VLANs
&
Trunks

Overview

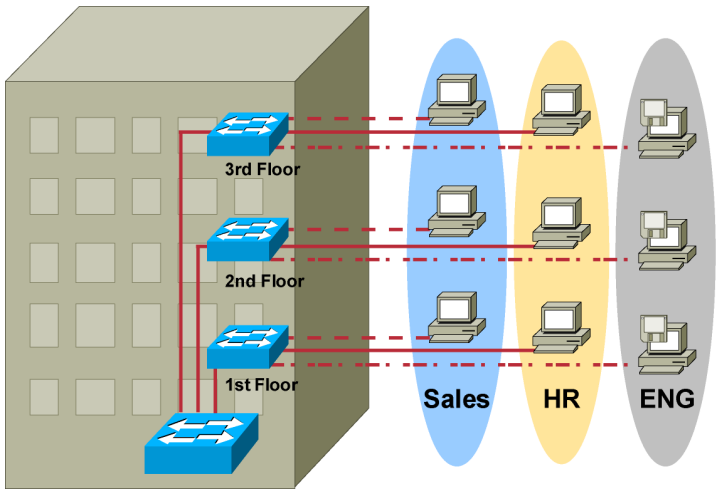
- A full layer 2 only switched network is referred to as a single broadcast domain, so network must be subdivided into VLANs
- By definition a VLAN is a single broadcast domain, VLAN is characterised by:

-They can allow load balancing with multiple parallel paths, so enhancing bandwidth utilization

-They enhance network security

-They confine broadcasts, so introducing better broadcast control

-They can span multiple switches (no physical boundaries), VLAN can group users based on their business requirements (business departments) independent of any physical locations



- Segmentation
- Flexibility
- Security

A VLAN = A Broadcast Domain = Logical Network (Subnet)

But using VLANs will cause the following:
- It will not simplify the network.
- It will not eliminate the need of L3 routing

Deploying VLANs

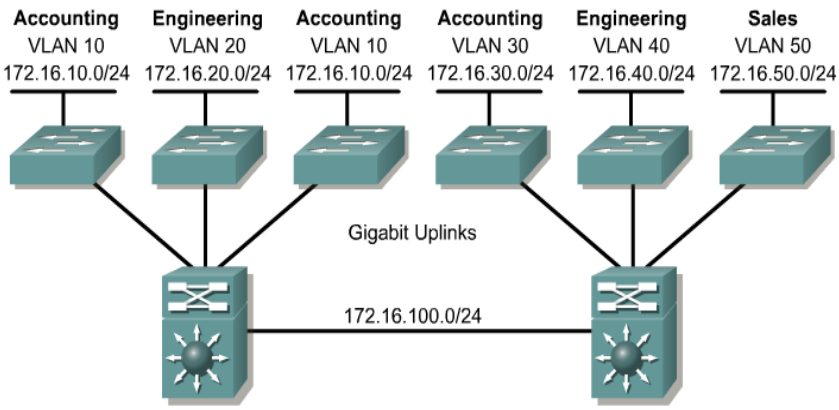
- The number of VLANS will be dependent on network requirement
- Cisco recommend the VLAN-IP relation to be one- to-one in order of isolating VLANs broadcasts & ability to form inter-VLAN-routing
- VLANs could be implemented using two basic methods

1) Local VLANs

2) End to End VLAN

1)Local VLAN

- It is called geographic VLANs, keeping the VLAN within a switch block
- Local VLANs are created based on geographic or physical locations
- Also Local VLANs design obey 20/80 rule



- VLANs based on physical location
- VLANs dedicated to each access layer switch cluster
- Accounting users connected to different layer 3 switches are on different VLANs, i.e. Accounting VLAN 10 and VLAN 30

