Cambios recientes a nivel físico en 802

1. Describa escenarios en los que resulten interesantes las nuevas versiones de Ethernet 2.5GBase-T y 5GBase-T y explique por qué.
2. ¿Un punto de acceso inalámbrico 802.11ac con un interfaz cableado 2.5GBase-T tiene suficiente tasa de transferencia en el interfaz cableado para cursar el máximo tráfico que pueda recibir por el interfaz inalámbrico? ¿Y si fuera 802.11n en vez de 802.11ac?
3. ¿Qué tipo de cableado requiere una Ethernet a 2.5 Gb/s?
4. 802.3br-2016 añade soporte para “preemption” en el tráfico. Explique el significado y utilidad del mismo.
5. ¿El tráfico "express" descrito en 802.3br es lo mismo que el tráfico "preemptable"?
6. Describa diferencias entre WiFi 4, WiFi 5, WiFi 6 y WiFi 6E.
7. Describa mejoras ofrecidas por equipos 802.11ac wave 2 frente a los wave 1.
8. Describa diferencias entre WiFi6 y WiFi6E.
9. Explique a qué se debe que en redes inalámbricas 802.11 el throughput esperado que se pueda conseguir pueda caer hasta el 70% respecto a la tasa de transmisión.
10. Explique qué ventajas presenta una tecnología 802.11 con soporte de MU-MIMO frente a una con solo SU-MIMO.
11. Describa escenarios en los que considere que resulten apropiadas para su uso las nuevas versiones de Ethernet 2.5GBase-T y 5GBase-T y explique por qué.

Ethernet es capa 2

1. ¿Por qué normalmente la PDU de un protocolo de capa 3 orientado a datagramas incluye un contador de tiempo máximo de vida o número máximo de saltos pero la trama Ethernet no lo incluye?
2. ¿Qué información contiene la cabecera de una trama Ethernet 802.3?

Arquitectura y elementos

1. Explique las diferencias entre un "scale-out" y un "scale-up" de servidores.
2. Describa un servicio para el que tenga más sentido un "scale-up" que un "scale-out".
3. En una arquitectura de un servicio con un frontend web con contenido estático y un backend donde se ejecute la lógica de aplicación explique qué características podría tener el servicio para que interesara hacer un scale-out del frontend antes que un scale-out del backend.

Introducción a los Datacenters

1. ¿A qué puede deberse la decisión en un centro de datos de añadir gran cantidad de servidores de potencia media en lugar de unos pocos de gran potencia para aumentar la capacidad de dar servicio?
2. Describa ventajas e inconvenientes del hosting de los servidores de una empresa en un data center gestionado por la misma empresa o en un data center de otra empresa donde contrate algún tipo de servicio de hosting (estas ventajas e inconvenientes pueden depender del tipo de servicio contratado).
3. Describa los tipos de redundancia de alimentación eléctrica que nos podemos encontrar para los equipos en un centro de datos.
4. Describa brevemente la problemática asociada a la refrigeración en un centro de datos.
5. Explique ventajas e inconvenientes de la centralización de los servidores de la empresa en una *Computer Room* frente a tenerlos distribuidos por las salas donde se encuentren los grupos de trabajadores de cada departamento de la empresa.

6. Opine y argumente sus opiniones sobre las ventajas e inconvenientes de un esquema de cableado Top-of-Rack y uno End-of-Row.

Diseño clásico del data center

1. Explique cómo una topología de conmutadores capa 2/3 en una granja de servidores siguiendo un esquema de 2 capas (switches de acceso y distribución) emplea ECMP en capa 3 y qué implicaciones tiene esta topología para al tráfico interno a cada VLAN.
2. ¿Serviría RIP como protocolo de encaminamiento en un escenario de red donde queremos emplear ECMP (por ejemplo una topología leaf+spine)? ¿Serviría OSPF? ¿IS-IS? ¿MSTP? ¿Por qué?
3. En una topología leaf+spine donde todos los conmutadores son capa 3 (IPv4) y se hace balanceo de carga entre los caminos que van por los distintos conmutadores del spine, describa motivos por los que el reparto de tráfico por los diferentes caminos se hace a nivel de flujo y no de paquete.

