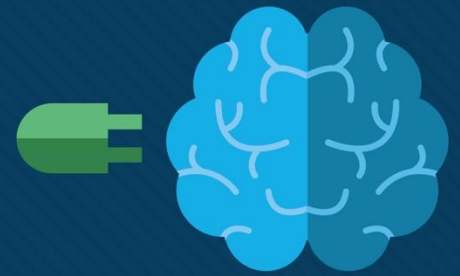


Chapter 1
Virtual LAN (VLAN)

CCNA Routing and Switching 6.0

Routing and Switching Essentials – Chapter 6

Scaling Networks – Chapter 2

Chapter 1 - Sections & Objectives

- VLAN Segmentation
  - Explain the purpose of VLANs in a switched network.
  - Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment.
- Inter-VLAN Routing Using Routers
  - Describe the two options for configuring Inter-VLAN routing.
  - Configure legacy Inter-VLAN Routing.
  - Configure Router-on-a-Stick Inter-VLAN Routing
- Layer 3 Switching
  - Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN.
    - Configure inter-VLAN routing using Layer 3 switching.
    - Troubleshoot inter-VLAN routing in a Layer 3 switched environment.

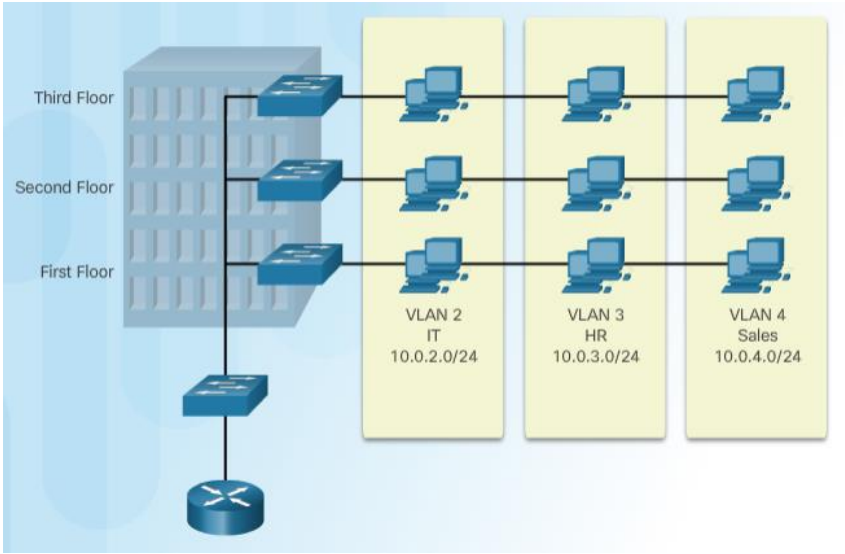
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

VLAN Segmentation

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

VLAN Definitions

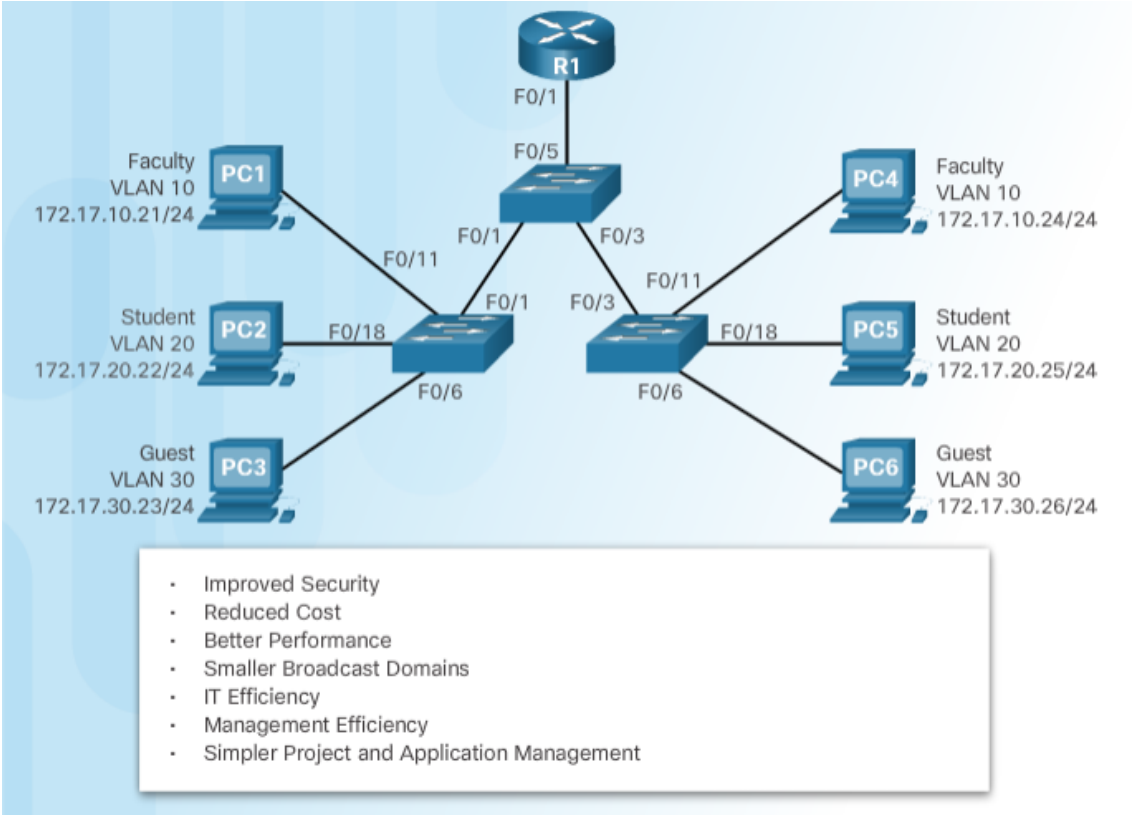
- VLANs can segment LAN devices without regard for the physical location of the user or device.
  - In the figure, IT users on the first, second, and third floors are all on the same LAN segment. The same is true for HR and Sales users.
- A VLAN is a logical partition of a Layer 2 network.
  - Multiple partitions can be created and multiple VLANs can co-exist.
  - The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
  - Each VLAN is a broadcast domain that can span multiple physical LAN segments.
  - Hosts on the same VLAN are unaware of the VLAN's existence.



- VLANs are mutually isolated and packets can only pass between VLANs via a router.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Benefits of VLANs



- Improved Security
- Reduced Cost
- Better Performance
- Smaller Broadcast Domains
- IT Efficiency
- Management Efficiency
- Simpler Project and Application Management

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of VLANs

- Common types of VLANs:
  - **Default VLAN** – Also known as VLAN 1. All switch ports are members of VLAN 1 by default.
  - **Data VLAN** – Data VLANs are commonly created for specific groups of users or devices. They carry user generated traffic.
  - **Native VLAN** – This is the VLAN that carries all untagged traffic. This is traffic that does not originate from a VLAN port (e.g., STP BPDU traffic exchanged between STP enabled switches). The native VLAN is VLAN 1 by default.
  - **Management VLAN** – This is a VLAN that is created to carry network management traffic including SSH, SNMP, Syslog, and more. VLAN 1 is the default VLAN used for network management.

