Vol.15 No.2 2019

ETECSA

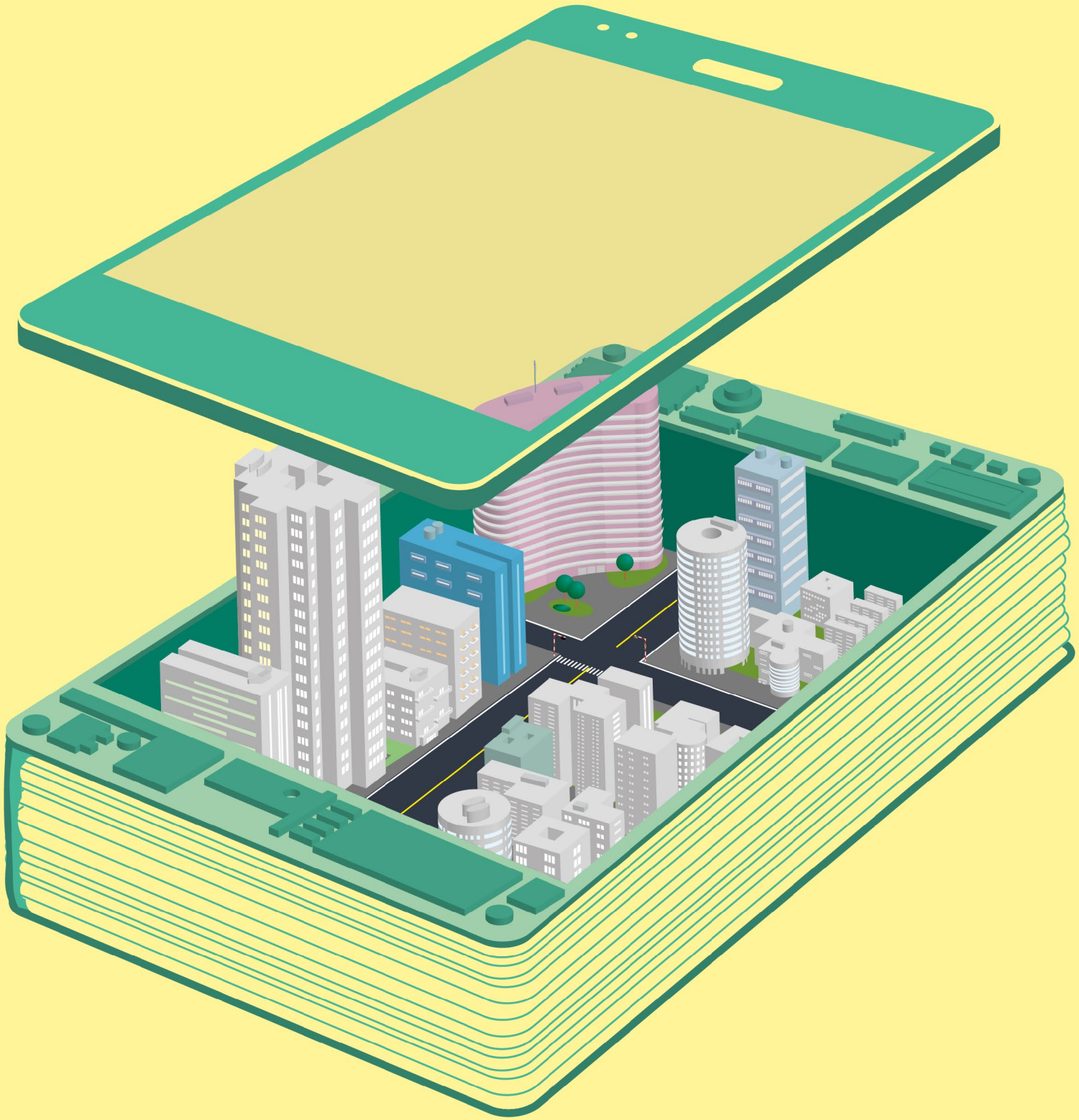
tono

Revista Científico-Técnica de la Empresa de Telecomunicaciones de Cuba S.A.

CITMA CERTIFICADO

RNPS: 0514

ISSN: 1813-5056



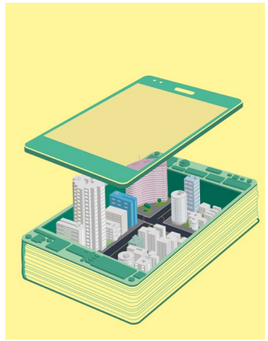
ETECSA
EMPRESA DE TELECOMUNICACIONES DE CUBA S.A.

tono
Revista Científico-Técnica

Publicación Semestral
Vol.15 - No. 2 - 2019

RNPS: 0514 ISSN: 1813-5056

Tono, Revista Científico-Técnica de la Empresa de Telecomunicaciones de Cuba, S.A.



Portada: Marcel Mazorra Martínez

Los artículos en esta publicación han sido sometidos a revisión por pares a doble ciego.

CONTÁCTENOS

Dirección de Información y Vigilancia Estratégica de ETECSA
Dirección: Centro de Negocios Miramar, calle 3ra, e/ 76 y 78, Edificio Beijing, 4to Piso, oficina 404. Playa, C.P.: 11300. La Habana, Cuba.
Teléfono : (53) 7266-8453
Correo electrónico: tono@etecsa.cu
Sitio web: www.revistatonoetecsa.cu

VOL.15 NO. 2 JULIO / DICIEMBRE 2019

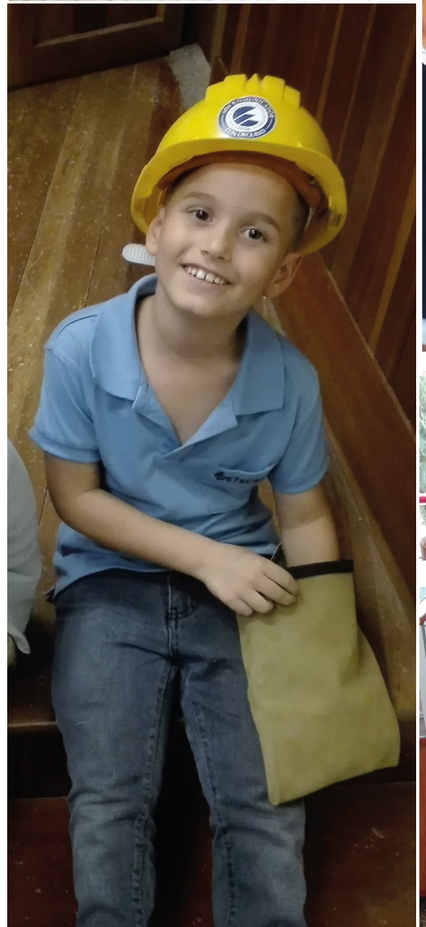
SUMARIO

CARTA DEL EDITOR

La cábala de 2019 trajo al sector de las telecomunicaciones en Cuba, muchas razones para celebrar. Los 25 años de la Empresa de Telecomunicaciones de Cuba, los 15 del Museo de las Telecomunicaciones y de la Revista Científico Técnica Tono y los 5 años del Suplemento Técnico Infantil Tonito, todos matizados por los 500 años de la fundación de la Villa San Cristóbal de La Habana. Son tiempos que se pueden precisar en pocas líneas, pero que han representado el esfuerzo, dedicación y amor a la ciencia misma, de todos aquellos que han trabajado en cada uno de estos espacios. Hemos tenido alegrías por la profesionalidad con la que ha evolucionado el trabajo en su sentido más amplio y, lamentablemente también hemos sufrido pérdidas irreparables para las cuales el mayor homenaje se revierte en la entrega a la misión que tenemos dentro de nuestro sector.

Desde las telecomunicaciones, se ha asumido cada reto con la exigencia que demandan estos tiempos, pero también con el amor y la cultura de detalle a la que nos ha convocado el país. Específicamente, la Revista Tono se ratifica como canal formal de comunicación científica, enfocada a ser el medio por el cual se transite hacia la colaboración, las investigaciones y la innovación. Para su Grupo Editorial este Número marca un hito especial con dos significados. En primera instancia, constituye un cierre de un período susceptible a ser analizado introspectivamente en aras de mejorar los próximos pasos y, por otro lado tiene la función ineludible de continuar optimizando nuestros procesos, en pos de impulsar la comunicación e implementación de los resultados de las investigaciones, como bases fundamentales para el despliegue de la informatización de nuestra sociedad. Espacio de debate, de reflexión, de visibilidad de nuestras soluciones —en todos los escenarios que nos convocan hoy—, de colaboración científica, de innovación; como tal se construye Tono día a día promoviendo desde su labor a la ciencia, como elemento fundamental para la sostenibilidad.

Grupo Editorial
Revista Científico-Técnica Tono



IPv6 para redes que soportan servicios de acceso por suscripción

Ipv6 for networks supporting subscription access services

MSc. Yussel Castrizano Jiménez [1]

Recibido: 06/2019 | Aceptado: 10/2019

Palabras clave

IPv4
IPv6
Agotamiento IPv4
Nat64
Ds-lite
Pila dual

Resumen

El agotamiento de las direcciones IPv4 y la gran densidad de equipos conectados a la red, por una parte, incluso con el eventual advenimiento de la Internet de las Cosas, y por otra, la demanda de los usuarios de más ancho de banda, ha hecho latente la necesidad de trabajar en el aumento constante de estos dos recursos: direcciones IP y Velocidad del acceso a la red de datos. El presente trabajo se concentra en analizar las estrategias actuales para la transición a IPv6 dirigido al aumento de las direcciones IP disponibles para el usuario y la inserción de estas estrategias en una red de Banda Ancha, la cual constituye el escenario propicio para que el usuario pueda satisfacer su demanda de acceder a más recursos de la red, con más velocidad. En esta investigación, se realiza una propuesta para enfrentar el agotamiento de IPv4 en un proveedor de servicios de banda ancha, a través del análisis de diferentes técnicas para el proceso de transición hacia una red completamente IPv6. Primero, se analizan dos formas de resolver el problema de agotamiento de IPv4 con sus ventajas y desventajas. Luego se describen las soluciones técnicas de banda ancha IPv6 y que impacto tiene cada una de estas soluciones en el equipamiento y la arquitectura de una red de Banda Ancha, basado en los estándares que rigen este tipo de redes. Cada una de estas soluciones se analiza y finalmente una de ellas se elige en función de algunos indicadores clave.

Keywords

IPv4
IPv6
IPv4 exhaustion
Nat64
Ds-lite
Dual-stack

Abstract

On the one hand, the depletion of IPv4 addresses and the high density of equipment connected to the network, even with the eventual advent of the Internet of Things, and, on the other hand, users demanding greater bandwidth, had become more latent the need to work on the constant increase of these two resources: IP addresses and access rate to the data network. This research focuses on analyzing the current strategies for the transition to IPv6, aimed at increasing the IP addresses available to the user; and inserting these strategies into a broadband network, which is the ideal scenario for the users to satisfy their demand to access to more network resources,

[1] Empresa de Telecomunicaciones de Cuba S.A. División de Servicios Fijos. La Habana, Cuba. yussel.castrizano@etecsa.cu

with higher speed. In this research, a proposal is made to face with the depletion of IPv4 in a broadband service provider, through the analysis of different techniques for the transition process towards a complete IPv6 network. First, two ways to solve the problem of IPv4 depletion are analyzed, with its respective advantages and disadvantages. Then, the IPv6 broadband technical solutions are described along with their impact on the equipment and architecture of a broadband network, based on the standards that govern this type of networks. Each of these solutions is analyzed and, finally, one of them is chosen, based on some key indicators.

Introducción

El agotamiento de las direcciones IPv4 (Postel,1981) es una realidad que enfrentan los Operadores de Telecomunicaciones actualmente. La convergencia de las redes fijas y móviles ha eliminado las redes paralelas y las ha unido en una plataforma IP —*Internet Protocol*—. En este escenario el uso de las direcciones IP ha crecido exponencialmente. En especial las direcciones IPv4 públicas usadas para el acceso a Internet se encuentran en la última fase de agotamiento. Esta situación obliga a los Operadores a buscar soluciones como la Traducción de Direcciones a Nivel de Operador o Carrier Grade Network o CGN (Perreault, Yamagata y Miyakawa, 2013). El uso del CGN conlleva obstáculos a nivel de hardware y software tanto para el usuario como para el Operador. Solo queda entonces como solución la migración a IPv6 —*Internet Protocol version 6*— (Deering y Hiden, 1998). Pero la transición a IPv6 no puede ser realizada sin mantener compatibilidad con los servicios IPv4 heredados. Por lo tanto, se hace necesario la implementación de técnicas que mantengan la escalabilidad de la red y que permitan que los actuales servicios IPv4 continúen corriendo sin afectación.

Materiales y métodos

El objetivo de este trabajo es presentar una propuesta técnica para la transición a IPv6 en los Servicios de Acceso por Suscripción los cuales permiten que los usuarios accedan a la Red luego de autenticarse y la facturación que realice la red sea a partir de los recursos que consumió el usuario en un tiempo determinado.

Fueron utilizados varios métodos: el método histórico-lógico permite contextualizar las Redes de Datos que dan Soporte a los Servicios de Suscripción, sus componentes fundamentales y la interrelación entre estos. Además, permite abordar sus antecedentes y el desarrollo actual de estas Redes. El analítico-sintético ya que es necesario trabajar cada componente del Modelo de Red de Datos para Servicios de Suscripción y sus relaciones para luego lograr la integración de las partes constitutivas del Modelo para llegar a la Propuesta de Configuración de Red de Datos para los Servicios de Suscripción.

Resultados y discusión

Como parte de la investigación se modeló una Red de Datos para el Servicio de Acceso por Suscripción (ver Figura 1) basado en las Redes Componentes y en las funciones que se realiza en cada Capa de Red.

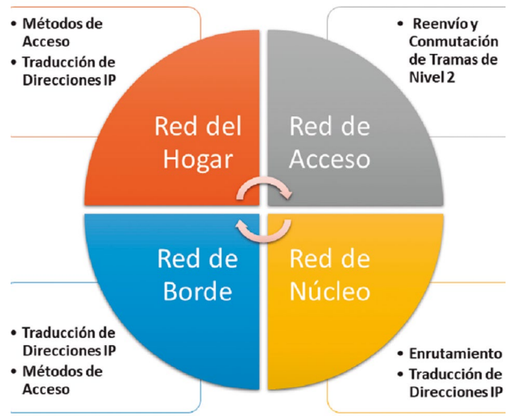


Figura 1. Modelo de Red de Datos para Servicios de Suscripción

Como se observa en la Figura 1 el modelo se divide en Capas de Red y Funciones que se realizan en cada una.

Como parte de la investigación se dividió el modelo en sus partes y se analizó cada una de ellas. Las Capas de Red pueden ser resumidas en una topología como describe la Figura 2.

Cada capa de Red, así como el equipamiento que la compone, son descritos a continuación:

Red del Hogar o Residencial

Esta Capa de Red involucra los terminales de usuario que se conectan al Equipo en la Sede del Cliente o CPE —*Customer Premises Equipment*—.

Red de Acceso

Esta Capa de Red involucra los equipos de la Capa de Enlaces del Modelo OSI —*Open Systems Interconnection*— cuya principal función es conmutar tramas Ethernet. En este caso pueden estar los Conmutadores Capa 2 y las Terminaciones Ópticas de Línea (ITU-T, 2008) u OLTs —*Optical Line Termination*—.

