DIAPOSITIVA1

El **L2TP (Layer 2 Tunneling Protocol)** es un protocolo de red estándar diseñado para soportar redes privadas virtuales (VPN) mediante la tunelización. Fue estandarizado por la IETF en el documento **RFC 2661** y surge históricamente como una solución híbrida que combina las mejores características de dos protocolos propietarios anteriores: el **PPTP** (Point-to-Point Tunneling Protocol) de Microsoft y el **L2F** (Layer 2 Forwarding) de Cisco.

La función técnica primordial de L2TP es permitir la extensión del **Protocolo Punto a Punto (PPP)** a través de una red pública de conmutación de paquetes, como Internet. En un entorno tradicional, una conexión PPP se establece directamente a través de un cable físico o línea telefónica; L2TP rompe esta limitación física encapsulando las tramas PPP (Capa 2) dentro de paquetes IP (Capa 3), permitiendo que un usuario remoto interactúe con el servidor de la red corporativa exactamente igual que si estuviera conectado localmente a la infraestructura física de la empresa.

Para el transporte de datos, L2TP utiliza el protocolo **UDP** (User Datagram Protocol) específicamente en el **puerto 1701**, tanto para el establecimiento del túnel como para la transmisión de datos. Se elige UDP sobre TCP para minimizar la sobrecarga (overhead) y evitar los problemas de retransmisión que causarían latencia innecesaria en un túnel en tiempo real.

Es crucial distinguir que, desde un punto de vista de ingeniería de seguridad, L2TP es un **protocolo de tunelización** y no un protocolo de encriptación. Por sí mismo, L2TP solo proporciona el "tubo" virtual y la autenticación de los extremos del túnel, pero **no cifra** el contenido de los datos que viajan por él (payload). Por esta razón, el tráfico L2TP puro es legible si es interceptado. Esta característica de diseño es lo que diferencia a L2TP de soluciones de seguridad completas y explica por qué en implementaciones comerciales casi siempre se encapsula dentro de IPsec para garantizar la confidencialidad.

DIAPOSITIVA 2

Para comprender cómo L2TP logra extender una red local a través de Internet, es necesario analizar su arquitectura, la cual se basa en un modelo cliente-servidor especializado que divide la responsabilidad de la conexión en dos puntos físicos distintos: el **LAC** y el **LNS**. Esta separación es lo que permite que la capa de enlace (Capa 2) sea independiente de la ubicación física del usuario.

El primer componente es el **LAC (L2TP Access Concentrator)** o Concentrador de Acceso. Este dispositivo actúa como el punto de entrada al túnel. Generalmente, el LAC es un dispositivo del proveedor de servicios de internet (ISP) o, en escenarios modernos de VPN cliente-a-sitio, es el software cliente instalado en la propia computadora del usuario (como el cliente VPN de Windows). Su función técnica es encapsular las tramas PPP originales generadas por el usuario dentro de paquetes L2TP/UDP y enviarlas hacia la red destino. El LAC es el "iniciador" de la llamada.

El segundo componente es el **LNS (L2TP Network Server)** o Servidor de Red. Este equipo se encuentra físicamente en la red privada de destino (la oficina central o el datacenter). El LNS actúa como el punto de terminación lógico del túnel. Su trabajo es recibir los paquetes encapsulados, desencapsularlos para recuperar la trama PPP original y procesarla como si hubiera llegado por un cable directo a la red local. Desde la perspectiva de la red interna, el LNS es quien autentica al usuario final y le asigna una dirección IP corporativa.

Entre estos dos puntos (LAC y LNS) se establece una **Sesión L2TP** que viaja a través de una red de conmutación de paquetes (normalmente IP/Internet). Es fundamental entender que esta arquitectura permite la **independencia del medio**: aunque el usuario se conecte vía fibra óptica, 4G o Wi-Fi al LAC, para el LNS la conexión siempre parecerá una interfaz lógica PPP directa, ocultando completamente la complejidad de la red intermedia (Internet).

DIAPOSITIVA 3

Para entender cómo L2TP gestiona simultáneamente el control del túnel y la transmisión de datos del usuario, es necesario analizar la anatomía de su encabezado. L2TP define dos tipos de mensajes que viajan por el mismo puerto UDP 1701 pero que se comportan de manera muy diferente: los **Mensajes de Control** y los **Mensajes de Datos**.

La diferenciación entre ambos comienza en el primer bit del encabezado. El **Bit T (Type Bit)** determina la naturaleza del paquete: si el valor es `1`, se trata de un mensaje de control (utilizado para establecer, mantener o cerrar el túnel); si es `0`, es un mensaje de datos (que transporta el tráfico del usuario). Esta distinción es crítica porque el manejo de errores cambia radicalmente: los mensajes de control tienen un sistema de entrega fiable (si se pierden, se retransmiten), mientras que los mensajes de datos no son fiables (si se pierden, se descartan para mantener la velocidad, delegando la corrección a capas superiores como TCP).

Dentro del encabezado, dos campos son fundamentales para la multiplexación: el **Tunnel ID** y el **Session ID**.

- El **Tunnel ID** identifica la conexión global entre un LAC y un LNS específicos.
- El **Session ID** identifica la conexión particular de un usuario dentro de ese túnel. Gracias a esta estructura jerárquica, un solo túnel L2TP puede transportar el tráfico de cientos de usuarios distintos simultáneamente, separando los flujos de datos mediante sus Session IDs únicos.

