Virtual Local Area Network (Basic)

Safwan Muntasir (Sufi)
Networking Enthusiast

Contents

Back to Contents

Introduction

VLANs are a fundamental technology in modern networking, allowing administrators to **logically divide a physical network** into multiple, **isolated broadcast domains**. Devices in different **VLANs cannot communicate** with each other directly, **unless they are routed** through a router or switch. Virtual local area networks (VLANs) were first conceived in the **late 1980s** by **W. David Sincoskie**, a computer engineer at Bellcore. Sincoskie was looking for a way to improve the performance and security of Ethernet networks, which were becoming increasingly congested as more devices were connected to them. Sincoskie's early work on VLANs was implemented using a bridging protocol called **GARP** (Generic Attribute Registration Protocol). GARP allowed switches to communicate with each other and dynamically assign devices to VLANs.

In **1998**, the **IEEE 802.1Q** standard was published, which defined a standard way to implement VLANs in Ethernet networks. The 802.1Q standard **added a new header to Ethernet frames** that allows switches to identify the VLAN that a frame belongs to. Today, VLANs are an essential part of many enterprise networks. They are used to improve performance, security, and manageability. VLANs are also being used in new and innovative ways, such as in cloud computing and software-defined networking.

Inter-Switch Link (**ISL**) is a **cisco proprietary** VLAN trunking protocol developed by Cisco Systems in the 1990s. ISL played a significant role in the early days of Virtual Local Area Networks (VLANs) before the IEEE 802.1Q standard became widely adopted.

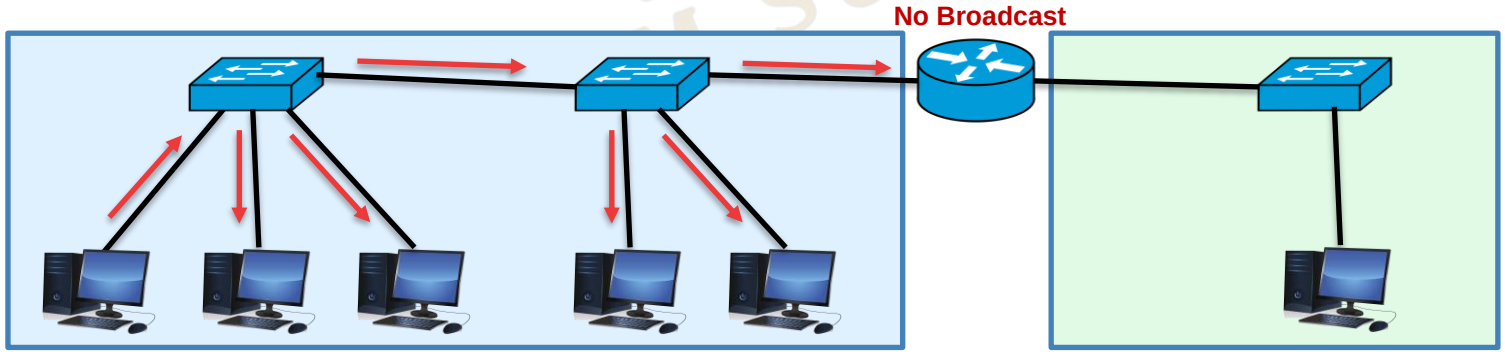
Back to Contents

Broadcast Domain

LAN: A Local Area Network (LAN) is a **single broadcast domain**, including all devices in that broadcast domain. In another word, LAN is a single network where various end devices communicates through **MAC Address** (Layer 2) without any routing (Layer 3).

Broadcast Domain: A broadcast domain is the group of devices which will receive a broadcast frame (destination MAC FFFF.FFFF.FFFF) sent by any one of the members.

- Switches broadcast ethernet frames if they **haven't learned** the destination **MAC address**.
- Switches **flood broadcast** traffic on all their interfaces, **except the one they received** the broadcast on.
- Size of the broadcast domain depends on number of devices connected in LAN/VLAN.
- Routers do not forward broadcast traffic, they break broadcast domains. But **VLANs on switches also break the broadcast domain**.



Back to Contents

VLAN Basics

VLAN: VLAN is a **logical grouping** of devices on a network that are treated as if they were on a separate physical network, even though they may be connected to the same switch or router.

- VLANs are configured on switches on a **per-interface basis** and it logically separate end hosts at layer 2.
- **Reduces broadcast domain** in a LAN.
- Switches do not forward traffic directly between hosts in different VLANs.
- VLANs limit the number of broadcast, better performance and enhance network security.
- Improves the network performance and **reduces network congestion**.

Every interfaces in a switch maintain a MAC-Address-Table to forward frames in Layer 2 communication. This table has four columns-

- **VLAN:** VLAN ID if used.
- **MAC-Address:** Connected or received end host's MAC addresses.
- **Type:** Static or Dynamic
- **Port:** Port on which the destination device is connected.

***Every Interfaces in Switch/Router has a Network Interface Card (NIC) and a unique MAC Address.**

***End host cannot understand VLAN information. Connected interfaces of the switch belongs to specific VLANs.**

Back to Contents

VLAN Types

There are mainly **five types** of VLAN-

1. **Default VLAN:** It is the VLAN that is **by default exist**. In different vendor switches like Cisco, HP, Huawei, etc, the default VLAN is **typically 1**. At the initial boot up of the switch, all the ports become a member of the default VLAN (one broadcast domain). VLAN 1 has all the features of any VLAN, except it **cannot be renamed or deleted**. It is commonly used for traffic that has not been explicitly tagged with a VLAN ID.

2. **Data VLAN:** It is the **most common type** of VLAN, also known as a **user VLAN**. The link connected to end devices like PC is assigned to a data VLAN. It is designed only **for user-generated data** such as regular network traffic. Data VLANs can help to improve network performance and security by isolating different groups of traffic from each other.

3. **Voice VLAN:** Voice VLANs are used to **carry voice over IP (VoIP)** traffic, also known as **Auxiliary VLAN** (AUX VLAN). Voice VLAN enables access ports to carry IP voice traffic from an IP Phone. VoIP traffic is **time-sensitive**, so it is important to isolate it from other types of traffic to avoid performance problems. Voice VLANs can also help to improve the quality of VoIP calls by **reducing jitter** and **latency**. IP Phones used the same UTP cables to connect to ethernet switch. PCs will be in a data VLAN and IP Phones will be in the Voice VLAN.

