TOPIC 5: VPN

Pregunta 1. Explica cuál es el propósito de contratar una VPN.

Dar conectividad con la misma QoS y privilegios a alguien de fuera de la sede central (ya sea un usuario desde su casa u otra red corporativa) que si estuvieran dentro de la sede central (poner una topología virtual por encima del proveedor).

Pregunta 2. Define y explica los principales parámetros de tráfico. Idem para los parámetros de calidad de servicio.

Parámetros de tráfico:

- **CIR (Committed Information Rate):** velocidad media contratada.
- **EIR (Excess Information Rate):** velocidad media en exceso respecto al CIR (cuánto te puedes pasar de tu CIR).
- **CBS (Commited Burst Size):** tamaño máximo que puedes transmitir en un paquete, normalmente corresponde al tamaño de un solo paquete.
- **EBS (Excess Burst Size):** exceso sobre paquetes enviados consecutivamente. No aumenta el throughput.

La modificación de estos parámetros permite crear contratos específicos de conexión para distintos tipos de usuarios. Por ejemplo Best-effort (CIR=0, CBS=0, EBS>0).

Parámetros de calidad de servicio:

- **Packet Delay:** retraso extremo a extremo de un paquete.
- **Jitter:** variación del retraso del paquete.
- **Packet Losses:** ratio de pérdida de paquetes.

Pregunta 3. ¿Cómo funciona el enrutamiento por MPLS? ¿Qué funcionalidades tiene la etiqueta MPLS?

La idea de MPLS es realizar la conmutación de paquetes a nivel 3 pero usando etiquetas en vez de direcciones IP. Este protocolo permite realizar ingeniería de tráfico, ofrecer servicios VPN, controlar la QoS… El funcionamiento es el siguiente:

Un paquete IP entra a una red MPLS y se les asigna una etiqueta. Dentro de esta red, los routers (ahora denominados LSRs) conmutarán via etiquetas en vez de direcciones IP, teniendo en cuenta por cual interfaz entran. Los paquetes se van conmutando de esta forma hasta salir del dominio MPLS.

La etiqueta contiene:

- Identificador de esta misma.
- Bits para determinar QoS.
- Bit para marcar la etiqueta más baja del stack (permite apilar etiquetas).
- Bits de TTL.

Pregunta 4. Explica en qué consiste el servicio EtherLAN de MetroEthernet y las diferencias entre un servicio EPLan (Ethernet Private LAN) y uno EVPLan (Ethernet Virtual Private LAN).

El servicio EtherLAN es un servicio de MetroEthernet que se basa en una topología multipunto a multipunto con conexiones EVC entre las diferentes UNIs de la red corporativa. Este servicio, al igual que los otros, permite definir una serie de atributos relacionados con la velocidad de transmisión, la calidad de servicio, etc…

Dentro de este servicio, encontramos una división en otros 2 servicios, EPLan y EVPLan. En EPLan, sólo es posible crear una EVC por cada conexión entre dos o varias UNIs sobre la cual definir los parámetros de calidad de servicio. En cambio, en EVPLan, se pueden soportar varias EVCs entre dos o vairias UNIs los cuales comparten los mismos parámetros de tráfico y calidad de servicio.

Pregunta 5. Explica en qué consiste el servicio EtherLine de MetroEthernet y las diferencias entre un servicio EPL (Ethernet Private Line) y uno EVPL (Ethernet Virtual Private Line).

El servicio EtherLAN es un servicio de MetroEthernet que se basa en una topología punto a punto con conexiones EVC entre los diferentes CE de la red corporativa. Este servicio, al igual que los otros, permite definir una serie de atributos relacionados con la velocidad de transmisión, la calidad de servicio, etc…

Dentro de este servicio, encontramos una división en otros 2 servicios, EPL y EVPL. En EPL, sólo es posible crear una EVC por cada point-tosip

-point sobre la cual definir los parámetros de calidad de servicio. En cambio, en EVPL, se pueden soportar varias EVCs entre dos UNIs los cuales comparten los mismos parámetros de tráfico y calidad de servicio.

Pregunta 6. Explica la diferencia entre un servicio EPL (Ether Private Line) y uno EVPL (Ether Virtual Private Line).

Dentro del servicio EtherLine de MetroEthernet, encontramos una división en otros 2 servicios, EPL y EVPL. En EPL, sólo es posible crear una EVC por cada point-to-point sobre la cual definir los parámetros de calidad de servicio. En cambio, en EVPL, se pueden soportar varias EVCs entre dos UNIs los cuales comparten los mismos parámetros de tráfico y calidad de servicio.

Pregunta 7. Explica cómo se usan las comunidades extendidas en una VPN MPLS-BGP.

Las comunidades extendidas se usan para marcar la ruta a seguir (VRF), se guarda allí la VRF que está siguiendo ese paquete y así se puede determinar si esa VRF es una conocida o no.

