Universidad Estatal a Distancia

Vicerrectoría Académica

Escuela De Ciencias Exactas y Naturales

Carrera de Bachillerato en Ingeniería Informática

Asignatura: Telemática y redes II

Código: 3076

Proyecto #2

Estudiante:

Francisco Campos Sandi

114750560

Sede: San Vito

Grupo 04

Tutor: Mauricio Montoya Huertas

I Cuatrimestre 2025

**Contenido**

[Introducción 4](#_Toc196053376)

[Desarrollo 5](#_Toc196053377)

[Tabla 1 Direccionamiento 5](#_Toc196053378)

[Paso 1: Realice la topología tal como se muestra en la Figura 1 6](#_Toc196053379)

[Paso 2: Configuración de los parámetros básicos del router 7](#_Toc196053380)

[Paso 3: Configuración de los parámetros básicos para cada switch 9](#_Toc196053381)

[Paso 4: Configure las PC 11](#_Toc196053382)

[Parte 2: Crear redes VLAN y asignar puertos de switch 11](#_Toc196053383)

[Paso 1: Crear las VLAN en los switches 11](#_Toc196053384)

[Paso 2: Asignar las VLAN a las interfaces del switch correctas 13](#_Toc196053385)

[Parte 3: Configurar un enlace troncal 802.1Q entre los switches 13](#_Toc196053386)

[Paso 2: Configurar manualmente la interfaz troncal de S1 E5 15](#_Toc196053387)

[Parte 4: Configure el enrutamiento entre VLAN en elrouter 16](#_Toc196053388)

[Paso 1: Configurar el router 16](#_Toc196053389)

[Parte 5: Verifique que el enrutamiento entre VLAN esté funcionando 18](#_Toc196053390)

[Paso 1: Complete las siguientes pruebas de PC-A. Todo debería tener éxito 18](#_Toc196053391)

[20](#_Toc196053392)

[Paso 2: Complete las siguientes pruebas de PC-A. Todo debería tener éxito 20](#_Toc196053393)

[Link del video 21](#_Toc196053394)

[https://youtu.be/I8Fw1r6ICg4 21](#_Toc196053395)

[Script completo de cada Router 21](#_Toc196053396)

[Script completo de cada Switch 22](#_Toc196053397)

[Script completo de cada PC 23](#_Toc196053398)

[Conclusión 24](#_Toc196053399)

[Referencias 25](#_Toc196053400)

**Tabla de ilustraciones**

[Ilustración 1 Topología proyecto 2 6](#_Toc195039646)

[Ilustración 2 Verifique que las VLAN estén asignadas 13](#_Toc195039647)

[Ilustración 3 Verificar los puertos de enlace troncal, la VLAN nativa 14](#_Toc195039648)

[Ilustración 4 Verifique la conexión troncal. 15](#_Toc195039649)

[Ilustración 5 Verifique que las subinterfaces estén operativas 17](#_Toc195039650)

[Ilustración 6 Ping desde la PC-A a su puerta de enlace predeterminada. 18](#_Toc195039651)

[Ilustración 7 Emitir un comando ping de PC-A a PC-B 18](#_Toc195039652)

[Ilustración 8 Haga ping desde la PC-A a la S2 19](#_Toc195039653)

[Ilustración 9 Comando trace 192.168.20.3 -P 1 19](#_Toc195039654)

# Introducción

En el presente proyecto, configuramos y verificamos la conectividad entre dos routers usando direcciones IPv4 e IPv6. Como parte del trabajo, configuramos los parámetros básicos de los routers. También se trabaja contraseñas cifradas y con avisos de seguridad para los usuarios que accedieran a los routers. Además, la configuración de cada dispositivo para asegurarnos de que los cambios se mantuvieran.

Por otro lado, configuramos las direcciones IP e IPv6 en cada interfaz de los routers. Además, se trabaja en el enrutamiento unicast de IPv6 y las configuraciones de las direcciones IPv6 de acuerdo a la tabla de direccionamiento. Así verificar que las configuraciones este bien, además se usan los comandos show ip interface brief y show ipv6 interface brief, que nos permitieron ver las direcciones asignadas y el estado de las interfaces.

