

Ejercicios SDN y NFV

Junio 2023

EJERCICIO 2. Puntuación: 1,4 puntos. Tiempo estimado: 15 minutos

A continuación, se muestran los contenidos de tres tablas de flujos de un switch SDN que sigue la especificación Openflow.

Table flow 0:

Match fields	Priority	Instructions
Ethertype = IPv4	10	Goto-Table 2
Any (wildcard)	0	Goto-Table 1

Nota: Ethertype identifica el protocolo que se encapsula en la trama Ethernet.

Table flow 1:

Match fields	Priority	Instructions
Ingress port = 2	10	Write-Actions {Output 5}
Any (wildcard)	0	Write-Actions {Output CONTROLLER}

Table flow 2:

Match fields	Priority	Instructions
Dir IP origen = 10.2.0.1	10	Write-Actions {Output 7}
Dir IP origen pertenece al prefijo 10.0.0.0/8	15	Write-Actions {Output CONTROLLER}
Dir IP destino pertenece al prefijo 10.0.0.0/8	20	Write-Actions {Output 8}

Teniendo en cuenta esta información, seleccione qué ocurrirá con cada uno de los siguientes paquetes si llegan a este switch SDN (cada respuesta correcta puntúa 0,2 puntos, cada respuesta incorrecta puntúa -0,05, cada respuesta en blanco puntúa 0).

- 1) Un paquete IPv4 con dirección IP origen = 10.2.0.1 y dirección IP destino = 10.2.0.2:
 - a) Será reenviado por el puerto 5 del switch.
 - b) Será reenviado por el puerto 7 del switch.
 - c) Será reenviado por el puerto 8 del switch. **CORRECTA**
 - d) Será enviado al controlador a través de un mensaje PACKET_IN.
 - e) Será descartado ("drop").
- 2) Un paquete IPv4 con dirección IP origen = 11.2.0.3 y dirección IP destino = 11.2.0.2:
 - a) Será reenviado por el puerto 5 del switch.
 - b) Será reenviado por el puerto 7 del switch.
 - c) Será reenviado por el puerto 8 del switch.
 - d) Será enviado al controlador a través de un mensaje PACKET_IN.
 - e) Será descartado ("drop"). **CORRECTA**

- 3) Un paquete IPv6 que haya entrado al switch por el puerto 2:
- a) Será reenviado por el puerto 5 del switch. **CORRECTA**
 - b) Será reenviado por el puerto 7 del switch.
 - c) Será reenviado por el puerto 8 del switch.
 - d) Será enviado al controlador a través de un mensaje PACKET_IN.
 - e) Será descartado ("drop").
- 4) Un paquete IPv6 que haya entrado al switch por el puerto 1:
- a) Será reenviado por el puerto 5 del switch.
 - b) Será reenviado por el puerto 7 del switch.
 - c) Será reenviado por el puerto 8 del switch.
 - d) Será enviado al controlador a través de un mensaje PACKET_IN. **CORRECTA**
 - e) Será descartado ("drop").

Añada una entrada en la tabla 0, 1 o 2 para que **únicamente** se modifique el comportamiento del switch para el tráfico ARP (es un protocolo que se encapsula directamente sobre Ethernet) **que no haya entrado al switch por el puerto 2**. Dicho tráfico debe ser reenviado por el puerto 9 del switch. Incluya a continuación la explicación detallada de su elección (en qué tabla ha añadido la entrada y el porqué de los valores de todas sus columnas: match fields, priority e instructions). (0,6 puntos)

Identificador de la tabla en la que añade la entrada: 1

Entrada que añade:

Match fields	Priority	Instructions
Ethertype = ARP	5	Write-Actions {Output 9}

Explicación detallada de sus elecciones:

Se selecciona la tabla 1 porque se trata de un tráfico que no es IPv4, por lo que según la primera entrada de la tabla 0, se irá a la tabla 1 para su tratamiento.

Una vez en la tabla 1, si el tráfico es ARP (match field: Ethertype = ARP) y su puerto es distinto de 2, solo encajaría con esta nueva entrada, con lo que saldría por el puerto 9 del switch (instrucción: añadir la acción {Output 9}).

Sin embargo, para todo el tráfico que entre por el puerto 2, incluyendo el tráfico ARP, se debe salir por el puerto 5. Por eso el campo "Priority" de esta nueva entrada se elige menor que 10, que es la prioridad de la primera entrada de la tabla 1, para asegurar que el tráfico ARP cuyo puerto de entrada sea el 2, saldrá por el puerto 5.

