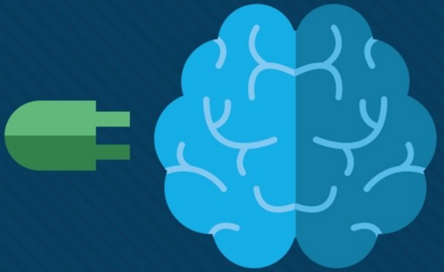


Module 4: Inter-VLAN Routing

Instructor Materials

Switching, Routing and Wireless
Essentials v7.0 (SRWE)

Téma 4.1

Co podle vás přispívá k omezení počtu VLAN podporovaných Router-on-a-Stick Inter-VLAN Routing?

Jaký je podle vás rozdíl mezi interface loopbacku routeru a subinterface routeru?

Téma 4.2

Jaká je primární výhoda uspořádání Router-on-a-stick na rozdíl od Legacy Inter-VLAN Routing?

Jak router zpracovává nativní VLAN?

Téma 4.3

Jaké jsou největší úspory, kterých můžete dosáhnout při použití přepínače L3 jako směrovače Inter-VLAN?

Jaký je dopad příkazu `no switchport`?

Téma 4.4

Co je podle vás nejčastější příčinou chyb při implementaci směrování Inter-VLAN?

Jaký druh směrování Inter-VLAN je podle vás vhodný z hlediska nejnižšího počtu chyb při implementaci?

Module Objectives

Module Objective: Troubleshoot inter-VLAN routing on Layer 3 devices

Topic Title	Topic Objective
Inter-VLAN Routing Operation	Describe options for configuring inter-VLAN routing.
Router-on-a-Stick Inter-VLAN Routing	Configure router-on-a-stick inter-VLAN routing.
Inter-VLAN Routing using Layer 3 Switches	Configure inter-VLAN routing using Layer 3 switching.
Troubleshoot Inter-VLAN Routing	Troubleshoot common inter-VLAN configuration issues.

4.1 Inter-VLAN Routing Operation

What is Inter-VLAN Routing?

VLANs are used to segment switched Layer 2 networks for a variety of reasons. Regardless of the reason, hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services.

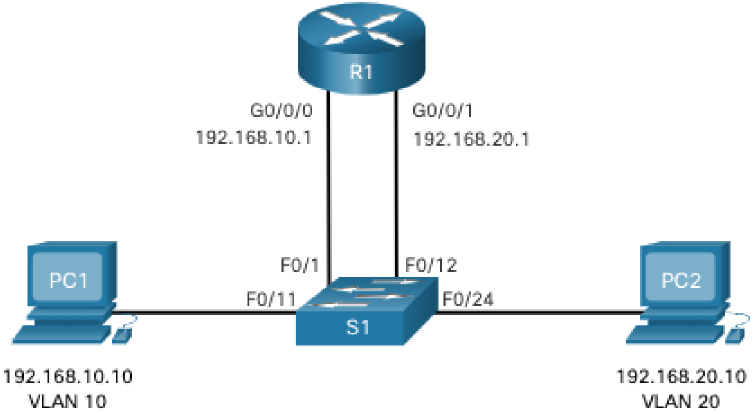
Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:

- **Legacy Inter-VLAN routing** - This is a legacy solution. It does not scale well.
- **Router-on-a-Stick** - This is an acceptable solution for a small to medium-sized network.
- **Layer 3 switch using switched virtual interfaces (SVIs)** - This is the most scalable solution for medium to large organizations.

Legacy Inter-VLAN Routing

- The first inter-VLAN routing solution relied on using a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. The router interfaces served as the default gateways to the local hosts on the VLAN subnet.
- Legacy inter-VLAN routing using physical interfaces works, but it has a significant limitation. It is not reasonably scalable because routers have a limited number of physical interfaces. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.
- **Note**: This method of inter-VLAN routing is no longer implemented in switched networks and is included for explanation purposes only.



Router-on-a-Stick Inter-VLAN Routing

The ‘router-on-a-stick’ inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method. It only requires one physical Ethernet interface to route traffic between multiple VLANs on a network.

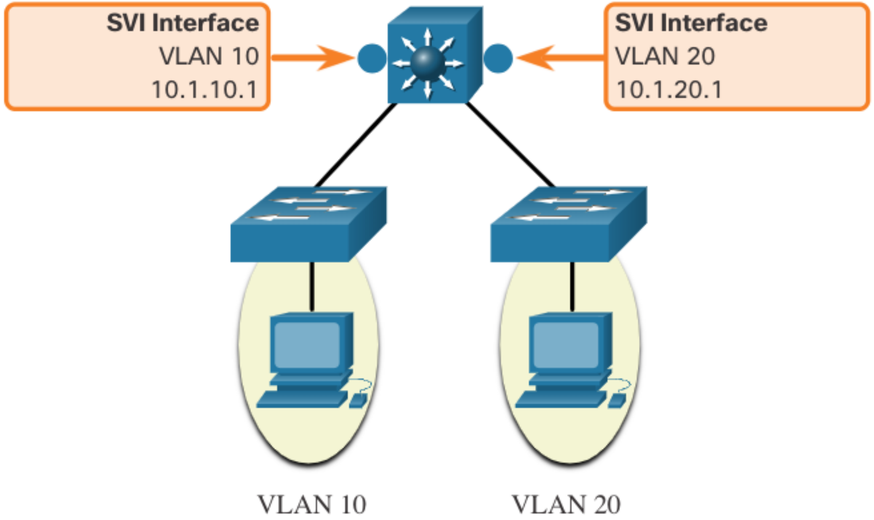
- A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using subinterfaces to identify routable VLANs.
- The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.
- When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic. If the exit interface is configured as an 802.1q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface

Note: The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

Inter-VLAN Routing on a Layer 3 Switch

The modern method of performing inter-VLAN routing is to use Layer 3 switches and switched virtual interfaces (SVI). An SVI is a virtual interface that is configured on a Layer 3 switch, as shown in the figure.

Note: A Layer 3 switch is also called a multilayer switch as it operates at Layer 2 and Layer 3. However, in this course we use the term Layer 3 switch.



Inter-VLAN Routing on a Layer 3 Switch (Cont.)

Inter-VLAN SVIs are created the same way that the management VLAN interface is configured. The SVI is created for a VLAN that exists on the switch. Although virtual, the SVI performs the same functions for the VLAN as a router interface would. Specifically, it provides Layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are **advantages** of using Layer 3 switches for inter-VLAN routing:

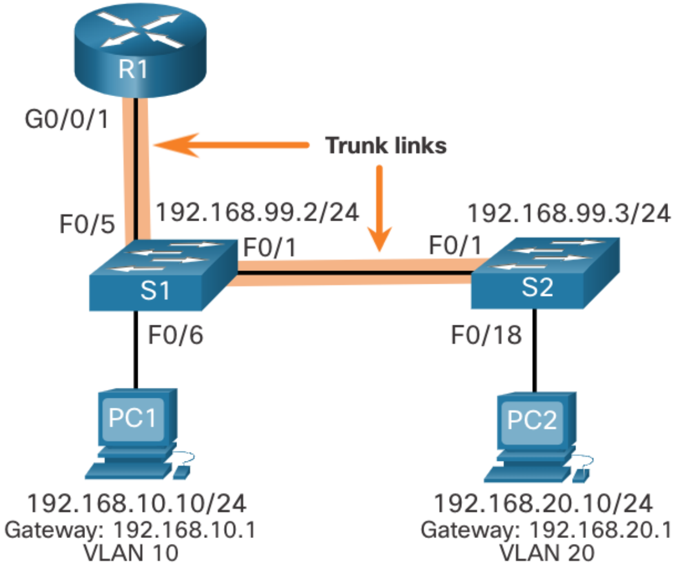
- They are much faster than router-on-a-stick because everything is hardware switched and routed.
- There is no need for external links from the switch to the router for routing.
- They are not limited to one link because Layer 2 EtherChannels can be used as trunk links between the switches to increase bandwidth.
- Latency is much lower because data does not need to leave the switch in order to be routed to a different network.
- They more commonly deployed in a campus LAN than routers.

- The only disadvantage is that Layer 3 switches are more expensive.

4.2 Router-on-a-Stick Inter-VLAN Routing

Router-on-a-Stick Scenario

- In the figure, the R1 GigabitEthernet 0/0/1 interface is connected to the S1 FastEthernet 0/5 port. The S1 FastEthernet 0/1 port is connected to the S2 FastEthernet 0/1 port. These are trunk links that are required to forward traffic within and between VLANs.
- To route between VLANs, the R1 GigabitEthernet 0/0/1 interface is logically divided into three subinterfaces, as shown in the table. The table also shows the three VLANs that will be configured on the switches.
- Assume that R1, S1, and S2 have initial basic configurations. Currently, PC1 and PC2 cannot **ping** each other because they are on separate networks. Only S1 and S2 can **ping** each other, but they but are unreachable by PC1 or PC2 because they are also on different networks.
- To enable devices to ping each other, the switches must be configured with VLANs and trunking, and the router must be configured for inter-VLAN routing.



Subinterface	VLAN	IP Address
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

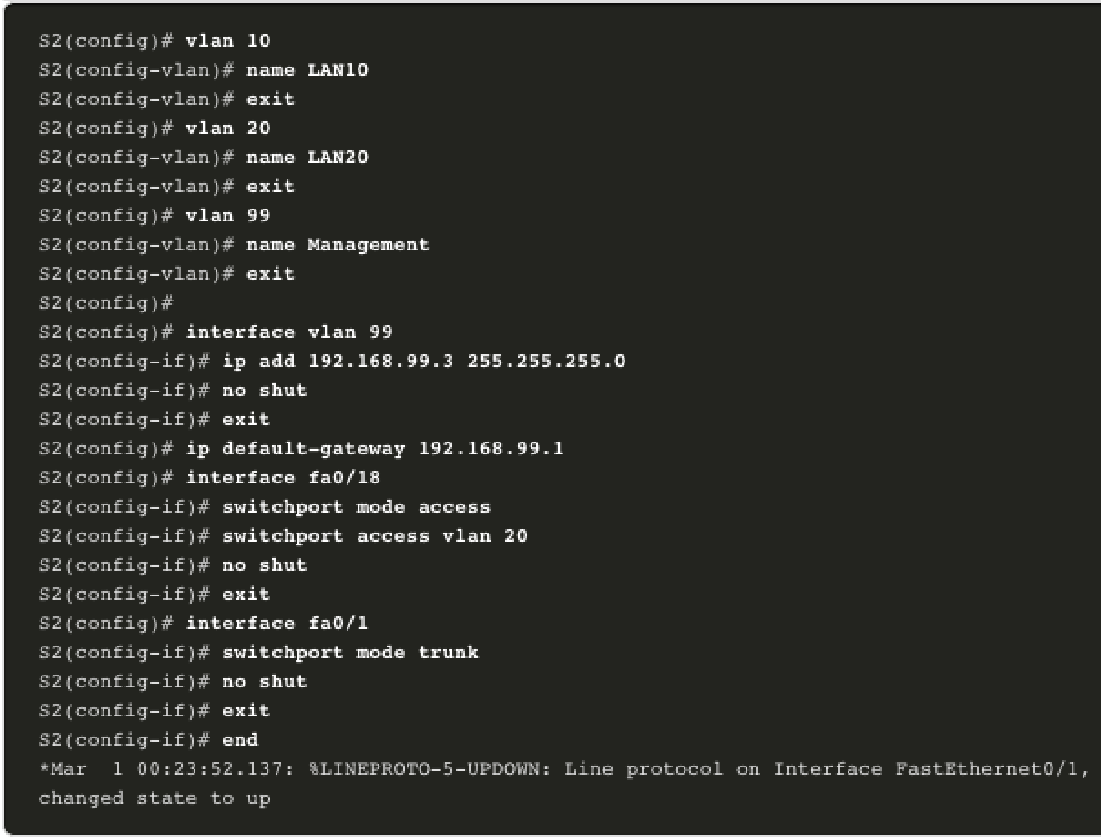
S1 VLAN and Trunking Configuration

Complete the following steps to configure S1 with VLANs and trunking:

- **Step 1**. Create and name the VLANs.
- **Step 2**. Create the management interface.
- **Step 3**. Configure access ports.
- **Step 4**. Configure trunking ports.

