



Networkforyou

Subscribe to our
You Tube Channel



Network for you



**Welcome
To
Network for you
VLAN**



Email us:
networkforyou4@gmail.com

1 of 18

WhatsApp Us : +966532984612



VLAN:

- VLAN Stand for Virtual Local Area Network.
- VLAN divides a Single Broadcast domain into Multiple Broadcast domains.
- By Default, all ports of the switch are in VLAN1.
- VLAN 1 is known as Administrative VLAN or Management VLAN.
- A VLAN is a network that collects a set of network ports on a switching device into a single broadcast domain.
- In other words, we can say Vlan separating large broadcast domains into smaller ones.
- If a device in one VLAN sends a broadcast frame all devices in that same VLAN receive and other VLAN devices will not receive that.
- VLAN are Most often used over Ethernet Network.
- In one Physical switch we can create multiple VLANs that connect to different network.
- VLAN separate an existing physical network into multiple logical networks. Thus, each VLAN creates its own broadcast domain.
- We can make communication between two VLAN with the help of Router that process is known as Inter VLAN.
- VLAN is layer 2 Security and it enhance network security.
- By default, in every switch there is five VLANs.
- VLAN 1 is the default VLAN for every switch port.
- The standard Vlan range is from VLAN 1 to 1005.
- The Extended VLAN range is from VLAN 1006 – 4094.
- Extended-range are store in running configuration.
- VTP version 3 and transparent mode support extended-range.
- VLAN used in Switches and it operates at Layer 2.
- The reserved VLAN range is from VLAN 1002-1005.
- VLANs 1, 1002 to 1005 are created automatically & cannot be removed.
- Voice VLAN enables the access port to carry IP voice traffic.
- By default, in every cisco Switch the voice VLAN is disabled.
- VLANs are stored in Cisco Switch `vlan.dat` file in Flash Memory.



Some Basic VLAN Commands:

Commands	Description
SW1(Config)#vlan100	Create a VLAN
SW1(Config)#name IT	Name VLAN
SW1(config)# no vlan 100	Delete VLAN
SW1# sh vlan br	Verify VLAN Creation
SW1# sh flash or dir	Verify VLAN database
SW1(Config)# Vlan 100	Configure a Voice Vlan
SW1(config-vlan)# name Voice	Name Voice vlan
SW1(config)# interface e0/1	Interface mode
SW1(config-if)# switchport voice vlan 100	Put the interface in Voice VLAN 100
SW1# sh int e0/0 switchport	Verify Switchport configuration
SW1# sh int e0/0 status	Determine the physical status

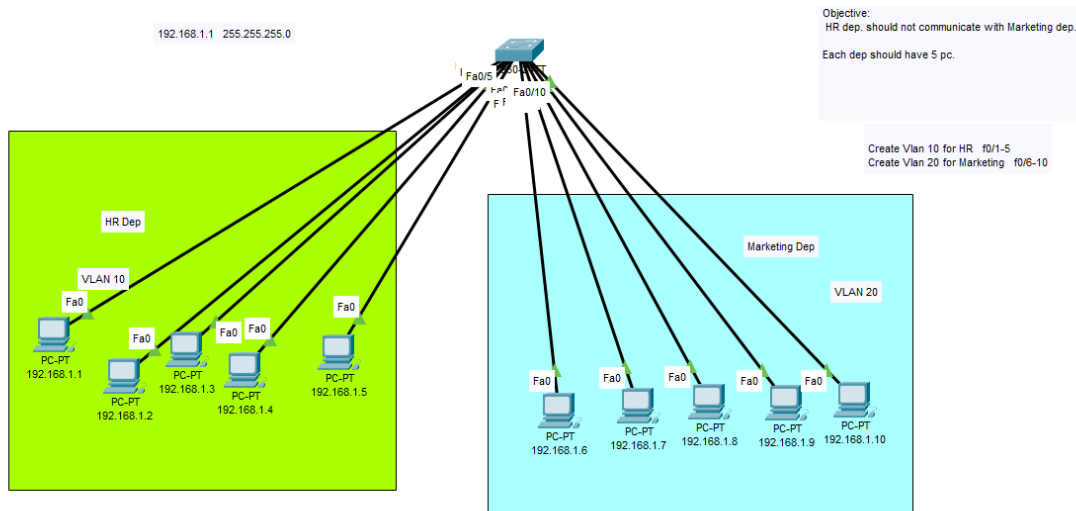
Basic Lab for VLAN:

Objective:

HR dep. should not communicate with Marketing dep.

