Building a Medium-Sized Network

Interconnecting Cisco Networking Devices, Part 1 (ICND1) v2.0

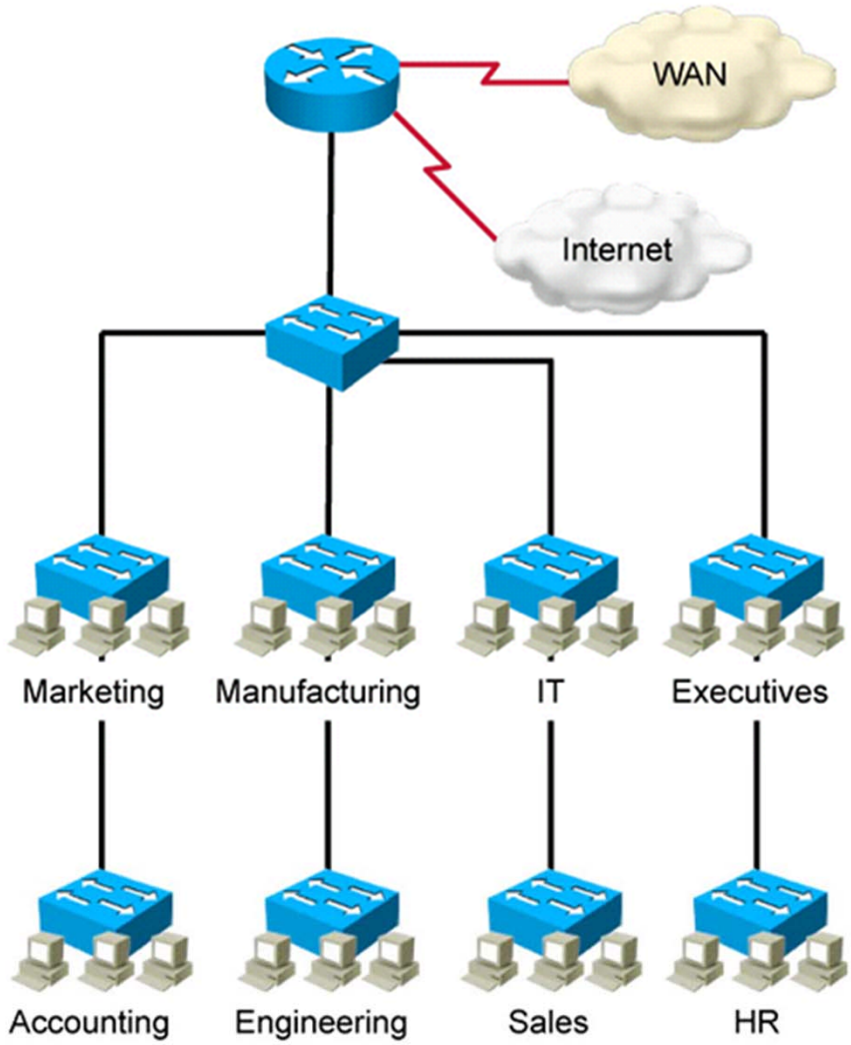
Implementing VLANs and Trunks

Building a Medium-Sized Network

Issues in a Poorly Designed Network

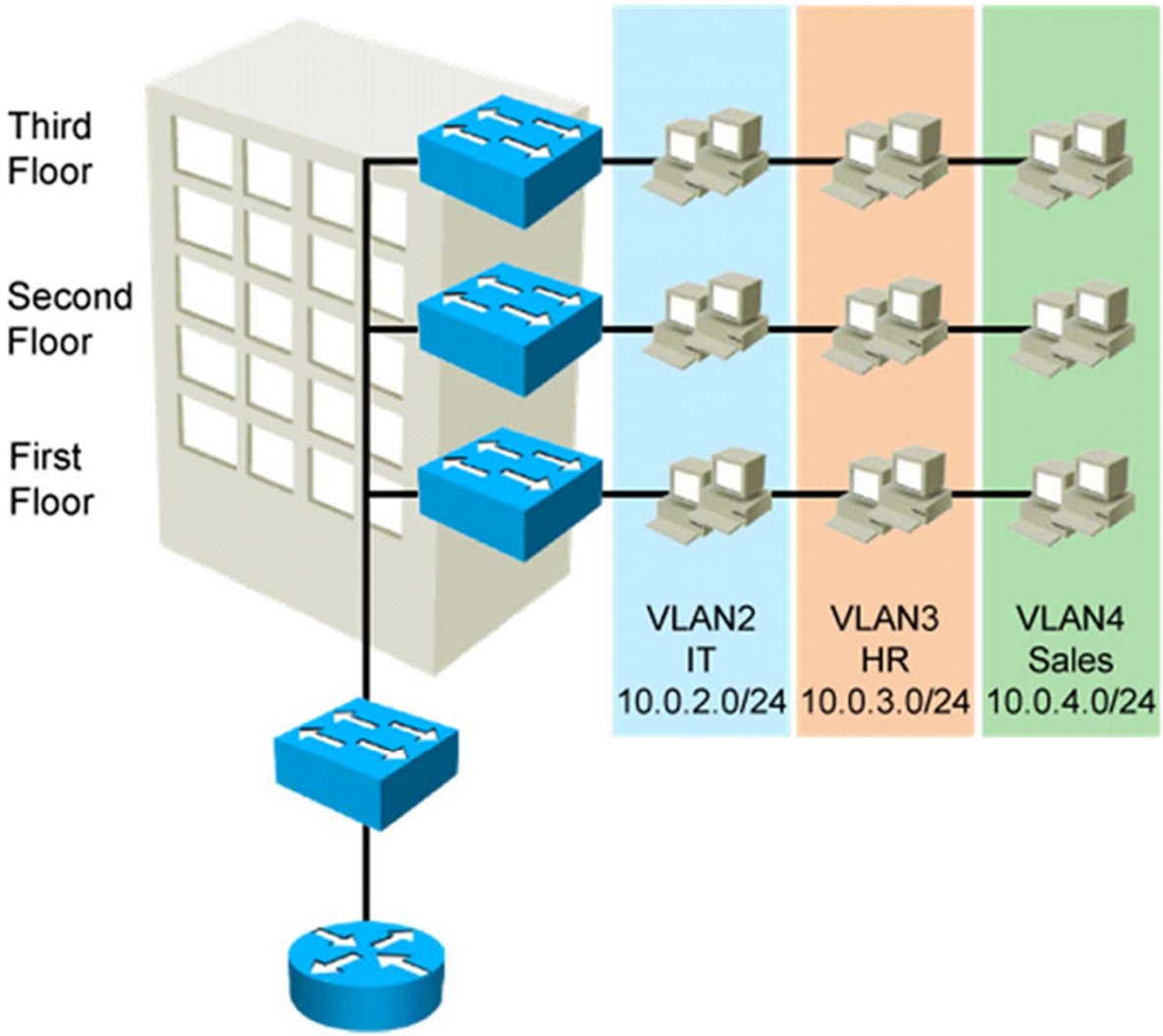
These issues are often found in poorly designed networks:

- Large broadcast domains
- Management and support challenges
- Possible security vulnerabilities



