**Access Control Lists**

Table of Contents

[Configuration 3](#_Toc87294003)

[Verification 4](#_Toc87294004)

**Access Control Lists** (ACL) define who can access what. For example, we could specify that only a specific host should be able to access out webserver, or that hosts from one specific network should be unable to communicate with hosts from a different network.

We will be learning about **Cisco IP ACL**, which filters network traffic based on IP addresses. There are several types of ACL for Cisco devices, and we will be concentrating on **Numbered Standard IPv4 ACL**.

## Configuration

The first step is to specify what the **rule** is.

Format:

Router(config)# access-list access-list-number {permit|deny} {source\_address source\_wildcard|any}

CLI

Example:

Router(config)# access-list 1 deny 192.168.10.0 0.0.0.255

CLI

We can either **permit** or **deny** a packet based on the source IP of the packet. Just like in OSPF, we also need to use a **wildcard mask** here.

One important thing to remember is that as soon as we apply an ACL to an interface, all traffic that does not match any ACL rule will be **discarded by default**. Thus, if we define an ACL to deny a certain IP address, other packets will end up getting denied as well because there are not rules on how to deal with those packets. Because of this, we must specify another ACL which permits or denies packets that do not match any of the previous rules (since the rules are matched from top to bottom).

Router(config)# access-list 1 permit any

CLI

Also note that the **access list numbers** must be in the range **1 to 99**. Other numbers are used for **extended numbered ACL**.

Once our ACL rules are defined, we also need to **apply** the ACL to an interface.

Format:

Router(config-if)# ip access-group access-list-number {in|out}

CLI

Example:

Router(config-if)# ip access-group 1 out

CLI

As can be seen, the rules can be applied for either **inbound** or **outbound** traffic.

## Verification

It is best practice to **verify** ACL rules before applying them.

Router# show access-lists

CLI