Default VLAN Assignment

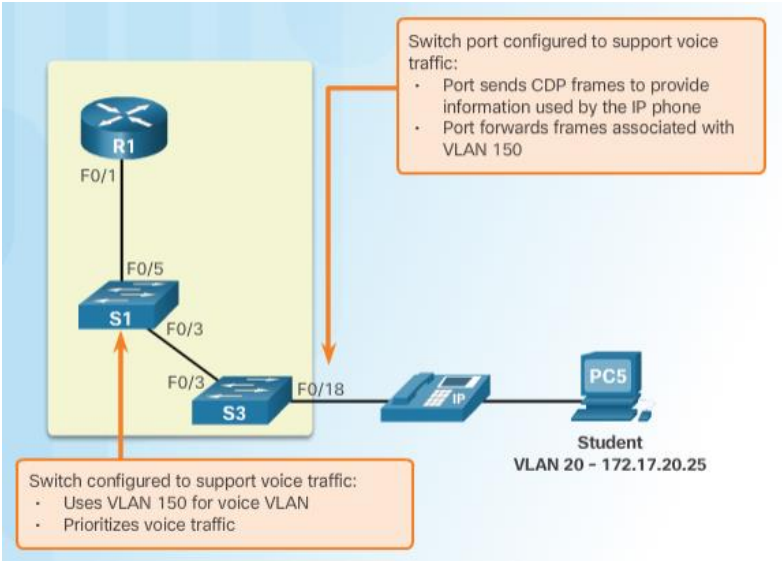
```
Switch# show vlan brief

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
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

Initially, all switch ports are members of VLAN 1.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Voice VLANs

- To support time-sensitive voice traffic, some vender switches, namely Cisco, support a voice VLAN that requires:
  - Assured bandwidth
  - Delay of less than 150 ms across the network to ensure voice quality
  - Transmission priority over other types of network traffic
  - Ability to be routed around congested areas on the network.

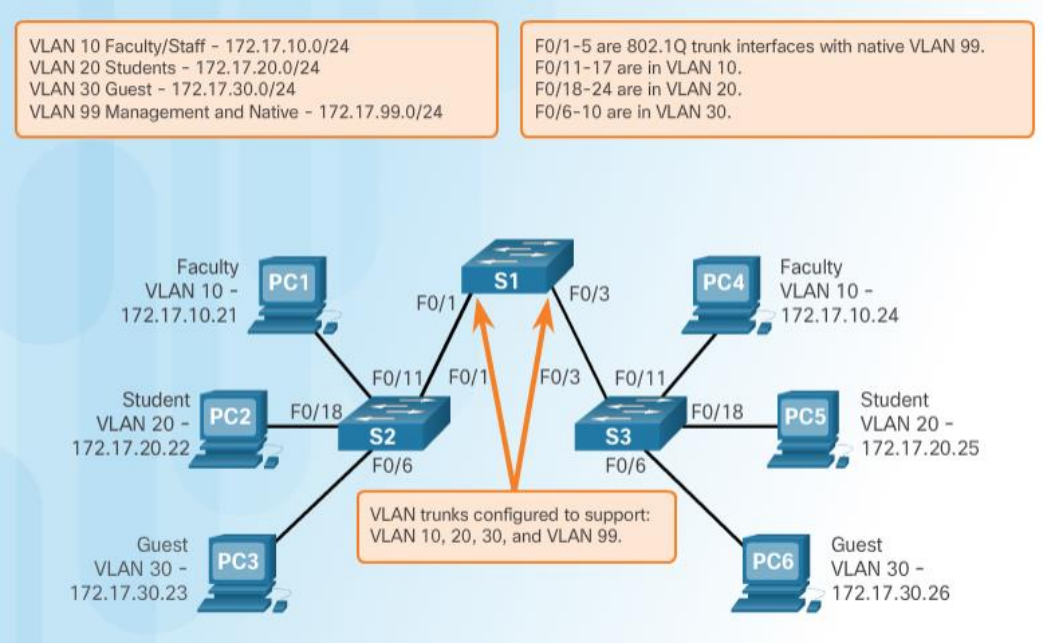


- The voice VLAN feature enables access ports to carry user and IP voice traffic.
  - In the figure, the S3 F0/18 interface has been configured to tag student traffic on VLAN 20 and voice traffic on VLAN 150.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

VLAN Trunks

- A VLAN trunk is a point-to-point link that carries more than one VLAN.
  - Usually established between switches to support intra VLAN communication.
  - A VLAN trunk or trunk ports are not associated to any VLANs.
- Cisco IOS supports IEEE 802.1q, a popular VLAN trunk protocol.

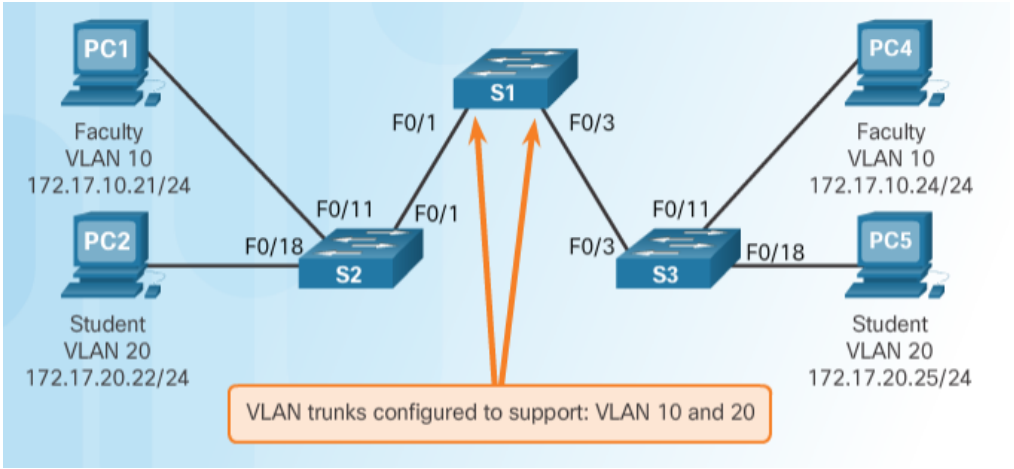


The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Controlling Broadcast Domains with VLANs

- If a switch port receives a broadcast frame, it forwards it out all ports except the originating port.
  - Eventually the entire network receives the broadcast because the network is one broadcast domain.
- VLANs can be used to limit the reach of broadcast frames because each VLAN is a broadcast domain.
  - VLANs help control the reach of broadcast frames and their impact in the network.
- In the figure, PC1 on VLAN 10 sends a broadcast frame.
  - Trunk links between S2 - S1 and S1 - S3 propagate the broadcast to other devices in VLAN 10.
  - Only devices in the same VLAN receive the broadcast therefore, PC4 would receive the broadcast.

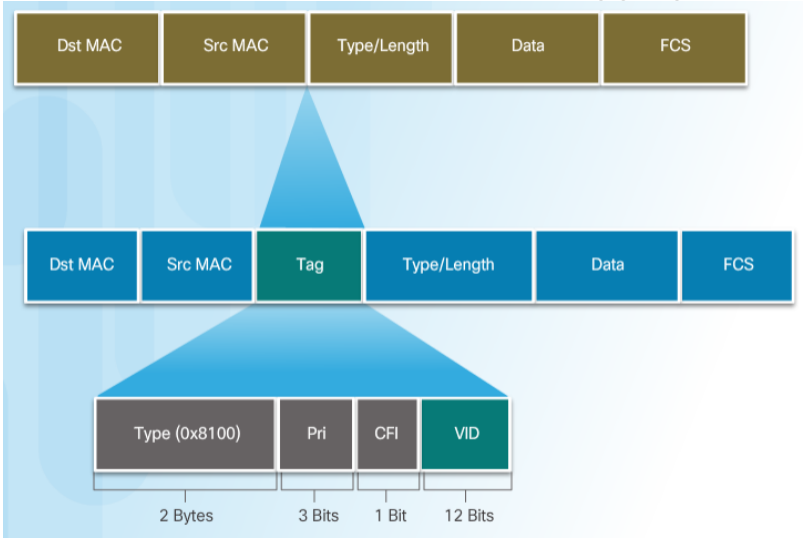


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tagging Ethernet Frames for VLAN Identification

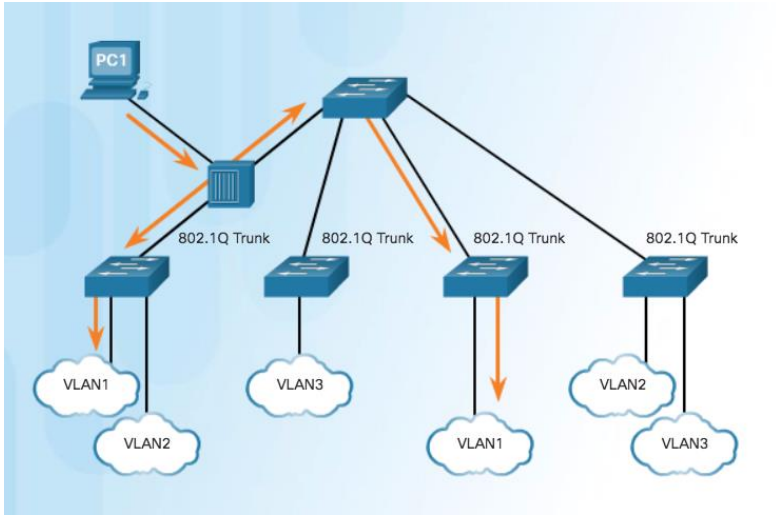