Red de Borde

Esta Capa de Red involucra los equipos encargados de la Asignación de las Direcciones IP, los Métodos de Acceso, y el comienzo-terminación de túneles para la técnica de tunelización y el CGN. El Servidor Remoto de Acceso de Banda Ancha (Ooghe, Varga y Dec, 2010) o BRAS —*Broadband Remote Access Server*— es el equipo principal de esta red, aunque en algunos Operadores la terminación de túneles y el CGN se puede realizar en un equipo dedicado diferente del BRAS.

Red de Núcleo

Esta Capa de Red involucra los equipos encargados del transporte de datos desde el BRAS hacia la red destino y viceversa. En la mayoría de las redes actuales se usa algún tipo de configuración por Conmutación de Etiquetas Multiprotocolo o MPLS —*Multiprotocol Label Switching*— (Rosen, Viswanathan y Callon, 2001), cuyos componentes principales son los P (enrutadores de proveedor) y los enrutadores de borde o PE —*Provider Edge*—.

Métodos para enfrentar el agotamiento de las direcciones IPv4

Como parte del método histórico lógico se estudiaron los antecedentes del agotamiento de las direcciones IPv4. A continuación se describen las técnicas usadas actualmente por los Proveedores de Servicio para enfrentar el efecto de este agotamiento.

Método de Pila Dual

Como se define en (Nordmark y Gilligan, 2005), el método de Pila Dual se refiere a proporcionar el interfuncionamiento de mensajes entre dispositivos terminales/nodos de red y nodos IPv4/ IPv6 mediante la instalación de pilas de protocolos IPv4 e IPv6 en dispositivos terminales y nodos de red (ver Figura 3).

Los enrutadores que admiten la pila dual IPv4/ IPv6 permiten que la red actúe como dos redes lógicas paralelas y permiten una transición sin problemas a IPv6.

Tunelización

La Tunelización se utiliza para interconectar redes IPv6 aisladas a través de una red IPv4 o islas

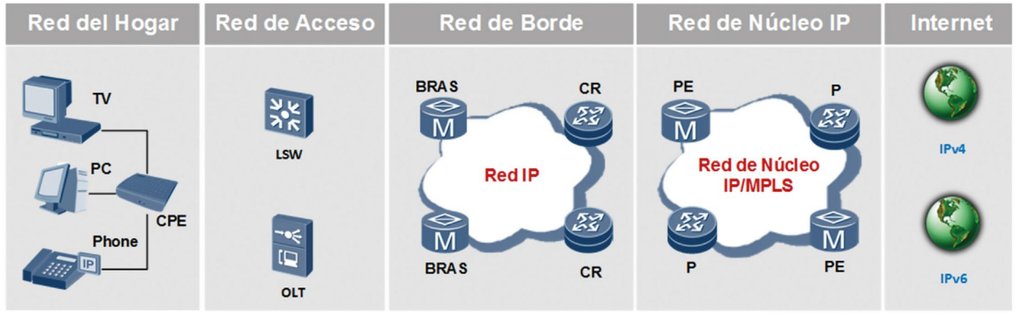


Figura 2. Red de Banda Ancha de un Operador de Telecomunicaciones Genérico

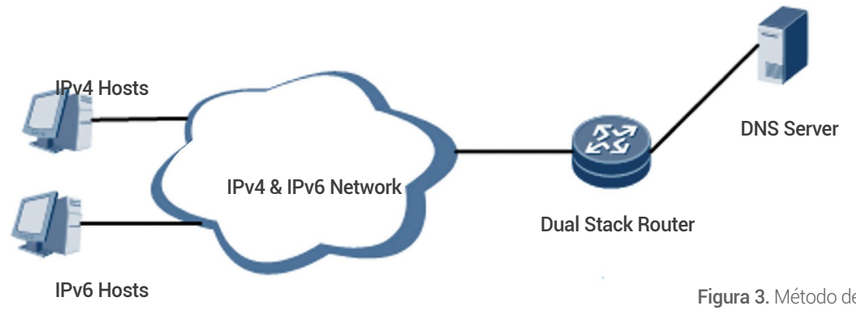


Figura 3. Método de Pila Dual

IPv4 aisladas a través de una red IPv6. Como se muestra en la Figura 4, la técnica de tunelización solo requiere que los nodos de borde implementen la Pila Dual y permite que los datos de una familia de direcciones atraviesen la red de otra familia de direcciones a través de un túnel.

La tunelización es un método más atractivo para la transición de IPv6 en una etapa temprana. A medida que se desarrolla la transición de IPv6, incluso las redes IPv4 aisladas pueden conectarse a través de túneles. Sin embargo, las desventajas del método de tunelización son que los encabezados de doble IP aumentan los costos de red, los puntos finales del túnel requieren un trabajo adicional en escalabilidad y confiabilidad, y pueden ocurrir algunos problemas de MTU, por sus siglas ampliadas en español, Unidad Máxima de Transferencia. En la Tabla 1 se muestran los tipos de tunelización que existen en la actualidad.

Método de Traducción

La traducción se utiliza para el interfuncionamiento entre redes solo IPv6 y redes solo IPv4. Los dispositivos de traducción se encuentran en el borde de dos redes. Necesitan intercambiar a la fuerza los campos correspondientes del encabezado IP y traducir la dirección IP que se lleva en el cuerpo del paquete.

Técnicas actuales de transición a IPv6

Como parte de la investigación se estudian las principales técnicas usadas en la actualidad para lidiar con el agotamiento de direcciones IPv4. Las técnicas de transición a IPv6 son el puente entre las dos familias de protocolos. La implementación de estas técnicas es la manera de aumentar los servicios (en IPv4 e IPv6) sin degradar la calidad de estos. En el caso específico del uso de estas técnicas para el soporte de Servicios de Acceso por Suscripción el Fórum de Banda Ancha o Broadband Forum ha liberado varios Reportes Técnicos (Wright y Cheng 2012) que abordan esta temática de una manera profunda.

Técnica Dual-Stack Lite

El estándar Dual-Stack Lite permite a un Operador de Telecomunicaciones compartir direcciones IPv4 entre clientes mediante la combinación de dos métodos conocidos: la tunelización (IPv4-en-IPv6) y traducción de direcciones de red NAT —*Network Address*

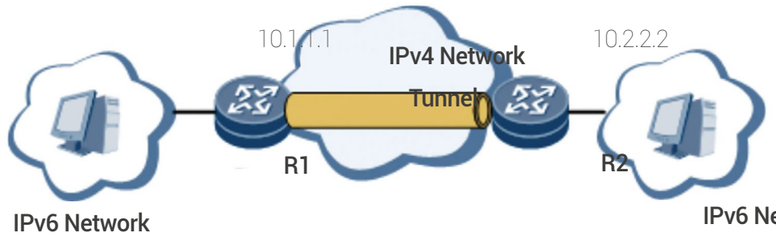


Figura 4. Método de Tunelización

Tipo de Tunelización	Descripción	Escenario de Uso
Manual	IP-en-IP o Encapsulación Genérica de Enrutadores GRE (Farinacci,2000) para la encapsulación de paquetes.	Los túneles de este tipo se configuran manualmente. Son fáciles de implementar y son ampliamente compatibles con dispositivos de red. Sin embargo, no son adecuados para el despliegue a gran escala.
Automática	Se utiliza el modo IPv6 en IP. La encapsulación automática de túnel es sin estado. Se implementa a través de direcciones IPv6 con direcciones IPv4 integradas. Las direcciones 6to4 usan el conocido prefijo, 2002:IPv4-Dir-Pub: Sufijo	Los túneles automáticos se utilizan solo como túneles IPv6 en IPv4. Se implementan a través de direcciones IPv4 integradas. Basándose en la topología de IPv4, los túneles automáticos son aplicables a la etapa inicial de la transición de IPv6.
Túnel MPLS	6PE/6VPE	Los túneles MPLS tienen un elevado rendimiento de reenvío. Son aplicables a los núcleos de red. Se requieren infraestructuras MPLS.

Tabla 1. Tipos de Tunelización

Translation— (Durand, Drooms, Woodyatt y Lee, 2011). Como se describe en la Figura 5 la solución se basa en usar un túnel establecido entre el Enrutador Residencial (CPE), el cual tiene el rol de iniciador de túnel, llamado DS-Lite Basic Bridging Broadband o B4, y un concentrador de túnel, llamado AFTR —*Address Family Transition Router*— ubicado en algún lugar de la Red del Operador.

El CPE soporta configuración híbrida en su interfaz de Red de Área Local, pero solo IPv6 en su interfaz con el Operador. El túnel DS-Lite se usa para transmitir datagramas IPv4 con direccionamiento privado que están encapsulados en datagramas IPv6.

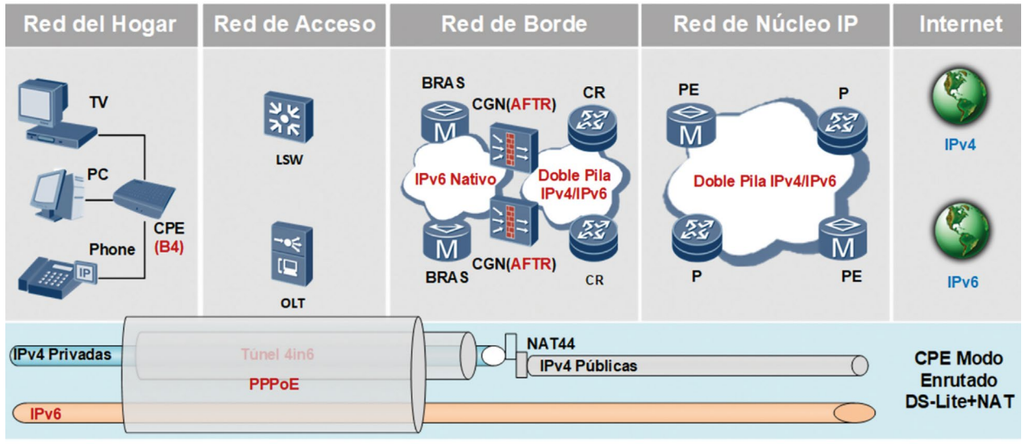


Figura 5. Mecanismo de Transición DS-Lite

Características

- No es necesario que las direcciones privadas IPv4 sean enrutadas dentro de la red del Operador.
- No se requiere la asignación de IPv4 por el Enrutador Residencial.

No es necesaria la existencia de un servidor DHCP —*Dynamic Host Configuration Protocol*— o PPP —*Point to Point Protocol*— para la red IPv4 del Proveedor de Servicios.

- Solo es necesario un nivel de traducción de direcciones (NAT) en la red (ubicado en el AFTR).
- Soporta una arquitectura centralizada y distribuida (pueden existir varios dispositivos CGN, ejemplo uno por Punto de Presencia y puede ser implementado de forma dinámica dentro o fuera del BRAS.

Técnica NAT64

La traducción de direcciones NAT64 es una tecnología que traduce IPv6 Direcciones de red en direcciones de red IPv4 (Bagnulo, 2011). NAT64 es requerido cuando los usuarios acceden a IPv4 Servicios a través de una red IPv6. Esta técnica se aplica a la última fase de la transición de IPv6 en la que IPv6 es la familia de protocolos principal. Los nuevos usuarios conectados a una red IPv6 pueden acceder a los servicios restantes de IPv4 a través de IPv6 red. En la Figura 6 se muestra la topología de la Técnica NAT64.

Principio de Operación (Figura 7)

Cuando una PC con IPv6 accede al servidor del servicio IPv4, la ruta y el procesamiento del tráfico de datos se describe a continuación:

1. La PC IPv6 envía el paquete de solicitud de DNS —*Domain Name System*— al servidor DNS4 y el tráfico de datos IPv6 pasa a través del SWITCH, BRAS, Servidor DNS64.
2. El servidor DNS64 envía un paquete de resolución DNS a PC IPv6 y pasa el tráfico de datos IPv6 pasa a través del BRAS, SWITCH, PC IPv6.
3. La PC IPv6 envía el paquete de solicitud de DNS al servidor DNS64 y el tráfico de datos IPv6 pasa a través del SWITCH, BRAS y el Servidor DNS64.
4. El servidor DNS64 envía un paquete de resolución DNS a PC IPv6 y el tráfico de datos IPv6 pasa a través del BRAS, SWITCH, PC IPv6.
5. El tráfico de datos de IPv6 se envía desde la PC de IPv6 y pasa SWITCH, BRAS, NAT64 CGN / CR.
6. En el dispositivo NAT64 CGN/CR —*Core Router*—, el NAT64 se realiza para convertir el tráfico de datos IPv6 en el tráfico de datos IPv4.

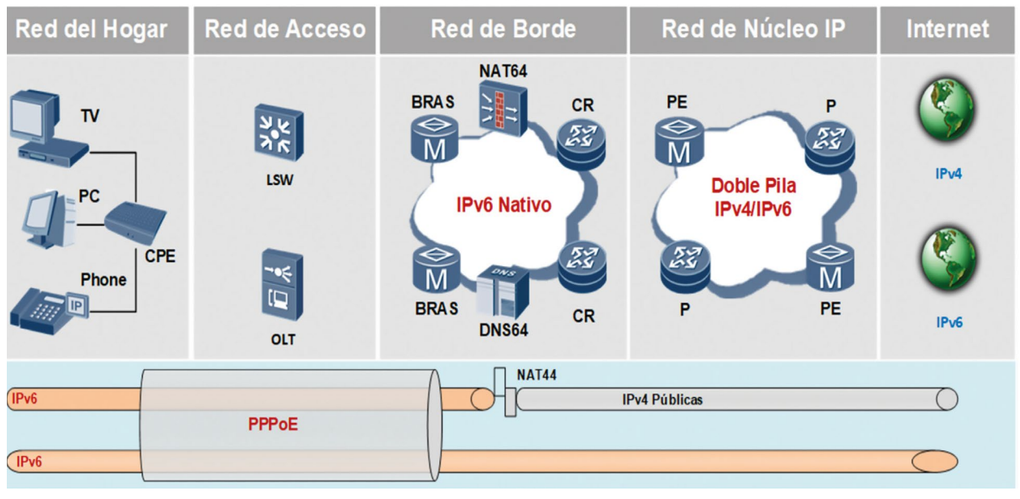


Figura 6. Técnica NAT64

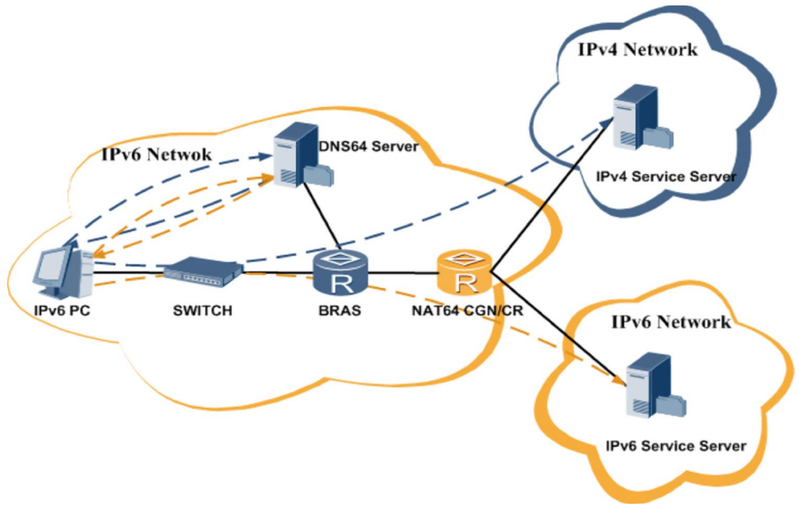


Figura 7. Principio de Operación Técnica NAT64

7. El tráfico de datos IPv4 se envía desde el dispositivo NAT64 CGN/CR al servidor de servicio IPv4.

Cuando la PC IPv6 accede al servidor del servicio IPv6, la ruta y el procesamiento del tráfico de datos es descrito como el mismo que cuando una PC con IPv6 evalúa el servidor de servicio IPv4.

