Expert Reference Series of White Papers

The Basics of Configuring and Using Cisco Access Control Lists

www.globalknowledge.com
The Basics of Configuring and Using Cisco Access Control Lists
Raymond B. Dooley, MBA, CCSI, CCNA, CCNP, CCDA, CCDP, SE, FE, Global Knowledge Course Director, Global Knowledge Course Director

Introduction
Cisco Access Control Lists (ACLs) are used in nearly all product lines for several purposes, including filtering packets (data traffic) as it crosses from an inbound port to an outbound port on a router or switch, defining classes of traffic, and restricting access to devices or services. Knowing how to design, configure, and troubleshoot ACLs is required for all network engineers working within a Cisco network.

The objective is to provide a fundamental explanation of Cisco ACLs with the following topics:

1. An analogy about filtering
2. The uses of ACLs
3. Types of ACLs, operations and best practices
4. Wildcard Masks
5. Configuring named ACLs with examples
6. Monitoring ACLs

An Analogy about Filtering
Honolulu—with its famous Waikiki Beach, Pearl Harbor, zoo, aquarium, and Hawaiian historical sites—is a favorite vacation spot. However, transportation to the beach and other local sites can be an issue, so it is important to know the criteria for using the transportation (filter) and the services offered (route, etc.). The following is a list of options.

- The **Pink Line trolley** passes all the beach hotels and the shopping center. If the passenger is staying at a beach hotel and has a key, then there is no fare. Otherwise, it is $2.50.

- **Charted Trolleys** have the same route as the Pink Line but the passenger must show proof of having paid for the service as part of a vacation tour package.

- The **city bus** will go anywhere on the island for a fare of $2.50 or $1.00 for seniors. However each bus has a strict route and schedule.

- **Shuttle Buses and Taxis** will follow any route chosen but with a higher metered or published fare. In other words, the only criterion is cash.
The point of the analogy is that filtering happens all of the time everywhere, not just in networks. Depending on the type of transportation service chosen, the passenger will be permitted if the fare conditions are met and denied if the conditions are not met. So, as the graphic shows, there are multiple levels of service and well defined permit/deny conditions. Another way to state this is that if proper criteria is matched, either a permit or deny is executed. With networks, the method to match must be defined and the application of the filter must be designed as well, and using an ACL is a method to do it.

### The Uses for Access Control Lists

#### Why Use ACLs?

- Filtering: Manage IP traffic by filtering packets passing through a router
- Classification: Identify traffic for special handling
One of the two major reasons to use ACLs in a Cisco network is to either filter traffic going through the router or switch, or traffic to and from the device. The other reason is to classify traffic for access to services or to trigger an event.

As the graphic shows, a good place for a filter is between the enterprise network and the Internet. An entire range of firewalling technologies exist here, and ACLs are one tool.

**ACL Applications: Filtering**

- Permit or deny packets moving through the router.
- Permit or deny Telnet access to or from the router.
- Without ACLs, all packets could be transmitted to all parts of your network.

The graphic further clarifies the idea. It is the company’s policy that not all traffic from the computer on the left will be allowed to exit the router via the interface on the right. Virtually all companies have detailed security policy (or should have one) and the policy is followed to implement proper filtering.

**ACL Applications: Classification**

Special handling for traffic based on packet tests
The graphic illustrates three more uses of ACLs to classify traffic (IP addresses) for specific purposes. For example, filtering can be used to identify the traffic which is allowed to traverse a virtual private network (VPN), and the block of IP addresses to be translated by the network address translation (NAT) process.

Also, routers and multi-layer switches run dynamic routing protocols such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Protocol (EIGRP) to exchange lists of reachable IP networks. These updates can be filtered with ACLs to limit the number of IP addresses in the list of routes learned.

**Types of Access Lists, Operations, and Best Practices**

### Types of ACLs

- **Standard ACL**
  - Checks source address
  - Generally permits or denies entire protocol suite

- **Extended ACL**
  - Checks source and destination address
  - Generally permits or denies specific protocols and applications

- **Two methods used to identify standard and extended ACLs:**
  - Numbered ACLs use a number for identification
  - Named ACLs use a descriptive name or number for identification

Access lists are categorized based on the granularity of the filtering. Similar to the analogy, the match criteria to ride the chartered trolleys is much more specific than to ride the city bus. Multiple protocols have ACLs in Cisco, but IP is by far the most common and the only one described here.

**Standard Access Lists** use the simplest matching criteria of all—the source IP address in the IP packet. Based on matching the source IP address, permit or deny logic can be applied.