Each dep should have 5 pc.

Create Vlan 10 for HR f0/1-5
Create Vlan 20 for Marketing f0/6-10



Email us:
networkforyou4@gmail.com

3 of 18

WhatsApp Us : +966532984612



Configuration

Configuration:

```
en
conf t
```

```
vlan 10
name HR
```

```
vlan 20
name Marketing
```

```
int range f0/1-5
switchport mode access
switchport access vlan 10
```

```
int range f0/6-10
switchport mode access
switchport access vlan 20
```

Multi switch VLANs using Trunking:

- Generally, we are configuring VLANs on a single switch and simply configuring each port to tell it the VLAN number to which the port belongs.
- But if we have multiple switches, then we need to consider additional concepts about how to forward traffic between the switches.
- When we are using VLANs in networks that have multiple interconnected switches the switches need to use VLAN Trunking on the links between the switches.
- VLAN Trunking causes the switches to use a process called **VLAN Tagging**, by which switch that is sending switch adds another header to the frame before sending it over the trunk.
- This extra Trunking header includes a VLAN identifier that is VLAN ID field so that the sending switch can associate the frame with a particular VLAN ID and receiving switch can then know in what VLAN each frame belongs.

Email us:
networkforyou4@gmail.com

4 of 18

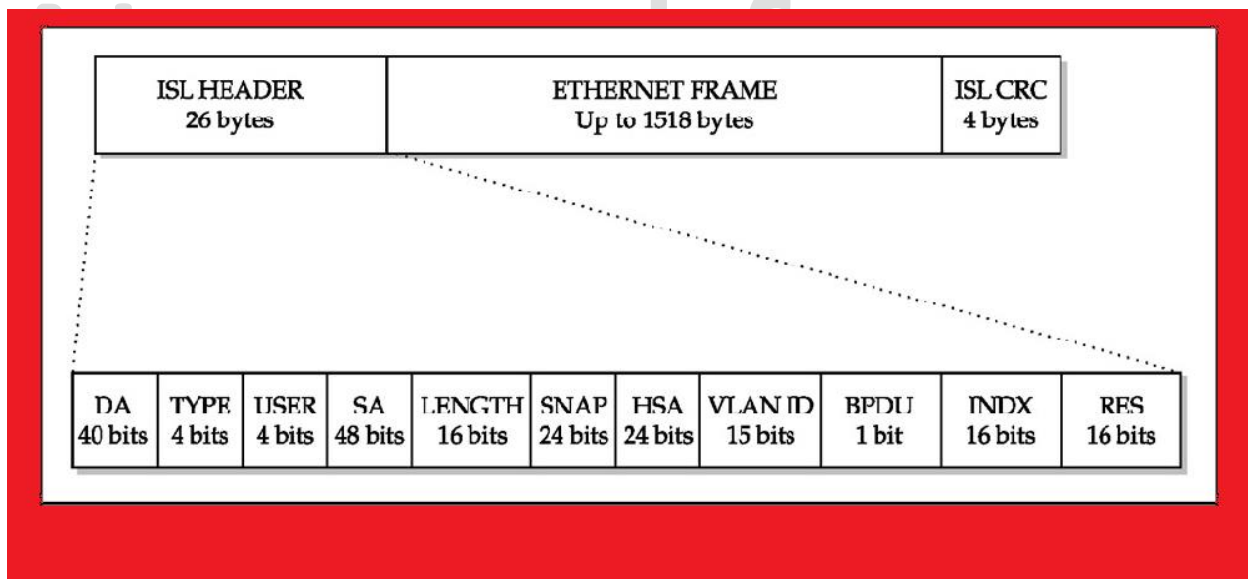
WhatsApp Us : +966532984612

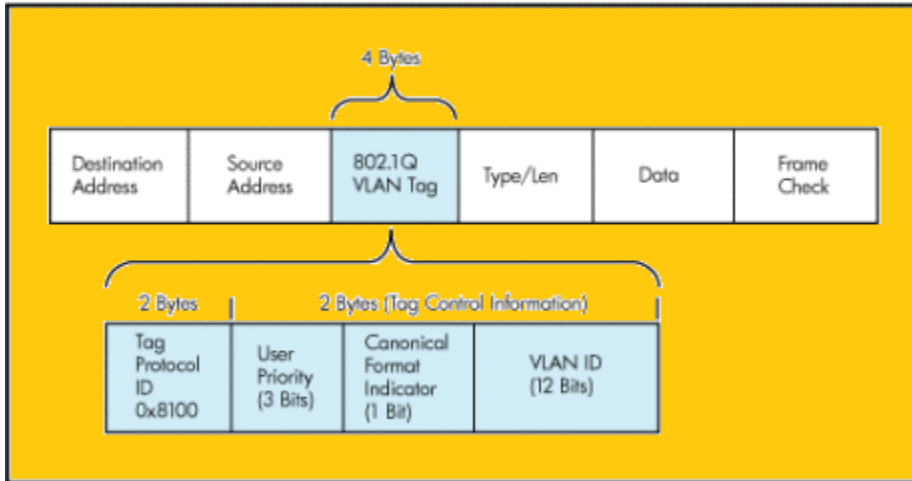


VLAN Trunking creates one link between switches that supports as many VLANs as we need.

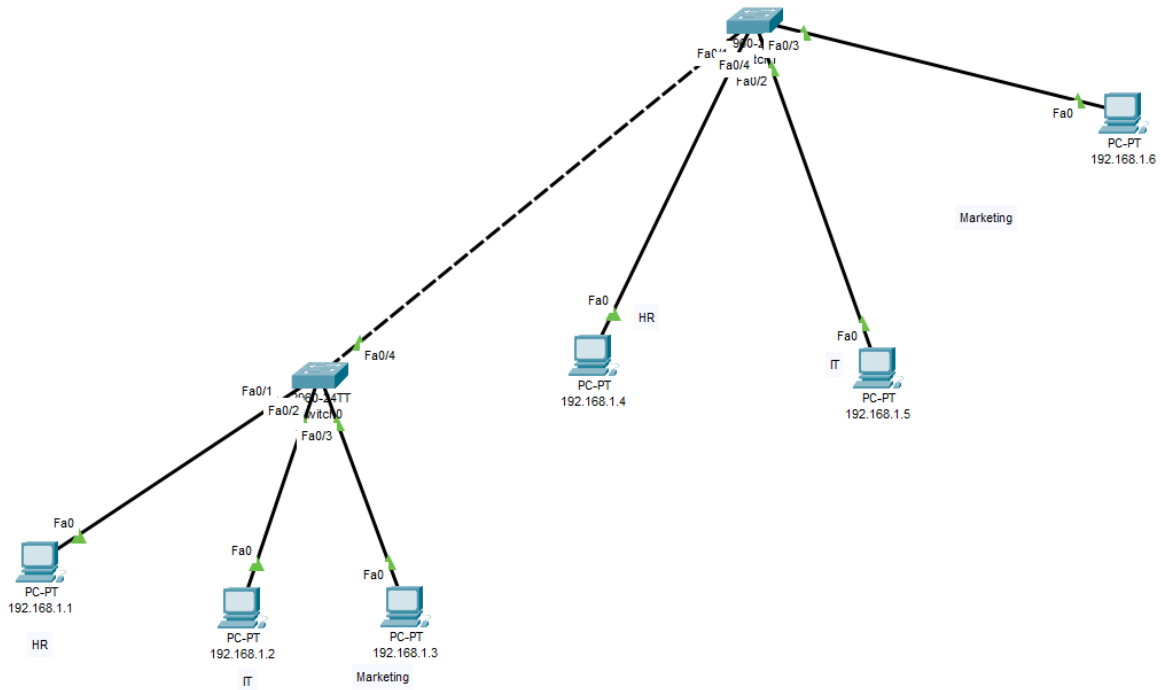
- CISCO has supported two different Trunking protocols.
 1. Inter-Switch Link (ISL) ----- CISCO created the ISL
 2. IEEE 802.1Q ----- IEEE

