LABORATORIO 3: SUBREDES Y VLANs

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

KEVIN NICOLÁS SIERRA GONZÁLEZ 20182020151

LUIS MIGUEL POLO 20182020158

YEISON ALEXANDER FARFAN PERALTA 20201020138

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

TELEINFORMATICA I

ANDRES ALEXANDER FONSECA

2024-III

RESUMEN

A través de este laboratorio, se puso en práctica la creación de VLANs, la asignación de direcciones IP con VLSM, y la configuración de enlaces troncales de una topología asignada en GNS3. Al haber realizado las configuraciones, las pruebas de conectividad confirmaron una comunicación exitosa entre dispositivos dentro de la misma VLAN, mientras que se bloqueó la comunicación entre VLANs distintas, validando así la correcta segmentación y la mejora en la seguridad de la red.

INTRODUCCION

En las redes actuales, la segmentación es una técnica clave para garantizar que tanto la seguridad como la eficiencia del tráfico de datos se mantengan bajo control. A medida que las redes crecen en tamaño y se conectan más dispositivos y usuarios, también aumenta la complejidad en la gestión del tráfico de datos. Sin segmentación, todo el tráfico se movería por una misma red sin restricciones, lo que aumentaría el riesgo de congestión, de accesos no autorizados y de ataques que podrían afectar a toda la infraestructura.

La segmentación permite dividir la red en diferentes segmentos o zonas más pequeñas, aislando áreas específicas, como departamentos o grupos de trabajo dentro de una organización. Esto ayuda a que cada segmento maneje su propio tráfico de datos de manera independiente, lo que significa que los usuarios o dispositivos dentro de un segmento solo pueden acceder a los recursos de ese segmento y no a los de toda la red. Esto mejora la administración porque cada segmento puede gestionarse de manera específica, con políticas de seguridad y control personalizadas.

OBJETIVOS

- Configurar las VLAN en los switches
- Configurar enlaces troncales en los switches
- Verificar la conectividad de extremo a extremo

MARCO TEORICO

VLAN

Las redes de área local virtuales (VLAN) divide los grupos de usuarios de una red física real en segmentos de red lógicas (*AIX 7.1*, 2021) es realizada en la capa de enlace de datos en la pila de protocolo, con el fin de mejorar la administración de red y la seguridad de toda la red local. Cada VLAN está identificada por un ID de VLAN, el ID de VLAN se asigna durante la configuración de la VLAN, como por ejemplo al configurar

conmutadores (switches) es necesario asignar un ID de VLAN a cada puerto. (*Implementación de VLAN Oracle Solaris 11.1*, 2013). La implementación está basada en estándar IEEE 802.1Q VLAN (enlace troncal) con la posibilidad de que se ejecute en los adaptadores Ethernet varios ID de VLAN, los adaptadores deben conectarse a un conmutador (switch) que soporte a IEEE 802.1Q VLAN (*AIX 7.1*, 2021).

