



TECH pedia



REDES FUTURAS - SDN & NFV

PODHRADSKÝ PAVOL,
HELEBRANDT PAVOL,
HALAGAN TOMÁŠ, DROZD IVAN

Título: Redes futuras - SDN & NFV
Autor: Podhradský Pavol, Helebrandt Pavol,
Halagan Tomáš, Drozd Ivan
Traducido por: Sandra Bermejo
Publicado por: České vysoké učení technické v Praze
Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 224352084
Print: (only electronic form)
Número de páginas: 40
Edición: Primera edición, 2017

ISBN 978-80-01-06249-4

TechPedia

European Virtual Learning Platform for
Electrical and Information Engineering

<http://www.techpedia.eu>



El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.

Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS



Definición



Interesante



Nota



Ejemplo



Resumen



Ventajas



Desventajas

ANOTACIÓN

El Internet actual sigue basándose en el protocolo de Internet que se definió hace más de 40 años para cierto conjunto de servicios. Durante décadas Internet adquirió grandes dimensiones y además no contaba con nuevas aplicaciones como Web, streaming de vídeo, uso compartido de archivos que cambiaron significativamente la naturaleza del tráfico de Internet. La infraestructura de Internet se ha desarrollado por las nuevas tecnologías de fijo óptica a redes inalámbricas. Las nuevas aplicaciones y servicios, tecnologías y cantidad y la variabilidad de dispositivos de los usuarios finales requieren soluciones flexibles. Como las soluciones más difíciles parecen ser interconexión programables - software definido redes y virtualización de los servicios de red. Este módulo se centra principalmente en estas tecnologías prometedoras para la Internet del futuro, pero también da una visión general de las redes de próxima generación.

OBJETIVOS

El objetivo principal de este curso es adquirir los conocimientos básicos sobre las nuevas tendencias en tecnologías de la información y de la comunicación, principalmente acerca de la evolución de las redes actuales hacia redes futuras, así como Internet del Futuro. Los participantes se familiarizan con características básicas de redes de próxima generación. Sin embargo, es importante que se disponga del conocimiento sobre el estado de las tecnologías más avanzadas como el Software Definido en Red y las Funciones de Red de virtualización desde el punto de vista de la arquitectura básica, principios y protocolos. Por otra parte, también se presta atención a las limitaciones y requisitos del Internet del Futuro reales.

LITERATURA

- [1] Mikoczy, E., Kotuliak, I., van Deventer, M. O.: Evolution of the converged NGN service platforms towards Future Networks. in Future Internet Journal, special issue Special Issue "Network vs. Application Based Solutions for NGN", 2011, ISSN 1999-5903.
- [2] Mikoczy, E.: Next Generation of Multimedia Services in Context of Future Networks. In Proceedings of ETSI Future Network Technologies Workshop, Sophia Antipolis, France, 10–11 March 2010.
- [3] Podhradský, P., Mikóczy, E., Lábaj, O., Londák, J., Trúchly, P., at al: NGN Architectures and NGN Protocols. LdV IntEleCT, Educational publication, 210 pages, Published by ČVUT Praha, ISBN: ISBN:978-80-01-04949-5, September 2011, CD version.
- [4] Podhradský, P., Mikóczy, E., Dúha, J., Trúchly, P., at al: NGN – Selected topics, LdV IMProVET. Educational publication, 137 pages, Published by ČVUT Praha, ISBN: 978-80-01-05295-2, August 2013, CD versions (SK, EN, CZ).

- [5] Nadeau, T. D., Gray, K.: SDN: Software Defined Networks. O'Reilly Media. 2013. ISBN: 978-1-449-34230-2.
- [6] Helebrandt, P., Kotuliak, I.: Novel SDN multi-domain architecture. In IEEE 12th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp.139-143, 2014.
- [7] Open Networking Foundation: Software-Defined Networking: The New Norm for Networks. White Paper, 2012
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>.
- [8] McKeown, N.: OpenFlow and Software Defined Networks. online, Presentation. 2011
http://www.openflow.org/documents/OpenFlow_2011.pps.
- [9] Open Networking Foundation. <https://www.opennetworking.org>.
- [10] McKeown, N. et al.: OpenFlow: Enabling innovation in campus networks. In: ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp.69-74, 2008.
- [11] Open Networking Foundation: OpenFlow Switch Specification version 1.3.5. 2015
<https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-switch-v1.3.5.pdf>.
- [12] Dong; L., Gopal, R., Halpern, J.: Forwarding and Control Element Separation (ForCES) Protocol Specification. IETF RFC 5810, 2010.
- [13] Chiosi, M., Clarke, D., Willis, P., Reid, A., Feger, J., Bugenhagen, M., Khan, W., at al.: Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges & Call for Action. SDN and OpenFlow World Congress, 2012.
https://portal.etsi.org/nfv/nfv_white_paper.pdf.
- [14] Chiosi, M., Wright, S., Clarke, D., Willis, P., at al.: Network Functions Virtualisation: Network Operator Perspectives on Industry Progress. SDN and OpenFlow World Congress, 2013. https://portal.etsi.org/nfv/nfv_white_paper2.pdf.
- [15] ETSI GS NFV-INF 001 V1.1.1, Network Functions Virtualisation: Infrastructure Overview. Specification, 2015. http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf.
- [16] ETSI GS NFV-MAN 001 V1.1.1, Network Functions Virtualisation: Management and Orchestration. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf.
- [17] ETSI GS NFV-SWA 001 V1.1.1, Network Functions Virtualisation: Virtual Network Functions Architecture. Specification, 2014. http://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf.

- [18] SdxCentral:Network Functions Virtualization Report. 2015.
<https://www.sdxcentral.com/reports/network-functions-virtualization-report-2015/>.
- [19] Gruber C. G.: CAPEX and OPEX in Aggregation and Core Networks. In: Optical Fiber Communication, IEEE, 2009, pp. 1-3.
- [20] Strategy Analytics: Global Internet Device Installed Base Forecast. August 2014.
<https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609>.
- [21] Wu, Y. et al.: CloudMoV: Cloud-Based Mobile Social TV. In: IEEE Transactions on Multimedia, vol.15, 2013, pp. 821-832.
- [22] Roberts, J.: The clean-slate approach to future Internet design: a survey of research initiatives. *annals of telecommunications - annales des télécommunications*, Volume 64, Issue 5, 2009. pp 271-276.
- [23] Banniza, T.R., Boettle, D., Klotsche, R., Schefczik, P., Soellner, M., Wuenstel, K.: A European Approach to a Clean Slate Design for the Future Internet. *Bell Labs Technical Journal - Core and Wireless Networks*, Volume 14 Issue 2, August 2009. pp. 5-22.
- [24] McKeown, N. et al.: Openflow: Enabling innovation in campus networks. In: *SIGCOMM Computer Communication Review*, vol.38, no.2, 2008, pp. 69-74.
- [25] Bashker, D., Cascio, W., Boudreau, J.: *How to Apply HR Financial Strategies (Collection)*, Addison Wesley. Chapter 1, August 2013, ISBN 9780133743173. pp. 6-10.
- [26] Barroso, L. A., Clidaras, J., Hölzle, U.: *The Datacenter as a Computer: An Introduction to the Design of Warehouse-Scale Machines - Second Edition*. Morgan & Claypool. Chapter 6., pp. 69-71, 2013, ISBN 9781627050104.
- [27] Tits, Y.: Lack of standardization concerning interfaces between network equipments. In: *Electricity Distribution (CIRED 2013)*, 22nd International Conference and Exhibition on, IET, 2013, pp. 1-4.
- [28] McKeown, N., Girod, B.: *Clean-Slate Design for the Internet A Research Program at Stanford University*. White paper Version 2.0, 18 April 2006.

Indice

1	Introducción.....	8
2	Evolución de la arquitectura NGN hacia arquitecturas de Red Futura.....	9
2.1	Conceptos y arquitecturas NGN.....	11
2.2	Capas de modelo conceptual.....	13
3	Redes definidas por software, Software Defined Networking (SDN).....	14
3.1	Introducción a las SDN.....	14
3.2	Separación de control de red de datos y el plano de reenvío.....	16
3.3	Control centralizado y la programación de la Red.....	18
3.4	Comparación del plano de control distribuido de las redes tradicionales.....	19
3.5	Protocolos SDN.....	21
4	Network Functions Virtualization (NFV) (virtualización de funciones de red).....	25
4.1	¿Qué ha permitido NFV?.....	27
4.2	Requisitos de la NFV.....	28
4.3	Arquitectura NFV.....	29
4.4	La infraestructura NFV - NFVI.....	30
4.5	Gestión y organización NFV (MANO).....	31
4.6	Arquitectura de software - funciones de red virtualizada, Virtualized Network Functions (VNF),.....	32
4.7	Los casos de uso para NFV.....	33
5	Futuro de Internet.....	35
5.1	Limitaciones de Internet.....	36
5.2	Características del nuevo Internet.....	38
5.3	Rediseño de las Tecnologías de Internet.....	39

1 Introducción

Un nuevo tema en el ámbito de las tecnologías de información y comunicación es una mayor evolución de las tecnologías hacia las futuras redes **NGN** (*Next Generation Networks, redes de nueva generación*). Hay varios aspectos que influyen en la arquitectura NGN basada IMS real para mejorar las funcionalidades adicionales para la próxima generación de servicios multimedia. El rápido desarrollo de los servicios de Internet y servicios de distribución de contenidos a través de redes heterogéneas están cambiando los requisitos de diferentes aspectos como funciones adicionales, la movilidad, la virtualización y el intercambio de recursos, la seguridad, la simplificación de la arquitectura y la flexibilidad en los modelos de control con sensibilidad al contexto.

Recientemente los debates en curso sobre los cambios de las arquitecturas de Internet (Internet del Futuro) también en el área de las telecomunicaciones para las *futuras redes, Future Networks (FN)* se están ejecutando en proyectos de investigación, así como a través de la normalización (UIT-T, ETSI).

