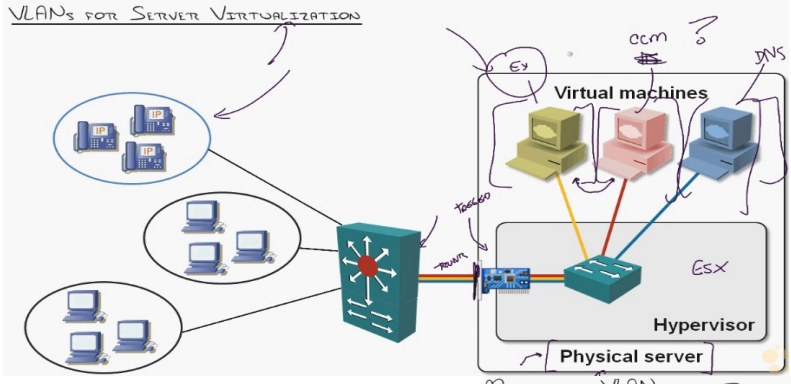
VLANs and VTP:

VLAN (Virtual LAN) and VTP (VLAN Trunking Protocol) (VLAN replication protocol).

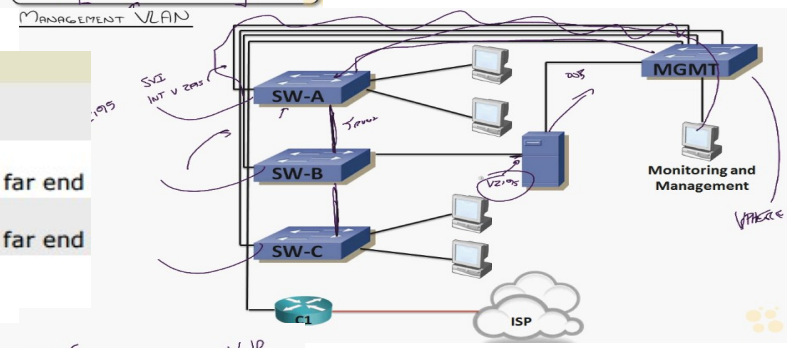
1. A VLAN (switch inside a switch) is a single broadcast domain. Users are only able to communicate within the same VLAN unless Inter-VLAN routing is used.
2. VLAN=One Broadcast domain=One subnet (0 to 4095 available VLANs)
3. Like type segmentation: e.g. servers, users, PCs, IP phones, printers etc.

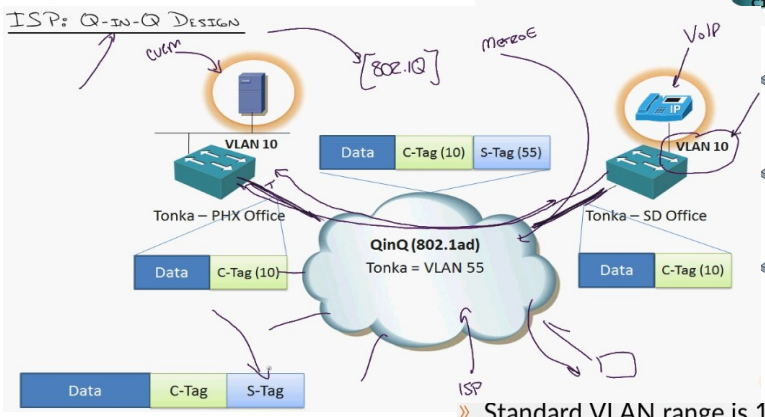


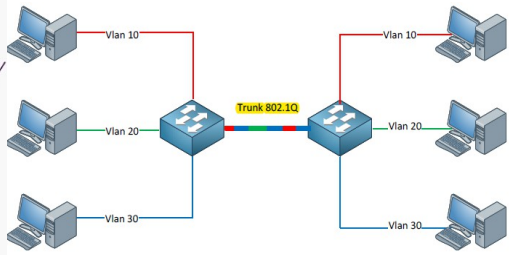
VLAN Numbers			
0	Reserved	**1004**	fdnet
1	default	**1005**	trnet
1002	fddi-default	**1006-4094**	Extended
1003	tr	**4095**	Reserved