Técnica Pila Dual + NAT444

En la técnica de Pila Dual + NAT444 al menos parte del Proveedor de Servicios soporta transmisión de paquetes IPv6. Además, la función NAT444 que es una modalidad CGN NAT444 responsable de traducir las direcciones IPv4 privadas en direcciones públicas, se ubica dentro de la red del Proveedor de Servicios. A cada Enrutador Residencial se le asigna al menos un prefijo IPv6 global, además de una red privada IPv4 localmente ruteable en la red del operador, la cual es luego nateada a una dirección globalmente ruteable por la función del CGN que ocurre en el BRAS o en otro dispositivo. Los paquetes IPv6 son transmitidos sin encapsulación dentro de la Red del Proveedor de Servicios. En la Figura 8 se muestra la topología de una red usando la Solución de Pila Dual + NAT444.

Los siguientes principios son fundamentales en la Técnica Pila Dual + NAT444:

Se ofrece Conectividad IPv6 nativa a los clientes.

Se mantiene compatibilidad de los servicios IPv4 compartiéndolos entre múltiples suscriptores.

No es necesario cambiar toda la red de núcleo a IPv6.

Principio de Operación

La red troncal debe ser configurada en modo de Pila Dual o Híbrido, esta configuración es conocida como 6PE en la cual los paquetes IPv6 se transmiten dentro de un túnel MPLS y pasan a través de la red troncal MPLS. Los equipos de borde deben tener habilitada la Pila Dual. Para habilitar el acceso de los usuarios a las redes públicas IPv4 es necesario el CGN. El CPE puede ser configurado en modo puente y en ese caso el modo del CGN será NAT44 ya que a traducción de direcciones IPv4 Privadas a Públicas se realizará solo una vez. Si el CPE se configura en modo de Enrutamiento, la modalidad del CGN será NAT444 ya que se realizará una doble traducción de direcciones: una en el Enrutador Residencial y la otra en el BRAS.

Selección de la Técnica a aplicar

Todas las técnicas de transición a IPv6 estudiadas tienen ventajas y desventajas. Por lo tanto, se usó un grupo de parámetros para decidir cuál sería la mejor

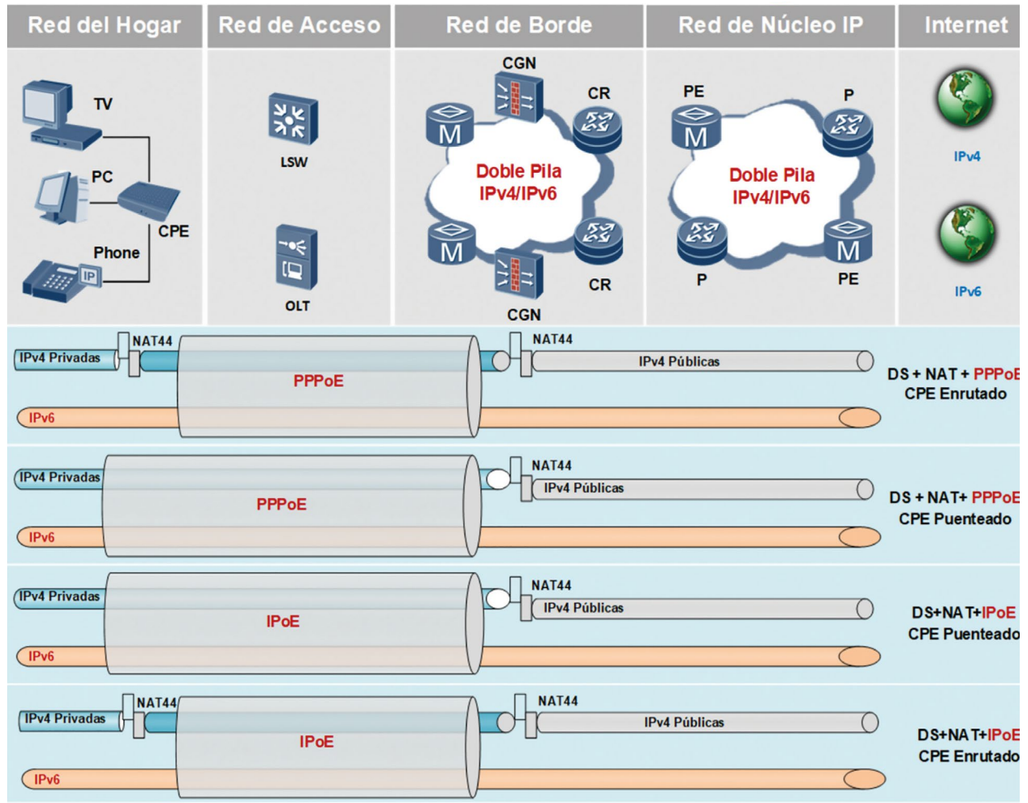


Figura 8. Técnica de Pila Dual+NAT444

técnica. La decisión tendría como premisa el caso de un Proveedor de Servicios cuyo direccionamiento público IPv4 está en Fase de Agotamiento. Este Proveedor de Servicios hipotético desea mantener sus servicios en IPv4 y poder crecer sin que esto le traiga fallas o pérdida en la Calidad del Servicio. Para el caso de un Operador que necesite mantener sus servicios IPv4 mientras permite un crecimiento masivo de su base de usuarios que pueden utilizar direccionamiento IPv6. Los parámetros de decisión que se tuvieron en cuenta están listados en la Tabla 2.

Cada uno de los parámetros de la Tabla 2 se evaluó y se obtuvo una gráfica como la que se muestra en la Figura 9.

Propuesta

Luego de seleccionar la técnica de Pila Dual + NAT444 como la mejor Técnica de Transición según el resultado mostrado en la Tabla 2, se describe la propuesta que tiene como objetivo la investigación. En esta sección se detalla la solución propuesta para la Red de Datos que soporte el Acceso a Internet por Suscripción. La propuesta se presenta dividida en sus cuatro partes fundamentales: Enrutamiento, Interrelación entre los Elementos de Red, el Flujo de Operaciones entre los Elementos de la Red y las Funciones de cada Capa de Red que componen el servicio.

Enrutamiento

Se propone que el enrutamiento sea basado en MPLS ya que es la tecnología de mayor madurez actualmente para el despliegue de redes de núcleo. La arquitectura MPLS ofrece mediante el uso de las etiquetas para trazar los trayectos de bondades como la Calidad de Servicio, la Ingeniería de Tráfico y la

Parámetro	Descripción
Impacto en el suscriptor y el servicio.	Se trata de escoger la Solución donde la experiencia del suscriptor se afectará menos.
Costo de la Migración	El costo de la migración hacia la Solución escogida debe ser el menor posible que permita la introducción de la tecnología.
Complejidad Operativa de la Solución	La Solución escogida debe ser la menos complicada a nivel de configuración y de mantenimiento en los equipos de la red.
Madurez de la Solución	La Madurez de la Solución se define en base a: Despliegue en las redes actuales Soporte en los dispositivos Definición en estándares

Tabla 2. Parámetros decisores

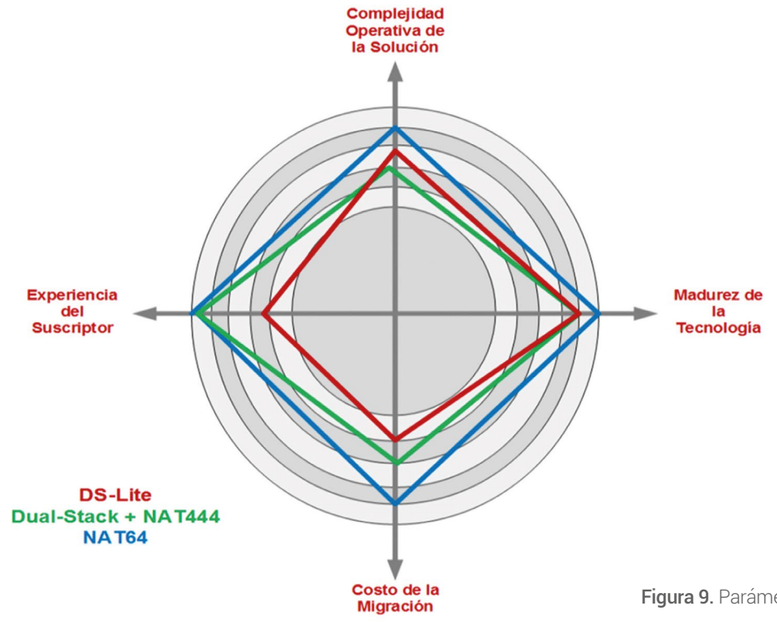


Figura 9. Parámetros decisores

posibilidad de reenviar tráfico unicast y multicast. Entre los enrutadores de borde PE y los enrutadores P se establecen adyacencias IS-ISv4 e IS-ISv6 con el objetivo de que se construyan las tablas de rutas necesarias para el plano de control de la red MPLS. El BGP4+ se usa para anunciar las direcciones IPv6 de los clientes. Los PEs establecen sesiones BG4+ con los reflectores de rutas (RRs). Los reflectores de rutas (Route Reflector en inglés) son enrutadores con la función específica de jerarquizar todas las sesiones BGP4+. De esta manera, no es necesario establecer una malla de sesiones BGP4+. (Figura 10)

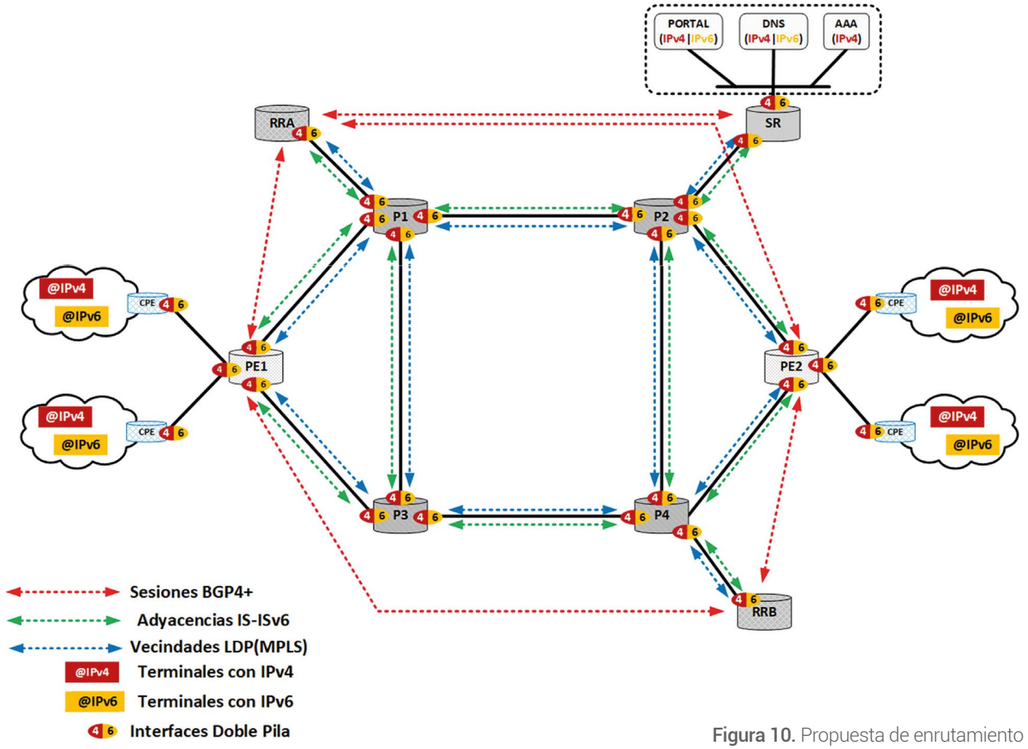


Figura 10. Propuesta de enrutamiento

Interrelación entre los Elementos de Red

La Figura 11 describe la interrelación entre los elementos de red que soporta el Servicio de Acceso a Internet por Suscripción. Los flujos en color naranja y verde indican los tráficos de IPv4 e IPv6 que el cliente será capaz de cursar. Se propone que el protocolo de enrutamiento de la red MPLS soporte la doble pila o pila dual. El método de acceso que se propone es el PPPoEv6 con asignación de direcciones de enlace WAN —*Wide Area Network*— y prefijos delegados (IA+PD). En la propuesta el BRAS debe ser capaz de seguir trabajando con CGN para permitir el ahorro de direcciones IPv4 en los clientes que utilicen solo la familia de direcciones IPv4. La comunicación del BRAS con los elementos de control y aplicaciones como el servidor RADIUS y el Portal puede ser IPv4, evitando migraciones complejas.

La Tabla 3 explica la interconexión lógica entre los Elementos de Red del Modelo la cual describe la forma en que se conectan a nivel de protocolos los elementos de red del modelo.

Flujo de Operaciones del Servicio de Acceso por Suscripción

En la Figura 12 se observan las diferentes capas del flujo de operaciones de la solución propuesta que se divide en las siguientes capas:

Acceso: Este nivel abarca el establecimiento de la sesión PPPoE —*Point-to-Point Protocol over Ethernet*— entre el CPE y el BRAS para lo cual se intercambian los mensajes de descubrimiento y establecimiento de la sesión que involucran la Capa de Protocolo de Control de Enlace del Protocolo Punto a Punto (PPP LCP). Los mensajes Reto y Respuesta (Challenge y Response) forman parte del mecanismo de autenticación usado en PPPoE (CHAP). El autenticador (BRAS) envía un reto al autenticado para originar la autenticación, el campo Datos contiene el

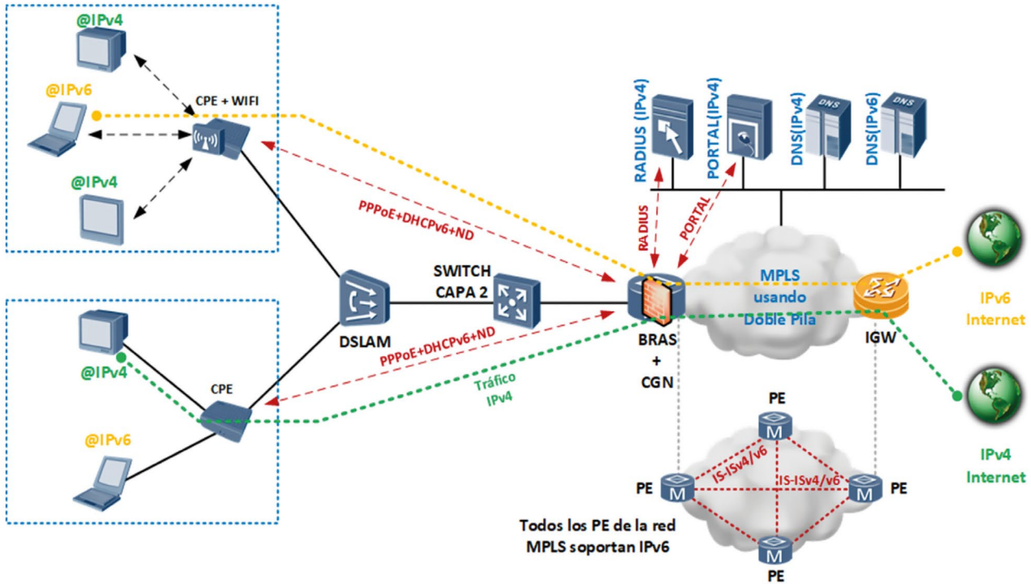


Figura 11. Interrelación entre elementos de la red

Red	Descripción
RED DEL HOGAR	El CPE establece sesiones PPPoE IPv4 con el BRAS para los terminales IPv4. El CPE establece sesiones PPPoE IPv6 con el BRAS para los terminales IPv6.
RED DE ACCESO	El BRAS establece sesiones usando el protocolo RADIUS con el servidor RADIUS. El BRAS establece sesiones usando el protocolo PORTAL con el servidor PORTAL.
RED DE TRANSPORTE	Los Enrutadores PE establecen adyacencias entre sí usando el protocolo de enrutamiento BGP y establecen sesiones BGP con el RR.
SERVIDORES	Los terminales con dirección IPv4 realizan solicitudes DNSv4 al Servidor de Nombres de Dominio DNSv4 y realizan solicitudes DNSv6 al Servidor de Nombres de Dominio DNSv6.