NICs

1. 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?
2. 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?
3. 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?
4. 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?
5. 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.
6. 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. Explique qué sucederá en la comunicación. Explique qué sucede si la configuración de MTUs es la contraria.
7. Describa las ventajas e inconvenientes del empleo de jumbo frames dentro de la red de una empresa tanto en los casos de comunicación entre las máquinas de la LAN Ethernet como de comunicación con máquinas fuera de esa LAN (enrutado).
8. Explique el mecanismo RSS (Receive Side Scaling) en NICs.
9. Describa funcionalidades que implementen algunas NICs para acelerar la comunicación descargando de trabajo a la CPU.

Virtualización

1. Explique cómo se ofrece un ahorro en consumo de electricidad y refrigeración mediante el empleo de virtualización de hosts en el centro de datos.
2. Explique diferencias entre un hipervisor de tipo 1 y uno de tipo 2.
3. Describa ventajas e inconvenientes de la virtualización de host.

Almacenamiento

1. 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?
2. ¿Qué nivel de RAID escogería en caso de querer implementar el almacenamiento de un proxy cache del mayor rendimiento (en velocidad y tiempo de respuesta) posible? ¿Por qué?
3. Compare las consecuencias del fallo de un disco entre un RAID 0, un RAID 1, un RAID 1+0 y un RAID 0+1.
4. Explique qué solución de RAID escogería para el almacenamiento de un proxy cache y por qué.
5. Describa y explique las diferencias entre un RAID 1 y un RAID 5.
6. Explique de qué orden de magnitud son los tiempos de acceso a discos mecánicos rotacionales y a qué se debe.

SAN

1. 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 L Km de longitud explique cómo afecta este enlace a los parámetros del control de flujo.
2. Explique las diferencias entre un despliegue SAN empleando una red Fibre Channel o empleando iSCSI.
3. ¿A qué hace referencia un Arbitrated Loop en una SAN Fibre Channel?
4. ¿Un switch Fibre Channel reenvía tramas Ethernet? ¿Por qué?

NAS y virtual storage

1. Enumere protocolos que den acceso a un disco a bloques frente al acceso a nivel de ficheros.
2. 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.
3. 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.
4. Evalúe la diferencia de coste entre una instalación de almacenamiento en red NAS o una SAN en una nueva empresa.
5. 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.
6. Explique las diferencias, ventajas y desventajas de una solución de almacenamiento basada en SAN o en NAS.

Virtualización (2)

