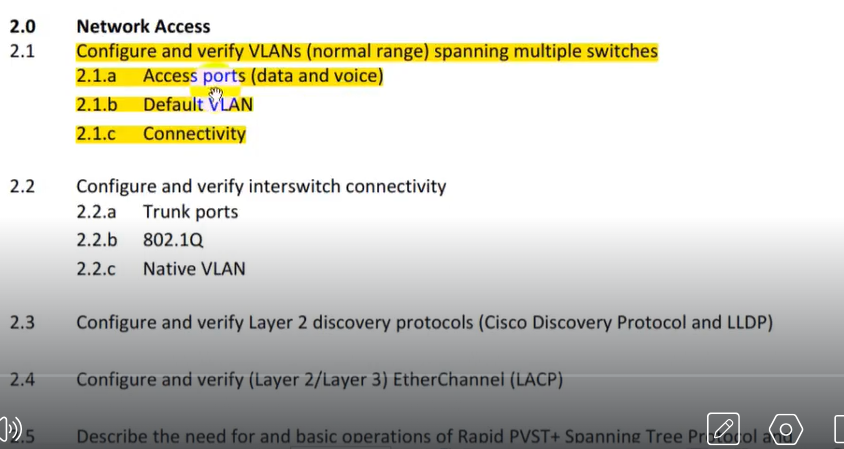
Configure and verify VLAN (virtual local area network)



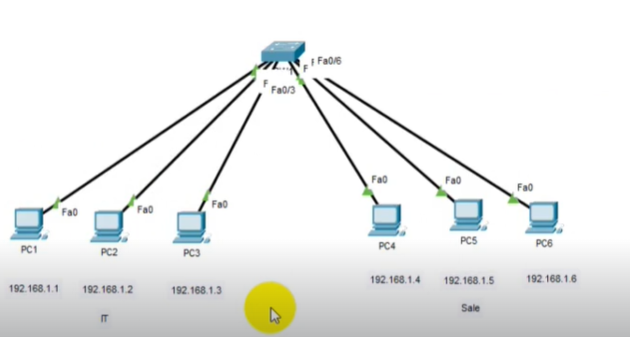
VLAN (Virtual Local Area Network):  
Dividing a network in sub-network due broadcast issue in switch is called Vlan.

**VLAN**

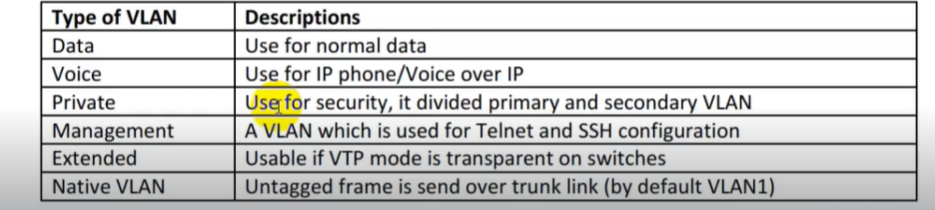
* VLAN stands for Virtual Local Area Network.
* VLAN is a logical grouping of networking devices.
* Break large broadcast domain in smaller broadcast domains.
* VLANs divide the switch into different LAN segments.
* Consider VLAN as a subnet.
* Two different subnets cannot communicate with each other without router.
* Two different VLANs also requires router to communicate.
* VLAN used in Switches and it operates at Layer 2,
* By default, in every switch there is five VLANs.
* VLAN 1 is the default VLAN for every switch port.
* The standard VAN range is from VLAN 1 to 1005.
* The Extended VLAN range is from VLAN 1006 — 4094.
* 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.

**VLAN Analogy**

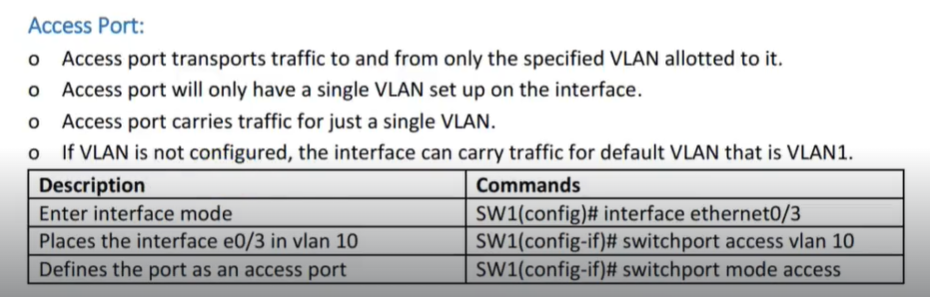
* Partition hard disks on a computer into several logical partitions.
* The main purpose of hard disks partition is to organize the disk space.
* It ensures that corruption of partition does not affect another partition.
* Like have a big room separated by partitions to make them two houses for use.
* It is as big office separated by partitions makes in many offices.
* It is like a big classroom, divide into many section such as Class A. B, C etc.



