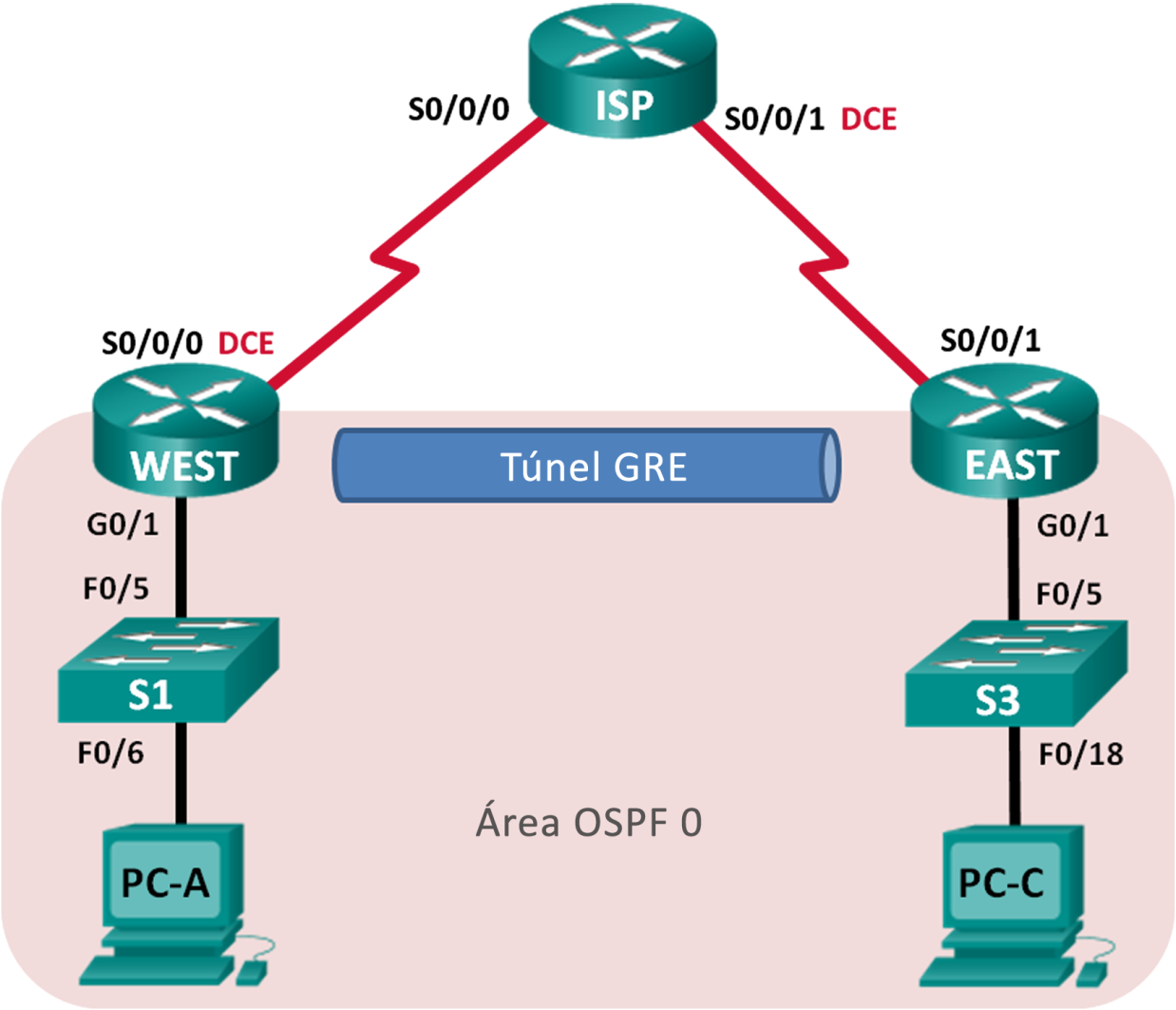
Práctica de laboratorio: Configuración de un túnel VPN GRE de punto a punto (versión para el instructor)