2 Evolución de la arquitectura NGN hacia arquitecturas de Red Futura

Se han identificado 2 corrientes principales de desarrollo potencial:

1. Enfoque de pizarra limpia o principio de revolución - El futuro de Internet, donde la nueva arquitectura y protocolos de Internet del futuro serán definidos y diseñados de nuevo (nuevos escenarios de red, modelos de nuevos protocolos y pruebas de los modos de arquitectura revolucionaria), [1]. Se espera un salto revolucionario como si Internet hubiera sido diseñado desde el enfoque borrón y cuenta nueva, por las nuevas tecnologías, no limitado por los conceptos actuales.
2. Concepto evolutivo donde arquitecturas NGN existentes se ven reforzadas por los nuevos requisitos y las funciones que llevan al concepto denominado Redes Futuras [1], [2]. La evolución NGN puede alcanzar capacidades esperadas de las futuras redes utilizando los protocolos y las capacidades de las NGN existentes (habilitado solo con la necesaria mejora de los mecanismos de la arquitectura y de control).

El segundo concepto es el enfoque más realista hacia las redes de futuro desde el punto de vista de la migración en las redes y tecnologías NGN que ya están disponibles.

Es conveniente examinar la evolución para delinear tendencias futuras de NGN y las cuestiones pendientes que hay que resolver también. Los escenarios de migración de diferentes tipos de plataformas de redes se basan en la idea de integrar plataformas TDM e IP en una plataforma convergente de las NGN (desde el punto de la infraestructura de red, así como los servicios). Nuevos conceptos y arquitecturas de nueva generación de las TIC basadas en las TIC convergentes y ofrecer a los NGN operadores nuevas oportunidades para poner en práctica y proporcionar una amplia gama de servicios multimedia y aplicaciones.

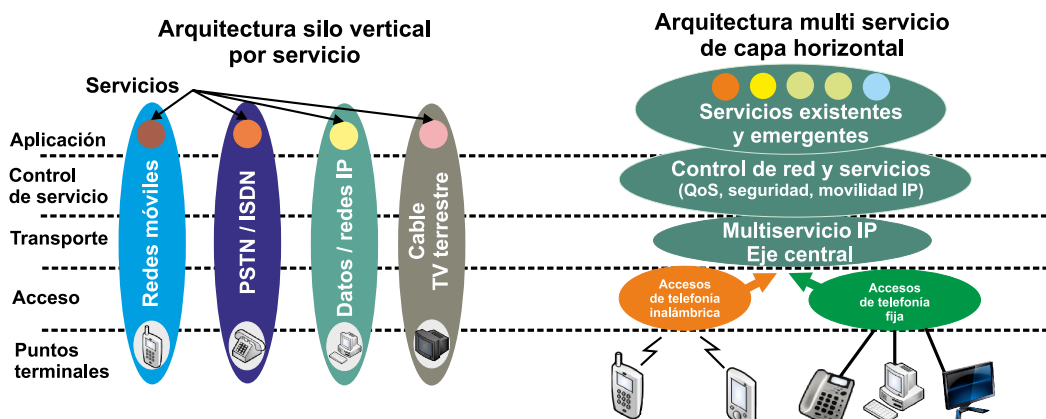


Fig. 1 – De silos verticales a arquitectura NGN horizontal [1]



Por lo tanto, los operadores pueden pasar de la arquitectura silo vertical donde cada tipo de servicio ha dedicado el acceso, el transporte, el control y la infraestructura de aplicaciones por servicio, a la arquitectura orientada horizontalmente más independiente de los servicios prestados (Fig. 1) .

2.1 Conceptos y arquitecturas NGN

Los principales principios de la NGN (Next Generation Networks), se formaron cuando surgió la propia idea del NGN. Las siguientes dos definiciones de ETSI e ITU-T describen NGN en detalle.

$E=m \cdot c^2$

ETSI describe NGN como concepto para la definición y el establecimiento de las redes, lo que permite una distribución formal de funcionalidades en capas y planos separados mediante el uso de interfaces abiertas. El concepto de NGN ofrece nuevas condiciones para la creación, implementación y gestión eficaz de los servicios innovadores. UIT-T NGN se describe como una red basada en la transferencia de paquetes, lo que le permite la prestación de servicios, incluidos los servicios de telecomunicaciones, y es capaz de utilizar varias tecnologías de transmisión de banda ancha que permitiendo garantizar QoS. Las funciones relacionadas con los servicios son al mismo tiempo independientes de las tecnologías de transmisión básicas. NGN proporciona acceso de usuarios ilimitado a diferentes proveedores de servicios. Es compatible con la movilidad general proporcionando a los usuarios la consistencia y la disponibilidad de los servicios.

Eso es lo que dicen las definiciones, pero probablemente con el tiempo las ventajas NGN son de mayor importancia. Vale la pena mencionar algunos de los requisitos a los que la NGN debe ajustarse:

- Separación de gestión de las funciones de las características de transmisión. Separación de aprovisionamiento de servicios de la red,
- Soporte para una amplia gama de servicios y aplicaciones,
- Las capacidades de banda ancha, cumplimiento de los requisitos de QoS (Calidad de Servicio),
- Varios tipos de movilidad (usuarios, terminales, servicios),
- Varios esquemas de identificación y el tratamiento,
- Servicios entre redes fijas y móviles convergentes (así como voz, datos y la convergencia de vídeo),
- La conformidad con los requisitos de regulación, tales como las llamadas de emergencia y requisitos de seguridad,
- Tecnologías más baratas y más eficaces.

—

Respecto a los conceptos NGN, las instituciones encargadas de estandarizar están resolviendo los siguientes aspectos y problemas:

- redes existentes de migración hacia las NGN,
- el desarrollo en el campo de las tecnologías de acceso,
- conexión de otras redes a las redes IP,

- prestación de servicios y el desarrollo de otros nuevos,
- interfuncionamiento en el área de direccionamiento,
- interoperabilidad de los sistemas de señalización,
- itinerancia y la movilidad.

Hay muchos modelos conceptuales y arquitecturas de referencia, tanto para las redes convergentes y arquitecturas VoIP. Por lo tanto, hemos tratado de encontrar rasgos comunes y definir un modelo conceptual adecuado para NGN. Uno de los objetivos del modelo conceptual es determinar capas funcionales (que cubren funcionalidades similares), sus entidades, puntos de referencia (interfaces) y los flujos de información entre ellos. Dicho modelo puede entonces ser asignado más fácilmente en la arquitectura de referencia física (y es independiente de las entidades físicas, es decir, componentes de la arquitectura).



En la mayoría de casos analizados las capas modelo conceptuales NGN están, desde el punto de vista de las funciones, divididas en partes independientes de la siguiente manera (Fig. 2): el acceso (algunas arquitecturas de referencia no incluyen directamente en el modelo NGN ni lo sustituyen por la adaptación), el transporte (transmisión, conmutación), control (llamar / sesiones de control) y de aplicaciones (servicios).

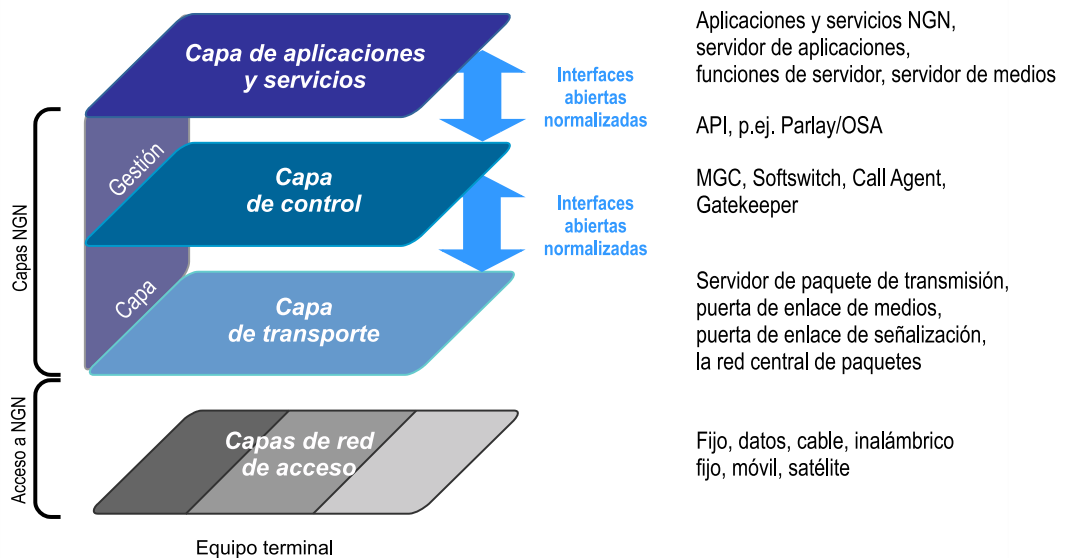
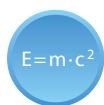


Fig. 2 – Modelo conceptual NGN y sus capas funcionales

2.2 Capas de modelo conceptual



La **capa de acceso** proporciona la infraestructura, por ejemplo una red de acceso entre el usuario final y la red de transporte.

La **capa de transporte** asegura el transporte entre los nodos individuales (puntos) de la red.

La **capa de control** incluye el control de los servicios y elementos de red. Esta capa es responsable de la puesta a punto / el establecimiento, control y cancelación de la sesión multimedia.

La **capa de servicio** ofrece las funciones de servicio básicos, que pueden ser utilizados para crear servicios y aplicaciones más complejas y sofisticadas.

En la NGN se requiere que el control de la red no esté determinada únicamente por las aplicaciones de equipos terminales, pero que la inteligencia de la red pueda llevar a cabo el control de la red en todos los niveles del modelo de referencia. El modelo de referencia de gestión de red implica las siguientes **tareas para la inteligencia de la red** que tiene que garantizar:

- Gestión de recursos (capacidad, puertos, y los elementos físicos) y QoS en el acceso a la red y en la red de transporte, según sea necesario.
- Varios procesados del medio, codificación, transferencia de datos (flujos de información).
- Gestión de llamadas y conexión. Gestión y la interoperabilidad de todos los elementos de la arquitectura de referencia.
- Control de Servicio.

El concepto de NGN y arquitecturas están descritos con más detalle en [3], [4].

Hay varios conceptos y tendencias de evolución que conducen a nuevas arquitecturas de red que son capaces de proporcionar el amplio espectro / cartera de nuevos servicios / contenidos multimedia.

