Redes de Datos 2

2º Parcial - 2022

Solución

Esta es una posible solución a las preguntas planteadas. Por razones didácticas normalmente contiene bastante más información que la mínima necesaria para responder la pregunta.

Pregunta 1 (4 puntos)

a) ¿Qué ventajas ofrece la arquitectura SDN respecto a las redes actuales?

La arquitectura SDN intenta brindar soluciones a algunas limitaciones identificadas en la arquitectura tradicional de las redes de datos, que pueden sintetizarse en que es una arquitectura estática y compleja, con alta dependencia de los fabricantes de equipos para gestionarla y con dificultades o lentitud para escalar y brindar nuevos servicios de forma más ágil. Mediante un plano de control centralizado se plantea lograr una mayor flexibilidad para implementar políticas de ruteo, ingeniería de tráfico, seguridad, que puedan desplegarse de forma más ágil y consistente. Asimismo se logra una independencia de los fabricantes que permite que la red se adapte a las necesidades del servicio y el negocio. Finalmente, el plano de datos se puede especializar en el forwarding de paquetes a alta velocidad. También la arquitectura incluye un plano de aplicaciones que brindan la capacidad de programar el comportamiento de la red a través de una interfaz (norte) con el controlador trabajando sobre una visión abstracta de la red, sin necesidad de llegar a los detalles de los equipos.

b) ¿Qué desventajas presenta una arquitectura como la propuesta por SDN?

Una de las principales desventajas señaladas a la arquitectura SDN es la centralización de funciones en un controlador que podría ser un punto singular de falla de la red. Podría señalarse como desventaja la necesidad que los dispositivos del plano de datos requieran disponer interfaces estandarizadas para controlar su comportamiento (ejemplo OpenFlow), algo que a los fabricantes podría no resultarles atractivo porque todos los dispositivos pasarían a ser cajas más o menos equivalentes.
SDN provee de soluciones para el cuestionamiento de la dependencia del controlador, mediante la previsión de soluciones de alta disponibilidad para la función del controlador y la operación contínua de los switches SDN cuando se pierde la comunicación con el controlador.

c) Explique qué es una tabla de flujo en la arquitectura de switches definida en Openflow y qué información básica contiene dicha tabla.

Una tabla de flujo (flow table) en un switch OpenFlow, asocia cada paquete entrante a un flujo particular y especifica qué acciones se deben hacer con él. Puede existir una cadena de tablas (pipeline) en un switch lo que ofrece mayor flexibilidad para aplicar acciones a un paquete. Las tablas están compuestas por entradas, y cada entrada tiene:

- *Match Fields: criterios de selección de paquetes en base a campos de los encabezados (de protocolos de capa 2, 3, 4)*
- *Instructions: define qué hacer cuando hay un match (por ejemplo enviarlo a otra table, agregar acciones al instruction-set, aplicar acciones, actualizar metadata asociada al paquete)*
- *Counters: Cuenta de paquetes que matchean la entrada.*
- *Timeouts: temporizadores que eliminan la entrada por inactividad o al cabo de un tiempo (idle_timeout, hard_timeout)*
- *Cookie: identificador usado por el controlador para actualizar o borrar una entrada*
- *Priority: para ordenar las entradas en la tabla*
- *Flags: que permiten alterar el procesamiento estándar*

Pregunta 2 (4 puntos)

a) ¿Qué es una FEC (Forwarding Equivalence Class) en MPLS?

En MPLS se dividen los posibles paquetes en "Clases", conjuntos de paquetes que comparten características y son encaminados de la misma manera (y por tanto utilizan para su encaminamiento la misma etiqueta de MPLS). Una Forwarding Equivalence Class es justamente una de esas clases de

equivalencia, un conjunto de posibles paquetes que comparten alguna(s) propiedad(es) y son encaminados de la misma manera en la red MPLS

b) En las VPNs capa 3 utilizando MPLS que vimos en el curso, ¿cuál sería una posible partición en FECs para la etiqueta interior? ¿Cuál es la FEC que se utiliza para la etiqueta exterior?

