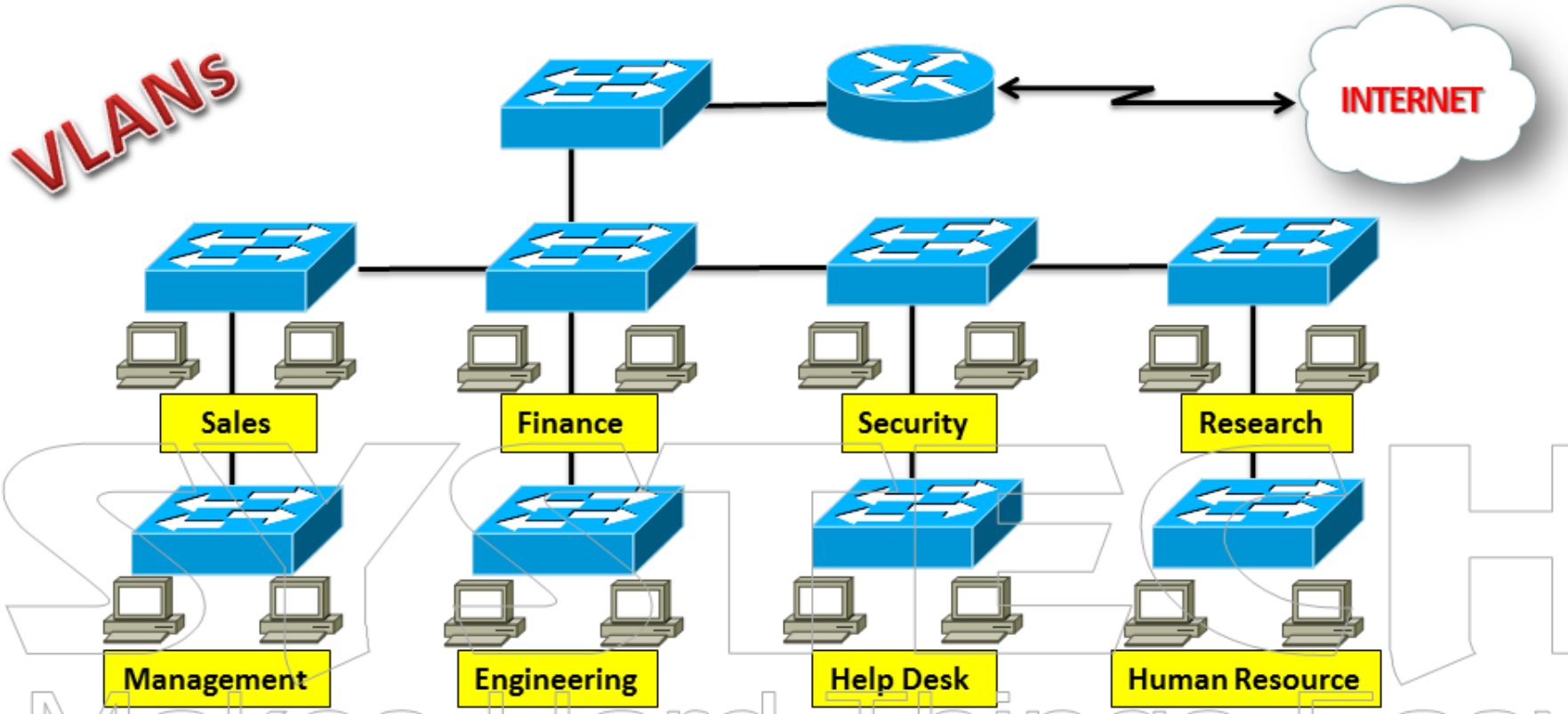
CCNP-SWITCH

300-115

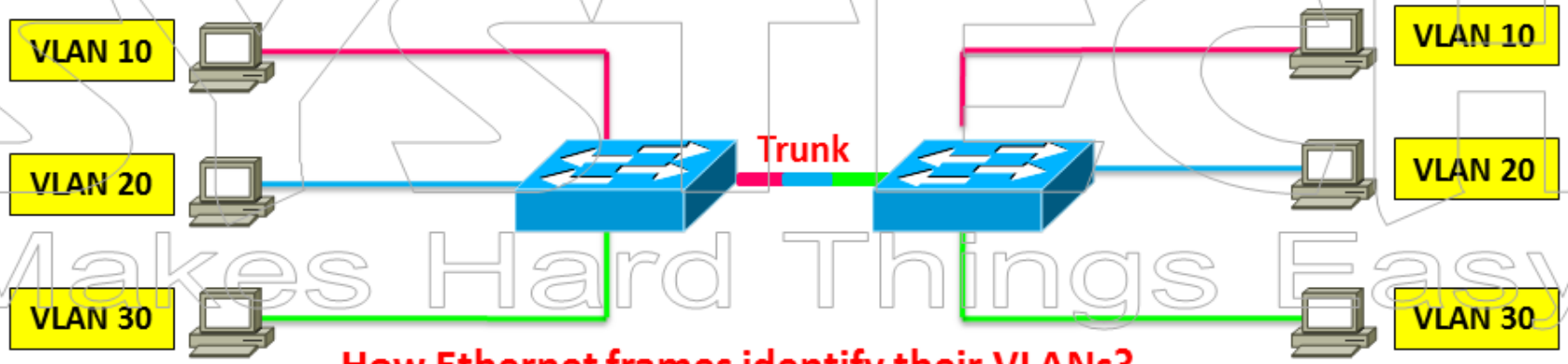


1. What will happen when computer connected to human resource switch sends broadcast like ARP request?
2. What happens when finance switch fails?
3. Will the users at engineering switch have fast network connectivity?
4. How can we implement security in this network?
5. How many collision domains are there?
6. How many broadcast domains are there?

VLANs are only way to solve the problem (switch inside switch)

VLANs (Virtual LANs)

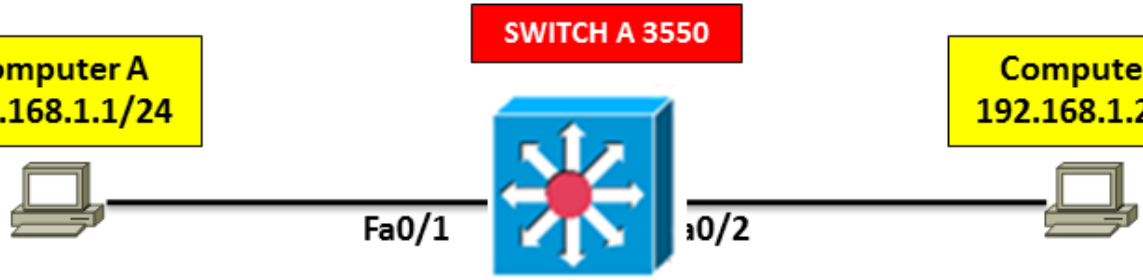
- ✓VLANs are developed to reduce broadcast
- ✓VLANs provide broadcast segmentation
- ✓Types : Static & Dynamic
- ✓VLAN is a single broadcast domain
- ✓ Broadcast frames will be flooded within the VLAN
- ✓Users don't have to be grouped physically together



How Ethernet frames identify their VLANs?

- ✓Its done by Trunking protocol
- ✓Allow multiple VLAN frames
  - IEEE 802.1Q: open standard
  - Cisco ISL (Inter-Switch Link): old Cisco proprietary protocol
- ✓The header contains VLAN identifier to find which VLAN the Ethernet frame belongs.

VLAN Lab 1



By default Computer A & B will ping within VLAN 1

SWITCH A

```
# sh vlan
# configure terminal
# vlan 50
# name  systech
# exit
# sh vlan
# interface fa0/1
# switchport mode access
# switchport access vlan 50
# interface fa0/2
# switchport mode access
# switchport access vlan 50
# sh vlan
```

(Now Computer A & B will ping inside VLAN systech)

```
#show interface fa0/1 switchport
Operation Mode: static access

#show interface fa0/2 switchport
Operation Mode: static access
```

```
# delete flash:vlan.dat
# erase nvram
```

VLAN Lab 2

SWITCH A

```
# sh vlan
# configure terminal
# vlan 50
# name  systech
# exit
# interface  fa0/1
# switchport  mode access
# switchport  access vlan 50
```

SWITCH B

```
# sh vlan
# configure terminal
# vlan 50
# name  systech
# exit
# interface  fa0/2
# switchport  mode access
# switchport  access vlan 50
```