S2 VLAN and Trunking Configuration

The configuration for S2 is similar to S1.



```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar  1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

R1 Subinterface Configuration

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed. A subinterface is created using the **interface** *interface_id subinterface_id* global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

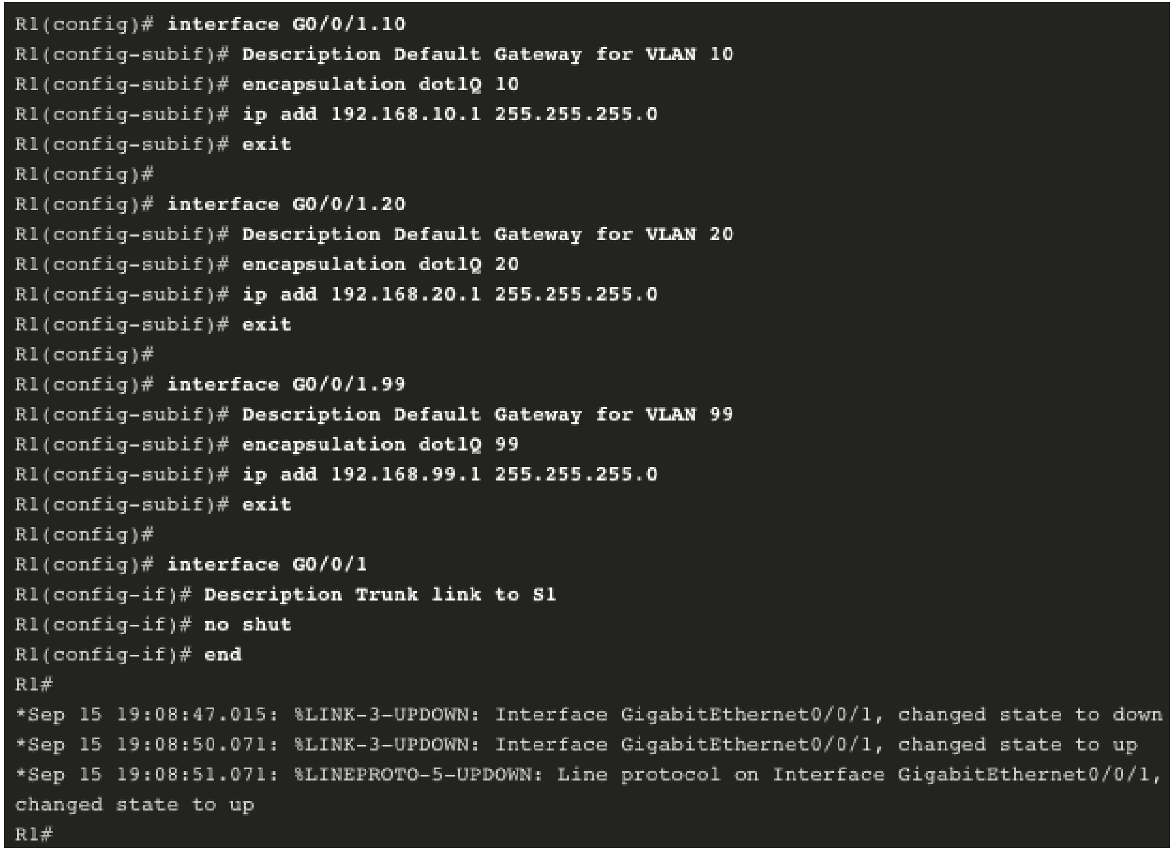
Each subinterface is then configured with the following two commands:

- **encapsulation dot1q** *vlan_id* **[native]** - This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified *vlan-id*. The **native** keyword option is only appended to set the native VLAN to something other than VLAN 1.
- **ip address** *ip-address subnet-mask* - This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, enable the physical interface using the **no shutdown** interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

R1 Subinterface Configuration (Cont.)

In the configuration, the R1 G0/0/1 subinterfaces are configured for VLANs 10, 20, and 99.



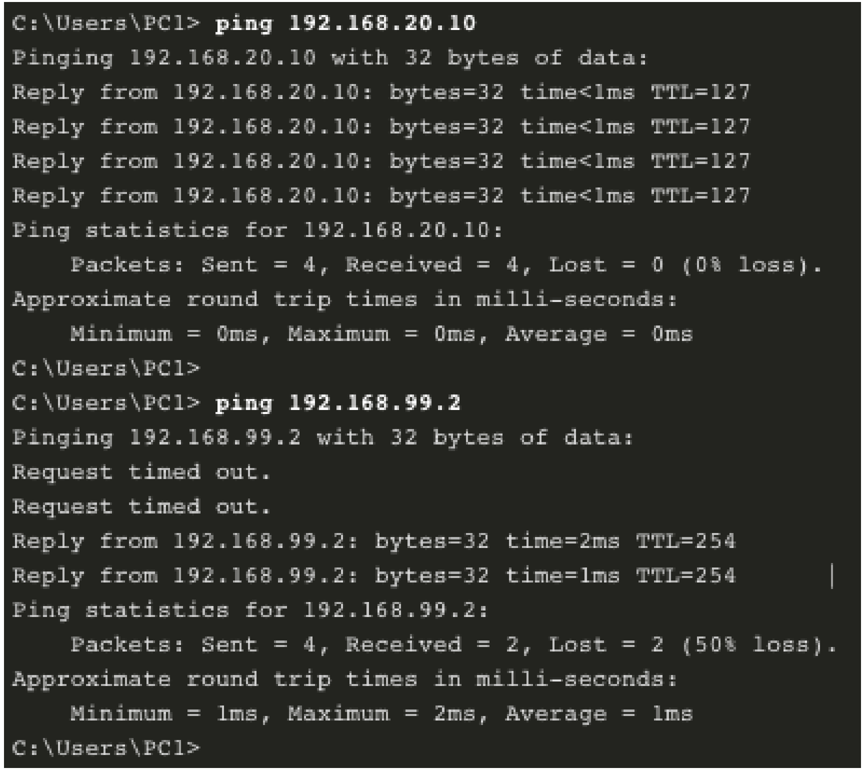
```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```

Verify Connectivity Between PC1 and PC2

The router-on-a-stick configuration is complete after the switch trunk and the router subinterfaces have been configured. The configuration can be verified from the hosts, router, and switch.

From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command.

Next, use **ping** to verify connectivity with PC2 and S1, as shown in the figure.
The **ping** output successfully confirms inter-VLAN routing is operating.



```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

Router-on-a-Stick Inter-VLAN Routing Verification

In addition to using **ping** between devices, the following **show** commands can be used to verify and troubleshoot the router-on-a-stick configuration.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

Packet Tracer– Configure Router-on-a-Stick Inter-VLAN Routing

In this Packet Tracer, you will complete the following objectives:

- Part 1: Add VLANs to a Switch
- Part 2: Configure Subinterfaces
- Part 3: Test connectivity with Inter-VLAN Routing

Lab – Configure Router-on-a-Stick Inter-VLAN Routing

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure Switches with VLANs and Trunking
- Part 3: Configure Trunk-Based Inter-VLAN Routing

4.3 Inter-VLAN Routing using Layer 3 Switches

Layer 3 Switch Inter-VLAN Routing

Inter-VLAN routing using the router-on-a-stick method is simple to implement for a small to medium-sized organization (**SMB**). However, a large enterprise requires a faster, much more scalable method to provide inter-VLAN routing.

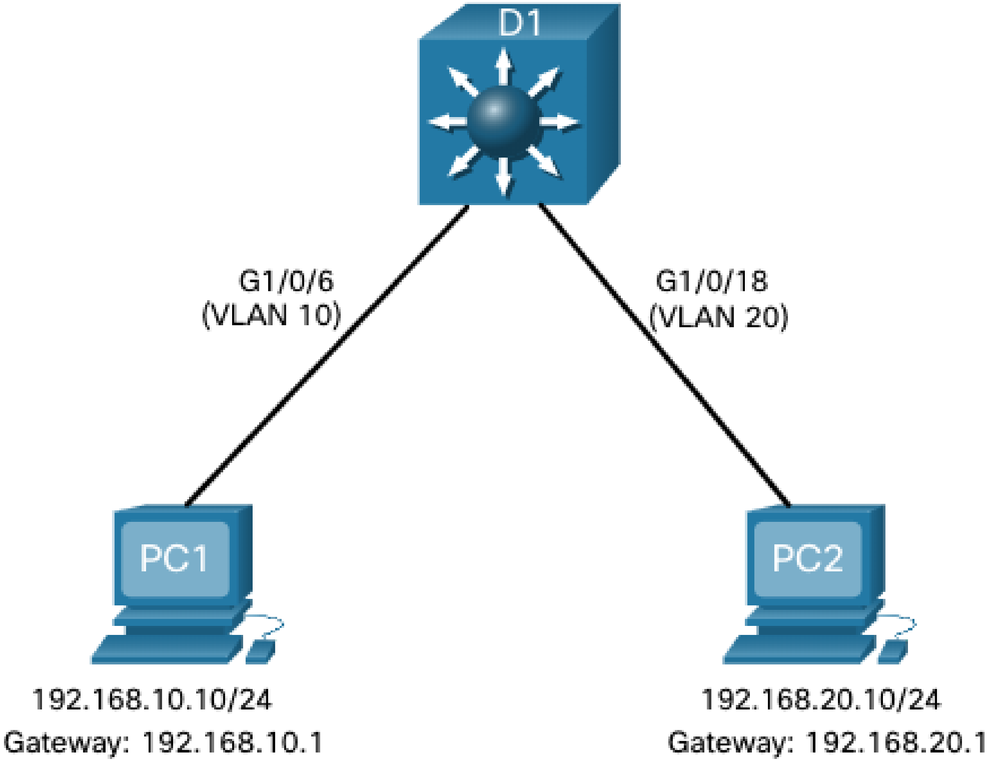
Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Layer 3 switches are also commonly implemented in enterprise distribution layer wiring closets.

Capabilities of a Layer 3 switch include the ability to do the following:

- Route from one VLAN to another using multiple switched virtual interfaces (SVIs).
- Convert a Layer 2 switchport to a Layer 3 interface (i.e., a routed port). A routed port is similar to a physical interface on a Cisco IOS router.
- To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan** *vlan-id* command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs.

Layer 3 Switch Scenario

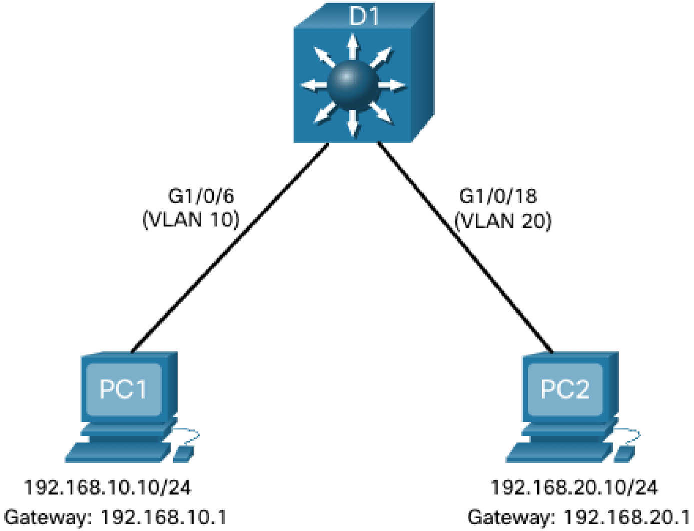
In the figure, the Layer 3 switch, D1, is connected to two hosts on different VLANs. PC1 is in VLAN 10 and PC2 is in VLAN 20, as shown. The Layer 3 switch will provide inter-VLAN routing services to the two hosts.



Layer 3 Switch Configuration

Complete the following steps to configure S1 with VLANs and trunking:

- **Step 1**. Create the VLANs. In the example, VLANs 10 and 20 are used.
- **Step 2**. Create the SVI VLAN interfaces. The IP address configured will serve as the default gateway for hosts in the respective VLAN.
- **Step 3**. Configure access ports. Assign the appropriate port to the required VLAN.
- **Step 4**. Enable IP routing. Issue the **ip routing** global configuration command to allow traffic to be exchanged between VLANs 10 and 20. This command must be configured to enable inter-VAN routing on a Layer 3 switch for IPv4.



Layer 3 Switch Inter-VLAN Routing Verification

Inter-VLAN routing using a Layer 3 switch is simpler to configure than the router-on-a-stick method. After the configuration is complete, the configuration can be verified by testing connectivity between the hosts.

- From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command.
- Next, verify connectivity with PC2 using the **ping** Windows host command. The successful **ping** output confirms inter-VLAN routing is operating.

Routing on a Layer 3 Switch

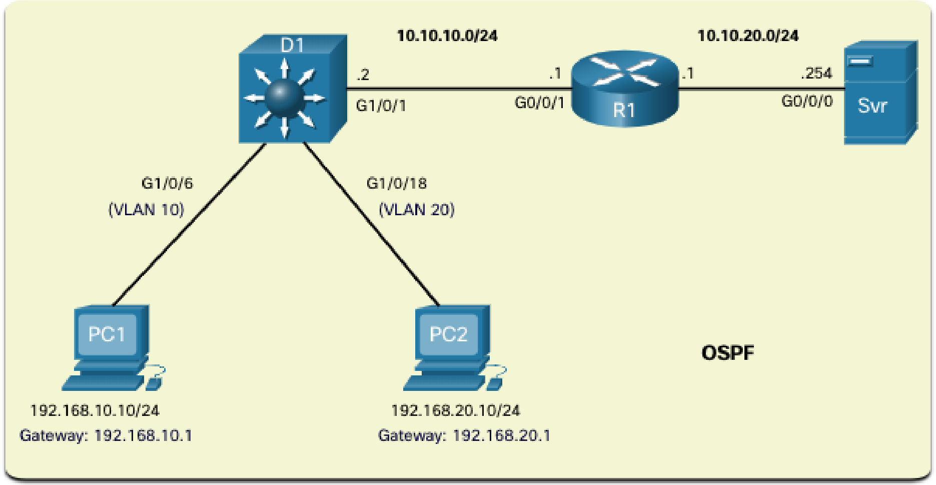
If VLANs are to be reachable by other Layer 3 devices, then they must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured.

A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. Specifically, configuring the **no switchport** interface configuration command on a Layer 2 port converts it into a Layer 3 interface. Then the interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.

Routing Scenario on a Layer 3 Switch

In the figure, the previously configured D1 Layer 3 switch is now connected to R1. R1 and D1 are both in an Open Shortest Path First (OSPF) routing protocol domain. Assume inter-VLAN has been successfully implemented on D1. The G0/0/1 interface of R1 has also been configured and enabled. Additionally, R1 is using OSPF to advertise its two networks, 10.10.10.0/24 and 10.20.20.0/24.

Note: OSPF routing configuration is covered in another course. In this module, OSPF configuration commands will be given to you in all activities and assessments. It is not required that you understand the configuration in order to enable OSPF routing on the Layer 3 switch.



Routing Configuration on a Layer 3 Switch

Complete the following steps to configure D1 to route with R1:

- **Step 1**. Configure the routed port. Use the **no switchport** command to convert the port to a routed port, then assign an IP address and subnet mask. Enable the port.
- **Step 2**. Enable routing. Use the **ip routing** global configuration command to enable routing.
- **Step 3**. Configure routing. Use an appropriate routing method. In this example, Single-Area OSPFv2 is configured
- **Step 4**. Verify routing. Use the **show ip route** command.
- **Step 5**. Verify connectivity. Use the **ping** command to verify reachability.

Packet Tracer – Configure Layer 3 Switching and inter-VLAN Routing

In this Packet Tracer, you will complete the following objectives:

- Part 1: Configure Layer 3 Switching
- Part 2: Configure Inter-VLAN Routing
- Part 3: Configure IPv6 Inter-VLAN Routing

4.4 Troubleshoot Inter-VLAN Routing

Common Inter-VLAN Issues

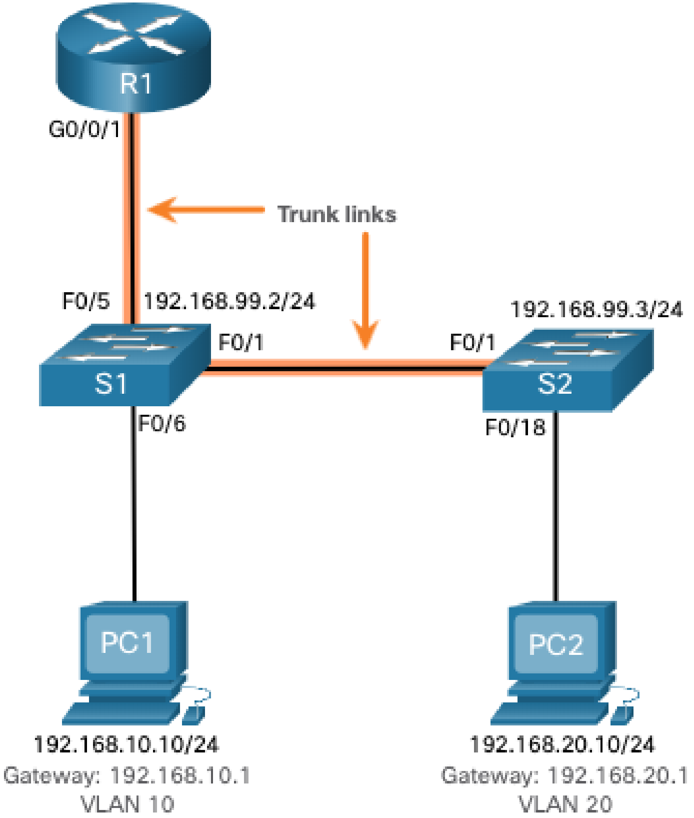
There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues. First, check the physical layer to resolve any issues where a cable might be connected to the wrong port. If the connections are correct, then use the list in the table for other common reasons why inter-VLAN connectivity may fail.

Issue Type	How to Fix	How to Verify
Missing VLANs	•Create (or re-create) the VLAN if it does not exist. •Ensure host port is assigned to the correct VLAN.	**show vlan [brief]** **show interfaces switchport** **ping**
Switch Trunk Port Issues	•Ensure trunks are configured correctly. •Ensure port is a trunk port and enabled.	**show interface trunk** **show running-config**
Switch Access Port Issues	•Assign correct VLAN to access port. •Ensure port is an access port and enabled. •Host is incorrectly configured in the wrong subnet.	**show interfaces switchport** **show running-config interface** **ipconfig**
Router Configuration Issues	•Router subinterface IPv4 address is incorrectly configured. •Router subinterface is assigned to the VLAN ID.	**show ip interface brief** **show interfaces**

Troubleshoot Inter-VLAN Routing Scenario

Examples of some of these inter-VLAN routing problems will now be covered in more detail. This topology will be used for all of these issues.

Router R1 Subinterfaces		
Subinterface	**VLAN**	**IP Address**
G0/0/0.10	10	192.168.10.1/24
G0/0/0.20	20	192.168.20.1/24
G0/0/0.30	99	192.168.99.1/24

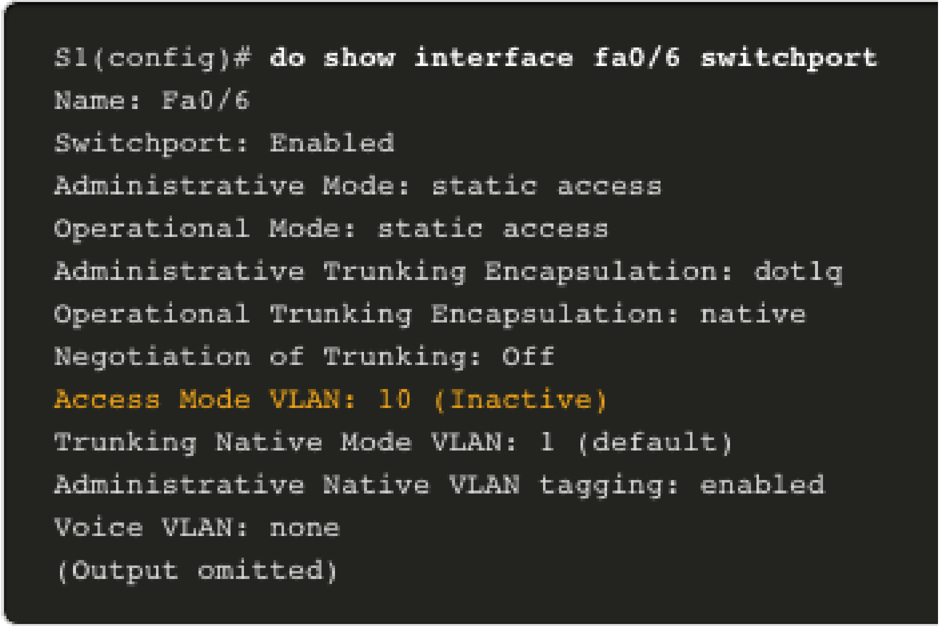


1. Error: Missing VLANs

An inter-VLAN connectivity issue could be caused by a missing VLAN. The VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link.

When a VLAN is deleted, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN or recreate the missing VLAN. Recreating the missing VLAN would automatically reassign the hosts to it.

Use the **show interface** *interface-id* **switchport** command to verify the VLAN membership of the port.



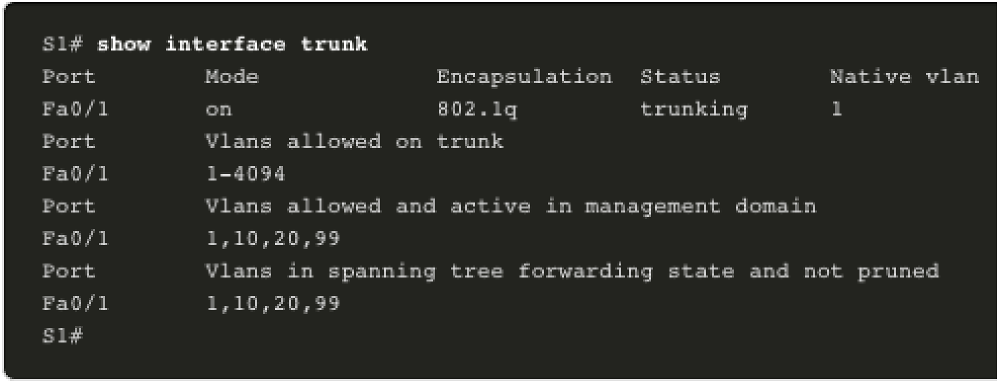
```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