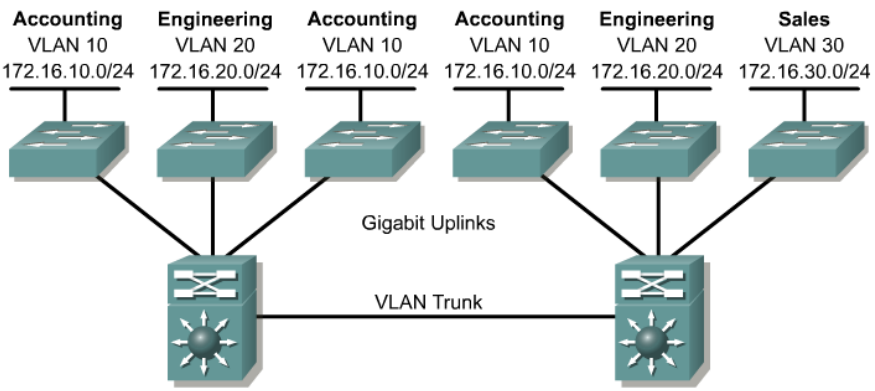
• Here are some local VLAN characteristics and user guidelines:
- Local VLANs should be created with physical boundaries in mind rather than the job functions of the users on the end devices.
- Traffic from a local VLAN is routed to reach destinations on other networks.
- A single VLAN does not extend beyond the Building Distribution submodule.

2)End to End VLAN

- It is called Campus-wide VLAN
- Users are assigned to VLANs regardless of their physical location, they are designed regarding their function (same VLAN are distributed on among different switch blocks)
- End to end VLAN disobey the 80/20 rule, where all traffic within a single VLAN could cross the core obeying 20/80 rule
- But end to end VLAN could help extending broadcast storms & it is difficult to maintain troubleshooting
- End to end VLAN deployment is not recommended by Cisco.

- An end-to-end VLAN has these characteristics:

  - The VLAN is geographically dispersed throughout the network.
  - Users are grouped into the VLAN regardless of physical location.
  - As a user moves throughout a campus, the VLAN membership of that user remains the same.
  - Users are typically associated with a given VLAN for network management reasons.
  - All devices on a given VLAN typically have addresses on the same IP subnet.



- VLANs based on functionality
- "VLAN everywhere" model
- VLANs with the same VLAN ID, i.e. Accounting VLAN 10, can be anywhere in the network

VLAN membership

1) Static VLAN membership

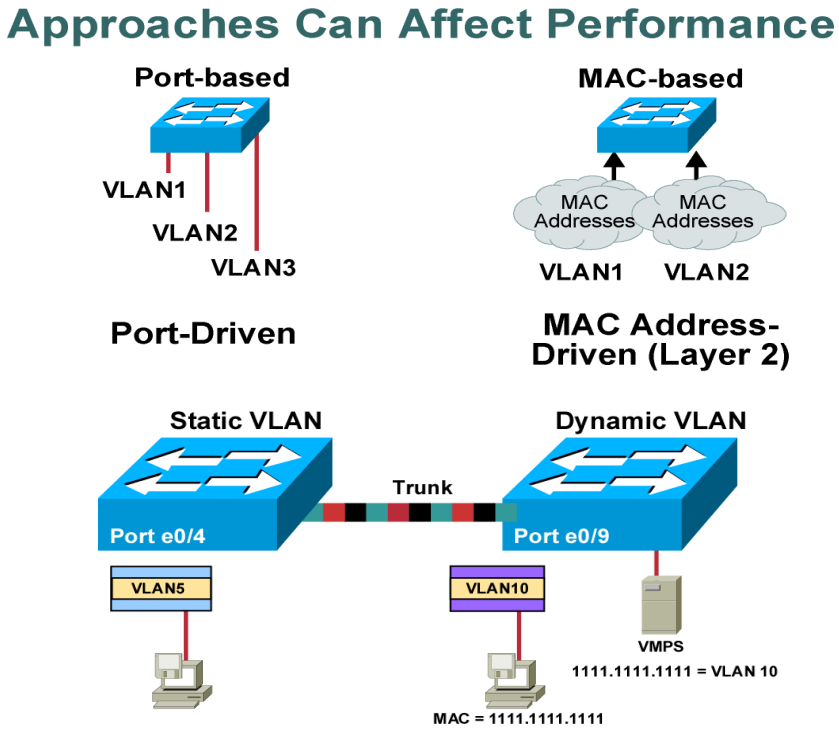
“Port based VLAN“

VLAN number is assigned to specific switch port, each port gets a PVID (Port VLAN ID)

2)Dynamic VLAN membership

"MAC based VLAN"

When a host is connected to a switch port, the switch must query a database to establish VLAN membership, so as to assign a MAC address of a user to a certain VLAN, a network administrator must assign the users MAC addresses to a VLAN in the database of VMPS (VLAN Membership Policy Server), which could be catalyst 6500/5000 or external server.