Por otro lado, configuramos el enrutamiento estático y predeterminado para IPv4. Además, se trabajan las configuraciones de las rutas estáticas hacia las redes Loopback en los routers, usando las interfaces adecuadas como siguiente salto. Además, se trabaja configuraciones una ruta estática flotante para tener una ruta alternativa en caso de que la principal fallara. Usamos comandos de verificación como show ip route y traceroute para comprobar que las rutas estaban bien configuradas.

Finalmente, se trabaja las configuraciones en el enrutamiento estático y predeterminado para IPv6. Configuramos rutas estáticas hacia las redes Loopback de los routers, usando direcciones IPv6 como siguiente salto. Se trabaja las rutas estáticas flotantes para asegurar la conectividad en caso de que se den fallos en las rutas principales. También se usan los comandos show ipv6 route y traceroute para verificar que las rutas estén operativas y que la conectividad IPv6 entre los routers sea exitosa.

# Desarrollo

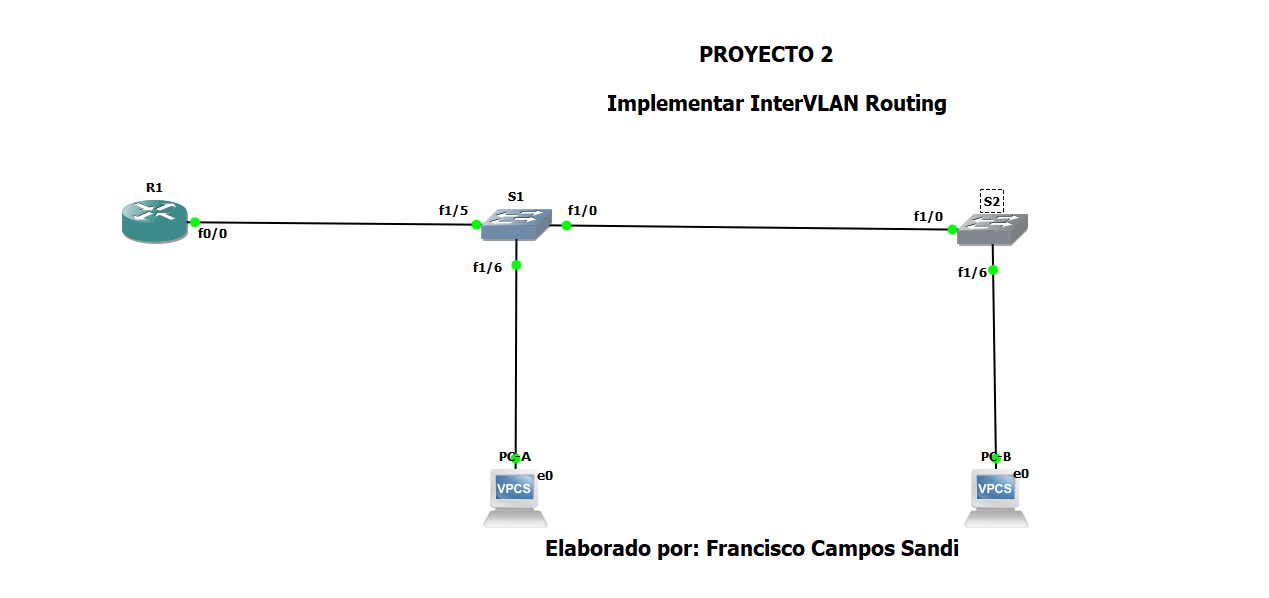
# Tabla 1 Direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dispositivos** | **Interfaz** | **Dirección IP** | **Máscara de**  **Subred** | **Gateway**  **Predeterminado** |
| **R1** | F0/0 | No corresponde | No corresponde | N/D |
| F0/0.10 | 192.168.10.1 | 255.255.255.0 |
| F0/0.20 | 192.168.10.20 | 255.255.255.0 |
| F0/0.30 | 192.168.10.30 | 255.255.255.0 |
| F0/0.1000 | No corresponde | No corresponde |
| **S1** | VLAN 10 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| **S2** | VLAN 10 | 192.168.10.12 | 255.255.255.0 | 192.168.10.1 |
| **PC-A** | NIC | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| **PC-B** | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