Back to Contents

VLAN Types

4. **Management VLAN:** Management VLANs are used to **group together devices** that need to be managed, such as switches, routers, and firewalls including **remote administration**, **device monitoring** and **configuring management** by using protocols such as telnet, SSH, SNMP, syslog etc. Normally the Management VLAN is VLAN 1, but it can be any VLAN. It is recommended to use separate VLAN for management traffic. Management VLANs can help to improve security by isolating management traffic from other types of traffic.

5. **Native VLAN:** The native VLAN is **often used in IEEE 802.1Q trunk links**. It is a special type of trunk VLAN. Native VLANs are used to **carry untagged traffic** on a trunk link. Untagged traffic is traffic that does not belong to any specific VLAN. Native VLANs are typically configured as VLAN 1.

Back to Contents

VLAN Ranges

The IEEE 802.1Q standard specifies a range of 0 to 4095 VLAN IDs (total 4096 VLANs). These VLANs are organized into several ranges-

VLANs	Type	Usage
0, 4095	Reserved	For system use only, cannot be seen or used
1	Default/Normal	Can be used but cannot be deleted
2-1001	Normal	For Ethernet VLANs. Can be created, used and deleted.
1002-1005	Reserved/Normal	Defaults for FDDI and Token Ring. Should not be used and cannot be deleted
1006-4094	Extended	For Ethernet VLANs. Can be created, used and deleted

Back to Contents

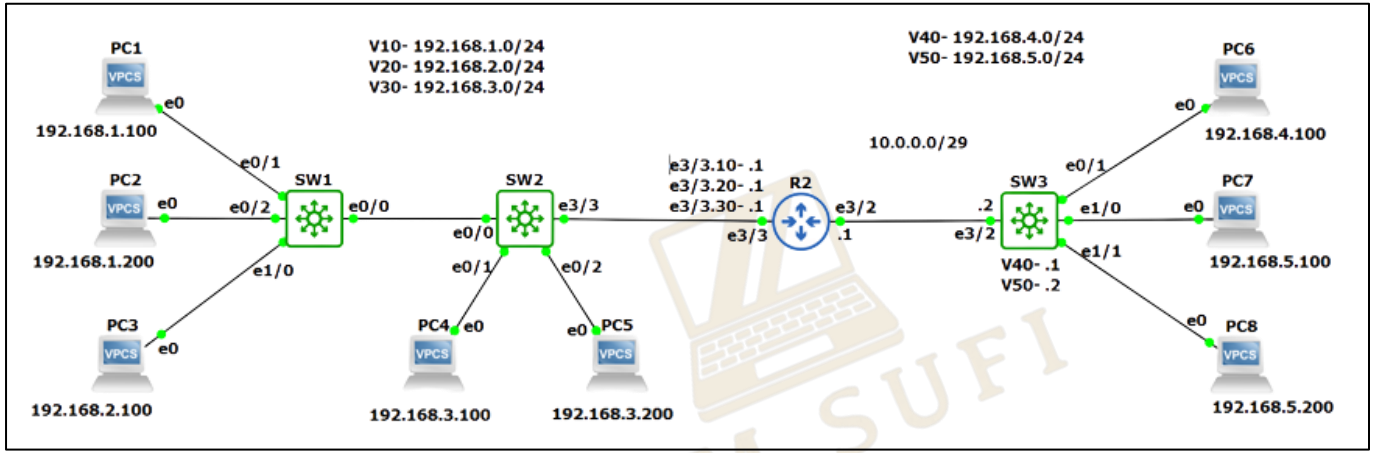
Switchport Modes

There are **mainly two** switchport modes-

1. **Access Mode:** Configured to **carry traffic for a single VLAN**. The switch **removes the VLAN tag** from all frames received on the port and forwards the frames to the switch's MAC address table. In access mode, the switch port is configured to **connect end-user devices** like computers, printers, and IP phones. The port belongs to a single VLAN, and all traffic on the port is untagged and associated with that VLAN. That's why it's called an access port, it gives the end hosts access to the network.

2. **Trunk Mode:** Configured to **carry traffic for multiple VLANs**. The switch **preserves the VLAN tag** on all frames received on the port and forwards the frames to the appropriate switchport or router interface based on the VLAN tag. Trunk ports are essential for inter-switch communication, as they can carry tagged frames representing different VLANs. The most common standard for VLAN tagging is **IEEE 802.1Q**. There is another VLAN tagging protocol named Inter-Switch Link (**ISL**) which is a Cisco Proprietary**. ISL doesn't support native VLANs**. That's why it is not used in today's networks.

Basic Configuration



*****This lab/topology was created in GNS3 2.2.43**

***Routers: Cisco Catalyst 7200 Series Router

***Switches: i86bi Linux L3 Cisco IOS Version 15.1

***PCs: GNS3 Default VPCS

- By default all the interface of a switch belongs to Default VLAN 1. Use this command to check-

  'SW# show vlan brief'

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Basic Configuration

- Create VLAN using following commands-

  'SW# configure terminal'

  'SW(config)# vlan <VLAN ID>'

  'SW(config-vlan)# name <VLAN name>'

```
SW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#vlan ?
  WORD            ISL VLAN IDs 1-4094
  access-log      Configure VACL logging
  access-map      Create vlan access-map or enter vlan access-map command mode
  accounting      VLAN accounting configuration
  configuration   vlan feature configuration mode
  dot1q           dot1q parameters
  filter          Apply a VLAN Map
  group           Create a vlan group
  internal        internal VLAN

SW1(config)#vlan 10
SW1(config-vlan)#name LAN
```

- Configuring switchport mode in interfaces connected to end devices-

  'SW(config)# interface range <interface ID range>'

  'SW(config-if-range)# switchport mode <access>'

  'SW9config-if-range)# switchport access vlan <VLAN ID>'

