TEMA 1

1.- La arquitectura de internet está compuesta por ISPs, end users, corporate networks y máquinas.

Los primeros se dedican a ofrecer servicios y conectividad (esto último lo diferencia de las redes corporativas) para los demás y a hacer negocio con ello. Ejemplos: Movistar, Orange…

Los end users son los particulares o pequeños grupos que necesitan una conexión a internet y servicios similares, como una línea telefónica o televisión.

Las redes corporativas suelen ser empresas u organizaciones que necesitan y ofrecen servicios adicionales, como conexiones dedicadas, seguridad adicional o housing de servidores. No te dan conectividad.

El grupo de máquinas se refiere a todo tipo de sensores (IoT), robots, cámaras de videovigilancia…

Todo está conectado entre sí, ya sea directa o indirectamente. Para conectar ISPs y que se pueda dar ese salto entre cualquier par de entidades existen los puntos neutros o exchange points.

2.- Una CDN es una red de servidores distribuidos por distintas zonas geográficas que sirven para dar un mejor servicio a los usuarios y que no tengan que esperar el RTT que supondría tener que enviar sus querys a un servidor en la otra parte del mundo cada vez que quieran acceder a un contenido de internet. También ayudan con el balanceo de carga y ofrecen servicios como introducir publicidad en el contenido o monitorizar los datos de consumo del mismo. El método más común de request routing es usando servidores DNS.

3.- Farm servers, mirrors y CDNs. Proxy caching. HTTP caching.

4.- Un SLA (Service Level Agreement) es un contrato que tiene que cumplir el proveedor de un servicio a su cliente. Incluye, entre otros, un mínimo de disponibilidad (downtime), throughput, bandwidth, seguridad, redundancia, tiempo de respuesta en caso de fallo, monitorización, QoS, etc. Si no se cumple, se paga una multa.

5.- Autonomous system es un dominio de enrutamiento, es decir un conjunto de redes que siguen una misma política de enrutamiento. Pueden ser distintas redes de distintos operadores. Inter-domain, entre dos AS, intra-domain, dentro del mismo AS.

Distintas relaciones:

- Customer to provider: pasa a su provider lo suyo y lo de sus clientes.

- Provider to customer: todo lo de su tabla de enrutamiento, menos su cliente y los clientes de éste.
- Peer to peer no transit: pasa a sus peers lo suyo y lo de sus clientes.
- Peer to peer transit (sibling): toda su tabla de enrutamiento, menos su peer y los clientes de éste.

6.- Un RIR es una organización que gestiona los recursos de internet como bloques de direcciones IPv4 e IPv6 en una zona geográfica determinada. Existen 5, y el europeo, junto con oriente medio, se llama RIPE. Obtienen esos recursos de IANA, y los distribuyen a los LIR (Local Internet Registry). Éstos son empresas o instituciones como Movistar o la UPC, que dan servicios a end users u otras empresas. Puedes ser AS sin ser LIR y obtener tus bloques IP de un LIR. Para ser AS, tu política de enrutamiento debe ser distinta a la de tu proveedor.

7.- UPC, LIR; CAIDA, rankea AS;RIPE, RIR; Euro-IX, exchange point; IANA, por encima de RIRs; Jazztel, ISP.

8.- Está en la 5.

9.- De net4 a net6 sí, al revés no.

10.- En este caso sí y sí.

11.-

Red	**AS path vector from AS4**
1	AS3-AS1 | AS5-AS6-AS2-AS1
2	AS5-AS6-AS2
3	AS3
4	-
5	AS5
6	AS5-AS6

Red	AS path vector from AS5
1	AS4-AS3-AS1 | AS6-AS2-AS1
2	AS6-AS2
3	AS4-AS3
4	AS4
5	-
6	AS6

Red	AS path vector from AS6
1	AS2-AS1
2	AS2
3	-
4	-
5	AS5
6	-

12.-

Red	AS path vector from AS4
1	AS3-AS1 | AS7-AS2-AS1
2	AS7-AS2
3	AS3
4	-
5	AS5
6	-
7	AS7

Red	AS path vector from AS5
1	AS4-AS7-AS2-AS1 | AS6-AS2-AS1
2	AS4-AS7-AS2 | AS6-AS2
3	-
4	AS4
5	-
6	AS6
7	AS4-AS7

Red	AS path vector from AS6
1	AS2-AS1 | AS5-AS4-AS7-AS2-AS1
2	AS2 | AS5-AS4-AS7-AS2
3	-
4	AS5-AS4
5	AS5
6	-
7	AS5-AS4-AS7

13.- El cono de clientes es una representación que hace CAIDA de todos los AS que solo tiene en cuenta las relaciones de cliente. Es muy representativo sobretodo para ver los tamaños e influencia de los AS y la diferencia entre ellos.