Types of Switch ports

- **Access-Link:**

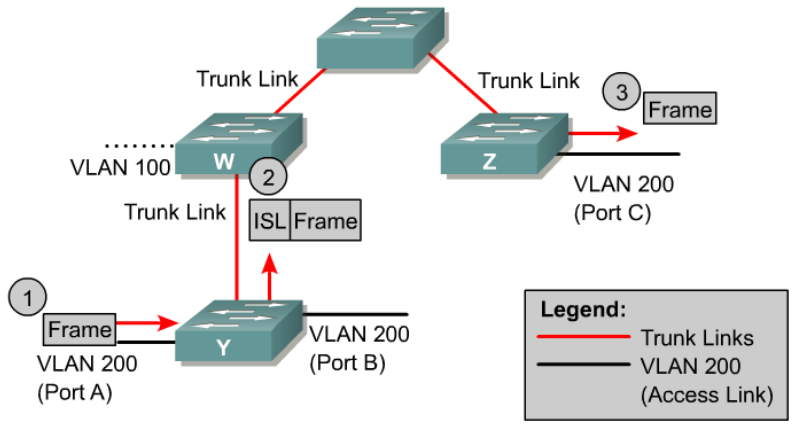
-Switch port that is member in only one VLAN (native VLAN by default)

-This port actually connect a switch to host

- **Trunk-Link:**

-Switch port that is member in all VLANs by default, so traffic from all VLANs can use a trunk link

-It is mainly used to connect two switches together or switch and a router



Configuring VLANs

To configure VLANs there are three requirements:

1- Create VLAN

2- Optionally name the VLAN

3- Activate VLAN (assign VLAN to switchport)

Method 1

```
#configure terminal
(config)#vlan <id>
(config-vlan)#name <vlan name>
```

```
Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
Switch(config)#
```

Deleting VLAN

```
Switch#configure terminal
Switch(config)#no vlan 3
Switch(config)#end
```

Method 2: old IOS methods

Alternatively, VLANs can be created and managed using VLAN database mode.

```
#vlan database
(vlan)# vlan vlan# [name vlan-name]
(vlan)#apply ,or (vlan)#exit
```

```
sw_2950#vlan database
sw_2950(vlan)#vlan 9 name sales
sw_2950(vlan)#exit
APPLY completed.
Exiting....
 sw_2950#
```

Deleting VLAN

```
Switch#vlan database
Switch(vlan)#no vlan 3
VLAN 3 deleted:
Switch(vlan)#exit
APPLY completed.
Exiting....
```

VLAN database mode is session oriented. When you add, delete, or modify VLAN parameters, the changes are not applied until you enter the apply or exit command. You can also exit VLAN database mode without applying the changes by entering the abort command.

From this mode, you can add, delete, and modify VLAN configurations for VLANs in the range 1 to 1005.

Note: This mode has been deprecated and will be removed in some future release.

To activate a VLAN

(config)#interface ____

(config-if)#switchort mode access

(config-if)#switchport access vlan <vlan id>

```
(config)#interface Fastethernet 0/3
(config-if)#switchort mode access
(config-if)#switchport access vlan 52
```

Troubleshooting VLANs:

```
Switch#show vlan [id | name] [vlan_num | vlan_name]
```

```
#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
-
1    default                          active    Fa0/1, Fa0/2, Fa0/5, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/11, Fa0/12
                                                Gi0/1, Gi0/2
2    VLAN0002                         active
52   Sales                            active    Fa0/3
…

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
52   enet  100052     1500  -      -      -        -    -        0      0
…
```