**Nota para el instructor:** el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

1. Topología



1. Tabla de asignación de direcciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| WEST | G0/1 | 172.16.1.1 | 255.255.255.0 | N/D |
| S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/D |
| Tunnel0 | 172.16.12.1 | 255.255.255.252 | N/D |
| ISP | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/D |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/D |
| EAST | G0/1 | 172.16.2.1 | 255.255.255.0 | N/D |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/D |
| Tunnel0 | 172.16.12.2 | 255.255.255.252 | N/D |
| PC-A | NIC | 172.16.1.3 | 255.255.255.0 | 172.16.1.1 |
| PC-C | NIC | 172.16.2.3 | 255.255.255.0 | 172.16.2.1 |

1. Objetivos

Parte 1: Configurar los parámetros básicos de los dispositivos

Parte 2: Configuración de GRE Tunnel

Parte 3: Habilitar el routing por el túnel GRE

1. Aspectos básicos/situación

La encapsulación de routing genérico (GRE) es un protocolo de tunneling que puede encapsular diversos protocolos de capa de red entre dos ubicaciones a través de una red pública, como Internet.

GRE se puede utilizar con lo siguiente:

* 1. La conexión de redes IPv6 a través de redes IPv4
  2. Paquetes de multidifusión, como OSPF, EIGRP y aplicaciones de transmisión

En esta práctica de laboratorio, configurará un túnel VPN GRE de punto a punto sin cifrar y verificará que el tráfico de la red utilice el túnel. También configurará el protocolo de routing OSPF dentro del túnel VPN GRE. El túnel GRE se encuentra entre los routers EAST y WEST en el área OSPF 0. El ISP no tiene conocimiento del túnel GRE. La comunicación entre los routers EAST, WEST e ISP se logra mediante rutas estáticas predeterminadas.

**Nota**: Los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco de la serie 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

**Nota**: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

**Nota para el instructor:** consulte el manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

1. Recursos necesarios

* 3 routers (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
* 2 switches (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
* 2 PC (Windows con un programa de emulación de terminal, como Tera Term)
* Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
* Cables Ethernet y seriales, como se muestra en la topología

1. Configurar los parámetros básicos de dispositivos

En la parte 1, configurará la topología de la red y los parámetros el router básicos, como las direcciones IP de las interfaces, el routing, el acceso a los dispositivos y las contraseñas.

* 1. Realizar el cableado de red tal como se muestra en la topología
  2. Inicializar y volver a cargar los routers y los switches
  3. Configurar los parámetros básicos para cada router
     1. Desactive la búsqueda de DNS.
     2. Configure los nombres de los dispositivos.
     3. Cifre las contraseñas de texto no cifrado.
     4. Cree un aviso de mensaje del día (MOTD) para advertir a los usuarios que el acceso no autorizado está prohibido.
     5. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
     6. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
     7. Establezca el inicio de sesión de consola en modo sincrónico.
     8. Aplique las direcciones IP a las interfaces Serial y Gigabit Ethernet según la tabla de direccionamiento y active las interfaces físicas. Todavía NO configure las interfaces Tunnel0.
     9. Establezca la frecuencia de reloj en **128000** para las interfaces seriales DCE.
  4. Configurar las rutas predeterminadas al router ISP.

WEST(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

EAST(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

* 1. Configurar las PC.

Asigne direcciones IP y gateways predeterminados a las PC según la tabla de asignación de direcciones.

* 1. Verifique la conectividad.

En este momento, las computadoras no pueden hacerse ping entre sí. Cada computadora debe poder hacer ping a su gateway predeterminado. Los routers pueden hacer ping a las interfaces seriales de los demás routers en la topología. De lo contrario, lleve a cabo la resolución de problemas hasta que pueda verificar la conectividad.

* 1. Guarde la configuración en ejecución.

