

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

FACULTAD TECNOLÓGICA

LABORATORIO DE CISCO: COMUNICACIÓN ENTRE VLANS



**UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS**

GESTIÓN DE REDES

ANDRES FELIPE GONGORA RAMIREZ – 20211578026

KEVIN SANTIAGO SALDAÑA HINCAPIÉ - 20211578002

BOGOTÁ, 5 DE MARZO DE 2024

Laboratorio de Cisco: Comunicación entre VLANs	3
Objetivo General	4
Objetivos Específicos	4
Marco Teórico	5
VLAN	5
Virtual Trunking Protocol (VTP)	5
Modos de operación del VTP	6
Spanning Tree Protocol (STP)	6
Tipos de STP	7
Desarrollo del laboratorio	7
Materiales y equipos	7
Topología	8
Desarrollo del Laboratorio	9
Conclusiones	18
Bibliografía	20

Laboratorio de Cisco: Comunicación entre VLANs

En el ámbito de la gestión de redes, la habilidad para facilitar la comunicación eficiente entre diferentes segmentos de red se vuelve cada vez más crítica. La implementación efectiva de la segmentación de VLANs (Virtual Local Area Networks) es fundamental para optimizar el rendimiento y la seguridad de una infraestructura de red. En este contexto, este informe detalla el desarrollo de un laboratorio avanzado destinado a explorar en profundidad los conceptos relacionados con la comunicación entre VLANs, empleando para ello un entorno de simulación con dos switches Cisco y un Multilayer Switch.

Los switches Cisco, dispositivos esenciales en la arquitectura de redes, sirven como puntos de interconexión que dirigen el tráfico de datos entre diferentes dispositivos. La configuración adecuada de estos switches para permitir la comunicación entre VLANs es crucial para la operatividad fluida de la red.

Este laboratorio tiene como objetivo principal proporcionar a los participantes una experiencia práctica sólida en la configuración y gestión de la comunicación entre VLANs. Se abordarán aspectos técnicos avanzados, como la configuración de interfaces de VLAN en capa 3, la asignación de direcciones IP, la configuración de rutas entre VLANs y la verificación de la conectividad entre dispositivos en diferentes segmentos de red.

Objetivo General

Profundizar en los conocimientos relacionados con la configuración y gestión de la comunicación entre VLANs en una infraestructura de red utilizando dispositivos Cisco. A través de ejercicios prácticos en un entorno simulado, los participantes adquirirán experiencia en la configuración de interfaces de VLAN en capa 3, la asignación de direcciones IP, la configuración de rutas entre VLANs y la verificación de la conectividad entre dispositivos en diferentes segmentos de red. Estando en la capacidad de diseñar, implementar y mantener redes empresariales con una segmentación efectiva de VLANs, optimizando así el rendimiento y la seguridad de la infraestructura de red.

Objetivos Específicos

- Configurar interfaces de VLAN en capa 3 en un Multilayer Switch Cisco.
- Asignar direcciones IP a las interfaces de VLAN para facilitar la comunicación entre segmentos de red.
- Establecer rutas entre VLANs para permitir el tráfico de datos entre diferentes segmentos de red.
- Verificar la conectividad entre dispositivos ubicados en VLANs separadas mediante pruebas de ping y otros métodos de diagnóstico.
- Configurar los puertos de los switches Cisco en modo troncal para facilitar la comunicación entre switches y el Multilayer Switch.
- Asignar los puertos de los switches Cisco a las VLANs correspondientes según el diseño de la red.
- Configurar correctamente la puerta de enlace predeterminada en los dispositivos finales para garantizar la conectividad fuera de la VLAN local.

- Realizar pruebas de conectividad para verificar el correcto funcionamiento de la comunicación entre VLANs y la conectividad externa.
- Identificar y solucionar posibles problemas de configuración que puedan surgir durante el proceso de configuración de la comunicación entre VLANs.

Marco Teórico

VLAN

Las VLAN (redes de área local virtuales) son una tecnología de redes que permite crear redes lógicas independientes dentro de la misma red física, es decir, nos permiten segmentar la red y aislar el tráfico dentro de una red local (LAN) más grande. Las VLAN obtienen soporte mediante el estándar de IEEE 802.1Q.

Las VLAN se usan para generar subredes pequeñas para proporcionar direccionamiento a las decenas de equipos que tengamos, y no solamente una subred donde haya cientos de dispositivos conectados, gracias a dicha segmentación se evidencia una mejora en el rendimiento de la red, porque, se está obteniendo la información o broadcast (el mensaje va para todos los que estén en la red) en dominios más pequeños.

