



UNIVERSIDAD DE LAS FUERZAS ARMADAS

REDES DE COMPUTADORES

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Configuración de VLANs y Enlaces Troncales

Estudiantes:

Ednan Josué Merino Calderón

Docente:

Ing. Walter Marcelo Fuertes Diaz

1. Objetivos de Aprendizaje

1.1. Objetivo General

Configurar una red con múltiples VLANs y enlaces troncales en Cisco Packet Tracer para simular un entorno de red segmentado, asegurando la comunicación adecuada entre dispositivos dentro de la misma VLAN y manteniendo el aislamiento entre VLANs diferentes.

1.2. Objetivos Específicos

- **Configuración de VLANs:**
 - Crear dos VLANs en los switches: VLAN 100 (Administrativa) y VLAN 200 (Contabilidad).
 - Asignar los puertos de los switches correspondientes a las VLANs apropiadas.
 - Verificar que los dispositivos en la misma VLAN puedan comunicarse entre sí.
- **Configuración de Enlaces Troncales:**
 - Configurar los enlaces troncales entre los switches para permitir el tráfico de múltiples VLANs.
 - Verificar que el tráfico de las VLANs se transmita correctamente a través de los enlaces troncales.
- **Asignación de Direcciones IP:**
- **Pruebas de Conectividad:**
 - Realizar pruebas de ping entre dispositivos dentro de la misma VLAN para verificar la conectividad.
 - Realizar pruebas de ping entre dispositivos en diferentes VLANs para verificar el aislamiento de tráfico.
- **Documentación y Análisis:**
 - Documentar cada paso de la configuración, incluyendo comandos utilizados y resultados observados.
 - Analizar y explicar cualquier problema encontrado durante la configuración y cómo se resolvió.

2. Topología de Prueba

1. Laptop
2. Conexión a Internet
3. Sistema operativo Windows/Linux
4. Cisco Packet Tracer

3. Marco Teórico

Una VLAN (Red de Área Local Virtual) es una subred lógica que agrupa un conjunto de dispositivos dentro de una red LAN física más grande, aunque estos dispositivos no estén físicamente conectados en la misma ubicación. Las VLANs permiten que los administradores de red segmenten una red física en múltiples redes lógicas, mejorando la gestión, la seguridad y el rendimiento de la red. Una de las principales características de las VLANs es la segmentación lógica, que permite dividir la red en subredes lógicas sin importar la ubicación física de los dispositivos. Esto facilita la administración de la red y mejora la eficiencia al reducir el dominio de difusión, limitando así la cantidad de tráfico innecesario que puede ralentizar la red. Además, las VLANs ofrecen una capa adicional de seguridad al permitir que los dispositivos de diferentes VLANs no se comuniquen directamente entre sí a menos que se configure específicamente para permitirlo.

Otro beneficio significativo de las VLANs es la mejora en la gestión del ancho de banda. Al segmentar la red, se puede asignar ancho de banda específico a diferentes VLANs según las necesidades de cada grupo de usuarios o dispositivos, optimizando así el uso de los recursos de red. Las VLANs también simplifican la administración de redes grandes y complejas, ya que los administradores pueden gestionar de manera centralizada los dispositivos de red y aplicar políticas uniformes de seguridad y gestión de tráfico. Además, las VLANs permiten una mayor flexibilidad en la reconfiguración de la red, ya que los dispositivos pueden ser reasignados a diferentes VLANs sin necesidad de cambiar la infraestructura física de la red.

En el contexto de las VLANs, los enlaces troncales juegan un papel crucial. Un enlace troncal es una conexión que transporta tráfico de múltiples VLANs entre dos dispositivos de red, generalmente switches. Estos enlaces utilizan un proceso de etiquetado (tagging) para identificar a qué VLAN pertenece cada paquete de datos, utilizando estándares como IEEE 802.1Q. El etiquetado permite que múltiples VLANs compartan un solo enlace físico, maximizando la eficiencia y reduciendo la necesidad de múltiples cables. Esto es especialmente útil en redes grandes, donde sería impráctico tener un

enlace físico separado para cada VLAN. Los enlaces troncales son esenciales para mantener la integridad de la segmentación de la red a medida que el tráfico se mueve a través de diferentes partes de la infraestructura de red.

