

**Ejercicio 8. Configuración de equipos de interconexión**

**Parte 1: Configura la topología física**

#### Atiende las explicaciones del profesor para completar el diseño físico de la red.

A blue and white objects

Description automatically generated with medium confidence

**Parte 2: Configura los dispositivos**

#### Tu tarea es realizar las configuraciones de todos los equipos para tener comunicación entre las estaciones de la red. Para lograr la conectividad, se sugiere proceder con el siguiente orden:

#### Utiliza la información de la **tabla de direccionamiento** para realizar la configuración solicitada de cada equipo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Default gateway |
| R1 | G0/0 | 192.168.0.33 | 255.255.255.224 | N/A |
|  | G0/1 | 192.168.0.1 | 255.255.255.224 | N/A |
|  | Lo0 | 192.168.0.65 | 255.255.255.224 | N/A |
|  | Lo1 | 192.168.0.97 | 255.255.255.224 | N/A |
| S1 | VLAN 1 | 192.168.0.29 | 255.255.255.224 | 192.168.0.1 |
| S2 | VLAN 1 | 192.168.0.61 | 255.255.255.224 | 192.168.0.1 |
| PC-A | NIC | 192.168.0.30 | 255.255.255.224 | 192.168.0.1 |
| PC-B | NIC | 192.168.0.62 | 255.255.255.224 | 192.168.0.33 |

1. Configure las PC ‘s con su dirección IP, máscara de subred y puerta de enlace predeterminada (default gateway)
2. Configure el ruteador R1

Las tareas de configuración para el ruteador **R1** incluyen lo siguiente:

|  |  |  |
| --- | --- | --- |
| Tarea | Descripción | Especificaciones |
| Nombre del ruteador | Asignar el nombre del ruteador | R1 |
| Disable DNS | Deshabilitar el DNS |  |
| Encrypted privileged exec password | Asignar **class** como password encriptado del modo privilegiado | **class** |
| Console access password | Asignar **cisco** como password de la consola y habilitar el inicio de sesión (login) | **cisco** |
| Telnet access password | Asignar **cisco** como password vtyy habilite el inicio de session (login) | **cisco** |
| Encrypt the clear text passwords | Encriptar los passwords |  |
| MOTD Banner | Configurar un banner de prevención de acceso al ruteador. | Prohibido entrar sin autorización |
| Interface g0/0  Interface g0/1  Interface Lo0  Interface Lo1 | Configurar y activar las interfaces Gigabit Ethernet y LoopBack utilizando la información contenida en la tabla de direccionamiento. | * Establece la dirección IPv4 de capa 3 * Activa la interface |

* + 1. Acceda al ruteador mediante el puerto de consola y habilite el modo EXEC privilegiado.

Router> **enable**

Router#

* + 1. Ingrese al modo de configuración global.

Router# **config terminal**

Router(config)#

* + 1. Asigne un nombre de dispositivo al ruteador.

Router(config)# **hostname R1**

* + 1. Deshabilite la búsqueda DNS para evitar que el ruteador intente traducir los comandos introducidos de manera incorrecta como si fueran nombres de host.

R1(config)# **no ip domain-lookup**

* + 1. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.

R1(config)# **enable secret class**

* + 1. Asigne **cisco** como la contraseña de consola, establezca un tiempo de espera, habilite el inicio de sesión y agregue el comando **logging synchronous**. El comando **logging synchronous** sincroniza la depuración y el resultado del software IOS de Cisco, y evita que estos mensajes interrumpan la entrada del teclado.

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

R1(config-line)# **password cisco**

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

R1(config-line)# **logging synchronous**

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

R1 config)#

* + 1. Asigne **ciscovty** como la contraseña de vty, para accesos remotos por telnet, habilite el inicio de sesión y agregue el comando **logging synchronous**.

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

R1(config-line)# **password ciscovty**

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

R1(config-line)# **logging synchronous**

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

* + 1. Cifre las contraseñas de texto no cifrado.

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

* + 1. Cree un aviso que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.

R1(config)# **banner motd #Prohibido entrar sin autorización#**

* + 1. Configure una dirección IP y una descripción de interfaz. Active las dos interfaces en el ruteador.