1. La movilidad de máquinas virtuales suele requerir extender la VLAN de ese guest de un host al otro para el correcto funcionamiento de su acceso a red tras el movimiento de la máquina virtual. ¿Qué sucede si el guest se encuentra enrutado por el host de cara a la salida hacia la LAN del centro de datos?
2. 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 que llegaría a las oficinas, tal y como se monitorizaría en su router de acceso a la WAN.
3. 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 cerca de los 20ms. Explique cómo afectan las pérdidas de paquetes en la WAN a la calidad del servicio experimentada por los usuarios.
4. Suponga un despliegue de escritorios remotos basado en RDP donde los usuarios trabajan en su ordenador local a través, exclusivamente, de la aplicación cliente de escritorio remoto. El servidor el escritorio se ofrece a cada usuario a partir de una VM exclusiva para él. El disco de dicha VM se crea en el host cada vez que se arranca, copiándose de una plantilla guardada en una SAN. Al arrancar cada vez de una copia de la plantilla cualquier infección se resuelve apagando la máquina pues ésta se destruye y la próxima vez se creará de nuevo. Esta VM emplea un sistema operativo Windows donde la carpeta de Documentos del usuario se almacena en un disco en red (un NAS) montado por este Windows y algunas aplicaciones se encuentran instaladas en otro disco en red (otro volumen ofrecido por el mismo NAS, el acceso al NAS se hace empleando SMB). Esto permite que la VM pueda arrancar cada vez con una instalación limpia pero el usuario tenga sus documentos. Por otro lado, el disco en red con aplicaciones permite añadir software a los usuarios sin tener que modificar la plantilla, solo con dejarlo en dicho volumen. En este escenario describa los diferentes flujos de tráfico que se puede encontrar entre la LAN de usuarios y el datacenter, dentro del datacenter y con el exterior cuando un nuevo trabajador arranca su sesión de escritorio remoto y emplea diferentes aplicaciones (como procesadores de texto, navegadores web, etc) que pueden estar en la instalación de la plantilla o en el disco de aplicaciones.
5. Explique el aislamiento que proveen las VRFs.
6. Un despliegue concreto de escritorio remoto lanza instancias virtuales en un centro de datos que actúan como los escritorios compartidos mientras los usuarios se encuentran distribuidos por la geografía del país empleando diferentes redes de acceso hasta el centro de datos. El RTT entre los usuarios y el centro de datos varía según el usuario entre 1ms y 5ms. Los servicios accedidos por los usuarios se encuentran en el mismo centro de datos, en otras máquinas, por lo que la comunicación es interna al centro de datos. Discuta los diferentes efectos de pérdidas de paquetes en las redes de acceso o dentro del centro de datos, principalmente desde el punto de vista del usuario y qué problemas percibirá en el servicio.
7. Se lleva a cabo en despliegue de escritorios virtuales remotos en una infraestructura de nube privada donde estos escritorios provienen de máquinas virtuales Windows corriendo sobre un hypervisor tipo 1 y empleando RDP en el propio guest para el acceso al escritorio remoto. Los usuarios emplean estos escritorios para acceder a servicios corporativos que se encuentran en una granja de servidores localizada en otro centro de datos y a la que el tráfico llega enrutado a través de una L3VPN. Cada máquina virtual es empleada por un único usuario a la vez. Una máquina se arranca cuando el hypervisor

recibe tráfico RDP (intento de conexión TCP) hacia la VM concreta. El hipervisor enruta para las VMs, estando cada una en un segmento de red independiente con direccionamiento con prefijo de 30 bits. El hypervisor implementa reglas de filtrado capa 3. Argumente si el filtrado en los hypervisores debería o no permitir y establecimiento de conexiones TCP originadas en las VMs hacia el exterior del host y por qué.

Virtualización (3)

1. Explique por qué un contenedor en un host Linux debe ser también una distribución de Linux.
2. Explique por qué una virtualización basada en contenedores requiere menos recursos del host que una solución basada en un hipervisor de tipo 1 o de tipo 2.
3. Explique diferencias entre *System Containers* y *Application Containers*.
4. Se quieren instanciar varias decenas máquinas virtuales Linux sobre un host con una sola CPU y 32 GB de RAM. Entre un hypervisor tipo 1, tipo 2 o una virtualización basada en contenedores explique qué alternativa escogería y por qué.
5. Un host H1 basado en GNU/Linux implementa un vSwitch S1a y un vSwitch S1b. En el host se crean los contenedores A1, B1, C1, D1 y E1. Cada uno de estos contenedores tiene un interfaz Ethernet virtual. Los contenedores A1, B1 y C1 están conectados a S1a con su interfaz Ethernet virtual mientras que D1 y E1 lo están a S1b. El host H1 posee una NIC física 10GE, conectada a un conmutador en una VLAN en concreto (sin encapsulado de trunking en ese puerto). El host H2 tiene una configuración similar a H1, con unos contenedores A2, B2, C2, D2 y E2 y unos vSwitches S2a y S2b; además se encuentra su NIC en una VLAN diferente. Ambos hosts tienen sus interfaces físicos configurados con direcciones IP de subredes diferentes (subredes H1s y H2s respectivamente). Entre ambos hosts existe conectividad IP con soporte para routing multicast IP. Los vSwitches S1a y S2a se enlazan mediante un túnel GRE. Los vSwitches S1b y S2b se intentan enlazar mediante otro túnel GRE. Los contenedores A1, B1, C1, A2, B2 y C2 tienen sus interfaces de red configurados con direcciones IP de la subred X mientras que los contenedores restantes están configurador con direcciones IP de la subred Y. Haga un esquema gráfico que muestre el escenario de red descrito de la forma más clara posible. Explique, en este escenario, entre qué contenedores se puede enviar tráfico IP, qué problemas puede encontrarse para crear este escenario y por qué. Describa el tráfico que se encontrará atravesando cada túnel GRE (tipo, cabeceras, etc).
6. La LAN Ethernet de una pequeña sala de servidores se encuentra compuesta por un conmutador Ethernet capa 2 y 2 hosts. El primero de ellos (host1) emplea una versión del sistema operativo Microsoft Windows. El segundo de ellos (host2) emplea una distribución de GNU/Linux. Host1 tiene instalado VirtualBox y una sola máquina virtual creada sobre este hypervisor. Esta máquina virtual (vm1) tiene instalada una distribución de GNU/Linux con una sola vNIC configurada. La vNIC de vm1 se configura en VirtualBox para estar puenteada a la NIC física de host1. En vm1 se han creado 2 contenedores (cA y cB) y un puente software (br0). La vNIC de vm1 se ha movido al namespace de red de cB. Se ha creado una pareja de veth, de los cuales uno (veth-cBin) se ha configurado en el namespace de cB y el otro (veth-cBout) se ha dejado en el namespace global. Con esto cB tiene dos interfaces de red; se ha activado el reenvío de paquetes entre ellos. El veth-cBout se añade al puente br0. Se crea una nueva pareja de veth, de los cuales uno de ellos (veth-cAout) se añade también al puente br0 mientras que el otro (veth-cAin) se configura en el namespace del cA. En host2 se han creado 5 contenedores (cC, cD, cE, cF y cG). Se han creado dos puentes en el sistema operativo