  If VLAN is not created, it will be created automatically after configuring switchport access to that VLAN.

```
SW1(config)#interface range e0/1-3
SW1(config-if-range)#switchport mode ?
  access          Set trunking mode to ACCESS unconditionally
  dot1q-tunnel    set trunking mode to TUNNEL unconditionally
  dynamic         Set trunking mode to dynamically negotiate access or trunk mode
  private-vlan    Set private-vlan mode
  trunk           Set trunking mode to TRUNK unconditionally

SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#
SW1(config-if-range)#interface range e1/0-3
SW1(config-if-range)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
```

Basic Configuration

- Configuring switchport mode in the up-links-

  'SW(config)# switchport interface <interface ID>'

  'SW(config-if)# switchport trunk encapsulation <dot1q>'

  'SW(config-if)# switchport mode <trunk>'

  'SW(config-if)# switchport trunk allowed vlan <VLAN IDs>'

```
SW1(config-if)#switchport trunk encapsulation ?
  dot1q       Interface uses only 802.1q trunking encapsulation when trunking
  isl         Interface uses only ISL trunking encapsulation when trunking
  negotiate   Device will negotiate trunking encapsulation with peer on
              interface

SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list

SW1(config-if)#switchport trunk allowed vlan 10,20
```

Encapsulation is the process of **adding a header and trailer** to a frame in order to prepare it for transmission over a network. The encapsulation header contains information about the frame, such as the source and destination MAC addresses, the VLAN ID (if VLANs are being used), and the type of traffic. The encapsulation trailer contains information about the end of the frame, such as a checksum.

Layer 2 switches do not need to encapsulate frames because they are only transmitting frames within the same network segment. Layer 2 switches use the MAC address tables to forward frames to the correct destination devices.

I have used Multilayer switches in the topology, that's why I have used ***'switchport trunk encapsulation dot1q'*** command before configuring switchport mode to trunk. We will learn about encapsulation in details in later slides In Sha Allah. Just remember for now, in case of Layer 2 switches like C2960, this command is not needed.

Basic Configuration

- Configuration on Switch 2-

```
SW2(config)#interface e0/0
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan 10,20
SW2(config-if)#interface range e0/1-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
SW2(config-if-range)#interface e3/3
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport tru
*Oct 31 12:01:49.854: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/
3, changed state to down
SW2(config-if)#switchport trunk
*Oct 31 12:01:52.864: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/
3, changed state to up
SW2(config-if)#switchport trunk allowed vlan 10,20,30
```

- Configuration on PCs-

```
PC1> ip 192.168.1.100/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.100 255.255.255.0 gateway 192.168.1.1
```

```
PC2> ip 192.168.1.200/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.200 255.255.255.0 gateway 192.168.1.1
```

```
PC3> ip 192.168.2.100/24 192.168.2.1
Checking for duplicate address...
PC1 : 192.168.2.100 255.255.255.0 gateway 192.168.2.1
```

```
PC4> ip 192.168.3.100/24 192.168.3.1
Checking for duplicate address...
PC1 : 192.168.3.100 255.255.255.0 gateway 192.168.3.1
```

```
PC5> ip 192.168.3.200/24 192.168.3.1
Checking for duplicate address...
PC1 : 192.168.3.200 255.255.255.0 gateway 192.168.3.1
```

Basic Configuration

- SW1 VLAN information-

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
10   LAN                              active    Et0/1, Et0/2, Et0/3
20   VLAN0020                         active    Et1/0, Et1/1, Et1/2, Et1/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- SW2 VLAN information-

```
SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2
30   VLAN0030                         active    Et0/1, Et0/2, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- To check trunk information, use this command-

  'SW# show interfaces trunk'

- SW1 trunk information-

```
SW1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       10,20

Port        Vlans allowed and active in management domain
Et0/0       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       10,20
```

- SW2 trunk information-

```
SW2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       10,20
Et3/3       10,20,30

Port        Vlans allowed and active in management domain
Et0/0       none
Et3/3       30

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       none
Et3/3       30
```

Back to Contents

Inter-VLAN Routing

VLANs have been created. PCs from same VLAN can ping each other, but cannot ping end devices in different VLAN. Inter-VLAN Routing must be enabled to ping/reach end devices on other VLANs. Gateway of VLAN 10, 20 and 30 will be on SW2. SW2 is a Layer 3 or Multilayer Switch.

```
PC1> ping 192.168.1.200 -c 3
84 bytes from 192.168.1.200 icmp_seq=1 ttl=64 time=1.156 ms
84 bytes from 192.168.1.200 icmp_seq=2 ttl=64 time=1.326 ms
84 bytes from 192.168.1.200 icmp_seq=3 ttl=64 time=0.990 ms

PC1> ping 192.168.2.100 -c 3
host (192.168.1.1) not reachable

PC1> ping 192.168.3.100 -c 3
host (192.168.1.1) not reachable
```

There are **two ways** to enable Inter-VLAN Routing-

1. **Router-On-A-Stick (ROAS):** Router-on-a-Stick is a common method for inter-VLAN routing **using a single physical router interface** connected to a switch. This router interface serves as a **gateway for multiple VLANs** using **sub-interfaces**, each configured with a unique IP address and VLAN ID. The router tags incoming frames with the appropriate VLAN tag, routes the packets, and untags them before sending them back to the switch.
2. **Layer-3 Switch:** A Layer 3 switch is a **multi-layer switch capable of routing traffic** between networks. It combines Layer 2 and Layer 3 functionality, allowing for routing without the need for an external router. VLANs are configured on the Layer 3 switch, and IP addresses are assigned to each VLAN interface. **The switch can route traffic between VLANs directly**, eliminating the need for external routing devices.

Back to Contents

Router-On-A-Stick (ROAS)

Gateway of VLAN 10, 20 and 30 is on the router. So, we have to configure Router-On-A-Stick to route between VLANs.

- To enable Inter-VLAN Routing on a router-

  'RTR(config)# ip routing'

- Sub-interface commands in routers-

  'RTR(config)# interface <interface no>.<sub-int no>'

  'RTR(config)# encapsulation dot1q <VLAN ID>'

  'RTR(config)# ip address <network ip> <subnet mask>'

  'RTR(config)# no shutdown'

