

Consideraciones sobre la arquitectura de Internet del Futuro

Nelson Rodriguez¹, Maria Murazzo¹, Diego Medel¹

¹Facultad de Ciencias Exactas, Físicas y Naturales, Universidad Nacional de San Juan.
Argentina. Complejo Islas Malvinas (CUIM), Rivadavia. San Juan. CP 5406

nelson@iinfo.unsj.edu.ar - marite@unsj-cuim.edu.ar -
mdiego88@gmail.com

***Abstract.** Internet was designed over 30 years ago , under various assumptions that currently are not met. New applications and requirements that they can be implemented, new integrations and business models involving greater connectivity , demand changes to the global Internet and networks that are part of it. New standards have emerged to improve the network of networks, but many have only managed to increase performance or improve certain parameters , without considering to the applications and how they interact with each other. This paper analyzes these difficulties and that directions will take to solve the same in an Internet of the near future.*

***Resumen.** Internet se diseñó hace más de 30 años, bajo varios supuestos que en la actualidad no se cumplen. Nuevas aplicaciones y requisitos para que las mismas puedan ejecutarse, nuevas integraciones y modelos de negocios que involucran una mayor conectividad, demandan cambios a la Internet global y a las redes que forman parte de la misma. Nuevos estándares han surgido para mejorar la red de redes, pero muchos solo han logrado aumentar la performance o mejorar ciertos parámetros, sin tener en cuenta a las aplicaciones y cómo interactúa entre ellas. Este trabajo analiza estas dificultades y cuáles son las direcciones para solucionar las mismas en una Internet de un futuro cercano.*

1. Introducción

Internet ha pasado de ser un desarrollo académico a un gran producto comercial. La simplicidad del diseño de su arquitectura ha permitido la convergencia de múltiples tecnologías de enlace y mecanismos de transporte de extremo a extremo. Sin embargo, los supuestos sobre lo que la Internet original fue diseñada han cambiado notablemente. Han surgido contextos nuevos y requerimientos específicos.

La comercialización de internet ha introducido preocupaciones sobre la seguridad, la confianza y los servicios de valor añadido. La introducción de sistemas inalámbricos de red ha obligado al paradigma de la movilidad [Paul et al, 2010].

El uso de internet como conducción de los productos básicos de las comunicaciones de negocios ha planteado la necesidad de mejorar la capacidad de resistencia y tolerancia a fallos a través del control y la gestión de grano fino. El modelo de mejor esfuerzo de entrega de IP ya no se considera adecuado.

Desde la perspectiva de nivel de aplicación, la evolución de Internet se caracteriza por una rápida transición de " intercambio " (Web 1.0) y " contribución " (Web 2.0) hacia la " contextualización " (Web3.0) [Caporuscioa y Ghezzi, 2015].

Las suposiciones sobre sistemas finales conectados persistentemente, no se sostienen con la introducción de paradigmas de protocolos tolerantes al retraso. Por otro lado, los protocolos diseñados sin preocuparse por la eficiencia energética no pueden integrar adecuadamente sistemas embebido con restricciones de energía como redes de sensores.

Por lo tanto, internet y las redes que la constituyen, presentarán cambios notables en los próximos años y deberán dar soporte adecuado para las aplicaciones. No bastará con un buen ancho de banda, dado que los sistemas distribuidos más utilizados requieren de redes definidas por el software y redes virtualizadas. Las redes del futuro serán definidas por las aplicaciones, y las mismas en algunos casos involucran muchísima comunicación entre los diversos componentes o unidades de procesamiento, como los sistemas recomendadores, big data y el análisis de redes sociales.

Durante los años 80's y 90's y principios de siglo, las redes cableadas fueron resolviendo los problemas de demanda por parte de los usuarios a costa de mayor velocidad de transferencia, aumentando en 10 sus especificaciones. Un ejemplo emblemático es Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (10000 Mbps) y 10 Gigabit Ethernet (100000 Mbps). En todos estos casos las aplicaciones casi no fueron tenidas en cuenta solo en cuanto a requisitos de ancho de banda. En redes de área extensa MPLS (Multiprotocol Label Switching es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI), aparece como una opción interesante de centrarse en el ruteo de los datos, más que en ofrecer mejor velocidad.