As the name implies, **Extended Access Lists** use a much more detailed list of match criteria, including source IP address, destination IP address, protocol type field in the IP header, TCP/UDP port number, and additional criteria such as time range.

For both types, the **wildcard mask** identifies a “range” or block of addresses or a specific host.

Cisco ACLs may be numbered or named. A range of numbers for each type of list has been defined by Cisco, and numbered ACLs have been used for years. The named access list is more convenient and easier to edit. The operation of each is identical. Named access lists are recommended for engineers learning ACLs for the first time. Configuration syntax will be covered later.
How to Identify ACLs

<table>
<thead>
<tr>
<th>IPv4 ACL Type</th>
<th>Number Range/Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbered Standard</td>
<td>1–99, 1300–1999</td>
</tr>
<tr>
<td>Numbered Extended</td>
<td>100–199, 2000–2699</td>
</tr>
<tr>
<td>Named (Standard and Extended)</td>
<td>Name</td>
</tr>
</tbody>
</table>

- Numbered standard IPv4 lists (1–99) test conditions of all IP packets for source addresses. Expanded range (1300–1999).
- Numbered extended IPv4 lists (100–199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports. Expanded range (2000–2699).
- Named ACLs identify IP standard and extended ACLs with an alphanumeric string (name).

The graphic shows the Cisco ACL numbering scheme.

ACL Configuration Guidelines

- Standard or extended indicates what can be filtered.
- Only one ACL per interface, per protocol, and per direction is allowed.
- The order of ACL statements controls testing, therefore, the most specific statements go at the top of the list.
- The last ACL test is always an implicit deny everything else statement, so every list needs at least one permit statement.
- ACLs are created globally and then applied to interfaces for inbound or outbound traffic.
- An ACL can filter traffic going through the router, or traffic to and from the router, depending on how it is applied.
- When placing ACLs in the network:
  - Place extended ACLs close to the source
  - Place standard ACLs close to the destination

Since the entries in an ACL are processed in order from the top down, and since ACLs require computer and memory resources in the device, a set of strict rules are applied as shown in the graphic.
The “protocol” defined in the list is IP, so there is a maximum of one IP ACL inbound and one outbound on an interface. The configuration will be covered later.

**Outbound ACL Operation**

The graphic shows router logic in checking for the existence of and using an outbound ACL. One thing to note with an outbound list is that the router has already expended the resources to route the packet before the permit/deny logic is applied to the packet. If the ACL is inbound, the permit/deny logic is applied before the routing process occurs.

**A List of Tests: Deny or Permit**

The graphic shows router logic in checking for the existence of and using an outbound ACL. One thing to note with an outbound list is that the router has already expended the resources to route the packet before the permit/deny logic is applied to the packet. If the ACL is inbound, the permit/deny logic is applied before the routing process occurs.
Each line in the list is processed in top-down order. As soon as a match for either permit or deny happens, the required action is taken and the list processing stops. That is why it is so important to permit or deny specific items such as hosts before permitting or denying entire subnets or larger address blocks.

The last line in all ACLs is an implicit deny of all packets.

**Wildcard Masks**

### Wildcard Bits: How to Check the Corresponding Address Bits

- 0 means to match the value of the corresponding address bit
- 1 means to ignore the value of the corresponding address bit

Binary masks are used in IP address subnetting and planning to identify the bit boundary between the network portion of the address and the host part. With a network mask, the ones in the mask imply network and the zeroes imply hosts. For example, 192.168.34.0 255.255.255.0 or 192.168.34.0/24 means that 24 bits of the address are network and 8 bits are host. Using the proper address and mask (subnetting) can be more complex than this example and is covered in Cisco training courses.

To identify IP addresses and blocks of addresses for ACLs, a **wildcard mask** is used. The principal is the same as subnetting but the bit order of the mask is reversed or “inverted.”

To identify the same hosts as in the previous example with a wildcard mask, it would be 192.168.34.0 0.0.0.255, where the zeroes in the mask mean match and the ones mean irrelevant.

The matching for the permit or deny action using IP addresses can then be very granular. The graphic provides another example of matching with the wildcard mask.
The graphic shows several abbreviations and shortcuts for identifying specific hosts and “wildcards” that mean any IP address is a match.

