

11W NET3011

CCNP SWITCH – Chapter 2

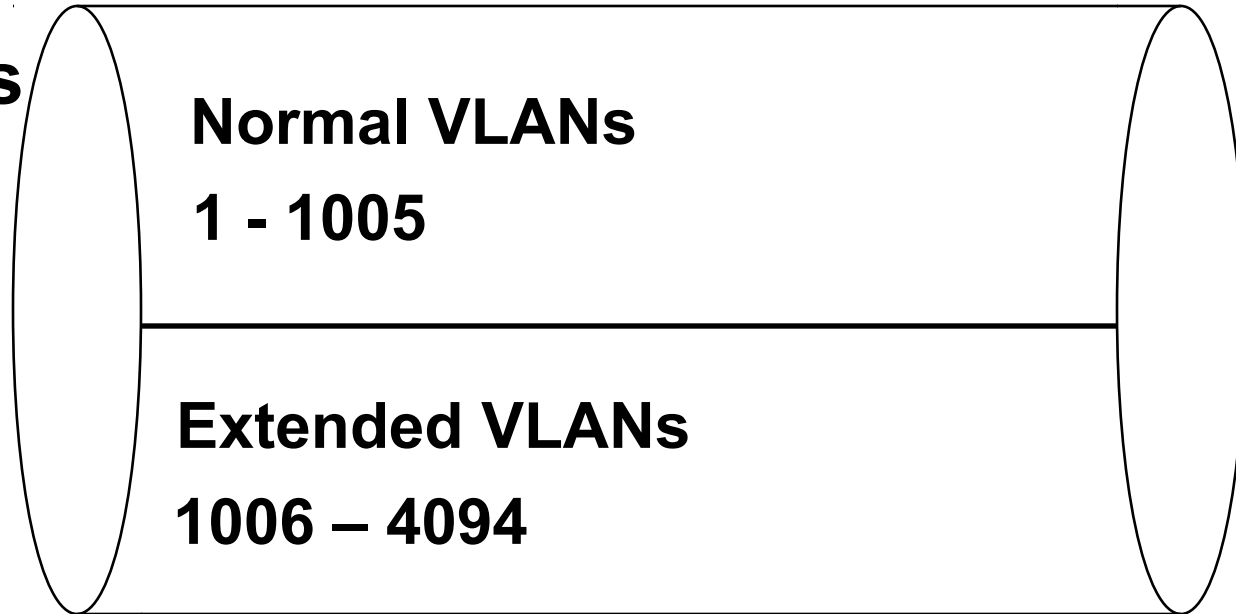
Implementing VLANs (Part 2)

David Bray

brayd@algonquincollege.com

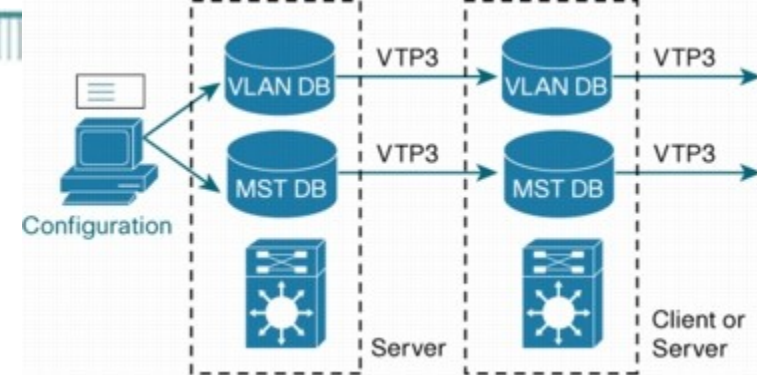
with contributions obtained from Rick Graziani & Cisco

Extended VLANs



- VLANs are typically from numbered 1 through 1005.
- The IEEE 802.1Q standard provides for support of up to 4096 VLANs.
 - VLANs 0 and 4095 are reserved by the IEEE 802.1Q standard and you cannot create, delete, or modify them (not displayed).
- Beginning with Cisco IOS Release 12.4(15)T, you can configure VLAN IDs in the **extended** range from 1006 to 4094 on specified platforms.
 - There are some configuration restrictions, for example it cannot be done in vlan database mode, VTP Transparent mode is needed, etc.
- This is outside the course scope, but for more information:
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/ht_xvlan.html

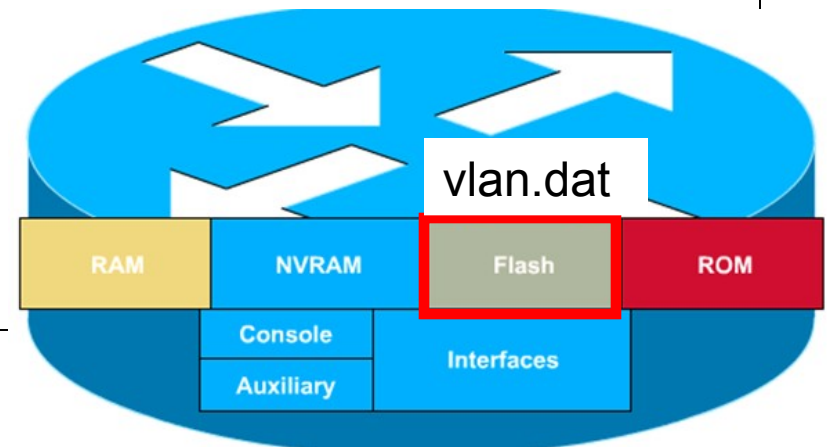
VTP version 3



- Again, outside the course scope and not part of CCNP SWITCH.
- Only available on CatOS, not IOS.
- “With 12.2(33)SXI VTP version 3 will be supported by IOS, closing the feature gap in this area compared to CAT OS. VTP version 3 will be available within all IOS feature sets.”
- Features:
 - Supports ISL VLAN range from 1 to 1001.
 - Supports 802.1Q VLAN range up to 4095.
 - Can transfer information regarding Private VLAN (PVLAN) structures.
- <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/solution>

Storing VLAN information

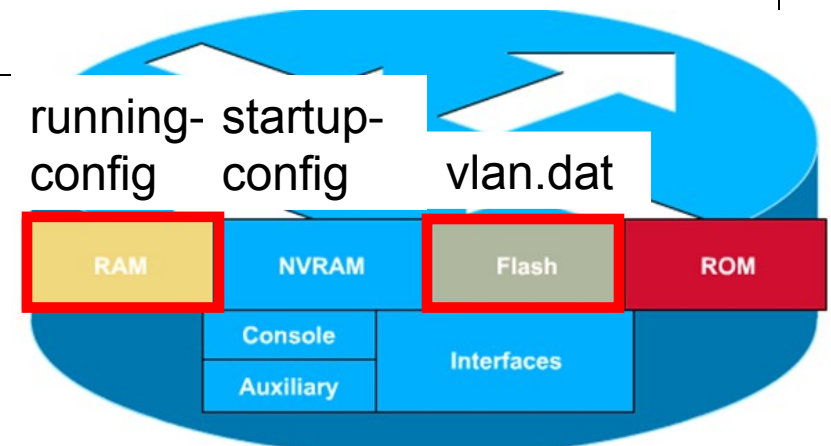
```
DLS1(config)# vtp domain West
DLS1(config)# vlan 10
DLS1(config-vlan)# name WestSales
DLS1(config-vlan)# vlan 11
DLS1(config-vlan)# name WestEng
```



- Storage of VLAN information is model dependent.
 - Cisco: “The memory location name where the vlan.dat file is stored varies from device to device. Refer to the respective product documentation before you issue the copy command.”
- VLAN information for 29xx and 35xx switches is automatically stored in the **vlan.dat** file in **flash**.
 - VTP information: **Domain Name, Configuration Revision Number**
 - VLAN information (configured or via VTP): **VLAN Number, VLAN Name**

Storing VLAN information

```
DLS1(config)# inter fa 0/1
DLS1(config-if)#switchport mode access
DLS1(config-if)# switchport access vlan 10
DLS1(config-if)# copy running-config startup-config
```



- Interface commands are stored in **running-config** and will need to be saved to **startup-config** in NVRAM
- Also, recall that 'vlan database' is being deprecated, in favour of performing vlan-related configurations directly from global configuration mode.

VTP Messages

VTP Messages

VTP Domain = **Cisco**

VTP Mode = Server

Config Rev = **2**

VLANs = 1, 2, 3

NOTE: Whenever you add, delete, or change (name) a VLAN on a VTP server, it increments the configuration revision number and a summary advertisement is sent.

Config Rev = **0**

VLANs = 1



- **VTP Summary advertisements**

- By default, sent **every five-minutes**.
- Inform adjacent switches of the current VTP **domain name** and the **configuration revision number**.
- Receiving switch **compares the received VTP domain name** to its own.
 - If its own name is Null, the received name is adopted.
 - Else, if the received name is different, the switch simply discards the packet.
 - Same or Different? **Same**
 - The switch then **compares the configuration revision** to its own.
 - If its own value is higher or equal, the packet is ignored.
 - » Own Config Rev higher or equal than sender's? **No, it is lower**
 - Otherwise, it is lower and a **VTP Advertisement Request** is sent.

VTP Messages

VTP Domain = **Cisco**

VTP Mode = Server

Config Rev = **2**

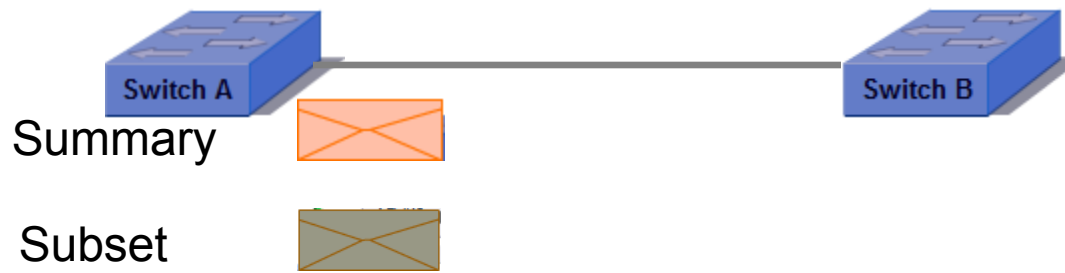
VLANs = 1 **2, 3** ←

VTP Domain = **Cisco**

VTP Mode = Server

Config Rev = **2**

VLANs = 1 **2, 3** ←



- VTP Subset advertisements

- Sent in response to a VTP Advertisement Request
- Also, sent whenever there is a change to VLAN information on a VTP server.
 - First the server sends a VTP Summary Advertisement
 - Then the server sends a VTP Subset Advertisement
- One or several subset advertisements follow the summary advertisement.
- A subset advertisement contains a list of VLAN information.

VTP Domain = null
VTP Mode = **Server**
Config Rev = 0
VLANs = 1



VTP Domain = null
VTP Mode = **Server**
Config Rev = 0
VLANs = 1



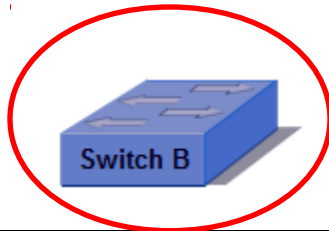
No Trunks Configured



VTP Domain = null
VTP Mode = **Server**
Config Rev = 0
VLANs = 1

- Let's take a look at VTP Messages and Server, Client and Transparent Switches.
- Switches are shown here with all VTP information at their defaults.

VTP Domain = null
VTP Mode = **Server**
Config Rev = 0
VLANs = 1



VTP Domain = null
VTP Mode = **Client**
Config Rev = 0
VLANs = 1

VTP Domain = null
VTP Mode = **Transparent**
Config Rev = 0
VLANs = 1



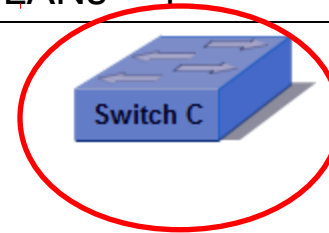
- Switch B is now a Client
- Switch C is now Transparent
- VLAN servers maintain a list of all VLANs in NVRAM.
- Client cannot add, delete or rename VLANs.
- Client does not store VLAN information in NVRAM.
- If a client reboots it loses VLAN information and relies on a VTP server to restore the information.

VTP Domain = null
VTP Mode = Server
Config Rev = 0
VLANs = 1



VTP Domain = null
VTP Mode = Client
Config Rev = 0
VLANs = 1

VTP Domain = null
VTP Mode = Transparent
Config Rev = 0
VLANs = 1



- Transparent mode switches must have their VLANs configured manually.
- Does not participate in VTP or advertise their VLANs.
- Ideal for switches with VLANs that should remain local to that switch.

