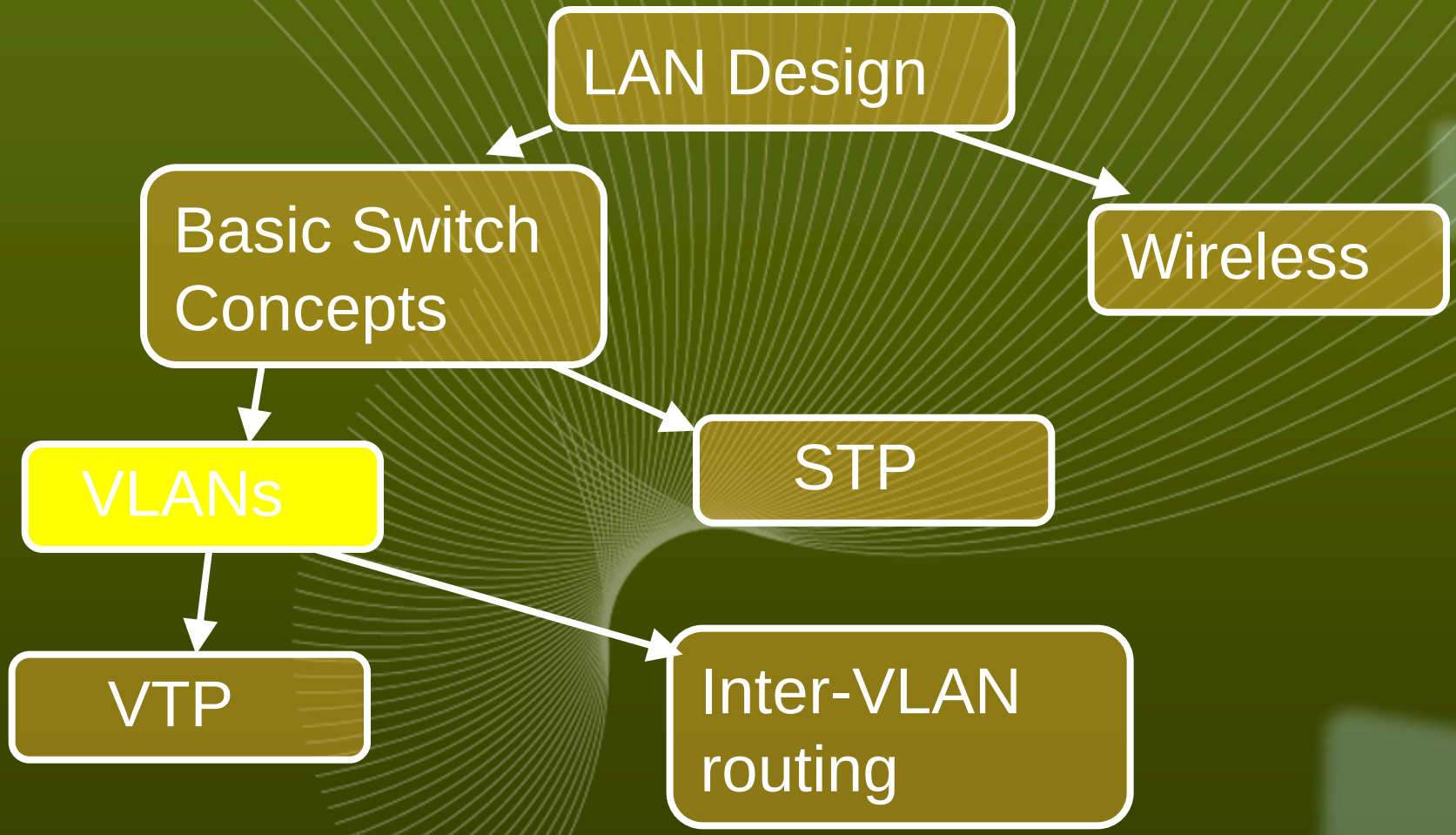
INSTITUT TEKNOLOGI TELKOM

Virtual LAN

Semester 3

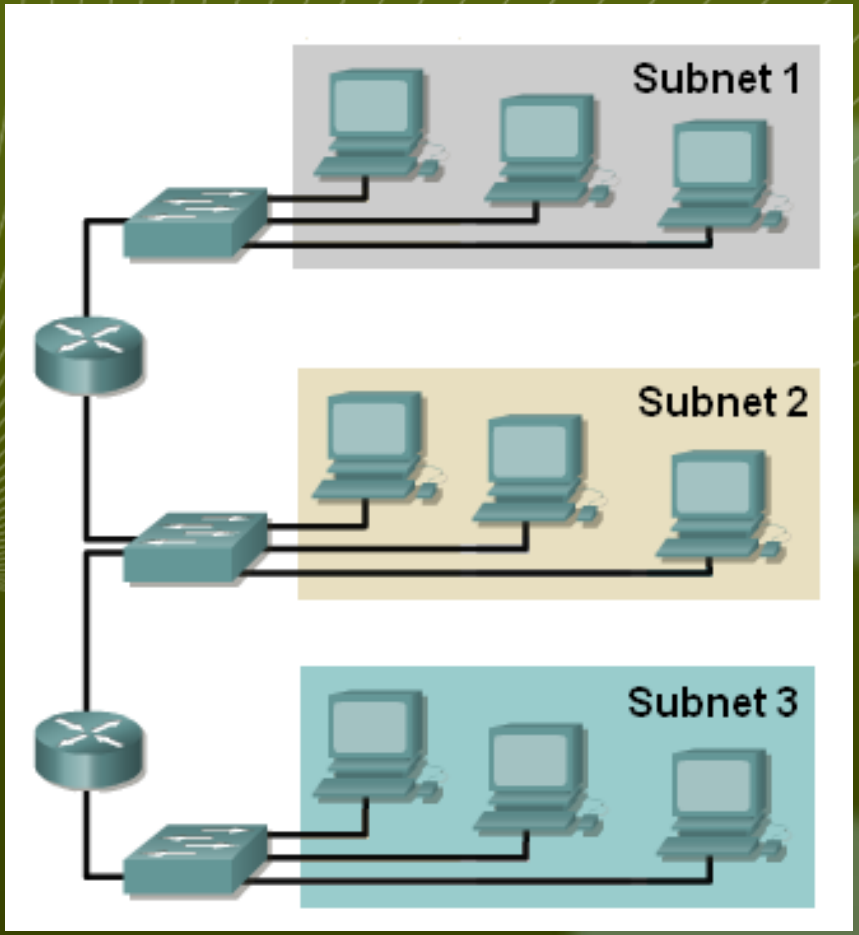

LAN Design
Basic Switch Concepts
Wireless
STP
VLANs
VTP
Inter-VLAN routing

Some requirements of LANs

- Need to split up broadcast domains to make good use of bandwidth
- People in the same department may need to be grouped together for access to servers
- Security: restrict access by certain users to some areas of the LAN
- Provide a way for different areas of the LAN to communicate with each other

Solution using routers

- Divide the LAN into subnets
- Use routers to link the subnets



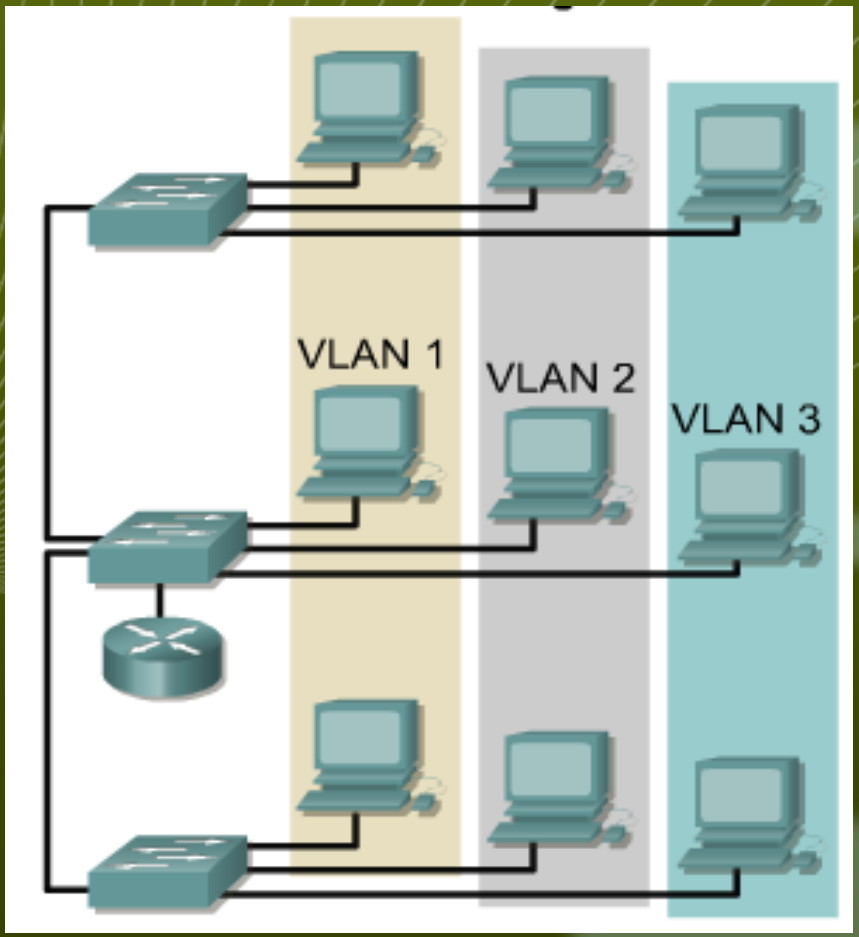
Solution using routers

BUT

- **Routers are expensive**
- **Routers are slower than switches**
- **Subnets are restricted to limited physical areas**
- **Subnets are inflexible**

Solution using VLANs

- VLAN membership can be by function and not by location
- VLANs managed by switches
- Router needed for communication between VLANs



VLANs

- All hosts in a VLAN have addresses in the same subnet. A VLAN is a subnet.
- Broadcasts are kept within the VLAN. A VLAN is a broadcast domain.
- The switch has a separate MAC address table for each VLAN. Traffic for each VLAN is kept separate from other VLANs.
- Layer 2 switches cannot route between VLANs.

VLAN numbers

- VLAN 1: default Ethernet LAN, all ports start in this VLAN.
- VLANs 1002 – 1005 automatically created for Token Ring and FDDI
- Numbers 2 to 1001 can be used for new VLANs
- Up to 255 VLANs on Catalyst 2960 switch
- Extended range 1006 – 4094 possible but fewer features

VLAN information

- VLAN information is stored in the VLAN database.
- vlan.dat in the flash memory of the switch.

Port based

- Each switch port intended for an end device is configured to belong to a VLAN.
- Any device connecting to that port belongs to the port's VLAN.
- There are other ways of assigning VLANs but this is now the normal way.
- Ports that link switches can be configured to carry traffic for all VLANs (trunking)

Types of VLAN

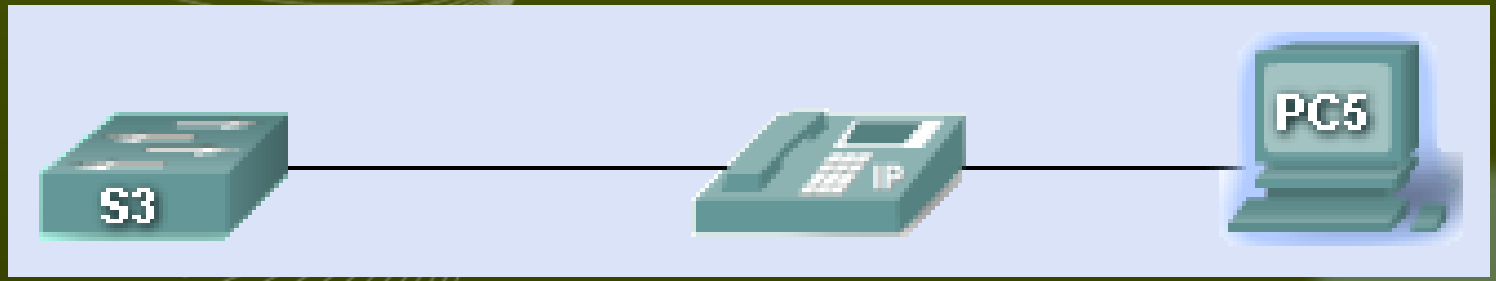
- Data or user VLAN
- Voice VLAN
- Management VLAN
- Native VLAN
- Default VLAN

Data VLAN

- Carry files, e-mails, shared application traffic, most user traffic.
- Separate VLAN for each group of users.

Voice VLAN

- Use with IP phone.
- Phone acts as a switch too.
- Voice traffic is tagged, given priority.
- Data not tagged, no priority.



Management VLAN

- Has the switch IP address.
- Used for telnet/SSH or web access for management purposes.
- Better not to use VLAN 1 for security reasons.

Native VLAN

- For backward compatibility with older systems.
- Relevant to trunk ports.
- Trunk ports carry traffic from multiple VLANs.
- VLAN is identified by a “tag” in the frame.
- Native VLAN does not have a tag.

Default VLAN

- VLAN 1 on Cisco switches.
- Carries CDP and STP (spanning tree protocol) traffic.
- Initially all ports are in this VLAN.
- Do not use it for data, voice or management traffic for security reasons.

Static VLAN

- The normal type. Port configured to be on a VLAN. Connected device is on this VLAN.
- VLAN can be created using CLI command, given number and name.
- VLAN can be learned from another switch.
- If a port is put on a VLAN and the VLAN does not exist, then the VLAN is created.

Static VLAN (Port-centric)

```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface fastEthernet0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#end
```

- If VLAN 20 did not exist before – then it does now.

Voice VLAN

```
S3#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface fastEthernet 0/18
S3(config-if)#mls qos trust cos
S3(config-if)#switchport voice VLAN 150
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#end
```

- Configured for voice VLAN and data VLAN.

Dynamic VLAN

- Not widely used.
- Use a VLAN Membership Policy Server (VMPS).
- Assign a device to a VLAN based on its MAC address.
- Connect device, server assigns VLAN.
- Useful if you want to move devices around.

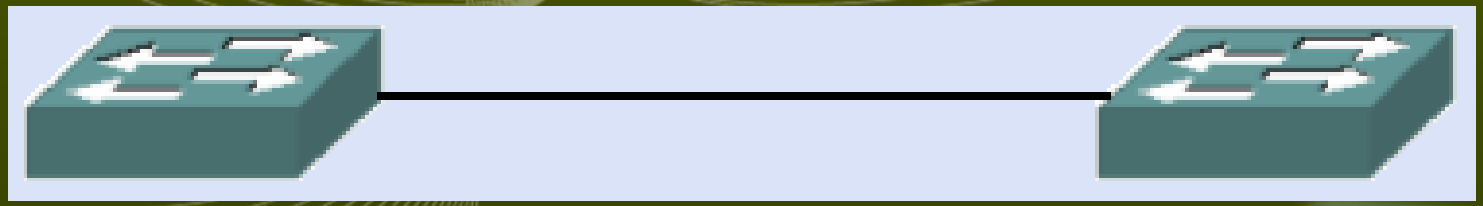
Traffic between VLANs

- Layer 2 switch keeps VLANs separate.
- Router can route between VLANs. It needs to provide a default gateway for each VLAN as VLANs are separate subnets.
- Layer 3 switch has a switch virtual interface (SVI) configured for each VLAN. These act like router interfaces to route between VLANs.

Trunking

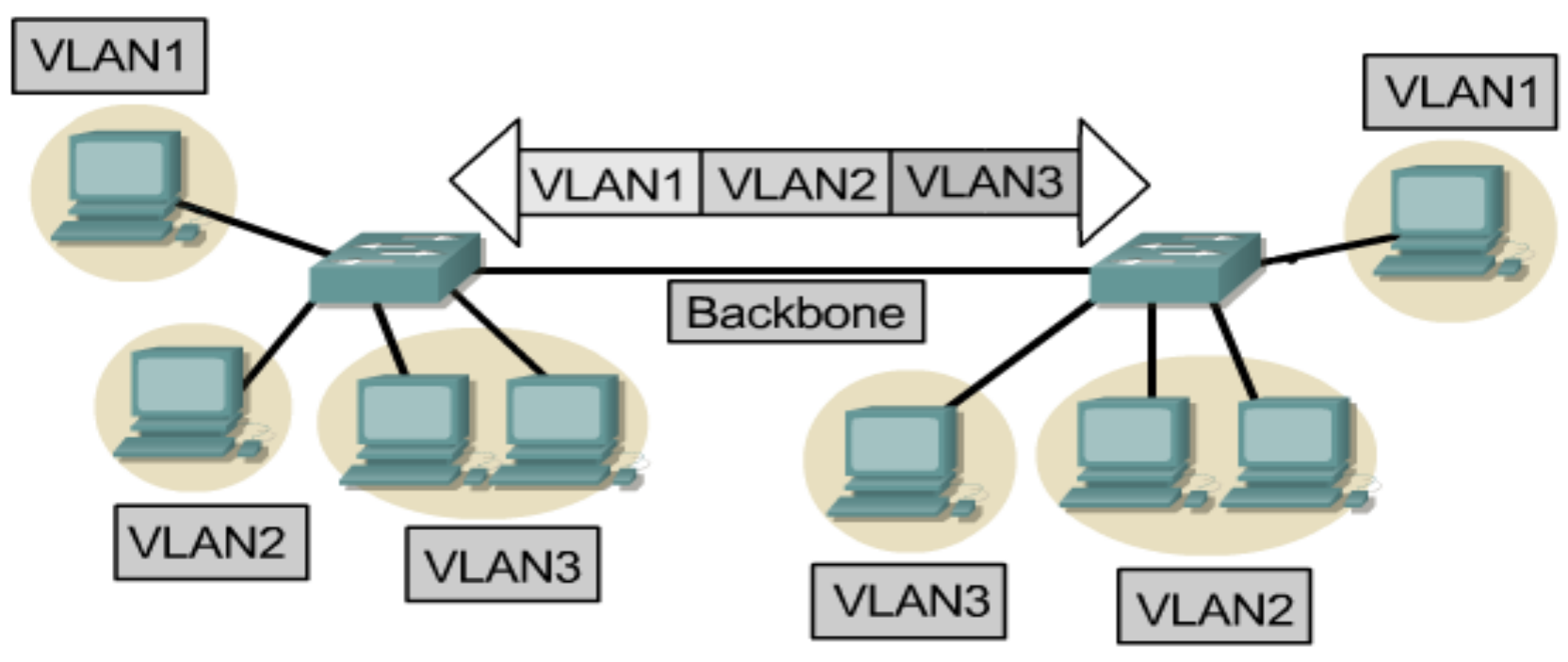
- Both switches have the same 5 VLANs.
- Do you have a link for each VLAN?

- More efficient for them to share a link.



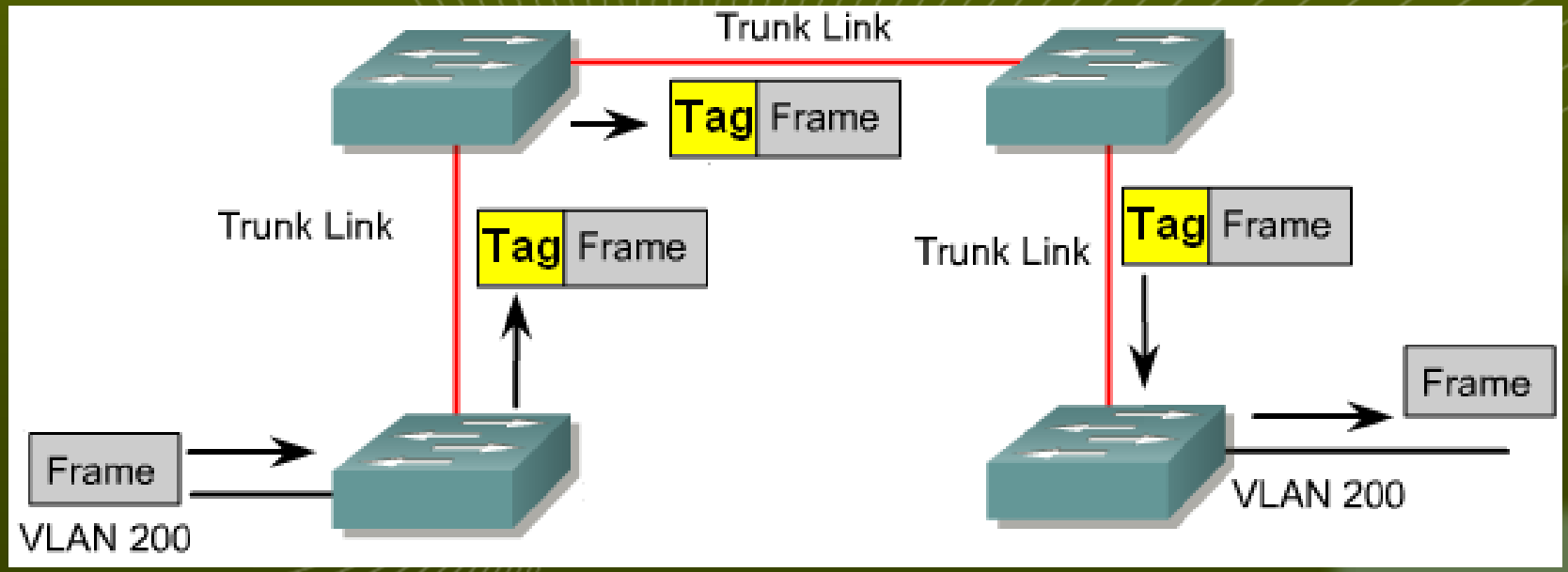
Trunking

- Traffic for all the VLANs travels between the switches on a shared trunk or backbone



