Frame Flooding

Frame flooding occurs when a frame enters a switch that doesn't have the destination MAC address within the MAC table. If this is the case, the switch does not know where to send the frame, so it sends it out all ports except the port from which the frame entered the switch. This is frame flooding. If the device with the destination MAC address in question is connected to one of the switch's ports, it will answer, and its MAC address will be added to the MAC table.

Learning Outcomes

After completing this exercise, you will be able to:

- Explain frame flooding, how it works and the vulnerabilities

Your Devices

You will be using the following devices in this lab.

- **NYEDGE1** (Cisco 2911 Router)
- **NYWAN1** (Cisco 2911 Router)
- **NYCORE1** (Cisco 3750v2-24PS Switch)
- **NYACCESS1** (Cisco 2960-24 Switch)
- **PLABCSCO01** (Cisco Tools Server)

NYEDGE1
Cisco 2911 Router
NYWAN1
Cisco 2911 Router
NYCORE1
Cisco 3750v2-24PS Switch
NYACCESS1
Cisco 2960-24 Switch
PLABCSCO01
Cisco Tools Server

Task 1 - Frame Flooding

In this task, you will see how frame flooding functions and also how it can contribute to a security vulnerability.

Step 1

Connect to the **NYCORE1** switch and view the dynamically added MAC addresses in the MAC table once again:

> ***Note:*** *Remember, your output will differ slightly.*

```
NYCORE1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0015.6227.8b8a    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0418    DYNAMIC     Fa1/0/22
   1    7426.ac67.0c70    DYNAMIC     Fa1/0/1
Total Mac Addresses for this criterion: 3
NYCORE1#
```

Imagine that the **PLABCSCO01** device chooses to send a frame to a device with a MAC address of **0745.abab.475c**. This MAC address is not in the MAC address table, so the switch will flood this frame out of all its ports except port **FastEthernet 1/0/22**.

Step 2

Every time a new MAC address is learned, it is added to the MAC table. The MAC table resides in the memory of the switch which is finite, so there is a limited number of entries it can hold. If the aging time is too large and the number of MAC addresses is also large, this memory may become exhausted.

To determine the maximum size of the MAC address table, issue the following command:

```
NYCORE1#show mac address-table count
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 3
Static  Address Count  : 1
```

```
Total Mac Addresses    : 4
Total Mac Address Space Available: 5995
NYCORE1#
```

In this particular instance, four MAC address entries exist, and there are **5995** spaces available, so the total number of entries available in the MAC address table is **5999**.

Step 3

MAC flooding is a security risk because this functionality can be used to cause the network to malfunction. Imagine that the user of the **PLABSCSO01** server is a hacker. He can initiate what is called a **MAC Flooding Attack**. Essentially, **PLABSCSO01** would send a multitude of frames each with a different source MAC address. The switch would then learn all of these fake MAC addresses and associate them with the port on which they are coming in.

Note: *You may wonder how a computer could send frames with many different source MAC addresses since a MAC address is "burned in" to the NIC of the computer and cannot be changed. It is true that the MAC assigned to a NIC cannot be changed, however, when sending frames, the MAC address is read into RAM and then placed in the* ***Source MAC Address*** *field of the header of the frame. Once the MAC address resides in the RAM, with the appropriate software, it can be manipulated and changed before it is placed in the header of the frame.*

The result would be a very large MAC Address Table similar to the following:

```
NYCORE1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0015.6227.8b8a    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0418    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0419    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0420    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0421    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0422    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0423    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0424    DYNAMIC     Fa1/0/22
   1    04da.d2b6.0425    DYNAMIC     Fa1/0/22
!<-- Output Omitted -->
   1    04da.d2b6.BA4C    DYNAMIC     Fa1/0/22
   1    04da.d2b6.BA4D    DYNAMIC     Fa1/0/22
Total Mac Addresses for this criterion: 5999
NYCORE1#
```

Alert: You will not be able to reproduce this output on your switch.

Notice the **Total Mac Addresses for this criterion** value is at its maximum.

At this point, any new and legitimate traffic will not be able to have its MAC address stored, and therefore the switch will always flood any frames that it receives out of all the interfaces. In essence, the **MAC Flooding Attack** has reduced the switch's functionality to that of a hub.

Note: *There are several ways that you can protect your switch from a MAC Flooding Attack. Most of these are found within the framework of* ***port security*** *which you will learn to implement in another lab of this series. Use your favorite search engine to research this topic further.*

Leave the devices in their current states and continue on to the next exercise.