Trunk Types	802.1Q	ISL
Header Size	4 bytes	26 bytes
Trailer Size	N/A	4 bytes
Standard	IEEE	Cisco
Maximum VLANs	4094	1000

Switch Port Modes	
trunk	Forms an unconditional trunk
dynamic desirable	Attempts to negotiate a trunk with the far end
dynamic auto	Forms a trunk only if requested by the far end
access	Will never form a trunk

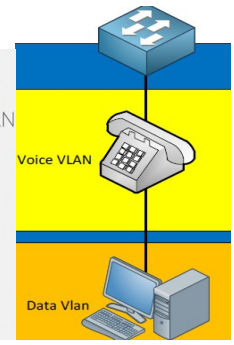


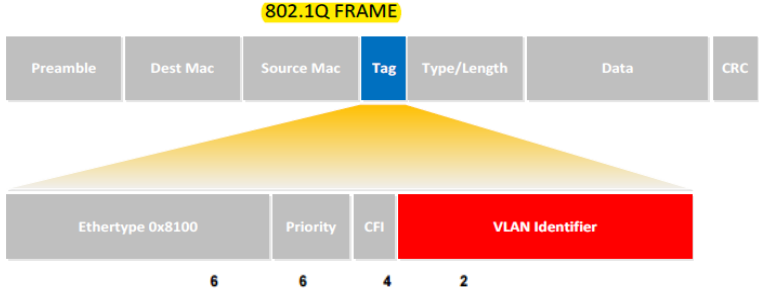




Terminology	
Trunking	Carrying multiple VLANs over the same physical connection
Native VLAN	By default, frames in this VLAN are untagged when sent across a trunk
Access VLAN	The VLAN to which an access port is assigned
Voice VLAN	If configured, enables minimal trunking to support voice traffic in addition to data traffic on an access port
Dynamic Trunking Protocol (DTP)	Can be used to automatically establish trunks between capable ports (insecure)
Switched Virtual Interface (SVI)	A virtual interface which provides a routed gateway into and out of a VLAN

- Standard VLAN range is 1 – 1005
- VLAN 1
  - Default Ethernet Access VLAN & default 802.1q Native VLAN
  - Cannot be deleted, but can be manually pruned from trunks
  - Cannot be pruned by VTP
  - Should not be used for actual port assignments
- VLANs 1002 – 1005
  - Default legacy Token Ring / FDDI VLANs
  - Cannot be deleted, but can be manually pruned from trunks
  - Cannot be pruned by VTP
  - Should not be used for actual port assignments





There are two types of trunking protocols: 802.1Q and ISL (Inter-Switch Link)
VLAN identifier (12-bits VLAN-ID) has the VLAN number. Priority field (3-bits CoS/802.1p) is used to give different priority to different types of traffic in QoS. 1-bit is DE (Discard Eligible)
The difference between 802.1Q and ISL is that 802.1 tags the Ethernet frame while ISL encapsulates the Ethernet Frame. 802.1Q will not tag the native VLAN while ISL does tag the native VLAN. [Port Types: Access, Trunk and Dynamic]

Methods to configure VLANs:

1. Static VLAN: Just configure the VLAN yourself on the interface (common)
2. Dynamic VLAN: Dynamic VLAN is where you have a VMPS server (VLAN Management Policy Server) which has a database of MAC address to VLAN information. MAC addresses can be spoofed so not a good idea.
3. Voice VLAN: Configured on a port which is connected to an IP phone. The port acts as a trunk because IP Phone acts as a switch for the PC connected to it.
4. You can use 802.1X and a RADIUS server to authenticate users and dynamically assign users to a VLAN. With NAC (Network Admission Control) enabled PC could end up in a quarantine VLAN unless updated.