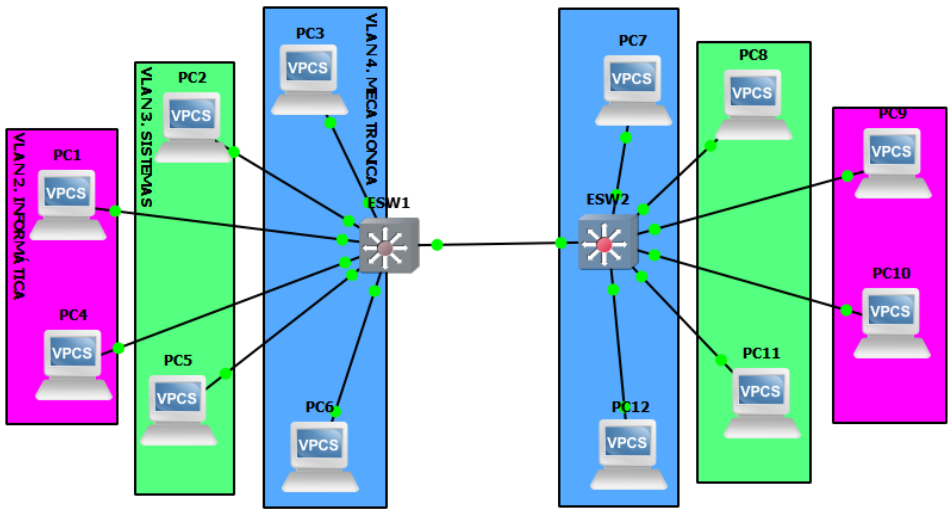
VLSM

Las máscaras de longitud variable o VLSM en inglés permite que un espacio de red se divida en partes desiguales (subredes), con VLSM la máscara de red variará dependiendo de cuantos bits se hayan prestado para una red particular, por lo tanto, es la parte variable de VLSM. En la división de subredes tradicional se asigna la misma cantidad de direcciones a cada subred. Sin embargo, las subredes que requieren menos direcciones tienen direcciones sin utilizar (desperdiciadas). Por ejemplo, los enlaces WAN sólo necesitan dos direcciones. Así que, la máscara de subred de longitud variable (VLSM) permite un uso más eficiente de direcciones debido al agotamiento del espacio público de direcciones IPv4 por lo cual se debe aprovechar al máximo las direcciones de host disponibles. (Walton, 2022)

MATERIALES

- GNS3
- IOS Cisco 2691 para EthernetSwitch1 y EthernetSwitch2

TOPOLOGIA Y DISTRIBUCIÓN DE RED



PROCEDIMIENTO

```
ESW1#vlan database
ESW1(vlan)#vlan 2 name informatica
VLAN 2 added:
    Name: informatica
ESW1(vlan)#vlan 3 name sistemas
VLAN 3 added:
    Name: sistemas
ESW1(vlan)#vlan 4 name mecatronica
VLAN 4 added:
    Name: mecatronica
```

1) Primer paso: se entra a la base de datos de las vlans que contiene el switch y se configura su nombre con cada número que le corresponde a las vlans propuestas en la topología.

```
ESW1#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
2    informatica                      active
3    sistemas                         active
4    mecatronica                      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

Con el comando show vlan-switch confirmamos que se crearon de manera efectiva las vlans.

```
ESW1(config)#interface range f1/0 - 1
ESW1(config-if-range)#switchport mode access
ESW1(config-if-range)#switchport access vlan 2
ESW1(config-if-range)#exit
ESW1(config)#interface range f1/2 - 3
ESW1(config-if-range)#switchport mode access
ESW1(config-if-range)#switchport access vlan 3
ESW1(config-if-range)#exit
ESW1(config)#interface range f1/4 - 5
ESW1(config-if-range)#switchport mode access
ESW1(config-if-range)#switchport access vlan 4
ESW1(config-if-range)#exit
```

2) Segundo paso: Dentro de la configuración del switch le asignamos las vlans correspondientes a cada puerto de fast-ethernet y que se encuentran conectados a un respectivo PC.

```
ESW2#
ESW2#
ESW2#vlan database
ESW2(vlan)#vlan 2 name informatica
VLAN 2 added:
    Name: informatica
ESW2(vlan)#vlan 3 name sistemas
VLAN 3 added:
    Name: sistemas
ESW2(vlan)#vlan 4 name mecatronica
VLAN 4 added:
    Name: mecatronica
ESW2(vlan)#exit
APPLY completed.
```

3) Tercer paso: Repetimos el primer paso para el segundo switch, dentro de la base de datos de las vlans del switch añadimos las vlans y sus respectivos nombres.

```
ESW2(config)#interface range fl/0 - 1
ESW2(config-if-range)#switchport mode access
ESW2(config-if-range)#switchport access vlan 2
ESW2(config-if-range)#exit
ESW2(config)#interface range fl/2 - 3
ESW2(config-if-range)#switchport mode access
ESW2(config-if-range)#switchport access vlan 3
ESW2(config-if-range)#exit
ESW2(config)#interface range fl/4 - 5
ESW2(config-if-range)#switchport mode access
ESW2(config-if-range)#switchport access vlan 4
ESW2(config-if-range)#exit
```

4) Cuarto paso: Repetimos el segundo paso para el segundo switch.