ISL	802.1Q
Proprietary	Open Standard
Encapsulated (ISL Header 26 Bytes and CRC 4 Bytes so total is 30 Bytes) CRC stand for cyclic redundancy check	Tagged (it uses 4 Bytes) it modifies the original frame
Encapsulates the old frame in a new frame	Add a field to the frame header





VLANs Lab using Trunking:



Email us:
networkforyou4@gmail.com

6 of 18

WhatsApp Us : +966532984612



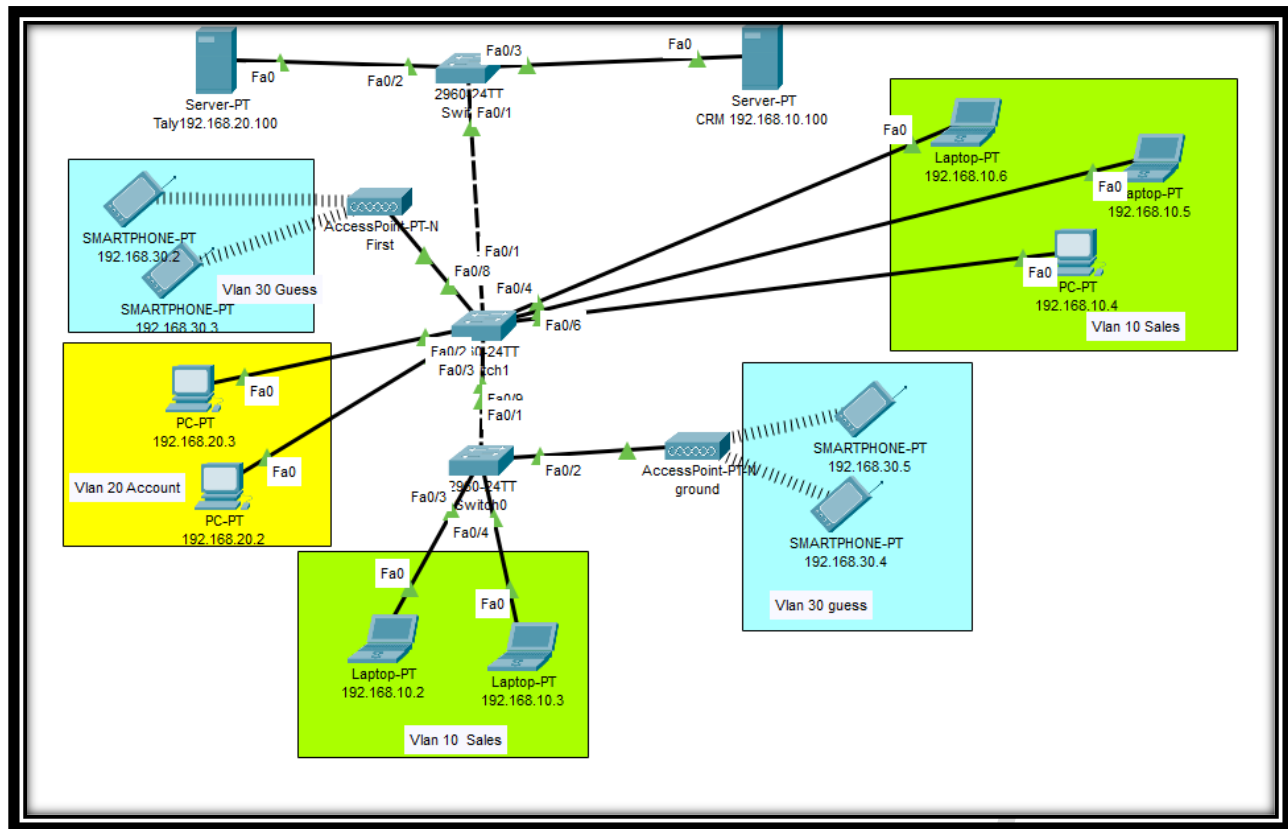
SW1 Configuration	SW2 Configuration
<pre>en config t hostname SW1 vlan 10 name HR vlan 20 name IT vlan 30 name Marking int f0/1 switchport mode access switchport access vlan 10 int f0/2 switchport mode access switchport access vlan 20 int f0/3 switchport mode access switchport access vlan 30 int f0/4 switchport mode trunk</pre>	<pre>en config t hostname SW2 vlan 10 name HR vlan 20 name IT vlan 30 name Marking int f0/1 switchport mode access switchport access vlan 10 int f0/2 switchport mode access switchport access vlan 20 int f0/3 switchport mode access switchport access vlan 30 int f0/4 switchport mode trunk</pre>