14.- Mismo que el anterior. Peering cone size ratio: figura = 50, (i) = 75, (ii) = 66.

15.- Las opciones en IPv6 se determinan mediante cabeceras extendidas, a las cuales apunta el campo NH del paquete IP. Para poner más de una extensión, el next header de la primera opción apuntaría a la siguiente. Algunos ejemplos son hop-by-hop options, routing, fragmentación, encriptación (ESP), movilidad…

16.- Un punto neutro es una entidad de red que permite interconectar dos o más ISPs. Los hay nacionales e internacionales. La matriz de peering de un punto neutro es una base de datos que representa las relaciones entre los AS que están conectados al exchange point, si son peers o no. Para ser miembro de un punto neutro te tienen que aceptar y además hay que pagar.

17.- Un bloque de direcciones IP PA que puede ser agregado por los protocolos de enrutamiento una vez sale del dominio (AS) para ahorrar recursos. En ese caso, cuando cambiamos de ISP perdemos ese bloque de direcciones. En cambio, en el caso de PI, eso no sucede, ya que son pequeños bloques independientes que ha asignado el RIR de la zona geográfica. Pese a que aportan versatilidad en el cambio de ISPs, es posible que algunos operadores de red decidan no enrutarlos.

18.- Para configurarla a partir de un prefijo se usa éste más la dirección MAC extendida del dispositivo. Ejemplo con prefijo 34:56:78 y MAC 9a:bc:de:
3**6**56:78**ff:fe**9a:bcde.
A partir de una dirección IPv4: 0:0:0:0:0 + ffff + @IPv4 (hex).

19.- Global se enrutan por todo Internet, site local se enrutan solo por la red local, link local no se enrutan por routers, solo switch.
Stateful es la versión de DHCP de IPv6, donde se proveen las direcciones automáticamente y el cliente y el servidor la mantienen durante un tiempo. Stateless es una configuración que se debe hacer manualmente de la dirección IP por parte del cliente.

20.- El prefijo consta de tres campos, TLA (Top), para los proveedores de Tier- 1 y de tamaño 13+8; NLA (Next), para los proveedores de Tier-2 y de tamaño 24; y SLA (Site), para corporaciones y de tamaño 16.

21.- IPv4 usa ARP, mientras que IPv6 usa NDP. Se obtienen los mismos resultados, naturalmente. Router/Neighbour Solicitation/Advertisement.

22.- Mismo que 21.

23.- @IPv4 = 12.5.5.4; MAC = 05:07:14:ab:ff:04.
Link-local IPv6 = fe80::0707:14ff:feab:ff04
Prefijo IPv6 =02ab::0707:14ff:feab:ff04
Desde IPv4 = 0:0:0:0:0:ffff:0c05:0504

TEMA 2

1.- Para poder tener redundancia y agregación en redes sin tener bucles, que ocasionan broadcast storms.

2.- Una tormenta broadcast es un fenómeno que ocurre cuando hay bucles en una red y se hace un ping a broadcast, es decir, a todos los dispositivos. Éste se va replicando sin fin por la red ocupando la potencia de procesamiento de los routers hasta saturarlos, con la única solución siendo tumbar la red.

3.- Básicamente, se hace una instancia de STP para cada VLAN, ya que son redes virtualmente distintas. MSTP es el estándar del IEEE.

4.- STP escoge un root bridge mediante las MACs de los dispositivos y las prioridades previamente asignadas (si no se asigna son todos de igual prioridad), el valor más bajo se queda el root bridge.

5.- Root bridge es el switch que gobierna la red, la raíz del árbol de STP. Se elige con la MAC+priority más pequeña de todos los de la red. Un root port es el puerto de cada switch de la red que está conectado al root bridge o al camino hacia éste. Un designated port es cualquier puerto que pueda transmitir pero no sea root port. Los que no son ni uno ni otro son blocked.