VTP Domain = **Cisco**
VTP Mode = **Server**
Config Rev = **2**
VLANs = 1 **2, 3**



VTP Domain = null
VTP Mode = Transparent
Config Rev = 0
VLANs = 1

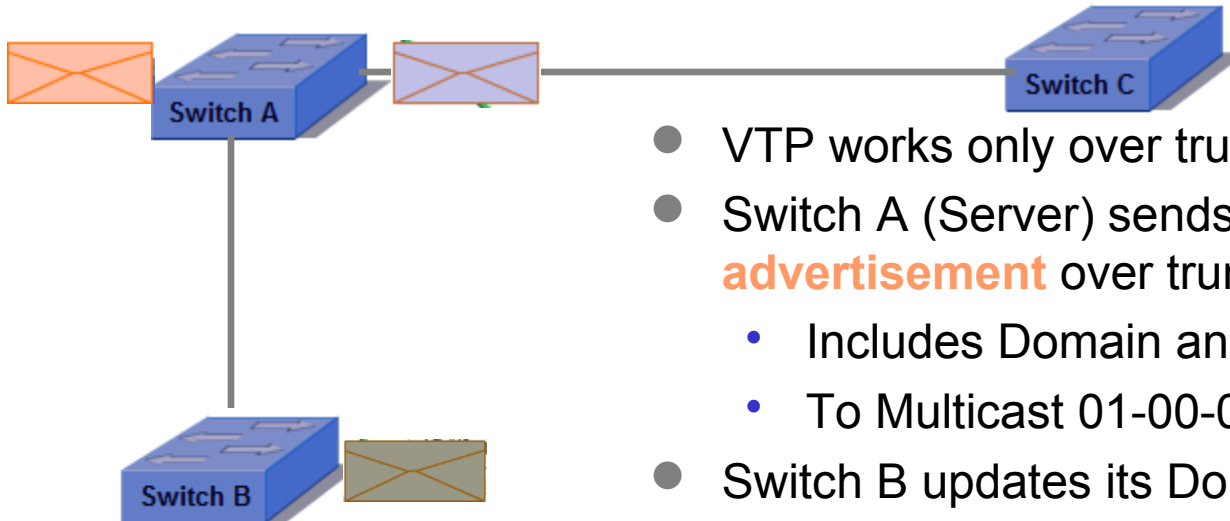


VTP Domain = null
VTP Mode = Client
Config Rev = 0
VLANs = 1

- VTP server:
 - Domain Name configured as Cisco
 - VLANs 2 and 3 added
 - Config Rev increased to 3 (one for each VLAN added)

VTP Domain = **Cisco**
 VTP Mode = Server
 Config Rev = **2**
 VLANs = 1, **2, 3**

VTP Domain = null
 VTP Mode = Transparent
 Config Rev = 0
 VLANs = 1

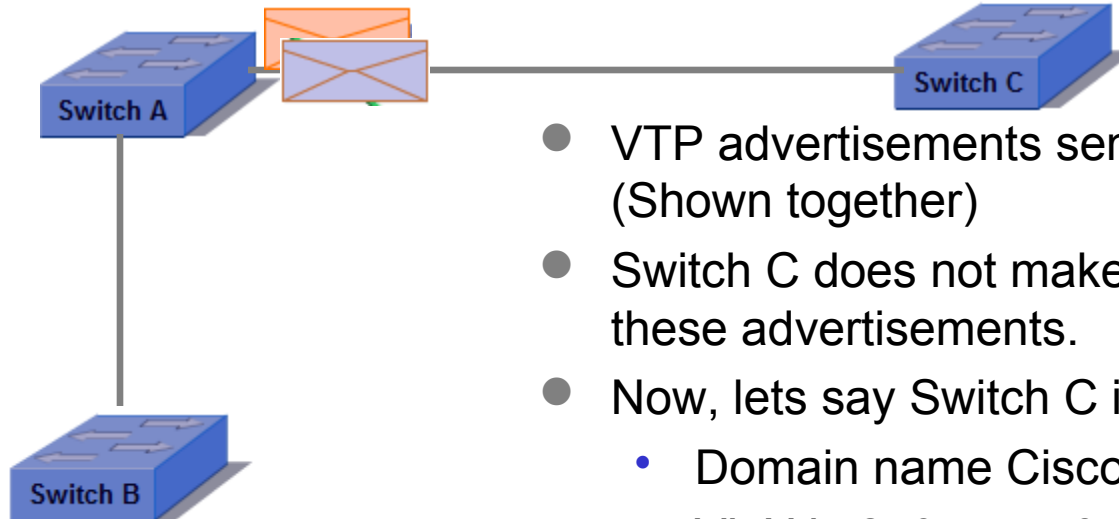


VTP Domain = **Cisco**
 VTP Mode = Client
 Config Rev = **2**
 VLANs = 1, **2, 3**

- VTP works only over trunk links.
- Switch A (Server) sends **summary advertisement** over trunk links on VLAN 1
 - Includes Domain and Revision Number
 - To Multicast 01-00-0C-CC-CC-CC
- Switch B updates its Domain
 - Because of the higher revision number in the Summary, B replies with **Advertisement Request**
- Switch A sends a VTP **Subset advertisement** (preceded by another Summary advertisement.)
- Switch B updates its configuration revision number and VLANs.

VTP Domain = **Cisco**
 VTP Mode = Server
 Config Rev = **2**
 VLANs = 1, **2, 3**

VTP Domain = **Cisco**
 VTP Mode = Transparent
 Config Rev = 0
 VLANs = 1, **2, 3, 4, 5, 6**



VTP Domain = Cisco
 VTP Mode = Client
 Config Rev = 2
 VLANs = 1, 2, 3

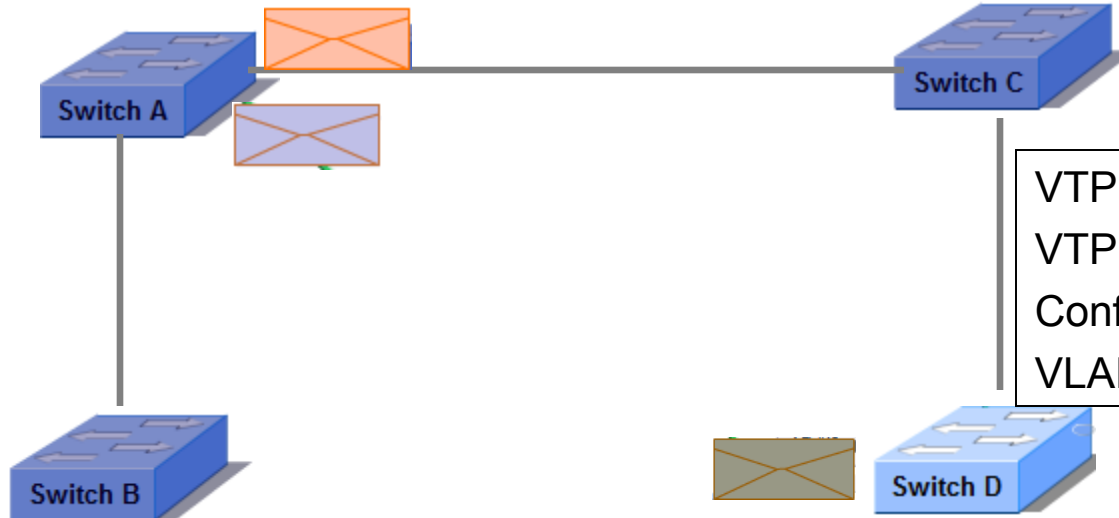
- VTP advertisements sent to Transparent switch. (Shown together)
- Switch C does not make any changes based on these advertisements.
- Now, lets say Switch C is configured with:
 - Domain name Cisco
 - VLANs 2, 3, 4, 5, 6
- Even though in same domain, Switch C does not advertise these VLANs to other switches.
- The Configuration Revision number remains at 0 even when VLAN configuration is changed.
- Transparent switches will relay VTP messages it receives to other switches if it is in the same domain or in a null domain (let's take a look...).

Relays VTP Advertisements

VTP Domain = **Cisco**
 VTP Mode = Server
 Config Rev = **2**
 VLANs = 1, **2, 3**

VTP Domain = Cisco
 VTP Mode = Transparent
 Config Rev = 0
 VLANs = 1, 2, 3, 4, 5, 6

**No changes to
 Rev or VLANs**



VTP Domain = **Cisco**
 VTP Mode = Client
 Config Rev = **2**
 VLANs = 1, **2, 3**

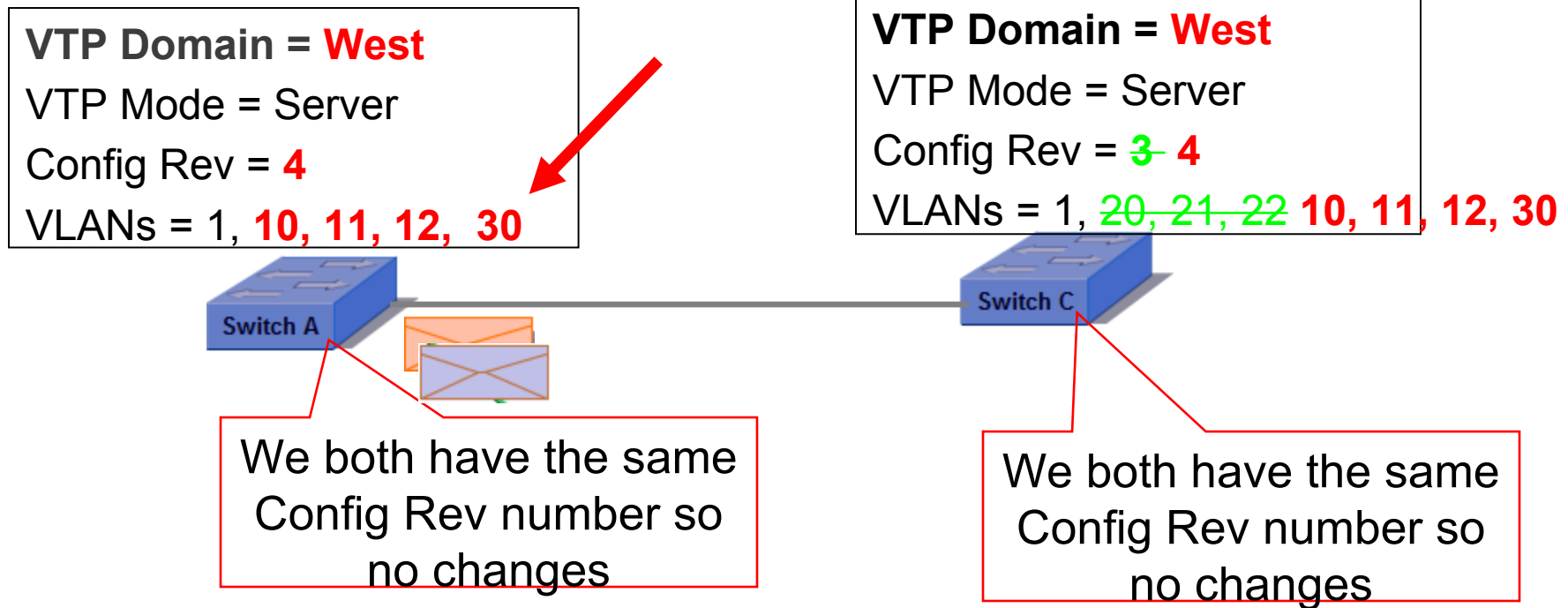
VTP Domain = Cisco
 VTP Mode = Client
 Config Rev = 2
 VLANs = 1, 2, 3

- VTP Client Switch D added to the network.
- Switch A (Server) sends **summary advertisement** over trunk links on VLAN 1
- Switch D updates its Domain
 - Replies with **Advertisement Request**
- Switch A sends a VTP **Subset advertisement**
- Switch D updates its configuration revision number and VLANs

Understanding and Troubleshooting

Common VTP Issues

Both switches are VTP Servers and in the same Domain, but have different VLAN information. Let's see what happens when trunking is enabled between the switches...



- When two switches with same Domain Name and same Configuration Revision Numbers exchange VTP information:
 - No change
- If Switch A adds a new VLAN, VLAN 30, Config Rev is increased by 1.
- Switch A will send VTP information to Switch B who will synchronize its VLAN information with Switch A, losing current “local” VLANs

Example: Using DLS1 (Switch A) and DLS2 (Switch B)

```
ALS2(config)# inter range fa 0/1 - 24
ALS2(config-if-range)# switchport mode dynamic auto

DLS2(config)# inter range fa 0/1 - 24
DLS2(config-if-range)# switchport mode dynamic auto
DLS2# show inter trunk

DLS2#
```



- Note: Because 2950's and 3550's default to **dynamic desirable** they will trunk by default and can give rise to unexpected results.
- Assuming consistent assignment of ALS2 to the 2950 and DLS2 to the 3550, we must configure ALS2 and DLS2 accordingly before connecting the cables.

When DLS1 gets a higher Config Rev Number...

```
DLS1# show vlan
```

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

- Default VLANs

When DLS1 gets a higher Config Rev Number...

```
DLS1#show vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           :
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
DLS1#
```

- Default VTP information:
 - Configuration Revision Number = 0
 - Increased by 1 whenever VLAN is added or deleted
 - VTP Mode = Server
 - VTP Domain Name = <blank> (null)

When DLS1 gets a higher Config Rev Number...

```
DLS2# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Gi0/1, Gi0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
DLS2# show vtp status
```

```
VTP Version : 2  
Configuration Revision : 0  
Maximum VLANs supported locally : 1005  
Number of existing VLANs : 5  
VTP Operating Mode : Server  
VTP Domain Name :  
<output omitted>
```

- Same on DLS2.

When DLS1 gets a higher Config Rev Number...

```
DLS1(config)# vtp domain West
DLS1(config)# vlan 10
DLS1(config-vlan)# name WestSales
DLS1(config-vlan)# vlan 11
DLS1(config-vlan)# name WestEng
DLS1(config-vlan)# vlan 12
DLS1(config-vlan)# name WestAdmin

DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 3
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 8
VTP Operating Mode         : Server
VTP Domain Name            : West
<output omitted>
```

- Add VTP Domain Name and configure VLANs
- Configuration Revision changed to 3 (one for each VLAN)
- Remember, no trunking (yet)

When DLS1 gets a higher Config Rev Number...

```
DLS1# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Gi0/1, Gi0/2
10 WestSales	active	
11 WestEng	active	
12 WestAdmin	active	

- Verified.

When DLS1 gets a higher Config Rev Number...