VLANs Lab 2 using Trunking:

Email us:
networkforyou4@gmail.com

7 of 18

WhatsApp Us : +966532984612



10 sales 192.168.10.0/24
20 Account 192.168.20.0/24
30 guess 192.168.30.0/24

Configuration for this Lab is given below.

Email us:
networkforyou4@gmail.com

8 of 18

WhatsApp Us : +966532984612



Ground Floor	First Floor	Second Floor
<pre>en config t hostname ground vlan 10 name sales vlan 20 name account vlan 30 name guestwifi int range f0/3-4 switchport mode access switchport access vlan 10 int f0/2 switchport mode access switchport access vlan 30 int f0/1 switchport mode trunk</pre>	<pre>en config t hostname First vlan 10 name sales vlan 20 name account vlan 30 name guestwifi int range f0/4-6 switchport mode access switchport access vlan 10 int range f0/2-3 switchport mode access switchport access vlan 20 int f0/8 switchport mode access switchport access vlan 30 int f0/9 switchport mode trunk int f0/1 switchport mode trunk</pre>	<pre>en config t hostname Second vlan 10 name sales vlan 20 name account int range f0/2 switchport mode access switchport access vlan 20 int range f0/3 switchport mode access switchport access vlan 10 int f0/1 switchport mode trunk</pre>

Email us:
networkforyou4@gmail.com

WhatsApp Us : +966532984612



Advantage of VLANs:

- Reduce CPU overhead on each device, improving hosting performance, by reducing the number of devices that receive each broadcast frame.
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches floods.
- To improve security for hosts through the application of different security policies per VLANs.
- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location.
- To solve problem more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain.
- To reduce the workload for the spanning Tree Protocol (STP) by limiting a Vlans to a single access switch.
- Limit the of broadcast, Better Performance and Security.

Type of VLAN	Descriptions
Data	Use for Normal data
Voice	Use for IP phone or Voice over IP
Management	A Vlan which is used for Telnet or SSH Configuration
Extended	Usable if VTP Mode is transparent on Switches
Native VLAN	Untagged frame is sent over trunk link by default VLAN 1 is native Vlan

Types of VLAN

1. Static VLAN -----> Base on Port number
2. Dynamic VLAN -----> Base on the MAC address

Static VLAN:

- Static VLAN's are based on port numbers.
- Need to configure manually i.e. Assign a port on a switch to a VLAN.
- One port can be a member of only one VLAN.
- It is also called Port Based VLANs.
- Static VLAN is a group of ports designated by the switch as belonging to the same broadcast domain.

VLAN Creation:

```
Switch(Config)# vlan <no>  
Switch(Config-vlan)#name <name>
```

Email us:
networkforyou4@gmail.com

10 of 18

WhatsApp Us : +966532984612



Assigning Ports in VLAN:

```
Switch(Cofig)# interface <interface type> <interface no.>  
Switch(Cofig-if)#switchport mode access  
Switch(Cofig-if)#switchport access Vlan <no>
```

Dynamic VLAN:

- Generally, we don't use Dynamic VLAN.
- Dynamic VLAN's are based on the MAC address of a PC.
- Switch automatically assign the port to a VLAN
- Each port can be a member of multiple VLAN's
- For Dynamic VLAN configuration, a software called VMPS (**VLAN Membership Policy Server**) is needed.