2. Error: Switch Trunk Port Issues

Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, this could be caused when the connecting router port is not assigned to the correct VLAN.

However, with a router-on-a-stick solution, the most common cause is a misconfigured trunk port.

- Verify that the port connecting to the router is correctly configured as a trunk link using the **show interface trunk** command.
- If that port is missing from the output, examine the configuration of the port with the **show running-config interface X** command to see how the port is configured.



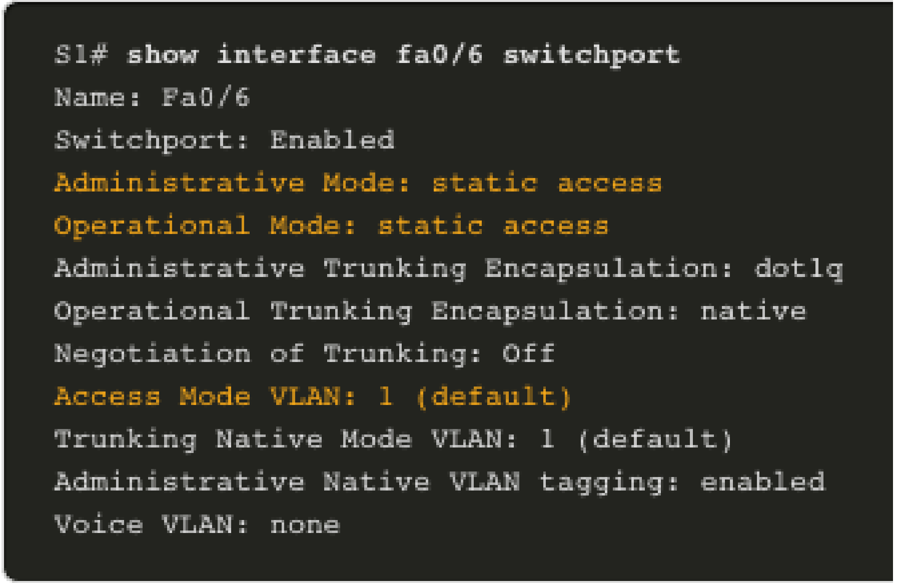
```
S1# show interface trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S1#
```

3. Error: Switch Access Port Issues

When a problem is suspected with a switch access port configuration, use verification commands to examine the configuration and identify the problem.

A common indicator of this issue is the PC having the correct address configuration (IP Address, Subnet Mask, Default Gateway), but being unable to ping its default gateway.

- Use the **show vlan brief**, **show interface X switchport** or **show running-config interface X** command to verify the interface VLAN assignment.

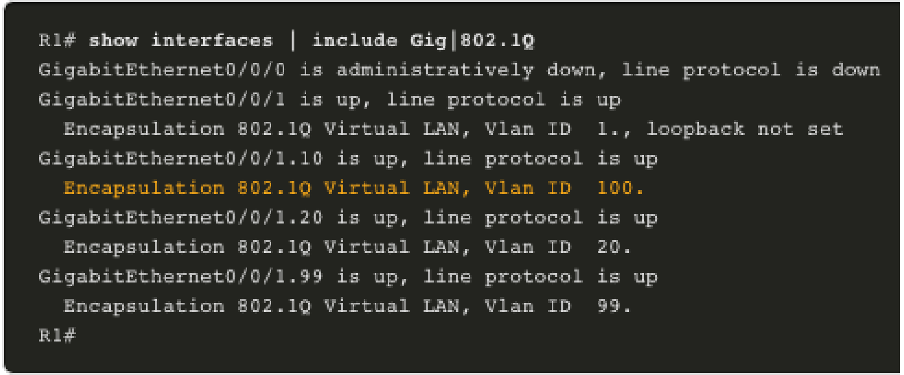


```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

4. Error: Router Configuration Issues

Router-on-a-stick configuration problems are usually related to subinterface misconfigurations.

- Verify the subinterface status using the **show ip interface brief** command.
- Verify which VLANs each of the subinterfaces is on. To do so, the **show interfaces** command is useful but it generates a great deal of additional unrequired output. The command output can be reduced using IOS command filters. In this example, use the **include** keyword to identify that only lines containing the letters “Gig” or “802.1Q”



```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

Packet Tracer – Troubleshoot Inter-VLAN Routing

In this Packet Tracer activity, you will complete the following objectives:

- Part 1: Locate Network Problems
- Part 2: Implement the Solution
- Part 3: Verify Network Connectivity

Lab – Troubleshoot Inter-VLAN Routing

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Load Device Configurations
- Part 2: Troubleshoot the Inter-VLAN Routing Configuration
- Part 3: Verify VLAN Configuration, Port Assignment and Trunking
- Part 4: Test Layer 3 Connectivity

4.5 Module Practice and Quiz

Packet Tracer – Inter-VLAN Routing Challenge

In this Packet Tracer activity, you will demonstrate and reinforce your ability to implement inter-VLAN routing, including configuring IP addresses, VLANs, trunking, and subinterfaces.

Lab– Implement Inter-VLAN Routing

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports
- Part 3: Configure an 802.1Q Trunk between the Switches
- Part 4: Configure Inter-VLAN Routing on the S1 Switch
- Part 5: Verify Inter-VLAN Routing is Working

What Did I Learn In This Module?

- Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.
- Three options include legacy, router-on-a-stick, and Layer 3 switch using SVIs.
- To configure a switch with VLANs and trunking, complete the following steps: create and name the VLANs, create the management interface, configure access ports, and configure trunking ports.
- The router-on-a-stick method requires a subinterface to be created for each VLAN to be routed. A subinterface is created using the **interface interface_id subinterface_id** global configuration mode command.
- Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, the physical interface must be enabled using the no shutdown interface configuration command.
- Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers.
- Capabilities of a Layer 3 switch include routing from one VLAN to another using multiple switched virtual interfaces (SVIs) and converting a Layer 2 switchport to a Layer 3 interface (i.e., a routed port).
- To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan vlan-id** command used to create the management SVI on a Layer 2 switch.