```
DLS2(config)# vtp domain West
DLS2(config)# vlan 20
DLS2(config-vlan)# name WestAcct
DLS2(config-vlan)# vlan 21
DLS2(config-vlan)# WestMngt
DLS2(config-vlan)# name WestMngt
DLS2(config-vlan)# vlan 22
DLS2(config-vlan)# name WestManuf

DLS2# show vtp status
VTP Version                : 2
Configuration Revision     : 3
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 8
VTP Operating Mode         : Server
VTP Domain Name            : West
<output omitted>
```

- Now on DLS2: Add VTP Domain Name and configure different VLANs
- Configuration Revision changed to 3
- Still no trunking

When DLS1 gets a higher Config Rev Number...

VTP Domain = **West**
VTP Mode = Server
Config Rev = **3**
VLANs = 1, **10, 11, 12**



VTP Domain = **West**
VTP Mode = Server
Config Rev = **3**
VLANs = 1, **20, 21, 22**

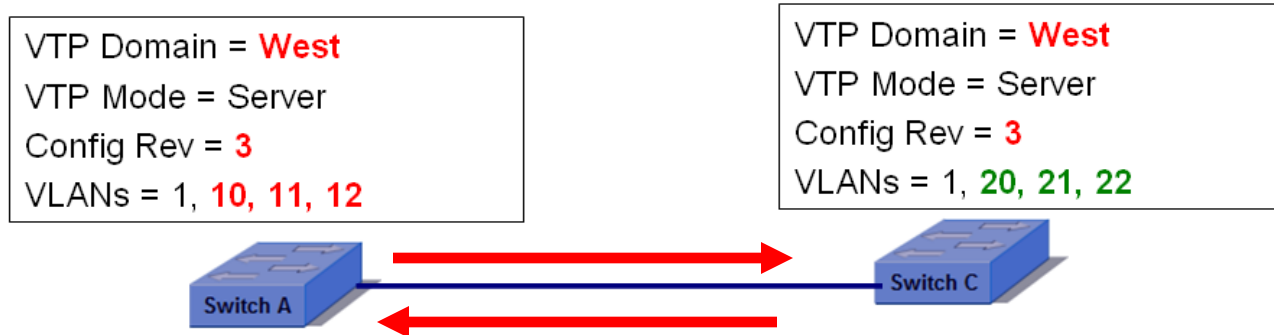


```
DLS2# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Gi0/1, Gi0/2
20 WestAcct	active	
21 WestMngt	active	
22 WestManuf	active	

● Verified.

When DLS1 gets a higher Config Rev Number...



```
DLS1(config)# inter range fa 0/11 - 12  
DLS1(config-if-range)# switchport trunk encap dot1q  
DLS1(config-if-range)# switchport mode trunk
```

```
DLS1# show inter trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/11	on	802.1q	trunking	1
Fa0/12	on	802.1q	trunking	1

- Trunking configured between DLS1 and DLS2.
- VTP messages can now be sent but no changes because Configuration Revision numbers are the same.

When DLS1 gets a higher Config Rev Number...

```
DLS1# show vtp status
```

```
VTP Version : 2  
Configuration Revision : 3  
Maximum VLANs supported locally : 1005  
Number of existing VLANs : 8  
VTP Operating Mode : Server  
VTP Domain Name : West  
<output omitted>
```

```
DLS2# show vtp status
```

```
VTP Version : 2  
Configuration Revision : 3  
Maximum VLANs supported locally : 1005  
Number of existing VLANs : 8  
VTP Operating Mode : Server  
VTP Domain Name : West  
<output omitted>
```

- Configuration Revision still 3
- Number of existing VLANs (known by each switch) still 8


When DLS1 gets a higher Config Rev Number...

```
DLS1# show vlan
VLAN Name                Status    Ports
-----
1      default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         <output omitted>
                                         Fa0/23, Fa0/24, Gi0/1, Gi0/2

10     WestSales
11     WestEng
12     WestAdmin
```

VTP Domain = **West**
VTP Mode = Server
Config Rev = **3**
VLANs = 1, **10, 11, 12**

VTP Domain = **West**
VTP Mode = Server
Config Rev = **3**
VLANs = 1, **20, 21, 22**



```
DLS2# show vlan
VLAN Name                Status    Ports
-----
1      default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                         <output omitted>
                                         Fa0/23, Fa0/24, Gi0/1, Gi0/2

20     WestAcct                active
21     WestMngt                active
22     WestManuf                active
```

- Verify that there are no DLS2 VLANs on DLS1.
- Verify that there are no DLS1 VLANs on DLS2.

When DLS1 gets a higher Config Rev Number...

```
DLS1(config)# vlan 30
DLS1(config-vlan)# name Guest

DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : West
<output omitted>
```

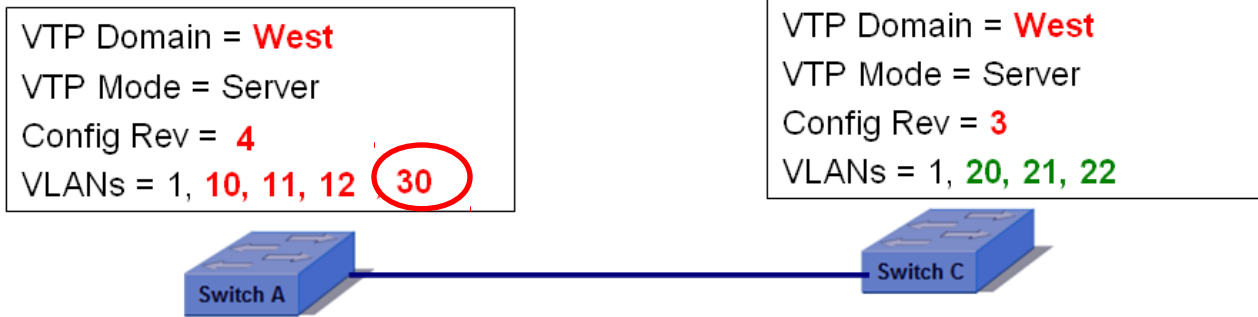
```
VTP Domain = West
VTP Mode = Server
Config Rev = 4
VLANs = 1, 10, 11, 12, 30
```

```
VTP Domain = West
VTP Mode = Server
Config Rev = 3
VLANs = 1, 20, 21, 22
```



- VLAN 30 added on DLS1.
- Configuration Revision increased by 1 to 4.
- DLS1 now has the higher Configuration Revision number between the two servers (the highest in the Domain).

When DLS1 gets a higher Config Rev Number...

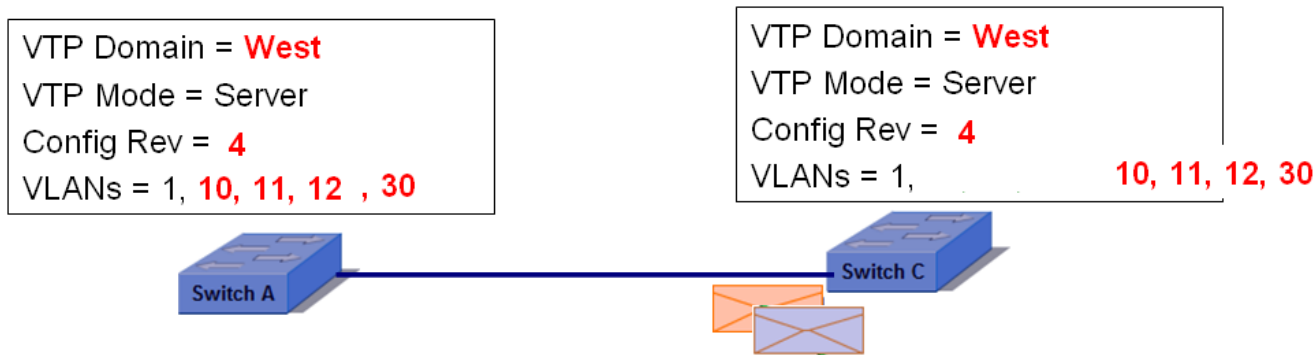


```
DLS1# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	WestSales	active	
11	WestEng	active	
12	WestAdmin	active	
30	Guest	active	

● Verified.

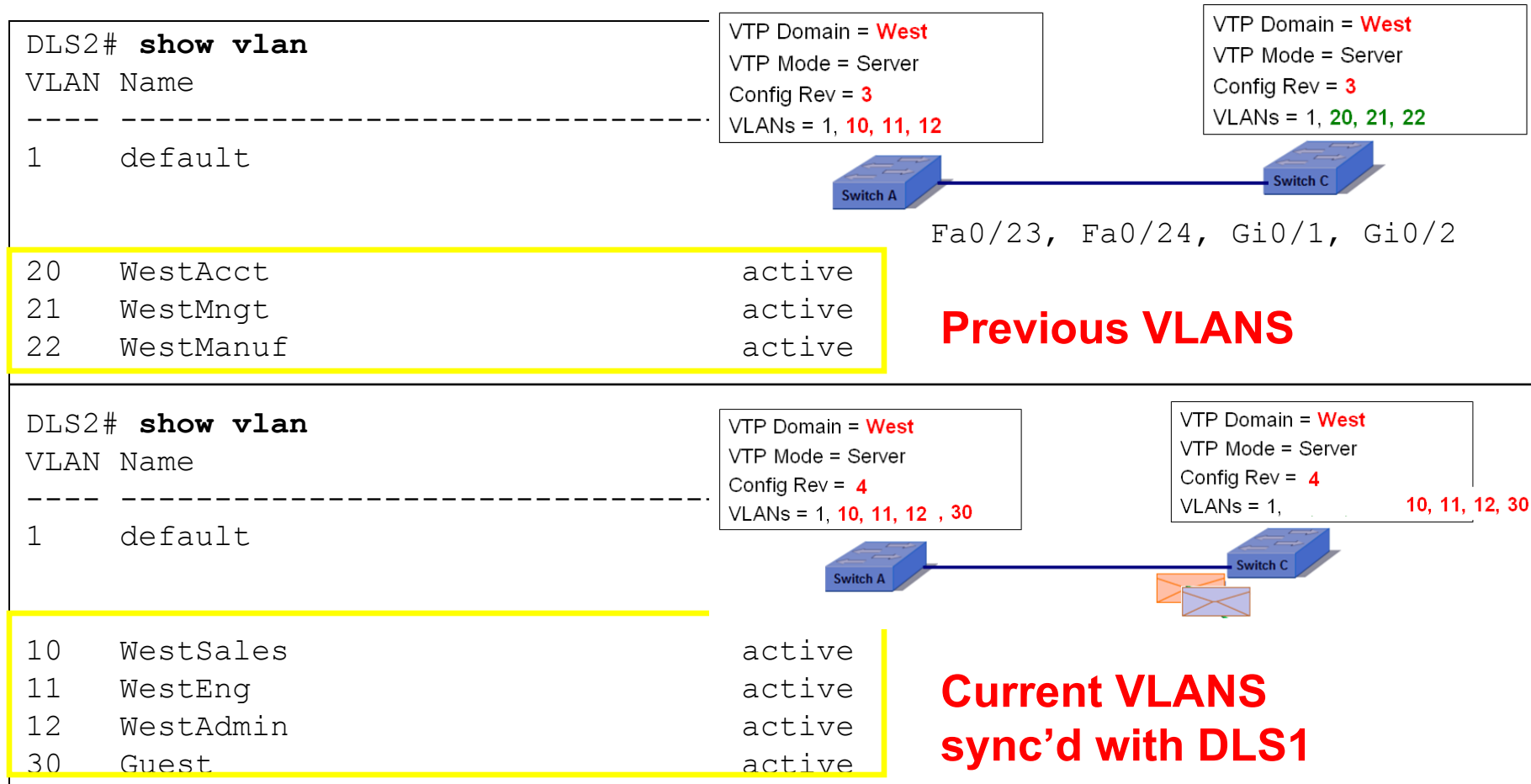
When DLS1 gets a higher Config Rev Number...



```
DLS2# show vtp status
VTP Version                : 2
Configuration Revision     : 4
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode        : Server
VTP Domain Name           : West
<output omitted>
```

- DLS2 receives VTP update from DLS1 with higher Configuration Revision Number.
- DLS2 synchronizes its VLAN database with DLS1's information including Configuration Revision Number and VLAN information.

When DLS1 gets a higher Config Rev Number...



- DLS2 lost previously configured VLANs 20, 21, and 22.
- DLS2's VLAN database overwritten with DLS1's information.
- Good news: Both Servers both in sync (identical) so any changes will mean the VLAN information is the same on both.

When DLS1 gets a higher Config Rev Number...

```
DLS2(config)# vlan 20
DLS2(config-vlan)# name WestAcct
DLS2(config-vlan)# vlan 21
DLS2(config-vlan)# name WestMngt
DLS2(config-vlan)# vlan 22
DLS2(config-vlan)# name WestManuf

DLS2# show vtp status
VTP Version                : 2
Configuration Revision     : 7
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 12
VTP Operating Mode         : Server
VTP Domain Name            : West
```

- To correct this we need to add the VLANs back to DLS2.
- DLS2 will send VTP update to DLS1 so VLAN information will be the same.

When DLS1 gets a higher Config Rev Number...

```
DLS2# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	WestSales	active	
11	WestEng	active	
12	WestAdmin	active	
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	

- Verified.

When DLS1 gets a higher Config Rev Number...

```
DLS1# show vtp status
```

```
VTP Version : 2
Configuration Revision : 7
Maximum VLANs supported locally : 1005
Number of existing VLANs : 12
VTP Operating Mode : Server
VTP Domain Name : West
<output omitted>
```

- DLS1 receives VTP update and updates VLAN information including Configuration Revision number.
- Domain is still in sync.

