UD7-1 WAN y REDES VIRTUALES

Índice

Arquitectura WAN

WAN significa **Red de Área Amplia** (Wide Area Network), y el nombre ya debería darte una buena idea de lo que es una WAN. Una WAN es una red que se extiende sobre un área geográfica extensa, por ejemplo, entre ciudades, entre países, etc. Por tanto, las WAN se usan para conectar redes LAN que están geográficamente separadas.

Por ejemplo, si una empresa tiene una oficina en Nueva York, otra en Toronto y otra en Londres, cada una de esas oficinas tiene su propia LAN (Red de Área Local), y las conexiones entre ellas forman una WAN. Aunque Internet en sí puede considerarse una WAN, el término WAN suele usarse para referirse a las conexiones privadas de una empresa que unen sus oficinas, centros de datos y otros sitios.

Así que, como dije, Internet puede considerarse una WAN, pero normalmente cuando hablamos de WAN no nos referimos a Internet. Aunque hay otra tecnología que puede usarse sobre Internet para crear conexiones privadas: **VPNs** (Redes Privadas Virtuales), que permiten crear conexiones privadas sobre conexiones públicas y compartidas como Internet. Te mostraré algunos tipos de VPNs en este vídeo.

Debes saber que ha habido muchas tecnologías WAN diferentes a lo largo del tiempo. Dependiendo de la ubicación, algunas estarán disponibles y otras no.

Introducción a las líneas dedicadas (Leased Lines)

Cada oficina está conectada al centro de datos mediante una **línea dedicada**, que es un tipo de conexión física dedicada entre dos sitios. No es una conexión compartida ni está conectada a Internet; es una conexión privada que la empresa utiliza para conectar sus sedes.

Cuando hablamos de WANs, en lugar de topología en estrella usamos un término más común que es *topología de hub-and-spoke* (concentrador y radios). El sitio central (el centro de datos) se llama *hub*, y las oficinas que se conectan al hub se llaman *spokes*.

Una ventaja de esta topología frente a una topología de malla completa es que es más fácil controlar de forma centralizada qué tráfico se permite y cuál no. Todo el tráfico entre oficinas puede enviarse, por ejemplo, a un cortafuegos en el centro de datos, que decidirá qué tráfico está permitido.

Cada sitio se conecta a un proveedor de servicios, que es quien los conecta entre sí.

Estas conexiones utilizan **cables seriales**, usan encapsulaciones de capa 2 como **HDLC** y **PPP**, no Ethernet. Sin embargo, hoy en día las conexiones WAN mediante Ethernet son cada vez más comunes. Las conexiones de **fibra óptica** permiten cables mucho más largos que los cables Ethernet tradicionales de cobre UTP, por lo que hoy en día las WANs mediante cables Ethernet de fibra óptica son bastante comunes.

Sin embargo, Internet no es una red privada. Es una red pública y compartida, así que no es buena idea enviar datos importantes sin protección. En este caso, cada sitio tiene una conexión física a Internet, pero para enviar tráfico entre sitios, la empresa configura **VPNs** (Redes Privadas Virtuales).

Veremos varios tipos de VPN pero básicamente los paquetes se cifran para que solo puedan ser leídos por los destinatarios previstos. Luego, el paquete cifrado se encapsula dentro de un nuevo paquete y se envía. Esto significa que el paquete original se mantiene protegido incluso al enviarse por Internet.

MPLS

MPLS significa *Multiprotocol Label Switching*. Al igual que Internet, las redes MPLS de los proveedores son infraestructuras compartidas que conectan muchas empresas. Sin embargo, el uso de **etiquetas** permite crear VPNs en la red MPLS, separando el tráfico de cada cliente para que no se mezcle.

Conceptos clave:

- **CE Router (Customer Edge)**: router del cliente
- **PE Router (Provider Edge)**: router del proveedor que se conecta al cliente
- **P Router**: router del proveedor interno, sin conexión directa al cliente

Las etiquetas MPLS se colocan entre la cabecera Ethernet (capa 2) y la cabecera IP (capa 3), por eso MPLS a veces se llama un protocolo de **Capa 2.5**. El enrutamiento se basa en etiquetas, no en direcciones IP.

