TEMA 4 – VPN (Virtual Private Networks)

Objetivos

1. Conectividad con sitios remotos
2. Saber que es una Virtual Private Networks y como funciona

Importantes

- En general, las **tecnologías de acceso WAN** (red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física) son en **L1** (modems ADSL, ISDN, optical technologies) y **L2**.

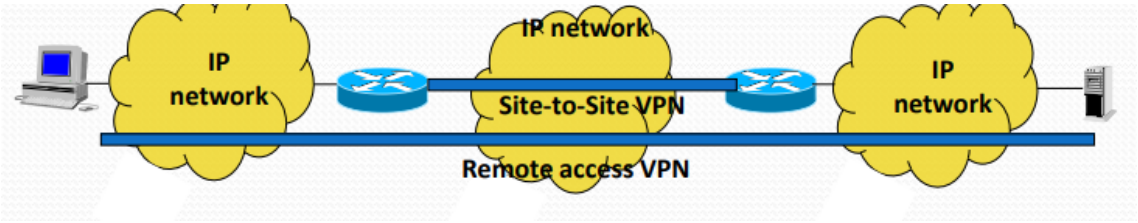
  ➔ Lo veremos como un **servicio ofrecido por el ISP**

- **Parámetros de tráfico** (puede preguntarlo):
  - **CIR** → Tasa de información comprometida (bits/s asociada a un servicio)
  - **EIR** → Tasa de información excesiva (bits/s en exceso respecto CIR)
  - **CBS** → Tamaño en bytes de la información transmitida.
  - **EBS** → Exceso de tamaño en bytes de la información transmitida.
- **Parámetros de calidad del servicio** o QOS (tenerlos en cuenta para un buen servicio y se pueden negociar con el ISP):
  - **Retardo de paquete** (packet delay) → Retardo en segundos de un paquete desde el momento que abandona el punto origen al momento que llega al punto destino.
  - **Jitter** → Variación de retardo de un paquete. Importante tenerlo en cuenta en aplicaciones de real-time. Se calcula como averageDelay-MinDelayOfPackets.
  - **Perdidas de paquetes** → 1-(Proporción de paquetes entregados/paquetes transmitidos). Importante para aplicaciones como VoiceIP (protocolo que sirve para que la voz viaje por Internet)
- Redes de acceso L1 y L2 (mirarlo del power, no sale en el examen)

VPN

- Red proporcionada por el ISP (L3) o por operadoras telecom (L2) que interconectan un sitio principal con sitios remotos o con end users.
- La conexión entre los dos puntos de las redes se hace usando técnicas de túnel que incluyen negocio Qos y seguridad entre otros.

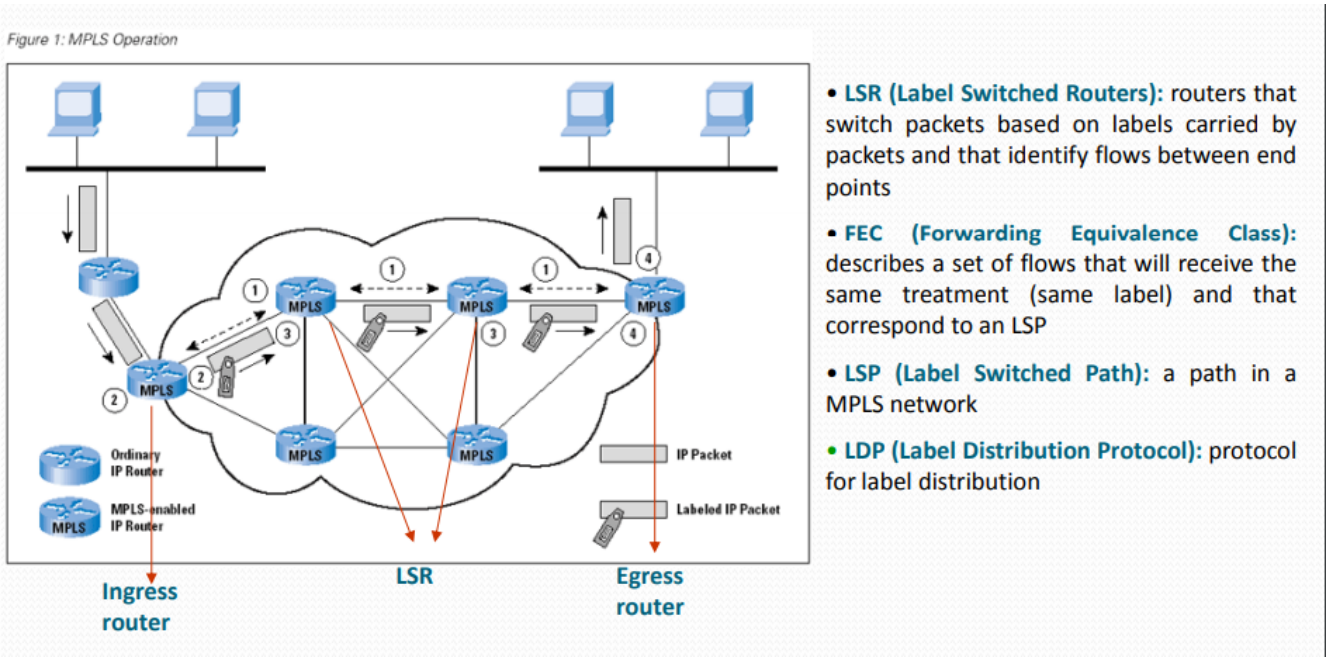
- Dos maneras de conectar el sitio principal con el remoto:



(Entre router y router / entre host y servidor)

- Túneles → Interface lógica que permite la encapsulación de paquetes en diferentes formatos (L4, L3 o L2). Tiene varias aplicaciones.
- **MPLS** (Multi-protocol label Switching, enrutamiento). Definido para permitir
    - **Qos** → Para garantizar cierta capacidad a los servicios de real-time y permitir retardo de paquete y control jitter.
    - **Servicios VPN** → Soporta segregación de paquetes en Internet usando BGP.
    - **Traffic Engineering** → Optimizar los recursos de red a partir de la demanda del usuario.
    - **Multi-Protocol support** → Independiente de la tecnología que sea.

Funcionamiento básico: (etiquetado de paquetes)



+ LSR → Cualquier router que realiza alguna operación MPLS

+ E-LSR → Cualquier router que se encuentra entre una red MPLS y red no MPLS.

+ Ingress-router → Es un E-LSR que recibe un paquete sin etiquetar y le inserta una.

+ Egress-router → Es un E-LSR que recibe el paquete etiquetado y se las quita todas.

- **LDP** (Label distribution protocol). Establece una comunicación bidireccional entre dos routers LSR para intercambiar información de etiquetado. Etiquetas: (32 bits de etiqueta)

  - Exp → 3-bit para definir QoS
  - S → 1-bit de flag (final de la stack o no)
  - TTL → 8-bit

  La etiqueta tiene un significado local, es decir, un enrutador que recibe un paquete etiquetado, lo verifica, le asigna uno nuevo y lo envía a la interfaz de salida.

  Paquetes con etiqueta diferente (pertenecen a un FEC diferente) reciben un **tratamiento diferente** en los routers.

- **MPLS + VPN** → Combina MPLS y BGP para crear una VPN IP (es decir, de L3). Nuevo:

  - **CE:** Customer Edge equipment
  - **PE:** Provider Edge equipment
  - **P/PC:** Provider (Core) router

  Tenemos las **direcciones VPN-IPv4.** Direcciones que identifican la VPN y están compuestas por un **Router distinguisher (RD, 8 bytes).** Ej. VPN 146:10.1.1.0 no es lo mismo que 37:10.1.1.0. → 8B(RD)+4B(@IP). Deben ser globalmente únicas. Pero, el RD también, es por eso que es necesario, diferentes tipos: (para que haya suficientes)

  - **Tipo 0**: El admin Fild debe contenter un ASN, asignado por el ISP. RD = 2B (Type Field) + 2B (Admin Field) + 4B (Assigned # Field)
  - **Tipo 1**: El admin Fild debe contenter una @IP, asignado por el ISP. RD= 2B (Type Field) + 4B (Admin Field) + 2B (Assigned # Field)
  - **Tipo2**: El admin Fild debe contenter un ASN de 4 octetos. RD= 2B (Type Field) + 4B (Admin Field) + 2B (Assigned # Field)