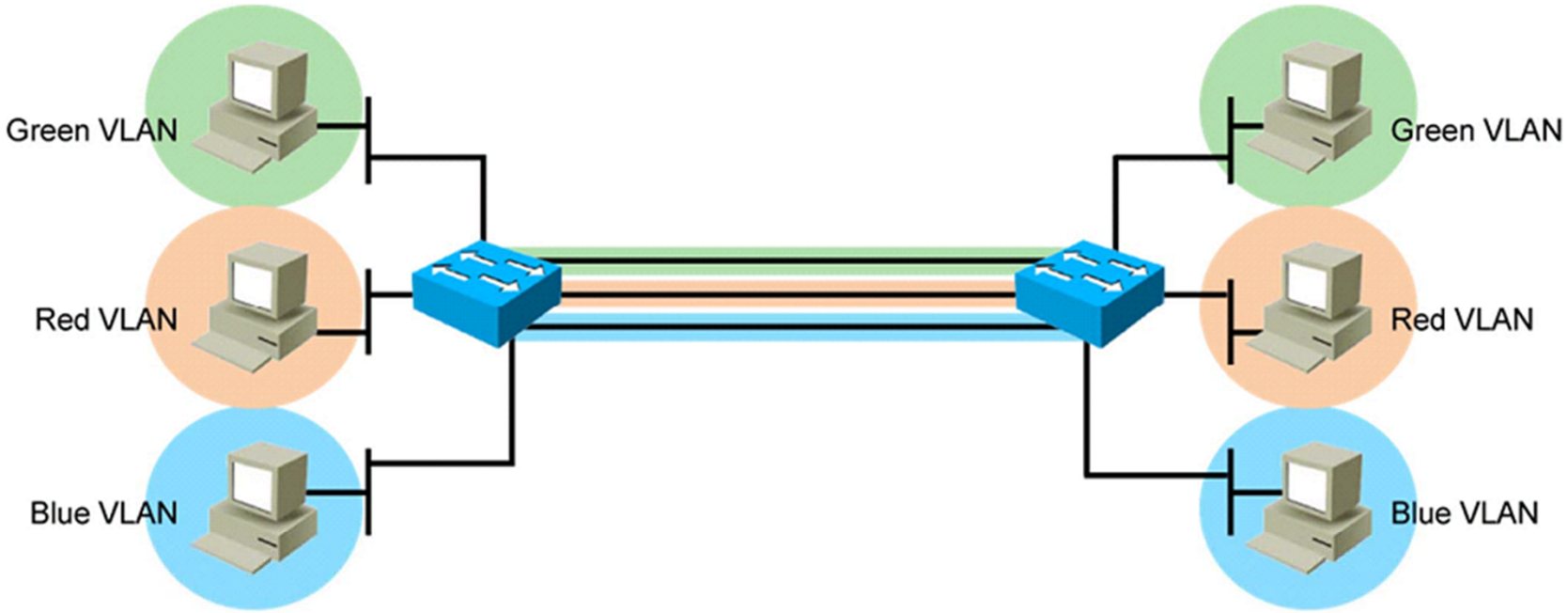
VLAN Introduction

- A VLAN is a virtual LAN.
- VLAN = broadcast domain
- VLAN = logical network (subnet)
- VLANs address these needs:
  - Segmentation
  - Security
  - Network flexibility



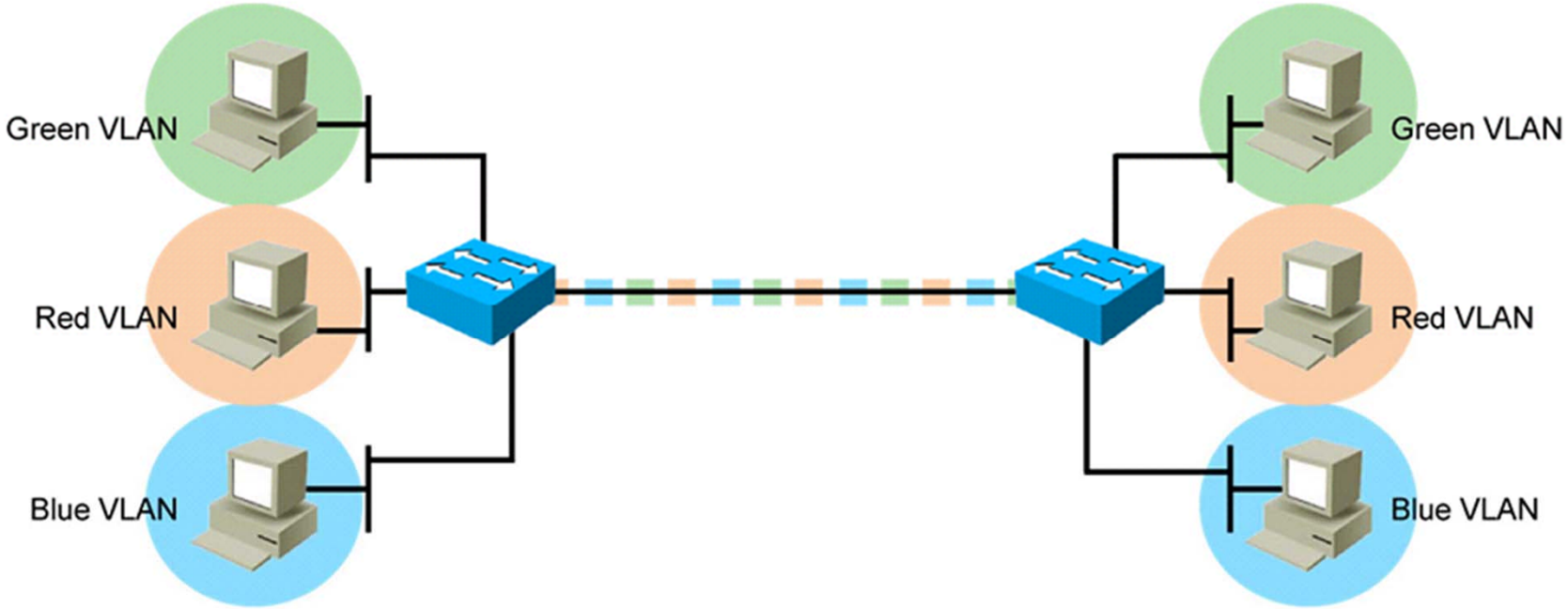
Trunking with 802.1Q

Running many VLANs between switches would require the same number of interconnecting links.

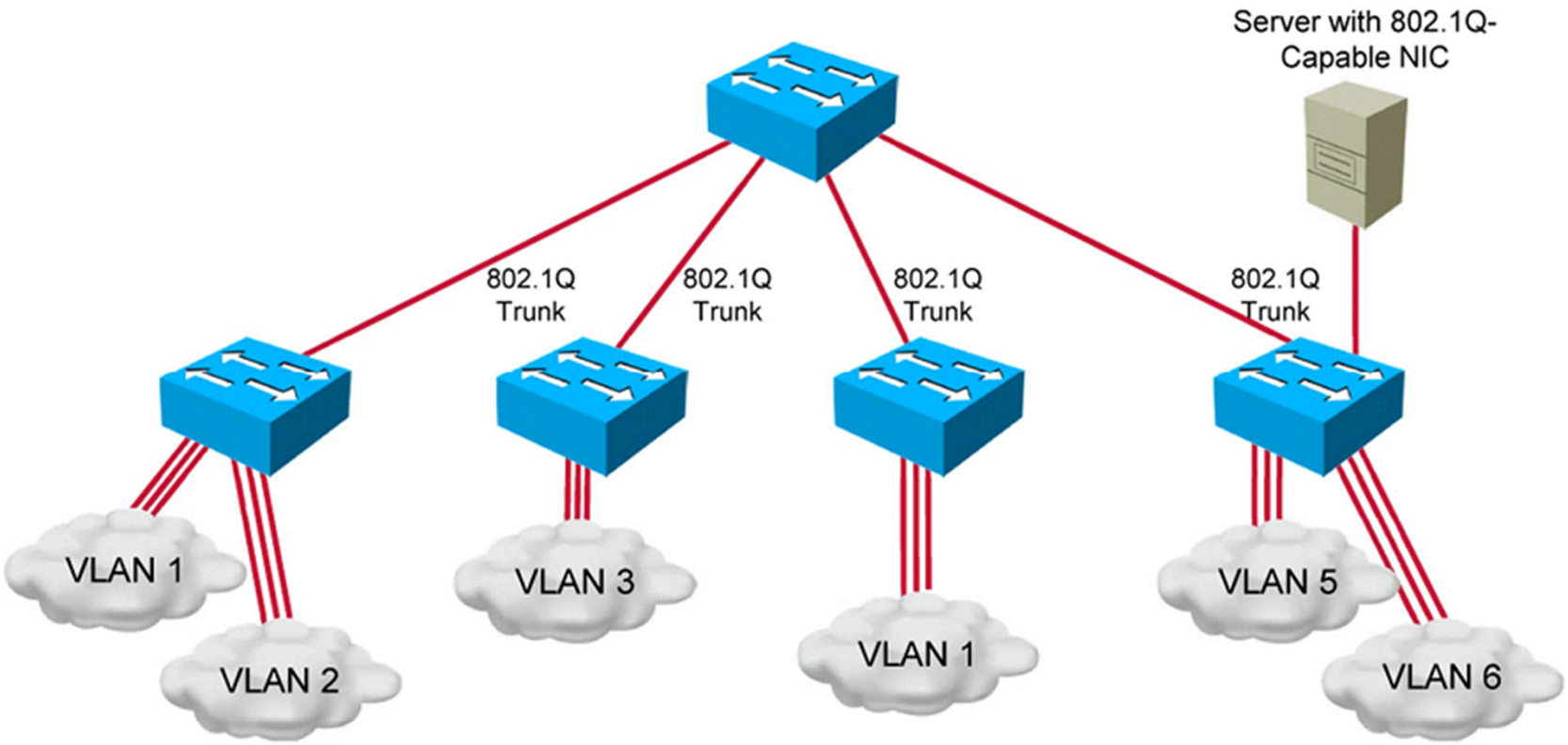


Trunking with 802.1Q (Cont.)