```
R1(config)#interface e3/3
R1(config-if)#no shutdown
R1(config-if)#
*Mar  1 04:03:10.666: %LINK-3-UPDOWN: Interface Ethernet3/3, changed state to up
*Mar  1 04:03:11.666: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/
3, changed state to up
R1(config-if)#interface e3/3.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface e3/3.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#interface e3/3.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.3.1 255.255.255.0
R1(config-subif)#no shutdown
R1(config-subif)#
R1(config-subif)#exit
R1(config)#ip routing
```

***Always remember**, physical interface must be on up state. If physical interface become down, sub-interfaces will also become down state.

Router-On-A-Stick (ROAS)

We have done Inter-VLAN Routing, still VLAN 10 and 20 cannot ping their gateway, though PCs from VLAN 30 can ping its gateway. **Can you tell why??**

```
PC1> ping 192.168.1.200 -c 3
84 bytes from 192.168.1.200 icmp_seq=1 ttl=64 time=0.922 ms
84 bytes from 192.168.1.200 icmp_seq=2 ttl=64 time=1.480 ms
84 bytes from 192.168.1.200 icmp_seq=3 ttl=64 time=1.075 ms

PC1> ping 192.168.1.1
host (192.168.1.1) not reachable

PC1> ping 192.168.2.100
host (192.168.1.1) not reachable
```

If you can remember our configuration till now, we have not created VLAN 10 and 20 on SW2. Packets from PCs n VLAN 10 and 20 are coming from SW1 to SW2, but SW2 doesn't recognize these VLANs. So, they don't know where to forward the packets and discards them.

```
PC4> ping 192.168.3.1 -c 3
84 bytes from 192.168.3.1 icmp_seq=1 ttl=255 time=16.122 ms
84 bytes from 192.168.3.1 icmp_seq=2 ttl=255 time=16.464 ms
84 bytes from 192.168.3.1 icmp_seq=3 ttl=255 time=15.352 ms

PC4> ping 192.168.1.100 -c 3
192.168.1.100 icmp_seq=1 timeout
192.168.1.100 icmp_seq=2 timeout
192.168.1.100 icmp_seq=3 timeout
```

Always remember, in every transit switch, transit VLANs must be created, or else those switch will discard the packets.

```
SW2(config)#vlan 10
SW2(config-vlan)#exit
SW2(config)#vlan 20
SW2(config-vlan)#exit
```

Now, VLAN 10, 20 and 30 has been created in SW2, but SW doesn't have to know about VLAN 30 although PCs from these VLAN can ping each other. **WHY?? Think of yourself!**

Router-On-A-Stick (ROAS)

- Now PCs from every VLANs can ping each other. First ping is lost because of ARP requests to know the MAC addresses.

```
PC1> ping 192.168.1.1 -c 3
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=15.878 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=16.572 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=16.213 ms

PC1> ping 192.168.2.100 -c 3
192.168.2.100 icmp_seq=1 timeout
84 bytes from 192.168.2.100 icmp_seq=2 ttl=63 time=32.492 ms
84 bytes from 192.168.2.100 icmp_seq=3 ttl=63 time=32.114 ms

PC1> ping 192.168.3.100 -c 3
192.168.3.100 icmp_seq=1 timeout
192.168.3.100 icmp_seq=2 timeout
84 bytes from 192.168.3.100 icmp_seq=3 ttl=63 time=31.506 ms
```

```
PC3> ping 192.168.2.1 -c 3
84 bytes from 192.168.2.1 icmp_seq=1 ttl=255 time=16.220 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=255 time=16.140 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=255 time=16.411 ms

PC3> ping 192.168.1.100 -c 3
84 bytes from 192.168.1.100 icmp_seq=1 ttl=63 time=32.296 ms
84 bytes from 192.168.1.100 icmp_seq=2 ttl=63 time=31.236 ms
84 bytes from 192.168.1.100 icmp_seq=3 ttl=63 time=31.985 ms

PC3> ping 192.168.3.200 -c 3
192.168.3.200 icmp_seq=1 timeout
84 bytes from 192.168.3.200 icmp_seq=2 ttl=63 time=31.876 ms
84 bytes from 192.168.3.200 icmp_seq=3 ttl=63 time=31.622 ms
```

- SW2 VLAN information-

```
SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active    Et0/1, Et0/2, Et0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- SW2 trunk information-

```
SW2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       10,20
Et3/3       10,20,30

Port        Vlans allowed and active in management domain
Et0/0       10,20
Et3/3       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       10,20
Et3/3       10,20,30
```

Router-On-A-Stick (ROAS)

- Interfaces and sub-interfaces of R1-

```
R1#show ip interface brief | begin Ethernet3/3
Ethernet3/3                unassigned      YES NVRAM  up                    up
Ethernet3/3.10             192.168.1.1     YES NVRAM  up                    up
Ethernet3/3.20             192.168.2.1     YES NVRAM  up                    up
Ethernet3/3.30             192.168.3.1     YES NVRAM  up                    up
Vlan1                      unassigned      YES NVRAM  up                    down
```

- Route table of R1

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.99.0 is directly connected, Ethernet3/2
C    192.168.1.0/24 is directly connected, Ethernet3/3.10
C    192.168.2.0/24 is directly connected, Ethernet3/3.20
C    192.168.3.0/24 is directly connected, Ethernet3/3.30
```

Layer-3 Switch Inter-VLAN Routing

Gateway of VLAN 40 and 50 is on the Multilayer SW3. After creating VLAN 40 and 50 we have to create VLAN interfaces and assign gateway address of these VLANs. Then SW3 will be able to route Inter-VLANs by enabling ip routing in the switch.

- Assigning ip addresses in the VLAN interfaces-

  'SW(config)# interface vlan <VLAN ID>'

  'SW(config-if)# ip address <IP Address> <subnet mask>'

```
SW3(config)#interface vlan 40
SW3(config-if)#ip addres
*Nov  2 20:03:10.583: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, ch
anged state to down
SW3(config-if)#ip address 192.168.4.1 255.255.255.0
SW3(config-if)#no shutdown
SW3(config-if)#
*Nov  2 20:03:39.192: %LINK-3-UPDOWN: Interface Vlan40, changed state to up
*Nov  2 20:03:40.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, ch
anged state to up
SW3(config-if)#exit
SW3(config)#interface vlan 50
SW3(config-if)#ip add
*Nov  2 20:03:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, ch
anged state to down
SW3(config-if)#ip address 192.168.5.1 255.255.255.0
SW3(config-if)#no shutdown
SW3(config-if)#
*Nov  2 20:04:10.688: %LINK-3-UPDOWN: Interface Vlan50, changed state to up
*Nov  2 20:04:11.694: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, ch
anged state to up
SW3(config-if)#exit
SW3(config)#ip routing
```

