:::::::notes::::::

InterVLAN (Routing between VLANs)

(Layer 2 Vs. Layer 3)

1.Layer 2 switches do not do frame modification i.e. transparent bridging

2.Implies hosts in a VLAN can only reach MACS's directly in the CAM table i.e. the local broadcast domain

3.Layer 2 routers/switches perform layer 2 packet rewrite (remove the layer 2 header and rebuild it)

4.implieas inter-vlan traffic must be router

(Three methods to router between VLANs)

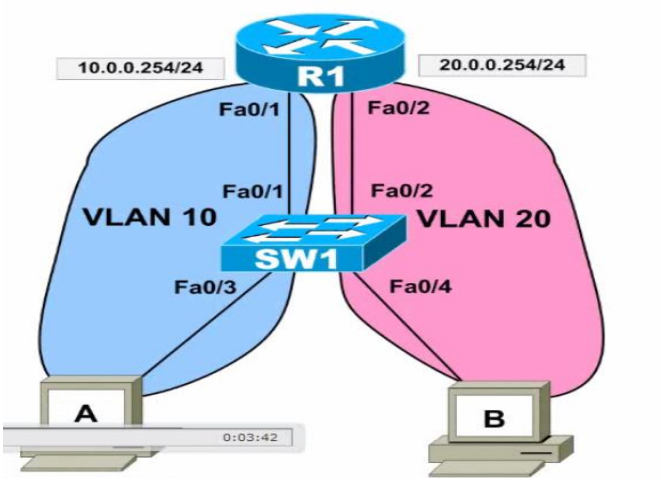
1.Separate port to each vlan (switch to router with multiple links)

1.one solution for inter-vlan routing is to use one physical link per vlan between the layer 2 switch and the layer 3 router

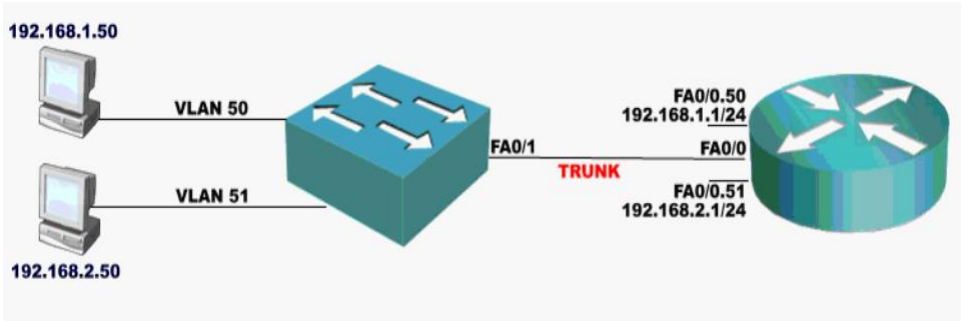
2.frame leaves switch on link 1 in vlan 10

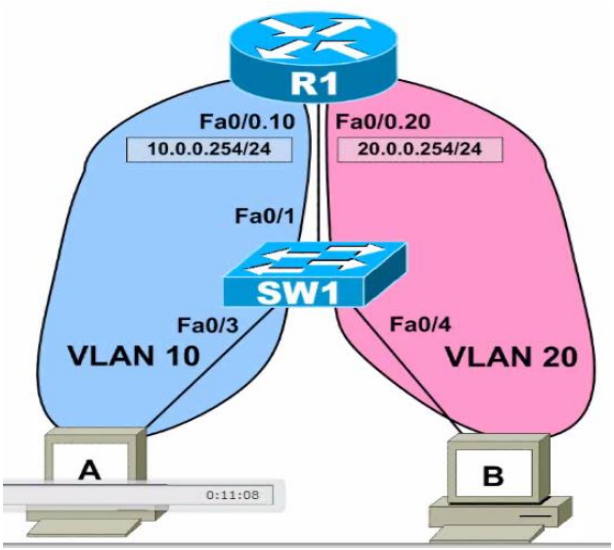
3.router rewrites frame to MAC in vlan 20 and sends back on link 2

4.switch uses CAM of vlan 20 to reach destination



2.Router on a stick (layer 2 switch trunks traffic to external layer 3 router)(legacy version of SVI)





1.router's physical interfaces divided into multiple subinterfaces

2.switchport connecting to router set up as trunk (isl/802.1q)

3.router's subinterfaces assigned specific vlan tag

4.physical interface doesn't get any ip address (only subinterfaces gets ip addresses)

5.Advantages:

1.simple to set up 2. lower cost

6.disadvantages:

1.congestion on link 2.single point of failure 3.delay of routing

7.frame leaves switch on trunk link with vlan 10 encapsulation

8.router rewrites frame to MAC in vlan 20 and sends back to the trunk link with new encapsulation

9.switch uses CAM of vlan 20 to reach destination

10.traffic comes on the physical interface and the router differentiates it based on vlan tags

11.router usually does not support DTP or VTP

12.native vlan must match (can be in the main interface or subinterface with native keyword)(S(config-if)#switchport trunk native vlan 50) (So you can also tag the native vlan -> S(config-if)#vlan dot1q tag native)or(R(config)#int fa0/0.50 R(config)#encap dot1q 50 native)

13.if SW1 is tagging the native vlan (vlan 1 by default) but the other switches are not then a hosts in vlan 1 on SW1 will not be able to reach hosts on SW3 in vlan 1. If SW1 is tagging native vlan but other switches are not then the inter-switch communication for that particular vlan number is lost because SW3 is expecting vlan 1 as untagged.

(Switch config/Configure trunk and access ports)

```
S(config)#vlan 50,51
S(config)#int f0/1
S(config-if)#switchport trunk encap dot1q
S(config-if)#switchport mode trunk
S(config-if)#switchport trunk allowed 50,51  (router usually does not support DTP or VTP)
S(config)#int fa0/2
S(config)#switchport mode access vlan 50
S(config)#int fa0/3
S(config)#switchport mode access vlan 51
```

(Router config/create sub-interfaces)

R(config)#int fa0/0

R(config)#no shut

R(config)#int fa0/0.50

R(config-subif)#encapsulation dot1q 50 (it should support baby giant frame i.e 1504 MTU)

R(config-subif)#ip address 192.168.1.1 255.255.255.0

R(config)#int fa0/0.51

R(config-subif)#encapsulation dot1q 51

R(config-subif)#ip address 192.168.2.1 255.255.255.0

:::::Verification/TSHOOT/Debug/Show commands::::::

1.sh vlan

2.sh ip int bri | inc fa (includes fastethernet interfaces)

3.ping 192.168.2.50

4.traceroute -d 192.168.2.50

5.sh int trunk

6.sh arp

3.Layer 3 switching (Multi-Layer Switching)(Virtual Interfaces are created)(Layer 3 switch)

inside of the switch there is a router board that can do layer 3 processing. done at wire speed. switching happens in the hardware. back plane bandwidth as a limiting factor (gigs/6500 switches redundant supervisor engines).

1.Advantages:

1.Routing at wire speed 2.Backplane bandwidth 3.redundancy-enabled

2.Disadvantages:

1.cost

3.Multi Layer switches support routing capabilities in one of two ways:

1. SVI/Switch Virtual Interfaces (virtual interface is created so all the ports in that particular vlan can reach that virtual interface) (L3 interface used for routing)

1.switch to router communication and rewrite happens on the backplane/fabric

2.Native Layer 3 Router Ports(Create Routed ports/Enable Routing Process)(any physical interface of the switch can be converted into a routed port)

1.native layer 3 ports treated just like an ethernet port on a router

2.typically used in designs where the uplinks are routed (access to distribution layer uplinks)(distribution to core layer)

3.eliminates stp convergence time (convergence is now a function of layer 3 routing)

4.you will choose native L3 routed interface over the SVI (using layer 2 trunk) is becaue there is no stp convergence issue and moreover only if the design specifies that the access to distribution or distribution to core requires the native routed ports.(3550/3560 to 4500/6500 e.g. stp shouldn't extend from access to distribution or distribution to core)

::::::::Commands/Config:::::::

1.SVI/Switch Virtual Interfaces (virtual interface is created so all the ports in that particular vlan can reach that virtual interface) (L3 interface used for routing)(interface vlan [1-4094])(VLAN must exist in the database first even before we assign a port as some platforms dont have error checking to notify whereas other platforms create the vlan automatically when assigned to a port)

S(config)#int vlan 50

S(config-if)#ip address 192.168.1.1 255.255.255.0

S(config-if)#no shut

S(config)#int vlan 51

S(config-if)#ip address 192.168.2.1 255.255.255.0

S(config-if)#no shut

S(config)#ip routing (to turn on layer 3 switching/on a router this command is by default)

:::::Verification/TSHOOT/Debug/Show commands::::::

1.sh vlan

2.sh ip int bri | in vlan(shows SVIs as vlan 50 and vlan 51)

