Title:
Cisco CCNA Exam Tutorial: Configuring Standard Access Lists

Word Count:
588

Summary:
Configuring standard ACLs is a skill you'll use on all your Cisco exams. Learn the basics from Chris Bryant, CCIE #12933.

Keywords:
cisco, ccna, exam, pass, certification, access, list, standard, wildcard, mask, extended, named

Article Body:
Access Control Lists (ACLs) allow a router to permit or deny packets based on a variety of criteria. The ACL is configured in global mode, but is applied at the interface level. An ACL does not take effect until it is expressly applied to an interface with the ip access-group command. Packets can be filtered as they enter or exit an interface.

If a packet enters or exits an interface with an ACL applied, the packet is compared against the criteria of the ACL. If the packet matches the first line of the ACL, the appropriate “permit” or “deny” action is taken. If there is no match, the second line’s criterion is examined. Again, if there is a match, the appropriate action is taken; if there is no match, the third line of the ACL is compared to the packet.

This process continues until a match is found, at which time the ACL stops running. If no match is found, a default “deny” takes place, and the packet will not be processed. When an ACL is configured, if a packet is not expressly permitted, it will be subject to the implicit deny at the end of every ACL. This is the default behavior of an ACL and cannot be changed.

A standard ACL is concerned with only one factor, the source IP address of the packet. The destination is not considered. Extended ACLs consider both the source and destination of the packet, and can consider the port number as well. The numerical range used for each is different: standard ACLs use the ranges 1-99 and 1300-1399; extended lists use 100-199 and 2000 to 2699.

There are several points worth repeating before beginning to configure standard

ACLs.

Standard ACLs consider only the source IP address for matches.

The ACL lines are run from top to bottom. If there is no match on the first line, the second is run; if no match on the second, the third is run, and so on until there is a match, or the end of the ACL is reached. This top-to-bottom process places special importance on the order of the lines.

There is an implicit deny at the end of every ACL. If packets are not expressly permitted, they are implicitly denied.

If Router 3's Ethernet interface should only accept packets with a source network of 172.12.12.0, the ACL will be configured like this:

```
R3#conf t

R3(config)#access-list 5 permit 172.12.12.0 0.0.0.255
```

The ACL consists of only one explicit line, one that permits packets from source IP address 172.12.12.0 /24. The implicit deny, which is not configured or seen in the running configuration, will deny all packets not matching the first line.

The ACL is then applied to the Ethernet0 interface:

```
R3#conf t

R3(config)#interface e0

R3(config-if)#ip access-group 5 in
```

But before you write any ACLs, it's a really good idea to see what other ACLs are already running on the router! To see the ACLs running on the router, use the command show access-list.

```
R1#show access-list

Standard IP access list 1

permit 0.0.0.0
```

```
Standard IP access list 5

permit 172.1.1.1

Standard IP access list 7

permit 23.3.3.3

Extended IP access list 100

permit tcp any any lt www (26 matches)

permit tcp any any neq telnet (12 matches)

deny ip any any


Extended IP access list 105

deny tcp any any eq www

deny tcp any any eq telnet
```

You're going to use ACLs all the way up the Cisco certification ladder, and throughout your career. The importance of knowing how to write and apply ACLs is paramount, and it all starts with mastering the fundamentals!