```
ESW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW1(config)#interface fl/15
ESW1(config-if)#switchport mode trunk
ESW1(config-if)#
*Mar  1 00:01:31.527: %DTP-5-TRUNKPORTON: Port Fa1/15 has become dotlq trunk
ESW1(config-if)#switchport trunk allowed vlan all
ESW1(config-if)#
```

5) Quinto paso: Corroboramos que en el puesto fas-ethernet 1/15 se encuentre disponible para realizar la conexión con el segundo switch, continuamos creando el enlace troncal, para establecer la conexión del primer switch con el segundo.

```
ESW2#
ESW2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW2(config)#interface fl/15
ESW2(config-if)#switchport mode trunk
ESW2(config-if)#
*Mar  1 00:02:35.151: %DTP-5-TRUNKPORTON: Port Fa1/15 has become dotlq trunk
ESW2(config-if)#switchport trunk allowed vlan all
ESW2(config-if)#
```

a. Repetimos el paso anterior para el segundo switch y así establecer de manera efectiva el enlace troncal.

```
ESW1#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14
2    informatica                      active    Fa1/0, Fa1/1
3    sistemas                         active    Fa1/2, Fa1/3
4    mecatronica                      active    Fa1/4, Fa1/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

6) Sexto paso: Corroboramos que el switch tenga las configuraciones para cada vlan que se asignó.

```
ESW1(config)#inter vlan 20
ESW1(config-if)#exit
ESW1(config)#int vlan 2
ESW1(config-if)#
*Mar  1 00:01:35.055: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
ESW1(config-if)#no sh
ESW1(config-if)#ip add 10.11.12.2 255.255.255.248
ESW1(config-if)#exit
ESW1(config)#service dhcp
ESW1(config)#ip dhcp pool info
ESW1(dhcp-config)#network
ESW1(dhcp-config)#network 10.11.12.0 255.255.255.248
ESW1(dhcp-config)#default
ESW1(dhcp-config)#default-router 10.11.12.1
ESW1(dhcp-config)#dns
ESW1(dhcp-config)#dns-server 8.8.8.4
ESW1(dhcp-config)#lease
ESW1(dhcp-config)#lease 0 7 20
ESW1(dhcp-config)#exit
ESW1(config)#ip dhcp exc
ESW1(config)#ip dhcp excluded-address 10.11.12.1 10.11.12.2
ESW1(config)#exit
```

7) Teniendo en cuenta la topología asignada para este laboratorio, tenemos 4 equipos para cada vlan por lo tanto le asignamos la máscara /29, esta brinda la posibilidad de proporcionar 6 host según la tabla de host/subred de clase A (*Explicación de las Cantidades de Hosts y Subredes*, 2024), excluyendo la dirección del DHCP server y la dirección del gateway quedan 4 direcciones de host disponibles, las direcciones que necesitamos para proporcionarles a cada PC de esta práctica de laboratorio. A continuación, para el switch 1 entramos a la configuración de la interfaz correspondiente a la vlan 2, al ser clase A, que son asignaciones para redes privadas que inician en 10.0.0.0 y la máscara para 6 host es 255.255.255.248 nuestra red comienza con 10.11.12.0, la puerta de enlace es10.11.12.1 y el dhcp server es el 10.11.12.2, excluimos las direcciones de la puerta de enlace y la del dhcp server para evitar que tengan la misma dirección con la de algún PC. Los PCs que hacen parte de la vlan 2 son PC1, PC4, PC9, PC10.

```
ESW2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW2(config)#inter vlan 2
ESW2(config-if)#
*Mar  1 00:24:43.571: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
ESW2(config-if)#no sh
ESW2(config-if)#
ESW2(config-if)#ip add 10.11.12.2 255.255.255.248
ESW2(config-if)#exit
ESW2(config)#service dhcp
ESW2(config)#ip dhcp pool info
ESW2(dhcp-config)#netw
ESW2(dhcp-config)#network 10.11.12.0 255.255.255.248
ESW2(dhcp-config)#default-rou
ESW2(dhcp-config)#default-router 10.11.12.1
ESW2(dhcp-config)#dns-
ESW2(dhcp-config)#dns-server 8.8.8.4
ESW2(dhcp-config)#lease 0 7 20
ESW2(dhcp-config)#exit
```