What Did I Learn In This Module? (Cont.)

- To configure a switch with VLANS and trunking, complete the following steps: create the VLANS, create the SVI VLAN interfaces, configure access ports, and enable IP routing.
- To enable routing on a Layer 3 switch, a routed port must be configured. A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. The interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.
- To configure a Layer 3 switch to route with a router, follow these steps: configure the routed port, enable routing, configure routing, verify routing, and verify connectivity.
- There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues such as missing VLANs, switch trunk port issues, switch access port issues, and router configuration issues.
- A VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link.
- Another issue for inter-VLAN routing includes misconfigured switch ports.
- In a legacy inter-VLAN solution, a misconfigured switch port could be caused when the connecting router port is not assigned to the correct VLAN.

What Did I Learn In This Module? (Cont.)

- With a *router-on-a-stick solution*, the most common cause is a misconfigured trunk port.
- When a problem is suspected with a switch access port configuration, use **ping** and **show interfaces interface-id switchport** commands to identify the problem.
- Router configuration problems with router-on-a-stick configurations are usually related to subinterface misconfigurations. Verify the subinterface status using the **show ip interface brief** command.

Téma 4.1

Co podle vás přispívá k omezení počtu VLAN podporovaných Router-on-a-Stick Inter-VLAN Routing?

Jaký je podle vás rozdíl mezi interface loopbacku routeru a subinterface routeru?

Téma 4.2

Jaká je primární výhoda uspořádání Router-on-a-stick na rozdíl od Legacy Inter-VLAN Routing?

Jak router zpracovává nativní VLAN?

Téma 4.3

Jaké jsou největší úspory, kterých můžete dosáhnout při použití přepínače L3 jako směrovače Inter-VLAN?

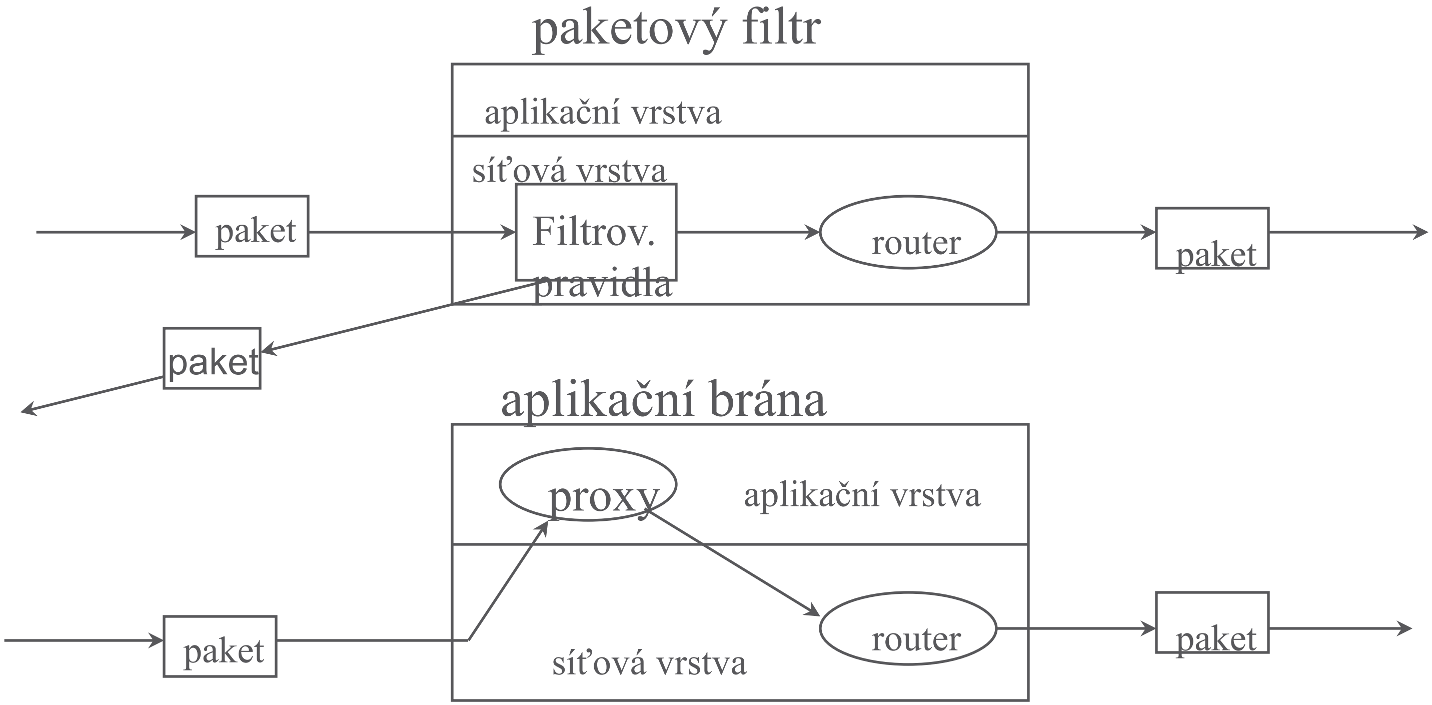
Jaký je dopad příkazu `no switchport`?

Téma 4.4

Co je podle vás nejčastější příčinou chyb při implementaci směrování Inter-VLAN?

Jaký druh směrování Inter-VLAN je podle vás vhodný z hlediska nejnižšího počtu chyb při implementaci?

Klasické firewally



Další firewally

- dynamické filtry
- kernel proxy
- adaptivní proxy

Protokoly, které bývají cílem útoku

TFTP
X-Window
RPC

Telnet
FTP
SMTP
RIP
DNS
UUCP
NNTP
NTP
HTTP

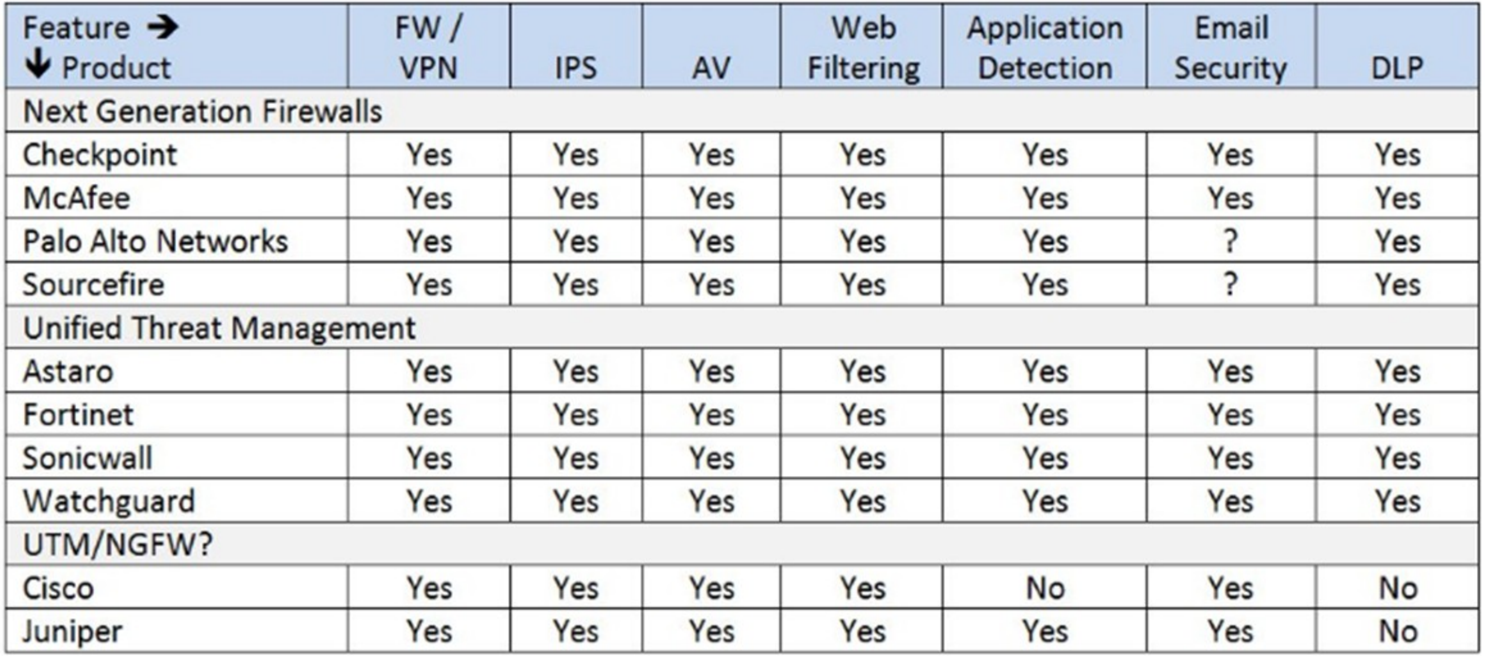
Dodatečné funkce mění firewall v UTM resp. NGFW

- tunelování
- translace adres
- autentizace uživatelů
- detekce průniků
- blokace, restrikce a antivirový nástroj
- podpora demilitarizovaného portu
- vzdálené řízení nastavování
- alarmy
- kešování informací atd.

UTM (unified threat management) a NGFW (nextgen FW)

- **UTM** byly původně firewally kategorie SMB rozšířené o funkce IDS/IPS, antimalwaru, antispamu a filtrování obsahu v jediném snadno spravovatelném zařízení. Nověji přidaly funkce, jako je VPN, vyvažování zátěže a prevence ztráty dat (DLP), a jsou stále častěji dodávány jako služba prostřednictvím cloudu.
- **NGFW** kombinují tradiční filtrování portů a protokolů s funkcemi IDS/IPS a schopností detekovat provoz na aplikační vrstvě; postupem času přidali další funkce, jako je hloubková kontrola paketů a detekce malwaru.
- Ochrana proti malwaru a virům, webový proxy a další, které existují v bráně firewall UTM, nejsou původní součástí architektury NGFW, protože tyto linie byly původně outsourcovány a odstraněny, což zajistilo bohaté stupně škálovatelnosti pro velká prostředí.

Výrobci NGEW a UTM



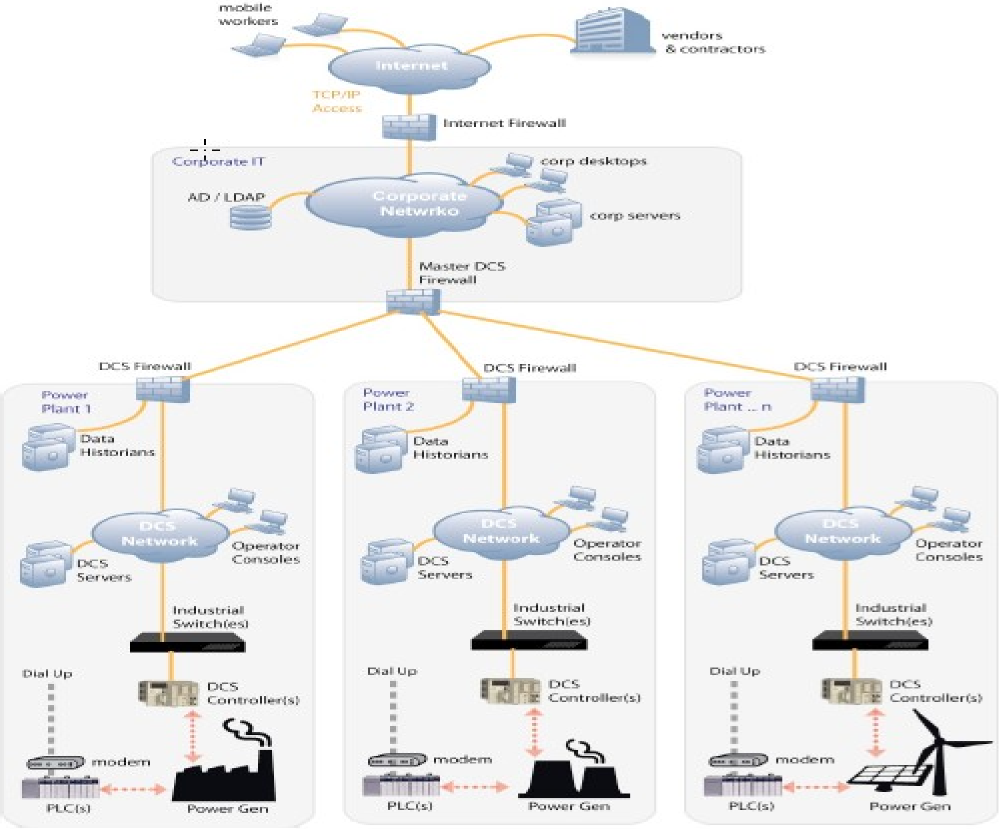
Feature → ↓ Product	FW / VPN	IPS	AV	Web Filtering	Application Detection	Email Security	DLP
Next Generation Firewalls							
Checkpoint	Yes	Yes	Yes	Yes	Yes	Yes	Yes
McAfee	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Palo Alto Networks	Yes	Yes	Yes	Yes	Yes	?	Yes
Sourcefire	Yes	Yes	Yes	Yes	Yes	?	Yes
Unified Threat Management							
Astaro	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fortinet	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sonicwall	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Watchguard	Yes	Yes	Yes	Yes	Yes	Yes	Yes
UTM/NGFW?							
Cisco	Yes	Yes	Yes	Yes	No	Yes	No
Juniper	Yes	Yes	Yes	Yes	Yes	Yes	No

