**Lab 4 & 5**

Virtual LAN (VLAN) & Port Security

**OBJECTIVE**

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Maintain VLAN Port Assignments and the VLAN Database

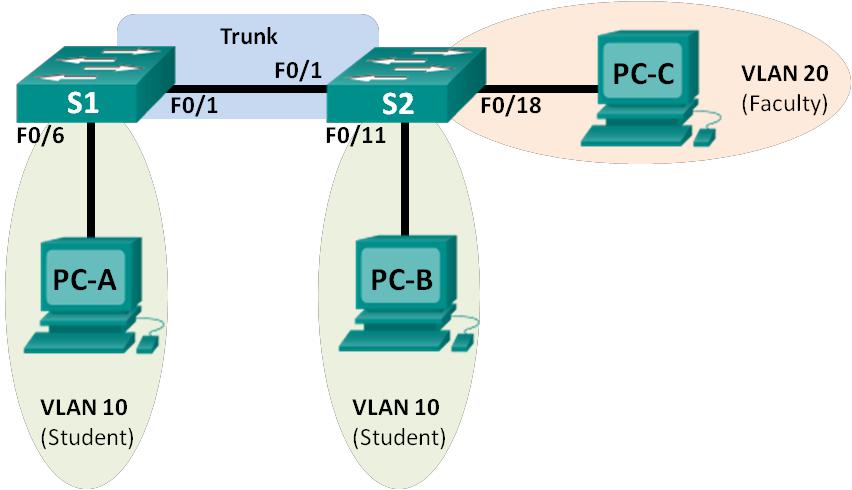
Part 4: Configure an 802.1Q Trunk between the Switches

**THEORY**

**VIRTUAL LAN (VLAN)**

A **virtual LAN**, commonly known as a **VLAN**, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

**Topology**

****

**Part 1:** **Build the Network and Configure Basic Device Settings**

In Part 1, you will set up the network topology and configure basic settings on the PC hosts and switches.

**Step 1:** **Cable the network as shown in the topology.**

Attach the devices as shown in the topology diagram, and cable as necessary.

**Step 2:** **Initialize and reload the switches as necessary.**

**Step 3:** **Configure basic settings for each switch.**

1. Console into the switch and enter global configuration mode.
2. Copy the following basic configuration and paste it to the running-configuration on the switch. no ip domain-lookup

service password-encryption enable secret class banner motd #

Unauthorized access is strictly prohibited. # line con 0

password cisco login

logging synchronous line vty 0 15 password cisco logging synchronous login

exit

1. Configure the host name as shown in the topology.
2. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.
3. Administratively deactivate all unused ports on the switch.
4. Copy the running configuration to the startup configuration.

**Step 4: Configure PC hosts.**

Refer to the Addressing Table for PC host address information.

**Step 5: Test connectivity.**

Verify that the PC hosts can ping one another.

**Note**: It may be necessary to disable the PCs firewall to ping between PCs.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Can PC-A ping PC-B? | \_\_\_\_\_\_\_\_\_ |  | Yes | | |
|  |  | | | | |
| Can PC-A ping PC-C? | \_\_\_\_\_\_\_\_\_ | No | | |  |
|  |  | | | | |
| Can PC-A ping S1? | \_\_\_\_\_\_\_\_\_ | No | |  | |
|  |  | | | | |
| Can PC-B ping PC-C? | \_\_\_\_\_\_\_\_\_ | No | | |  |
|  |  | | | | |
| Can PC-B ping S2? | \_\_\_\_\_\_\_\_\_ | No | | |  |
|  |  | | | | |
| Can PC-C ping S2? | \_\_\_\_\_\_\_\_\_ | No | |  | |
|  |  | | | | |
| Can S1 ping S2? | \_\_\_\_\_\_\_\_\_ | | Yes | | |
|  |  | |  | | |

**Part 2:** **Create VLANs and Assign Switch Ports**

In Part 2, you will create student, faculty, and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

**Step 1:** **Create VLANs on the switches.**

1. Create the VLANs on S1.

S1(config)# **vlan 10** S1(config-vlan)# **name Student** S1(config-vlan)# **vlan 20** S1(config-vlan)# **name Faculty** S1(config-vlan)# **vlan 99** S1(config-vlan)# **name Management** S1(config-vlan)# **end**

