VLANs and Inter-VLAN Routing

SDC, CNW(CSE 4541)

Department of Computer Science & Engineering
ITER, Siksha 'O' Anusandhan Deemed To Be University
Jagamohan Nagar, Jagamara, Bhubaneswar, Odisha - 751030

Book(s)

Text Book(s)

Glen E. Clarke, Richard Dea

CCT/CCNA Routing and Switching

Complete Study Guide: Exam 100-490
Exam 200-301

McGraw-Hill Education

Todd Lammle

CCNA Routing and Switching

Complete Study Guide: Exam 100-105
Exam 200-105
Exam 200-125

SYBEX Publication

Talk Flow

Recap: Collision Domain and Broadcast Domain

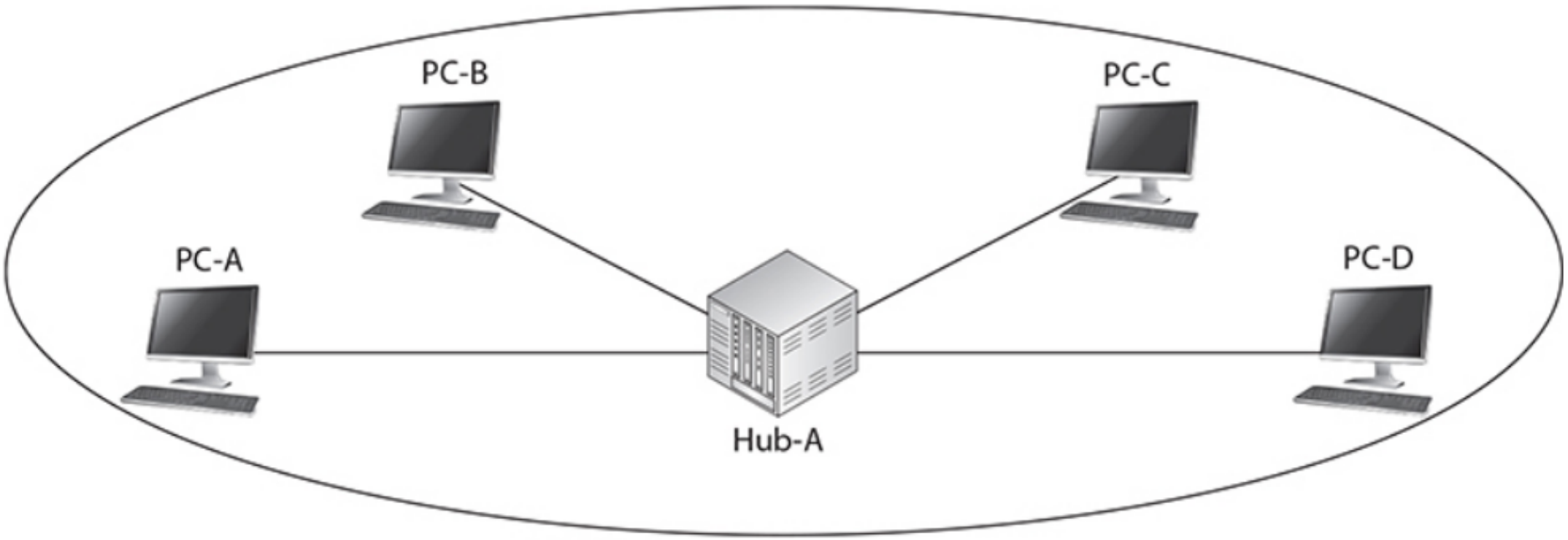

Figure 1: Find out the Collision and Broadcast domain

Recap: Collision Domain and Broadcast Domain

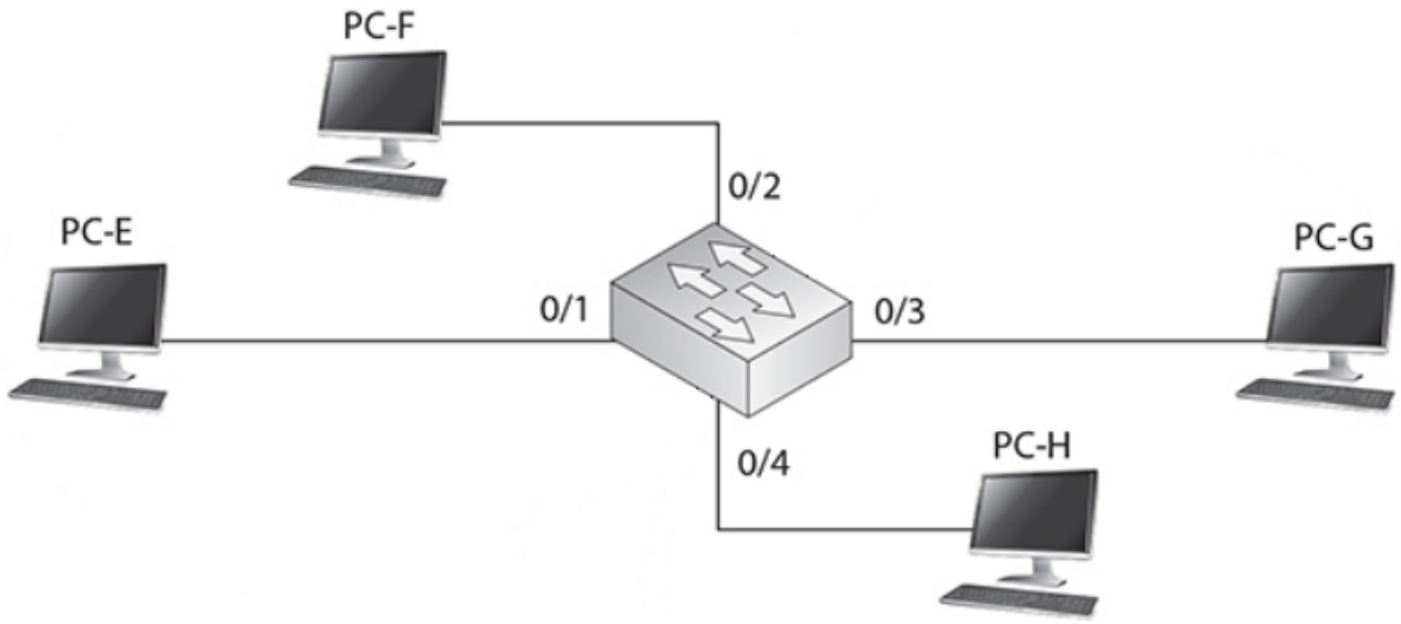

Figure 2: Find out the Collision and Broadcast domain