4. Desarrollo

A través de 3 Switchs se diagrama la red. El Switch 1 se conecta a dos computadoras, el Switch 2 se conecta a 2 computadoras y hay un Switch 0 que conecta a los dos switches:

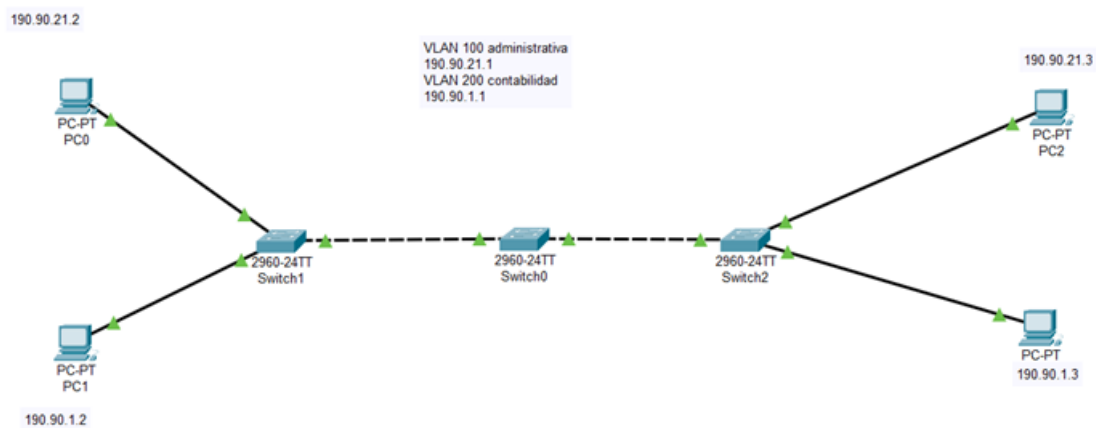


Figura 1: Red Física

A cada PC se le agrega una dirección estática como se demuestra en el diagrama:

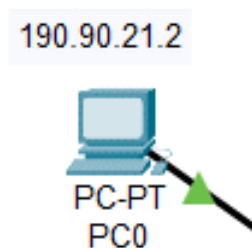


Figura 2: ip 1

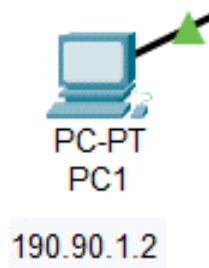


Figura 3: ip 2

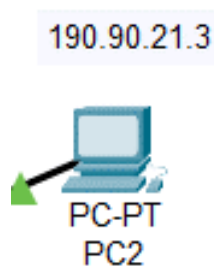


Figura 4: ip 3

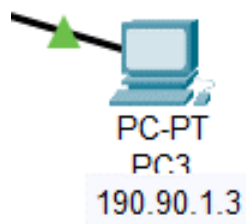


Figura 5: ip 4

Se accede al modo de configuración de administración de cada switch, se crean las VLANs y se les agrega el nombre:

- VLAN 100: administrativa
- VLAN 200: contabilidad

Configuración de VLANs y Enlaces Troncales

```
1 Switch>enable
2 Switch#conf t
3 Switch(config)#vlan 100
4 Switch(config-vlan)#name administrativa
5 Switch(config-vlan)#vlan 200
6 Switch(config-vlan)#name contabilidad
```

Acto seguido se da acceso a los puertos (Debidamente llamados) en los switches 1 y 2, a través de los comandos:

```
1 Switch(config-vlan)#int f0/2
2 Switch(config-if)#switchport acces vlan 100
3 Switch(config-if)#int f0/1
4 Switch(config-if)#switchport acces vlan 200
```

Después, se establecen los enlaces troncales mediante los comandos:

```
1 Switch(config-if)#int f0/3
2 Switch(config-if)#switchport mode trunk
3 Switch(config-if)#switchport trunk native vlan 1
```

Se hace la prueba de comunicación de paquetes entre VLANs iguales con éxito:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC0	PC2	ICMP		0.000
	Successful	PC1	PC3	ICMP		0.000

Figura 6: Prueba Exitosa


Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC0	PC2	ICMP		0.000
	Successful	PC1	PC3	ICMP		0.000

Figura 7: Prueba Exitosa

Se hace la prueba de comunicación de paquetes entre VLANs diferentes y se prueba que no se puede realizar con éxito:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Failed	PC0	PC3	ICMP		0.000
	Failed	PC1	PC2	ICMP		0.000

Figura 8: Prueba Fallida

```
C:\>ping 190.90.1.2

Pinging 190.90.1.2 with 32 bytes of data:

Request timed out.

Ping statistics for 190.90.1.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss)
```

Figura 9: Prueba Fallida

5. Conclusiones

La configuración de VLANs y enlaces troncales en una red utilizando Cisco Packet Tracer proporciona una comprensión práctica de cómo segmentar y gestionar redes de manera eficiente. Al crear VLANs, se mejora la seguridad y la administración de la red al permitir que los dispositivos se agrupen lógicamente sin importar su ubicación física. Esto facilita la reducción del dominio de difusión y la optimización del uso del ancho de banda.