Nuevas arquitecturas de red basadas en "redes definidas por software, Software Defined Networking" y "Funciones de red de virtualización" se introducen y se describen en el capítulo 3 y 4, respectivamente, y el concepto de "Internet del Futuro" en el capítulo 5 de este "módulo de aprendizaje"

3 Redes definidas por software, Software Defined Networking (SDN)

3.1 Introducción a las SDN

$E=m \cdot c^2$

SDN (*Software Defined Networking* *redes definidas por software*.) es un nuevo enfoque de la arquitectura de red de las TIC con el objetivo de controlar la programación de toda la red.

Esto permite la solución de muchos problemas en los enfoques tradicionales para la creación de redes a la vez que permite nuevas características. En general, la idea de la SDN es aumentar la flexibilidad, capacidad de gestión y capacidad de ampliación de las redes de TIC, con el objetivo secundario de la disminución de los costos de equipo. Esto se puede lograr mediante el aprovechamiento de desarrollo rápido y ciclo de despliegue de aplicaciones de software relativamente baratos en contraste con el costoso hardware especializado de redes.

La principal motivación para la SDN en un principio surgió de la necesidad de una mejor solución para la innovación en la investigación y desarrollo de la red. En ese momento, sólo había dos métodos disponibles para probar nuevas características - software de simulación o bancos de pruebas de hardware.

+

La simulación ofrece gran flexibilidad y repetibilidad.

-

Sin embargo, las simulaciones por lo general no se ejecutan en tiempo real - en paralelo con la producción de código, y no es fácil conectar la red simulada a la red real y probar la coexistencia de las nuevas características en un entorno más realista. Por otra parte, los bancos de pruebas llevadas a cabo con hardware personalizado son difíciles de programar, puede ser difícil de modificar una vez establecido y son muy caros.

Esto puede conducir a compromisos en su adopción - ya sea usando un banco de pruebas compartido utilizado por más proyectos de investigación que limita el tiempo disponible para experimentos y repetibilidad, o, alternativamente, creando un propio banco de pruebas utilizando dispositivos de red tradicionales que ofrecen los proveedores de equipos. Éstos se suministran sobre todo como una caja negra con una personalización mínima, lo que limita la capacidad del banco de pruebas para experimentos nuevos y más exóticos necesarios para innovaciones más revolucionarias que las evolutivas.

A finales de los 90 y principios del 2000, la potencia de cálculo de los ordenadores de propósito general aumentó significativamente en comparación con el hardware de red especializado. Esto está relacionado con los avances en la virtualización y algunas otras tecnologías dirigidas a su utilización en la ejecución para el control del software implementado de nodos de red simples que se usan para la

conmutación rápida de paquetes. El software de control podría modificarse tan fácilmente como la simulación, mientras que el hardware barato con características limitadas de alto nivel utilizados para la conmutación de paquetes proporciona tasas de manipulación de paquetes comparables a los bancos de pruebas de hardware personalizado. Fue uno de los pilares centrales de la SDN, que se encuentra en la separación de los planos de control y reenvío que se describe en la siguiente sección con más detalle [5].

3.2 Separación de control de red de datos y el plano de reenvío

Antes de describir el concepto de la SDN, es necesario definir lo que son el plano de control y el plano de datos de reenvío.

$E=m \cdot c^2$

En la mayoría de los routers (o cualquier equipo de red para el caso) no hay un hardware especializado para la conmutación rápida de datos entre las interfaces – Plano de reenvío de datos. El reenvío es administrado por reglas creadas por el procesador que ejecutan el sistema operativo, los algoritmos de enrutamiento, traducción de direcciones y otras funciones superiores - este es el plano de control.

i

En las redes tradicionales, tanto en el plano de control como en el de reenvío se implementan en cada nodo de la red. Esto permite que cada dispositivo sea totalmente autónomo y tome todas las decisiones de alto nivel, como el enrutamiento de paquetes de forma independiente.

Esto se deriva del origen de la Internet - ARPANET, inicialmente diseñado por y para los militares con alta resistencia y capacidad de supervivencia como principal preocupación. La flexibilidad, la modificación directa o la adopción de nuevas características eran como mucho un objetivo secundario.

El principio fundamental de SDN es la separación del plano de control y datos de reenvío en la red tal y como se representa en la Fig. 3. Mediante la implementación de planos de control separados por el software para ordenadores de propósito general desde el plano de reenvío en los equipos de red, es posible el encaminamiento centralizado y las decisiones de conmutación, así como la configuración de todos los dispositivos de red.

+

El plano de control centralizado implementado en software ejecutado en los procesadores de propósito general puede traer muchas ventajas a la creación de redes - sobre todo la aceleración de la innovación, las nuevas características de desarrollo y despliegue.

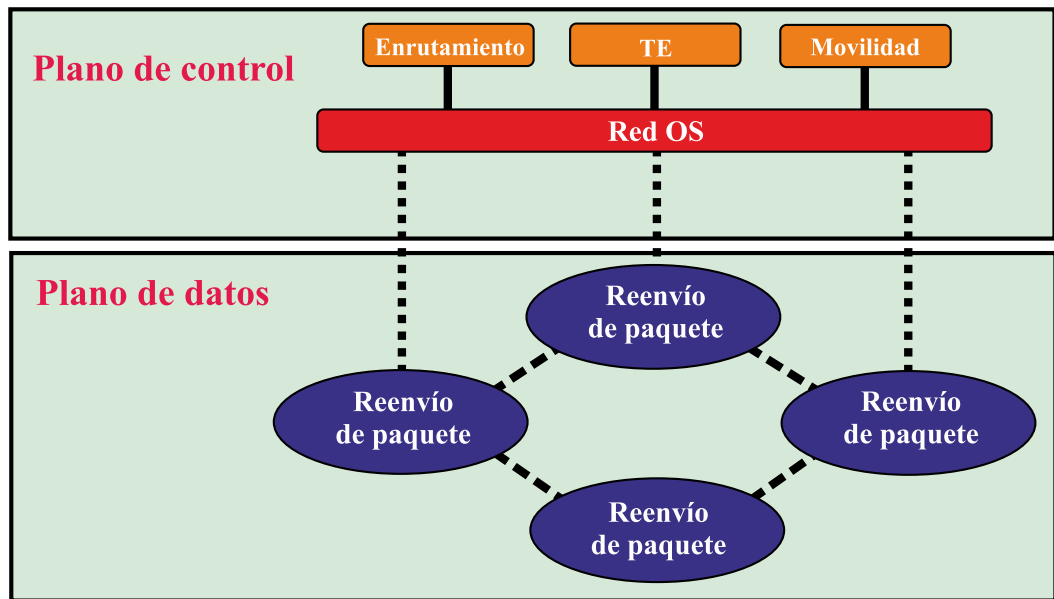


Fig. 3 – Arquitectura básica SDN

3.3 Control centralizado y la programación de la Red

En los equipos de red moderna el plano de control obtiene información sobre el estado de las conexiones a los vecinos y de la red en su conjunto que se suministra a los algoritmos de enrutamiento. Los algoritmos distribuidos proporcionan una solución automática para el tráfico de red de enrutamiento, pero uno de sus defectos es un posible problema con la convergencia. Dado que cada dispositivo recopila información acerca de la red y toma decisiones de enrutamiento por sí mismo, el retraso en la propagación de información sobre cambios en la red puede dar lugar a problemas de funcionamiento de la red.



La eliminación del plano de control de cada nodo de la red y el uso del plano de control centralizado no sólo permite una visión completa de la red sin dificultades con la convergencia inherente a algoritmos de encaminamiento distribuido, sino que también disminuye el coste. Además, sin necesidad de encaminamiento de tráfico distribuido, nuevos algoritmos pueden ser utilizados, modificados y desarrollados. Por otra parte, la configuración del plano de control central hace más simple la gestión de red, eliminando la necesidad de configurar cada nodo separado. Esto reduce la posibilidad de errores de configuración y también acelera la resolución de problemas. El beneficio añadido de la implementación del software de plano de control centralizado es la facilidad de modificación y el desarrollo de nuevas características.



Sin embargo, los opositores del SDN y del plano de control centralizado sobre todo apuntan a los límites de su capacidad de uso en redes de gran escala, tales como Internet. Sus críticas se centran en que el controlador sea el único punto de fallos para toda la red e insuficiente escala.

La solución de estos problemas es utilizar el plano de control centralizado lógicamente, pero físicamente distribuido - donde una serie de controladores de gestión de la parte de la red se comunican entre sí para reducir la latencia del plano de control, proporcionar una alta disponibilidad y un solo punto de administración lógico de la administración de la red. La nueva arquitectura para la conexión interdominio con el protocolo de comunicación asociado para los controladores SDN se propone en [6].

3.4 Comparación del plano de control distribuido de las redes tradicionales

El equipo de red tradicional incorpora el plano de control, las aplicaciones de red y otras funciones de nivel superior en el firmware del dispositivo. Esto significa que todos los nodos de la red toman decisiones de enrutamiento local – utilizando de manera eficaz el plano de control totalmente distribuido, como se muestra en la Fig. 4. Esto se puede contrastar con el plano de control centralizado en la arquitectura SDN, que se muestra en la Fig. 3.



La integración de muchas funciones proporciona una mayor funcionalidad de cada nodo y los hace más independientes, casi eliminando los puntos únicos de fallo.



Pero se consigue a expensas de una mayor complejidad que se correlaciona con el equipo más caro; mayor consumo de energía y puede dar lugar a retrasos en el tratamiento de tráfico causado por la necesidad de procesar varias aplicaciones. Además, la configuración o la modificación de la red requiere la configuración manual de muchos dispositivos y, a menudo el uso de herramientas de gestión complejas. La gestión de redes se complica de manera adicional a causa de la implementación y la configuración de disparidades entre los diferentes proveedores que causan problemas de interoperabilidad.

Como se afirma en [7], toda esa complejidad conduce a las redes estáticas, lo que está en contraste con la necesidad de un entorno dinámico con una mayor movilidad de los usuarios y la virtualización de servidores. Las inconsistencias en las políticas de toda la red y escalabilidad de red limitada son otros efectos de complejidades tradicionales de la red en redes de gran tamaño.



El plano de control centralizado en SDN permite al administrador de la red la forma de tráfico sin la necesidad de configurar manualmente muchos dispositivos, proporcionando así la gestión más fácil de redes y una mayor flexibilidad.

