IRT: MPLS

1. Aspectos previos

Tipos de señales más comunes:

* De tiempo real (inelásticas)
  + Requiere red garantizada a nivel de paquete: Cotas para prob. pérdida, retardo máximo y jitter (voz, video interactivo…)
  + Representación analógica y digital
  + Continua en el tiempo
* De datos (elásticas)
  + Desea red garantizada a nivel de paquete: Cotas SOLO para prob. pérdida
  + Texto e imágenes
  + Representación digital
* Semi-elásticas
  + Para Streaming

Las redes multiservicio está basada en conmutación de paquetes.

SP (Servicio Portador): abstracción para describir un servicio de transporte de información. Se define entre 2 o más SAPs (Service Access Point) en los nodos extremos (Punto a Punto o Punto a Multipunto)

**SP – Conmutación de Circuitos**

* Reservan recursos para el uso exclusivo de cada comunicación (Protocolo de señalización especifico)
* Circuito es el conjunto de recursos
* Eficiente en señales continuas en el tiempo
* Garantías para pérdidas, retardo y jitter
* Ineficiente para transporte de datos

**SP – Conmutación de Paquetes**

* Pueden requerir o no el establecimiento previo de la conexión
* Recursos compartidos
* Eficiente en señales discontinuas
* Sin garantías
* Las redes modernas ofrecen SP mejorados

Multiplexación síncrona para redes TDM

Multiplexación asíncrona produce ganancia estadística

La agregación de tráfico crea señales con menor variabilidad. Se aprovecha en las redes multiservicio para ofrecer QoS.

**SP en Redes Multiservicio**

Se caracteriza por unos parámetros de tráfico y otros de QoS. La red solo puede garantizar la QoS de un SP cuando el tráfico que inyectan las aplicaciones en el SAP tiene un perfil temporal conocido en el tiempo de establecimiento.

Las aplicaciones que solicitan un SP deben declarar a la red los parámetros que definen el perfil temporal del tráfico que van a inyectar y los parámetros de QoS. La cantidad de recursos reservados van en función de estos parámetros.

Las redes multiservicio emplean conmutación de paquetes.

Permiten garantizar:

* Cota para probabilidad/tasa de pérdidas. Los paquetes con señales de tiempo real no se pueden retransmitir, por lo que hay que limitar sus pérdidas.
* Cota para el retardo máximo. Para comunicaciones interactivas
* Cota para jitter máximo. Limita la variabilidad del tiempo entre paquetes consecutivos en el receptor, evitando que el buffer del receptor se vacíe durante la reproducción.

**QoS**

Garantias para limitar el retardo y las pérdidas de paquete. Algunas aplicaciones requieren cotas específicas. El flujo de paquete designa un conjunto de paquetes que deben ser tratados de forma similar por la red. Una sesión es un conjunto de paquetes con la misma IP y puerto origen/destino y con el mismo protocolo.

Aproximaciones de QoS:

* Relativa. Los paquetes de una clase se tratan diferente a los de otra
* Absoluta. Define objetivos de QoS que deben cumplirse

El internet convencional solo ofrece servicios *best-effort* (*connectionless service* sin garantías de ningún tipo sobre los paquetes de red)

La necesidad de implementar QoS pueden deberse a restricciones de los seres humanos o a necesidades de negocio. Los ISP ofrecen QoS a sus clientes como forma de aumentar sus ganancias.

El SLA es un contrato entre cliente y el ISP que recoge los parámetros de mérito que definen la QoS del servicio y sus objetivos.

También puede incorporar otros contenidos menos técnicos como la política de tarificación

La red QoS se asegura mediante la reserva de recursos de red: ancho de banda en enlaces, y espacio en las colas de los routers (necesario protocolo de señalización).