1. Create the same VLANs on S2.
2. Issue the **show vlan** command to view the list of VLANs on S1.

S1# **show vlan**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **VLAN** | **Name** |  |  |  | **Status** | | | **Ports** | |  |  |  |
| ---- | -------------------------------- --------- ------------------------------- | | | | | | | | | | | |
| 1 | default | |  |  | active | | | Fa0/1, Fa0/2, Fa0/3, Fa0/4 | | | | |
|  |  |  |  |  |  |  |  | Fa0/5, Fa0/6, Fa0/7, Fa0/8 | | | | |
|  |  |  |  |  |  |  |  | Fa0/9, Fa0/10, Fa0/11, Fa0/12 | | | | |
|  |  |  |  |  |  |  |  | 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 | | |  |  |
|  |  | |  |  |  | | |  |  |  |  |  |
| 10 | Student | |  |  | active | |  |  |  |  |  |  |
|  |  | |  |  |  | | |  |  |  |  |  |
| 20 | Faculty | |  |  | active | |  |  |  |  |  |  |
|  |  | |  |  |  | | |  |  |  |  |  |
| 99 | Management | |  |  | 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 Trans2 | |
| ---- | ----- | ---------- | ----- ------ ------ -------- | | | | | | ---- | -------- | ------ | ------ |
| 1 | enet | 100001 | 1500 | - | - | - |  |  | - | - | 0 | 0 |
| 10 | enet | 100010 | 1500 | - | - | - |  |  | - | - | 0 | 0 |
| 20 | enet | 100020 | 1500 | - | - | - |  |  | - | - | 0 | 0 |
| 99 | enet | 100099 | 1500 | - | - | - |  |  | - | - | 0 | 0 |
| VLAN | Type | SAID | MTU | Parent | RingNo | BridgeNo | | | Stp | BrdgMode | Trans1 Trans2 | |
| ---- | ----- | ---------- | ----- ------ | | ------ | -------- | | | ---- | -------- | ------ | ------ |
| 1002 | fddi | 101002 | 1500 | - | - | - |  |  | - | - | 0 | 0 |
| 1003 | tr | 101003 | 1500 | - | - | - |  |  | - | - | 0 | 0 |
| 1004 | fdnet | 101004 | 1500 | - | - | - |  |  | ieee | - | 0 | 0 |
| 1005 | trnet | 101005 | 1500 | - | - | - |  |  | ibm | - | 0 | 0 |

**Step 2:** **Assign VLANs to the correct switch interfaces.**

1. Assign VLANs to the interfaces on S1.
   1. Assign PC-A to the Student VLAN.

S1(config)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 10**

* 1. Move the switch IP address VLAN 99.

S1(config)# **interface vlan 1** S1(config-if)# **no ip address** S1(config-if)# **interface vlan 99**

S1(config-if)# **ip address 192.168.1.11 255.255.255.0** S1(config-if)# **end**

1. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

S1# **show vlan brief**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VLAN** | | **Name** | **Status** | **Ports** | |  |
| ---- | -------------------------------- | | --------- | ------------------------------- | | |
| 1 | default | | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 | | |
|  |  | |  | Fa0/5, Fa0/7, Fa0/8, Fa0/9 | | |
|  |  | |  | Fa0/10, Fa0/11, | | Fa0/12, 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 | |  |
|  |  | |  |  | |  |
| 10 | Student | | active | Fa0/6 |  |  |
| 20 | Faculty | | active |  |  |  |
| 99 | Management | | active |  |  |  |
| 1002 | fddi-default | | act/unsup |  |  |  |
| 1003 | token-ring-default | | act/unsup |  |  |  |
| 1004 | fddinet-default | | act/unsup |  |  |  |
| 1005 | trnet-default | | act/unsup |  |  |  |

1. Issue the **show ip interface brief** command

S1# **show ip interface brief**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Interface | IP-Address | OK? Method | Status | | Protocol | |
| Vlan1 | unassigned | YES unset | up | | up | |
|  |  |  |  |  |  |  |
| Vlan99 | 192.168.1.11 | YES manual |  | up | down |  |
| FastEthernet0/1 | unassigned | YES unset | up | | up | |
| FastEthernet0/2 | unassigned | YES unset |  | administratively down down | | |
| FastEthernet0/3 | unassigned | YES unset |  | administratively down down | | |
| FastEthernet0/4 | unassigned | YES unset |  | administratively down down | | |
| FastEthernet0/5 | unassigned | YES unset |  | administratively down down | | |
| FastEthernet0/6 | unassigned | YES unset | up | | up | |
| FastEthernet0/7 | unassigned | YES unset |  | administratively down down | | |

d. Use the Topology to assign VLANs to the appropriate ports on S2.