  Importante:

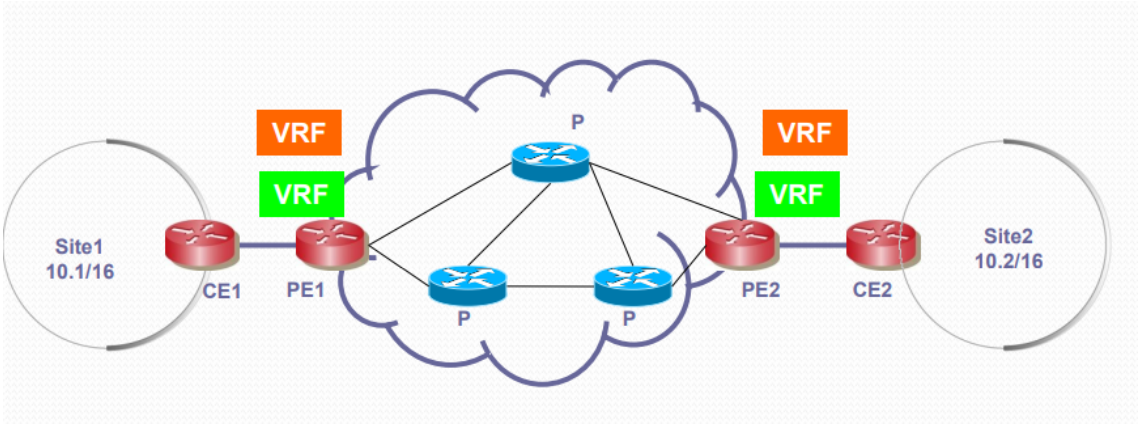
  - **CE** → Router que da acceso al proveedor. Usa E-BGP para anunciar/aprender rutas
  - **PE** → Router que actúa como punto de ingreso y egreso para las rutas de conmutación de etiquetas. Intercambia rutas via BGP con el CE. Mantiene una tabla (llamada **VRF,** define la relación VPN entre un sitio del cliente adjunto a un router PE) con cada uno de los sitios conectados. Para intercambiar la información de VRP con otros PE se usa **MBGP** que soporta @VPN-IPv4.
  - **P/PC** → Es cualquier router que no esta adjunto a un CE. Envía el trafico entre los routers PE. Solo necesita saber información de routing para alcanzar los routers PE.

¿Cómo se intercambian paquetes entre dos CEs?

Usando BGP para exportar rutas, usando Extended Communities (8 bytes) para flitrar y asociar tráfico BGP a un VRF y usando MPLS para dirigir el tráfico.

Ejemplo de funcionamiento (que puede salir)

+VRF naranja para nada xd, solo para diferenciar que puede haber más de una por router



Site 1 y Site 2 comparten el VRP verde.

CE1 anuncia la red 10.1/16 via E-BGP por PE1. PE1 añade la red a la VRF verde usando el identificador RD. PE1 determina que 10.1/16 se debe conectar al VRF verde mediante el puerto de recepción físico. PE1 exporta via I-BGP la ruta nueva (añade una etiqueta 353 como ejemplo, selecciona la @loopback IP como next-hop y asocia la ruta a la VRF verde usando comunidades!)

P2 seguidamente recibe la ruta de PE1 (y hace route filtering, es decir, si la ruta pertenece a una VRF conocida, gracias a la extended community). La acepta porque pertenece a la VRF verde (que comparten). Se usa MPLS para enviar el tráfico y para ello debe haber una ruta entre PE1 Y PE2 establecida. (Ej. 979 de etiqueta)

Label 959 → Se usa para el envío de paquetes en la MPLS network

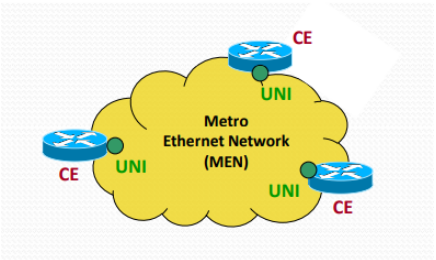
Label 353→ Se usa para identificar quien es el Remote Site (site1)

Luego, cuando un host de site2 quiere comunicarse con uno del site1, PE2 determina la VRP basándose en el puerto y busca en la VRF 10.1.1.1 (ejemplo de host en site1). Obteniendo, la etiqueta asociada al sitio remoto (353), el next-hop que es la @ de loopback de PE1 y la etiqueta asociada a MPLS para alcanzar PE1 (979).