SWITCH A&B

```
# interface fa0/14
# switchport mode trunk
#switchport trunk encapsulation dot1q
#show interfaces fa0/14 switchport
```

Administrative trunking Encapsulation: dot1q

```
#switchport mode trunk
#show interface fa0/14 switchport
```

Operational trunking Encapsulation: dot1q

(Now Computer A & B will ping)

```
#show vlan
```

Show vlan command shows only interfaces in access mode

```
#show interfaces fa0/14 trunk
#int fa0/14
#switchport trunk allowed vlan  remove 1-4094
#switchport trunk allowed vlan add 1-50
```

SWITCH PORT MODES

	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

SWITCH A

interface fa0/1
switchport mode ?
#switchport mode dynamic ?

SWITCH A

interface fa0/14
#switchport mode access

SWITCH B

interface fa0/14
switchport mode ?
#switchport mode trunk

Spanning tree error message on switch A so computer A & B will not ping

SWITCH A

show interface fa0/14 switchport
operation mode: static access

SWITCH B

show interface fa0/14 switchport
operation mode: trunk

SWITCH A&B

show interface fa0/14 trunk
Switch A only allows VLAN1

SWITCH A&B

Change Fa0/1 in switch A and Fa0/2 in switch B to vlan1

Now computer A&B are pinging so even though we have mismatch between the switchport types we still have limited connectivity & only VLAN 1 is allowed

- ✓ Systech recommends you never to use “dynamic” types.
- ✓ Set your interfaces in trunk or access mode.
- ✓ If your switch ports are in dynamic desirable by default then its a security issue.
- ✓ If a hacker connects a switch insted of his laptop then he can make the port as trunk and he can access to our VLANs.
- ✓ For security reasons we have to disable negotiation of switchport status .

Trunk interfaces:
#switchport mode trunk
#switchport nonegotiate

Access interfaces:
#switchport mode access
#switchport nonegotiate

- ✓ For security reasons systech recommends you to change your native vlan also .

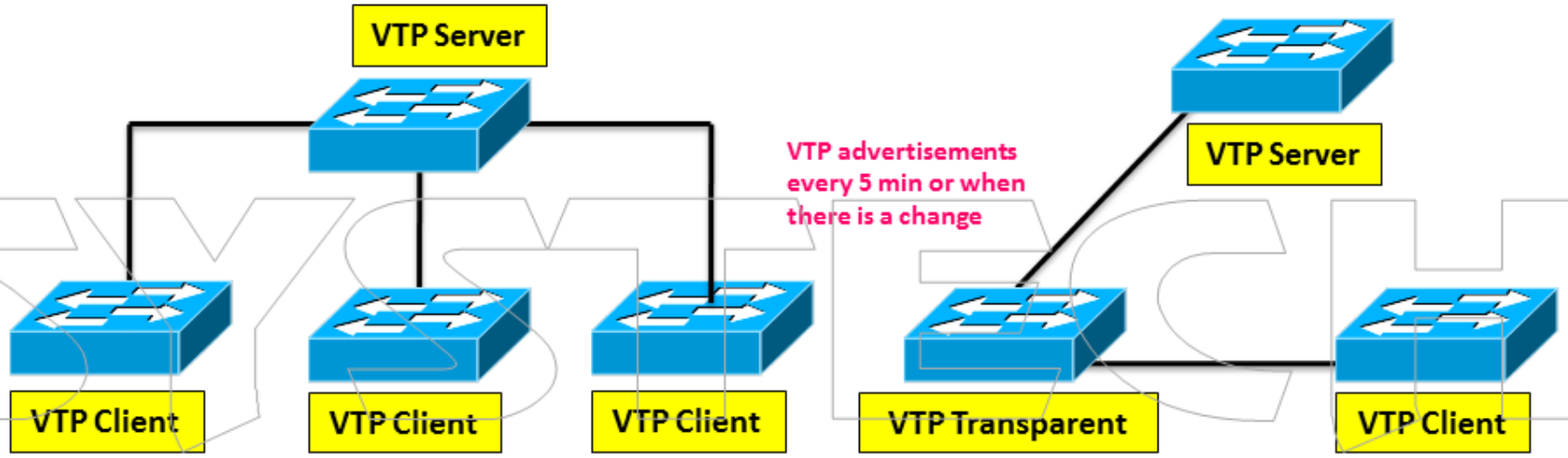
SWITCH A&B

#show interfaces fa0/14 trunk
#int fa0/14
#switchport trunk native vlan 100
#show interfaces fa0/14 trunk