Recap: Collision Domain and Broadcast Domain

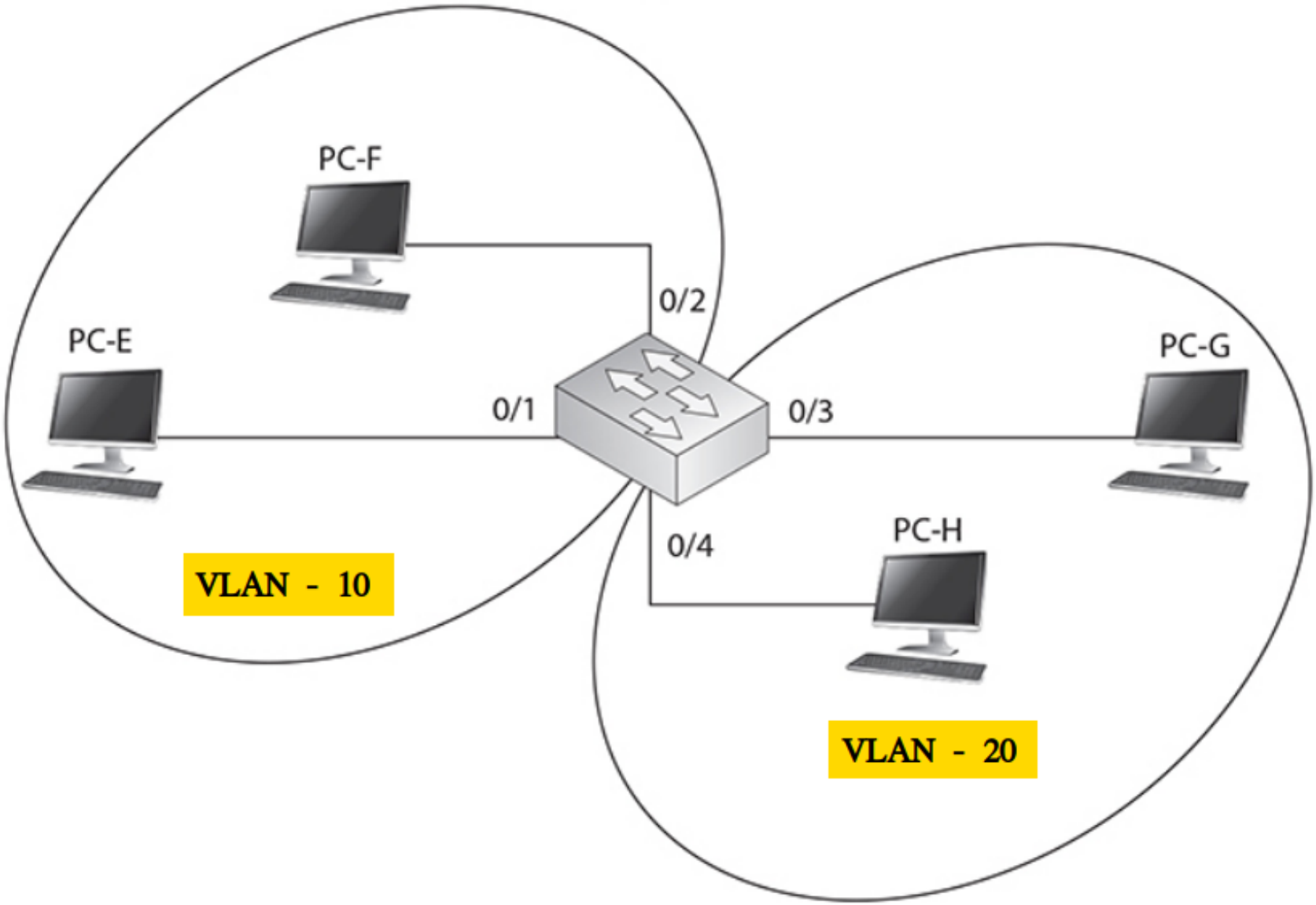

Figure 3: Find out the Collision and Broadcast domain

VLAN Basics

Definition

A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch.

- When you create VLANs, you can create smaller broadcast domains within a layer 2 switched inter-network by assigning different ports on the switch to service different sub-networks.
- Switches are used to create VLANs, or separate broadcast domains.
- VLANs are not restricted to any physical boundary in the switched network, assuming that all the devices are interconnected via switches and that there is no intervening layer 3 devices.
- VLAN could be spread across multiple switches or contained in the same switch.

