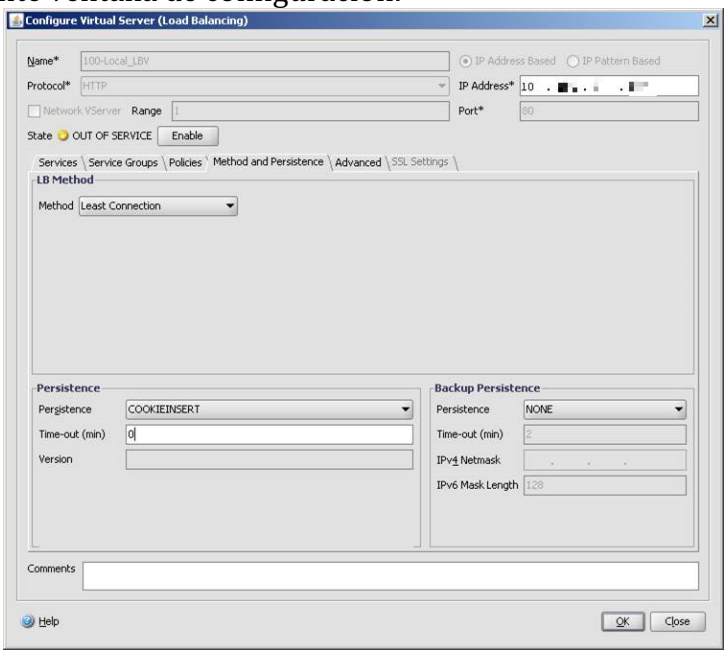
## Tema 1

1. Describa escenarios en los que resulten interesantes las nuevas versiones de Ethernet 2.5GBase-T y 5GBase-T y explique por qué.
2. 802.3br-2016 añade soporte para “preemption” en el tráfico. Explique el significado y utilidad del mismo.
3. Explique las diferencias entre el *health-tracking in-band* y *out-of-band* en balanceadores.
4. Describa servicios que se verían impactados ante un fallo de un elemento de una pareja redundante de balanceadores que emplean *sticky failover*. Explique a qué se debe el impacto sobre el servicio y valore su gravedad.
5. Muchos equipos de balanceo de carga requieren que el tráfico en ambos sentidos pase por ellos y no funcionan correctamente si solo circula uno de los dos sentidos. Explique a qué puede deberse y qué consecuencias puede tener sobre la red el requerir este encaminamiento simétrico.
6. Explique cómo emplean algunos balanceadores una funcionalidad de NAT donde cambian la dirección destino de los paquetes entrantes hacia el servicio balanceado.
7. Explique qué ventajas e inconvenientes tiene que un balanceador que hace NAT modifique en el tráfico entrante al servicio balanceado no solo la dirección destino sino también la dirección origen.
8. Un balanceador actúa como NAT sobre la dirección destino del tráfico entrante al servicio balanceado. Explique para qué puede servir que no solo modifique la dirección IP destino sino también el puerto destino.
9. Una empresa tiene un servicio tras un balanceador a nivel de red. El servicio está basado en web con SSL así que cada servidor tras el balanceador es un servidor seguro. Se están planteando descargar el trabajo de encriptación de los servidores al balanceador, con lo que las conexiones entre el balanceador y los servidores pasarían a ser no seguras. Todos los equipos se encuentran en su sala de servidores. La empresa está especialmente preocupada por la seguridad. ¿Qué le recomendaría entre mantener la solución con SSL en los servidores o desplazarla al balanceador? ¿Qué argumentos emplearía?
10. Explique la siguiente ventana de configuración:



11. Un equipo anuncia que ofrece “SSL Offloading”. Explique esta funcionalidad y dónde podría encajar este equipo en una arquitectura de un servicio web con 3 tiers.
12. Un usuario de nuestra empresa trabaja en movilidad, accediendo a un servidor de la empresa con un portátil que dispone de un módem 3G. El modem obtiene de forma dinámica una dirección IP pública del proveedor de telefonía móvil. Por parte de la empresa, el acceso a dicho servidor pasa solo por equipos de conmutación capa 2 y capa 3 desde el equipo de acceso de la empresa a su ISP. El usuario inicia una conexión TCP con el puerto 80 de ese servidor central de la empresa que tiene también una dirección IP pública. La conexión se establece correctamente y los paquetes que se observan tanto en el portátil del usuario como en el servidor son los esperados. Tras unos 10 segundos desde el establecimiento de la conexión, sin que el usuario haya mandado ningún tráfico por la misma recibe un FIN por parte del servidor, con lo que el cliente cierra también su sentido de la conexión. Ninguno de estos paquetes de FIN se ven en el lado del servidor de la empresa, para el cual la conexión sigue establecida. Un minuto después el usuario móvil inicia una nueva conexión contra el mismo servidor. El usuario móvil ve el intercambio habitual de paquetes (SYN, SYN+ACK, ACK) con el servidor. En el lado del servidor no se ve ninguno de esos paquetes. A continuación el usuario envía el contenido de una petición HTTP por la conexión TCP. Ese contenido llega al lado del servidor como paquetes de la conexión inicial. Explique qué puede estar sucediendo.
13. Los accesos a Internet de una cierta empresa se hacen siempre a través de un proxy corporativo que está configurado en los navegadores de los PCs de la empresa solo para el servicio web. No hay acceso a otros servicios. Este proxy, cuando recibe una solicitud de un URL por parte de un cliente manda esta solicitud a un firewall para que valide que puede pedir ese recurso. Esta nueva petición se hace mediante una conexión independiente entre el proxy y el firewall, que emplea un protocolo específico para este servicio (ICAP, RFC 3507). Una vez validada la petición el proxy puede establecer la conexión con el servidor remoto y obtener el recurso solicitado. Una vez obtenido el recurso web, el proxy lo envía de nuevo al firewall para que revise el contenido y autorice a entregárselo al usuario. Si obtiene la autorización enviará el recurso por la conexión por la que el cliente le ha hecho la petición. Un usuario está empleando una web que muestra cotizaciones de bolsa en tiempo real en la página web, mediante una gráfica que se va redibujando ella sola con el tiempo (mediante Javascript). El usuario dice que desde su domicilio esa web le funciona perfectamente pero no le funciona desde su puesto de trabajo en la empresa. ¿Qué puede estar sucediendo?
14. Explique el diferente comportamiento y utilidad de una cache web cerca del cliente (por ejemplo en un proxy web a la salida de la red corporativa del cliente) y una cache cerca del servidor (por ejemplo cerca del servidor web al que se solicitan los documentos).
15. Describa algunos usos que se den a TCAMs en equipos de red
16. Explique los cuellos de botella que impidan escalar un conmutador basado en memoria compartida a una elevado número de puertos de alta velocidad.
17. Un fabricante de Firewalls tiene un modelo que anuncia que “puede insertarse entre dos segmentos de red en modo router o en modo transparente”. Explique cómo interpretaría los posibles funcionamientos de ese equipo en base a esa frase y qué implicaciones podrían tener en un despliegue de red.
18. Una SAN Fibre Channel empleando la clase de servicio 3 recurre al control de flujo salto a salto (mediante básicamente una ventana deslizante) para evitar las pérdidas. Si entre dos conmutadores de la SAN se introduce un enlace fibra de 50Km de longitud explique cómo afecta este enlace a los parámetros del control de flujo.