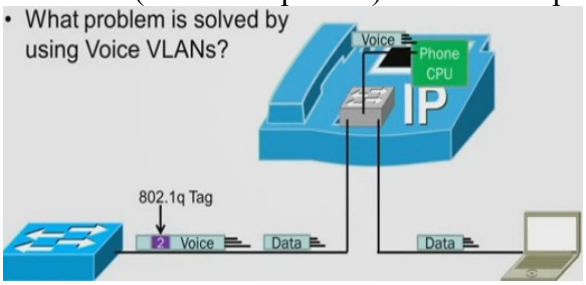
Deleting VLAN information (decommissioning):

VLAN information is not saved in the running-config or startup-config but in a separate file called vlan.dat on your flash memory. So 'delete flash:vlan.dat' to delete VLAN information.

Native VLAN (default is VLAN 1) (Used for management traffic):

Native VLAN is not tagged. So anything that is not tagged will fall under native VLAN. (Management frames) CDP,VTP,STP on your Cisco switch uses the native VLAN, even if it is manually pruned (VLAN1 minimization) you will see in packet capture VLAN1 traffic.
Native VLAN must be the same on both switches otherwise Native VLAN mismatch error occurs.
SW(config)#vlan dot1q tag native !(to tag even the native vlan)

Voice VLAN: Implies two VLANs operating on a switchport (Voice and Data VLANs)
Uses CDP (if cisco IP phones) and DHCP option-156 (for non cisco phones)



VLAN Creation:

this creates mac-address-table and stp instance straight away.
Switch(config)# vlan 100
Switch(config-vlan)# name Engineering
!(This method is the only way to configure extended range VLANs as opposed to database mode)
!(Normal VLAN 1-1005. Extended VLAN(1006-4094) transparent mode or V3.Internal 1002-1005)

VLAN database mode (is being deprecated):

Switch#vlan database
Switch(vlan)#vlan 4 name sales
Switch(vlan)#apply
Switch(vlan)#exit

Access Port Configuration (Assigning a port to an access VLAN):

Switch(config-if)# switchport mode access !(can belong only to one VLAN. Will not send DTP)
!(It is good security measure to disable DTP/trunk negotiation on unused ports)
Switch(config-if)# switchport access vlan 100
Switch(config-if)# switchport voice vlan 150 !(options: vlan-id | dot1p | untagged | none)
!(You can configure the switch port, which is connected to an IP Phone, to use one VLAN for voice traffic and another VLAN for data traffic originating from a device that is connected to the access

port of the IP Phone)

Trunk (tagged) Port Configuration: !(Trunk port can be connected to a server, switch or a router)

Switch(config-if)# switchport trunk encapsulation dot1q !(do this first before making it a trunk)

OR

Switch(config-if)# switchport trunk encapsulation isl !(not all switches support this anymore)

Switch(config-if)# switchport mode trunk !(transmits DTP messages as courtesy)

Switch(config-if)# switchport nonegotiate !(will not send DTP messages even it is a trunk port)

Switch(config-if)# switchport trunk native vlan 10

!(it is a good security measure to change the native vlan to something other than VLAN 1)

Allowed VLANs on the trunk:

Switch(config-if)# switchport trunk allowed vlan 10,20-30 !(these are the only allowed. Careful!)

Switch(config-if)#switchport trunk allowed vlan remove 1- 4094

Switch(config-if)#switchport trunk allowed vlan add 1-50 !(adds to the previous ones)

Switch(config-if)#switchport trunk allowed vlan none

Switch(config-if)#switchport trunk allowed vlan all !(default so won't see in show run)

Trunk Negotiation (DTP Negotiation): 1. dynamic auto and dynamic desirable.