* A single network is divided into 2 local networks it happened through Vlan.
* A single switch handles two lan of same network.

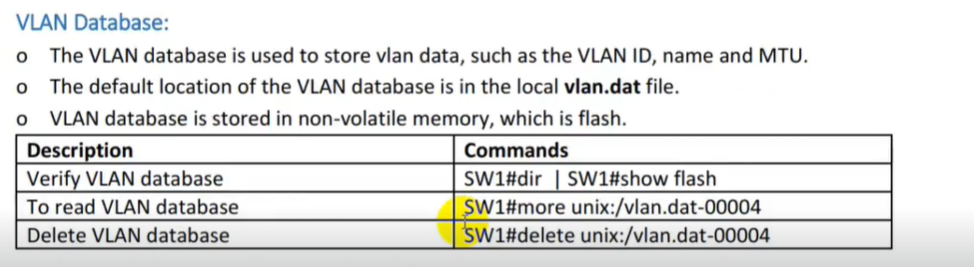
**Types of VLAN:**

**Access Port**

* Access port transports traffic to and from only the specified VLAN allotted to it.
* Access port will only have a single VLAN set up on the interface.
* Access port carries traffic for just a single VLAN.
* If VLAN is not configured, the interface can carry traffic for default VLAN that is VLANI. 
* Accessport is port that can be assign to a single vlan.

**VLAN Database**

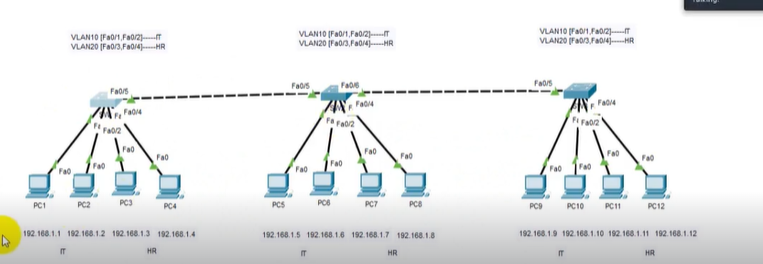
* The VLAN database IS used to store vlan data, such as eV NID, name an
* The default location of the VLAN database is in the local vlan.dat file.
* VLAN database is stored in non-volatile memory, which is flash.

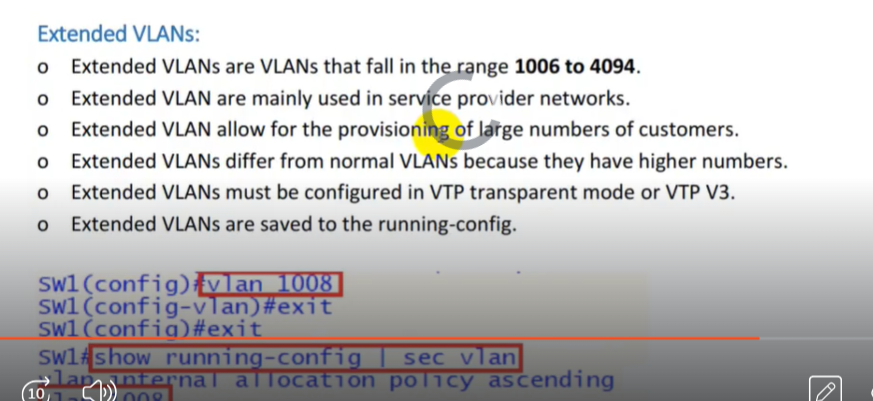


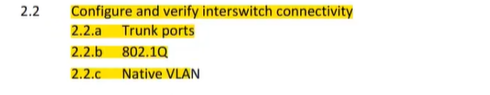
**Normal VLAN**

* Normal VLANs range are from VLANs 1 to VLAN 1005.
* Normal range VLANs can be configured in both database configurations mode & global.
* Normal VLANs are stored in vlan.dat file in Flash memory.
* VTP versions 1 and 2 can advertise normal range VLANs only.