En las VPN capa 3 sobre MPLS, la etiqueta interior (bottom of stack) es asignada por el PE aguas abajo utilizando BGP, y se asocia a todos o algunos los destinos en ese PE de una VRF. Ejemplos de posibles FEC son:

- Todos los paquetes destinados a IPs correspondientes a prefijos de la VRF x alcanzables por el PE
- Todos los paquetes destinados a IPs correspondientes a prefijos de la VRF x alcanzables por el PE con un determinado next-hop
- Todos los paquetes destinados a IPs correspondientes a un determinado prefijo alcanzable por el PE

La etiqueta exterior es la que nos permite alcanzar el PE de salida, por lo que corresponderá con la FEC que nos lleve a la IP del peer BGP multiprotocolo (por ejemplo aprendida por el IGP y LDP o encaminado por un túnel de ingeniería de tráfico).

Pregunta 3 (5 puntos)

¿Qué es el PHP (penultimate hop popping) en MPLS?

PHP es un mecanismo opcional en MPLS, pensado para optimizar el encaminamiento en el LER de salida. Consiste en indicar al penúltimo nodo que debe retirar la etiqueta exterior (realizar un "POP") de forma que el LER de salida recibe el paquete con un nivel menos de etiquetas (sin etiqueta MPLS si esta era la última del stack), por lo cual evita tener que realizar una búsqueda en la tabla de etiquetas MPLS. La desventaja es que perdemos la información de los bits de calidad de servicio de MPLS.

En LDP, ¿Cómo indica un nodo que se debe realizar PHP (qué debe anunciar y por qué)?

En MPLS se reserva un valor de etiqueta para esta función (valor 3, "implicit null"). Entonces el LER de egreso, en el mensaje de "label mapping" correspondiente al prefijo para el cual se va a realizar PHP indica a sus vecinos LDP que la etiqueta asociada es la implicit-null. Cualquier enrutador MPLS que recibe un mapeo de una FEC a la etiqueta implicit-null sabe que debe realizar la función "POP" de la etiqueta exterior si utiliza ese mapeo

Pregunta 4 (4 puntos)

En un protocolo de distribución de etiquetas en MPLS, ¿qué significa que la distribución de etiquetas sea "unsolicited downstream"? ¿y que la retención sea "liberal"?

"Unsolicited downstream" refiere a cómo decide un LSR cuándo anunciar los mapeos de etiquetas. En el caso "unsolicited downstream", el LSR enviará las asociaciones FEC – etiqueta a todos los vecinos, sin esperar una solicitud de mapeo (el otro modo es el "on demand", donde se espera la solicitud del vecino para enviar el mapeo FEC – etiqueta)

La retención refiere a qué hace un LSR cuando tiene o recibe información de un mapeo FEC – etiqueta que no precisa (en este momento). La retención liberal significa que guardará todos los mapeos disponibles, ya sea que estén en uso o no (la otra política posible es el modo conservador, donde solo se almacenan los mapeos en uso)

Pregunta 5 (5 puntos)

En las VPNs capa 2 (por ejemplo para transporte de 802.3, Ethernet) que vimos en el curso,

a) ¿cómo se utiliza el stack de etiquetas de MPLS?

En las VPNs capa 2 que vimos en el curso el servicio se emula utilizando pseudocables (pseudowires). Los pseudocables se implementan utilizando un stack de dos etiquetas (más una palabra de control opcional), y emulan el servicio que nos darìa un "cable" de la tecnologìa correspondiente.

La etiqueta exterior (la más cercana a capa 2) se utiliza para encaminar los paquetes al enrutador MPLS de salida. Se aprende ya sea por LDP y el protocolo de enrutamiento interno, o por ingeniería de tráfico.

La etiqueta interior (bottom of stack) identifica al servicio, y es señalizada utilizando LDP dirigido

b) ¿Por qué en una VPLS (Virtual Private Lan Service) básica se precisa una malla de LSPs entre todos los PE participantes?