A VLAN through multiple and single Switch

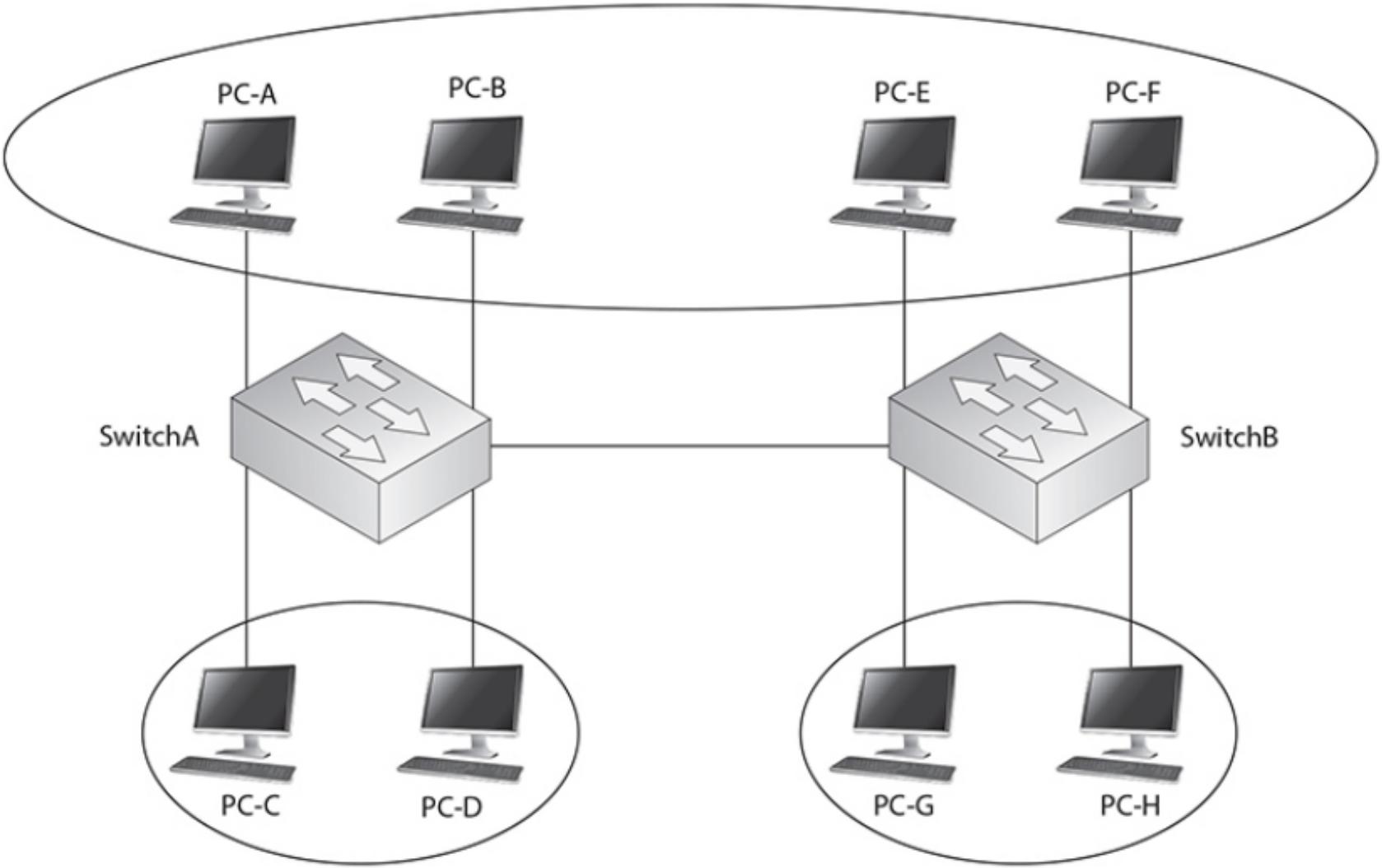

Figure 4: A VLAN through multiple and single Switch

Are VLAN and subnet same?

- Logically, Yes.
- A subnet, or a network, is a contained broadcast domain. A broadcast that occurs in one subnet will not be forwarded, by default, to another subnet.
- Each of these separate broadcast domains is a separate VLAN.
- To move from one network number to another, we need a router. (Inter-VLAN communication).

