# ¿Qué solución VPN es la adecuada para usted?

## Contenido



## Introducción

Las redes privadas virtuales (VPN) se están tornando notablemente populares a un costo menor y de un modo más flexible para desplegar una red a través de un área ancha. Con los avances en la tecnología viene una variedad de opciones en aumento para implementar soluciones VPN. Esta nota técnica explica algunas de estas opciones y describe dónde podrían utilizarse mejor.

## Antes de comenzar

### Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

### Prerequisites

No hay requisitos previos específicos para este documento.

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

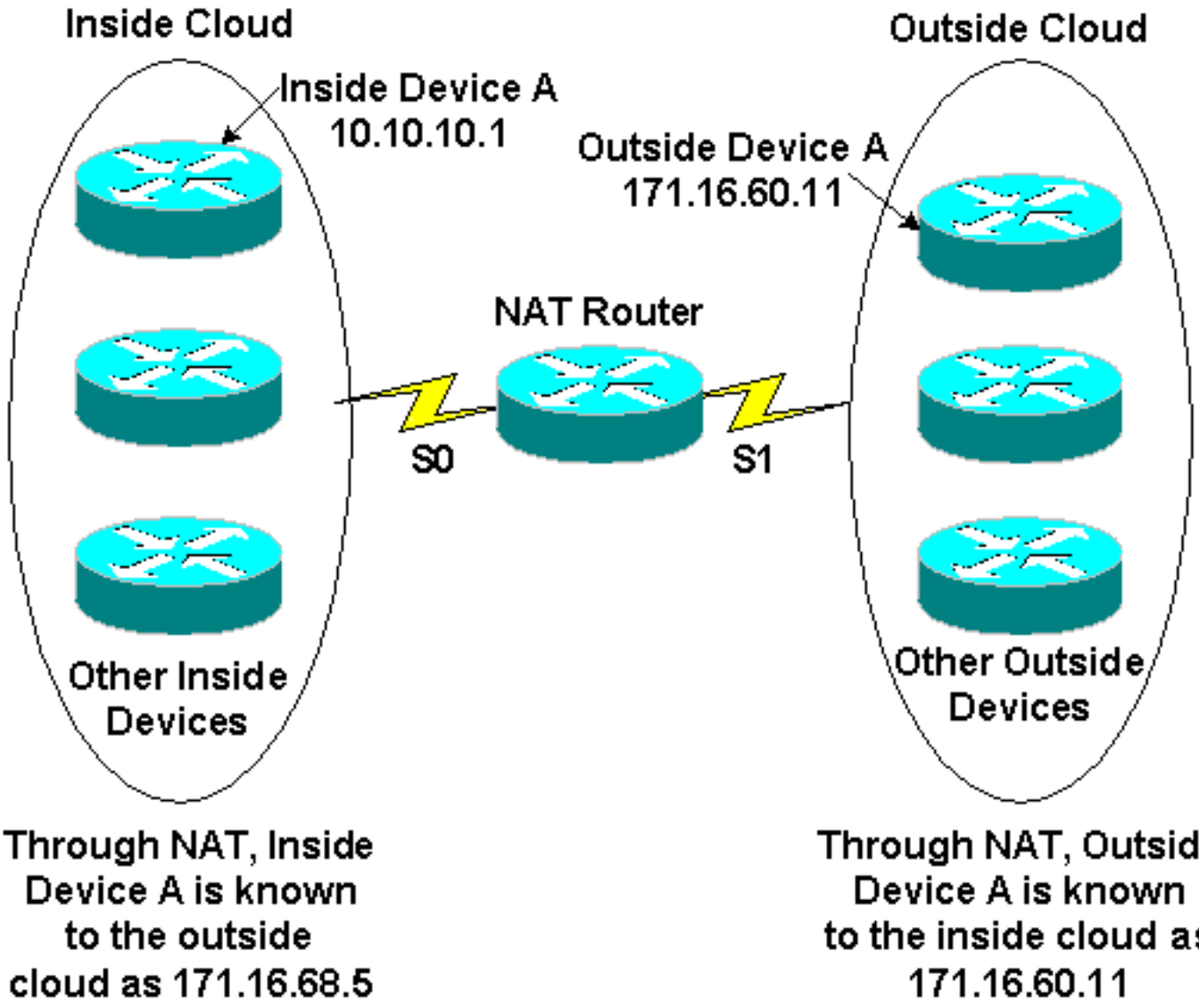
**Nota:** Cisco también proporciona soporte de cifrado en plataformas que no son de IOS, incluido el Cisco Secure PIX Firewall, el Cisco VPN 3000 Concentrator y el Cisco VPN 5000 Concentrator.