(br1 y br2). El interfaz de host2 correspondiente a su NIC física se ha añadido a br2. Se ha creado una pareja de veth, de los cuales uno (veth-cCin) se ha configurado en el namespace de cC y el otro (veth-cCout) se ha añadido al puente br1. Se ha creado otra pareja de veth, de los cuales uno (veth-cDin) se ha configurado en el namespace de cD y el otro (veth-cDout) se ha añadido al puente br1. Se ha creado otra pareja de veth, de los cuales uno (veth-cEin) se ha configurado en el namespace de cE y el otro (veth-cEout) se ha añadido al puente br2. Se ha creado otra pareja de veth, de los cuales uno (veth-cFin) se ha configurado en el namespace de cF y el otro (veth-cFout) se ha añadido al puente br2. Se ha creado otra pareja de veth, de los cuales uno (veth-cGin) se ha configurado en el namespace de cG y el otro (veth-cGout) se ha configurado en el namespace de cF. Se ha activado el reenvío de paquetes IP en cF. Todos los hosts con un interfaz en un dominio capa 2 (LAN) tienen configurada dirección IP en la misma subred, correspondiente a ese dominio capa 2. Haga un esquema gráfico que muestre el escenario de interconexión de equipos físicos y virtuales descrito de la forma más clara posible, incluida la pertenencia de cada solución de virtualización a su host correspondiente (del estilo de los esquemas vistos en las prácticas 1 y 2). Haga un esquema de red capa 3, donde aparezcan los hosts, routers y subredes (un esquema del estilo de los vistos en asignaturas tipo Redes de Ordenadores), incluyendo una propuesta de direccionamiento IP para todos los interfaces. ¿Cómo podría conseguir que los contenedores cA, cB, cC y cD se encontraran en el mismo dominio capa 2?.