Obrana průmyslových zařízení pomocí zónové obrany

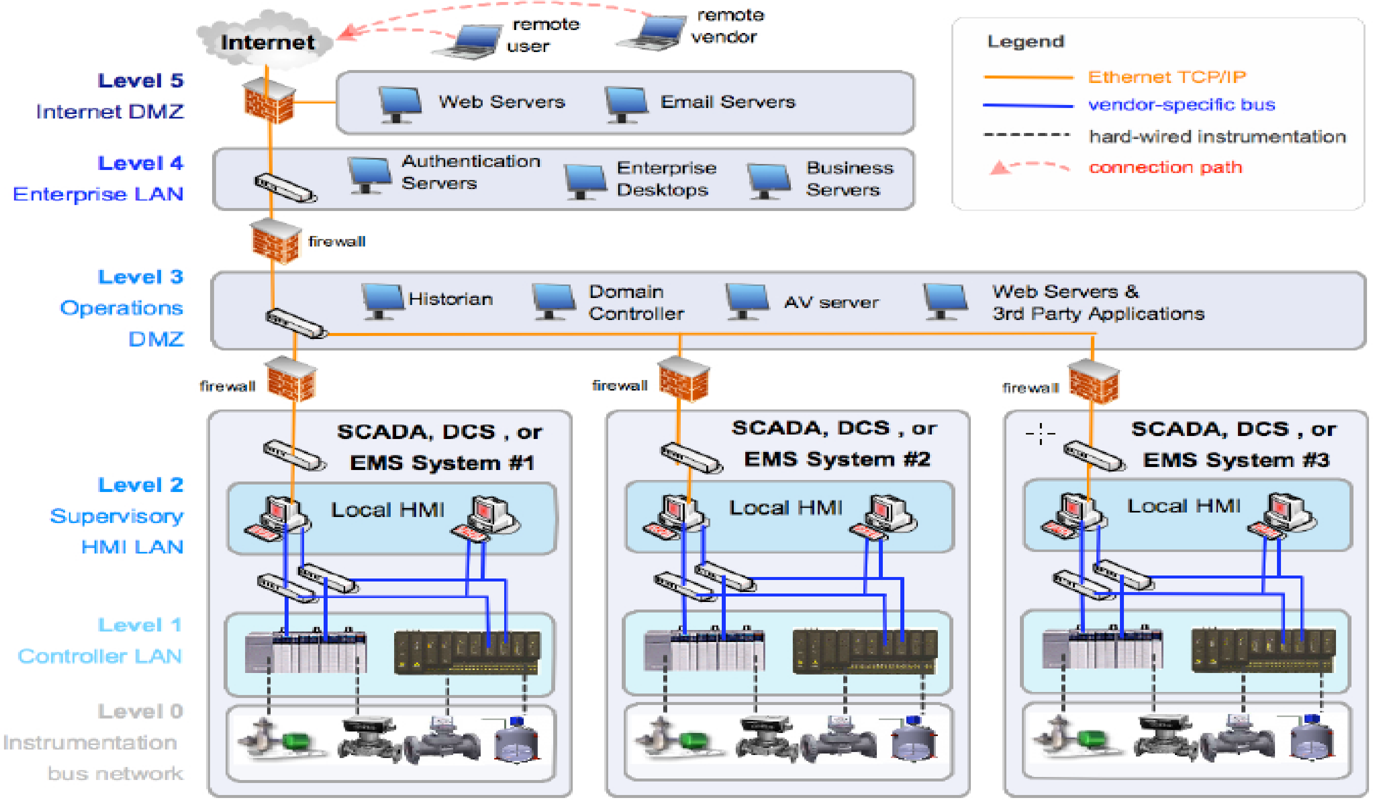
- Speciální firewally (conduits) mají pomocí seznamů povolených příkazů zabránit přelévání problémů z jedné zóny do druhé. Řada od sebe oddělených zón umožňuje realizovat tzv. obranu v hloubce.

- Typickým conduitem je např. Tofino Security Appliance (TSA):

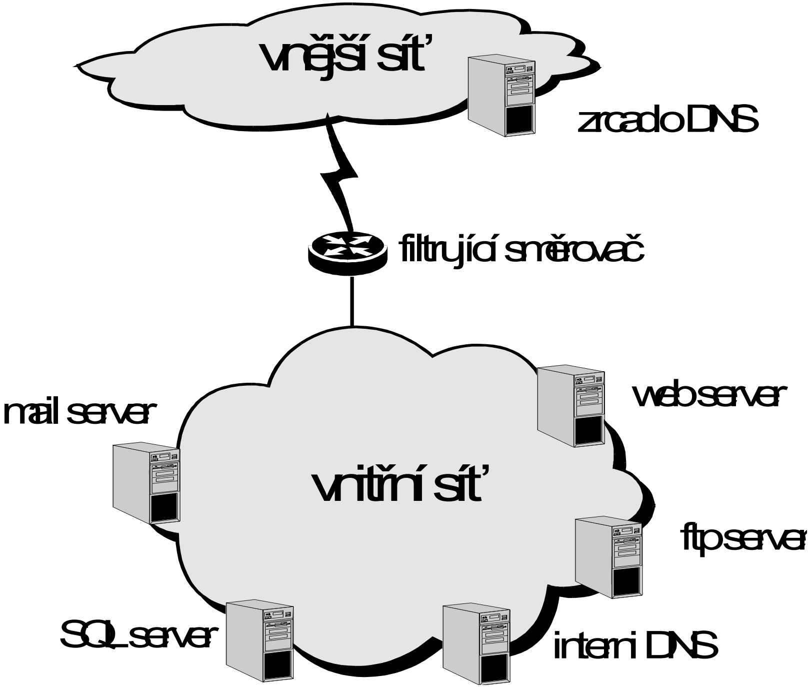
Schéma typického průmyslového objektu – zde elektrárny



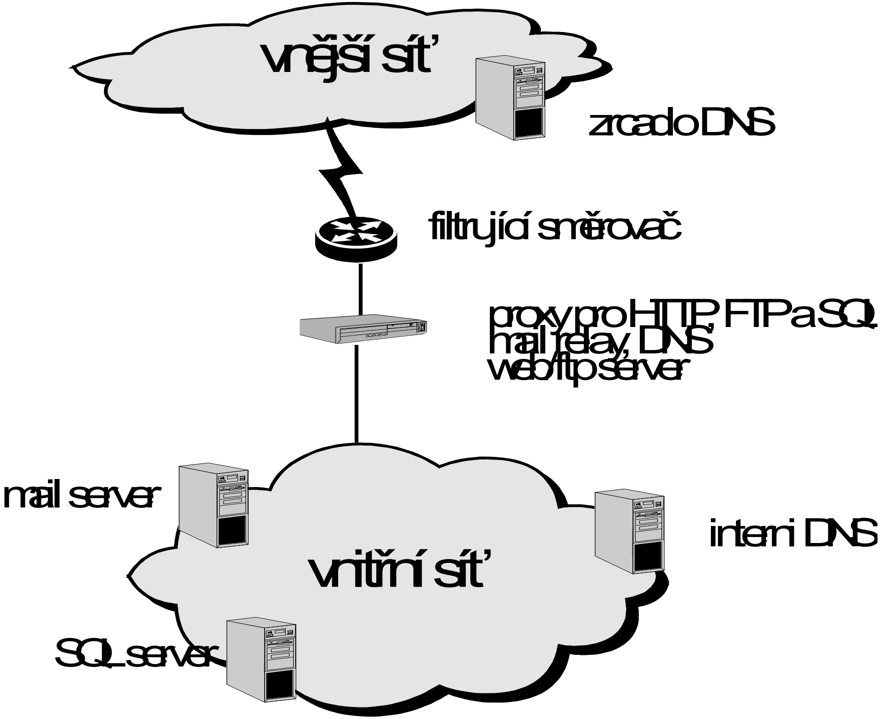
Příklad rozdělení řízení elektrárny do jednotlivých úrovní