Un servicio VPLS emula un switch transparente que interconecta todos los puntos del cliente. Para ello, cada LSR se comporta como un switch transparente, conectado a los otros switches PE de la red del proveedor mediante pseudowires (y conectando los puertos ethernet del cliente). Para evitar loops (recordar que en un switch transparente las tramas broadcast, multicast y aquellas a direcciones MAC cuya localización no se conoce se inundan por todos los puertos), en el caso de las VPLS se impone una restricción: que las tramas recibidas por un pseudowire, no puede reenviarse por otro pseudowire. Por tanto, para que pueda haber comunicación entre cualquier par de puertos del servicio VPLS es necesario que todos los PE que participan de la VPLS estén conectados por pseudowires (malla)

Pregunta 6 (5 puntos)

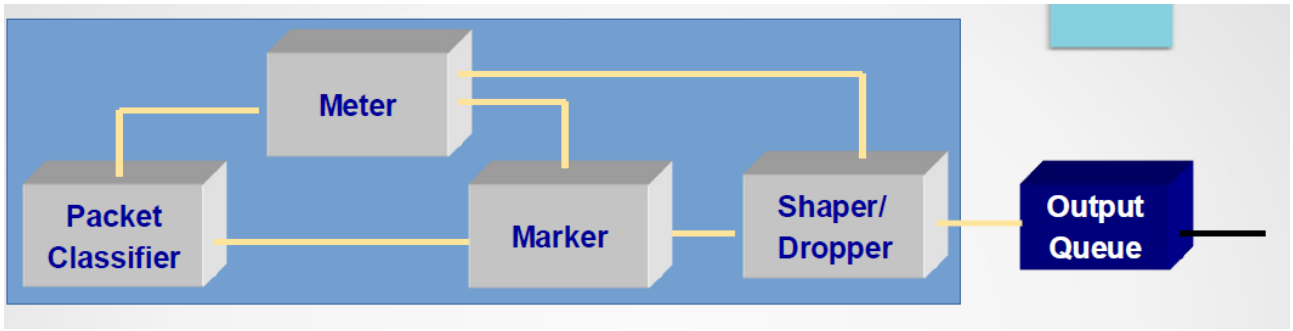
a) Explique brevemente los principales componentes del modelo de DiffServ para implementar QoS.

b) ¿Por qué es importante la implementación de un scheduler en la implementación de Diffserv?

c) Explicar las estrategias Weigthed Round Robin, Strict Priority y Random Early Detection.

a) Diffserv requiere que el tráfico se marque (DSCP en IPv4, Traffic Class en IPv6, o EXP bit en MPLS).

El objetivo de los nodos externos es clasificar el tráfico a la marca adecuada y verificar (en lazo abierto) que el tráfico es acorde al acuerdo de trafico establecido (traffic profile). Los nodos externos deben implementar los siguientes bloques:



*El bloque de **clasificación** es quien se encarga de clasificar el tráfico. El criterio puede ser por ejemplo un campo del encabezado IP o varios.*

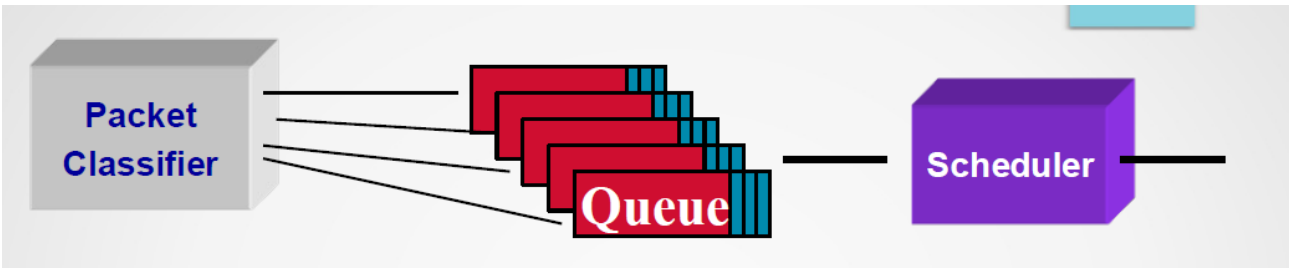
*El bloque de **medición** realiza la medición de los parámetros de acuerdo de tráfico, verificando si este esta dentro del acuerdo o fuera del acuerdo.*