- Before a frame is forwarded across a trunk link, it must be tagged with its VLAN information.
  - Frame tagging is the process of adding a VLAN identification header to the frame.
  - It is used to properly transmit multiple VLAN frames through a trunk link.

- IEEE 802.1Q is a vey popular VLAN trunking protocol that defines the structure of the tagging header added to the frame.
  - Switches add VLAN tagging information after the Source MAC address field.
  - The fields in the 802.1Q VLAN tag includes VLAN ID (VID).
  - Trunk links add the tag information before sending the frame and then remove the tags before forwarding frames through non-trunk ports.



Native VLANs and 802.1Q Tagging

- Control traffic sent on the native VLAN should not be tagged.
- Frames received untagged, remain untagged and are placed in the native VLAN when forwarded.
- If there are no ports associated to the native VLAN and no other trunk links, an untagged frame is dropped.
- When configuring a switch port on a Cisco switch, configure devices so that they do not send tagged frames on the native VLAN.
- In Cisco switches, the native VLAN is VLAN 1, by default.

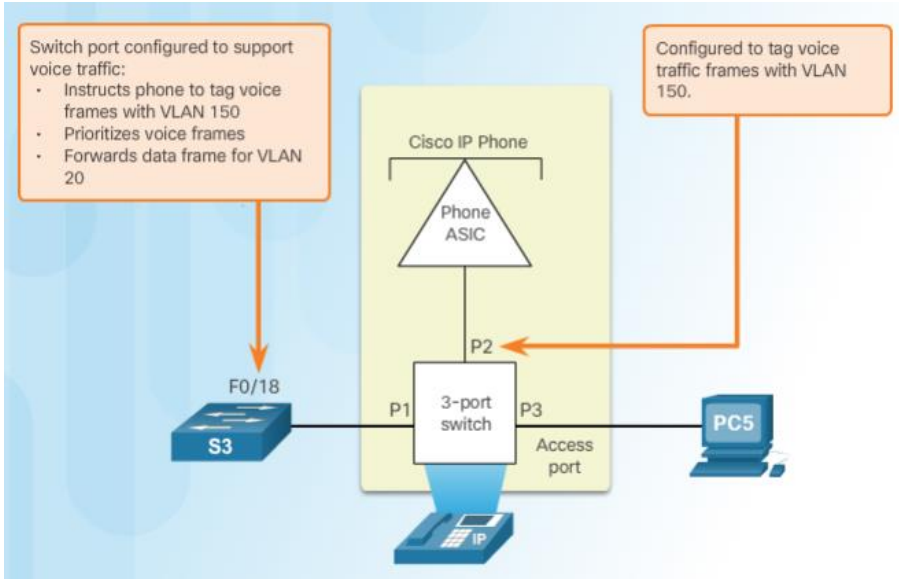


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Voice VLAN Tagging

- An access port connecting a Cisco IP phone can be configured to use two separate VLANs:
  - A VLAN for voice traffic
  - A VLAN for data traffic from a device attached to the phone.

- The link between the switch and the IP phone behaves like a trunk to carry traffic from both VLANs.



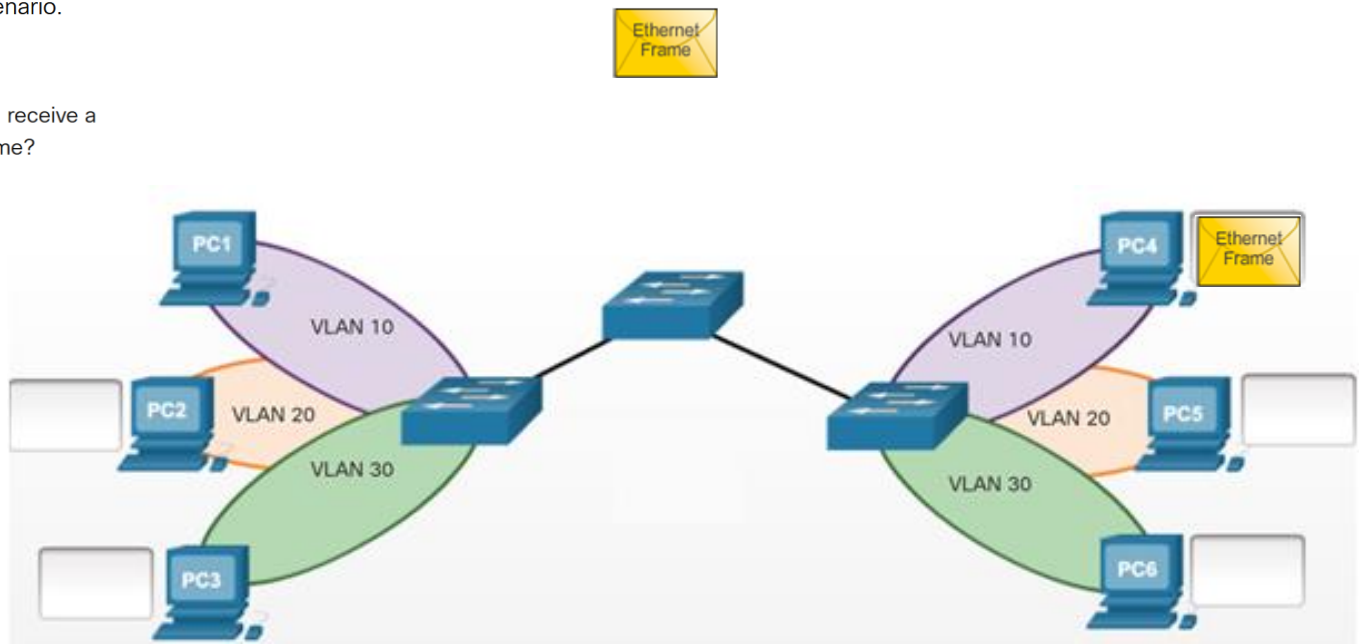
- Cisco IP Phone contains an integrated three-port 10/100 switch dedicated to these devices:
  - Port 1 connects to the switch or other VoIP device.
  - Port 2 is an internal 10/100 interface that carries the IP phone traffic.
  - Port 3 (access port) connects to a PC or other device.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Activity – VLAN trunk in action

Drag the Ethernet Frames (yellow envelopes) to their destination PCs for the scenario. Not all envelopes will be used in every scenario.

Scenario 1: PC 1 sends a broadcast. Which PCs will receive a copy of the broadcast frame?

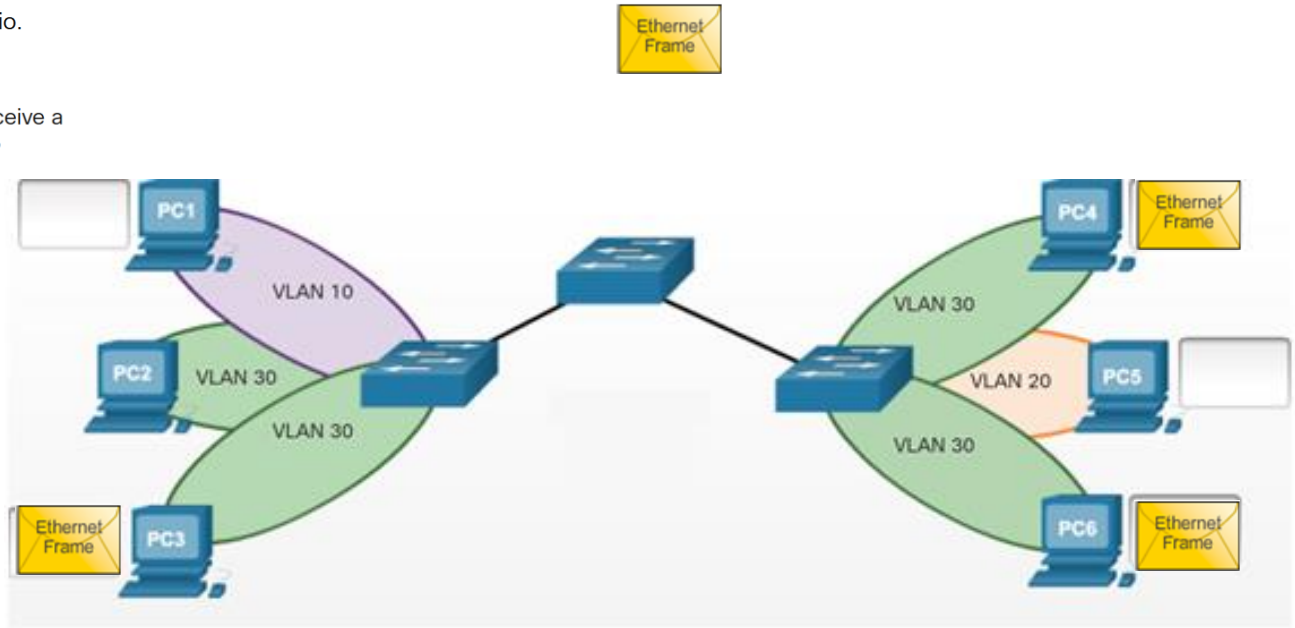