Tag to identify VLAN

- Tag is added to the frame when it goes on to the trunk
- Tag is removed when it leaves the trunk



Frame tagging IEEE 802.1Q

Normal frame

Add 4-byte tag, recalculate FCS

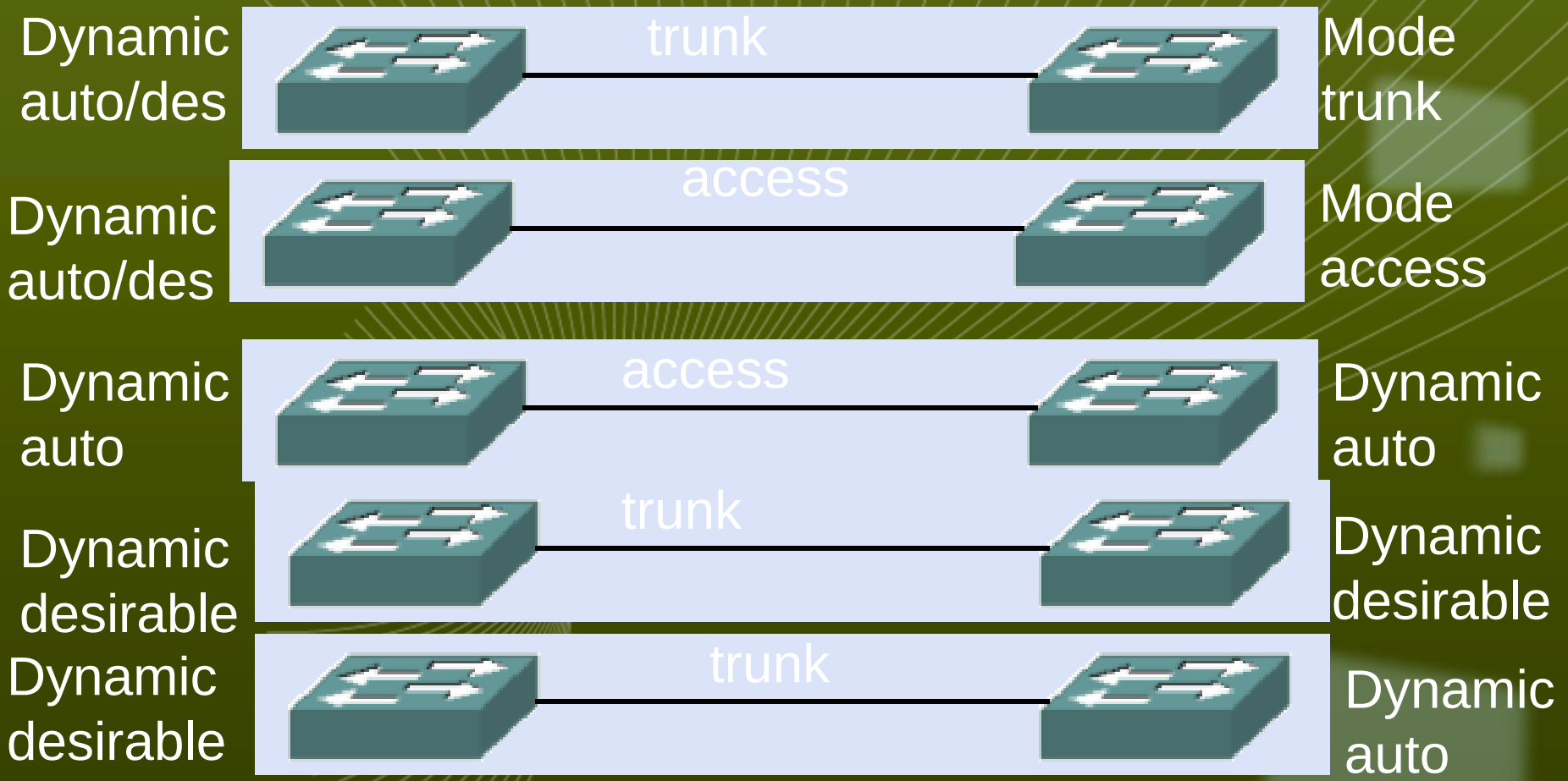
Native VLAN

- Untagged frames received on a trunk port are forwarded on to the native VLAN.
- Frame received from the native VLAN should be untagged.
- Switch will drop tagged frames received from the native VLAN. This can happen if non-Cisco devices are connected.

Configure trunk port

- Make a port into a trunk port and tell it which VLAN is native.
- SW1(config)#int fa0/1
- SW1(config-if)switchport mode trunk
- SW1(config-if)switchport trunk native vlan 99
- By default native VLAN is 1.