```
PC6> ip 192.168.4.100/24 192.168.4.1
Checking for duplicate address...
PC1 : 192.168.4.100 255.255.255.0 gateway 192.168.4.1
```

```
PC7> ip 192.168.5.100/24 192.168.5.1
Checking for duplicate address...
PC1 : 192.168.5.100 255.255.255.0 gateway 192.168.5.1
```

```
PC8> ip 192.168.5.200/24 192.168.5.1
Checking for duplicate address...
PC1 : 192.168.5.200 255.255.255.0 gateway 192.168.5.1
```

```
SW3(config)#vlan 40
SW3(config-vlan)#exit
SW3(config)#vlan 50
SW3(config-vlan)#exit
SW3(config)#interface range e0/1-3
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 40
SW3(config-if-range)#interface range e1/0-3
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 50
```

Back to Contents

Layer-3 Switch Inter-VLAN Routing

Now every end devices will be able to ping other VLANs end devices.

```
PC6> ping 192.168.4.1 -c 3
84 bytes from 192.168.4.1 icmp_seq=1 ttl=255 time=0.730 ms
84 bytes from 192.168.4.1 icmp_seq=2 ttl=255 time=0.808 ms
84 bytes from 192.168.4.1 icmp_seq=3 ttl=255 time=0.844 ms

PC6> ping 192.168.5.100 -c 3
84 bytes from 192.168.5.100 icmp_seq=1 ttl=63 time=2.140 ms
84 bytes from 192.168.5.100 icmp_seq=2 ttl=63 time=2.094 ms
84 bytes from 192.168.5.100 icmp_seq=3 ttl=63 time=0.957 ms
```

```
PC8> ping 192.168.5.1 -c 3
84 bytes from 192.168.5.1 icmp_seq=1 ttl=255 time=0.861 ms
84 bytes from 192.168.5.1 icmp_seq=2 ttl=255 time=0.697 ms
84 bytes from 192.168.5.1 icmp_seq=3 ttl=255 time=0.731 ms

PC8> ping 192.168.4.100 -c 3
84 bytes from 192.168.4.100 icmp_seq=1 ttl=63 time=2.429 ms
84 bytes from 192.168.4.100 icmp_seq=2 ttl=63 time=6.878 ms
84 bytes from 192.168.4.100 icmp_seq=3 ttl=63 time=1.463 ms
```

```
SW3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et2/0, Et2/1, Et2/2
                                                Et2/3, Et3/0, Et3/1, Et3/2
                                                Et3/3
40   VLAN0040                         active    Et0/1, Et0/2, Et0/3
50   VLAN0050                         active    Et1/0, Et1/1, Et1/2, Et1/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
SW3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
Vlan40                 192.168.4.1     YES manual up                    up
Vlan50                 192.168.5.1     YES manual up                    up
```

```
SW3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, Vlan40
L        192.168.4.1/32 is directly connected, Vlan40
      192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.5.0/24 is directly connected, Vlan50
L        192.168.5.1/32 is directly connected, Vlan50
```

IEEE 802.1Q

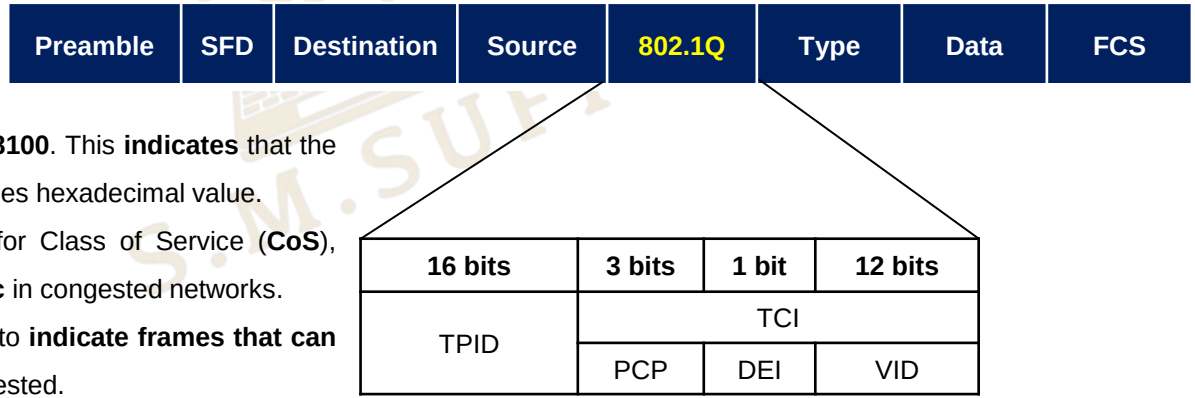
Switches will 'tag' all frames that they send over a trunk link. This allows the receiving switch to know which VLAN the frame belongs to.

- **Trunk ports** are **tagged ports**.
- **Access ports** are **untagged ports**.

The 802.1Q tag is inserted between the source and type/length fields of the Ethernet frame. The tag is **4 bytes (32 bits) in length**.

The tag consists of two main fields-

- Tag Protocol Identifier (**TPID**)
- Tag Control Information (**TCI**)



All the fields are discussed below:

- **TPID:** Always set to a value of **0x8100**. This **indicates** that the **frame is 802.1Q tagged**. '0x' defines hexadecimal value.
- **PCP:** Priority Code Point- used for Class of Service (**CoS**), which **prioritizes important traffic** in congested networks.
- **DEI:** Drop Eligible Indicator- used to **indicate frames that can be dropped** if the network is congested.
- **VID:** VLAN ID- **identifies the VLAN the frame belongs** to. It is **12 bits** in length = 4096 total VLANs (2^12), range 0 to 4095.

Back to Contents

Native VLAN

- 802.1Q has a feature called the **native VLAN**, ISL does not have this feature.
- A native VLAN is a special VLAN that is used to **carry untagged traffic on a trunk port**. Untagged traffic is traffic that does not belong to any specific VLAN.
- Native VLANs are **typically configured as VLAN 1 by default** on all trunk ports, however this can be manually configured on each trunk port.
- The switch **does not add an 802.1Q tag to frames** in the native VLAN. When a switch receives an untagged frame on a trunk port, it assumes the frame belongs to the native VLAN.
- **It is very important that the native VLAN matches**.
- For security purposes, it is best to change the native VLAN to an unused VLAN.

There are two methods of configuring the native VLAN on a router-

1. Using the command '***encapsulation dot1q <VLAN ID> native'*** on the router sub-interface.
2. Configure the IP address for the native VLAN on the router's physical interface, no encapsulation command is necessary.

Native VLAN

- Commands for configuring Native VLAN on trunk ports-

  'SW(config)# interface <interface no>'

  'SW(config-if)# switchport trunk encapsulation dot1q'

  'SW(config-if)# switchport mode trunk'

  'SW(config-if)# switchport trunk allowed vlan <VLAN IDs>'

  'SW(config-if)# switchport trunk native vlan <native VLAN ID>'

- Trunk information of SW2 after configuring native VLAN-