Tabla 3. Interrelación entre los Elementos de Red

reto. El autenticado (CPE) retorna la información de usuario al autenticador. El campo Datos contiene la información retornada sobre el usuario y la contraseña encapsulada.

Autenticación: El BRAS y el servidor AAA —*Authentication, Authorization and Accounting*— intercambian paquetes RADIUS para autenticar al CPE utilizando las credenciales obtenidas del intercambio entre Autenticador y Autenticado.

Asignación de Direcciones IP: En este bloque se describen los mensajes que se intercambian entre el BRAS y el CPE con el objetivo de que el BRAS asigne al CPE direcciones de ambas familias tanto IPv4 como IPv6. El protocolo IPCP se encarga de la negociación y el control de los parámetros IPv4 de tal manera que PPPoE se pueda usar para transmitir paquetes IP. Del mismo modo, el homólogo del protocolo IPCP, IPv6CP es utilizado para la familia de

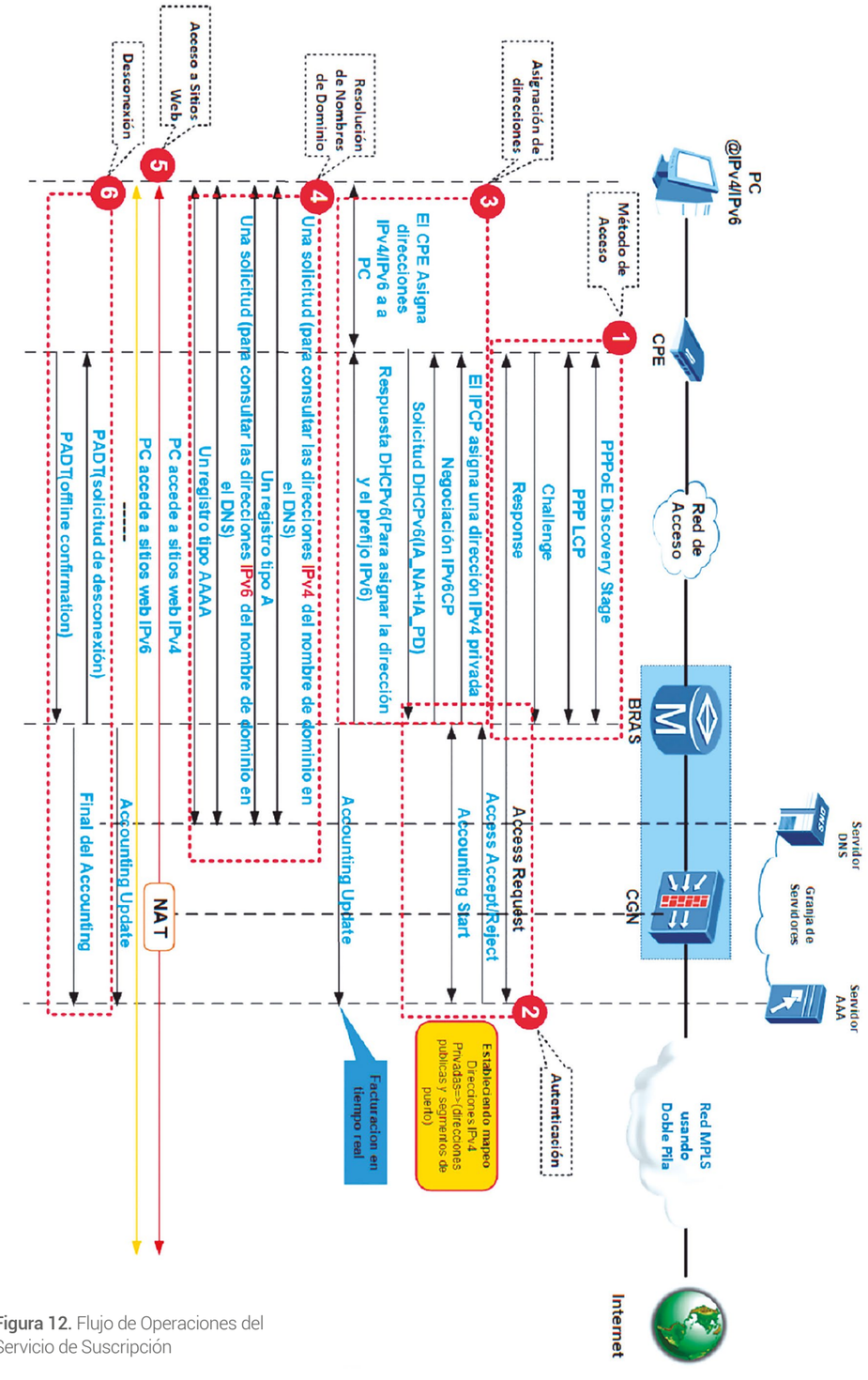


Figura 12. Flujo de Operaciones del Servicio de Suscripción

direcciones IPv6. El protocolo DHCP en sus versiones v4 y v6 es el encargado de asignar al CPE direcciones de las familias IPv4 e IPv6 respectivamente. Para el caso específico de DHCPv6 se propone la modalidad de IANA+IAPD para que en una misma respuesta DHCPv6 se asignen la IPv6 del CPE para conectarse al BRAS, así como la del prefijo que el CPE va a entregar a los terminales en la Red del Hogar.

Resolución de Nombres de Dominio: Las solicitudes DNS se realizan a servidores por separado, los terminales IPv4 a los servidores DNSv4 y los terminales IPV6 a los servidores IPv4.

Acceso a los Sitios Web: Los terminales IPv4 e IPv6 establecen conexiones con servidores pertenecientes a las mismas familias de direcciones respectivamente.

Desconexión: El proceso de desconexión involucra al protocolo PPPoE el cual usa los mensajes PADT y PADS entre el BRAS y el CPE para la terminación de la sesión. Asimismo, el servidor RADIUS deja de facturar al usuario por lo cual el BRAS le envía un mensaje de Accounting-Stop o Final de la Facturación.

Funciones de las Capas de Red para el Acceso a Internet por Suscripción

En la Tabla 4 se definen cuáles son las funciones y cómo se propone implementarlas en el Modelo de Red de Datos para el Servicio de Acceso a Internet Suscripción.

Conclusiones

El agotamiento de las direcciones IPv4 públicas es ya hoy un hecho para los Proveedores de Servicio. Los Servicios de Acceso a Internet por Suscripción se suman a la convergencia sobre las plataformas IP/MPLS como el servicio residencial por excelencia. Las técnicas de transición a IPv6 varían en base a los métodos que las fundamentan. Cada una de ellas es preferible para una fase de la Migración a IPv6. En la presente investigación se llega a la propuesta de la técnica de Doble Pila + NAT444 basado en el requerimiento de mantener los servicios IPv4 y poder ampliar la red usando el IPv6 para aumentar los servicios.

Red	Descripción
MÉTODO DE ACCESO	Protocolo Punto a Punto sobre Ethernet o PPPoE (Mamakos, Lidl, Evarts, Carrel y Simone, 1999) en modo de Enrutamiento con provisión dinámica de direcciones IPv4 y con DHCPv6(IA_NA + IA _PD) (Mrigalski y cols., 2018).
ENRUTAMIENTO DE DATAGRAMAS IPv6	Para el enrutamiento se proponen los protocolos de enrutamiento IS-ISv6 y BGP4+.
COMPATIBILIDAD CON SERVICIOS IPv4	Para la traducción de direcciones se propone seguir utilizando la solución NAT444 en los casos en los que el terminal no use direccionamiento IPv6.
APLICACIONES	Autenticación, Autorización y Facturación: Se propone el uso de un servidor que soporte el protocolo RADIUS (Rigney, Willens, Rubens y Simpson, 2000) y tenga configurado los atributos Framed-IPv6-Prefix y Framed-IPv6-Pool DNS: Se propone el uso de un servidor DNSv6.

Tabla 4. Funciones de las Capas de Red para el Acceso a Internet por Suscripción

Referencias

Bagnulo, M. M. (2011). Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. Obtenido de Internet Engineering Task Force (IETF), RFC 6146: https://tools.ietf.org/html/rfc6146.

Deering, S., y Hinden, R. (1998). Internet Protocol Version 6 (IPv6) Specification. Obtenido de Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc2460.

Durand, A., Droms, R., Woodyatt, G., y Lee, Y. (2011). Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. Obtenido de Internet Engineering Task Force (IETF), RFC 6333.

ITU-T. (2008). Gigabit-capable Passive Optical Networks (G-PON). ITU-T Recommendation, G.984.

Mamakos, L., Lidl, K., Evarts, J., Carrel, D., y Simone, D. W. (1999). A Method for Transmitting PPP Over Ethernet (PPPoE). Obtenido de Internet Engineering Task Force (IETF), RFC 2516.

Mrigalski, T., M., S., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., y otros. (2018). Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Obtenido de Internet Engineering Task Force (IETF), RFC 8415: https://tools.ietf.org/html/rfc8415.

Nordmark, E., y Gilligan, R. (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers. . Obtenido de Internet Engineering Task Force (IETF), RFC 4213: https://tools.ietf.org/html/rfc4213.

Ooghe, S., Varga, B., y Dec, W. (2010). IPv6 in the context of TR-101. Obtenido de Broadband Forum.

Perreault, S., Yamagata, I., y Miyakawa, S. (2013). Common Requirements for Carrier-Grade NATs (CGNs). Obtenido de Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc6888.

Postel, J. (1981). INTERNET PROTOCOL. Internet Engineering Task Force (IETF).

Rigney, C., Willens, S., Rubens, A., y Simpson, W. (2000). Remote Authentication Dial In User Service (RADIUS). Obtenido de Internet Engineering Task Force (IETF), RFC 2865: https://tools.ietf.org/html/rfc2865.

Rosen, E., Viswanathan, A., y Callon, R. (2001). Multiprotocol Label Switching Architecture. Obtenido de Internet Engineering Task Force (IETF), RFC 3031: https://tools.ietf.org/html/rfc3031.

Wright, S., y Cheng, D. (2012). IPv6 Transition Mechanisms for Broadband Networks. Obtenido de Broadband Forum, TR-242.

Rosen E., Viswanathan A., Callon R. (2001), Multiprotocol Label Switching Architecture. Internet Engineering Task Force (IETF), RFC 3031.

Wright S., Cheng D. (2012), IPv6 Transition Mechanisms for Broadband Networks. Broadband Forum, TR-242.

RESEÑA

Plataformas de control de acceso a redes WLAN. Tendencias, aplicaciones y nuevas tecnologías

Access control platform for WLAN networks. Trends, applications and new technologies

Ing. Reinier Consuegra Peniche[1]

Recibido: 06/2019 | Aceptado: 10/2019

Palabras clave

WLAN
Infraestructura
Herramientas de Control de acceso

Resumen

En este artículo se caracteriza un grupo de herramientas de control de acceso a redes WLAN —*Wireless Local Area Network*—. Además, se ratifica lo brutal que es el bloqueo económico impuesto a Cuba, por el gobierno de Estados Unidos y su impacto en las ramas tecnológicas. Este trabajo pretende promover el desarrollo propio dentro del país de este tipo de soluciones e infraestructura tecnológica existentes. Para el desarrollo del mismo fue utilizado el método de investigación descriptivo basando los resultados en la caracterización de las distintas tecnologías, que se expone en el contenido del presente.

Keywords

WLAN
Infrastructure
Control Access Tools

Abstract

This article features a group of access control tools for WLAN —*Wireless Local Area Network*— networks. In addition, the brutality of the economic blockade imposed on Cuba by the United States government and its impact on the technological branches is ratified. This work aims to promote the development of this type of existing technological infrastructure and solutions within the country. For its development, the descriptive research method was used, basing the results on the characterization of the different technologies that is stated in the content of the present.

Introducción

Con el crecimiento de los servicios WLAN en Cuba y en particular el servicio WLAN público de ETECSA, se ha hecho necesario acondicionar la infraestructura que soporta el mismo, con el objetivo de garantizar una mejor calidad y seguridad. Este servicio está siendo víctima de disímiles ataques, suplantación de identidades y virus, entre otros fenómenos; que están afectando la integridad del mismo. El presente trabajo se basa en el estudio de nuevas tendencias, aplicaciones y nuevas tecnologías para estos fines a nivel mundial.

Por motivos relacionados con el bloqueo económico impuesto brutalmente a Cuba por el Gobierno de los Estados Unidos de América, la adquisición de soluciones de seguridad es compleja para el país. Es por ello que se ha hecho necesario apostar por soluciones de software libre y desarrollo propio con niveles de personalización acordes a las necesidades y requerimientos dispuestos.

[1] Empresa de Telecomunicaciones de Cuba S.A. Dirección de Operaciones de Seguridad, La Habana, Cuba. reinier. consuegra@etecsa.cu

Materiales y métodos

La metodología aplicada para el desarrollo de este trabajo fue fundamentalmente la revisión y análisis de artículos y publicaciones corporativas de distintos proveedores de equipamientos y tecnologías, como Huawei, Cisco, HP entre otros. Estos aplicados con el objetivo de analizar informaciones existentes, así como el análisis de la realidad donde se propone desarrollar la solución.

Resultados y discusión

El presente trabajo expone algunas de las plataformas implementadas en la actualidad para el control de acceso a las redes WLAN. Esto con el objetivo de proponer algunas ideas para posibles despliegues de soluciones de redes inalámbricas. Como parte del desarrollo y crecimiento de las redes de telecomunicaciones a nivel mundial, la exposición e intentos de vulneración a las mismas ha crecido, así como los intentos de clientes de burlar cobros y pagos en los servicios de este tipo brindados por los diferentes proveedores alrededor del mundo. Por esto y otros motivos los distintos proveedores de servicios de internet a través de redes inalámbricas se han dado a la tarea de buscar alternativas para elevar la seguridad y calidad de este tipo de servicios.

Entre los principales proveedores de soluciones de seguridad para redes inalámbricas se encuentra la empresa CISCO, Palo Alto, Juniper entre otras. A continuación, se presenta un resumen de algunas de las soluciones para el control de acceso a redes WLAN.

