Access Control Lists

Standard ACL

The number range is from 1-99 and 1300-1999. It is comprised of permit or deny statement/s from a source address with a wildcard mask only. The single deny statement requires that you add **permit any** as a last statement for any standard ACL or all packet are denied from all sources.

```
access-list 99 deny host 172.33.1.1
access-list 99 permit any
```

Standard Named ACL

This is defined with a name instead of a number and has the same rules as a standard ACL. The following ACL named ***internet*** and will deny all traffic from all hosts on 192.168.1.0/24 subnet. It will log any packets that are denied.

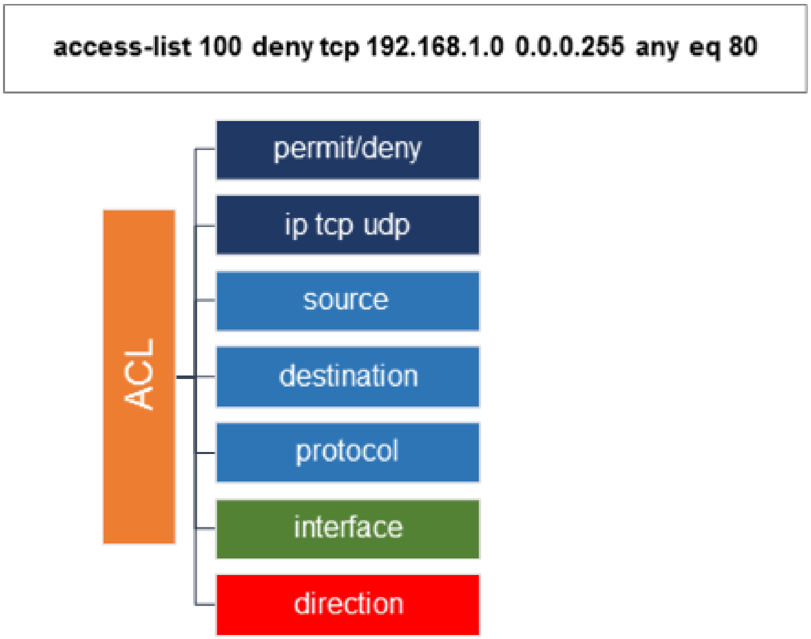
```
ip access-list internet log
deny 192.168.1.0 0.0.0.255
permit any
```

Extended ACL

The number range is from 100-199 and 2000-2699. It supports multiple permit and deny statements with source / destination IP address or subnet. In addition you can filter on IP, TCP or UDP protocols and destination port. Extended ACL must have a permit all source and destination traffic with **permit ip any any** as a last statement.

Cisco best practices for creating and applying ACLs

- apply extended ACL near source
- apply standard ACL near destination
- order ACL with multiple statements from most specific to least specific
- one ACL can be applied inbound or outbound per interface per Layer 3 protocol
- ACL is applied to an interface with **ip access-group in | out** command



```
access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 80
```

Extended Named ACL

They are defined with a name and supports all syntax commands available with extended ACLs. You can dynamically add or delete statements to any named ACL without having to delete and rewrite all lines. They are easier to manage and troubleshoot based on naming conventions. The following named ACL permits http traffic from hosts assigned to 192.168.0.0 subnets access to server 192.168.3.1

```
ip access-list extended http-filter
remark permit http to web server
permit tcp 192.168.0.0 0.0.255.255 host 192.168.3.1 eq 80
permit ip any any
```

The following are primary differences between IPv4 and IPv6 for ACLs

- IPv6 supports only named ACLs
- IPv6 permits ICMP neighbor discovery (ARP) as implicit default
- IPv6 denies all traffic as an implicit default for the last line of the ACL

ACL Example 1

The following command permits http traffic from host 10.1.1.1/24 to host 10.1.2.1/24

```
access-list 100 permit tcp host 10.1.1.1 host 10.1.2.1 eq 80
```

The access control list (ACL) statement reads from left to right as - *permit all tcp traffic from source host only to destination host that is http (80)*. The TCP refers to applications that are TCP-based. The UDP keyword is used for applications that are UDP-based such as SNMP for instance.