Finalmente, para gestionar la fiabilidad del canal de control, el encabezado incluye los campos **Ns (Number Sequence)** y **Nr (Number Received)**. Estos contadores funcionan de manera similar a los números de secuencia de TCP: aseguran que las instrucciones de control lleguen en el orden correcto y permiten confirmar la recepción (ACK) de los mensajes críticos. Es importante notar que, para reducir la sobrecarga de procesamiento,

estos campos de secuencia suelen ser ignorados o puestos a cero en los mensajes de datos (donde el Bit T es 0).

DIAPOSITIVA 4

El establecimiento de una comunicación L2TP no es un evento instantáneo, sino un proceso de negociación estricto y secuencial. A diferencia de protocolos más simples, L2TP debe construir la infraestructura lógica en dos fases jerárquicas: primero debe establecerse el **Túnel de Control** (la carretera) y, solo después, puede establecerse la **Sesión individual** (el vehículo del usuario).

Fase 1: Establecimiento de la Conexión de Control Antes de procesar cualquier dato de usuario, el LAC y el LNS deben reconocerse y crear el túnel base. Esto se logra mediante un intercambio de tres mensajes clave:

1. **SCCRQ (Start-Control-Connection-Request):** El LAC envía este mensaje inicial solicitando la apertura del túnel y proponiendo parámetros de configuración.
2. **SCCRP (Start-Control-Connection-Reply):** Si el LNS acepta la conexión, responde con este mensaje, confirmando los parámetros aceptados.
3. **SCCN (Start-Control-Connection-Connected):** El LAC envía la confirmación final. En este punto, el túnel de control está activo y listo para gestionar llamadas.

Fase 2: Establecimiento de la Sesión (Incoming Call) Una vez que el túnel existe, se debe negociar la conexión para el usuario específico que está intentando acceder. Esto se denomina típicamente "Incoming Call" (Llamada Entrante) desde la perspectiva del LAC:

1. **ICRQ (Incoming-Call-Request):** El LAC informa al LNS que un usuario específico está solicitando acceso y envía los detalles de la llamada.
2. **ICRP (Incoming-Call-Reply):** El LNS responde asignando un ID de sesión único para ese usuario y reservando los recursos necesarios.
3. **ICCN (Incoming-Call-Connected):** El LAC confirma que la llamada ha sido aceptada.

Inmediatamente después del mensaje ICCN, el túnel cambia de estado y comienza a fluir el tráfico de datos (tramas PPP). Es crucial entender que, si se tienen 50 usuarios remotos, la Fase 1 ocurre solo una vez (un solo túnel), pero la Fase 2 se repite 50 veces (una sesión por cada usuario dentro del mismo túnel).

DIAPOSITIVA 5

Finalmente, para comprender por qué L2TP es un protocolo tan flexible y longevo, es necesario analizar cómo transporta la información de configuración dentro de los mensajes de control. A diferencia de protocolos rígidos donde cada bit tiene una posición fija e inamovible, L2TP utiliza una arquitectura modular basada en **AVPs (Pares Atributo-Valor)**.

Los mensajes de control que vimos en la diapositiva anterior (como SCCRQ o ICRQ) son en realidad "contenedores". Dentro de estos contenedores viaja una lista variable de AVPs. Cada AVP es un bloque de datos que define un parámetro específico de la conexión, como el nombre del host (`Host Name`), el fabricante del equipo (`Vendor Name`), el tipo de entramado (`Framing Type`) o el tamaño máximo de unidad de recepción (`Receive Window Size`). Esta estructura permite que el protocolo sea extensibles: si en el futuro se necesita agregar una nueva funcionalidad a L2TP, simplemente se define un nuevo tipo de AVP sin necesidad de reescribir todo el protocolo ni cambiar la estructura del encabezado principal.

Desde el punto de vista de la ingeniería del paquete, cada AVP tiene una estructura genérica que incluye un campo de **Longitud**, un **ID de Vendedor**, un **Tipo de Atributo** y el **Valor** del dato en sí.

Un mecanismo de seguridad crítico dentro de los AVPs es el **Bit M (Mandatory bit)**. Este bit define la importancia del atributo:

- Si el **Bit M está activo (1)**, el atributo es crítico. Si el equipo receptor (LNS o LAC) no reconoce este atributo o no sabe cómo procesarlo, **debe cerrar la conexión inmediatamente**. Esto evita configuraciones erróneas o inseguras.
- Si el **Bit M está inactivo (0)**, el atributo es opcional. Si el receptor no lo entiende, simplemente lo ignora y continúa con la conexión.

Gracias a este sistema de AVPs y al manejo inteligente del Bit M, L2TP garantiza la interoperabilidad entre diferentes fabricantes (Cisco, Microsoft, Juniper, MikroTik) y permite que dispositivos antiguos puedan comunicarse con dispositivos modernos, ignorando simplemente las características nuevas que no comprenden.

Texto explicativo para el gráfico:

"En este diagrama podemos ver el ciclo de vida completo de una conexión L2TP. Todo comienza a la izquierda con el **CPE** (el router del usuario), que inicia una sesión **PPP** (indicada por la flecha larga inferior) buscando conectarse a la red. Esta solicitud llega primero al **LAC** (Concentrador de Acceso), que actúa como la puerta de entrada; este dispositivo consulta al servidor **AAA** (los cilindros superiores) para validar las credenciales básicas. Una vez autorizado, el LAC encapsula la conexión y establece el **Túnel L2TP** (el tubo central) a través de la red pública. Los paquetes viajan protegidos hasta llegar al **LNS** (Servidor de Red) a la derecha, el cual retira el encapsulamiento, consulta nuevamente a su servidor **AAA** para la autorización final y entrega los datos a Internet o a la red privada, logrando que la conexión **PPP** lógica del usuario se mantenga intacta de extremo a extremo sin importar la distancia física."