Virtual Trunking Protocol (VTP)

El Virtual Trunking Protocol (VTP) es un protocolo de mensajería de nivel 2 que se utiliza para configurar y administrar VLAN en una red de área local. Permite la creación, modificación y eliminación de VLAN de manera centralizada en un switch designado como servidor VTP, lo que simplifica la gestión de VLAN en redes de gran tamaño.

El VTP desempeña un papel crucial en la gestión de VLAN en redes de gran tamaño, ya que permite una configuración centralizada y una propagación automática de la información de VLAN a

través de la red. Esto simplifica la administración, reduce la posibilidad de errores de configuración y garantiza la consistencia de la información de VLAN en toda la red.

Definición y funcionalidad. El VTP es un protocolo propietario de Cisco que permite la propagación de información de configuración de VLAN a través de toda la red de switches que estén en el mismo dominio VTP. Esto evita la necesidad de configurar manualmente cada VLAN en cada switch de la red, lo que ahorra tiempo y reduce la probabilidad de errores de configuración.

Modos de operación del VTP

- **Servidor.** Es el modo en el que un switch puede crear, modificar y eliminar VLAN. Solo puede haber un servidor VTP en un dominio VTP.
- **Cliente.** Los switches en modo cliente no pueden crear, modificar o eliminar VLAN, pero pueden recibir y propagar actualizaciones de VLAN desde el servidor VTP.
- **Transparente.** Los switches en modo transparente no participan en el VTP, pero pueden transmitir anuncios VTP a otros switches.

Spanning Tree Protocol (STP)

El Spanning Tree Protocol (STP) es un protocolo de red utilizado en redes de área local para evitar bucles de red, lo que puede causar tormentas de difusión y fallas en la red.

El STP es fundamental para garantizar la estabilidad y el rendimiento de las redes de área local. Al evitar bucles de red, el STP previene problemas como tormentas de difusión, uso excesivo de ancho de banda y fallas de red. Además, proporciona redundancia al permitir que los enlaces bloqueados se activen en caso de un fallo en un enlace activo, lo que mejora la disponibilidad de la red.

Definición y propósito. El STP es un protocolo de capa 2 que crea una topología de árbol lógico sin bucles a partir de una topología de red física redundante. Esto garantiza que no haya bucles en la red,

lo que evita que los datos se transmitan de forma indefinida en un bucle, consumiendo ancho de banda y recursos de red.

Funcionamiento. El STP funciona eligiendo un switch raíz y habilitando todos los enlaces necesarios para crear un árbol de spanning tree sin bucles. Los switches restantes se convierten en switches designados o bloqueados. Los enlaces bloqueados se mantienen en estado de escucha y solo se activan cuando se produce un fallo en un enlace activo.

Tipos de STP

- **Spanning Tree Protocol (STP).** Es la versión original del protocolo, diseñado para redes Ethernet.
- **Rapid Spanning Tree Protocol (RSTP).** Es una versión mejorada del STP que converge más rápidamente después de un cambio en la topología de red.
- **Multiple Spanning Tree Protocol (MSTP).** Es una variante del STP que permite la creación de múltiples instancias de spanning tree en una red, lo que mejora el uso del ancho de banda.

