Purpose of ACLs

4.1.1

What is an ACL?

Routers make routing decisions based on information in the packet header. Traffic entering a router interface is routed solely based on information within the routing table. The router compares the destination IP address with routes in the routing table to find the best match and then forwards the packet based on the best match route. That same process can be used to filter traffic using an access control list (ACL).

An ACL is a series of IOS commands that are used to filter packets based on information found in the packet header. By default, a router does not have any ACLs configured. However, when an ACL is applied to an interface, the router performs the additional task of evaluating all network packets as they pass through the interface to determine if the packet can be forwarded.

An ACL uses a sequential list of permit or deny statements, known as access control entries (ACEs).

Note: ACEs are also commonly called ACL statements.

When network traffic passes through an interface configured with an ACL, the router compares the information within the packet against each ACE, in sequential order, to determine if the packet matches one of the ACEs. This process is called packet filtering.

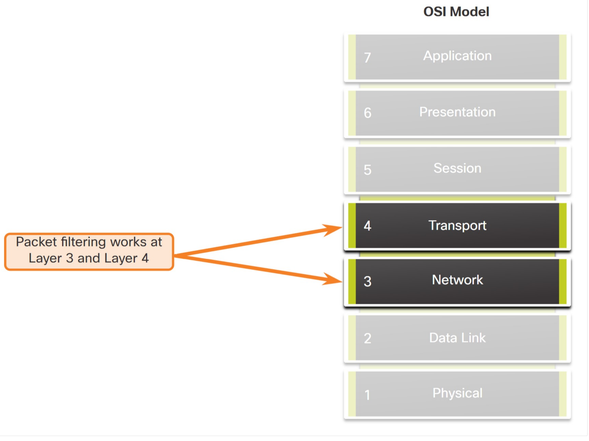
Several tasks performed by routers require the use of ACLs to identify traffic. The table lists some of these tasks with examples.

Task	Example
Limit network traffic to increase network performance	• A corporate policy prohibits video traffic on the network to reduce the network load. • A policy can be enforced using ACLs to block video traffic.
Provide traffic flow control	• A corporate policy requires that routing protocol traffic be limited to certain links only. • A policy can be implemented using ACLs to restrict the delivery of routing updates to only those that come from a known source.
Provide a basic level of security for network access	• Corporate policy demands that access to the Human Resources network be restricted to authorized users only. • A policy can be enforced using ACLs to limit access to specified networks.
Filter traffic based on traffic type	• Corporate policy requires that email traffic be permitted into a network, but that Telnet access be denied. • A policy can be implemented using ACLs to filter traffic by type.
Screen hosts to permit or deny access to network services	• Corporate policy requires that access to some file types (e.g., FTP or HTTP) be limited to user groups. • A policy can be implemented using ACLs to filter user access to services.
Provide priority to certain classes of network traffic	• Corporate traffic specifies that voice traffic be forwarded as fast as possible to avoid any interruption. • A policy can be implemented using ACLs and QoS services to identify voice traffic and process it immediately.

4.1.2

Packet Filtering

Packet filtering controls access to a network by analyzing the incoming and/or outgoing packets and forwarding them or discarding them based on given criteria. Packet filtering can occur at Layer 3 or Layer 4, as shown in the figure.



Cisco routers support two types of ACLs:

- **Standard ACLs** - ACLs only filter at Layer 3 using the source IPv4 address only.
- **Extended ACLs** - ACLs filter at Layer 3 using the source and / or destination IPv4 address. They can also filter at Layer 4 using TCP, UDP ports, and optional protocol type information for finer control.

4.1.3

ACL Operation

ACLs define the set of rules that give added control for packets that enter inbound interfaces, packets that relay through the router, and packets that exit outbound interfaces of the router.

ACLs can be configured to apply to inbound traffic and outbound traffic, as shown in the figure.

Note: ACLs do not act on packets that originate from the router itself.

An inbound ACL filters packets before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the ACL, it is then processed for routing. Inbound ACLs are best used to filter packets when the network attached to an inbound interface is the only source of packets that need to be examined.

An outbound ACL filters packets after being routed, regardless of the inbound interface. Incoming packets are routed to the outbound interface and then they are processed through the outbound ACL. Outbound ACLs are best used when the same filter will be applied to packets coming from multiple inbound interfaces before exiting the same outbound interface.

When an ACL is applied to an interface, it follows a specific operating procedure. For example, here are the operational steps used when traffic has entered a router interface with an inbound standard IPv4 ACL configured.

1. The router extracts the source IPv4 address from the packet header.
2. The router starts at the top of the ACL and compares the source IPv4 address to each ACE in a sequential order.
3. When a match is made, the router carries out the instruction, either permitting or denying the packet, and the remaining ACEs in the ACL, if any, are not analyzed.
4. If the source IPv4 address does not match any ACEs in the ACL, the packet is discarded because there is an implicit deny ACE automatically applied to all ACLs.

The last ACE statement of an ACL is always an implicit deny that blocks all traffic. By default, this statement is automatically implied at the end of an ACL even though it is hidden and not displayed in the configuration.

Note: An ACL must have at least one permit statement otherwise all traffic will be denied due to the implicit deny ACE statement.

4.1.4

Packet Tracer - ACL Demonstration

In this activity, you will observe how an access control list (ACL) can be used to prevent a ping from reaching hosts on remote networks. After removing the ACL from the configuration, the pings will be successful.

ACL Demonstration

ACL Demonstration

4.1.5

Check Your Understanding - Purpose of ACLs

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

1. What are the permit or deny statements in an ACL called?

- (•) access control entries
- ( ) arbitrary statements
- ( ) content control entries
- ( ) control statements

2. Which packet filtering statement is true?

- ( ) Extended ACLs filter at Layer 3 only.
- ( ) Extended ACLs filter at Layer 4 only.
- (•) Standard ACLs filter at Layer 3 only.
- ( ) Standard ACLs filter at Layer 4 only.

3. Which statement about the operation of a standard ACL is incorrect?

- ( ) The router extracts the source IPv4 address from the packet header.
- ( ) The router starts at the top of the ACL and compares the address to each ACE in sequential order.
- ( ) When a match is made, the ACE either permits or denies the packet, and any remaining ACEs are not analyzed.
- (•) If there are no matching ACEs in the ACL, the packet is forwarded because there is an implicit permit ACE automatically applied to all ACLs.

Check

Show Me

Reset