Types of IPv4 ACLs

4.4.1

Standard and Extended ACLs

The previous topics covered the purpose of ACL and the guidelines for ACL creation. This topic will cover standard and extended ACLs, named and numbered ACLs, and the examples of placement of these ACLs.

There are two types of IPv4 ACLs:

- **Standard ACLs** – These permit or deny packets based only on the source IPv4 address.
- **Extended ACLs** – These permit or deny packets based on the source IPv4 address and destination IPv4 address, protocol type, source and destination TCP or UDP ports and more.

For example, refer to the following standard ALC command.

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#
```

ACL 10 permits hosts on the source network 192.168.10.0/24. Because of the implied "deny any" at the end, all traffic except for traffic coming from the 192.168.10.0/24 network is blocked with this ACL.

In the next example, an extended ACL 100 permits traffic originating from any host on the 192.168.10.0/24 network to any IPv4 network if the destination host port is 80 (HTTP).

```
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)#
```

Notice how the standard ACL 10 is only capable of filtering by source address while the extended ACL 100 is filtering on the source, and destination Layer 3, and Layer 4 protocol (i.e., TCP) information.

Note: Full ACL configuration is discussed in another module.

4.4.2

Numbered and Named ACLs

Numbered ACLs

ACLs number 1 to 99, or 1300 to 1999 are standard ACLs while ACLs number 100 to 199, or 2000 to 2699 are extended ACLs, as shown in the output.