*El bloque de **marcado** puede remarcar el tráfico entrante, definir marcas diferentes si el tráfico esta dentro o fuera del acuerdo.*

*El bloque de **shapper/dropper** acondiciona el tráfico de salida para que cumpla con las condiciones del contrato de tráfico, en caso de no cumplirlo a la entrada, lo termina ajustando, bien sea demorando paquetes o descartando.*

*El tráfico luego debería ir a diferentes colas de acuerdo a la marca, de forma que un **scheduler** pueda distribuir el tiempo de atención entre las diferentes colas, de forma de poder priorizar el tráfico entre las diferentes colas (por ejemplo, VoIP), o garantizar un mínimo de tiempo de atención.*

En el modelo DiffServ los nodos internos asumen que el tráfico ya fue correctamente marcado y controlado de acuerdo a contrato de tráfico, por lo cual lo único que hacer es identificar la marca, asignarla a la cola adecuada y luego el scheduler impone las reglas de priorización de tráfico entre las colas.



*b) El **scheduler** es quien en definitiva impone como distribuir la atención entre las diferentes colas, permitiendo implementar comportamiento de prioridad estricta entre las clases, garantizar un mínimo de servicio a cada clase, o colas con bajo delay.*

c) Explicar las estrategias Weigthed Round Robin, Strict Priority y Random Early Detection.

WRR: *El scheduler garantiza un mínimo de atención a cada una de las colas. Se van recorriendo todas las colas en un orden prefijado asignándole un tiempo de servicio a cada una, y a diferencia del Round Robin sin pesos, el tiempo de servicio puede depender del peso de cada cola (o sea que el mínimo de atención puede depender de la cola). Como ejemplo podemos pensar en 4 colas con distintos pesos, y un intervalo de tiempo (ejemplo 1 segundo), que luego ranuramos (por ejemplo en 10 intervalos de 100 ms, de los cuales asignamos 4 intervalos a la cola con mayor peso, 3 intervalos a la segunda, 2 intervalos a la tercera, y 1 intervalo a la de menor peso). Luego vamos recorriendo las 4 colas, asignando a cada una de ellas los intervalos indicados. En caso de no haber paquetes en una cola se prosigue a a siguiente por lo que no se desperdicia capacidad, y hablamos de garantizar un mínimo de atención ya que en el peor de los casos en este ejemplo cada cola tendrá al menos el 40/30/20/10% de la capacidad cada segundo.*

Strict Priority*: Este esquema aplica prioridad estricta entre las clases, hasta no vaciar de paquetes la cola de prioridad mayor, el scheduler no se fija si hay paquetes en las restantes colas de prioridad menor.*

RED: *Los objetivo de RED son:*

- *Evitar que la cola llegue a llenarse, y por tanto se descarten todos los subsiguientes paquetes, que llevan segmentos TCP de varios clientes, ya que esto haría que muchos de ellos se sincronicen y apliquen al mismo tiempo el control de congestión.*
- *Evitar que unos pocos flujos acaparen en determinado momento la totalidad de la cola.*
- *Balancear el compromiso entre que idealmente la cola se encuentre vacía y no agregue retardos, pero tenga capacidad suficiente para absorber ráfagas.*

Para hacer esto, implementa una prioridad de descarte de paquetes dependiendo del nivel medio de ocupación de la cola, junto con dos umbrales de utilización. Un mínimo a partir del cual comienzo a descartar aleatoriamente paquetes con probabilidad p, incrementando la probabilidad de descarte mientras estoy por encima del mínimo y por debajo del máximo, y un máximo a partir del cual descarto todos los nuevos paquetes.