**Extended VLANs:**

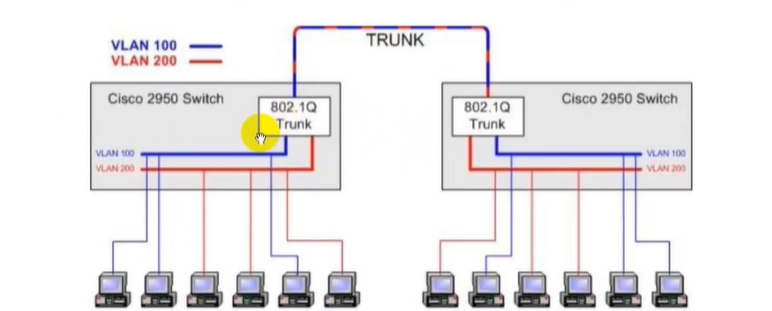
* Extended VLANs are VLANs that fall in the
* range 1006 to 4094
* Extended VLAN are mainly used in se e provider networks.
* Extended VLAN allow for the provision of large numbers of customers.
* Extended VLANs differ from normal VLANs because they have higher numbers.
* Extended VLANs must be configured in VTP transparent mode or VTP V3.
* Extended VLANs are saved to the running-config.

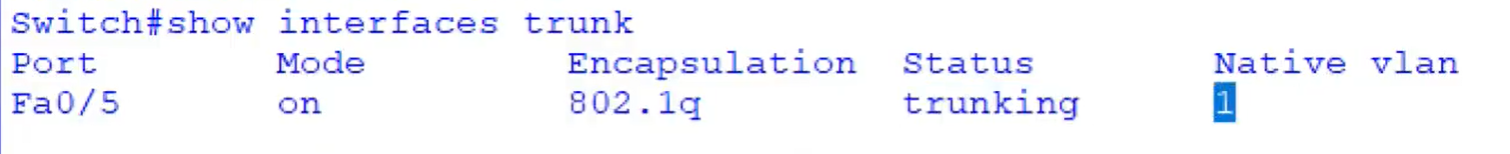




**Trunk Port**

* A Trunk port is a port that is assigned to carry traffic for all the VLANs.
* In order to pass the traffic from VLANs on one switch to another switch.
* We need to implement what is called a 'trunk' port or trunk interface.
* That are accessible by a specific switch, a process known as trunking.
* It mark frames with unique identifying tags either 802.1Q/dot.1Q tags or ISL (By cisco no longer used) tags.
* Trunk Port or interface mark the traffic When move between cisco switches.
* Therefore, every single frame can be directed to its designated VLAN.
* Trunk ports are designed for interconnecting and allow one or more VLANs.
* Trunk ports are designed for interconnecting switches and support all VLANs.
* Trunk switch ports belongs to and carry the traffic of more than one VLAN.
* Each port on a switch can be configured as either an access or a trunk port.

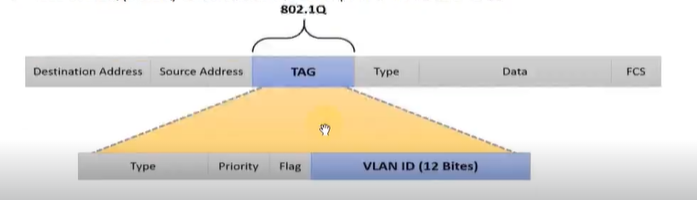




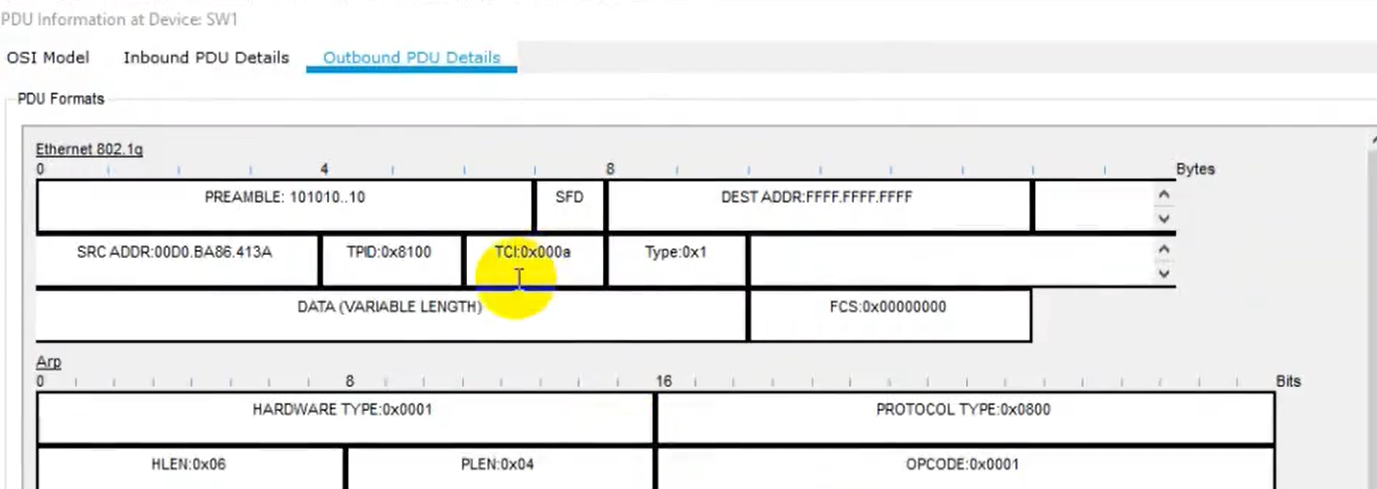
* Trunk port is not included in any vlan.