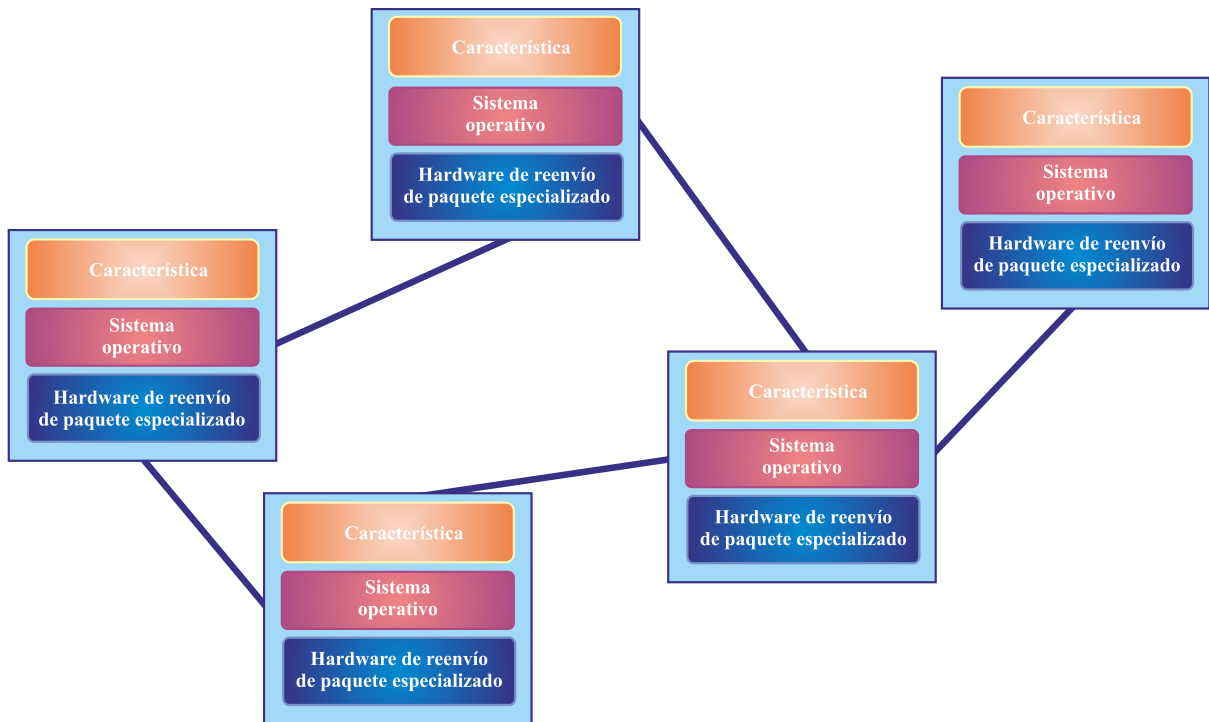


Fig. 4 - Arquitectura de red de paquetes tradicionales [8]



Aunque el MPLS es superficialmente similar a SDN con conmutación rápida de los flujos de tráfico establecido por el plano de control, lo hace de una manera diferente. No hay plano de control centralizado, que está en cada router MPLS con cada LER capaz de crear un camino y distribuirlo mediante el protocolo de distribución de etiquetas (LDP).

3.5 Protocolos SDN

La separación del plano de control y transmisión de datos - uno de los pilares centrales de SDN junto con la centralización de plano de control significa que hay una necesidad de protocolo de comunicación. En esta sección se presentan algunas de ellas, empezando por el más popular – *OpenFlow* (flujo abierto).

OpenFlow (flujo abierto)

OpenFlow es un estándar abierto desarrollado originalmente en las universidades y en la actualidad mantiene por la *Open Network Foundation (ONF) Fundación Red Abierta* [9] - un consorcio sin ánimo de lucro con la misión de comercializar y promover SDN basado en OpenFlow. ONF ha tenido un éxito espectacular, con OpenFlow es el protocolo más utilizado para la comunicación entre el plano de control y reenvío de datos plano - convirtiéndose en el estándar de facto. Sin embargo, esta campaña ONF llevó a muchos malentendidos haciendo indicar que OpenFlow es igual a SDN.



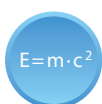
A pesar de las soluciones basadas en software de conmutación existentes que permiten la investigación de nuevos métodos y protocolos de red, la mayoría no proporciona el suficiente rendimiento computacional y / o densidades de puerto para experimentos a gran escala.

El más simple de los ejemplos son muchas implementaciones basadas en software abierto de enrutamiento o protocolos de conmutación que se ejecutan en ordenadores de propósito general con varias interfaces de red. Estas técnicas se pueden clasificar en el primer grupo que es el de falta de rendimiento, en comparación con los equipos de red dedicada. En el otro extremo del espectro se encuentran soluciones de investigación de redes basadas en hardware como la utilización de la tarjeta FPGA especializada NetFPGA para su procesamiento a velocidad de línea del tráfico.



La NetFPGA se utiliza principalmente en el ámbito académico y de prototipado rápido, ya que se limita a sólo 4 puertos por tarjeta.

Como se menciona en [10] estos factores son limitantes para los investigadores de redes académicas, con OpenFlow siendo un compromiso entre la generalidad de bajo rendimiento y la libertad de soluciones de investigación y muy modificable de alto rendimiento cerrada y no de equipos de redes de proveedores comerciales.



El protocolo OpenFlow define la interfaz de comunicación entre los dispositivos del plano de control y de expedición y lo que debe ser aplicado por ambos lados. Desde OpenFlow se proporciona un control muy granular en función de cada flujo, que permite a la red reaccionar a cambios en la topología, aplicación o usuario, en tiempo real.

El libro Blanco de la ONF [9] señala que las soluciones de enrutamiento de red clásicas actuales no son compatibles con el control en este nivel de la granularidad.

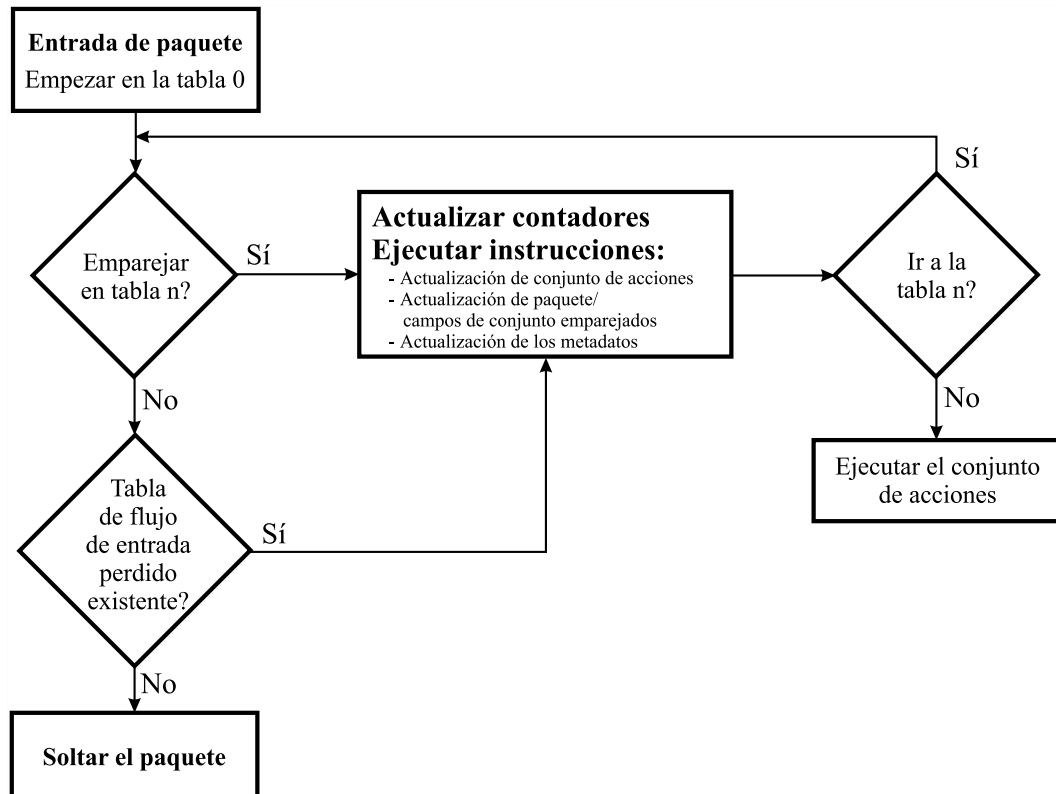
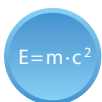


Fig. 5 - Diagrama de flujo que detalla el manejo de paquetes en el switch lógico OpenFlow [11]

Cuando se recibe un paquete por el interruptor OpenFlow habilitado, se trata en la tubería de OpenFlow compuesta de una o más tablas de flujos, cada una con entradas que contienen normas y acciones a realizar en el paquete que pertenece a fluir. Si no se encuentra el emparejamiento del paquete en cualquier Mesa de flujo y la regla para enviar los paquetes desconocidos al regulador es puesta a punto, se envía al controlador. El controlador procesa el paquete y, o bien abandona el paquete o bien establece un nuevo flujo, mediante la creación de una nueva entrada en la tabla de flujo. El mecanismo de manejo de un paquete recibido en el interior del interruptor de OpenFlow está trazado en la Fig. 5.

ForCES



El protocolo de *reenvío y control de separación de elementos* (*Forwarding and Control Element Separation*) (**ForCES**) [12] define un marco arquitectónico y protocolos asociados para estandarizar el intercambio de información entre el plano de control y el plano de reenvío en un elemento de red ForCES.

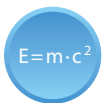
ForCES se refiere principalmente a la API / protocolo abierto que proporciona una clara separación entre los planos de control y de reenvío.



La principal fortaleza de ForCES radica en su modelo de reenvío de elementos que permite la descripción de nuevas funcionalidades del plano de reenvío sin cambiar el protocolo entre los planos de control y reenvío.

El desarrollo de ForCES está dirigido a dividir el dispositivo de red en los planos de control distinto y de reenvío. La motivación detrás de esto surgió del deseo de construir un plano de reenvío de elementos de red de componentes de hardware flexibles independientemente del plano de control. Esto da lugar a ForCES creando una nueva arquitectura para los dispositivos de red, mientras que OpenFlow tiene como objetivo crear una nueva arquitectura de red.

