90398 - Tecnologias de Redes de Computadores

Aula 17 – Virtual LANs

Pedro Gonçalves – pasg@ua.pt

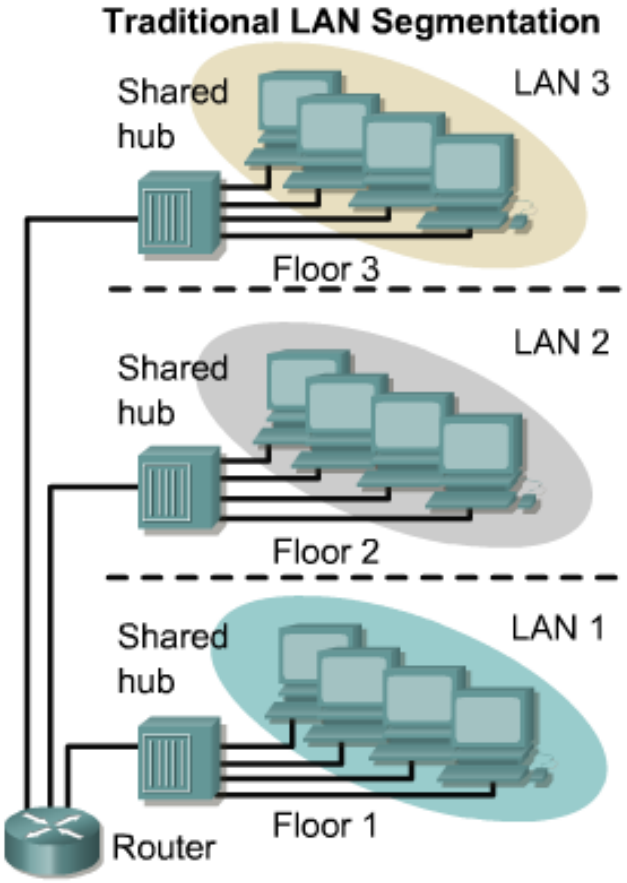
Sumário

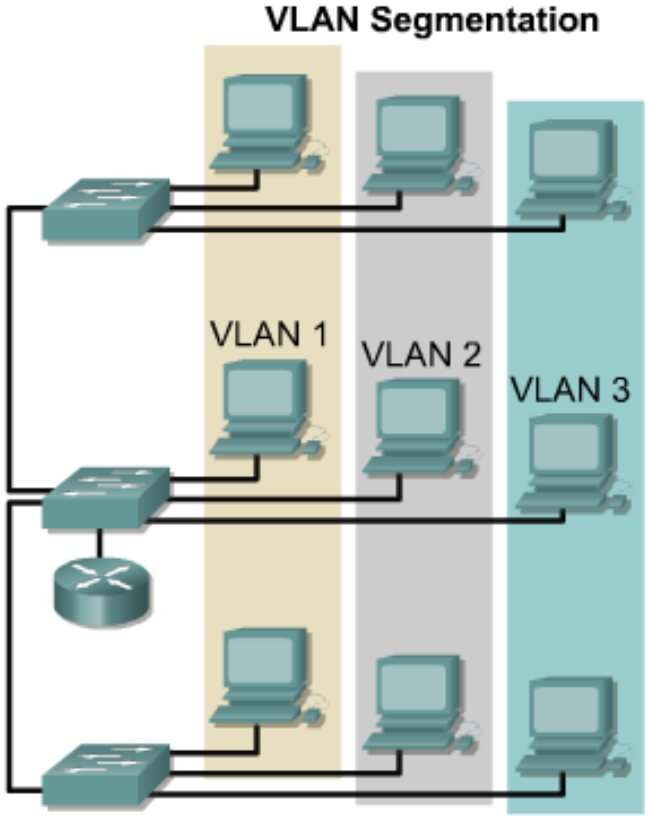
- Virtual LANs
  - Conceito e vantagens
  - VLAN configuration

- VLANs propagation between switchs
  - VTP Protocol

- Encaminhamento de tráfego entre VLANs
  - Routing using na external router
  - Routing using a L3 Switch

VLANs - conceito





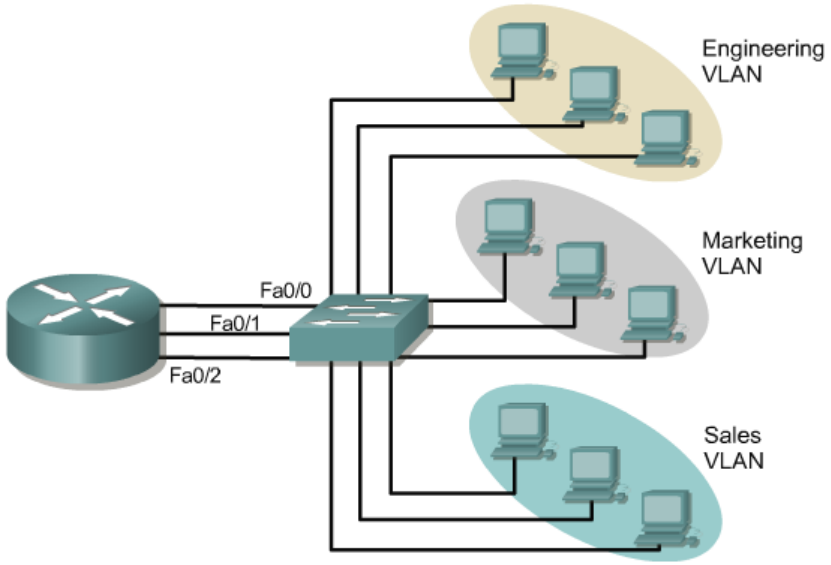
Virtual LANs – VLANs

- Definidas na norma IEEE802.1Q.
- VLAN's são grupos virtuais de estações e de equipamentos de rede.
  - Estações são os "computadores" ligados
- VLAN's são criadas como grupos de departamentos, grupos de trabalho, independentemente da localização física das estações.
  - Uma forma *lógica* de ter diferentes redes em cima da mesma rede *física*
- Estações só comunicam com estações da sua VLAN, tráfego entre VLAN's é limitado:
  - *switches* encaminham só tráfego unicast, multicast e broadcast entre segmentos da mesma VLAN.
- Diz-se que um ou mais switchs criam um **domínio de broadcast**.

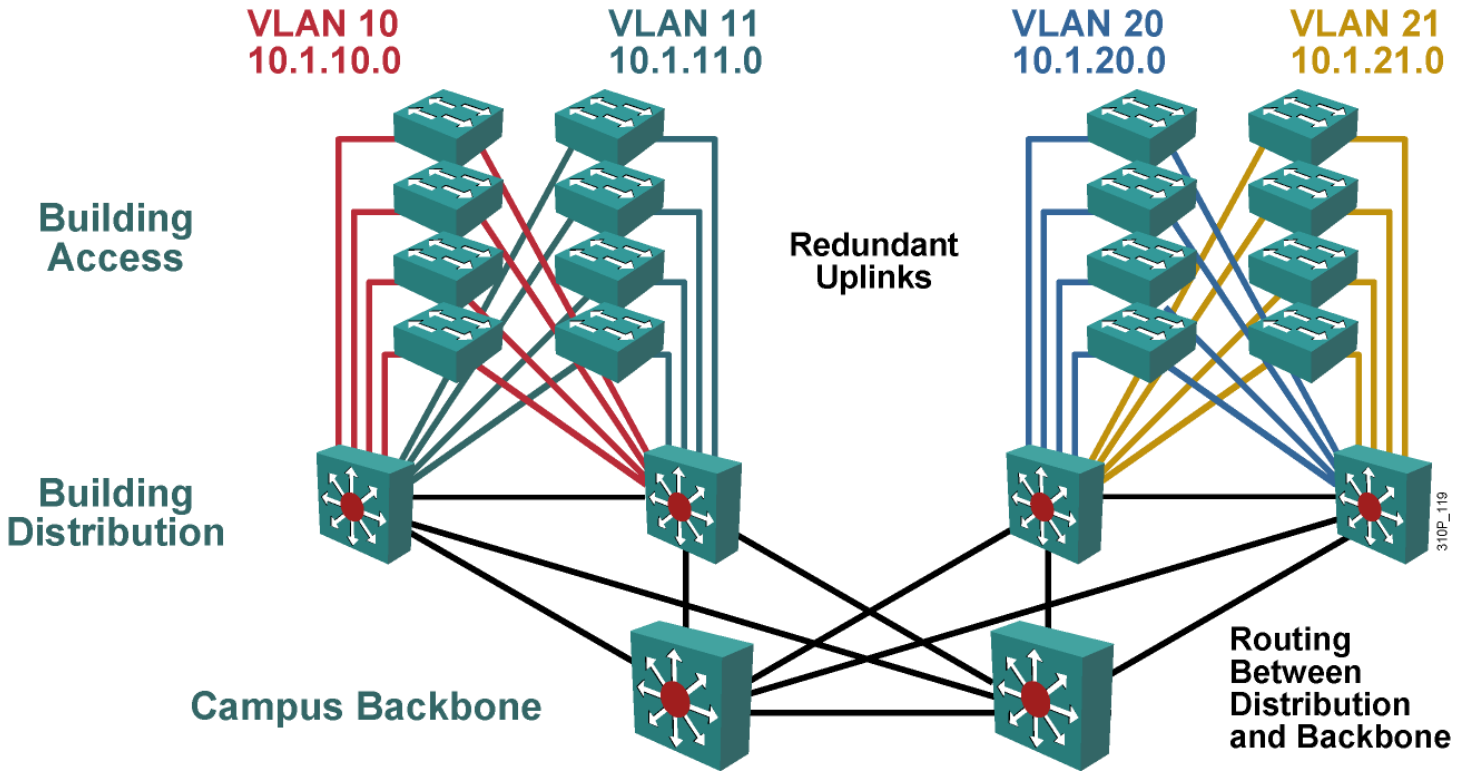
VLAN - funcionamento

- Switch mantém brigding table por cada VLAN.
- Se uma frame vier de uma porta da VLAN1 o switch procura a tabela de bridging da VLAN1.
- Quando um frame é recebido o switch adiciona o endereço de origem à tabela de bridging, se ele ainda não existir.
- O destino é analisado para se tomar decisão de comutação (switching).
- A aprendizagem e o encaminhamento são feitos com base na tabela daquela VLAN.