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Activity – VLAN trunk in action

Drag the Ethernet Frames (yellow envelopes) to their destination PCs for the scenario. Not all envelopes will be used in every scenario.

Scenario 2: PC 2 sends a broadcast. Which PCs will receive a copy of the broadcast frame?



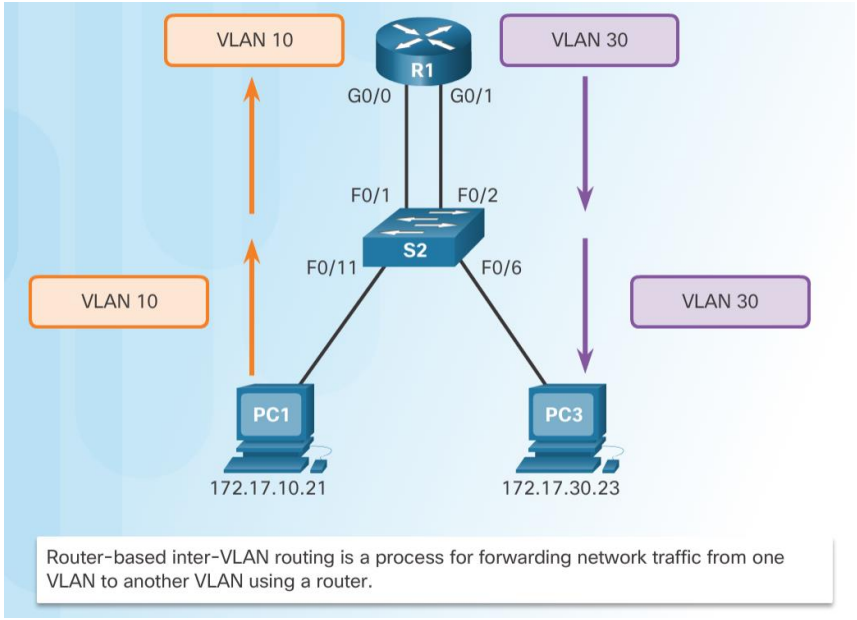
© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Inter-VLAN Routing Using Routers

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is Inter-VLAN Routing?

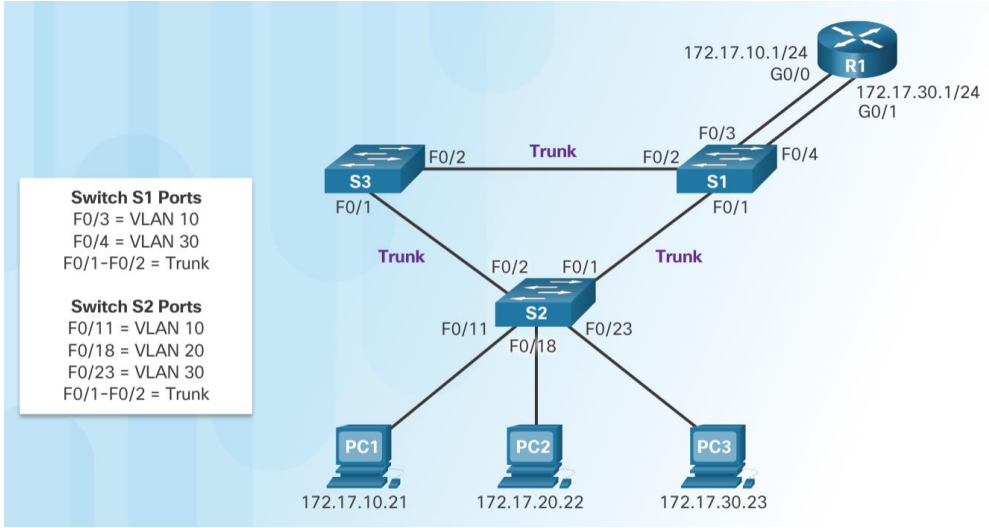
- Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.
- There are three options for inter-VLAN routing:
  - Legacy inter-VLAN routing
  - Router-on-a-Stick
  - Layer 3 switching using SVI



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Legacy Inter-VLAN Routing

- In the past:
  - Router interfaces were used to route between VLAN.
  - Each VLAN was connected to a different physical router interface.
  - Packets would arrive on the router through one interface, be routed and leave through another.
  - Because the router interfaces were connected to VLAN and had IP addresses from that specific VLAN, routing between VLANs was achieved.
  - Large networks with large number of VLAN required many router interfaces.



In this example, the router was configured with two separate physical interfaces to interact with the different VLAN and perform the routing.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

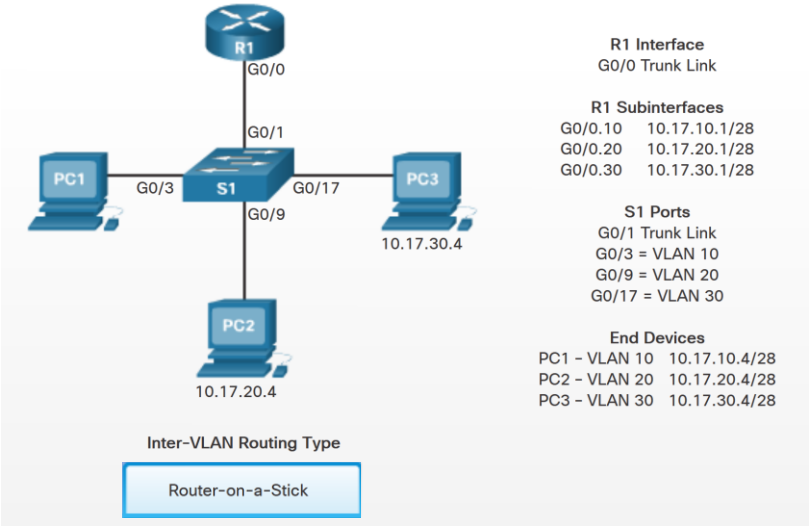
Activity – Identify the types of inter-VLAN routing (1)

Identify this topology as a legacy, router-on-a-stick, or multilayer switch inter-VLAN routing by dragging the appropriate answer to the field provided.

Multilayer Switch

Router-on-a-Stick

Legacy



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

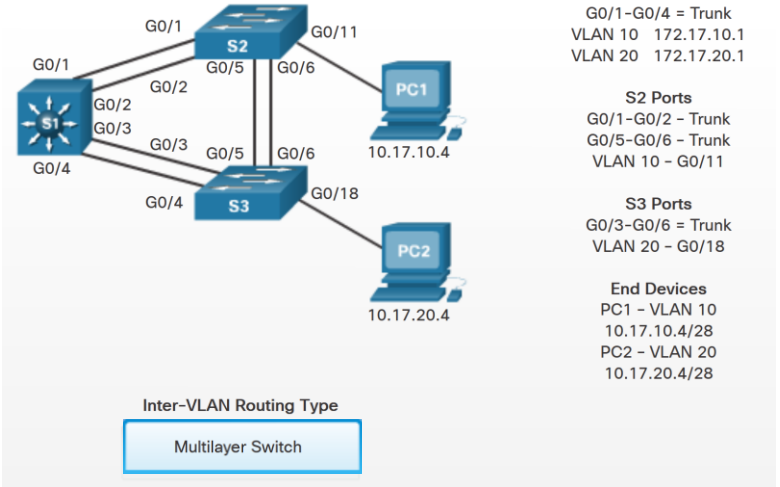
Activity – Identify the types of inter-VLAN routing (2)

Identify this topology as a legacy, router-on-a-stick, or multilayer switch inter-VLAN routing by dragging the appropriate answer to the field provided.

Multilayer Switch

Router-on-a-Stick

Legacy



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

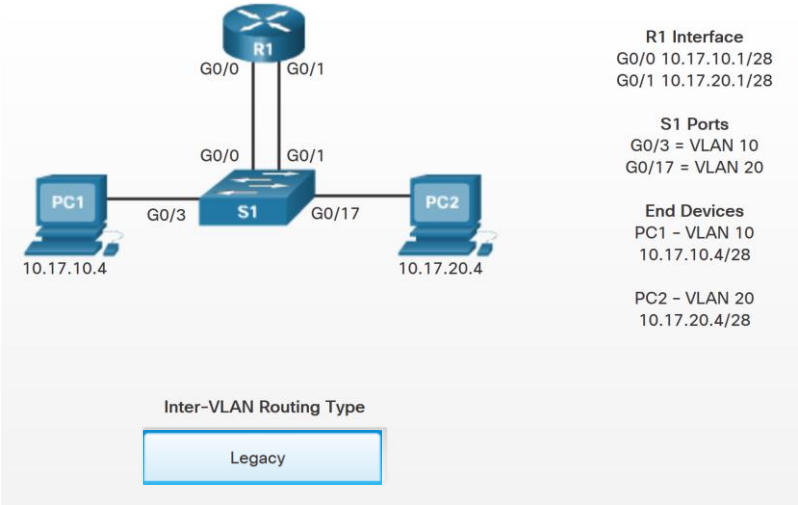
Activity – Identify the types of inter-VLAN routing (3)