- **Metro Ethernet**

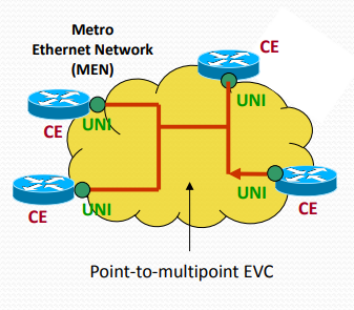
Ethernet en la red de área metropolitana. Son **switches interconectados y routers** con un ISP para transportar cualquier servicio usando VPN de banda ancha.

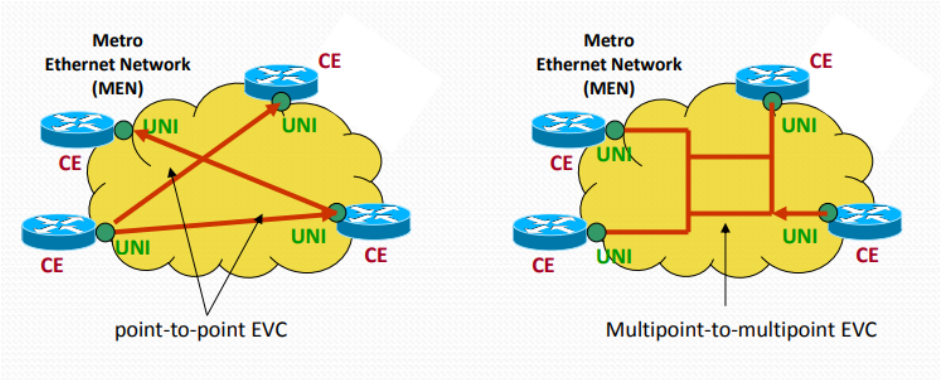
Cuando un ISP ofrece un servicio de Metro Ethernet, una o más entidades lógicas llamadas UNI situadas en el CE transportan tramas a través de un canal lógico llamado EVC hacia uno (punto a punto) o más (Punto a multipunto) UNIs destino. Esto en una red llamada MEN (Metro Ethernet Network).



Hay tres tipos de servicios:

- Ethernet Line (de punto a punto)
- Ethernet LAN (de multipunto a multipunto)
- Ethernet Tree (de punto a multipunto)





- **Servicio EtherLine**

  Puede operar con ambos anchos de banda, dedicado o conmutado y es una tecnología **de punto a punto**. Puede ser:

  - **EPL** (Ethernet Private Line) → Se puede ver como un EVC puro punto a punto donde admite un EVC único entre dos UNI. Dado que solo hay un EVC, el usuario no ve la etiqueta “VLAN”.
  - **EVPL** (Ethernet Virtual Line Privada) → Permite la multiplexación del servicio, por lo tanto, el punto a punto admite varios EVC entre dos UNI. Como hay varios EVC, el usuario tiene que etiquetar los paquetes con una etiqueta “VLAN” por EVC.

- **Servicio EtherLAN**

  Puede operar con ambos anchos de banda, dedicado o conmutado y es una tecnología **de multipunto a multipunto**. Puede ser:

  - **EPLAN** (Ethernet Private LAN) → Conectividad multipunto a multipunto entre dos o más UNIs. Cada UNI solo se adjunta a un EVC, si quiere otro EVC, debe activar otro UNI. No ven la etiqueta “VLAN”
  - **EVPLAN** (Ethernet Virtual LAN Privada) → Conectividad multipunto a multipunto entre dos o más UNI, con soporte de múltiples EVC, el usuario tiene que etiquetar paquetes con una "etiqueta VLAN" por EVC.