## NAT

Internet ha experimentado un crecimiento explosivo en poco tiempo, mucho más de lo que los diseñadores originales podrían haber previsto. El número limitado de direcciones disponibles en IP versión 4.0 es una evidencia de este crecimiento, y el resultado es que el espacio de la dirección está cada vez menos disponible. La traducción de direcciones de red (NAT) es una solución a este problema.

Al usar NAT, un router se configura con límites internos/externos de tal manera que el externo (generalmente Internet) vea una o algunas direcciones registradas, mientras que el interno podría tener cualquier número de hosts con un esquema de direccionamiento privado. Para preservar la integridad del esquema de la traducción de dirección, NAT debe ser configurado en cada router de frontera entre la red (privada) interna y la red (pública) externa. Una de las ventajas de NAT desde el punto de vista de la seguridad es que los sistemas en la red privada no pueden recibir una conexión IP entrante de la red externa a menos que la gateway NAT esté configurada específicamente para permitir la conexión. Además, NAT es completamente transparente para los dispositivos de origen y destino. La operación recomendada de NAT incluye RFC 1918 , que describe los esquemas de direccionamiento de red privada adecuados. El estándar para NAT se describe en RFC1631 .

La siguiente figura muestra la definición del límite del router NAT con un conjunto de direcciones de red de traducción interna.

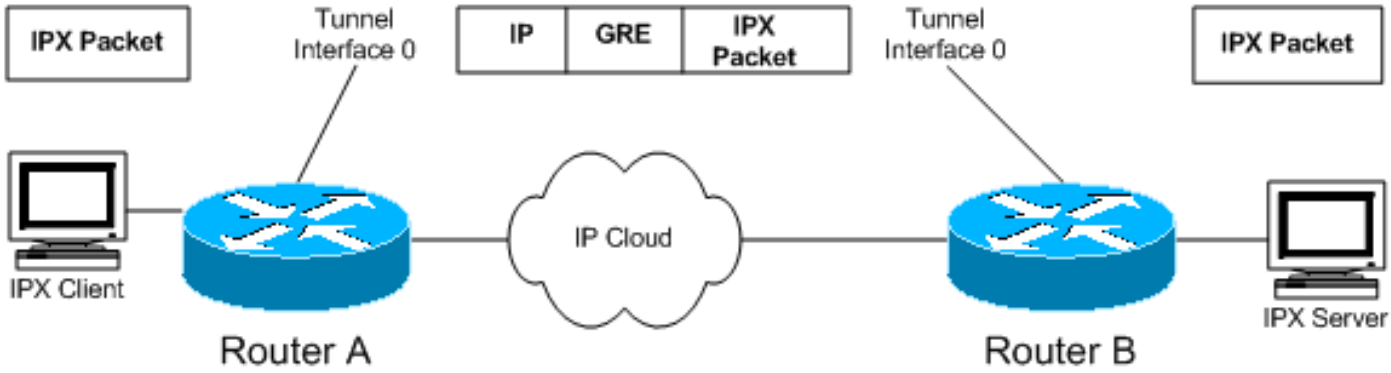



La NAT se utiliza generalmente para conservar las direcciones IP enrutables en Internet, que son costosas y tienen un número limitado. NAT también proporciona seguridad al ocultar la red interna de Internet.