Now native vlan is changed from 1 to 100

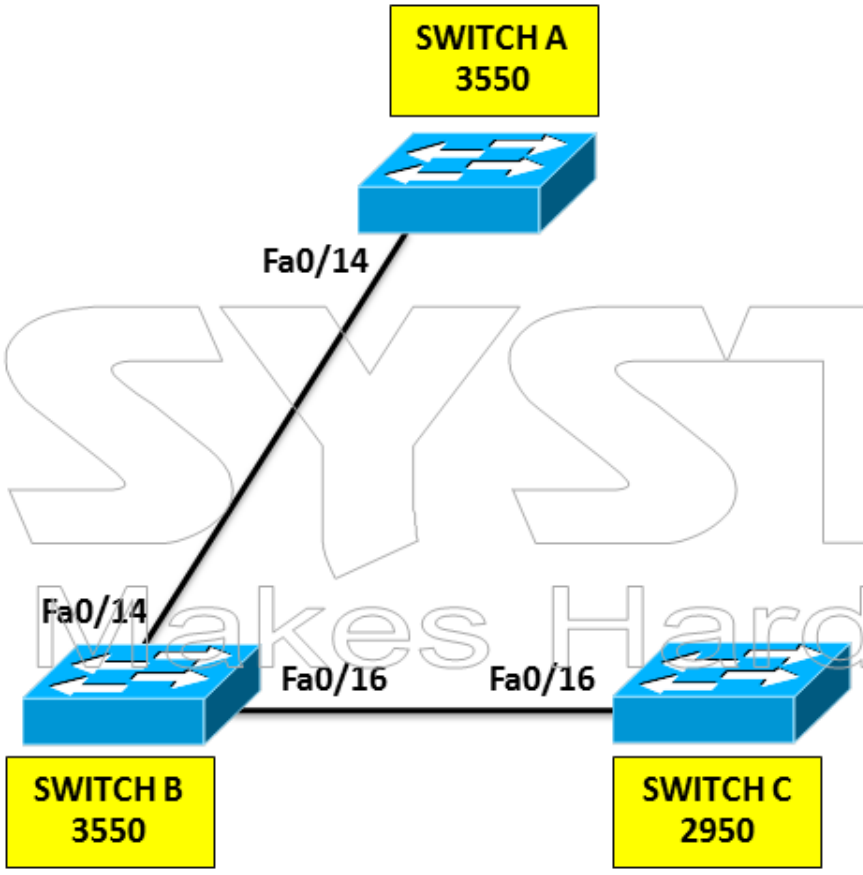
VTP (vlan trunking protocol)

- ✓ VTP helps to create VLAN on one switch and it is synchronize with other switches in the network
- ✓ VTP server,VTP client & VTP transparent



- ✓ VTP server is the switch used to create/modify or delete vlans
- ✓ VTP server will be synchronized with VTP clients
- ✓ We can have multiple VTP servers which will also function like VTP client so we can configure VLANs on multiple switches
- ✓ We cannot create /modify/delete vlan in VTP clients
- ✓ When you create or delete Vlan the revision number will be incresed by 1.
- ✓ VTP transparent will forward advertisements from VTP server to VTP client but it will not sysnchronize with VTP server
- ✓ We can create/modify/delete vlans in VTP transparent but only local
- ✓ VTP transparent mode stores VLAN information in running-config & VTP server stores in VLAN database (vlan.dat on flash)
- ✓ Security risk!!! VTP client can overwrite a VTP server if the revision number is higer becauseVTP server is also VTP client

VTP Lab 1



SWITCH A,B&C

Show vtp status
Configuration Revision : 0
VTP operating mode : server

SWITCH A

vlan 10
name printers
#exit
#show vlan
#show vtp status
Configuration
Revision : 1