19. Explique qué necesidades llevan a implementar colas virtuales a la salida en conmutadores.
20. Explique varios ejemplos en los que suceda un *Head-of-line blocking*.
21. ¿Tiene sentido que la capacidad de conmutación de un conmutador pueda no ser suficiente para absorber el mayor tráfico que pueda querer atravesarla? ¿Por qué sí/no?
22. Explique cómo una topología de conmutadores capa 2/3 en una granja de servidores siguiendo un esquema *leaf+spine* emplea ECMP en capa 3 y qué implicaciones tiene esta topología para al tráfico interno a cada VLAN.
23. Si las NICs de los servidores de una empresa dicen que soportan *TCP Segmentation Offload*, ¿necesitamos soporte de algún mecanismo especial en los conmutadores capa 2 y capa 3 de la red de la empresa para sacar provecho a dicho soporte? ¿Por qué sí/no?
24. En una topología de conmutadores capa 2/3 siguiendo un esquema *leaf+spine* y ECMP en capa 3 tenemos los conmutadores *spine* y los hosts que soportan *jumbo frames*, pero los conmutadores *leaf* no las soportan. ¿Se puede activar el empleo de *jumbo frames* en los hosts o habrá algún tipo de problemas de comunicación? ¿Por qué?
25. Si la NIC de un servidor soporta TCP Segmentation Offload, ¿tienen que cambiar la forma de enviar o recibir aplicaciones que empleen TCP? ¿y las que empleen UDP? ¿a qué se deben los cambios en rendimiento para las aplicaciones (si es que los hay)? ¿y para los equipos de conmutación?
26. Un conmutador Ethernet tiene en un enlace configurada una MTU de 9000 bytes y en otro una MTU de 1500 bytes. Recibe una trama de 8000 bytes por el primer enlace. Explique qué sucede si debe hacer conmutación en capa 2 hacia el segundo enlace o si debe hacerla en capa 3.
27. Un host tiene configurada en su NIC una MTU de 4000 bytes pero el switch Ethernet al que va su enlace tiene en ese puerto configurada una MTU de 1500 bytes. Expliqué qué sucederá en la comunicación. Explique qué sucede si la configuración de MTUs es la contraria.
28. Explique el funcionamiento de un posible escenario de NIC teaming en un servidor sin emplear agregación de enlaces (802.3ad o 802.1AX). ¿Qué ventajas e inconvenientes tiene de cara a fiabilidad y rendimiento?
29. Soluciones software como memcache permite implementar una cache en memoria distribuida entre múltiples hosts. Eso quiere decir que antes de buscar un recurso en un sistema de almacenamiento magnético (un disco duro) se busca en la cache, la cual no está entera en el host local que hace la pregunta sino que se encuentra repartida entre muchos hosts en la LAN. Estime los tiempos de respuesta que podría obtener si la LAN es una topología leaf+spine con enlaces 10GE a los hosts y sin bloqueo, comparándolos con los tiempos que obtendría en caso de un fallo en la cache y por lo tanto recurrir a la búsqueda en un disco local. Finalmente compare con el caso en que el sistema de almacenamiento secundario no sea local sino una SAN. Explique las hipótesis que añada en su estimación.
30. La lectura de un disco magnético incurre, entre otros, en unos tiempos de búsqueda (seek time), retardo de rotación (rotational latency) y tiempo de transferencia (transfer time). Explique cuál o cuáles de ellos se ven afectados por la velocidad de rotación del disco. ¿Qué sucede con esos retardos en el caso de un disco SSD?
31. ¿Qué nivel de RAID escogería en caso de querer implementar el almacenamiento de un proxy cache del mayor rendimiento posible? ¿Por qué?
32. Explique las diferencias entre un despliegue SAN empleando una red Fibre Channel o empleando iSCSI.

33. Enumere protocolos que den acceso a un disco a bloques frente al acceso a nivel de ficheros.
34. ¿A qué hace referencia un Arbitrated Loop en una SAN Fibre Channel?
35. ¿Un switch Fibre Channel reenvía tramas Ethernet? ¿Por qué?
36. Una red de almacenamiento ofrece acceso a los volúmenes a nivel de bloques de disco. Explique qué ventajas e inconvenientes ofrece ese tipo de acceso en comparación con un acceso a nivel de ficheros.
37. Explique cómo puede ofrecer un ahorro en consumo de electricidad y refrigeración el empleo de virtualización de hosts en el centro de datos.
38. Un hypervisor ofrece la posibilidad de bridging entre las vNIC de las máquinas virtuales que corren en el mismo y el interfaz físico del host. Explique qué consecuencias tiene este esquema para las bases de datos de filtrado de los conmutadores en un despliegue de centro de datos donde la conmutación entre todos los hypervisores sea en capa 2. ¿Y si cada host se encuentra en una LAN diferente, enrutado con el resto?
39. ¿La movilidad de máquinas virtuales suele requerir extender la VLAN de ese guest de un host al otro? ¿Qué sucede si el guest se encuentra enrutado por el host de cara a la salida hacia la LAN del centro de datos?
40. En un escenario de replicación de datos en dos sistemas de almacenamiento (para ofrecer mayor fiabilidad) se suele hablar de la posibilidad de replicación síncrona y asíncrona. Explique las diferencias y escenarios donde sea mejor cada una de ellas.
41. Un despliegue concreto de escritorio remoto entre oficinas y el centro de datos de una empresa emplea un protocolo de escritorio remoto sobre TCP. El RTT entre las oficinas y el centro de datos está por debajo de los 50ms. Explique cómo afectan las pérdidas de paquetes en la WAN a la calidad del servicio experimentada por los usuarios.
42. Una empresa emplea un despliegue de escritorio remoto donde los PCs de los usuarios son clientes de este servicio que acceden a máquinas virtuales en el centro de datos. En dichas máquinas corren un navegador web para acceder a los servicios corporativos que se encuentran en el mismo centro de datos. Explique cómo es el tráfico web que llegaría a las oficinas, tal y como se monitorizaría en su router de acceso a la WAN.
43. Explique cómo consigue el mecanismo de Priority-based Flow Control (PFC) en Ethernet que convivan el tráfico de almacenamiento y de LAN en la misma Ethernet.
44. Un centro de datos emplea sistemas de almacenamiento con iSCSI. Su topología de red es un leaf+spine con conmutación capa 3 en los ToR y spines para ofrecer ECMP y el mayor ancho de banda de bisección. Explique cómo se puede sacar provecho a PFC (Priority-based Flow Control) en este escenario.
45. Explique en qué se diferencia PFC (802.1Qbb) del control de flujo ofrecido en 802.3x.
46. ¿A qué tipo de planificadores hace referencia ETS (Enhanced Transmission Selection, 802.1Qaz) para Ethernet?
47. ¿Qué diferencias hay entre el control de congestión ofrecido por QCN en Ethernet frente al control de congestión ofrecido por TCP/IP con ECN?
48. ¿Por qué FCoE requiere una MTU mayor de 1500 bytes?
49. ¿Por qué hemos pasado de tener más tráfico norte-sur a tener más tráfico este-oeste en los centros de datos? ¿Qué consecuencias tiene esto para el rendimiento en una topología diseñada para un predominio del tráfico norte-sur?
50. Explique por qué el HOL es negativo para el rendimiento.
51. Explique las diferentes utilidades de una cache cerca del cliente o cerca de los servidores.
52. Describa cómo y por qué emplea ECMP una topología de conmutadores leaf&spine.

