

# Cisco Router Access Lists

Access lists can be used to control IP and IPX traffic

Named access lists, IOS 11.2, use the following syntax:  
**ip access-list standard/extended name**  
 (In config mode, you need to type "exit" after entering  
 permit / deny commands)

## Layout of an Extended IP Access List

access-list	100 to 199*	permit, deny or dynamic	IP or ICMP	source IP address xxx.xxx.xxx.xxx	source IP mask xxx.xxx.xxx.xxx	destination IP address xxx.xxx.xxx.xxx	destination IP mask xxx.xxx.xxx.xxx	testing TCP/UDP
			TCP - addresses (or ICMP - pings / trace routes)	255=ignore 0=apply	255=ignore 0=apply			
			ports	any - ANY source host - A single source	any - ANY destination host - A single destination			
			eigrp, ospf, igrp, gre, nos, ipinip, igrp <0-255> IP Protocol	ports		eq=equal gt=greater lt=less neq=not equal with port range=match port range		

\*When building the list, every line must be labeled with the same access list number.

Put a 255 corresponding to every octet in the IP address that you want to ignore, and 0 for every octet that you want the packet match to apply to.

## Layout of an Extended IPX Access List

access-list	900 to 999	permit or deny	-1 any IPX <0-255> IPX Protocol type	source IPX network -1 any IPX net <0-FFFFFFF> N.H.H.H (net.host address)	source IPX socket 0 for all sockets <0-FFFFFFF>	destination IPX network -1 any IPX net <0-FFFFFFF>
-------------	------------	----------------	---	---	---	--

### interface serial1

ip access-group <1-199 or list-name> in (out)  
 ipx access-group <800-999> in (out)  
 ipx input-sap-filter <1000-1099> | name

```
access-list 110 deny ip 192.10.0.0 0.0.255.255 any
access-list 110 permit ip any any
```

! Deny access from all nets for file services (4):

```
access-list 1001 deny -1 4
```

! Permit access from all nets to all other services:

```
access-list 1001 permit -1
```

There are two types of access lists - **standard** and **extended**.

Standard access list can analyze the packet header. Packets source IP address can be used to filter traffic (either inbound or outbound) to the interface. IPX access lists filter on IPX source and destination network layer addresses.

Extended access list can analyze the packet header. Destination IP address can be used to filter traffic. IPX extended access lists filter on IPX source and destination network layer addresses.

A router can have multiple access lists on an interface, but **only one access list is allowed per interface.**

Copyright © IT charts.com