Una forma aceptada de describir un perfil de tráfico es a través de un *token bucket* (TB)

* r: Tasa media (B/s)
* b: Long máxima (B)
* p: Tasa de pico (B/s)
* M: Tamaño máx. de paquete (B)
* m: Tamaño mín. de paquete (B)

Para establecer un SP, los terminales comunican a la red los parámetros de tráfico (traffic profile) <r,b,p,m,M>, y los de QoS. Cada router calcula la cantidad de ancho de banda y memoria que desea reservar. Cada router debe llevar una cuenta de los recursos reservados. Si algún router no tiene más recursos la conexión falla.

Token Bucket Conservador: Los paquetes se transmiten por el enlace a una tasa máxima de p (B/s). En general r < p.

Durante un tiempo T, se transmiten como máximo M+pT B

Localización de los TB, pueden estar localizados en distintos puntos de la red.

* En los terminales, o a la salida de la red del cliente. Conformación de tráfico para garantizar SLA
* Entrada y salida del trafico de cliente en la red del ISP, o entre redes de distintos ISP. Para asegurar que el trafico inyectado cumple el SLA. El trafico excedente puede suponer un peligro para el cumplimiento del SLA con otros clientes. Los paquetes que no cumplen pueden ser descartados en la red o marcados con una prioridad de descarte alta.
* TSpec es el conjunto de parámetros que forman el *Token Bucket*
* RSpec está formado por el TSpec y los objetivos del QoS solicitados

**Routing Mechanisms**

Aunque el encaminamiento es independiente del QoS, coordinando ambas funciones se consigue mejorar las prestaciones de la red y utilizar los recursos de forma más eficiente.

*Traffic Engineering*

La aparición de episodios de congestión se debe a que los recursos demandados superan los recursos de red o debido a un reparto inadecuado del tráfico en la red. La primera se soluciona aumentando los recursos y la segunda aplicando estrategias de TE que permitan repartir y balancear la carga por los enlaces.

*Constraint-based Routing*

El encaminamiento convencional se basa en seleccionar la ruta más corta. Con CbR, las decisiones de encaminamiento se toman en base a múltiples restricciones (número de saltos, ancho de banda libre en enlaces, requerimientos del flow…). Mejora el uso de los recursos pero es más complejo y puede dar lugar a inestabilidad en las rutas.

*Multiprotocol Label Switching*

Es una alternativa al encaminamiento del tipo datagrama. En MPLS el encaminamiento se basa en circuitos virtuales y se pueden definir rutas explicitas. La cabecera de los paquetes MPLS incorpora el campo *class of service,* que permite definir prioridades para los paquetes

**Circuito Virtual vs Datagrama**

CV están orientadas a la conexión. Se establece una conexión antes de transferir información

Datagrama NO está orientada a la conexión. Los terminales NO establecen una conexión, si no que pueden transferir la información inmediatamente.

Un CV consiste en:

* Una ruta entre terminales extremos
* Identificadores de CV (ICV). Diferentes en cada enlace de ruta
* Entradas en las tablas de encaminamiento

La cabecera contiene un ICV que cambia en cada enlace:

* El nuevo ICV se obtiene en cada tabla de encaminamiento y se configura al establecer la conexión.
* Las entradas de la TE se borran al terminar la conexión
* Los ICV libres podrán ser reutilizados por conexiones futuras
* Ventajas del uso ICV diferentes por enlace para una misma conexión
  + Reduce la longitud de lCV
  + Recude la carga de señalización para acordar el ICV entre conmutadores. La selección de lCV se hace de forma independiente en cada conmutador

Fases del CV:

* Establecimiento del CV
  + Mediante señalización se intercambian las etiquetas
  + La red decide la ruta más apropiada
  + Cada conmutador decide su ICV
  + Se añaden las entradas en las tablas de encaminamiento
* Transferencia de información
* Liberación del CV
  + Mediante señalización se informa de que la conexión va a finalizar.
  + Se liberan los enlaces.

Datagrama

Cuando un host requiere transmitir un paquete, le añade la dirección del receptor y lo envía. Los conmutadores intermedios encaminan paquetes en base a la dirección. Los conmutadores NO mantienen información de estado para cada sesión.