Impulse SafeConnect

Producto desarrollado por Impulse, empresa emplazada en Estados Unidos. En sus inicios la compañía comenzó en la educación y se ha expandido a los mercados gubernamentales y corporativos. El producto Impulse SafeConnect presenta las siguientes características: soporta la supervisión de 250 a 25 000 terminales con capacidad de conexión en la red. La plataforma está diseñada en una arquitectura escalable lo que posibilita su fácil despliegue operacional. Esta herramienta se centra en lograr control, crear marcos de responsabilidad y mitigar vulnerabilidades en las redes en las que despliega (Impulse, 2019).

ExtremeControl

Producto desarrollado por la empresa Extreme TM, fundada en 1996 y radicada en Estados Unidos. El producto permite aplicar controles granulares sobre quién, qué, cuándo, dónde y cómo se comportan los dispositivos en la red. Puede habilitar BYOD —*Bring Your Own Device*—, acceso de invitados e IoT —*Internet of Things*—, seguros mediante la implementación de políticas en tiempo real, basadas en la postura de seguridad de los dispositivos. ExtremeControl hace coincidir los dispositivos en la red con atributos, como usuario, tiempo, ubicación, vulnerabilidad o tipo de acceso, para crear una identidad contextual que lo abarque todo. Las identidades basadas en roles siguen a un usuario, sin importar desde dónde o cómo se conecta a la red. Se pueden utilizar para aplicar políticas de acceso altamente seguras. Además, permite la supervisión de hasta 200 000 dispositivos conectados a la red y ofrece una arquitectura basada en reglas para automatizar el acceso según los casos de uso (Extreme TM, 2019). (Figura 1)

Auconet BICS

El producto Auconet BICS —*Business Infrastructure Control Solution*— está desarrollado por la empresa Auconet fundada en 1998 por un ingeniero alemán. Esta radica en San Francisco, Estados Unidos. La plataforma propone un sistema NAC —*Network Access Control*— robusto. A diferencia de la mayoría de los proveedores de NAC, BICS puede combinar la autenticación basada en MAC y 802.1X, para una protección más segura orientada para cada tipo de dispositivo. BICS proporciona capacidades para autorizar a los usuarios, dispositivos y puertos, por separado o en cualquier combinación, o bloquea cualquiera de ellos, de acuerdo con las políticas que se predefinan en el sistema, proporcionando así un mayor grado de seguridad. Propone una implementación a gran escala de hasta 1 000 000 de dispositivos identificados en la red, soportada en entornos virtualizados (Aucconet, s.f.).

ForeScout CounterACT

El producto ForeScout CounterACT está desarrollado por la empresa ForeScout radicada en San José, California, Estados Unidos. Es una plataforma orientada a entornos regulados como defensa, finanzas, atención médica y ventas. Además, tiene la capacidad de monitoreo sobre más de un 1 000 000 de distintos tipos

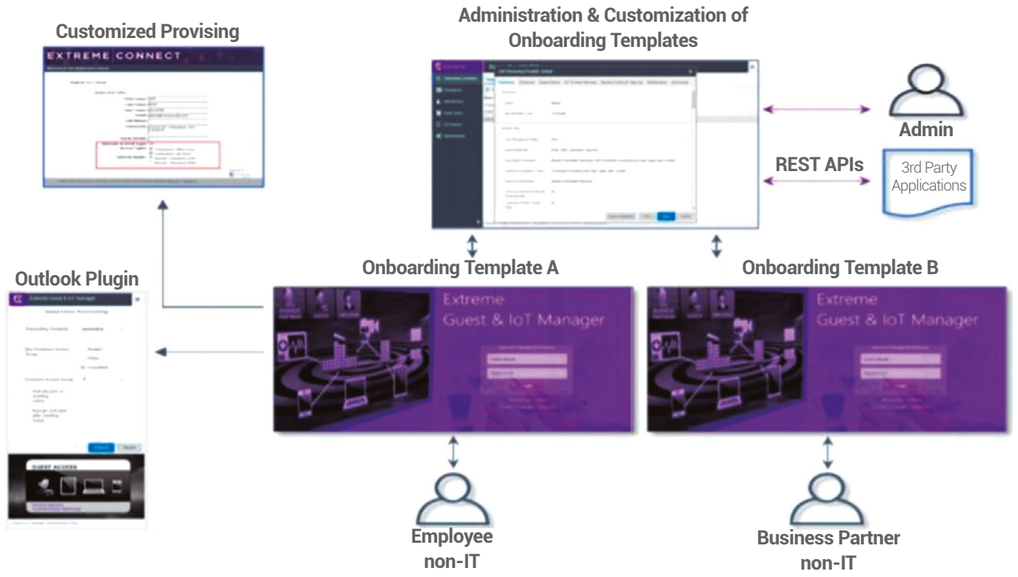


Figura 1. Esquema funcional de ExtremeControl

de dispositivos de red. Es una plataforma que propone una arquitectura escalable vertical y horizontalmente. También propone solución en la nube de internet y está consagrada como una de las principales soluciones de este tipo a nivel mundial (Forescout, s.f.). (Figura 2)

HPE Aruba ClearPass

El producto HPE Aruba ClearPass es un producto desarrollado por empresa holandesa Wentzo Wireless. Es una plataforma que está adecuada fundamentalmente a entornos alto volumen de autenticación, ya que soporta más de 10 millones de autenticaciones por día. Además, se ajusta especialmente a entornos distribuidos geográficamente distantes. Está basada en una arquitectura escalable y de rápido despliegue. También responde a los estándares de las tecnologías BYOD (Wentzo Wireless, s.f.). (Figura 3)

Cisco Identity Services Engine

La plataforma Cisco Identity Services Engine es un producto desarrollado por la empresa Cisco radicada en Estados Unidos. Cisco ISE como también se le conoce está entre los líderes de este tipo de herramientas a nivel mundial. Entre las características que más se destacan se tiene que admite hasta 500 000 sesiones concurrentes y soporta hasta 1 500 000 de dispositivos por cada implementación. Ofrece motores de inteligencia adaptativa, detección y respuesta automatizada y aprendizaje automático. Además, posee una arquitectura de despliegue y escalabilidad tanto horizontal como vertical (Cisco, s.f.).

Figura 2. Alcance operacional plataforma ForeScout CounterACT

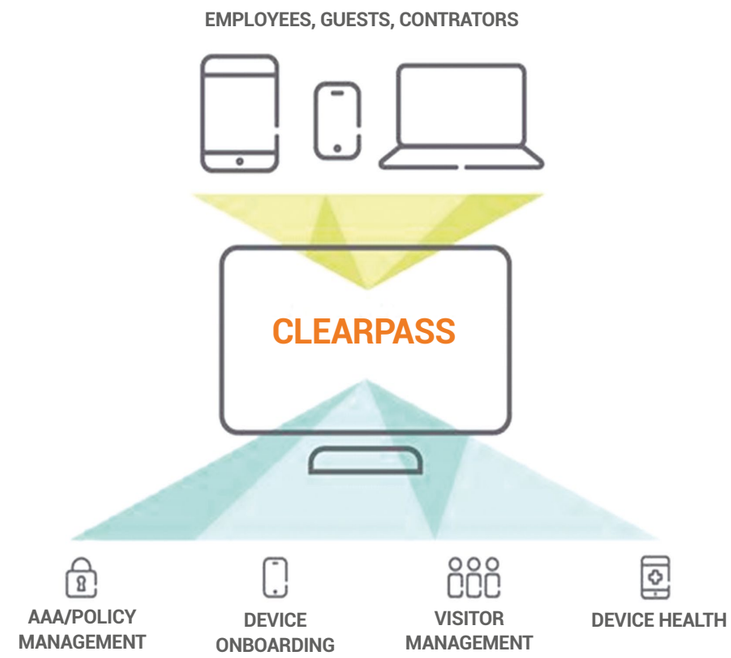


Figura 3. Aruba ClearPass

OpenNAC

OpenNAC es una plataforma de control de acceso a la red de código abierto para entornos LAN / WAN corporativos. Permite la autenticación, la autorización y la auditoría basada en todos los accesos a la red. Es compatible con diferentes proveedores de redes como Cisco, Alcatel, 3Com o Extreme Networks, y diferentes clientes como PC con Windows o Linux, Mac, dispositivos como teléfonos inteligentes y tabletas. Basado en componentes de código abierto y autodesarrollo. Está basado en estándares de la industria como FreeRadius, 802.1x, AD, ldap. Es muy extensible, pueden incorporarse nuevas características porque está diseñado en los complementos. Se integra fácilmente con los sistemas existentes.Por último, pero no menos importante, proporciona servicios de valor agregado tales como administración de configuración, red, configuraciones de respaldo, descubrimiento de red y monitoreo de red (Opennac, s.f.).

Conclusiones

El presente trabajo realizó una caracterización de un grupo de herramientas y plataformas que existen en el mercado de los sistemas de control de acceso para las redes WLAN. También reafirma la complejidad para Cuba de adquirir este tipo de plataformas por los temas relacionados con el brutal bloqueo económico impuesto a Cuba por el gobierno de Estados Unidos de América. Además, reafirma el llamado de estos tiempos a seguir abogando por la soberanía tecnológica que debe tener Cuba en el entorno tecnológico.

Referencias

Aucconet. (s.f.). *Solutions bics for security*. Obtenido de Aucconet.com: https://aucconet.com/solutions/bics-for-security

Cisco. (s.f.). *Cisco Identity Services Engine*. Obtenido de Cisco: https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

Extreme TM. (2019). *ExtremeControl*. Obtenido de Extreme Networks: https://extremenetworks.com

Forescout. (s.f.). *Plataform Counteract*. Obtenido de Forescout : https://www.forescout.com/platform/counteract/

Impulse. (2019). *Safe Connect*. Obtenido de Impulse: https://impulse.com/

Opennac. (s.f.). *Open Source Nac Solution*. Obtenido de Opennac: http://www.opennac.org/opennac/en.html

Wentzo Wireless. (s.f.). *Aruba ClaerPass*. Obtenido de Clearpass: https://www.clearpass.net/

INVESTIGACIÓN

Proyecto de Telemedicina para el Cardiocentro de Villa Clara

Telemedicine project for the Cardiocenter of Villa Clara

MSc. Arelys Emiliana Ramos Fleites[1*], Ing. Lidisvey Herrero González[2], Dr.Sc. Félix Álvarez Paliza[3]

Recibido: 06/2019 | Aceptado: 10/2019

Palabras clave

Telemedicina
PACs
DICOM
Modelación
Simulación de redes

Resumen

La telemedicina abarca varias líneas de investigación siendo el telediagnóstico y la teleimagenología de los temas que se les ha prestado especial importancia en la actualidad. En Cuba, esta es un área que se le ha dedicado mucha atención y es el Cardiocentro de Villa Clara uno de los centros médicos más beneficiados con estos avances. Actualmente, el centro quirúrgico cuenta con una red de alcance nacional, con modernos medios de diagnóstico y terapéuticos y con un personal médico de alta calificación profesional. La presente investigación se centra en evaluar si la actual red del Cardiocentro puede soportar los nuevos servicios de transmisión, recepción y procesamiento de las imágenes que se generan en el tomógrafo computarizado, el angiógrafo y el ecocardiógrafo entre otros equipos usando herramientas de simulación de redes que permiten evaluar el desempeño de la red.

Keywords

Telemedicine
PACs
DICOM
Modeling
Network simulation

Abstract

Telemedicine encompasses several lines of research, with telediagnosis and the imaging of topics that have been particularly important today. In Cuba this is an area in which special attention has been dedicated and it is the Cardiocentro of Villa Clara from the medical centers that benefit most from these advances. Currently, the surgical center has a network of national scope, with modern diagnostic and therapeutic means and with highly qualified medical personnel. This research focuses on evaluating whether the current Cardiocentro network can support the new transmission, reception and processing services of the images generated in the computerized tomograph, the angiograph and the echocardiograph among others using network simulation tools that allow evaluate network performance.

[1*] Universidad Central “Marta Abreu” de las Villas. Villa Clara, Cuba. arelys@uclv.edu.cu
[2] Hospital Cardiocentro Villa Clara. Villa Clara, Cuba. lidisvey@infomed.sld.cu
[3] Universidad Central “Marta Abreu” de las Villas. Villa Clara, Cuba. fapaliza@uclv.edu.cu.

Introducción

Partiendo de la siguiente premisa: La mayoría de los gobiernos se encuentran ante el desafío de adoptar políticas adecuadas que proporcionen servicios sanitarios de calidad; la telemedicina puede significar la solución de muchos problemas en los que la distancia y el tiempo son factores críticos, sin que ello suponga la sustitución del médico por el internet y las computadoras.

La telemedicina se define, según la OMS (1998), como "el suministro de servicios de atención sanitaria en los que la distancia constituye un factor crítico, realizado por profesionales que apelan a tecnologías de la información y de la comunicación con objeto de intercambiar datos para hacer diagnósticos, preconizar tratamientos y prevenir enfermedades y heridas, así como para la formación permanente de los profesionales de atención de salud y en actividades de investigación y evaluación, con el fin de mejorar la salud de las personas y de las comunidades en que viven". (Ruiz Ibáñez, Zuluaga de Cadena y Trujillo y Zea, 2007)

Para la aplicación de cualquier modalidad de la telemedicina es importante diseñar y aplicar estrategias que permitan convertir los conocimientos y las tecnologías de la información y las comunicaciones en instrumentos a disposición del desarrollo integral de las potencialidades y el bienestar de cada uno de sus ciudadanos.

El Cardiocentro de Villa Clara es una de las instituciones élites en el país que presta servicios de cardiología a la región central de Cuba, donde se brinda tratamiento y rehabilitación a los pacientes (adultos y niños) con afecciones cardíacas congénitas y adquiridas. Aquí se realizan acciones asistenciales, docentes, investigativas y de introducción de nuevas tecnologías, en coordinación con la atención primaria en la Red Cardiológica Central (desde Villa Clara a Camagüey). El centro comenzó su trabajo en julio de 1986 y desde sus inicios ha ido desarrollando y diversificando su trabajo asistencial y quirúrgico con novedosas técnicas y equipos de diagnóstico que lo han llevado a ser un centro insigne en el país. Actualmente presta servicios de cirugía cardíaca, cardiología intervencionista, electrofisiología, cirugía vascular mayor, angioTAC con un moderno tomógrafo de doble cabezal y 128 detectores que realiza todo tipo de estudio.

Partiendo de un análisis cualitativo de la infraestructura actual de la red y teniendo en cuenta el equipamiento de diagnóstico que forma parte del sistema Xavia-PACs —*Picture Archiving and Comunications System*— para almacenar, procesar y visualizar las imágenes médicas generadas en los equipos de diagnóstico se proponen una serie de mejoras a la actual red del Cardiocentro de Villa Clara para soportar los nuevos servicios de transmisión de imágenes médicas en formato DICOM (Miguel Chavarría Día, n.d.) que se generan en los equipos de diagnóstico. Para esto se analizan y describen los elementos actuales que forman el sistema de telemedicina y la red con que cuenta el centro para sobre esta evaluación previa proponer las mejoras a la red y evaluar su comportamiento teniendo en cuenta el tráfico que se genera hacia la red inalámbrica la inclusión de nuevos puntos de acceso inalámbricos desde donde serán consultados y visualizados los diagnósticos médicos de los pacientes.

La simulación de la red se hace con el software de simulación y modelación de redes OPNET 14.5 (Honghi Yang, n.d.) que permite diseñar varios escenarios con variantes diferentes y evaluar un alto número de variables y estadísticas globales de nodo y de enlace que miden el desempeño de la red relacionadas en este caso con los tiempos de respuesta de los servidores, el retardo de la red, los porcientos de utilización de los enlaces, la carga en los servidores, el tráfico de la red inalámbrica, etc.

