



Access Control List Overview and Guidelines

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as access lists). You can configure access control lists (ACLs) for all routed network protocols (IP, AppleTalk, and so on) to filter protocol packets when these packets pass through a device. You can configure access lists on your device to control access to a network; access lists can prevent certain traffic from entering or exiting a network. This module provides an overview of access lists.

- [Information About Access Control Lists, page 1](#)
- [Access Control List Configuration, page 2](#)
- [Feature Information For Access Control Lists Overview and Guidelines, page 6](#)

Information About Access Control Lists

Overview of an Access Control List

Access lists filter network traffic by controlling the forwarding or blocking of routed packets at the interface of a device. A device examines each packet to determine whether to forward or drop that packet, based on the criteria specified in access lists.

The criteria that can be specified in an access list include the source address of the traffic, the destination address of the traffic, and the upper-layer protocol.



Note

Some users might successfully evade basic access lists because these lists require no authentication.

Functions of an Access Control List

There are many reasons to configure access lists; for example, to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide security for your network, which is the focus of this module.

Use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your device, all packets passing through the device are allowed access to all parts of your network.

Access lists can allow a host to access a part of your network and prevent another host from accessing the same area. In the figure below, Host A is allowed to access the Human Resources network, but Host B is prevented from accessing the Human Resources network.

You can also use access lists to define the type of traffic that is forwarded or blocked at device interfaces. For example, you can permit e-mail traffic to be routed but at the same time block all Telnet traffic.

Scenarios for Configuring an Access Control List

Access lists should be configured on “firewall” devices, which are often positioned between your internal network and an external network such as the Internet. You can also use access lists on a device positioned between two parts of your network to control traffic entering or exiting a specific part of your internal network.

To use the security benefits of access lists, you should, at the minimum, configure access lists on edge devices. Configuring access lists on edge devices provides a basic buffer from the outside network or from a less controlled area of your own network into a more sensitive area of your network.

On border devices, you should configure access lists for each network protocol that is configured on device interfaces. You can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

Access lists must be defined on a per-protocol basis. In other words, you should define access lists for every protocol enabled on an interface if you want to control traffic flow for those protocols.

**Note**

Some protocols refer to access lists as filters.

Differences Between Basic and Advanced Access Control Lists

This module describes how to use standard and static extended access lists, which are types of basic access lists. A basic access list should be used with each routed protocol that is configured on device interfaces.

Besides basic access lists described in this module, there are also advanced access lists available, which provide additional security features and provide greater control over packet transmission.

Access Control List Configuration

Each protocol has its own set of specific tasks and rules to provide traffic filtering. In general, most protocols require at least two basic steps to be completed. The first step is to create an access list, and the second step is to apply the access list to an interface.

**Note**

Some protocols refer to access lists as filters and to the act of applying the access lists to interfaces as filtering.

Create an Access Control List

Create access lists for each protocol that you wish to filter, per device interface. For some protocols, you can create one access list to filter inbound traffic and another access list to filter outbound traffic.

To create an access list, specify the protocol to be filtered, assign a unique name or number to the access list, and define packet filtering criteria. A single access list can have multiple filtering statements.

We recommend that you create access lists on a TFTP server and then download these access lists to the required device to simplify the maintenance of access lists. For details, see the “Create or Edit Access List Statements on a TFTP Server” section.

Assign a Unique Name or Number to Each Access Control List

When configuring access lists on a device, you must identify each access list uniquely within a protocol by assigning either a name or a number to that protocol’s access list. Access lists of some protocols must be identified by a name, and access lists of other protocols must be identified by a number. Some protocols can be identified by either a name or a number. When a number is used to identify an access list, the number must be within the specific range of numbers that is valid for the protocol.

You can specify access lists by names for the following protocols:

- Apollo Domain
- Internetwork Packet Exchange (IPX)
- IP
- ISO Connectionless Network Service (CLNS)
- NetBIOS IPX
- Source-route bridging NetBIOS

You can specify access lists by numbers for the protocols listed in the table below.

Table 1: Protocols with Access Lists Specified by Numbers

Protocol	Range
AppleTalk	300–399
DECnet and extended DECnet	600–699
Ethernet address	700–799
Ethernet type code	200–299
Extended IP	100–199, 2000–2699
Extended IPX	900–999
Extended transparent bridging	1100–1199

Protocol	Range
Extended Virtual Integrated Network Service (VINES)	101–200
Extended Xerox Network Systems (XNS)	500–599
IP	1–99, 1300–1999
IPX	800–899
IPX Service Advertising Protocol (SAP)	1000–1099
Simple VINES	201–300
Source-route bridging (protocol type)	200–299
Source-route bridging (vendor code)	700–799
Standard VINES	1–100
Transparent bridging (protocol type)	200–299
Transparent bridging (vendor code)	700–799
XNS	400–499

Define Criteria for Forwarding or Blocking Packets

When creating an access list, define criteria that are applied to each packet that is processed by the device so that the device can forward or block each packet based on whether or not the packet matches the criteria.

