**Ejercicio 12: Configuración básica de VLANs, SSH y seguridad**

.

A diagram of a computer network

Description automatically generated

# **Objetivos:**

# Conocer la utilidad de la programación de VLANs.

# Interconectar VLANs distintas.

Un método para proporcionar enrutamiento y conectividad para varias VLAN es mediante el uso de un **enlace troncal 802.1Q** entre uno o más switches y una sola interfaz del router. Este método también se conoce como enrutamiento entre VLANs de **router-on-a-stick**. En este método, la interfaz del ruteador se divide en varias subinterfaces que proporcionan rutas lógicas a todas las VLAN conectadas.

En este ejercicio, configuraremos el enrutamiento entre VLANs basado en troncales y verificaremos la conectividad a los hosts en diferentes VLANs, así como también con un loopback en el router.

Nuestro objetivo es lograr la interconexión de VLANs, en este caso la **VLAN 10** de **Estudiantes** y la **VLAN 20** de la **Facultad**. Estas subredes no pueden comunicarse, solamente si pertenecieran a la misma VLAN. Para poder comunicarse entre VLANs distintas requerimos un router, ya que el router toma decisiones capa 3. De manera nativa los switches no pueden realizar este proceso, ya que los switches no toman decisiones o rutean.

Tenemos en cada VLAN dominios distintos de broadcast o subredes. Utiliza e diseño lógico de la red (segmentación de tráfico) de la siguiente tabla:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Segmento** | **VLAN** | **Puertos asignados** | **Dirección de subred** | **Máscara de subred** |
| **Estudiantes** | 10 | F0/3-10 | 192.168.10.0 | 255.255.255.0 |
| **Facultad** | 20 | F0/11-18 | 192.168.20.0 | 255.255.255.0 |
| **Nativa** | 1 | No aplica | 192.168.1.0 | 255.255.255.0 |

# **Tabla de direccionamiento:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivo** | **Interface** | **IP Address** | **Máscara de subred** | **Default Gateway** |
| R1 | G0/1.1 | 192.168.1.1 | 255.255.255.0 | N/A |
|  | G0/1.10 | 192.168.10.1 | 255.255.255.0 | N/A |
|  | G0/1.20 | 192.168.20.1 | 255.255.255.0 | N/A |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC0 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| PC1 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| PC2 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |
| PC3 | NIC | Asignada por DHCP | Asignada por DHCP | Asignada por DHCP |

Para lograr la conectividad entre los equipos de las VLANs, se sugiere proceder con el siguiente orden:

1. Complete la configuración del switch **S1**
2. Configuración de la **VLAN1** con los datos de la tabla y el **default Gateway**.
3. Creación de las VLANs.
4. Definición de los tipos de puertos que se va a utilizar: acceso o troncal.
5. Asignación de puertos a las VLANs y definición de los puertos de acceso.
6. Definición de los puertos troncales.

**NOTA:** Verifique los nombres y números de VLAN con el comando: **sh vlan brief**

1. Complete la configuración del switch **S2**
2. Configuración de la **VLAN1** con los datos de la tabla y el **default Gateway**.
3. Creación de las VLANs.
4. Definición de los tipos de puertos que se va a utilizar: acceso o troncal.
5. Asignación de puertos a las VLANs y definición de los puertos de acceso.
6. Definición de los puertos troncales.

**NOTA:** Verifique los nombres y números de VLAN con el comando: **sh vlan brief**

1. Complete la configuración del router **R1**
2. Configurar la interface serial
3. Configurar las subinterfaces. Configurar **R1** para enrutar a varias VLANs mediante la creación de subinterfaces para cada VLAN.

* Configurar una subinterface para la VLAN 1.
* Configurar una subinterface para la VLAN 10.
* Configurar una subinterface para la VLAN 20.

1. Configurar el servicio **DHCP** para entregar direccionamiento dinámico a las VLANs de **Estudiantes** y **Facultad**.
2. Configurar una ruta por default hacia el **ISP**.
3. Complete la configuración del **ISP**

Configurar rutas estáticas hacia las subredes de las VLANs 1, 10 y 20.

1. Realice pruebas de conectividad
2. Activar el servicio de**DHCP** en todos los equipos terminales de las VLANs de **Estudiantes** y **Facultad**.
3. Realizar las pruebas de conectividad necesarias para comprobar la conexión entre los dispositivos.

