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:

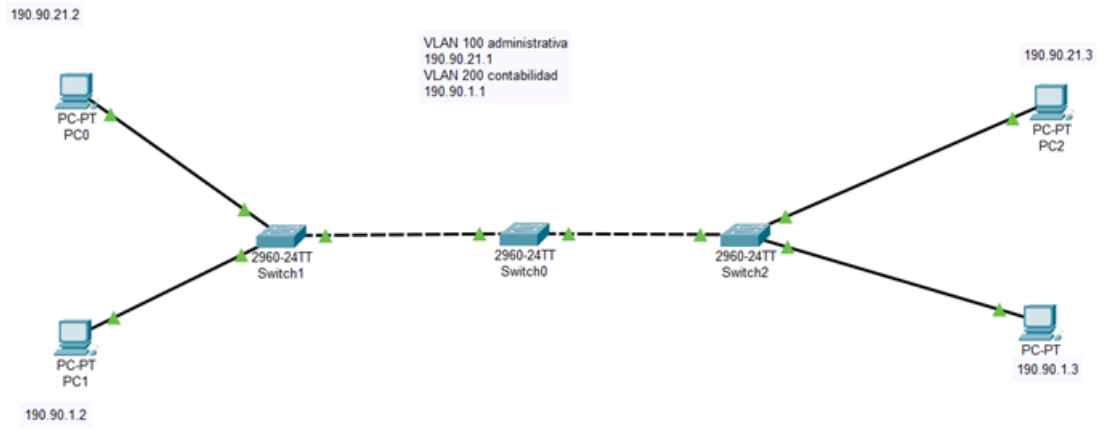

Figura 1: Red Física

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

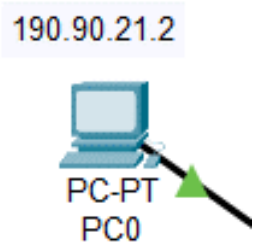

Figura 2: ip 1

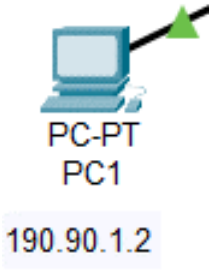

Figura 3: ip 2

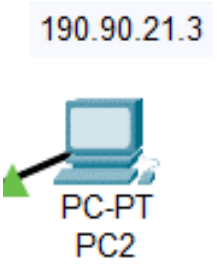

Figura 4: ip 3

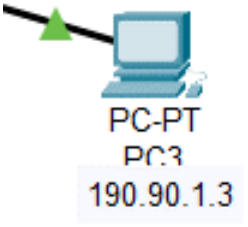

Figura 5: ip 4

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

```
Switch>enable
Switch#conf t
Switch(config)#vlan 100
Switch(config-vlan)#name administrativa
Switch(config-vlan)#vlan 200
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:

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

Después, se establecen los enlaces troncales mediante los comandos:

```
Switch(config-if)#int f0/3
Switch(config-if)#switchport mode trunk
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

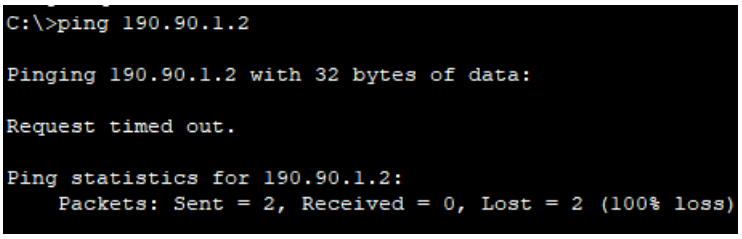

Figura 9: Prueba Fallida

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 Single-Area OSPFv2

Estudiantes:
Ednan Josué Merino Calderón

Docente:
Ing. Walter Marcelo Fuertes Diaz

Objetivos de Aprendizaje

Objetivos

- Crear la red y configurar los parámetros básicos de los dispositivos.
- Configurar y verificar OSPFv2 de área única para el funcionamiento básico.
- Optimizar y verificar la configuración OSPFv2 de área única.