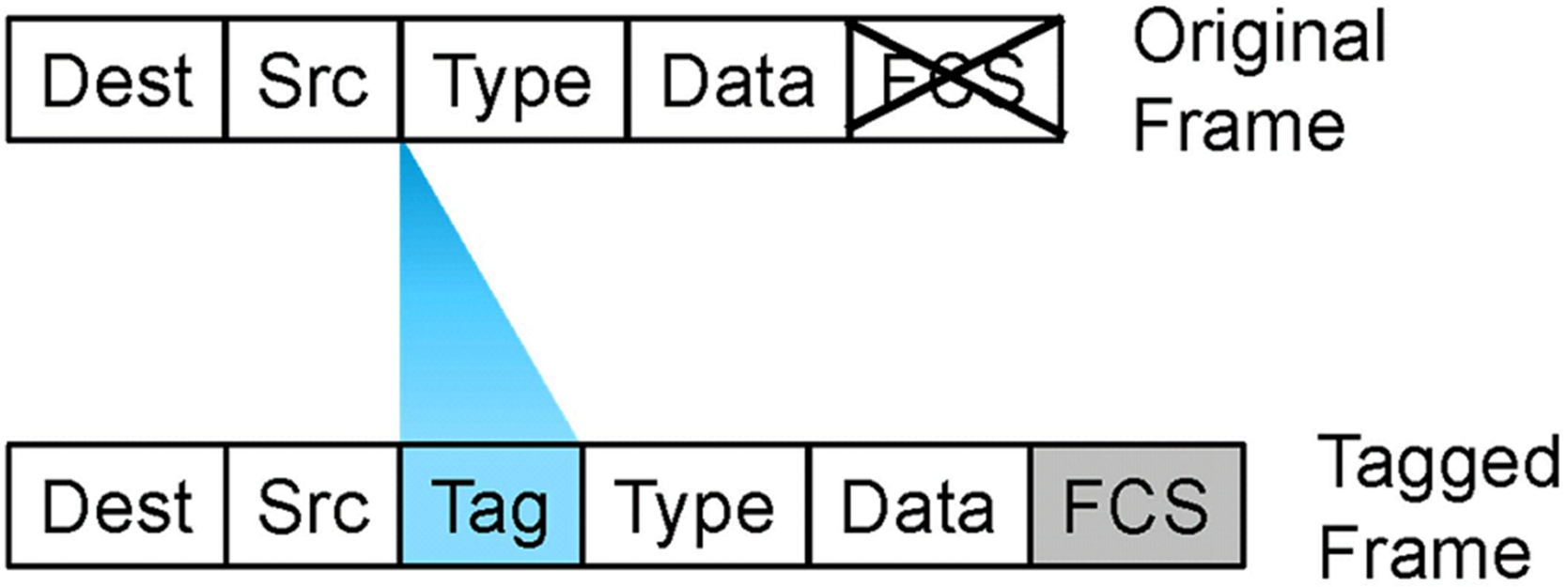
- Combining many VLANs on the same port is called *trunking*.
- A trunk allows the transportation of frames from different VLANs.
- Each frame has a tag that specifies the VLAN that it belongs to.
- Frames are forwarded to the corresponding VLAN based on the tag information.



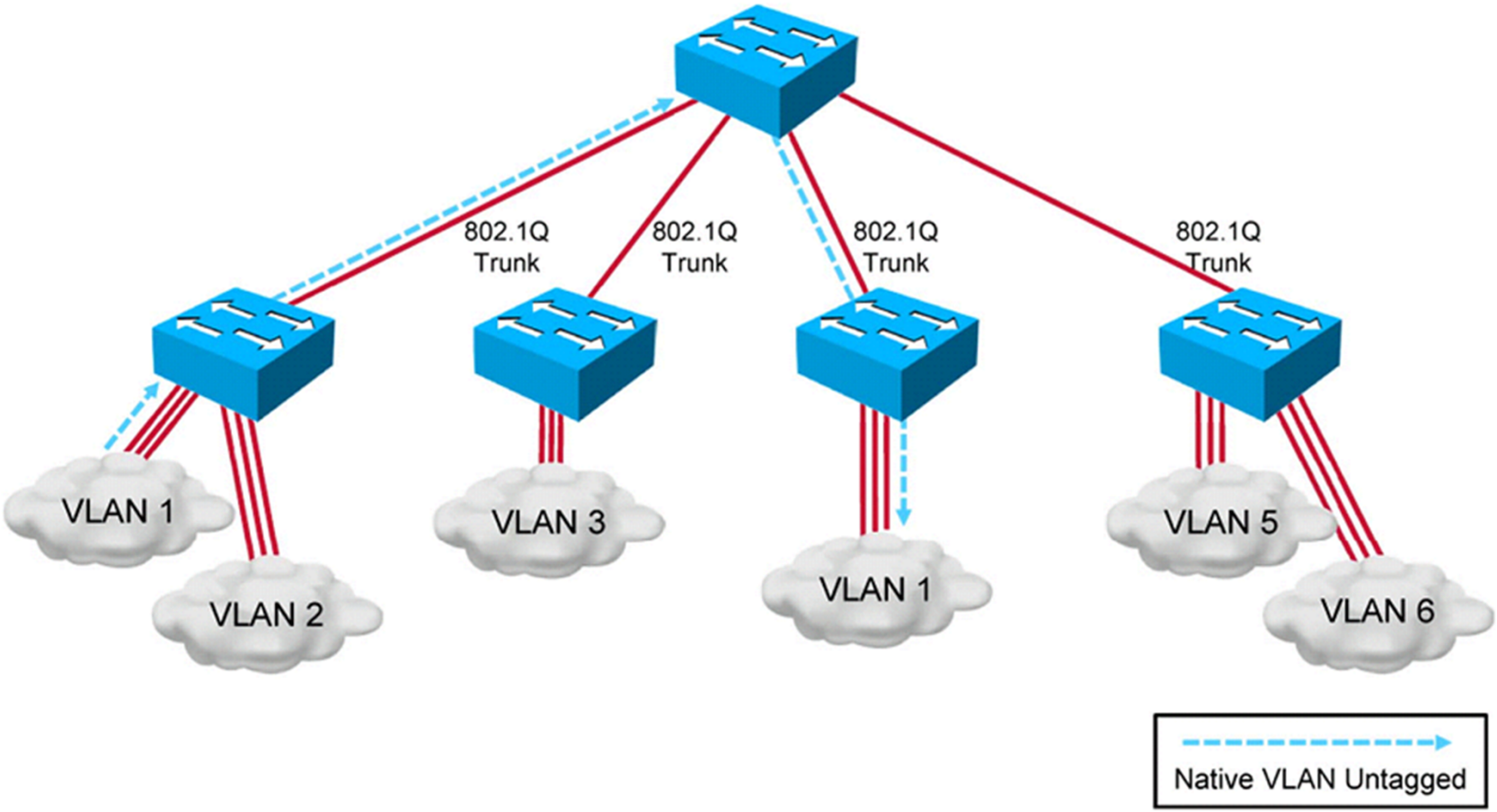
Trunking with 802.1Q (Cont.)



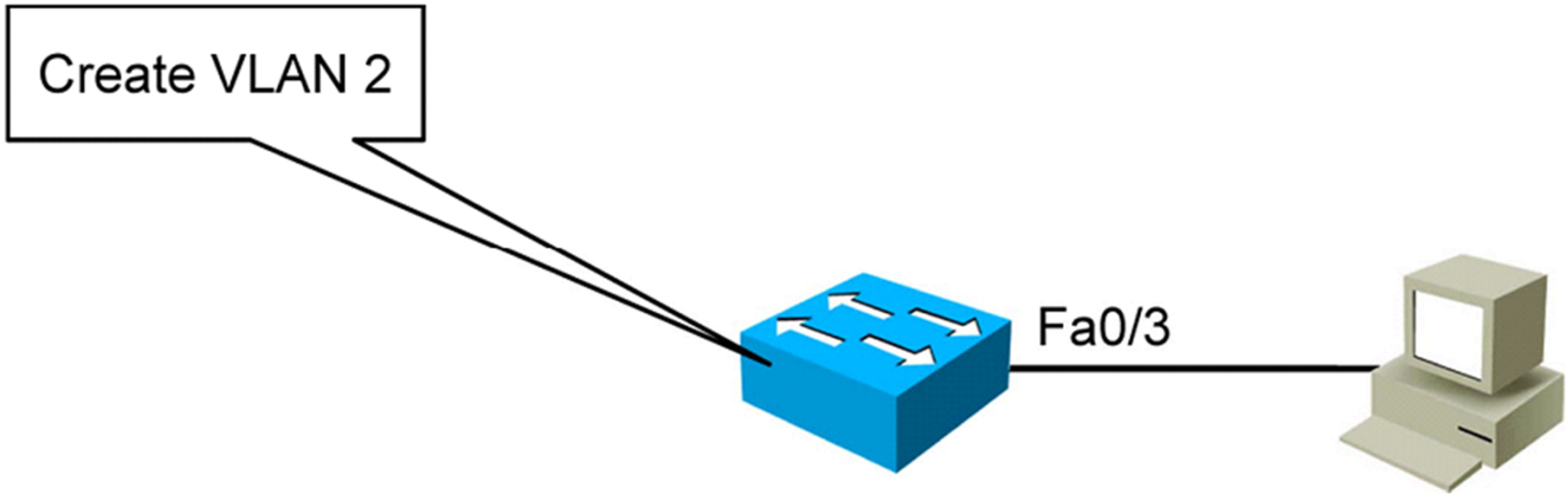
Trunking with 802.1Q (Cont.)