Las redes basadas en CV se inspiraron en las redes telefónicas. Internet fue la primera red basada en datagrama.

**Direccionamiento IP**

* Concepto de subred
  + La red enmarcada forma una subred
  + En IP se asigna una dirección a esta subred 223.1.1.0/24
  + La parte /24 es la máscara de subred.
* CIDR
  + A las corporaciones se les asignan bloques de direcciones contiguas que tienen un prefijo de subred común.
  + Originalmente diseñado para ajustar el tamaño del bloque de direcciones a las necesidades de un ISP
* Agregación de Rutas
  + Los routers anuncian las rutas mediante prefijos de subred. Un único prefijo agrupa un gran número de IP
  + Ventaja de la Agregación de Rutas
    - Minimización del tamaño de las tablas de encaminamiento
    - Minimización de la información que deben intercambiarse los routers cuando ejecutan los protocolos de encaminamiento. La reducción dela fracción del ancho de banda dedicada a soportar el tráfico de control en la red (advertising reachability).
* Dirección IP de Broadcast
  + Cuando IP se transporta sobre Ethernet, los hosts de una subred configura un dominio de broadcast. La IP de broadcast es 255.255.255.255
  + Cuando se envía un datagrama a esa dirección, el mensaje se difunde SÓLO a todos los host de la misma subred. No se propaga fuera de la subred

Longest Prefix Matching: Coincidencia exacta del prefijo de subred más largo.

Una vez seleccionada la entrada en la tabla de encaminamiento se obtiene la IP del *next hop*.

ARP permite encontrar la dirección MAC del siguiente salto, conociendo su IP dentro de una subred. Los hosts almacenan las asociaciones MAC-IP en una tabla

1. MPLS

MPLS: MultiProtocol Label Switching.

Método para el forwarding de paquetes a través de Internet usando etiquetas adicionales a las de la SDU.  
Convergencia de dos paradigmas. Datagrama y Circuito Virtual

MPLS introduce un esquema de encaminamiento basado en CV en redes basadas en datagrama de forma que ambos coexisten simultáneamente en el tiempo.

**Beneficios de MPLS**

* Encaminamiento basado en etiquetas (CV) era más rápido que el basado en datagrama.
* Puede funcionar en un escenario multiprotocolo de L3 y L2
* Facilita el soporte de VPN
* Soporta QoS
* Permite aplicar esquemas de TE. Balanceo de carga y FastReRoute

Encaminamiento IP convencional

* Packet Flow
* Los routers toman una decisión de encaminamiento independiente para cada paquete basándose en el análisis de cabecera, resultado de la ejecución del algoritmo LPM (longest prefix matching), estado de tabla de encaminamiento
* Esa decisión resulta en la asociación de cada paquete con una entrada de la TE, los paquetes de un mismo MEC comparten el mismo *next-hop*
* Dos tipos de asociación paquete/flujo a FEC
  + Grano grueso: se asocia subnet prefix next hop
  + Grano fino: se tienen en cuenta otros campos
* Un FEC es un conjunto de *flows* que se reenvían con mismas características.
* Cada router realiza una asignación independiente de *flows* a FECs