```
DLS1# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Fa0/23, Fa0/24, Gi0/1, Gi0/2
10 WestSales	active	
11 WestEng	active	
12 WestAdmin	active	
20 WestAcct	active	
21 WestMngt	active	
22 WestManuf	active	
30 Guest	active	

What happens when Client/Server enters with higher Configuration Revision number?

VTP Domain = **West**
VTP Mode = Server
Config Rev = ~~10~~ **13**
VLANs = 1, ~~10, 11, 12~~ **20, 21, 22, 30**

VTP Domain = **West**
VTP Mode = **Client** (or Server)
Config Rev = **13**
VLANs = 1, **20, 21, 22, 30**



- Both switches are in the same domain.
- Switch C can be **Client OR Server**
- Switch C has the Higher Configuration Revision number
- Even if Switch C is a **Client** when enters VTP domain it will overwrite DLS1's VLAN information because it has the higher Configuration Revision number.

VTP Domain = **West**

VTP Mode = Server

Config Rev = **10**VLANs = 1, **10, 11, 12, 20, 21, 22, 30**

Client/Server enters with Higher Revision

```
DLS1(config)# inter fa 0/1
DLS1(config-if)# switchport mode access
DLS1(config-if)# switchport access vlan 10
DLS1(config-if)# exit
DLS1(config)# inter fa 0/2
DLS1(config-if)# switchport mode access
DLS1(config-if)# switchport access vlan 11
DLS1# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 <output omitted> Gi0/1, Gi0/2
10	WestSales	active	Fa0/1
11	WestEng	active	Fa0/2
12	WestAdmin	active	
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	



- Assign VLANs to interfaces.

Client/Server enters with Higher Revision

```
VTP Domain = West  
VTP Mode = Server  
Config Rev = 10  
VLANs = 1, 10, 11, 12, 20, 21, 22, 30
```



```
DLS1(config)# inter range fa 0/11 -12  
DLS1(config-if-range)# shutdown
```

- Shutdown interface so we can modify DLS2 (Switch B)
- We will later restore the trunk to simulate a new switch entering the network.

Client/Server enters with Higher Revision

```
DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 10
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 12
VTP Operating Mode         : Server
VTP Domain Name            : West
<output omitted>
```

```
DLS2#show vtp status
VTP Version                : 2
Configuration Revision     : 10
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 12
VTP Operating Mode         : Server
VTP Domain Name            : West
```

- Right now both switches have the same Configuration Revision number; let's change that.
- Note: Configuration Revision numbers not necessarily the same as previous example due to this was done in a different session.

Client/Server enters with Higher Revision

```
DLS2#show vlan
```

VLAN Name	State
-----	-----
1 default	active
10 WestSales	active
11 WestEng	active
12 WestAdmin	active
20 WestAcct	active
21 WestMngt	active
22 WestManuf	active
30 Guest	active

VTP Domain = **West**
 VTP Mode = **Client** (or Server)
 Config Rev = **13**
 VLANs = 1, **20, 21, 22, 30**



Gi0/1, Gi0/2

- We are going to remove these three VLANs on DLS2 so it has different VLANs and a higher Configuration Revision Number.
- Remember, DLS1 has same VLAN information and also has:
 - Fa0/1 in VLAN 10
 - Fa0/2 in VLAN 11

Client/Server enters with Higher Revision

```
DLS2(config)# no vlan 10
DLS2(config)# no vlan 11
DLS2(config)# no vlan 12

DLS2(config)# vtp mode client
Setting device to VTP CLIENT mode.
```

```
DLS2# show vtp status
VTP Version                : 2
Configuration Revision     : 13
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode        : Client
VTP Domain Name           : West
<output omitted>
```

```
VTP Domain = West
VTP Mode = Client (or Server)
Config Rev = 13
VLANs = 1, 20, 21, 22, 30
```



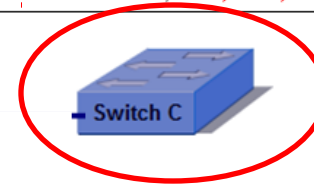
- Three VLANs deleted.
- Change VTP mode to Client
- Configuration Revision updated from 10 to 13

Client/Server enters with Higher Revision

VTP Domain = **West**
 VTP Mode = Server
 Config Rev = **10**
 VLANs = 1, **10, 11, 12, 20, 21, 22, 30**



VTP Domain = **West**
 VTP Mode = **Client** (or Server)
 Config Rev = **13**
 VLANs = 1, **20, 21, 22, 30**



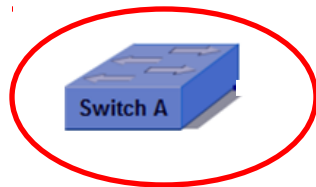
```
DLS2# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Gi0/1, Gi0/2
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	

- Verify VLANs 10, 11, and 12 were deleted.

Client/Server enters with Higher Revision

VTP Domain = **West**
VTP Mode = Server
Config Rev = **10**
VLANs = 1, **10, 11, 12, 20, 21, 22, 30**



VTP Domain = **West**
VTP Mode = **Client** (or Server)
Config Rev = **13**
VLANs = 1, **20, 21, 22, 30**



```
DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 10
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 12
VTP Operating Mode        : Server
VTP Domain Name           : West
<output omitted>
```

- DLS1 has a lower Configuration Revision number 10.
- DLS2's Configuration Revision number is 13.

VTP Domain = **West**
 VTP Mode = Server
 Config Rev = **13**
 VLANs = 1, **20, 21, 22, 30**

VTP Domain = **West**
 VTP Mode = **Client** (or Server)
 Config Rev = **13**
 VLANs = 1, **20, 21, 22, 30**



```
DLS1(config)# inter range fa 0/11 -12
DLS1(config-if-range)# no shutdown

DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 13
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode        : Server
VTP Domain Name           : West
<output omitted>
```

```
DLS2# show vtp status
VTP Version                : 2
Configuration Revision     : 13
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode        : Client
VTP Domain Name           : West
<output omitted>
```

- DLS2 (Switch B) is brought online (“no shut” on DLS1).
- DLS2 (Client) has higher Configuration Revision number 13.
- DLS1 (Switch A) with lower revision number (10) updates its VLAN information to be in sync with DLS2 and also adopts 13 as its new Configuration Revision number.

VTP Revision Number

```
DLS1# show vlan
```

VLAN	Name	Status	
1	default	active	
10	WestSales	active	Fa0/1
11	WestEng	active	Fa0/2
12	WestAdmin	active	
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	

VTP Domain = **West**

VTP Mode = Server

Config Rev = **10**

VLANs = 1, **10, 11, 12, 20, 21, 22, 30**



Previous VLANS

```
DLS1# show vlan
```

VLAN	Name	Status	
1	default	active	
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	

VTP Domain = **West**

VTP Mode = Server

Config Rev = **13**

VLANs = 1, **20, 21, 22, 30**

VTP Domain = **West**

VTP Mode = **Client** (or Server)

Config Rev = **13**

VLANs = 1, **20, 21, 22, 30**



**Current VLANS
sync'd with DLS2**

Missing VLANs 10, 11, and 12 => DLS1 f0/1 and f0/2 are now inactive.

Fix it

```
DLS1(config)# vlan 10
DLS1(config-vlan)# name WestSales
DLS1(config-vlan)# vlan 11
DLS1(config-vlan)# name WestEng
DLS1(config-vlan)# vlan 12
DLS1(config-vlan)# name WestAdmin
DLS1# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 <output omitted> Gi0/1, Gi0/2
10	WestSales	active	Fa0/1
11	WestEng	active	Fa0/2
12	WestAdmin	active	
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	

- To fix it, we reconfigure the missing VLANs on DLS1.
- Interfaces Fa0/1 and Fa0/2 brought from inactive to active

VTP Domain = **West**
VTP Mode = **Server**
Config Rev = **16**
VLANs = 1, **10, 11, 12, 20, 21, 22, 30**

VTP Domain = **West**
VTP Mode = **Client** (or Server)
Config Rev = **16**
VLANs = 1, **10, 11, 12, 20, 21, 22, 30**



```
DLS2# show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 <output omitted> Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	WestSales	active	
11	WestEng	active	
12	WestAdmin	active	
20	WestAcct	active	
21	WestMngt	active	
22	WestManuf	active	
30	Guest	active	

```
DLS2(config)# no vlan 10
```

VTP VLAN configuration not allowed when device is in CLIENT mode.

```
DLS2(config)#
```

- DLS2 gets VLANS 10, 11, 12 in VTP update from DLS1.
- DLS2 is a Client and can no longer delete (or add) VLANs.

AU VTP Domain = **West**
VTP Mode = **Server**
Config Rev = **16**
VLANs = 1, **10, 11, 12, 20, 21, 22, 30**

VTP Domain = **West**
VTP Mode = **Client** (or Server)
Config Rev = **16**
VLANs = 1, **10, 11, 12, 20, 21, 22, 30**



```
DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 16
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 12
VTP Operating Mode         : Server
VTP Domain Name            : West
```

```
DLS2# show vtp status
VTP Version                : 2
Configuration Revision     : 16
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 12
VTP Operating Mode         : Client
VTP Domain Name            : West
```

● **Still in sync!**

How to make sure switch has Lower Config Rev: VTP Mode

VTP Domain = West
 VTP Mode = Server
 Config Rev = 10
 VLANs = 1, 10, 11, 12, 20, 21, 22, 30

VTP Domain = West
 VTP Mode = Client Transparent Client
 Config Rev = 16 0 10
 VLANs = 1 10, 11, 12, 20, 21, 22, 30



- Setting a switch to Transparent mode resets the config rev to 0.
- Then set it back to Client or Server.

```
DLS2 (config) #VTP mode ?
client          Set the device to client mode.
server         Set the device to server mode.
transparent    Set the device to transparent mode.
```

How to make sure switch has Lower Config Rev: VTP Domain

VTP Domain = **West**
 VTP Mode = Server
 Config Rev = **16**
 VLANs = 1, **10, 11, 12, 20, 21, 22, 30**

VTP Domain = **West** ~~East~~ **West**
 VTP Mode = **Client**
 Config Rev = **16** **0** **16**
 VLANs = 1 **10, 11, 12, 20, 21, 22, 30**



- Changing the Domain Name on a switch will reset the configuration to 0.
- Then set it back to the correct Domain Name.

```
DLS2(config)# vtp domain West
Changing VTP domain name from East to West
```

Final Word on VTP Issues

- A VTP domain name will only be learned by a switch if its name is Null.
 - Once a switch's VTP Domain Name is set, it can only be changed by manual intervention!
- All switches participating in the same VTP domain must be contiguous.
 - Any intervening switch configured in a different VTP domain will block the flow of VTP advertisements because switches only forward VTP messages belonging to their home domain.
 - Even switches in Transparent mode will only forward VTP messages belonging to their configured domain.
- When using VTP passwords (secure mode), begin by configuring passwords on the VTP servers.
 - VTP clients will not be able to adopt any changes until they are also reconfigured with the appropriate password, but no VLAN information will be lost.
 - All active ports in pre-existing VLANs will continue to operate normally.
 - The password is never propagated across the network; only a hash of it is sent for authentication purposes.
- Remember that Domain Names & Passwords are case-sensitive.

VTP Pruning



VTP Pruning

No access ports
on VLAN 120

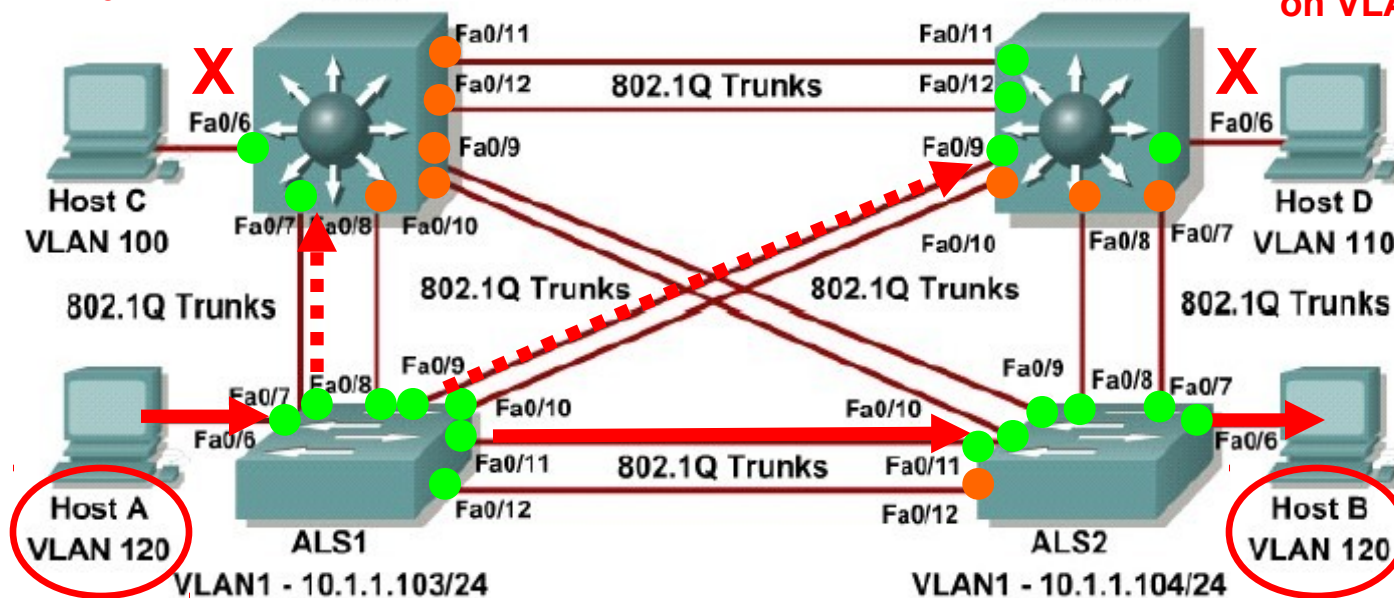
VLAN1 - 10.1.1.101/24

DLS1

VLAN1 - 10.1.1.102/24

DLS2

No access ports
on VLAN 120



- How would VLANs affect A's ARP broadcast for B's L2 address?
 - Host C and Host D would not receive the ARP Request.
 - But the broadcast would be transmitted across all trunk links.
- If VTP pruning is enabled, ALS1 would not send broadcasts for VLAN 120 to DLS1 or DLS2 (dashed lines).
- VTP pruning increases the available bandwidth by restricting flooded traffic only to those trunks that lead to member VLAN devices.