**Acceso a dispositivos de red mediante SSH**

1. Introducción

En el pasado, **Telnet** era el protocolo de red más común que se usaba para configurar dispositivos de red en forma remota. El protocolo **Telnet** no cifra la información entre el cliente y el servidor. Esto permite que un programa detector de redes intercepte contraseñas e información de configuración.

**Shell seguro (SSH)** es un protocolo de red que establece una conexión de emulación de terminal segura con un ruteador u otro dispositivo de red. SSH cifra toda la información que atraviesa el enlace de red y proporciona autenticación de los equipos remotos. SSH está reemplazando rápidamente a Telnet como la herramienta de conexión remota preferida por los profesionales de red. SSH se utiliza con mayor frecuencia para conectarse a un dispositivo remoto y ejecutar comandos.

Para que el protocolo SSH funcione, los dispositivos de red que se comunican deben estar configurados para admitirlo. En este ejercicio, deberá habilitar el servidor SSH en un ruteador y luego conectarse a ese ruteador desde una PC con un cliente SSH instalado. En una red local, la conexión generalmente se realiza utilizando Ethernet e IP.

Parte 1. Configurar el ruteador para el acceso por SSH

Usar el protocolo Telnet para conectarse a un dispositivo de red es un riesgo de seguridad, porque toda la información se transmite en formato de texto no cifrado. El protocolo SSH cifra los datos de sesión y ofrece autenticación del dispositivo, por lo que se recomienda usar SSH para conexiones remotas. En la parte 1, configurará el ruteador para que acepte conexiones SSH por las líneas VTY.

1. Configurar la autenticación del dispositivo.

El nombre y el dominio del dispositivo se usan como parte de la clave de cifrado cuando esta se genera. Por lo tanto, estos nombres deben introducirse antes de emitir el comando **crypto key**.

* + 1. Configure el dominio para el dispositivo.

R1(config)# **ip domain-name tec.com**

2. Configurar el método de la clave de cifrado.

R1(config)# **crypto key generate rsa**

**Type the value of 1024 as the answer to the question and press enter.**

How many bits in the modulus [512]: **1024**

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

R1(config)#

\*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

3. Configurar un nombre de usuario de la base de datos local.

R1(config)# **username admin privilege 15 secret adminpass**

**Nota**: el nivel de privilegio 15 otorga derechos de administrador al usuario.

4. Habilitar SSH en las líneas VTY.

* + 1. Habilite Telnet y SSH en las líneas VTY entrantes mediante el comando **transport input**.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input ssh**

5. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

R1(config-line)# **login local**

R1(config-line)# **end**

R1#

5. Guardar la configuración en ejecución en el archivo de configuración de inicio.

R1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

R1#

6. Establecer una conexión SSH con el ruteador R1.

* + 1. Acceda remotamente al **R1** desde el servidor **www.google.com** con el comando **SSH**. Use el nombre de usuario **admin** y la contraseña **adminpass**. En la línea de comandos (**Command Prompt**) del servidor, inserta el siguiente comando:

ssh –l admin 190.40.0.18

Use el password adminpass

* + 1. ¿Pudo conectarse remotamente? \_\_\_\_

Parte 2. Configurar el switch para el acceso por SSH

En la parte 2, configurará el switch en la topología para que se acepten conexiones SSH. Una vez configurado el switch, establezca una sesión de SSH desde el servidor **www.google.com**

1. Configurar el switch para que tenga conectividad de SSH.

Para configurar SSH en el switch, utilice los mismos comandos que usó para configurar SSH en el ruteador.

* + 1. Configure el dominio para el dispositivo.

S1(config)# **ip domain-name tec.com**

* + 1. Configure el método de la clave de cifrado.

S1(config)# **crypto key generate rsa**

**Type the value of 1024 as the answer to the question and press enter.**

How many bits in the modulus [512]: **1024**

* + 1. Configure un nombre de usuario de la base de datos local.

S1(config)# **username admin privilege 15 secret adminpass**

* + 1. Habilite Telnet y SSH en las líneas VTY.

S1(config)# **line vty 0 15**

S1(config-line)# **transport input ssh**

* + 1. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

S1(config-line)# **login local**

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

5. Establecer una conexión SSH con el switch S1

* + 1. Acceda remotamente a la interfaz SV1 del switch **S1** desde el servidor **www.google.com** con el comando SSH. En la línea de comandos (**Command Prompt**) del servidor, inserta el siguiente comando:

ssh –l admin 192.168.1.11

Use el password adminpass

* + 1. ¿Pudo conectarse remotamente? \_\_\_\_

Reflexión:

**¿Cómo proporcionaría acceso a un dispositivo de red a varios usuarios, cada uno con un nombre de usuario diferente?**

Se agregaría el nombre de usuario y la contraseña de cada usuario a la base de datos local mediante el comando username.