Logical topology using VLANs

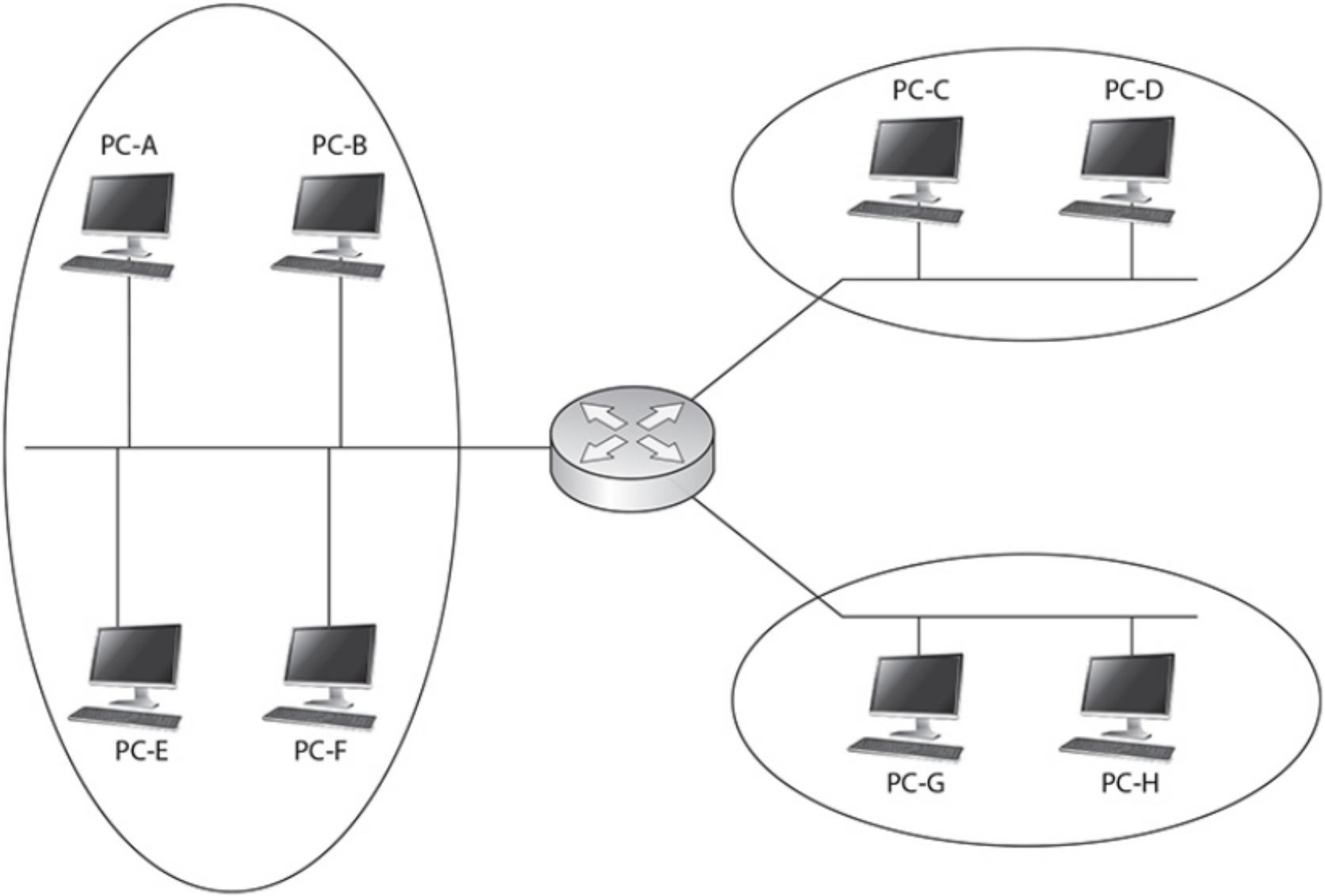

Figure 5: Logical topology using VLANs

Advantages of VLAN

- Broadcast Control - VLAN controls the broadcast domain.
- Security - VLAN imposes security on Switch, Inter-VLAN communication can be done only after proper configurations,
- Scalability -
  - VLANs increase your network's scalability by segmenting broadcast domains.
  - VLANs are a logical construct; a user can be located anywhere in the switched network and still belong to the same broadcast domain.
  - If you move a user from one switch to another switch in the same switched network, you can still keep the user in his or her original VLAN.

VLAN Membership

- Static VLAN - In Static VLAN, we must manually assign a port on a switch to a VLAN using an interface subconfiguration mode command. VLANs configured in this way are typically called port-based VLANs.
  —If we are using static VLANs, not only we have to configure the switch port manually with this updated information, but, if we move the user from one switch to another, we will also have to perform this manual configuration to reflect the user's new port.
- Dynamic VLAN - With dynamic VLANs, the switch automatically assigns the port to a VLAN using information from the user device, such as its MAC address, IP address, or even directory information (a user or group name, for instance).
  —The switch then consults a policy server, called a VLAN membership policy server (VMPS), which is proprietary to Cisco and contains a mapping of device information to VLANs.
- Voice VLAN - Voice VLANs are unique. They are associated to ports that have VoIP phones attached.

VLAN Basic Configuration

Create VLAN

```
Switch(config)#vlan 10
Switch(config-vlan)#name HR
Switch(config-vlan)#exit
Switch(config)#
```

Display VLAN

```
Switch#sh vlan
```

*Execute the above command and find out the outcome.

*How many total VLAN can be seen? why such so?

VLAN Connections

- On dealing with VLANs, switches support two types of switch ports:
  - Access Ports - Access port connections can be associated only with a single VLAN (voice VLAN ports are an exception to this). Any device or devices connected to this port will be in the same broadcast domain.
  - Trunk Ports - Trunk ports are capable of carrying traffic for multiple VLANs and are configured on ports that are connecting to other switches/routers.
- We must know about the connection of interface and should configure it properly.

Access Ports

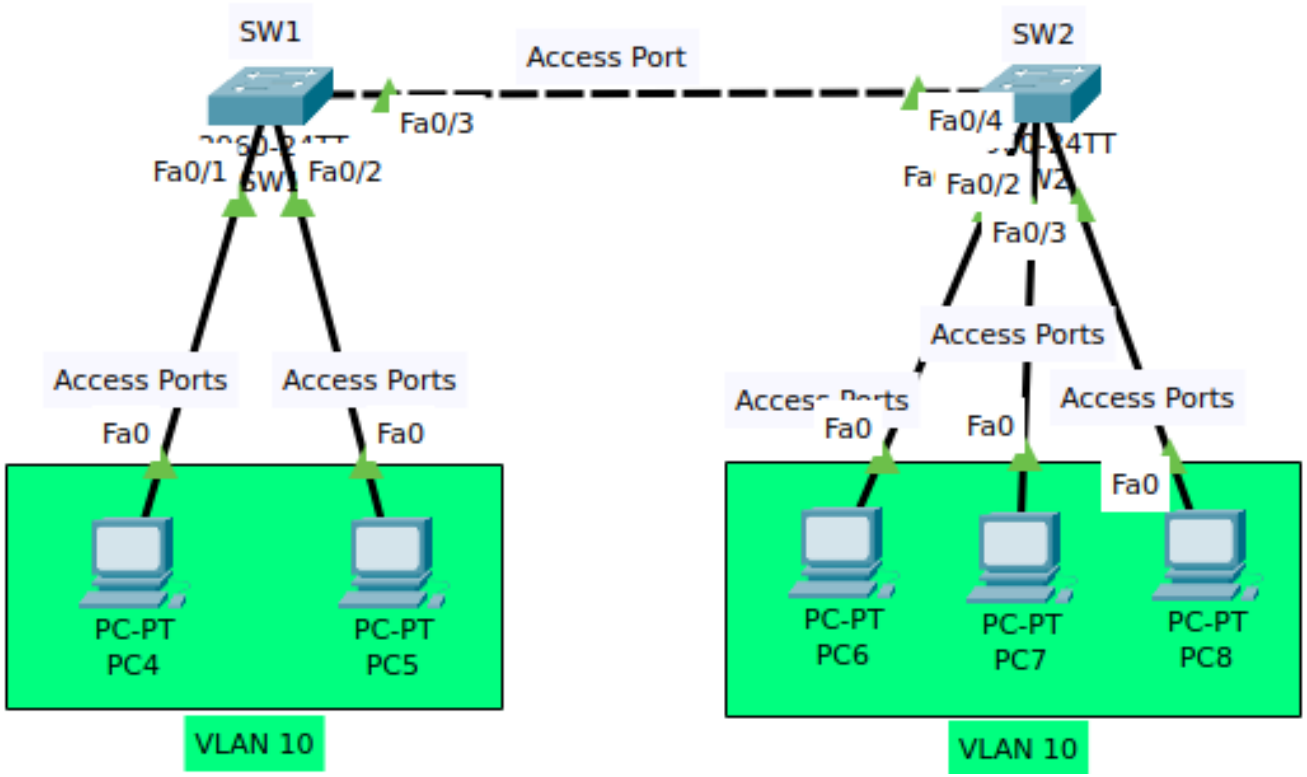

Figure 6: All PC belong to same VLAN, Fa 0/3 on SW1 should be connected via access port

*Examine what will happen if PC6 doesn't belong to VLAN 10? Consider it is in default VLAN.