En cuanto a redes inalámbricas, la consolidación de algunas tecnologías permitió normalizar lo que antes era una diversidad de especificaciones y productos. Esto permitió abaratar costos y mejorar los distintos componentes. Actualmente las redes WLAN son la tecnología de acceso a Internet más común, pero también se han expandido a través de una amplia variedad de mercados, incluyendo los consumidores, dispositivos móviles y automóviles de alta gama. WLANs están ampliamente disponibles en todas partes (hogares, puntos de acceso público, entornos empresariales) y las interfaces de radio basadas en IEEE 802.11 se encuentran en muchos tipos de dispositivos.

Las WLANs pasaron de 11 Mbps a 54 Mbps y luego por medio de MIMO (Multiple Input Multiple Output), se logró mejorar las velocidades llegando a con 802.11n a 450 Mbps. Además nuevos estándares como 802.11ac (Wave 2), 802.11ad (WiGig 1.0) y 802.11ah (Super Wi-Fi), prometen alcanzar velocidades inimaginables para el medio inalámbrica. Otras nuevas especificaciones como 802.11af (HaLow) se han diseñado para bajo consumo y mayor alcance fundamentalmente para IoT [Bellalta et al, 2015]. Por otro lado las redes Mesh implementaron la existencia de transferencias a 5 Ghz y 2,4 Ghz dentro de la misma red, mejorando la concurrencia y reduciendo la interferencia. En todos los casos descriptos, las redes mejoraron pero en ningún caso se tuvo en cuenta a las aplicaciones.

Con los avances en la computación en nube y las máquinas inteligentes, y el advenimiento de la IoT, se espera que el tráfico en las redes de telecomunicaciones se dispare. Se está considerando el desarrollo de redes aéreas de vehículos aéreos no tripulados (UAVo drones), para el establecimiento de una red móvil en tres dimensiones de una manera ad hoc. Mediante el despliegue de una red desde el cielo, se puede utilizar el medio inalámbrico inactivo y con alta movilidad libre de obstáculos del terreno. Estas redes aéreas son especialmente eficaces para apoyar el aumento temporal de la población, así como zonas de desastre debido a que la construcción de una infraestructura de red adicional requiere mucho tiempo. [Kyung-Nam Park et al, 2016]

Por otro lado, La quinta generación (5G) de redes de comunicaciones móviles requerirá un cambio de paradigma importante para satisfacer la creciente demanda de velocidad de datos, menores latencias de red, una mayor eficiencia energética y la conectividad ubicua fiable [Akyildiz et al, 2016]. Debido a la diferente demanda de los usuarios, estas redes deberán soportar compatibilidad hacia atrás y mayor flexibilidad. Las tecnologías que van hacer posible esto son: virtualización de las funciones de red, espectro de ondas milimétrico, MIMO masivo, redes ultra-densas, conectividad dispositivo a dispositivo con alta movilidad, nuevas técnicas de acceso por radio y redes definidas por el software inalámbricas.

2. SDN

Las redes definidas por el software son un buen intento para adaptar las redes a los requerimientos actuales.

Las SDN son una manera de abordar la creación de redes en la cual el control se desprende del hardware y se le da el mismo a una aplicación de software llamada controlador. El término SDN (Software Defined Network o red definida por software) se ha venido acuñando en los últimos años para hacer referencia a una arquitectura de red que permite separar el plano del control, del plano de datos, para conseguir redes más programables, automatizables y flexibles. Con SDN se virtualiza la red independizándola de la infraestructura física subyacente.

La tecnología SDN elimina la inteligencia de las redes tradicionales del hardware, delegando las capacidades de toma de decisiones en el servidor. La tecnología desacopla la capa de datos (data layer: información real que viaja en una red) de la capa de control (control layer: la tecnología que determina cómo, cuándo y dónde la información flujos), y cada capa está automatizada. Esto significa que el control independiente de cada capa es posible sin el costoso y complicado hardware y software (por ejemplo, routers y switches) o la necesidad de profesionales altamente calificados para gestionar dichos dispositivos.

Cuando un paquete llega a un conmutador en una red convencional, las reglas integradas al firmware propietario del conmutador le dicen al conmutador adónde transferir el paquete. El conmutador envía cada paquete al mismo destino por la misma trayectoria – y trata a todos los paquetes de la exacta misma manera. En la empresa, los conmutadores inteligentes diseñados con circuitos integrados de aplicación específica.