Tabela que diz os MACs dos PC's ligados a cada porto do switch

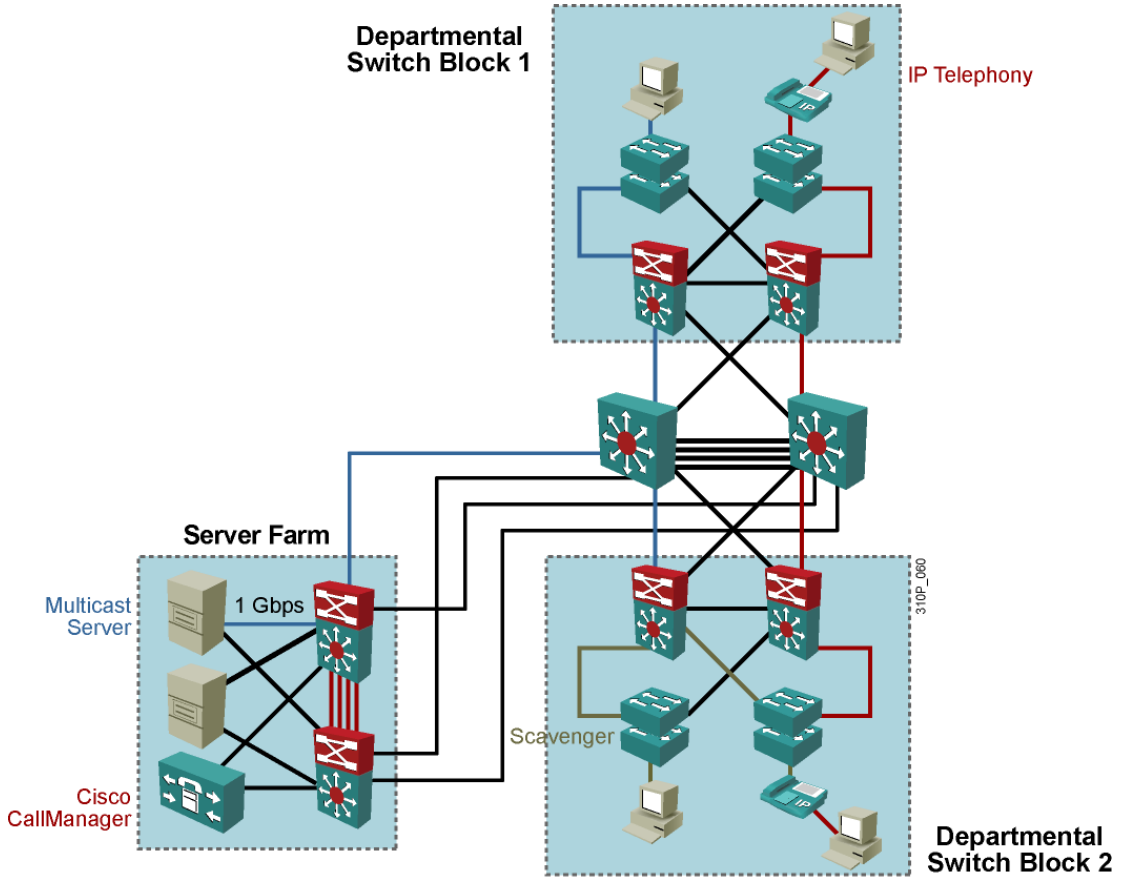


VLANs and the Logical Network



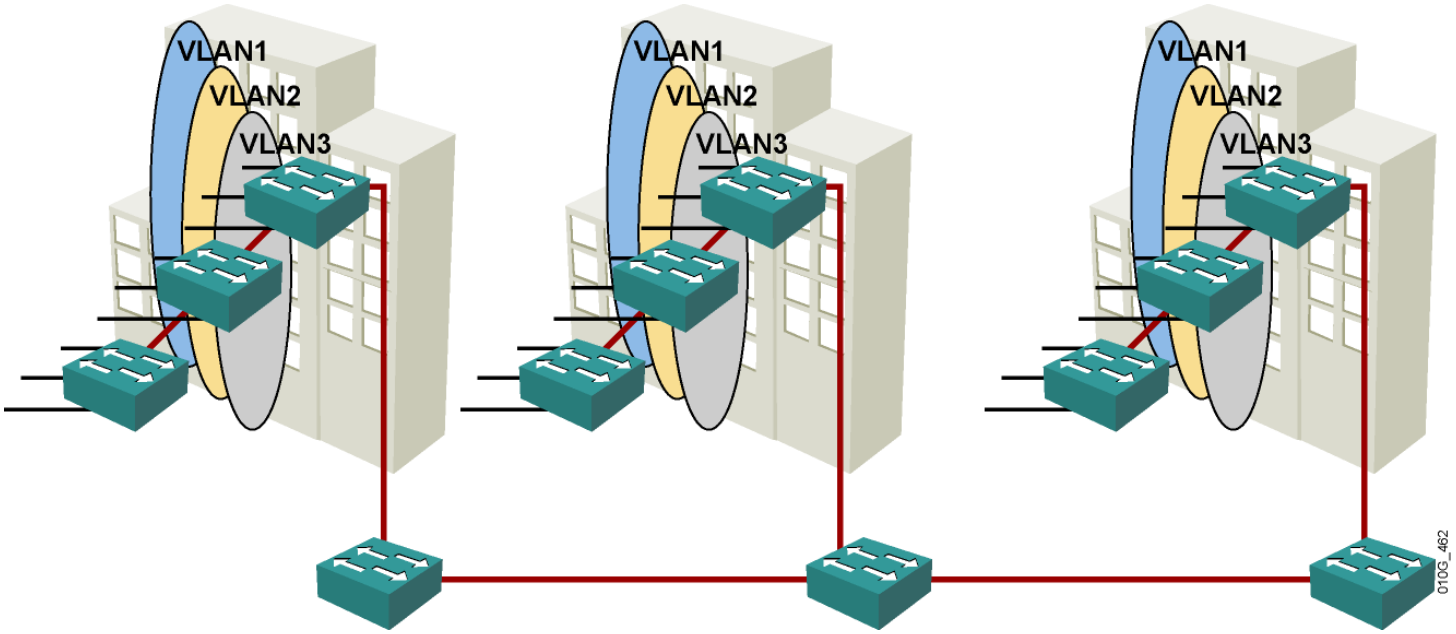
Network Traffic Types

- Traffic types to consider:
  - Network management
  - IP telephony
  - Multicast
  - Normal data
  - Scavenger class



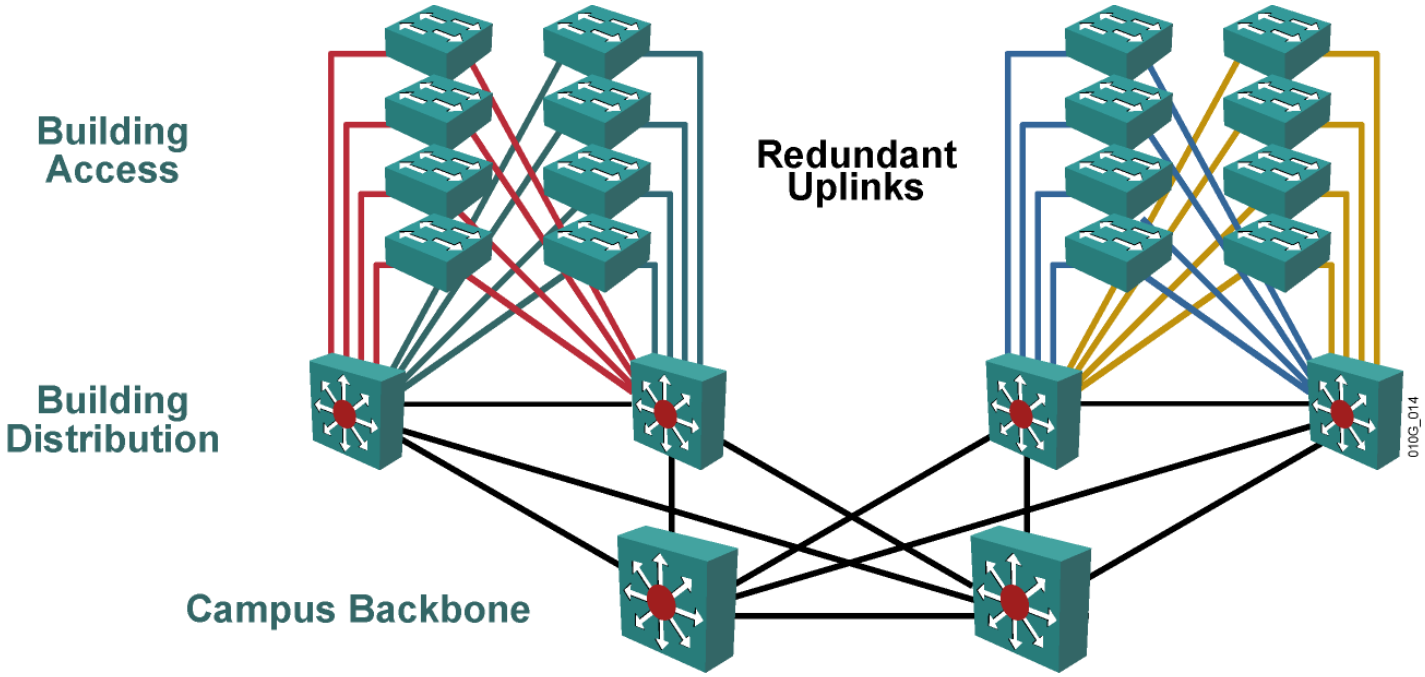
Implementing VLANs

What Is an End-to-End VLAN?



- Users are grouped into VLANs independent of physical location.
- If users are moved within the campus, their VLAN membership remains the same.

What Is a Local VLAN?



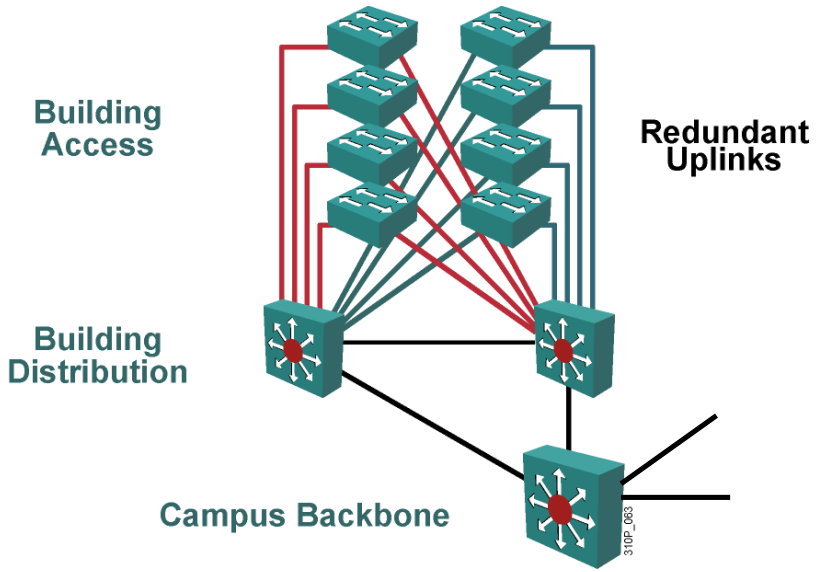
•Local VLANs are generally confined to a wiring closet.

Benefits of Local VLANs in the ECNM

- Deterministic traffic flow
- Active redundant paths

- High availability
- Finite failure domain

- Scalable design



VLAN Configuration Modes

- Global Mode

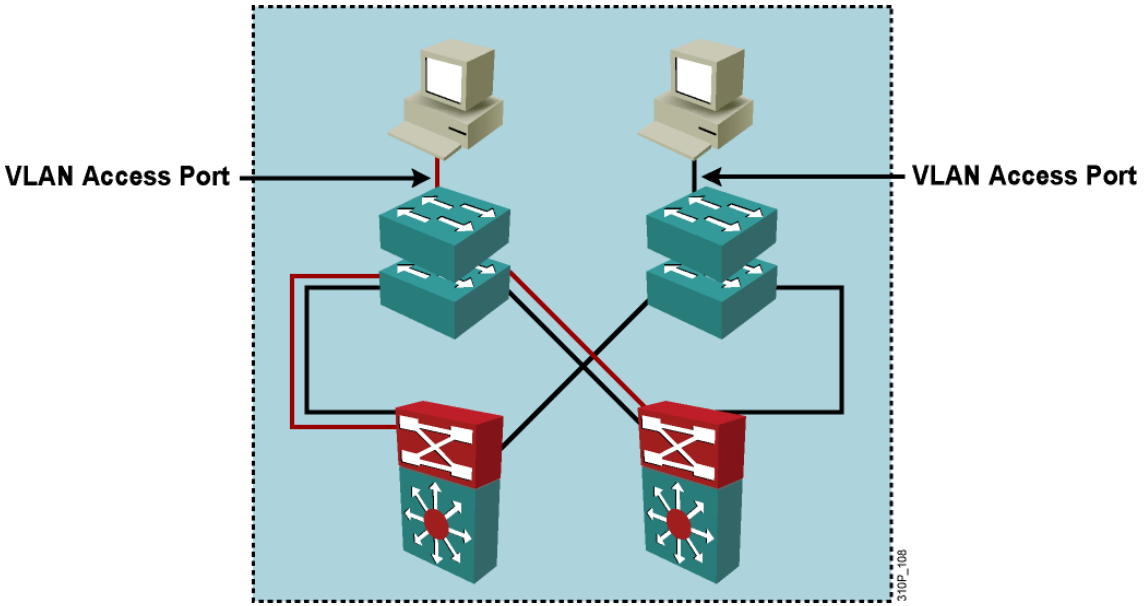
```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# name Vlan3
Switch(config-vlan)# exit
Switch(config)# end
```

VLAN Configuration Modes

- Database Mode

```
Switch# vlan database
Switch(vlan)# vlan 3

VLAN 3 added:
    Name: VLAN0003
Switch(vlan)# exit
APPLY completed.
Exiting....
```

VLAN Access Ports



The access switch port associated with a single data VLAN

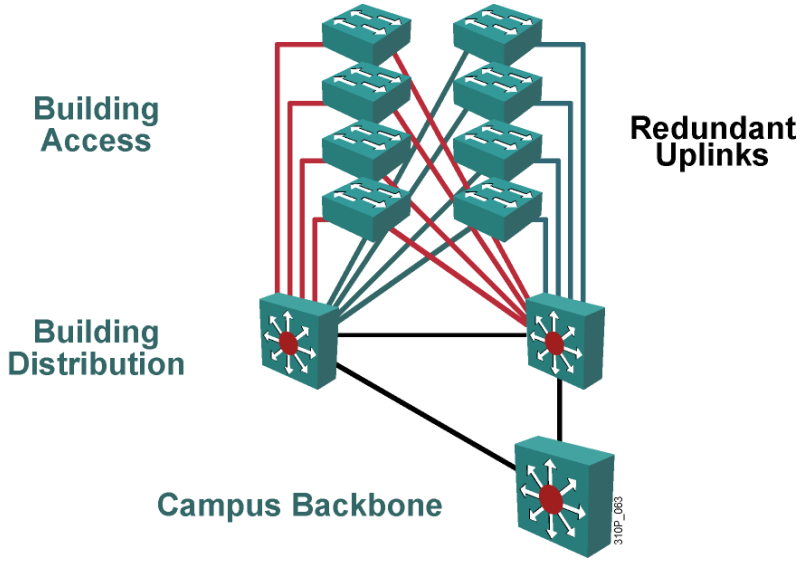
VLAN Implementation Commands

- Configuring VLANs
  - vlan 101
  - switchport mode access
  - switchport access vlan 101

- Verifying VLANs
  - show interfaces
  - show vlan

How to Implement a VLAN

- Create or configure a VLAN.
- Verify VLAN configuration.
- Associate switch ports with the VLAN.
- Verify switch port configuration.
- Test VLAN connectivity.
- Implement VLAN and switch security.



Configuring an Access VLAN

```
Switch(config)# vlan vlan_id
```

Create a VLAN.

```
Switch(config-vlan)# name vlan_name
```

Provide a VLAN name.

```
Switch(config-if)# switchport mode access
```

Place the switch port into access mode.

```
Switch(config-if)# switchport access vlan vlan_id
```

Associate the access switch port with a VLAN.