(NOTA: otras soluciones correctas son posibles).

Mayo 2022

EJERCICIO 2. Puntuación: 1 punto. Tiempo estimado: 8 minutos

Describe las características fundamentales de las redes de área extendida definidas por software relativas a:

1. Service Assurance of each SD-WAN tunnel

Las prestaciones de QoS son medidas en tiempo real en cada túnel de SD-WAN.

Determinar si una WAN en particular cumple con los requisitos de rendimiento de una aplicación.

2. Service Automation via Centralized Management, Control and Orchestration

Control y orquestación de túneles SD-WAN con configuración automática de SD-WAN en los SD-WAN Edge.

"Zero touch provisioning" (ZTP) información de configuración preinstalada en el sistema central.

3. WAN Optimization

Puede incluir "data deduplication", "data compression", "data caching", "forward error correction" y "protocol spoofing".

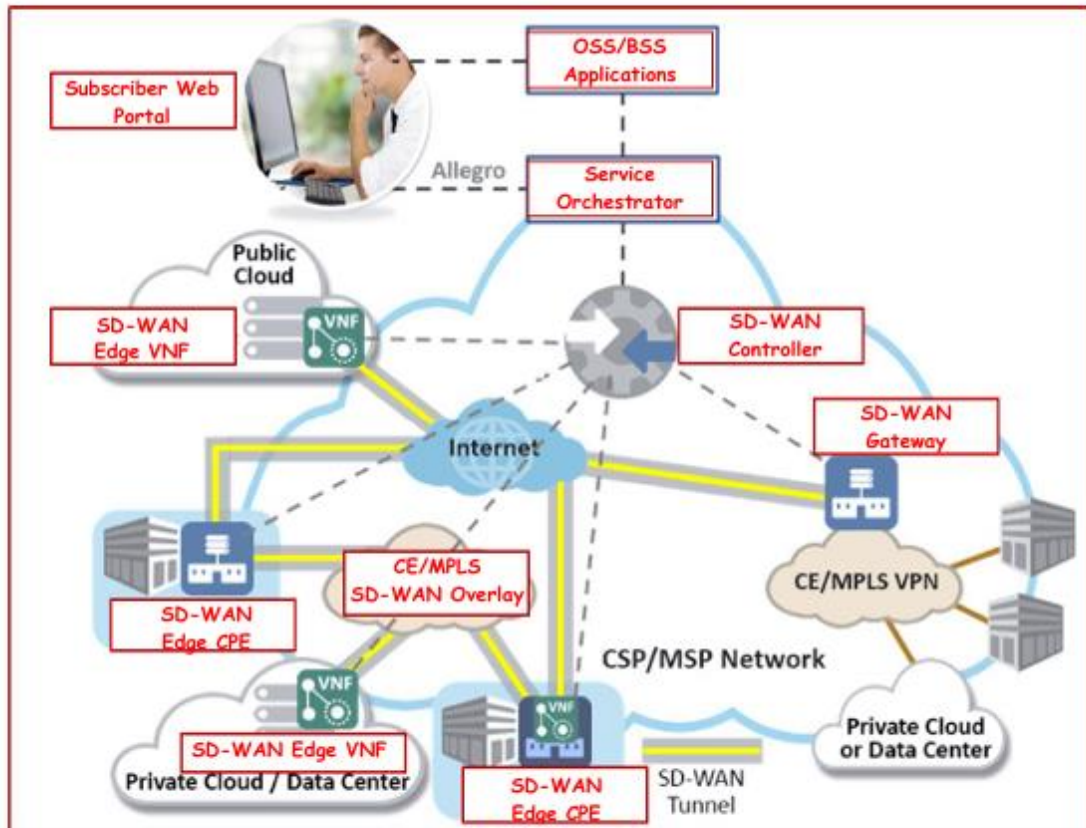
4. Secure, IP based Virtual Overlay Network

Túneles IPsec sobre "underlay networks" Internet y/o LTE y/o MPLS.

SD-WANs soporta cualquier topología: "full/partial mesh" y "hub & spoke".

EJERCICIO 3. Puntuación: 1 punto. Tiempo estimado: 10 minutos

Rellene las cajas que aparecen en el siguiente dibujo correspondientes a componentes que forman la arquitectura de SD-WAN.