Desarrollo del laboratorio

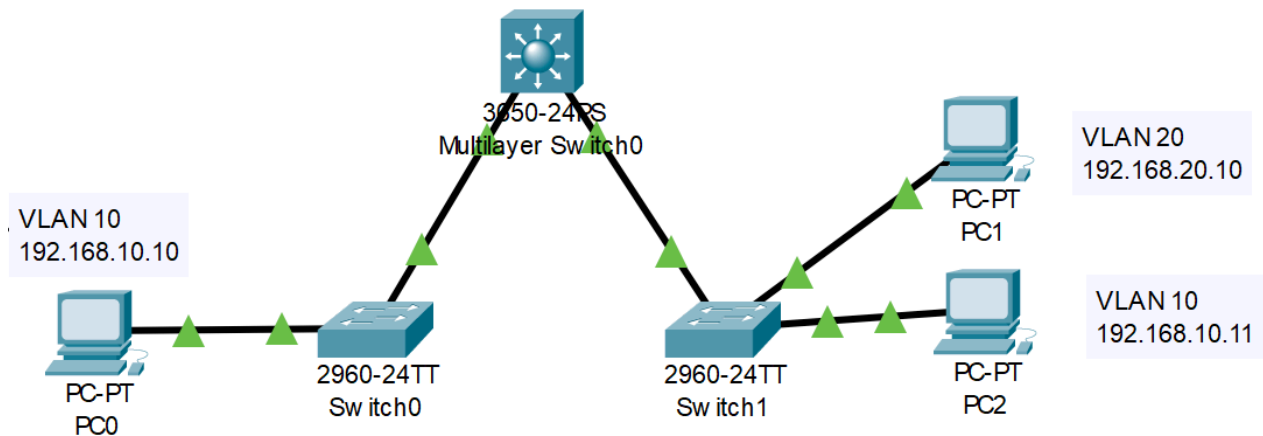
Materiales y equipos

- Software Cisco Packet Tracer
 - 2 Switch 2690
 - 1 MultiLayer Switch 3650
 - 3 PC

Topología

Figura 1

Topología de Red: Comunicación entre VLANs



La topología de red diseñada para este laboratorio se presenta en la imagen adjunta, proporcionando una representación visual clara de la disposición y las interconexiones de los dispositivos. En esta configuración, se emplean dos switches Cisco 2960, identificados como Switch 0 y Switch 1.

Cada uno de estos switches se conecta al Switch de distribución 0, un Multilayer Switch, mediante sus puertos GigabitEthernet 0/1 (Switch 0) y GigabitEthernet 0/2 (Switch 1), los cuales se conectan a los puertos GigabitEthernet 0/1 y GigabitEthernet 0/2 del Switch de distribución 0, respectivamente.

Además, cada switch tiene un PC conectado a través de sus puertos FastEthernet Fa0/0, con PC0 conectado al puerto FastEthernet Fa0/1 del Switch 0 y PC1 conectado al puerto FastEthernet Fa0/1 del Switch 1.

En resumen, la conexión de la topología de este laboratorio se distribuye de la siguiente manera:

- PC0 se conecta al puerto FastEthernet Fa0/1 del Switch 0 a través de su respectivo puerto FastEthernet Fa0/0.
- PC1 se conecta al puerto FastEthernet Fa0/1 del Switch 1 a través de su respectivo puerto FastEthernet Fa0/0.
- Switch 0 se conecta desde su puerto GigabitEthernet 0/1 al puerto GigabitEthernet 1/0/1 del Switch de distribución 0.
- Switch 1 se conecta desde su puerto GigabitEthernet 0/2 al puerto GigabitEthernet 1/0/2 del Switch de distribución 0.

Desarrollo del Laboratorio

Se procedió a configurar los switches Cisco accediendo a la Interfaz de Línea de Comandos (CLI) de cada dispositivo. Esto se logró utilizando el comando **en** para ingresar al modo privilegiado. Una vez dentro del modo privilegiado, se efectuó la transición al modo de configuración con el comando **configure terminal**, lo que permitió al usuario acceder a las funciones de configuración avanzadas del dispositivo.

En primer lugar, en el Switch 0, se ejecutó el comando **hostname SW_ACCESO_1** para asignarle un nombre descriptivo al dispositivo. Del mismo modo, en el Switch 1, tras acceder al modo privilegiado y luego al modo de configuración, se procedió a ejecutar el comando **hostname SW_ACCESO_2** para asignarle un nombre similar al segundo switch.

Posteriormente, se crearon las respectivas VLANs en cada switch de acuerdo con sus roles en la red. En el Switch 0, se utilizó el comando **vlan 10** para crear la VLAN 10, la cual se denominó **producción** mediante el comando **name**. Luego, se accedió a la configuración del puerto FastEthernet 0/1 (Fa0/1)

utilizando el comando **int fa0/1**, donde se configuró el puerto en modo acceso con el comando **switchport mode acc**. Finalmente, se asignó el puerto a la VLAN 10 utilizando el comando **switchport acc vl 10**.

Figura 2

Vista CLI Switch 0

```
Switch>en
Switch#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW_ACCESO_1
SW_ACCESO_1(config)#vlan 10
SW_ACCESO_1(config-vlan)#name PRODUCCION
SW_ACCESO_1(config-vlan)#interface fa0/1
SW_ACCESO_1(config-if)#switchport mode acc
SW_ACCESO_1(config-if)#switchport acc vl 10
```

Por otro lado, en el Switch 1, se creó la VLAN 20 utilizando los mismos comandos mencionados anteriormente, pero con el nombre *pruebas* para identificarla. Se configuró el puerto FastEthernet 0/1 (Fa0/1) en modo acceso y se asignó a la VLAN 20 para completar la configuración de la red.

