

IOS IPv4 ACCESS LISTS

Standard 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 configuration comment
evaluate	Evaluate a reflexive ACL

Extended 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	IP standard
1300-1999	IP extended
100-199	Protocol
200-299	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

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 the specified IP DSCP
fragments	Check non-initial fragments
option <option>	Match the specified IP option
precedence {0-7}	Match the specified IP precedence
ttl <count>	Match the specified IP time to live (TTL)

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 entry
time-range <name>	Enable rule only during the given 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>]
```

Logging Options

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