R1(config)# **username admin privilege 15 secret adminpass**

R1(config)# **username usuario1 privilege 1 secret userpass**

R1(config)# **username usuario2 privilege 1 secret userpass**

**Nota:** Un nivel de privilegio de **15** otorga al usuario derechos de **administrador**.

La CLI del Cisco IOS tiene dos niveles de acceso a los comandos:

* **Modo EXEC de usuario (nivel de privilegio 1)**: proporciona los privilegios de usuario de modo EXEC más bajos y permite que solo estén disponibles los comandos del nivel de usuario en el prompt **router>**.
* **Modo EXEC privilegiado (nivel de privilegio 15)**: incluye todos los comandos de nivel de privilegiado en el prompt **router#**.

**Protección de dispositivos de red**

1. Introducción

Se recomienda que todos los dispositivos de red se configuren con al menos un conjunto de comandos de seguridad recomendados. Esto incluye dispositivos para usuarios finales, servidores y dispositivos de red, como routers y switches.

En este ejercicio utilizará la CLI del IOS para configurar medidas de seguridad básicas según las prácticas recomendadas. Luego, probará las medidas de seguridad para verificar que estén implementadas de manera apropiada y que funcionen correctamente.

Parte 1. Configurar medidas de seguridad básicas en el router

1. Encripte las contraseñas de texto no cifrado.

R1(config)# **service password-encryption**

2. Refuerce las contraseñas.

Un administrador debe garantizar que las contraseñas cumplan con las pautas estándar para contraseñas seguras. Estas pautas podrían incluir combinar letras, números y caracteres especiales en la contraseña y establecer una longitud mínima.

* + 1. Cambie la contraseña cifrada del modo EXEC privilegiado según las pautas.

R1(config)# **enable secret Enablep@55**

* + 1. Exija que se utilice un mínimo de 10 caracteres para todas las contraseñas.

R1(config)# **security passwords min-length 10**

3. Proteja las líneas de consola y VTY.

* + 1. Puede configurar el router para que se cierre la sesión de una conexión que estuvo inactiva durante un período especificado. Si un administrador de red inicia sesión en un dispositivo de red y, de repente, se debe ausentar, este comando cierra automáticamente la sesión del usuario después de un plazo especificado. Los siguientes comandos harán que se cierre la sesión de la línea después de cinco minutos de inactividad.

R1(config)# **line console 0**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **line vty 0 4**

R1(config-line)# **exec-timeout 5 0**

R1(config-line)# **exit**

R1(config)#

* + 1. El siguiente comando impide los intentos de inicio de sesión por fuerza bruta. Si alguien falla en dos intentos en un período de **120 segundos**, el router bloquea los intentos de inicio de sesión durante **30 segundos**. Este temporizador está configurado en un valor especialmente bajo para esta actividad de laboratorio.

R1(config)# **login block-for 30 attempts 2 within 120**

4. Verifique que todos los puertos sin usar estén inhabilitados.

Los puertos del router están inhabilitados de manera predeterminada, pero siempre es prudente verificar que todos los puertos sin utilizar tengan un estado inactivo en términos administrativos. Esto se puede verificar rápidamente emitiendo el comando **show ip interface brief**. Todos los puertos sin utilizar que no estén en un estado inactivo en términos administrativos se deben inhabilitar por medio del comando **shutdown** en el modo de configuración de la interfaz.

R1#**sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 unassigned YES unset up up

GigabitEthernet0/1.1 192.168.1.1 YES manual up up

GigabitEthernet0/1.10 192.168.10.1 YES manual up up

GigabitEthernet0/1.20 192.168.20.1 YES manual up up

Serial0/0/0 190.40.0.18 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Vlan1 unassigned YES unset administratively down down

Emita el comando **show running-config** en la petición del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.

Parte 2. Configurar medidas de seguridad básicas en el switch S1

1. Encripte las contraseñas de texto no cifrado.

S1(config)# **service password-encryption**

2. Refuerce las contraseñas en el switch.

Cambie la contraseña cifrada del modo EXEC privilegiado según las pautas de contraseñas seguras.