**Tabla 2 VLAN**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **Nombre** | **Interfaz Asignada** |
| 10 | UNED | S1: VLAN 10  S2: VLAN 10 |
| 20 | SEDE | S1: E6 |
| 30 | OPERACIONES | S2: E6 |
| 999 | PARQUEO | S1: E0, E2-4, E7  S2: E0, E2-5, E7 |
| 1000 | NATIVE | N/D |

## Paso 1: Realice la topología tal como se muestra en la Figura 1



**Ilustración 1 Topología proyecto 2**

## Paso 2: Configuración de los parámetros básicos del router

a) Asignar el nombre al router como se ve en la Figura 1

|  |
| --- |
| R1 |
| enable  configure terminal  hostname R1 |

b) Deshabilite el DNS en cada router para que evite traducir los comandos mal introducidos como si fueran nombres de Hosts

|  |
| --- |
| R1 |
| no ip domain lookup |

c) Asigne **proyecto** como contraseña cifrada del modo EXEC privilegiado en cada router

|  |
| --- |
| R1 |
| enable proyecto class |

d) Asigne **proyecto-dos** como la contraseña de la consola y active el inicio de sesión en el router

|  |
| --- |
| R1 |
| line console 0  password proyecto-dos  login |

e) Asigne **proyecto-dos** como la contraseña VTY y active el inicio de sesión en el router f) En el router cifre las contraseñas de texto sin formato

|  |
| --- |
| R1 |
| line vty 0 15  password proyecto-dos  login |

g) En el router cree un aviso que advierta a todo el que acceda al dispositivo que el “**Solamente Usuarios Autorizados**”

|  |
| --- |
| R1 |
| banner motd $ Solamente Usuarios Autorizados $ |

h) Ajuste el reloj del router

|  |
| --- |
| R1 |
| clock set 20:30:00 15 may 2025 |

i) Guarde la configuración del router

|  |
| --- |
| R1 |
| exit  copy running-config startup-config |

**Nota:** Utilice el signo de interrogación (?) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar los comandos.

## Paso 3: Configuración de los parámetros básicos para cada switch

a) Asignar el nombre a los switches como se ve en la Figura 1

|  |  |
| --- | --- |
| S1 | S2 |
| enable  configure terminal  hostname S1 | enable  configure terminal  hostname S2 |

b) Deshabilite el DNS en cada router para que evite traducir los comandos mal introducidos como si fueran nombres de Hosts

|  |  |
| --- | --- |
| S1 | S2 |
| no ip domain-lookup | no ip domain-lookup |

c) Asigne **proyecto** como contraseña cifrada del modo EXEC privilegiado en cada switch

|  |  |
| --- | --- |
| S1 | S2 |
| enable secret proyecto | enable secret proyecto |

d) Asigne **proyecto-dos** como la contraseña de la consola y active el inicio de sesión en cada switch

|  |  |
| --- | --- |
| S1 | S2 |
| line console 0  password proyecto-dos  login | line console 0  password proyecto-dos  login |

e) Asigne **proyecto-dos** como la contraseña VTY y active el inicio de sesión en cada switch

|  |  |
| --- | --- |
| S1 | S2 |
| line vty 0 15  password proyecto-dos  login | line vty 0 15  password proyecto-dos  login |

|  |  |
| --- | --- |
| S1 | S2 |
| service password-encryption | service password-encryption |

f) En cada switch cifre las contraseñas de texto sin formato

g) En cada switch cree un aviso que advierta a todo el que acceda al dispositivo que el “**Solamente Usuarios Autorizados**”

|  |  |
| --- | --- |
| S1 | S2 |
| banner motd $ Solamente Usuarios Autorizados $ | banner motd $ Solamente Usuarios Autorizados $ |

h) Ajuste el reloj de cada switch

|  |  |
| --- | --- |
| S1 | S2 |
| clock set 20:30:00 15 may 2025 | clock set 20:30:00 15 may 2025 |

i) Guarde la configuración de cada switch

|  |  |
| --- | --- |
| S1 | S2 |
| copy running-config startup-config | copy running-config startup-config |

**Nota:** Utilice el signo de interrogación (?) para poder determinar la secuencia correcta de parámetros necesarios para ejecutar los comandos.

