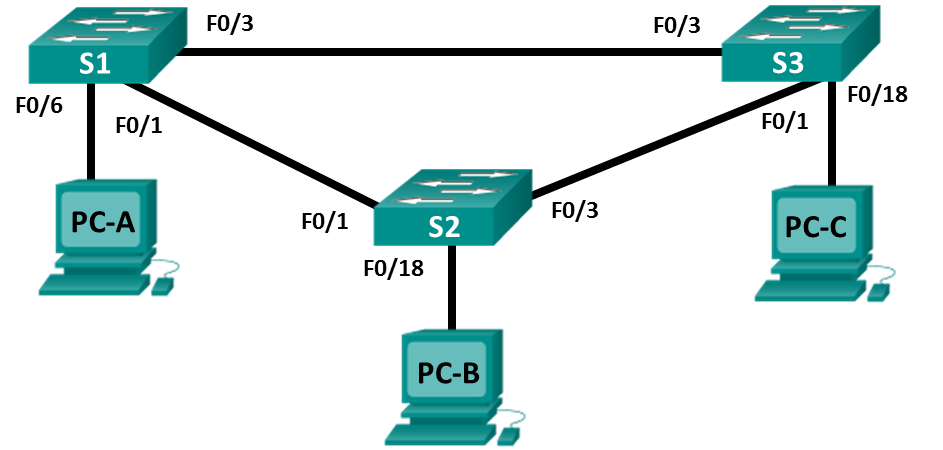
Lab – Configure Extended VLANs, VTP, and DTP

1. Topology



1. Addressing Table

|  |  |  |  |
| --- | --- | --- | --- |
| Table Heading | Interface | IP Address | Subnet Mask |
| S1 | VLAN 99 | 192.168.99.1 | 255.255.255.0 |
| S2 | VLAN 99 | 192.168.99.2 | 255.255.255.0 |
| S3 | VLAN 99 | 192.168.99.3 | 255.255.255.0 |
| PC-A | NIC | 192.168.10.1 | 255.255.255.0 |
| PC-B | NIC | 192.168.20.1 | 255.255.255.0 |
| PC-C | NIC | 192.168.10.2 | 255.255.255.0 |

1. Objectives

Part 1: Configure VTP

Part 2: Configure DTP

Part 3: Add VLANs and Assign Ports

Part 4: Configure Extended VLAN

1. Background / Scenario

It can become challenging to manage VLANs and trunks in a network, as the number of switches increases. VLAN trunking protocol (VTP) allows a network administrator to automate the management of VLANs. Automated trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP). DTP is enabled by default on Catalyst 2960 and Catalyst 3560 switches.

In this lab, you will configure trunk links between the switches. You will also configure a VTP server and VTP clients in the same VTP domain. Furthermore, you will configure an extended VLAN on one of the switches, assign ports to VLANs and verify end-to-end connectivity within the same VLAN.

**Note**: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

**Note**: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

1. Required Resources

* 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 3 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet cables as shown in the topology

1. Configure VTP

All the switches will be configured to use VTP for VLAN updates. S2 will be configured as the server. Switches S1 and S3 will be configure as clients. They will be in the **CCNA** VTP domain using the password **cisco**.

* + - 1. Configure S2 as a VTP server in the **CCNA** VTP domain using **cisco** as the VTP password.

S2(config)# **vtp domain CCNA**

Changing VTP domain name from NULL to CCNA

S2(config)#

\*Mar 1 00:03:44.193: %SW\_VLAN-6-VTP\_DOMAIN\_NAME\_CHG: VTP domain name changed to CCNA.

S2(config)# **vtp mode server**

Device mode already VTP Server for VLANS.

S2(config)# **vtp password cisco**

Setting device VTP password to cisco

* + - 1. Configure S1 and S3 as VTP clients in the **CCNA** VTP domain using **cisco** as the VTP password. VTP configurations are displayed below.

S1(config)# **vtp domain CCNA**

Changing VTP domain name from NULL to CCNA

S1(config)#

\*Mar 1 00:03:44.193: %SW\_VLAN-6-VTP\_DOMAIN\_NAME\_CHG: VTP domain name changed to CCNA.

S1(config)# **vtp mode client**

Device mode VTP client for VLANS.

S1(config)# **vtp password cisco**

Setting device VTP password to cisco

* + - 1. Verify VTP configurations by entering the **show vtp status** command on all switches. The VTP status for S3 is displayed below.

S3# **show vtp status**

VTP Version capable : 1 to 3

VTP version running : 1

VTP Domain Name : CCNA

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0cd9.96d2.3580

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:

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

VTP Operating Mode : Client

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

Configuration Revision : 0

MD5 digest : 0x8B 0x58 0x3D 0x9D 0x64 0xBE 0xD5 0xF6

0x62 0xCB 0x4B 0x50 0xE5 0x9C 0x6F 0xF6

1. Configure DTP
   * 1. Configure dynamic trunk links between S1 and S2.
        1. Enter the **show interfaces f0/1 switchport** command on S1 and S2.

What is the administrative and operational mode of switchport f0/1?

Modo administrativo: auto dinámico

Modo operativo: Acceso estático

* + - 1. In interface configuration mode, configure a dynamic trunk link between S1 and S2. Because the default mode is dynamic auto, only one side of the link needs to be configured as dynamic desirable.

S1(config)# **interface f0/1**

S1(config-if)# **switchport mode dynamic desirable**

S1(config-if)#

\*Mar 1 00:30:45.082: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

\*Mar 1 00:30:48.102: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

* + - 1. Verify trunking link between S1 and S2 using the **show interfaces trunk** command.

S1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 desirable 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 none

S2# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 auto 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1

* + 1. Configure static trunk link between S1 and S3.
       1. Between S1 and S3, configure a static trunk link using the **switchport mode trunk** command in the interface configuration mode for port F0/3.

S1(config)# **interface f0/3**

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

* + - 1. Verify the trunks using **show interfaces trunk** command on S1.

S1# **show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 desirable 802.1q trunking 1

Fa0/3 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-4094

Fa0/3 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1

Fa0/3 1

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 none

Fa0/3 none

* + - 1. Configure a permanent trunk between S2 and S3.
      2. Record the commands you used to create the static trunk.

Enable

Configure terminal para configurar el switch

Accedemos a la interface con el cuál se va a hacer el trunk

Switchport mode trunk

1. Add VLANs and Assign Ports
   * 1. Add VLANs on the switches.
        1. On S1, add VLAN 10.

S1(config)# **vlan 10**

Were you able to create VLAN 10 on S1? Explain.

No se puede crear la VLAN 10 en S1 porque está configurado como cliente.

* + - 1. On S2, add the following VLANs.

|  |  |
| --- | --- |
| VLAN | Name |
| 10 | Red |
| 20 | Blue |
| 30 | Yellow |
| 99 | Management |

S2(config)# **vlan 10**

S2(config-vlan)# **name Red**

S2(config-vlan)# **vlan 20**

S2(config-vlan)# **name Blue**

S2(config-vlan)# **vlan 30**

S2(config-vlan)# **name Yellow**

S2(config-vlan)# **vlan 99**

S2(config-vlan)# **name Management**

S2(config-vlan)# **end**

S2# **show vlan brief**

VLAN Name Status Ports

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

1 default active Fa0/2, 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 Red active

20 Blue active

30 Yellow active

99 Management active

<output omitted>

* + 1. Verify VTP updates on S1 and S3.

Because S2 is configured as a VTP server, and S1 and S3 are configured as VTP clients, S1 and S3 should learn and implement the VLAN information from S2.

What **show** commands did you use to verify the VTP updates on S1 and S3?

Show vtp status

* + 1. Assign ports to VLANs.

In this step, you will associate ports to VLANs and configure IP addresses according to the table below.

|  |  |  |
| --- | --- | --- |
| Port Assignment | VLAN | Attached PC IP Address and Prefix |
| S1 F0/6 | VLAN 10 | PC-A: 192.168.10.1 / 24 |
| S2 F0/18 | VLAN 20 | PC-B: 192.168.20.1 /24 |
| S3 F0/18 | VLAN 10 | PC-C: 192.168.10.2 /24 |

* + - 1. On S1, configure F0/6 to access mode and assign F0/6 to VLAN 10.

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

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

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

* + - 1. Repeat the procedure for switchport F0/18 on S2 and S3. Assign the VLAN according to the table above.
      2. Assign the IP addresses to the PCs according to the table above.
    1. Configure IP addresses on the switches.
       1. On S1, assign an IP address to the SVI for VLAN 99 according to the Addressing Table and activate the interface.

S1(config)# **interface vlan 99**

S1(config-if)# **ip address 192.168.99.1 255.255.255.0**

S1(config-fi)# **no shutdown**

* + - 1. Repeat step a. for S2 and S3.
    1. Verify end-to-end connectivity
       1. Ping PC-A from PC-B. Was it successful? Explain.

El ping no tiene éxito porque la PC-A y la PC-B no pertenecen a la misma VLAN, ni a la misma red.

* + - 1. Ping PC-A from PC-C. Was it successful? Explain.

El ping es exitoso porque ambos PCs pertenecen a la VLAN 10 y a la misma red.

* + - 1. Ping PC-A from S1. Was it successful? Explain.

El ping no es exitoso porque no pertenecen a la misma VLAN y a la misma red.

* + - 1. Ping S1 from S2. Was it successful? Explain.

El ping es exitoso porque pertenecen a la misma VLAN y están en la misma red.

1. Configure Extended VLAN

An extended VLAN is a VLAN between 1025 and 4096. Because the extended VLANs cannot be managed with VTP, VTP must be configured in transparent mode. In this part, you will change the VTP mode on S1 to transparent and create an extended VLAN on S1.

* + 1. Configure VTP mode to transparent on S1.
       1. On switch S1, set VTP mode to transparent.

S1(config)# **vtp mode transparent**

Setting device to VTP Transparent mode for VLANS.

S1(config)# **exit**

* + - 1. Verify the VTP mode on S1.

S1# **show** **vtp status**

VTP Version capable : 1 to 3

VTP version running : 1

VTP Domain Name : CCNA

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0cd9.96e2.3d00

Configuration last modified by 0.0.0.0 at 3-1-93 02:36:11

Feature VLAN:

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

VTP Operating Mode : Transparent

Maximum VLANs supported locally : 255

Number of existing VLANs : 9

Configuration Revision : 0

MD5 digest : 0xB2 0x9A 0x11 0x5B 0xBF 0x2E 0xBF 0xAA

0x31 0x18 0xFF 0x2C 0x5E 0x54 0x0A 0xB7

* + 1. Configure an extended VLAN on S1.
       1. Display the current VLAN configurations on S1.
       2. Create an extended VLAN 2000.

S1# **conf t**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# **vlan 2000**

S1(config-vlan)# **end**

* + - 1. Verify the VLAN creation.

S1# **show vlan brief**

VLAN Name Status Ports

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

1 default active Fa0/2, 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 Red active Fa0/6

20 Blue active

30 Yellow 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

2000 VLAN2000 active

1. Reflection

What are the advantages and disadvantages of using VTP?

consistencia en la configuración de la VLAN a través de la red.

Seguimiento y monitoreo preciso de las VLAN.

Informes dinámicos sobre las VLAN que se agregan a una red.

Configuración de enlace troncal dinámico cuando las VLAN agregan a la red.

1. Router Interface Summary Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Router Interface Summary | | | | |
| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface. | | | | |