NETCONF



NETCONF es un protocolo de gestión de red que proporciona mecanismos para instalar de forma remota, manipular y eliminar la configuración de dispositivos de red.

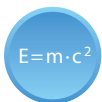
El protocolo NETCONF protocolo en sí mismo se divide en cuatro capas con un conjunto de operaciones de protocolo de base utilizando métodos **RPC** (*Remote Procedure Call, llamada de procedimiento remoto*) con parámetros de mensaje XML codificado.

Uno de los objetivos de NETCONF es proporcionar una interfaz de programación al dispositivo que sigue de cerca la funcionalidad de interfaz nativa del dispositivo.



A pesar de que fue desarrollado inicialmente como un sucesor de SNMP y de algunos de los protocolos de la CLI para la configuración de elementos de red, las capacidades NETCONF se pueden utilizar para crear una forma de SDN híbrido. Por otra parte, el apoyo NETCONF es un requisito para los dispositivos de red para que sean compatibles con una parte de OF-CONFIG de la especificación OpenFlow.

PCE-P



El *Path Computational Element (PCE) (Elemento de ruta computacional)* es una entidad que calcula rutas en nombre de los nodos de la red que pueden encontrar rutas óptimas para los tráficos MPLS y GMPLS P2P y P2MP de ingeniería *label switched paths (LSPs) (caminos de conmutación de etiquetas)*.

PCE comunica entonces este camino de nodos de red con el protocolo de comunicación PCE. Por lo tanto, PCE también se puede percibir como extender las capacidades MPLS y GMPLS TE reduciendo la brecha entre SDN y el estándar MPLS / GMPLS.

Aunque PCE en sí mismo no se ha desarrollado principalmente como una tecnología que permite SDN, puede proporcionar lógicamente un modelo de gestión centralizado para las tecnologías existentes con un poco de mejora adicional.

Interfaz con el sistema de enrutamiento

Interface to the Routing System (I2RS) (*interfaz con el sistema de enrutamiento*) es uno de los enfoques más ambiciosos a SDN que todavía está en las primeras etapas, siendo desarrollado por el IETF. El I2RS es una interfaz de programación bidireccional para la comunicación entre el sistema de enrutamiento y aplicaciones - permitiendo supervisión de la red, la reserva de recursos y modificación de la configuración de enrutamiento. El I2RS se ocupa de la comunicación hacia y desde el sistema de enrutamiento, no es la intención proporcionar interfaces directas para el plano de reenvío, haciendo uso de los mecanismos existentes para distribuir rutas seleccionadas en plano de reenvío.

Cisco ONE (Cisco UNO)

A pesar de que Cisco es una parte de la Open Networking Foundation (fundación de redes abiertas) y está participando activamente en el desarrollo OpenFlow, no es el único proyecto SDN que se está trabajando. Una de sus alternativas propietarias es una red abierta para el Medio Ambiente *Open Network Environment* (Cisco **ONE**), que está proporcionando interfaz de programación para controlar directamente los equipos de Cisco. El componente clave de Cisco se trata de una plataforma *ONE Platform Kit (onePK)* - kit de desarrollo que incluye varias APIs de la plataforma, lo que permite un fácil desarrollo de aplicaciones de red mediante el acceso directo a los equipos de red a través de la capa de abstracción de red.

Nuage

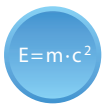


En abril de 2013 Alcatel-Lucent puso en marcha la empresa spin-out Redes Nuage con el propósito de crear una solución SDN basado en su anterior Application Fluent Network (red fluida de aplicación), pero con la libertad de utilizar tecnologías alternativas frescas. El producto de este esfuerzo es Nuage Virtualized Service Platform (plataforma de servicios Nuage virtualizada), una solución de software que se centra en el problema de la virtualización de la red de centros de datos y proveedores de servicios cloud *Cloud Service Providers (CSPs)*. Debido a que la VSP Nuage se implementa en software y utiliza VXLAN como la encapsulación a través de hipervisores, no es dependiente de un tipo o marca de interruptores TOR específico para funcionar.

4 Network Functions Virtualization (NFV) (virtualización de funciones de red)

Una parte integral de los operadores Telco (operadores de telecomunicaciones) son dispositivos de hardware propietario. Telco (operadores de telecomunicaciones) no evita la compra de nuevo hardware con la misma funcionalidad y los servicios, ya que se requieren estos dispositivos para la prestación de nuevos servicios. Presenta muchas complicaciones asociadas tanto con los costos crecientes y con las exigencias de tiempo de este despliegue, como con el **TTM** (*time to market*) (tiempo de comercialización) y el **TTD** (*time to deploy*) (tiempo de implementación). Estas complicaciones se están convirtiendo hoy en día para los operadores de telecomunicaciones, en factores limitantes a proporcionar la calidad de los servicios.

Fig. 6 ilustra un nuevo enfoque en la arquitectura de red basada en la virtualización de las funciones de red, *Network Functions Virtualization* (NFV).



Este enfoque proporciona a los operadores de red / telecomunicaciones la oportunidad de consolidar muchos tipos de equipos de red en la industria estándar de servidores, conmutadores y almacenamiento de alto volumen, que podrían estar ubicados en centros de datos, nodos de la red y en las instalaciones del usuario final.

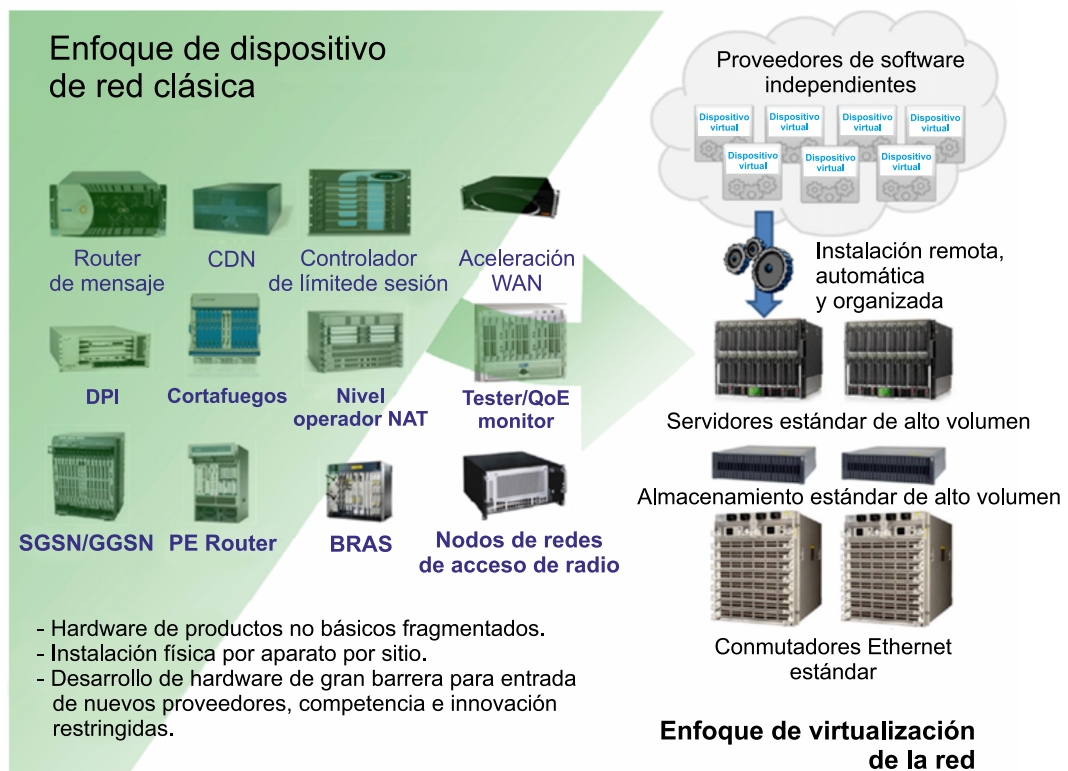


Fig. 6 – Visión de la virtualización de las funciones de red [13]



Beneficios para los operadores de red / telecomunicaciones:

- La reducción de **CAPEX** (*capital expenditure, gastos de capital*) y **OPEX** (*operational expenses, gastos operativos, como la reparación y mantenimiento*) mediante la reducción del coste de los equipos y la reducción del consumo de energía,
- Menor tiempo de comercialización para el despliegue de nuevos servicios de red
- Mejor rendimiento de la inversión de nuevos servicios,
- Mayor escalabilidad de la flexibilidad o servicios de revelado
- Oportunidades para las pruebas y el despliegue de nuevos servicios innovadores con menor riesgo.

En octubre de 2012 se publicó el documento que presentó el primer proyecto de NFV [13]. ETSI expuso los diversos requisitos que se necesitan en la tecnología y describe los beneficios que vienen con la tecnología NFV y que esta tecnología debe traer. El grupo de especificación de la industria de virtualización, *Functions Virtualization Industry Specification Group (NFV ISG)* ha sido creado para cubrir todas las tareas relacionadas con las nuevas tecnologías que han surgido. Este grupo fue creado por el Instituto Europeo de Normas de Telecomunicaciones, *European Telecommunications Standards Institute (ETSI)*. A partir de octubre de 2012, el Grupo ISG NFV se incrementó gradualmente y alrededor de 235 empresas realizadas asistieron a varias reuniones en Asia, Europa y América del Norte. Las salidas de la primera reunión del grupo NFV ISG eran en forma de documentos, y se emitieron en octubre de 2013. Los documentos cubren toda la arquitectura NFV con todos los componentes y las interfaces entre ellos anotados. A partir de 2013 hasta 2015 este grupo corrió la segunda fase y los documentos más recientes están disponibles directamente en el sitio web NFV ISG.

4.1 ¿Qué ha permitido NFV?



Si es posible construir redes de una manera que representa la tecnología NFV, la pregunta lógica que se plantea es porqué la red, desde el comienzo mismo de su creación, utiliza hardware propietario. La respuesta es que los servidores estándar de la industria con el sistema operativo y el software han adquirido recientemente un alto rendimiento para poder competir eficazmente con los dispositivos patentados, particularmente en términos de precios, el consumo de electricidad y la fiabilidad.