Trunking with 802.1Q (Cont.)



Creating a VLAN




```
SwitchX#configure terminal
SwitchX(config)#vlan 2
SwitchX(config-vlan)#name Sales
```

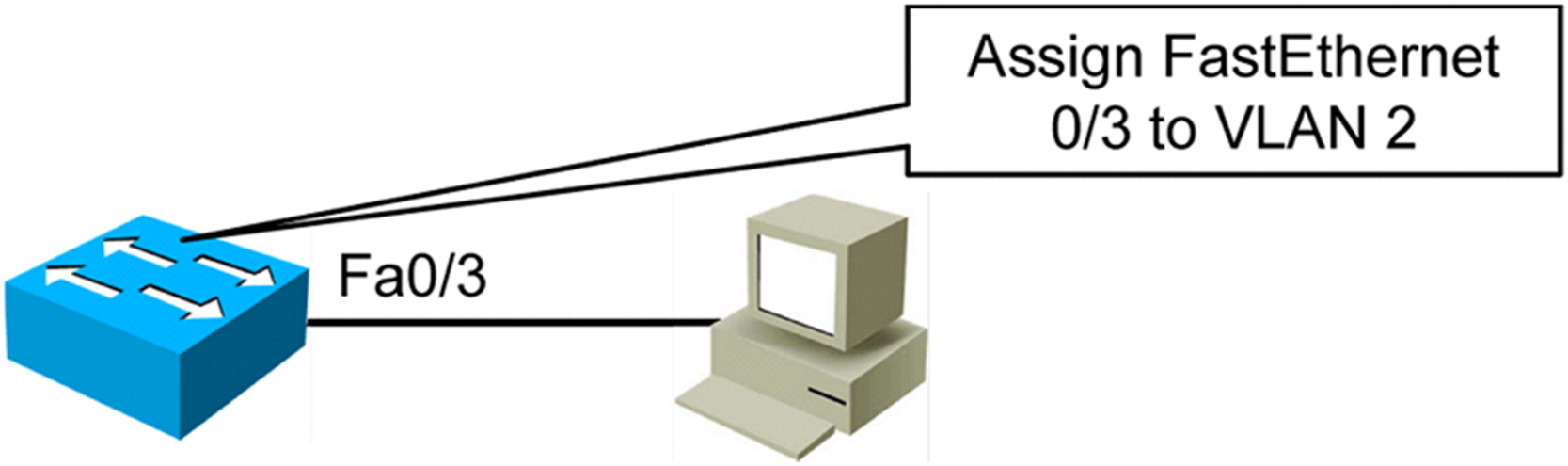
- Adds VLAN 2 and names it "Sales"

Creating a VLAN (Cont.)

```
SwitchX# show vlan id 2

VLAN Name                 Status    Ports
---- -------------------- -------   ---------------------
2          Sales                    active    Fa0/2, Fa0/12

VLAN Type SAID    MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ---- ------- ----- ------ ------ -------- --- --------- ------ ------
2    enet 100002  1500  -      -      -        -    -        0      0

<output omitted>
```

- Verifies VLAN2

Assigning a Port to a VLAN




```
SwitchX#configure terminal
SwitchX(config)#interface FastEthernet 0/3
SwitchX(config-if)#switchport access vlan 2
```

- Assigns port FastEthernet0/3 to VLAN 2

Assigning a Port to a VLAN (Cont.)

```
SwitchX#show vlan brief
VLAN  Name                                Status     Ports
----  --------------------------------    ---------  -------------------
1     default                             active     Fa0/1
2     Sales                               active     Fa0/3
3     vlan3                               active
4     vlan4                               active

<output omitted>
```

- Verifies that port FastEthernet0/3 was assigned to VLAN 2

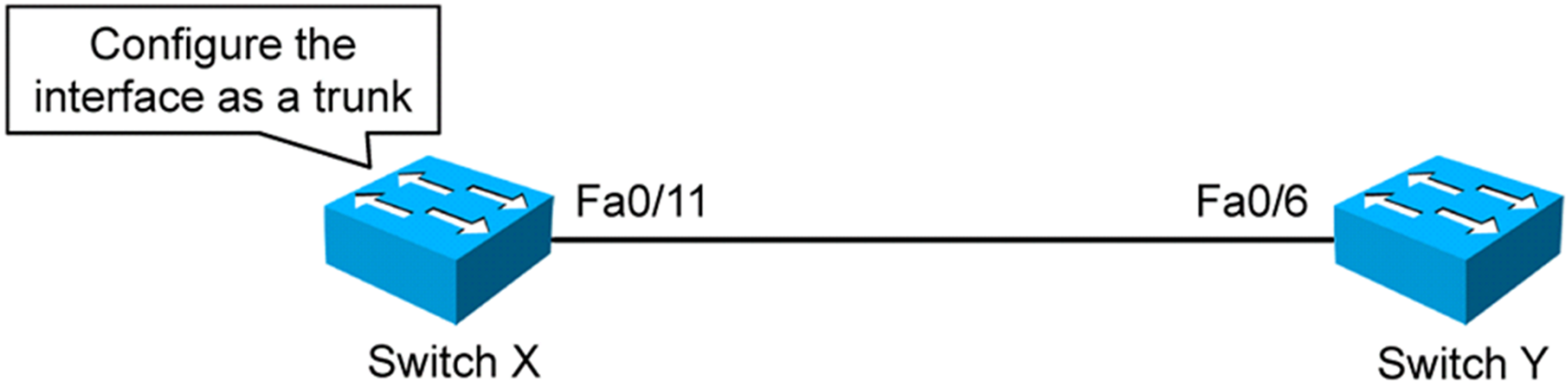
Assigning a Port to a VLAN (Cont.)

```
SwitchX#show interface FastEthernet0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 2 (Sales)

<output omitted>
```

- Verifies VLAN membership on the Fa0/3 interface

Configuring an 802.1Q Trunk

- Enter the interface configuration mode.
- Configure the Fa0/11 interface as a VLAN trunk.
- Change the native VLAN from 1 to 99.




```
SwitchX#configure terminal
SwitchX(config)#interface FastEthernet 0/11
SwitchX(config-if)#switchport mode trunk
SwitchX(config-if)#switchport trunk native vlan 99
```

Configuring an 802.1Q Trunk (Cont.)

```
SwitchX#show interfaces FastEthernet0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 99
Trunking Native Mode VLAN: 99

<output omitted>
```

```
SwitchX#show interfaces FastEthernet0/11 trunk
Port     Mode    Encapsulation  Status        Native vlan
Fa0/11   on      802.1q         trunking      99
 Port       Vlans allowed on trunk
Fa0/11       1-4094
 Port         Vlans allowed and active in management domain
Fa0/11       1-13

<output omitted>
```

- Verifies a trunk on the Fa0/11 interface

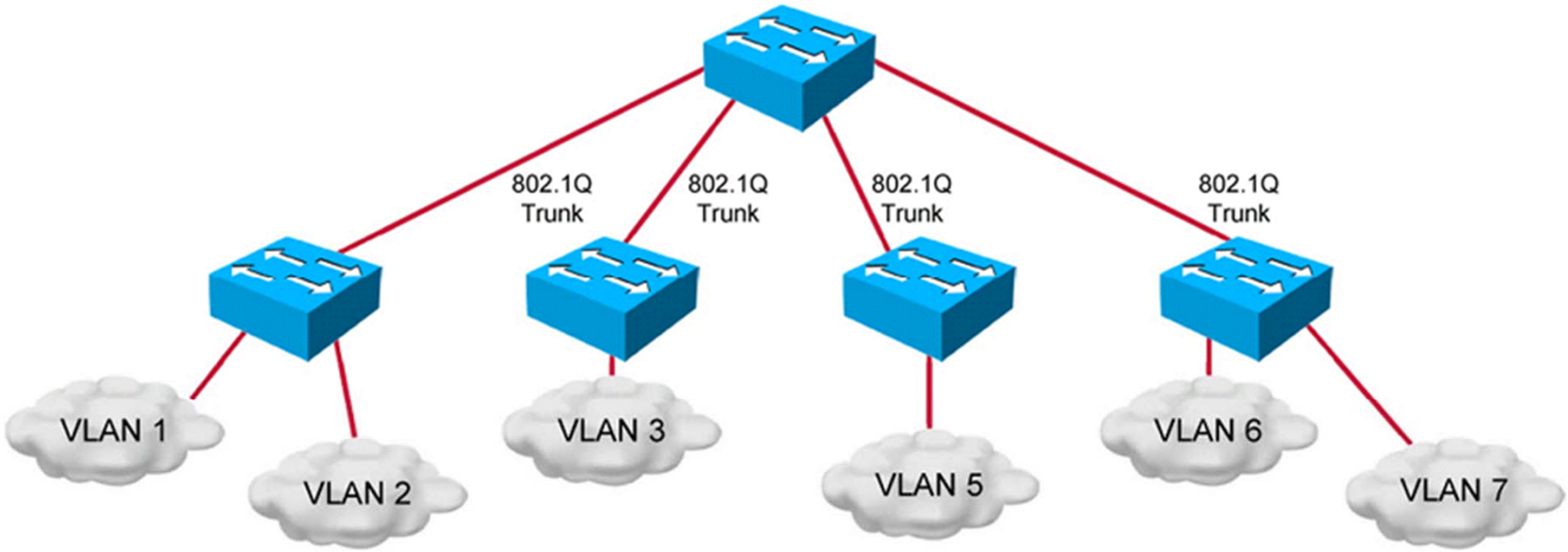
VLAN Design Considerations

- The maximum number of VLANs is switch-dependent.
- VLAN 1 is the factory-default Ethernet VLAN.
- A use-dedicated VLAN is for the Cisco switch management IP address.
- Keep management traffic in a separate VLAN.
- Change the native VLAN to something other than VLAN 1.