Verifying the Access VLAN Configuration

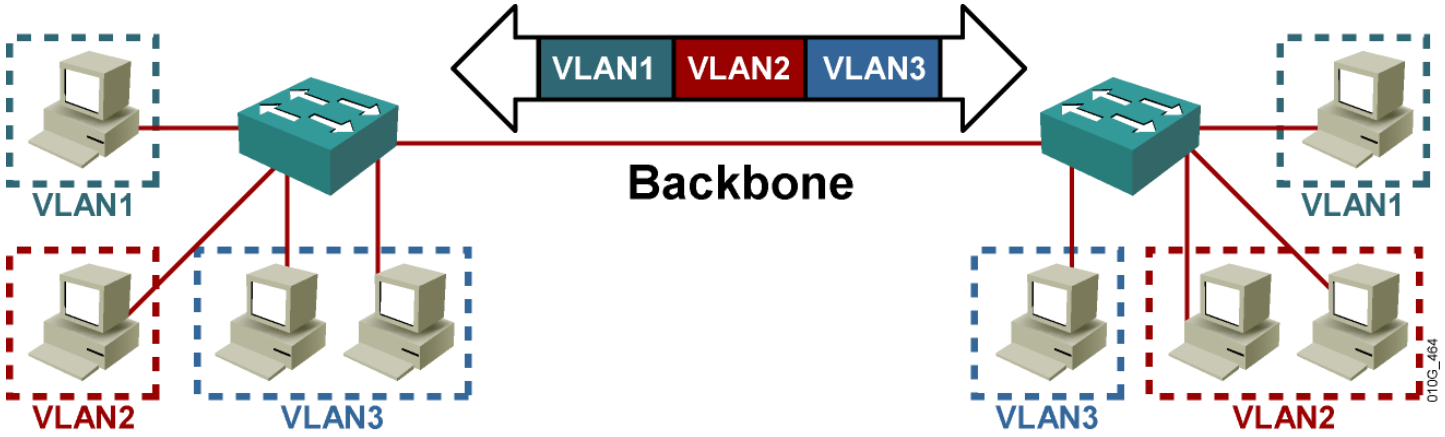
```
Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                    Fa0/5, Fa0/7, Fa0/9
11   asw11_data                          active
12   asw12_data                          active
95   VLAN0095                            active    Fa0/8
99   Trunk_Native                        active
100  Internal_Access                     active
111  voice-for-group-11                  active
112  voice-for-group-12                  active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
----- ---------- ----- ------ ------ -------- ---- -------- ------
1    enet  100001     1500  -      -      -        -    -        0
11enet  100011     1500  -      -      -        -    -        0
. . . . .
. . . .
. . .
```

Summary

- An end-to-end VLAN is geographically dispersed throughout the network.
- Local VLANs should be created with physical boundaries in mind.
- VLANs solve issues that arise in a Layer 2 switched network.
- VLANs can be configured globally or in VLAN database mode.
- An access switch port is associated with one VLAN.
- Cisco provides a series of commands to configure a VLAN and verify configuration on an access switch.
- A series of ordered steps should be followed to implement a VLAN.

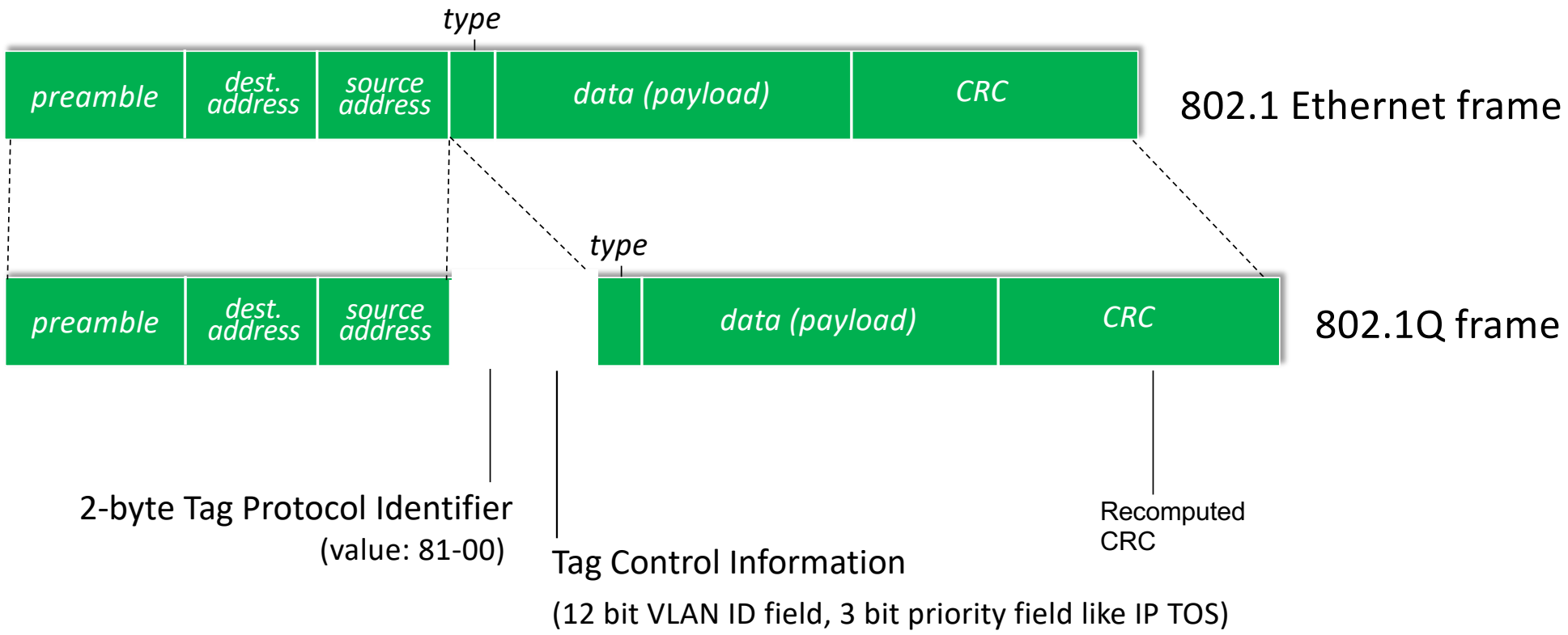
Propagação de VLANs

Maintaining Specific VLAN Identification

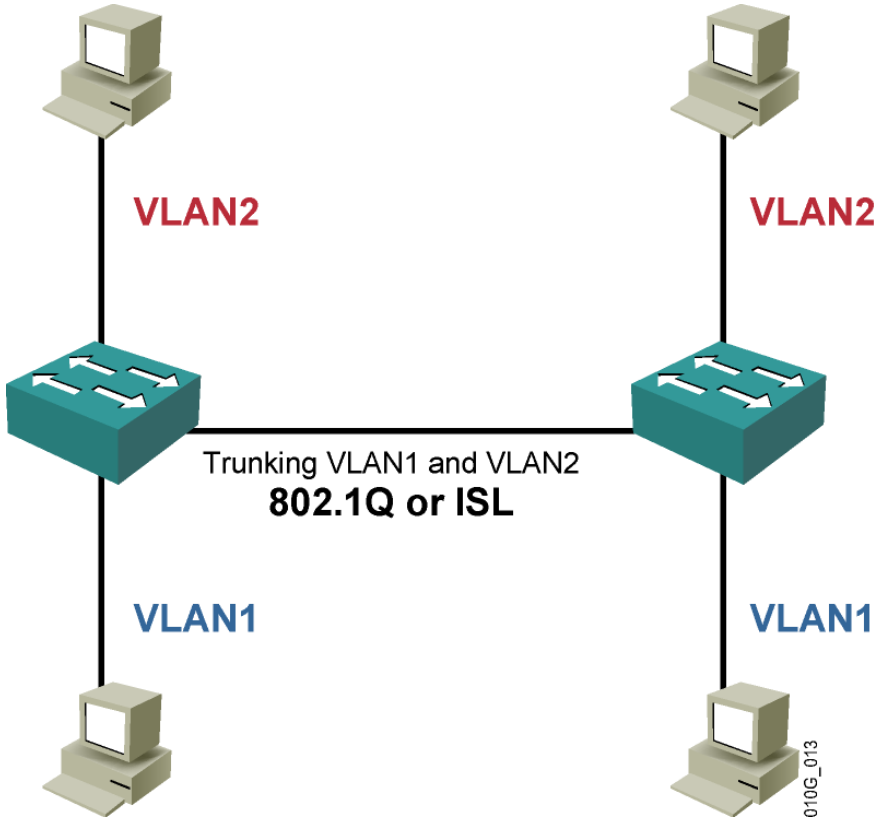


- **Specifically developed for multi-VLAN interswitch communications**
- **Places a unique identifier in each frame**
- **Functions at Layer 2**

802.1Q VLAN frame format



VLAN Trunking

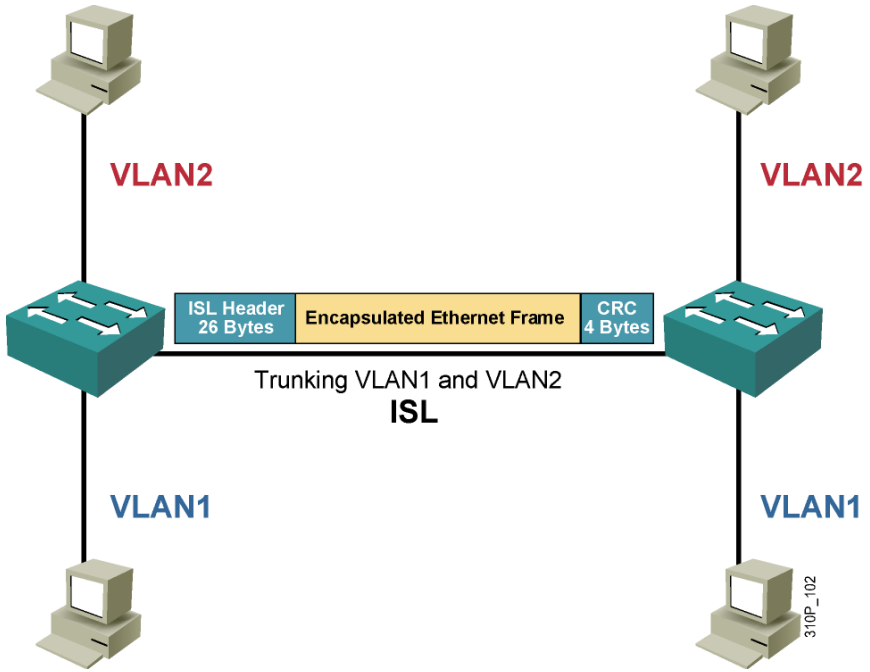


Comparing ISL and 802.1Q

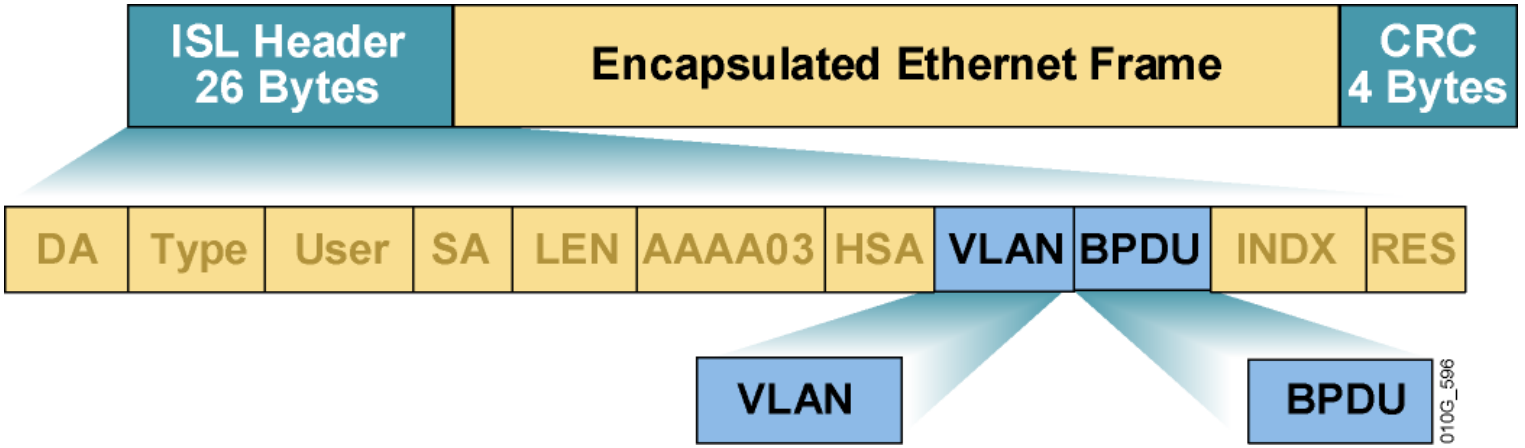
ISL	802.1Q
Proprietary	Nonproprietary
Encapsulated	Tagged
Protocol independent	Protocol dependent
Encapsulates the old frame in a new frame	Adds a field to the frame header

Trunking with ISL

- Is a Cisco proprietary protocol
- Supports PVST
- Uses an encapsulation process
- Does not modify the original frame

