresses for 2 hosts per subnet.

Table D-9 .252 Network Mask Addresses

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
1	.0	.1	.2	.3
2	.4	.5	.6	.7

Table D-9 .252 Network Mask Addresses (continued)

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
3	.8	.9	.10	.11
4	.12	.13	.14	.15
5	.16	.17	.18	.19
6	.20	.21	.22	.23
7	.24	.25	.26	.27
8	.28	.29	.30	.31
9	.32	.33	.34	.35
10	.36	.37	.38	.39
11	.40	.41	.42	.43
12	.44	.45	.46	.47
13	.48	.49	.50	.51
14	.52	.53	.54	.55
15	.56	.57	.58	.59
16	.60	.61	.62	.63
17	.64	.65	.66	.67
18	.68	.69	.70	.71
19	.72	.73	.74	.75
20	.76	.77	.78	.79
21	.80	.81	.82	.83
22	.84	.85	.86	.87
23	.88	.89	.90	.91
24	.92	.93	.94	.95
25	.96	.97	.98	.99
26	.100	.101	.102	.103
27	.104	.105	.106	.107
28	.108	.109	.110	.111
29	.112	.113	.114	.115
30	.116	.117	.118	.119
31	.120	.121	.122	.123
32	.124	.125	.126	.127
33	.128	.129	.130	.131
34	.132	.133	.134	.135
35	.136	.137	.138	.139
36	.140	.141	.142	.143
37	.144	.145	.146	.147

Table D-9 .252 Network Mask Addresses (continued)

Subnet Number	Network Address	Starting Host Address	Ending Host Address	Broadcast Address
38	.148	.149	.150	.151
39	.152	.153	.154	.155
40	.156	.157	.158	.159
41	.160	.161	.162	.163
42	.164	.165	.166	.167
43	.168	.169	.170	.171
44	.172	.173	.174	.175
45	.176	.177	.178	.179
46	.180	.181	.182	.183
47	.184	.185	.186	.187
48	.188	.189	.190	.191
49	.192	.193	.194	.195
50	.196	.197	.198	.199
51	.200	.201	.202	.203
52	.204	.205	.206	.207
53	.208	.209	.210	.211
54	.212	.213	.214	.215
55	.216	.217	.218	.219
56	.220	.221	.222	.223
57	.224	.225	.226	.227
58	.228	.229	.230	.231
59	.232	.233	.234	.235
60	.236	.237	.238	.239
61	.240	.241	.242	.243
62	.244	.245	.246	.247
63	.248	.249	.250	.251
64	.252	.253	.254	.255