Dynamic trunking protocol



Create a VLAN

- SW1(config)#vlan 20
- SW1(config-vlan)#name Finance
- SW1(config-vlan)#end
- VLAN will be saved in VLAN database rather than running config.
- If you do not give it a name then it will be called vlan0020.

Assign port to VLAN

- SW1(config)#int fa 0/14
- SW1(config-if)#switchport mode access
- SW1(config-if)#switchport access vlan 20
- SW1(config-if)#end

show vlan brief

- List of VLANs with ports

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
20   student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Show commands

- show vlan brief (list of VLANs and ports)
- show vlan summary
- show interfaces vlan (up/down, traffic etc)
- Show interfaces fa0/14 switchport (access mode, trunking)

Remove port from VLAN

- SW1(config)#int fa 0/14
- SW1(config-if)#no switchport access vlan
- SW1(config-if)#end
- The port goes back to VLAN 1.
- If you assign a port to a new VLAN, it is automatically removed from its existing VLAN.

Delete a VLAN

- SW1(config)#no vlan 20
- SW1(config)#end
- VLAN 20 is deleted.
- Any ports still on VLAN 20 will be inactive – not on any VLAN. They need to be reassigned.

Delete VLAN database

- Erasing the startup configuration does not get rid of VLANs because they are saved in a separate file.
- SW1#delete flash:vlan.dat
- Switch goes back to the default with all ports in VLAN 1.
- You cannot delete VLAN 1.

Configure trunk

- SW1(config)#int fa0/1
- SW1(config-if)#switchport mode trunk
- SW1(config-if)#switchport trunk native vlan 99
- SW1(config-if)#switchport trunk allowed vlan add 10, 20, 30
- SW1(config-if)#end

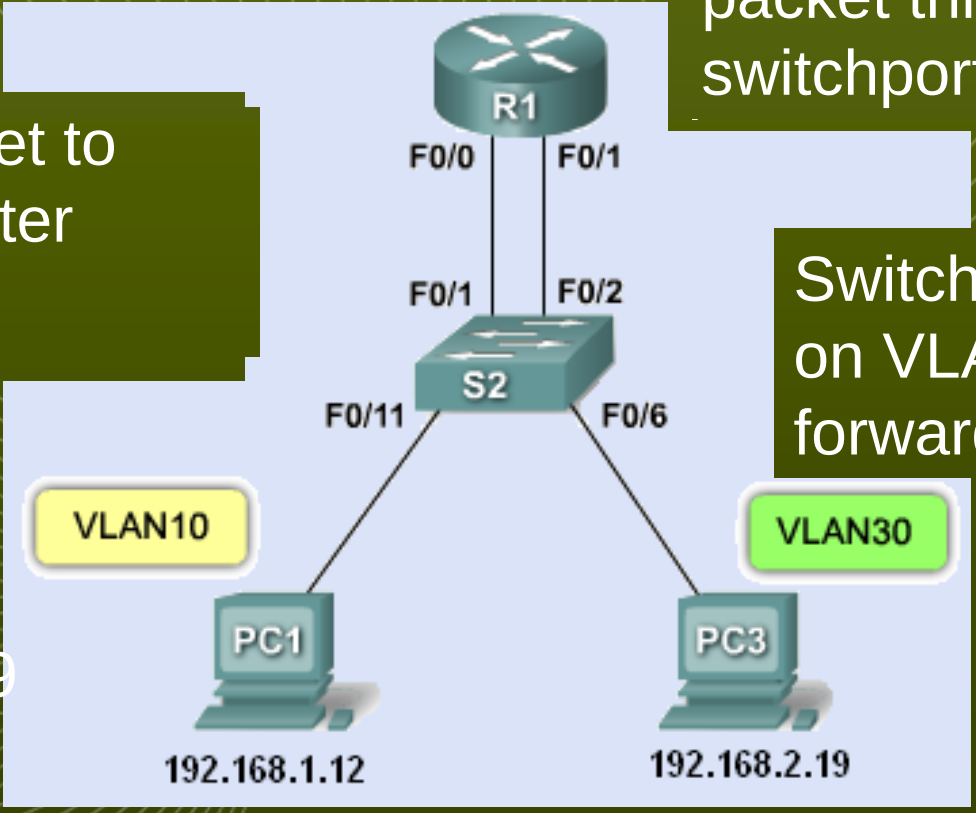
Traditional inter-VLAN routing

- The router has one physical port for each VLAN.
- Each port has an IP address on its own VLAN.
- Routing is the same as routing between any subnets.

Traditional inter-VLAN routing

Router sends out packet through F0/1 to switchport F0/2

Send packet to F0/0 of router



Switchport F0/2 is on VLAN30 and forwards to PC3.