Encaminamiento MPLS

* A los paquetes de un FEC se les asigna la misma etiqueta
* Para la asignación de la etiqueta, además de la información del FEC IP, se pueden utilizar parámetros adicionales.
* Los conmutadores MPLS se denominan LSR (Label Switch Router)
* La tabla de encaminamiento se llama LFIB (Label Forwarding Información Base)
* El circuito virtual se denomina LSP (Labrl Switched Path)
* La LFIB en un LSR tienen la estructura
* Asociar etiqueta a paquete IP
* La etiqueta resume toda la información esencial para forwarding
* El forwarding en los LSR está basado sólo en etiquetas.
* La etiqueta se usa como índice de la LFIB, que indica
  + El siguiente salto del paquete (puerto de salida)
  + El valor de la nueva etiqueta (label swapping)
  + Operaciones para realizar sobre la etiqueta (pop/push)
  + La LFIB puede contener información del encapsulado de capa de enlace necesario, y otra información para retransmitir el paquete correctamente
* A la salida de la red MPLS se elimina la etiqueta.
* Una misma entrada en la LFIB puede tener varias subentradas, cada una con etiqueta de salida, interfaz y cola en puerto de salida diferente.
* Cada subentrada se llama NHLFE (Next Hop Label Forwarding Entry)
  + El ILM (Incoming Labrl Map) define la asociación entre etiquetas entrantes y el NHLFE
  + MPLS no define cómo escoger una NHLFE
* La existencia de múltiples NHLFE permite el balanceo de carga, protección de los caminos y soporte multicast y QoS.
* Soporte multicast
  + El soporte de comunicaciones multicast requiere que los LSR realicen múltiples copias de un mismo paquete y lo retransmitan por las diferentes interfaces de salida.
  + Estas comunicaciones requieren la creación de un árbol de distribución, con una raíz y múltiples hojas
* Soporte QoS
  + Puede requerir enviar los paquetes a diferentes colas asociadas a una misma interfaz/puerto de salida
  + Cada cola puede estar asociada a una prioridad diferente



Plano de control: El objetivo de distribuir etiquetas, establecer/liberar las LFIB. Depende del protocolo. Con LDP cada router establece sesiones TCP con vecinos para intercambiarse etiquetas

Plano de datos: Añadir/eliminar etiquetas a paquetes IP y retransmitir paquetes MPLS usando la LFIB. Usan un servicio orientado a la conexión

**Ventajas del encaminamiento en MPLS**

* Integrado con el encaminamiento IP en los routers
* La asignación de un paquete/FEC a un LSP se hace solo una vez, a la entrada de la red MPLS
* El desencapsulado de paquetes IP se realiza en el edge, donde la carga es baja
* Se puede forzar a que un *packet flow* siga una ruta preestablecida con anterioridad a su llegada a la red
  + Con encaminamiento convencional esto no es posible. Para cada paquete, cada router de la red determina de forma autónoma y dinámica el siguiente salto
  + Las rutas predefinidas son la base de la TE con MPLS
* LSR de entrada pueden asignar paquetes con mismo destinos a diferentes LSP en función de diferentes criterios. Punto de entrada a la red (permite definir VPN)…
* El LSR de entrada puede seleccionar una clase de servicio. Base para QoS

MPLS es una forma de encapsular paquetes de cualquier protocolo de capa de red y dirigir dicho tráfico a través de una determinada ruta hacia su destino, basándose en una técnica de conmutación de etiquetas. La etiqueta se añade entre las cabeceras de capa 2 y 3

Gráfico de cajas y bigotes

Descripción generada automáticamente

Dominio MPLS es el conjunto de LSR interconectados en el mismo dominio administrativo o de encaminamiento.

Los LSR edges no seleccionan ninguna etiqueta de entrada, esta etiqueta es la que un LSR espera encontrar en todos los paquetes MPLS entrantes de un determinado FEC.

El etiquetado de los paquetes debe realizarse por los LSR que son upstream a un LSR dado.

Para que un LSR reciba los paquetes etiquetados con el valor seleccionado lo debe notificar a sus vecinos. Cuando un LSR recibe una asociación etiqueta-FEC, si es upstream actualizará la etiqueta de salida del FEC, en cambio si NO es upstream descartará la información o la almacenará por si la necesita en el futuro. Un LSR X decide que es upstream de un FEC cuando recibe la asociación de otro LSR Y por el mismo puerto por el que X retransmite los paquetes asociados al FEC

Los LSP son unidireccionales. Muchas veces, varios LSP se asocian al mismo FEC, formando un árbol (merging). Tipicamente agregan tráfico desde el edge hacia el backbone

Los LSP pueden ser:

* Estáticos: se establecen a mano
* Dinámicos: se establecen con LDP

Espacio de etiquetas:

* 15 etiquetas especiales
* Etiquetas compartidas por LSP estáticos y constraint-based routed
* Etiquetas de asignación dinámica
  + LDP
    - Se definió específicamente para distribuir etiquetas
    - Establece los LSP hop-by-hop
    - Identifica el siguiente hop utilizando la RIB de IP. La RIB se crea ejecutando IGP y BGP
  + RSVP-TE
    - Se diseñó para reservar recursos en los routers de una ruta
  + MP-BGP
    - Es una extensión de BGP y soporta la distribución de etiquetas en VPN definidas mediante MPLS

**Unsolicited Downstream**

* LSR realiza asociación FEC-label y lo almacena en su LFIB
* Ese LSR anuncia la asociación a sus vecinos. La etiqueta se crea en el nodo downstream y se anuncia a los vecinos sin que estos lo soliciten

**Downstream On Demand**

* Un LSR realiza asociación FEC-label y la almacena en su LFIB
* NO anuncia a sus vecinos, sino que los vecinos preguntan al LSR acerca de dicha asociación

Si un LSR recibe una asociación FEC-label y no es upstream:

* CLR: Conservative Label Retention Mode: Ignora la asociación. LFIB más pequeñas
* LLR: Liberal Label Retention Mode: Almacena la asociación. Adaptación a cambios en las rutas más rápida

**Dos procedimientos para establecer un LSP**

* Control de LSP independiente:
  + Cuando un LSR detecta un nuevo FEC, le asocia una nueva etiqueta y lo anuncia
  + Converge más rápidamente
  + Algunos LSR pueden empezar a conmutar paquetes antes de que el LSP esté establecido
* Control de LSP ordenado
  + La asociación se hace de forma ordenada desde el edge de salida.
  + Un LSR solo crea una asociación local en uno de los siguientes caos
    - Si es el edge LSR de salida para ese FEC
    - Si ha recibido una asociación del siguiente salto de ese FEC
  + El LSR que lo inicia selecciona la asociación FEC-label y todos los LSR del LSP utilizarán el mismo FEC. Las asociaciones se tienen que propagar antes de que pueda establecerse la conexión
  + Mejores capacidades de prevención de bucles.

Ambos tipos de control pueden coexistir en la misma red

MPLS usa la información de encaminamiento IP para el establecimiento de LSPs

MPLS también permite la creación de LSP que sigan una ruta explícita

* No tiene porqué coincidir con la ruta IP
* Útil para satisfacer QoS
  + El encaminamiento IP minimiza el numero de saltos
  + En MPLS se puede minimizar el retardo extremo a extremo y maximizar el throughput
* Útil para proveer balanceo de carga
* Útil para hacer túneles y VPN, incluso con QoS

El encaminamiento explicito admite dos modalidades

* Ruta estricta: Se define la ruta completamente
* Ruta no estricta o imprecisa: No se especifican todos los LSR por los que pasará el LSP. Se emplean cuando se atraviesan varios dominios MPLS pertenecientes a otros ISP.

MPLS soporte múltiples etiquetas por paquete, organizadas como una pila

**Pila (*stack*):** Es una estructura de datos que permite almacenar y recuperar datos. Es de tipo LIFO. Para el manejo de los datos cuenta con dos operaciones básicas. PUSH, añade un objeto y POP retira el último elemento apilado**.**

Se pueden realizar tres operaciones sobre la etiqueta:

* Label Swapping: Reemplazar la etiqueta de nivel más salta de la pila por una nueva etiqueta. La realizan los LSR intermedios
* Labrl Popping: Eliminar la etiqueta. Se elimina la etiqueta superior de la pila, y reenvía el paquete de acuerdo con la siguiente etiqueta o, si no tiene más etiquetas, como paquete IP
* Label Pushing: Añade una o más etiquetas a la pila. Se empuja la etiqueta cabecera de la pila hacia abajo del *stack*, añadiéndose una nueva etiqueta visible.