Repetimos el paso anterior para el switch 2 y la vlan 2.

```
ESW1(config-if)#ip add 10.11.12.10 255.255.255.248
ESW1(config-if)#exit
ESW1(config)#inter vlan 3
ESW1(config-if)#exit
ESW1(config)#service dhcp
ESW1(config)#ip dhcp pool sist
ESW1(dhcp-config)#new
ESW1(dhcp-config)#net
ESW1(dhcp-config)#networ
ESW1(dhcp-config)#network 10.11.12.8 255.255.255.248
ESW1(dhcp-config)#default-
ESW1(dhcp-config)#default-router 10.11.12.9
ESW1(dhcp-config)#dns-
ESW1(dhcp-config)#dns-server 8.8.8.4
ESW1(dhcp-config)#lease 0 7 20
ESW1(dhcp-config)#exit
ESW1(config)#ip dhcp excluded-
ESW1(config)#ip dhcp excluded-address 10.11.12.9 10.11.12.10
```

Teninedo en cuenta que la cantidad de host disponibles para asignar según la máscara y comprendiendo que la máscara 255.255.255.248 nos permite dar 8 direcciones IP las siguientes direcciones comenzaran en 10.11.12.8, por lo tanto, para la siguiente subred de vlan 3 asignaremos la dirección de dhcp server como 10.11.12.10 y la puerta de enlace siendo 10.1.12.9 y excluyendo las direcciones de l puerta de enlace y la del dhcp server.

```
PC1> ip dhcp
DORA IP 10.11.12.3/29 GW 10.11.12.1

PC1> show ip

NAME        : PC1[1]
IP/MASK     : 10.11.12.3/29
GATEWAY     : 10.11.12.1
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.2
DHCP LEASE  : 26150, 26400/13200/23100
MAC         : 00:50:79:66:68:00
LPORT       : 10054
RHOST:PORT  : 127.0.0.1:10055
MTU:        : 1500
```

Con el comando ip dhcp en el PC1 se asigna de manera automatica las direcciones ip de mascara y gatway para los PC que se encuentren en la vlan previamente configurada.

```
PC4> show ip

NAME        : PC4[1]
IP/MASK     : 10.11.12.4/29
GATEWAY     : 10.11.12.1
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.2
DHCP LEASE  : 26137, 26400/13200/23100
MAC         : 00:50:79:66:68:03
LPORT       : 10060
RHOST:PORT  : 127.0.0.1:10061
MTU:        : 1500
```

Repetimos el mismo comando para PC4 y pedimos que nos muestre la ip del PC4

```
PC9> show ip

NAME        : PC9[1]
IP/MASK     : 10.11.12.5/29
GATEWAY     : 10.11.12.1
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.2
DHCP LEASE  : 26268, 26400/13200/23100
MAC         : 00:50:79:66:68:08
LPORT       : 10070
RHOST:PORT  : 127.0.0.1:10071
MTU:        : 1500
```

Repetimos los pasos anteriores para el PC9

```
PC10> show ip

NAME        : PC10[1]
IP/MASK     : 10.11.12.6/29
GATEWAY     : 10.11.12.1
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.2
DHCP LEASE  : 26111, 26400/13200/23100
MAC         : 00:50:79:66:68:09
LPORT       : 10072
RHOST:PORT  : 127.0.0.1:10073
MTU:        : 1500
```

Repetimos los pasos anteriores para el PC10

```
DORA IP 10.11.12.11/29 GW 10.11.12.9

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 10.11.12.11/29
GATEWAY     : 10.11.12.9
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.10
DHCP LEASE  : 26396, 26400/13200/23100
MAC         : 00:50:79:66:68:01
LPORT       : 10056
RHOST:PORT  : 127.0.0.1:10057
MTU:        : 1500
```

En este PC se ve la diferencia de direcciones IP que se asignaron de manera debido a las configuraciones que se le dieron a la vlan 3 y las conexiones fast-ethernet que tiene este PC con el switch. Con el comando ip dhcp asigna la dirección, mascara y gateway de manera automática y con el comando show ip mostramos la dirección ip asignada.

```
DORA IP 10.11.12.12/29 GW 10.11.12.9

PC5> show ip

NAME        : PC5[1]
IP/MASK     : 10.11.12.12/29
GATEWAY     : 10.11.12.9
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.10
DHCP LEASE  : 26396, 26400/13200/23100
MAC         : 00:50:79:66:68:04
LPORT       : 10062
RHOST:PORT  : 127.0.0.1:10063
MTU:        : 1500
```

Repetimos los comandos anteriormente comentados para el PC 5 que también pertenece a la vlan 3.