53. Cada cajero automático de un banco establece al arrancar una única conexión TCP con un servidor central, empleando SSL sobre ella y transportando dentro todas las consultas que necesite hacer el cajero para su operativa con los usuarios. Se emplea un par de balanceadores en activo-pasivo para repartir estas conexiones entre un conjunto de terminadores de sesiones SSL (que posteriormente dan acceso al Mainframe). Explique qué modo de funcionamiento de failover sería más adecuado para ese par de balanceadores y por qué.
54. Explique el funcionamiento de un balanceador que haga inserción de cookies.
55. Describa ventajas e inconvenientes de las jumbo frames.

## Tema 2

1. La empresa donde usted trabaja como ingeniero de red dispone de una Campus LAN corporativa. Emplea en ella direccionamiento IP privado y está aislada de Internet. Se comunica con las redes de sus proveedores y de sus clientes para llevar a cabo acciones de compra y venta (compra piezas a sus proveedores y vende productos elaborados a sus clientes). Su Campus LAN y las sedes de clientes y proveedores están físicamente alejadas. Para comunicarse con las redes de sus proveedores ha contratado una VPN con un operador. Para comunicarse con las redes de sus clientes ha contratado una segunda VPN con el mismo operador. Ha coordinado el direccionamiento IP de los equipos de su Campus LAN con el direccionamiento de los equipos de sus proveedores y clientes (al menos los que hablan entre si) para que no haya solape de direcciones. El operador emplea una L3VPN (RFC 4364) para ofrecer estas (y otras) VPNs sobre una infraestructura WAN común. El operador coloca en su Campus LAN dos routers: uno para darle acceso a una VPN y otro para darle acceso a la otra. Para anunciar rutas desde su Campus LAN a las VPNs el operador le pide a su empresa establecer dos sesiones BGP (eBGP), una entre el router frontera de su Campus LAN y el router frontera del operador de la VPN con clientes y la otra entre su router frontera de Campus y el router frontera del operador de la VPN con proveedores. En cada sesión BGP el router del operador emplea un ASN diferente (65001 para el router de la VPN de clientes y 65002 para el router de la VPN de proveedores). Su jefe le pregunta: ¿Necesitamos emplear dos ASNs, uno para cada sesión BGP o podemos emplear el mismo ASN para ambas sesiones en nuestro lado? ¿Por qué?
2. Dado un protocolo de ventana deslizante y un enlace por fibra de 100Km a 2.4Gbps calcule el tamaño en bytes mínimo que debe tener la ventana anunciada para poder mantener saturado ese enlace.
3. ¿Existen soluciones en capa 2 Ethernet que ofrezcan ECMP? Si es así descríbalas brevemente y si no diga por qué cree que no existen.
4. ¿Pueden emplearse los múltiples enlaces de una topología leaf+spine con alguna solución Ethernet previa a SPB?
5. ¿En qué se diferencia un esquema de protección 1+1 con un esquema 1:1?
6. ¿Por qué SDH no puede ofrece una clase de servicio similar al rt-VBR ofrecido en una red ATM?
7. Se dice que ATM ofrece mayor “granularidad” a la hora de la reserva de recursos para un PVC en comparación con el caso para un circuito en una red SDH. Expliqué a qué se hace referencia.