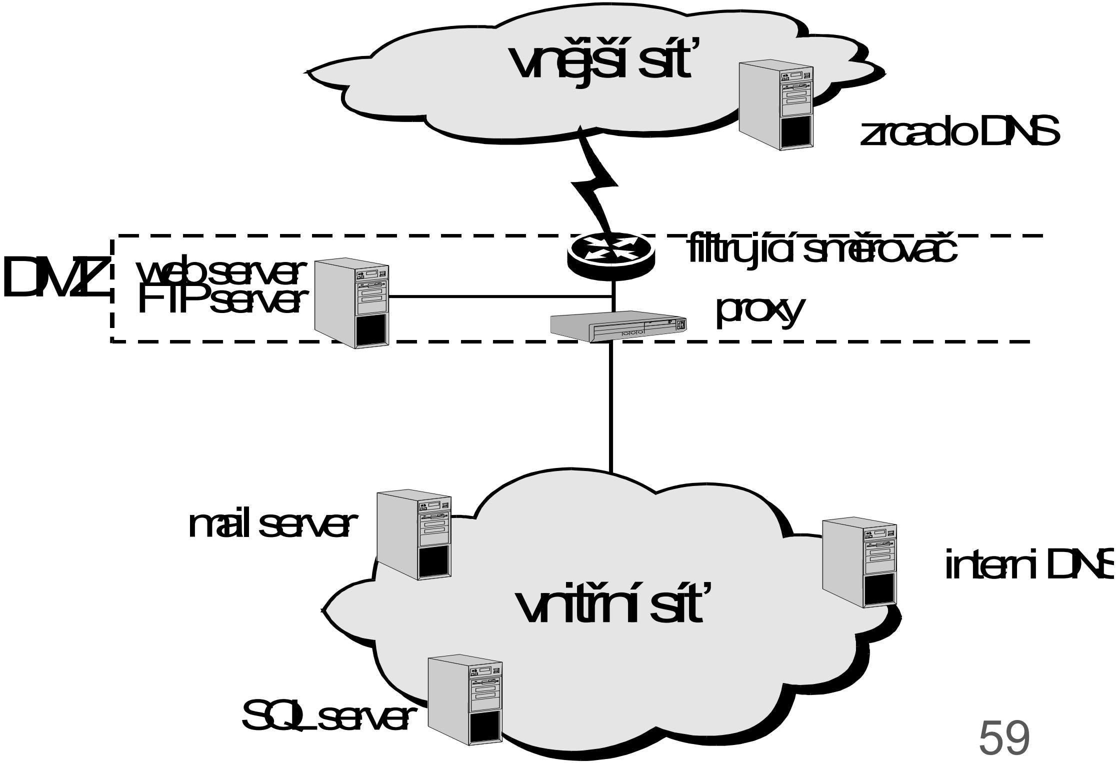
typ 1
Dual Homed Gateway



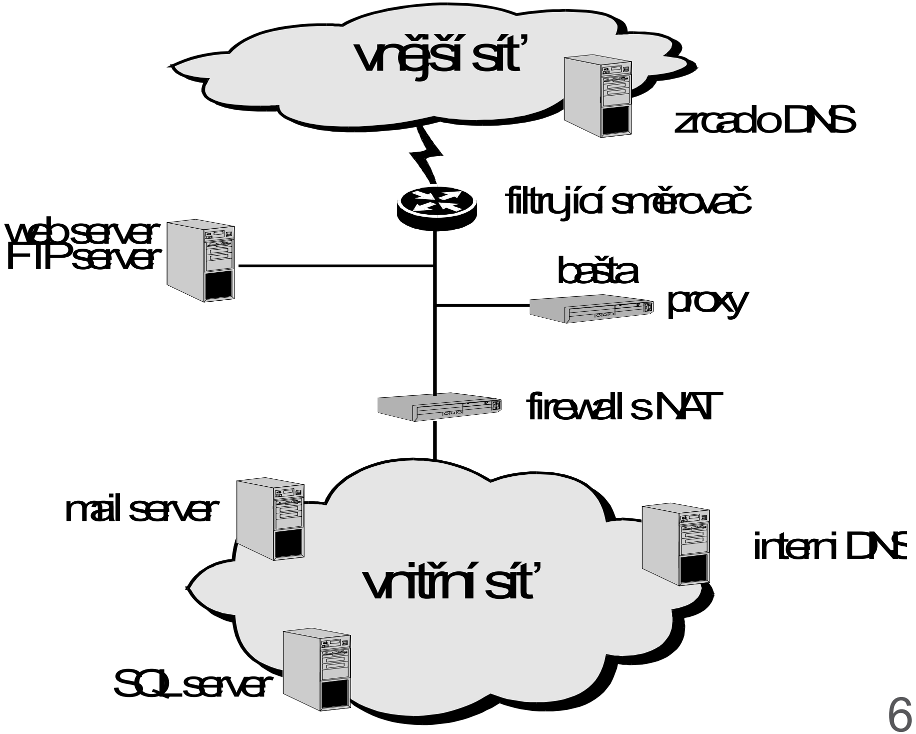
typ 2
Předsunutá obrana



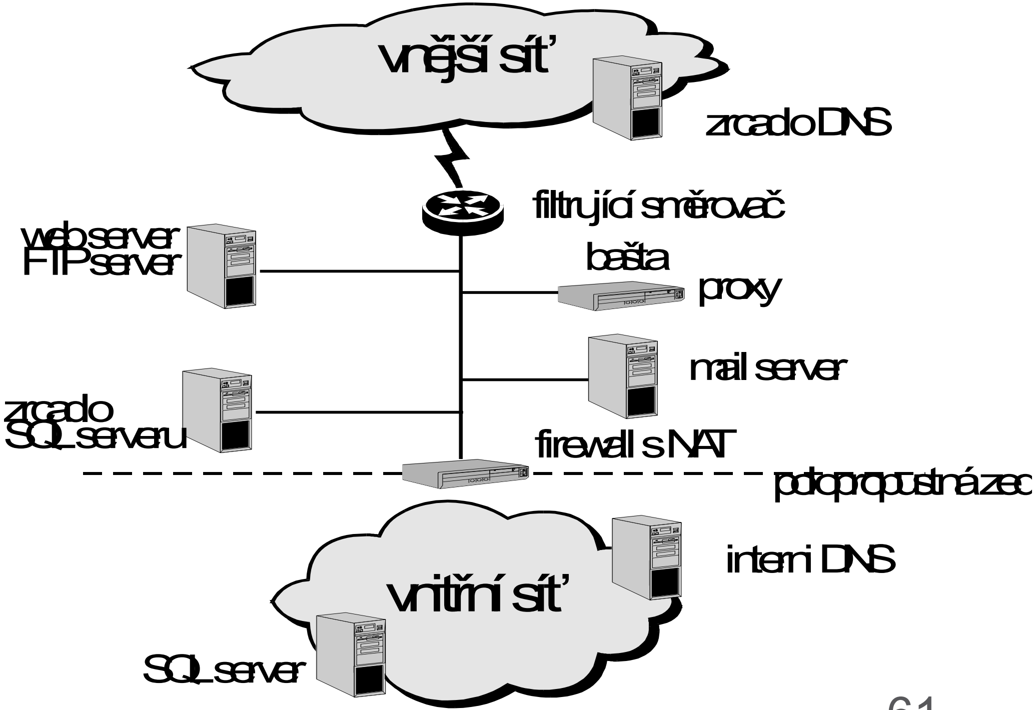
typ 3
Diverzifikovaná obrana



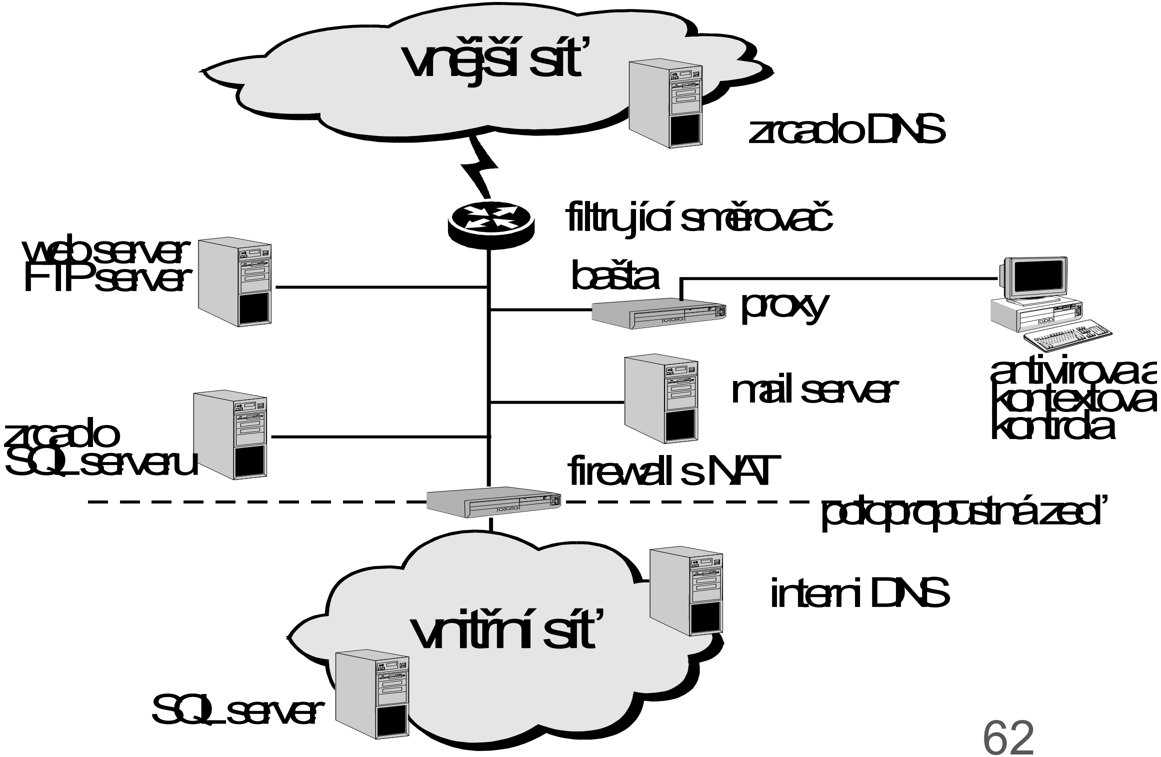
typ 4
Screen subnet



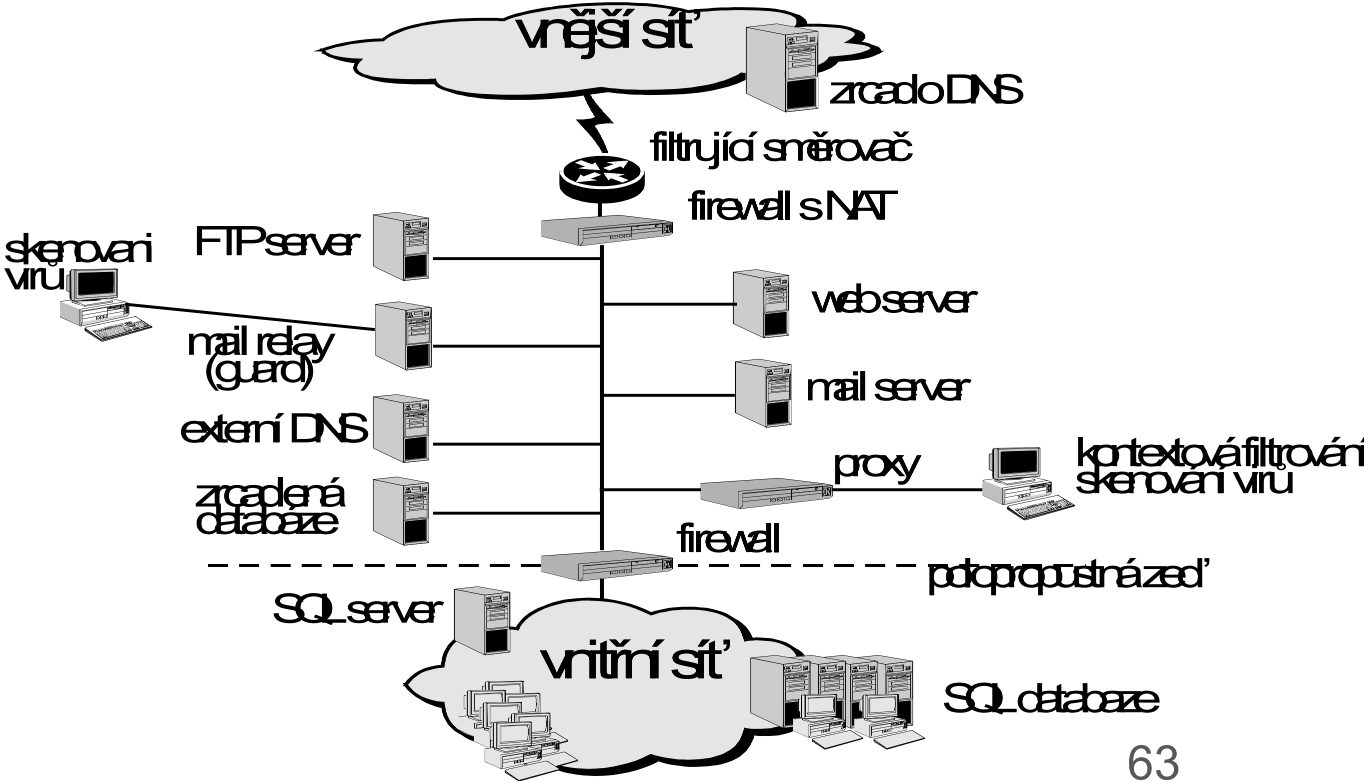
typ 5
Polopropustná zeď



typ 6
Context vectoring

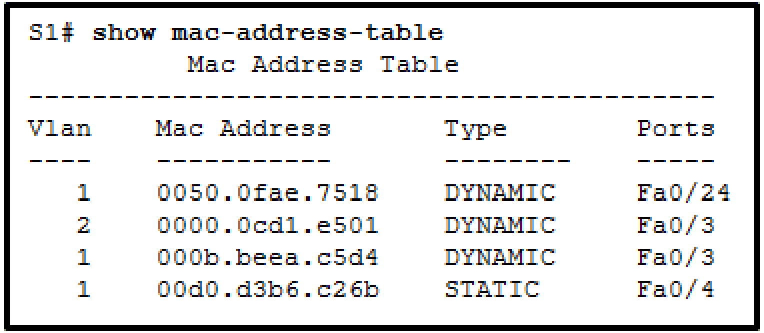


typ 7
Metafirewall



Ukázka potencionálních otázek testu

20. Refer to the exhibit. A switch receives a Layer 2 frame that contains a source MAC address of 000b.a023.c501 and a destination MAC address of 0050.0fae.75aa. Place the switch steps in the order they occur. (Not all options are used.)



```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0050.0fae.7518    DYNAMIC     Fa0/24
   2    0000.0cd1.e501    DYNAMIC     Fa0/3
   1    000b.beea.c5d4    DYNAMIC     Fa0/3
   1    00d0.d3b6.c26b    STATIC      Fa0/4
```

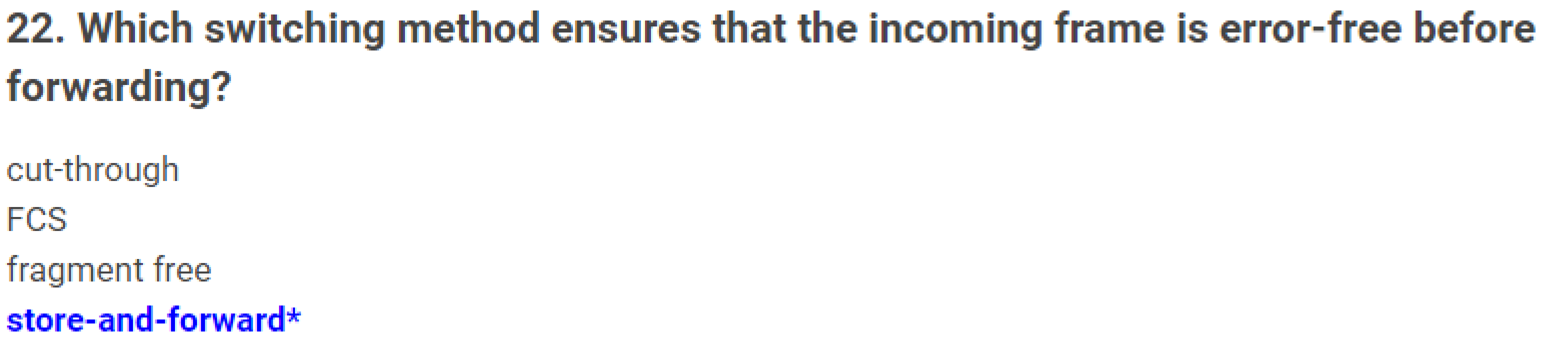
21. What information is added to the switch table from incoming frames?