## Paso 4: Configure las PC

a) Consulte la tabla 1 para obtener la información de direcciones de los equipos host

|  |  |
| --- | --- |
| PC-A | PC-B |
| ip 192.168.20.3 255.255.255.0 192.168.20.1 | ip 192.168.30.3 255.255.255.0 192.168.30.1 |

# Parte 2: Crear redes VLAN y asignar puertos de switch

En la Parte 2, se van a crear VLAN como se especifica en la tabla 2 en ambos switches. A continuación, asignará las VLAN a la interfaz adecuada y verificará los valores de configuración. Complete las siguientes tareas en cada switch.

## Paso 1: Crear las VLAN en los switches

a) a Cree y asigne un nombre a las VLAN necesarias en cada switch de la tabla 2.

|  |  |
| --- | --- |
| S1 | S2 |
| vlan database  vlan 10 name UNED  vlan 20 name SEDE  vlan 30 name OPERACIONES  vlan 999 name PARQUEO  vlan 1000 name NATIVE  exit  interface vlan 10 | vlan database  vlan 10 name UNED  vlan 20 name SEDE  vlan 30 name OPERACIONES  vlan 999 name PARQUEO  vlan 1000 name NATIVE  exit |

b) Configure la interfaz de administración y el gateway predeterminado en cada switch con la información de dirección IP incluida en la tabla de direccionamiento.

|  |  |
| --- | --- |
| S1 | S2 |
| ip address 192.168.10.11 255.255.255.0  no shutdown  exit  ip default-gateway 192.168.10.1 | interface vlan 10  ip address 192.168.10.12 255.255.255.0  no shutdown  exit  ip default-gateway 192.168.10.1 |

c) Asigne todos los puertos no utilizados de los switches a la VLAN Parqueo, los deben configurar en modo acceso y apáguelos de forma administrativa

|  |  |
| --- | --- |
| S1 | S2 |
| interface range f1/2 - 4 , f1/7 – 15  switchport mode access  switchport access vlan 999  shutdown | interface range f1/0 , f1/2 – 5 , f1/7 – 15  switchport mode access  switchport access vlan 999  shutdown |

**Nota**: El comando range es útil para llevar a cabo este punto

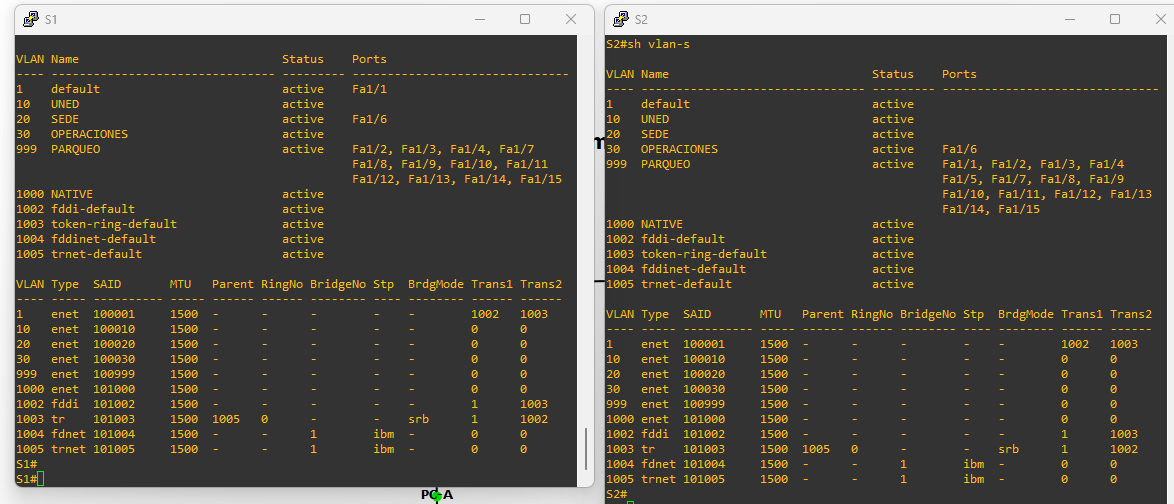
## Paso 2: Asignar las VLAN a las interfaces del switch correctas