Actualmente, la especificación más popular para crear una SDN es un estándar abierto llamado OpenFlow. OpenFlow permite a los administradores de red controlar tablas de enrutamiento de forma remota. El protocolo OpenFlow constituye la base de

las redes abiertas definidas por software (Software-Defined Networking, SDN) basadas en estándares. OpenFlow comenzó a desarrollarse en 2007 y es el resultado de la colaboración de los sectores académico y empresarial. Fueron las universidades de Stanford y California en Berkeley quienes llevaron las riendas en primera instancia. En la actualidad, la Open Networking Foundation (ONF) se encarga de la definición del estándar. HP ha sido líder en tecnología OpenFlow desde sus inicios, además de ser miembro fundador de la ONF. Cisco ha lanzado su arquitectura ONE, que proporciona un framework para la programación de red, la provisión automatizada y las interacciones basadas en las aplicaciones. VMware, por otra parte, cuenta en su portfolio con la solución SDN vCloud Networking & Security y ha adquirido recientemente la compañía Nicira, especializada en este tipo de redes.

3. Tráfico Heterogéneo

Internet originariamente fue desarrollada para tráfico de texto, recién cuando aparece la Web con la hipermedia como modelo de documento, imagen, audio y video se agregaron al texto original. En los últimos años, se ha producido un notable aumento en la demanda de aplicaciones multimedia sobre medios cableados e inalámbricos, tales como: voz sobre IP (VoIP), audio conferencia, video conferencia, audio, etc. Estas aplicaciones requieren que los servicios suministrados a los usuarios ofrezcan garantías de QoS en cuanto al ancho de banda, retardo de extremo a extremo (latencia), variabilidad en el retardo (jitter) o tasa de error. En concreto, muchas aplicaciones multimedia son sensibles a la variabilidad en la tasa de transmisión, al retardo y a la variabilidad en el retardo, aunque toleran ciertas pérdidas de datos.

Por otro lado, existen las aplicaciones clásicas, flexibles al retardo y a la disponibilidad de ancho de banda, como pueden ser: correo electrónico, transferencia de archivos, navegación web y login remoto, que en general tienen requisitos distintos a las aplicaciones multimedia. En las mismas, la variabilidad en el retardo o en la disponibilidad de ancho de banda, aunque actúan en su detrimento, no impiden que se realice el servicio.

Muchas aplicaciones que antes eran solo texto en la actualidad llevan imágenes y video. Por ejemplo WhatsApp se amplió notablemente y recientemente Twitter habilitó la transmisión de video de hasta 140 segundos.

El tráfico mayor desde un smartphone ya no se realiza por llamadas o telefonía celular, sino por Internet.

El término QoS se refiere a la garantía de proveer un servicio con cierto grado de fiabilidad en la transmisión de información, a través de una red. Los principales parámetros que se utilizan para medir la misma, que puede ofrecer una red son: la disponibilidad de la red, el ancho de banda, el retardo de los paquetes, la variación del retardo, la tasa de errores y la tasa de pérdida de paquetes. En función de los requisitos de las aplicaciones, algunos parámetros serán más importantes que otros en el momento de definirla [Murazzo, Rodríguez et al 2013].

QoS es la capacidad de la red de proveer mejor servicio a cierto tipo de tráfico. Internet (al menos la versión 4 de IP), no puede manejar QoS.

Para brindar la satisfacción a los usuarios es necesario contar con una plataforma para soportar aplicaciones clásicas (tráfico elástico) y aplicaciones multimediales (tráfico inelástico). El objetivo principal de esto es lograr que el usuario pueda correr todo tipo de aplicaciones, las cuales poseerán diferentes requerimientos de recursos.

A medida que el tráfico aumenta y alcanza el límite de ancho de banda, aumenta la cantidad de cortes o mala calidad de video, se interrumpe el sonido, o aparecen otros efectos no deseados.

En 2015, las PC representaron el 53 por ciento del tráfico IP total, pero en 2020 las PC representarán sólo el 29 por ciento del tráfico. Los teléfonos inteligentes representarán el 30 por ciento del tráfico IP totales en 2020, por encima del 8 por ciento en 2015. El tráfico originado por PCs crecerá a una tasa compuesta anual del 8 por ciento, mientras que los televisores, tabletas, teléfonos inteligentes, y de máquina a máquina (M2M) tendrán tasas de crecimiento del tráfico de 17 por ciento, 39 por ciento, 58 por ciento, y 44 por ciento, respectivamente [Cisco,2016].