Figura 3

Vista CLI Switch 1

```
Switch>en
Switch#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW_ACCESO_2
SW_ACCESO_2(config)#vlan 20
SW_ACCESO_2(config-vlan)#name PRUEBAS

SW_ACCESO_2(config-vlan)#int fa0/1
SW_ACCESO_2(config-if)#switchport mode acc
SW_ACCESO_2(config-if)#switchport acc vl 20
```

Este proceso aseguró que cada switch estuviera correctamente configurado con su nombre descriptivo y VLAN correspondiente, lo que sentó las bases para la segmentación y gestión efectiva de la red.

Luego se procedió a configurar el modo troncal en los switches 0 y 1 para establecer la comunicación con el Multilayer Switch. En el Switch 0, se accedió al CLI y se ingresó a la interfaz GigabitEthernet 0/1 utilizando el comando **int Gi0/1**. Posteriormente, se configuró el puerto en modo

troncal con el comando **switchport mode trunk**. De manera similar, en el Switch 1, se realizó el mismo procedimiento accediendo a la interfaz GigabitEthernet 0/2 y estableciendo el modo troncal.

Figura 4

Vista CLI del Switch 0 configurando el modo troncal

```
SW_ACCESO_1>en
SW_ACCESO_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_ACCESO_1(config)#int G0/1
SW_ACCESO_1(config-if)#switchport mode trunk
```

Figura 5

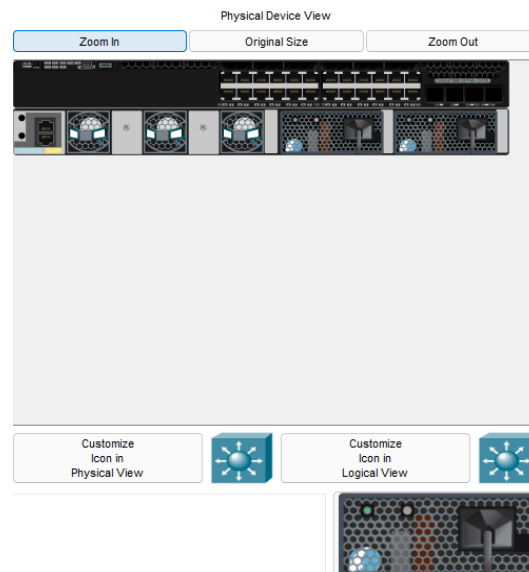
Vista CLI del Switch 1 configurando el modo troncal

```
SW_ACCESO_2>en
SW_ACCESO_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_ACCESO_2(config)#int Gi0/2
SW_ACCESO_2(config-if)#switchport mode tr
```

Luego, se procedió a configurar el Multilayer Switch. Tras arrastrar las fuentes de energía desde el apartado *Physical* al dispositivo en dos ocasiones para encenderlo, se accedió al CLI. Al aparecer la advertencia de que el equipo no se había encendido previamente, se prosiguió con la configuración. Se declinó la configuración inicial cuando se solicitó, y se ingresó al modo privilegiado con el comando **en**. Posteriormente, se accedió a la configuración de terminal con el comando **conf t** y se cambió el nombre del switch a **SW_CORE** utilizando el comando **hostname**.

Figura 6

Vista Physical del Multilayer Switch 0 con las fuentes



Dado que el Multilayer Switch actúa como el puente de comunicación entre las VLANs, se procedió a crear las VLANs correspondientes en él. Utilizando los comandos ***vlan 10*** y ***name PRODUCCION***, se creó la primera VLAN, y luego, utilizando los comandos ***vlan 20*** y ***name PRUEBAS***, se creó la segunda VLAN.

Esta configuración garantiza que el Multilayer Switch, ahora denominado ***SW_CORE***, esté preparado para facilitar la comunicación entre las VLANs en la red, al tiempo que los switches 0 y 1 están configurados para comunicarse correctamente con él en modo troncal.