La configuración de enlaces troncales es esencial para transportar tráfico de múltiples VLANs a través de un único enlace físico, maximizando la eficiencia y simplificando la infraestructura de red. El uso del estándar IEEE 802.1Q para el etiquetado de VLAN garantiza que el tráfico se identifique y dirija correctamente a lo largo de la red, manteniendo la integridad de la segmentación.

Las pruebas de conectividad y el aislamiento de tráfico entre VLANs demostraron la efectividad de la configuración y proporcionaron una validación práctica de los conceptos teóricos. Además, la posibilidad de configurar enrutamiento inter-VLAN permite una mayor flexibilidad y funcionalidad en redes más complejas, facilitando la comunicación entre diferentes segmentos de la red.

6. Referencias

- Fernández, L. (2024, 10 abril). Cómo configurar un enlace trunk en un switch gestionable. RedesZone. <https://www.redeszone.net/tutoriales/redes-cable/configurar->

enlace-troncal-switch/

- Aprende Redes.com» Enlaces troncales. (s. f.). <https://aprenderedes.com/2019/12/trunking/>
- Walton, A. (2020, 10 junio). Enlaces Troncales de VLAN» CCNA desde Cero. CCNA Desde Cero. <https://ccnadesdecero.es/enlaces-troncales-vlan/>



UNIVERSIDAD DE LAS FUERZAS ARMADAS

REDES DE COMPUTADORES

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Configuración de VLANs y Enlaces Troncales

Estudiantes:

Ednan Josué Merino Calderón

Docente:

Ing. Walter Marcelo Fuertes Diaz

Objetivos

- **Configurar y verificar el enrutamiento RIP v2:**
 - Aprender a habilitar el protocolo de enrutamiento RIP versión 2 en routers.
 - Comprender las diferencias entre RIP v1 y RIP v2, especialmente en el manejo de subredes y direcciones IP.
- **Implementar configuraciones básicas de enrutamiento:**
 - Configurar las interfaces de los routers con direcciones IP y máscaras de subred adecuadas.
 - Habilitar y verificar el enrutamiento dinámico utilizando RIP v2 en una red pequeña.
- **Propagación de rutas entre routers:**
 - Asegurarse de que todas las rutas dentro de la red se propagan correctamente utilizando el protocolo RIP v2.
 - Verificar la tabla de enrutamiento en cada router para confirmar que todas las rutas se han aprendido y que el enrutamiento es funcional.
- **Solucionar problemas de enrutamiento:**
 - Identificar y corregir problemas comunes que pueden surgir al configurar RIP v2, como la falta de rutas o configuraciones incorrectas.
 - Implementar comandos de diagnóstico, como `show ip route`, para verificar la conectividad y la propagación de rutas.

1. Topología de Prueba

1. Laptop
2. Conexión a Internet
3. Sistema operativo Windows/Linux
4. Cisco Packet Tracer

Desarrollo

- **Configuración inicial de los routers:**

- Conectar los routers entre sí utilizando cables adecuados y asegurarse de que todas las interfaces estén activas.
 - Asignar direcciones IP a las interfaces según el esquema de direccionamiento proporcionado en la práctica.
 - Configurar las interfaces en cada router utilizando el comando `interface` y `ip address`.
- **Habilitar RIP v2 en cada router:**
- Ingresar al modo de configuración global en cada router.
 - Activar el protocolo RIP v2 usando el comando `router rip`.
 - Configurar el protocolo para utilizar la versión 2 exclusivamente con el comando `version 2`.
 - Publicar las redes directamente conectadas utilizando el comando `network`.
- **Verificación de la configuración:**
- Utilizar el comando `show ip protocols` para verificar que RIP v2 esté configurado correctamente y que las redes se estén anunciando.
 - Revisar la tabla de enrutamiento con el comando `show ip route` para asegurar que todas las rutas se hayan aprendido correctamente a través de RIP v2.
 - Realizar pruebas de conectividad usando `ping` entre dispositivos en diferentes redes para comprobar que el enrutamiento funcione como se espera.
- **Solución de problemas:**
- Revisar la configuración en busca de errores comunes, como redes faltantes en la configuración de RIP o interfaces que no estén correctamente configuradas.
 - Utilizar comandos de depuración como `debug ip rip` si es necesario, para observar el tráfico RIP y solucionar problemas más detallados.
 - Asegurarse de que todas las rutas se propagan adecuadamente entre los routers y corregir cualquier discrepancia.