3.arp -a

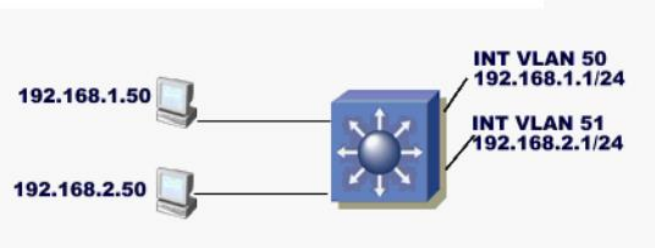
4.ping 192.168.2.1

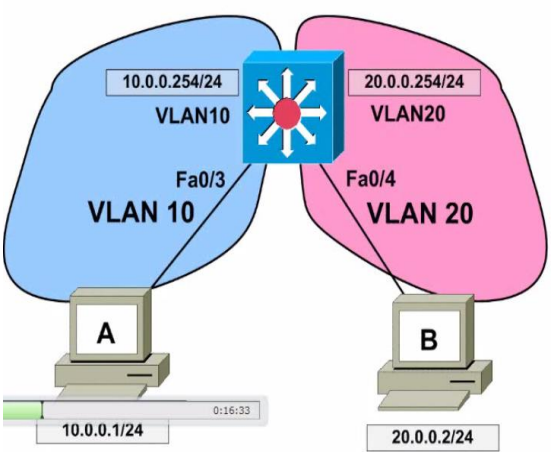
5.traceroute 192.168.2.50

6.sh spa vlan 50

7.sh vlan bri (to see if the vlan exists or not)

8.sh int trunk





2.(Create Routed ports/Enable Routing Process)(any physical interface of the switch can be converted into a routed port)(no switchport)

S(config)#int fa0/24

S(config-if)#no switchport

S(config-if)#ip address 10.1.24.1 255.255.255.252

->doesn't change the physical characteristics i.e you don't have to use crossover cable back to back

S(config)#router eigrp 1

S(config-router)#no auto

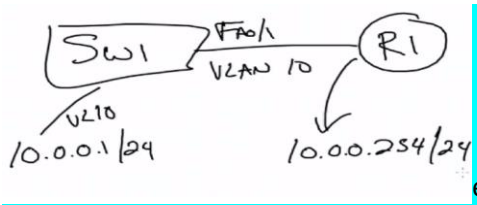
S(config-router)#network 10.0.0.0

:::::Verification/TSHOOT/Debug/Show commands::::::

1.sh ip eigrp nei

2.sh ip route (when ip routing on a switch is not enabled it shows default gateway not set or ICMP

redirect cache is empty/when routing is off on the switch will try to arp the deafult gateway automatically/this happens when you forget to do ip routing command on switch)

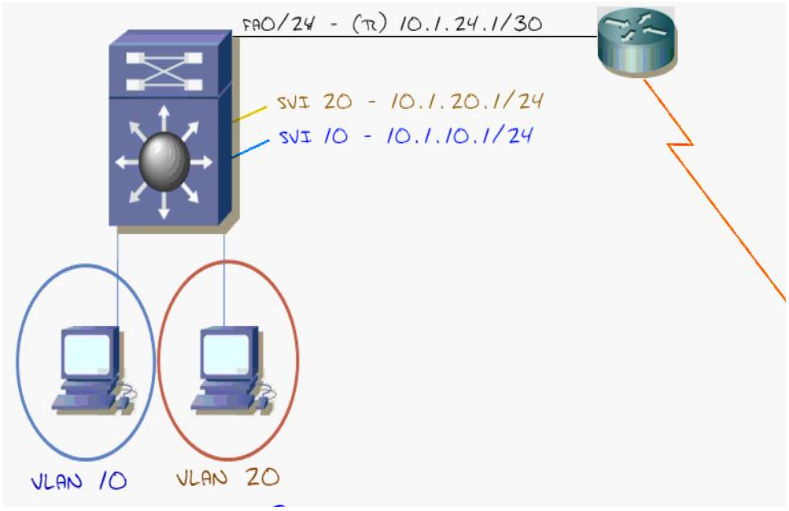


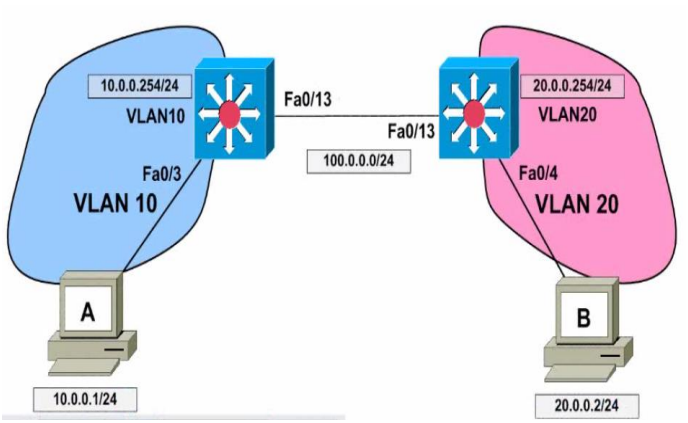
e.g. if you create a loopback on R1 then SW1 will be able to ping the loopback even though it shows that there is nothing in the routing table.this happens because when the default gateway is not set switch tries to arp for everything.