1. Configurar un túnel GRE

En la parte 2, configurará un túnel GRE entre los routers EAST y WEST.

* 1. Configurar la interfaz de túnel GRE.
     1. Configure la interfaz de túnel en el router WEST. Utilice S0/0/0 en el router WEST como interfaz de origen del túnel y 10.2.2.1 como destino del túnel en el router EAST.

WEST(config)# **interface tunnel 0**

WEST(config-if)# **ip address 172.16.12.1 255.255.255.252**

WEST(config-if)# **tunnel source s0/0/0**

WEST(config-if)# **tunnel destination 10.2.2.1**

* + 1. Configure la interfaz de túnel en el router EAST. Utilice S0/0/1 en el router EAST como interfaz de origen del túnel y 10.1.1.1 como destino del túnel en el router WEST.

EAST(config)# **interface tunnel 0**

EAST(config-if)# **ip address 172.16.12.2 255.255.255.252**

EAST (config-if) # **tunnel source 10.2.2.1** **NO FUNCIONA PACKET TRACER**

EAST (config-if) # **tunnel source 10.2.2.1 S0/0/1**

EAST(config-if)# **tunnel destination 10.1.1.1**

**Nota**: para el comando **tunnel source**, tanto el nombre de la interfaz como la dirección IP se pueden utilizar como origen.

* 1. Verificar que el túnel GRE funcione.
     1. Verifique el estado de la interfaz de túnel en los routers EAST y WEST.

WEST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.1.1 YES manual up up

Serial0/0/0 10.1.1.1 YES manual up up

Serial0/0/1 unassigned YES unset administratively down down

Tunnel0 172.16.12.1 YES manual up up

EAST# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Embedded-Service-Engine0/0 unassigned YES unset administratively down down

GigabitEthernet0/0 unassigned YES unset administratively down down

GigabitEthernet0/1 172.16.2.1 YES manual up up

Serial0/0/0 unassigned YES unset administratively down down

Serial0/0/1 10.2.2.1 YES manual up up

Tunnel0 172.16.12.2 YES manual up up

* + 1. Emita el comando **show interfaces tunnel 0** para verificar el protocolo de tunneling, el origen y el destino de túnel que se utilizan en este túnel.

¿Qué protocolo de tunneling se utiliza? ¿Cuáles son las direcciones IP de origen y destino de túnel asociadas al túnel GRE en cada router?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

El protocolo de tunneling que se utiliza es GRE. Para el router WEST, el origen del túnel es 10.1.1.1 (Serial0/0/0) y el destino es 10.2.2.1. Para el router EAST, el origen del túnel es 10.2.2.1 y el destino es 10.1.1.1.

WEST# **show interfaces tunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.1/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/0

Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 0:00:12, output 0:00:12, output hang never

Last clearing of "show interface" counters 0:01:29

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

EAST# **show interfaces tunnel 0**

Tunnel0 is up, line protocol is up

Hardware is Tunnel

Internet address is 172.16.12.2/30

MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation TUNNEL, loopback not set

Keepalive not set

Tunnel source 10.2.2.1, destination 10.1.1.1

Tunnel Subblocks:

src-track:

Tunnel0 source tracking subblock associated with Serial0/0/1

Set of tunnels with source Serial0/0/1, 1 member (includes iterators), on interface <OK>

Tunnel protocol/transport GRE/IP

Key disabled, sequencing disabled

Checksumming of packets disabled

Tunnel TTL 255, Fast tunneling enabled

Tunnel transport MTU 1476 bytes

Tunnel transmit bandwidth 8000 (kbps)

Tunnel receive bandwidth 8000 (kbps)

Last input 0:01:28, output 0:01:28, output hang never

Last clearing of "show interface" counters 0:02:50

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/0 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

5 packets input, 620 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicasts)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

5 packets output, 620 bytes, 0 underruns

0 output errors, 0 collisions, 0 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

* + 1. Haga ping a través del túnel desde el router WEST hasta el router EAST con la dirección IP de la interfaz de túnel.