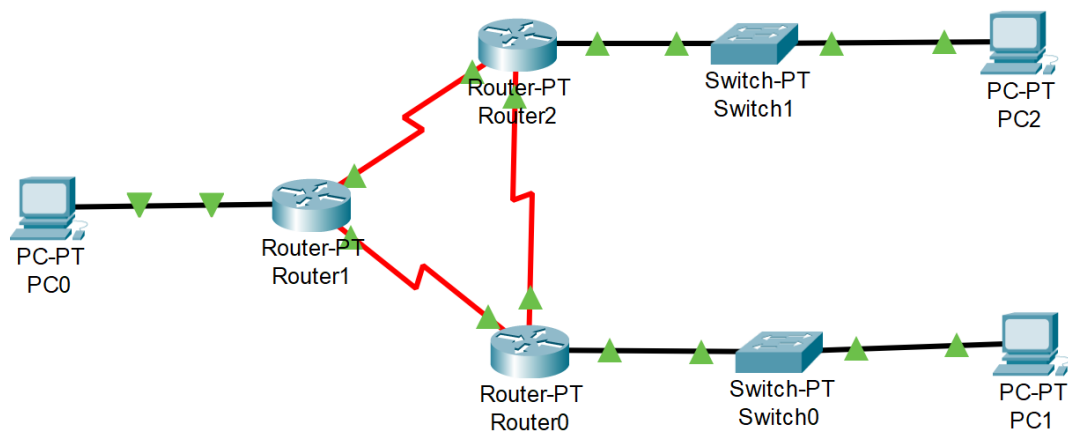


Figura 1: Rip v2

Conclusiones

- La configuración de RIP v2 permite la implementación de enrutamiento dinámico en redes pequeñas, facilitando la propagación de rutas entre routers sin necesidad de configuraciones manuales extensas.
- RIP v2 mejora sobre RIP v1 al soportar subredes y al utilizar el enrutamiento basado en IP claseless, lo que permite una mayor flexibilidad en la configuración de redes.
- La verificación y solución de problemas son cruciales para garantizar que el protocolo RIP v2 funcione correctamente y que las rutas se propaguen adecuadamente. Los comandos de diagnóstico, como `show ip route` y `debug ip rip`, son herramientas esenciales para identificar y resolver problemas.
- La práctica proporciona una comprensión sólida de cómo configurar y verificar RIP v2, destacando la importancia de la correcta configuración de las interfaces y la correcta implementación del protocolo en cada router.

Referencias

- Fernández, L. (2024, 10 abril). Cómo configurar un enlace trunk en un switch gestionable. RedesZone. <https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/>

- Aprende Redes.com» Enlaces troncales. (s.f.). <https://aprenderedes.com/2019/12/trunking/>
- Walton, A. (2020, 10 junio). Enlaces Troncales de VLAN» CCNA desde Cero. CCNA Desde Cero. <https://ccnadesdecero.es/enlaces-troncales-vlan/>



UNIVERSIDAD DE LAS FUERZAS ARMADAS

REDES DE COMPUTADORES

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

Configuración de un Switch en GNS3

Estudiantes:

Ednan Josué Merino Calderón

Docente:

Ing. Walter Marcelo Fuertes Diaz

Objetivos

- **Configurar y verificar el enrutamiento RIP v2:**
 - Aprender a habilitar el protocolo de enrutamiento RIP versión 2 en routers.
 - Comprender las diferencias entre RIP v1 y RIP v2, especialmente en el manejo de subredes y direcciones IP.
- **Implementar configuraciones básicas de enrutamiento:**
 - Configurar las interfaces de los routers con direcciones IP y máscaras de subred adecuadas.
 - Habilitar y verificar el enrutamiento dinámico utilizando RIP v2 en una red pequeña.
- **Propagación de rutas entre routers:**
 - Asegurarse de que todas las rutas dentro de la red se propagan correctamente utilizando el protocolo RIP v2.
 - Verificar la tabla de enrutamiento en cada router para confirmar que todas las rutas se han aprendido y que el enrutamiento es funcional.
- **Solucionar problemas de enrutamiento:**
 - Identificar y corregir problemas comunes que pueden surgir al configurar RIP v2, como la falta de rutas o configuraciones incorrectas.
 - Implementar comandos de diagnóstico, como `show ip route`, para verificar la conectividad y la propagación de rutas.