6.-

a) Para conseguir esa topología hay que seleccionar a S4 como root bridge y romper el enlace directo entre S1 y S2 (bloqueando un puerto). Para ello disminuimos la prioridad de S4 y aumentamos la de S1. Bloqueamos el enlace fe0 de S1. Para ello hay que reducir la prioridad de S3 un poco para que sea menor a la de S2. S4<S3<S2<S1

b) Para topología, mismas prioridades. Para enlaces, disminuir la prioridad de los enlaces que queremos a algo menor a 128.

	S1	**S2**	**S3**	**S4**
fe0	block	designated	block	designated
fe1	block	root	designated	designated
fe2	root	block	designated	designated
fe3	-	-	root	designated

c) En el caso de cada VLAN hay que poner una prioridad más baja a los puertos que queremos usar.

7.-
a) Hay que cambiar las prioridades a: S4<S2<S3<S1
Y las de los siguientes puertos a 127 (cualquier valor menor que 128): S4-fe2, S2-fe3.

b) Hay que cambiar las prioridades a: S3<S1<S4<S2.
Y las de los siguientes puertos a 127 (cualquier valor menor que 128): S3-fe2, S1-fe3.

c) Se activaría fe0. S1-S2-S4-R1.

d) Se tendría que reconfigurar el STP para que el puerto fe1 de S1 se activase y de esa forma S1 colgara de S3. S1-S3-S4-R1.

e) Se activa el router de backup (R2), el camino será S1-S2-S4-S3-R2.

f) Se activa el router de backup (R2), se reconfigura el STP de forma que S2 cuelga de S1, S1 y S4 cuelgan de S3 y S3 cuelga de R2. El camino será S1-S3-R2.

8.- Se suelen tener como mucho tantas instancias STP como VLANs, pero en casos más extremos vienen limitados por hardware, no son capaces de gestionar tantas instancias. Cada line card puede tener hasta un máximo de puertos virtuales, eso actúa como factor limitante.

9.- Integran funcionalidades de L2 con de L3 con la idea de acelerar el intercambio de paquetes IP entre VLANs. Se tiene una caché donde se almacenan las rutas y así no tiene que subir a L3 en los siguientes paquetes, va directamente por hardware, más rápido.

10.- El mecanismo de tolerancia a fallos que usamos es poner un router de backup y configurar un protocolo como VRRP. Éste hace que, si cae el enlace hacia un primer router, los paquetes circulen hacia el de backup y no se pierda la conectividad.

11.- Tiene muchas funcionalidades como detectar duplicados en @IPs, limpiar la ARP cache y las tablas de MAC de los switches. ARP request con el target con la IP origen. Todos

recibirían ese mensaje y si alguien responde es que tiene tu IP. VRRP lo usa para limpiar tablas MAC y que los paquetes vayan al nuevo router, el de backup.

12.- VRRP en esta figura es con una sola VLAN y con balanceo de cargas, Creamos una instancia VRRP con RA como master y RB como backup, y otra con los valores inversos. La idea es asignar a un subset de hosts la dirección de RA como gw principal y al subset restante asignarle RB. En el caso de que uno caiga se irá todo el tráfico al router que quede activo.

20.- 96*1/4*10 = 2.4 veces más servidores a 1Gbps de los que podemos aguantar.
40/96 = 0.4167 Gbps
Si solo 20%, 96*0.2/2*10 = 0.96
Podría soportar 100

21.- 192*0.55 = 105.6 Gb > 80 Gbps
Necesitaríamos 3 enlaces de 10 Gbps más.

TEMA 3

1.- Control son los mensajes que envían los protocolos en sí para que la red funcione, LSAs forwarding la retransmisión de paquetes en sí, forwarding, scheduling, policy (Leaky Bucket)...

2.- Dentro de AS vs entre AS, info solo de su AS vs de todos, algoritmo distinto

3.- Formato y contenido de paquetes, periodicidad, algoritmos de selección de caminos.

4.- Las clases, A, B, C, D. Sumarizar es expresar una red con subnetting como una sola, Agregar es hacer supernetting, es decir juntar 2 redes en una con un mismo Net-ID.