Preguntas

- ¿Qué implicaciones tiene para la red el uso de VLANs?

  Las VLANs permiten segmentar la red definiendo LANs Virtuales, es decir facilita la comunicación entre una misma área o departamento, que no están físicamente en el mismo espacio o que están distribuida en varias partes por ejemplo en una organización (como en distintos pisos de un edificio). Esto promueve que haya mejor seguridad en la red, donde determinado grupo de usuarios tengan accesibilidad a cierta parte de la red.

- ¿Qué ocurre si intenta corroborar conexión con equipos de la misma VLAN y de diferentes (haciendo ping)?

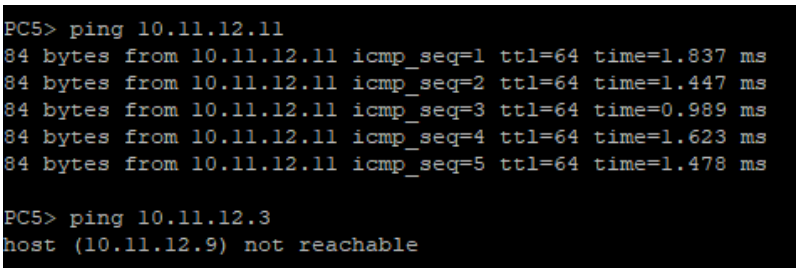
  Cuando se prueba conectividad entre equipos que pertenecen a la misma VLAN por medio del protocolo ICMP con el comando ping, la conectividad es exitosa, es decir, los equipos pueden comunicarse. Por ejemplo, en la topología se hace ping entre el PC9 y PC1 que pertenecen a la VLAN 2 donde se envían varios paquetes por el PC9 y se reciben de manera exitosa por el PC1.

```
PC9> show ip

NAME        : PC9[1]
IP/MASK     : 10.11.12.5/29
GATEWAY     : 10.11.12.1
DNS         : 8.8.8.4
DHCP SERVER : 10.11.12.2
DHCP LEASE  : 26268, 26400/13200/23100
MAC         : 00:50:79:66:68:08
LPORT       : 10070
RHOST:PORT  : 127.0.0.1:10071
MTU:        : 1500

PC9> ping 10.11.12.3
84 bytes from 10.11.12.3 icmp_seq=1 ttl=64 time=1.086 ms
84 bytes from 10.11.12.3 icmp_seq=2 ttl=64 time=2.213 ms
84 bytes from 10.11.12.3 icmp_seq=3 ttl=64 time=1.464 ms
84 bytes from 10.11.12.3 icmp_seq=4 ttl=64 time=1.307 ms
84 bytes from 10.11.12.3 icmp_seq=5 ttl=64 time=1.350 ms
```

Cuando se prueba conectividad entre equipos que no pertenecen a la misma VLAN aun cuando se encuentre en la misma LAN física (conectados por el mismo Switch) no pueden comunicarse entre sí, los paquetes enviados de un host origen en una VLAN por el protocolo ICMP con el comando ping no son recibidos en el host destino de otra VLAN. Por ejemplo, inicialmente se hace ping entre el PC5 y el PC2 donde si se establece comunicación, porque pertenecen a la misma VLAN 2, pero al hacer ping a la dirección ip 10.11.12.3 del PC1 que pertenece a la VLAN 1, no fue exitoso, no pudo establecerse una comunicación.



- ¿Para qué se emplean los enlaces troncales?