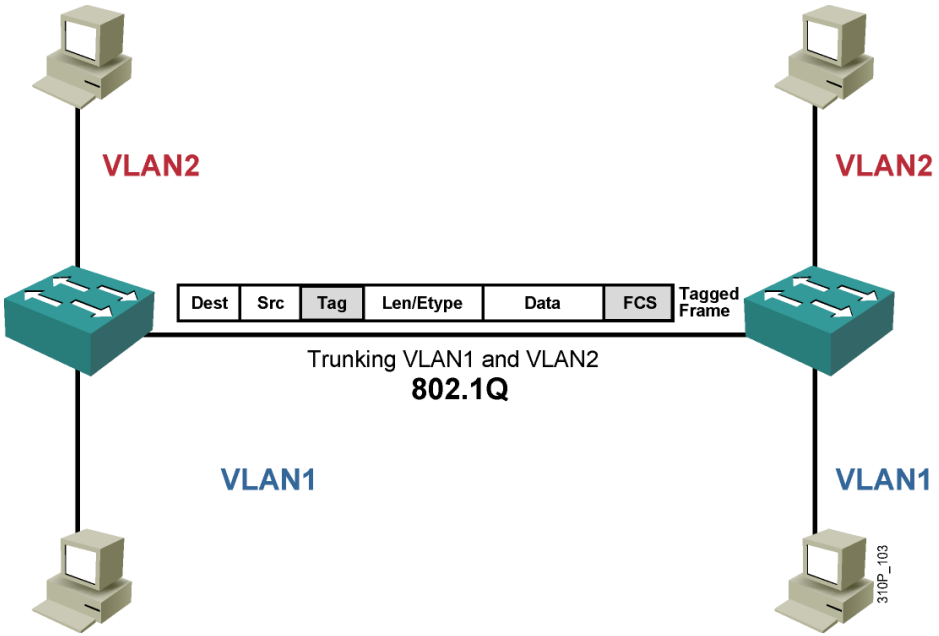


ISL Encapsulation

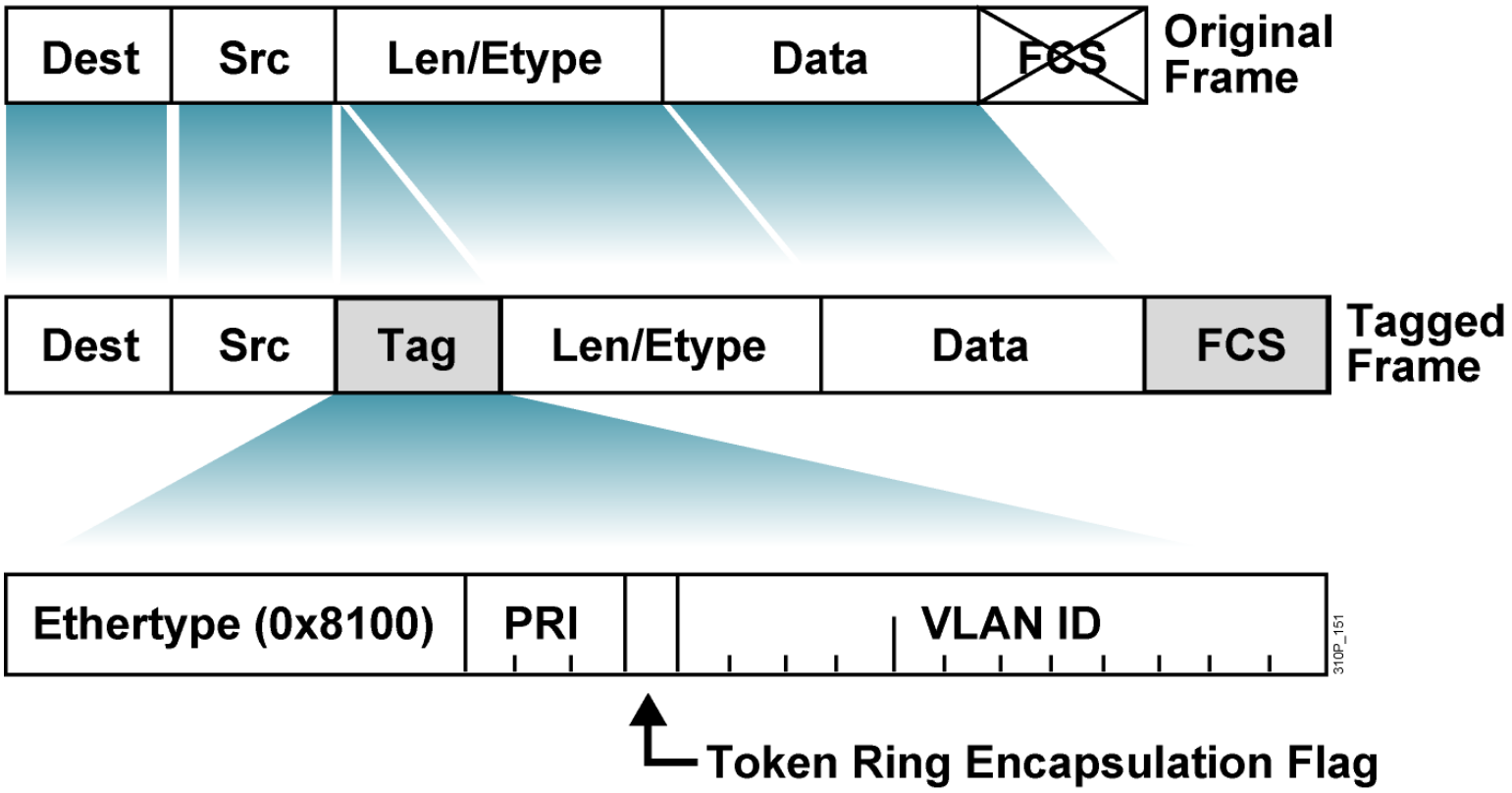


Trunking with 802.1Q

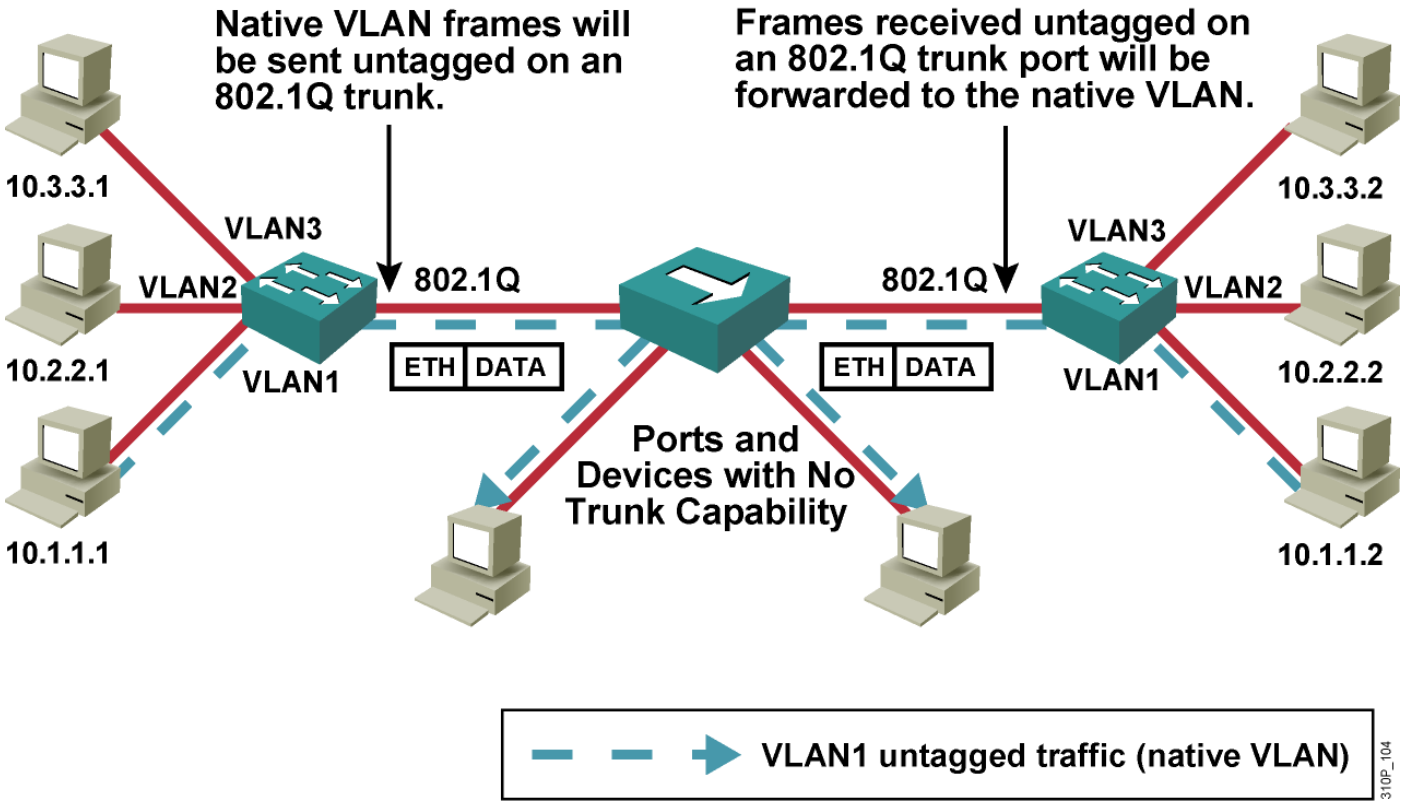
- An IEEE standard
- Adds a 4-byte tag to the original frame
- Additional tag includes a priority field
- Does not tag frames that belong to the native VLAN
- Supports Cisco IP telephony



The 802.1Q Tagging Process



802.1Q Native VLAN

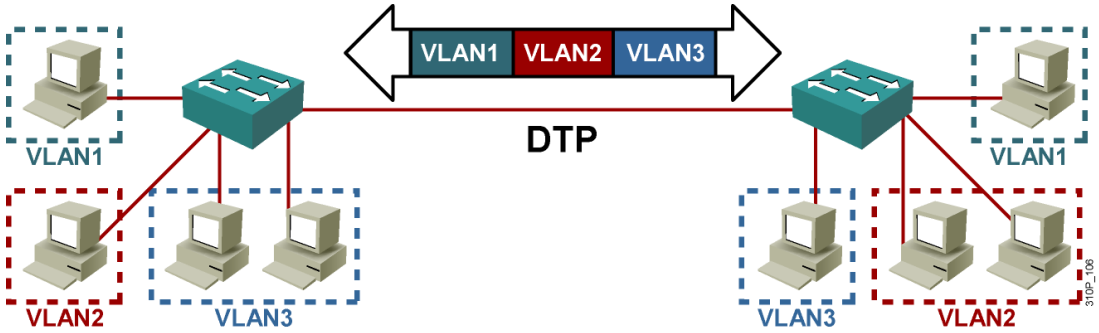


Native VLAN frames are carried over the trunk link untagged.

VLAN Ranges

VLAN Range	Use
0, 4095	Reserved for system use only
1	Cisco default
2–1001	For Ethernet VLANs
1002–1005	Cisco defaults for FDDI and Token Ring
1006–4094	Ethernet VLANs only, unusable on specific legacy platforms

Trunking Configuration Commands



- **Trunks can be configured statically or via DTP.**
- **DTP provides the ability to negotiate the trunking method.**

•Configuring a Trunk

- switchport trunk
- switchport mode
- switchport nonegotiate

Switchport Mode Interactions

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	**Access**	**Trunk**	**Trunk**	**Access**
Dynamic Desirable	**Trunk**	**Trunk**	**Trunk**	**Access**
Trunk	**Trunk**	**Trunk**	**Trunk**	**Not recommended**
Access	**Access**	**Access**	**Not recommended**	**Access**

Note: Table assumes DTP is enabled at both ends.

- show dtp interface – **to determine current setting**

How to Configure Trunking

1. Enter interface configuration mode.
2. Shut down interface.
3. Select the encapsulation (802.1Q or ISL).
4. Configure the interface as a Layer 2 trunk.
5. Specify the trunking native VLAN (for 802.1Q).
6. Configure the allowable VLANs for this trunk.
7. Use the no shutdown command on the interface to activate the trunking process.
8. Verify the trunk configuration.

802.1Q Trunk Configuration

```
Switch(config)#interface fastethernet 5/8
Switch(config-if)#shutdown
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 1,5,11,1002-1005
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 99
Switch(config-if)#switchport nonegotiate
Switch(config-if)#no shutdown
```

Verifying the 802.1Q Configuration

```
Switch#show running-config interface {fastethernet |
gigabitethernet} slot/port
```

```
Switch#show interfaces [fastethernet | gigabitethernet] slot/port
[ switchport | trunk ]
```

```
Switch#show interfaces fastEthernet 5/8 switchport
Name: fa5/8
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (trunk_only)
Trunking VLANs Enabled: 1,5,11,1002-1005
Pruning VLANs Enabled: 2-1001
. . .
```

Verifying a 802.1Q Dynamic Trunk Link

```
Switch#show running-config interface fastethernet 5/8
Building configuration...
Current configuration:
!
interface FastEthernet5/8
 switchport mode dynamic desirable
 switchport trunk encapsulation dot1q

Switch#show interfaces fastethernet 5/8 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa5/8     desirable    802.1q         trunking      99

Port      Vlans allowed on trunk
Fa5/8     1,5,11,1002-1005

Port      Vlans allowed and active in management domain
Fa5/8     1,5,1002-1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa5/8     1,5,1002-1005
```

ISL Trunk Configuration

```
Switch(config)#interface fastethernet 2/1
Switch(config-if)#shutdown
Switch(config-if)#switchport trunk encapsulation isl
Switch(config-if)#switchport trunk allowed vlan 1-5,1002-1005
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport nonegotiate
Switch(config-if)#no shutdown
```

Verifying ISL Trunking

```
Switch#show running-config interface {fastethernet | gigabitethernet}
slot/port
```

```
Switch#show interfaces [fastethernet | gigabitethernet] slot/port [
switchport | trunk ]
```

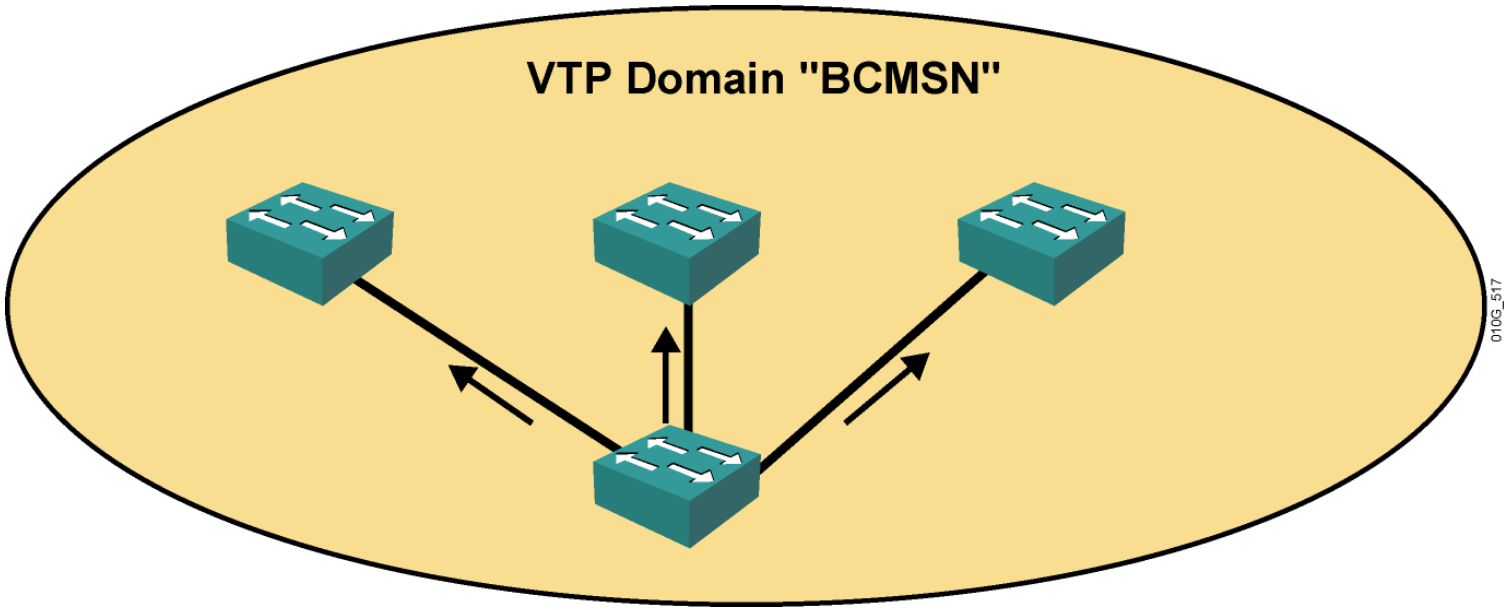
```
Switch#show interfaces fastethernet 2/1 trunk

     Port        Mode         Encapsulation  Status        Native VLAN
     Fa2/1       trunk        isl            trunking      99

     Port        VLANs allowed on trunk
     Fa2/1       1-5,1002-1005

     Port        VLANs allowed and active in management domain
     Fa2/1       1-2,1002-1005

     Port        VLANs in spanning tree forwarding state and not pruned
     Fa2/1       1-2,1002-1005
```

Summary

- Trunk links carry traffic from multiple VLANs.
- ISL is Cisco proprietary and encapsulates the Layer 2 frames.
- 802.1Q is an IEEE standard for trunking, which implements a 4-byte tag.
- The 802.1Q native VLANs forward frames without the tag.
- VLAN numbers have specific ranges and purposes.
- Various commands are used to configure and verify ISL and 802.1Q trunk links.
- Allow only required VLANs over the trunk.

