Native VLAN Configuration

Frames that are placed on a trunk are tagged with the VLAN ID that they belong to. What happens if a frame without a tag is placed on a trunk link? The answer is, the frame is placed on the Native VLAN.

Each trunk is configured with a Native VLAN. If it is not configured properly, it could be a source of network vulnerabilities that attackers can take advantage of.

Learning Outcomes

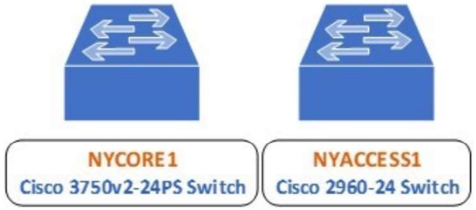
After completing this exercise, you will be able to:

- Identify Native VLANs, their uses, and vulnerabilities
- Configure Native VLANs for secure connectivity

Your Devices

You will be using the following devices in this lab. Please make sure these are powered on before proceeding.

- **NYCORE1** (Cisco 3750v2-24PS Switch)
- **NYACCESS1** (Cisco 2960-24 Switch)



Task 1 - Native VLAN Configuration

In this task, you will examine the default Native VLAN configuration of a trunk, and you will learn how to configure the Native VLAN on your network more securely.

Step 1

Connect to the **NYCORE1** switch and examine the trunk interface once again with the following command:

```
NYCORE1#show interface trunk
Port        Mode             Encapsulation  Status
Native vlan
Fa1/0/22    on               802.1q         trunking
1
Fa1/0/23    auto             n-802.1q       trunking
1
Port        Vlans allowed on trunk
Fa1/0/22    10,20
Fa1/0/23    1-4094
Port        Vlans allowed and active in management
domain
Fa1/0/22    10,20
Fa1/0/23    1,10,20,30
Port        Vlans in spanning tree forwarding state and
not pruned
Fa1/0/22    10,20
Fa1/0/23    1,10,20,30
NYCORE1#
```

You can see that the native VLAN for this trunk is **1**.

> ***Note:*** *It is considered a best practice to create a new VLAN other than the default VLAN, shut it down and use it as the Native VLAN. This will protect your network from vulnerabilities associated with the Native VLAN. For more information and to find out why use your favorite search engine to research this subject further.*

Step 2

Create a new VLAN with ID **99**, name it Native and shut it down.

> ***Note:*** *Remember that any VLANs you create in the* ***NYCORE1*** *switch will*

*automatically be created in the **NYACESS1** switch.*

```
NYCORE1#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
NYCORE1(config)#vlan 99
NYCORE1(config-vlan)#name Native
NYCORE1(config-vlan)#shutdown
NYCORE1(config-vlan)#exit
NYCORE1(config)#
```

Step 3

Next, configure the trunk on interface **FastEthernet 1/0/22** to use VLAN **99** as the native VLAN:

```
NYCORE1(config)#interface fastethernet 1/0/22
NYCORE1(config-if)#switchport trunk native vlan 99
NYCORE1(config-if)#exit
NYCORE1(config)#exit
NYCORE1#
```

Step 4

Verify this configuration by viewing the trunk interface information:

```
NYCORE1#show interface trunk
Port        Mode              Encapsulation  Status
Native vlan
Fa1/0/22    on                802.1q         trunking
99
Fa1/0/23    auto              n-802.1q       trunking
1
Port        Vlans allowed on trunk
Fa1/0/22    10,20
Fa1/0/23    1-4094
Port        Vlans allowed and active in management
domain
Fa1/0/22    10,20
Fa1/0/23    1,10,20,30
Port        Vlans in spanning tree forwarding state and
not pruned
Fa1/0/22    10,20
Fa1/0/23    1,10,20,30
NYCORE1#
```

The native VLAN has been successfully changed.

> ***Note:*** *It is important to note here that the trunk is currently not functioning correctly. There is what is called a Native VLAN mismatch. This is when the Native VLAN is configured differently on each end. This could be used to gain access to destination devices in a VLAN different from the VLAN that a source device is located in. This is known as VLAN hopping.*

Step 5

In order to complete the configuration, you must connect to **NYACCESS1** and configure the native VLAN correctly on the trunk. To do this, type these commands:

```
NYACCESS1#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
NYACCESS1(config)#interface fastethernet 0/24
NYACCESS1(config-if)#switchport trunk native vlan 99
NYACCESS1(config-if)#exit
NYACCESS1(config)#exit
NYACCESS1#
```

Step 6

Verify that the trunk is currently using the right native VLAN:

```
NYACCESS1#show interface trunk
Port        Mode             Encapsulation  Status
Native vlan
Fa0/24      on               802.1q         trunking
99
Port        Vlans allowed on trunk
Fa0/24      10,20
Port        Vlans allowed and active in management
domain
Fa0/24      10,20
Port        Vlans in spanning tree forwarding state and
not pruned
Fa0/24      10,20
NYACCESS1#
```

The native VLAN has been configured successfully.

Leave the devices you have powered on in their current state and proceed to the next exercise.