Observar *que RED puede ser complementario a WRR y Strict Priority, incluso si trabajamos con AF, tenemos subclases con prioridad de descarte diferente (Weigthed RED).*

Pregunta 7 (6 puntos)

a) ¿A qué se llama túnel de Ingeniería de Tráfico dentro de MPLS-TE?

b) Explique el mecanismo de protección de link FRR en MPLS-TE.
   i. ¿Qué supuesto se realiza sobre la gestión de etiquetas?
   ii. ¿Cuándo se crean los túneles de protección?
   iii. ¿Cómo se detecta una falla en FRR?
   iv. ¿Qué túneles puede proteger?
   v. ¿Por qué es necesario que se entere de la falla el extremo inicial del tunel (head-end)?
   Nota: Para la explicación puede utilizar un ejemplo de restauración de túnel, donde el túnel a proteger utiliza etiqueta 45. Defina la topología y el resto de las etiquetas que sean necesarias.

a) Ingeniería de tráfico termina implicando en ultima instancia el poder seleccionar routers y links por donde quiero que vaya el tráfico en la red (entre dos puntos), cumpliendo con las restricciones (necesidades) que tenga el tráfico. Esto cambia el esquema de forwarding por red de destino, bien sea por protocolos de ruteo clásico o LDP.

En MPLS-TE llamamos túneles de Ingeniería de trafico a los LSP que construimos de forma explicita (camino explicito), cumpliendo con las restricciones que el administrador imponga.

b) Explique el mecanismo de protección de link FRR en MPLS-TE.
i. ¿Qué supuesto se realiza sobre la gestión de etiquetas?
El supuesto que se realiza es que las etiquetas tienen significado global a los router (espacio de etiquetas global y no por interfaz), de esta forma, alcanza con llegar al router con el mismo valor de etiqueta, sin importar la interfaz de entrada, y el procesamiento de forwarding es el mismo.

Un requerimiento para poder utilizar túneles de respaldo, debo llegar al MP (Merge Point) con el mismo valor de etiqueta, tanto por el camino principal, como por el de respaldo.

ii. ¿Cuándo se crean los túneles de protección?
Los túneles de protección se crean "a priori" (antes que suceda ninguna falla) como túneles normales, luego se declaran en los links que quiero proteger. Al momento de detectar una falla, recien el PLR (Point of Local Repair) que detecta la falla, es quien decide que túnel de respaldo utilizar y que túneles respaldar.

iii. ¿Cómo se detecta una falla en FRR?
Las fallas se detectan principalmente por dejar de ver los mensajes de RSVP Hello en los links. El envío de mensajes de Hello periódicos fue un agregado al protocolo RSVP cuando se decidió utilizarlo para ingeniería de tráfico, dado que esperar a la pérdida de soft-state implicaba tiempos de 30 segundos, y el objetivo fue obtener una detección rápida de fallas.

Existen otros mecanismos que permiten detectar la caída de un link, y que permiten acelerar el tiempo de detección

vi. ¿Qué túneles puede proteger?