R1(config)# **int g0/0**

R1(config-if)# **description Enlace con PC-B**

R1(config-if)# **ip address 192.168.0.33 255.255.255.224**

R1(config-if)# **no shutdown**

R1(config-if)# exit

R1(config)# **int g0/1**

R1(config-if)# **description Enlace con PC-A**

R1(config-if)# **ip address 192.168.0.1 255.255.255.224**

R1(config-if)# **no shutdown**

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

R1(config)# **int Lo0**

R1(config-if)# **ip address 192.168.0.65 255.255.255.224**

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

R1(config)# **int Lo1**

R1(config-if)# **ip address 192.168.0.97 255.255.255.224**

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

* + 1. Configure el reloj en el ruteador, por ejemplo:

R1# **clock set 12:00:00 8 Nov 2024**

* + 1. Guarde la configuración en ejecución en el archivo de configuración de inicio.

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

Destination filename [startup-config]?

Building configuration...

[OK]

1. Configura el switch S1

Las tareas de configuración para el switch **S1** incluyen lo siguiente:

|  |  |  |
| --- | --- | --- |
| Tarea | Descripción | Especificaciones |
| Switch name | Asignar el nombre del switch | S1 |
| Disable DNS | Deshabilitar el DNS |  |
| Encrypted privileged exec password | Asignar **class** como password encriptado del enable | class |
| Console access password | Asignar **cisco** como password de la consola y habilitar el inicio de sesión (login) | cisco |
| Telnet access password | Asignar **cisco** como password vty, para accesos remotos por telnet, y habilite el inicio de session (login). | ciscovty |
| MOTD Banner | Configurar un banner de prevención de acceso al switch. | Prohibido entrar sin autorización |
| Configure Management Interface (SVI) | Configurar la VLAN 1 del switch. | * Establece la dirección IPv4 de capa 3 * Activa la interface |
| Configure the default gateway | Configurar la puerta de enlace predeterminada. | * Establece la dirección IPv4 de capa 3 |

**Parte 3: Probar y verificar la conectividad de extremo a extremo de IPv4**

1. Para probar la configuración realizada, ejecutar un ping desde el equipo terminal **PC-A**, del diseño de red a la dirección IP de las interfaces **loopback** del **R1**, la dirección IP del Switch **S1** y el equipo terminal **PC-B**. Si los pings son exitosos, tu configuración está correcta.

|  |  |  |  |
| --- | --- | --- | --- |
| **Desde** | **Hacia** | **Dirección IP** | **Resultados del ping**  (Fail / Success) |
| **PC-A** | **Lo0** | 192.168.0.65 |  |
| **PC-A** | **Lo1** | 192.168.0.97 |  |
| **PC-A** | **S1** | 192.168.0.29 |  |
| **PC-A** | **PC-B** | 192.168.0.62 |  |

1. Accesos remotos por telnet. Utiliza password **cisco** y **class** para acceder al modo privilegiado del ruteador y switch. Si el telnet es exitoso, la configuración está correcta

|  |  |  |  |
| --- | --- | --- | --- |
| **Desde** | **Hacia** | **Dirección IP** | **Resultados del telnet**  (Fail / Success) |
| PC-B | **S1** | 192.168.0.29 |  |
| PC-B | **Lo0** | 192.168.0.65 |  |

**Acceso a dispositivos de red mediante SSH**

**Topología física**

A blue and white objects

Description automatically generated with medium confidence

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 la **PC-A** con el comando **SSH**. Use el nombre de usuario **admin** y la contraseña **adminpass**. En la línea de comandos (**Desktop > Command Prompt**) de la **PC-A**, inserta el siguiente comando:

ssh –l admin 192.168.0.1

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 la **PC-A**.

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 desde la PC-B

* + 1. Acceda remotamente a la interfaz SV1 del switch **S1** desde la **PC-B** con el comando SSH. En la línea de comandos (**Desktop > Command Prompt**) de la PC **HR02**, inserta el siguiente comando:

ssh –l admin 192.168.0.29

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#**.