```
R1(config)# access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
  <1300-1999>  Extended 48-bit MAC address access list
  <1300-1999>  IP standard access list (expanded range)
  <200-299>  Protocol type-code access list
  <2000-2699>  IP extended access list (expanded range)
  <700-799>  48-bit MAC address access list
  rate-limit  Simple rate-limit specific access list
  template   Enable IP template acls
R1(config)# access-list
```

Named ACLs

Named ACLs is the preferred method to use when configuring ACLs. Specifically, standard and extended ACLs can be named to provide information about the purpose of the ACL. For example, naming an extended ACL FTP-FILTER is far better than having a numbered ACL 100.

The **ip access-list** global configuration command is used to create a named ACL, as shown in the following example.

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

The following summarizes the rules to follow for named ACLs.

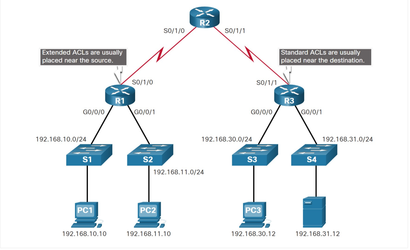
- Assign a name to identify the purpose of the ACL.
- Names can contain alphanumeric characters.
- Names cannot contain spaces or punctuation.
- It is suggested that the name be written in CAPITAL LETTERS.
- Entries can be added or deleted within the ACL.

4.4.3

Where to Place ACLs

Every ACL should be placed where it has the greatest impact on efficiency.

The figure illustrates where standard and extended ACLs should be located in an enterprise network. Assume the objective to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.



Extended ACLs should be located as close as possible to the source of the traffic to be filtered. This way, undesirable traffic is denied close to the source network without crossing the network infrastructure.

Standard ACLs should be located as close to the destination as possible. If a standard ACL was placed at the source of the traffic, the "permit" or "deny" will occur based on the given source address no matter where the traffic is destined.

Placement of the ACL and therefore, the type of ACL used, may also depend on a variety of factors as listed in the table.

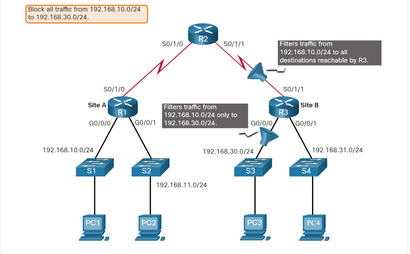
Factors Influencing ACL Placement	Explanation
The extent of organizational control	Placement of the ACL can depend on whether or not the organization has control of both the source and destination networks.
Bandwidth of the networks involved	It may be desirable to filter unwanted traffic at the source to prevent transmission of bandwidth-consuming traffic.
Ease of configuration	• It may be easier to implement an ACL at the destination, but traffic will use bandwidth unnecessarily. • An extended ACL could be used on each router where the traffic originated. This would save bandwidth by filtering the traffic at the source, but it would require creating extended ACLs on multiple routers.

4.4.4

Standard ACL Placement Example

Following the guidelines for ACL placement, standard ACLs should be located as close to the destination as possible.

In the figure, the administrator wants to prevent traffic originating in the 192.168.10.0/24 network from reaching the 192.168.30.0/24 network.



Following the basic placement guidelines, the administrator would place a standard ACL on router R3. There are two possible interfaces on R3 to apply the standard ACL:

- **R3 S0/1/1 interface (inbound)** – The standard ACL can be applied inbound on the R3 S0/1/1 interface to deny traffic from .10 network. However, it would also filter .10 traffic to the 192.168.31.0/24 (.31 in this example) network. Therefore, the standard ACL should not be applied to this interface.
- **R3 G0/0 interface (outbound)** – The standard ACL can be applied outbound on the R3 G0/0/0 interface. This will not affect other networks that are reachable by R3. Packets from .10 network will still be able to reach the .31 network. This is the best interface to place the standard ACL to meet the traffic requirements.

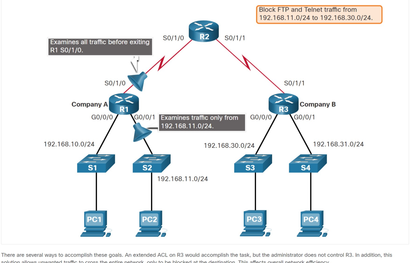
4.4.5

Extended ACL Placement Example

Extended ACL should be located as close to the source as possible. This prevents unwanted traffic from being sent across multiple networks only to be denied when it reaches its destination.

However, the organization can only place ACLs on devices that they control. Therefore, the extended ACL placement must be determined in the context of where organizational control extends.

In the figure, for example, Company A wants to deny Telnet and FTP traffic to Company B's 192.168.30.0/24 network from their 192.168.11.0/24 network while permitting all other traffic.



There are several ways to accomplish these goals. An extended ACL on R3 would accomplish the task, but the administrator does not control R3. In addition, this solution allows unwanted traffic to cross the entire network, only to be blocked at the destination. This affects overall network efficiency.

The solution is to place an extended ACL on R1 that specifies both source and destination addresses.

There are two possible interfaces on R1 to apply the extended ACL:

- **R1 S0/1/0 interface (outbound)** – The extended ACL can be applied outbound on the S0/1/0 interface. However, this solution will process all packets leaving R1 including packets from 192.168.10.0/24.
- **R1 G0/0/1 interface (inbound)** – The extended ACL can be applied inbound on the G0/0/1 and only packets from the 192.168.11.0/24 network are subject to ACL processing on R1. Because the filter is to be limited to only those packets leaving the 192.168.11.0/24 network, applying the extended ACL to G0/1 is the best solution.

4.4.6

Check Your Understanding - Types of IPv4 ACLs

Check your understanding of the types of IPv4 ACLs by choosing the BEST answer to the following questions.

1. Which ACL is capable of filtering based on TCP port number?
   - (•) extended ACL
   - ( ) standard ACL

2. Which statement about ACLs is true?
   - ( ) Extended ACLs are numbered 1300 - 2699.
   - (•) Named ACLs can be standard or extended.
   - (•) Numbered ACLs is the preferred method to use when configuring ACLs.
   - ( ) Standard ACLs are numbered 1 - 199.

3. Where should a standard ACL be placed?
   - ( ) Standard ACL location is not important.
   - (•) Standard ACLs should be placed as close to the destination as possible.
   - ( ) Standard ACLs should be placed as close to the source as possible.
   - ( ) Standard ACLs should be placed on serial interfaces.

4. Where should an extended ACL be placed?
   - ( ) Extended ACL location is not important.
   - ( ) Extended ACLs should be located as close to the destination as possible.
   - (•) Extended ACLs should be located as close to the source as possible.
   - ( ) Extended ACLs should be located on serial interfaces.

Check | Show Me | Reset