S1(config)# **enable secret Enablep@55**

**Nota**: el comando de seguridad **password min-length** no está disponible en el switch 2960.

3. Proteja las líneas de consola y VTY.

* + 1. Configure el switch para que se cierre una línea que haya estado inactiva durante 10 minutos.

S1(config)# **line console 0**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **line vty 0 15**

S1(config-line)# **exec-timeout 10 0**

S1(config-line)# **exit**

S1(config)#

4. Verifique que todos los puertos sin usar estén inhabilitados.

Los puertos del switch están habilitados de manera predeterminada. Desactive todos los puertos que no se estén usando en el switch.

* + 1. Puede verificar el estado de los puertos del switch emitiendo el comando **show ip interface brief**.

S1#

S1#**sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual up up

FastEthernet0/2 unassigned YES manual up up

FastEthernet0/3 unassigned YES manual down down

FastEthernet0/4 unassigned YES manual up up

FastEthernet0/5 unassigned YES manual down down

FastEthernet0/6 unassigned YES manual down down

FastEthernet0/7 unassigned YES manual down down

FastEthernet0/8 unassigned YES manual down down

FastEthernet0/9 unassigned YES manual down down

FastEthernet0/10 unassigned YES manual down down

FastEthernet0/11 unassigned YES manual down down

FastEthernet0/12 unassigned YES manual down down

FastEthernet0/13 unassigned YES manual down down

FastEthernet0/14 unassigned YES manual down down

FastEthernet0/15 unassigned YES manual down down

FastEthernet0/16 unassigned YES manual up up

FastEthernet0/17 unassigned YES manual down down

FastEthernet0/18 unassigned YES manual down down

FastEthernet0/19 unassigned YES manual down down

FastEthernet0/20 unassigned YES manual down down

FastEthernet0/21 unassigned YES manual down down

FastEthernet0/22 unassigned YES manual down down

FastEthernet0/23 unassigned YES manual down down

FastEthernet0/24 unassigned YES manual down down

GigabitEthernet0/1 unassigned YES manual down down

GigabitEthernet0/2 unassigned YES manual down down

Vlan1 192.168.1.11 YES manual up up

S1#

* + 1. Use el comando **interface range** para desactivar varias interfaces a la vez.

S1(config)# interface f0/3

S1(config-if-range)# shutdown

S1(config-if-range)# exit

S1(config)# **interface range f0/5-15, f0/17-24, g0/1-2**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **end**

S1#

* + 1. Verifique que todas las interfaces inactivas tengan un estado inactivo en términos administrativos.

S1#**sh ip interface brief**

Interface IP-Address OK? Method Status Protocol

FastEthernet0/1 unassigned YES manual up up

FastEthernet0/2 unassigned YES manual up up

FastEthernet0/3 unassigned YES manual administratively down down

FastEthernet0/4 unassigned YES manual up up

FastEthernet0/5 unassigned YES manual administratively down down

FastEthernet0/6 unassigned YES manual administratively down down

FastEthernet0/7 unassigned YES manual administratively down down

FastEthernet0/8 unassigned YES manual administratively down down

FastEthernet0/9 unassigned YES manual administratively down down

FastEthernet0/10 unassigned YES manual administratively down down

FastEthernet0/11 unassigned YES manual administratively down down

FastEthernet0/12 unassigned YES manual administratively down down

FastEthernet0/13 unassigned YES manual administratively down down

FastEthernet0/14 unassigned YES manual administratively down down

FastEthernet0/15 unassigned YES manual administratively down down

FastEthernet0/16 unassigned YES manual up up

FastEthernet0/17 unassigned YES manual administratively down down

FastEthernet0/18 unassigned YES manual administratively down down

FastEthernet0/19 unassigned YES manual administratively down down

FastEthernet0/20 unassigned YES manual administratively down down

FastEthernet0/21 unassigned YES manual administratively down down

FastEthernet0/22 unassigned YES manual administratively down down

FastEthernet0/23 unassigned YES manual administratively down down

FastEthernet0/24 unassigned YES manual administratively down down

GigabitEthernet0/1 unassigned YES manual administratively down down

GigabitEthernet0/2 unassigned YES manual administratively down down

Vlan1 192.168.1.11 YES manual up up

S1#

* + 1. Emita el comando **show running-config** en la petición del modo EXEC privilegiado para ver la configuración de seguridad que aplicó.