**Penultimate Hop Popping (PHP)**

El penultimo LSR del LSP elimina la etiqueta. El último LSR recibe el paquete IP sin etiqueta y realiza el forwarding IP convencional. Se emplea para eliminar la complejidad del hardware al tener que procesar la etiqueta y realizar una búsqueda en la tabla de encaminamiento IP en el *egress* LSR

**Bucles en MPLS**

Los LSP se construyen haciendo use de los protocolos de encaminamiento de capa 3

* Estos protocolos tratan de evitar los bucles pero casi todos los protocolos pueden producir bucles en determinadas condiciones transitorias al caer un enlace.
* Puede haber errores de configuración

Si no se previenen los bucles pueden ocurrir bucles en los paquetes de control de LSPs o bucles en los paquetes de datos MPLS

Estrategias para controlar los bucles en MPLS:

* Reactiva: detección de bucles
  + Se permite la formación de bucles
  + No se permite que los paquetes que estén en un bucle afecten a los paquetes que no lo forman
  + Dos escenarios
    - En segmentos TTL
      * Parecido a TTL de IP
      * Campo TTL se decrementa a 0
    - En segmentos NO TTL
      * TTL no está disponible si se usa MPLS sobre ATM
      * Dos opciones
        + En cada LSR se limitan los recursos de cada CV
        + Se utiliza un contador de saltos en los mensajes LDP
* Preventiva: prevención de bucles
  + Previene la formación de bucles en LSP antes de que se envíen paquetes sobre esos LSP
  + Permiten detectar que se está formando un bucle antes que los mecanismos de detección
    - Útiles si no disponemos de TTL
    - Si se quiere detectar antes de que venza el contador de saltos
    - Los mecanismos de prevención añaden mayor sobrecarga que los de detección
  + Dos técnicas
    - Algoritmo del vector camino
      * Se previene la formación de bucles usando una lista de direcciones de LSR
      * Vector de camino: Lista de LSR por los que ha pasado un mensaje de solicitud o de asociación de etiqueta
      * Cada mensaje de control para solicitar o asociar una etiqueta puede contener una lista de direcciones de LSR, de manera que dicha lista se amplía cuando un LSR reenvía el mensaje.
      * Si un LSR detecta su direccion en dicha lista se detecta el bucle y se impide que se forme el LSP
    - Algoritmo del hilo coloreado
      * Requiere, como mecanismo de establecimiento de camino, el de control ordenado
      * Puede modelarse como un hilo coloreado que se extiende desde el inicio hasta el final del LSP
      * Cualquier LSR intermedio detectaría un bucle si el hilo vuelve sobre si mismo, lo que evita que se construya el LSP
      * Los LSR entonces esperan hasta que las tablas de encaminamiento converjan, y se estabilicen antes de intentar extender otro hilo

1. L3VPN

Las VPN son un tipo de redes que interconectan diferentes sedes utilizando una infraestructura de red compartida, típicamente del proveedor de servicios.

Existen dos tipos de VPN

* Intranet: Si las sedes son de la misma corporación
* Extranet: Si son de corporaciones distintas

Típicamente las VPNs se emplean para interconectar LANs en diferentes sedes de una corporación. Antes se hacía mediante enlaces dedicados o mediante circuitos virtuales. Actualmente se emplean túneles basados en IP o MPLS

Los requerimientos de una VPN son:

* Provisión de conectividad y transporte de datos
* Garantías de servicio
* Sencilles de configuración y operación
* Seguridad
  + Autenticación
  + Autorización
  + Cifrado

El aislamiento del tráfico se consigue mediante túneles de capa 2 o de capa 3.

**L3VPNs:** Sedes de la VPN intercambian paquetes IP

* En Internet es común que los túneles encapsulen paquetes con direcciones IP privadas en paquetes con direcciones IP públicas. IPSec, MPLS, L2TP. IPSec es el servicio más usado y solo ofrece un servicio *best-effort*

**L2VPNs:** Las sedes se intercambian tramas L2. Permite transporte de tramas broadcast y otras tramas L2

Los túneles son un esquema de transmisión que permite usar una red de tránsito para interconectar 2 o más redes privadas. Los datos para transmitir son tramas o paquetes. Estos se encapsulan en tramas/paquetes con el formato de la red de tránsito y la cabecera adecuada para que sean encaminados al destino deseado. La ruta lógica se llama túnel. El túnel tiene dos extremos y es unidireccional. El usuario percibe el túnel como un enlace punto a punto dedicado. El establecimiento de túneles es similar al de una sesión. Dos protocolos: de señalización y de transporte de datos.