Typical criteria that you define in access lists include packet source addresses, packet destination addresses, and upper-layer protocol of the packet. However, each protocol has its own specific set of criteria that can be defined.

In a single access list, you can define multiple criteria in separate access list statements. Each of these statements must reference the same identifying name or number to bind statements to the same access list. You can have as many criteria statements as you want, limited only by the available memory of the device. The more statements there are in an access list, the more difficult it will be to comprehend and manage an access list.

Deny All Traffic Criteria Statement

At the end of every access list is an implied “deny all traffic” criteria statement. This statement implies that if a packet does not match any criteria statement, the packet will be blocked.

**Note**

For most protocols, if you define an inbound access list for traffic filtering, you should include explicit access list criteria statements to permit routing updates. If you do not, you might effectively lose communication from the interface when routing updates are blocked by the “deny all traffic” statement at the end of the access list.

Order of Criteria Statements

Each criteria statement that you enter is appended to the end of the access list statements. You cannot delete individual statements after they are created. You can delete only an entire access list.

The order of access list statements in an access list is important. When a device is deciding whether to forward or block a packet, Cisco software tests the packet against each criteria statement in the order in which the statements were created. After a match is found, no more criteria statements are checked.

If you create a criteria statement that explicitly permits all traffic, statements added later will not be checked. If you need additional statements, you must delete the access list and configure a new access list.

Create or Edit Access Control List Statements on a TFTP Server

Because the order of access list criteria statements is important and you cannot reorder or delete criteria statements on your device, we recommend that you create all access list statements on a TFTP server and that you download the entire access list to your device.

Create access list statements using any text editor, and save access list statements in ASCII format to a TFTP server that is accessible from your device. Then, on your device, use the **copy tftp: file-id system:running-config** command to copy the access list from the TFTP server to your device. Finally, use the **copy system:running-config nvram:startup-config** command to save the access list to your device’s NVRAM.

If you want to make changes to an access list, you can make them to the text file on the TFTP server and copy the edited file to your device.

**Note**

The first command of an edited access list file should delete the previous access list (for example, use the **no access-list** command at the beginning of the file). If you do not delete the previous version of the access list, when you copy the edited file to your device you will merely be appending additional criteria statements to the end of the existing access list.

Apply an Access Control List to an Interface

With some protocols, you can apply up to two access lists to an interface: one inbound access list and one outbound access list. With other protocols, you apply only one access list that checks both inbound and outbound packets.

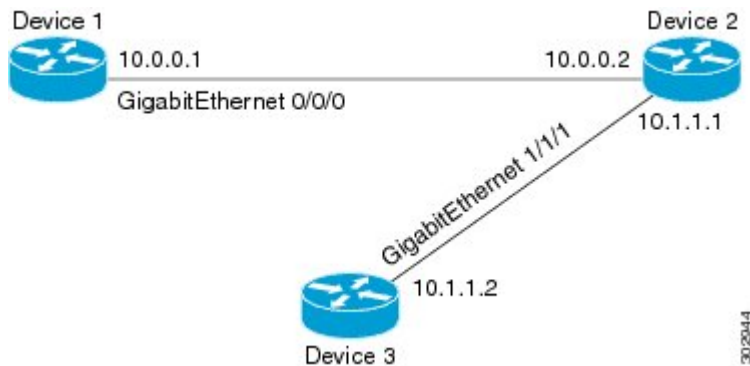
If the access list is inbound, when a device receives a packet, Cisco software checks the access list’s criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.

If the access list is outbound, after receiving and routing a packet to the outbound interface, Cisco software checks the access list's criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.

**Note**

Access lists that are applied to interfaces on a device do not filter traffic that originates from that device.

Figure 2: Topology for Applying Access Control Lists



The figure above shows that Device 2 is a bypass device that is connected to Device 1 and Device 3. An outbound access list is applied to Gigabit Ethernet interface 0/0/0 on Device 1. When you ping Device 3 from Device 1, the access list does not check for packets going outbound because the traffic is locally generated.

The access list check is bypassed for locally generated packets, which are always outbound.

By default, an access list that is applied to an outbound interface for matching locally generated traffic will bypass the outbound access list check; but transit traffic is subjected to the outbound access list check.

**Note**

The behavior described above applies to all single-CPU platforms that run Cisco software.

Feature Information For Access Control Lists Overview and Guidelines

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.