Figura 7

Vista del CLI del Multilayer Switch 0 creando las VLANs

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW_CORE
SW_CORE(config)#vlan 10
SW_CORE(config-vlan)#name PRODUCCION
SW_CORE(config-vlan)#vlan 20
SW_CORE(config-vlan)#name PRUEBAS
```

Se procedió a configurar los puertos GigabitEthernet 1/0/1 y GigabitEthernet 1/0/2 del Multilayer Switch para establecer la comunicación troncal con los switches 0 y 1. En el CLI del Multilayer Switch, se accedió a la configuración de cada puerto utilizando los comandos **int Gi1/0/1** y **int Gi1/0/2**. Posteriormente, se configuró cada puerto en modo troncal con el comando **switchport mode trunk**.

Figura 8

Vista CLI del Multilayer Switch 0 configurando los puertos en modo troncal

```
SW_CORE(config)#int gil/0/1
SW_CORE(config-if)#switch
SW_CORE(config-if)#switchport mode trunk
SW_CORE(config-if)#int gil/0/2
SW_CORE(config-if)#switchport mode trunk
```

Al mismo tiempo, se realizó una configuración adicional en el Switch 1 para establecer una conexión entre la VLAN 10 y un nuevo PC. Primero, se creó la VLAN 10 con el nombre *produccion* utilizando los comandos correspondientes en el CLI del Switch 1. Luego, se accedió a la configuración del puerto FastEthernet 0/2 (Fa0/2) y se configuró en modo acceso utilizando el comando **switchport mode acc**. Finalmente, se asignó el puerto a la VLAN 10 con el comando **switchport acc vl 10**.

Figura 9

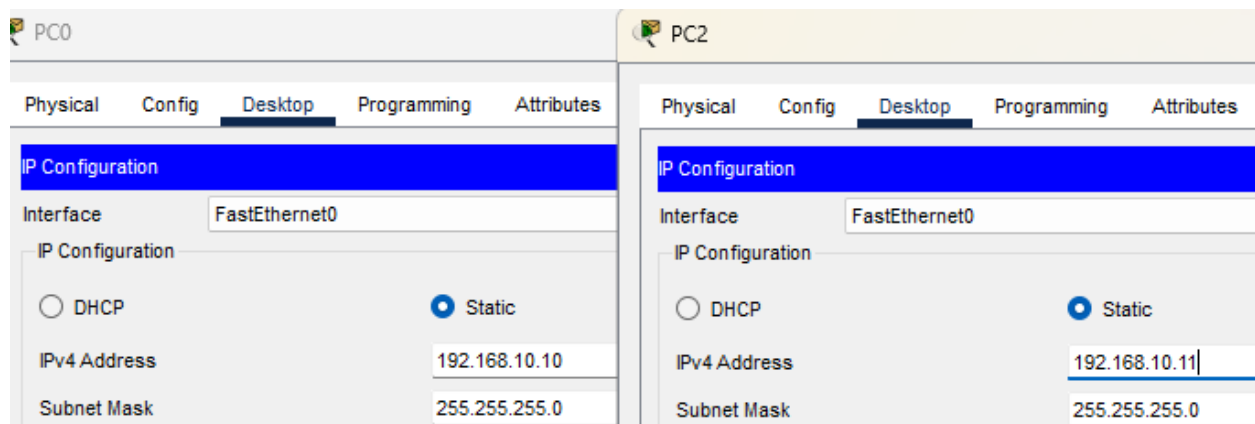
Vista CLI del Switch 1 configurando el PC2 y la VLAN 10