ACL Example 2

What is the purpose or effect of applying the following ACL?

```
access-list 100 deny ip host 192.168.1.1 host 192.168.3.1
access-list 100 permit ip any any
```

The first statement denies **all** application traffic from host-1 (192.168.1.1) to web server (host 192.168.3.1). The ***ip*** keyword refers to Layer 3 and affects all protocols and applications at layer 3 and higher. The last statement is required to permit all other traffic.

ACL Example 3

What is the purpose or effect of applying the following ACL?

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq telnet
access-list 100 permit ip any any
```

The first statement permits Telnet traffic from all hosts assigned to subnet 192.168.1.0/24 subnet. That include host-1 (192.168.1.1) and host-2 (192.168.1.2). The ***tcp*** keyword is Layer 4 and affects all protocols and applications at Layer 4 and higher. The ***permit tcp*** configuration allows the specified TCP application (Telnet).

The ***any*** keyword allows Telnet sessions to any destination host. The last statement is mandatory and required to permit all other traffic.

ACL Example 4

What is the purpose or effect of applying the following ACL?

```
access-list 100 permit ip 172.16.1.0 0.0.0.255 host 192.168.3.1
access-list 100 deny ip 172.16.2.0 0.0.0.255 any
access-list 100 permit ip any any
```

- The first ACL permits only hosts assigned to subnet 172.16.1.0/24 access to all applications on server-1 (192.168.3.1)

- The second statement denies hosts assigned to subnet 172.16.2.0/24 access to either server. That would include any additional hosts added to that subnet and any new servers added.

- The last ACL statement is required to permit all other traffic not matching previous filtering statements.

- ACL is applied to an interface with **ip access-group** command**.** Most **r**outers often have multiple interfaces (subnets) with hosts assigned. ACL applied outbound to an interface shared by multiple subnets will filter traffic from all hosts for each subnet.

Wildcard Masks

The wildcard mask is a technique for matching specific IP address or range of IP addresses. Cisco access control lists (ACL) filter based on the IP address range configured from a wildcard mask.

The wildcard mask is an inverted mask where the matching IP address or range is based on 0 bits. The additional bits are set to 1 as no match required. The wildcard 0.0.0.0 is used to match a single IP address. The wildcard mask for 255.255.224.0 is 0.0.31.255 (invert the bits so zero=1 and one=0) noted with the following example.

11111111.11111111.111 00000.00000000 = subnet mask

00000000.00000000.000 11111.11111111 = wildcard mask

ACL wildcards are configured to filter (permit/deny) based on host address range. That could include multiple hosts, all hosts per subnet or multiple subnets. All clients (desktop etc.) and network devices have network interfaces that are assigned an IP address. Each subnet has a range of host IP addresses that are assignable to network interfaces.

Classful Wildcard Example

The following wildcard **0.0.0.255** will only match on the 192.168.3.0 subnet and not match on everything else. This could be used with an ACL for example to permit or deny a subnet.

192 . 168 . 3 . 0

11000000.10101000.00000011.00000000

00000000.00000000.00000000.11111111 = 0.0.0.255

192.168.3.0 0.0.0.255 = match on 192.168.3.0 subnet only

Classless Wildcard Example

The following wildcard mask **0.0.0.3** matches on all of the addresses for 192.168.4.0/30 zero subnet only. It is equivalent to the 255.255.255.252 subnet mask. There is network address (192.168.4.0), broadcast address (192.168.4.3) and two host IP addresses for that subnet.

192 . 168 . 4 . 0

11000000.10101000.00000100.00000000

00000000.00000000.00000000.00000011 = 0.0.0.3

192.168.4.0 0.0.0.3 = match on 192.168.4.1 and 192.168.4.2 (host addresses)

ACL Example 1

Filter only on 172.16.1.0 subnet for permit or deny of packets

172.16.1.0 **0.0.0**.255

ACL Example 2

Filter only on 192.168.1.0 subnet for permit or deny of packets

192.168.1.0 **0.0.0**.255

ACL Example 3

Filter all 172.16.0.0 subnets for permit or deny of packets

172.16.0.0 **0.0.**255.255