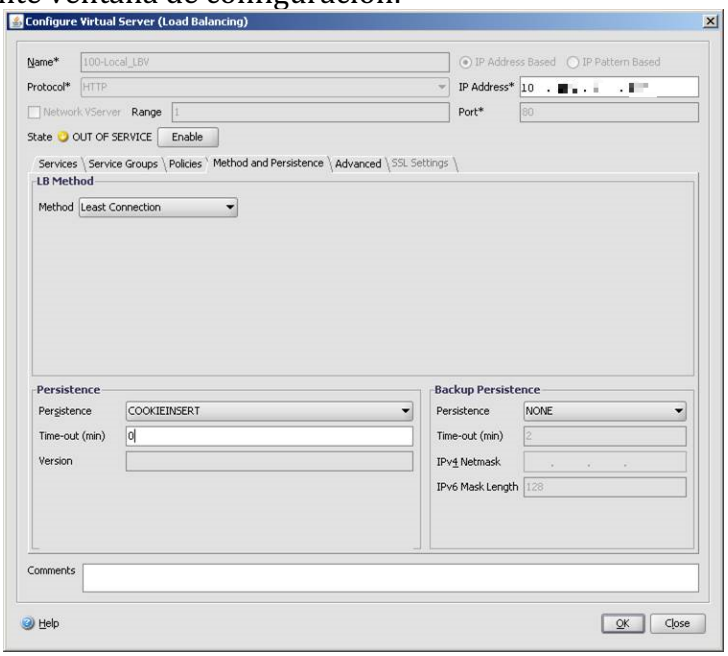
Overlays y VXLAN

1. Describa el proceso de aprendizaje en el plano de datos en VXLAN.
2. Explique en qué se diferencia GRE de NVGRE.
3. Si dos máquinas virtuales están en la misma overlay, ¿pueden tener sus NIC virtuales la misma dirección MAC? ¿Y si están en distintas? ¿Qué es lo que lo permite o impide?
4. Explique ventajas de túneles GRE frente a túneles IP sobre IP.
5. Explique ventajas de overlays VXLAN frente a una topología con túneles GRE que transportan tramas Ethernet entre vSwitches.
6. Explique qué soluciones de túneles y overlays y por qué, permiten sacar provecho de ECMP en la underlay y cuáles no.
7. En una overlay, ¿la overlay tiene o puede tener protocolos del plano de control? Argumente la respuesta.

Balanceadores

1. Explique las diferencias, ventajas e inconvenientes entre el *health-tracking in-band* y *out-of-band* en balanceadores.
2. Describa servicios (aplicaciones) que requieren balanceadores que empleen sticky failover para no verse impactados ante un fallo de un elemento de una pareja redundante de balanceadores. Explique a qué se debe el impacto sobre el servicio y valore su gravedad.
3. 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.
4. Explique cómo emplean algunos balanceadores una funcionalidad de NAT donde cambian la dirección destino de los paquetes entrantes hacia el servicio balanceado.

5. 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.
6. Ante un balanceador que 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.
7. Explique el funcionamiento de un balanceador que haga inserción de cookies.
8. Explique las diferencias entre tipos de failover entre balanceadores en función de la información de estado que guarden y compartan.
9. Compare el tráfico entre el usuario y un balanceador frente a la misma petición del balanceador al servidor seleccionado entre que el balanceador actúe como NAT de la dirección del servidor o actúe como Proxy.
10. 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?
11. Explique la siguiente ventana de configuración:



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. 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.
14. La figura siguiente está extraída de la hoja de características de un balanceador. Explique a qué cree que hace referencia cada uno de los parámetros mostrados. No se limite a traducirlos, debe explicar a qué tipo de comportamiento cree que se refieren y qué implican.

Performance	Maximum*
L7 requests per second	450,000
L4 connections per second	135,000
Throughput	10 Gbps**
Maximum connections	10 million

15. Explique por qué si un balanceador hace NAT de la dirección del servidor para llevar a cabo el reparto entre los servidores físicos es necesario que el tráfico de vuelta pase por el mismo balanceador. En caso de que el balanceador haga NAT solo de la dirección de cliente y el reparto entre los servidores lo haga mediante mecanismos de capa 2 (cambiando la dirección MAC destino para mandar el paquete a cada servidor) explique si es necesario que el tráfico de vuelta pase también por el balanceador y por qué.

Otros servicios

1. 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.
2. 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).
3. Explique las diferentes utilidades de una cache cerca del cliente o cerca de los servidores.
4. 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?

5. 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.

I/O consolidation

1. 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.
2. Explique en qué se diferencia PFC (802.1Qbb) del control de flujo ofrecido en 802.3x.
3. ¿A qué tipo de planificadores hace referencia ETS (Enhanced Transmission Selection, 802.1Qaz) para Ethernet?
4. ¿Qué diferencias hay entre el control de congestión ofrecido por QCN en Ethernet frente al control de congestión ofrecido por TCP/IP con ECN?
5. ¿Por qué FCoE requiere una MTU mayor de 1500 bytes?
6. 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.