EJERCICIO 4. Puntuación: 0,5 puntos. Tiempo estimado: 7 minutos

Describe el procesamiento de las tablas de Openflow cuando un paquete de entrada al dispositivo no produce ninguna coincidencia.

Procesamiento: Busca la entrada de flujo de mayor prioridad.

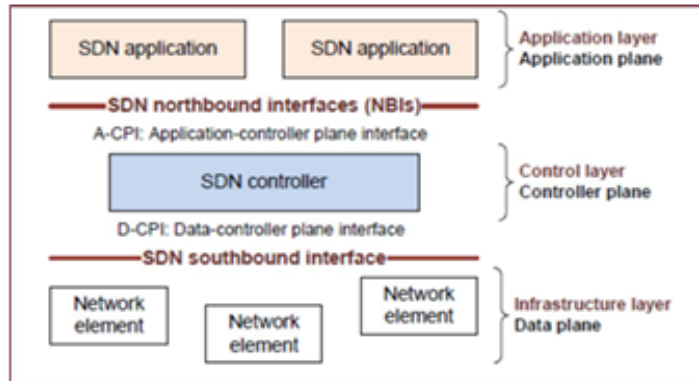
Si no hay ninguna coincidencia en ninguna entrada y no hay ninguna entrada en la **table-miss**, el paquete se descarta. Si hay una coincidencia solo en una entrada de **"table-miss"**, esa entrada especifica una de tres acciones:

- Enviar el paquete al controlador. Esta acción permitirá que el controlador defina un nuevo flujo para este y otros paquetes similares, o decida descartar el paquete.
- Dirigir el paquete a la siguiente tabla de flujo.
- Descartar el paquete.

Mayo 2021

EJERCICIO 2. Puntuación: 1 punto. Tiempo estimado: 10 minutos

- a) Represente gráficamente los componentes de la arquitectura SDN, identificando claramente los niveles y planos a los que pertenece cada uno de dichos componentes, así como las interfaces entre los diferentes niveles. Describa, además, de forma breve la funcionalidad de cada uno de los niveles o planos de la arquitectura. (0,5 puntos)

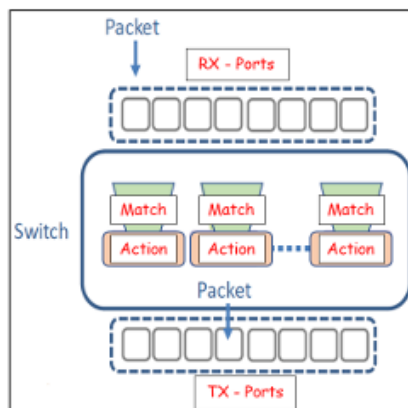


Nivel de Aplicación. Comprende una o más aplicaciones, cada una de las cuales tiene control exclusivo de un conjunto de recursos expuestos por uno o más controladores SDN.

Nivel de Control. Compuesto por un conjunto de controladores SDN, cada uno de los cuales tiene control exclusivo sobre un conjunto de recursos expuestos por uno o más elementos de red en el plano de datos.

Nivel de infraestructura - Plano de Datos. Formado por un conjunto de elementos de red, cada uno de los cuales contiene un conjunto de recursos para procesamiento o reenvío de tráfico.

- b) En la figura siguiente se muestran los componentes del plano de datos de OpenFlow (OF), en los que se han eliminado los nombres de cada uno de ellos. Escriba sobre la figura los nombres de dichos componentes y describa brevemente las tres instrucciones básicas asociadas a cada flujo de entrada. (0,5 puntos)



Reenvío del flujo de paquetes a un puerto dado (o puertos). Esto permite que los paquetes puedan ser encaminados a través de la red. En la mayoría de los switches sucede a la velocidad de la línea.

Encapsulación y reenvío del flujo de paquetes al controlador. El paquete será enviado al Canal Seguro, donde se encapsula y se envía al controlador. Típicamente se usa para el primer paquete en un nuevo flujo, para que el controlador pueda decidir si el flujo debe ser añadido a la tabla de flujos. También se puede usar para reenviar todos los paquetes al controlador para que sean procesados por este.

Descarte del flujo de paquetes. Puede ser usado por seguridad, para parar ataques de denegación de servicio o reducir el falso tráfico de descubrimiento broadcast desde los hosts finales.