a) Asigne los puertos usados a la VLAN apropiada (especificada en la tabla 2) y configúrelos para el modo de acceso

|  |  |
| --- | --- |
| S1 | S2 |
| interface f1/6  switchport mode access  switchport access vlan 20  interface FastEthernet1/5  switchport mode access  switchport access vlan 10 | interface f1/6  switchport mode access  switchport access vlan 20 |

b) Verifique que las VLAN estén asignadas a las interfaces correctas

|  |  |
| --- | --- |
| S1 | S2 |
| sh vlan-s | sh vlan-s |



**Ilustración 2 Verifique que las VLAN estén asignadas**

# Parte 3: Configurar un enlace troncal 802.1Q entre los switches

En la Parte 3, configurará manualmente la interfaz E1 como troncal.

**Paso 1: Configure manualmente la interfaz troncal E1 en el interruptor S1 y S2**

a) Configure la conexión troncal estática en la interfaz E1 para ambos switches

|  |  |
| --- | --- |
| S1 | S2 |
| interface f0/1  switchport mode trunk | interface f0/1  switchport mode trunk |

b) Establezca la VLAN nativa en 1000 en ambos switches.

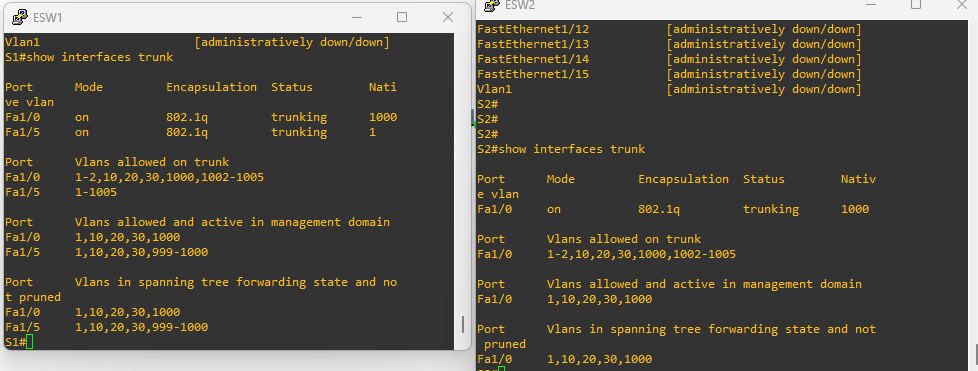
|  |  |
| --- | --- |
| S1 | S2 |
| switchport trunk native vlan 1000 | switchport trunk native vlan 1000 |

c) Especifique que las VLAN 10, 20, 30 y 1000 pueden cruzar el troncal

|  |  |
| --- | --- |
| S1 | S2 |
| switchport trunk allowed vlan 10,20,30,1000 | switchport trunk allowed vlan 10,20,30,1000 |

d) Verifique los puertos de enlace troncal, la VLAN nativa y las VLAN permitidas en el troncal

|  |  |
| --- | --- |
| S1 | S2 |
| show interfaces trunk | show interfaces trunk |

****

**Ilustración 3 Verificar los puertos de enlace troncal, la VLAN nativa**

## Paso 2: Configurar manualmente la interfaz troncal de S1 E5

a) Configure la interfaz E5 de S1 con los mismos parámetros de troncal que E1. Este es el troncal del router

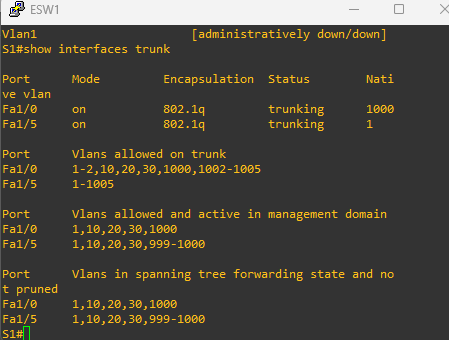
|  |
| --- |
| S1 |
| configure terminal  interface FastEthernet1/5  switchport mode trunk  switchport trunk encapsulation dot1q  switchport trunk allowed vlan all |