5.- Patricia Tree. Cogemos el primer octeto de la dirección IP, buscamos eso. Luego el segundo de entre los que empiezan por el primero, y así sucesivamente. Cuando se encuentra se acabó y si no se encuentra se envía a la que más se ha acercado. Si no, a 0.0.0.0.

6.- Propagamos LSPs a todos los routers de la red, enviando desde cada router un paquete a sus vecinos. Cuando un router recibe un LSP, compara números de secuencia y sólo el más reciente es el que se reenvía a sus vecinos. También aumenta el aging field para detectar si un mensaje es nuevo o el mismo que ha llegado por otro camino.
El flooding área vs multiárea se realiza siempre dentro de un área y no entre ellas.

7/8.- La convergencia es el estado en el cual todos los routers de la red han llegado a la misma conclusión en cuanto a la topología de la red, es decir, coinciden en esa topología.
Influencian, entre otros, número de routers, bandwidth, carga de la red, capacidad de procesamiento de los routers, protocolo utilizado, topología de la red…
En STP es cuando se han seleccionado root, designated y blocked ports. Tarda 50 segundos si tiene que pasar por los 4 estados.
Órdenes de magnitud: RIP segundos, OSPF milisegundos, BGP minutos.

9.- El primero determina el camino por el número de saltos a los que está cierto nodo (también puede añadir métricas como velocidad de los enlaces entre nodos), el segundo calcula el camino usando su topología.
Classless son los que se usan actualmente y permiten subnetting, classful no, tienen clases como RIP tiene A, B, C, D.
Vector de distancia classless: BGP

Vector de distancia classful: RIP
Estado del enlace classless: OSPF
Estado del enlace classful: -

10.- Descubrimiento de vecinos, flooding, algoritmo de mínimo coste.

11.- Descubrimiento de vecinos (HELLO), flooding (LSAs), mantenimiento de una base de datos, algoritmo de mínimo coste (Dijkstra).

12.- Definir los Router IDs y seleccionar los routers óptimos para tomar el papel de DR y BDR para hacer el flooding.

13.- 224.0.0.5 → multicast, All-OSPF-routers. 224.0.0.6 → multicast, All-DR-BDR-routers.

14.- Son los encargados de hacer el flooding de LSAs en la red y así generar la base de datos en la que se usará Dijkstra para determinar el camino de coste mínimo. Se eligen por prioridad (0 no puede ser elegido) y entre las mismas prioridades se escoge al de mayor Router ID. Si una vez seleccionados aparece en la red uno con mayor RID que el DR o el BDR, no afectará. Cuando dejan de recibir los HELLO durante 4 intervalos de tiempo, avisan a los demás routers.

15.- La escalabilidad. Tener una sola área simplemente no es posible, ya que recalcular la topología de la ruta y aplicar los algoritmos de mínimo coste consume mucho más tiempo, además de que, teniendo más nodos en la red, la probabilidad de fallo es mucho más alta. Llegar al estado de convergencia por lo tanto, sería mucho más difícil. A nivel de negocio, una distribución jerárquica permite tener equipamiento más barato hacia los límites de la red, ya que las necesidades de cálculo y velocidad son mucho menores. Los routers de gama más alta solo los necesitaremos para el centro, el *backbone*.
Tipos de router en una red OSPF:

- Internal router: todas sus interfaces en el mismo área.
- Backbone o tránsito: todas sus interfaces en el área 0 o backbone.
- Area Border Router: interfaces en más de una área, limítrofe.
- Autonomous System Boundary Router: una interfaz hacia otro AS.

16.- DR = R4; BDR = R2, R3, R1.

17.- DR = R9, R4, R5, R7; BDR = R5, R2, R4, R1.

18.- Porque si el L2 no tiene soporte para broadcast no puede funcionar el L3 con normalidad, no podría enviar mensajes a broadcast. La solución que nos ofrecen las tecnologías de L2 son circuitos virtuales uno a uno. Para que tenga efecto hay que tener una red full-meshed de circuitos virtuales, es decir, todos con todos. Si no, podría pasar que dos routers llegaran a conclusiones distintas sobre la topología de la red y sobre quién es DR y BDR.
También existe una solución más escalable que es el point multipoint, teniendo un DR y un BDR para cada par de routers. Su inconveniente es que el fabricante debe añadir soporte para esta funcionalidad, modificando el comportamiento de los HELLO para que la red converja con normalidad.

