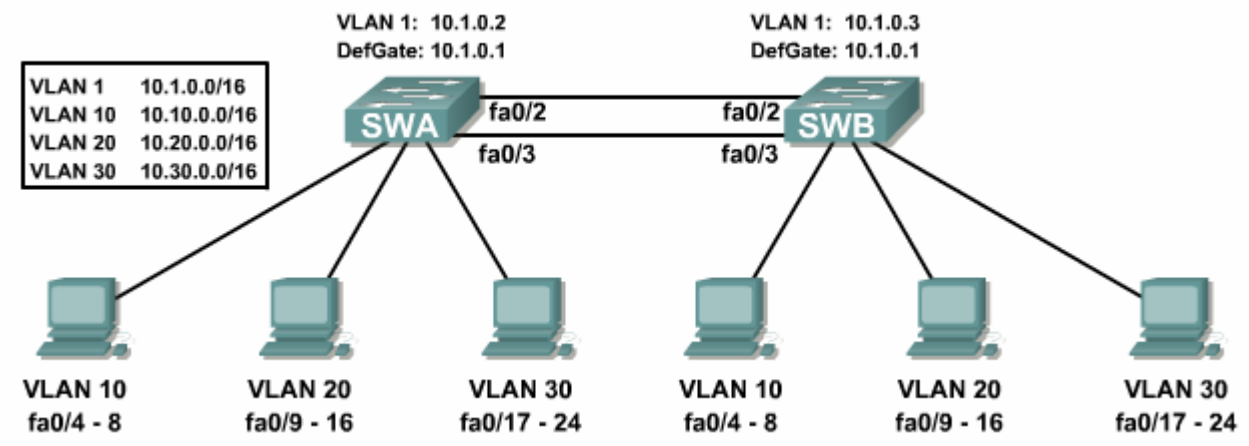
CCNA3 Module 8 Challenge Lab



Objectives

- Configure VLANs, STP and port security

Step 1: Cable the Topology and Basic Configuration

- Choose two 2950 switches and one router with a Fast Ethernet interface (1700 or 2600) and cable them according to the topology. (If using NetLab, choose a Basic Switch Pod. Portions of this lab will not be verifiable.)
- Configure the switches according to your Instructor's required basic configurations including hostnames, passwords, host tables, banner, and lines. Configure each of the switches with the correct VLAN1 IP addresses and the correct default gateway.
- Verify connectivity between SWA and SWB. Pings should be successful. If not, troubleshoot. Note: Switches should NOT be able to ping the router yet.

Step 2: Configure VLANs

- Configure the following VLANs on both SWA and SWB.
  - VLAN 10 is the Accounting VLAN
  - VLAN 20 is the Marketing VLAN
  - VLAN 30 is the Purchasing VLAN
- Configure the appropriate ports on SWA and SWB for Trunking. Verify Trunking is properly configured with the show interface trunk command on both SWA and SWB.

```
SWA#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/2       1-4094
Fa0/3       1-4094
```



```
Port        Vlans allowed and active in management domain
Fa0/2       1,10,20,30
Fa0/3       1,10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       1,10,20,30
Fa0/3       1,10,20,30
```

- Assign access ports to their correct VLAN as specified in the topology.
- Verify the VLAN configuration on both switches with the **`show vlan brief`** command. Your output should look similar to the output below.

```
SWA#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1
10   Accounting                       active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8
20   Marketing                        active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
30   Purchasing                       active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Step 3: Configure the Root Bridge for STP

- SWA should always be the root bridge. Configure SWA with a spanning tree priority of 4096 for all four VLANs (1, 10, 20, and 30)
- Verify SWA is the root with the **`show spanning-tree summary`** command. SWA should be listed as the root bridge as shown in the output below.

```
SWA#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001, VLAN0010, VLAN0020, VLAN0030
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          2          2
VLAN0010                    0         0        0          2          2
VLAN0020                    0         0        0          2          2
VLAN0030                    0         0        0          2          2
---------------------- -------- --------- -------- ---------- ----------
4 vlans                     0         0        0          8          8

SWB#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    1         0        0          1          2
VLAN0010                    1         0        0          1          2
VLAN0020                    1         0        0          1          2
VLAN0030                    1         0        0          1          2
---------------------- -------- --------- -------- ---------- ----------
4 vlans                     4         0        0          4          8
```


Step 3: Configure Port Security

- As a security precaution, disable the FastEthernet 0/1 interface on SWB since this interface will not be used for access mode or trunk mode.

On both SWA and SWB…

- Configure the access ports (fa0/4 – 24) for access mode and turn on port security.
- The first MAC address learned should "stick" to the port and no other MAC addresses should be allowed (maximum of 1 MAC per port).
- A security violation should automatically shutdown the port.
- Verify port security with the **`show port-security`** command. Your output should look similar to the output below

```
SWA#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------
     Fa0/4           1               0              0              Shutdown
     Fa0/5           1               0              0              Shutdown
     Fa0/6           1               0              0              Shutdown
     Fa0/7           1               0              0              Shutdown
     Fa0/8           1               0              0              Shutdown
     Fa0/9           1               0              0              Shutdown
     Fa0/10          1               0              0              Shutdown
     Fa0/11          1               0              0              Shutdown
     Fa0/12          1               0              0              Shutdown
     Fa0/13          1               0              0              Shutdown
     Fa0/14          1               0              0              Shutdown
     Fa0/15          1               0              0              Shutdown
     Fa0/16          1               0              0              Shutdown
     Fa0/17          1               0              0              Shutdown
     Fa0/18          1               0              0              Shutdown
     Fa0/19          1               0              0              Shutdown
     Fa0/20          1               0              0              Shutdown
     Fa0/21          1               0              0              Shutdown
     Fa0/22          1               0              0              Shutdown
     Fa0/23          1               0              0              Shutdown
     Fa0/24          1               0              0              Shutdown
-------------------------------------------------------------------------------
Total Addresses in System : 0
Max Addresses limit in System : 1024
```

Step 4: Verify VLANs and Port Security

- Test the VLAN configuration by verifying that a host attached to VLAN 10 cannot ping the hosts of VLAN 20 or VLAN 30
- Test the Port Security configuration by disconnecting a host from a port and connecting a different host to the same port. The port should automatically shutdown. How do you, as the administrator, re-enable the port?