*Examine what will happen if PC5 and PC6 belong to Other VLAN, say 20?

Access Ports (Configuration)

With one interface at a time

```
SW1(config)#int fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

With multiple interfaces at a time

```
SW2(config)#int range fastEthernet 0/1-4
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 10
SW2(config-if)#ex
```

Multiple VLAN with Access Ports

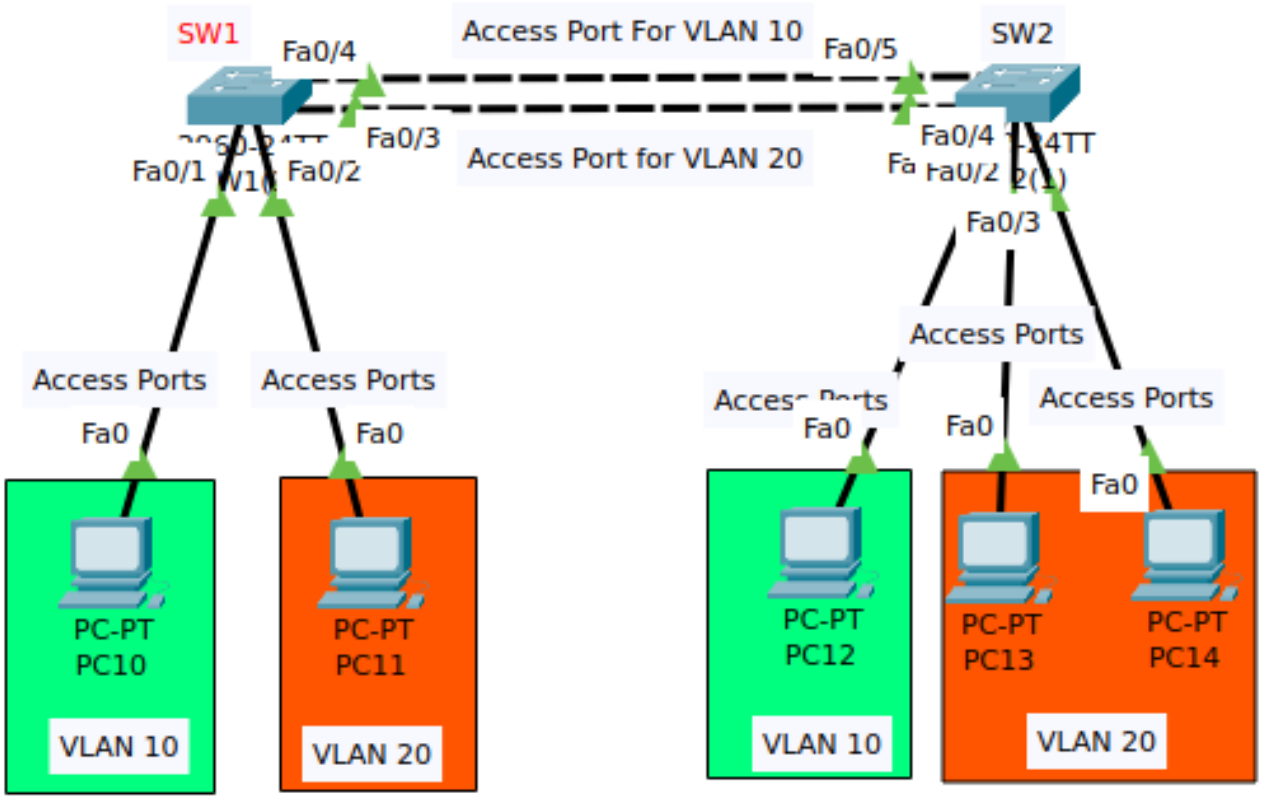

Figure 7: Multiple VLAN with Access Ports

Is it a feasible solution having multiple link between switches?

Trunk Ports

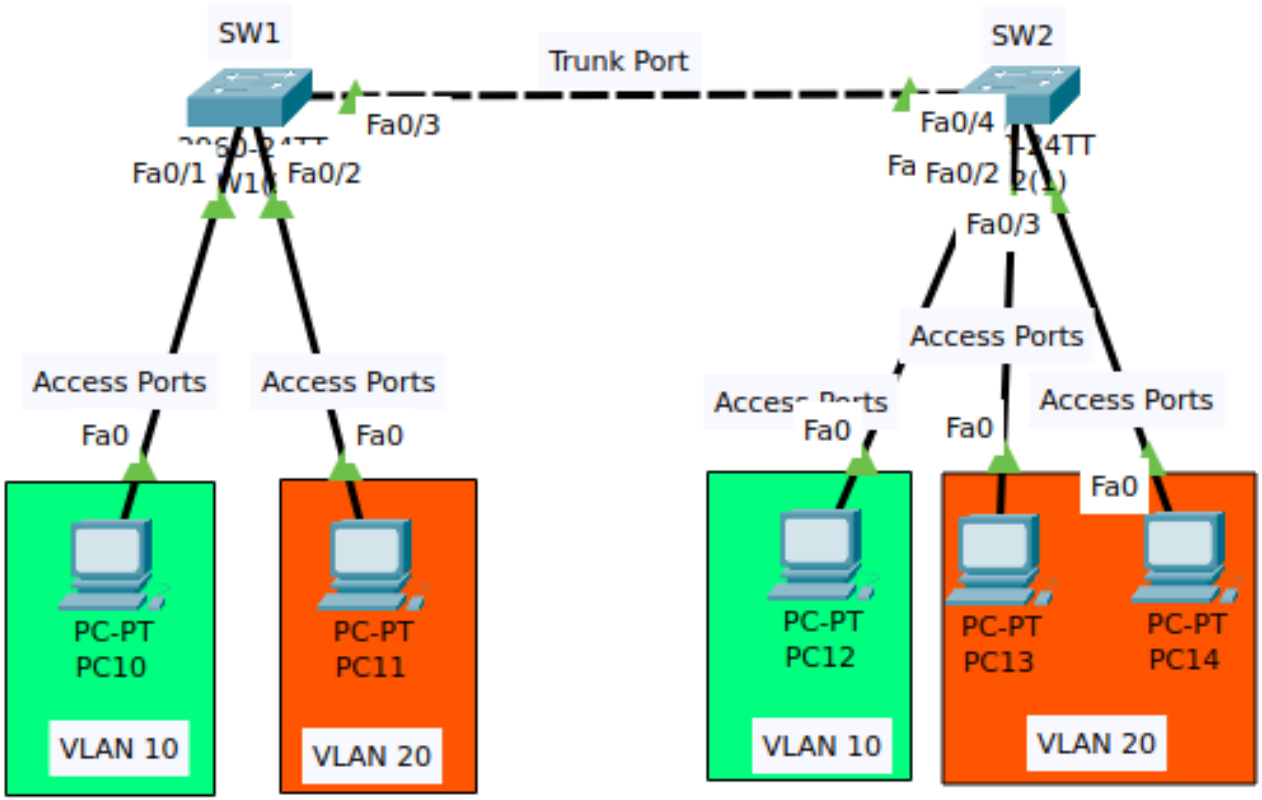

Figure 8: All PC are not in same VLAN, Fa 0/3 on SW1 must be connected via trunk port

Trunk Ports (Configuration)

Change PC-11 in VLAN 20