VLAN Design Considerations (Cont.)

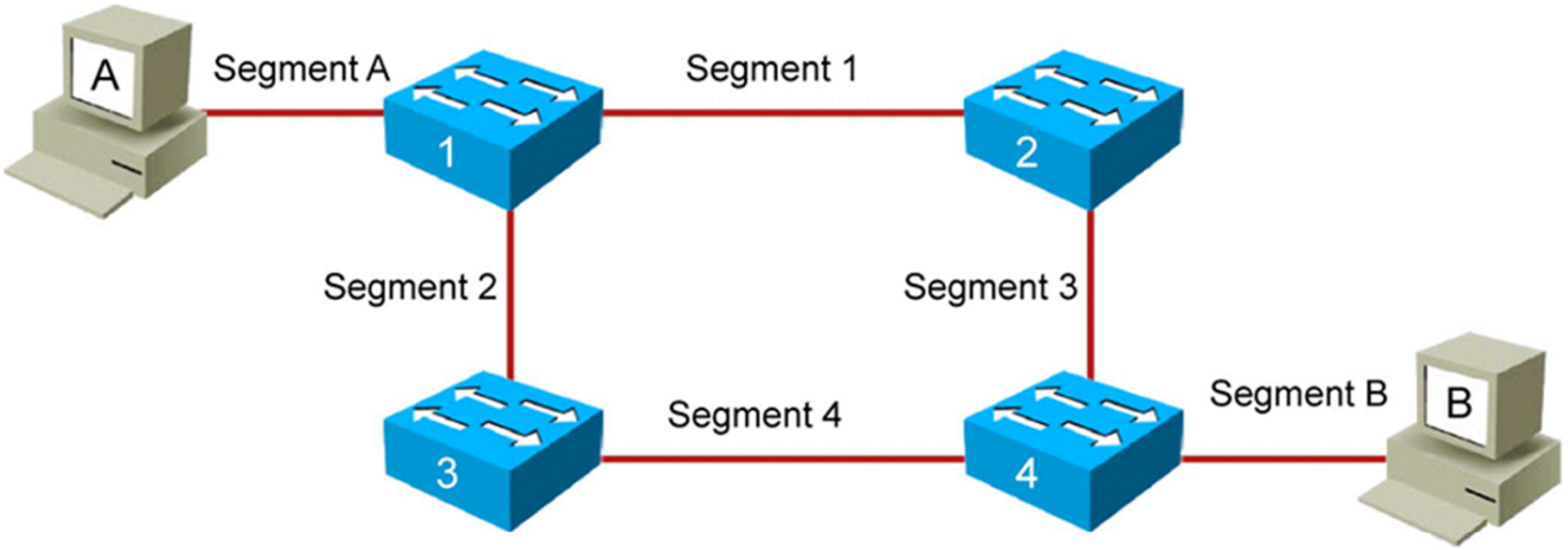
When configuring a trunk link, consider the following:

- Make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link.
- DTP manages trunk negotiations between Cisco switches.

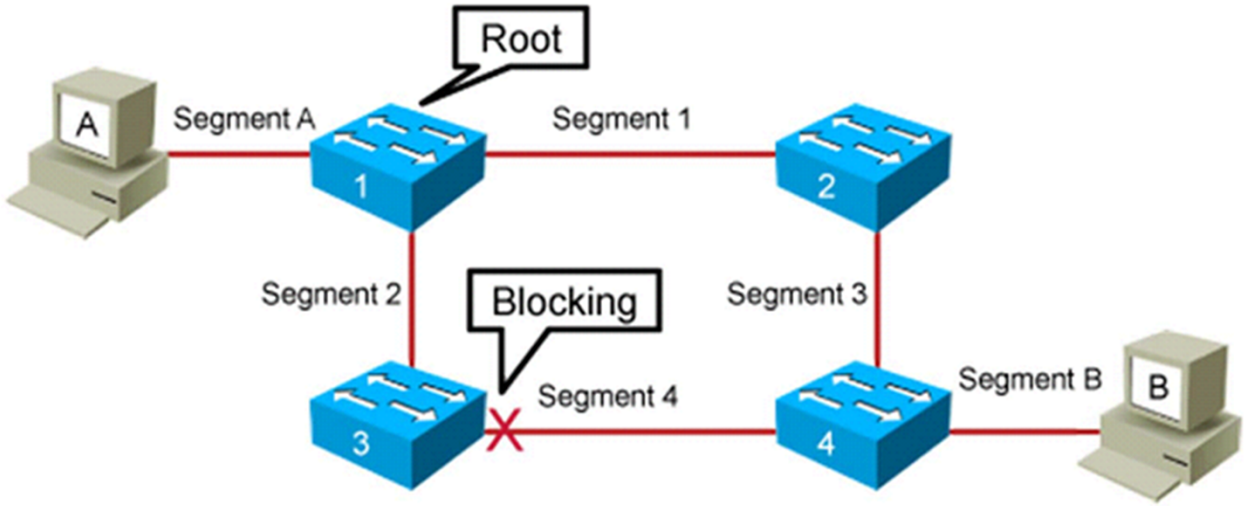


Physical Redundancy in a LAN

Loops may occur in the network as part of a design strategy for redundancy.



Physical Redundancy in a LAN (Cont.)



Summary

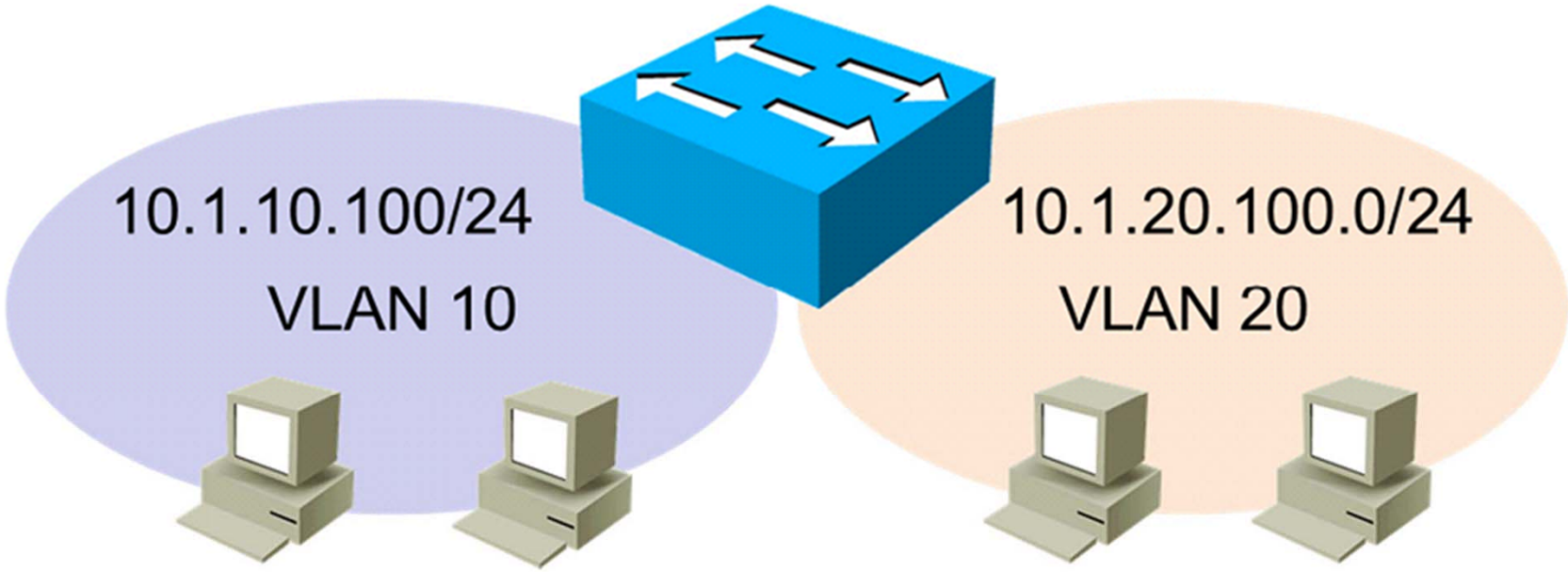
- VLANs are independent LAN networks and address segmentation, security, and organizational flexibility.
- Ethernet trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across many switches.
- To implement VLANs and trunking, you need to create VLANs, configure trunk links, and assign switch ports to selected VLANs.
- Physical redundancy is required for network reliability.
- STP ensures a loop-free topology.