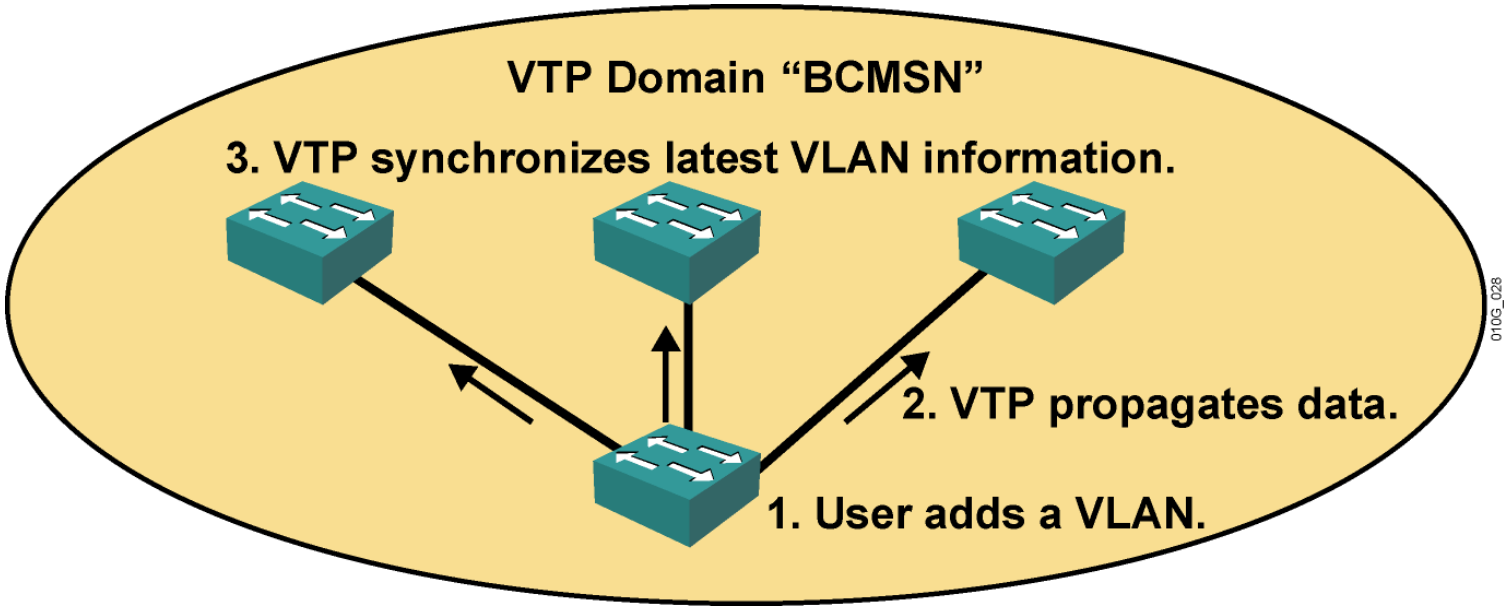
Propagação de VLANs com VTP

The VTP Domain



- **Group of switches that exchange VLAN information**
- **VLANs administered centrally at a chosen switch**

The VTP Protocol

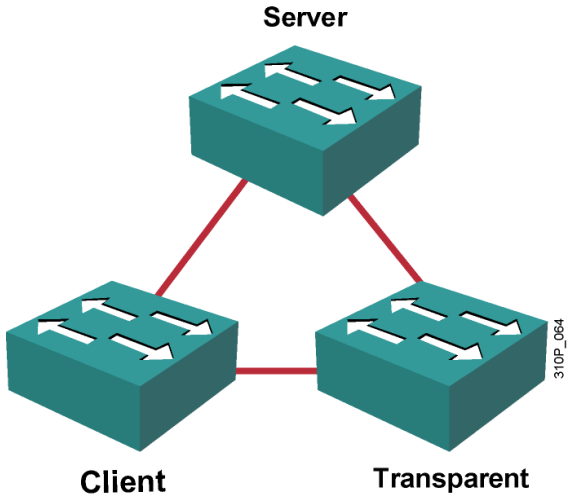


- Advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- Sends advertisements on trunk ports only

VTP Modes

Server (default mode)

- Creates, modifies, and deletes VLANs
- Sends and forwards advertisements
- Synchronizes VLAN configurations
- Saves configuration in NVRAM



Client

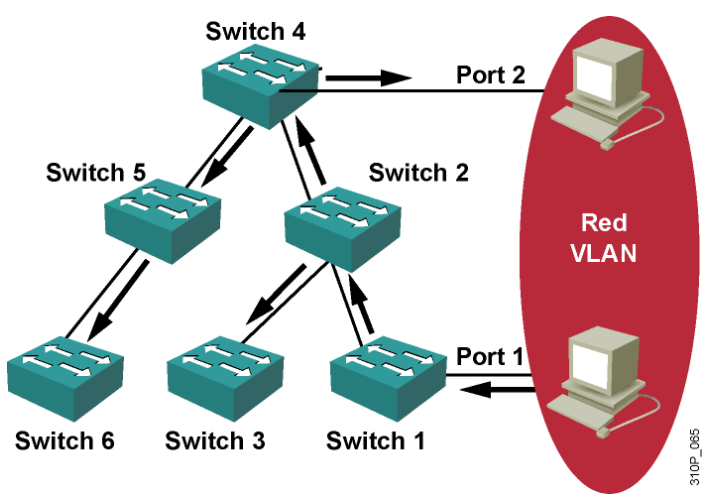
- Cannot create, change, or delete VLANs
- Forwards advertisements
- Synchronizes VLAN configurations
- Does not save in NVRAM

Transparent

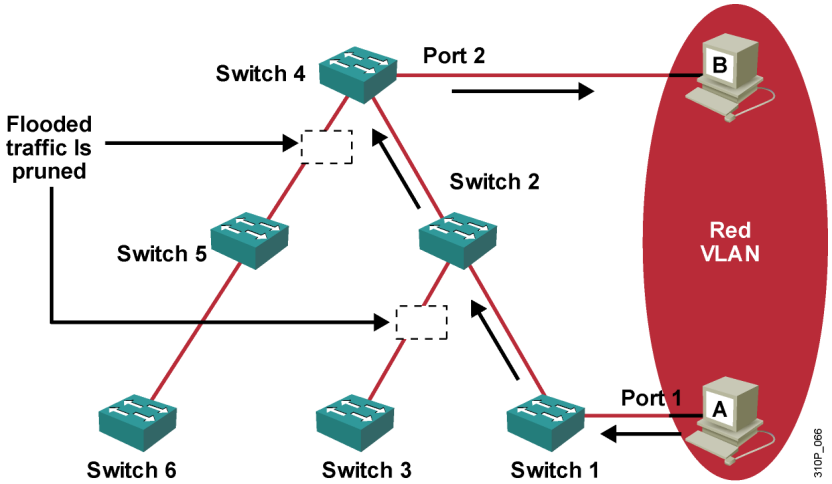
- Creates, modifies, and deletes local VLANs
- Forwards advertisements
- Does not synchronize VLAN configurations
- Saves configuration in NVRAM

VTP Pruning

- Uses bandwidth more efficiently by reducing unnecessary flooded traffic
- Example: Station A sends broadcast; broadcast flooded only toward any switch with ports assigned to the red VLAN



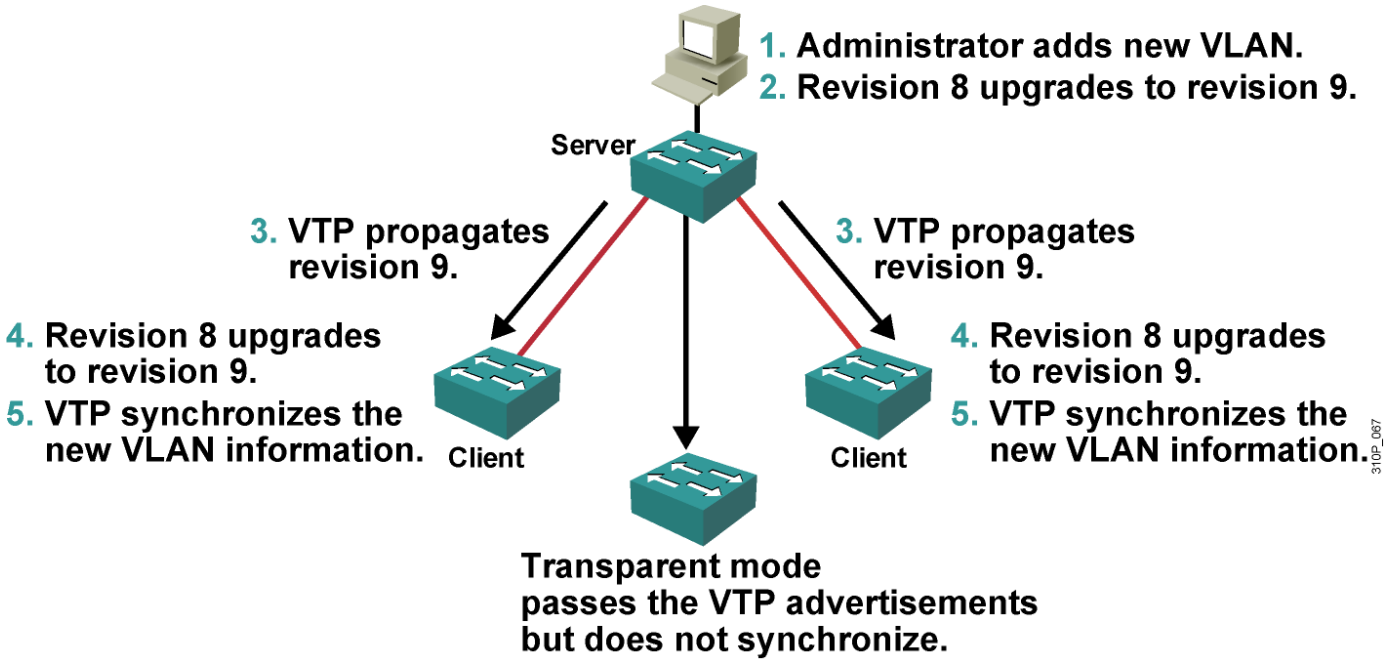
Pruning Disabled



Pruning Enabled

VTP Operation

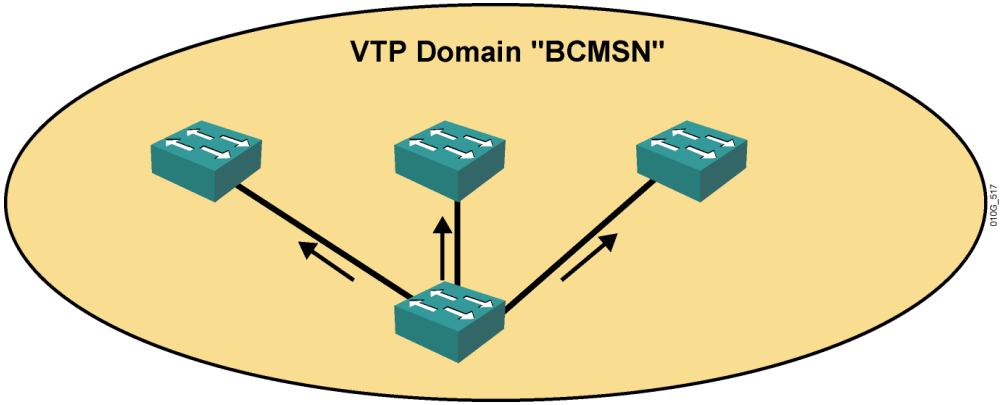
- **VTP advertisements are sent as multicast frames.**
- **VTP servers and clients are synchronized to the latest revision number.**
- **VTP advertisements are sent every 5 minutes or when there is a change.**