```
SW_ACCESO_2>en
SW_ACCESO_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_ACCESO_2(config)#vlan 10
SW_ACCESO_2(config-vlan)#name PRODUCCION
SW_ACCESO_2(config-vlan)#int fa0/2
SW_ACCESO_2(config-if)#switchport mode acc
SW_ACCESO_2(config-if)#switchport acc vl 10
```

Posteriormente, en ambos PC que trabajan sobre la VLAN 10, se configuraron las direcciones IPv4 respectivas. El PC0 se configuró con la dirección IP 192.168.10.10 y el PC2 con la dirección IP 192.168.10.11, cómo se había mencionado anteriormente.

Figura 10

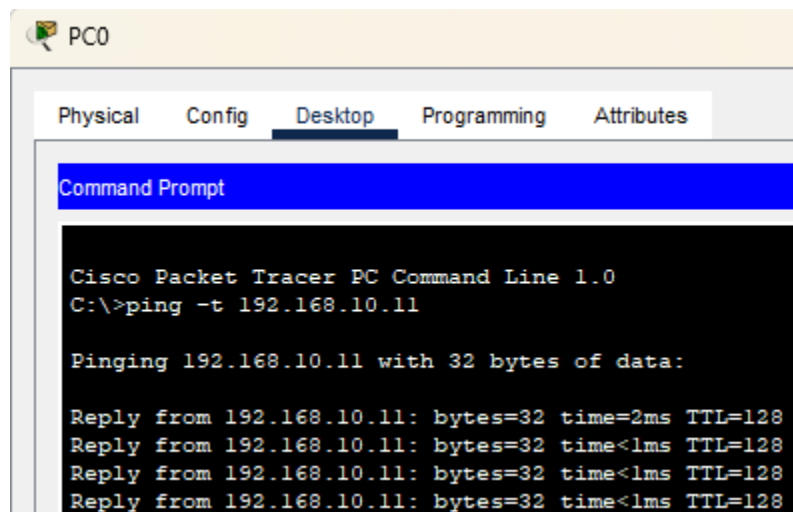
Vista del IP configuration de PC0 y PC2 asignando la dirección IP



Finalmente, se verificó que todos los pasos se hubieran realizado correctamente y se intentó establecer una conexión de ping entre los dos PC desde el PC0 en el Command Prompt utilizando el comando ***ping -t 192.168.10.11***.

Figura 11

Vista del Command Prompt del PC0 haciendo ping con PC2



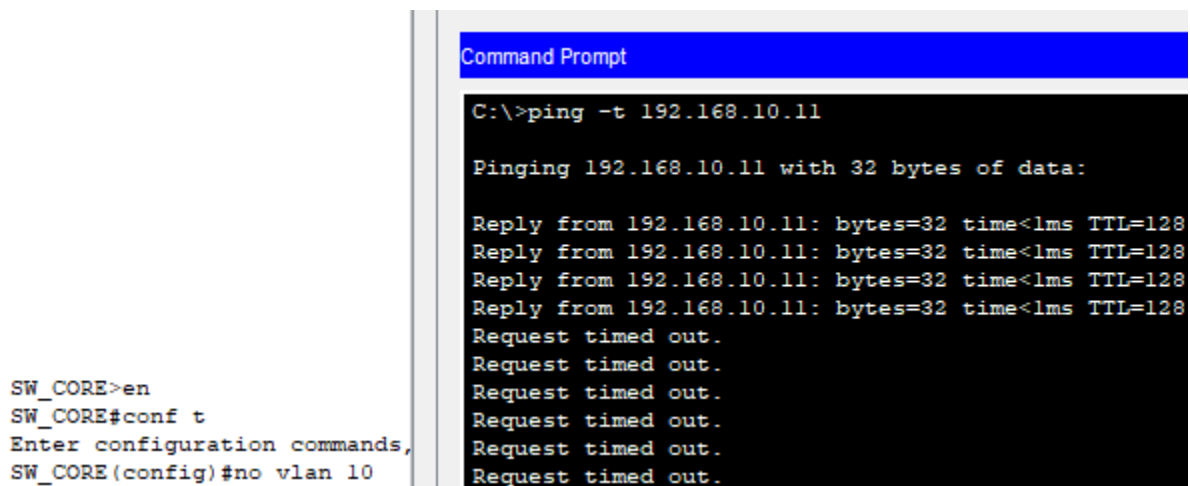
Este proceso asegura que la comunicación entre los dispositivos dentro de la VLAN 10 se haya establecido correctamente y permite verificar la conectividad entre ellos mediante la prueba de ping.

Se simuló un error en la comunicación entre VLANs al eliminar la VLAN 10 en el Multilayer Switch. En el CLI del Multilayer Switch, se utilizó el comando ***no vlan 10*** para eliminar la VLAN que había sido creada previamente.

Posteriormente, al intentar establecer una conexión de ping desde el PC0 al PC2 utilizando el comando ***ping -t 192.168.10.11***, se confirmó que la comunicación se interrumpió. Este resultado evidenció que la eliminación de la VLAN 10 en el Multilayer Switch afectó la comunicación entre los dispositivos de las VLANs correspondientes.

Figura 12

Vista CLI del MultiLayer Switch & Command Prompt del PC0 eliminando la VLAN 10 para simular un error en el ping del PC0 y PC2

The image shows a split-screen view of network equipment. On the left, the CLI of a Multilayer Switch (SW_CORE) is shown. The user has entered 'en' to enter configuration mode, then 'conf t' to enter global configuration mode. The prompt is 'SW_CORE(config)#'. The user has entered the command 'no vlan 10' to delete VLAN 10. On the right, a Windows Command Prompt window is open. The user has executed the command 'ping -t 192.168.10.11'. The output shows the first four ping attempts succeeding with 'Reply from 192.168.10.11: bytes=32 time<1ms TTL=128', followed by four 'Request timed out.' messages, indicating a loss of connectivity after the VLAN was removed from the switch.