Routing Between VLANs

Building a Medium-Sized Network

Purpose of Inter-VLAN Routing

- A VLAN creates a separate switching segment.
- Traffic cannot be switched between VLANs.
- VLANs have different IP subnets.
- Routing is necessary to forward traffic between VLANs.



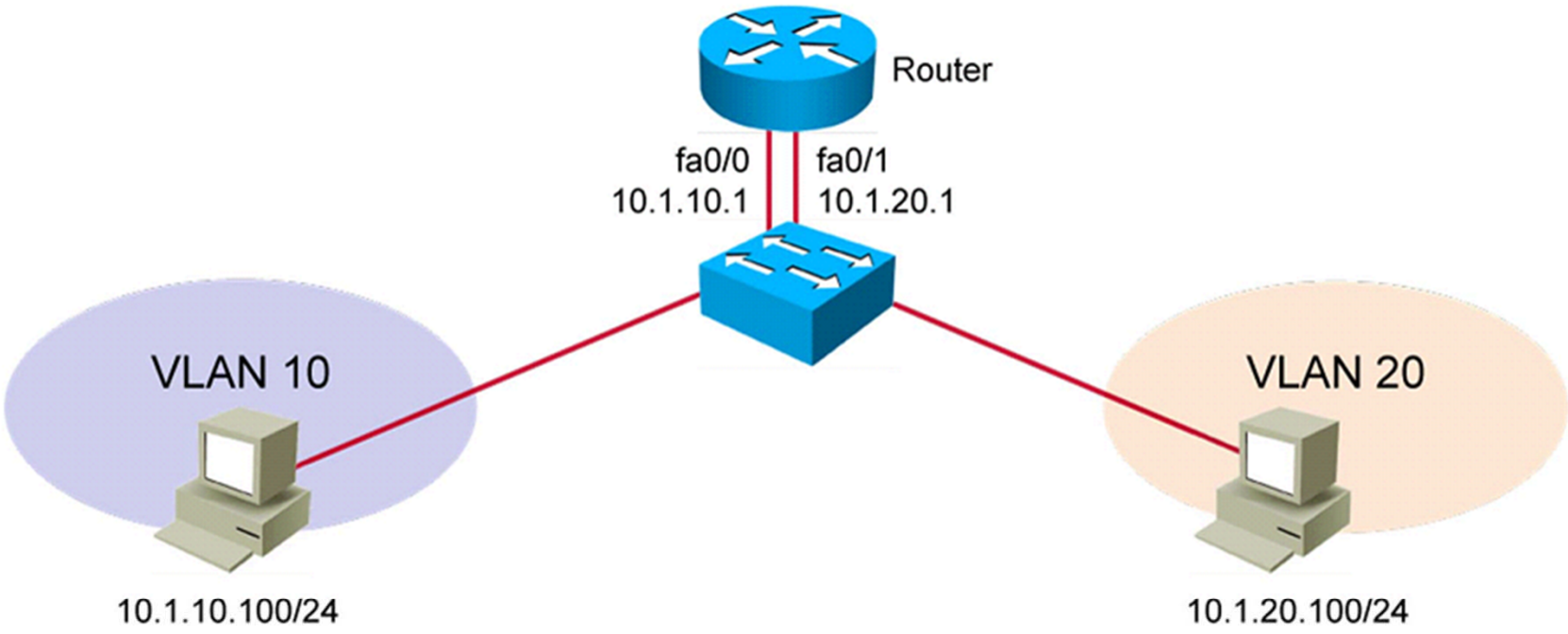
Options for Inter-VLAN Routing

These solutions can provide inter-VLAN routing:

- Router with a separate interface in each VLAN
- Router with a trunk link
- Layer 3 switch

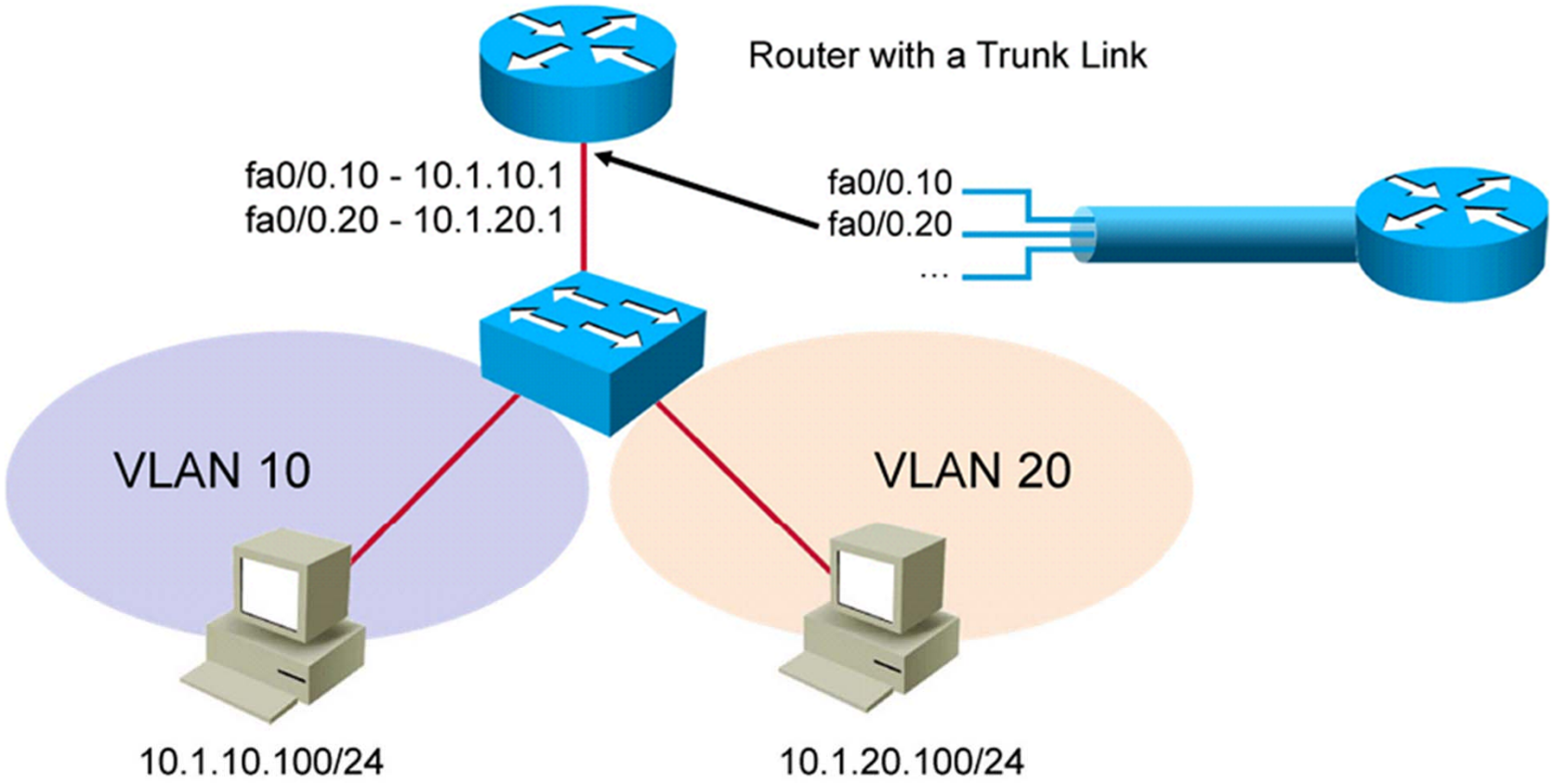
Options for Inter-VLAN Routing (Cont.)