19/20/21.- Tipos de router en una red OSPF:

- Internal router: todas sus interfaces en el mismo área. Mantiene una DB.
- Backbone o tránsito: todas sus interfaces en el área 0 o backbone. Mantiene una DB.
- Area Border Router: interfaces en más de una área, limítrofe. Mantiene una DB por área.
- Autonomous System Boundary Router: una interfaz hacia otro AS. Mantiene una DB por área.

Tipos de LSA:

- Router LSA: todos los de una red. Describe link state y coste para routers internos.
- Network LSA: el DR. Describe los routers conectados a la red.
- Summary LSA: el ABR. Describe rutas externas sumarizadas.
- ASBR Summary LSA: el ABR. Describe rutas hacia ASBR.
- AS external LSA: el ASBR. Describe rutas externas de otros AS.
- NSSA external LSA: el ASBR. Describe rutas externas de otros AS para stub.

TEMA 4

1.- La política de encaminamiento es el conjunto de la política de exportación, la decisión de un AS de anunciar la ruta hacia una de sus subnets, y la política de importación, la decisión sobre qué rutas se aceptarán y añadirán a la tabla de encaminamiento.

2.- Si no se aplica filtrado, la tabla crece en rutas * AS vecinos, ya que se guarda una ruta (la mejor) por vecino.

3.- En el contexto de BGP, definir una loopback sirve para una optimización usando dummy, cada router tiene una dirección y habla con las de los demás. Al no ser una dirección asociada a una interfaz física, cuando cae un enlace físico, ese router se sigue pudiendo comunicar (mientras alguna otra interfaz conectada).

4.- Gracias a los AS-PATH vectors. Cuando un paquete circula por un AS, se añade el número del AS al vector. Si en algún momento volvemos al mismo AS, éste detectará que el número que debería poner está repetido y por lo tanto se ha generado un bucle, por lo que rechazará el paquete.

5.- Son dos variantes de BGP que se usan dentro de un AS (internal BGP) y entre AS (external BGP). La diferencia se encuentra en el anuncio de rutas, si hemos aprendido la ruta vía eBGP, la reenviaremos por eBGP e iBGP, si la hemos aprendido por iBGP, solo la reenviaremos por eBGP.

6.- OSPF anuncia las redes de su área, BGP depende de interno o externo anuncia: si hemos aprendido la ruta vía eBGP, la reenviaremos por eBGP e iBGP, si la hemos aprendido por iBGP, solo la reenviaremos por eBGP.

7.- Hay una serie de características que definen BGP
Conocido/opcional, tiene que estar implementado por el fabricante del router o no. AS path vector, origen, next hop.
Mandatorio/discrecional, atributo tiene que ser enviado en todos los updates
Transitivo/no transitivo, cuando recibe update tiene que retransmitirlo, los conocidos lo son siempre.
Completo/incompleto indica si los routers del camino han implementado los atributos.
Tipos de atributos BGP:

- WELL-KNOWN/OPTIONAL: Si todos los fabricantes deben implementarlo.
- MANDATORY/DISCRETIONAL: Si es obligatorio en un update.
- TRANSITIVE/NON-TRANSITIVE: Si debe ser forwarded.
- COMPLETE/PARTIAL: Si un opcional ha sido implementado por todos los routers por los que ha pasado el paquete.

Atributos y su tipo:

- WELL-KNOWN MANDATORY: AS PATH, Next Hop, Origin
- WELL-KNOWN DISCRETIONAL: local pref, atomic aggregate
- OPTIONAL TRANSITIVE: aggregator, community
- OPTIONAL NON TRANSITIVE: MED

8.- El atributo origen es un flag que puede ser I, E o ?. I, el atributo se generó de forma natural con el comando network, E utiliza un protocolo diferente a BGPv4, ? significa que haces una redistribución de rutas, inyecta todo lo que ha aprendido, suele ser ligado a una ACL para que no reenvíe las direcciones privadas.
9.- Aggregator + AS-SET ok, si no AS-SET, se activa atomic aggregate para detectar bucles.