```
SW_CORE>en
SW_CORE#conf t
Enter configuration commands,
SW_CORE(config)#no vlan 10

Command Prompt
C:\>ping -t 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Lo cual resalta la importancia de tener en cuenta la configuración de VLANs en todos los dispositivos intermedios, como switches y Multilayer Switches, cuando se busca establecer comunicación entre diferentes VLANs. La eliminación accidental o incorrecta de una VLAN puede afectar la conectividad y causar interrupciones en la red. Por lo tanto, es fundamental realizar una configuración adecuada y verificar la consistencia de las VLANs en todos los equipos involucrados para garantizar una comunicación eficiente entre VLANs en la red.

Ahora se procedió a configurar las interfaces de VLAN en el Multilayer Switch para habilitar la comunicación en capa 3 entre VLANs. En el CLI del Multilayer Switch, se utilizó el comando ***interface vlan 10*** para acceder a la configuración de la *VLAN 10*. Posteriormente, se asignó una dirección IP a esta interfaz utilizando el comando ***ip address 192.168.10.1 255.255.255.0***. Del mismo modo, se repitió el proceso para la *VLAN 20*, utilizando el comando ***interface vlan 20*** seguido del comando ***ip address 192.168.20.1 255.255.255.0*** y para validar la configuración de las interfaces VLAN creadas, se utilizó el comando ***show ip interface brief*** para verificar que ambas VLAN estuvieran en estado UP.

Figura 13

Vista CLI del MultiLayer Switch configurando las vlan 10 y 20

```
SW_CORE(config-if)#vlan 10
SW_CORE(config-vlan)#interface vlan 10
SW_CORE(config-if)#ip add 192.168.10.1 255.255.255.0
SW_CORE(config-if)#vlan 20
SW_CORE(config-vlan)#interface vlan 20
SW_CORE(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
ip add 192.168.20.1 255.255.255.0
```

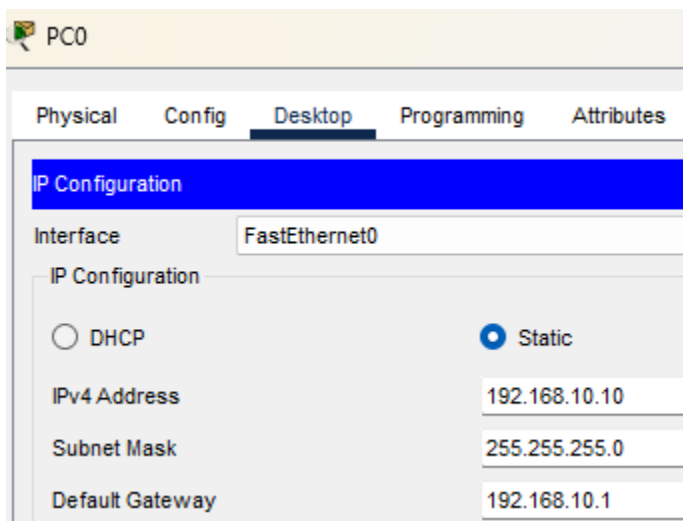
Figura 13

Vista CLI del MultiLayer Switch rectificando

GigabitEthernet1/1/1	unassigned	YES	unset	down	down
GigabitEthernet1/1/2	unassigned	YES	unset	down	down
GigabitEthernet1/1/3	unassigned	YES	unset	down	down
GigabitEthernet1/1/4	unassigned	YES	unset	down	down
Vlan1	unassigned	YES	unset	administratively down	down
Vlan10	192.168.10.1	YES	manual	up	up
Vlan20	192.168.20.1	YES	manual	up	up
SW CORE#					

Una vez configuradas las interfaces VLAN en el Multilayer Switch, se procedió a asignar el *default gateway* correspondiente a cada PC de las VLANs. En los PC de la *VLAN 10* se configuró el *default gateway* como 192.168.10.1, mientras que en los PC de la *VLAN 20* se configuró como 192.168.20.1.