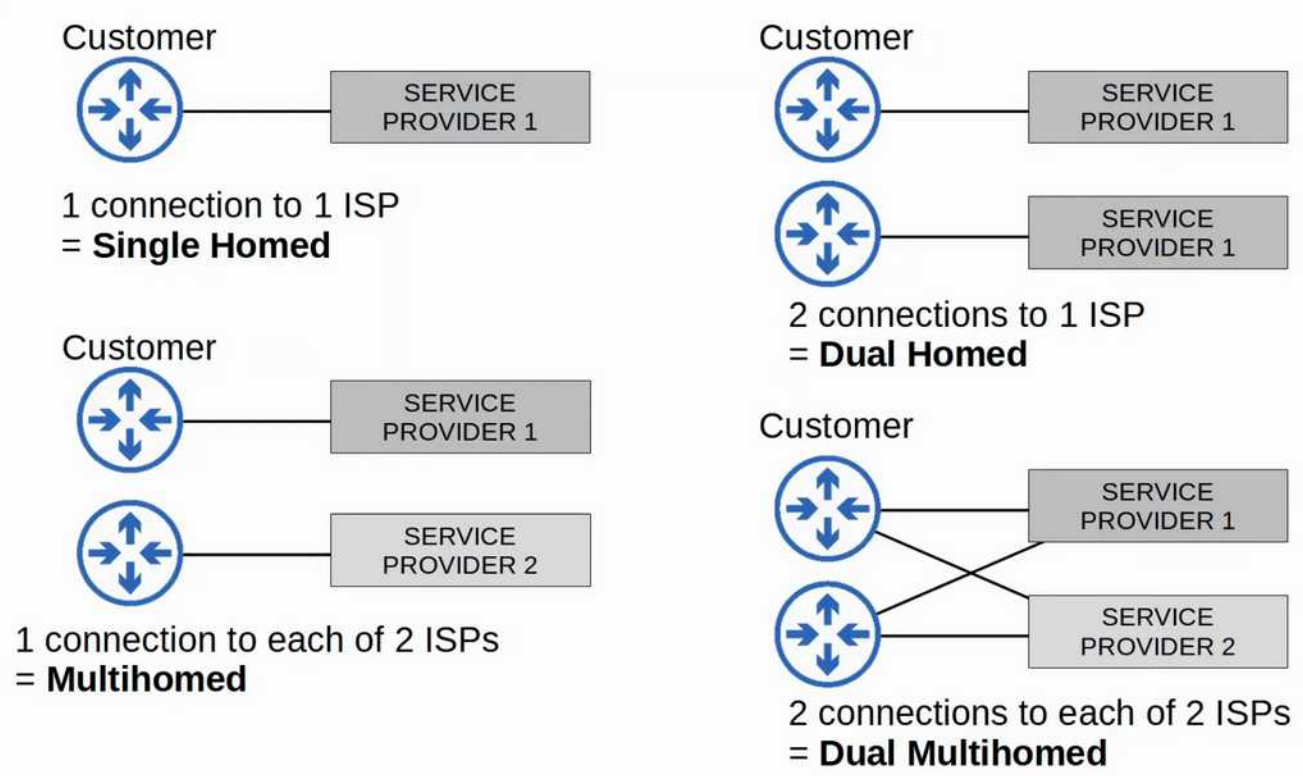
Hay dos tipos de VPN sobre MPLS:

1. **MPLS VPN de Capa 3**: los routers CE se conectan a los PE mediante protocolos de enrutamiento (como OSPF) o rutas estáticas.
2. **MPLS VPN de Capa 2**: los routers CE están en la misma subred y es como si estuvieran directamente conectados, aunque haya una red MPLS entre ellos.

Los sitios pueden conectarse a la red MPLS mediante diversos medios: fibra, 4G/5G, cable coaxial (CATV), líneas arrendadas, etc.

Conexiones redundantes a Internet

Para los usuarios domésticos, perder Internet no es un desastre. Pero para una empresa puede ser crítico, por eso se recomienda tener conexiones redundantes. Términos importantes:



VPN

Cada vez que alguien se conecta a Internet, lo hace a través de un determinado dispositivo, ya sea un ordenador de mesa, un portátil, un teléfono móvil, una tableta, etc. La cuestión es que cada uno de esos dispositivos tiene asignada una dirección IP, por lo que no es difícil poder rastrear desde dónde se están conectando. Internet, al igual que el resto de redes públicas, son poco seguras y suelen ser el coto de caza habitual de los piratas informáticos.