VTP Configuration Commands

- Configuring VTP
  - vtp domain
  - vtp mode
  - vtp password

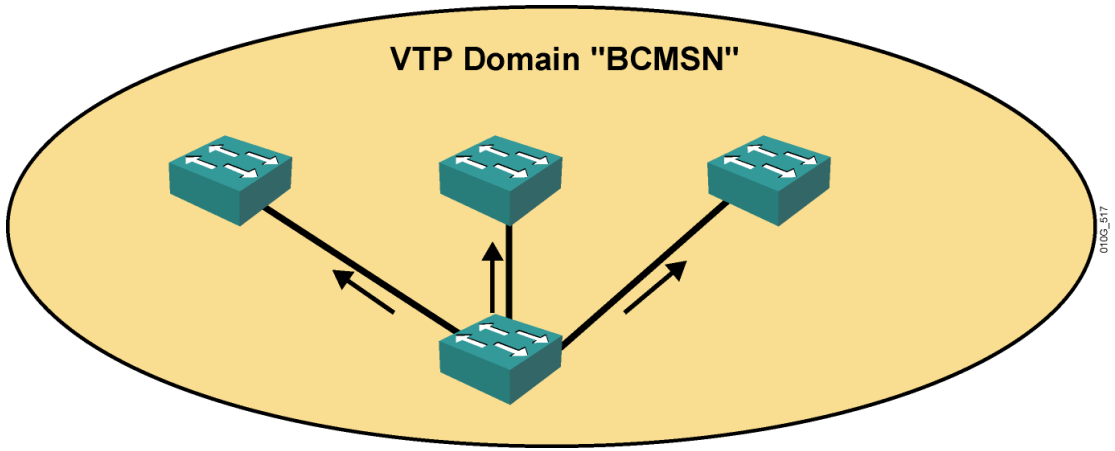
- Verifying VTP
  - show vtp status
  - show vtp counters



Configuring a VTP Management Domain

•Configure each switch in the following order to avoid dynamic learning of the domain name:

- VTP password
- VTP domain name (case sensitive)
- VTP mode (server mode is the default)



Configuring and Verifying VTP

```
Switch#show vlan brief
```

- Displays a list of current VLANs

```
Switch(config)#vtp password password_string
```

- Sets the VTP password

```
Switch(config)#vtp domain domain_name
```

- Sets the VTP domain name

```
Switch(config)#vtp mode
```

- Sets the VTP mode to server, client, or transparent

```
Switch# show vtp status
```

- Displays the current settings for VTP

Verifying the VTP Configuration

```
Switch#show vtp status
```

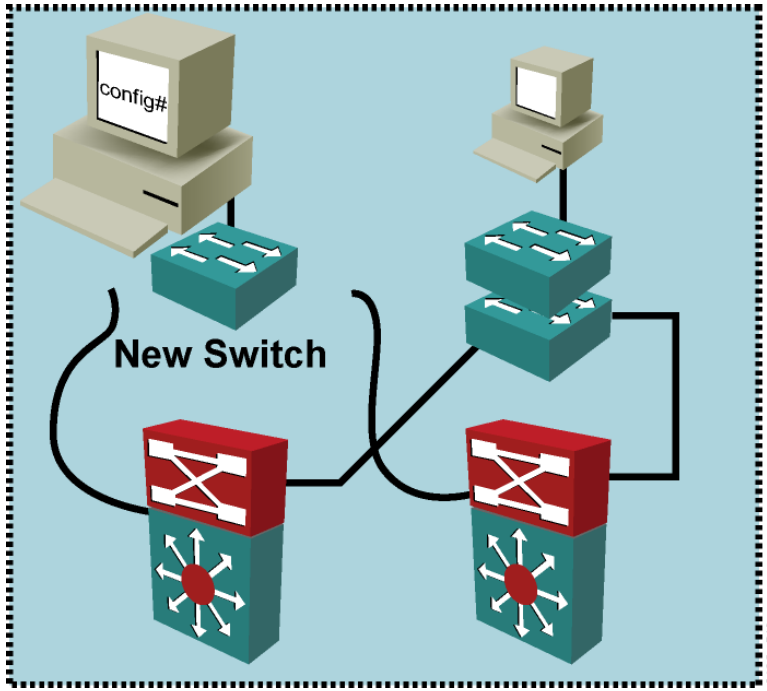
```
Switch#show vtp status

VTP Version                     : 2
Configuration Revision          : 28
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 17
VTP Operating Mode              : Client
VTP Domain Name                 : BCMSN
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49
0x80
Configuration last modified by 10.1.1.1 at 8-12-05 15:04:49
Switch#
```

Verifying the VTP Configuration (Cont.)

```
Switch#show vtp counters
```

```
Switch#show vtp counters

VTP statistics:
Summary advertisements received    : 7
Subset advertisements received     : 5
Request advertisements received    : 0
Summary advertisements transmitted : 997
Subset advertisements transmitted  : 13
Request advertisements transmitted : 3
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:
Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa5/8               43071            42766            5
```

Adding a Switch to an Existing VTP Domain



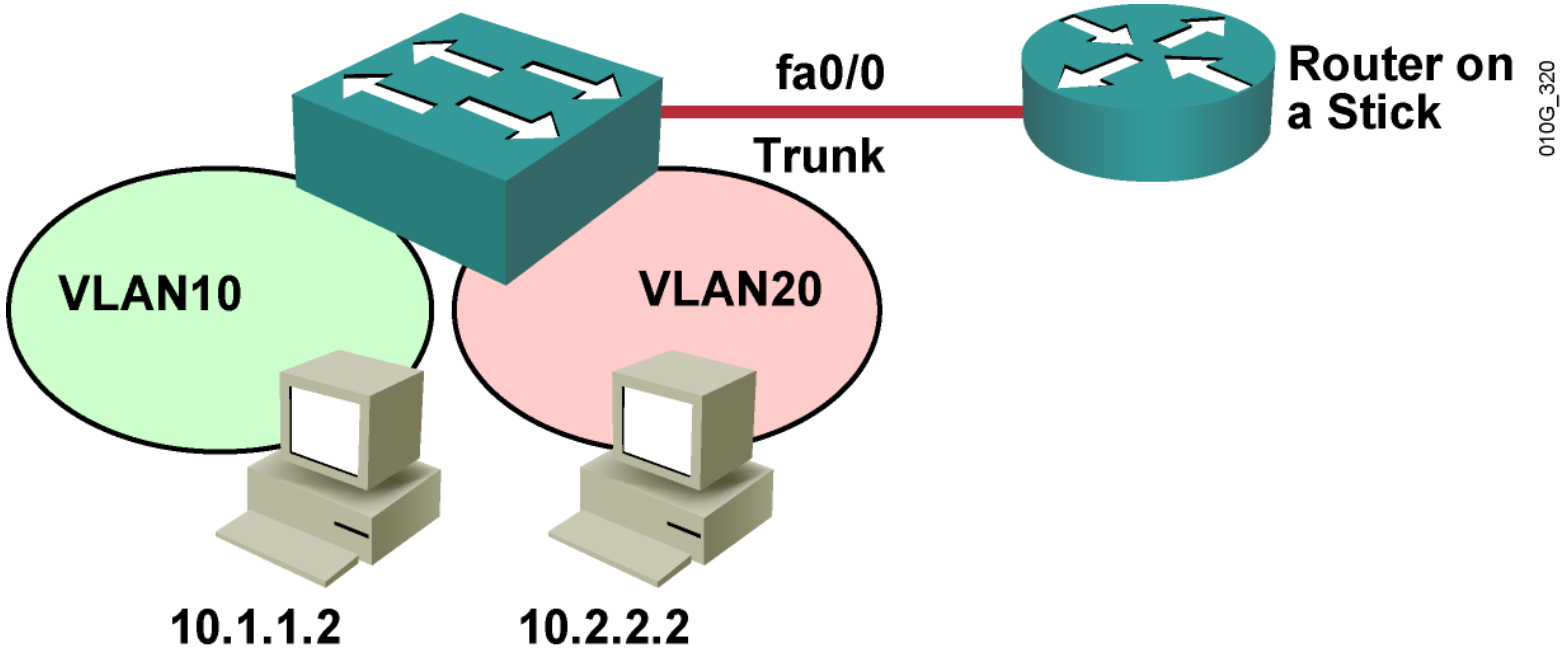
Ensure a new switch has VTP revision 0 before adding it to a network.

Summary

- Switches in a VTP domain share VLAN information.
- VTP advertises VLAN information.
- VTP operates in one of three modes: server, client, or transparent.
- VTP Pruning uses available bandwidth more efficiently.
- VTP uses a specific process to distribute and synchronize VLAN information between switches.
- Various commands are used to configure and verify VTP operation on a switch.
- VTP commands should be applied in a particular order.
- Specific steps should be followed when adding a new switch to an existing VTP domain.

Comutação de VLANs

Inter-VLAN Routing with External Router

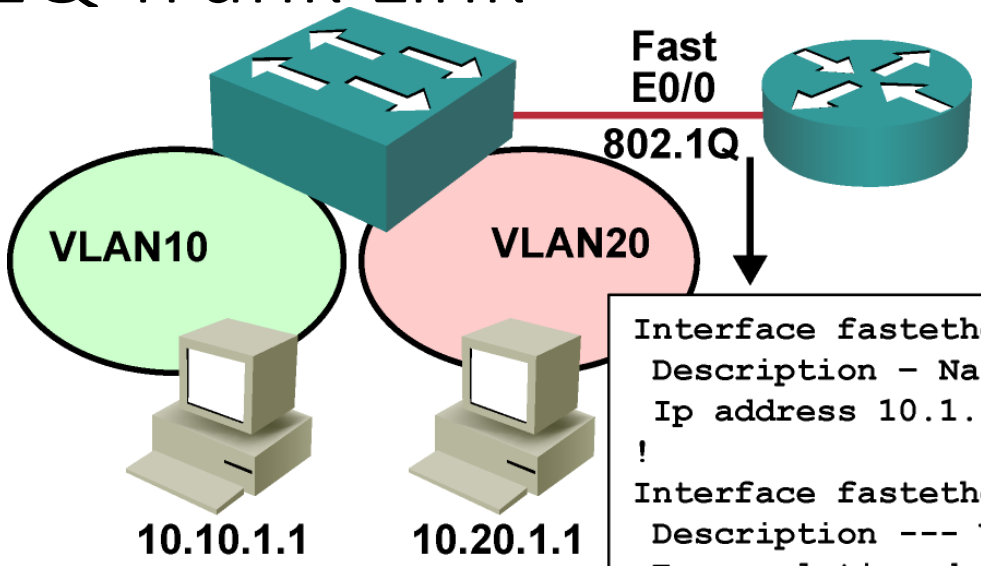


- **Single trunk link carries traffic for multiple VLANs to and from router.**

Inter-VLAN Routing
External Router Configuration Commands

- Configure on subinterface
  - encapsulation dot1Q (or isl) 10
  - ip address 10.10.1.1 255.255.255.0
- Verify
  - show vlan 10
  - show ip route

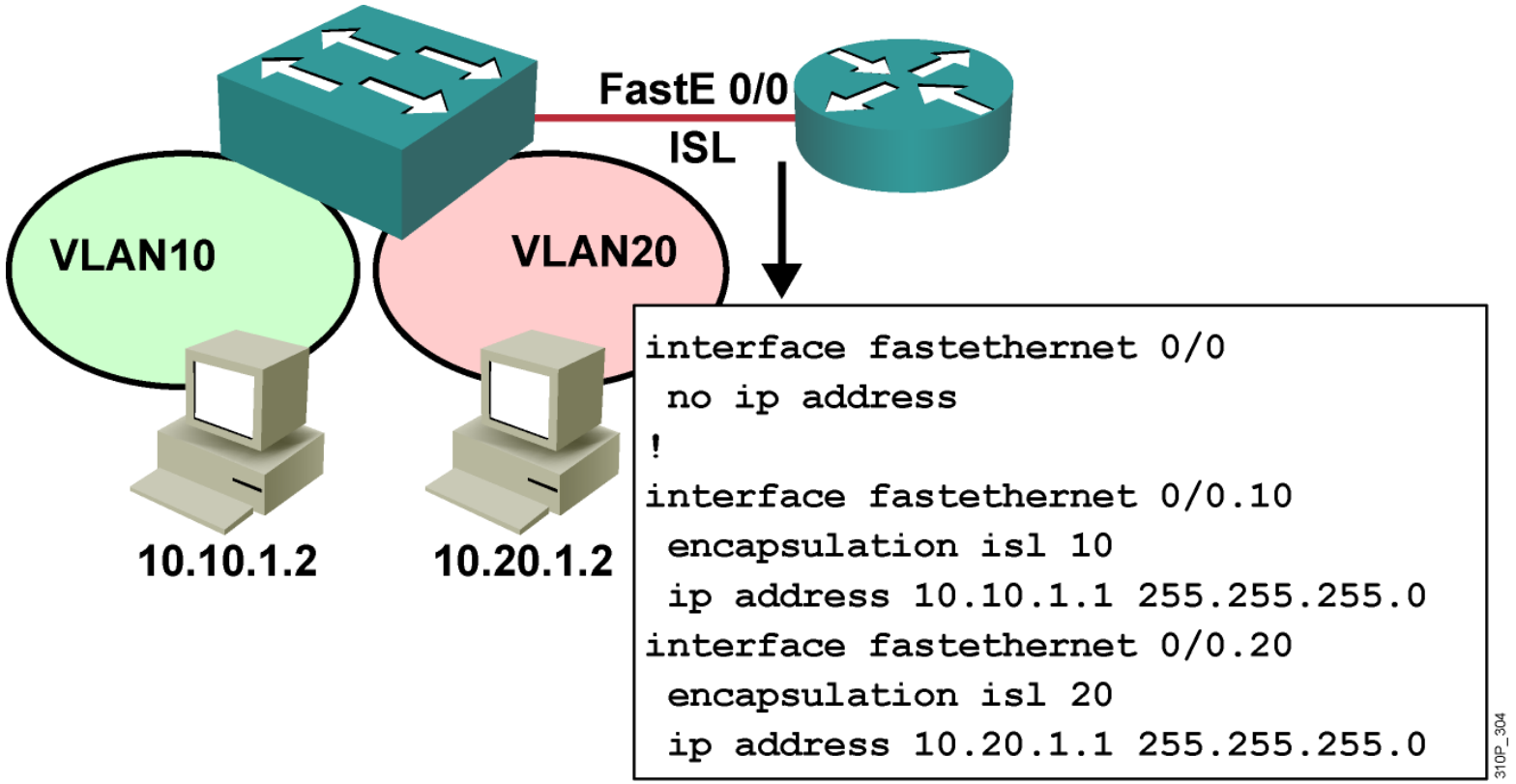
Inter-VLAN Routing on External Router: 802.1Q Trunk Link