Limitaciones y escalabilidad en topología del data center

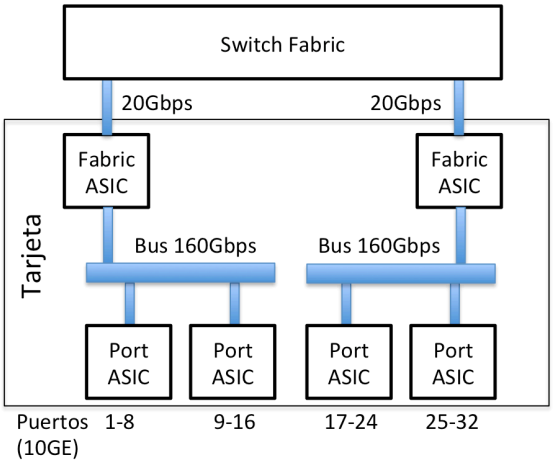
1. Un hypervisor ofrece la posibilidad de bridging entre las vNIC de las máquinas virtuales que corren en el mismo y el interfaz físico del host. Explique qué consecuencias tiene este esquema para las bases de datos de filtrado de los conmutadores en un despliegue de centro de datos donde la conmutación entre todos los hypervisores sea en capa 2. ¿Y si cada host se encuentra en una LAN diferente, enrutado con el resto?
2. ¿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?
3. Dispone de un solo modelo de conmutador para data center. Este modelo cuenta con 48 puertos 10GE y 6 puertos 40GE, es capaz de crear hasta 8 LAGs con hasta 8 puertos cada uno y es capaz de hacer ECMP con hasta 16 caminos alternativos. Diseñe una topología de data center basada en ECMP empleando dos capas de conmutadores de este modelo. Describa (y si puede dibuje) la topología para obtener al menos 140 puertos 10GE con el menor coste por puerto (es decir, el menor cociente nºconmutadores/nºpuertos). Indique claramente el número de conmutadores en cada capa, así como cuántos puertos y de qué tipo se orientan en la capa de acceso hacia hosts y cuántos hacia la capa de agregación. En caso de no poder lograr el diseño explique por qué.
4. Describa cómo y por qué emplea ECMP una topología de conmutadores leaf&spine
5. Dispone de un solo modelo de conmutador para data center. Este modelo cuenta con 48 puertos 10GE y 6 puertos 40GE, es capaz de crear hasta 8 LAGs con hasta 8 puertos cada uno (de igual velocidad en el mismo LAG) y es capaz de hacer ECMP con hasta 16 caminos alternativos. Diseñe una topología de tipo Leaf&Spine para el data center basada en ECMP empleando conmutadores de este modelo. Describa (y si puede dibuje) la topología para obtener al menos 140 puertos 10GE con el menor coste por puerto (es

decir, el menor cociente Coste_conmutadores/nºpuertos). Indique claramente el número de conmutadores en cada capa, así como cuántos puertos y de qué tipo se orientan en la capa de acceso hacia hosts y cuántos hacia la capa de agregación. En caso de no poder lograr el diseño explique por qué. Suponga que el precio de uno cualquiera de esos conmutadores está en el rango de unos pocos miles de euros.

6. Explique para cada uno de estos protocolos si es adecuado o no y por qué para obtener reparto de carga entre múltiples caminos en una topología leaf+spine con conmutadores capa 3: OSPF, MSTP, IS-IS, RIP.