10.- Mediante preferencia, Inbound decide el link de entrada, se puede regular con el MED, pero al ser no transitivo a veces es mejor usar una combinación de comunidades con LOCAL-PREF, para hacer que el otro router prefiera enviar por el enlace que quieres. Outbound decide el link de salida, se regula con el LOCAL-PREF.

11.- Significa añadir AS extra en el path vector para que a la hora de elegir mejor ruta, los demás routers no elijan esa ya que entenderán que es más larga.
Outbound → LOCAL-PREF, si ponemos un valor mayor y ambas rutas tienen un path vector del mismo tamaño, escogerá ese.

12.- NO-EXPORT: recibo ruta, no la transmito fuera del AS. NO-ADVERTISE: mando ruta y le digo que no la anuncie ni tan solo dentro del AS.

14.- IN es para la interfaz de entrada y OUT para la de salida, se modificará la tabla BGP local o la del vecino.

15.- Tiene que ser full-meshed porque eBGP se envía a iBGP y eBGP pero iBGP no se reenvía por iBGP entonces cuando llega un mensaje por eBGP a un router, se tiene que enviar directamente al router de salida del AS porque dando 2 saltos usaríamos iBGP y no se reenviaría el mensaje ya que el segundo router lo recibiría por iBGP y no por eBGP como el primero.

16.- Significa tener más de una conexión con uno o más ISP. Entonces usaremos una como predeterminada y otra como backup. El ISP determinará cuál es usando el MED desde su router, para que automáticamente nuestro tráfico vaya por el camino que prefieran. En el caso de que caiga el enlace principal, se reajustará para enviar por el backup.

17.- La sincronización está relacionada con dos problemas: primero, que si no tenemos una red full-meshed (todos los routers entre 2 routers BGP deben ser BGP) se puede dar el

caso de que hagamos una sesión BGP entre 2 routers que no están directamente conectados y los routers del camino no sepan de la existencia de la red que se pide y no envíen el paquete. Segundo, que OSPF y BGP tienen que estar sincronizados, ya que el next hop de BGP debe ser conocido por OSPF. OSPF tiene que haber anunciado antes las redes frontera.

18/19/20/21.- (n*(n-1))/2 = 4950. Confederaciones o route reflector. El primero es subdividir el AS en partes y conectarlas mediante eBGP, si dividimos la red de 100 en 3, una de 40 y dos de 30 por ejemplo, tendremos 1650 conexiones iBGP. Route reflector significa dar la funcionalidad de reenviar por iBGP los iBGP recibidos, reduciendo así la necesidad de conectar los routers 1 y 3 si el 2 es reflector.
22/28.- La escalabilidad de BGP en el caso interno viene determinada (n*(n-1))/2 (total sumar min externas), pero se puede mejorar con confederaciones o route reflectors, la sincronización es esperar a que todos los routers de un AS tengan la información antes de reenviar a otro, la convergencia es que todos los routers hayan llegado a la misma conclusión en cuanto a la topología de la red. Para cada router interno es simplemente la de su AS y las rutas que tiene que tomar para salir de éste. También se usa dampening, una técnica que consta de un valor de penalización y un threshold. Cada vez que ocurre un evento que ralentiza el proceso de convergencia, se incrementa el valor de penalización. Cuando se alcanza el threshold, el link pasa a down. Una vez pasado un tiempo, se prueba a volver a activar, y mientras ocurran eventos se irá decrementando a la mitad.

23.- Como están al mismo número de saltos, aumentando el LOCAL-PREF de la línea que quiere.

24.- RA y RB no deben saber de los caminos alternativos, por lo tanto debemos enviar con la comunidad NO-EXPORT cuando hablemos con R1 y R2, para que éstos no exporten la ruta hacia AS3.

25.- Enviaríamos la comunidad con un LOCAL-PREF mayor para R5, luego R1 y finalmente R4. 300, 200, 100.

26.- (n*(n-1))/2 para confederaciones. sum(routes por reflector) + (nr*(nr-1))/2 para RR.

29.- max penalty = reuse-limit*2^(max-suppress-time/half-life)=32.000. Suppress limit en 4 half life se reactiva el enlace.