8. En un dominio MPLS, si se dispone del protocolo LDP, ¿hace falta un protocolo de encaminamiento interno como por ejemplo OSPF? Si es así, explique por qué y para qué y si no explique por qué no hace falta.
9. ¿Qué añade GMPLS a MPLS?
10. La empresa en que trabaja es un sistema autónomo de la Internet con enlaces a varios ISPs (un enlace con cada ISP). Describa técnicas para hacer ingeniería de tráfico mediante BGP y controlar por qué enlace recibe el tráfico que va a algunas de sus redes. ¿Puede controlarlo por subred destino o aplicaría a todos los prefijos públicos de su empresa?
11. Explique para qué se emplea el atributo AS_PATH en los anuncios BGP.
12. Los routers frontera de un sistema autónomo que emplean BGP con sistemas autónomos vecinos añaden su ASN al AS_PATH de los prefijos que anuncian solo cuando hacen dichos anuncios a router de otro AS. ¿Cómo se evitan bucles si en los anuncios internos entre los routers BGP del mismo AS no se añade al ASN al AS_PATH?
13. Un AS tiene 80 routers frontera que emplean BGP. Explique cuántos vecinos BGP tiene cada uno de esos routers frontera, según se esté empleando un reflector de rutas interno al AS o no.
14. Una pequeño ISP posee un Provider Independent Address Space IPv4. Ha contratado un enlace con un ISP Tier-1 que le provee acceso a la Internet global. Por otro lado tiene acuerdos particulares con otros dos ISPs en respectivos IXPs donde intercambian tráfico sin coste. Explique brevemente lo que pueda recomendar para la configuración de BGP de los routers frontera de este ISP en base a esta información.
15. Explique cómo se logra ofrecer un servicio anycast con la ayuda de BGP.
16. Un ISP nacional hace intercambio de tráfico IP con dos proveedores y tres peers. Si ya se emplea un protocolo de encaminamiento (BGP) para el aprendizaje de las rutas de la Internet pública, ¿necesita el ISP emplear un protocolo de encaminamiento interior? ¿por qué? ¿en qué casos?
17. Una empresa tiene varias sedes, interconectadas mediante una L3VPN (RFC 4364) ofrecida por un ISP. En una de las sedes existe un host donde existen varios contenedores para ofrecer ciertos servicios. En otra de las sedes existe un host idéntico al anterior, con contenedores para ofrecer backup de cada uno de esos servicios. Todos los contenedores de uno cualquiera de los hosts están conectados a un vSwitch creado por el host. El host enruta la LAN creada por el vSwitch hacia su única NIC. Esa NIC está conectada a un switch físico, en un puerto en trunking 802.1Q. El routing se hace hacia el interfaz virtual del host en la VLAN 100 en una de las sedes mientras que en la otra se hace hacia la VLAN 200. La VLAN 100 existe solo en la primera sede y la 200 solo en la segunda. Cada VLAN emplea una subred IP diferente. Se desea que los contenedores de la primera sede y de la segunda se encuentren en el mismo dominio capa 2, dado que lo requiere el protocolo para el failover de las aplicaciones que se ejecutan en los mismos. Los administradores se plantean crear un túnel GRE para transportar las tramas Ethernet de la LAN de los contenedores entre los dos vSwitch. Haga un esquema de red lo más claro posible de lo que se ha descrito. Evalúe si esta solución es factible o qué problemas podrían aparecer. Compare con la posibilidad de emplear VXLAN en la interconexión.
18. Una empresa está desplegando internamente una solución L3VPN (RFC 4364) para separar mediante VRF el tráfico de diferentes departamentos de la misma. Ha contratado a una empresa externa para que lleve a cabo todo el despliegue. Una vez que la gestión de los equipos de red recae sobre el personal de IT de la empresa, en el cual

usted trabaja, descubre que los routers core del nuevo despliegue emplean un protocolo llamado LDP. ¿Por qué? ¿Para qué?