Arquitectura de conmutadores

1. Describa algunos usos que se den a TCAMs en equipos de red
2. Explique los cuellos de botella que impidan escalar un conmutador basado en memoria compartida a un elevado número de puertos de alta velocidad.
3. Explique qué necesidades llevan a implementar colas virtuales a la salida en conmutadores.
4. Explique varios ejemplos en los que suceda un Head-of-line blocking.
5. ¿Tiene sentido diseñar un conmutador en el que la capacidad de conmutación del mismo no sea suficiente para absorber el mayor tráfico que pueda querer atravesarlo? ¿Por qué sí/no?
6. Explique por qué el HOL es negativo para el rendimiento.
7. Explique la diferencia en la funcionalidad ofrecida por una CAM y una TCAM y para qué se emplean dentro de chips de conmutación de paquetes.
8. Enumere y describa brevemente funcionalidades de un switch Ethernet/IP (multilayer) que se implementan o bien en el ASIC o en una CPU y por qué.
9. Suponga que una tarjeta de puertos para un conmutador Ethernet modular tiene la arquitectura interna aproximada que se muestra en la siguiente figura. Razone las hipótesis que plantee sobre el funcionamiento de dicha tarjeta y con ello explique dónde considera que existen cuellos de botella (si es que los hay). Suponiendo que existen varias tarjetas de este tipo en el conmutador explique brevemente cómo sería el camino que sigan los paquetes por dentro del conmutador entre un puerto de una tarjeta y un puerto de otra tarjeta si el esquema de decisiones de reenvío es centralizado en una tarjeta controladora o si las decisiones se toman de forma distribuida.



10. ¿La fragmentación de paquetes IP se lleva a cabo en el ASIC o en la CPU?

TRILL

1. ¿Qué protocolo emplea TRILL como sustituto de STP y qué mejoras obtiene con ello?

2. Explique por qué en una trama TRILL con datos de usuario nos encontramos con 4 direcciones MAC.
3. 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.
4. Explique ventajas de TRILL frente a STP.

SPB

1. Explique las diferentes técnicas implementadas en SPB para poder hacer balanceo de carga.
2. 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.
3. Enumere similitudes y diferencias entre TRILL y SPB.
4. Describa diferencias entre un despliegue TRILL y uno SPBM (Shortest Path Bridging MAC Mode)
5. Explique qué utilidad administrativa tiene el hacer *reflective relay* en un conmutador cuando el hypervisor está comportándose como un *Virtual Edge Port Aggregator* (VEPA) en lugar de un *Virtual Edge Bridge* (VEB).

SDN y OpenFlow

1. Explique a qué se llama en SDN un protocolo *Southbound* y uno *Northbound*.
2. Dado el modelo de tablas y acciones empleado por OpenFlow explique para qué tipo de conmutadores está diseñado (¿capa 2 Ethernet? ¿capa 3 IP?)

NFV

1. Enumere equipos de red que sea virtualizables en un despliegue NFV y busque ejemplos comerciales de los mismos.
2. Explique ventajas e inconvenientes de la sustitución en un ISP de equipos por su alternativa NFV

MPLS y GMPLS

1. ¿Qué añade GMPLS a MPLS?
2. 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.
3. Explique qué utilidad puede tener configurar PHP (Penultimate Hop Popping) en un LSP MPLS.
4. Describa un escenario en el que un paquete MPLS llegue a tener 3 etiquetas en su pila.

BGP

1. 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?
2. Explique para qué se emplea el atributo AS_PATH en los anuncios BGP.
3. 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?
4. 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.
5. Explique cómo se logra ofrecer un servicio anycast con la ayuda de BGP.
6. Explique las diferencias entre una sesión BGP externo y BGP interno.
7. Explique un ejemplo de prefix hijacking en BGP.
8. Un 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.
9. 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?

L3VPNs y L2VPNs

1. Explique por qué para implementar una L3VPN (RFC 4364) ha sido necesario crear un nuevo address family.
2. 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.
3. 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?
4. 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."
5. 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.
6. Describa el proceso de aprendizaje en el plano de datos en VXLAN y compárelo con una EVPN VXLAN.
7. Explique la utilidad de dos etiquetas MPLS en una L3VPN (RFC 4364).
8. 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?
9. 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?

10. Describa las diferencias entre el uso de BGP en una L3VPN (RFC 4364) y en un escenario de encaminamiento inter-dominio en la Internet.
11. Dada una L3VPN (RFC 4364) explique las diferencias entre implementarla mediante LSPs MPLS o mediante túneles GRE entre los PE routers.
12. Explique la utilidad del atributo AS_PATH en una L3VPN.