Ping **172.16.12.2 de WEST#**

Escriba la secuencia de escape para interrumpir la acción.

Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms

* + 1. Utilice el comando **traceroute** en el router WEST para determinar la ruta a la interfaz de túnel en el router EAST. ¿Cuál es la ruta al router EAST? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 172.16.12.1 > 172.16.12.2

WEST# **traceroute 172.16.12.2**

Escriba la secuencia de escape para interrumpir la acción.

Tracing the route to 172.16.12.2

VRF info: (vrf in name/id, vrf out name/id)

1 172.16.12.2 20 msec 20 msec \*

* + 1. Haga ping a la ruta a través del túnel y rastréela desde el router EAST hasta el router WEST con la dirección IP de la interfaz de túnel.

¿Cuál es la ruta al router WEST desde el router EAST? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 172.16.12.2 > 172.16.12.1

¿A qué interfaces se asocian estas direcciones IP? Explique.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A las interfaces de túnel 0 tanto en el router WEST como en el router EAST. El tráfico utiliza el túnel.

* + 1. Los comandos **ping** y **traceroute** deberían realizarse correctamente. De lo contrario, lleve a cabo la resolución de problemas antes de continuar con la parte siguiente.

1. Habilitar el routing por el túnel GRE

En la parte 3, configurará el routing OSPF de modo que las LAN en los routers EAST y WEST se puedan comunicar mediante el túnel GRE.

Después de configurar el túnel GRE, se puede implementar el protocolo de routing. Para la túneles GRE, una sentencia de red incluye red IP del túnel, en lugar de la red conectada a la interfaz serial. como lo haría con otras interfaces, como serial y Ethernet. Recuerde que el router ISP no participa en este proceso de routing.

* 1. Configurar el routing OSPF para el área 0 a través del túnel.
     1. Configure la ID de proceso OSPF 1 con el área 0 en el router WEST para las redes 172.16.1.0/24 y 172.16.12.0/24.

WEST(config)# **router ospf 1**

WEST(config-router)# **network 172.16.1.0 0.0.0.255 area 0**

WEST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

* + 1. Configure la ID de proceso OSPF 1 con el área 0 en el router EAST para las redes 172.16.2.0/24 y 172.16.12.0/24.

EAST(config)# **router ospf 1**

EAST(config-router)# **network 172.16.2.0 0.0.0.255 area 0**

EAST(config-router)# **network 172.16.12.0 0.0.0.3 area 0**

* 1. Verificar el routing OSPF.
     1. Desde el router WEST, emita el comando **show ip route** para verificar la ruta a la LAN 172.16.2.0/24 en el router EAST.

WEST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 10.1.1.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.1.1.0/30 is directly connected, Serial0/0/0

L 10.1.1.1/32 is directly connected, Serial0/0/0

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

C 172.16.1.0/24 is directly connected, GigabitEthernet0/1

L 172.16.1.1/32 is directly connected, GigabitEthernet0/1

O 172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.1/32 is directly connected, Tunnel0

¿Cuál es la interfaz de salida y la dirección IP para llegar a la red 172.16.2.0/24?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Para llegar a 172.16.2.0/24, se utiliza la interfaz de túnel 0 con la dirección IP 172.16.12.2.

* + 1. Desde el router EAST, emita el comando para verificar la ruta a la LAN 172.16.1.0/24 en el router WEST.

¿Cuál es la interfaz de salida y la dirección IP para llegar a la red 172.16.1.0/24?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Para llegar a 172.16.1.0/24, se utiliza la interfaz de túnel 0 con la dirección IP 172.16.12.1.

