This page was exported from - Free Cisco Training & Resources - Certification Exam Preparation
Export date: Wed Mar 11 1:23:31 2026 / +0000 GMT

IP Access Control List (ACL)

Standard IP Access Control Lists

Filtering logic could be configured on any router and on any of its interfaces. Cisco IOS software applies the filtering logic of an ACL either as a packet enters an interface or as it exits the interface. In other words, IOS associates an ACL with an interface, and specifically for traffic either entering or exiting the interface. After you have chosen the router on which you want to place the access list, you must choose the interface on which to apply the access logic, as well as whether to apply the logic for inbound or outbound packets. The key features of Cisco ACLs are: . Packets can be filtered as they enter an interface, before the routing decision. . Packets can be filtered before they exit an interface, after the routing decision. . Deny is the term used in Cisco IOS software to imply that the packet will be filtered. . Permit is the term used in Cisco IOS software to imply that the packet will not be filtered. . The filtering logic is configured in the access list. . If a packet does not match any of your access list statements, it is blocked. Access lists have two major steps in their logic: matching, which determines whether it matches the access-list statement; and action, which can be either deny or permit. Deny means to discard the packet, and permit implies that the packet should be allowed. However, the logic that IOS uses with a multiple-entry ACL can be much more complex. Generally, the logic can be summarized as follows: Step 1: The matching parameters of the access-list statement are compared to the packet. Step 2: If a match is made, the action defined in this access-list statement (permit or deny) is performed. Step 3: If a match is not made in Step 2, repeat Steps 1 and 2 using each successive statement in the ACL until a match is made. Step 4: If no match is made with an entry in the access list, the deny action is performed.

Wildcard Masks

IOS IP ACLs match packets by looking at the IP, TCP, and UDP headers in the packet. Standard IP access lists can also examine only the source IP address. You can configure the router to match the entire IP address or just a part of the IP address. When defining the ACL statements you can define a wildcard mask along with the IP address. The wildcard mask tells the router which part of the IP address in the configuration statement must be compared with the packet header. The wildcard masks look similar to subnet masks, in that they represent a 32-bit number. However, the wildcard mask's 0 bits tell the router that those corresponding bits in the address must be compared when performing the matching logic. The binary 1s in the wildcard mask tell the router that those bits do not need to be compared. Thus, wildcard mask 0.0.0.0, which in binary form is 00000000.00000000.00000000.00000000, indicates that the entire IP address must be matched, while wildcard mask 0.0.0.255, which in binary form is 00000000.00000000.00000000.11111111, indicates that the first 24 bits of the IP address must be matched, and wildcard mask 0.0.31.255, which in binary form is 00000000.00000000.00011111.11111111, indicates that the first 24 bits of the IP address must be matched.

Standard IP Access List Configuration

A standard access list is used to match a packet and then take the directed action. Each standard ACL can match all, or only part, of the packet's source IP address. The only two actions taken when an access-list statement is matched are to either deny or permit the packet. The configuration commands required are: . ip access-group {number | action [in | out]}, in which action can be either permit of deny and is used to enable access lists; and . access-class number | action [in | out], which can be used to enable either standard or extended access lists. The standard access list configuration can be verified using the following show commands: . show ip interface[type number], which includes a reference to the access lists enabled on the interface; . show access-lists [access-list-number | access-list-name], which shows details of configured access lists for all protocols; and . show ip access-list [access-list-number | access-list-name], which shows the access lists.

Extended IP Access Control Lists

Extended IP access lists are similar to standard IP ACLs in that you enable extended access lists on interfaces for packets either entering or exiting the interface. IOS then searches the list sequentially. The first statement matched stops the search through the list and defines the action to be taken. The key difference between the extended ACLs and standard ACLs is the variety of fields in the packet that can be compared for matching by extended access lists. A single extended ACL statement can examine multiple parts of the packet headers, requiring that all the parameters be matched correctly in order to match that one ACL statement. That matching logic is what makes extended access lists both much more useful and much more complex than standard IP ACLs. You can configure extended ACL to match the IP protocol type, which identifies what header follows the IP header. You can specify all IP packets, or those with TCP headers, UDP headers, ICMP, etc, by checking the Protocol field. You can also check the source and destination IP addresses, as well as the TCP source and destination port numbers. An extended access list is more complex than standard access lists. Therefore the configuration commands are more complex. The configuration command for extended access lists is: . access-list access-list-number action protocol source source-wildcard destination destination-wildcard [log | log-input], which can be used to enable access lists;

Named IP Access Lists

Named ACLs can be used to match the same packets, with the same parameters, you can match with standard and extended IP ACLs. Named IP ACLs do have some differences, however. The most obvious difference is that IOS identifies named ACLs using names you assign them as opposed to numbers. Named ACLs also have another key feature that numbered ACLs do not: You can delete individual lines in a named IP access list. In addition, two

important configuration differences exist between numbered and named access lists. One key difference is that named access lists use a global command that places the user in a named IP access list submode, under which the matching and permit or deny logic is configured. The other key difference is that when a named matching statement is deleted, only that one statement is deleted. With numbered lists, the deletion of any statement in the list deletes all the statements in the list. Controlling Telnet Access with ACLs Access into and out of the virtual terminal line (vty) ports of the Cisco IOS software can also be controlled by IP access lists. IOS uses vtys to represent a user who has Telnetted to a router, as well as for Telnet sessions a user of a router has created to other devices. You can use ACLs to limit the IP hosts that can Telnet into the router, and you can also limit the hosts to which a user of the router can Telnet.