Option: Router with a separate interface in each VLAN



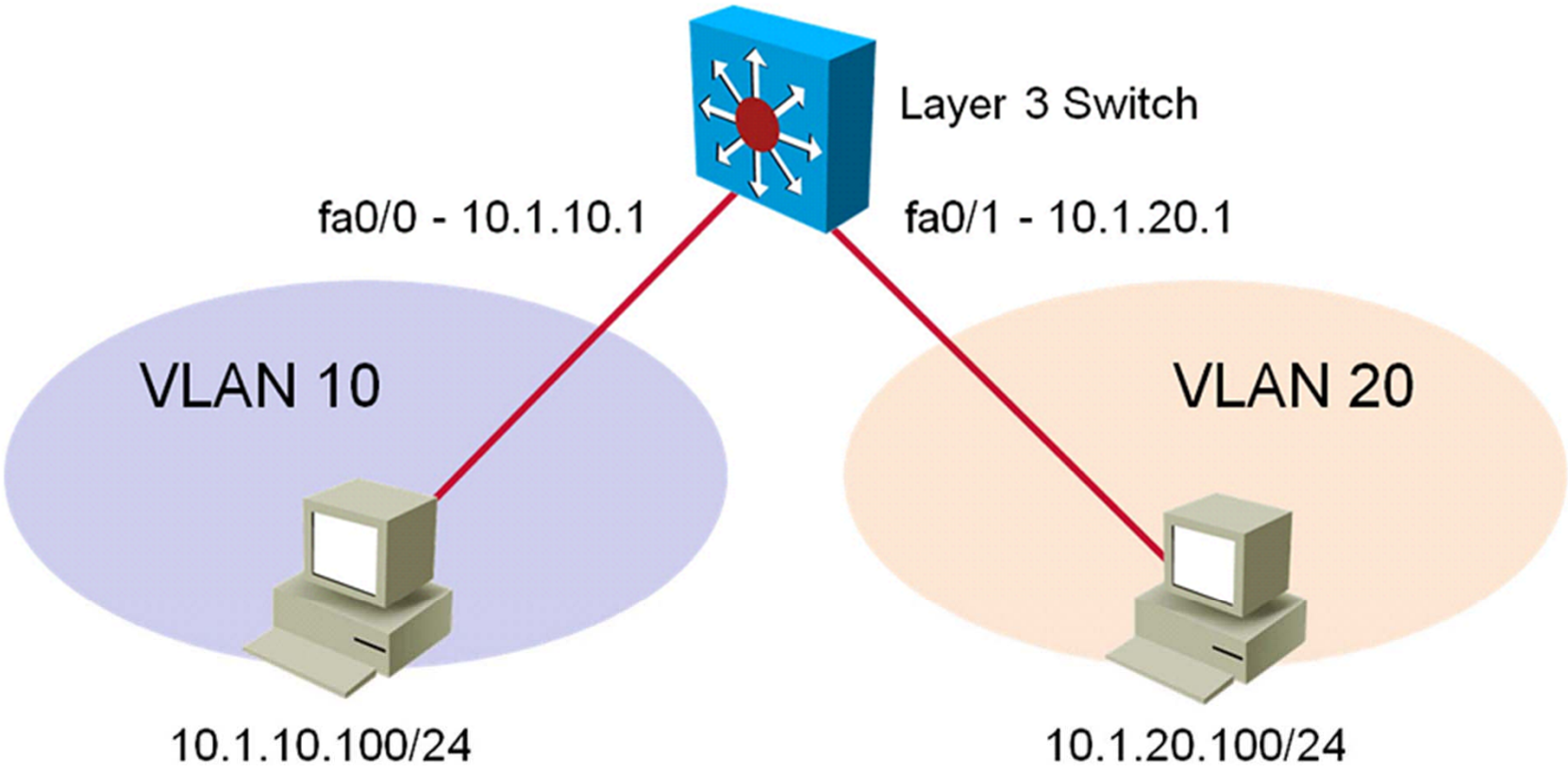
Options for Inter-VLAN Routing (Cont.)

Option: Router with a trunk link



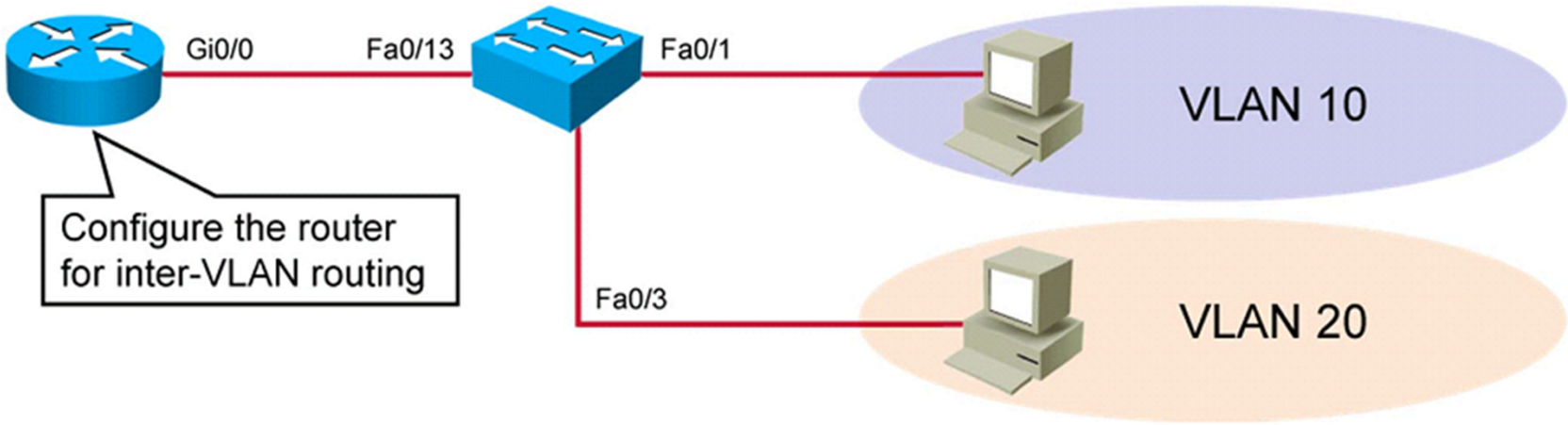
Options for Inter-VLAN Routing (Cont.)

Option: Layer 3 switch



Configuring a Router with a Trunk Link

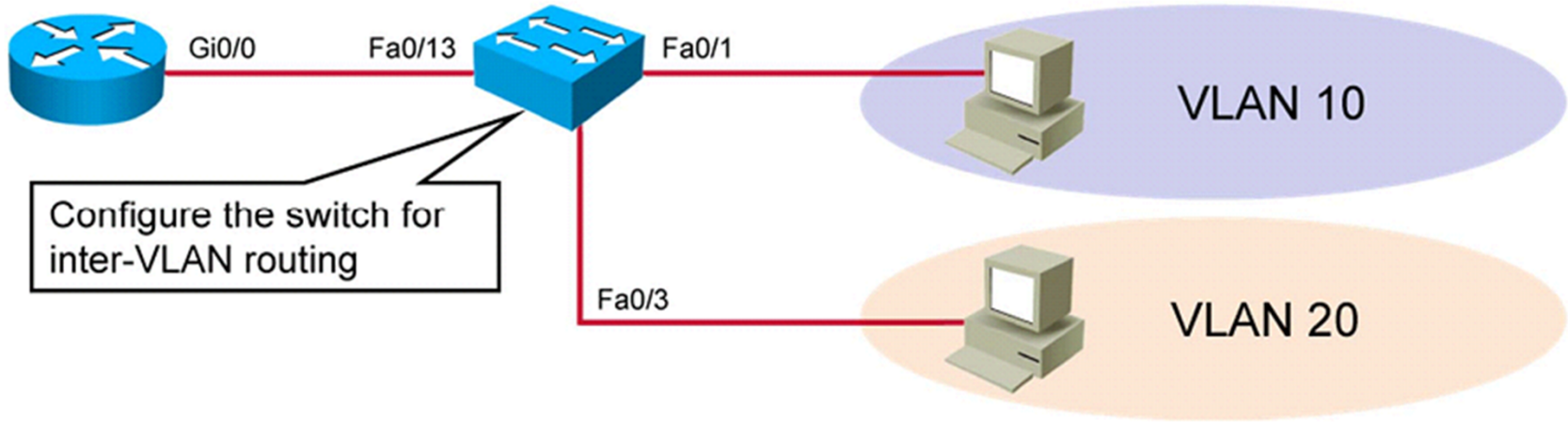
Configures subinterfaces and trunking on the router




```
Router(config)#interface GigabitEthernet 0/0.10
Router(config-if)#encapsulation dot1Q 10
Router(config-if)#ip address 10.1.10.1 255.255.255.0
Router(config-if)#interface GigabitEthernet 0/0.20
Router(config-if)#encapsulation dot1Q 20
Router(config-if)#ip address 10.1.20.1 255.255.255.0
```

Configuring Router with a Trunk Link (Cont.)

Assigns ports to specific VLANs and configures the port toward the router as a trunk




```
Switch(config)#interface FastEthernet 0/13
Switch(config-if)#switchport mode trunk
Switch(config-if)#interface FastEthernet 0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface FastEthernet 0/3
Switch(config-if)#switchport access vlan 20
```

Configuring Router with a Trunk Link (Cont.)