Cada vez es más frecuente que las organizaciones de pequeño y medio tamaño usen "intranets" como redes de comunicación principal, las cuales utilizan la infraestructura de redes públicas como Internet. Este tipo de redes aportan un grado razonable de seguridad, pero tienen ciertas limitaciones en su acceso. De hecho, es habitual que un empleado de la organización quiera conectarse a su intranet desde cualquier lugar, por ejemplo, a través de una red wifi abierta en un aeropuerto, en un centro comercial, etc. Y es aquí donde toma especial importancia el uso de las redes privadas virtuales (VPN), para poder asegurar que esos accesos se realicen con total garantía.

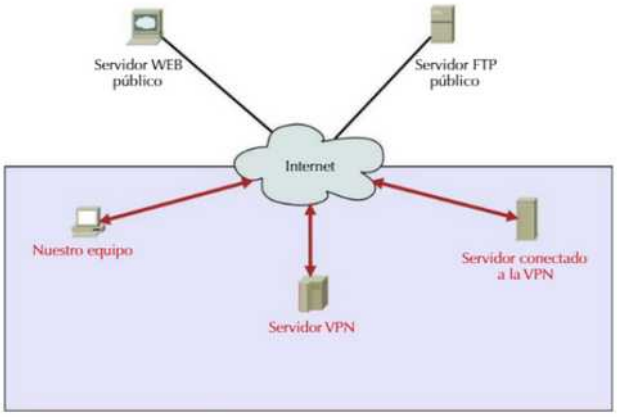
Entre los usos típicos que pueden hacerse de las VPN, cabe destacar:

- Conectarse de manera remota con la red del trabajo de forma segura.
- Navegar por Internet de forma más segura.
- Obtener una mayor privacidad y ocultar la ubicación.
- Saltarse ciertas restricciones del proveedor propio.

Una red privada virtual es un servicio mediante el cual un equipo se conecta a otro, que hace de intermediario (el servidor VPN) entre dicho equipo y los servicios de Internet a los que desea acceder (correo electrónico, redes sociales, servicios en la nube, etc.). La conexión entre este equipo y el servidor VPN siempre está cifrada, por lo que, si alguien intercepta esas comunicaciones, sería incapaz de leer la información. Las redes privadas virtuales dividen la conexión en dos partes o zonas: la primera se extiende desde el equipo que se conecta hasta el servidor VPN y la segunda lo hace desde el servidor VPN hasta el servidor o servicio al que se va a conectar.

La zona más vulnerable en cuanto a la seguridad es la primera, ya que “acceder” a una red local de usuario es mucho más sencillo que acceder al servidor VPN o a los servidores de los servicios que se utilizan (web, ftp, etc.), debido a que las medidas de seguridad implementadas en la LAN del usuario dependen del nivel de conocimientos informáticos del mismo, que suele ser por lo general, bastante bajo.

Las organizaciones necesitan redes seguras, confiables y rentables para interconectar varias redes, por ejemplo, para permitir que las sucursales y los proveedores se conecten a la red de la oficina central de una empresa. Además, con el aumento en la cantidad de trabajadores a distancia, hay una creciente necesidad de las empresas de contar con formas seguras, confiables y rentables para que los empleados que trabajan en oficinas pequeñas y oficinas domésticas (SOHO), y en otras ubicaciones remotas se conecten a los recursos en sitios empresariales.



Las organizaciones utilizan las VPN para crear una conexión de red privada de extremo a extremo a través de redes externas como Internet o las extranets. El túnel elimina la barrera de distancia y

permite que los usuarios remotos accedan a los recursos de red del sitio central. Una VPN es una red privada creada mediante tunneling a través de una red pública, generalmente Internet. Una VPN es un entorno de comunicaciones en el que el acceso se controla de forma estricta para permitir las conexiones de peers dentro de una comunidad de interés definida.

Las primeras VPN eran exclusivamente túneles IP que no incluían la autenticación o el cifrado de los datos. Por ejemplo, la encapsulación de routing genérico (GRE) es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolo de capa de red dentro de los túneles IP. Esto crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP.

En la actualidad, las redes privadas virtuales generalmente se refieren a la implementación segura de VPN con cifrado, como las VPN con IPsec.