```
SW1(config)#vlan 20
SW1(config-vlan)#name Admin
SW1(config-vlan)#ex
SW1(config)#int range fastEthernet 0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
```

*Do the same for PC13 and PC14

Set Fa0/3 of SW1 as Trunk Port

```
SW1(config)#int fastEthernet 0/3
SW1(config-if)#switchport mode trunk
```

*Do we need to set Fa0/4 of SW2 as trunk port?

Trunk Tagging

Trunking methods create the illusion that instead of a single physical connection between the two trunking devices, a separate logical connection exists for each VLAN between them. When trunking, the switch adds the source port's VLAN identifier to the frame so that the device (typically a switch) at the other end of the trunk understands what VLAN originated this frame and the destination switch can make intelligent forwarding decisions on not just the destination MAC address, but also the source VLAN identifier.

Default Tag Frame: 802.1Q (in short we call this as dot1Q)

Troubleshooting Trunk ports

Execute the following commands and find out the outcomes.

- SW1# sh interfaces fastEthernet 0/3
- SW1# sh interfaces fastEthernet 0/3 ?
- SW1# sh interfaces fastEthernet 0/3 switchport
- SW1# sh interfaces trunk

Inter VLAN communication

Hosts in a VLAN live in their own broadcast domain and can communicate freely. VLANs create network partitioning and traffic separation at layer 2 of the OSI.

By default devices within different VLANs can not communicate due to separate broadcast domain. However, inter VLAN communication can be achieved by including layer 3 devices such as router, layer 3 switch.

Types of inter VLAN communication

We can achieve inter VLAN communication in three ways -

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

Legacy Inter-VLAN Routing

For each VLAN there will be dedicated access port from layer 3 device (router) to layer 2 device (switch).

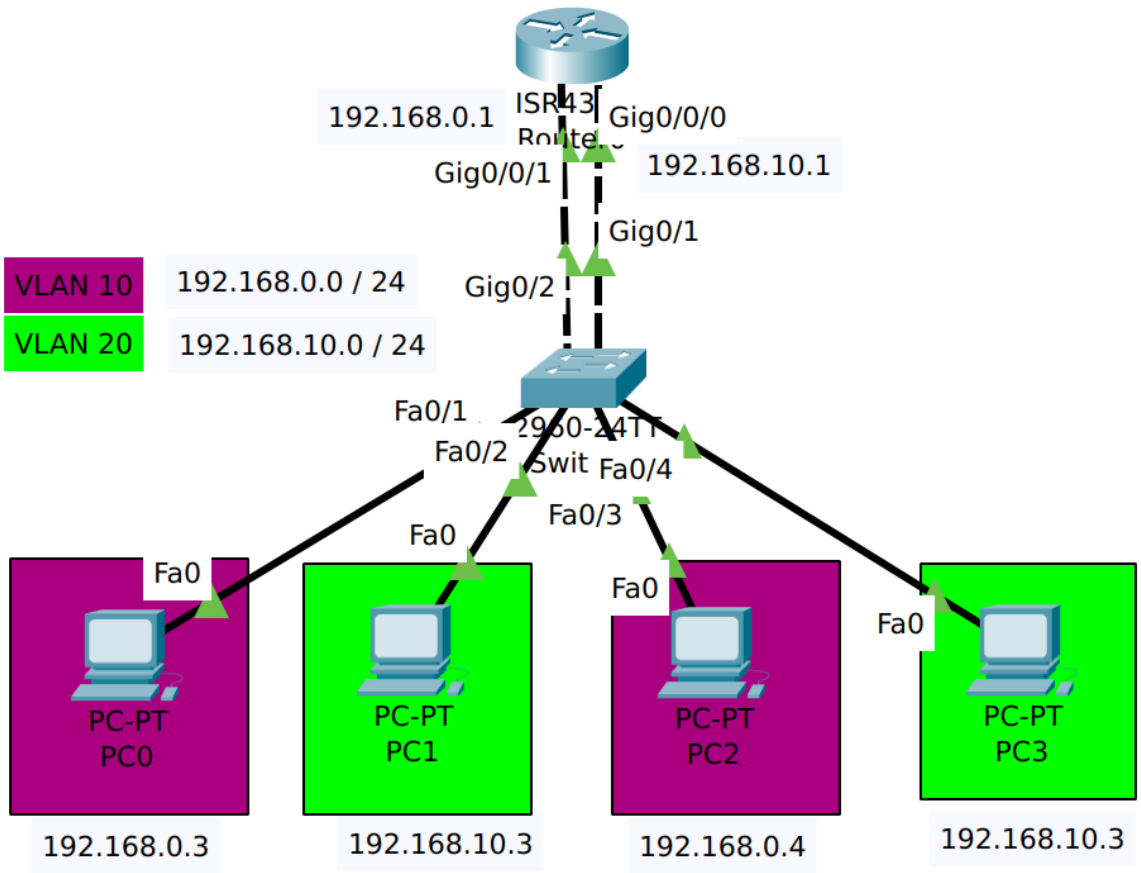

Figure 9: Legacy Inter-VLAN Routing.

Cable Configuration

Interface	VLAN	Port Type
Fa0/1	10	Access
Fa0/2	20	Access
Fa0/3	10	Access
Fa0/4	20	Access
Gig0/1	10	Access
Gig0/2	20	Access
Gig0/0/0	–	No Switchport
Gig0/0/1	–	No Switchport

VLAN database in devices

Device	VLANs
SW	10, 20
R	–

Legacy Inter-VLAN Routing (Configuration)

Create VLAN & assign to interfaces