Para obtener información sobre el funcionamiento de NAT, vea Cómo funciona NAT.

## Tunelización de Encapsulación GRE

Los túneles GRE (Generic Routing Encapsulation) proporcionan una ruta específica a través de la WAN compartida y encapsulan el tráfico con nuevos encabezados de paquete para garantizar la entrega a destinos específicos. La red es privada porque el tráfico puede entrar en un túnel solamente en un punto final y sólo puede salir en el otro extremo. Los túneles no proporcionan verdadera confidencialidad (como el cifrado), pero pueden transportar tráfico cifrado. Los túneles son extremos lógicos configurados en las interfaces físicas a través de las cuales se transporta el tráfico.




Como se ilustra en el diagrama, la tunelización GRE también se puede utilizar para encapsular el tráfico no IP en IP y enviarlo a través de Internet o de la red IP. Los protocolos Internet Packet Exchange (IPX) y AppleTalk son ejemplos de tráfico que no es de IP. Para obtener información sobre la configuración de GRE, vea "Configuración de una Interfaz de Túnel GRE" en Configuración de GRE.

GRE es la solución VPN adecuada para usted si tiene una red multiprotocolo como IPX o AppleTalk y tiene que enviar tráfico a través de Internet o una red IP. Además, la encapsulación GRE se utiliza generalmente junto con otros medios para proteger el tráfico, como IPSec.

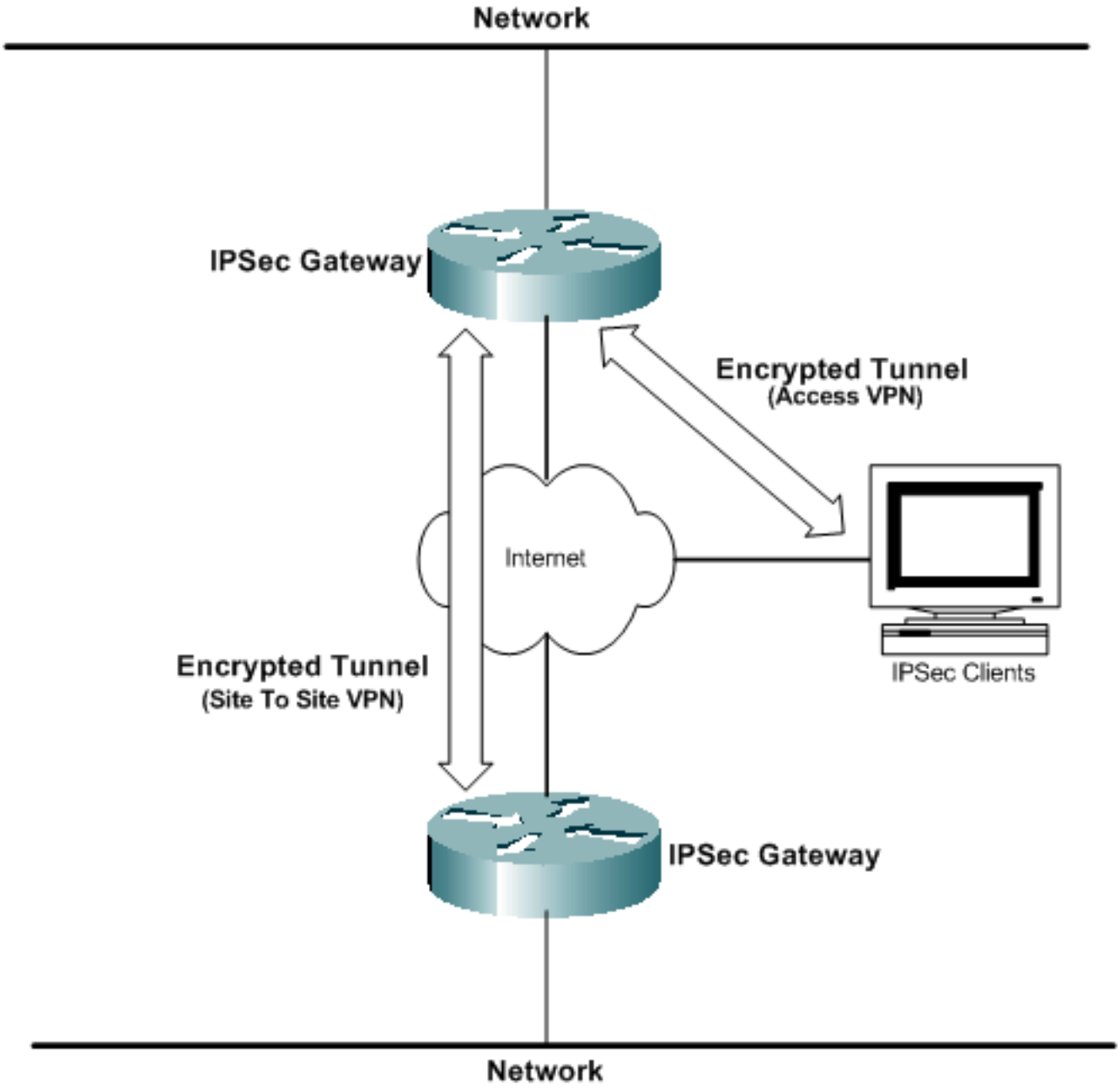
Para obtener más detalles técnicos sobre GRE, consulte RFC 1701 y RFC 2784 .