source MAC address and incoming port number*

destination MAC address and incoming port number

source IP address and incoming port number

destination IP address and incoming port number



22. Which switching method ensures that the incoming frame is error-free before forwarding?

cut-through

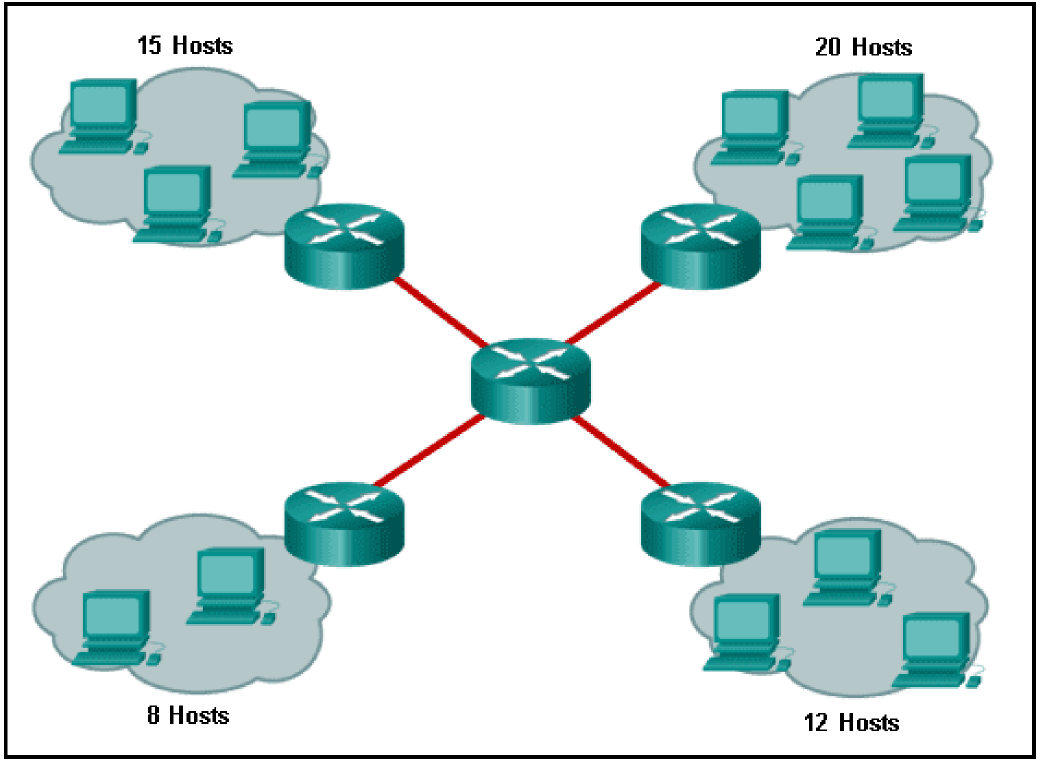
FCS

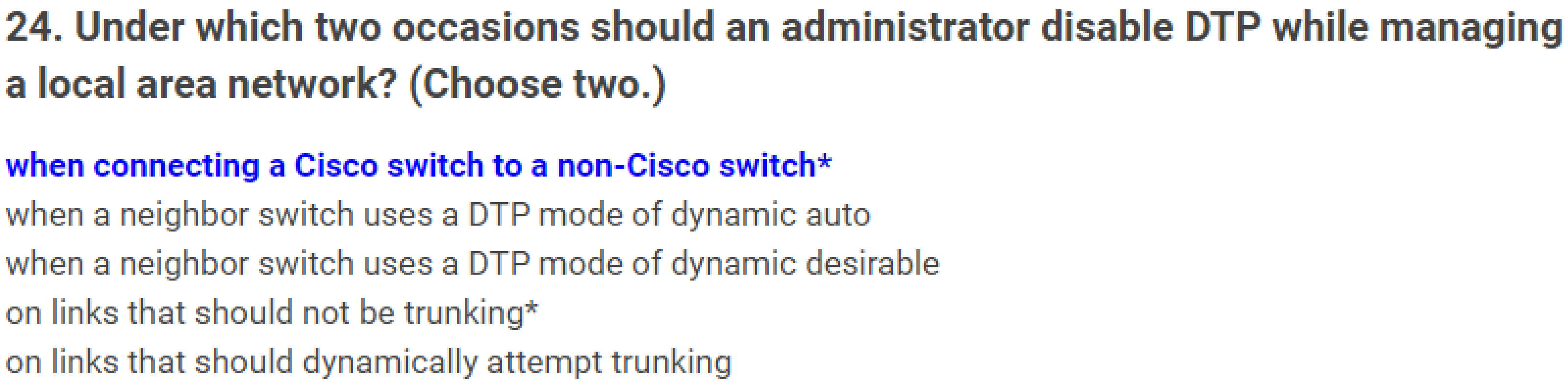
fragment free

store-and-forward*

Kolik je tam broadcast domén? (8)

23. Refer to the exhibit.





24. Under which two occasions should an administrator disable DTP while managing a local area network? (Choose two.)

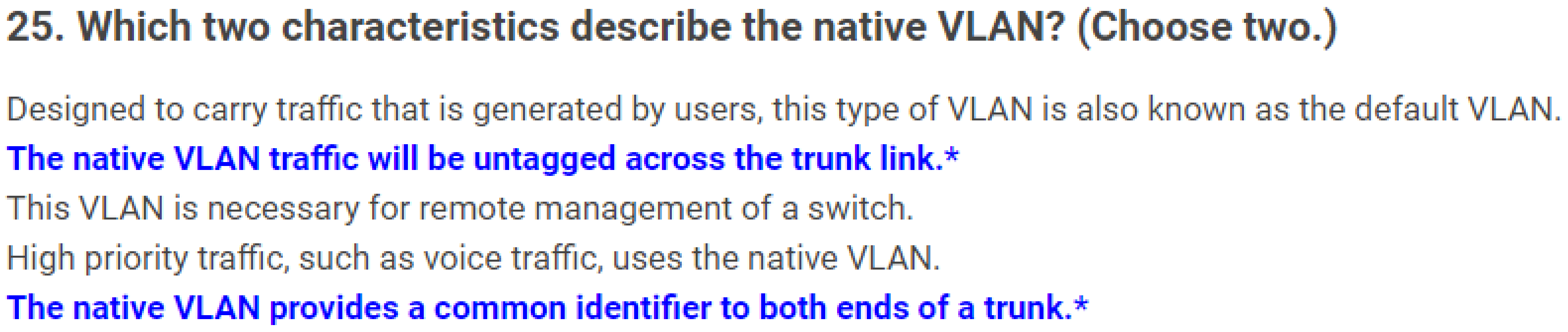
when connecting a Cisco switch to a non-Cisco switch*

when a neighbor switch uses a DTP mode of dynamic auto

when a neighbor switch uses a DTP mode of dynamic desirable

on links that should not be trunking*

on links that should dynamically attempt trunking



25. Which two characteristics describe the native VLAN? (Choose two.)

Designed to carry traffic that is generated by users, this type of VLAN is also known as the default VLAN.

The native VLAN traffic will be untagged across the trunk link.*

This VLAN is necessary for remote management of a switch.

High priority traffic, such as voice traffic, uses the native VLAN.

The native VLAN provides a common identifier to both ends of a trunk.*

37. Which four steps are needed to configure a voice VLAN on a switch port? (Choose four).

Configure the interface as an IEEE 802.1Q trunk.

Assign the voice VLAN to the switch port.*

Activate spanning-tree PortFast on the interface.

Ensure that voice traffic is trusted and tagged with a CoS priority value.*

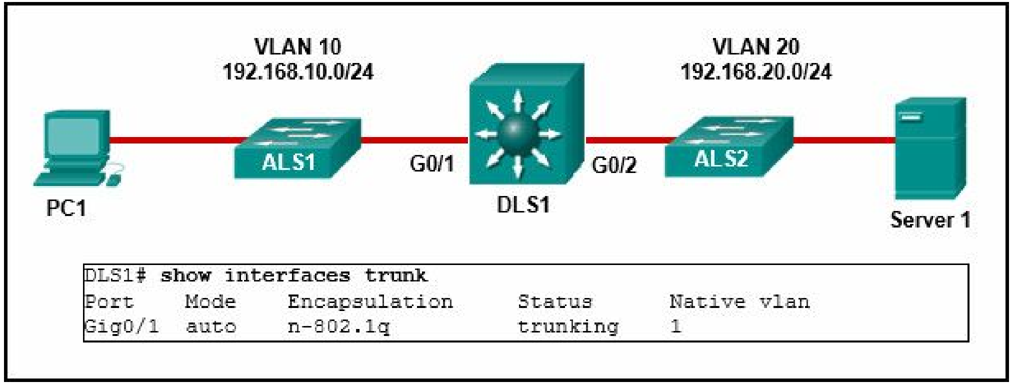
Add a voice VLAN.*

Configure the switch port interface with subinterfaces.

Assign a data VLAN to the switch port.

Configure the switch port in access mode.*

38. Refer to the exhibit.



```
DLS1# show interfaces trunk
Port     Mode     Encapsulation      Status      Native vlan
Gig0/1   auto     n-802.1q           trunking    1
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p38

PC1 is unable to communicate with server 1. The network administrator issues the show interfaces trunk command to begin troubleshooting. What conclusion can be made based on the output of this command?

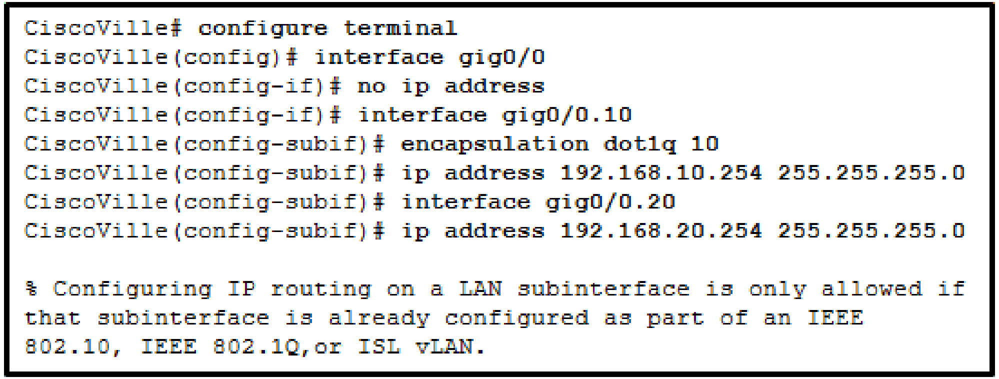
Interface G0/2 is not configured as a trunk.*

VLAN 20 has not been created.

The encapsulation on interface G0/1 is incorrect.

The DTP mode is incorrectly set to dynamic auto on interface G0/1.

39. Refer to the exhibit.



```
CiscoVille# configure terminal
CiscoVille(config)# interface gig0/0
CiscoVille(config-if)# no ip address
CiscoVille(config-if)# interface gig0/0.10
CiscoVille(config-subif)# encapsulation dot1q 10
CiscoVille(config-subif)# ip address 192.168.10.254 255.255.255.0
CiscoVille(config-subif)# interface gig0/0.20
CiscoVille(config-subif)# ip address 192.168.20.254 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if
that subinterface is already configured as part of an IEEE
802.10, IEEE 802.1Q,or ISL vLAN.
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p39

What is the cause of the error that is displayed in the configuration of inter-VLAN routing on router CiscoVille?

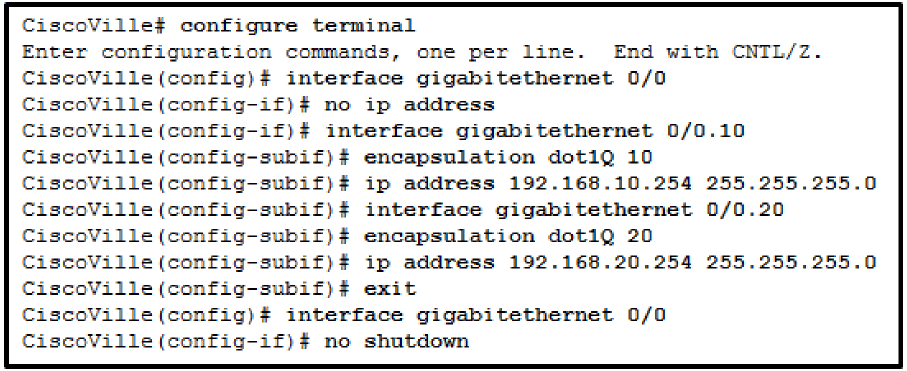
The gig0/0 interface does not support inter-VLAN routing.

The no shutdown command has not been configured.

The IP address on CiscoVille is incorrect.

The encapsulation dot1Q 20 command has not been configured.*

40. Refer to the exhibit.



```
CiscoVille# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no ip address
CiscoVille(config-if)# interface gigabitethernet 0/0.10
CiscoVille(config-subif)# encapsulation dot1Q 10
CiscoVille(config-subif)# ip address 192.168.10.254 255.255.255.0
CiscoVille(config-subif)# interface gigabitethernet 0/0.20
CiscoVille(config-subif)# encapsulation dot1Q 20
CiscoVille(config-subif)# ip address 192.168.20.254 255.255.255.0
CiscoVille(config-subif)# exit
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no shutdown
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p40

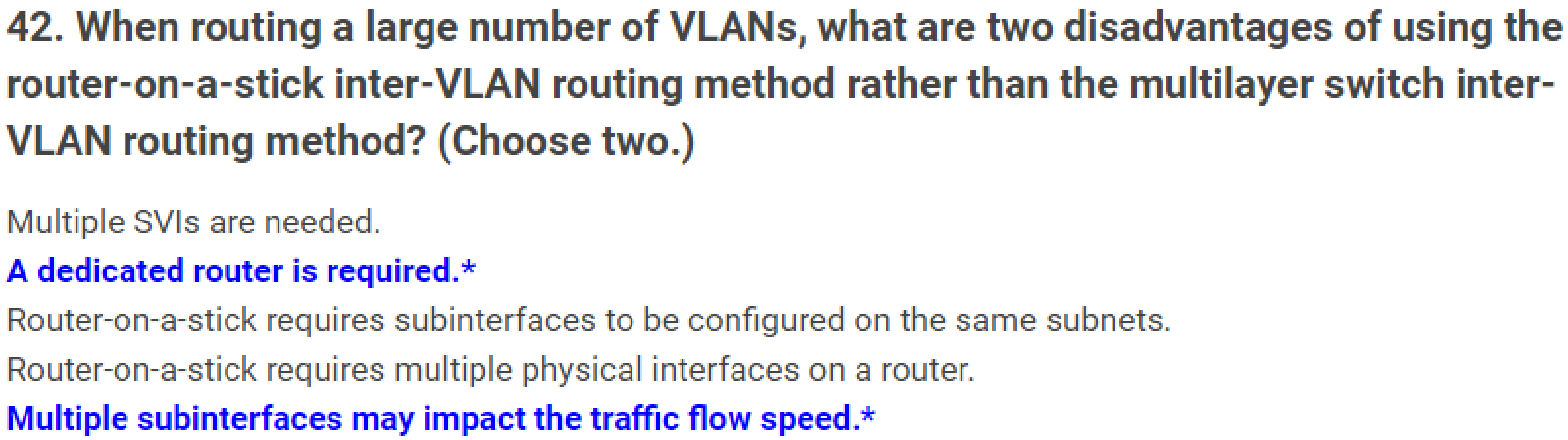
A network administrator has configured router CiscoVille with the above commands to provide inter-VLAN routing. What command will be required on a switch that is connected to the Gi0/0 interface on router CiscoVille to allow inter-VLAN routing?

switchport mode access

no switchport

switchport mode trunk*

switchport mode dynamic desirable



42. When routing a large number of VLANs, what are two disadvantages of using the router-on-a-stick inter-VLAN routing method rather than the multilayer switch inter-VLAN routing method? (Choose two.)

Multiple SVIs are needed.

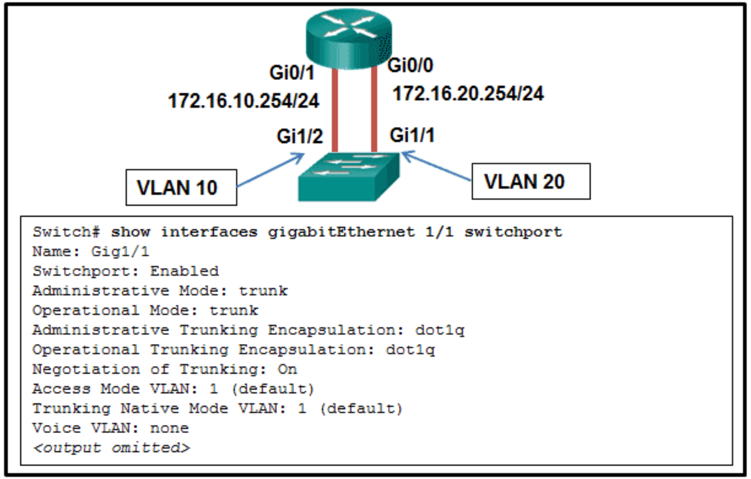
A dedicated router is required.*

Router-on-a-stick requires subinterfaces to be configured on the same subnets.

Router-on-a-stick requires multiple physical interfaces on a router.

Multiple subinterfaces may impact the traffic flow speed.*

43. Refer to the exhibit.



