Wildcard Masks in ACLs

4.2.1

Wildcard Mask Overview

In the previous topic, you learned about the purpose of ACL. This topic explains how ACL uses wildcard masks. An IPv4 ACE uses a 32-bit wildcard mask to determine which bits of the address to examine for a match. Wildcard masks are also used by the Open Shortest Path First (OSPF) routing protocol.

A wildcard mask is similar to a subnet mask in that it uses the ANDing process to identify which bits in an IPv4 address to match. However, they differ in the way they match binary 1s and 0s. Unlike a subnet mask, in which binary 1 is equal to a match and binary 0 is not a match, in a wildcard mask, the reverse is true.

Wildcard masks use the following rules to match binary 1s and 0s:

- **Wildcard mask bit 0** - Match the corresponding bit value in the address
- **Wildcard mask bit 1** - Ignore the corresponding bit value in the address

The table lists some examples of wildcard masks and what they would identify.

Wildcard Mask	Last Octet (in Binary)	Meaning (0 - match, 1 - ignore)
`0.0.0.0`	`00000000`	Match all octets.
`0.0.0.63`	`00111111`	• Match the first three octets • Match the two left most bits of the last octet • Ignore the last 6 bits
`0.0.0.15`	`00001111`	• Match the first three octets • Match the four left most bits of the last octet • Ignore the last 4 bits of the last octet
`0.0.0.252`	`11111100`	• Match the first three octets • Ignore the six left most bits of the last octet • Match the last two bits
`0.0.0.255`	`11111111`	• Match the first three octet • Ignore the last octet

4.2.2

Wildcard Mask Types

Using wildcard masks will take some practice. Refer to the examples to learn how the wildcard mask is used to filter traffic for one host, one subnet, and a range IPv4 addresses.

Click each button to see how the wildcard mask is used in ACLs.

Wildcard to Match a Host | Wildcard Mask to Match an IPv4 Subnet | Wildcard Mask to Match an IPv4 Address Range

Wildcard to Match a Host

In this example, the wildcard mask is used to match a specific host IPv4 address. Assume ACL 10 needs an ACE that only permits the host with IPv4 address 192.168.1.1. Recall that “0” equals a match and “1” equals ignore. To match a specific host IPv4 address, a wildcard mask consisting of all zeroes (i.e., 0.0.0.0) is required.

The table lists in binary, the host IPv4 address, the wildcard mask, and the permitted IPv4 address.

The 0.0.0.0 wildcard mask stipulates that every bit must match exactly. Therefore, when the ACE is processed, the wildcard mask will permit only the 192.168.1.1 address. The resulting ACE in ACL 10 would be **access-list 10 permit 192.168.1.1 0.0.0.0.**

	Decimal	Binary
IPv4 address	192.168.1.1	`11000000.10101000.00000001.00000001`
Wildcard Mask	0.0.0.0	`00000000.00000000.00000000.00000000`
Permitted IPv4 Address	**192.168.1.1**	`11000000.10101000.00000001.00000001`

4.2.3

Wildcard Mask Calculation

Calculating wildcard masks can be challenging. One shortcut method is to subtract the subnet mask from 255.255.255.255. Refer to the examples to learn how to calculate the wildcard mask using the subnet mask.

Click each button to see how to calculate each wildcard mask.

Example 1 | Example 2 | Example 3 | Example 4

Example 1

Assume you wanted an ACE in ACL 10 to permit access to all users in the 192.168.3.0/24 network. To calculate the wildcard mask, subtract the subnet mask (i.e., 255.255.255.0) from 255.255.255.255, as shown in the table.

The solution produces the wildcard mask 0.0.0.255. Therefore, the ACE would be **access-list 10 permit 192.168.3.0 0.0.0.255.**

Starting value	255.255.255.255
Subtract the subnet mask	- 255.255.255. 0
Resulting wildcard mask	0. 0. 0.255

4.2.4

Wildcard Mask Keywords

Working with decimal representations of binary wildcard mask bits can be tedious. To simplify this task, the Cisco IOS provides two keywords to identify the most common uses of wildcard masking. Keywords reduce ACL keystrokes and make it easier to read the ACE.

The two keywords are:

- **host** - This keyword substitutes for the 0.0.0.0 mask. This mask states that all IPv4 address bits must match to filter just one host address.
- **any** - This keyword substitutes for the 255.255.255.255 mask. This mask says to ignore the entire IPv4 address or to accept any addresses.

For example, in the command output, two ACLs are configured. The ACL 10 ACE permits only the 192.168.10.10 host and the ACL 11 ACE permits all hosts.

```
R1(config)# access-list 10 permit 192.168.10.10  0.0.0.0
R1(config)# access-list 11 permit  0.0.0.0 255.255.255.255
R1(config)#
```

Alternatively, the keywords **host** and **any** could have been used to replace the highlighted output.

The following commands accomplishes the same task as the previous commands.

```
R1(config)# access-list 10 permit  host  192.168.10.10
R1(config)# access-list 11 permit  any
R1(config)#
```

4.2.5

Check Your Understanding - Wildcard Masks in ACLs

Check your understanding wildcard masks in ACLs by choosing the BEST answer to the following questions.

1. Which wildcard mask would permit only host 10.10.10.1?
   - (•) 0.0.0.0
   - ( ) 0.0.0.31
   - ( ) 0.0.0.255
   - ( ) 0.0.255.255
   - ( ) 255.255.255.255
2. Which wildcard mask would permit only hosts from the 10.10.0.0/16 network?
   - ( ) 0.0.0.0
   - ( ) 0.0.0.31
   - ( ) 0.0.0.255
   - (•) 0.0.255.255
   - ( ) 255.255.255.255
3. Which wildcard mask would permit all hosts?
   - ( ) 0.0.0.0
   - ( ) 0.0.0.31
   - ( ) 0.0.0.255
   - ( ) 0.0.255.255
   - (•) 255.255.255.255
4. Which wildcard mask would permit all hosts from the 192.168.10.0/24 network?
   - ( ) 0.0.0.0
   - ( ) 0.0.0.31
   - (•) 0.0.0.255
   - ( ) 0.0.255.255
   - ( ) 255.255.255.255

Check | Show Me | Reset