Switch(config-if)#switchport mode dynamic auto

OR

Switch(config-if)#switchport mode dynamic desirable

	Trunk	Access	Dynamic Auto	Dynamic Desirable
Trunk	Trunk	Limited	Trunk	Trunk
Access	Limited	Access	Access	Access
Dynamic Auto	Trunk	Access	Access	Trunk
Dynamic Desirable	Trunk	Access	Trunk	Trunk

DTP (Dynamic Trunking Protocol) (Cisco proprietary): The negotiation of the switchport status by using dynamic auto or dynamic desirable is called DTP. It is a good measure to disable DTP/trunk negotiation on unused ports i.e. nonegotiate command. Security issue: Don't use "dynamic" types. Hard code trunk OR access mode. Default on most switches are 'dynamic auto' or on old ones 'dynamic desirable'. Anyone can connect a laptop and negotiate a trunk.

VTP Configuration(Cisco proprietary)(advertise VLAN attributes to reduce admin overhead)

	VTP Server	VTP Client	VTP Transparent
Create/Modify/Delete VLANs	Yes	No	Only local
Synchronizes itself	Yes	Yes	No
Forwards advertisements	Yes	Yes	Yes

Server(default):1.Power to change vlan info
2.sends & receive vtp updates3.saves vlan config
Client: 1.Cannot change vlan info
2.sends & receive vtp updates3.does not saves vlan config
Transparent:1.Power to change vlan info
2.forwards (passes through vtp updates
3.does not listen to vtp advertisements4.saves vlan config

VLAN Trunking Protocol (VTP)

Domain
Common to all switches participating in VTP

Server Mode
Generates and propagates VTP advertisements to clients; default mode on unconfigured switches

Client Mode
Receives and forwards advertisements from servers; VLANs cannot be manually configured on switches in client mode

Transparent Mode
Forwards advertisements but does not participate in VTP; VLANs must be configured manually

Pruning
VLANs not having any access ports on an end switch are removed from the trunk to reduce flooded traffic

1. Every time a vlan is created/modified/deleted the revision number is increased by 1 and the information gets replicated to other VTP servers and clients. VTP domain/pass/version must match. Transparent mode only forwards advertisement, whereas server and client modes synchronizes themselves alongside forwarding the information. Transparent mode doesn't increment revision number. Off mode in version 3 doesn't even pass through advertisements.

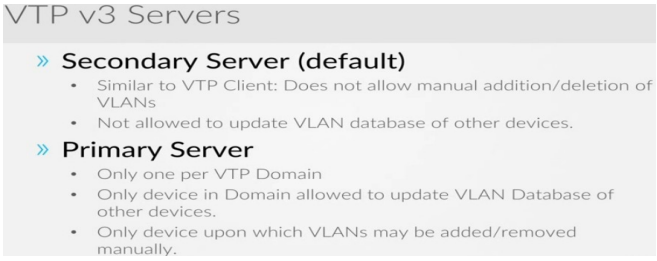
VTP Version Compatibility

- VTP v1 device (v2 Capable) will automatically upgrade itself to v2 if:
  - Detects it is connected to v2 neighbor.
  - Detects it is connected to a v3 neighbor.
- VTP v2 device will remain as v2 if a v3 neighbor is detected.
- VTP version-3 must be manually configured.

VTP Version 3

- Backwards compatible with Version-2 (on a per-link basis)
- Adds additional functionality to VTP:
  - Support for full-range of VLANs (normal and extended)
  - Support for propagation of Private VLANs
  - Option of clear-text or hidden VTP passwords.
  - Support for propagation of 802.1s MST configuration information.
  - Can turn VTP off (globally or per-port)