```
SW(config)#int range f0/1, f0/3, gig0/1
SW(config-if-range)#switchport mode access
SW(config-if-range)#switchport access vlan 10
```

Assign Default Gateway to router interfaces

```
R(config)#int gigabitEthernet 0/0/0
R(config-if)#ip address 192.168.0.1 255.255.255.0
R(config-if)#no sh
```

*Configure the other interfaces

Router-on-a-Stick (RoaS)

There will be only one link between switch (layer 2) and router (layer 3) for all VLANs as trunk port.

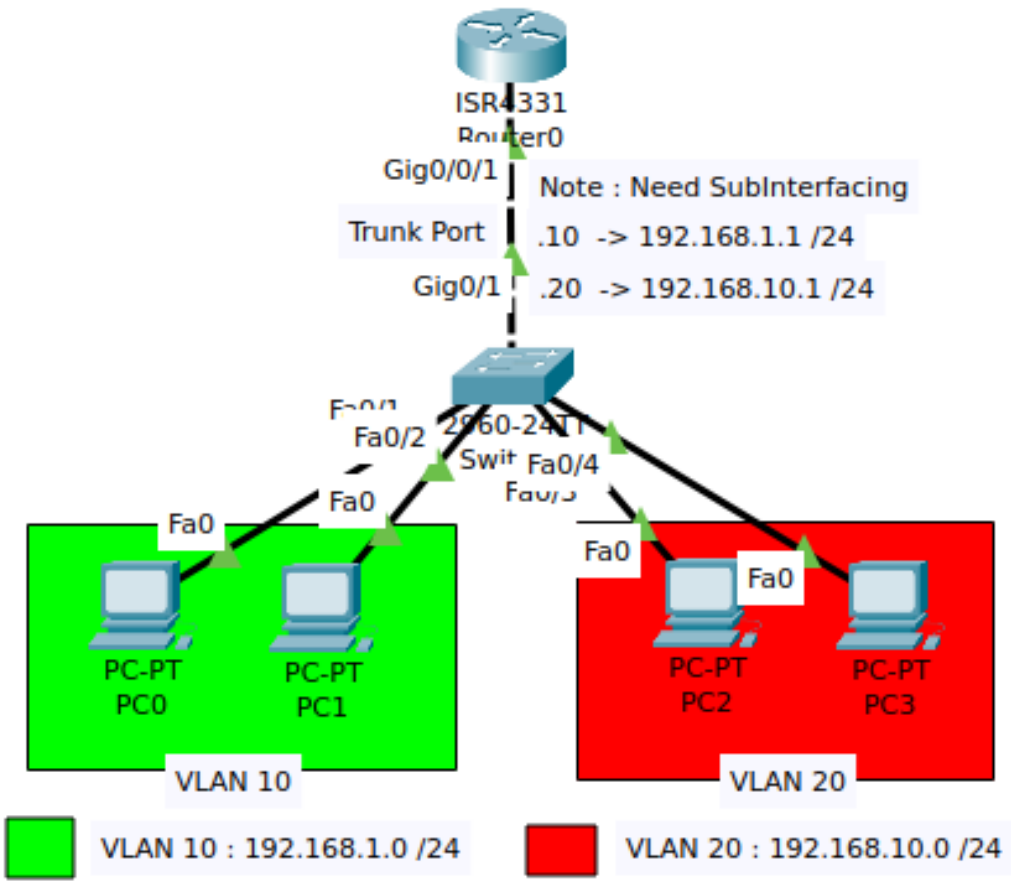

Figure 10: Router-on-a-Stick (RoaS).

Cable Configuration

Interface	VLAN	Port Type
Fa0/1	10	Access
Fa0/2	10	Access
Fa0/3	20	Access
Fa0/4	20	Access
Gig0/1	–	Trunk
Gig0/0/1	–	No Switchport

VLAN database in devices

Device	VLANs
SW	10, 20
R	-

Sub-interface

Sub interface

A subinterface is a virtual interface (L3 interface) created by dividing one physical interface (layer 3 device) into multiple (max 4094) logical interfaces.

If we have one Router with one physical interface, but needed to have the router connected to two IP networks to route traffic between two routers, we can create two sub interfaces within the physical interface, assign each sub interface an IP address within each subnet and then route the data between two subnets.

Example

interface gig 0/0/0 => Physical Interface
interface gig 0/0/0.10 => Logical/sub Interface
interface gig 0/0/0.20 => Logical/sub Interface

Router-on-a-Stick (RoaS) (Configuration)

Create VLAN & assign to interfaces

Set Gig0/1 of SW to trunk port

```
SW(config)#int range gig 0/1
SW(config-if-range)#switchport mode trunk
```

Assign Default Gateway to router subinterfaces