SWITCH B&C

#sh vlan
#sh vtp status
Configuration
Revision : 0

✓No changes on switch B&C because we need to configure VTP domain-name

SWITCH B&C

debug sw-vlan vtp events

SWITCH A

vtp domain systech

SWITCH B&C

no debug all
#sh vtp status
Configuration
Revision : 1
show vlan

✓Now switch B&C have learned VLAN 10 through VTP

All the three switches are in server mode so we can create vlan on any switch

SWITCH B

vlan 20
name servers

SWITCH C

vlan 30
name Management

SWITCH A,B&C

show vlan

✓ Now all switches have the vlans

show vtp status

Configuration
Revision : 3

SWITCH B

#vtp mode client
#show vtp status

✓ Now switch B is VTP client

SWITCH A

vlan 40
name sales

SWITCH B&C

#show valn

✓ Now switch B&C learns VLAN 40

SWITCH B

vlan 50

✓ VLAN cannot be created in VTP client mode

SWITCH B

#vtp mode transparent
#show vtp status

✓ Now switch B is VTP transparent

SWITCH A

vlan 50
name accounts

SWITCH B

sh vlan

✓ No VLAN 50 because it is VTP transparent

SWITCH C

sh vlan

✓ VLAN 50 is received from switch B
✓ VTP transparent will not synchronize but forward VTP advertisements

SWITCH B

vlan 60
name cameras
#show vlan

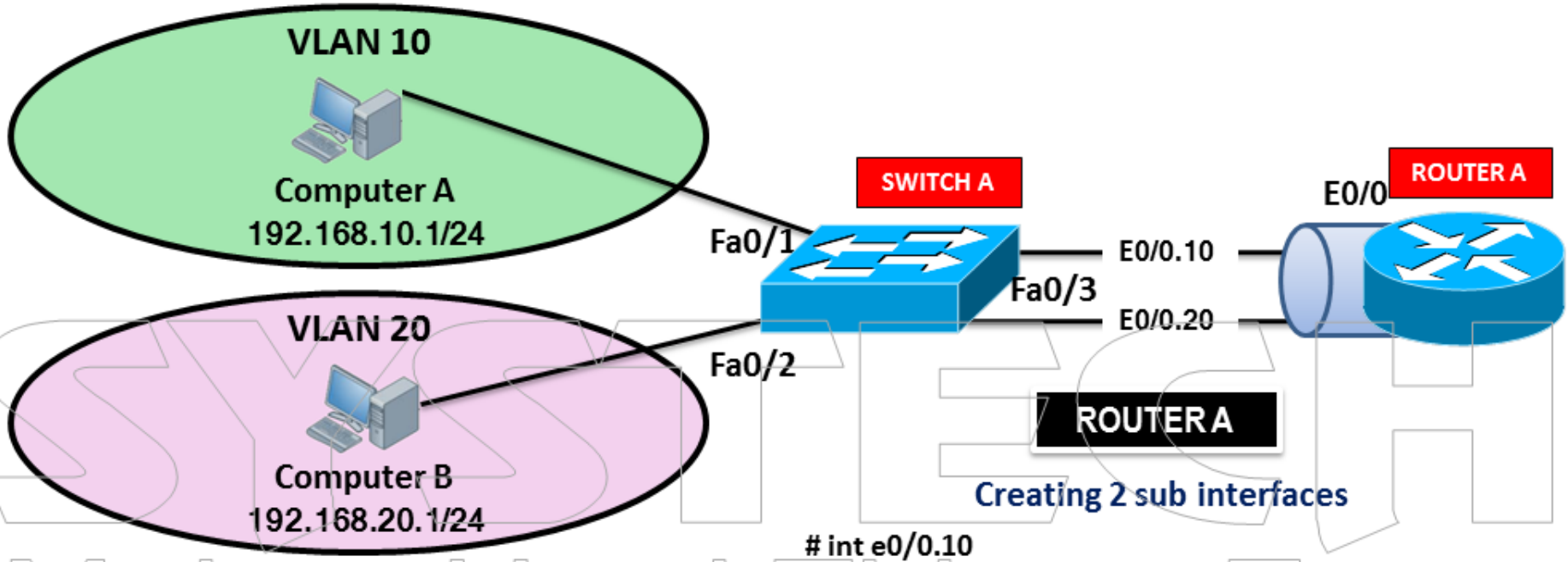
SWITCH A&C

#show valn

✓ No VLAN 60
✓ Will not advertise its own VLANs because they are only known locally