Podemos especificar el tiempo "Recientemente" hasta los últimos cuatro o cinco años. Durante este periodo, hemos sido testigos de una notable mejora en el rendimiento de la red y el rendimiento de procesamiento de paquetes de procesadores x86, así como aumentar rápidamente el número de núcleos de procesador disponible en un único servidor industrial de dispositivo físico.

4.2 Requisitos de la NFV

Listado de los requisitos esenciales que NFV debería cumplir [13]:

- Portabilidad - habilidades para resolver la carga y puesta en marcha de las funciones de software en movimiento a través de varios centros de datos estándar.
- Rendimiento - funciones de software objetivos de rendimiento.
- Gestión y organización - mecanismos que deben existir para las funciones de organización y gestión del ciclo de vida de software, recursos, infraestructura y diversas operaciones para hacerlas.
- Flexibilidad - capacidad para proporcionar soluciones más fáciles de escalabilidad de los recursos de hardware.
- Seguridad - las dimensiones fijas que se deben analizar, ya que el entorno de virtualización puede ser sometido a los ataques externos.
- La continuidad de los servicios - funciones que son necesarias para la provisión continua de servicios de acuerdo con la especificación del acuerdo de nivel de servicios de *Service Level Agreement (SLA)*.
- Operaciones - automatización de las funciones operativas (por ejemplo, la adaptación de la capacidad de la red, actualización de software descargable, reparación de averías detectadas, etc.).
- La eficiencia energética - ayudará a minimizar el consumo de energía de las grandes redes virtualizadas.
- Migración y coexistencia con las plataformas existentes - apoyar la transición de las redes actuales, donde la red no virtualizada coexiste con la virtualizada sin interrupción de los servicios u otros efectos desagradables en el usuario.

La capacidad de despliegue remoto y la operación de las funciones de red virtualizadas en la infraestructura NFV proporcionada por diferentes proveedores de servicios permite un servicio eficiente a los clientes en todo el mundo.

4.3 Arquitectura NFV

La tecnología de la architecture of NFV fue diseñada en la segunda edición de papel blanco [14] (Fig. 7) y consiste en los siguientes componentes:

- **NFVI** (*virtualized network functions infrastructure*, infraestructura de las funciones de red virtualizadas) - ofrece los recursos virtuales necesarios para apoyar la implementación de las funciones de red virtualizadas - componentes de hardware COTS comerciales para la aceleración, capa de software que virtualiza y abstrae el hardware subyacente.
- **VNF** (*virtualized network feature*, función de red virtualizada) - implementación de software de funciones de red que es capaz de correr por NFVI y puede estar acompañada por EMS - Element Management System, sistema de gestión de elementos, que gestiona el VNF. VNF es una entidad correspondiente al nodo de red de hoy en día, que se espera que sea entregado como un software independiente del hardware puro.
- **NFV MANO** (*management and orchestration*, gestión y organización) - cubre la organización y el ciclo de vida de la gestión de herramientas físicas y / o software que soportan las VNFs de gestión del ciclo de vida de virtualización e infraestructura. NFV MANO se centra en las tareas de gestión de virtualización, que es necesaria para un marco NFV. También colabora con la NFV externa OSS / BSS y permite la integración del NFV a las redes existentes.

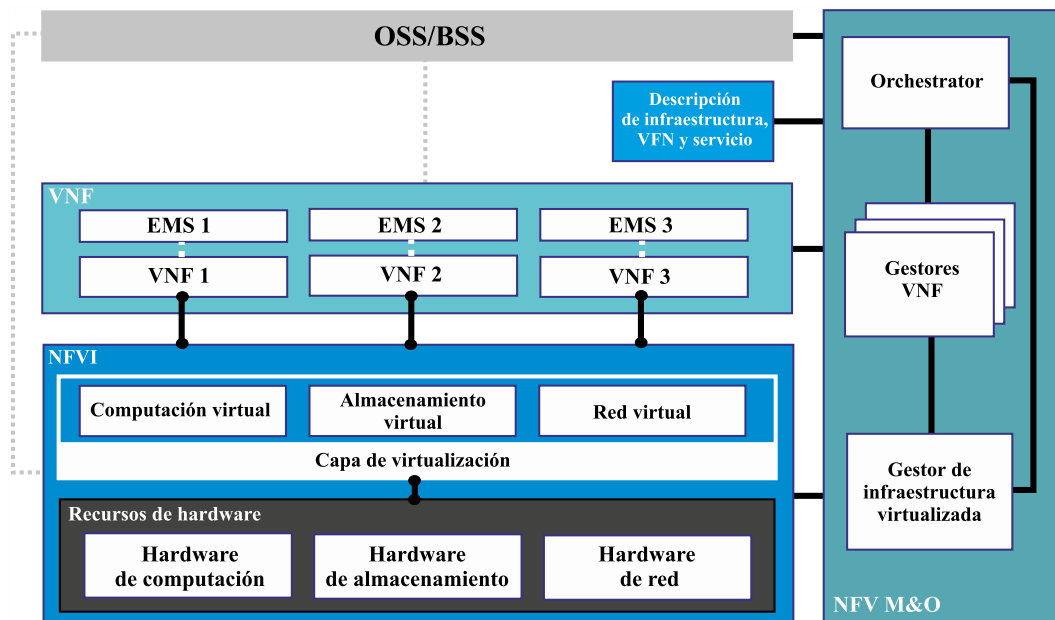


Fig. 7 – Arquitectura NFV [14]

Todo el sistema es alimentado por un conjunto de metadatos que describen NFV los servicios VFNs y los requisitos de la infraestructura NFV MANO para gestionar en consecuencia. Estas descripciones junto con los servicios, VNFs y la infraestructura pueden ser proporcionados por otros actores de la industria.

4.4 La infraestructura NFV - NFVI

La infraestructura NFV está dividida en tres dominios [15]:

- Dominio del equipo - el dominio de la función de equipo es proporcionar recursos informáticos y de almacenamiento y cuando se utiliza junto con el hipervisor. Se proporciona una interfaz a una infraestructura de red de dominio, pero no se conecta a la red en sí misma.
- Dominio del hipervisor - el papel de dominio es mediar software del de recursos computacionales que se ejecutan en máquinas virtuales. Hipervisores se han desarrollado para las necesidades de soluciones en la nube, y dan importancia a la asignación del hardware disponible, simplemente se puede lograr un alto nivel de portabilidad de máquinas virtuales. El hipervisor puede emular (imitar) cada tipo de plataforma de hardware e incluso en algunos casos, emular completamente el establecimiento de la instrucción de manera que la máquina virtual considere que se ejecuta en diferentes arquitecturas de procesador que la real.
- Infraestructura de red de dominio - su papel:
 - crear un canal de comunicación entre múltiples **VNFC** (*virtualized network functions components*, componentes de las funciones de red virtualizada) distribuido (VNF funciones de red virtualizada)
 - crear un canal de comunicación entre múltiples VNF
 - crear un canal de comunicación entre VNF y MANO
 - crear un canal de comunicación entre los componentes NFV y su organización y gestión
 - proporcionar un medio de control remoto VNFC
 - proporcionar un medio de enlace con el operador de red existente

4.5 Gestión y organización NFV (MANO)

La gestión y organización incluye tres componentes [16]:

- Organizador NFV- es responsable de la organización (gestión) de la fuente de NFV a **VIM** (*Virtualized Infrastructure Manager*, organizador de infraestructura virtualizada) múltiple, lleva a cabo las funciones de organización de recursos, gestión del ciclo de vida de los servicios de red (instancias políticas por ejemplo, gestión, escala de medición del desempeño, la correlación de eventos), la función de llenado, la organización de servicios de red, gestión de los recursos mundiales, validación y aprobación de las fuentes de aplicaciones NFV.
- Organización VNF - responsable de la gestión del ciclo de vida de las instancias de la VNF (que puede ser asignado a la gestión de una instancia VNF, y también se puede administrar varias instancias del mismo o de otro tipo), la coordinación general y la adaptación de las configuraciones y la notificación de incidentes entre NFVI y e / NMS
- Virtualized Infrastructure Manager (VIM), organizador de infraestructura virtualizada - es responsable de los recursos de control y gestión de cálculo NFVI, memoria y de red dentro de la infraestructura subdominios de un solo operador, las medidas del funcionamiento de recogida y transmisión y eventos.

4.6 Arquitectura de software - funciones de red virtualizada, Virtualized Network Functions (VNF),

La función de red virtualizada es una función de red capaz de operar en la infraestructura NFV (NFVI) y es administrada por *NFV orchestrator, organizador NFV (NFVO)* y por el administrador VNF. La arquitectura interna VNF se ilustra en la Fig. 8.

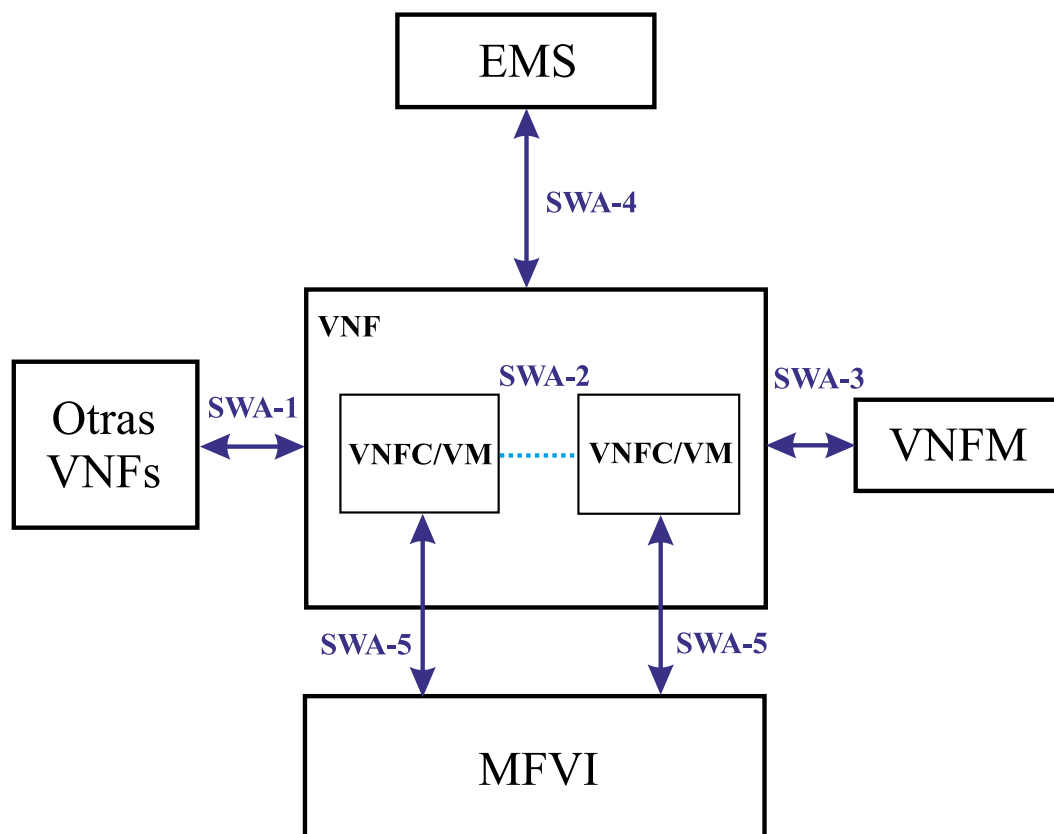


Fig. 8 – Arquitectura NFV [17]