Switch(config-if)#no vtp

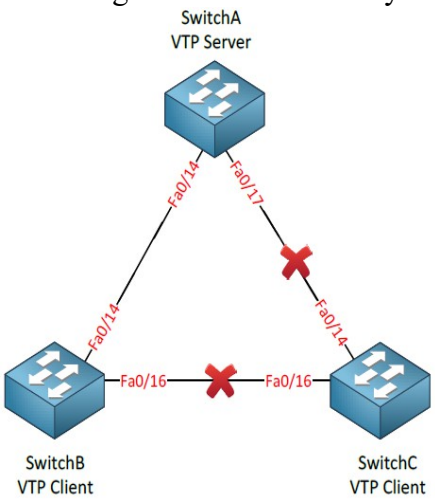


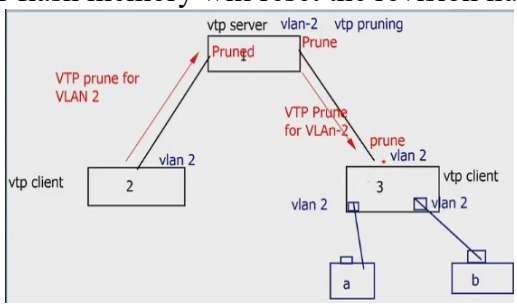
2. server or a client will change to the learnt domain name only if it was set to a NULL value.

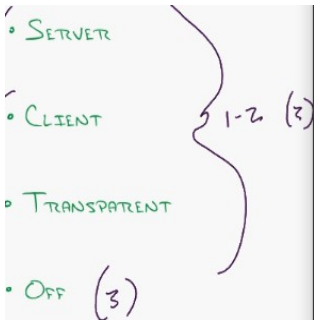
Switch(config)# vtp mode server !(options: server | client | transparent)
Switch(config)# vtp domain CBTNuggets
Switch(config)# vtp password MyPassword !(must be the same on all the switches)
Switch(config)# vtp v2-mode !(options: 1 | 2 | 3)
OR
Switch(config)# vtp version 2 !(options: 1 | 2 | 3) !(must be the same on all the switches)

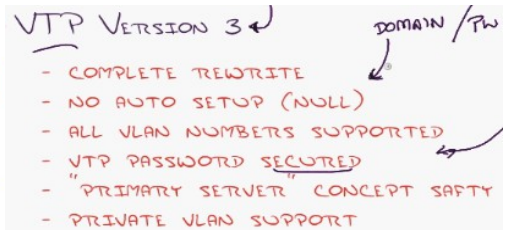
3. **Important Note:** VTP server also acts as a VTP client and can get information from any other VTP client with higher revision number. So for example if you remove a client SwitchC, convert it into a server, add/remove vlans, change it back to a client and then connect it back to the network, it will create havoc i.e. all the switches with lower revision than SwitchC will get everything replicated off SwitchC. Measure: If you do want to use VTP Server / Client mode you need to make sure you reset the revision number:

1. Changing the domain-name will reset the revision number.
2. Deleting the vlan.dat file on your flash memory will reset the revision number.









(When you delete a VLAN all interfaces in that VLAN are in 'no-man's land'. They don't return to VLAN 1)

4. **Steps to configure VTP version 3 (resolves all the problems with older versions):**

1.config vtp domain name 2.change mode to vtp version3 3.config one switch as vtp primary 4. config vtp password (optional)

Switch(config)#vtp domain CBT
Switch(config)# vtp mode server
Switch(config)#vtp version 3
Switch(config)#vtp primary !(this will be the only one to make changes and advertise)
Switch(config)#vtp password cisco hidden !(hashed password, more like service password)
Switch(config)#vtp password <32 chars length hash> secret

VTP Pruning (Dynamic Pruning) (VLAN 2 - 1001 prune eligible):

Only works on VTP servers/clients, but on version3 you have to mention it manually on all.

Reduces broadcasts. By enabling VTP pruning we'll make sure there is no unnecessary VLAN traffic on trunks when there's nobody in a particular VLAN. Depending on your switch model VTP pruning is either turned on or off by default.