✓ security risk: if switch C's revision number increase then its state will be updated to switch A&B
✓ If we want to use VTP/server/client mode than we have to reset the revision number
✓ Changing domain name will reset the revision number
✓ Deleting the vlan.dat file on flash memory will reset the revision number

Inter VLAN routing by Router on a stick



Creating 2 sub interfaces

SWITCH A

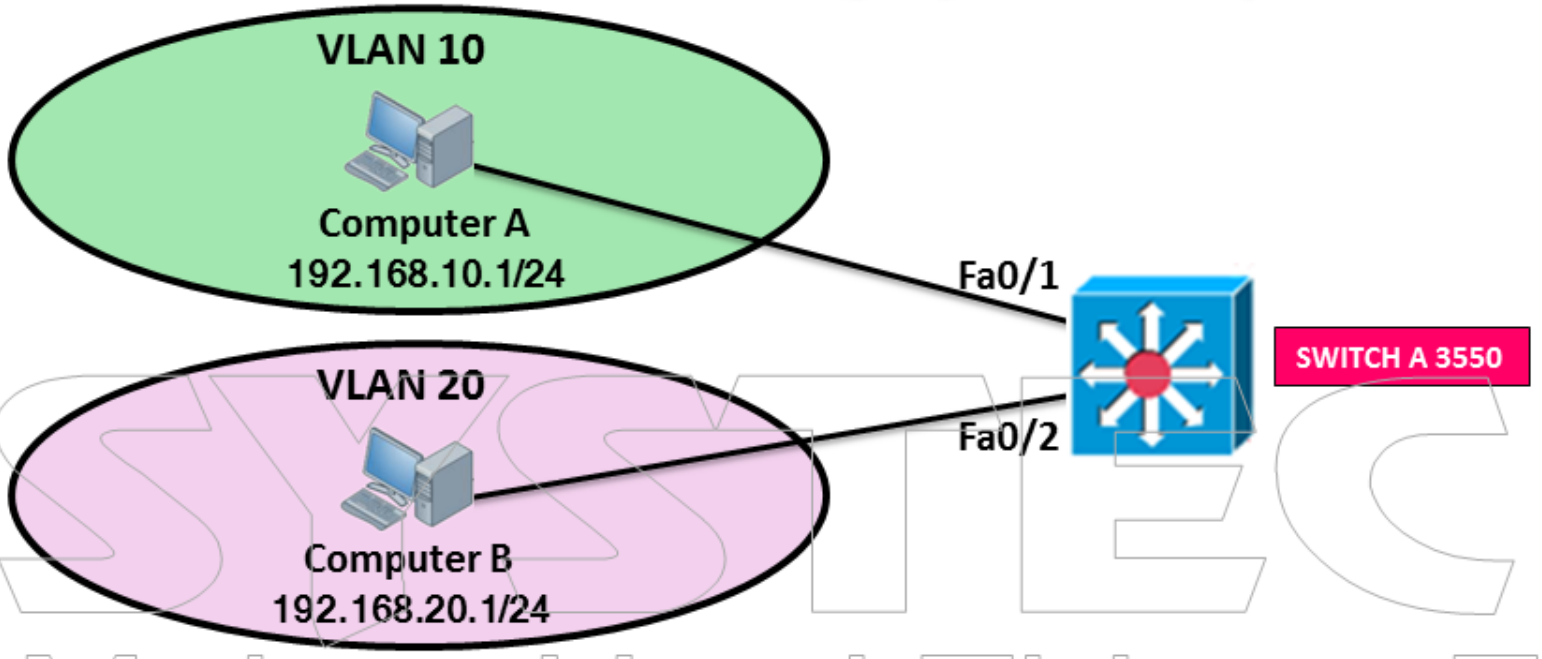
```
# int fa0/3
#switchport trunk encapsulation dot1q
#switchport mode trunk
#switchport trunk allowed vlan 10,20
```

```
# int e0/0.10
#encapsulation dot1q 10
#ip address 192.168.10.254 255.255.255.0
#no sh
#int e0/0.20
#encapsulation dot1q 20
#ip address 192.168.20.254 255.255.255.0
#no sh
#sh ip route
```