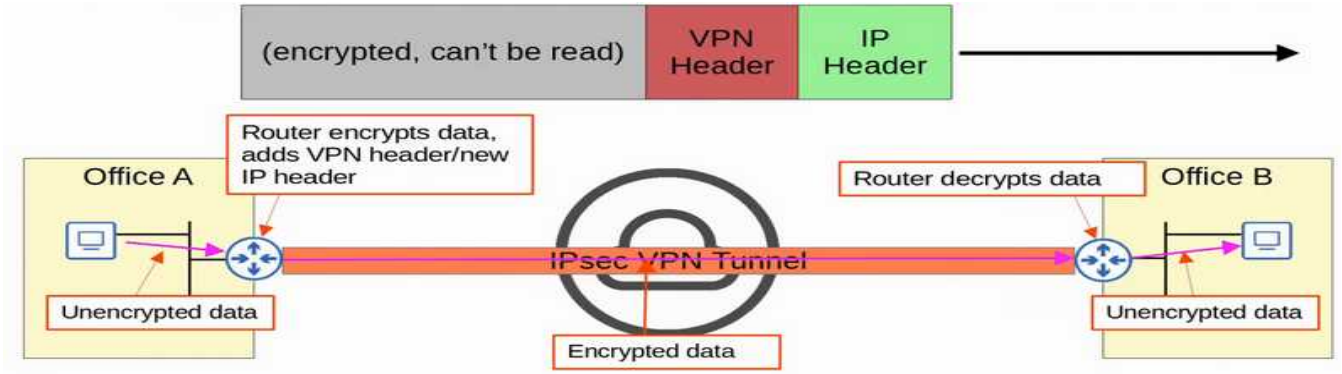
Para implementar las VPN, se necesita un gateway VPN. El gateway VPN puede ser un router, un firewall o un dispositivo de seguridad adaptable (ASA) de Cisco. Un ASA es un dispositivo de firewall independiente que combina la funcionalidad de firewall, concentrador VPN y prevención de intrusiones en una imagen de software.

VPN de sitio a sitio

Una VPN de sitio a sitio se crea cuando los dispositivos en ambos lados de la conexión VPN conocen la configuración de VPN con anticipación, como se muestra en la ilustración. La VPN permanece estática, y los hosts internos no saben que existe una VPN. En una VPN de sitio a sitio, los hosts terminales envían y reciben tráfico TCP/IP normal a través de un “gateway” VPN. El gateway VPN es el responsable de encapsular y cifrar el tráfico saliente para todo el tráfico de un sitio en particular. Después, el gateway VPN lo envía por un túnel VPN a través de Internet a un gateway VPN de peer en el sitio de destino. Al recibirlo, el gateway VPN de peer elimina los encabezados, descifra el contenido y transmite el paquete hacia el host de destino dentro de su red privada.

Una VPN de sitio a sitio es una extensión de una red WAN clásica. Las VPN de sitio a sitio conectan redes enteras entre sí, por ejemplo, pueden conectar la red de una sucursal a la red de la oficina central de una empresa. En el pasado, se requería una conexión de línea arrendada o de Frame Relay para conectar sitios, pero dado que en la actualidad la mayoría de las empresas tienen acceso a Internet, estas conexiones se pueden reemplazar por VPN de sitio a sitio.

Estas conexiones suelen ser utilizadas generalmente por empresas y organismos que buscan conectar de forma segura dos o más sedes muy distantes geográficamente. El protocolo más utilizado debido a su simplicidad es IPSec. Para establecer la conexión, se deben definir los dispositivos encargados de encapsular y desencapsular el tráfico que viaja de extremo a extremo (generalmente, routers). También deben definirse los usuarios y contraseñas y los certificados que se van a utilizar. Las redes IPSec son mucho más dinámicas que las redes VPN basadas en cliente, por lo que desde ellas se va a poder configurar el tipo de tráfico e incluso aplicar una serie de reglas o filtros, aumentando tanto el rendimiento de las redes como la seguridad