Topología de Prueba

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

Marco Teórico

Desarrollo

Construir la red y configurar ajustes básicos de los dispositivos

1. Realizar el cableado de red

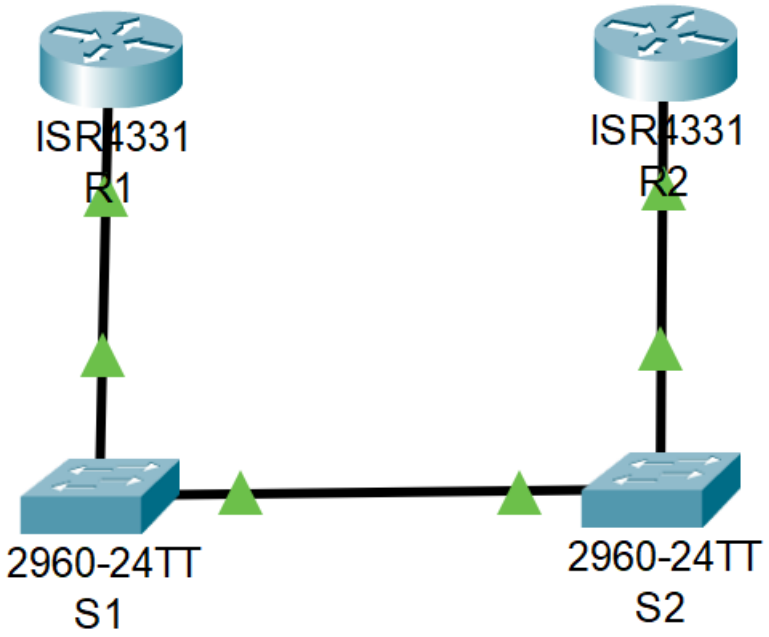

Figura 1: Red

2. Configurar los parámetros básicos para cada router

   a) Asignar un nombre a cada router.

```
router(config)# hostname R1
router(config)# hostname R2
```

   b) Inhabilitar la búsqueda DNS, para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

```
R1(config)# no ip domain lookup
R2(config)# no ip domain lookup
```

   c) Asignar class como la contraseña cifrada del modo EXEC privilegiado.

```
R1(config)# enable secret class
R2(config)# enable secret class.
```

   Asignar cisco como la contraseña de la consola y habilite el inicio de sesión.

```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R2(config)# line console 0
```

```
R2 (config-line) # password cisco
R2 (config-line) # login
```

d) Asignar cisco como la contraseña de VTY y habilite el inicio de sesión

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R2 (config) # line vty 0 4
R2 (config-line) # password cisco
R2(config-line) # login
```

e) Cifrar las contraseñas

```
R1(config)# service password-encryption
R2(config)# service password-encryptiong
```

f) Crear un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
R1(config)# banner motd $ Authorized Users Only! $
R2(config)# banner motd $ Authorized Users Only! $
```

g) Guardar la configuración en ejecución en el archivo de configuración de inicio

```
R1# copy running-config startup-config
R2# copy running-config startup-config
```

3. Configurar cada switch

a) Asignar un nombre a cada router.

```
router(config)# hostname S1
router(config)# hostname S2
```

b) Inhabilitar la búsqueda DNS, para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.

```
S1(config)# no ip domain lookup
S2(config)# no ip domain lookup
```

c) Asignar class como la contraseña cifrada del modo EXEC privilegiado.

```
S1(config)# enable secret class
S2(config)# enable secret class.
```

Asignar cisco como la contraseña de la consola y habilite el inicio de sesión.

```
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line console 0
S2 (config-line) # password cisco
S2 (config-line) # login
```

d) Asignar cisco como la contraseña de VTY y habilite el inicio de sesión

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S2 (config) # line vty 0 4
S2 (config-line) # password cisco
S2(config-line) # login
```

e) Cifrar las contraseñas

```
S1(config)# service password-encryption
S2(config)# service password-encryptiong
```

f) Crear un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

```
S1(config)# banner motd $ Authorized Users Only! $
S2(config)# banner motd $ Authorized Users Only! $
```

g) Guardar la configuración en ejecución en el archivo de configuración de inicio