Materiales y métodos

Para el análisis de la red se utiliza la herramienta de modelación y simulación de redes OPNET Modeler en su versión 14.5. Se adiciona al análisis el servicio ofrecido por la red Wifi para que los médicos y pacientes puedan desde sus dispositivos móviles acceder a los diagnósticos emitidos. Este proyecto brinda una caracterización de los principales softwares y equipos que componen la red. Se describe el producto Xavia PACS, diseñado por la Universidad de Ciencias Informáticas (UCI) y de vital importancia en el funcionamiento de los principales servicios que ofrece el Cardiocentro.

Elementos que forman un sistema de telemedicina

Un sistema de telemedicina está integrado por varios elementos que se definirán a continuación:

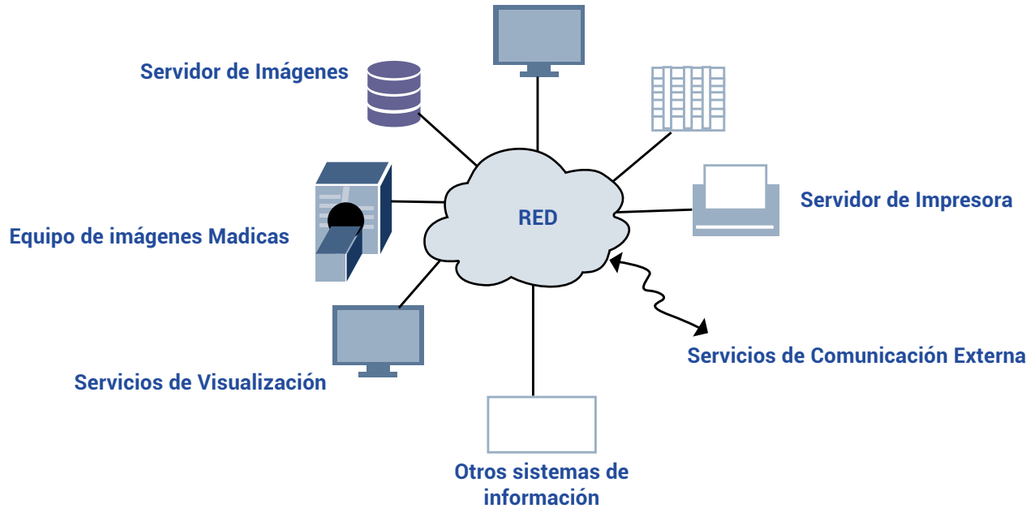


Figura 1. Elementos que componen el sistema PACs.

PACs: Es un sistema de almacenamiento lógico de imágenes radiológica y su distribución (figura 1), las cuales pueden ser recuperadas desde programas habilitados para tal fin según la necesidad del usuario, ya sea de forma inmediata para estudios actuales o de forma retardada para estudios almacenados en dispositivos de almacenamiento secundario, estas imágenes son recibidas desde las distintas modalidades o técnicas usadas para la obtención de la imagen médica (Smith y Berlin, 2012). Esta definición corresponde a la traducción literal de sus siglas *Picture Archiving and Comunications System*.

DICOM —*Digital Imaging Communication on Medicine*—: Es el estándar o protocolo específico que utilizan los sistemas PACs y que posibilita la comunicación entre equipos generadores de imagen, sistemas de almacenamiento PACs, clientes visores de imágenes y cualquier otro evento relacionado con la imagen médica (K. Delac, n.d.). La última versión adoptada es la 3, las imágenes que se generan en estos equipos son compatibles con el estándar DICOM. Los ficheros DICOM constan de una cabecera con campos estandarizados y campos de forma libre, y un cuerpo con la imagen propiamente dicha. La cabecera del archivo DICOM presenta etiquetas o campos que permiten situar a la imagen en el contexto, identificándola correctamente y vinculándola a un paciente concreto. (Figura 2)

Sistema HIS-RIS-PACs

RIS —Sistema de Información Radiológica—: Es el programa que gestiona las tareas administrativas del departamento de radiología: citaciones, gestión de salas, registro de actividad e informes.

HIS —Sistema de Información Hospitalaria—: (Álvarez y Vargas Solís, 2013). Programa de gestión del hospital.

Interacción: El RIS proporcionará al PACs toda la información sobre las citaciones existentes, esto implica que cualquier estudio que se quiera almacenar en el PACs ha de tener una cita previa en el RIS.

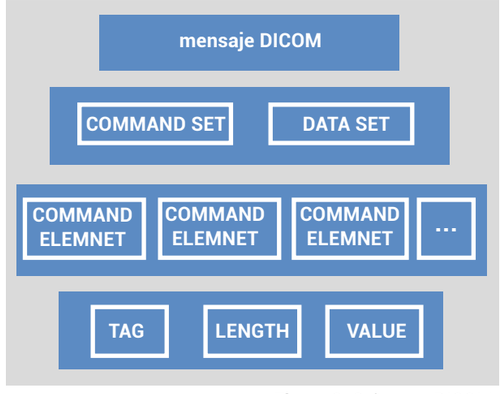


Figura 2. Cabecera DICOM

A su vez el PACs notificará al RIS que el estudio ha sido realizado y completado para posteriormente proporcionar al radiólogo las imágenes de la exploración realizada de forma que este pueda elaborar el informe correspondiente en el RIS. Una vez finalizado el referido informe, el RIS envía una copia al PACs y la notificación de que el informe ha sido realizado. (Nm y G, 2016).

Visor Web: se considera parte del PACs, ya que es la herramienta que permite la visualización de las imágenes en cualquier PC del hospital que disponga de un navegador. A su vez el visor Web puede distribuir el informe asociado al estudio, reduciendo el tiempo de recepción para el destinatario y la supresión del papel. El visor Web recibe la imagen en formato DICOM y la convierte a un formato diferente de menor tamaño, usando para ello una comprensión con pérdida, esto implica una reducción de la calidad por debajo de la considerada como diagnosticable.

Producto XAVIA-PACs: Desarrollado por la UCI —Universidad de Ciencias Informáticas— puesto a prueba en varios hospitales nacionales. Tiene como objetivo ayudar a informatizar los servicios de diagnóstico por imágenes en el sistema de salud y a un aprovechamiento más óptimo de los equipos de adquisición de imágenes, dándole mayor capacidad y brindando un servicio de mejor calidad a los pacientes. Sus principales componentes son:

XAVIA PACs Viewer —Estación de diagnóstico general—: Posee herramientas para el procesamiento, análisis y visualización de las imágenes médicas con herramientas básicas y de post procesamiento 3D. Permite la conexión remota desde las estaciones de trabajo hasta el servidor de imágenes del hospital, recibe los estudios directamente de los equipos de generación de imágenes e intercambia estudios entre las estaciones de trabajo de los especialistas. Permite además la generación de informes imagenológicos, la exportación a formatos comunes de imágenes, videos digitales y la impresión de imágenes en papel o películas radiográficas. Se integra al PACs-RIS. Tiene 3 módulos principales: bandeja de casos, visor y configuración que se visualizan a través de su interfaz gráfica. (Figura 3)

XAVIA PACs Reporter —Herramienta de edición de informes imagenológicos—: Sistema para la emisión de informes de estudios radiológicos que cubre los

Figura 3. Ventana de inicio del visor Web del Xavia-PACs

distintos flujos que se pueden presentar en un servicio de radiología. Puede trabajar en modo desconectado. Entre sus principales funcionalidades se encuentran: generar informes imagenológicos, creación de plantillas para informes de diagnósticos que se repitan, impresión de reportes en formato estándares de edición de documentos, corrección ortográfica y codificación de enfermedades.

XAVIA PACs Server —Servidor de imágenes médicas—: Posibilita la gestión de la información de los estudios que se generan en las diferentes modalidades diagnósticas, garantiza el archivo de los estudios de forma ordenada, búsqueda y recuperación de los estudios desde cualquier estación de trabajo o equipo de generación de imágenes. Cuenta con un grupo de herramientas para la administración de sus recursos y permite crear políticas de mantenimiento como compresión y borrado según configuración, además de la ejecución de tareas programadas ante situaciones críticas y la sincronización de la información que hay en las bases datos y el archivo físico.

Esquema topológico de la red del Cardiocentro

La red sigue una topología tipo árbol donde los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al switch central. La mayoría de los dispositivos se conectan a uno secundario que, a su vez, se conecta al switch central existiendo varias cascadas que afectan el desempeño de la red. Esta topología brinda la posibilidad de que cada nuevo nivel pueda a su vez ramificarse en otros lo

que genera un árbol jerárquico de conexiones, donde la falla en un nivel afecta a los siguientes, pero no a los anteriores. Los enlaces con el switch principal son con cable UTP categoría 6 con una velocidad de transmisión de 1Gbps. También se aprecia la existencia de muchas cascadas, lo cual afecta el desempeño final de la red, estas cascadas son necesarias en el diseño actual debido a que la distancia existente entre los switches es mayor que 100 metros, esto equivale a tener que usar esa misma cantidad de metros de cable UTP lo cual no está permitido según la norma TIA/EIA 568-C referente al cableado estructurado. La red actual es escalable pero no tiene redundancia. El swicht principal es de la marca TP-Link es capa 2 y tiene 24 puertos de cobre RJ45 a gbps y 4 ranuras de fibra óptica. Los enlaces al switch central son a 1gbps. Se cuenta con aproximadamente 110 PCs algunas de alta resolución para poder visualizar las imágenes DICOM.

El servidor PACs es del tipo Dell POWEREDGE T610 diseñado para simplificar las operaciones diarias y minimizar el tiempo de subida de un archivo, brinda un gráfico basado en estadísticas de la red y una pantalla LCD interactiva para sistemas de salud monitorizados, también posee una capacidad interna de almacenamiento de 16Tb (“Redes de Computadoras, 5ta Edición - redes_de_computadoras-freelibros-org.pdf,” n.d.).

La red se complementa con 7 routers gigabit inalámbricos de banda dual N600, que soporta conexiones simultáneas de 2.4GHz 300Mbps y 5GHz 300Mbps para una banda ancha total disponible de 600Mbps, proporciona potentes capacidades de procesamiento de datos, posee 4 puertos LAN y 1 puerto MAN, todos a Gigabit (Figura 4). Estos puntos de acceso posibilitan el acceso inalámbrico del personal médico a los diagnósticos y otros servicios como chat, transmisión de videos en línea, que puede incluir hasta una cirugía. Con este estudio se pretende extender estos servicios a los clientes o pacientes previamente registrados en el sistema HIS-RIS para acceder a sus propios diagnósticos que hoy se hace grabándolos en CD-ROM con los inconvenientes que este procedimiento trae consigo.

Servicios que presta la red

Videoconferencia: Servicios de teleconsulta y teleeducación con los siguientes anchos de bandas mínimos para una buena calidad de video ante el ojo humano. (Nm y G, 2016)

Base de datos: Almacenaje y procesamiento de la información, que hacen que la información esté siempre actualizada y consistente. Los nuevos sistemas de gestión de bases de datos ya poseen servicios que permiten almacenar contenidos multimedia, objetos y datos complejos.

Web: Transferir información entre un cliente o navegador web y un servidor web.

Correo: En telemedicina fue una de las primeras fuentes en la era internet que permitió poder establecer contactos con colegas para segundos diagnósticos.

Calidad (fps)	Ancho de Banda mínimo
15 cuadro por segundo	128 kbps
30 cuadros por segundo	192 kbps
30-40 fps (calidad mejorada de imagen)	384kbps y 2mbps
Telecirugía (alta calidad de imagen)	8 y 16 Mbps

Tabla 1. Relación entre ancho de banda y calidad del video en telemedicina.

Líneas fijas de emergencia	Analógico	8KB	64
Consulta remota, telediagnóstico	Digital	8KB	126
Videoconferencias Consulta remota, telediagnóstico	**Video y audio** Analógico	800KB	**512** 534
Señales biomédicas Preadquiridas Electrocardiografía	**Datos** ECG	40MB	**256**
Acceso a base de datos médicas Información Médica	**Datos** Word PDF	 800KB 80KB	**64**
Transmisión de imágenes médicas 1. Radiografía 2. Tomografía 3. Resonancia magnética 4. Imagen digitalizada	**Imagen y datos** 1. Radio 2. TAC 3. MN 4. ECO 5. Digital	 1. 60MB 2. 9.6MB 3.15.36MB 4. 2.3 MB 5. 5.9 MB	**512**

Tabla 2. Información médica y ancho de banda recomendado (para uso en Telemedicina).

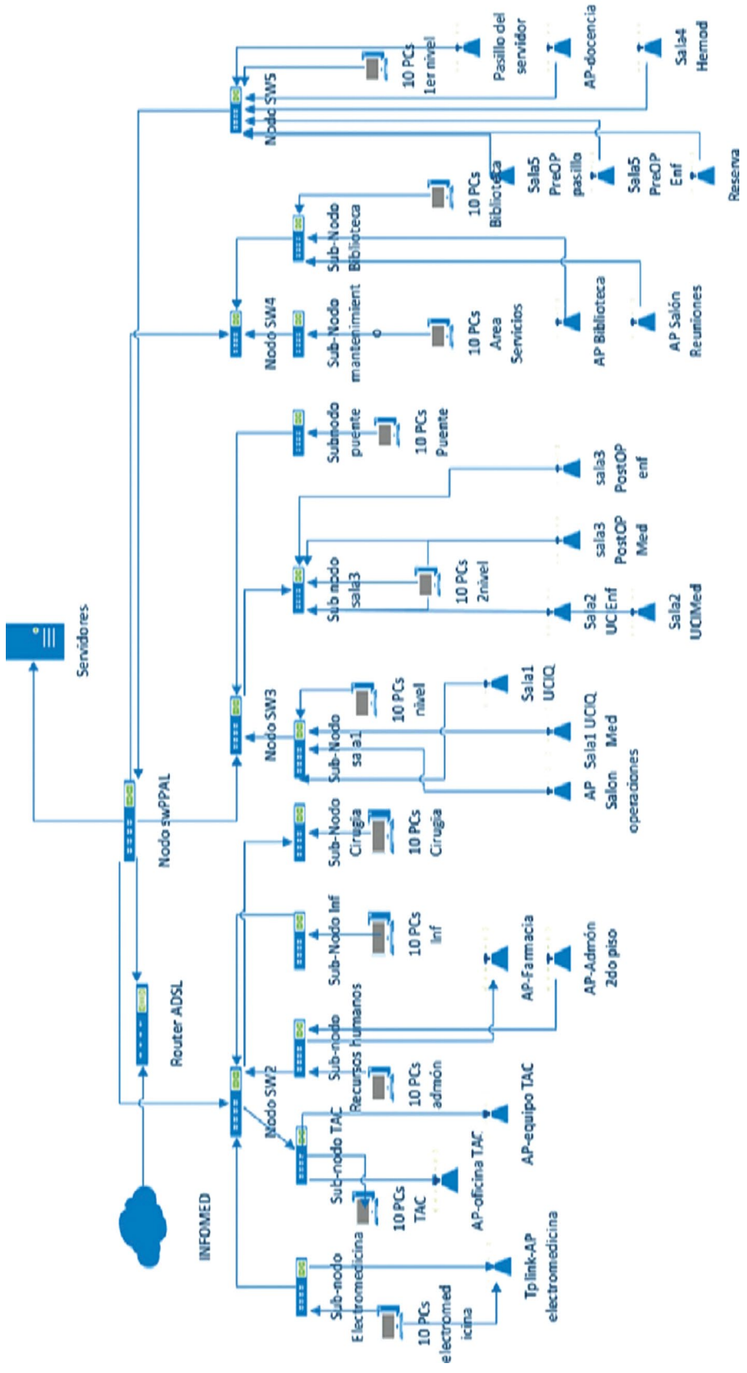


Figura 4. Red del Cardiocentro. Esquema topológico

Servicio de VoIP: Es un servicio que proporciona la comunicación de voz y sesiones multimedia (tales como video) sobre Protocolo de Internet (IP).