VTP Pruning is disabled by default

```
DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : Cabrillo
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xAB 0x0C 0xEB 0xDE 0x6A 0x89
                           0x0C 0xAD
Configuration last modified by 10.1.1.101 at 3-1-93 00:17:55
Local updater ID is 10.1.1.101 on interface V11 (lowest numbered
VLAN interface found)
DLS1#
```

It is easy to configure

```
DLS1(config)# vtp pruning
DLS1(config)# end

DLS1# show vtp status
VTP Version                : 2
Configuration Revision     : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : Cabrillo
VTP Pruning Mode           : Enabled
VTP V2 Mode                 : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xAB 0x0C 0xEB 0xDE 0x6A 0x89
                           0x0C 0xAD
Configuration last modified by 10.1.1.101 at 3-1-93 00:17:55
Local updater ID is 10.1.1.101 on interface Vl1 (lowest numbered
VLAN interface found)
DLS1#
```

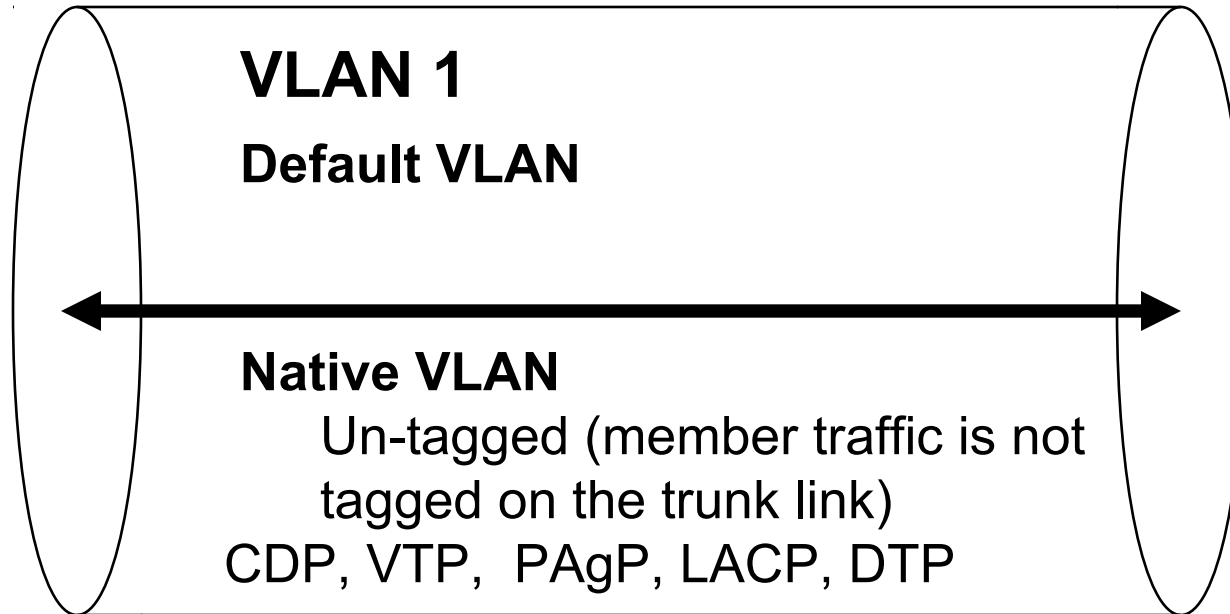
- Enable VTP pruning on all switches.

Default, Native and Management VLANs

FLAN: (Predecessor to the VLAN?)



Native VLAN



- By default all traffic is carried across VLAN 1.
- VLAN 1 is:
 - The **default VLAN** (all user traffic)
 - **Native VLAN**: No trunking encapsulation even if configured as a trunk.
 - VLAN for CDP, VTP, PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol), and DTP
- A topic that causes considerable confusion is the native VLAN.

Native VLAN

Common VLAN configuration

Note: We have not yet discussed routing between these VLANS. (But we will!)

VLAN 1 – *Native* VLAN, Un-tagged, (no 802.1Q /ISL encap)

CDP, VTP, PAgP, DTP

VLAN 10 – Tagged, User VLAN

172.16.10.0/24

VLAN 20 – Tagged, User VLAN

172.16.20.0/24

VLAN 99 – Tagged, Management VLAN

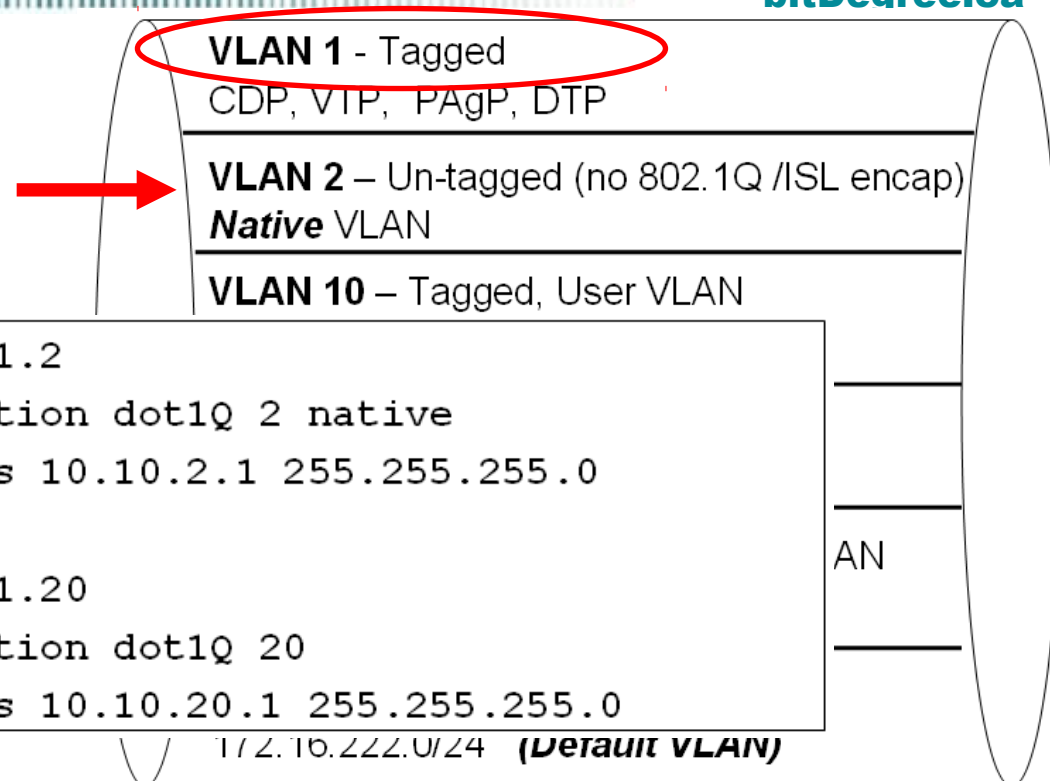
172.16.99.0/24

VLAN 222 – Tagged, Garbage VLAN

172.16.222.0/24 (**Default VLAN**)

- The IEEE committee that defined 802.1Q decided to support a native VLAN for backwards compatibility:
 - Allows 802.1Q capable ports to talk to old 802.3 ports directly by sending and receiving **untagged traffic**.
 - Loss of identification also means a loss of classification.
 - You should avoid using VLAN 1 (or whatever your Native VLAN is) for data traffic, so it is eligible to be classified with QoS for differentiated delivery.
 - We will see examples later with IP Telephony.

Best Practices



- **Native VLAN**

- Can be modified to be a VLAN other than VLAN 1.
- Must be the same on both link partners.
- Should not be used for user VLAN or Management VLAN.
- Control traffic (CDP, VTP, PAgP, DTP) still transmitted over VLAN 1.
 - If Native VLAN is other than VLAN 1 then control traffic is sent tagged.
- It is fine to leave VLAN 1 as the Native VLAN but should only carry control traffic and not user or management traffic.
- Note: Router uses subinterfaces for trunking and the native VLAN is configured using the native option. (Discussed later)

Best Practices



VLAN 1 - Tagged
CDP, VTP, PAgP, DTP

VLAN 2 – Un-tagged (no 802.1Q /ISL encap)
Native VLAN

VLAN 10 – Tagged, User VLAN
172.16.10.0/24

VLAN 20 – Tagged, User VLAN
172.16.20.0/24

VLAN 99 – Tagged, Management VLAN
172.16.99.0/24

VLAN 222 – Tagged, Garbage VLAN
172.16.222.0/24 (**Default VLAN**)

```
Switch(config)# hostname DLS2
DLS2(config)# interface vlan 99
DLS2(config-if)# ip address 10.0.99.1 255.255.255.0
```

- Management VLAN
 - The Management VLAN is the VLAN used to reach (ping, telnet) network devices.

Best Practices



VLAN 1 - Tagged
CDP, VTP, PAgP, DTP

VLAN 2 – Un-tagged (no 802.1Q /ISL encap)
Native VLAN

VLAN 10 – Tagged, User VLAN
172.16.10.0/24

VLAN 20 – Tagged, User VLAN
172.16.20.0/24

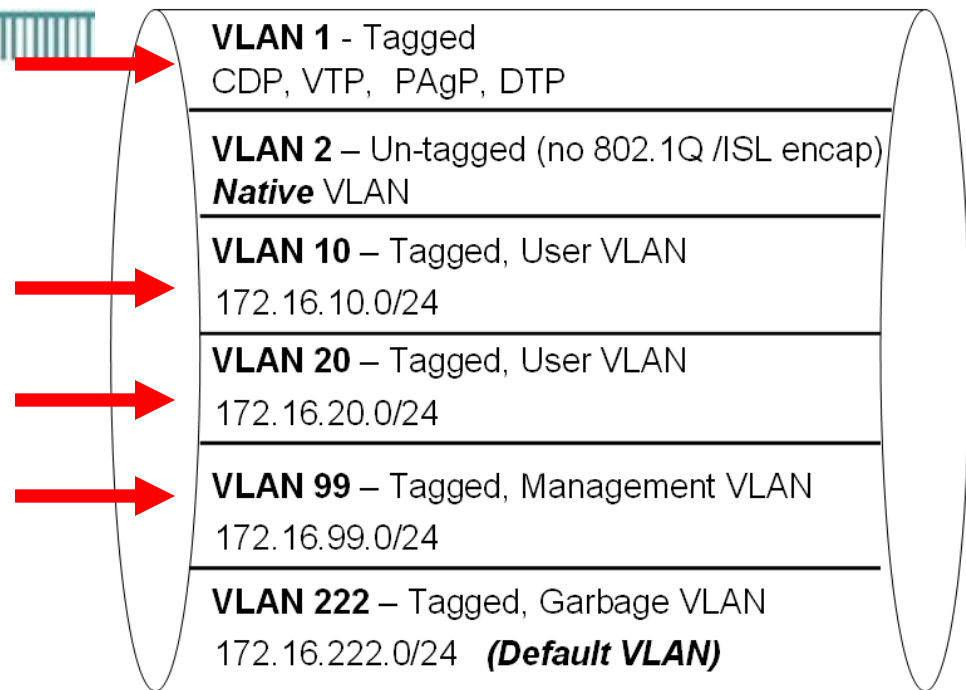
VLAN 99 – Tagged, Management VLAN
172.16.99.0/24

VLAN 222 – Tagged, Garbage VLAN
172.16.222.0/24 (**Default VLAN**)

```
DLS2 (config) # interface range fa 0/1 - 24
DLS2 (config-if) # switchport mode access
DLS2 (config-if) # switchport access vlan 222
```

- Garbage VLAN (Quarantined)
 - This is the VLAN you can assign to all switch ports until it is assigned to a user or management VLAN.
 - A way of isolating or managing all non-business traffic.
 - You may wish to limit this VLAN as an access port and not include this VLAN across trunk links.

