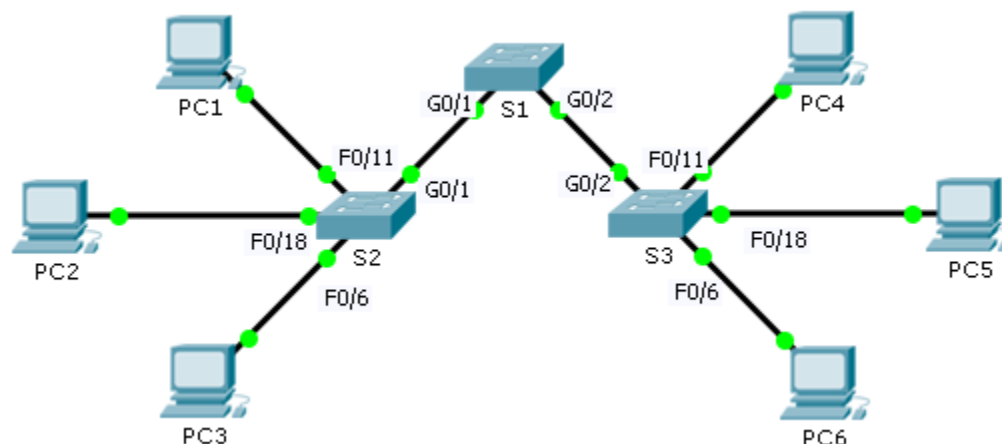


Packet Tracer – Skills Integration Challenge (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 88	172.31.88.2	255.255.255.0	172.31.88.1
S2	VLAN 88	172.31.88.3	255.255.255.0	172.31.88.1
S3	VLAN 88	172.31.88.4	255.255.255.0	172.31.88.1
PC1	NIC	172.31.10.21	255.255.255.0	172.31.10.1
PC2	NIC	172.31.20.22	255.255.255.0	172.31.20.1
PC3	NIC	172.31.30.23	255.255.255.0	172.31.30.1
PC4	NIC	172.31.10.24	255.255.255.0	172.31.10.1
PC5	NIC	172.31.20.25	255.255.255.0	172.31.20.1
PC6	NIC	172.31.30.26	255.255.255.0	172.31.30.1

VLANs and Port Assignment Table

Ports	Assignment	Network
F0/7 - 12	VLAN 10 - Sales	172.31.10.0/24
F0/13 -20	VLAN 20 - Production	172.31.20.0/24
F0/1 - 6	VLAN 30 - Marketing	172.31.30.0/24
Interface VLAN 88	VLAN 88 - Management	172.31.88.0/24
Trunks	VLAN 99 - Native	N/A

Scenario

In this activity, two switches are completely configured. On a third switch, you are responsible for assigning IP addressing to the Switch Virtual Interface, configuring VLANs, assigning VLANs to interfaces, configuring trunking, and performing basic switch security.

Requirements

S1 and **S2** are fully configured. You cannot access these switches. You are responsible for configuring **S3** with the following requirements:

- IP addressing and default gateway configuration, according to the **Addressing Table**.
- Create, name, and assign VLANs according to the **VLANs and Port Assignment Table**.
- Assign the native VLAN 99 to the trunk port and disable DTP.
- Restrict the trunk to only allow VLANs 10, 20, 30, 88, and 99.
- Use VLAN 99 as the native VLAN on the trunk ports.
- Configure basic switch security on S3.
 - Encrypted secret password of **itsasecret**
 - Console password of **letmein**
 - VTY password of **c1\$c0** (where 0 is the number zero)
 - Encrypted plain text passwords
 - MOTD banner with the message **Authorized Access Only!!**
 - Disable unused ports.
- Configure port security on **F0/6**.
 - Only two unique devices are allowed to access the port.
 - Learned MACs are added to the running configuration.
 - Secure the interface so that a notification is sent when there is a violation, but the port is not disabled.
- Verify the PCs in the same VLAN can now ping each other.

```
!S3!!!!!!!!!!!!!!!!!!
```

```
en
```

```
conf t
```

```
interface vlan 88
```

```
ip address 172.31.88.4 255.255.255.0
```

```
no shutdown
ip default-gateway 172.31.88.1
!VLAN names are accepted as long as the first 3 letters are correct
vlan 10
name Sales
vlan 20
name Production
vlan 30
name Marketing
vlan 88
name Management
vlan 99
name Native
!Ports Fa0/6, Fa0/11 and Fa0/18 are checked for VLAN assignment
interface range fa0/7 - 12
switchport mode access
switchport access vlan 10
interface range fa0/13 - 20
switchport mode access
switchport access vlan 20
interface range fa0/1 - 6
switchport mode access
switchport access vlan 30
interface g0/2
switchport trunk native vlan 99
switchport trunk allowed vlan 10,20,30,88,99
switchport mode trunk
switchport nonegotiate
enable secret itsasecret
line console 0
password letmein
login
line vty 0 15
password c1$c0
login
service password-encryption
!Only the first 3 letters of the word 'Access' in banner text are checked
banner motd $Authorized Access Only!!$
int fa0/6
switchport port-security
```

```
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!Ports fa0/4, fa0/14 and fa0/24 are checked for shutdown
interface range fa0/1 - 5, fa0/7 - 10, fa0/12 - 17, fa0/19 - 24, g0/1
shutdown
```