Switch(config)# vtp pruning !(send VTP prune message and not VTP Join message)
Switch(config-if)#switchport trunk pruning vlan remove 4,20-30 !(Removes VLANs 4 and 20-30)
Switch(config-if)#switchport trunk pruning vlan except 40-50 !(All VLANs are added to the pruning list except for 40-50)

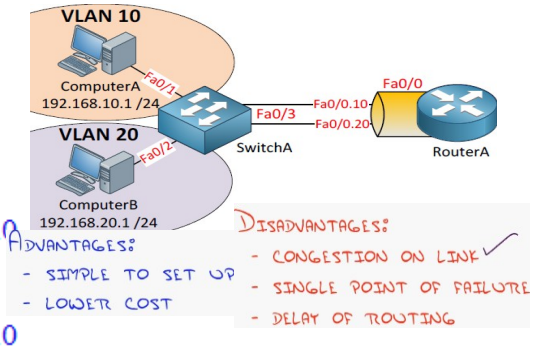
Quarantine VLAN:

Switch(config)# vlan 999
Switch(config-vlan)#stat suspended
Switch(config-vlan)#int range fa0/1 – 24
Switch(config-if-range)#switchport access vlan 999

SVI(Switch Virtual Interface)/Inter-VLAN Routing/L3 Switching/MultiLayer Switch Config:

InterVLAN Routing (Router-on-a-stick) (each sub-interface share the same mac address)**:**

SwitchA(config)#interface fa0/3
SwitchA(config-if)#switchport trunk encapsulation dot1q
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan 10,20
RouterA(config)#interface fa0/0.10
RouterA(config-subif)#encapsulation dot1Q 10
RouterA(config-subif)#ip address 192.168.10.254 255.255.255.0
RouterA(config)#interface fa0/0.20
RouterA(config-subif)#encapsulation dot1Q 20
RouterA(config-subif)#ip address 192.168.20.254 255.255.255.0

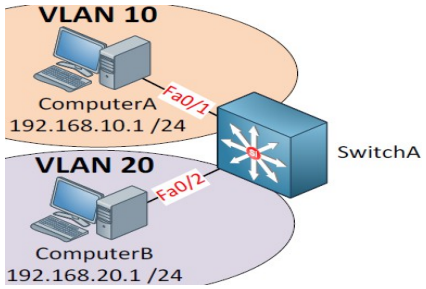


SVI (Using MultiLayer Switch for routing) (each SVI interface has different a mac address)**:**

1. Logical layer3 VLAN interface (Switch routing capabilities. Config SVI for each VLAN and put an IP address on it, used by computers as their default gateway.)

SwitchA(config)#ip routing
SwitchA(config)#interface vlan 10
SwitchA(config-if)#no shutdown
SwitchA(config-if)#ip address 192.168.10.254 255.255.255.0
SwitchA(config)#interface vlan 20
SwitchA(config-if)#no shutdown
SwitchA(config-if)#ip address 192.168.20.254 255.255.255.0

- ROUTING AT WIRE SPEED
- BACKPLANE BANDWIDTH
- REDUNDANCY-ENABLED

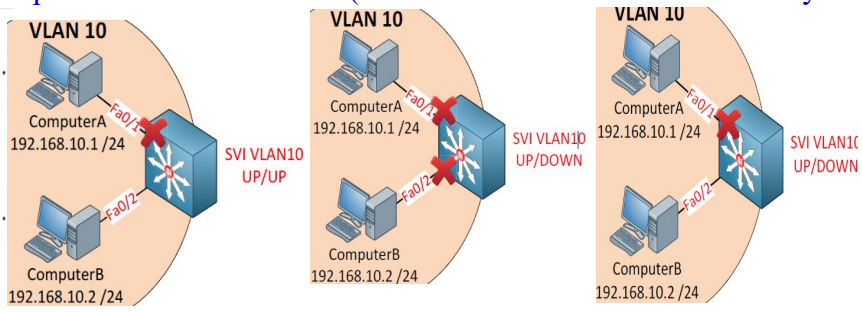


Once you create a SVI and type no shutdown it will normally be “up” since it’s only a virtual interface, there are however a number of requirements or it will show up as “down” (sh vlan):

- TSHOOT: The VLAN has to exist in the VLAN database and it should be active.
- TSHOOT: At least one access or trunk port should use this VLAN actively and it should be in spanning-tree forwarding mode.

SwitchA(config)#interface fa0/2
SwitchA(config-if)#switchport autostate exclude !(won't influence the state of SVI anymore)

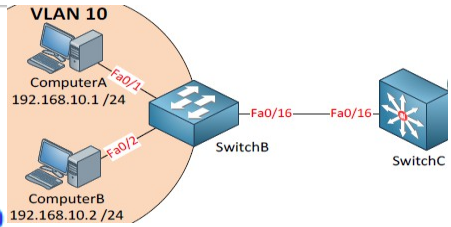
```
interface FastEthernet0/19
 no switchport
 ip address 10.0.0.3 255.255.255.
end

vlan 1006
!
interface vlan 1006
 ip address 10.0.0.3 255.255.255.
!
interface fastethernet0/19
 switchport
 switchport mode access
 switchport access vlan 1006
```



Routed Ports (Using MultiLayer Switch for routing):

By default all interfaces on a switch are switchports (layer 2) but we can change them to routed ports (layer 3). A routed port is the exact same interface as what we use on a router.

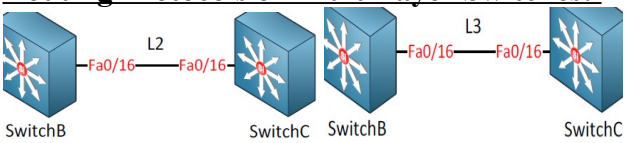
```
SwitchB(config)#interface fa0/16
SwitchB(config-if)#switchport mode access
SwitchB(config-if)#switchport access vlan 10
SwitchC(config)#interface fa0/16
SwitchC(config-if)#no switchport
SwitchC(config-if)#ip address 192.168.10.254 255.255.255.0
```



There are two things you should remember about this routed port:

- It's no longer a switchport so it's not associated with any VLAN.
- It's a routed port but it doesn't support sub-interfaces like a router does.

Routing Protocols on MultiLayer Switches:



SVI:

```
SwitchB(config-if)#switchport trunk encapsulation dot1q
SwitchB(config-if)#switchport mode trunk
SwitchB(config)#vlan 10
SwitchB(config)#interface vlan 10
SwitchB(config-if)#ip address 192.168.10.1 255.255.255.0
SwitchB(config)#ip routing
SwitchB(config)#router eigrp 10
SwitchB(config-router)#network 192.168.10.0
!(same an opposite config on SwitchC)
```

Routed Ports:

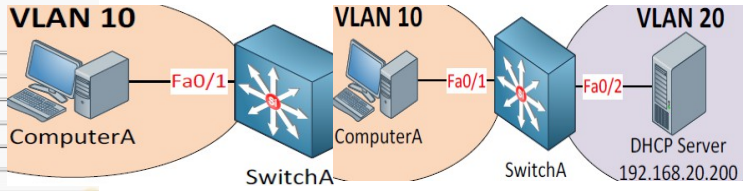
```
SwitchB(config)#no interface vlan 10
SwitchB(config)#interface fa0/16
SwitchB(config-if)#no switchport
SwitchB(config-if)#ip address 192.168.10.1 255.255.255.0
SwitchB(config)#router ospf 10
SwitchB(config-router)#network 192.168.10.0 0.0.0.255 area 0
!(same an opposite config on SwitchC)
```

DHCP and DHCP Helper address (DHCP relay) with SVI:

```
Switch(config)# interface vlan 100
Switch(config-if)#ip helper-address 10.59.22.9
Switch(config)#no ip forward-protocol 37    !(if you don't want to forward some protocols below)
```

- HELPER ADDRESS FORWARDS BROADCASTS AS UNICAST
- DEFAULT UDP PORTS:

UDP PORT	Common Name.
69	TFTP
67	BOOTP Client
68	BOOTP Server
37	Time Protocol
49	TACACS
53	DNS
137	NetBios
138	NetBios Datagram



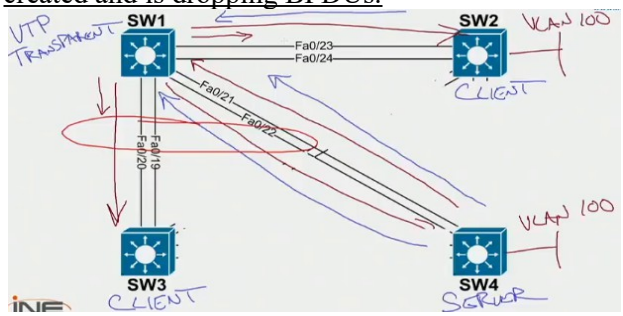

```
SwitchA(config)#interface vlan 10
SwitchA(config-if)#ip address 192.168.10.254 255.255.255.0
SwitchA(config)#interface fa0/1
SwitchA(config-if)#switchport access vlan 10
SwitchA(config)#ip dhcp pool VLAN10POOL
SwitchA(dhcp-config)#network 192.168.10.0 255.255.255.0
SwitchA(dhcp-config)#default-route 192.168.10.254
SwitchA(config)#ip dhcp excluded-address 192.168.10.254
SwitchA#debug ip dhcp server packet
SwitchA#show ip dhcp binding
```

```
SwitchA(config)#interface vlan 10
SwitchA(config-if)#ip address 192.168.10.254 255.255.255.0
SwitchA(config-if)#ip helper 192.168.20.200
SwitchA(config)#interface vlan 20
SwitchA(config-if)#ip address 192.168.20.254 255.255.255.0
SwitchA(config)#interface fa0/1
SwitchA(config-if)#switchport access vlan 10
SwitchA(config)#interface fa0/2
SwitchA(config-if)#switchport access vlan 20
```

Verification and Troubleshooting commands:

1. Make sure the interface is in the correct VLAN. Interface vlan shows Procotol down if there is no port assigned to that vlan.
2. Make sure the interface is in the correct switchport mode (access or trunk).
3. Make sure you have checked interfaces (speed/duplex), port-security and VACL.
4. Make sure you have the same encapsulation protocol when trunking
5. Allowed VLAN mismatch.
6. DTP mismatch (one needs to be desirable instead of both auto)
7. Native VLAN mismatch. (CDP complains about it. So CDP needs to be enabled)
8. VTP domain name (Case sensitive), password mismatch.
9. Incorrect IP address/Inactive VLAN/wrong port assignment.
10. If you are running pruning and you have a trunk that goes to a switch which is transparent, in a different domain or not not running pruning (ESXi), it will send all the VLANs so do manual prune.

SW2, SW3 and SW4 could think that they all are root because SW1 hasn't got a spanning-tree instance created and is dropping BPDUs.



sh vlan !(only shows interfaces in access mode and no trunk interfaces)
sh vlan bri
sh ip int bri
sh vlan bri vlan 10
sh int trunk !(shows trunk interfaces in use and allowed vlans)
sh int fa0/14 trunk !(shows allowed vlans on a trunk. Also shows native vlan)
sh int fa0/1 switchport !(see the operational and admin modes of a port. Also trunk encapsulation)
sh vlan id 2
sh vlan name sales
sh int vlan 1
sh int status !(shows up/down state and access/trunk state)
sh int switchport
sh vlan-switch !(used in gns3)
sh vtp status !(to see almost everything vtp)
sh int fa0/14 pruning !(to see pruned vlans)
sh vtp counters
sh vtp password
debug sw-vlan vtp events
debug sw-vlan vtp pruning
sh spa vlan 10
sh internal usage