VLAN Database:

- The VLAN database is used to store vlan data, such as the VLAN ID, name and MTU.
- The default location of the VLAN database is in the local vlan.dat file.
- VLAN database is stored in non-volatile memory, which is flash.

Commands	Description
SW1# dir or show flash	Verify VLAN database
SW1#more unix:/vlan.dat-00002	To Ready Vlan database
SW1#delete unix:/vlan.dat-00002	To Delete Vlan database

Normal VLAN:

- Normal VLANs range are from VLANs 1 to VLAN 1005.
- Normal VLANs are stored in vlan.dat file in Flash memory.
- VTP versions 1 and 2 can advertise normal range VLANs only.

Extended VLAN:

- Extended VLANs are VLANs that fall in the range 1006 to 4094.
- Extended VLANs are mainly used in Service Provider Networks.
- Extended VLANs allow for the provisioning of Large numbers of customers.
- Extended VLANs must be configured in VTP transparent mode or VTP V3.
- Extended VLANs are saved and store in switch running-configuration.

Email us:
networkforyou4@gmail.com

11 of 18

WhatsApp Us : +966532984612



Dynamic Trunking Protocol (DTP):

- It is CISCO proprietary Protocol.
- If two CISCO switches are cabled together, they can negotiate a trunk connection using CISCO DTP.
- It is however recommended to manually configure switch ports.
- Manual configuration for Trunk port as given below.

Command we use is given below:

- Switchport mode access
- Switchport mode trunk

DTP Configuration:

1. Switchport mode dynamic auto
2. Switchport mode dynamic desirable
3. Switchport no negotiate

Switchport mode **dynamic auto:**

- Switch will form a trunk if the neighbor switch port is set to **trunk or desirable**.
- Trunk will not be formed if both sides are set to auto.
- In newer switches default we have auto.

Switchport mode **dynamic desirable:**

- Switch will form a trunk if the neighbor switch port is set **trunk, desirable or auto**.

Switchport mode no negotiate:

- Disable DTP

For Layer 3 Switch we use below given command to make trunk Port:

```
Int f0/1  
Switchport trunk encapsulation dot1q  
Switchport mode trunk  
End
```

Email us:
networkforyou4@gmail.com

12 of 18

WhatsApp Us : +966532984612



Command	Description
Sh int f0/1 switchport	This command is for checking status of interface.
Int f0/1 Switchport mode dynamic auto	This command is for setting interface as dynamic Auto.
Int f0/1 Switchport mode dynamic desirable	This command is for setting interface as dynamic desirable.
Sh interfaces trunk	To Check Interface Trunk

Trunking Administrative Mode Options with the Switchport Mode Command:

Command	Description
Access	Always act as an access (nontrunk) port.
Trunk	Always act as trunk port.
Dynamic desirable	Initiates negotiation message and responds to negotiation message to dynamically choose whether to start using trunking.
Dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking.

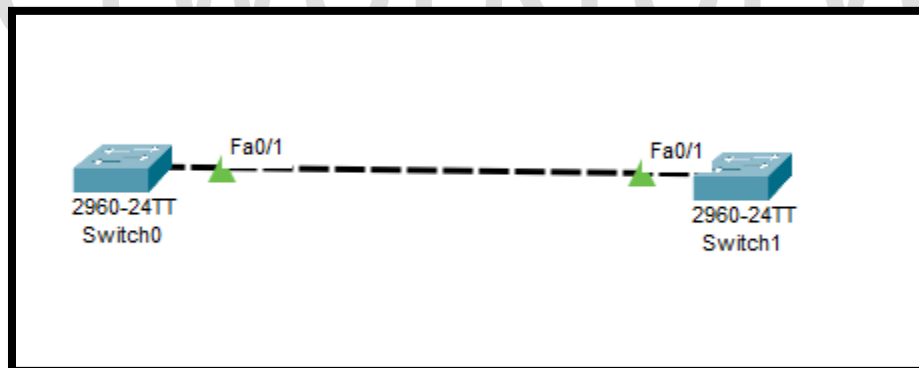
Email us:
networkforyou4@gmail.com

WhatsApp Us : +966532984612



Native VLAN:

- If any Frame is received without VLAN tagged then it assumed that it belongs to Native VLAN.
- All native VLAN traffic is untagged; it doesn't have an 802.1Q tag on the Ethernet frame.
- Default Native VLAN is VLAN 1. We can change this if we want
- When Cisco switches receive an Ethernet frame without a tag on an 802.1Q enabled interface, it will assume that it belongs to the native VLAN. For this reason, you need to make sure that the native VLAN is the same on both sides of the trunk port switches.
- Best practice is to configure the Native VLAN ID to other than VLAN 1.
- No ports should be assigned to the native vlan.
- An attacker who attempts to use the **VLAN hopping attack** will end up in a dead VLAN that has no hosts to attack.
- We can change Native vlan from vlan 1 to other.



Let do small lab for this Native VLAN and Check.

Email us:
networkforyou4@gmail.com

14 of 18

WhatsApp Us : +966532984612



Switch	Switch2
<pre>Switch#config t Switch(config)#int f0/1 Switch(config-if)#switchport mode trunk %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up Switch(config-if)#do sh int trunk</pre>	<pre>Switch2# sh int trunk</pre>

```
Switch(config-if)#do sh int trunk
Port      Mode      Encapsulation  Status  Native vlan
Fa0/1     on        802.1q         trunking  1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
```

Email us:
networkforyou4@gmail.com

WhatsApp Us : +966532984612



```
Switch2#sh int trun
Port      Mode      Encapsulation  Status  Native vlan
Fa0/1    auto      n-802.1q       trunking  1

Port      Vlans allowed on trunk
Fa0/1    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1
```

Let change Native Vlan from 1 to any other vlan.

First Let change native Vlan for Switch1 wait and see Native Vlan mismatch alert. Then we will do Native Vlan change to Switch2. Let create Vlan 10 and make it Native Vlan for Both Switch.

Switch	Switch2
En	En
Config t	Config t
Vlan 10	Vlan 10
Int f0/1	Int f0/1
Switchport trunk native vlan 10	Switchport trunk native vlan 10

For Switch1 and Switch 2 we have Native Vlan Mismatch Alert. As given below then we will make in Switch 2 as vlan 10 as Native Vlan.

Email us:
networkforyou4@gmail.com

WhatsApp Us : +966532984612



```
Switch(config-if)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan
id 10 on FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent local
vlan.

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1),
with Switch2 FastEthernet0/1 (10).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1),
with Switch2 FastEthernet0/1 (10).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1),
with Switch2 FastEthernet0/1 (10).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1),
with Switch2 FastEthernet0/1 (10).
```

```
Switch2#En
Switch2#Config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#Vlan 10
Switch2(config-vlan)#Int f0/1
Switch2(config-if)#Switchport trunk native vlan 10
Switch2(config-if)#
Switch2(config-if)#
Switch2(config-if)#
Switch2(config-if)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer
vlan id 1 on FastEthernet0/1 VLAN10.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0010. Inconsistent local
vlan.

Switch2(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (10),
with Switch FastEthernet0/1 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (10),
with Switch FastEthernet0/1 (1).
```

Email us:
networkforyou4@gmail.com

17 of 18

WhatsApp Us : +966532984612



```
Switch2#Config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#Vlan 10
Switch2(config-vlan)#Int f0/1
Switch2(config-if)#Switchport trunk native vlan 10
Switch2(config-if)#
Switch2(config-if)#do sh int trun
Switch2(config-if)#do sh int trun
Port          Mode          Encapsulation  Status      Native vlan
Fa0/1         auto          n-802.1q       trunking    10

Port          Vlans allowed on trunk
Fa0/1         1-1005

Port          Vlans allowed and active in management domain
Fa0/1         1,10

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         none
```

Now no notification for Mismatch for Native Vlan as we make both end same native Vlan 10.

Networkforyou

Email us:
networkforyou4@gmail.com

18 of 18

WhatsApp Us : +966532984612