```
R(config)#int gigabitEthernet 0/0/0.10
R(config-subif)#encapsulation dot1Q 10
R(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no sh
```

Note: 10 indicates VLAN ID 10

*Configure the other interfaces

Switched virtual interfaces (SVIs)

Multilayer Switch (Layer 3) with virtual interface need to be used. Connection type between switches will be trunk mode.

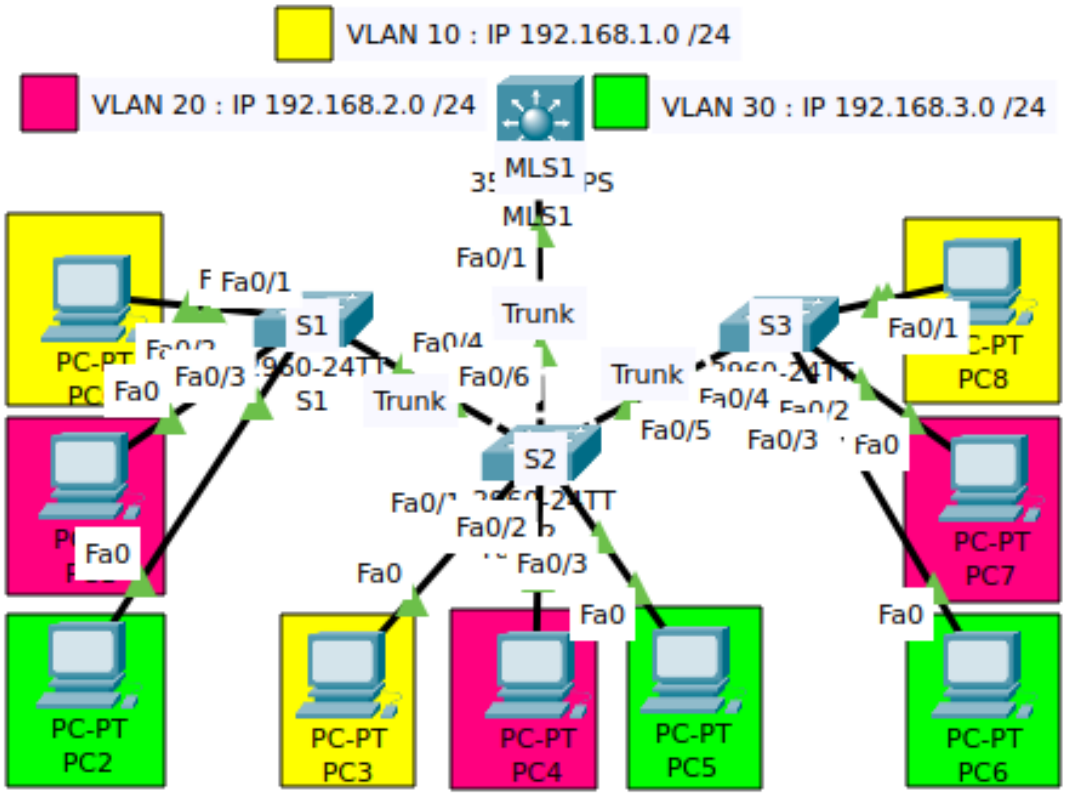

Figure 11: Router-on-a-Stick (RoaS).

Cable Configuration

Interface/ Device	VLAN	Port Type
PC 0,3,8	10	Access
PC 1,4,7	20	Access
PC 2,5,6	30	Access
S1 – S2	–	Trunk
S2 – S3	–	Trunk
S2 – MLS1	–	Trunk

VLAN database in devices

Device	VLANs
SW1, SW2, SW3	10, 20, 30
MLS1	10, 20, 30

Virtual interface

Virtual interface

A virtual interface is a L2 virtual interface that are assigned with VLAN, or simply SVI is bound to a VLAN used for L2 switching.

Example

The ip address of VLAN 10 can be 192.168.1.0 /24
The ip address of VLAN 20 can be 192.168.2.0 /24
The ip address of VLAN 30 can be 192.168.3.0 /24

Switched virtual interfaces (SVIs) (Configuration)

Create VLANs & assign to interfaces

Set S1-S2 and S2-S3 interface to trunk port

Set Fa0/1 of MLS1 interface to trunk port

```
MLS(config)#interface FastEthernet0/1
MLS(config-if)#switchport trunk encapsulation dot1q
MLS(config-if)#switchport mode trunk
R1(config-if)#no sh
```

*Configure the other interfaces

Switched virtual interfaces (SVIs) (Configuration)

Assign Default Gateway to MLS1 virtual interfaces / VLAN

```
MLS(config)#int vlan 10
MLS(config-if)#ip address 192.168.1.1 255.255.255.0
MLS(config-if)#no sh
```

*Assign gateway address for other VLANs

Activate routing in MLS

```
MLS(config)#ip routing
```

Some troubleshooting commands

Execute (from privileged mode) and find out the outcomes.

- sh run
- sh ip int br
- sh ip route
- sh ip interface vlan 10
- sh ip interface fa 0/1
- sh mac address-table
- sh mac address-table ?
- sh vlan
- sh vlan ?

Practice Questions

- Which of the following statements is true with regard to VLANs?
  A. VLANs greatly reduce network security.
  B. VLANs increase the number of collision domains while decreasing their size.
  C. VLANs decrease the number of broadcast domains while decreasing their size.
  D. Network adds, moves, and changes are achieved with ease by just configuring a port intothe appropriate VLAN.
- Write the command that must be present for this layer 3 switch to provide inter-VLAN routing between the two VLANs created with these commands:
  S1(config)#int vlan 10
  S1(config-if)#ip address 192.168.10.1 255.255.255.0
  S1(config-if)#int vlan 20
  S1(config-if)#ip address 192.168.20.1 255.255.255.0

Practice Questions

- What is the only type of second VLAN of which an access port can be a member?
  A. Secondary
  B. Voice
  C. Primary
  D. Trunk
- In the following configuration, what command is missing in the creation of the VLAN interface?
  2960#config t
  2960(config)#int vlan 1
  2960(config-if)#ip address 192.168.10.2 255.255.255.0
  2960(config-if)#exit
  2960(config)#ip default-gateway 192.168.10.1
  A. no shutdown under int vlan 1
  B. encapsulation dot1q 1 under int vlan
  C. switchport access vlan 1
  D. passive-interface

Practice Questions

- Which of the following statements is true with regard to ISL and 802.1q?
  A. 802.1q encapsulates the frame with control information; ISL inserts an ISL field along with tag control information.
  B. 802.1q is Cisco proprietary.
  C. ISL encapsulates the frame with control information; 802.1q inserts an 802.1q field along with tag control information.
  D. ISL is a standard.
- Write the command that places an interface into VLAN 2. Write only the command and not the prompt.
- 802.1q untagged frames are members of the _____ VLAN.
  A. Auxiliary
  B. Voice
  C. Native
  D. Private