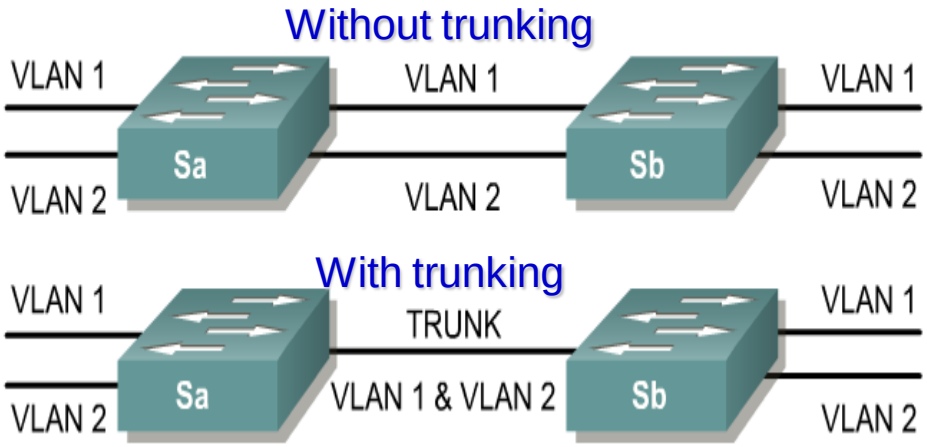
```
#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -----------------
1    default                           active    Fa0/1, Fa0/2, Fa0/5, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/11, Fa0/12
                                                 Gi0/1, Gi0/2

2       VLAN0002                          active
52      Sales                             active    Fa0/3

1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

VLAN Trunks

- To connect switch port to another switch port or a router while deploying VLANs we need a method for VLAN Inter-switch communication where a VLAN can span multiple switches
- VLAN trunks will help for communication between same VLAN members that exist on different physical switches



VLAN frame identifier

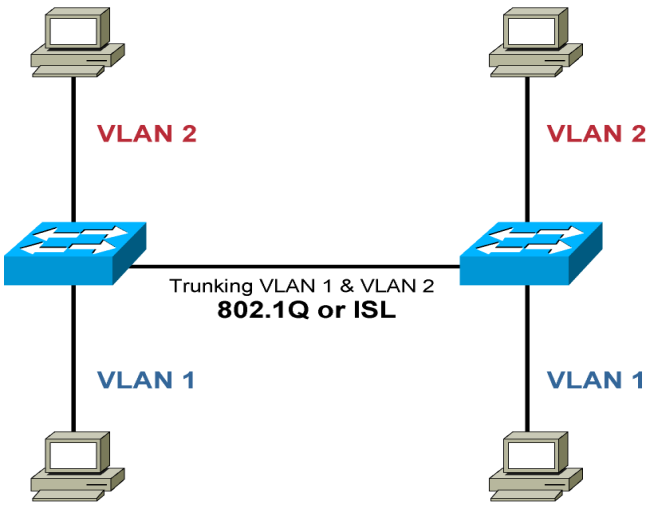
- Each frame originated from a PC and received on a switch port must have a VLAN id before retransmitted on a trunk link, this is called trunk VLAN tagging, this must be done to assure VLAN inter-switch communication.
- VLAN tagging types:

1-ISL (Inter Switch Link) for Ethernet

2-IEEE 802.1q (dot1q) for Ethernet

3-Cisco extension for 802.10 for FDDI

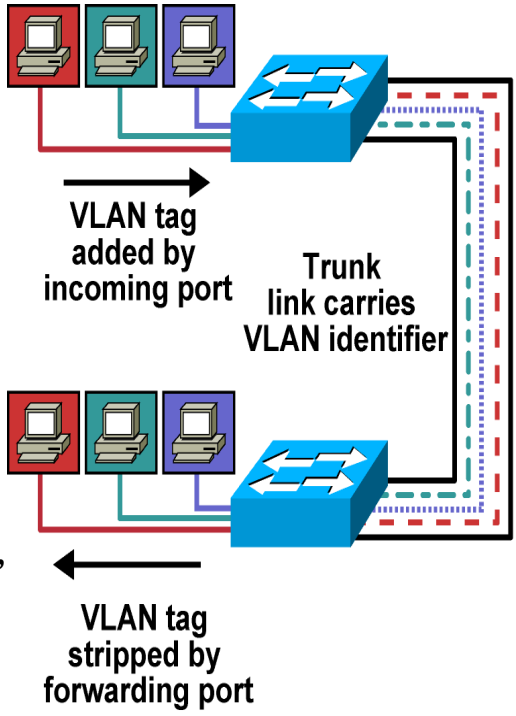
4-LANE (LAN Emulation) for ATM

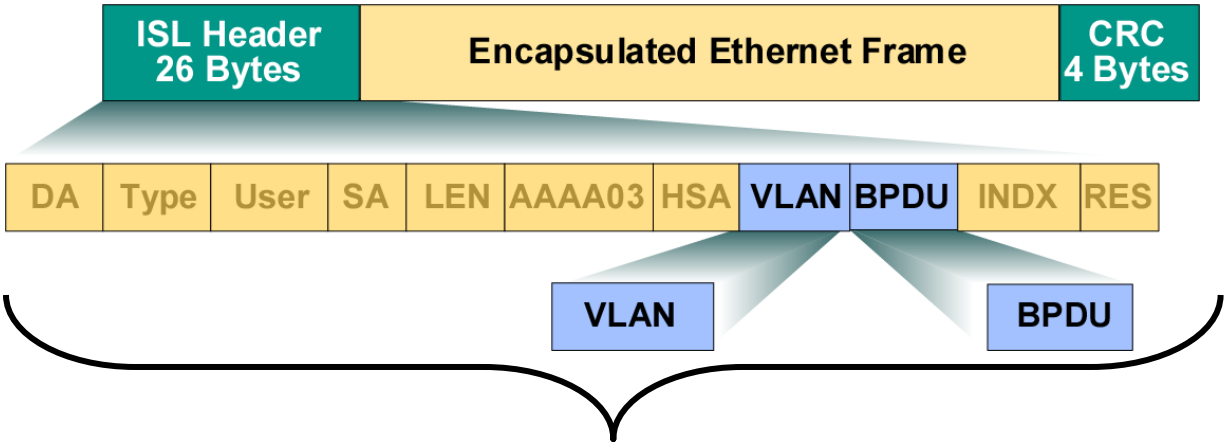


- Cisco implements VLAN tagging using ASICs.

1)ISL

- It a Cisco proprietary VLAN tagging protocol, but it is no longer supported by Cisco new edge switches
- It is also called double tagging, because it encapsulates the original frame with new header (ISL header 26byte) & new trailer (ISL trailer 4byte new CRC)
- The ISL header contains a 10 bit for VLAN id, which support VLANs from 0-1023, where used VLANs are 1-1005
- Ethernet can use 1-1001 and 1002-1005 are reserved for token ring & FDDI



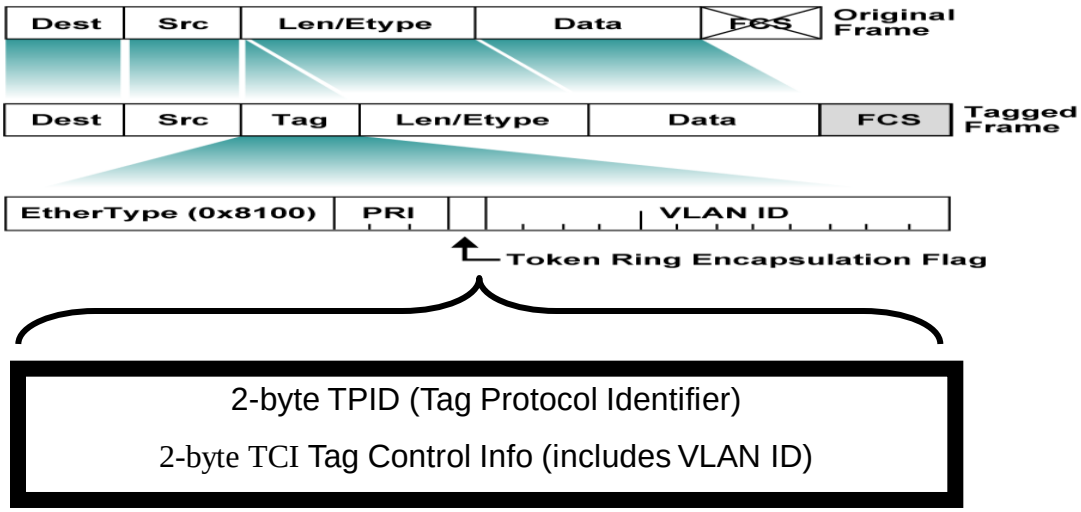


Standard NIC cards and networking devices don't understand this giant frame. A Cisco switch must remove this encapsulation before sending the frame out on an access link.

- ISL is now supported only on core switches, but Cisco Catalyst 2950 & 2960 access switches support only dot1q.