Esto no significa que se sustituirá un dispositivo por otro, sino el tráfico aumentará notablemente a un ritmo anual de 1.1 zettabyte (ZB; 1000 exabytes). El número de dispositivos conectados a redes IP será tres veces tan alta que la población mundial en el año 2020. Se estima que será de 3.4 dispositivos en red per cápita para el año 2020, comparado con los 2,2 dispositivos conectados en red en la actualidad. Además el aumento de los dispositivos y las capacidades de esos provocará un incremento en el tráfico que alcanzará a 25 GB per cápita en 2020, frente a los 10 GB per cápita en 2015. Todo un desafío para los administradores de las redes.

4. Seguridad

La Internet original fue diseñada en forma conjunta por universidades y laboratorios de investigación, y fue considerada segura. Sin embargo, esta hipótesis hace tiempo que se ha invalidado con la comercialización de Internet. La seguridad se ha convertido en uno de las áreas más importantes de la investigación. Con más y más negocios en línea y una plétora de nuevas aplicaciones que ocasionan nuevos usos de Internet, la seguridad es, sin duda va a ser uno de los principales preocupación por la próxima generación.

El aumento de la complejidad del entorno informático está introduciendo nuevas vulnerabilidades, lo que resulta en más ataques de red y una mayor demanda de fuerte rendimiento de la red y una conectividad segura dramáticamente. Teniendo en cuenta lo anterior, se debe encontrar una manera de acomodar múltiples tipos de dispositivos, múltiples sistemas operativos y permitir el acceso seguro a los recursos de la red al tiempo que protege los activos corporativos. Junto con la red, también se sea necesario para asegurar la variedad de dispositivos en uso. [Nagel, 2016]

Se han detectado ataques con código malicioso propagado a través de internet de las cosas, dirigidas a agotar las baterías de los dispositivos, manteniéndolos despiertos. Este ataque podría generar Denegación de Servicio y fallos en cascada, que en un sistema distribuido es sumamente difícil de solucionar (no hay forma de realizar un roll-back en este caso). Varias soluciones han sido propuestas como: las redes de corto rango o alcance, que impedirán que hackers puedan acceder a la misma si no están en la cercanía y además consumen menos energía para la transferencia de datos.

Algunas propuestas de los investigadores es utilizar como arquitectura de internet del futuro, la redes centradas en el contenido, que pueden manejar adecuadamente varios tipos de ataques [Lutz, 2016].

Por todo lo descrito, en la próxima generación de internet, la seguridad debe ser una parte de la arquitectura en lugar de ser superpuesta en alguna de las capas como ocurre actualmente. Los expertos en seguridad tienen establecido el hecho de que la seguridad no es una singular función de cualquier capa en particular del protocolo, sino que es una responsabilidad conjunta de todos los componentes y debe ser una función principal de la comunicación.

5. Nuevas Aplicaciones

Las aplicaciones actuales no solo requieren mayor ancho de banda. Las interacciones entre las distintas aplicaciones y componentes dejan de lado el modelo cliente servidor clásico de uno a uno o uno a muchos. Si comparamos M2M (machine to machine) con IoT se pueden percibir diferencias importantes, aunque parezcan muy similares. Los sistemas M2M tradicionales normalmente se han aplicado a la supervisión, el control o la optimización de un solo proceso. Ellos se han especificado, diseñado e implementado para hacer frente a un problema de tipo punto a punto. Usando la arquitectura M2M clásica, por ejemplo, un edificio puede tener sistemas separados para el control de HVAC, seguridad y de detección de incendios.

IoT por el contrario, se trata de sistemas de sistemas. Son productores de publicación de datos de información que no necesitan saber qué aplicaciones o usuarios estarán consumiendo esos datos. Se trata de hacer que dichos datos estén disponibles para varios sistemas de manera que puede ser ampliada y revisada a medida que surgen nuevas necesidades

Como modelo de interacción pueden observarse claramente en la figura 1 las diferencias entre las comunicaciones en ambos modelos.