```
Switch# show interfaces gigabitEthernet 1/1 switchport
Name: Gig1/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted>
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p43

A network administrator is verifying the configuration of inter-VLAN routing. Users complain that PCs on different VLANs cannot communicate. Based on the output, what are two configuration errors on switch interface Gi1/1? (Choose two.)

Gi1/1 is in the default VLAN.*

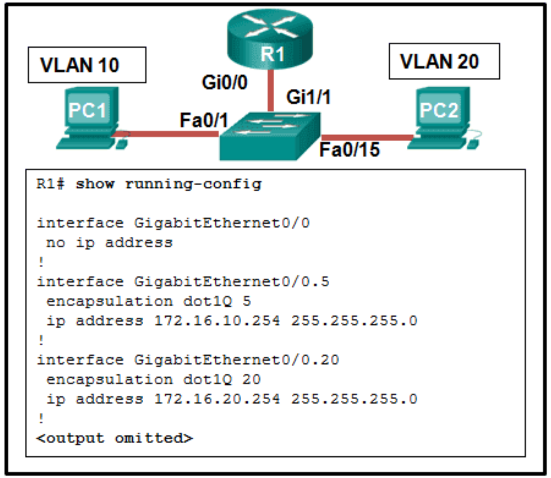
Voice VLAN is not assigned to Gi1/1.

Gi1/1 is configured as trunk mode.*

Negotiation of trunking is turned on on Gi1/1.

The trunking encapsulation protocol is configured wrong.

44. Refer to the exhibit.



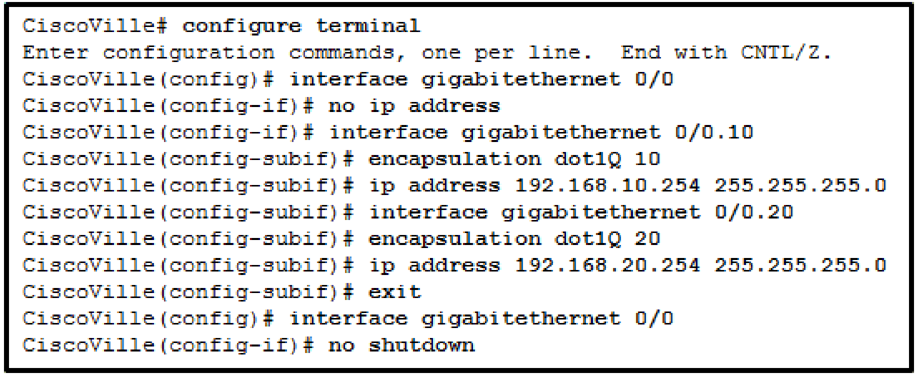
```
R1# show running-config

interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.5
 encapsulation dot1Q 5
 ip address 172.16.10.254 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.20.254 255.255.255.0
!
<output omitted>
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p44

A network administrator is verifying the configuration of inter-VLAN routing. Users complain that PC2 cannot communicate with PC1. Based on the output, what is the possible cause of the problem?

Gi0/0 is not configured as a trunk port.
The command interface GigabitEthernet0/0.5 was entered incorrectly.
There is no IP address configured on the interface Gi0/0.
The no shutdown command is not entered on subinterfaces.
The encapsulation dot1Q 5 command contains the wrong VLAN. *

45. Refer to the exhibit.



```
CiscoVille# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no ip address
CiscoVille(config-if)# interface gigabitethernet 0/0.10
CiscoVille(config-subif)# encapsulation dot1Q 10
CiscoVille(config-subif)# ip address 192.168.10.254 255.255.255.0
CiscoVille(config-subif)# interface gigabitethernet 0/0.20
CiscoVille(config-subif)# encapsulation dot1Q 20
CiscoVille(config-subif)# ip address 192.168.20.254 255.255.255.0
CiscoVille(config-subif)# exit
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no shutdown
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p45

A network administrator has configured router CiscoVille with the above commands to provide inter-VLAN routing. What type of port will be required on a switch that is connected to Gi0/0 on router CiscoVille to allow inter-VLAN routing?

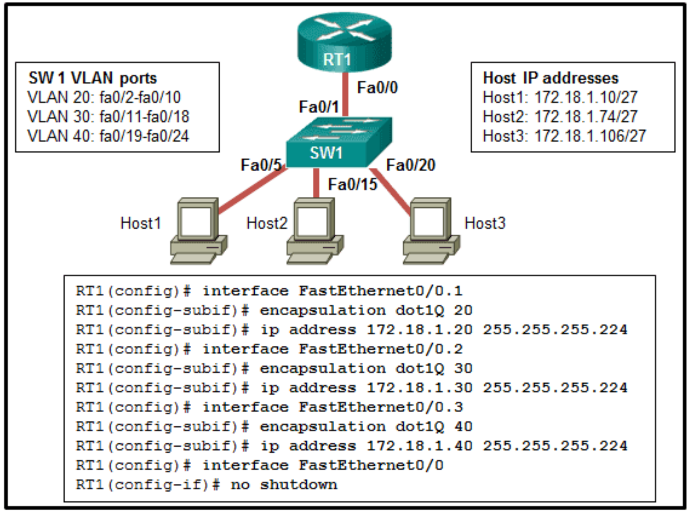
routed port

access port

trunk port*

SVI

46. Refer to the exhibit.



SW 1 VLAN ports
VLAN 20: fa0/2-fa0/10
VLAN 30: fa0/11-fa0/18
VLAN 40: fa0/19-fa0/24

Host IP addresses
Host1: 172.18.1.10/27
Host2: 172.18.1.74/27
Host3: 172.18.1.106/27

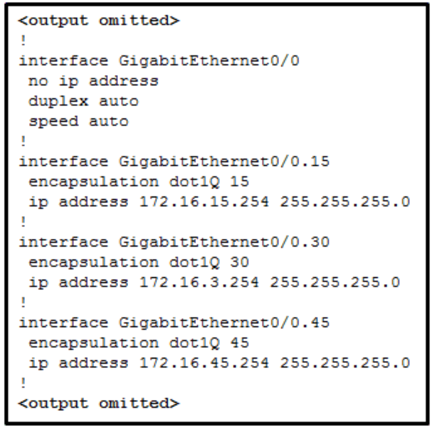
```
RT1(config)# interface FastEthernet0/0.1
RT1(config-subif)# encapsulation dot1Q 20
RT1(config-subif)# ip address 172.18.1.20 255.255.255.224
RT1(config)# interface FastEthernet0/0.2
RT1(config-subif)# encapsulation dot1Q 30
RT1(config-subif)# ip address 172.18.1.30 255.255.255.224
RT1(config)# interface FastEthernet0/0.3
RT1(config-subif)# encapsulation dot1Q 40
RT1(config-subif)# ip address 172.18.1.40 255.255.255.224
RT1(config)# interface FastEthernet0/0
RT1(config-if)# no shutdown
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p46

A network administrator is configuring RT1 for inter-VLAN routing. The switch is configured correctly and is functional. Host1, Host2, and Host3 cannot communicate with each other. Based on the router configuration, what is causing the problem?

Interface Fa0/0 is missing IP address configuration information.
IP addresses on the subinterfaces are incorrectly matched to the VLANs.*
Each subinterface of Fa0/0 needs separate no shutdown commands.
Routers do not support 802.1Q encapsulation on subinterfaces.

47. Refer to the exhibit.

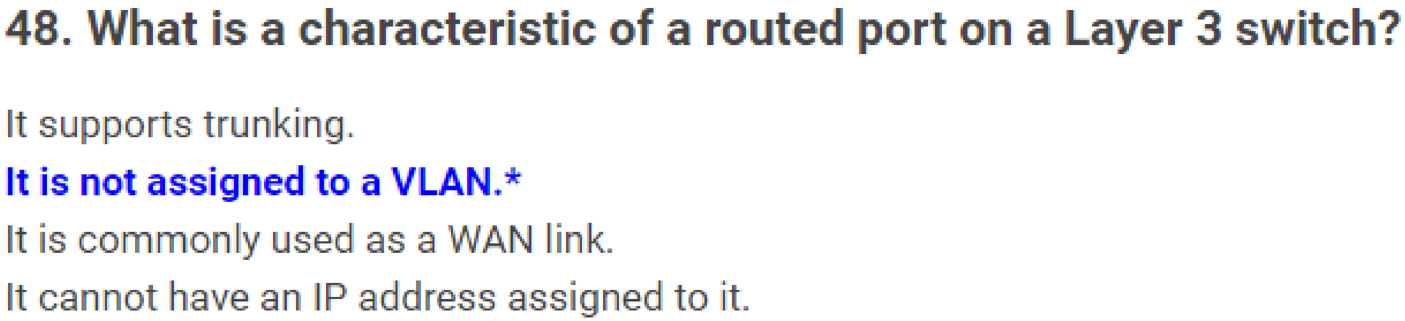


```
<output omitted>
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 172.16.15.254 255.255.255.0
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.3.254 255.255.255.0
!
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45
 ip address 172.16.45.254 255.255.255.0
!
<output omitted>
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p47

A router-on-a-stick configuration was implemented for VLANs 15, 30, and 45, according to the show running-config command output. PCs on VLAN 45 that are using the 172.16.45.0 /24 network are having trouble connecting to PCs on VLAN 30 in the 172.16.30.0 /24 network. Which error is most likely causing this problem?

The wrong VLAN has been configured on GigabitEthernet 0/0.45.
The command no shutdown is missing on GigabitEthernet 0/0.30.
The GigabitEthernet 0/0 interface is missing an IP address.
There is an incorrect IP address configured on GigabitEthernet 0/0.30.*



48. What is a characteristic of a routed port on a Layer 3 switch?

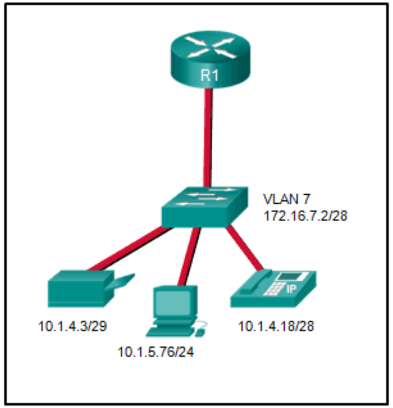
It supports trunking.

It is not assigned to a VLAN.*

It is commonly used as a WAN link.

It cannot have an IP address assigned to it.

49. Refer to the exhibit.

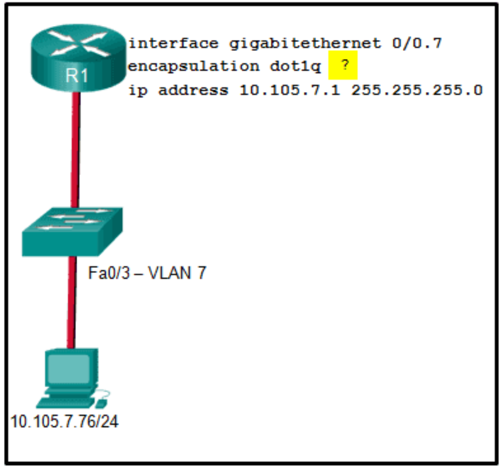


CCNA 2 v7.0 Modules 1 – 4 Exam Answers p49

A network administrator needs to configure router-on-a-stick for the networks that are shown. How many subinterfaces will have to be created on the router if each VLAN that is shown is to be routed and each VLAN has its own subinterface?

1
2
3
4*
5

74. Refer to the exhibit.



```
interface gigabitethernet 0/0.7
encapsulation dot1q  ?
ip address 10.105.7.1 255.255.255.0
```

CCNA 2 v7.0 Modules 1 – 4 Exam Answers p74

A network administrator is configuring inter-VLAN routing on a network. For now, only one VLAN is being used, but more will be added soon. What is the missing parameter that is shown as the highlighted question mark in the graphic?

It identifies the subinterface.

It identifies the VLAN number.*

It identifies the native VLAN number.

It identifies the type of encapsulation that is used.

It identifies the number of hosts that are allowed on the interface.

cisco