2)dot1q

- It is called single tagging, where 4 byte of dot1q tag is inserted after the source MAC of the frame and before the length field of the frame
- The 4 bytes specify the following:



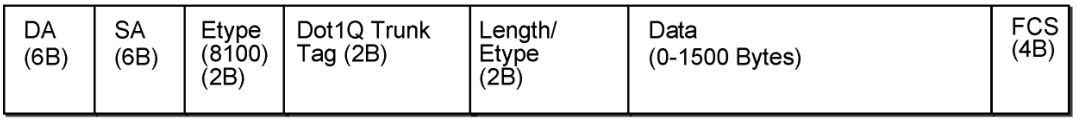
- 2 bytes for indication of type of encapsulated data
- 12 bit for VLAN tag, which give VLAN ranges from 0-4095, where 0,1,1002-1005 & 4095 are reserved.
- 3 bits COS (Class Of Service), which indicates the priority of the frame, they are called the 802.1q/802.1p bits
- 1 bit for CFI (Canonical Frame Indicator), flag which indicates whether the frame is Ethernet or Token ring & FDDI

VLAN Ranges and Mappings

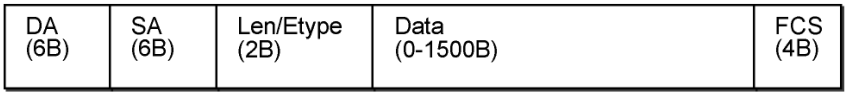
VLAN Range	Range	Usage
0, 4095	Reserved	For system use only
1	Normal	Cisco default
2-1001	Normal	For Ethernet VLANs
1002-1005	Normal	Cisco defaults for FDDI and Token Ring
1025-4094	Extended	For Ethernet VLANs only

- Dot1q also introduced the concept of native VLAN on a trunk, where frames belonging to this VLAN are not tagged with any VLAN id, using this feature 802.1q tagging device & non-802.1q devices can co-exist on a 802.1q trunk.
- Native VLAN is by default VLAN 1, which is also called the management VLAN (management VLAN is the VLAN that carries frames from all protocols (CDP, VTP, DTP,….)), the native VLAN can be changed by configuration.

802.1Q Tagged Layer 2 Frame from an 802.1Q Trunk Port



Untagged and Unencapsulated Layer 2 Frame from an Access Port



- IEEE 802.3ac standard is used to extended MTU of Ethernet frame to 1522 byte

NIC cards and networking devices can understand this "baby giant" frame (1522 bytes). However, a Cisco switch must remove this encapsulation before sending the frame out on an access link.

DTP
(Dynamic Trunk Protocol)

- Cisco proprietary protocol, that is used to automatically negotiate a common trunking mode (negotiate whether link will be access or trunk) between two switches, also negotiation of trunk encapsulation type can be done, DTP negotiation is made periodically every 30 sec.
- A router can not participate in DTP, so if a switch port is connected to a router, DTP must be disabled & switch port must be manually configured.