Resultados y discusión

Evaluación de la red

La propuesta de simulación se realiza con el software OPNET Modeler 14.5 ampliamente utilizado para diseñar, estudiar redes, dispositivos, protocolos y aplicaciones con un editor gráfico y que da la posibilidad de simular variables que miden el desempeño de la red usando modelos de red, de nodos y de procesos que utilizan el modo de simulación de eventos discretos (DES). En la figura 5 se muestra el escenario de la red del Cardiocentro que ya tiene aplicadas las mejoras que son necesarias introducir para garantizar los servicios antes descritos y que incluye la disminución de las cascadas, enlaces principales a gbps y con fibra óptica para llegar a los lugares donde, por problemas de distancia, el cableado UTP no cumple los requisitos técnicos lo que implica la sustitución de los switches. Se configuran las aplicaciones, los perfiles según los servicios que se necesitan monitorear (videoconferencia, http, base de datos, email, VoIP), se adicionan 7 nodos WLAN según la norma IEEE 802.11g, los nodos y servidores. Se configuran las estadísticas a medir y los parámetros de la simulación.

Se evalúan varios parámetros, entre ellos se tienen:

1. Promedio de tráfico global enviado y recibido desde el servidor web (Figura 6). Es el número total de paquetes por segundo enviados o recibidos por las aplicaciones HTTP en la red (Figura 7).

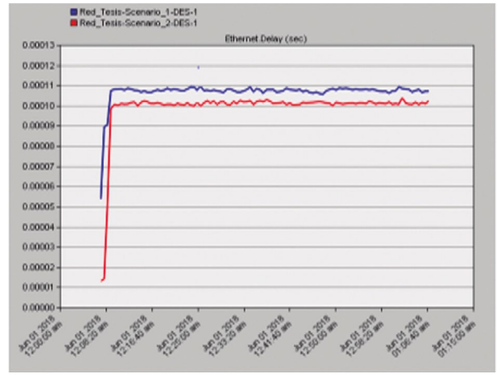


Figura 6. Retardo de la red

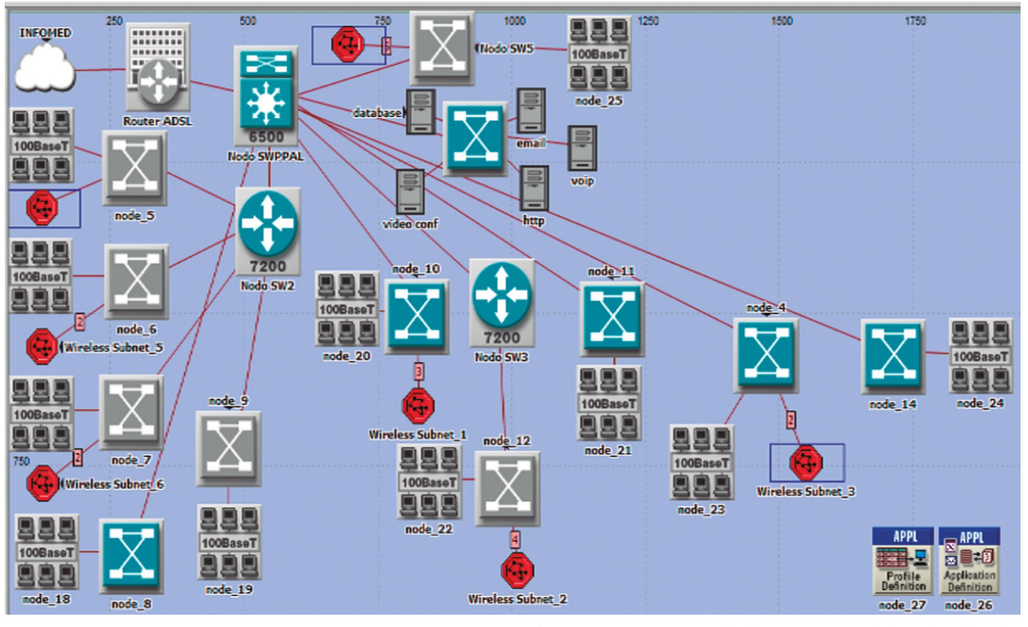


Figura 5. Esquema topológico en OPNET de la red mejorada

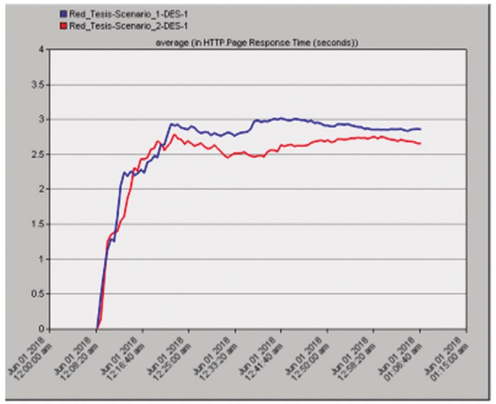


Figura 7. Tiempo de respuesta del servidor web

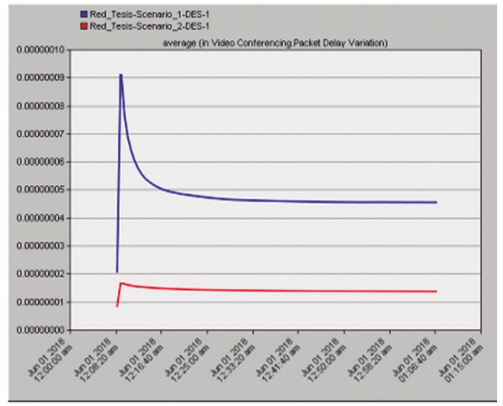


Figura 9. Variacion del retardo para el servicio de videoconferencia

2. Tiempo promedio de respuesta a la consulta de la base de datos. Es el tiempo que transcurre desde que el paquete fue enviado hasta que es recibida la respuesta (Figura 8).

3. Variación del retardo en videoconferencia (Figura 9), que es el tiempo de llegada de los paquetes de audio y video.

4. Retardo de paquetes punto a punto en el servicio de videoconferencias que es el tiempo en que reconstituye la transmisión de voz y video en el receptor (Figura 10).

5. El tráfico enviado y recibido para la VoIP en ambos escenarios se muestra en la Figura 11.

6. Con la adición a la red inalámbrica de 7 nodos se muestra el retardo total con respecto a los 10 que ya existían y se observa que el retardo es menor que para la red propuesta debido a las mejoras que se introduci-

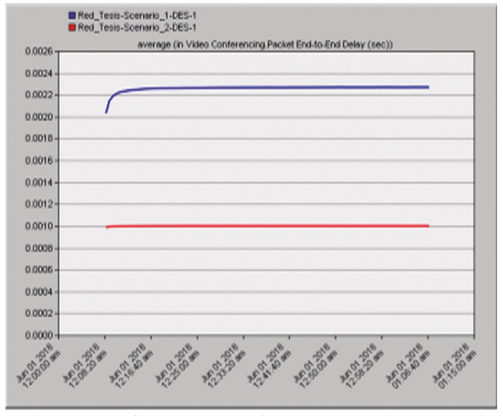


Figura 10. Retardo extremo a extremo para la videoconferencia

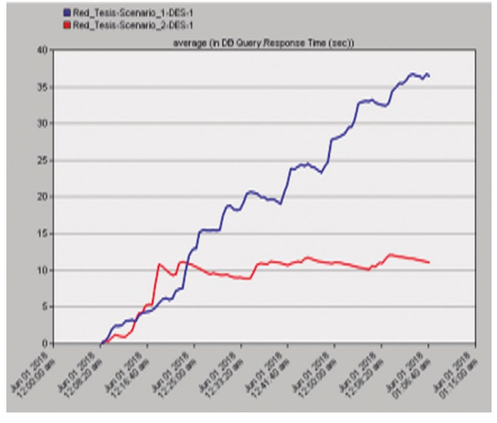


Figura 8. Tiempo de respuesta de la consulta a la base de datos

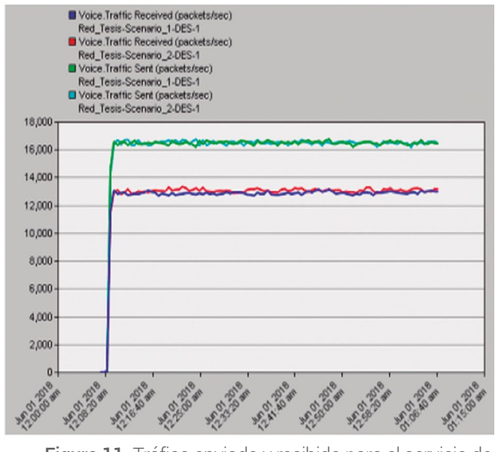


Figura 11. Tráfico enviado y recibido para el servicio de VoIP

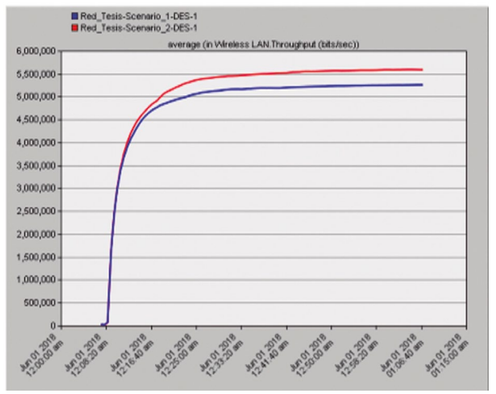


Figura 12. Throughput de la red inalámbrica

das a la red y también aumenta el número de paquetes enviados y recibidos (*throughput*) (Figura 12). esto mejora la razón de transmisión a pesar del aumento del número de usuarios a la red Wlan y como consecuencia la carga en la red.

Evaluación del sistema Xavia-PACs

Para evaluar el desempeño del sistema Xavia-PACs se tiene en cuenta que en el tiempo que se ha utilizado esta aplicación se ha comprobado que es una aplicación estable y que se encuentra disponible para los especialistas las 24 horas, siendo la seguridad una de sus principales características.

No obstante, se ha detectado que presenta algunas deficiencias con las consultas a la base de datos, debido al gran cúmulo de registros de imágenes, haciendo las búsquedas más demoradas, el servidor solo puede configurarse para almacenar imágenes en una partición, dejándole la responsabilidad al administrador del sistema de cambiar manualmente la configuración hacia una nueva partición de almacenamiento; además, el trabajo de los administradores del sistema se hace muy engorroso debido a que para hacer algún cambio en la configuración del mismo, es necesario ir hasta el nodo donde se encuentra instalado.

A continuación, se muestra la tabla 3 con los resultados de pruebas preliminares comparando al Xavia-PACs-Server 3.0 y al Xavia-PACs-Server 2.9.3. Estas operaciones de almacenamiento, búsqueda y obtención de estudios de diferentes modalidades en una base de datos con 10 546 203 referencias de imágenes fueron realizadas desde 4 estaciones de trabajo, simulando equipos médicos de adquisición de imágenes y estaciones de visualización.

Conclusiones

Luego de los resultados obtenidos en el proceso de evaluación de la red y teniendo en cuenta que la telemedicina se ha convertido en una de las prioridades para el desarrollo de la medicina actual, unido al desarrollo de los equipos de diagnóstico y la posibilidad que ellos brindan al personal médico especializado para brindar imágenes médicas de diagnóstico que son captadas y almacenadas por los sistemas PACs y su integración con los sistemas HIS-RIS, se logra un sistema de transmisión completo de la imagen médica usando a DICOM como estándar internacional.

La propuesta de red mejorada al Cardiocentro mejora la mayoría de los parámetros simulados a pesar del

Modalidad del estudio	**CT**		**Modalidad del estudio**	**MR**	
Cantidad de imágenes	Tamaño total (MB)		Cantidad de imágenes	Tamaño total (MB)	
415	216		72	35.8	
Operación	Xavia PACSServer 3.0	Xavia PACSServer 2.93	Operación	Xavia PACSServer 3.0	Xavia PACSServer 2.93
Almacenamiento	89	186	Almacenamiento	17	81

Tabla 3. Pruebas preliminares.

aumento de la carga en la red que presupone el acceso inalámbrico y el aumento de los servicios.

El software XAVIA PACs WEB para clientes es de fácil entendimiento para los médicos que lo usan, ya que cuenta con una interfaz visual en sus 3 módulos muy interactiva.

Asimismo, en este sentido a partir de las mejoras que se proponen a la red se recomienda establecer de manera adicional redundancia de los enlaces principales a los equipos de diagnóstico y a los switches centrales de la red para que en caso de fallos la red continúe operativa. Extender la red de transmisión de imágenes entre otras dependencias hospitalarias de la provincia para tener la posibilidad de segundos diagnósticos y extender los servicios de copia de diagnósticos a los pacientes a través de la red Wifi.

Referencias

A. Trujillo Zea, C. R. I. (2007). Redalyc.TELEMEDICINA: Introducción, aplicación y principios de desarrollo - 261120984009.pdf. 21n.o 1, 78.

Álvarez, L. R., y Vargas Solís, R. (2013). DICOM RIS/PACS Telemedicine Network Implementation using Free Open Source Software. IEEE LATIN AMERICA TRANSACTIONS, 11(1), 168–171.

HONGJI YANG, Z. L. (n.d.). Unlocking the Power of OPNET Modeler. Retrieved from http://solutionsproj.net/software/opnet_unlock_pdf.pdf

K. Delac, M. M. (n.d.). Overview of the DICOM Standard.pdf. 1, 39–44. Retrieved from http://vcl.fer.hr/papers_pdf/Overview%20of%20the%20DICOM%20Standard.pdf

Miguel Chavarría Día, F. B. i R. (n.d.). Almacenamiento y Transmision de Imagenes PACs. Retrieved November 19, 2019, from http://www.conganat.org/SEIS/is/is45/IS45_54.pdf

Nm, N., y G, V. (2016). La discusión de casos por videoconferencia mejora la eficiencia de la consulta externa de cirugía torácica. Archivos de Bronconeumología, 52(11), 549–552. https://doi.org/10.1016/j.arbres.2016.04.002

Redes de Computadoras, 5ta Edición - redes_de_computadoras-freelibros-org.pdf. (n.d.). Retrieved November 19, 2019, from https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf

Smith, J. J., y Berlin, L. (2012). Picture Archiving and Communication Systems (PACS) and the Loss of Patient Examination Records. American Journal of Roentgenology, 176(6), 1381–1384. https://doi.org/10.2214/ajr.176.6.1761381

Whetherall, T. (n.d.). Computer Networking: A Top-Down Approach. Retrieved from /content/one-dot-com/one-dot-com/us/en/higher-education/product.html

Funciones de redes virtualizadas en red trunking digital eLTE

Virtual network functions in eLTE digital trunking network

Ing. Fidel Alejandro Fernández Carcasés [1*], Ing. Raquel Leal Mieres[2], MSc. Alejandro Ruiz Douglas[3]

Recibido: 02/2019 | Aceptado: 03/2019

Palabras clave

Redes virtualizadas
eLTE
Comunicaciones móviles

Resumen

La empresa cubana Movitel en el proceso de migración hacia los sistemas digitales de radio troncalizado se propone como objetivo principal brindar servicios de banda ancha con el despliegue de una red de cuarta generación, para alcanzarlo será necesario la implementación de nuevas herramientas y el desarrollo de aplicaciones que complementen las funcionalidades del sistema. Este trabajo abordará algunas de las soluciones para la transmisión de datos en banda ancha que Movitel ha implementado sobre la red eLTE —*enterprise Long Term Evolution*— de Huawei en su proceso de despliegue a nivel nacional, aprovechando los conceptos de las funciones de redes virtualizadas y redes definidas por software. La estructura de la investigación se compone por el análisis de la tecnología eLTE como sistema de comunicaciones móviles, el análisis de las arquitecturas de los sistemas NFV —*Virtualización de Funciones en Red*—, las pruebas experimentales realizadas con los equipos terminales para el acceso y las funcionalidades del sistema donde se aplicaron los conceptos de virtualización de funciones de redes. En conclusión, se presenta el esquema final de la solución de conectividad desarrollada mediante la implementación de los sistemas virtuales y las posibilidades de modelos de servicios en comparación con tecnologías emergentes para la transmisión de datos de banda ancha móvil.