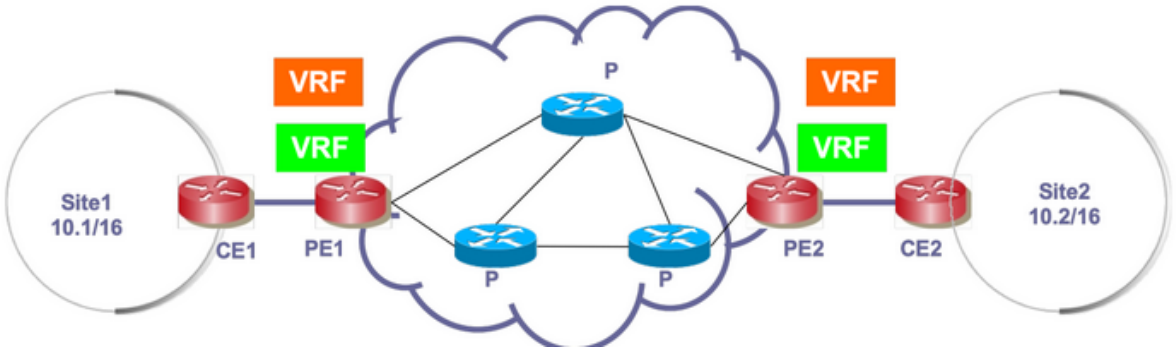
Pregunta 8. Explica cómo se estructuran las direcciones VPN-IPv4, explicando los distintos tipos de direcciones que se pueden generar. Explica cómo las usa y para qué BGPv4.

Son direcciones de IP de 12 Bytes y todas han de ser públicas. Se componen de 8 bytes correspondientes al RD (ha de ser único) y otros 4 bytes de una dirección IP que puede ser tanto pública como privada, ya que el identificador será el RD.

Para que el RD sea universal, se definen 3 tipos de prefijos:

- Tipo 0: RD = 2 bytes del tipo, 2 bytes campo administració, 4 bytes más que determinan el número de VPN-IPv4 que podemos generar de este tipo. El campo de administración ha de contener el número de sistema autónomo.
- Tipo 1: RD = 2 bytes del tipo, 4 bytes de campo administración y 2 bytes más que determinan número de VPN-IPv4 que podemos generar de este tipo. El campo administración ha de contener una dirección IP pública.
- Tipo 2: RD = 2 bytes del tipo, 4 bytes de campo administración y 2 bytes más que determinan número de VPN-IPv4 que podemos generar de este tipo. El campo administración ha de contener un número de sistema autónomo extendido.

Pregunta 9. Explica cómo se crea una VPN MPLS-BGP entre las sedes Site-1 y Site-2. Explica también el proceso de envío de un paquete IP entre el Site-1 y el Site-2.



Creacion:

- El site1 y 2 comparten la misma etiqueta, en este caso la verde.

1. CE1 anuncia la red 10.1/16 via E-bgp a PE1
2. PE1 añade la red 10.1/16 a la VRF verde usando el RD identifier.
3. PE1 envia a través de I-BGP.
    a. Asocia la ruta a la VRF verde añadiendo una comunidad extendida
    b. Añade la etiqueta site-id a la ruta

    c. Selecciona la dirección de loopback y la añade como next-hop

4. PE2 recibe la ruta 10.1/16 y hace un filtrado

    a. Revisa la comunidad extendida para (VRF verde) para ver si pertenece a alguno de los VRF conocidos

5. PE2 accepta la ruta porque ésta pertenece a la VRF verde

    a. Se guarda la etiqueta site-id para poder enviar mensajes

6. PE2 anuncia a PE1 la etiqueta VRF verde (el mismo proceso a la inversa)

Cuando PE2 aprende la ruta anunciada por PE1, este crea un tunel MPLS entre PE1 y PE2 (y viceversa)

MPLS LABELS:

- **LSP tag:** Se usa para enviar paquetesw de PE1 aPE2
- **Site-tag:** Se usa para identificar quien es el Remote site

Envío de mensaje:

- El host 10.2.1.1 en site2 se comunica con el host 10.1.1.1 (por ejemplo)

1. PE2 obtiene la VRF basado en el puerto en el que recibe el paquete.
    a. El MPLS site-id (Entregado durante la creación de la vpn)
    b. El next hop es la loopback de PE1
    c. LSP TAG
2. El tag LSP se usa para hacer llegar los paquetes al LSP apropiado, mientras que el Site tag se usa por el PE remoto para enviar los paquetes al puerto indicado

El host 10.2.1.1 en site2 se comunica con el host 10.1.1.1. PE2 identifica la VRF por el puerto por el que recibe el paquete. Seguidamente, observa cual es la dirección IP destino y le asocia al paquete la site-tag correspondiente. Además, le asocia por encima otra etiqueta llamada LSP tag que será utilizada para que el paquete se dirija desde PE2 hasta PE1. Cuando el paquete llega a PE1, elimina la LSP tag y mira el contenido de la site-tag. De esta forma, mira la tabla VRF e identifica la interfaz de salida.

- **How to exchange packets between two CE ?**
    - Use BGP to export routes
    - Use **Extended Communities** (8-byte) to filter and associate BGP traffic to a VRF (Virtual Router and Forwarding)
    - VRF are tables associated to PE routers
    - Use MPLS to switch traffic in the Internet core