Esta arquitectura asegura la conexiones de calidad utilizando la interfaz:

- Interfaz SWA-1 - con esta interfaz varias VNF se comunican entre sí, pueden utilizar esta interfaz para trabajar juntos y realizar tareas a través de una red.
- Interfaz SWA-2 - con ayuda de esta interfaz los componentes están conectados dentro de VNF, cada componente tiene un papel para el funcionamiento de las funciones de red virtualizadas.
- Interfaz SWA-3 - Esta interfaz se conecta con el Administrador de VNF.
- Interfaz SWA-4 - Utilizando esta interfaz se conecta a la VNF (EMS).
- Interfaz SWA-5 - NFVI conectada con cada VNFC.

4.7 Los casos de uso para NFV



NFV, por una parte ofrece muchas ventajas, la simplificación, enfoques innovadores para las funciones de red y, por otro lado, se abre un sin fin de casos de uso, que son más o menos útiles en el tráfico de red real.

Sin embargo, en la actualidad podemos decir que NFV no es una solución viable totalmente independiente, aunque la organización ETSI desarrolla continuos esfuerzos para crear un estándar fuerte de NFV unificado. NFV es la idea de sacar provecho de la virtualización, qué enfoque se tomarán para la provisión de funcionalidades de la red y la forma de gestionar y organizar todo.



El portal web SDxCentral publica anualmente un informe exhaustivo llamado Network Functions Virtualization Report, informe sobre la virtualización de las funciones de red [18], que incluye la idea principal de NFV, su evolución, y una visión general de proveedor de la solución NFV, así como casos de uso más beneficiosos, enumerados a continuación.

Funciones de red virtualizada

Hoy en día, el buen funcionamiento de la nube ya ofrece muchas oportunidades para de manera fácil, flexible y rápida distribuir o desarrollar aplicaciones, infraestructura y plataformas. Las funciones de red virtualizadas se están adaptando a respetar plenamente los métodos que ya existen en el mundo de la nube. Para los proveedores de servicios en la nube es más interesante la prestación de enrutamiento virtual, red privada virtual (VPN), la capa de 4-7 aceleración y servicios de seguridad para ayudar a conectar, escalar y proteger sus aplicaciones basadas en la nube.

Red de acceso radioeléctrico virtualizado/en la nube

Este caso de uso es particularmente importante para los proveedores de servicios móviles que están buscando maneras de simplificar y acelerar la creación de redes de acceso de radio *radio access networks* (RANs) nuevos, manteniendo el control de los costes. Una serie de funcionalidades que se ejecutan en hardware propietario situado en una estación base se puede mover en la máquina virtual o conjunto de máquinas virtuales que podrían operar localmente en los servidores de COTS, en un punto de agregación o en la nube.

Núcleo móvil virtualizado

Los operadores móviles se enfrentan a menudo con las tareas de actualización de sus redes, servicios y también para extender sus servicios a las zonas rurales, que son difíciles de alcanzar. Un caso útil radica en la adopción de las funciones de hardware propietario en el núcleo móvil y ponerlos en los servidores de COTS en un entorno de nube. Los operadores móviles están buscando virtualizar

principalmente los siguientes servicios: IMS, EPC, MME, S-GW, P-GW, HSS y PCRF.

Límite virtualizado

Los proveedores de servicios también están tratando de encontrar una solución fácil para simplificar su límite, que incorpora un equipo de instalación de cliente, *Customer Premises Equipment (CPE)* Customer Premises Equipment (CPE) y un cliente final, *Customer Edge (CE)*, para vender más servicios a los clientes consumidores y empresas. NFV puede ser una posible solución para hacer crecer sus ingresos. Para permitir que el NFV entre en el mundo de proveedor de servicios, es necesario disponer de componentes finales virtualizados - vCPE y vCE.

5 Futuro de Internet

Los tiempos de hoy podrían ser caracterizados como los tiempos de las tecnologías de la comunicación y la información (TIC) *Information and Communication Technologies (ICT)*. Internet tal como la conocemos hoy en día es un claro éxito. Sin embargo, algunos aspectos de la actual Internet no están a la altura de las expectativas actuales tanto para una infraestructura de comunicación fiable como de las demandas futuras que nos gustaría ser capaz de poner en una red de este tipo.



En 2015 se conectarán a la red de Internet pública mundial aproximadamente 6 mil millones de personas, más de 4 millones de personas van a utilizar los servicios de red a través de dispositivos móviles y más de 2 mil millones de personas usarán conexión de banda ancha por cable a Internet.

Estas suposiciones se pueden encontrar en el papel de Claus G. Gruber [19], así como la suposición de que el tráfico de red tendrá la tasa de crecimiento del 40% al 200% en comparación con el tráfico de red de hoy en los próximos años. Por tanto, es conveniente evaluar en qué estado se encuentran las redes de ordenadores de hoy en día y otros elementos que son parte integrante del mismo. La alta penetración de Internet fomenta y también se acelera también el uso de dispositivos móviles como ordenadores portátiles, teléfonos móviles, tablets. En la Fig. 9 podemos ver el pronóstico de los dispositivos conectados a la Internet pública mundial [20].

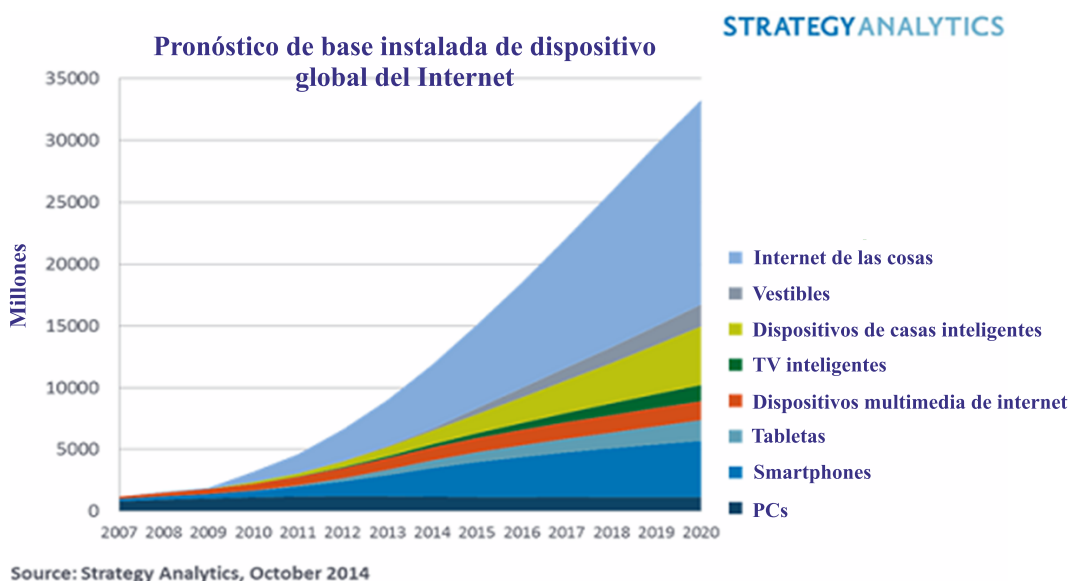


Fig. 9 - Pronóstico de dispositivos instalados global a Internet Global

Los requisitos de las redes móviles a menudo son más exigentes que los requisitos de los usuarios en la red cableada, en particular en lo relativo a la disponibilidad de cualquier tiempo, en cualquier lugar [21]. Por lo tanto, las redes de hoy en día deben ser adaptables y ágiles proporcionando no sólo una alta disponibilidad de los servicios, sino también su calidad.

5.1 Limitaciones de Internet

El Internet actual se basa principalmente en el protocolo IP. Fue creado hace más de 40 años por un grupo de científicos para la interconexión de sus redes locales. Principalmente para la transferencia de archivos, la comunicación por correo electrónico, etc.



La Internet de hoy ha superado considerablemente los supuestos originales. De menos de unos pocos cientos de ordenadores interconectados a varios cientos de millones de ellos en la actualidad. Internet tampoco contaba con nuevas aplicaciones como Web, streaming de vídeo, compartición de archivos que han cambiado significativamente la naturaleza del tráfico de Internet. La infraestructura de Internet ha sido desarrollada por el proceso tecnológico de óptica, inalámbrico, etc. [22].

En la Fig. 10 se puede ver la evolución de Internet desde el pasado hasta el presente. El IP está en el centro del modelo de capas con aplicaciones en la parte superior y las tecnologías en la parte inferior.