EJERCICIO 3. Puntuación: 1 punto. Tiempo estimado: 10 minutos

- a) ¿En qué consiste el "Service Chaining" en NFV? Explique cómo se relaciona este concepto con los de "Network Service" y "Virtual Network Function". (0,5 puntos)

Service Chaining es una funcionalidad que permite crear una cadena ordenada de VNF (Virtual Network Function) a aplicar al tráfico, gracias al establecimiento automático de conexiones entre dichas VNF con SDN, para componer servicios de red (Network Services) sofisticados entre extremos de la red (end points).

- b) Defina y compare los siguientes conceptos de SD-WAN: "Underlay" vs "Overlay". ¿Cómo se relacionan con los túneles cifrados que se establecen entre los nodos "edge"? (0,5 puntos)

Mediante SD-WAN se consigue virtualizar la red física (denominada "Underlay") que interconecta los extremos de la red (los nodos "edge") mediante el establecimiento de túneles cifrados que conforman una red virtual denominada "Overlay". De esta manera se permite la implementación de soluciones versátiles sobre la red así virtualizada, abstrayéndose de las múltiples tecnologías que pueden estar presentes en el "Underlay" (MPLS, redes celulares, Internet, ...).

Julio 2023

EJERCICIO 2. Puntuación: 1,1 puntos. Tiempo estimado: 15 minutos

- a) En la arquitectura de virtualización de funciones de red (NFV) definida por ETSI, ¿qué elementos funcionales forman parte del MANO (Management and Orchestration)? Para cada uno de ellos diga su nombre y resuma su funcionalidad. (0,7 puntos)

- **Gestión de la infraestructura: VIM - Virtualised Infrastructure Manager**
 - Tiene una visión completa de los recursos HW, gestiona la capa de virtualización (ciclo de vida y escalado de las VMs), y gestiona las conexiones entre VMs y VNFs.
- **Gestión de las VNFs: VNFM - VNF Manager**
 - Gestiona el ciclo de vida y gestión FCAPS de las VNF.
- **Orquestación: NFV Orchestrator**
 - Tiene visión del encadenado de VNFs para formar servicios de red, y gestiona el número y características del despliegue de varias VNFs, comunicándose con VNFM y VIM si es necesario.

Al respecto del "pipeline" de tablas de un switch SDN, y en concreto en lo relacionado con la entrada denominada "table miss", responda a las siguientes preguntas:

- b) ¿Cuáles son sus características? (es decir, ¿cómo se puede saber qué entrada es la "table miss" de una tabla?) (0,2 puntos)

Todos los "match fields" son "wildcard", y su prioridad es 0.

- c) ¿Qué utilidad tiene esa entrada? (0,2 puntos)

Permite especificar qué hacer con un paquete "por defecto", es decir, si no coincide con ninguna otra entrada de la tabla.