19. Explique por qué para implementar una L3VPN (RFC 4364) ha sido necesario crear un nuevo address family.
20. Compare el plano de control de una L3VPN donde se aprenden rutas VPN-IPv4 con el plano de control en un escenario VPLS para el aprendizaje de direcciones MAC.
21. Tome un switch ATM que está actuando como un LSR MPLS. No se puede emplear como punto de agregación de un LSP multipunto-a-punto, es decir, como punto en el que varias ramas del multipunto se unen. ¿Por qué puede ser? Recuerde cómo se produce la segmentación y reensamblado de la PDU AAL5 en celdas ATM. ¿Qué tendría que ser capaz de hacer el switch ATM para poder ofrecer esta funcionalidad?
22. Si una empresa emplea una L3VPN para interconectar sus sedes, ¿puede emplear OSPF para calcular rutas entre las subredes de todas sus sedes? ¿Por qué? ¿Y si la interconexión es mediante una L2VPN?
23. Explique esta afirmación: "En una EVPN el aprendizaje de direcciones MAC entre PE y CE se lleva a cabo en el plano de datos mientras que entre PE y PE se hace en el plano de control."
24. Un fabricante vende una tecnología para una L2VPN que según dice es "una EVPN con el plano de datos VXLAN". Explique en un poco más detalle cómo puede funcionar esa L2VPN.
25. Tanto LDP como RSVP-TE se pueden emplear para la creación de LSPs en una red MPLS. En el caso de querer hacer ingeniería de tráfico para esos LSPs entonces lo normal es verse obligado a emplear RSVP-TE. Teniendo en cuenta que RSVP-TE consiste en una serie de extensiones a RSVP explique a qué se debe esta situación.
26. Explique las diferencias entre una sesión BGP externo y BGP interno.
27. ¿Qué protocolo emplea TRILL como sustituto de STP y qué mejoras obtiene con ello?
28. Explique por qué en una trama TRILL con datos de usuario nos encontramos con 4 direcciones MAC.
29. Cuando un RBridge en un dominio TRILL recibe una trama con este encapsulado, explique cómo se diferencia el uso que hace de la dirección MAC origen en la trama, el Egress RBridge Nickname en la misma y la dirección MAC destino en la trama encapsulada según el RBridge sea o no el de egreso para dicha trama.
30. Acceda al contenido de la Especificación funcional y desarrollo del Nuevo Servicio Ethernet de Banda Ancha (NEBA), que puede descargar de: http://www.movistar.es/operadores/ServiciosRegulados/ficha/PRO_NEBA?paramPestania=soporte&posicionScroll=0 ¿Qué tipo de DSLAM son compatibles con este servicio? ¿Qué tipo de paquetes se transportan entre el usuario y el punto de acceso indirecto? ¿Qué tipo de tecnología FTTH parece emplearse según el documento? Comente el diferente encapsulado para accesos ADSL2+ frente a accesos VDSL2, especialmente preste atención a la capa existente entre Ethernet y xDSL.
31. Explique las diferentes técnicas implementadas en SPB para poder hacer balanceo de carga.
32. Explique en qué se diferencia el uso que se hace de las direcciones MAC más externas de la trama Ethernet entre un dominio SPBM, uno SPBV y uno TRILL.
33. Explique la utilidad de dos etiquetas MPLS en una L3VPN (RFC 4364).
34. Explique un ejemplo de prefix hijacking en BGP.
35. Describa el proceso de aprendizaje en el plano de datos en VXLAN.
36. Enumere equipos de red que sea virtualizables en un despliegue NFV y busque ejemplos comerciales de los mismos.

## Tema 3

1. Compare la funcionalidad de un Media Gateway Controller en un despliegue VoIP y de un controlador en una SDN.
2. Describa estrategias que servirían para reducir la posibilidad de un colapso por Incast
3. Explique si Multipath TCP (MPTCP) puede funcionar o no cuando hay un NAT en el camino entre los extremos.
4. QUIC se implementa en la aplicación, empleando como protocolo de transporte UDP. Explique las implicaciones que tiene para la estructura de proxies web y firewalls de una empresa el que los navegadores de los usuarios empleen QUIC.
5. ¿Necesita HTTP/2 soporte para enviar *Cookies* en la cabecera HTTP?