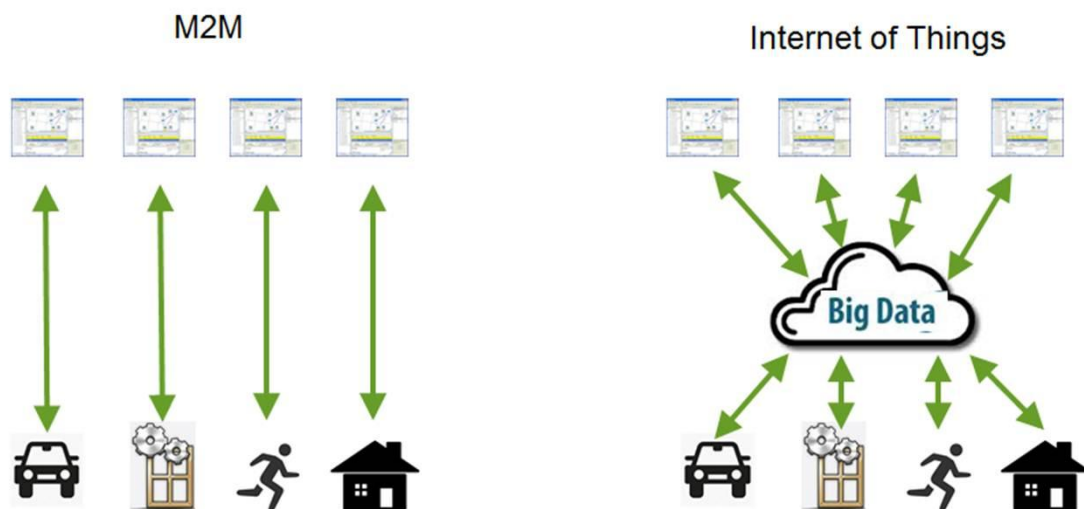


Figura 1: Comparación de la interacción entre M2M e IoT

A la izquierda se puede observar que se pueden tener dispositivos específicos conectados entre sí a través de algún tipo de comunicaciones. Así que se puede enviar un fax o comprobar la condición física de una persona.

A la derecha, se pueden añadir comunicaciones ubicuas, servicios en la nube y la correlación de big data, resultando en un ecosistema de energía mucho más que también crea un valor adicional. Y eso es lo que está impulsando el crecimiento de la IoT, el valor adicional que crea.

Si bien IoT está en sus inicios, la consolidación de la plataforma resultará clave. Aparecerán cada vez más aplicaciones y su costo se reducirá. Las plataformas de IoT agrupan muchos de los componentes de infraestructura y realizan diversas tareas como: control de dispositivo y operaciones de bajo nivel, monitorización y gestión de dispositivos, seguridad, actualizaciones de firmware, adquisición, transformación y gestión de datos del Internet de las cosas.

Para ello es necesario también que surjan estándares para comunicación de bajo consumo y redes de corto alcance

6. Redes inteligentes

La tendencia del uso de la tecnología de la informática empresarial están exigiendo cada vez más los límites de las redes. El consumo de las TICs, la movilidad, la virtualización y computación en la nube, junto con un aumento masivo en el tráfico de video generan demandas crecientes en la red.

Las empresas también están utilizando cada vez más las tecnologías de vídeo para vigilancia, la comunicación y la señalización digital. En los últimos años muchas capacitaciones de empresas y de universidades han migrado del formato documento (presentaciones, pdf) a formatos de video. Esto exige una necesidad de asegurar que las inversiones de red proporcionen la inteligencia necesaria para planificar previamente auto-configuración y solucionar problemas de las terminales de video y flujos de vídeo.

Del mismo modo la movilidad ha pasado de ser demanda de los empleados a una necesidad de la empresa. Los teléfonos inteligentes, tablets, PCs y otros dispositivos móviles no sólo han revolucionado la comunicación personal, sino que también están ayudando a aumentar la productividad y mantener las empresas que operan durante todo el día.

Muchos de estos dispositivos se emplean para acceder a datos corporativos, que combinan imágenes de alta resolución y vídeo en documentos ricos. A pesar de que (BYOD - Bring Your Own Device - es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativo) no tuvo el éxito que se esperaba, muchas empresas utilizan esta modalidad y se espera que aumente a 30 por ciento en los próximos dos años.

Estas redes, deberán integrarse con redes fronteras para ofrecer un nuevo conjunto de servicios de red, para apoyar las demandas del negocio y de los usuarios finales. Sin embargo, la creación de un sistema operativo de red que es más inteligente y contextualizada obliga a las empresas a centrarse en la aplicación de software, software

de gestión y el sistema operativo de la red debido a la integración de las tres unidades de inteligencia dentro de la red.