```
S1# copy running-config startup-config
S2# copy running-config startup-config
```

4. Configurar y verificar la operación básica de OSPFv2
5. Optimizar la configuración de the OSPFv2

Conclusiones

- **Configuración básica y seguridad:** La configuración inicial de los routers y switches, incluyendo la asignación de nombres, la deshabilitación de la búsqueda DNS, y la configuración de contraseñas cifradas, es fundamental para asegurar la seguridad y el buen funcionamiento de la red. Este paso asegura que los dispositivos estén protegidos contra accesos no autorizados.

- **Implementación de OSPFv2:** La configuración y verificación de OSPFv2 de área única permite una eficiente propagación de rutas en la red. Este protocolo es esencial para redes de tamaño medio donde se requiere una convergencia rápida y una gestión eficaz de rutas.
- **Optimización de OSPFv2:** La optimización adicional de OSPFv2 mejora el rendimiento de la red, reduciendo la latencia y mejorando la estabilidad. Es crucial realizar ajustes después de la configuración inicial para garantizar que la red opere de manera óptima, adaptándose a cambios y cargas de trabajo variables.
- **Importancia de la verificación:** La verificación de cada paso, desde la configuración básica hasta la implementación y optimización de OSPFv2, asegura que la red esté configurada correctamente y funcionando según lo esperado. Esto ayuda a identificar y corregir errores tempranamente, lo que es vital para el mantenimiento de una red robusta y fiable.
- **Uso de herramientas de simulación:** El uso de Cisco Packet Tracer para la simulación de la red es una práctica valiosa para el aprendizaje y la experimentación antes de implementar configuraciones en un entorno de producción. Esto permite una comprensión más profunda de los procesos y reduce el riesgo de errores en la configuración real.

UNIVERSIDAD DE LAS FUERZAS ARMADAS

Redes de Computadores

Departamento de Ciencias de la Computación

Configuración de Routers Estáticos

Estudiantes:
Ednan Josué Merino Calderón

Docente:
Ing. Walter Marcelo Fuertes Diaz

Objetivos de Aprendizaje

- Aprender a configurar rutas estáticas en routers para dirigir el tráfico entre diferentes redes.
- Usar comandos para verificar que las rutas estáticas están configuradas correctamente y que el tráfico se enruta adecuadamente.

Desarrollo

Modelo Físico

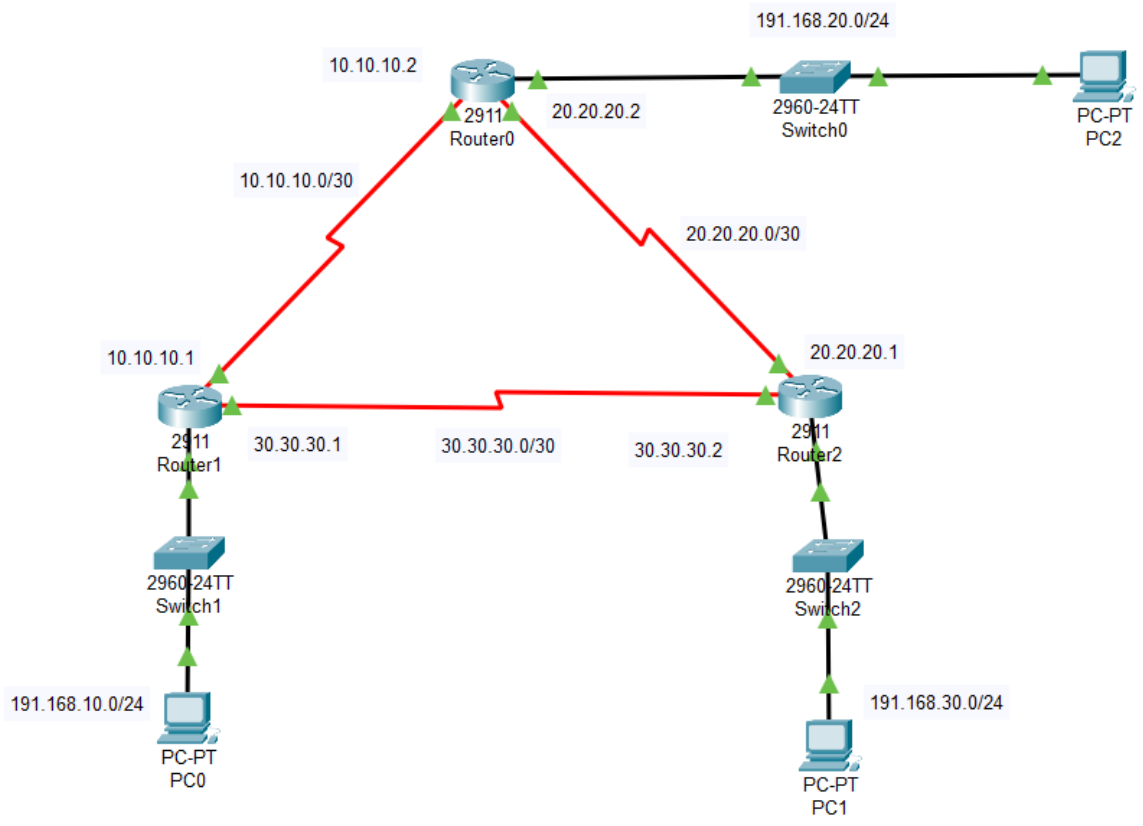

Figura 1: Modelo Físico

Configuración Router 1

```
Router>enable
```

```
Router#
Router#config ter
Router(config)#
Router(config)#hostname R1
R1(config)#
!Configuración Puerto Serial
R1(config)#interface Serial0/3/0
R1(config-if)#ip address 192.168.2.1 255.225.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.225.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
```

Configuración Router 2