Identify this topology as a legacy, router-on-a-stick, or multilayer switch inter-VLAN routing by dragging the appropriate answer to the field provided.

Multilayer Switch

Router-on-a-Stick

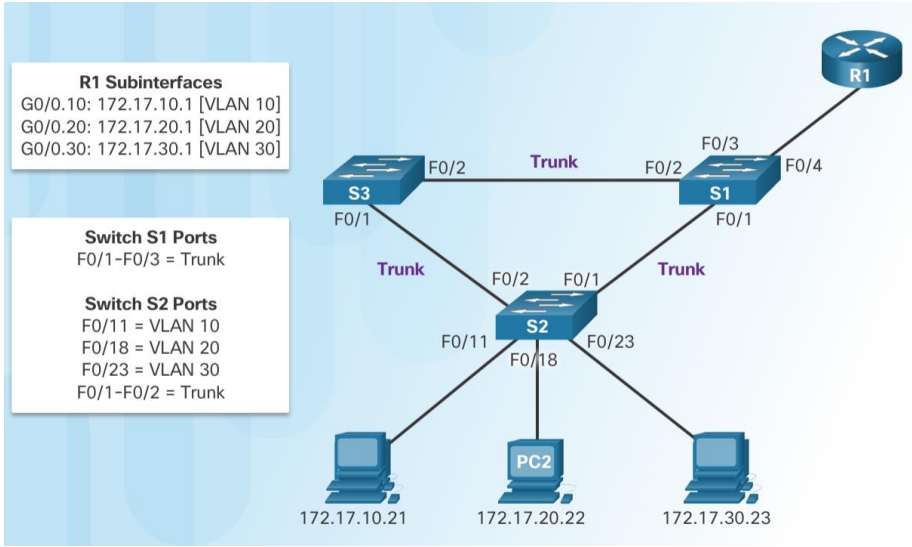
Legacy



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Router-on-a-Stick Inter-VLAN Routing

- The router-on-a-stick approach uses only one of the router's physical interface.
  - One of the router's physical interfaces is configured as an 802.1Q trunk port so it can understand VLAN tags.
  - Logical subinterfaces are created; one subinterface per VLAN.
  - Each subinterface is configured with an IP address from the VLAN it represents.
  - VLAN members (hosts) are configured to use the subinterface address as a default gateway.



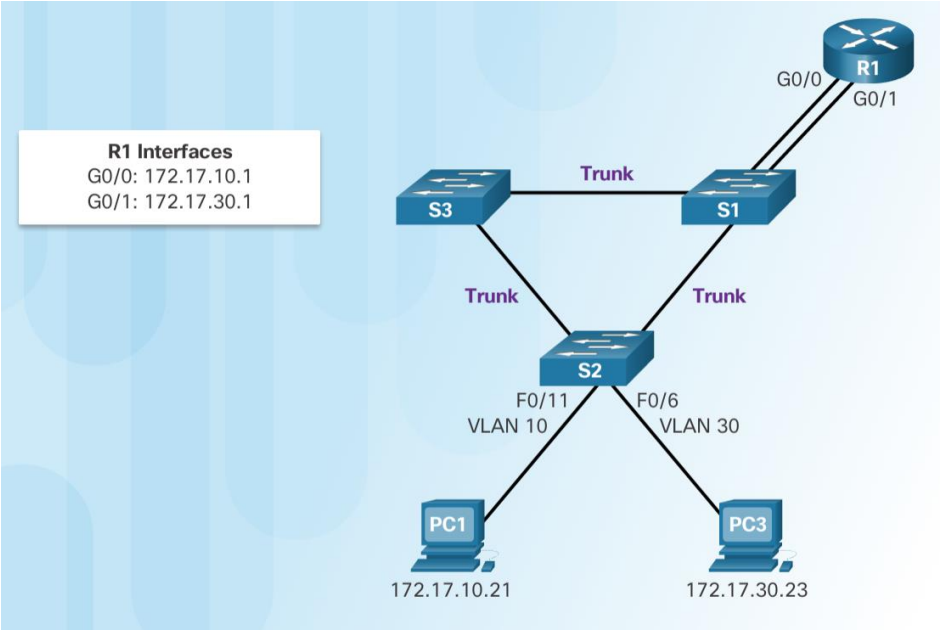
In this example, the R1 interface is configured as a trunk link and connects to the trunk F0/4 port on S1.

- Router accepts VLAN-tagged traffic on the trunk interface
- Router internally routes between the VLAN using subinterfaces.
- Router then forwards the routed traffic as VLAN-tagged for the destination VLAN out the trunk link.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

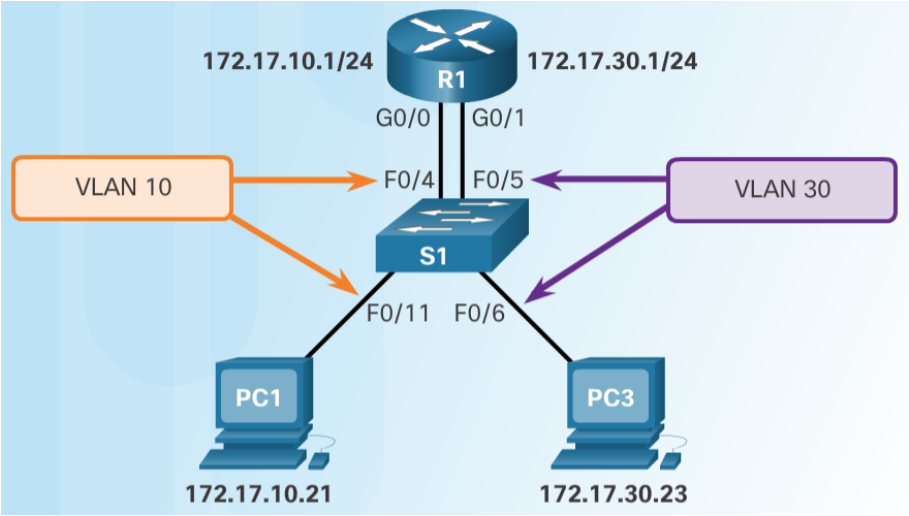
Configure Legacy Inter-VLAN Routing: Preparation

- Legacy inter-VLAN routing requires routers to have multiple physical interfaces.
- Each one of the router's physical interfaces is connected to a unique VLAN.
- Each interface is also configured with an IP address for the subnet associated with the particular VLAN.
- Network devices use the router as a gateway to access the devices connected to the other VLANs.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Legacy Inter-VLAN Routing: Switch Configuration

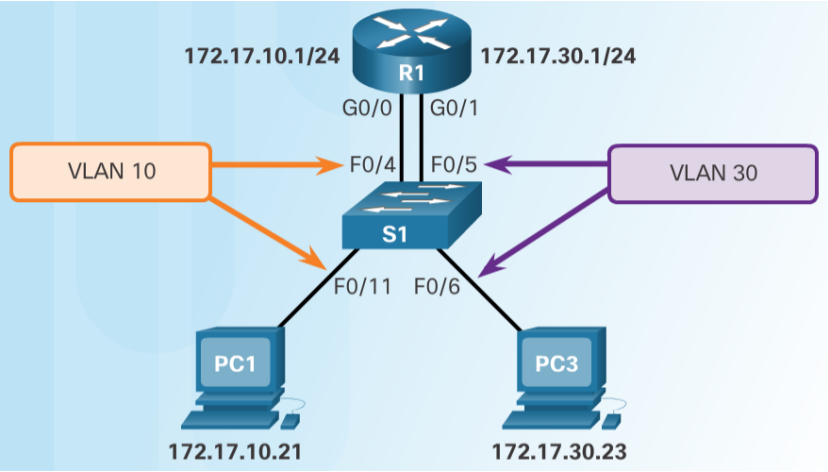


- Configure the VLAN on the switch and then assign the ports to their respective VLAN.
- In this example, the S1 ports are configured as follows:
  - Ports F0/4 and F0/11 of S1 are on VLAN 10
  - Ports F0/5 and F0/16 ports are on VLAN 30.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Legacy Inter-VLAN Routing: Router Interface config



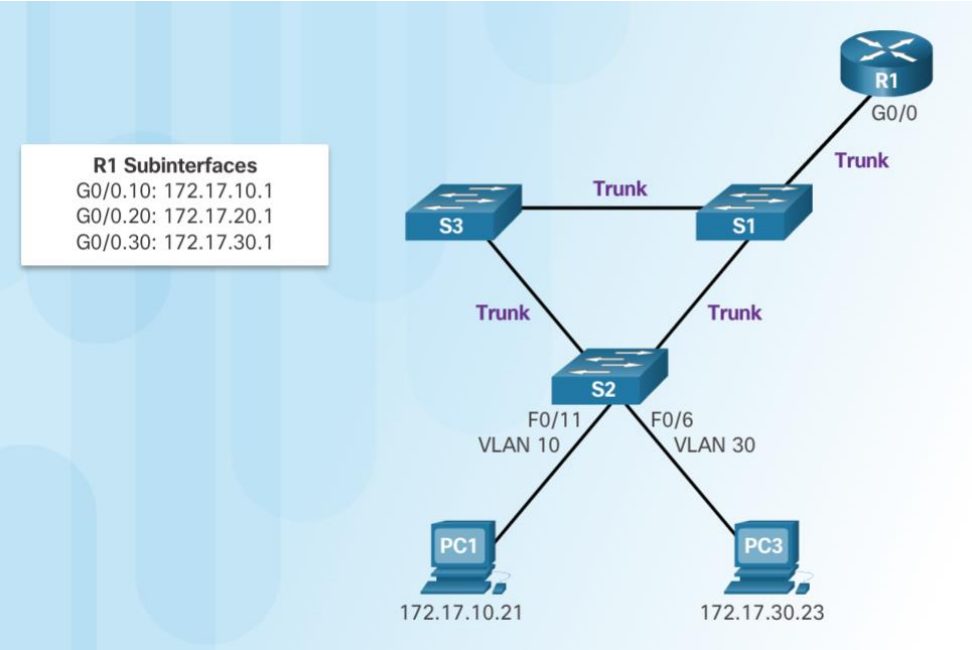
- Next configure the router interfaces.