Evidentemente la red del futuro debe ser flexible e inteligente. Los servicios se consumirán de forma dinámica, y esto se hará posible gracias a los servicios de red, dinámicos y flexibles. Deberán contemplar eficientemente las crecientes necesidades de la empresa, ser escalables, soportar dispositivos móviles propios o mediante BYOD, conectarse a los servicios de nube pública, utilizar medios ricos como videoconferencia y otros medios interactivos, y ofrecer fiabilidad, seguridad, agilidad y rendimiento.

7. El profesional de Redes

No solo las redes deberán adaptarse a los cambios, sino también el rol de los administradores de red, debido a que más que enfocarse en como las aplicaciones y dispositivos se conectan a la red, deberán observar el rendimiento de las aplicaciones en la red, cómo interactúan entre ellas, realizando ajustes en la velocidad de transferencia y otros parámetros e integrar la virtualización en el sistema operativo de red.

De acuerdo con el estudio sobre habilidades en redes en América Latina, comisionado por Cisco a la empresa IDC, en Latinoamérica la demanda de profesionales con habilidades en Tecnologías de la Información y Comunicación rebasará la oferta y harán falta 449 mil empleados de tiempo completo en tres años. Dicho estudio, analiza la disponibilidad de profesionales con habilidades TIC en la región entre 2015 y 2019 en 10 países: Argentina, Brasil, Chile, Colombia, Costa Rica, República Dominicana, Ecuador, México, Perú y Venezuela. La brecha entre la oferta de profesionales en red y la demanda llegará al 32%. Además de las habilidades básicas de redes – switching y routing, seguridad, redes inalámbricas – hoy se requieren conocimientos de tecnologías emergentes que incluyen: comunicaciones unificadas, video, Cloud Computing, movilidad, centro de datos y virtualización, big data, ciberseguridad, IoT y desarrollo de software en red. [Cisco-IDC].

Teniendo en cuenta que las redes de próxima generación serán los suficientemente versátiles para soportar acceso de móviles, IoT, tráfico multimedia, autoconfiguraciones, deberán estar definidas por el software, en ambientes virtualizados y con comunicaciones unificadas, acceder a Cloud público seguramente desde su cloud privado y protegerse de una variedad de ataques, el profesional que se ocupe de la administración deberá estar acorde con estas capacidades.

En un estudio realizado en 2012 sobre los conocimientos de ARSO (arquitectura, sistemas operativos y redes) que la industria considera necesarios, figuran muchos de los conceptos que hoy se ven necesarios en los egresados de las universidades como virtualización, computación en la nube, computación móvil, desarrollo de aplicaciones Web, computación ubicua y pervasiva, computación dependiente del contexto, construcción de redes virtuales privadas (VPN) y aplicaciones para sistemas embebidos y tablets, entre otros [Rodríguez et al, 2012].

8. Otras consideraciones

El gran incremento de tráfico en internet, el aumento de la cantidad de dispositivos que se conectan y la ampliación de los centros de datos fruto del éxito de Cloud Computing va a impactar fuertemente en el consumo de energía.

Las regulaciones sobre las emisiones de carbono están siendo desarrolladas y aplicadas y las empresas deben estar preparadas para supervisar y gestionar la huella de carbono. Las innovaciones en la tecnología de red pueden conducir una estrategia de eficiencia energética consolidada. Por lo tanto, es fundamental para garantizar que la infraestructura de red puede controlar y administrar el uso de energía y las emisiones de carbono, algo en que en teoría es muy difundido, pero en la práctica no ocurre lo mismo.

Otro problema siempre presente y que va a seguir siendo motivo de discusión son la internacionalización, disputas legales, acuerdos a nivel de servicio (muy necesario en computación en la nube). Esto es porque internet atraviesa las fronteras, pero cada país tiene legislación que pueden entrar en conflicto con las leyes de otro país que comparten algún servicio, transferencia, transacción u otra operación comercial.

9. Conclusiones

Las nuevas aplicaciones e interacciones entre las mismas, exigen repensar la arquitectura de la internet global. No basta con mejorar el ancho de banda de las redes de soporte y algunos parámetros secundarios.

El futuro de Internet se concibe a nivel de aplicación, como un ambiente de alcance mundial conectando una gran colección de recursos autónomos y heterogéneos, que pueden ser cosas, servicios y contenidos los cuales interactúan con otros en cualquier momento y en cualquier lugar.