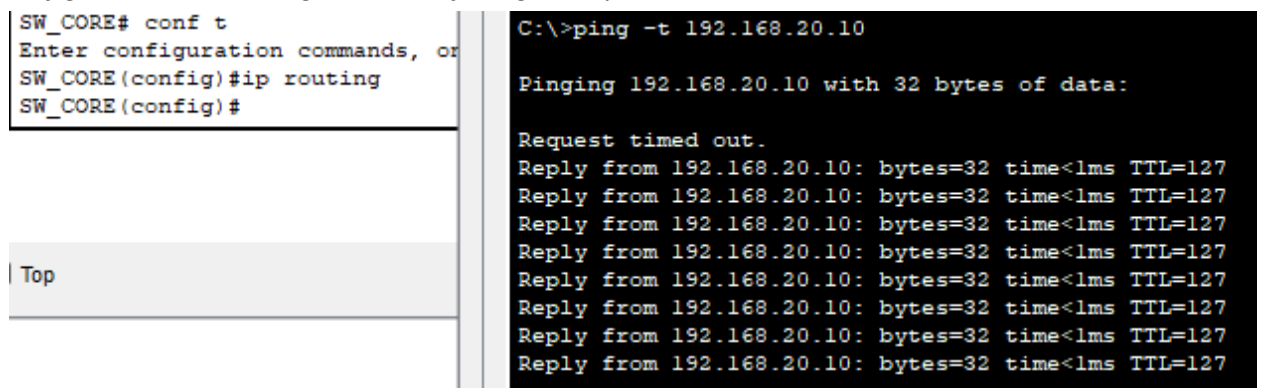
Vista IP Configuration del PC0 asignando el default gateway



Para permitir la comunicación entre las VLANs, se habilitó el enrutamiento IP en el Multilayer Switch utilizando el comando ***ip routing*** en el CLI.

Finalmente, se verificó la conectividad entre las VLANs realizando una prueba de ping desde un PC en la *VLAN 10* al otro PC en la *VLAN 20* utilizando el comando ***ping -t 192.168.20.10***, confirmando así que la comunicación inter-VLAN estaba establecida correctamente.

Vista IP Configuration del PC0 asignando el default gateway



Este proceso asegura que las VLANs estén correctamente configuradas para permitir la comunicación entre ellas y que los dispositivos puedan acceder a recursos ubicados en diferentes VLANs dentro de la red.

Conclusiones

- Es fundamental comprender la importancia de la segmentación de VLANs en la optimización del rendimiento y la seguridad de una red empresarial. La configuración adecuada de las VLANs permite organizar el tráfico de red de manera eficiente y limitar la difusión de broadcast, mejorando así la experiencia del usuario y fortaleciendo la seguridad de la red.
- Es necesario configurar todas las VLANs en los dispositivos intermedios, como switches y Multilayer Switches, para permitir la comunicación entre VLANs. Al experimentar con la eliminación de una VLAN en el Multilayer Switch, hemos observado cómo esta acción afecta la conectividad entre dispositivos en VLANs separadas, subrayando la importancia de una configuración coherente en toda la red.
- La configuración de interfaces de VLAN en capa 3 y la asignación de direcciones IP son pasos críticos para habilitar la comunicación entre VLANs. Permitiendo así implementar y mantener redes segmentadas de manera efectiva en entornos empresariales.
- La correcta configuración de las rutas entre VLANs es esencial para permitir el tráfico de datos entre diferentes segmentos de red. Estableciendo rutas estáticas en el Multilayer Switch para dirigir el tráfico entre VLANs, se brinda un mayor control sobre el flujo de datos en la red y permite diseñar topologías de red más flexibles y escalables.
- Durante las pruebas de conectividad, se corrobora la importancia de verificar la configuración y la conectividad entre dispositivos en VLANs separadas. La realización de pruebas de ping y otros

métodos de diagnóstico nos permite identificar y solucionar posibles problemas de conectividad, garantizando así un funcionamiento óptimo de la red.

Bibliografía

- De Luz, S. (2024, 20 enero). VLANs: Qué son, tipos y para qué sirven. *RedesZone*.
<https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/#446967-p-ara-que-sirven-las-vlan>
- *IBM documentation*. (s. f.).
<https://www.ibm.com/docs/es/aix/7.1?topic=cards-virtual-local-area-networks>
- Collado, E. (2018, abril 1). VTP, VLAN Trunking Protocol. Eduardo Collado.
<https://www.eduardocollado.com/2018/04/02/pocast-142-vtp-vlan-trunking-protocol/>
- Explicación del protocolo troncal de VLAN (VTP). (2024, enero 26). Cisco.
https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.html
- How do Spanning Tree Protocols work? (2023, septiembre 1). IONOS Digital Guide;
IONOS. <https://www.ionos.com/digitalguide/server/know-how/spanning-tree-protocol/>
- Walton, A. (2018, agosto 1). Spanning Tree Protocol (STP): Qué hace y cómo funciona.
CCNA desde Cero. <https://ccnadesdecero.es/spanning-tree-protocol-stp-como-funciona/>