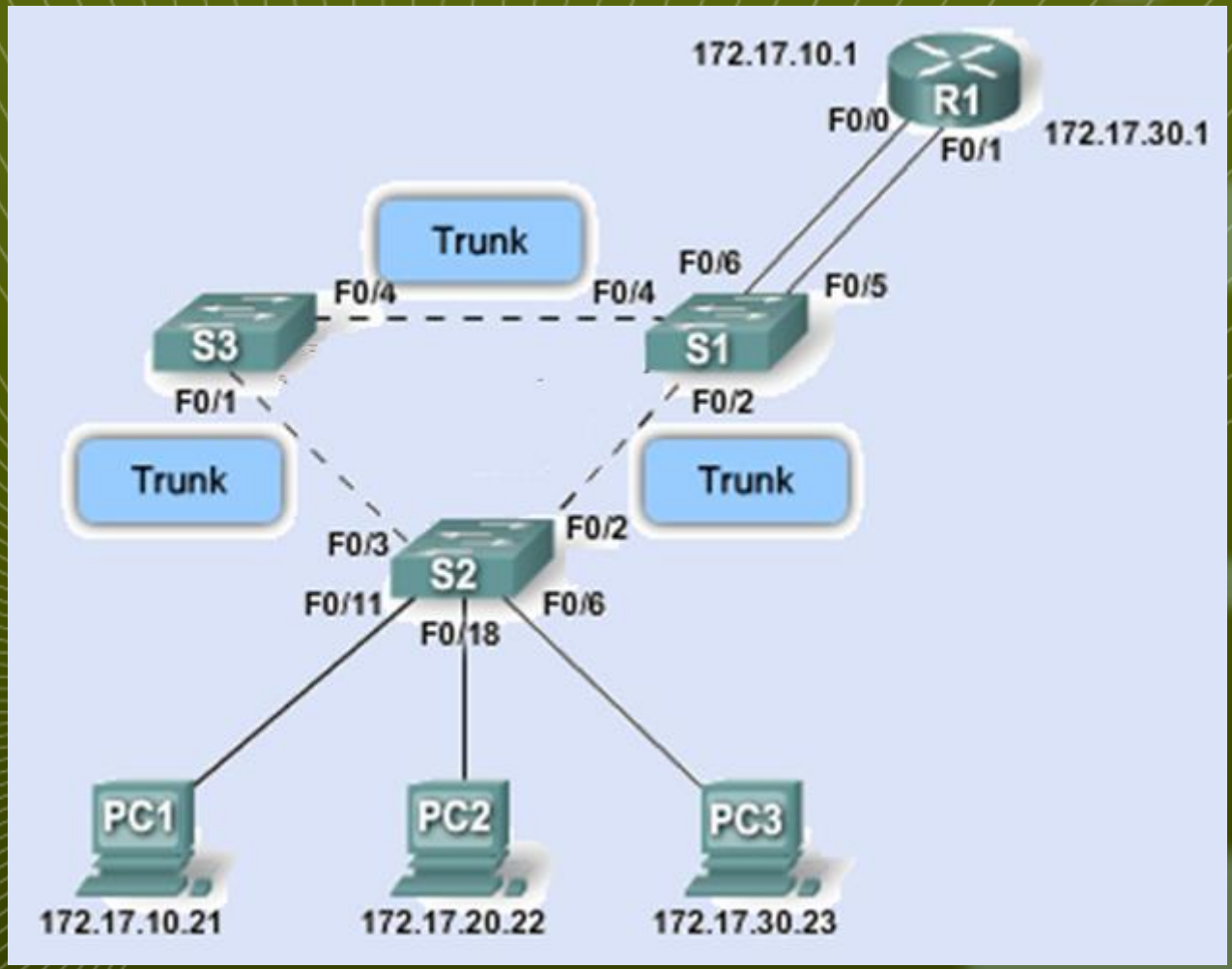
PC1 has a packet for 192.168.2.19 – different subnet

Traditional inter-VLAN routing

Trunks between switches.

No trunk to router.

No tags on frames to router.

