IP Access Lists

packetlife.net

Standard IP ACL Syntax

```
! Legacy syntax
access-list <number> {permit | deny} <source> [log]

! Modern syntax
ip access-list standard {<number> | <name>}
 [<sequence>] {permit | deny} <source> [log]
```

Actions

permit	Allow matched packets
deny	Deny matched packets
remark	Record a config comment
evaluate	Evaluate a reflexive ACL

Extended IP ACL Syntax

```
! Legacy syntax
access-list <number> {permit | deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]

! Modern syntax
ip access-list extended {<number> | <name>}
 [<sequence>] {permit | deny} <protocol> <source> [<ports>] <destination> [<ports>] [<options>]
```

ACL Numbers

1-99 **1300-1999**	IP standard
100-199 **2000-2699**	IP extended
200-299	Protocol
300-399	DECnet
400-499	XNS
500-599	Extended XNS
600-699	Appletalk
700-799	Ethernet MAC
800-899	IPX standard
900-999	IPX extended
1000-1099	IPX SAP
1100-1199	MAC extended
1200-1299	IPX summary

TCP Options

ack	Match ACK flag
fin	Match FIN flag
psh	Match PSH flag
rst	Match RST flag
syn	Match SYN flag
urg	Match URG flag
established	Match packets in a pre-established session

Logging Options

log	Log ACL entry matches
log-input	Log matches with ingress interface and source MAC

Source/Destination Definitions

any	Any address
host <address>	A single address
<network> <mask>	Any address matched by the wildcard mask

IP Options

dscp <DSCP>	Match packets with the given DSCP value
fragments	Check non-initial fragments
option <option>	Match packets with the specified IP option
precedence <0-7>	Match packets with the given precedence value
ttl <count>	Match packets with the given Time To Live

TCP/UDP Port Definitions

eq <port>	Equal to	**neq <port>**	Not equal to
lt <port>	Less than	**gt <port>**	Greater than
range <port> <port>	Matches a range of port numbers		

Miscellaneous Options

reflect <name>	Create a reflexive ACL
time-range <name>	Enable rule only during the specified time range

Applying ACLs to Restrict Traffic

```
interface FastEthernet0/0
 ip access-group {<number> | <name>} {in | out}
```

Troubleshooting

```
show access-lists {<number> | <name>}
show ip access-lists {<number> | <name>}
show ip access-lists interface <interface>
show ip access-lists dynamic
show ip interface [<interface>]
show time-range [<name>]
```

by Jeremy Stretch

v1.1