Para acceso remoto de usuarios a la red corporativa mediante línea DSL o WLAN, se usan soluciones L2: PPTP y L2TP

Para la interconexión de redes remotas se usa: GRE, IPSec o MPLS. Los túneles por si mismo no proveen de seguridad. IPSec incluye cifrado.

**GRE**

* Se usa para encapsular paquetes no IP en paquetes IP
* Junto con PPTP crea túneles
* E-GRE hace más eficiente la transmisión
* Simple, rápido y permite QoS

**PPTP**

* PPTP es un protocolo de capa 2 usado en conexiones punto a punto
* Deriva del PPP
* Es inseguro

**L2TP**

* Sustituye PPTP
* Tiene su propio protocolo de túnel (UDP 1701)
* Emula una conexión PPP y usa dos canales uno para datos y otro para control
* No provee seguridad. Para ello se usa IPSec

**IPSec**

* Protocolo de transporte más seguro y eficiente
* Provee seguridad a nivel L3
* En modo túnel crea una nueva cabecera IP para cada paquete
* No permite QoS
* Complejo

**Modelos VPN**

* Overlay
  + Requiere definir un conjunto de enlaces punto a punto entre los router CE del cliente en diferentes sedes
  + Los enlaces pueden ser L1, L2 o L3
  + Los CE realizan peering entre ellos. Piensan que están conectados por enlaces punto a punto
  + Los routers de la SPN transportan datos del cliente entre sedes, pero no realizan peering con los CE. SPN es transparente para los CE
  + La inteligencia está en los CE routers
    - Se implementa en la sede del cliente
    - Requiere conocimientos por parte del cliente
    - Si el cliente traspasa la gestión al operador, el operador debe gestionar muchos CE en “casa” del cliente.
  + Cada vez que se añade una nueva sede hay que conectarla al resto y reconfigurar el resto de sedes
  + Problemas de escalabilidad

La inteligencia y el control de la VPN radica en los routers frontera del cliente (CE). CE routers interconectados mediante una “malla” lógica intercambian información de encaminamiento (peering) SÓLO entre ellos, no con los routers de la SPN. Requiere configuración manual.

* Peer to Peer
  + Los CE solo se comunican con los PE (provider edge)
  + PE hacen peering con CE y con los SPN
  + Gran reducción de peerings
  + Encaminamiento más sencillo
  + La inteligencia se traslada a los PE

La gestión del encaminamiento entre sedes de un cliente se traslada al proveedor. La inteligencia se traslada a los PEs, que hacen peering entre ellos a través de la SPN. Los CEs hacen peering SÓLO con los PEs, pero NO entre sí.

**Overlay vs Peer-to-Peer**

* Añadir una sede a una VPN requiere únicamente cambios en el nuevo CE y su PE asociado.
* No aumenta el numero
* Encaminamiento simple desde un punto de vista del CE
  + Cada CE anuncia a su PE información de alcanzabilidad para las subredes de la sede a la cual pertenece la CE
* Cada sede puede ejecutar protocolos internos de encaminamiento diferentes
* El modelo Peer-to-Peer es más atractivo.

**BGP/MPLS L3VPN**

* Las L3VPN basadas en MPLS se conocen como BGP/MPLS VPNs porque
  + BGP es necesario para distribuir la RIB entre los PE del SP
  + MPLS se usa para en transporte de datos de una sede a otra

Los BGP speakers son routers que ejecutan BGP. Los BGP speakers no se descubren mutuamente de forma automática. Los BGP peers de un BGP speaker deben ser configurados de forma explícita. No necesitan estar conectados directamente. Un grupo de BGP peers que establecen conexión entre ellos intercambian sus RIBs. Una sesión se soporta mediante TCP.