✓Router will be able to route because they are directly connected

✓Assign gateway for Computer A & B and now they are pinging

Inter VLAN routing by Multi layer switch



SWITCH A

ip routing

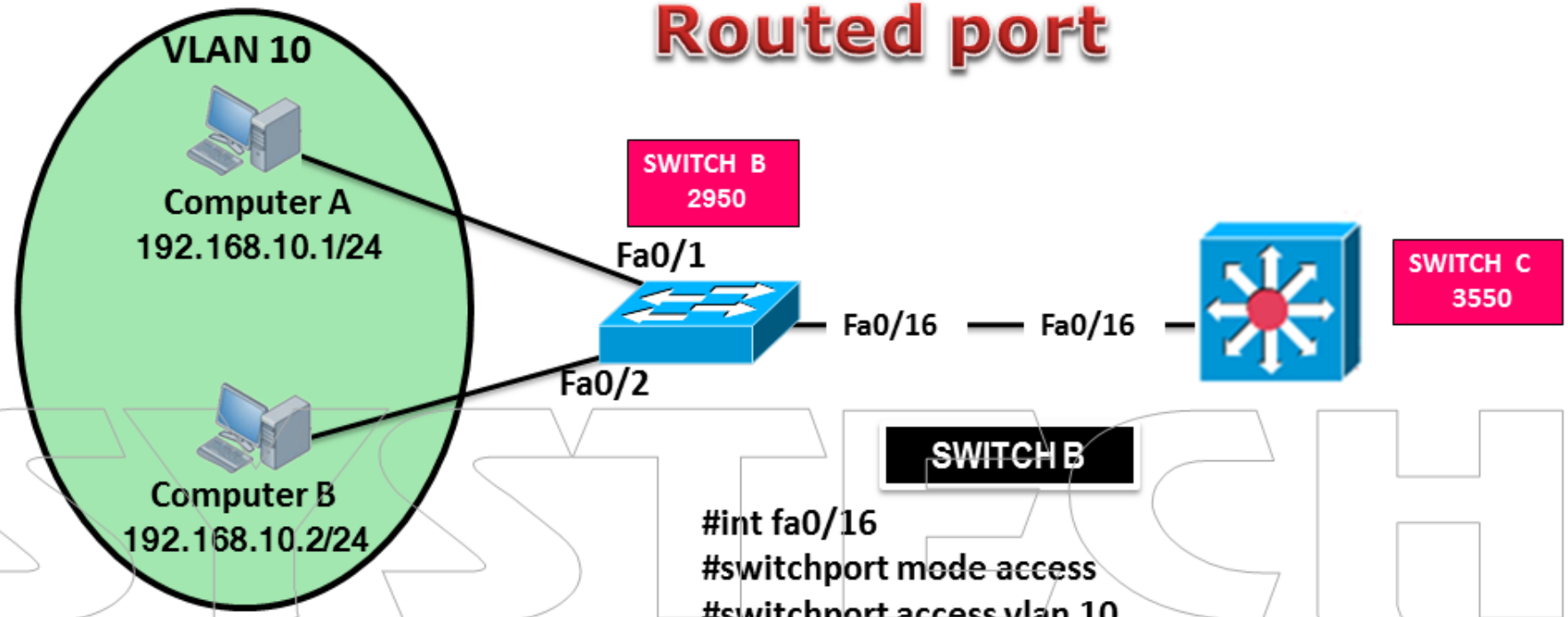
✓Configure SVI (Switch Virtual Interface)

```
#Interface vlan 10
#no sh
#ip address 192.168.10.254 255.255.255.0
#Interface vlan 20
#no sh
#ip address 192.168.20.254 255.255.255.0
```

✓Now Computer A & B will ping

```
#sh ip int brief vlan 10
#int fa0/1
#sh
#sh ip int brief vlan 10
# int fa0/2
#switchport autostate exclude
```