  Estos enlaces permiten transmitir todo el tráfico de red realizado por todas las VLANs a través de dispositivos como switches, es decir todos los tráficos de red realizados por cada una de las VLANs converge en dispositivos como el switch que está configurado con un enlace troncal y luego se envía por este enlace y es recibido por otro dispositivo como otro switch que también está configurado con un enlace troncal, que luego segmenta a cada VLAN.

- ¿Qué beneficio le presta el uso de VLSM?

  El uso de VLSM permite dividir una red en varias subredes que pueden tener diferentes máscaras de red, es decir, diferentes tamaños de hosts con el fin de utilizar el menor número posible de direcciones ip de acuerdo con la cantidad de hosts qué hay en cada una de las subredes, para que puedan aprovecharse de manera eficiente y no desperdiciar direcciones ip de una red específica.

- ¿Cuántas máscaras de subred creo para su configuración?

  Se utilizó una máscara de subred para cada VLAN, la cual fue 255.255.255.248 con prefijo /29 que admite 6 hosts, la cual nos permitió crear tres subredes, es decir, para cada VLAN, las subredes fueron 10.11.12.0/29; 10.11.12.8/29 y 10.11.12.16/29

- ¿Qué concluye respecto a la seguridad de la red?

La configuración de VLANs en una red e implementar VLSM es importante porque permite segmentar la red y utilizar de manera eficiente las direcciones de hosts, minimiza el impacto de un ataque o intrusión a la red por usuarios no autorizados, al no estar expuesta o vulnerable toda la red sino sólo una parte (VLAN) a la cual el atacante logró acceder, restringiéndose lo más posible el acceso a otras partes de la red (otras VLANs) y poderse aislar esa parte de red y no toda la red para actuar frente a estos problemas de seguridad.

CONCLUSIONES

Configuración de VLAN en los switches

La segmentación de la red mediante VLANs permite agrupar usuarios y dispositivos de acuerdo a criterios lógicos, mejorando la administración y la seguridad. Cada VLAN se identifica con un ID único, y su correcta configuración asegura que los dispositivos dentro de la misma puedan comunicarse sin interferencias externas. La práctica demostró que, al asignar correctamente las VLANs a los puertos de los switches, se logró una comunicación efectiva entre los dispositivos dentro de la misma VLAN, mientras que los dispositivos de diferentes VLANs no pudieron comunicarse, lo que confirma la efectividad de la segmentación.

Configuración de enlaces troncales en los switches

Los enlaces troncales son esenciales para permitir la comunicación entre múltiples VLANs a través de un único enlace físico. La configuración adecuada de estos enlaces asegura que el tráfico de todas las VLANs se transmita de manera eficiente entre switches. En la práctica, se establecieron enlaces troncales entre los switches, lo que permitió la transmisión del tráfico de todas las VLANs configuradas, garantizando así que la red mantenga su integridad y funcionalidad.

Verificación de la conectividad de extremo a extremo

La verificación de la conectividad de extremo a extremo es crucial para asegurar que la red funcione como se espera. Durante la práctica, se realizaron pruebas de conectividad utilizando el comando ping, lo que permitió confirmar que los dispositivos dentro de la misma VLAN podían comunicarse exitosamente. Sin embargo, se observó que los dispositivos en diferentes VLANs no podían establecer conexión, lo que reafirma la importancia de la configuración de VLANs para la seguridad y el control del tráfico en la red. Esto demuestra que la segmentación de la red no solo mejora la organización, sino que también aumenta la seguridad al limitar la comunicación entre diferentes segmentos de la red.

BIBLIOGRAFÍA

AIX 7.1. (2021, 3 marzo). IBM. https://www.ibm.com/docs/es/aix/7.1?topic=cards-virtual-local-area-networks

Implementación de VLAN: descripción general - Gestión del rendimiento de red de Oracle Solaris 11.1. (2013, 1 enero). https://docs.oracle.com/cd/E37929_01/html/E36606/fpjve.html

Walton, A. (2022, 2 noviembre). *▷ VLSM: Máscaras de subred de longitud variable » CCNA 200-301*. CCNA Desde Cero. https://ccnadesdecero.es/vlsm-mascaras-subred-longitud-variable/

Explicación de las cantidades de hosts y subredes. (2024, 16 febrero). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/routing-information-protocol-rip/13790-8.html