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

|  |
| --- |
| S1 |
| copy running-config startup-config |

c) Verifique la conexión troncal.

|  |
| --- |
| S1 |
| show interfaces trunk |



**Ilustración 4 Verifique la conexión troncal.**

Pregunta: ¿Qué sucede si f0/0 en R1 está caído?

**Si la interfaz** **Fa0/0 en R1 está caída, la interfaz Fa1/5 en el switch S1 no se mostrará como activa, ya que no existe un enlace físico entre ambos dispositivos y el puerto del switch permanecerá en estado down**

# Parte 4: Configure el enrutamiento entre VLAN en elrouter

## Paso 1: Configurar el router

a) Active la interfaz F0/0 según sea necesario en el router

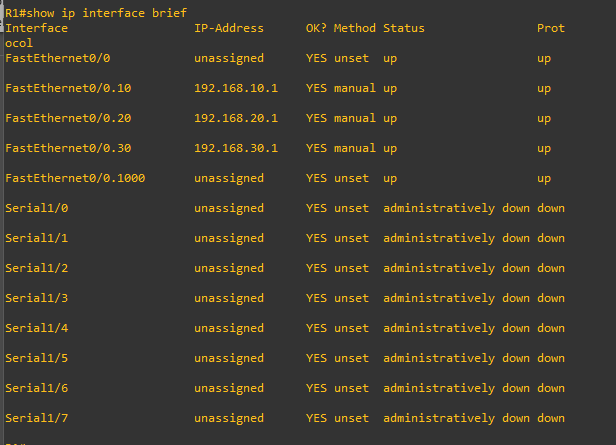
|  |
| --- |
| R1 |
| Interface f0/0  no shutdown  exit |

b) Configure las subinterfaces para cada VLAN como se especifica en la tabla de direcciones IP. Todas las subinterfaces utilizan encapsulación 802.1Q. Asegúrese de que la subinterfaz de la VLAN nativa no tenga asignada una dirección IP. Incluya una descripción para cada subinterfaz.

|  |
| --- |
| R1 |
| configure terminal  interface FastEthernet0/0.10  description UNED VLAN  encapsulation dot1q 10  ip address 192.168.10.1 255.255.255.0  interface FastEthernet0/0.20  description SEDE VLAN  encapsulation dot1q 20  ip address 192.168.10.1 255.255.255.0  interface FastEthernet0/0.30  description OPERACIONES VLAN  encapsulation dot1q 30  ip address 192.168.10.1 255.255.255.0  interface FastEthernet0/0.1000  description Native VLAN  encapsulation dot1q 1000 native  no ip address |

c) Verifique que las subinterfaces estén operativas

|  |
| --- |
| R1 |
| show ip interface brief |



**Ilustración 5 Verifique que las subinterfaces estén operativas**

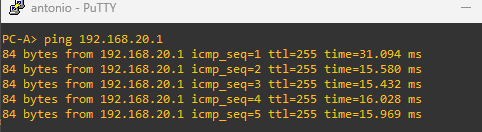
# Parte 5: Verifique que el enrutamiento entre VLAN esté funcionando

## Paso 1: Complete las siguientes pruebas de PC-A. Todo debería tener éxito

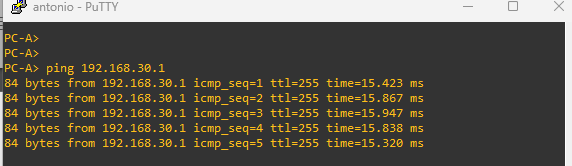
**Nota:** Es posible que tenga que deshabilitar el firewall de las PC para que funcionen los pings

a) Haga ping desde la PC-A a su puerta de enlace predeterminada.