## Cifrado IPSec

El cifrado de los datos enviados a través de una red compartida es la tecnología VPN asociada con más frecuencia a las VPN. Cisco admite los métodos de cifrado de datos de seguridad IP (IPSec). IPSec es un marco de estándares abiertos que proporciona confidencialidad de datos, integridad de datos y autenticación de datos entre los pares participantes en la capa de red.

El cifrado IPSec es un estándar de Internet Engineering Task Force (IETF) que admite el estándar de cifrado de datos (DES) de 56 bits y el triple estándar de cifrado simétrico (3DES) de 168 bits en el software cliente IPSec. La configuración de GRE es opcional con IPSec. IPSec también admite autoridades de certificado y la negociación de Intercambio de clave de Internet (IKE). El encripción IPSec puede desplegarse en entornos autónomos entre clientes, routers y firewalls, o puede usarse junto con la tunelización L2TP en VPN de acceso. IPSec se admite en varias plataformas de sistemas operativos.

El cifrado IPSec es la solución VPN adecuada para usted si desea una verdadera confidencialidad de los datos de sus redes. IPSec también es un estándar abierto, por lo que la interoperabilidad entre diferentes dispositivos es fácil de implementar.




## PPTP y MPPE

El protocolo de túnel punto a punto (PPTP) fue desarrollado por Microsoft; se describe en RFC2637 . PPTP se implementa ampliamente en Windows 9x/ME, Windows NT y Windows 2000, y en el software cliente de Windows XP para habilitar VPN voluntarias.

El Cifrado punto a punto de Microsoft (MPPE) es un borrador IETF informativo que utiliza encripción de 40 ó 128 bits basado en RC4. MPPE es parte de la solución de software cliente PPTP de Microsoft y es útil en arquitecturas de VPN de acceso de modo voluntario. PPTP/MPPE es compatible con la mayoría de las plataformas de Cisco.

El soporte PPTP se agregó a la versión 12.0.5.XE5 de software del IOS de Cisco en las plataformas Cisco 7100 y 7200. Se incorporó compatibilidad para más plataformas en Cisco IOS 12.1.5.T. Cisco Secure PIX Firewall y el Concentrador VPN 3000 también incluyen soporte para las conexiones de cliente PPTP.

Dado que PPTP admite redes que no son IP, resulta útil que los usuarios remotos tengan que

marcar a la red corporativa para acceder a redes corporativas heterogéneas.

Para obtener información sobre la configuración de PPTP, vea Configuración de PPTP.

