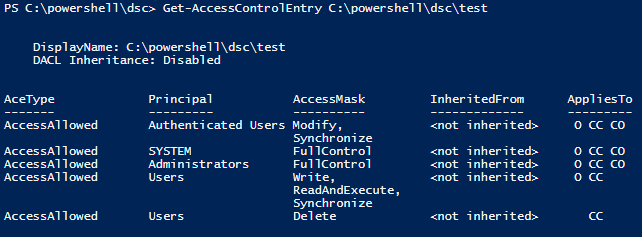
**Access Control Entry**



Class: Cyber Security

Prepared by: Rickardo Brown, St Patrick Currey

Date: 18/08/2023

In this example, we are configuring an Access Control List (ACL) on a network device to permit network access for a specific group of users. The goal is to allow access for 14 users in the subnet 192.168.3.32/28.

To achieve this, you need to create an Access Control Entry (ACE) in the ACL with the appropriate settings. In this case, the ACE will be permitting traffic for the IP addresses within the range of 192.168.3.32 to 192.168.3.47 (since the subnet 192.168.3.32/28 has a prefix length of 28, meaning it covers the range from 192.168.3.32 to 192.168.3.47).

Now, an important aspect of an ACE is the wildcard mask, which is used to specify which bits in the IP address should be matched. A wildcard mask of 0 means "match exactly," while a wildcard mask of 255 means "ignore" (i.e., match any value).

To calculate the wildcard mask, you start with the subnet mask, which is 255.255.255.240 in this case (since it's a /28 subnet, the first 28 bits are set to 1, and the remaining 4 bits are set to 0).

To obtain the wildcard mask, you subtract the subnet mask from the all-ones IP address (255.255.255.255). The bitwise subtraction is performed as follows:

255.255.255.255

- 255.255.255.240

-----------------

0. 0. 0. 15

So, the resulting wildcard mask is 0.0.0.15.

Now that you have the wildcard mask, you can create the ACE in the ACL. The ACE will be written as follows:

access-list 10 permit 192.168.3.32 0.0.0.15

This ACE will permit network access for the 14 users in the subnet 192.168.3.32/28, as desired.

* What is an ACL? An Access Control List (ACL) is like a set of rules or instructions for a network device (like a router or firewall) to decide what traffic is allowed or blocked from entering or leaving a network.
* What is an ACE? An Access Control Entry (ACE) is a single rule within an ACL. Each rule specifies conditions for matching packets and what action should be taken if a packet matches those conditions.
* The Goal of the Example: In this example, the goal is to allow network access for 14 specific users who are part of a subnet with IP addresses in the range 192.168.3.32 to 192.168.3.47. This subnet is represented as 192.168.3.32/28.
* Understanding the Subnet Mask: The subnet mask (255.255.255.240) tells us which part of the IP address identifies the network and which part identifies individual devices (hosts) within that network.
* In binary, the subnet mask 255.255.255.240 looks like this: 11111111.11111111.11111111.11110000.
* The 1s represent the network part, and the 0s represent the host part.
* Calculating the Wildcard Mask: The wildcard mask is the opposite of the subnet mask. It helps determine which parts of the IP address will be matched when evaluating the ACE.
* To find the wildcard mask, subtract each bit of the subnet mask from 1. So, 0 in the subnet mask becomes 1, and 1 in the subnet mask becomes 0.
* The resulting wildcard mask is 00000000.00000000.00000000.00001111, which is equivalent to 0.0.0.15 in decimal form.
* Writing the ACE for the ACL: Now that we have the wildcard mask, we can write the ACE in the ACL. The ACE will look like this:

access-list 10 permit 192.168.3.32 0.0.0.15

* access-list 10: This means we are working with ACL 10.
* permit: This means the rule allows traffic that matches the conditions.
* 192.168.3.32: This is the starting IP address of the subnet we want to permit.
* 0.0.0.15: This is the wildcard mask that specifies the range of IP addresses to permit. In this case, it allows IP addresses from 192.168.3.32 to 192.168.3.47.
* Conclusion: The ACE access-list 10 permit 192.168.3.32 0.0.0.15 is added to ACL 10, allowing network access for the 14 users within the subnet 192.168.3.32/28.