1. Remove the IP address for VLAN 1 on S2.
2. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.
3. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

S2# show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/12, Fa0/13

Fa0/14, Fa0/15, Fa0/16, Fa0/17

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24, Gi0/1, Gi0/2

10 Student active Fa0/11

20 Faculty active Fa0/18

99 Management active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

****

1. Remove the IP address for VLAN 1 on S2.
2. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.
3. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces

**Part 3: Maintain VLAN Port Assignments and the VLAN Database**

**In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.**

**Step 1: Assign a VLAN to multiple interfaces.**

1. On S1, assign interfaces F0/11 – 24 to VLAN 10.

S1(config)# **interface range f0/11-24** S1(config-if-range)# **switchport mode access** S1(config-if-range)# **switchport access vlan 10** S1(config-if-range)# **end**

1. Issue the **show vlan brief** command to verify VLAN assignments.

S1# **show vlan brief**

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN | Name | Status | Ports |
| ---- | -------------------------------- | --------- | ------------------------------- |
| 1 | default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 |
|  |  |  | Fa0/5, Fa0/7, Fa0/8, Fa0/9 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | Fa0/10, Gi0/1, Gi0/2 | | | |
|  |  |  |  |  | |  | |
| 10 | Student | active | Fa0/6, Fa0/11, Fa0/12, Fa0/13 | | | |  |
|  |  |  |  |  |  |  | |
|  |  |  |  | Fa0/14, Fa0/15, | Fa0/16, Fa0/17 | | |
|  |  |  |  |  |  |  | |
|  |  |  |  | Fa0/18, Fa0/19, | Fa0/20, Fa0/21 | | |
|  |  |  |  |  |  | | |
|  |  |  |  | Fa0/22, Fa0/23, | Fa0/24 |  | |
| 20 | Faculty | active |  |  |  |  |  |
| 99 | Management | active |  |  |  |  |  |
| 1002 | fddi-default | act/unsup |  |  |  |  |  |
| 1003 | token-ring-default | act/unsup |  |  |  |  |  |
| 1004 | fddinet-default | act/unsup |  |  |  |  |  |
| 1005 | trnet-default | act/unsup |  |  |  |  |  |

Reassign F0/11 and F0/21 to VLAN 20.

S1(config)# **interface range f0/11, f0/21** S1(config-if-range)# **switchport access vlan 20** S1(config-if-range)# **end**

1. Verify that VLAN assignments are correct.

S1# **show vlan brief**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| VLAN | Name | Status | Ports | | |  |
| ---- | -------------------------------- | --------- | ------------------------------- | | | |
| 1 | default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4 | | | |
|  |  |  |  | Fa0/5, Fa0/7, Fa0/8, Fa0/9 | | |
|  |  |  |  | Fa0/10, Gi0/1, Gi0/2 | | |
| 10 | Student | active | Fa0/6, Fa0/12, Fa0/13, Fa0/14 | | | |
|  |  |  |  | Fa0/15, Fa0/16, | | Fa0/17, Fa0/18 |
|  |  |  |  | Fa0/19, Fa0/20, | | Fa0/22, Fa0/23 |
|  |  |  |  | Fa0/24 | |  |
|  |  |  |  |  | |  |
| 20 | Faculty | active |  | Fa0/11, Fa0/21 |  |  |
| 99 | Management | active |  |  |  |  |
| 1002 | fddi-default | act/unsup |  |  |  |  |
| 1003 | token-ring-default | act/unsup |  |  |  |  |
| 1004 | fddinet-default | act/unsup |  |  |  |  |
| 1005 | trnet-default | act/unsup |  |  |  |  |

**Part 4: Configure an 802.1Q Trunk Between the Switches**

**Step 1: Manually configure trunk interface F0/1.**

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

1. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

S1(config)# **interface f0/1** S1(config-if)# **switchport mode trunk**

S2(config)# **interface f0/1** S2(config-if)# **switchport mode trunk**

1. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

S2# **show interfaces trunk**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Port | Mode | | Encapsulation | Status | Native vlan |
|  |  | |  |  |  |
| Fa0/1 | on |  | 802.1q | trunking | 1 |
| Port | Vlans allowed on trunk | | |  |  |
| Fa0/1 | 1-4094 | |  |  |  |
| Port | Vlans allowed and active in management domain | | | |  |
| Fa0/1 | 1,10,20,99 | |  |  |  |
| Port | Vlans in spanning tree forwarding state and not pruned | | | | |
| Fa0/1 | 1,10,20,99 | |  |  |  |

**HOME ASSIGNMENTS**

Q1: What are some primary benefits that an organization can receive through effective use of VLANs?

Q2: [What are three benefits of implementing VLANs?](https://www.proprofs.com/discuss/q/1192739/what-are-three-benefits-of-implementing-vlans-choose-2wh)

Q3: What are three advantages of VLANs?

Q4: What is the purpose of Trunk ?

**Port Security**

**OBJECTIVE**

To secure campus network from unhealthy systems by implementing port security on switches.

**THEORY**

**PORT SECURITY**

Port security can be used with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

A security violation occurs in either of these situations:

* When the maximum number of secure MAC addresses is reached on a secure port and the source MAC address of the ingress traffic is different from any of the identified secure MAC addresses, port security applies the configured violation mode.
* If traffic with a secure MAC address that is configured or learned on one secure port attempts to access another secure port in the same VLAN, applies the configured violation mode.



**Fig 12.1** Port security restricts port access by MAC address



**Fig 12.2** Network setup for applying port security

**Verify MAC table and ports**

* Checking the MAC Address table first, DYNAMIC means that no MAC address has been configured on ports. Use the privileged EXEC mode to view the MAC Address table**.**

**Switch# show mac-address-table**

Mac Address Table

-------------------------------------------

Vlan Mac Address Type Ports

---- ------------------- -------- -----

1 0001.4267.74a9 DYNAMIC Fa0/6

1 0002.4a20.a5ed DYNAMIC Fa0/1

1 0003.e4b2.29a0 DYNAMIC Fa0/10

1 0004.9a54.2174 DYNAMIC Fa0/9

1 0004.9ab2.c6c8 DYNAMIC Fa0/7

1 000b.be7c.7c4b DYNAMIC Fa0/3

1 00d0.5830.a010 DYNAMIC Fa0/5

1 00d0.58de.4a21 DYNAMIC Fa0/8

1 00e0.b0d2.49c7 DYNAMIC Fa0/4

It is good practice to check that all ports are up

**Switch#sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual up up

FastEthernet0/2 unassigned YES manual up up

FastEthernet0/3 unassigned YES manual up up

FastEthernet0/4 unassigned YES manual up up

FastEthernet0/5 unassigned YES manual up up

FastEthernet0/6 unassigned YES manual up up

FastEthernet0/7 unassigned YES manual up up

FastEthernet0/8 unassigned YES manual up up

FastEthernet0/9 unassigned YES manual up up

FastEthernet0/10 unassigned YES manual up up

--More—

**EXERCISE 12.2**

**Step 1: select range to apply port security**

Interface configuration commands modify the operation. In order to configure a specific interface range, you need to enter interface configuration mode, from global configuration mode, by entering the interface interface range command. The prompt Switch (config-if)# indicates that you are in interface configuration mode.

Switch(config)# **interface range fastEthernet 0/1 - 10**

**Step 2: Access mode**

By default, the port security is turned off on all interfaces. In order to turn it on, a port **must be in an access mode**. Otherwise the command will be rejected. Check out the below attempt of enabling it when the port is in a 'dynamic desirable' rather than an access mode.

*Switch(config-if-range)#* ***switchport mode access***

**Step 3: Applying Mac-address-sticky**

Port security with sticky MAC addresses provides many of the same benefits as port security with static MAC addresses, but sticky MAC addresses can be learned dynamically. Port security with sticky MAC addresses retains dynamically learned MAC addresses during a link-down condition.

*Switch(config-if-range)#* ***switchport port-security mac-address sticky***

**Step 4: Set maximum address to learn**

How many MAC addresses can be considered secure on a given port (platform dependent). The default is: 1.

*Switch(config-if-range)#* ***switchport port-security maximum 1***

**Step 5: violation condition to shutdown**

When configuring port security violation modes, note the following information:

* **protect**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
* **restrict**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.
* **shutdown**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification

*Switch(config-if-range)#* ***switchport port-security violation shutdown***

**Step 6: Applying port security**

If this command is not performed than port security will not be applied

*Switch(config-if-range)#* ***switchport port-security***

**Step 7: checking port security**

Switch# show port-security interface fastEthernet 0/5

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 00d0.5830.a010

Security Violation Count : 0

**EXERCISE 12.3**

**Change the PC on port FastEthernet 0/5 and verify port security**

Switch# **show port-security interface fastEthernet 0/5**

Port Security : Enabled

Port Status : Secure-shutdown

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0001.C971.1829:1

Security Violation Count : 1

**Check that Last source MAC address and compare it with MAC address in last exercise**

Switch# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual up up

FastEthernet0/2 unassigned YES manual up up

FastEthernet0/3 unassigned YES manual up up

FastEthernet0/4 unassigned YES manual up up

FastEthernet0/5 unassigned YES manual down down

FastEthernet0/6 unassigned YES manual up up

FastEthernet0/7 unassigned YES manual up up

Switch# **show interfaces fastEthernet 0/5**

FastEthernet0/5 is down, line protocol is down (err-disabled)

Hardware is Lance, address is 0030.a354.e505 (bia 0030.a354.e505)

BW 100000 Kbit, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

<OUTPUT OMITTED>

**HOME ASSIGNMENTS**

Q1: Perform other violation modes on other ports.