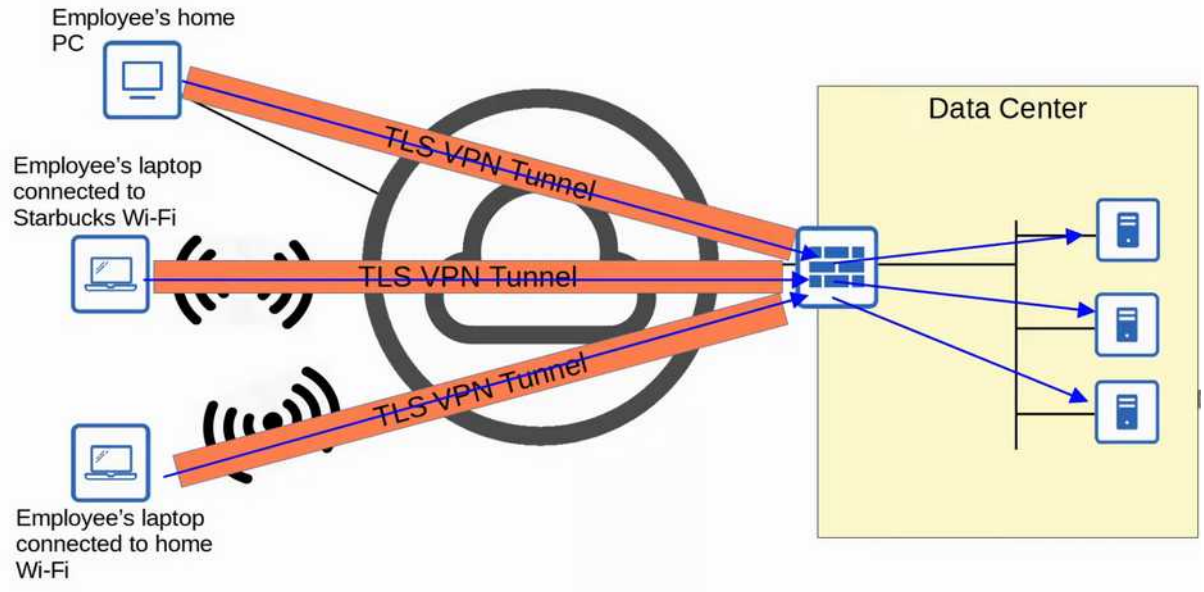
VPN de acceso remoto

Si se utiliza una VPN de sitio a sitio para conectar redes enteras, la VPN de acceso remoto admite las necesidades de los empleados a distancia, de los usuarios móviles y del tráfico de extranet de cliente a empresa. Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y se puede habilitar y deshabilitar. Las VPN de acceso remoto admiten una arquitectura cliente/servidor, en la que el cliente VPN (host remoto) obtiene acceso seguro a la red empresarial mediante un dispositivo del servidor VPN en el perímetro de la red.

Las VPN de acceso remoto se utilizan para conectar hosts individuales que deben acceder a la red de su empresa de forma segura a través de Internet. La conectividad a Internet que utilizan los trabajadores a distancia suele ser una conexión por banda ancha, DSL, cable, fibra o inalámbrica

Las VPNs de acceso remoto típicamente usan TLS (Transport Layer Security), a diferencia de las VPNs de sitio a sitio que típicamente usan IPsec.

Es posible que se deba instalar un software de cliente VPN en la terminal del usuario móvil; por ejemplo, cada host puede tener el software Cisco AnyConnect Secure Mobility Client instalado. Cuando el host intenta enviar cualquier tipo de tráfico, el software Cisco AnyConnect VPN Client encapsula y cifra este tráfico. Después, los datos cifrados se envían por Internet al gateway VPN en el perímetro de la red de destino. Al recibirlos, el gateway VPN se comporta como lo hace para las VPN de sitio a sitio.



Estas redes hacen uso de una aplicación (cliente) que es la encargada de controlar completamente la conexión y establecerla. Para poder navegar por esta red, generalmente, los usuarios necesitan de un usuario y una contraseña que les identifica ante el servidor VPN.

Una vez se inicia sesión, se establece la conexión de manera que toda la comunicación entre el cliente y el servidor se realiza de forma segura y privada. Este es el método más rápido y sencillo para conectar prácticamente cualquier equipo o dispositivo. Los protocolos más utilizados para este tipo de conexiones son L2TP, PPTP y SSTP. Además, si se quiere obtener una seguridad superior, pueden utilizarse protocolos OpenVPN, aunque son más complejos.

Códigos de error

Las redes privadas virtuales (VPN) son una gran forma de dar a la persona que administre la red una ventaja adicional en la batalla contra los ciberdelincuentes, así como contra los países que desean restringir los sitios que se pueden ver. Pero, aunque el concepto de la VPN es muy atractivo, también tienen obstáculos y barreras que deben superarse para que funcionen adecuadamente. Entre los códigos de errores más comunes de VPN que suelen aparecer están:

● Código 691. La conexión remota fue denegada porque la combinación de nombre de usuario y contraseña que se introdujo no fue reconocida, o el protocolo de autenticación seleccionado no está permitido en el servidor de acceso remoto. Normalmente, esto se debe a la escritura errónea del nombre de usuario o contraseña. En el caso del protocolo, el administrador simplemente deberá verificar que ambos extremos de la conexión utilizan el mismo.

● Código 800. El cliente VPN no puede conectarse al servidor. El administrador tendrá que verificar que la información del servidor de VPN es correcta y, si todo está bien, comprobar que el cortafuegos no esté configurado para bloquear las conexiones IP.