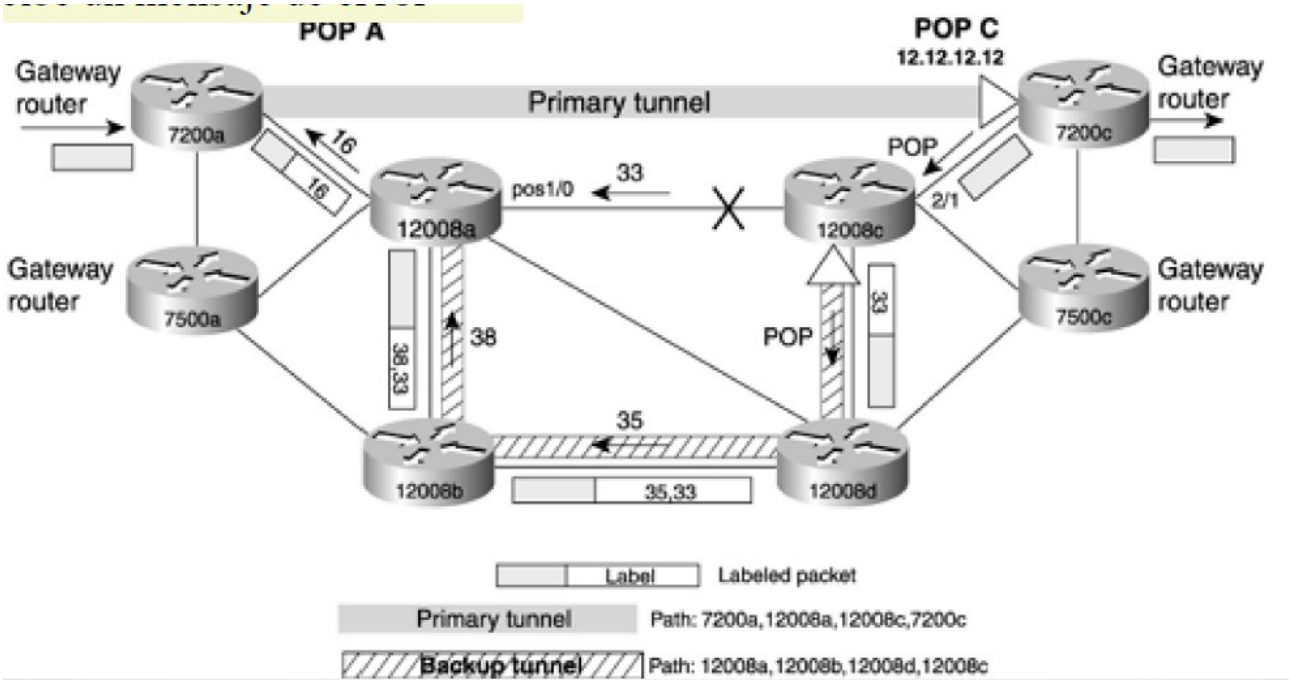
A diferencia del respaldo de túnel, el respaldo FRR de link puede proteger a varios túneles a la vez.
La solicitud de protección de túnel se envía al momento de crear los túneles primarios, de esta forma el nodo PLR conoce la lista de túneles que requieren protección.

La cantidad final de túneles protegidos por un túnel de respaldo dependerá de la cantidad de túneles que pasen por el nodo y utilicen el link protegido, la cantidad de túneles que solicitaron respaldo, el tipo de respaldo (ancho de banda), y cuantos túneles de respaldo pueda tener en simultáneo. Este proceso es controlado por el nodo que detecta la falla.

v. ¿Por qué es necesario que se entere de la falla el extremo inicial del tunel (head-end)?
El objetivo de la protección FRR es ofrecer un respaldo temporal, este respaldo puede ser preservando el ancho de banda reservado por el túnel principal, o no. En caso de preservar ancho de banda, es posible que no alcance para todos los túneles a respladar. Si el respaldo es sin preservar el ancho de banda, se desconoce el ancho de banda que realmente se dispone mientras actúa el respaldo.

Por este motivo, siempre se busca que llegue el mensaje de RSVP Path Error el head-end, para que este se entere que hubo una falla y que actúa el respaldo. El head-end puede entonces buscar un camino (si es que existe ya que cambió la topología) que cumpla con las restricciones del túnel original. En caso de encontrarlo, lo señaliza y luego transfiere el tráfico original al nuevo túnel.

El mensaje RSVP Path Error también se envía al head-end para los túneles que no solicitaron respaldo por FRR o no pudieron ser respaldados, pero en este caso hasta que llega el mensaje al head-end el tráfico se pierde, y mientras se establece el nuevo túnel se utilizará el forwarding de IP (posiblemente LDP si está disponible), sin garantías del ancho de banda disponible mientras se logra encontrar y señalizar un nuevo camino.