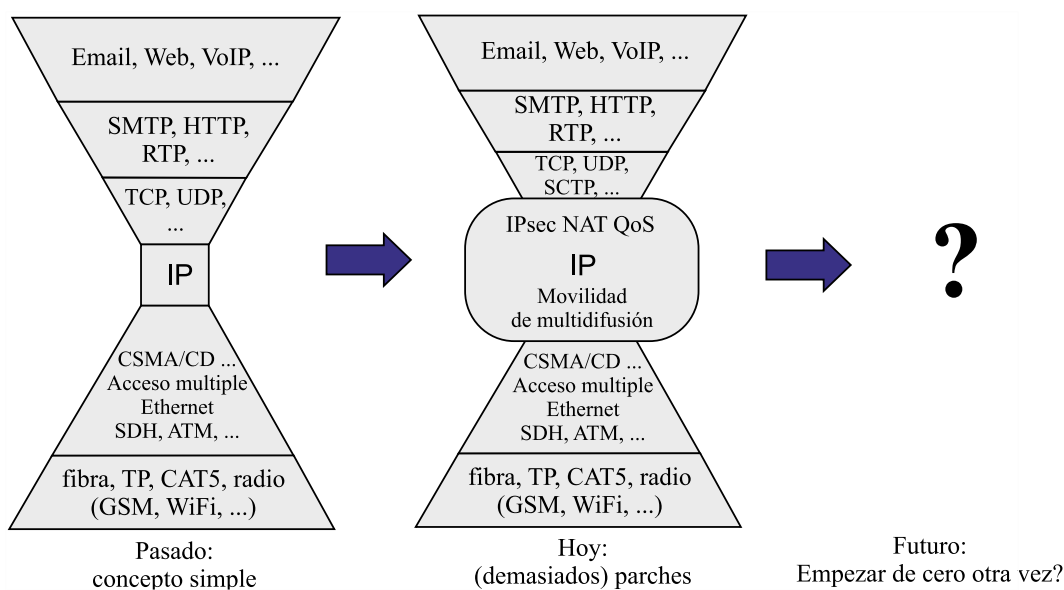


Fig. 10 – Evolución de Internet [23]

En la actualidad, no hay casi ninguna posibilidad de una manera práctica de experimentar con nuevos protocolos de red, la configuración del dispositivo, en la medida en que este experimento puede ganar credibilidad para el amplio despliegue de las redes de proveedores de servicios Internet *Internet Service Providers (ISP)* y proveedores de servicios de red *Network Service Providers (NSP)*.



Los autores en [24] confirman que la enorme cantidad de dispositivos de red ya instalados utilizando la misma infraestructura de red con el mismo protocolo de red, han sido utilizados desde hace décadas, formando una enorme barrera de entrada para soluciones innovadoras, investigación y desarrollo en las redes de ordenadores.

El resultado de este enfoque de la trayectoria es también el hecho de que una serie de ideas nuevas de la comunidad de investigación no se han probado. Los atributos de las redes de ordenadores de hoy en día están "anquilosadas".

Es importante tener en cuenta que sólo el proyecto de Internet se está construyendo para fines de investigación. Los arquitectos, que construyeron la infraestructura de Internet, no se dieron cuenta de la posibilidad de la llegada de las enormes redes que tenemos actualmente. La seguridad, la movilidad, la flexibilidad, la resistencia de las redes nunca ha sido resuelta, porque en tiempos de formalización de la Internet, los ordenadores no eran móviles y los investigadores querían difundir nuevas ideas en condiciones de ambiente abierto. La visión del entorno perfecto Internet ha comenzado a desvanecerse a medida que aumenta el número de usuarios en la red. La cantidad de conceptos básicos en la época de su formación ha cambiado. Con el rápido desarrollo de las tecnologías en el ámbito de las tecnologías informáticas y de información, la Internet pública no puede cumplir y satisfacer las demandas emergentes. Es obvio que las redes de hoy en día necesitan una nueva propuesta, que se adapte mejor a las nuevas tendencias.

El funcionamiento de las redes de ordenadores requiere un número de recursos que está relacionado con el coste. Los costes se pueden dividir en los costes de inversión y los operativos - costes de explotación que se llaman como los gastos de capital (CAPEX) y los gastos de operación (OPEX) [25]. CAPEX se refiere a las inversiones que se deben hacer con antelación y dadas de baja después de un cierto período de tiempo. Un ejemplo sería la construcción del centro de datos (DC) o el precio de compra del servidor, equipos de red y otros componentes críticos de la red. Los gastos de explotación OPEX asociados con los costes mensuales recurrentes de funcionamiento real del equipo, tales como los costes de energía, reparaciones, mantenimiento, salarios de personal administrativo.

5.2 Características del nuevo Internet

Características del nuevo Internet:

- Robusto y disponible – las redes futuras deben ser robustas, y estar disponibles con tolerancia a fallos.
- Seguridad - Uno de las mayores cuestiones de la Internet de hoy es la seguridad, especialmente la seguridad del usuario final. Esa es la razón por la cual el futuro diseño de la red debe ser construido con la seguridad en mente desde el principio. La red debe proporcionar herramientas para poner en cuarentena las infecciones de rápida propagación, mitigar ataques de Denegación de Servicio, y ofrecer un mejor autenticación del origen [22].
- Soporte Móvil para usuarios finales - Como mencionamos en el texto anterior el número de usuarios finales de Internet aumentará rápidamente y el número de usuarios móviles formarán parte principal de ellos. El futuro de Internet está destinado a facilitar la movilidad de los usuarios, terminales y redes, e incluso de las aplicaciones, cuando una comunicación se mueve de un dispositivo a otro, por ejemplo [22].
- Económicamente viable y rentable - Las futuras redes deberían ser rentables para los que prestan servicios de red.
- Evolucionable - la arquitectura de la Internet del futuro debe pre-suponer que va a cambiar y evolucionar con el tiempo.
- Previsible - El usuario debe saber qué esperar de la red, y debe proporcionar un servicio predecible y repetible.
- Soporte anonimato cuando sea prudente, y la rendición de cuentas cuando sea necesario.

5.3 Rediseño de las Tecnologías de Internet



Como ya se ha mencionado, una serie de dispositivos conectados a Internet tiende a un crecimiento constante e imparable, año tras año de manera desproporcionalmente multiplicada.

Para obtener una red estable, segura, flexible y ágil, ya no podemos permanecer en los niveles de los años sesenta y setenta, sino que se está obligado a moverse hacia adelante y abrir las puertas a las nuevas tecnologías. El mayor desafío parece ser la interconexión de redes programables - definidas por software y la virtualización de servicios de red. Tal arquitectura de nueva creación no sólo promete una conexión de las indiscutibles ventajas de ambas tecnologías, sino también la aparición de nuevas mejoras.



La idea revolucionaria es sin duda la arquitectura para el aprovisionamiento automático de servicios de red en forma virtualizada. Las redes definidas por software pueden crear el entorno de red automatizado perfecto que configura automáticamente la red de la empresa, así como el entorno del cliente. Por otra parte, las aplicaciones en la parte superior del controlador SDN serán capaces de generar y evaluar la calidad de la red y si es necesario el cambio necesario de la ruta de red dinámicamente de manera que los parámetros de la red se mantengan, pero también para intervenir en caso de fallo de una línea de red particular.

En el contexto de la automatización, también se puede reflexionar sobre las plantillas específicas, o las políticas de servicios virtualizados específicos, pero también señalar las políticas a medida para el cliente específico. A través del enfoque de software dedicado somos capaces de mantener la configuración deseada a través de una serie de servicios de red que son incluso más coherentes - esto evitará las incoherencias que pudieran producirse a partir del factor humano.

El mayor desafío es la centralización y la transferencia de los servicios propios, denominado "viaje con mis servicios de red". Al ya no estar los servicios en una forma física en los grandes, pesados y difíciles dispositivos portátiles, cada cliente es capaz de viajar con sus servicios, en una red configurada en todo el mundo sin la necesidad de transferir la actividad de manera física.



Gracias a la flexibilidad de estas futuras redes es mucho mejor para controlar y ajustar el producto a la oferta - un servicio, así como ofrecer nuevas mejoras, que aún no ha sido posible para aparatos diseñados para aplicaciones dedicadas.



Todas estas ideas parecen tentadoras, pero la implementación de la arquitectura de interconexión de tecnologías SDN y NFV requieren el reemplazo de la infraestructura obsoleta existente, que no es tan simple. A medida que se produce la transición puede ser posible la integración y las pruebas de la arquitectura SDN y NFV en el entorno existente y la posterior sustitución de tecnologías obsoletas.

La creación de redes definidas por software es un nuevo enfoque que debería permitirnos gestionar, cambiar y controlar la red de forma dinámica a través de interfaces bien definidas. El control centralizado incrusta toda la inteligencia y mantiene una visión de toda la red de los elementos de la ruta de datos y enlaces que los conectan. Esta visión centralizada actualizada hace el controlador adecuado para llevar a cabo las funciones de gestión de red al tiempo que permite modificaciones sencillas a las funciones de red a través del plano de control centralizado. SDN hace posible la gestión de toda la red a través de un sistema de organización y aprovisionamiento inteligente que permite la asignación de recursos bajo demanda.

Los supuestos básicos de la nueva arquitectura de la red [22]:

- Reconocimiento de Flujo - los investigadores en [22] creen que es importante el reconocimiento de flujo.
- Direccionamiento de red – el direccionamiento debería ser más intuitivo, en referencia a los servicios y las personas y no a las interfaces.
- Los protocolos de enrutamiento - Los protocolos de enrutamiento deben ser más fiables y estables.
- La explotación de la estructura.
- Conmutación de circuitos dinámicos.
- El diseño del Backbone (eje central) – los backbone deben ser más predecibles, resistentes a fallos y estables.
- Modelos de funcionamiento de extremo a extremo.
- El diseño Cross-layer - No hay duda de que el modelo en capas tiene un montón de ventajas, pero también tiene una gran cantidad de ineficiencias.
- Virtualización de red - la infraestructura de red debe evolucionar con el tiempo.

En esta sección, se presentaron algunas ideas básicas sobre la Internet del Futuro.



En la actualidad, hay muchos proyectos que se ejecutan simultáneamente y que trabajan para crear un concepto de Internet a partir de cero. Esta investigación está todavía en sus inicios por lo que es difícil hablar de ello e introducir la arquitectura de red exacta, tendencias, etc. Muchos investigadores están trabajando en ello y cada grupo de investigación habla de ello desde su punto de vista. Pero una cosa está clara. Debido a que la actual Internet basado en el IP existe desde hace 40 años, ya se están sufriendo sus limitaciones. El concepto de Internet partiendo de cero ha a ser muy importante y su despliegue es sólo una cuestión de tiempo.