Las redes del futuro deberán ser flexibles e inteligentes. Los servicios serán consumidos dinámicamente tanto como sea posible y dependerán de la infraestructura de red disponible.

En el caso particular de las redes inalámbricas, se han construido teniendo en cuenta la variedad de dispositivos y aplicaciones, en algunos casos mejorado la velocidad de transferencia, en otros el alcance, la geolocalización, la comunicación en grupo, la transmisión de HDTV o la transmisión eficiente de pequeños datos.

La construcción de plataformas de IoT y la generación de estándares, generará nuevas aplicaciones, un aumento notable del tráfico, pero también nuevas vulnerabilidades.

Las organizaciones deben invertir en unas redes de próxima generación, construidas para permitir las capacidades de negocio para hoy y mañana, ahorrar costos, obtener una ventaja competitiva, mejorar la productividad y la agilidad de la empresa.

Es dificultoso predecir que puede suceder con la mejor invención de TIC del siglo XX, o sea Internet. Se ha visto que muchas aplicaciones asesinas han cambiado paradigmas, muchas empresas líderes del sector están a punto de desaparecer, varios estándares o desarrollos prometían ser la panacea y luego no llegaron a imponerse (como CORBA o computación grid). Se esperaba que BYOD y SOA un mayor nivel de adopción por parte de las empresas.

Nadie sabe a ciencia cierta cuál será el nivel de adopción de IoT y si esa será la tecnología que condicione el anunciado apagón digital que pase de IPV4 a la versión 6.

Dentro de todo este océano de tecnologías, las organizaciones que tienen una gran responsabilidad como las universidades y centros de investigación, no solo deben

estar actualizados, sino además deben estimar adecuadamente lo que puede pasar, para enfocar sus tareas de investigación o cambios de plan de estudios, propuestas de cursos de grado y posgrado e incluso especializaciones o maestrías.

10. Bibliografía

- Ian Akyildiz, Shuai Nie, Shih-Chun Lin, Manoj Chandrasekaran (2016) " 5G roadmap: 10 key enabling technologies". *Computer Networks* 106 (2016) 17–48.
- Barbeau y Kranakis (2007). "Principles of Ad-Hoc Networking". John Wiley and Sons.
- Boris Bellalta, Luciano Bononi, Raffaele Bruno, Andreas Kessler (2015). " Next generation IEEE802.11 Wireless Local Area Networks: Current status, future directions and open challenges". *Computer Communications* 75 (2016) 1–25.
- Mauro Caporuscio, Carlo Ghezzi (2015). "Engineering Future Internet applications: The Prime approach". *Journal of Systems and Software* Vol. 106, Ag. 2015, Pág. 9-27.
- Cisco IDC, Networking Skills in LatinAmerica (2013). <https://www.netacad.com/es/web/about-us/idc-skills-gap>
- Cisco Visual Networking Index: Forecast and Methodology, 2015–2020 White Paper (2016).
- Roman Lutz (2016). "Security and Privacy in Future Internet Architectures Benefits and Challenges of Content Centric Networks" . arXiv:1601.01278. <https://arxiv.org/abs/1601.01278>
- Murazzo, Rodríguez, Villafañe (2013). "Análisis de las prestaciones de 802.11e en redes MANET". CACIC 2013, Mar del Plata, Buenos Aires, Argentina.
- David Nagel " Security Tops List of Trends That Will Impact the Internet of Things" (2016). <https://campustechnology.com/articles/2016/02/25/security-tops-list-of-trends-that-will-impact-the-internet-of-things.aspx>
- Kyung-Nam Park, Jin-Hyeok Kang, Byeong-Moon Cho, Kyung-Joon Park, Hwangnam Kim (2016) "Handover Management of Net-Drones for Future Internet Platforms". *International Journal of Distributed Sensor Networks* Volume 2016 (2016), Article ID 5760245, 9 pages <http://dx.doi.org/10.1155/2016/5760245>
- N. Rodríguez, M. Murazzo, D.Villafañe, S. Chávez, A. Valenzuela, A.Martín (2012) Cuáles son los conocimientos de ARSO (Arquitectura, Redes y Sistemas Operativos) que la industria considera importantes VII Congreso de Tecnología en Educación y Educación en Tecnología.
- Subharthi Paul, Jianli Pan, and Raj Jain (2010). "Architectures for the Future Networks and the Next Generation Internet: A Survey". *Computer Communications* 34 (2011) 2-42.