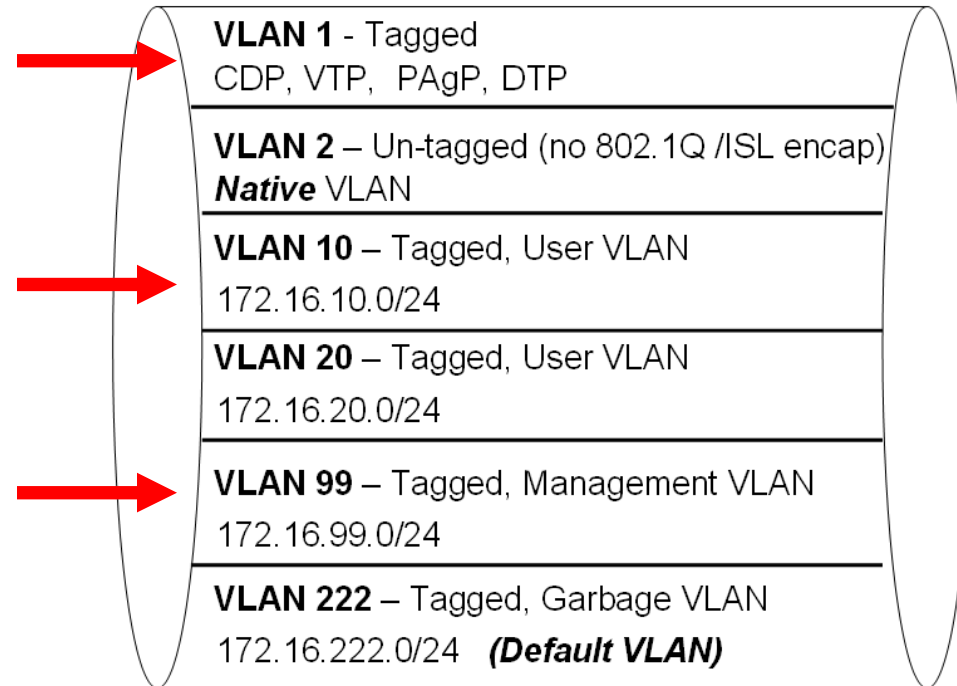
Best Practices



```
DLS2 (config) # interface fa 0/11
DLS2 (config-if) # switchport trunk allowed vlan 1, 10-99
DLS2 (config-if) # switchport trunk allowed vlan remove 20
```

- Limiting VLANs on a trunk
 - You can manually configure which VLANs should be allowed on a trunk.
 - If you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, CDP, PAgP, LACP, DTP and VTP in VLAN 1.
 - Sometimes done to reduce the risk of VLAN 1 STP loops or storms usually due to misconfiguration. (CCIE stuff)

Best Practices



```
DLS2(config)# interface fa 0/11
DLS2(config-if)# switchport trunk encapsulation dot1q
DLS2(config-if)# switchport mode trunk
DLS2(config-if)# switchport trunk native vlan 2
DLS2(config-if)# switchport trunk allowed vlan 1, 10-99
DLS2(config-if)# switchport trunk allowed vlan remove 20
```

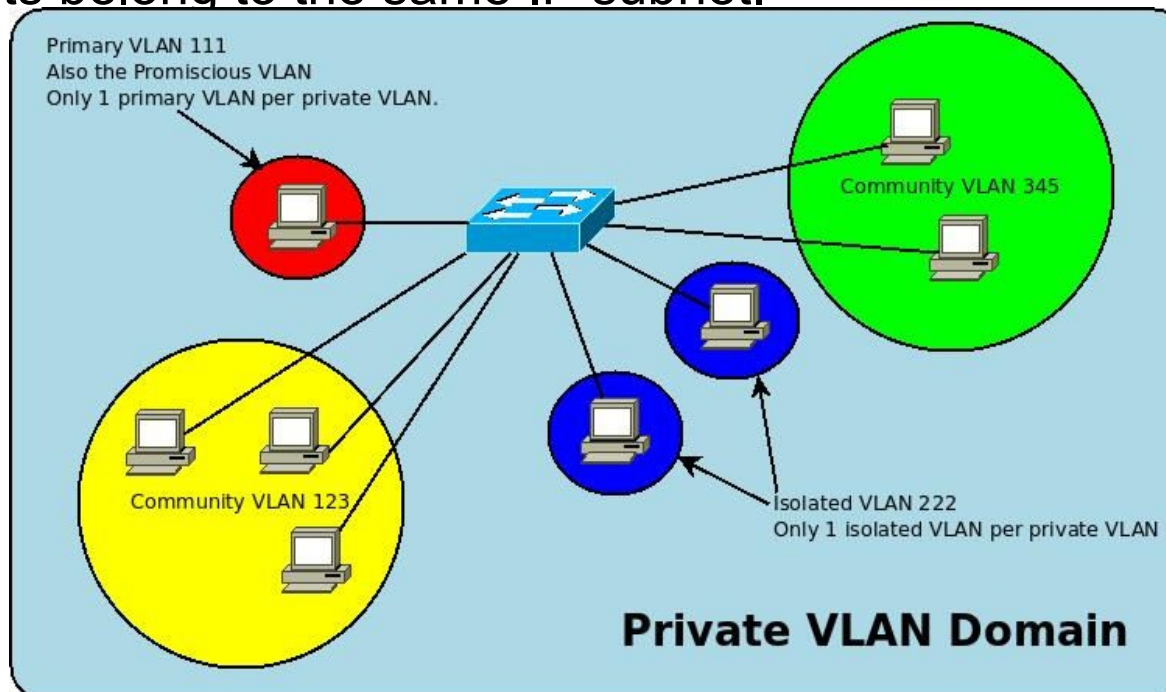
- Looking at a complete configuration for a trunk link

Private VLAN

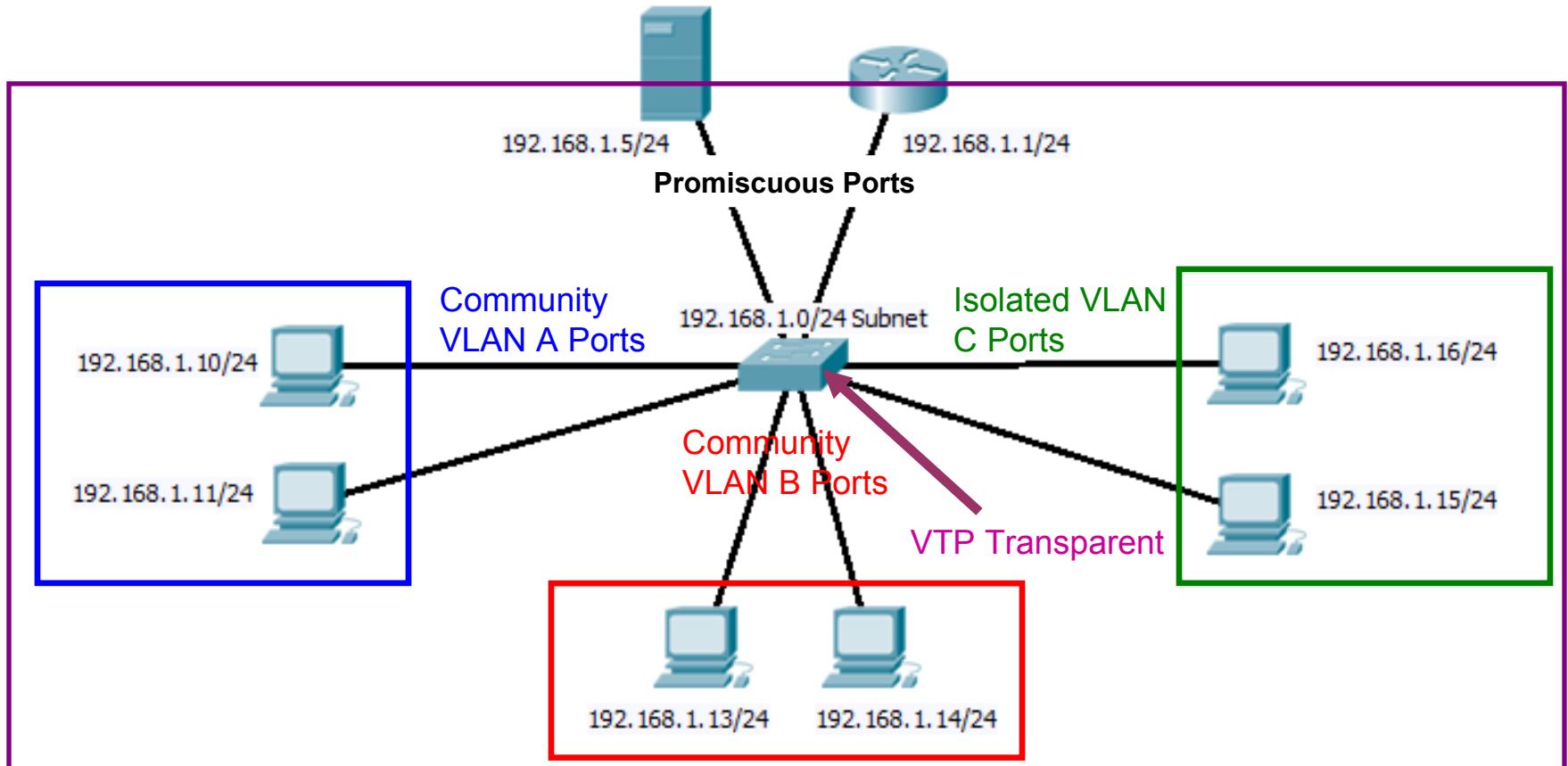


Motivation for Private VLANs

- Service providers often have devices from multiple clients, in addition to their own servers, in a single Demilitarized Zone (DMZ) segment or VLAN. As security issues abound, it becomes more important to provide traffic isolation between devices, even though they might exist on the same Layer 3 segment (and perhaps even the same VLAN).
- Most Cisco IOS-based switches implement private VLANs to keep some switch ports shared and some switch ports isolated, even though all ports belong to the same IP subnet.

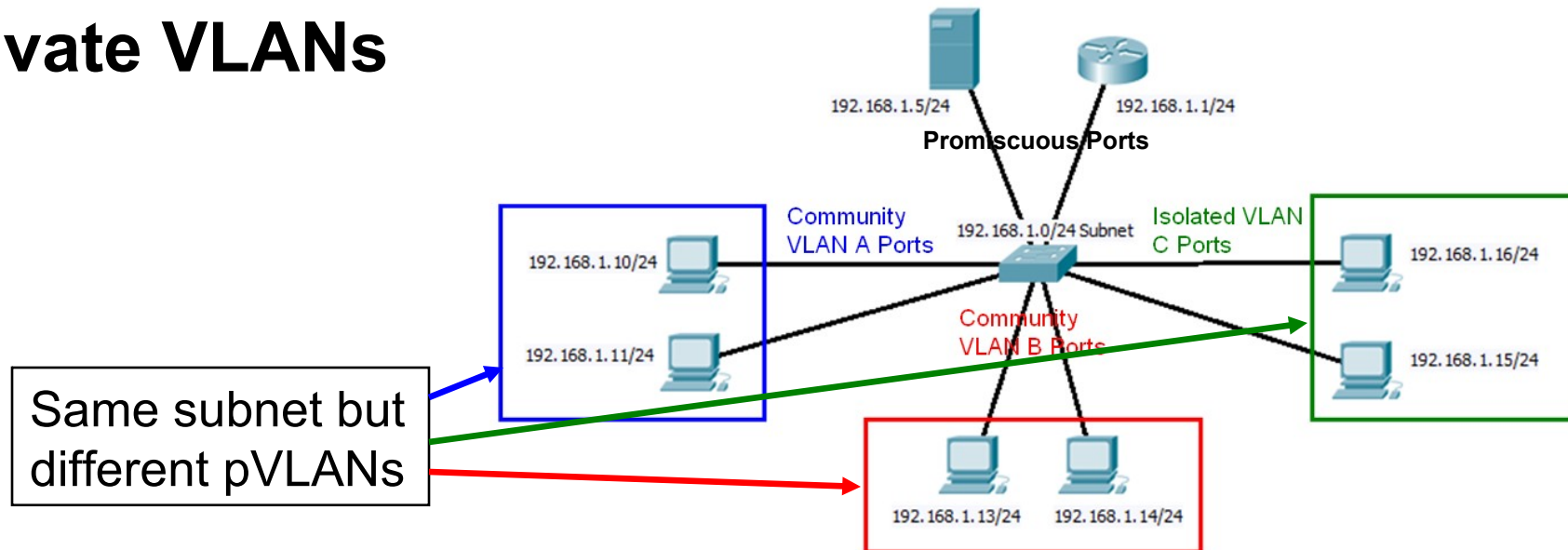


Private VLANs



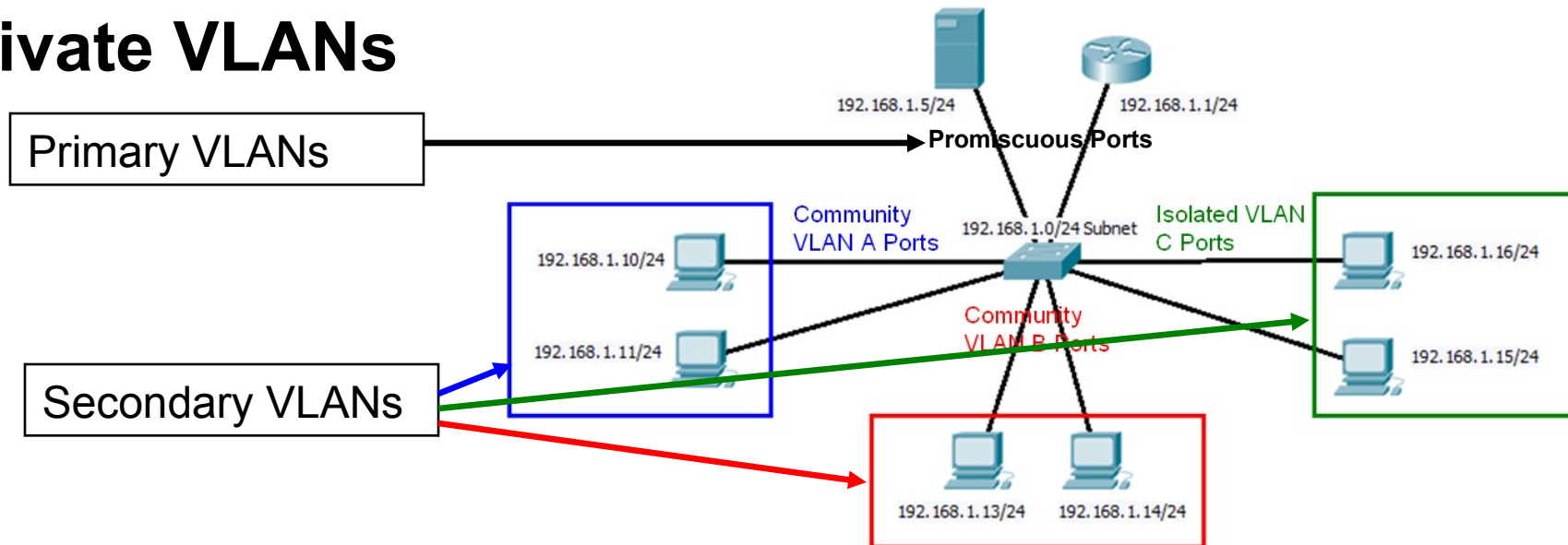
- Private VLANs (pVLAN) provide L2 isolation between ports, even within the same VLAN.
- pVLANs require VTP v2 switches to be in transparent mode.
- pVLANs can traverse trunks.

