

**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 |
| 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 PCs
   * 1. Configure las PCs con una dirección IP y una máscara de subred.
     2. Configure la puerta de enlace predeterminada (Gateway) en las PCs.
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 Conexion 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 Conexion 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 10:00:00 24 May 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping results** (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

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Telnet results** (Fail / Success) |
| PC-B | **S1** | 192.168.0.29 |  |
| PC-B | **Lo0** | 192.168.0.65 |  |