|  |
| --- |
| **Access control list** |

ACLs are basically a set of commands, grouped together by a number or name that is used to filter traffic entering or leaving an interface.

When activating an ACL on an interface, you must specify in which direction the traffic should be filtered:

* **Inbound (as the traffic comes into an interface)**
* **Outbound (before the traffic exits an interface)**

**Inbound ACLs:** Incoming packets are processed before they are routed to an outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet will be discarded after it is denied by the filtering tests. If the packet is permitted by the tests, it is processed for routing.

**Outbound ACLs:** Incoming packets are routed to the outbound interface and then processed through the outbound ACL.

**Universal fact about Access control list**

1. ACLs come in two varieties : **Numbered and named**
2. Each of these references to ACLs supports two types of filtering: **standard and extended.**
3. Standard IP ACLs can filter only on the **source IP address** inside a packet.
4. Whereas an extended IP ACLs can filter on the **source and destination IP addresses** in the packet.
5. There are two actions an ACL can take: **permit or deny.**
6. Statements are processed top-down.
7. Once a match is found, no further statements are processed—therefore, order is important.
8. If no match is found, the imaginary **implicit deny statement at the end of the ACL** drops the packet.
9. An ACL should have at least one permit statement; otherwise, all traffic will be dropped because of the hidden implicit deny statement at the end of every ACL.

No matter what type of ACL you use, though, you can have only one ACL per protocol, per interface, per direction. For example, you can have one IP ACL inbound on an interface and another IP ACL outbound on an interface, but you cannot have two inbound IP ACLs on the same interface.

**Access List Ranges**

|  |  |
| --- | --- |
| **Type** | **Range** |
| IP Standard | 1–99 |
| IP Extended | 100–199 |
| IP Standard Expanded Range | 1300–1999 |
| IP Extended Expanded Range | 2000–2699 |

**Standard ACLs**

A standard IP ACL is simple; it filters based on source address only. You can filter a source network or a source host, but you cannot filter based on the destination of a packet, the particular protocol being used such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), or on the port number. You can permit or deny only source traffic.

**Extended ACLs:**

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

**Named ACLs**

One of the disadvantages of using IP standard and IP extended ACLs is that you reference them by number, which is not too descriptive of its use. With a named ACL, this is not the case because you can name your ACL with a descriptive name. The ACL named Deny Mike is a lot more meaningful than an ACL simply numbered 1. There are both IP standard and IP extended named ACLs.

Another advantage to named ACLs is that they allow you to remove individual lines out of an ACL. With numbered ACLs, you cannot delete individual statements. Instead, you will need to delete your existing access list and re-create the entire list.

**Configuration Guidelines**

* Order of statements is important: put the most restrictive statements at the top of the list and the least restrictive at the bottom.
* ACL statements are **processed top-down until a match is found,** and then no more statements in the list are processed.
* If no match is found in the ACL, the packet is dropped (implicit deny).
* Each ACL needs either a unique number or a unique name.
* The router cannot filter traffic that it, itself, originates.
* You can have only one IP ACL applied to an interface in each direction (inbound and outbound)—you can't have two or more inbound or outbound ACLs applied to the same interface. (Actually, you can have one ACL for each protocol, like IP and IPX, applied to an interface in each direction.)
* Applying an empty ACL to an interface permits all traffic by default: in order for an ACL to have an implicit deny statement, you need at least one actual permit or deny statement.
* Remember the numbers you can use for IP ACLs.Standard ACLs can use numbers ranging **1–99 and 1300–1999,** and extended ACLs can use **100–199 and 2000–2699.**
* Wildcard mask is not a subnet mask. Like an IP address or a subnet mask, a wildcard mask is composed of 32 bits when doing the conversion; subtract each byte in the subnet mask from 255.

**There are two special types of wildcard masks:**

0.0.0.0   and   255.255.255.255

A 0.0.0.0 wildcard mask is called a host mask

255.255.255.255. If you enter this, the router will cover the address and mask to the keyword any.

**Placement of ACLs**

Standard ACLs should be placed as close to the destination devices as possible.

Extended ACLs should be placed as close to the source devices as possible.