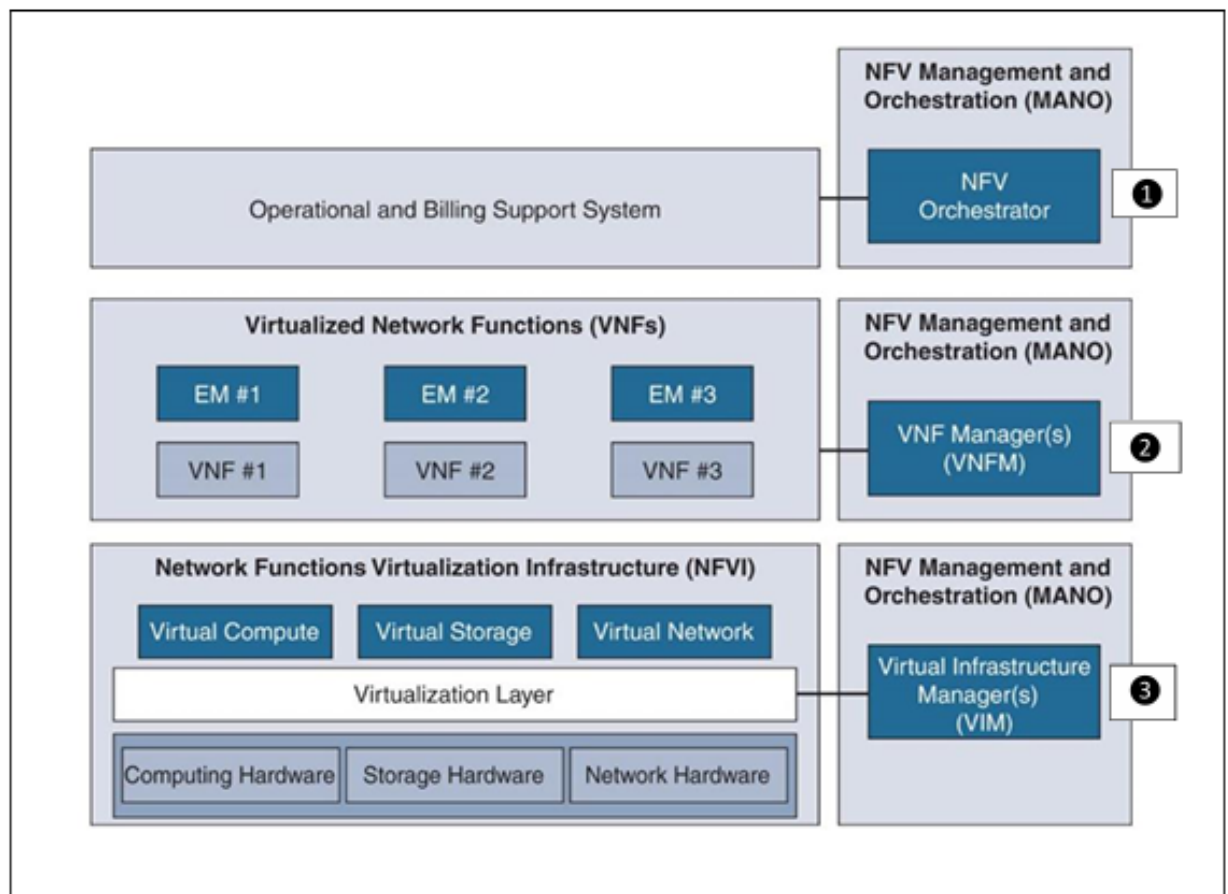
EJERCICIO 1. Puntuación: 4 puntos. Tiempo estimado: 35 minutos

- a) Explique los requerimientos y las ventajas de las herramientas que recopilan y analizan datos de red ("*Network Analytics*") basadas en tecnologías de inteligencia artificial. (1 punto)

Network Analytics: AI Technologies

- ❑ Requiere "**Machine Learning**" (ML), que es el uso de algoritmos para analizar datos, aprender de ellos y hacer una determinación o predicción sin requerir instrucciones explícitas.
- ❑ ML ha evolucionado recientemente hacia modelos estructurados más complejos, como el "**Deep Learning**" (DL), que utiliza redes neuronales para una mayor comprensión y automatización.
- ❑ Beneficios:
 - ❑ **Detección de anomalías en series temporales** para encontrar rápidamente relaciones entre eventos que no serían evidentes ni siquiera para un especialista en redes experimentado.
 - ❑ **Correlación de eventos y análisis de causa raíz** mediante el uso de minería de datos para identificar rápidamente qué función de red está más relacionada con un problema de red.
 - ❑ **Predicción de experiencias de usuario** permitiendo modificar anchos de banda en función del comportamiento del usuario.
 - ❑ **Autoconducción "self-driven"**. AI permite que los sistemas de TI se autocorrijan para maximizar la disponibilidad y proporcionar acciones prescriptivas sobre cómo solucionar los problemas que ocurren. Además, las redes impulsadas por IA pueden capturar y guardar datos antes de un evento o interrupción de la red, lo que ayuda a acelerar la resolución de problemas.

- b) Complete sobre la siguiente figura la información de los diferentes elementos que componen la arquitectura de referencia NFV definida por la ETSI. (0,5 puntos)



- c) Describa brevemente las responsabilidades de las cajas marcadas con los números ❶ a ❸ en la figura anterior. (0,5 puntos)

❶ NFV Orchestrator (NFVO) es responsable de:

Gestión del ciclo de vida del Servicio de red (NS) (incluida la instanciación, la ampliación / reducción, las mediciones de rendimiento, la correlación de eventos, la terminación)
 Gestión global de recursos, validación y autorización de solicitudes de recursos NFVI
 Gestión de políticas para instancias de "Network Services".

❷ VNF Manager (VNFM) es responsable de:

Gestión del ciclo de vida de las instancias de VNF.
 Rol general de coordinación y adaptación para la configuración y el informe de eventos entre NFVI y EM.