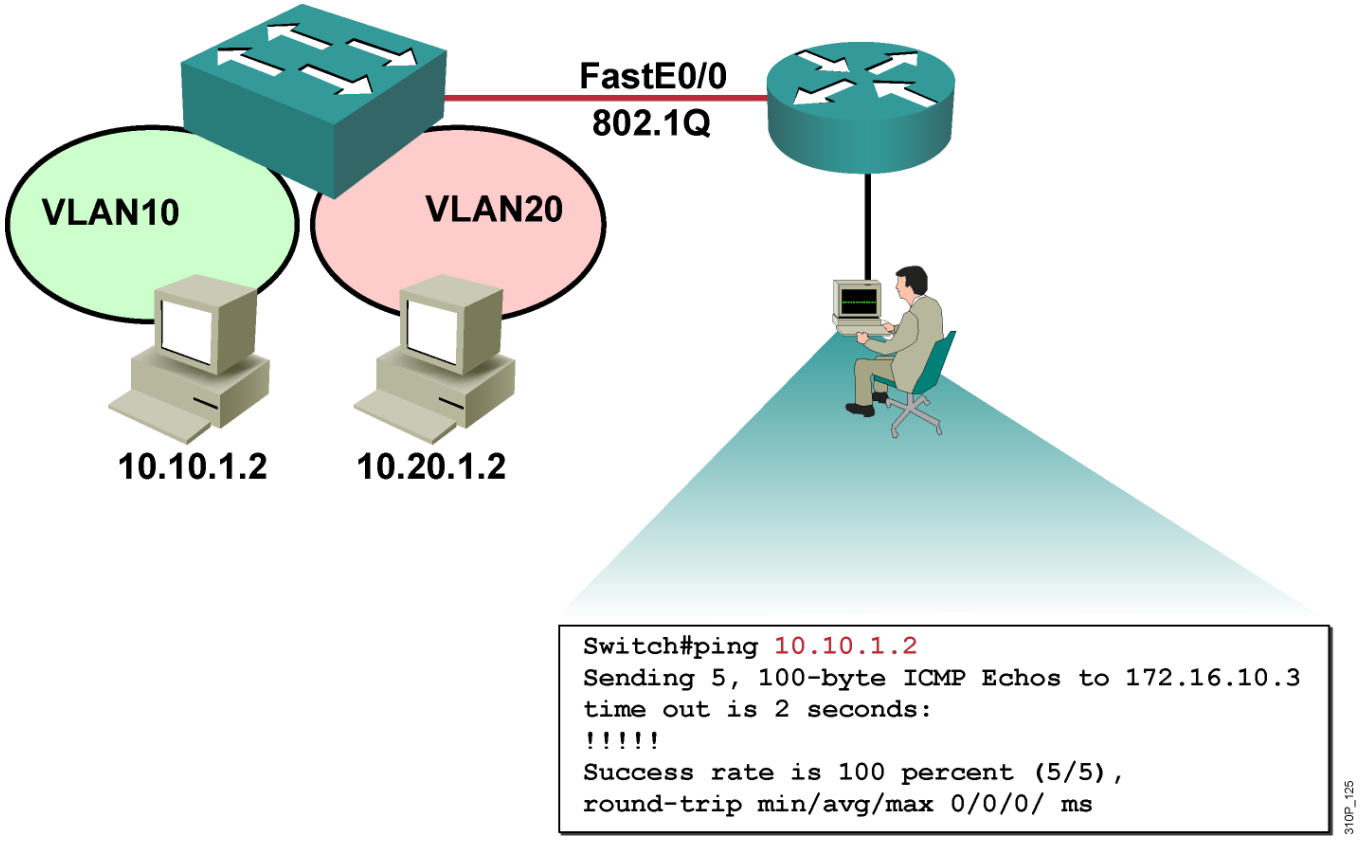

```
Interface fastethernet 0/0
 Description – Native 802.1q VLAN –
 Ip address 10.1.1.1 255.255.255.0
!
Interface fastethernet 0/0:10
 Description --- VLAN 10 w/ 802.1q ---
 Encapsulation dot1q 10
 Ip address 10.10.1.1 255.255.255.0
!
Interface fastethernet 0/0:20
 Description --- VLAN 20 w/ 802.1q ---
 Encapsulation dot1q 20
 Ip address 10.20.1.1 255.255.255.0
```