WAN optimization

1. Un equipo de aceleración de acceso WAN se coloca en la frontera de red de dos sedes de una empresa alejadas entre sí. En la comunicación entre ellas actúa como proxy, partiendo las conexiones TCP extremo a extremo en 3: una entre host y acelerador local, una segunda entre los aceleradores y la tercera entre host y acelerador de la otra sede. Explique qué mejoras se pueden conseguir con este procedimiento, cómo y por qué.

HTTP

2. Describa similitudes entre HTTP 1.1 y HTTP/2.
3. ¿Necesita HTTP/2 soporte para enviar Cookies en la cabecera HTTP?
4. Explique cómo funciona y la utilidad del *Server Push* en HTTP/2
5. Explique si el pipelining de HTTP 1.1 resuelve el problema de head-of-line blocking y por qué
6. Explique cómo resuelve HTTP/2 el problema de head-of-line blocking de HTTP 1.1
7. Explique las mejoras que incluye HTTP/2 sobre QUIC frente a HTTP/2 sobre TCP.
8. Explique el problema de head-of-line blocking que se mantiene en HTTP/2 sobre TCP y cómo lo resuelve su transporte sobre QUIC.
9. Explique qué tipo de *head-of-line blocking* existe en HTTP/2 y que resuelve HTTP/3, así como cómo lo resuelve.

Otros nuevos protocolos

1. Describa estrategias que servirían para reducir la posibilidad de un colapso por Incast
2. Explique si Multipath TCP (MPTCP) puede funcionar o no cuando hay un NAT en el camino entre los extremos.
3. 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.
4. Discuta el efecto que pueden tener los siguientes valores sobre la máxima velocidad de transferencia de datos que pueda alcanzar una conexión TCP que tenga una cantidad ilimitada de datos a enviar: el valor del puerto del servidor, la probabilidad de pérdida de paquetes en la red, el valor mínimo del timer de retransmisión, el tamaño inicial de la

ventana de control de congestión, el tamaño máximo de la ventana de control de flujo y el RTT entre los dos extremos.

5. Compare la funcionalidad de un Media Gateway Controller en un despliegue VoIP y de un controlador en una SDN.
6. Describa dos escenarios donde comunicación entre los extremos empleando MPTCP en lugar de simple TCP suponga una ventaja y explique dicha ventaja.

Tráfico de datos

1. Un centro de datos contiene hosts donde se instancian máquinas virtuales que son empleadas mediante servicios de escritorio remoto por los trabajadores de un call center. Estos trabajadores cuentan cada uno con un thin client que emplean para mostrar el escritorio de una de esas máquinas virtuales, las cuales emplean como si fuera su ordenador local, para por ejemplo navegar a destinos web internos de la misma LAN de la empresa. ¿Es este escenario susceptible de un problema de colapso por Incast en el centro de datos?
2. Discuta la influencia de los siguientes mecanismos de TCP en que se produzca una situación de colapso por Incast en un datacentre: el timer de delayed ACK, el valor mínimo del temporizador de retransmisión, el tamaño máximo de la ventana de control de flujo.
3. Discuta los diferentes efectos sobre conexiones TCP en un datacentre entre que se emplee una topología con ECMP por paquete o por flujo.
4. Explique si a un escenario de colapso por Incast le ayudaría para evitarlo reducir o aumentar el tamaño del buffer de paquetes en los conmutadores de interconexión, suponiendo que todos emplean una arquitectura de memoria compartida

Otras

1. 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.
2. ¿Existen soluciones en capa 2 Ethernet que ofrezcan ECMP? Si es así descríbalas brevemente y si no diga por qué cree que no existen.
3. ¿Pueden emplearse los múltiples enlaces de una topología leaf+spine con alguna solución Ethernet previa a SPB? Describa tal solución si es que existe.
4. ¿En qué se diferencia un esquema de protección 1+1 con un esquema 1:1?
5. ¿Por qué SDH no puede ofrece una clase de servicio similar al rt-VBR ofrecido en una red ATM?
6. 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.
7. 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.
8. 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?
9. 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.
10. 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.