TEMA 5

1.- El propósito de contratar una VPN es conectarse de forma segura a una red interna desde el exterior mediante un túnel encriptado. Es muy útil a la hora de teletrabajar, ya que los empleados necesitan el mismo acceso que tendrían si estuvieran físicamente en la oficina. También puede ser usada para enmascarar tu dirección IP de cara a un servidor y que éste entienda que estás en una localización que no es la real, entre otras funcionalidades.

2.- Parámetros de tráfico:

- CIR: La información que enviamos (data rate), no debe superar la capacidad del enlace. b/s
- EIR: Exceso de información por encima del CIR. peak - CIR = exceso b/s
- CBS: Tamaño de la información que enviamos. bytes
- EBS: Exceso de la información que enviamos por encima de CBS. bytes

Parámetros de QoS:

- Packet delay: Tiempo desde que un paquete abandona el punto A y llega al punto B.
- Jitter: Variación en el packet delay.
- Packet losses: ratio de paquetes perdidos sobre el total.

3.- MPLS es un protocolo de nivel 3 que redirige los paquetes mediante etiquetas que añaden e intercambian los LSR y no direcciones IP. Eso permite tener cierto control sobre los parámetros de QoS, necesarios para poder ofrecer servicios como videollamadas en condiciones, tener VPNs, optimizar los recursos de la red según la demanda, etc. Además, es independiente de la tecnología de L2.

Los paquetes siguen los caminos marcados llamados LSP, gracias a que el router interpreta la etiqueta del paquete y le pone una nueva indicando de dónde viene y que será usada por el siguiente router para determinar hacia dónde debe ser reenviado. Para determinar esos caminos mediante dos routers, se intercambian información sobre las etiquetas mediante LDP.

4.- EtherLAN es un servicio de MetroEthernet que ofrece conectividad en una arquitectura multipunto a multipunto. La diferencia entre EPLan y EVPLan es que en el primero cada UNI solo está asociado a un EVC mientras que en el segundo se permite más de un EVC por UNI pero añade la complejidad de que el usuario tiene que etiquetar los paquetes con la etiqueta VLAN para saber su destino.

5/6.- EtherLine es un servicio de MetroEthernet que ofrece conectividad en una arquitectura punto a punto. La diferencia entre EPL y EVPL es que en el primero cada UNI solo está asociado a un EVC mientras que en el segundo se permite más de un EVC por UNI pero añade la complejidad de que el usuario tiene que etiquetar los paquetes con la etiqueta VLAN para saber su destino.

7/8.- Las comunidades se usan para filtrar y asociar el tráfico a una tabla VRF, dependiendo de un identificador, las direcciones VPN-IPv4. Éstas son de 12 bytes están compuestas por un Route Distinguisher (RD) siempre de 8 bytes y una dirección de red IP de 4.
El RD puede ser generado de distintas maneras:

- Tipo 0 (2+2+4): Tipo (0) + admin (número del AS) + 4 bytes para tener 2^{16} posibilidades
- Tipo 1 (2+4+2): Tipo (1) + admin (@IP pública) + 2 bytes para tener 2^{8} posibilidades.
- Tipo 2 (2+4+2): Tipo (2) + admin (número del AS de 4 octetos, el extended) + 2 bytes para tener 2^{8} posibilidades.

9.- Para crear el túnel se exporta la ruta por BGP poniendo como next hop el loopback del router, para que el otro extremo del túnel sepa dónde tiene que enviar. Para filtrar y asociar el tráfico BGP a una tabla VRF, usamos la comunidad extendida, ya que tenemos un identificador único y podemos añadirlo a la tabla VRF y buscarlo cuando recibamos un paquete con ese destino. Para que los paquetes circulen por la red, usamos MPLS: primero el router PE le pone una etiqueta con el site y luego le empila la necesaria para dar el siguiente salto hacia un Provider router. El paquete circula por la red con MPLS, cada LSR cambiando la etiqueta externa por la necesaria para llegar al destino. Una vez ha llegado, el PE del destino desempila la etiqueta MPLS y la del site. Mirando en su tabla VRF comprueba el mismo site y reenvía ese paquete en la dirección que toque.

TEMA 6

1.- Lossless significa que la información es comprimida para ser descomprimida sin que haya pérdidas, es decir, recuperando el archivo íntegro previo a comprimir. Un ejemplo sería un ZIP. Lossy en cambio elimina parte de la información para poder comprimir más el archivo y que ocupe menos espacio, i.e. MP3.
Mecanismo Lossless → Huffman coding:

- Ordenamos los símbolos por frecuencia.
- Agregamos los 2 de menor frecuencia y le asignamos un símbolo alternativo que describe su unión. Ponemos en un árbol un nodo s_{alt} y 2 hojas s_{og}. Sumamos por

tanto las frecuencias de los dos símbolos y se la ponemos al alternativo. Ponemos el alternativo en la lista ordenada.

- Repetimos hasta que lleguemos a una frecuencia del 100%. Habremos obtenido un árbol con el que podemos determinar el código de cada símbolo original.

Mecanismo lossy → MP3:

- Recreamos el archivo pero con una frecuencia de muestreo menor. Estamos perdiendo detalle, pero para el oído humano es casi imperceptible.

2.- Los frames I son independientes, no requieren de otros frames para ser decodificados pero son menos comprimibles. En el caso de los frames P, se usa la información de frames anteriores para generar el actual, y por lo tanto son más compresibles.

3.- Sus problemas residen en el uso de RSVP. Primero, que en el core network hay que procesar miles de flows por link, y eso limita la escalabilidad. Segundo, el per-flow scheduling, que para cada paquete el router tiene que acceder al estado del flujo a tiempo real.

6/7/8.- Los mecanismos de compresión se aprovechan de la redundancia espacial y temporal del contenido multimedia. El primero, dada una matriz de píxeles, consiste en aplicarle una transformación como por ejemplo una transformada de coseno para obtener una matriz de coeficientes. Éstos los cuantizamos, por lo que perdemos algo de información pero obtenemos un dataset con muchos valores iguales, que podrán ser codificados usando Huffman y obtendremos un factor de compresión alto, ya que podremos codificar los símbolos que más se repiten con códigos de poca longitud.
El segundo hace referencia a la similitud que tienen los frames contiguos en el tiempo entre ellos. Cabe mencionar que en un contenido como un vídeo se aplican ambos, espacial y temporal. Un ejemplo: Primero obtenemos un frame de referencia que llamaremos I, que será un frame original comprimido espacialmente. A partir de éste y compensación de movimiento, generaremos un frame P que será lo que esperamos obtener. Al ser la diferencia de I, es mucho más compresible. Entre I y P, podemos generar frames B. Cada suposición agrega un % de error a la imagen, así que cada *n* frames debemos volver a coger un frame I que represente la imagen original (aunque comprimida).
GOP (Group Of Pictures) tiene 2 parámetros: M, la distancia entre frames I o P y N, el número de frames en una secuencia (de I a I).

9/14/15/16/17.- Los protocolos que pueden intervenir en una descarga de un vídeo de Internet son:

- RTSP: Signaling. Este se encarga de encontrar el contenido que pedimos y gestionar la transmisión de éste, ya sea parando o reanudando el vídeo, pidiendo un timestamp concreto, adelantar, retroceder, etc. Básicamente es un manager de la transmisión que no envía nada de datos del vídeo. Va en TCP.
- RTP: Envía el contenido en sí. Va en UDP, ya que si hay pérdidas (muy probables) no queremos que se detenga el vídeo, sino que se asuma el error y se siga.
- RTCP: Recopila datos sobre el estado de la transmisión del vídeo, como ratio de frames perdidos.
- TCP y UDP: capa de transporte.
- IP: capa de red.
- Ethernet: capa del enlace.

10/11/12/13.- IntServ implementa:

- Reserva de recursos
- Control de admisión
- Clasificación de paquetes y colas
- Políticas
- Scheduling

El problema es que no es escalable, ya que se hace a nivel de flow, y cada usuario tiene mínimo 1. Cuando el número de usuarios crece, es imposible procesar todos los datos de QoS. En el caso de DiffServ, agrupa las conexiones por similitud en clases, cada una con su SLA, y estudia el QoS de la clase en general. Es mucho más al por mayor, pero es viable en servicios masivos y por eso es el que se usa en la gran mayoría de ocasiones. Para decidir el tratamiento que se le realizará a un paquete, los core routers solo tendrán en cuenta la clase y no cada flow.