Cuando dos BGP están en AS mantienen una internal BGP session. Si están en distintos AS mantienen una external BGP session. BGP utiliza los mismos tipos de mensajes para IBGP y EBGP, pero las reglas de envío e interpretación cambian. Los IBGP de un mismo AS deben estar conectados mediante una malla lógica completa. Los EBPG peers no necesitan estar conectados mediante una malla completa

* BGP peers: un grupo de routers que realizan peering BGP entre sí.
* BGP speaker: un router que ejecuta BGP (uno del grupo BGP peers).

**Mensajes BGP**

* Open Message. Es el primero que se intercambian. Contiene info que permite decidir si necesitan establecer conexión. Número de AS y otros parámetros
* Update Message. Es el más importante y se usa para anunciar rutas.
* Keepalive mesasge. Determina si una conexión TCP funciona correctamente
* Notification message. Para terminar una sesión con otro BGP peer

**Route Reflectors**

* Dispositivos de encaminamiento usados en BGP
* Actúan de servidor que reflejan la información de encaminamiento
* En grandes redes reduce en número de comandos de consola de gestión
* El uso de múltiples route reflectors evitan el punto único de fallo

**Arquitectura de la solución**

* Para un SP, una VPN es una colección de políticas que definen la conectividad entre las sedes.
* Una sede de un cliente se conecta a la SPN por medio de uno o varios interfaces
* CEs (Customer Edge Devices)
  + Ofrecen acceso a la SPN
  + Un CE puede ser un host, conmutador L2…
  + Hace peering a un PE y anuncia su alcanzabilidad
* PEs (Provider Edge Routers)
  + Un PE intercambia info de routing con los CEs usando encaminamiento estático
  + Un PE sólo mantiene rutas hacia VPNs con las que está conectado
  + Interfaces de PE conectados con sedes de diferentes VPNs soportan tablas de encaminamiento distintas. VRF. Múltiples interfaces pueden compartir una misma tabla VRF cuando estás pertenecen a la misma VPN.
  + Los PEs intercambian info de alcanzabilidad entre ellos empleando IBGP. Los routers P no almacenan rutas a VPNs
  + Los PEs pueden mantener sesiones con router reflectors
  + Para la retransmisión de datos MPLS
    - El ingress PE funciona como ingress LSR.
    - El egress PE router como egress LSR.
* Ps (Provider routers)
  + Es un router de la SPN que no se conecta directamente con un CE
  + Los routers P funcionan como LSRs de tránsito en la red MPLS cuando retransmiten paquetes entre VPNs
  + Los paquetes entre VPNs se encapsulan en MPLS. Estos pueden utilizar un stack de dos etiquetas
    - La visible define el LSP entre PEs extremos y la utilizan los P
    - La no visible identifica el VPN al que pertenecen

**Problemas y soluciones**

* Soporte de espacios de direcciones solapados entre VPNs. Solución: route distinguishers y MP-BGP
  + Cuando los usuarios usan direccionamiento privado, la misma dirección IPv4 puede asignarse en VPNs de diferentes clientes.
  + Cuando BGP observa rutas diferentes al mismo prefijo piensa que son equivalentes, e instala sólo una ruta. Entonces, sólo un destino (una VPN) es alcanzable, y el resto dejan de ser alcanzables. Es necesario un mecanismo para ‘desambiguar’ los prefijos, y permitir que se instalen rutas diferentes para cada uno de los destinos (VPNs) con la misma dirección IPv4 privada.
    - Una dirección VPN-IPv4 es de 12 bytes, compuesta por los 8 bytes del route distinguishers (RD) y los 4 bytes de la dirección IPv4.
* Limitar la conectividad en la SPN. Solución: BGP Extended Communities
  + Evitar que PEs instalen rutas VPNs que no tienen directamente conectadas
  + Se mejora el aislamiento del tráfico