```
SW2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      20
Et3/3       on               802.1q         trunking      20

Port        Vlans allowed on trunk
Et0/0       10,20
Et3/3       10,20,30

Port        Vlans allowed and active in management domain
Et0/0       10,20
Et3/3       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       10,20
Et3/3       10,20,30
```

- We are making VLAN 20 as native VLAN in the topology.

  Configuring SW1 and SW2-

```
SW1(config)#interface e0/0
SW1(config-if)#switchport trunk ?
  allowed        Set allowed VLAN characteristics when interface is in trunking
                 mode
  encapsulation  Set trunking encapsulation when interface is in trunking mode
  native         Set trunking native characteristics when interface is in
                 trunking mode
  pruning        Set pruning VLAN characteristics when interface is in trunking
                 mode

SW1(config-if)#switchport trunk native vlan 20
SW1(config-if)#
*Nov  4 07:10:37.373: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discover
ed on Ethernet0/0 (20), with SW2 Ethernet0/0 (1).
```

```
SW2(config)#interface e0/0
SW2(config-if)#
*Nov  4 07:10:56.461: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discover
ed on Ethernet0/0 (1), with SW1 Ethernet0/0 (20).
SW2(config-if)#switchport trunk native vlan 20
SW2(config-if)#exit
SW2(config)#interface e3/3
SW2(config-if)#switchport trunk native vlan 20
```

Native VLAN

- Commands for configuring ROAS for native vlan-

  'RTR(config)# interface <interface no>'

  'RTR(config-if)# ip address <gateway ip of native VLAN>'

```
R1(config)#no interface e3/3.20
% Not all config may be removed and may reappear after reactivating the sub-inte
rface
R1(config)#interface e3/3
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
```

- OR,

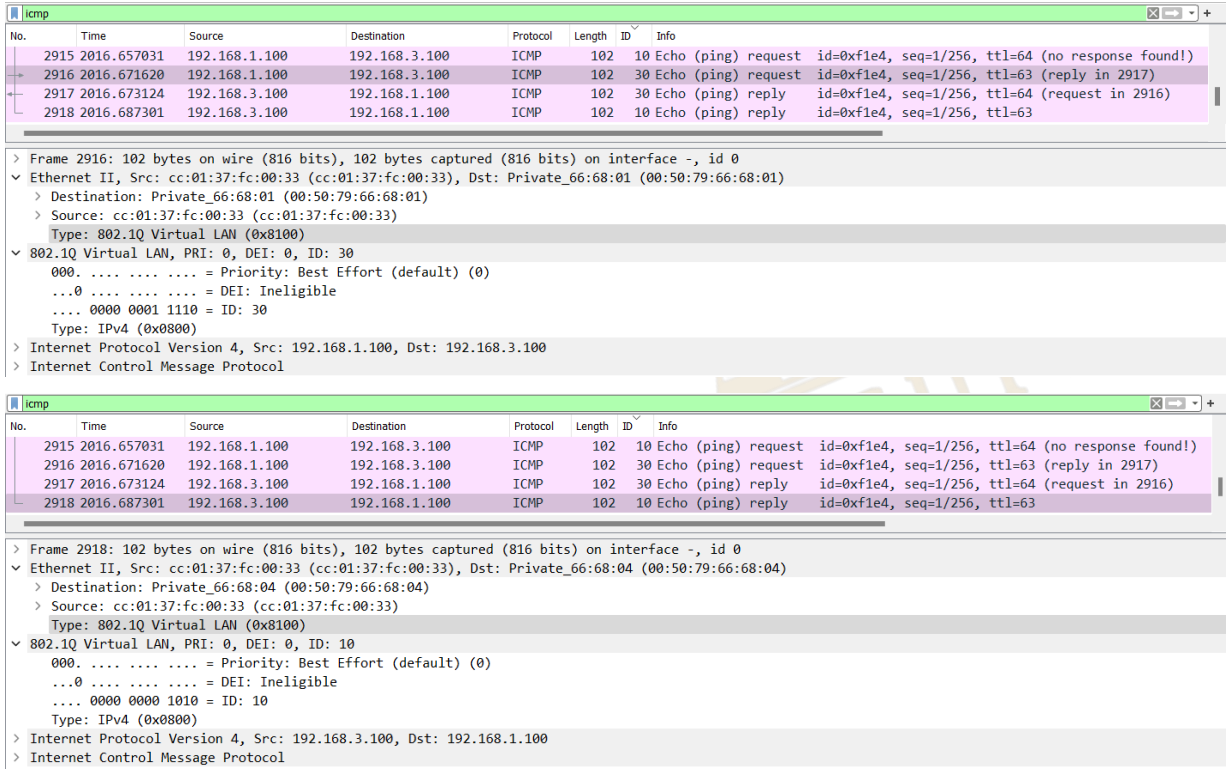
  'RTR(config)# interface <interface no>'

  'RTR(config-if)# encapsulation dot1q <native VLAN ID> native'