En el siguiente ejemplo, tomando como referencia la figura, el túnel principal utiliza el camino superior, 7200a, 12800a, 12800c y 7200c..

El túnel de respaldo se establece entre el nodo 12800a y el 12800c, utilizando el camino 12800a- 12800b (label 38), 12800b-12800d (label 35), 12800d-12800c (POP).

Cuando el router 12800a detecta la falla, se activa la protección de FRR, por lo cual se envía el tráfico original por el túnel de respaldo (stack de etiquetas). Lo podemos ver como un túnel dentro de otro túnel. La etiqueta externa corresponde al camino de respaldo, luego en el MP (router 12800c) se recibe la etiqueta del camino original (por el POP en el nodo anterior). Como la etiqueta tiene significado global dentro de 12800c, esto permite que el nodo sepa que corresponde al túnel primario y desde ahí prosigue con el camino original.

Pregunta 8 (5 puntos)

a) Realice un análisis de las diferencias, ventajas y desventajas, entre la virtualización basada en hypervisor (VM) y la virtualización del sistema operativo (Containers).
Desarrolle al menos 5 de estas diferencias.
Mencione y sustente las dos diferencias que a su juicio lo haría inclinarse al uso de Containers

b) ¿Qué es una Virtual Network Function (VNF)?

c) Explique la relación que hay entre VNF, VNFC y VM.

a)

	VM	VE
Acceso al HW	Hipervisor	Directo
Performance	Interrupción al OS, luego interrupción al Hipervisor.	Interrupción al OS (as good as baremetal)
Inicialización	Minutos, tiene que inicializar el OS.	Segundos, tiene que inicializar una App.
Diferentes OS	VM con diferente OS	Un solo tipo de OS
Objetivo (“inicial”)	Consolidación de HW	Performance, Despliegue distribuido y Agilidad.
Cloud	Adaptado a, la noción de “cloud” está en la VM, no en la app.	Son nativos del ambiente de cloud
Cambios y Actualizaciones	Hay que actualizar el OS, ventaja de replicar la imagen y hacerlo off-line. ¿Cómo vuelve on-line?	Proceso más simple para probar un cambio en una instancia (**“canary test”**). El tiempo de arranque es “chico”, repositorio central.

Falta desarrollar cada tema

b) ¿Qué es una Virtual Network Function (VNF)?

Virtualized Network Function (VNF): *Una implementación de una NF (Network Function) despliega-*

da dentro de NFVI (Network Function Virtualization Infraestructure). Esto implica que se despliega como una virtualización (ya sea VM o contenedores) sobre una infraestructura física genérica y que de sporte a estas técnicas de virtualización.

c) Explique la relación que hay entre VNF, VNFC y VM.

Al revisar un poco mas en detalle una VNF (Funcion de red virtualizada), esta puede ser implementada de diversas formas, por ejemplo un bloque que recibe el tráfico y luego distribuye la carga. Por lo que una VNF puede descomponerse en funciones mas simples que se llaman VNFC (Virtual Network Function Component), siendo estos componentes los que luego efectivamente se pueden mapear con el esquema de virtualización, por ejemplo un VNFC se implementa en una VM,

Esto implica que una VNF se puede descomponer en N diferentes componentes (VNFC, que no tienen porque ser todos iguales), luego cada VNFC se implementa en una VM (y solo una VM).

Si bien no fue visto en detalle en el curso, el escenario con contenedores es un poco diferente, y como es posible realizar contenedores sobre VM o sobre baremtal, o VNF híbridas, esto puede llevar a confusión. Pero aplica que una VNF (se llama CNF), se desagrega en varios PODs (unidad elemental que se despliega en contenedores), lo usual es que cada POD se implemente en un contenedor diferente.

Esto hace que podamos usar la analogía de VNF por CNF, VNFC por POD, VM por contenedor.