|  |
| --- |
| PC-A |
| ping 192.168.20.1 |

****

**Ilustración 6 Ping desde la PC-A a su puerta de enlace predeterminada.**

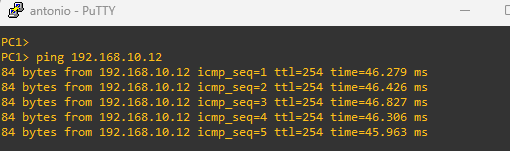
 b) Emitir un comando ping de PC-A a PC-B

**Ilustración 7 Emitir un comando ping de PC-A a PC-B**

|  |
| --- |
| ping de PC-A a PC-B |
| ping 192.168.30.1 |

c) Haga ping desde la PC-A a la S2

|  |
| --- |
| ping desde la PC-A a la S2 |
| ping 192.168.10.12 |

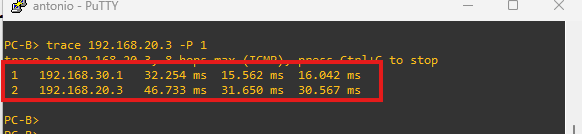


**Ilustración 8 Haga ping desde la PC-A a la S2**

## Paso 2: Complete las siguientes pruebas de PC-A. Todo debería tener éxito

a) Desde la ventana Símbolo del sistema en PC-B, ejecute el comando **trace** a la dirección de PC-A.

|  |
| --- |
| PC-A |
| trace 192.168.20.3 -P 1 |



**Ilustración 9 Comando trace 192.168.20.3 -P 1**

Pregunta: ¿Qué direcciones IP intermedias se muestran en los resultados?

**La salida de tracert debe mostrar dos entradas en los resultados. El primer salto es la dirección de interfaz F0/0.30 de R1, que es la dirección de puerta de enlace para PC-B. El segundo salto es la dirección de PC-A.**

Al ejecutar el comando **trace 192.168.20.3 -P 1** desde **PC-B** hacia **PC-A**, se muestra el recorrido de los paquetes a través de la red. Dado que solo hay un router, **R1**, en los resultados aparecerán dos saltos. El primer salto será la dirección IP del router **R1**, por ejemplo **192.168.30.1**, y el segundo salto será la dirección IP de **PC-A**, que es **192.168.20.3**. Este comando utiliza paquetes ICMP para trazar la ruta, y la opción **-P 1** indica que se utiliza solo un paquete por salto. En los resultados, se verán las direcciones IP de los dispositivos intermedios (en este caso, solo el router **R1**) y el tiempo de respuesta de cada uno.

# Link del video

# <https://youtu.be/I8Fw1r6ICg4>

# Script completo de cada Router

|  |
| --- |
| R1 |
| R1:  enable  configure terminal  hostname R1  no ip domain lookup  enable secret proyecto  line console 0  password proyecto-dos  login  line vty 0 15  password proyecto-dos  login  service password-encryption  banner motd $ Solamente Usuarios Autorizados $  interface FastEthernet0/0.10  description UNED VLAN  encapsulation dot1q 10  ip address 192.168.10.1 255.255.255.0  interface FastEthernet0/0.20  description SEDE VLAN  encapsulation dot1q 20  ip address 192.168.20.1 255.255.255.0  interface FastEthernet0/0.30  description OPERACIONES VLAN  encapsulation dot1q 30  ip address 192.168.30.1 255.255.255.0  interface FastEthernet0/0.1000  description Native VLAN  encapsulation dot1q 1000 native  no ip address  interface FastEthernet0/0  no shutdown  end  clock set 20:30:00 15 may 2025  copy running-config startup-config |