```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

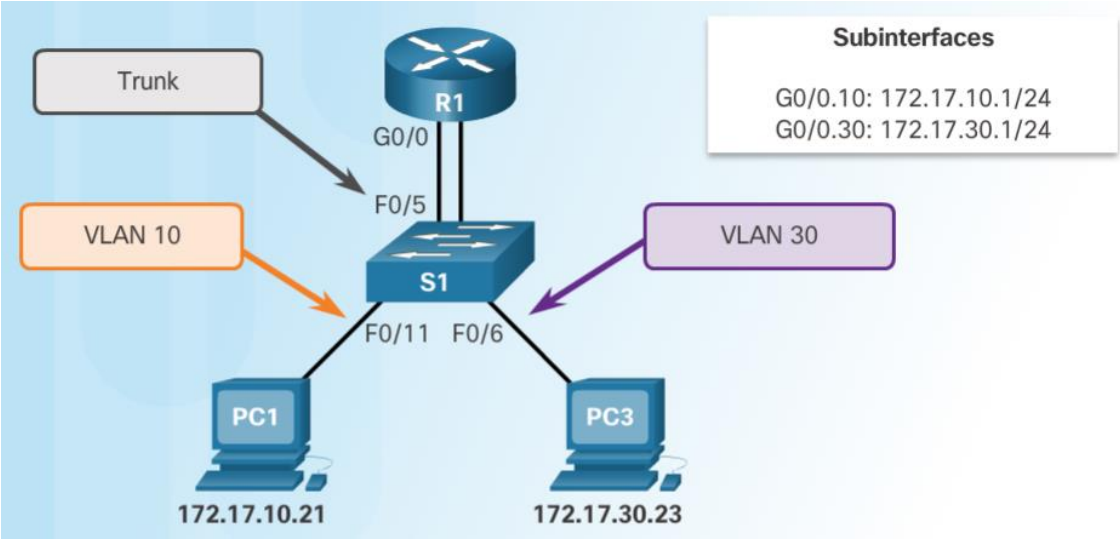
Configure Router-on-a Stick: Preparation

- An alternative to legacy inter-VLAN routing is to use VLAN trunking and subinterfaces.
- VLAN trunking allows a single physical router interface to route traffic for multiple VLAN.
- The physical interface of the router must be connected to a trunk link on the adjacent switch.
- On the router, subinterfaces are created for each unique VLAN.
- Each subinterface is assigned an IP address specific to its subnet or VLAN and is also configured to tag frames for that VLAN.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Router-on-a Stick: Switch Configuration