Verifies the VLAN subinterfaces

```
Router#show vlans

<output omitted>

Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   GigabitEthernet0/0.10

   Protocols Configured:   Address:        Received:  Transmitted:
           IP              10.1.10.1             11             18

<output omitted>

Virtual LAN ID:  20 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   GigabitEthernet0/0.20

   Protocols Configured:   Address:        Received:  Transmitted:
           IP              10.1.20.1             11              8

<output omitted>
```

Configuring Router with a Trunk Link (Cont.)

Verifies the IP routing table for VLAN subinterfaces

```
Router#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

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L        10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C        10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
L        10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
```

Summary

- Inter-VLAN communication cannot occur without a Layer 3 device (Layer 3 switch or router).
- Routing is necessary to forward traffic between VLANs.
- A router with a trunk link is configured with a subinterface for each VLAN.

Using a Cisco Network Device as a DHCP Server

Building a Medium-Sized Network

Need for a DHCP Server

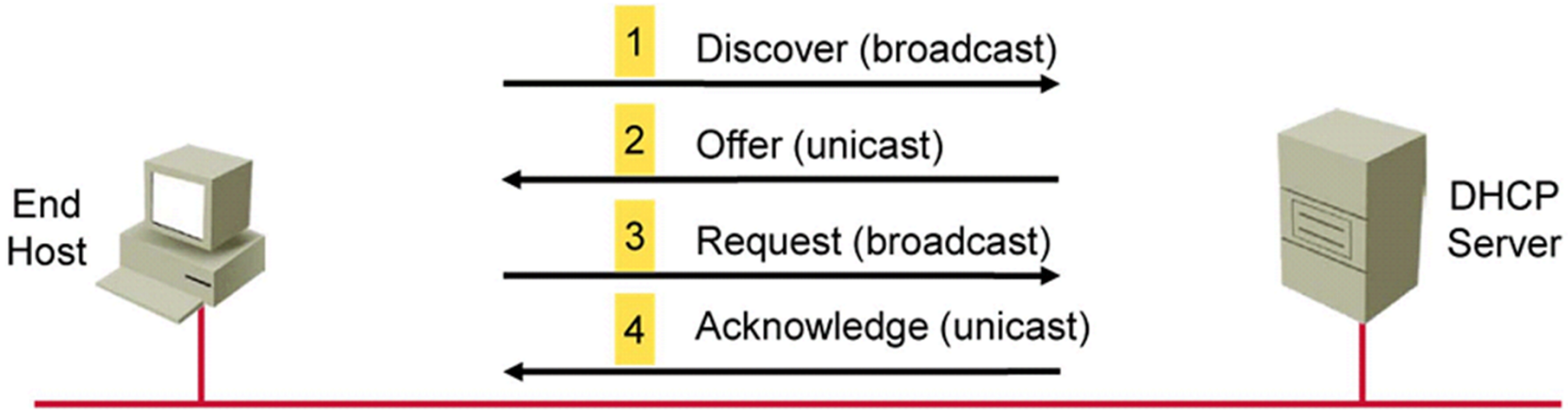
A manual IP address assignment in a medium-sized LAN is as follows:

- Time consuming
- Prone to errors
- Unfavorable to employee mobility

A DHCP IP address assignment in a segmented LAN is as follows:

- An IP address that is automatically assigned in accordance with user VLAN settings
- A centralized IP address allocation that enables consistency across the whole organization

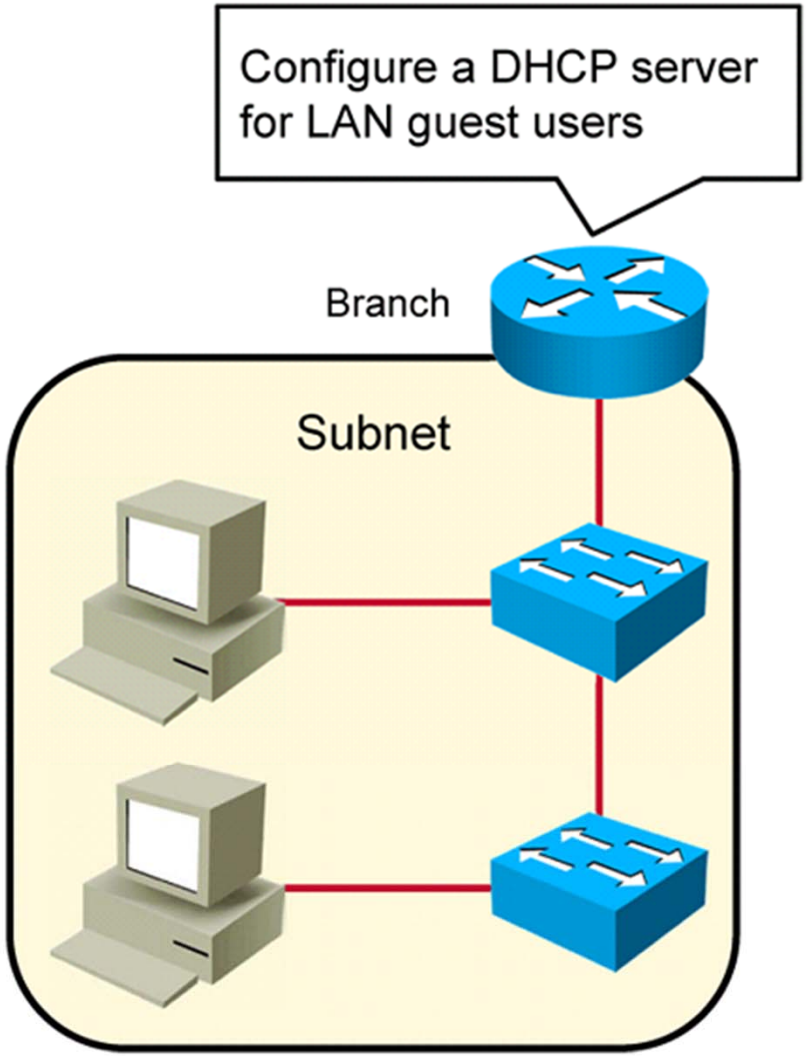
Understanding DHCP



Configuring a DHCP Server

Configuration scenario:

- Configure a DHCP server on a Cisco router
- Assign IP addresses from address pool 10.1.50.0/24 with a lease time of 12 hours
- Do not assign IP addresses from 10.1.50.1 to 10.1.50.50
- Additional parameters: default gateway, domain name, and DNS server



Configuring a DHCP Server (Cont.)

Cisco IOS DHCP server configuration:

- Enter the DHCP pool configuration mode
- Assign DHCP parameters to the DHCP pool
- Exclude IP addresses from the DHCP assignment

```
Branch(config)# ip dhcp pool Guests
Branch(dhcp-config) #network 10.1.50.0 /24
Branch(dhcp-config)# default-router 10.1.50.1
Branch(dhcp-config)# dns-server 10.1.50.1
Branch(dhcp-config)# domain-name example.com
Branch(dhcp-config)# lease 0 12
Branch(dhcp-config)# exit
Branch(config)# ip dhcp excluded-address 10.1.50.1 10.1.50.50
```

Monitoring DHCP Server Functions

```
Branch# show ip dhcp pool

Pool Guests :
 Utilization mark (high/low)     : 100 / 0
 Subnet size (first/next)        : 0 / 0
 Total addresses                 : 254
 Leased addresses                : 2
 Pending event                   : none
 1 subnet is currently in the pool :
 Current index       IP address range              Leased addresses
 10.1.50.55          10.1.50.1  - 10.1.50.254      2
```

- Verifies information about configured DHCP address pools

Monitoring DHCP Server Functions (Cont.)

```
Branch# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address    Client-ID/              Lease expiration        Type
              Hardware address/
              User name
10.1.50.54    0100.0c29.8807.34   Oct 18 2012 06:56 PM  Automatic
10.1.50.56    0100.0c29.4532.be   Oct 18 2012 07:08 PM  Automatic
```

- Displays address bindings information

Monitoring DHCP Server Functions (Cont.)

```
Branch# show ip dhcp conflict
IP address        Detection method   Detection time          VRF
10.1.50.52        Gratuitous ARP     Oct 18 2012 06:56 AM
10.1.50.53        Ping               Oct 18 2012 07:08 AM
```

- Displays the address conflicts that are found by a DHCP server
  - **IP Address:** The IP address of the host as recorded on the DHCP server
  - **Detection Method:** The manner in which the IP address of the hosts were found on the DHCP server; can be a ping or a gratuitous ARP
  - **Detection time:** The time when the conflict was found

DHCP Relay Agent

The need for a centralized DHCP solution:

- Managing individual DHCP servers across many locations is time-consuming.
- Ensuring consistency in several different places can easily lead to errors.

To support a centralized DHCP solution in branch offices, only the DHCP relay agent needs to be configured.