Private VLANs



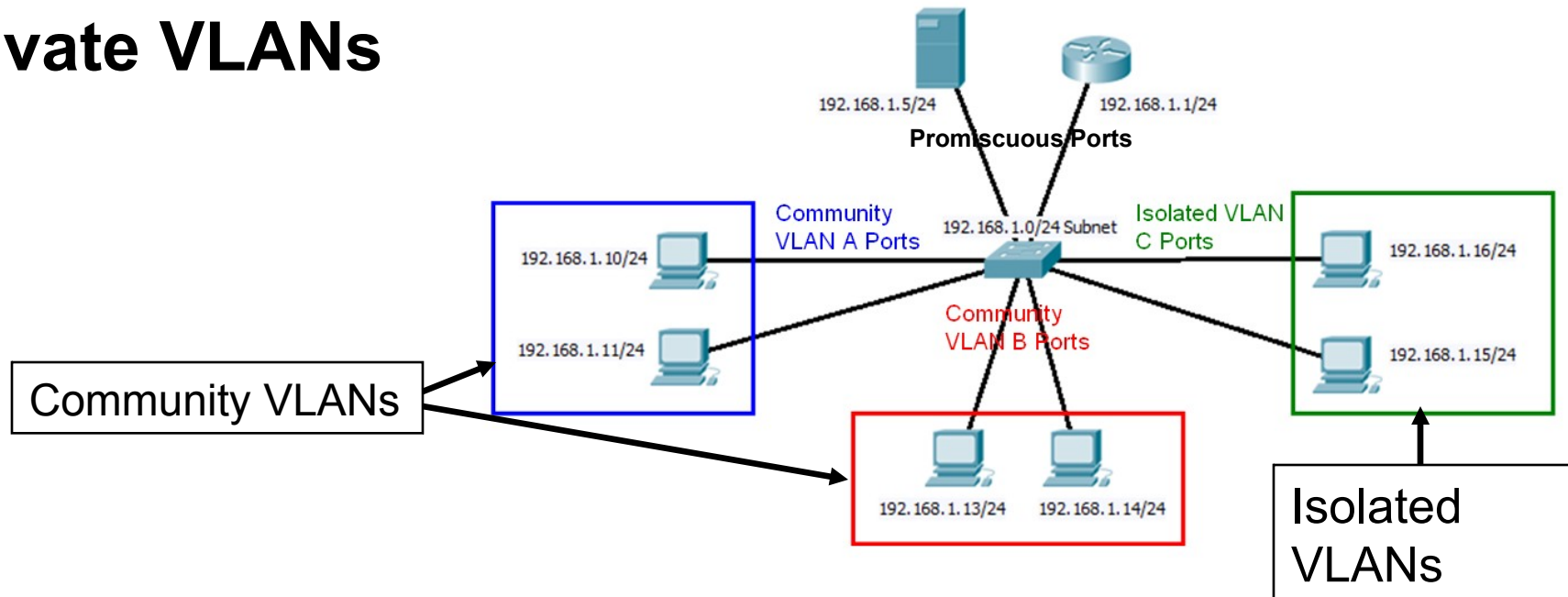
- pVLANs:
 - Provide improved security (through isolated frame delivery)
 - Reduce the number of IP subnets
- Service providers use pVLANs to deploy hosting services and network access where all devices reside in the same subnet but only communicate directly (at L2) to a restricted set of hosts (e.g. default gateway, on-segment servers, other hosts in its identified *subdomain*). All other communications must be *routed*.

Private VLANs



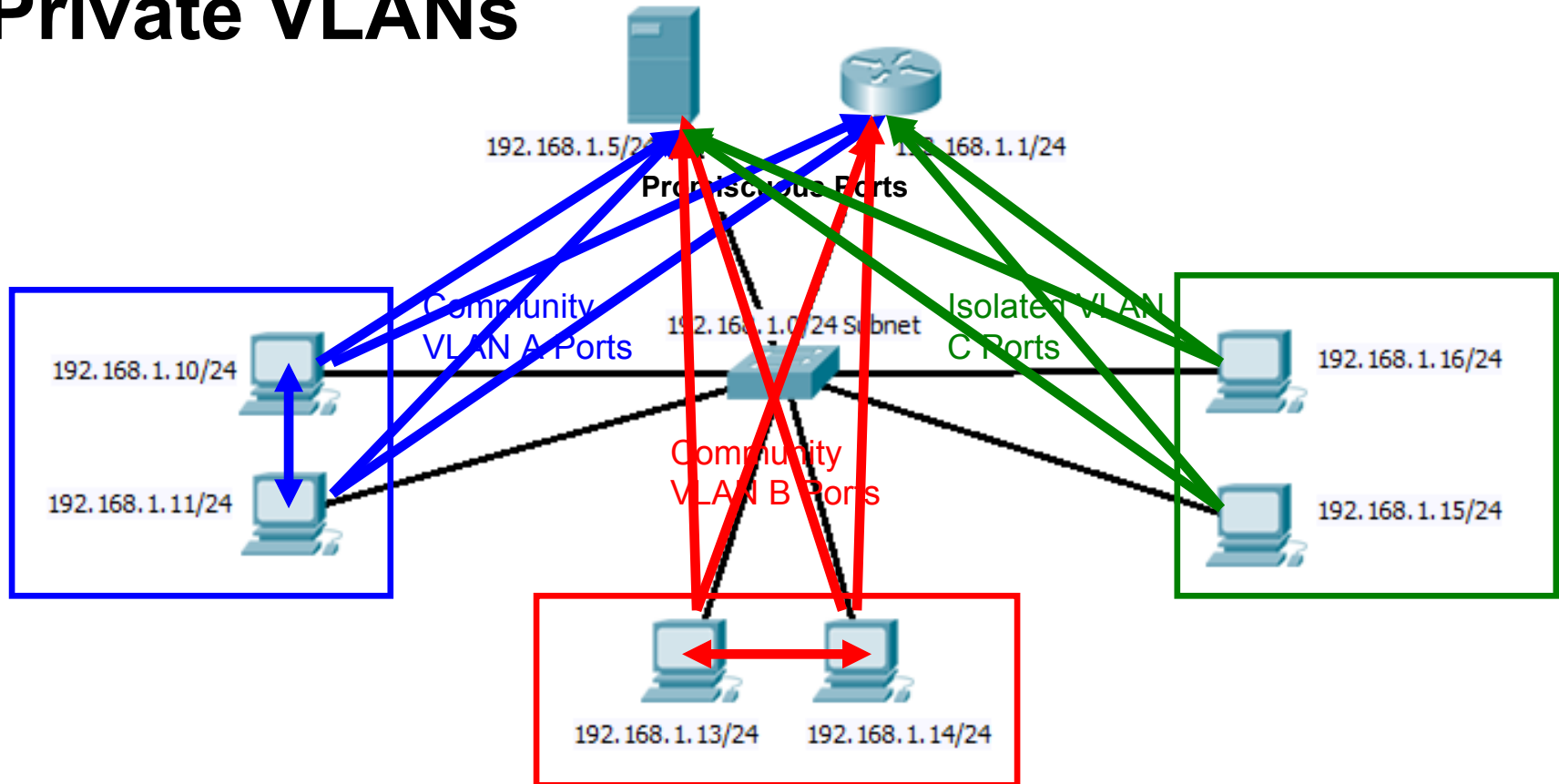
- pVLANs consist of two types of supporting VLANs:
 - **Primary VLAN**
 - High-level VLAN
 - Can have many secondary VLANs
 - Secondary VLANs belong to same subnet as Primary VLAN
 - **Secondary VLAN**
 - Child to a Primary
 - non-promiscuous end devices connect to a secondary VLAN

Private VLANs



- Two types of secondary VLANs:
 - **Community VLANs**
 - These ports communicate with other ports in the same community and promiscuous ports.
 - **Isolated VLANs**
 - These ports can only communicate with promiscuous ports.
 - Maximum of one isolated VLAN associated with a Primary VLAN.

Private VLANs



- Community VLAN ports communicate with other ports in the same community and promiscuous ports.
 - What devices can **Community VLAN A** PCs communicate with?
 - What devices can **Community VLAN B** PCs communicate with?
- Isolated VLANs ports can only communicate with promiscuous ports.
 - What devices can **Isolated VLAN C** PCs communicate with?

Implementing pVLANs

- not available on the C29xx platform
 - use Cisco’s “Feature Navigator” to determine which platforms support any needed feature
 - <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>
- pVLAN implementation and configuration commands (and options) vary greatly between platforms
 - download the command reference and/or configuration guide associated with your platform(s) from cisco.com
 - if you don’t already have a CCO account, you should
- where a command parameter is a list of VLAN IDs:
 - a single value can be specified (e.g. 100)
 - multiple values separated by commas, with some platforms disallowing spaces (e.g. 100,101,104)
 - a range can be specified using a hyphen (e.g. 100-105)

Configuring pVLANs – Steps (For Lab 6-3)

- **Step 1.** Set VTP mode to transparent.
- **Step 2.** Create the secondary pVLANs.
- **Step 3.** Create the primary pVLAN.
- **Step 4.** Associate the secondary pVLAN with the primary pVLAN.
 - Only one isolated pVLAN can be mapped to a primary pVLAN, but more than one community pVLAN can be mapped to a primary pVLAN.
- **Step 5.** Configure interfaces that are isolated or community ports.
- **Step 6.** Associate the isolated ports and community ports with their corresponding primary-secondary pVLAN pair.
- **Step 7.** Configure interfaces that are promiscuous ports.
- **Step 8.** Map the promiscuous ports to the secondary pVLANs with which they will communicate.
- **Step 9.** Create all primary and secondary pVLANs on any intervening switches that may be traversed, even if they contain no pVLAN ports.

Configuring pVLANs – Command Summary

- Create private VLANs (primary & secondaries)

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

```
Switch(config-vlan)# private-vlan {community | isolated | primary}
```

- Associate primary VLAN to all secondary VLANs

```
Sw(config)# vlan primary-vlan-id
```

```
Sw(config-vlan)# private-vlan association [add | remove] secondary-vlan-list
```

- If L3 switching, map primary VLAN SVI to all secondary VLANs

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

```
Switch(config-if)# private-vlan mapping [add | remove] secondary-vlan-list
```

- Configure switch ports where hosts will be connected

```
Switch(config)# interface type slot/port
```

```
Switch(config-if)# switchport ← if port defaults to L3 operation
```

```
Switch(config-if)# switchport mode private-vlan {host | promiscuous}
```

... for primary VLAN promiscuous ports, associate the list of reachable secondary VLANs

```
Switch(config-if)# switchport private-vlan mapping primary-vlan-id  
[add | remove] secondary-vlan-  
list
```

... for secondary VLAN ports, associate the primary VLAN

```
Switch(config-if)# switchport private-vlan host-association  
primary-vlan-id secondary-vlan-
```

Verifying pVLAN Configuration

- The two most useful commands for this purpose are **show vlan private-vlan** and **show interfaces *interface* switchport**.