**Dot1Q/IEEE 802.1Q:**

* DotlQ is IEEE 802.1Q, the standard for trunking encapsulation.
* Common trunking protocol, standard and supported by many vendors.
* On Cisco Switches, you configure IEEE 802.1Q (Dot1Q) on trunk ports.
* DotlQ allow tagged frames to be transported on a trunk link or ports.
* DotlQ allowing multiple VLANs to traverse through one link or ports.
* IEEE 802.1Q (DotlQ) extends the VLANs across the whole network.
* IEEE 802.1Q (DotlQ ) trunks use VLAN I as the default native VLAN.
* VLAN tagging is usually done based on the standard IEEE 802. IQ
* Tag includes info related to particular VLAN which frame belongs to.
* Its indicate VLAN membership within a frame going across the network.
* 802.1Q also adds a 4-byte tag into the Ethernet frame for VLAN tagging.
* IEEE 802.1Q (DotlQ) Supports both Normal and Extended range VLANs.
* IEEE 802.1Q (DotlQ) Inserts tag into existing Switches Ethernet header.



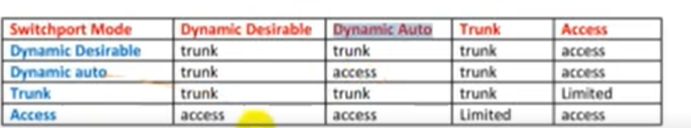




* Switch one tagged frame with hexadecimal equivalent to vlan number. Like **a** shows vlan 10.

**DTP (Dynamic Trunking Protocol):**

* DTP Cisco proprietary protocol which stand for Dynamic Trunking Protocol.
* DTP is point-to-protocol negotiates common trunking mode between Switches.
* DTP is used to dynamically build trunk links between the two Cisco Switches.
* Which is used to automatically negotiate trunks between the Cisco Switches.
* DTP is used to negotiate & form trunk connection between switches dynamically.
* DTP can also be used for negotiating encapsulation type of either IEEE 802.1Q or ISL.
* Dynamic Trunking Protocol is Layer 2 (Data Link) protocol and is enabled by default.
* The default mode can be "Dynamic Auto" or "Dynamic Desirable" depend on Switches.
* A Non-Cisco Switches does not support Dynamic Trunking Protocol (DTP) only Cisco.
* Port configures as no negotiate prevents generating Dynamic Trunking Protocol frames.
* DTP has two default timers that cannot be changed one is Hello & other is the timeout.



**Native Vlan:**

* Without tag, Switch will not know what VLAN the traffic belongs to.
* Switch associates untagged traffic with configured as the Native VLAN.
* A VLAN that any received untagged traffic gets assigned to on Trunk port.
* A VLAN that travel without tag it assigned to an 802.1Q trunk port.
* By default, the Native Virtu4i Local Area Network (VLAN) is one 1.
* Packet without tagged on a dotlq link belongs to Native VLAN.
* Best practice and security to change Native VLAN on all switches.
* Native VLAN ID must match on both end of the Cisco Switch trunk.
* The VLAN dotlq tag native command will tag VLAN on all trunks.
* SW(config-if) # switchport trunk native vlan vlan-id

**Configure VLAN:**

sw#enable

sw#config

sw(config)#vlan 10

sw(config)#name IT

sw(config)#exit

sw(config)#do show vlan br // show vlan brief table

.....................

......................

......................

sw(config)#int f0/1

sw(config-if)#switchport access/voice vlan 10

sw(config)#exit

// similarly we can add our more devices for separate vlan