❸ Virtualized Infrastructure Manager (VIM) es responsable de:

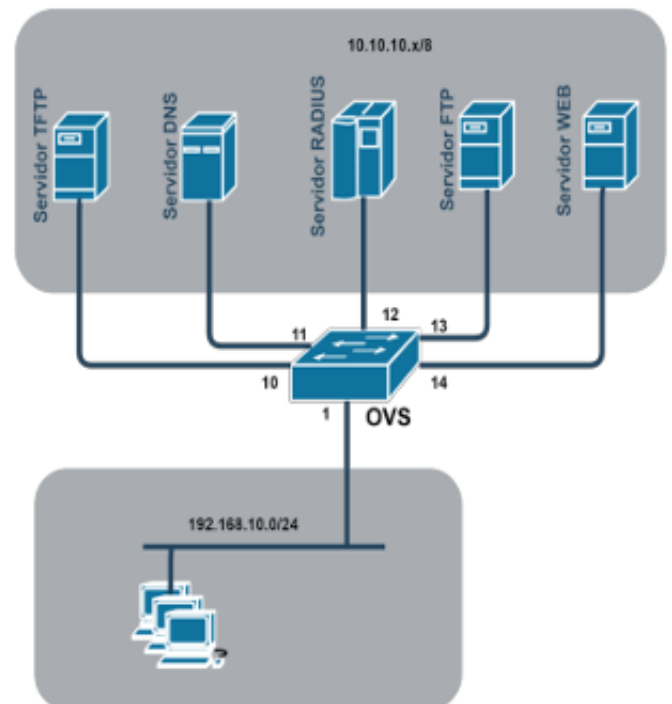
Controlar y administrar los recursos de computación, almacenamiento y red de NFVI, dentro del subdominio de infraestructura de un operador.
 Recopilación y envío de mediciones de rendimiento y eventos.

- d) Identifique a cuál de las características fundamentales de SD-WAN corresponde cada una de las siguientes afirmaciones (0,5 puntos):

"Zero touch provisioning" (ZTP) información de configuración preinstalada en el sistema central	"Service Automation via Centralized Management, Control and Orchestration"
Determinar si una WAN en particular cumple con los requisitos de rendimiento de una aplicación	"Service Assurance of each SD-WAN Tunnel"
Túneles IPsec sobre "underlay networks" Internet y/o LTE y/o MPLS	"Secure, IP-based Virtual Overlay Network"
Puede incluir "data deduplication", "data compression", "data caching", "forward error correction" y "protocol spoofing"	"WAN Optimization"

- e) La siguiente figura muestra una red OpenFlow de servidores y clientes que utilizan el conjunto de aplicaciones indicadas en la tabla.

Aplicación	Protocolo de Transporte/ Número	Puerto TCP/UDP
Trivial File Transfer Protocol - TFTP	UDP/17	69
File Transfer Protocol - FTP	TCP/6	20,21
Domain Name System DNS	UDP/17	53
RADIUS authentication protocol	UDP/17	1812
Hypertext Transfer Protocol (HTTP)	TCP/6	80



Rellene la tabla siguiente con los flujos de OpenFlow para que se cumplan las condiciones indicadas en la figura, utilizando la técnica de anidamiento de tablas y flujos. (1,5 puntos)

*NOTA. Todos los paquetes que no cumplan ninguna de las condiciones anteriores deben ser enviados al controlador. El controlador tiene activada la aplicación de **PROXY/ARP***

[illegible]

Julio 2021

EJERCICIO 2. Puntuación: 1 punto. Tiempo estimado: 10 minutos.

Enumere los “Principios de SDN basados en Abstracción”, incluyendo una breve descripción de cada uno de ellos. (1 punto)

Principio de SDN # 1:

- Control Programable: APIs en lugar de protocolos: Reemplazar los protocolos del plano de control con APIs bien definidas para aplicaciones de red, ocultando los detalles de la red y los relacionados con el servicio a las aplicaciones.

Principio de SDN # 2:

- El reenvío de paquetes como un problema computacional: Los elementos de red solo necesitan:
 - Recibir un paquete
 - Observar los campos del paquete
 - Aplicar algoritmo (clasificación, lógica de decisión),
 - Opcionalmente editar el paquete,
 - Reenviar o descartar el paquete

Principio de SDN # 3:

- Flujos de datos: Los paquetes se manejan únicamente en función del flujo al que pertenecen.
 - Un flujo puede ser determinado por:
 - Un prefijo IP, una etiqueta en una red MPLS, VLAN en redes de interconexión de VLAN, etc.