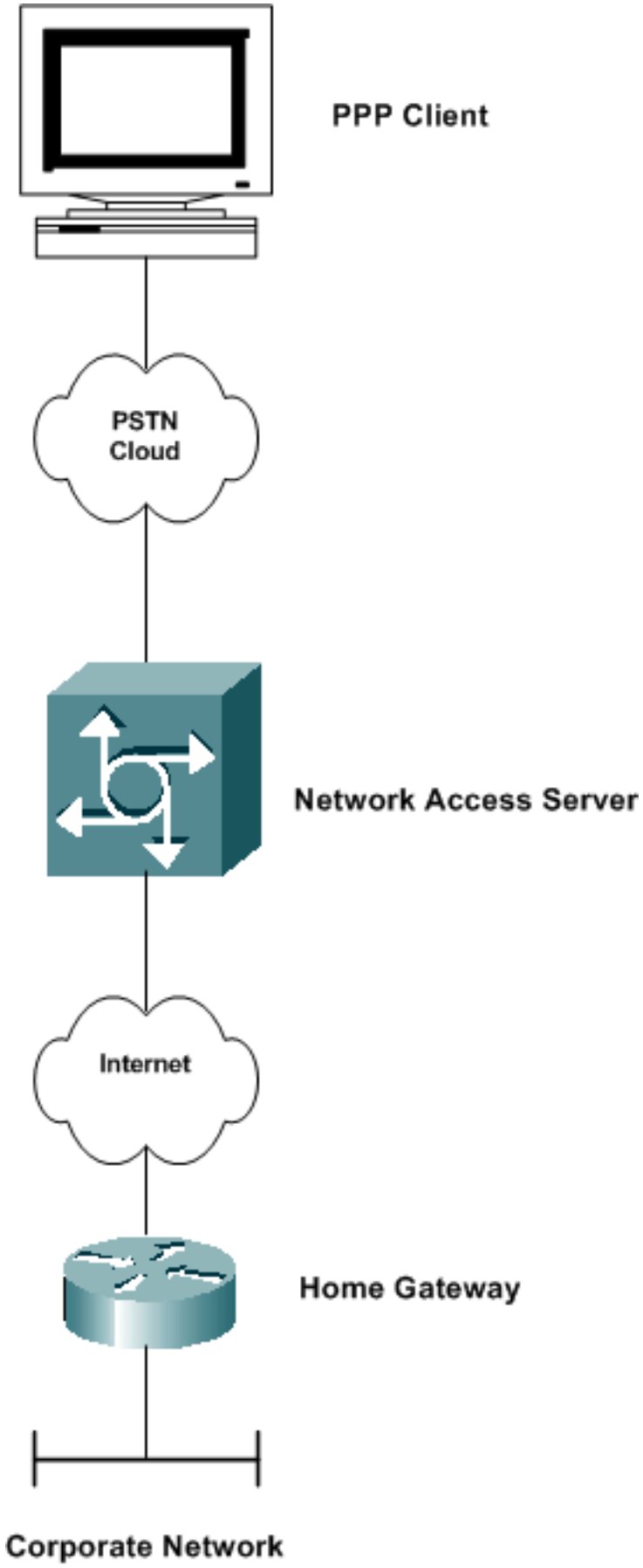
# VPDN y L2TP

## VPDN

El Virtual Private Dialup Network (VPDN) es un estándar de Cisco que permite que un servicio de marcado manual para red privada se expanda hacia servidores de acceso remoto. En el contexto de VPDN, el servidor de acceso (por ejemplo, un AS5300) al que se llama, generalmente se lo denomina Servidor de acceso a la red (NAS). El destino del usuario de marcado se denomina gateway de inicio (HGW).

El escenario básico es que un cliente de Point-to-Point Protocol (PPP) marca hacia un NAS local. El NAS determina que la sesión PPP se debe reenviar a un router de gateway de inicio para ese cliente. La HGW luego autentica al usuario y comienza la negociación PPP. Una vez finalizada la configuración de PPP, todas las tramas son enviadas a través de los NAS hacia el cliente y las gateways de inicio. Este método integra varios protocolos y conceptos.