1. Topología de Prueba

1. Laptop
2. Conexión a Internet
3. Sistema operativo Windows/Linux
4. Cisco Packet Tracer

Introducción

Configurar un switch en GNS3 es una habilidad clave para cualquier profesional de redes. Los switches son componentes esenciales en la infraestructura de una red, ya

que permiten conectar varios dispositivos y gestionar eficientemente el tráfico de datos. Estos dispositivos operan principalmente en la capa 2 del modelo OSI (Interconexión de Sistemas Abiertos), utilizando direcciones MAC (Control de Acceso de Medios) para tomar decisiones sobre el reenvío de paquetes. Los switches no solo facilitan la comunicación dentro de una red local (LAN), sino que también optimizan el uso del ancho de banda y mejoran la seguridad mediante técnicas como el filtrado de direcciones MAC y la creación de VLANs.

Interfaz de Administración y Configuración

Configurar un switch implica varios pasos clave para asegurar su correcta operación y administración. Uno de los primeros pasos es asignar una dirección IP a la interfaz de gestión del switch, generalmente la interfaz VLAN 1, lo que permite la administración remota del dispositivo.

Desarrollo

Paso 1: Se instala GNS3 desde la [https://www.gns3.com/página oficial](https://www.gns3.com/página%20oficial) y abrilo.

Paso 2: Se crea un nuevo proyecto llamado "switch3725"

Paso 3: Se descarga la IOS e importamos nuestro modelo de switch entrando a preferencias ¿Dynamips ¿IOS Routers ¿New

Paso: 4 Se coloca el switch importado en el proyecto, se lo inicia y se lo abrimos en modo de consola.

Paso: 5 Entrar en el modo de configuración global

```
Switch> enable
Switch# configure terminal
```

Paso: 6 Cambiar de nombre al switch

```
Switch(config)# hostname espe
espe(config)#
```

Paso: 7 Configurar la interfaz VLAN 1 con una dirección IP


```
espe(config)# interface vlan 1
espe(config-if)# ip address 192.168.1.2 255.255.255.0
espe(config-if)# no shutdown
```

Paso: 8 Configura el mensaje del día

```
espe(config)# banner motd #Mi Primera Configuración en Cisco#
```

Paso: 9 Configura la contraseña para el acceso al modo privilegiado:

```
espe(config)# enable secret espe123
```

Paso: 10 Configura la contraseña para el acceso por consola:

```
espe(config)# line console 0
espe(config-line)# password espe123
espe(config-line)# login
espe(config-line)# exit
```

Paso: 11 Configura la contraseña para el acceso por terminal virtual (VTY)

```
espe(config)# line vty 0 4
espe(config-line)# password
```

Paso: 12 Salir del modo de Configuración y Guardar Cambios

```
espe(config-if)# exit
espe# write memory
```

Paso: 13 Mostrar Contraseñas No Encriptadas

```
espe# show running-config
```

Conclusiones

La configuración de switches en GNS-3 es una habilidad clave para los profesionales de redes, permitiéndoles diseñar, implementar y gestionar redes de manera eficiente. La práctica en este entorno simulado proporciona una comprensión profunda de principios como la asignación de direcciones IP, la activación de interfaces y la creación de VLANs, mejorando la seguridad y el rendimiento de la red. Además, dominar estas habilidades en GNS-3 prepara a los profesionales para enfrentar desafíos en redes reales, garantizando una infraestructura robusta y confiable.

Referencias

- Cesar. (2023, 16 marzo). ¿Qué es GNS3 y para qué sirve? Topologías de Red. <https://topologiasdered.com/simulador/que-es-gns3-vm/>
- colaboradores de Wikipedia. (2024h, julio 16). GNS3. Wikipedia, la Enciclopedia Libre. <https://es.wikipedia.org/wiki/GNS3>