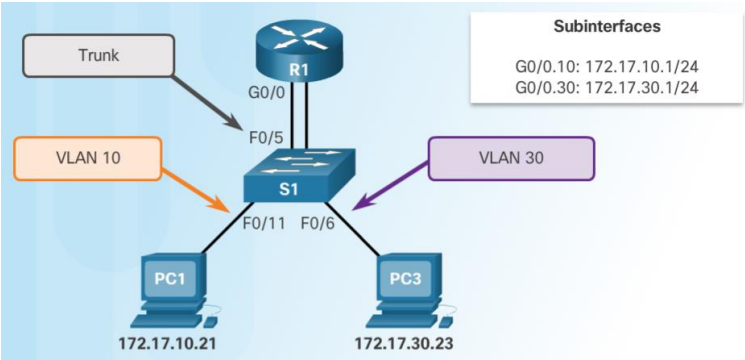


- To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.

```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Router-on-a Stick: Router Subinterface Configuration



- The router-on-a-stick method requires subinterfaces to be configured for each routable VLAN.
  - The subinterfaces must be configured to support VLANs using the **encapsulation dot1Q** *VLAN-ID* interface configuration command.

```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface   GigabitEthernet0/0, changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Router-on-a Stick: Verifying Subinterfaces

- By default, Cisco routers are configured to route traffic between local subinterfaces.
  - As a result, routing does not specifically need to be enabled.
- Use the **show vlan** and **show ip route** commands to verify the subinterface configurations.

```
R1# show vlan
<output omitted>

Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:     Address:         Received:      Transmitted:
         IP                 172.17.10.1            11                18
<output omitted>

Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:     Address:         Received:      Transmitted:
         IP                 172.17.30.1            11                 8
<output omitted>
```

The **show vlan** command displays information about the Cisco IOS VLAN subinterfaces.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF, IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, i - IS-IS,
       su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP,
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C     172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L     172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C     172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L     172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

The **show ip route** command displays the routing table containing the networks associated with outgoing subinterfaces.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

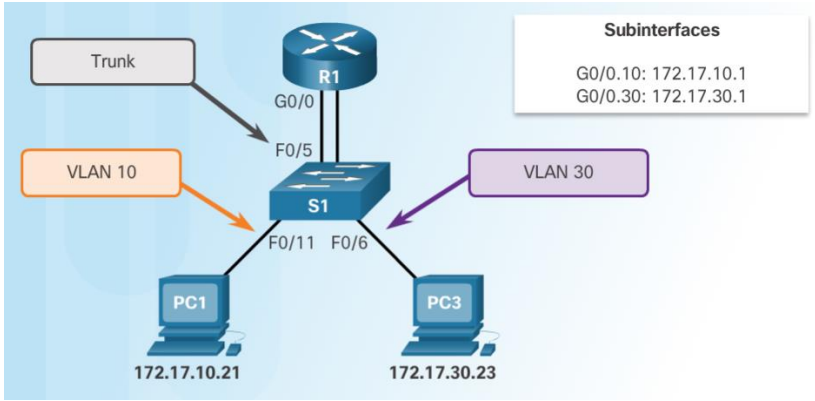
Configure Router-on-a Stick: Verifying Routing

- Remote VLAN device connectivity can be tested using the **ping** command.
  - The command sends an ICMP echo request and when a host receives an ICMP echo request, it responds with an ICMP echo reply.

```
PC1> ping 172.17.30.23

Pinging 172.17.30.23 with 32 bytes of data:

Reply from 172.17.30.23: bytes=32 time=17ms TTL=127
Reply from 172.17.30.23: bytes=32 time=15ms TTL=127
Reply from 172.17.30.23: bytes=32 time=18ms TTL=127
Reply from 172.17.30.23: bytes=32 time=19ms TTL=127

Ping statistics for 172.17.30.23:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- **Tracert** is a useful utility for confirming the routed path taken between two devices.

```
Approximate round trip times in milli-seconds:
   Minimum = 15ms, Maximum = 19ms, Average = 17ms

PC1> tracert 172.17.30.23

Tracing route to 172.17.30.23 over a maximum of 30 hops:

 1    9 ms      7 ms      9 ms      172.17.10.1
 2    16 ms     15 ms     16 ms     172.17.30.23