3.ping 10.1.24.2

4.sh arp

5.sh run | b router eigrp



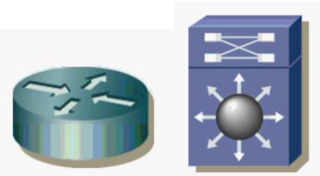


(Layer 3 vs. Multi Layer Switching)(Cisco Express Forwarding/CEF)

1.First packet goes to the router in a switch and then rest of the packets goes through CEF(ASIC) of the switch.

2.A layer 3 switch is a switch with a router inside. Multi layer switch is a switch that has the ability to cache router information i.e. CEF.

3.Every layer 3 switch is also a multi layer switch, but not every multi layer switch is not a layer 3 switch.



4.Router and L3 switch both have IOS software routing

5.software routing is relatively slow compared to asics

6.L3 switches can play a little software-hardware trick

(How Cisco Switches Use CEF)

1.As switch boots up it learns its whole routing table (hight processor time/routing is intense task)

2.It then copies the whole routing table into the FIB(Forwarding Information Base)(high speed cache in the ASIC hardware)(so switch/router knows about it)

3.every switch/router has its adjacency table (keeps all layer 2 information)

4.then it proactively starts looking every single next hop address and looks up the mac address(layer 2 address) and populates that in adjacency table. this all happens at wired speed at layer 3. this is the major advantage of buying a layer three switch.

5.Exceptions to CEF:

1.packet with header options

2.packet with TTL expired

3.packets destined to a tunnel interface

4.packets with unsupported exncapsulations

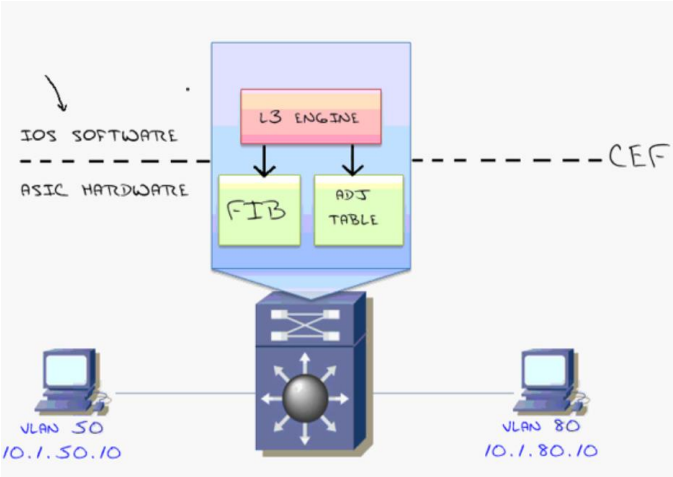
5.packets requiring fragmentation (MTU exceeded)

S(config)#ip cef (tunrs on cef)

1.sh ip cef summary (shows all the prefixes)

2.sh ip cef vlan 100 (shows all the CEF enteries)

3.sh ip arp 192.168.1.1



:::::::Extra notes::::::::::

sh ip int bri (shows vlan interfaces)

sh arp (to check arp cache)

arp -a (on PC)

sh cdp nei (shows remote and local interfaces/platform)

sh cdp nei detail (shows interfaces/platform/duplex/vtp domain/native vlan)

sh ip route (what ip networks can be reached/C -directlly connected if no routing protocol running/routing table always looks for the longest match)

route pring (sh ip router sort of command on PC)

->ip route 0.0.0.0 0.0.0.0 192.168.1.5 (you can spicify the exit interface but in that case you are not sure where will it router in multiaccess ethernet network.so you use next hop address)

sh ip route 192.168.2.3 (to check a router to single ip address/network is not in table comes up even if you have a default router and not a specific router to it)

ping 192.168.1.1

tracerouter 192.168.1.1

debug arp

debug ip icmp

debug ip packet

debug ip packet dump (shows what is inside the ip packet and you can paste it in wireshark)

->when a packet comes from an ethernet and goes into PPP link the layer 2 rewrite is done but the layer 3 remains the same.