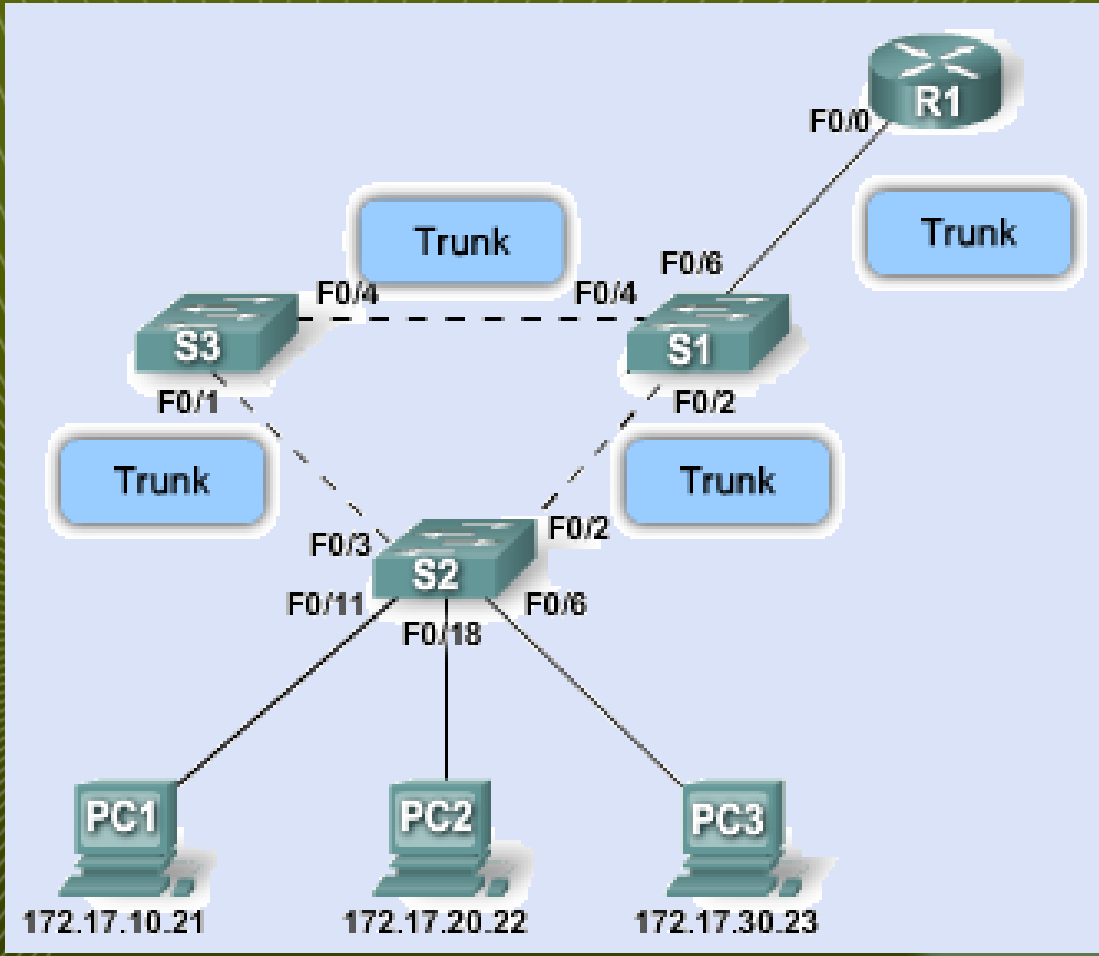


Trunk to the router

- You soon run out of router ports.
- What about making a trunk link to the router?
- A trunk link can be used with several VLANs on the same physical port.
- But each VLAN needs a different IP address.
- So use subinterfaces, each with its own IP address.

Router on a stick

- R1 F0/0 has subinterfaces, one for each VLAN.
- Each has its own IP address.
- VLAN tags on trunk.



Availability of trunking

- Not all routers allow subinterfaces for VLAN trunking on Ethernet ports.
- It depends on the IOS feature set.
- Some of ours do, others do not.

Subinterfaces

- Subinterfaces take the interface name followed by a dot and a number.
- It is normal to use the VLAN number. If this ties in with the IP address, even better.
- E.g. interface f0/0.10
- The subinterfaces each have an IP address.
- The physical interface has no IP address
- The physical interfaces needs no shutdown

Configuring subinterfaces

- R1(config)#interface f0/0.10
- R1(config-subif)#encapsulation dot1q 10
- R1(config-subif)#ip address 172.17.10.1 255.255.255.0
- (add any other subinterfaces)
- R1(config-subif)#interface f0/0
- R1(config-if)#no shutdown

Routing table

- Subinterfaces are shown

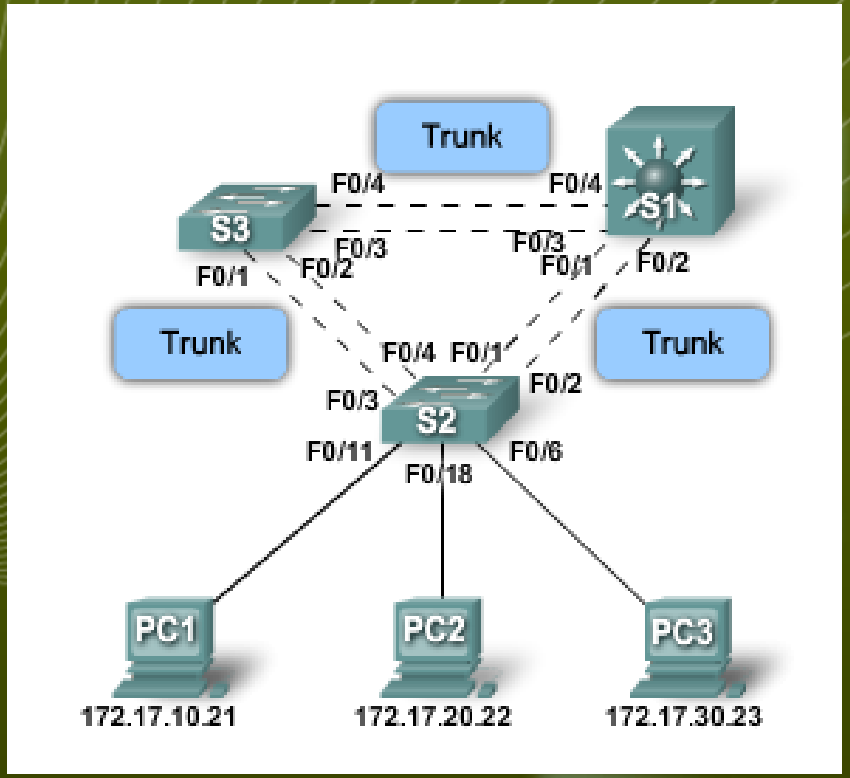
```
     172.17.0.0/24 is subnetted, 2 subnets
C       172.17.10.0 is directly connected,
     FastEthernet0/0.10
C       172.17.30.0 is directly connected,
     FastEthernet0/0.30
```

Subinterface considerations

- Routers have a limited number of interfaces, so subinterfaces help where there are many VLANs.
- Subinterfaces share the bandwidth on a physical interface so can cause bottlenecks.
- Cheaper to use subinterfaces.
- Simpler physical layout but more complex configuration with subinterfaces.

Multilayer switch

- A multilayer switch can route between VLANs.



INSTITUT TEKNOLOGI TELKOM

Thank You

Ref : S Ward Abingdon and Witney College