# Script completo de cada Switch

|  |  |
| --- | --- |
| S1 | S2 |
| enable  configure terminal  hostname S1  no ip domain-lookup  enable secret proyecto  line console 0  password proyecto-dos  login  line vty 0 15  password proyecto-dos  login  service password-encryption  banner motd $ Solamente Usuarios Autorizados $  end  clock set 20:30:00 15 may 2025  copy running-config startup-config  vlan database  vlan 10 name UNED  vlan 20 name SEDE  vlan 30 name OPERACIONES  vlan 999 name PARQUEO  vlan 1000 name NATIVE  exit  configure terminal  interface FastEthernet1/6  switchport mode access  switchport access vlan 20  interface range FastEthernet1/2 - 4, FastEthernet1/7 - 15  switchport mode access  switchport access vlan 999  no shutdown  interface FastEthernet1/0  switchport mode trunk  switchport trunk native vlan 1000  switchport trunk allowed vlan 1,2,10,20,30,1000,1002-1005  interface FastEthernet1/5  switchport mode trunk  switchport trunk encapsulation dot1q  switchport trunk allowed vlan all  end  copy running-config startup-config | enable  configure terminal  hostname S2  no ip domain-lookup  enable secret proyecto  line console 0  password proyecto-dos  login  line vty 0 15  password proyecto-dos  login  service password-encryption  banner motd $ Solamente Usuarios Autorizados $  end  clock set 20:30:00 15 may 2025  copy running-config startup-config  vlan database  vlan 10 name UNED  vlan 20 name SEDE  vlan 30 name OPERACIONES  vlan 999 name PARQUEO  vlan 1000 name NATIVE  exit  configure terminal  interface FastEthernet1/6  switchport mode access  switchport access vlan 30  interface range FastEthernet1/1 - 5, FastEthernet1/7 - 15  switchport mode access  switchport access vlan 999  shutdown  interface FastEthernet1/0  switchport mode trunk  switchport trunk native vlan 1000  switchport trunk allowed vlan 1,2,10,20,30,1000,1002-1005  end  copy running-config startup-config |

# Script completo de cada PC

|  |  |
| --- | --- |
| PC-A | PC-B |
| ip 192.168.20.3 255.255.255.0 192.168.20.1 | ip 192.168.30.3 255.255.255.0 192.168.30.1 |

# Conclusión

En conclusión, la realización de este proyecto me ha permitido comprender de manera más profunda la configuración de redes utilizando direcciones IPv4 para asegurar la conectividad entre los dispositivos en una topología compuesta por routers, switches y PC. La configuración de parámetros básicos en los dispositivos, como la asignación de contraseñas cifradas, la creación de banners de seguridad y la asignación de direcciones IP en cada dispositivo, resultó ser fundamental para garantizar una red segura y bien estructurada.

Además, la creación y asignación de VLAN en los switches permitió segmentar la red de manera eficiente, y el uso de enlaces troncales 802.1Q facilitó la comunicación entre las diferentes VLANs, asegurando una correcta transmisión de datos. La implementación del enrutamiento entre VLANs, mediante subinterfaces en el router, también fue clave para asegurar que la red fuera capaz de comunicar sus diferentes segmentos de manera efectiva.

Durante las pruebas de conectividad, el uso de comandos como ping y trace permitió verificar que las configuraciones realizadas eran correctas y que los dispositivos se comunicaban entre sí sin inconvenientes. El proyecto ha sido fundamental para afianzar mis conocimientos en la configuración y gestión de redes, además de proporcionarme habilidades valiosas para la administración de redes en entornos reales y dinámicos

# Referencias

Comandos relacionados con IPv6 (Guía de administración del sistema: Servicios IP). (s. f.). Recuperado 23 de marzo de 2025, de https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-ref-74/index.html

Configuración del Ruteo Inter-VLAN con Switches Catalyst. (s. f.). Cisco. Recuperado 6 de abril de 2025, de https://www.cisco.com/c/es\_mx/support/docs/lan-switching/inter-vlan-routing/218429-configure-inter-vlan-routing-with-cataly.html

Configuración de IPv4 e IPv6 en un punto de acceso inalámbrico. (s. f.). Cisco. Recuperado 23 de marzo de 2025, de https://www.cisco.com/c/es\_mx/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5176-configure-ipv4-and-ipv6-on-a-wireless-access-point.html

Comer, D. E. (2015). REDES DE COMPUTACION E INTERNET, 6th Edition. [[VitalSource Bookshelf version]]. Retrieved from vbk://9786073233248

Online IP Subnet Calculator and CIDR Calculator. (s. f.). Recuperado 21 de febrero de 2025, de https://www.subnet-calculator.com/