- Note: DTP is negotiated between switches working in the same VTP domain or if one of these domains is null domain, so if switches are in different domains, you must set trunk configuration to "on" or "nonegotiate", this setting will force the trunk to be established.

- **DTP modes:**

Mode	Function
access	Unconditionally sets a switch port to access mode, regardless of other DTP functions
trunk	Sets the switch port to unconditional trunking mode and negotiates to become a trunk link, regardless of neighbor interface mode
nonegotiate	Specifies that DTP negotiation packets are not sent on the Layer 2 interface
dynamic desirable	Sets the switch port to actively send and respond to DTP negotiation frames. Default for Ethernet
dynamic auto	Sets the switch port to respond but not to actively send DTP negotiation frames

Configuring trunking

(config)#interface <_>

(config-if)#switchport mode {access/trunk/dynamic desirable/dynamic auto/nonegotiate}

-access: only in one VLAN, no negotiation (no DTP messages).

-trunk: permanently trunk & generate DTP messages.

-dynamic desirable: (default), actively (sending messages) attempts to be trunk.

-dynamic auto: only if far end desire a trunk, it will turn to trunk which means it is passively (does not initiate messages) attempts to be trunk.

-nonegotiate: disables DTP & force permanent trunk.

(config-if)#switchport trunk encapsulation {isl/dot1q/negotiate}

default is negotiate, ISL is favoured if both exist on negotiating switches.

Switchport Mode Interactions

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

To identify native VLAN

(config-if)#switchport trunk native vlan <vlan id>

default is VLAN 1, this is used only with dot1q & trunking mode

- **To specify allowed VLANs on trunk:**

(config-if)#switchport trunk allowed vlan {<vlan list> / all / {add/except/remove} <vlan list> }

Add: add VLAN list to an existing pre-configured list

Except: means, all except a certain VLAN list

Remove: remove VLANs from existing VLAN list

By default all VLANs exist ion the trunk link.

Trunking configuration example:

```
Switch(config)#interface fastethernet 5/8
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 1,15,11,1002-1005
Switch(config-if)#switchport mode trunk
Switch(config-if)#no shutdown
```

Troubleshooting

#sh dtp

#sh interface <_> trunk

#sh interface <_> switchport

#sh interface <_> capabilities

#sh run interface <_>

#sh vlan

#sh vlan brief

```
ASW11#show dtp interface fa0/1

DTP information for FastEthernet0/1:

  TOS/TAS/TNS:                          TRUNK/DESIRABLE/TRUNK

  TOT/TAT/TNT:                          802.1Q/802.1Q/802.1Q

  Neighbor address 1:                   001646FA9B01

  Neighbor address 2:                   000000000000

  Hello timer expiration (sec/state):   17/RUNNING

  Access timer expiration (sec/state):  287/RUNNING
```

```
Switch#show interfaces fastethernet 2/1 trunk

     Port        Mode         Encapsulation  Status        Native VLAN
     Fa2/1       desirable    isl            trunking      1

     Port        VLANs allowed on trunk
     Fa2/1       1-1005

     Port        VLANs allowed and active in management domain
     Fa2/1       1-2,1002-1005

     Port        VLANs in spanning tree forwarding state and not pruned
     Fa2/1       1-2,1002-1005
```

```
Switch#show interfaces gigabitEthernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

. . .
```

Troubleshooting VLAN Issues

Configuration problems can arise when user traffic must traverse several switches. The following sections list some common configuration errors. But before you begin troubleshooting, create a plan. Check the implementation plan for any changes recently made, and determine likely problem areas.

Troubleshooting User Connectivity

User connectivity can be affected by several things:

- **Physical connectivity:** Make sure the cable, network adapter, and switch port are good. Check the port's link LED.
- **Switch configuration**: If you see FCS errors or late collisions, suspect a duplex mismatch. Check configured speed on both sides of the link. Make sure the port is enabled and set as an access port.
- **VLAN configuration:** Make sure the hosts are in the correct VLAN.
- **Allowed VLANs:** Make sure that the user VLAN is allowed on all appropriate trunk links.

Troubleshooting Trunking

When troubleshooting trunking, make sure that physical layer connectivity is present before moving on to search for configuration problems such as

- Are both sides of the link in the correct trunking mode?
- Is the same trunk encapsulation on both sides?
- If 802.1Q, is the same native VLAN on both sides? Look for CDP messages warning of this error.
- Are the same VLANs permitted on both sides?
- Is a link trunking that should not be?