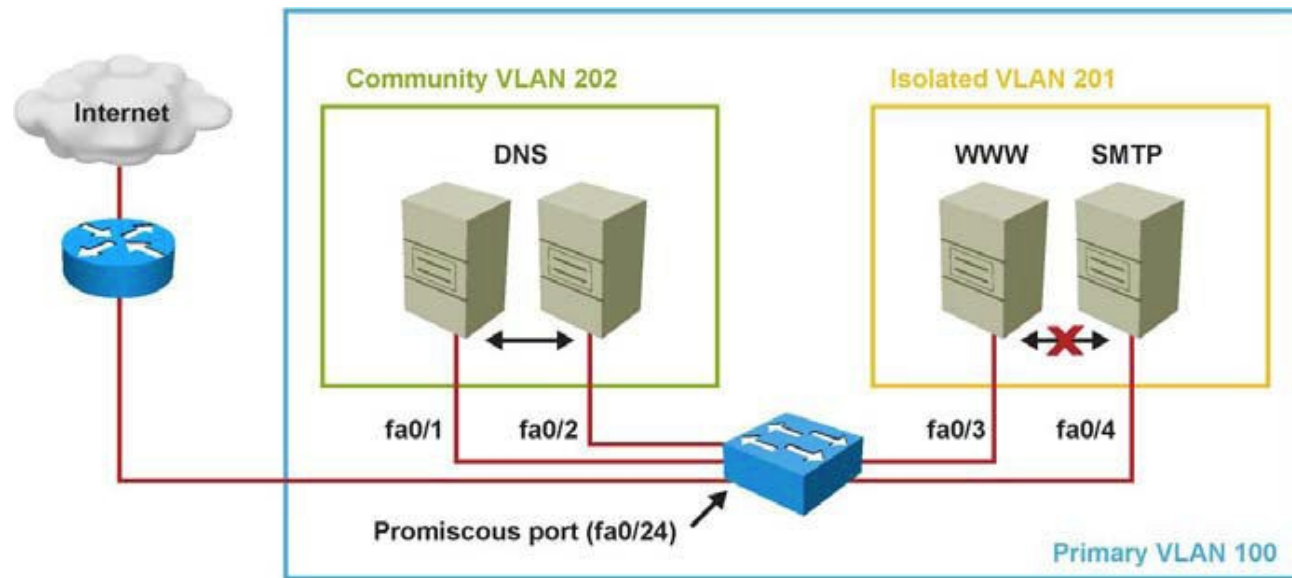
```
Switch# show vlan private-vlan
```

Primary	Secondary	Type	Interfaces
-----	-----	-----	-----
100	200	community	
100	300	isolated	Fa5/2

```
Switch# show interfaces FastEthernet 5/2 switchport
```

```
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: 100 (VLAN0200) 300 (VLAN0300)
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

pVLAN Scenario 1: Single Switch



- A corporate DMZ contains two DNS servers, one web server and one SMTP server. All servers and their connecting router are in the same subnet.
- DNS servers are redundant copies, so they need to communicate with each other to update their entries and to the Internet. In addition to that, they also need to communicate with the Internet.
- The Web Server and the SMTP server needs to communicate with the Internet, but for security purposes, the SMTP server should not be reachable from the Web or the DNS servers. The web server needs to be accessible from the Internet but not from the SMTP server.

pVLAN Configuration for Scenario 1

```
Switch(config)# vtp mode transparent      VTP transparent needed for pVLANs

Switch(config)# vlan 201                  configure secondary pVLANs
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan community

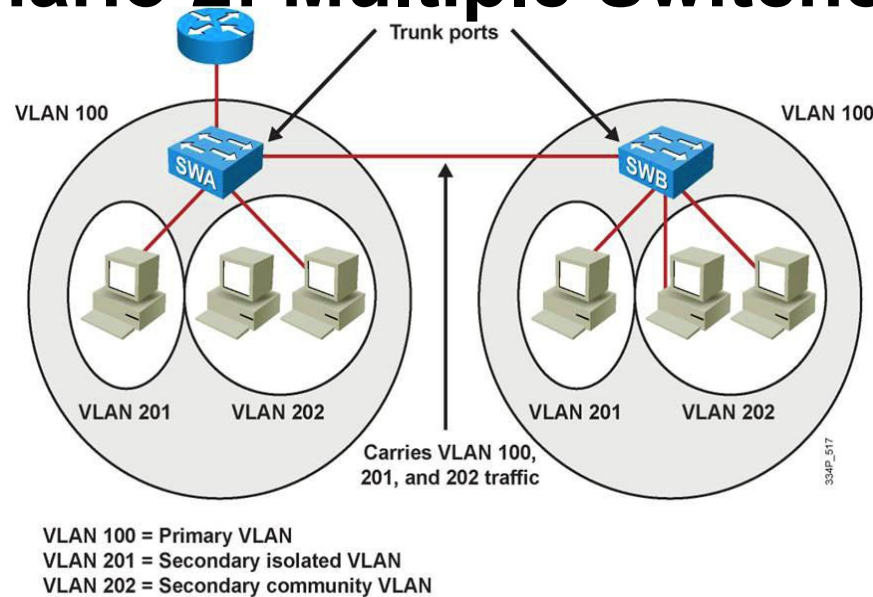
                                                configure primary pVLAN, associating secondaries
Switch(config-vlan)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 201,202

                                                promiscuous port on VLAN 100
Switch(config-vlan)# interface fastethernet 0/24
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100 201,202

                                                community ports on VLAN 202
Switch(config-if)# interface range fastethernet 0/1 - 2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 202

                                                isolated ports on VLAN 201
Switch(config-if)# interface range fastethernet 0/3 - 4
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 201
```

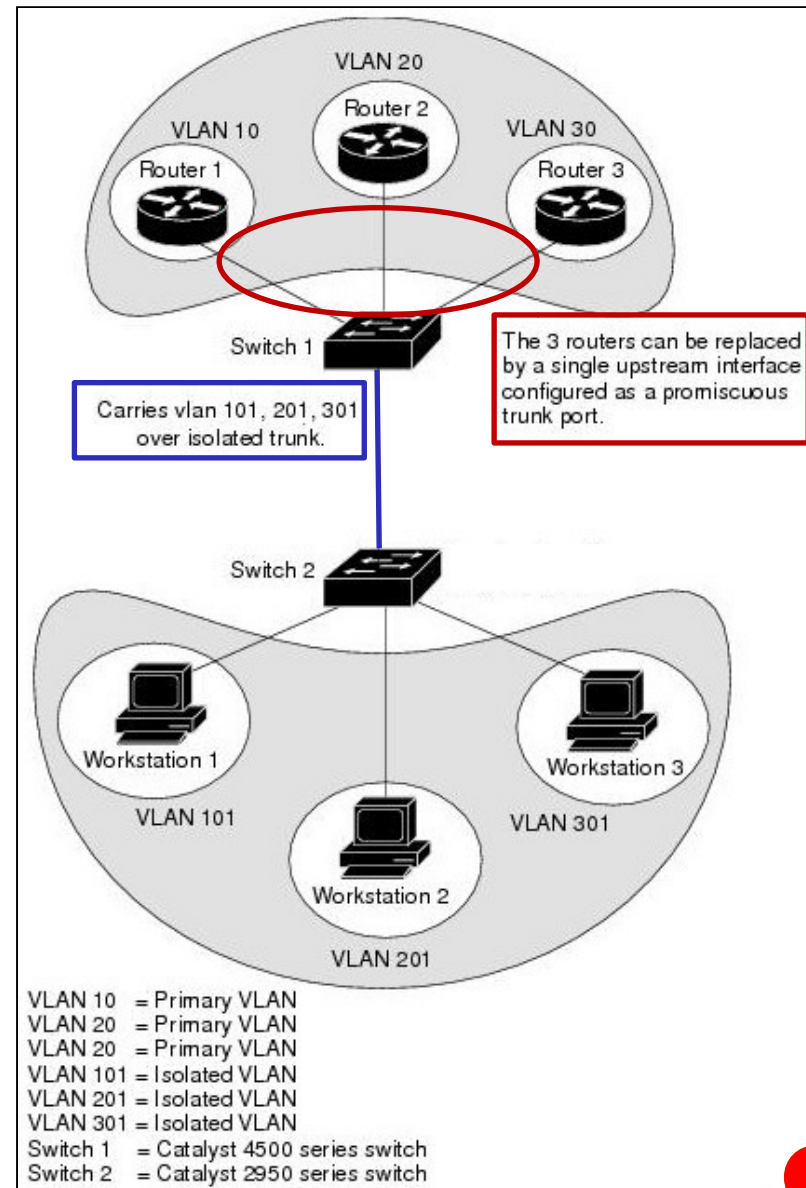
pVLAN Scenario 2: Multiple Switches



- A standard trunk port carries traffic for primary and secondary VLANs to a neighbouring switch just like any other VLAN. This is **NOT** a pVLAN trunk! (next)
- Frames on a trunk originating from a pVLAN host are tagged with the VLAN ID on which that host's switchport is configured (whether primary or secondary).
 - For example, from the rightmost host on SWB a frame sent to the router will be tagged with VLAN ID 202 across the trunk link, but the router's reply will be tagged with VLAN ID 100.
- A feature of pVLANs across multiple switches is that traffic from an isolated port in one switch does not reach an isolated port on another switch.
- Configure pVLANs on all switches along the path, including devices that have no pVLAN ports – this maintains the security of your pVLAN configuration.
 - But of course, do NOT associate ports to those VLAN IDs already configured as pVLANs!
 - It is recommended that all switches having pVLAN ports be contiguous, connected by trunks.

Private VLAN Trunk Links

- ... can be used to carry traffic for multiple pVLANs and non-pVLANs, concurrently.
- pVLAN trunk links are only supported on the Catalyst 4500 and 6500 series switches over 802.1q encapsulation.
- pVLAN trunk links can be configured as **isolated** or **promiscuous**.
- Isolated** (option: **trunk secondary**)
 - combines traffic for normal VLANs and all secondary pVLAN ports over a single link
 - useful for connecting to a downstream switch that does NOT support pVLANs
 - e.g. traffic for secondary pVLANs 101, 201, 301 from Switch 1 to Switch 2
- Promiscuous** (option: **trunk promiscuous**)
 - combines traffic for multiple promiscuous ports over a single link
 - useful for connecting to an upstream router that does NOT support pVLANs
 - e.g. traffic for primary pVLANs 10, 20, 30 from Switch 1 to a single router replacing Routers 1 through 3



pVLAN Trunk Configuration

- Identify the type of pVLAN trunk to be configured on the chosen interface:

```
Sw(config-if) # switchport mode private-vlan trunk  
                  { promiscuous | secondary }
```

- List each primary/secondary pVLAN pair to be carried:

```
Sw(config-if) # switchport private-vlan association trunk  
                  primary_vlan_ID secondary_vlan_ID
```

- If the port is set to promiscuous, use map each primary to its secondaries:

```
Sw(config-if) # switchport private-vlan mapping  
                  primary_vlan_ID secondary_vlan_list
```

- Specify the VLAN IDs allowed on the trunk:

```
Sw(config-if) # switchport private-vlan trunk allowed vlan vlan_list
```

- Configure the native VLAN:

```
Sw(config-if) # switchport private-vlan trunk native vlan vlan_id
```

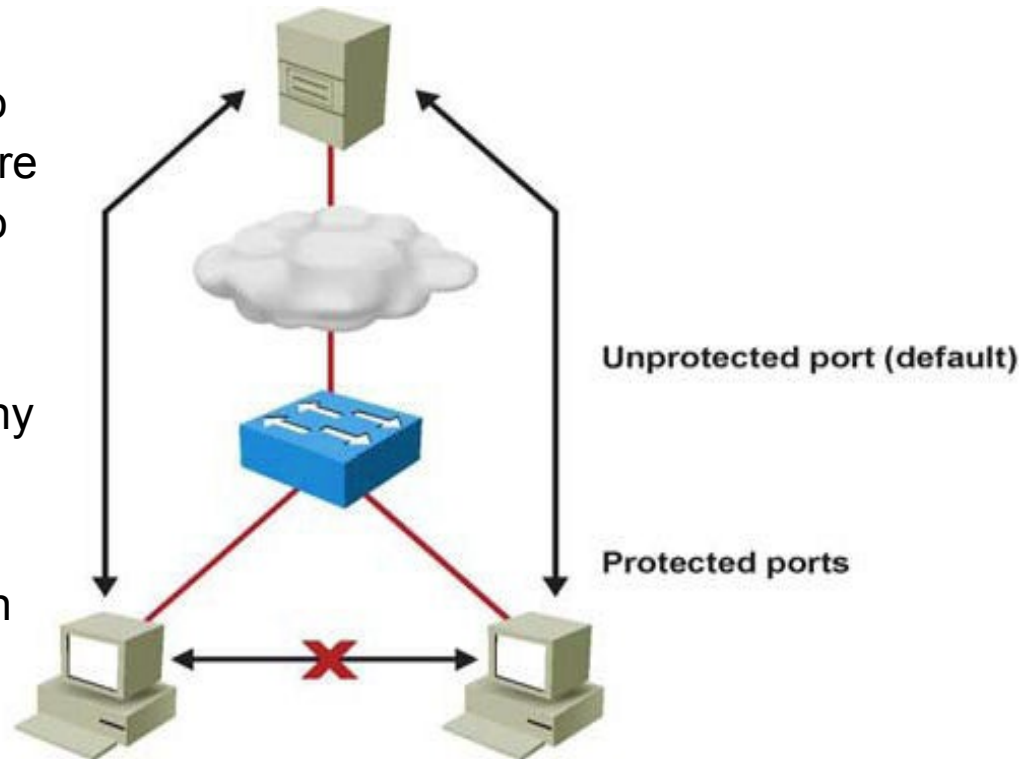
```
Switch(config) # interface fastethernet 5/2  
Switch(config-if) # switchport mode private-vlan trunk secondary  
Switch(config-if) # switchport private-vlan trunk native vlan 10  
Switch(config-if) # switchport private-vlan trunk allowed vlan 10,3,301-302  
Switch(config-if) # switchport private-vlan association trunk 3 301  
Switch(config-if) # switchport private-vlan association trunk 3 302
```

pVLAN Trunk Verification

```
Switch# show interfaces fastethernet 5/2 switchport
Name: Fa5/2
Switchport: Enabled
Administrative Mode: private-vlan trunk secondary
Operational Mode: private-vlan trunk secondary
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: 10
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations:
3 (VLAN0003) 301 (VLAN0301)
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Operational Normal VLANs: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

pVLAN Edge (Protected Port) Feature

- The PVLAN edge (protected port) feature has only local significance to the switch (unlike pVLANs), and there is no isolation provided between two protected ports located on different switches.
- A protected port does not forward any traffic to any other port that is also a protected port on the same switch.
- Traffic cannot be forwarded between protected ports at L2; all traffic passing between protected ports must be forwarded through an L3 device.



```
Switch(config-if) # switchport protected
```