### Configuring Named Access Control Lists

#### Named IP ACL Configuration

```bash
RouterX(config)#
  ip access-list {standard | extended} name
  # Alphanumeric name string must be unique

RouterX(config {std- | ext-}nacl)#
  [sequence-number] {permit | deny} {ip access list test conditions}
  {permit | deny} {ip access list test conditions}
  # If not configured, sequence numbers are generated automatically starting at 10 and incrementing by 10
  # no sequence number removes the specific test from the named ACL

RouterX(config-if)#
  ip access-group name {in | out}
  # Activates the named IP ACL on an interface
```
The Cisco IOS syntax for configuring a named ACL is shown in the graphic. The ACLs can be easily edited by removing and inserting sequence numbered lines without removing the entire list.

**Named Standard IPv4 ACL Example**

In the standard access list shown in the graphic, an individual host is denied and the rest of that host’s subnet is permitted. Remember, all traffic from the host is denied including responses to packets sent to the denied host.

The ACL is applied outbound on the E0 interface with the `access-group` command.

**Standard ACLs to Control vty Access**

```
RouterX(config-line)#
access-class access-list-number/name {in | out}
```

- Restricts incoming or outgoing connections between a particular vty and the addresses in an ACL

**Example:**

```
ip access-list standard notelnet
permit 192.168.1.0 0.0.0.255
(implicit deny any)
line vty 0 4
access-class notelnet in
```

- Permits only hosts in network 192.168.1.0 0.0.0.255 to connect to the router vty lines
The graphic shows a method to allow only the users of a specific network to telnet to the router. Incoming telnets to a Cisco router are accepted on vty lines and that is where the filter is applied with the `access-class` command.

**Named Extended IPv4 ACL Example**

```
RouterX(config)#ip access-list extended badgroup
RouterX(config-ext-nacl)#deny tcp 172.16.4.0 0.0.0.255 any eq 23
RouterX(config-ext-nacl)#permit ip any any
RouterX(config-ext-nacl)#interface e0
RouterX(config-if)#ip access-group badgroup out
```

**Deny Telnet from a specific subnet**

A named access-list is depicted in the graphic. Notice that the source and destinations are both shown along with a destination TCP port. It is applied to the interface with the same commands as a standard access list.

### Commenting ACL Statements

```
RouterX(config)#
ip access-list {standard|extended} name
```

- Creates a named ACL

```
RouterX(config {std- | ext-}nacl)#
remark remark
```

- Creates a named ACL comment

Or

```
RouterX(config)#
access-list access-list-number remark remark
```

- Creates a numbered ACL comment

Comments or remarks in the ACL are helpful in that they provide information about the purpose of the list to others who may look at it for troubleshooting or monitoring. The graphic shows how these comments may be added.
Monitoring Access Control Lists

Monitoring ACL Statements

To monitor ACLs for troubleshooting, there are only two commands:

1. **Show access-list** is used to determine if the ACL is written properly to meet the security policy objectives.

2. **Show ip interface** is used to determine the interface on which the ACL has been implemented and in what direction—in or out.

Verifying ACLs

To monitor ACLs for troubleshooting, there are only two commands:

1. **Show access-list** is used to determine if the ACL is written properly to meet the security policy objectives.

2. **Show ip interface** is used to determine the interface on which the ACL has been implemented and in what direction—in or out.
3. If an ACL is implemented on a vty line to limit telnet access, show line can be used to monitor the location.

Troubleshooting ACLs is then a simple process:

- Make sure the list is correct
- Verify that it is applied on the correct interface and correct direction

Conclusion

If the configuration files on a thousand or more Cisco multilayer devices in enterprise networks were analyzed, there would be ACLs in almost every one of them. There are also many trouble tickets generated in network operations centers every day requiring the repair of an ACL. From this, it is simple to conclude that understanding, designing, implementing, and troubleshooting ACLs are required skills for network engineers. The topic also appears in the CCNA examination in multiple questions and simulations.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

ICND1 v2.0 - Interconnecting Cisco Networking Devices, Part 1
ICND2 v2.0 - Interconnecting Cisco Networking Devices, Part 2
CCNAX v2.0 - CCNA Routing and Switching Boot Camp
IINS 2.0 - Implementing Cisco IOS Network Security

Visit www.globalknowledge.com or call 1-800-COURSES (1-800-268-7737) to speak with a Global Knowledge training advisor.

About the Author

Ray Dooley has been a network professional for over 30 years. He is a Global Knowledge Course Director for CCDA, ARCH, SWITCH, ROUTE, TSHOOT, and ICMI. Ray has developed courses for Global Knowledge, Cisco, and General Electric.