```
Router>enable
Router#
Router#config ter
Router(config)#
Router(config)#hostname R2
R2(config)#
!Configuración Puerto Serial
R2(config)#interface Serial0/3/0
R2(config-if)#ip address 192.168.2.2 255.225.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface Serial0/3/1
R2(config-if)#ip address 192.168.4.1 255.225.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
!Configuración Gigabit Ethernet
R2(config)#interface GigabitEthernet0/0
R2(config-if)#ip address 192.168.3.1 255.225.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Configuración Router 3

```
Router>enable
Router#
Router#config ter
Router(config)#
Router(config)#hostname R3
R3(config)#
!Configuración Puerto Serial
R3(config)#interface Serial0/3/0
R3(config-if)#ip address 192.168.4.2 255.225.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
!Configuración Gigabit Ethernet
R3(config)#interface GigabitEthernet0/0
R3(config-if)#ip address 192.168.5.1 255.225.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

Configuración de los computadores

1. Acceder a los computadores
2. Ir al apartado de destktop
3. Seleccionar la opción de Ip Configuration
4. Asginar la siguiente dirección Ip a la primer computadora 192.168.1.10
5. Asignar la siguiente submáscara 255.255.255.0
6. Asignar el gateway por default 192.168.1.1
7. Para la segunda computadora repetimos los pasos anteriores pero con las siguientes direcciones, para la Ip 192.168.2.10, para la submáscara 255.255.255.0 y para el gateway por default 192.168.2.1
8. Para la tercera computadora repetimos los pasos anteriores pero con las siguientes direcciones, para la Ip 192.168.3.10, para la submáscara 255.255.255.0 y para el gateway por default 192.168.3.1

Resultados

Se realizó una configuración de los routers estáticos para establecer una red de comunicación entre los dispositivos. Los resultados indican que se enviaron tres paquetes ICMP desde la fuente PC0 a los destinos PC1 y PC2. Todos los envíos fueron exitosos, con un tiempo de respuesta de 0.000 segundos en cada caso. No se configuraron como periódicos, y se observa que cada paquete fue numerado secuencialmente (0, 1 y 2). Los colores asociados a cada entrada reflejan visualmente los diferentes destinos, lo que facilita la identificación de las rutas en el entorno de simulación.

UNIVERSIDAD DE LAS FUERZAS ARMADAS

Redes de Computadores

Departamento de Ciencias de la Computación

Matriz Comparativa Cisco Packet Tracer y GNS3

Estudiantes:
Ednan Josué Merino Calderón

Docente:
Ing. Walter Marcelo Fuertes Diaz

Matriz

Característica	Packet Tracer	GNS3
Uso principal	Simulador educativo enfocado en el aprendizaje de redes y preparación para certificaciones Cisco	Emulador de redes avanzado utilizado para simulación realista de redes, con soporte para dispositivos virtuales
Facilidad de uso	Fácil de usar, con una interfaz gráfica intuitiva	Requiere más conocimiento técnico, configuración más compleja
Soporte para dispositivos	Limitado a dispositivos y comandos Cisco	Soporte extenso para una amplia variedad de dispositivos y sistemas operativos de red
Recursos de hardware	Requiere pocos recursos de hardware	Puede consumir muchos recursos dependiendo de la complejidad de la red y los dispositivos emulados
Licencia	Gratuito para estudiantes y educadores	Gratuito, pero algunos dispositivos requieren licencias adicionales (e.g., IOSv de Cisco)
Capacidades de simulación	Buenas para escenarios educativos y básicos de redes	Excelente para simulaciones realistas y complejas, incluyendo redes de producción
Actualización y soporte	Actualizado por Cisco regularmente con nuevas versiones y características	Comunidad activa y soporte continuo; se actualiza frecuentemente para incluir nuevas funcionalidades
Integración con hardware real	No soporta la integración directa con hardware real	Soporta la integración con hardware real a través de interfaces y conexiones externas
Plataformas soportadas	Windows, macOS, Linux (limitado)	Windows, macOS, Linux
Comunidad y recursos de aprendizaje	Amplia comunidad, con muchos recursos educativos oficiales de Cisco	Comunidad fuerte, con abundantes recursos en línea, pero requiere conocimientos más avanzados
Escenarios de aprendizaje	Ideal para principiantes y para la preparación de certificaciones Cisco como CCNA	Ideal para profesionales de redes que necesitan emular redes complejas y específicas
Soporte para virtualización	No soporta máquinas virtuales o sistemas operativos de terceros	Soporta máquinas virtuales y sistemas operativos de terceros, permitiendo una emulación completa