Para obtener información sobre la configuración de VPDN, vea *Configuración de una Red de Marcado Privado Virtual* en Configuración de Funciones de Seguridad.




## L2TP

El Protocolo de tunelización de Capa 2 (L2TP) es un estándar IETF que incorpora los mejores atributos de PPTP y L2F. Los túneles L2TP se utilizan principalmente en modo obligatorio (es decir, NAS de marcado hacia HGW) para acceder a los VPN tanto para el tráfico IP como no IP.

Windows 2000 y Windows XP agregaron compatibilidad nativa con este protocolo como medio de conexión de cliente VPN.

L2TP se utiliza para tunelizar PPP a través de una red pública, como Internet, mediante IP. Dado que el túnel ocurre en la Capa 2, los protocolos de capa superior ignoran el túnel. Al igual que GRE, L2TP también puede encapsular cualquier protocolo de Capa 3. El puerto UDP 1701 se utiliza para enviar tráfico L2TP por el iniciador del túnel.

**Nota:** En 1996, Cisco creó un protocolo de reenvío de capa 2 (L2F) para permitir que se produjeran conexiones VPDN. L2F todavía es compatible con otras funciones pero ha sido reemplazado por L2TP. El protocolo de tunelización punto a punto (PPTP) también se creó en 1996 basado en un borrador de Internet de IETF. PPTP proporcionó una función similar al protocolo de túnel similar a GRE para conexiones PPP.

Para obtener más información sobre L2TP, vea Layer 2 Tunnel Protocol.

## PPPoE

PPP over Ethernet (PPPoE) es un RFC informativo que se implementa principalmente en entornos de línea de suscriptor digital (DSL). PPPoE aprovecha las infraestructuras Ethernet para permitir a los usuarios iniciar sesiones PPP múltiples dentro de la misma LAN. Esta tecnología permite la selección del servicio de capa 3, una aplicación emergente que permite a los usuarios conectarse simultáneamente a varios destinos a través de una sola conexión de acceso remoto. PPPoE con protocolo de autenticación de contraseña (PAP) o protocolo de autenticación por desafío mutuo (CHAP) se utiliza a menudo para informar al sitio central qué routers remotos están conectados a él.

PPPoE se utiliza principalmente en implementaciones de DSL de proveedores de servicios y topologías Ethernet puenteadas.

Para obtener más información sobre la configuración de PPPoE, vea Configuración de PPPoE sobre Ethernet y VLAN IEEE 802.1Q.

## MPLS VPN

El Multiprotocol Label Switching (MPLS) es una nueva norma IETF basada en Cisco Tag Switching que permite el aprovisionamiento automatizado, un desarrollo rápido y características de escalabilidad que los proveedores necesitan para suministrar acceso a la intranet y servicios de extranet VPN económicos. Cisco colabora estrechamente con los proveedores de servicios para garantizar una transición fluida a los servicios VPN con MPLS. MPLS funciona sobre un paradigma basado en etiquetas y etiqueta paquetes a medida que ingresan a la red del proveedor, a fin de acelerar el reenvío a través de un núcleo IP sin conexión. MPLS utiliza los diferenciadores de rutas para identificar la pertenencia a VPN y contener el tráfico dentro de una comunidad VPN.

MPLS también añade las ventajas de un enfoque orientado a la conexión al paradigma de ruteo IP, a través del establecimiento de trayectorias conmutadas por etiquetas, que se crean en función de la información de topología en lugar del flujo de tráfico. MPLS VPN se implementa ampliamente en el entorno de proveedor de servicios.

Para obtener información sobre la configuración de MPLS VPN, vea Configuración de una MPLS

VPN Básica.

## Información Relacionada

- Página de soporte de IPSec
- Cómo funcionan las redes privadas virtuales
- Página de Soporte de NAT
- Página de soporte de GRE
- Página de soporte de VPDN
- Página de soporte de PPTP
- Página de soporte de PPPoE
- Soporte Técnico - Cisco Systems