Trace complete.
```

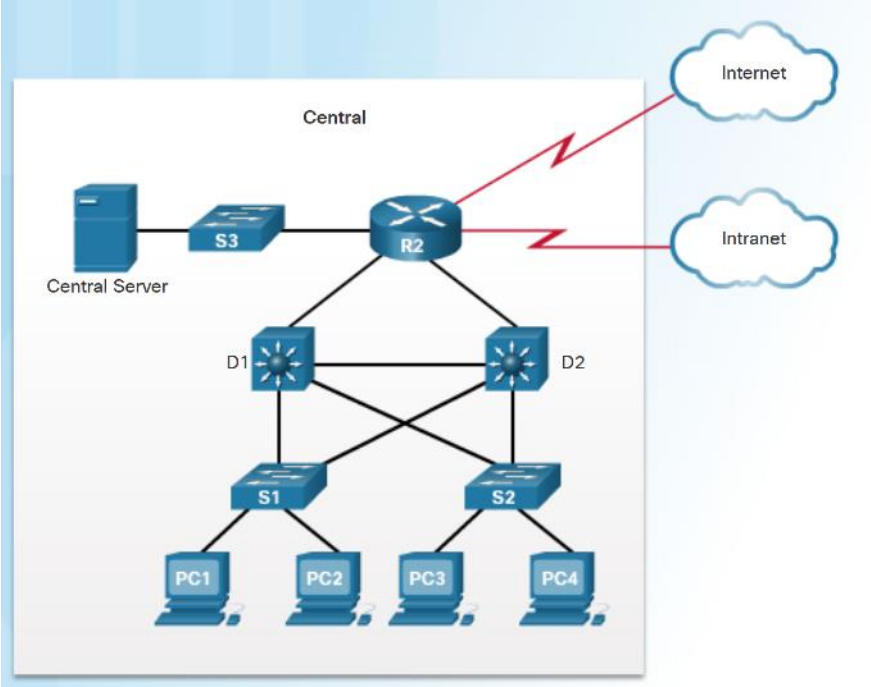


© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Layer 3 Switching

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Introduction to Layer 3 Switching

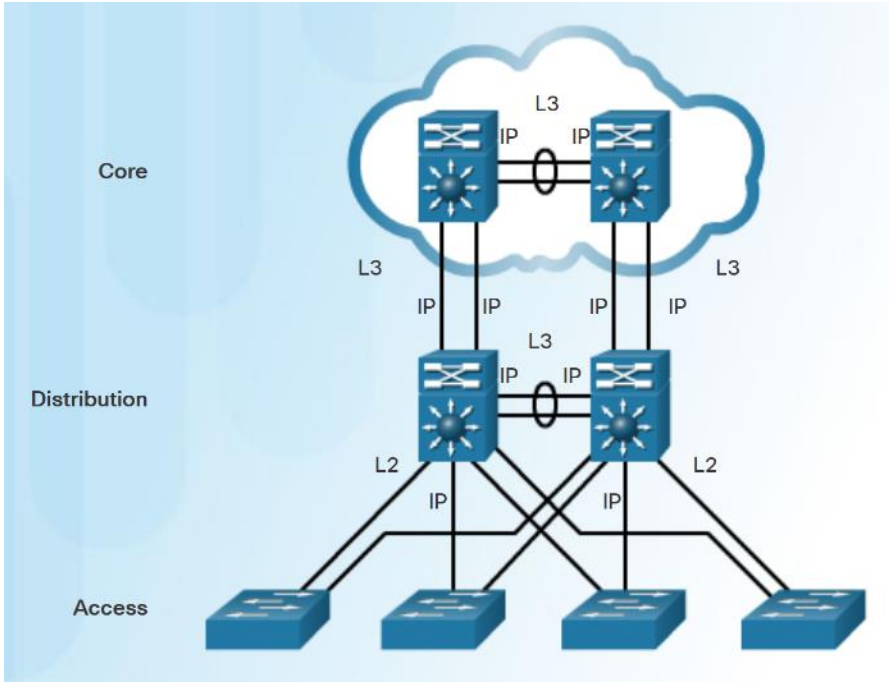


- Multilayer switches provide high-packet processing rates using hardware-based switching.
- Catalyst multilayer switches support the following types of Layer 3 interfaces:
  - **Routed port** - A layer 3 interface
  - **Switch virtual interface (SVI)** - Virtual Interface for inter- VLAN routing
- All Layer 3 Cisco Catalyst switches support routing protocols, but several models require enhanced software for specific routing protocol features.
- Catalyst 2960 Series switches running IOS 12.2(55) or later, support static routing.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Inter-VLAN Routing with Switch Virtual Interfaces

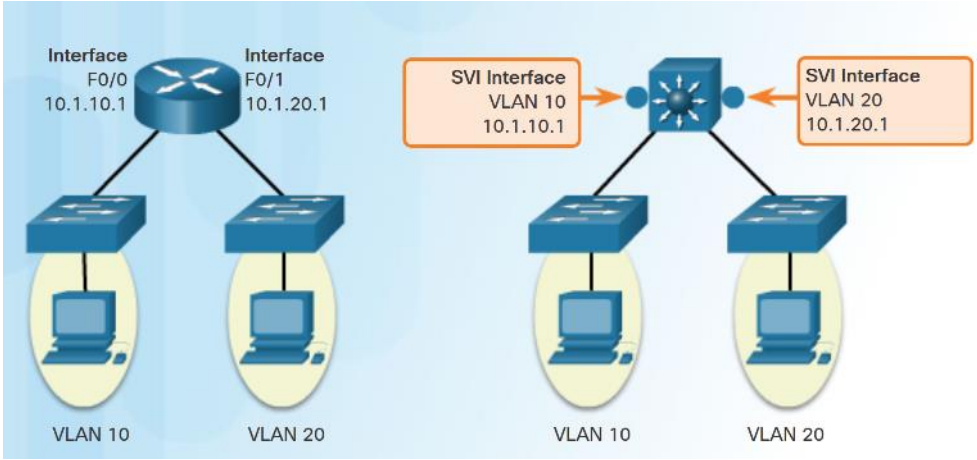
- In the early days of switched networks, switching was fast and routing was slow. Therefore the layer 2 switching portion was extended as much as possible into the network.
- Now routing can be performed at wire speed, and is performed at both the distribution and core layers.
- Distribution switches are configured as Layer 3 gateways using Switch Virtual Interfaces (SVIs) or routed ports.
- Routed ports are usually implemented between the distribution and core layers.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

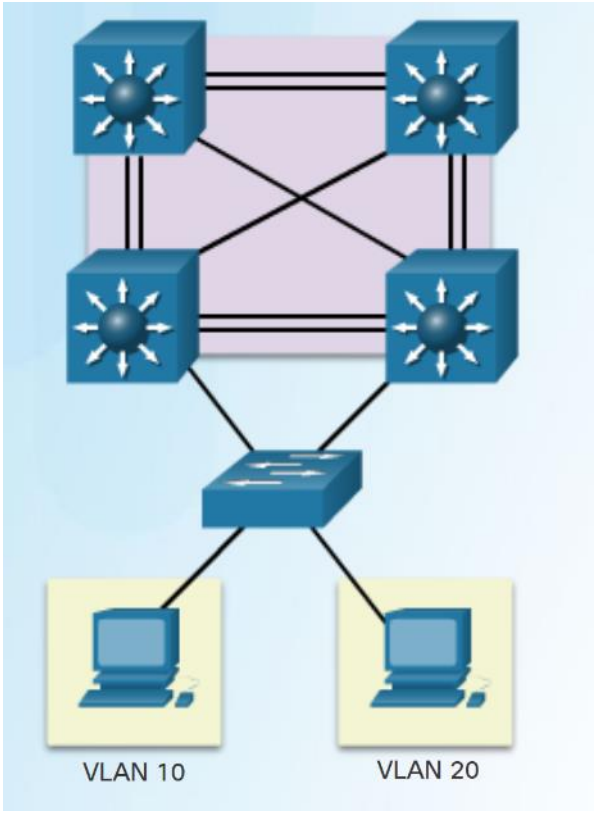
Inter-VLAN Routing with Switch Virtual Interfaces (Cont.)

- An SVI is a virtual interface that is configured within a multilayer switch:
  - To provide a gateway for a VLAN so that traffic can be routed into or out of that VLAN.
  - To provide Layer 3 IP connectivity to the switch.
  - To support routing protocol and bridging configurations.
- Advantages of SVIs:
  - Faster than router-on-a-stick.
  - No need for external links from the switch to the router for routing.
  - Not limited to one link. Layer 2 EtherChannels can be used to get more bandwidth.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Inter-VLAN Routing with Routed Ports

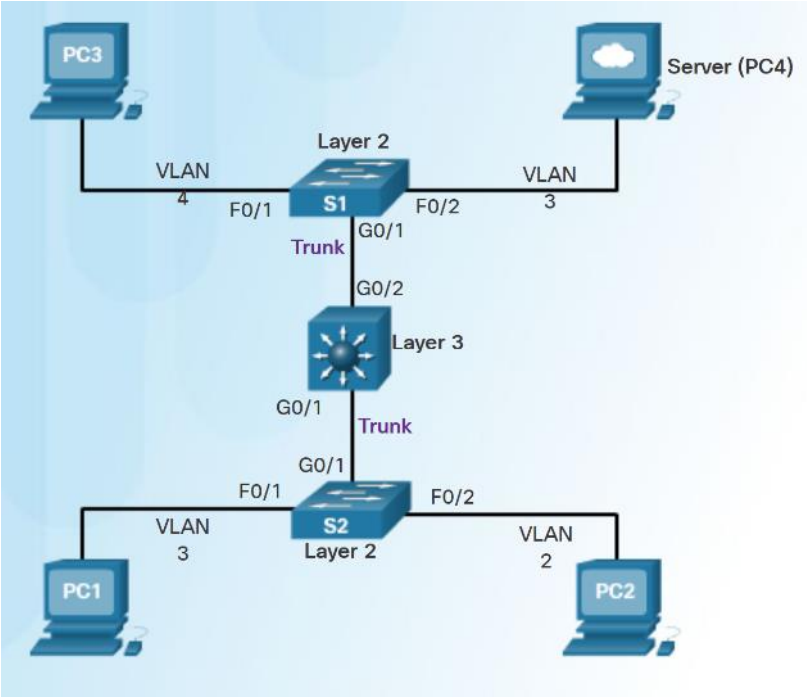


- A routed port is a physical port that acts similarly to an interface on a router:
  - It is not associated with a particular VLAN.
  - It does not support subinterfaces.
- Routed ports are primarily configured between switches in the core and distribution layer.
- Use the **no switchport interface** command on the appropriate port to configure a routed port.

Note: Routed ports are not supported on Catalyst 2960 Series switches.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Layer 3 Switch Configuration Issues



- To troubleshoot Layer 3 switching issues check the following:
  - **VLANs** – verify correct configuration.
  - **SVIs** - verify correct IP, subnet mask and VLAN number.
  - **Routing** - verify that either static or dynamic routing is correctly configured and enabled.
  - **Hosts** – verify correct IP, subnet mask, and default gateway.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 1: Inter-VLAN routing

- Explain how VLANs segment broadcast domains in a small to medium-sized business network.
- Implement VLANs to segment a small to medium-sized business network..
- Configure routing between VLANs in a small to medium-sized business network.
- Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN.
- Configure enhanced inter-switch connectivity technologies.
- Troubleshoot issues in an inter-VLAN routing environment.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential