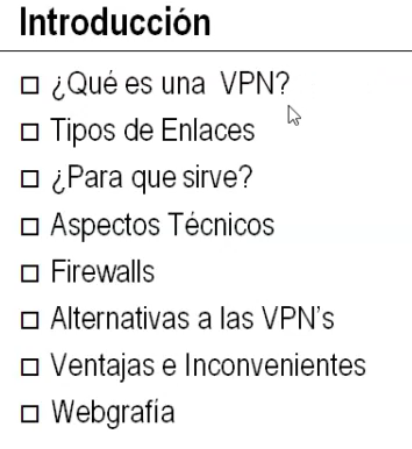
**VPN**





**📖 Apunte: Redes VPN**

**1. ¿Qué es una VPN?**

* **Primer punto importante.** Una **VPN (Virtual Private Network)** se utiliza para **conectar dos redes inseguras** (generalmente a través de Internet) de forma **segura**.
* La VPN crea un **algoritmo de encriptación de extremo a extremo** que protege la información tanto (túnel virtual):
  + **En reposo (estática)**: cuando está almacenada.
  + **En tránsito (dinámica)**: cuando circula por la red.
* Se habla de que una VPN **genera un “túnel virtual” en una red pública** (ej.: GRE, PPTP, etc.)., es decir **canal cifrado dentro de Internet**.
  + Este túnel permite que, **independientemente de la ubicación física**, se pueda acceder a los recursos de una red privada.
  + En condiciones normales de red, para conectarse es necesario estar físicamente cerca de un switch; la VPN elimina esa limitación.

**VPN en redes públicas y privadas**

* Se suele mencionar que las VPN se utilizan en redes públicas, pero **también pueden armarse dentro de una LAN** (VPN interna).
* Esto tiene sentido porque la **NIST** recomienda la **segmentación de redes**, por ejemplo:
  + Que cada departamento de una empresa tenga su propia red interna.
* Recordar: para que dos hosts se comuniquen **sin un tercero** deben estar en la **misma red**.
* Si se segmenta, dejan de estar en la misma red → en lugar de que cada red tenga su propio servidor, se las conecta a **un único servidor** a través de la VPN.

**Segmentación de redes**

Existen dos formas principales:

**a) Segmentación física**

* Requiere equipamiento adicional: switches, fibra óptica, media converters, etc.
* **Desventaja:** costos muy altos.
* Ejemplo: si la sala de producción está a 4 km del Data Center, habría que:
  + Instalar un switch en el Data Center.
  + Tender fibra hasta la sala de producción.
  + Colocar otro switch y un media converter para pasar a cobre.
  + Y repetir el esquema por cada red adicional.

**b) Segmentación virtual/Lógica**

**b.1. Segmentación Lógica I: Subredes (Capa 3) 🔢**

Una **Subred** (*Subnet*) es una división **lógica** de una red IP más grande, definida por la **dirección IP** y la **Máscara de Subred**.

* **Función:** Divide el espacio de direcciones IP en grupos más pequeños.
* **Comunicación:** Dos dispositivos en la **misma subred** se comunican **directamente** (Capa 2). Dos dispositivos en **subredes diferentes** necesitan un **Router** (Capa 3) para comunicarse.
* **Ventaja:** Reduce el tamaño de los dominios de broadcast (tráfico innecesario) y facilita el enrutamiento.

**b.2. Segmentación Lógica II: VLANs (Capa 2) 💻**

Una **VLAN** (*Virtual LAN*) es una división **lógica de un switch físico** o de un grupo de switches.

* **Función:** Aísla el tráfico de Capa 2 (tráfico de difusión o *broadcast*) dentro de un único dominio lógico, sin importar a qué puerto físico del switch esté conectado el dispositivo.
* **Mecanismo:** Usa etiquetas (tags **802.1Q**) en los paquetes para identificar a qué red virtual pertenece el tráfico.
* **Relación Clave con Subredes:** La **mejor práctica** en diseño de redes es tener una relación **uno a uno** entre una **VLAN** y una **Subred** (1:1).

**❌ Importante:** Asignar **varias VLANs** a una **sola subred IP** rompe el protocolo ARP, impide la comunicación directa de Capa 2 y es una mala práctica.

**b.3. Conexión Lógica III: VPN (Túnel Cifrado) 🛡️**

Una **VPN** (*Red Privada Virtual*) es una tecnología que crea un **túnel cifrado y seguro** a través de una red pública (Internet) para extender lógicamente una red privada.

**Tipos de VPN y su Relación con Subredes:**

| Tipo de VPN | Propósito | Subredes Involucradas | Función en la Subred |
| --- | --- | --- | --- |
| **Acceso Remoto** | Conectar un usuario individual a la red central. | **Una** (la del usuario) y **Otra** (la de la empresa). | Asigna al usuario una IP de la subred de la empresa, integrándolo **lógicamente** como un host local. |
| **Sitio a Sitio** | Conectar dos redes (sucursales) geográficamente separadas. | **Dos o más subredes** (las de cada sucursal). | Une las redes. El router/firewall de cada lado enruta el tráfico entre las subredes a través del túnel. |

* **Implementación de Sitio a Sitio:** Requiere **dos dispositivos VPN** (routers/firewalls), uno en cada extremo del túnel, para cifrar y descifrar el tráfico entre las subredes.

⚠️ **Conclusión:** no siempre es necesario armar las VPN desde el ISP hacia afuera; también pueden implementarse dentro de la red interna.

**Segundo punto importante:**

* Una VPN **proporciona un túnel IP encriptado y/o encapsulado** a través de Internet.
* Sin embargo, este concepto es **relativo** y debe analizarse según el caso (ejemplo: no siempre aplica exactamente igual en todos los escenarios).

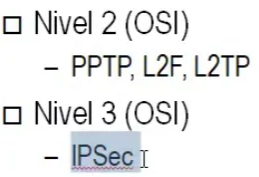
**VPN vs VLAN**

* **VPN** = cómo accedo a una red **desde afuera**.
* **VLAN** = cómo organizo la red **desde adentro**.
* La **tecnología es distinta**, pero el **concepto de segmentación** es similar.

**Diferencias clave:**

* **VPN** → servicio que crea túneles seguros.
* **VLAN** → funciona como una **subred lógica** dentro de un switch.

La tecnología es distinta el concepto el mismo.  
La diferencia entre una VLAN (capa 2) y una VPN (Capa 3) es la siguiente:



**Seguridad:**

* Protocolos iniciales como PPTP, L2F y L2TP **no son seguros por sí solos** → requieren **IPSec** u otros mecanismos de cifrado.

**Ejemplos de uso de VPN dentro de una LAN**

Creo una VPN dentro de una LAN cuando:

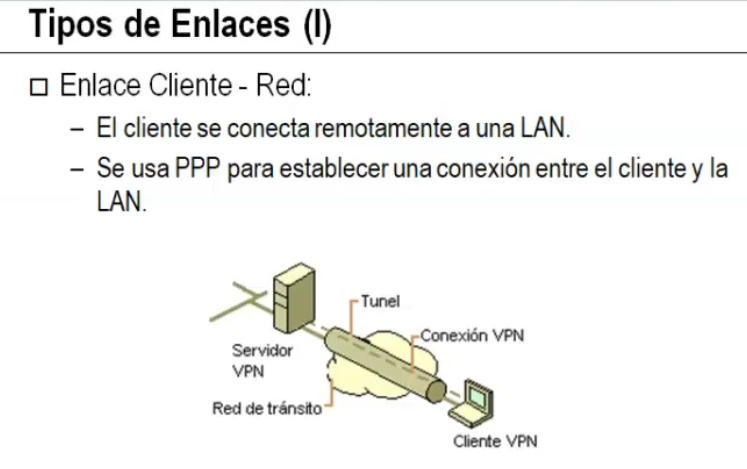
* Dos LAN que están separadas.

Pensamos que la LAN es interna, pero si puedo mostrarla, lo hago a través de una VPN.

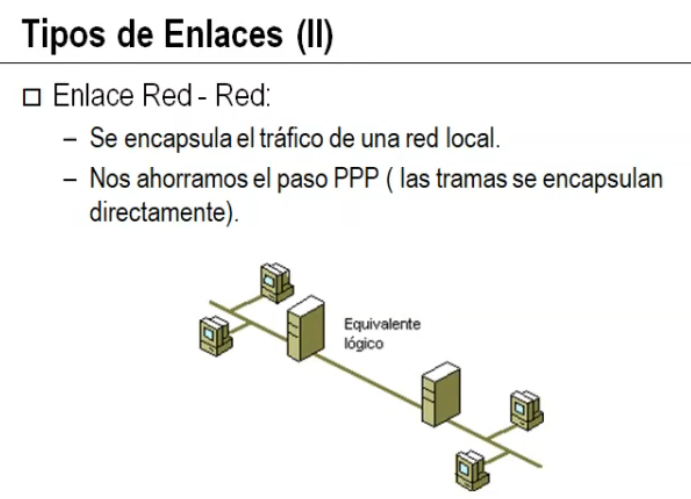
Los primeros protocolos no eran seguros. Hoy en día armas OTRA red, por ej red\_clientes y a esa RED le conecto todos los servicios que quiero mostrar y armo una VPN para cada red. Cada red va a tener sus servicios.

Entonces una VPN dentro de una red local LAN, tiene 2 conexiones:

1. **Conexión LAN a LAN**
   * Dos redes locales separadas que se interconectan a través de Internet.
   * Pero es una única red.
2. **VPN de acceso remoto**
   * Un usuario se conecta desde cualquier lugar a la LAN de la empresa.
   * ⚠️ Riesgo: no debería conectarse directo a la LAN interna → se recomienda hacerlo “aguas arriba” en la **DMZ** para mayor seguridad.



Las primeras VPN no tenían ni autenticación ni cifrado de datos, las actuales lo hacen en tiempo real y usan como seguridad el IPSec.



Necesito un GATEWAY DE VPN. Puede ser un firewall, router, switch capa 3, necesito que tenga capacidad de ruteo.

**Protocolos relacionados con VPN y sus capas**

**PPP (Point-to-Point Protocol)**

* 📍 **Capa OSI**: **Capa 2 – Enlace de datos**
* Usado para enlaces punto a punto (módems, serial, etc.).
* Transporta distintos protocolos de red sobre un enlace físico.
* Autenticación básica (PAP, CHAP), sin cifrado fuerte.
* **Base** para el desarrollo de PPTP.

**PPTP (Point-to-Point Tunneling Protocol)**

* 📍 **Capa OSI**: trabaja sobre **Capa 2 (Enlace)** pero transporta tráfico de capa 3 encapsulado.
* Basado en PPP.
* Primer protocolo de túnel ampliamente usado en VPN.
* Cifrado muy débil, inseguro → obsoleto.

**L2F (Layer 2 Forwarding, de Cisco)**

* 📍 **Capa OSI**: **Capa 2 – Enlace de datos**
* Protocolo propietario de Cisco.
* Encapsula tráfico de capa 2 para crear túneles.
* No incluía cifrado → solo transportaba.

**L2TP (Layer 2 Tunneling Protocol)**

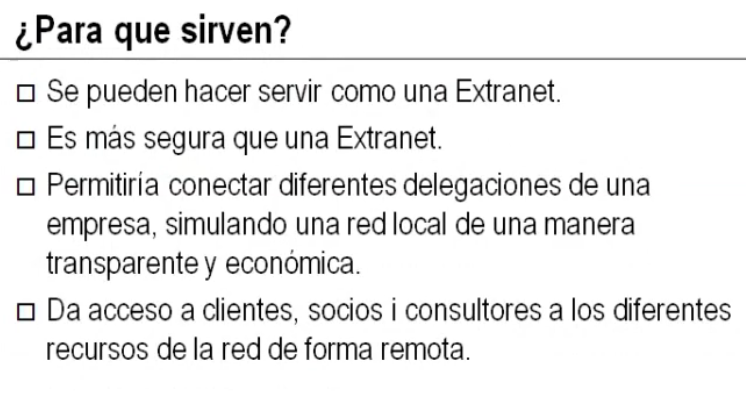
* 📍 **Capa OSI**: **Capa 2 – Enlace de datos**
* Combina PPTP + L2F.
* Estándar más abierto que permite tunelizar a nivel de enlace.
* Sin cifrado propio → siempre usado con IPSec (**L2TP/IPSec**).

**IPSec (Internet Protocol Security)**

* 📍 **Capa OSI**: **Capa 3 – Red**
* Protege directamente los paquetes IP (tanto datos como cabeceras).
* Ofrece:
  + Cifrado fuerte (AES, 3DES).
  + Autenticación robusta.
  + Integridad de datos.
* Es el estándar actual de seguridad en VPNs.

**Diferencia principal: la seguridad**

* **GRE**:
  + Solo encapsula.
  + No cifra ni autentica.
  + Ejemplo: sirve para pasar tráfico multicast, IPv6 sobre IPv4, etc.
  + Se suele usar en combinación con IPSec.
* **PPTP, L2TP, L2F** (capa 2):
  + También encapsulan.
  + Algunos con cifrado débil (PPTP) o sin cifrado (L2F, L2TP).
  + Necesitan ayuda extra (L2TP + IPSec).
* **IPSec (capa 3):**
  + Encapsula y además cifra, autentica e integra.
  + Es el más completo y seguro.



1ra y 2da es para uso externo (acceso remoto), 3ra y 4ta es conexión interna (conexión de redes privadas). En la 4ta hay que tener cuidado ya que es importante no darle acceso a la red local a cualquiera 🡪 Primer concepto de seguridad es negar todo.

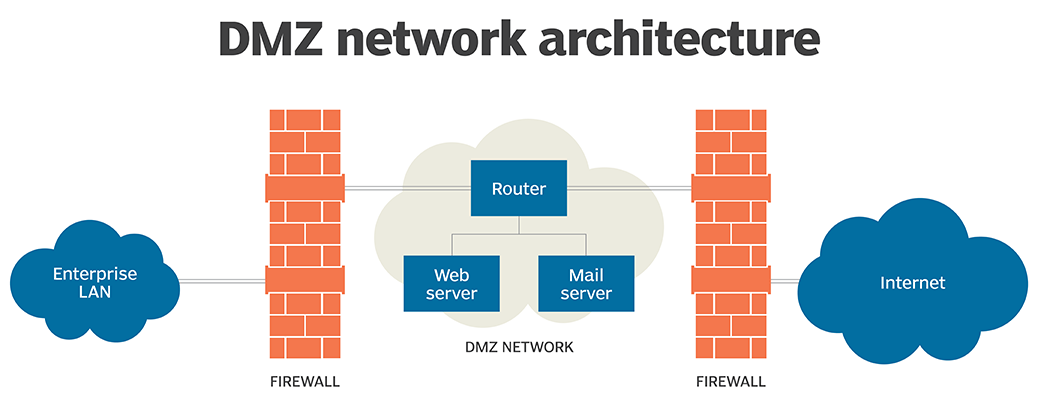
Con respecto al 4to punto entonces:

Las **VPN** permiten que usuarios externos se conecten a la red de la empresa como si estuvieran físicamente dentro de ella. El gran problema aparece cuando esa conexión se hace de manera directa hacia la **LAN interna**: en ese caso, cualquier usuario que ingrese por la VPN tendría el mismo nivel de acceso que un equipo dentro de la red corporativa. Esto es riesgoso, porque un error de configuración o unas credenciales comprometidas pueden abrirle la puerta a atacantes hacia toda la infraestructura.

Por este motivo, el primer principio de seguridad que se aplica es el de **“negar todo por defecto”**. En otras palabras, cuando se configura una VPN no se debe permitir acceso completo a toda la LAN, sino únicamente a los servicios o servidores estrictamente necesarios. Por ejemplo, un consultor externo que entra a la red debería poder ver solo un servidor de reportes, pero nunca tener visibilidad de todas las computadoras de la oficina.

La solución más segura es que el tráfico de VPN no llegue directo a la red interna, sino que termine en una **DMZ (zona desmilitarizada)**. La DMZ es una red intermedia entre Internet y la LAN privada, diseñada justamente para alojar servidores que necesitan estar expuestos hacia afuera, como el servidor VPN o un servidor web. De esa manera, si ocurre un ataque desde Internet, este impacta primero en la DMZ y no en la red interna. El firewall que separa la DMZ de la LAN se encarga de filtrar y permitir únicamente el tráfico autorizado.

Respecto a los ataques de **denegación de servicio (DDoS)**, lo que el profesor explicó es que no es posible ejecutar un DDoS “a través de un túnel VPN”. Esto se debe a que el túnel requiere autenticación y cifrado: si un atacante no tiene credenciales válidas, no puede enviar tráfico masivo dentro de la VPN para saturar la LAN. Lo que sí puede suceder es que intenten un DDoS contra el propio servidor VPN ubicado en la DMZ, ya que este es el punto que está públicamente expuesto en Internet.

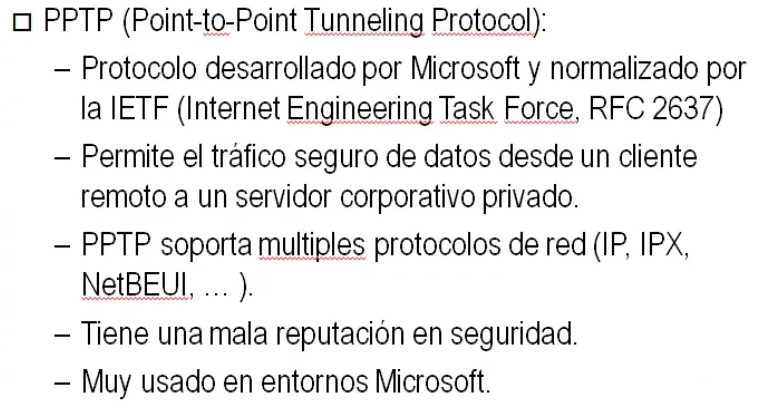


En conclusión, las VPN son una herramienta fundamental para el acceso remoto, pero deben configurarse con cautela. No se debe otorgar acceso directo a la LAN, sino canalizar las conexiones a través de una DMZ, aplicar el principio de “negar todo” y habilitar solo lo necesario. Así, se logra un equilibrio entre conectividad para usuarios externos y protección de la red interna frente a amenazas.

**VPN usa Protocolos de tunelización de Red**

**Aspectos Técnicos**

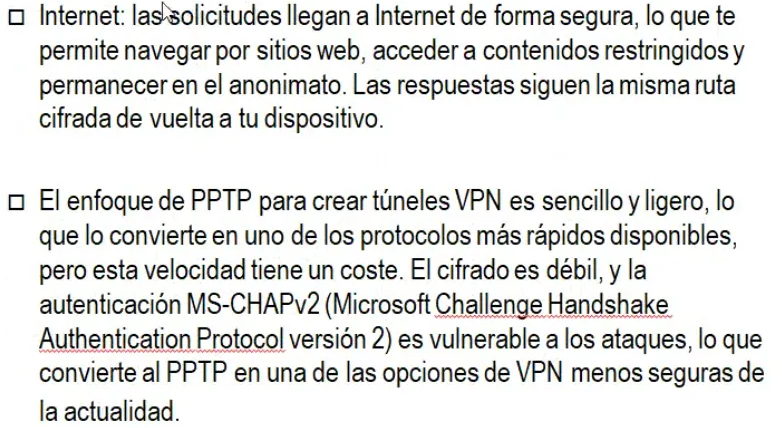
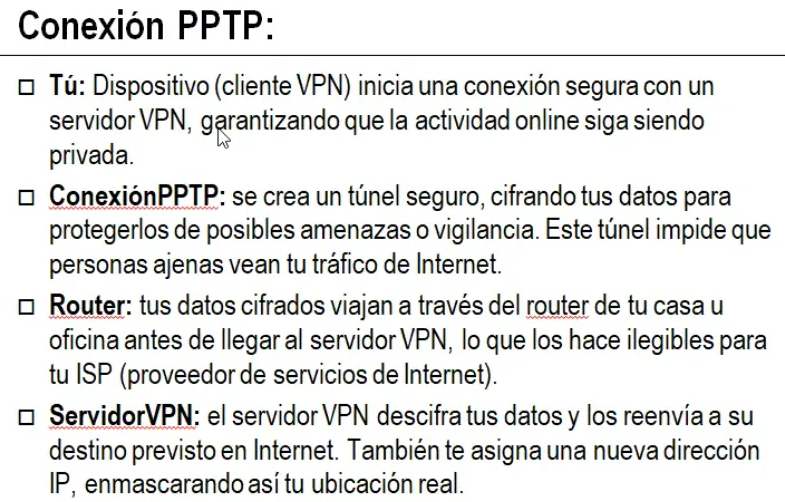
****

*****el PPTP soporta IP y permite: trafico seguro desde un cliente remotoa un servidor privado. La seguridad es malísima se usaba antes.*

****

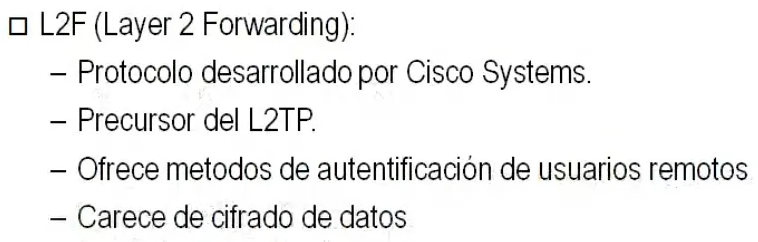
El **servidor VPN** siempre está en la **red de destino**, es decir:

* Puede estar en el **router/firewall de la empresa** (que maneja la segmentación).
* Puede estar en un **servidor dedicado** dentro de la red corporativa.
* O puede estar en un **servicio en la nube** (ejemplo: VPNs comerciales como NordVPN, ProtonVPN) cómo es el caso de la imagen.

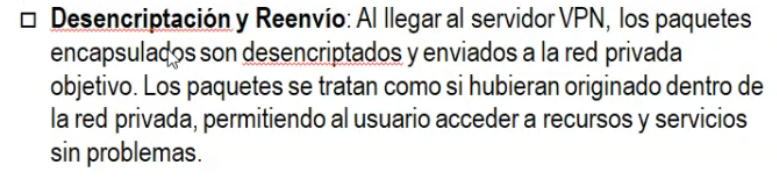
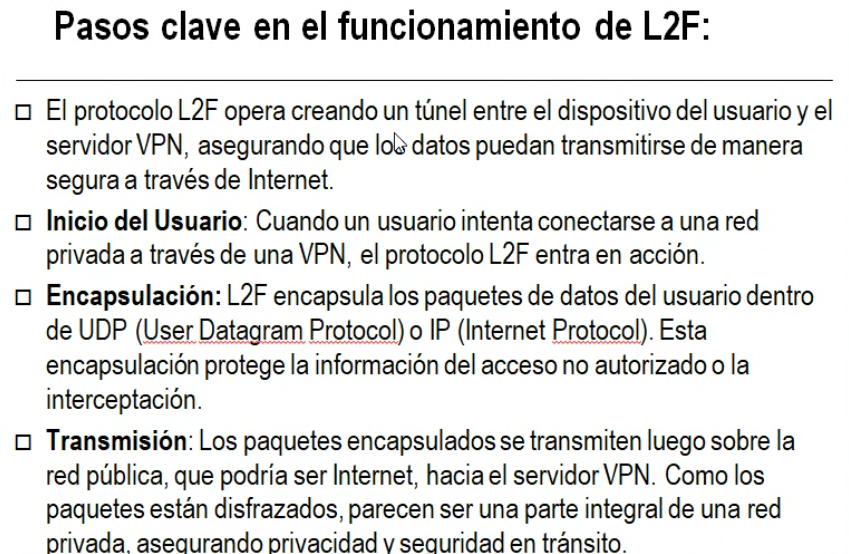
****

**El PPTP parece todo muy lindo por lo que se comenta anteriormente, es rápido y parece seguro, pero cuando hablamos de criptografía el cifrado es importante, y el que usa el PPTP es BASTANTE DÉBIL.**

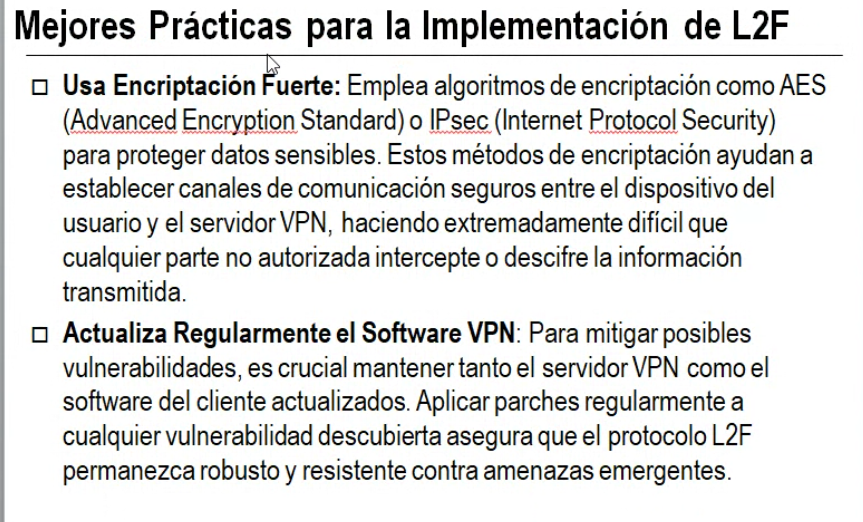
**Luego vino el:**

****

**No tiene cifrado de datos, por eso lo tengo que meter en un IPSec.**

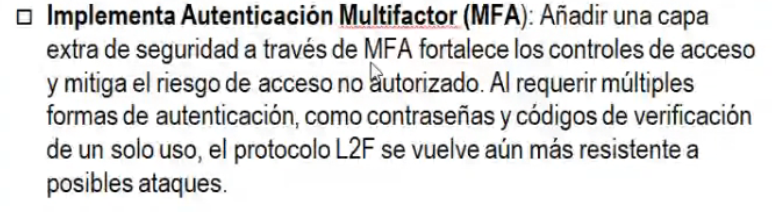
****

El usuario se conecta a la RED, agrega la cabecera el L2F, este encapsula los datos (capa 2) dentro de un UDP o un IP. Esta cabecera L2F va a proteger la información en caso de que alguien lo intercepte. Una vez encapsulado lo transmito en la capa física. Estos paquetes viajan encapsulados con L2F, por lo cual está protegido, me asegura seguridad y privacidad en tránsito. Cuando llega al servidor VPN lo desencapsula y lo desencripta.

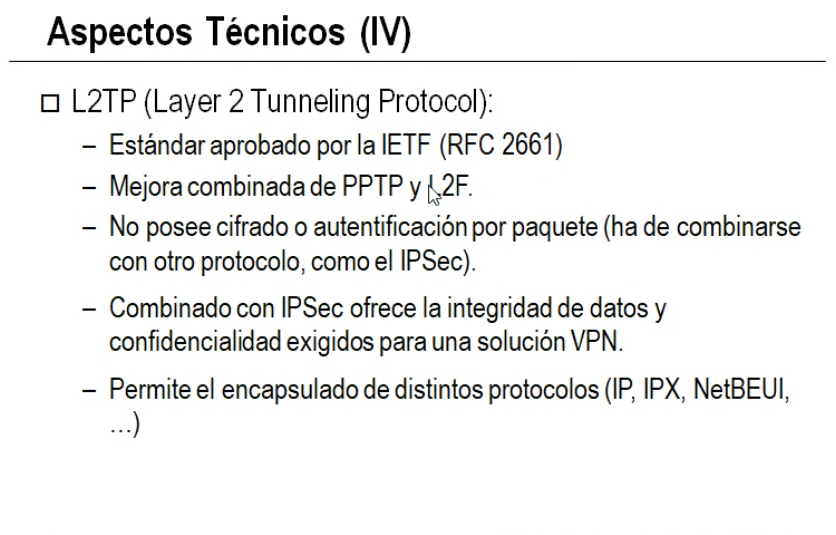


Si no uso un AES o un IPSec, el algoritmo de por sí no encripta. El AES es medio inseguro. El IPSec no, este si es MUY SEGURO.

Normalmente se usa un software de VPN, esto es un problema si el software de VPN no está actualizado con los parches de seguridad del protocolo.

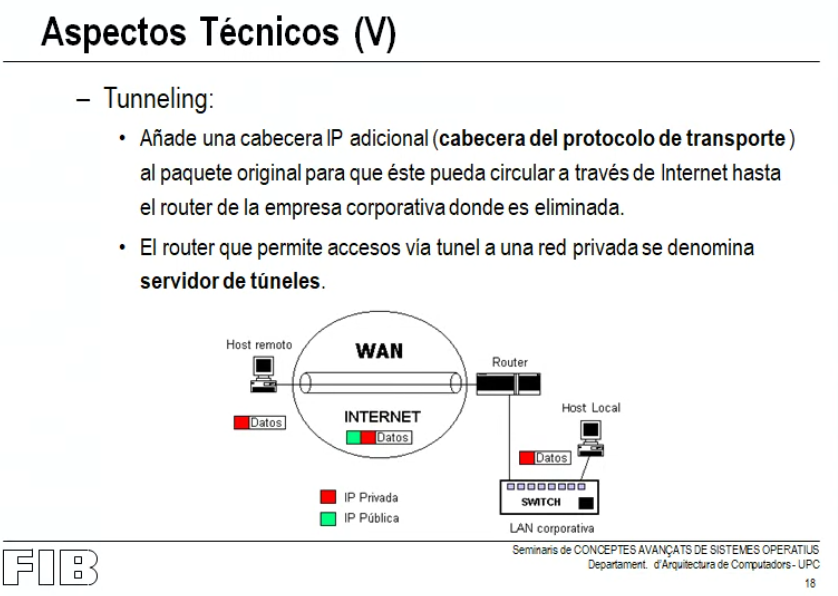


Siguiente:



Toma del PPTP la encapsulación

ASPECTOS DEL TUNNELING:



La idea de túnel que le profe quiere que nos llevemos es la siguiente: Se mete un paquete dentro de otro paquete para que se pueda transportar, hasta acá eso es encapsulamiento, pero al agregar una cabecera GRE al paquete viaja encapsulado de manera mas seguro en redes donde no tengo control.

GRE: Generic Routing Encapsulation. 🡪 Es un protocolo de encapsulamiento. Su función es **tomar un paquete original** (puede ser IP, IPv6, multicast, etc.) y **meterlo dentro de otro paquete IP** para transportarlo a través de la red. No ofrece **cifrado ni autenticación**, solo túnel. PERO al combinarlo con IPSec se utiliza como base de VPN, igual mejor usar alternativas más simples (como OpenVPN o WireGuard).

El protocolo GRE funciona de la misma manera, pero es mejor para explicar el concepto de tunneling.

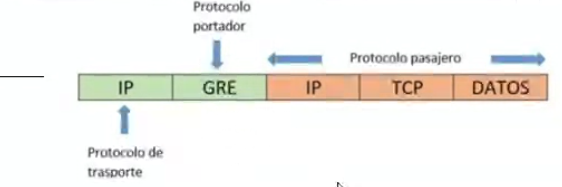
**GRE (Generic Routing Encapsulation)** fue desarrollado por Cisco y permite crear un **túnel de encapsulación**. La idea del túnel es meter un paquete dentro de otro para que pueda viajar a través de una red IP sin que se modifique el contenido original. GRE agrega una cabecera adicional y un nuevo encabezado IP externo, de modo que el paquete original se transporta encapsulado de extremo a extremo. Al llegar al destino, el router quita la cabecera GRE y entrega el paquete tal cual como salió del origen.

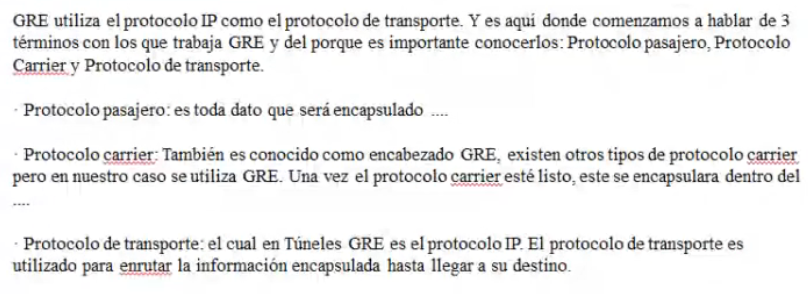
GRE, por sí mismo, no cifra ni autentica la información, por lo que no es seguro. Para usarlo como base de una VPN se suele combinar con **IPSec**, que le agrega la seguridad necesaria.

**GRE (Generic Routing Encapsulation)** es útil porque permite encapsular paquetes de red y transportarlos a través de infraestructuras que no controlo, como Internet o la red de un proveedor. De esta manera puedo enviar tráfico que normalmente no estaría soportado o que tendría restricciones. Por ejemplo, si mi empresa usa **IPv6** internamente pero mi proveedor solo soporta **IPv4**, con GRE puedo encapsular los paquetes IPv6 dentro de IPv4 para que viajen por la red del proveedor sin problema y, al llegar al destino, recuperar el tráfico original tal cual salió del origen.

**Proceso de Encapsulamiento**

**El proceso de GRE (Generic Routing Encapsulation)** consiste en tomar un paquete original (generalmente con direcciones privadas que no podrían circular por Internet), agregarle una cabecera GRE y una nueva cabecera IP externa con direcciones públicas de los routers que forman el túnel. De esta forma, el paquete viaja por Internet como si fuera tráfico IP común, y el ISP solo se encarga de transportarlo sin interpretar el contenido. Cuando llega al router destino, este elimina la cabecera externa y la GRE, recuperando el paquete original para entregarlo al host final.





Protocolos:

* Pasajero: Es todo lo que voy a encapsular → el paquete original que realmente te interesa.
* Portador (carrier): Es el encabezado GRE, es lo que encapsula y me permite agregarle la cabecera del túnel GRE que es otro protocolo IP.
* Transporte: El protocolo IP → IP externa (públicas de routers) → lleva el túnel por Internet.

Cuando usás GRE (o cualquier túnel), **tenés que ajustar el MTU de tus interfaces** para que el paquete más la cabecera GRE quepa dentro del límite físico (ej. 1500).

* Ejemplo: si GRE agrega 24 bytes extra, deberías configurar el MTU de tu túnel en **1476 bytes** (1500 – 24).

**🔹 5. Ejemplo práctico**

Cuando un paquete viaja con GRE, el **destino externo** (IP pública de la cabecera externa) es **el router del otro extremo del túnel**.

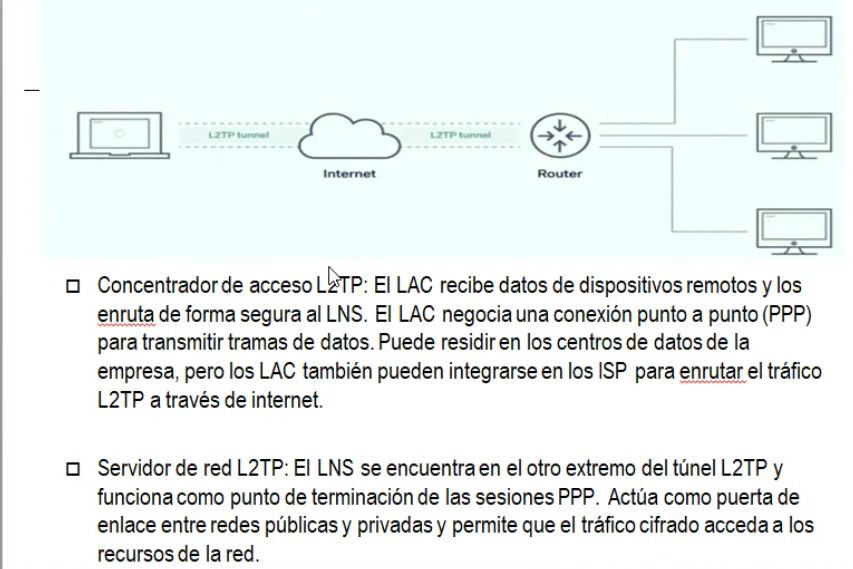
* Ese router “entiende” GRE, quita la cabecera externa + la GRE y recupera el paquete original.
* Luego lo reinyecta en su red interna y lo entrega al host final.

👉 O sea, **el receptor directo es el router destino** que tiene configurado el túnel GRE.

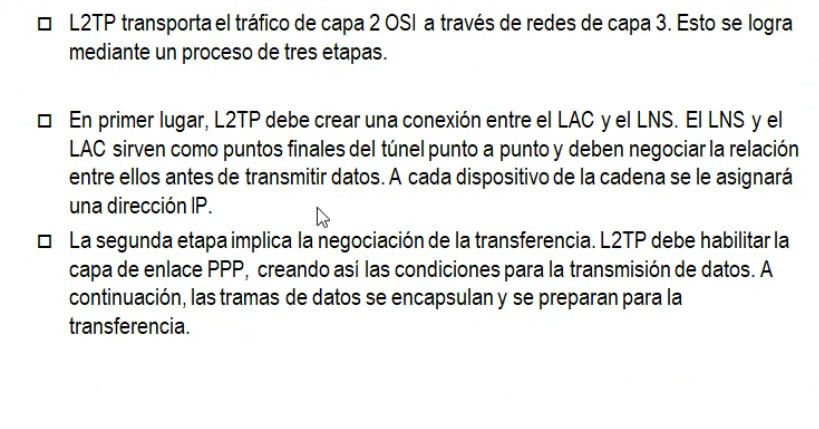
**Características fundamentales de GRE son:**

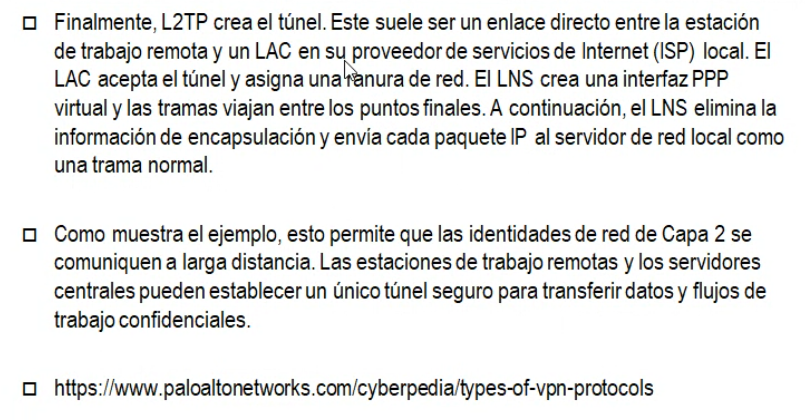
* Soporte para tráfico **multicast**.
* Soporte para tráfico **broadcast**. Si no lo hiciese no podría establecer la VPN.
* Es un protocolo no seguro: no ofrece encriptación, lo que significa que cualquier paquete que sea capturado, puede ser leído. El túnel de por si no viaja encriptado, lo tengo que pasar por un IPSec (este es unicast).
* Es un protocolo sin estado y no contiene ningún protocolo de control de flujo.

En conclusión: El GRE va de la mano del IPSec.



LAC: Nos sirve para recibir los datos de un dispositivo remoto y los enruta hacia el LNS, negocio la comunicación punto a punto hacia el LNS. El LNS es un servidor de red, esta en el otro extremo del túnel y termina la sesión del punto a punto, es el GATEWAY entre la red pública y la red privada.





Altenativa a la VPN, tenemos el acceso remoto.

PPTP → encapsula solo PPP, cifra pero con algoritmos inseguros → descartado hoy.

L2F → encapsula solo PPP, sin cifrado propio => se usa con IPSec → obsoleto hoy.

L2TP (PPTP+ L2F) → encapsula cualquier protocolo de capa 2, sin cifrado propio → se usa con IPSec.

IPSec → encapsula tráfico IP unicast y lo cifra → estándar actual, pero debe combinarse con algún protocolo anterior para soportar broadcast/multicast.

**Resumen claro**

* **Unicast solamente** → PPTP, L2F, IPSec.
* **Unicast + Broadcast + Multicast** → L2TP (por trabajar en capa 2).
* GRE es un protocolo de túnel en capa 3 que permite encapsular unicast, broadcast y multicast (e incluso protocolos no IP). No cifra ni autentica, por eso suele combinarse con IPSec para agregar seguridad.

GRE 🡪 No usa Cifrado ni **autenticación**

|  |  |  |
| --- | --- | --- |
| **Concepto** | **Responde a** | **Rol** |
| VPN (Red Privada Virtual) | ¿Qué hace? | Es el objetivo o la función: crear una conexión privada, segura y lógica sobre una red pública. |
| Protocolos de VPN (IPSec, OpenVPN, etc.) | ¿Cómo lo hace? | Es el método o el mecanismo para establecer, mantener y asegurar ese túnel VPN (a través de encapsulamiento, cifrado y autenticación). |