```
R1(config)#interface e3/3
R1(config-if)#no ip address
R1(config-if)#interface e3/3.20
R1(config-subif)#encapsulation dot1q 20 native
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#no shutdown
```

Back to Contents

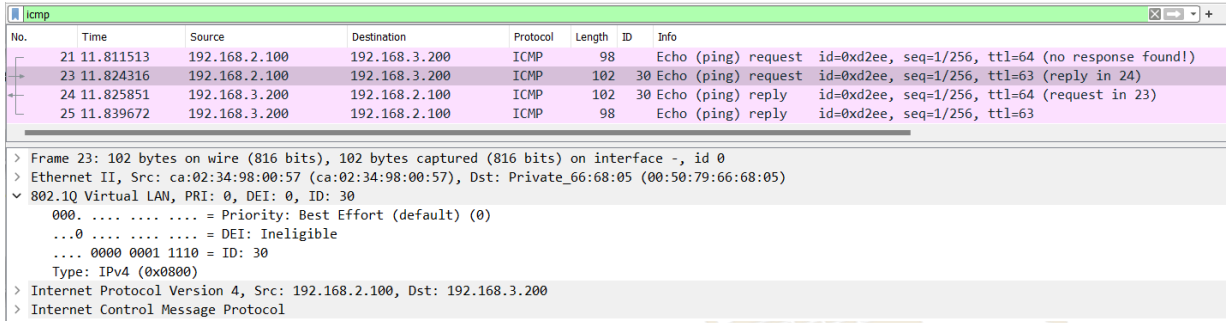
Native VLAN

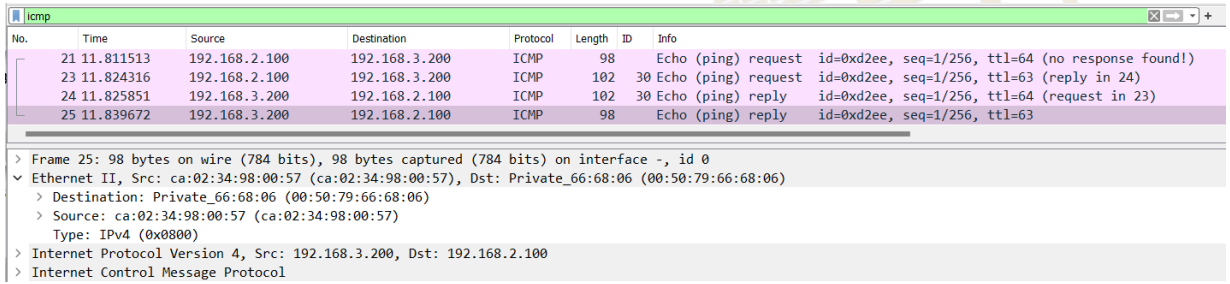


- **ICMP packet captured in Wireshark** of PC1 from VLAN 10 pinging PC4 from VLAN 30
- Focus on 802.1Q tag fields

Back to Contents

Native VLAN





- **ICMP packet captured in Wireshark** of PC3 from Native VLAN 20 pinging PC5 from VLAN 30
- Focus on 802.1Q tag fields

Back to Contents

DTP (Dynamic Trunking Protocol)

Dynamic Trunking Protocol (**DTP**) is a **Cisco proprietary** protocol that allows switches to **negotiate trunking** between each other. DTP is used to automatically configure trunk ports on switches. DTP works by exchanging messages between switches to determine the trunking mode of each port. The DTP messages contain information about the following:

- The desired **trunking mode** (**trunk or access**)
- The supported **trunking encapsulation types** (**IEEE 802.1q or ISL**)

When two switches receive DTP messages from each other, they will negotiate the trunking mode and encapsulation type. If the switches cannot agree on a trunking mode or encapsulation type, the ports will be configured as access ports. **DTP is enabled by default** on all Cisco switch interfaces.

There are **two modes** of DTP-

1. **Auto:** A switchport in **dynamic auto** mode **will not actively try to form a trunk** with other Cisco switches, however it will form a trunk if the switch connected to it is actively trying to form a trunk. It will form a trunk with a switchport in **trunk/dynamic desirable** modes.
2. **Desirable:** A switchport in **dynamic desirable** mode **will actively try to form a trunk** with other Cisco switches. It will form a trunk if connected to another switchport in **trunk/dynamic desirable/dynamic auto** modes.

DTP (Dynamic Trunking Protocol)

- Commands of DTP in switches-

  'SW(config)# interface <interface no>'

  'SW(config-if)# switchport mode dynamic <auto/desirable>'

- Commands to check DTP switchport mode-

  'SW# show interface <interface no> switchport'

Configuring DTP mode of SW1 to desirable-

```
SW1(config)#interface e0/0
SW1(config-if)#switchport mode ?
  access        Set trunking mode to ACCESS unconditionally
  dot1q-tunnel  set trunking mode to TUNNEL unconditionally
  dynamic       Set trunking mode to dynamically negotiate access or trunk mode
  private-vlan  Set private-vlan mode
  trunk         Set trunking mode to TRUNK unconditionally

SW1(config-if)#switchport mode dynamic ?
  auto       Set trunking mode dynamic negotiation parameter to AUTO
  desirable  Set trunking mode dynamic negotiation parameter to DESIRABLE

SW1(config-if)#switchport mode dynamic desirable
```

```
SW1#show interface e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
```

Configuring DTP mode of SW2 to auto-

```
SW2(config)#interface e0/0
SW2(config-if)#switchport mode dynamic auto
```

```
SW2#show interface e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
```

There are also **'dynamic access'** ports, in which a server automatically assigns the VLAN depending on the MAC address of the connected device.

'static access' means as access port that belongs to a single VLAN that doesn't change (unless we configure a different VLAN).

What happens if a manually configured TRUNK is connected to a manually configured ACCESS port?

Since both are manually configured, they are forced to operate mismatched in trunk and access modes. This configuration does not work and will result in an error.

DTP (Dynamic Trunking Protocol)

- The following chart summarizes the resulting operational mode given different administrative modes-

SW1 Administrative Mode	SW2 Administrative Mode	Operational Mode
Trunk	Trunk	Trunk
Access	Access	Access
Trunk	Access	X
Dynamic Desirable	Trunk	Trunk
Dynamic Desirable	Dynamic Desirable	Trunk
Dynamic Desirable	Dynamic Auto	Trunk
Dynamic Desirable	Access	Access
Dynamic Auto	Trunk	Trunk
Dynamic Auto	Dynamic Desirable	Trunk
Dynamic Auto	Dynamic Auto	X
Dynamic Auto	Access	Access

- DTP will not form a trunk with a router, end devices like PC, etc.
- On older switches, **switchport mode dynamic desirable** is the default administrative mode.
- On newer switches, **switchport mode dynamic auto** is the default administrative mode.
- DTP negotiation on an interface can be disabled with the command- **'switchport nonegotiate'**

DTP (Dynamic Trunking Protocol)

- Switches that support both **802.1Q** and **ISL** trunk encapsulations ca use DTP to negotiate the encapsulation they use.
- This negotiation is enabled by default. Command to enable switchport trunk encapsulation mode-

  'SW(config)# interface <interface no>'

  'SW(config-if)# switchport trunk encapsulation <dot1q/isl/negotiate>'

- **ISL** is favored over **802.1Q**, so if both switches support ISL, it will be selected in auto negotiation-

```
SW1(config)#interface e0/0
SW1(config-if)#switchport mode dynamic desirable
SW1(config-if)#do show interface e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
```

```
SW2(config)#interface e0/0
SW2(config-if)#switchport mode dynamic auto
SW2(config-if)#do show interface e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
Negotiation of Trunking: On
```

- If one switch is configured as **802.1Q**, the other switch will also select **802.1Q** in auto negotiation-

```
SW1(config)#interface e0/0
SW1(config-if)#switchport mode dynamic desirable
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#do show interface e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

```
SW2(config)#interface e0/0
SW2(config-if)#switchport mode dynamic auto
SW2(config-if)#do show interface e0/0 switchport
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

Back to Contents

VTP (VLAN Trunking Protocol)

- VLAN Trunking Protocol (**VTP**) is a **Cisco proprietary** protocol that propagates the definition of Virtual Local Area Networks (VLANs) on the whole local area network.
- It allows network administrators to **configure**, **update**, and **maintain VLAN information** consistently across multiple Cisco switches, making network management more efficient.
- VTP **carries VLAN** information to all switches **in a VTP domain**.
- VTP **advertisements** can **be sent over 802.1Q**, and **ISL trunks**.
- It is designed for large networks with many VLANs, so that we don't have to configure each VLAN on every switch.
- There are **three VTP versions**- 1, 2 and 3.
- VTPv1 and VTPv2 do not support the extended VLAN range (1006-4094). Only VTPv3 supports them.
- There are **three VTP modes**- VTP **server**, VTP **client** and VTP **transparent**.
- Cisco switches operate in **VTP server mode by default**.
- If a switch with no VTP domain (Null) receives a VTP advertisement with a VTP domain name, it will automatically join that VTP domain.
- If a switch receives a VTP advertisement in the same VTP domain with **a higher revision number**, it will update it's VLAN database to match.
- ***One danger of VTP:** It we connect an old switch with a higher revision number to our network (and the VTP domain name matches), all switches in the domain will sync their VLAN database to that switch. That's why it is recommended to turn off VTP in switches and manually add corresponding VLANs on the switches.

Back to Contents

VTP (VLAN Trunking Protocol)

There are three VTP modes-

1. **VTP Server: Can add/modify/delete VLANs**. **Store the VLAN database** in non-volatile RAN (NVRAM). Will **increase the revision number** everytime a VLAN is added/modified/deleted. Will **advertise the latest version** of the VLAN database on trunk interfaces, and the **VTP clients will synchronize** their VLAN database to it. VTP servers **also functions as VTP clients**. Therefore, a VTP server will synchronize to another VTP server with a higher revision number.
2. **VTP Client: Cannot add/modify/delete VLANs**. **Do not store the VLAN database** in NVRAM (in VTPv3, they do). Will **synchronize** their VLAN database to the server with the **highest revision number** in their **VTP domain**. Will advertise their VLAN database, and forward VTP advertisements to other clients over trunk ports.
3. **VTP Transparent:** A VTP transparent switch is a switch that **does not participate in VTP**. VTP transparent switches send VTP advertisements to other switches but do not learn about VLANs from VTP advertisements. They act as "**pass-through**" switches, **forwarding VTP advertisements but not processing them**. They maintain their own VLAN database in NVRAM. They can add/modify/delete VLANs, but won't be advertised to other switches.

How to reset VTP on a switch-

- Changing the CTP domain to an unused domain will reset the revision number to 0.
- Changing the VTP mode to transparent will also reset the revision number to 0.

VTP (VLAN Trunking Protocol)

- Command to check VTP status-

  'SW# show vtp status'

- Command to set VTP modes-

  'SW(config)# vtp mode <client/off/server/transparent>'

- Command to create VTP domain-

  'SW(config)# vtp domain <VTP domain name>'

- Command to change VTP versions-

  'SW(config)# vtp version <1/2/3>'

```
SW2(config)#vtp ?
  domain      Set the name of the VTP administrative domain.
  file        Configure IFS filesystem file where VTP configuration is stored.
  interface   Configure interface as the preferred source for the VTP IP updater
              address.
  mode        Configure VTP device mode
  password    Set the password for the VTP administrative domain
  pruning     Set the administrative domain to permit pruning
  version     Set the administrative domain to VTP version

SW2(config)#vtp domain gns3lab.com
Changing VTP domain name from NULL to gns3lab.com
```

```
SW1(config)#vtp mode ?
  client       Set the device to client mode.
  off          Set the device to off mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.

SW1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
```

```
SW2#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : gns3lab.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 11-5-23 04:17:02
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 9
MD5 digest                      : 0xE8 0xFD 0x8D 0xA7 0xCC 0x8E 0x1C 0xAA
                                  0x37 0x3C 0x74 0xF3 0x01 0x96 0xA5 0xAD
```

```
SW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : gns3lab.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 11-5-23 04:17:02

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
Configuration Revision          : 9
MD5 digest                      : 0xE8 0xFD 0x8D 0xA7 0xCC 0x8E 0x1C 0xAA
                                  0x37 0x3C 0x74 0xF3 0x01 0x96 0xA5 0xAD
```

Thank You

Feel free to reach out to me for any **suggestions** or **feedback** via **LinkedIn** or **Mail**

 www.github.com/smsufi

 www.linkedin.com/in/smsufi

 safwanm.cse@gmail.com