310P_158

Inter-VLAN Routing on External Router: ISL Trunk Link



Verifying Inter-VLAN Routing



The ping **command tests connectivity to remote hosts.**

Verifying the Inter-VLAN Routing Configuration

```
Router#show vlan
```

- **Displays the current IP configuration per VLAN**

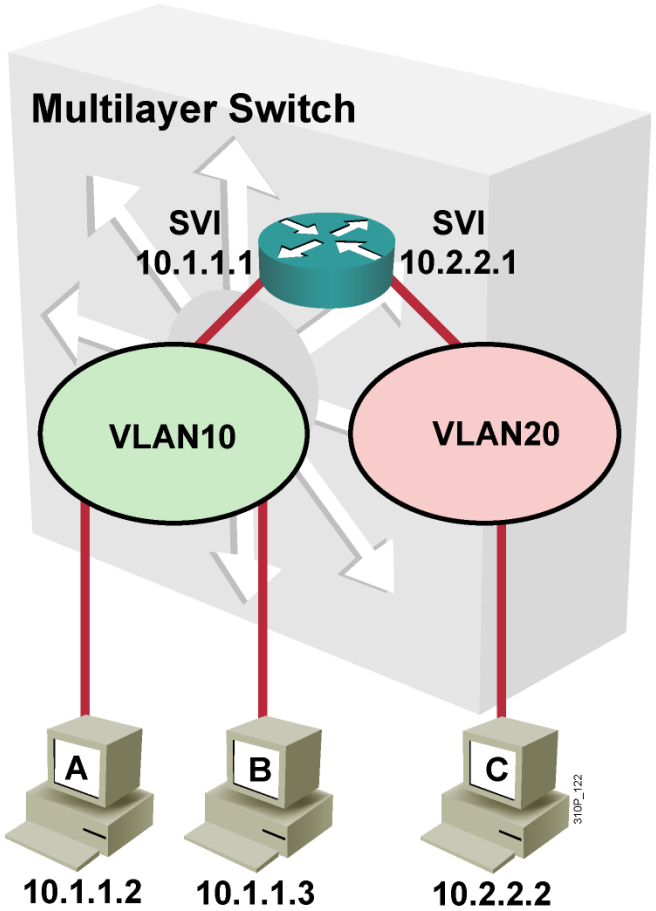
```
Router#show ip route
```

Displays IP route table information

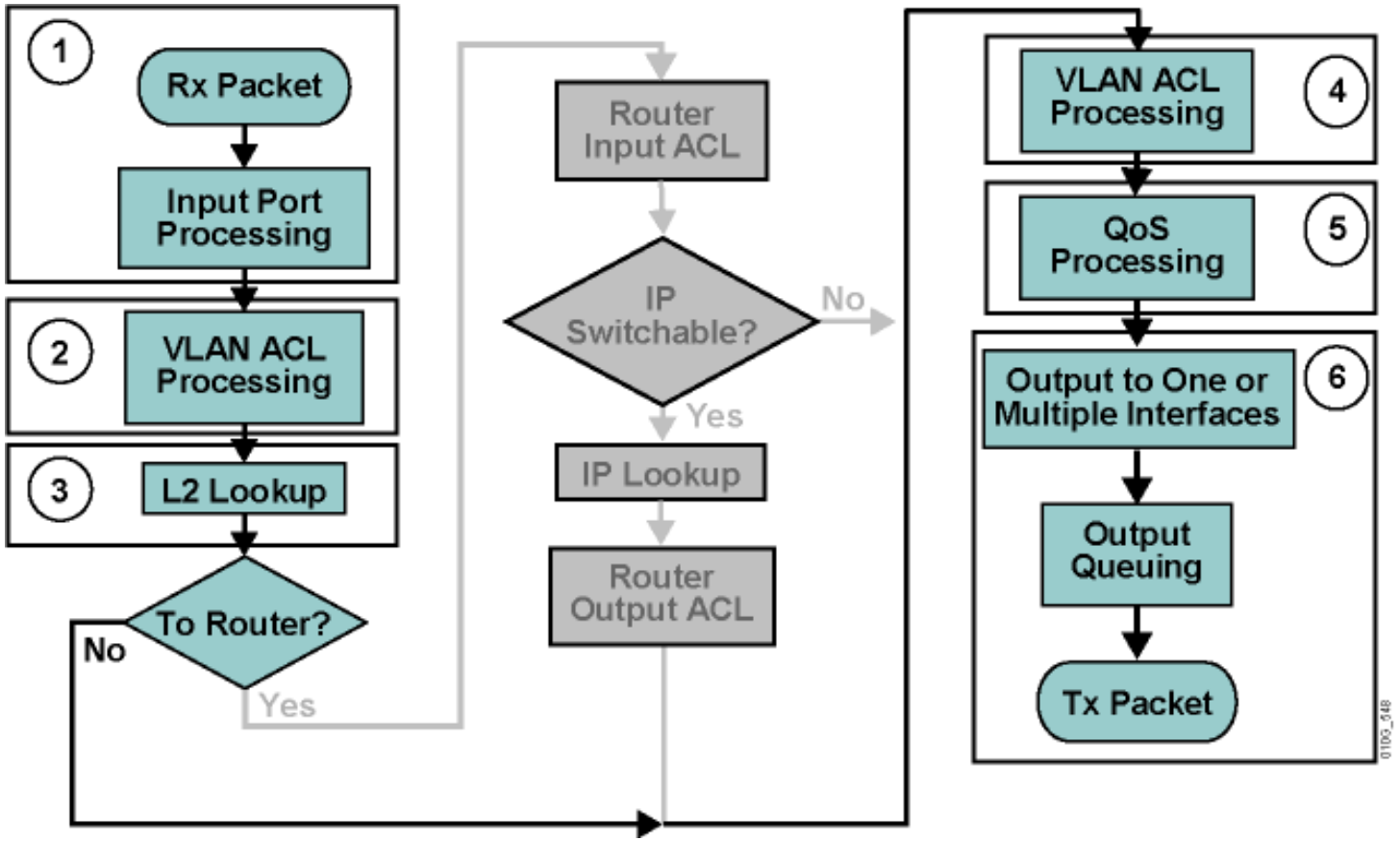
```
Router#show ip interface brief
```

- **Displays IP address on interfaces and current state of interface**

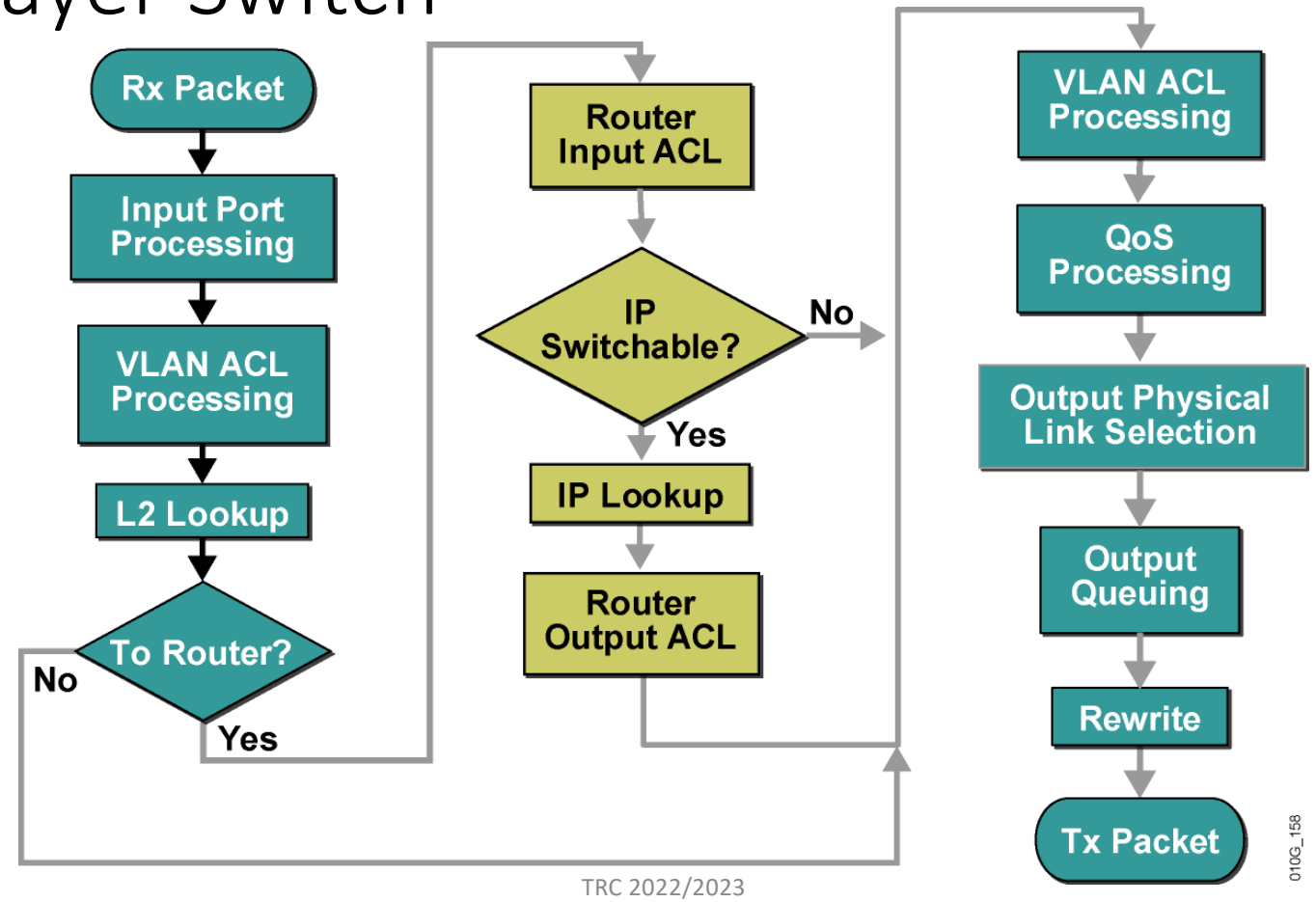
Explaining Multilayer Switching



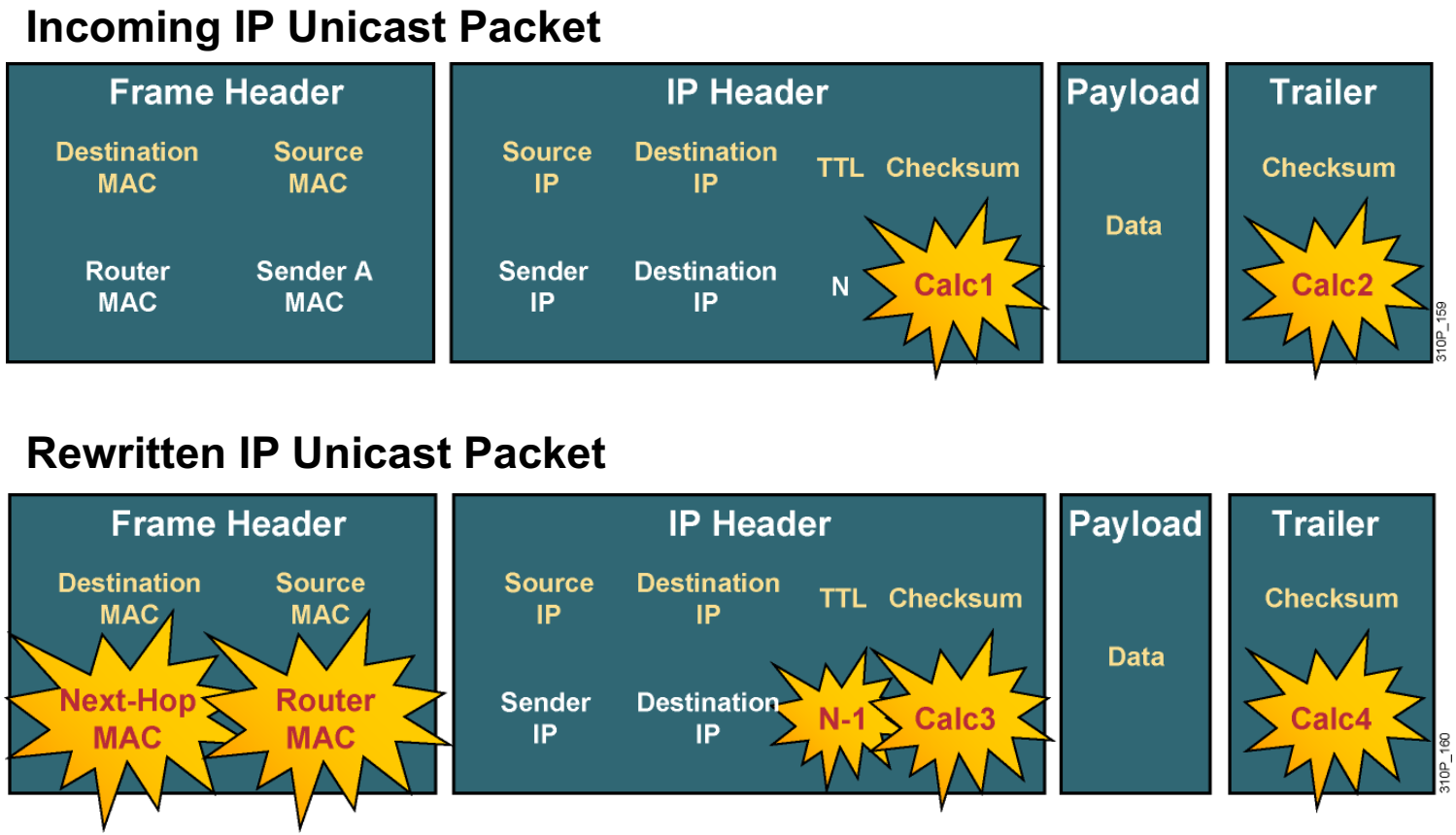
Layer 2 Switch Forwarding Process



Logical Packet Flow for a Multilayer Switch

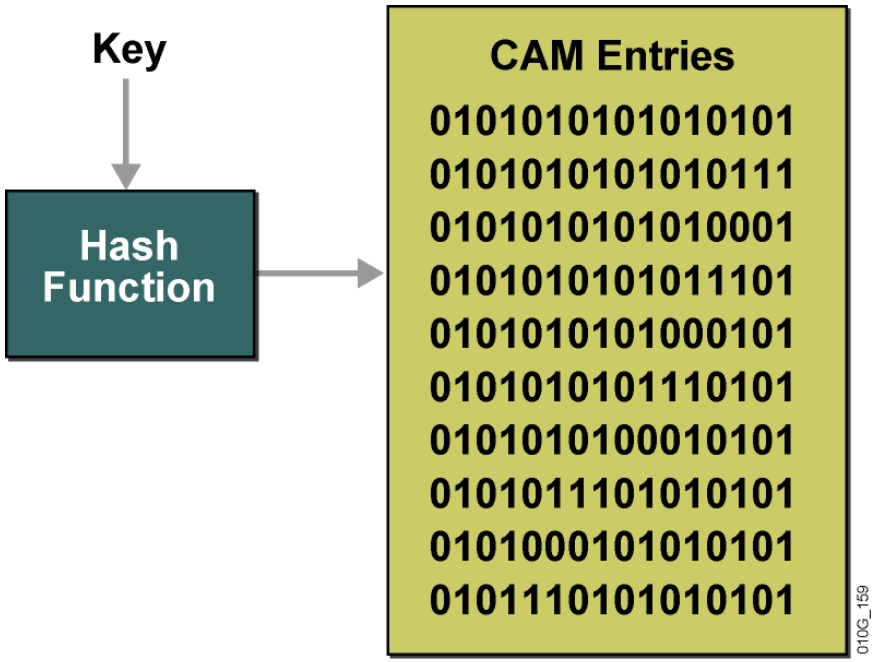


IP Unicast Frame and Packet Rewrite



CAM Table

- Requires an exact match on all bits
- Matching is a binary operation: 0 or 1
- Provides very high-speed lookups



TCAM Table

- Matches only significant values
- Matches based on three values: 0, 1, or X (either)
- Masks used to wildcard some content fields

Mask	Patterns
Mask 1 Match: All 32 bits of source IP address	Src IP = 10.1.1.1
	Empty 2
	Empty 3
	Empty 4
	Empty 5
Do Not Care: All remaining bits	Empty 6
	Empty 7
	Empty 8
Mask 2 Match: Most significant 24 bits of source IP address	Src IP = 10.1.1.0
	Empty 2
	Empty 3
	Empty 4
	Empty 5
Do Not Care: All remaining bits	Empty 6
	Empty 7
	Empty 8

010G_160

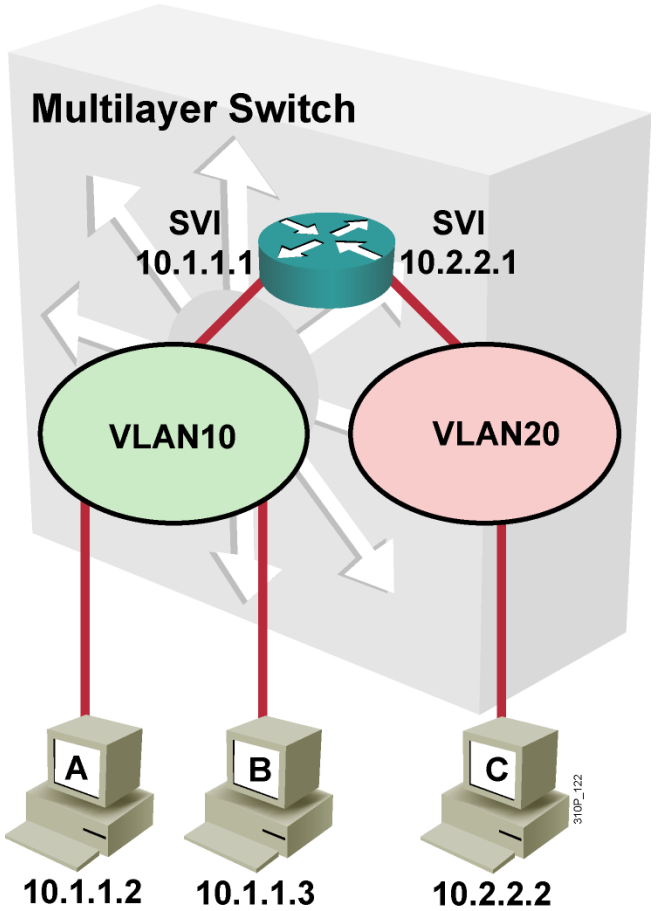
Summary

- A router on a stick can be used to route between VLANs using either ISL or 802.1Q as the trunking protocol.
- A router on a stick requires subinterfaces, one for each VLAN.
- Verify inter-VLAN routing by generating IP packets between two subnets.
- Multilayer switches can forward traffic at both Layer 2 and Layer 3.
- Multilayer switches rewrite the Layer 2 and Layer 3 header using tables held in hardware.

Implementing Inter-VLAN Routing

Enabling Routing Between VLANs on a Multilayer Switch

Layer 3 SVI


Multilayer Switch
SVI
10.1.1.1
SVI
10.2.2.1
VLAN10
VLAN20
A
B
C
10.1.1.2
10.1.1.3
10.2.2.2
310P_122

SVI on a Multilayer Switch

- Configure
  - ip routing
  - interface vlan 10
    - ip address 10.1.1.1 255.255.255.0
  - router eigrp 50
    - network 10.0.0.0
- Verify
  - show ip route

Configuring Inter-VLAN Routing Through an SVI

Step 1 : Configure IP routing.

```
Switch(config)#ip routing
```

Step 2 : Create an SVI interface.

```
Switch(config)#interface vlan vlan-id
```

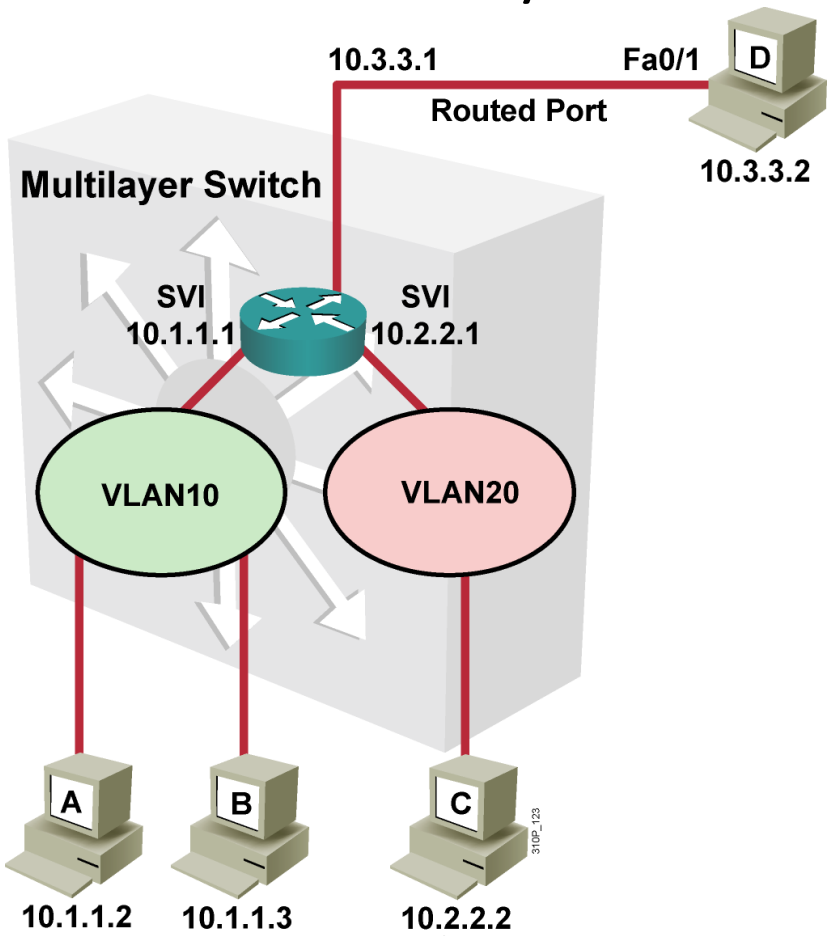
Step 3 : Assign an IP address to the SVI.

```
Switch(config-if)#ip address ip-address mask
```

Step 4 : Configure the IP routing protocol if needed.

```
Switch(config)#router ip_routing_protocol <options>
```

Routed Ports on a Multilayer Switch (Cont.)



Routed Ports on a Multilayer Switch

- Physical switch port with Layer 3 capability
- Not associated with a VLAN
- Requires removal of Layer 2 port functionality

Configure

- ip routing
- interface fa0/1
  - no switchport
  - ip address 10.3.3.1 255.255.255.0
- router eigrp 50
  - network 10.0.0.0

Configuring a Routed Port

Step 1 : Configure IP routing.

```
Switch(config)#ip routing
```

Step 2 : Create a routed port.

```
Switch(config-if)#no switchport
```

Step 3 : Assign an IP address to the routed port.

```
Switch(config-if)#ip address ip-address mask
```

Step 4 : Configure the IP routing protocol if needed.

```
Switch(config)#router ip_routing_protocol <options>
```

Summary

- SVI is a VLAN of switch ports represented by one interface to the routing system.
- Specific commands are used to configure and verify routing on multilayer switch interfaces.
- The interface vlan command creates the SVI.
- A routed port has Layer 3 attributes.
- A routed port requires the removal of Layer 2 port functionality with the no switchport command.
- To receive dynamic updates, a routing protocol is required.

E é tudo...

- Questões?
- Comentários?