● Código 619. No se puede establecer la conexión con un ordenador remoto. La persona que administre la red deberá asegurarse de que solo un cliente VPN funciona a la vez en el ordenador. Si eso no arregla este error usual de VPN, intentará deshabilitar el cortafuegos o antivirus temporalmente para ver si lo están bloqueando. En ocasiones puede arreglarse al reiniciar o reinstalar el cliente.

● Código 51. No se puede comunicar con el subsistema de la VPN. No hay muchas soluciones o trucos para arreglar este error de VPN que no sean reiniciar el servicio de VPN o ejecutar un diagnóstico de problemas de la conexión de red local.

● Código 412. El par remoto no responde. Frecuentemente, se debe a un fallo de red del lado del cliente, pero si la conexión de red es potente, entonces el problema seguramente esté en el cortafuegos, que está interfiriendo. Habrá que volver a conectar con el cortafuegos deshabilitado.

● Código 721. El ordenador remoto no respondió. El administrador debe comenzar por comprobar los ajustes del router para garantizar que el puerto TCP 1723. También deberá asegurarse de que el protocolo PPTP esté activado en el router y que el cortafuegos no está configurado para bloquear el tráfico.

● Código 720. No hay protocolos de control de PPP configurados. La solución a esta incidencia tiene bastante carga técnica, ya que implica que el administrador compruebe los protocolos que soporta el servidor y adapte los del cliente VPN

VRF

Virtual Routing and Forwarding (VRF) es un enrutador físico con múltiples enrutadores virtuales. Puedes pensarlo como VLANs para enrutadores.

- VLANs dividen un switch en múltiples switches virtuales, cada uno con su propio dominio de broadcast. Por defecto, todos los interfaces están en el mismo dominio de broadcast.

- VRF divide un enrutador en múltiples enrutadores virtuales, cada uno con su propia tabla de enrutamiento. Todos los interfaces estarán en el mismo "dominio de enrutamiento".

VRF no funciona en packet tracer.

Lo que hace VRF es permitir que un enrutador construya tablas de enrutamiento separadas. Normalmente, un enrutador tiene una sola tabla de enrutamiento, pero con VRF puede tener múltiples. Las interfaces (específicamente interfaces Capa 3) se configuran para estar en una instancia VRF específica.

- El tráfico en un VRF no puede pasar a otro VRF.

- Los proveedores de servicios usan VRF para:

1. Aislar el tráfico de diferentes clientes en un mismo dispositivo.

Cada cliente se conecta a su propio enrutador virtual (VRF) dentro del enrutador físico del proveedor.

2. Permitir direcciones IP solapadas entre clientes.

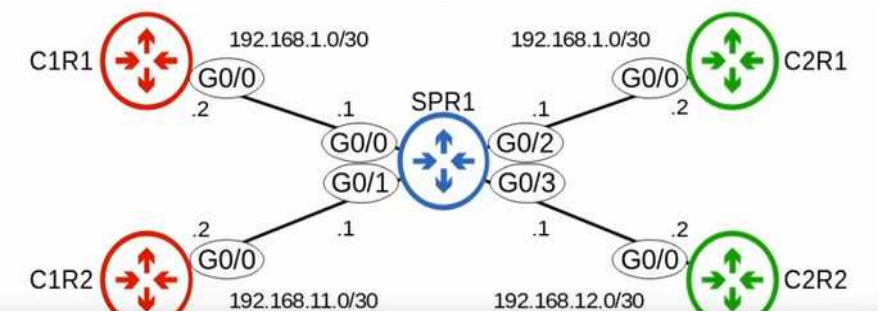
Configuración de VRF

1. Crear los VRFs (en modo de configuración global):

R1(config)# **ip vrf CUSTOMER1**

R1(config)# **ip vrf CUSTOMER2**

- Verificación: **show ip vrf**



2. Asignar interfaces a los VRFs:

R1(config-if)# interface GigabitEthernet0/0

R1(config-if)# **ip vrf forwarding CUSTOMER1**

R1(config-if)# ip address 192.168.1.1 255.255.255.252

Al asignar una interfaz a un VRF, su dirección IP se borra y hay que reconfigurarla.

show ip route muestra la tabla de enrutamiento global (vacía si todas las interfaces están en VRFs).

show ip route vrf CUSTOMER1 muestra la tabla de enrutamiento del VRF CUSTOMER1.

show ip route vrf CUSTOMER2 muestra la del VRF CUSTOMER2.