Routed port



SWITCH B

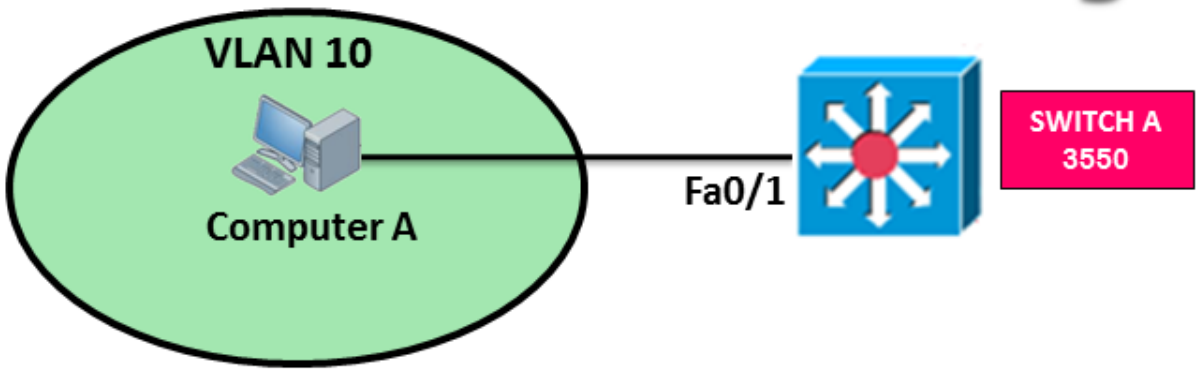
```
#int fa0/16
#switchport mode access
#switchport access vlan 10
```

SWITCH C

```
#int fa0/16
#no switchport
#ip address 192.168.10.254 255.255.255.0
# sh interface status
```

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

DHCP Configuration



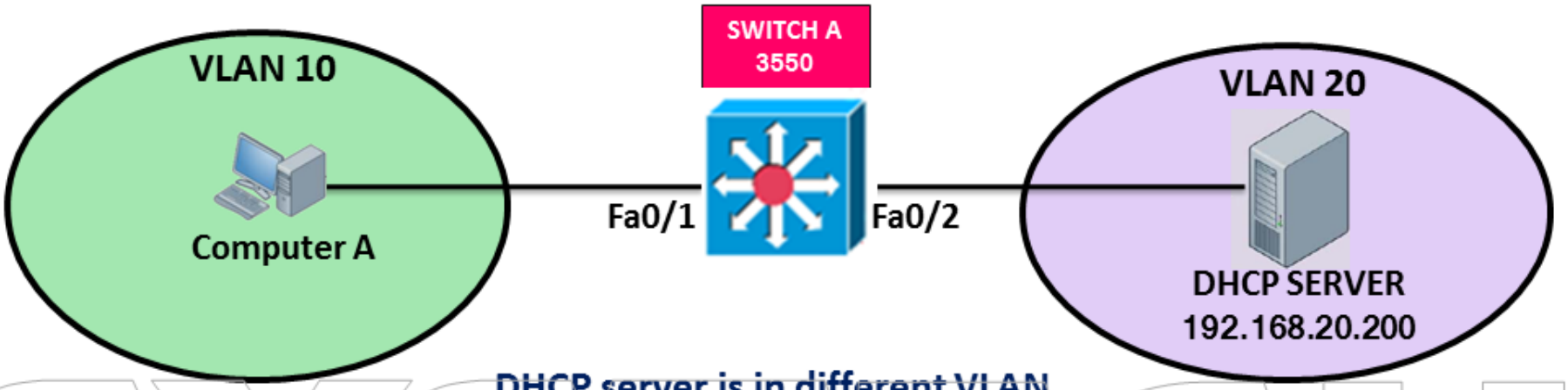
✓If we use multilayer switch as gateway we might have to configure it as DHCP server as well

SWITCH A

```
#int vlan 10
#ip address 192.168.10.254 255.255.255.0
#int fa0/1
#switchport access vlan 10
```

```
#ip dhcp pool systechvlan10
#network 192.168.10.0 255.255.255.0
#default-router 192.168.10.254
#exit
#ip dhcp excluded-address 192.168.10.254

#debug ip dhcp server packet
#show ip dhcp binding
```



DHCP server is in different VLAN

SWITCH A

```
#int vlan 10
#ip address 192.168.10.254 255.255.255.0
#ip helper 192.168.20.200
#interface vlan 20
#ip address 192.168.20.254 255.255.255.0
#int fa0/1
#switchport access vlan 10
#int fa0/2
#switchport access vlan 20
```