Principio de SDN # 4:

- Eliminar protocolos distribuidos: Reemplaza los protocolos de enrutamiento distribuidos con algoritmos realizados en el Controlador central.

Principio de SDN # 5:

- Configuración: Los flujos se configuran en los elementos de red (NE) por un controlador SDN. Por tanto, los elementos de red (NE) pueden ser más simples.

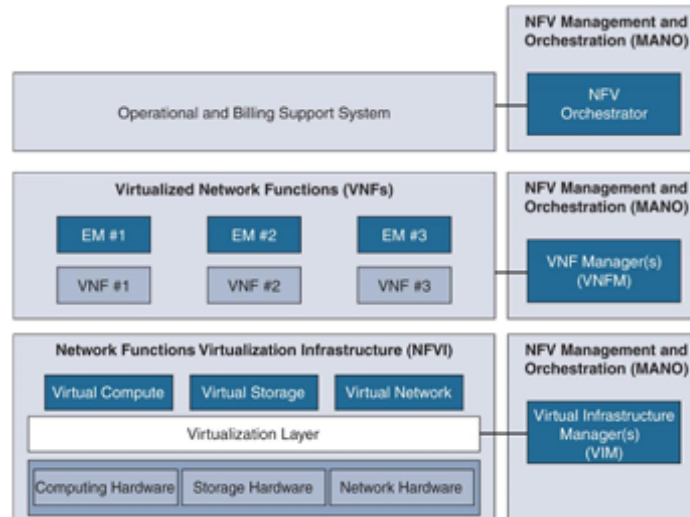
EJERCICIO 3. Puntuación: 1 punto. Tiempo estimado: 10 minutos

- a) SDN introduce potenciales problemas de escalabilidad y disponibilidad con respecto a una red convencional con control distribuido. Describa por qué, poniendo uno o varios ejemplos de situaciones en las que estos problemas se manifiesten. A este respecto, tanto ONOS como otros controladores prevén una posibilidad de aliviar ambos problemas. Describala y explique sobre los ejemplos que ha elegido anteriormente en qué consisten estas soluciones y cómo consiguen su objetivo. (0,5 puntos)

Problemas: si hay un único controlador, puede no tener capacidad para controlar en solitario un número lo suficientemente elevado de nodos en la red (problema de escalabilidad) ya que debe establecer una conexión Openflow con cada uno de ellos, además de comunicarse con ellos en función de la cantidad y tipo de tráfico y aplicaciones instaladas en la red. Además, si deja de estar disponible ese único controlador, parte o toda la funcionalidad de la red puede verse afectada (disponibilidad).

Solución: tener más de un controlador SDN, que funcionen en condiciones de normalidad con reparto de carga (de manera que cada uno se comunica con un subconjunto de nodos), con lo que el problema de escalabilidad se alivia. Estos controladores, sin embargo, tienen que estar sincronizados entre sí para proporcionar a las capas superiores una visión consistente y única de toda la red, lo que también permitirá que, si uno deja de estar disponible, el resto pueda recuperar las sesiones con los nodos "huérfanos" y continuar dando servicio (aliviando el problema de disponibilidad).

- b) En la siguiente figura se representan gráficamente las capas de la arquitectura de referencia NFV, incluyendo sus principales componentes. Describa la funcionalidad de cada una de las capas y sus componentes mostrados. (0,5 puntos)



- **NFV Infrastructure:** Proporciona una virtualización del HW a las funciones virtuales de red. Comprende los recursos físicos de hardware, la capa de virtualización y los recursos virtuales.
- **Virtualized Network Functions (VNF):** Es la capa donde se implementa la virtualización de las funciones de red, haciendo uso de la virtualización del HW proporcionada por la NFVI. El bloque VNF se define como una combinación de bloques VNF y Element Management (EM).
- **OSS/BSS:** Sistema de operación y facturación del operador.
- **Management and Orchestration (MANO):** contiene el orquestador que se encarga de la gestión de los servicios de red (que pueden involucrar varias VNF cada uno), así como la gestión del ciclo de vida de las VNF y la administración de los recursos de computación, almacenamiento y red de NFVI.