EAST# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, \* - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 10.2.2.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.2.2.0/30 is directly connected, Serial0/0/1

L 10.2.2.1/32 is directly connected, Serial0/0/1

172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks

O 172.16.1.0/24 [110/1001] via 172.16.12.1, 0:02:44, Tunnel0

C 172.16.2.0/24 is directly connected, GigabitEthernet0/1

L 172.16.2.1/32 is directly connected, GigabitEthernet0/1

C 172.16.12.0/30 is directly connected, Tunnel0

L 172.16.12.2/32 is directly connected, Tunnel0

* 1. Verificar la conectividad de extremo a extremo
     1. Emita un comando ping de la PC-A a la PC-C. Esta acción de realizarse correctamente. De lo contrario, lleve a cabo la resolución de problemas hasta que haya conectividad de extremo a extremo.

**Nota**: Puede ser necesario desactivar el firewall de las computadoras para hacer ping entre ellas.

* + 1. Traceroute de la PC-A a la PC-C. ¿Cuál es la ruta de la PC-A a la PC-C?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

172.16.1.1 > 172.16.12.2 (interfaz de túnel en el router EAST) > 172.16.2.3

1. Reflexión
   1. ¿Qué otra configuración se necesita para crear un túnel GRE protegido?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Se puede configurar IPsec a fin de cifrar los datos para un túnel GRE seguro.

* 1. Si agregara más redes LAN al router WEST o EAST, ¿qué debería hacer para que la red utilice el túnel GRE para el tráfico?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Se deberían agregar las nuevas redes a los mismos protocolos de routing que la interfaz del túnel.

1. Tabla de resumen de interfaces de router

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resumen de interfaces de router | | | | |
| Modelo de router | Interfaz Ethernet 1 | Interfaz Ethernet 2 | Interfaz serial 1 | Interfaz serial 2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Nota**: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de hacer una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz. | | | | |

1. Configuraciones de dispositivos
2. Router WEST

WEST# show run

Building configuration...

Current configuration : 1798 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname WEST

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

no ip domain lookup

no ipv6 cef

multilink bundle-name authenticated

!

interface Tunnel0

ip address 172.16.12.1 255.255.255.252

tunnel source Serial0/0/0

tunnel destination 10.2.2.1

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 172.16.1.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.1 255.255.255.252

clock rate 128000

!

interface Serial0/0/1

no ip address

shutdown

!

router ospf 1

network 172.16.1.0 0.0.0.255 area 0

network 172.16.12.0 0.0.0.3 area 0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 10.1.1.2

!

control-plane

!

!

banner motd ^C

Unauthorized Access Prohibited.

^C

!

line con 0

password 7 14141B180F0B

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 05080F1C2243

login

transport input all

!

scheduler allocate 20000 1000

!

end

1. Router ISP

**ISP#** show run

Building configuration...

Current configuration : 1406 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname ISP

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

redundancy

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

shutdown

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.1.1.2 255.255.255.252

!

interface Serial0/0/1

ip address 10.2.2.2 255.255.255.252

clock rate 128000

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

control-plane

!

!

banner motd ^C

Unauthorized Access Prohibited.

^C

!

línea con 0

password 7 02050D480809

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 045802150C2E

login

transport input all

!

scheduler allocate 20000 1000

!

end

1. Router EAST

EAST# show run

Building configuration...

Current configuration : 1802 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname EAST

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

redundancy

!

interface Tunnel0

ip address 172.16.12.2 255.255.255.252

tunnel source 10.2.2.1

tunnel destination 10.1.1.1

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

interface GigabitEthernet0/0

no ip address

shutdown

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 172.16.2.1 255.255.255.0

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

!

interface Serial0/0/1

ip address 10.2.2.1 255.255.255.252

!

router ospf 1

network 172.16.2.0 0.0.0.255 area 0

network 172.16.12.0 0.0.0.3 area 0

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 0.0.0.0 0.0.0.0 10.2.2.2

!

control-plane

!

banner motd ^C

Unauthorized Access Prohibited.

^C

!

line con 0

password 7 00071A150754

logging synchronous

login

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport input all

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

password 7 030752180500

login

transport input all

!

scheduler allocate 20000 1000

!

end