Keywords

Virtualized networks
eLTE
Mobile communications.

Abstract

Movitel, in the process of migration to digital trunked radio systems, aims to provide broadband services with the deployment of a fourth generation network, to achieve this it will be necessary to implement new tools and develop applications that complement the functionalities of the system. This paper will address some of the solutions for broadband data transmission that Movitel has implemented on the Huawei eLTE network through the nationwide deployment process, taking advantage of the concepts of virtualized networks and software-defined networks. The research structure is the analysis of eLTE technology as a mobile communications system, the analysis of the architectures of the NFV systems, the experimental tests carried out with the terminal equipment for access and the functionalities of the system where

[1*] Movitel, Cuba. fidel@movitel.co.cu
[2] Movitel, Cuba. raquel@movitel.co.cu
[3] Movitel, Cuba. douglas@movitel.co.cu

the virtualization concepts of network functions were applied. Finally, the final scheme of the connectivity solution developed through the implementation of virtual systems and the possibilities of service models in comparison to emerging technologies for mobile broadband data transmission is presented.

Introducción

La empresa cubana MoviTel es un operador que brinda servicios de radio troncalizado y se encuentra en el proceso de despliegue de un sistema de banda ancha digital de cuarta generación eLTE —*enterprise Long Term Evolution*—, para brindar soluciones a las empresas del país. La tecnología digital 4G eLTE del proveedor chino Huawei está basada en el estándar LTE, diseñada para alcanzar picos de velocidades máximas de 100Mbit/s en el enlace descendente y 50Mbit/s en el enlace ascendente en óptimas condiciones para brindar acceso a comunicaciones móviles de banda ancha (Agusti, Bernardo, Casadevall, Ferrús, Pérez-Romero, y Sallent, 2010). eLTE es una solución troncal de banda ancha empresarial diseñada para proporcionar comunicación a sistemas críticos en un amplio rango de escenarios, como aeropuertos, redes eléctricas, minería, puertos, extracción de petróleo y gas. La plataforma del sistema brinda servicios de voz de alta calidad, mensajería instantánea, trasmisión de video de alta definición en tiempo real, geolocalización y comunicaciones de emergencia.

Los principales objetivos de la evolución de las redes móviles actuales son responder a los desafíos futuros y establecer el camino hacia las redes 5G con necesidad de alta capacidad y baja latencia. En este sentido se están considerando diferentes tecnologías, como la virtualización de funciones de red (NFV) y la red definida por software (SDN) para abordar las grandes demandas de acceso a datos. Los medios para una operación eficiente de los recursos de red podrían llegar a ser incluso más importantes que los costos futuros del elemento de red (Gokani, 2018).

La cantidad cada vez mayor de dispositivos que acceden a la red está en correspondencia con el incremento de aplicaciones y servicios que requieren nuevas formas de diseñar, administrar y operar las redes, por lo que las tecnologías SDN y NFV son testigos de la demanda de su aplicación. Sus funcionalidades se utilizan para modificar el servicio y la arquitectura de la red. SDN permite controlar los dispositivos de red sin actualizar el software cada vez que se implementa un nuevo protocolo, mientras que NFV mejora las capacidades de red haciéndola más flexible y escalable (Costa-Requera y otros, 2015).

Aplicar estos conceptos actuales sobre la infraestructura existente puede aportar soluciones a las demandas insatisfechas y marcar las pautas de la evolución de las redes de manera flexible, escalable y funcional. Esto podría disminuir los altos costos de inversión que puede suponer un cambio de equipamiento, así como las molestas pérdidas de servicio que se introducen durante un proceso de actualización o interrupción de la infraestructura; como son cambios de equipamiento o fallas de software en los elementos de red.

Materiales y métodos

Para el desarrollo de la investigación se emplearon métodos inductivos, que utiliza la observación directa de los fenómenos, la experimentación y el estudio de las relaciones que existen entre ellos. Se estudiaron las características fundamentales y los principios de funcionamiento que corresponden a las tecnologías de la red Trunking Digital eLTE y las Arquitectura NFV. Se realizó un estudio de las funciones de redes del sistema eLTE que se necesitaban para lograr la solución de conectividad y que no se podían implementar. Finalmente se estudiaron las posibilidades de incorporar estas funciones de redes al sistema actual mediante el uso las tecnologías de virtualización como SDN y NFV.

Para las pruebas y experimentos durante la investigación se utilizaron como materiales de desarrollo, los terminales de datos de la infraestructura eLTE (EG860 CPE —*Customer Permise Equipment*—), terminales portátiles y un servidor de propósito general RH2288 con altas capacidades de procesamiento que permite el despliegue del soporte para los sistemas de virtualización.

La estructura de la investigación se compone por el análisis de las tecnologías mencionadas, las pruebas experimentales realizadas con los distintos protocolos de redes, túneles GRE —*Generic Routing Encapsulation*—, BGP —*Border Gateway Protocol*—, VRF —*Virtual Routing and Forwarding*—, el esquema final de la solución de conectividad desarrollada mediante la implementación de los sistemas virtuales y las posibilidades de modelos de servicios en comparación a tecnologías emergentes para la transmisión de datos de banda ancha móvil.

Trunking Digital eLTE 4G y Arquitecturas NFV

eLTE de Huawei de manera simplificada es una infraestructura de comunicaciones móviles de cuarta generación que cuenta con un conjunto de servidores de propósitos general en el que se despliegan las aplicaciones que brindan los servicios básicos del sistema. Por otra parte, cuenta con un núcleo de red o CoreNetwork en inglés (eCNS210) que es el encargado de garantizar la conmutación y la transmisión de los paquetes de datos hacia las radiobases (eNodeB) las que deben establecer las comunicaciones directas con los terminales y brindar amplias aéreas de cobertura para el acceso de los usuarios (Figura 1).

La red troncalizada eLTE de Huawei en sus primeras versiones de software está diseñada para proveer un grupo de funcionalidades donde cada empresa o industria garantiza los servicios básicos que brinda la solución de manera centralizada, sin embargo, la infraestructura se puede convertir en una red de transporte para múltiples empresas aprovechando la capacidad de conmutación de paquetes que ofrece el Core de la red (eCNS).

Entre los terminales disponibles que comercializa el fabricante para la transmisión de datos se encuentra el EG860 CPE, este es un terminal de acceso inalámbrico de banda ancha que sirve como dispositivo de conectividad en una red privada de datos. Se puede instalar en interiores o exteriores. Soporta varios mecanismos de enrutamiento para facilitar el acceso a redes privadas como son Routing Behind MS (la tarea del enrutamiento se realiza en el Core de la red), NAT —*Network Address Translation*— en combinación de Port Forwarding, y el empleo de otros protocolos como GRE y Layer 2 Tunneling Protocol (L2TP) usando tablas de rutas estáticas para enrutar VPNs —*Virtual Private Network*— (Huawei, 2017).

eLTE, permite crear APNs —Access Point Name— por cliente donde cada uno podría tener su propio rango de direcciones IP para sus terminales. En la versión actual del sistema estos rangos no pueden

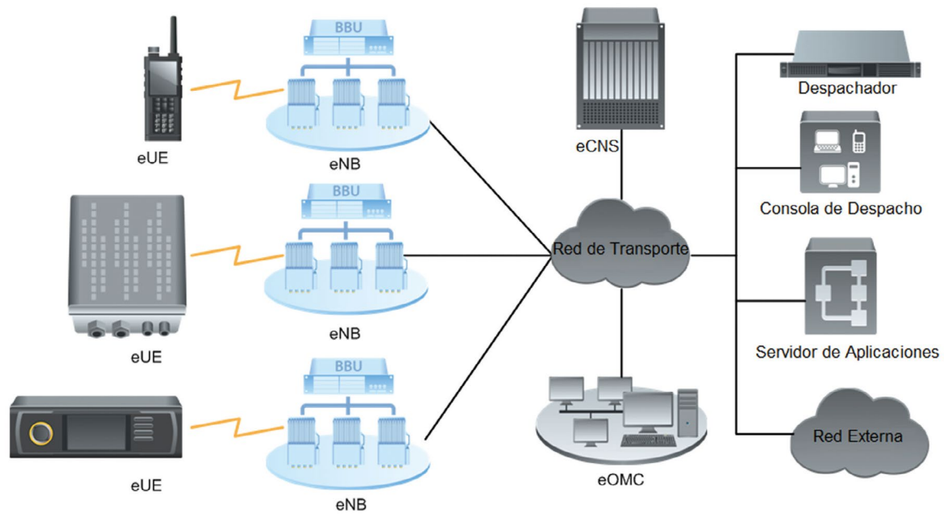


Figura 1. Esquema simplificado de eLTE

solaparse sin provocar la pérdida de servicio del sistema troncalizado, representando una limitante para el enrutamiento de paquetes y en la escalabilidad del sistema. La introducción de los conceptos de NFV y SDN podrían abrir las puertas para lograr cubrir en alguna medida las limitantes de la red actual, haciéndola más flexible escalable y eficiente, sin incurrir en gastos económicos por conceptos de inversión en equipamiento de uso específico o servicios de actualización de software de los mismos.

La virtualización llega también a las telecomunicaciones; ya no solo se virtualizan los sistemas sino también las redes. Con el fin de obtener redes más escalables y flexibles, que permitan una mayor innovación en los servicios ofrecidos, aparecen las tecnologías NFV —*Network Function Virtualization*— y SDN —*Software Defined Network*—. Con ellas se consigue desplazar la funcionalidad de red al software, utilizar servidores de propósito general en lugar de dispositivos específicos, APIs para su desarrollo y organizar y automatizar los servicios de red eficientemente (Santana, 2018).

Las arquitecturas de NFV más comunes de manera resumida están separadas por varias capas donde se encuentra generalmente un hardware de propósito general y altas prestaciones, sobre el cual se despliega algún Hipervisor como plataforma de virtualización, en este, se instalan las máquinas virtuales que son conocidas como funciones de red virtualizadas o VNFs y finalmente una capa superior que incluye operación, interfaz de usuario, sistema de gestión y control, en una plataforma integral, que administra dinámicamente todos los recursos, conocido como el Orquestador. En la literatura actual respecto al tema se encuentran muchos esquemas de las capas de un sistema NFV, y además se detallan cada una de las funciones de los elementos que lo componen. (Figura. 2) (McCann y Shaw, 2016).

El despliegue, asimilación y puesta en marcha de un sistema NFV y SDN completo puede llegar a ser bastante complejo, así como alcanzar a sustituir las funciones de red y lograr la separación entre el software y hardware específico.

Solución de conectividad implementada

Aplicando estos conceptos se desplegó el Hypervisor Esxi 6.5 de VMWare sobre un servidor RH2288 de Huawei de altas prestaciones con interfaces de 10Gb/s. Entre las funciones de red que se necesitaban virtualizar se encontraba implementar enrutamiento con protocolos MP-BGP, túneles GRE, túneles L2TP, IPsec, Vlans y posibilidad de trabajar con VRFs y VPN4 (VPNs de nivel 4). Se

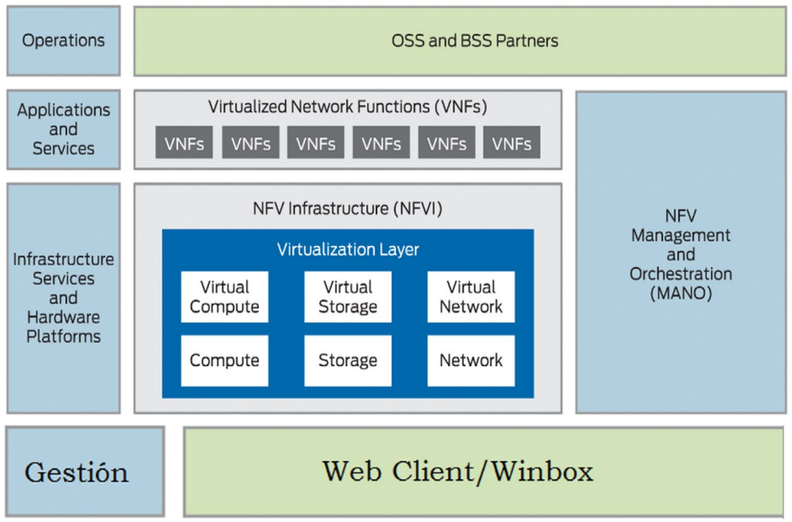


Figura 2. Esquema referente de la arquitectura en sistemas NFV

instaló un Router virtual que agrupaba todas estas funcionalidades de redes. RouterOS es el sistema operativo de los RouterBoard, el cual, puede ser instalado en una PC para convertirla en un enrutador con todas las funciones necesarias como son: enrutamiento, firewall, administración de ancho de banda, punto de acceso inalámbrico, enlace de backhaul, puerta de enlace de punto de acceso, servidor VPN y más (Mikrotik, 2019).

Se decidió separar algunas de las funciones de los protocolos de red necesarios en dos Routers Virtuales, para lograr una mayor eficiencia en la ejecución de los procesos y el manejo de las tablas de rutas, además de crear un punto de respaldo ante fallas de cualquiera de los dos sistemas. Finalmente, la gestión no se realiza de manera centralizada y no existe un "orquestador", por el momento, que maneje los recursos y aplique configuraciones de redes dinámicamente. Por tanto, se realiza la gestión del Hipervisor Esxi usando el servicio Web Cliente y la herramienta Winbox para la gestión de los routers virtuales (Figura 3).

Con las principales funciones de redes virtualizadas, se decidió utilizar el terminal de acceso a datos EG860(CPE) para las soluciones de conectividad. Entre los mecanismos de enrutamiento que soporta este terminal se seleccionó la variante del túnel GRE por permitir una mayor flexibilidad en el manejo de las rutas y ser más adecuado para dar servicio a distintos clientes. Sin embargo, cada CPE solo permite manejar dos túneles GRE presentando una limitación en cuanto a soluciones punto-multipunto y no cuenta con protocolos para el monitoreo del tráfico de datos, como SNMP —*Simple Network Management Protocol*—.

En la solución integral se concibió la utilización de dos routers virtuales que lograrán cumplir dos funciones fundamentales respectivamente: establecer una conexión punto a punto con el proveedor de las VPNs empresariales en la que se utilizarían los protocolos VRFs y BGP para colectar las tablas de rutas de los clientes y funcionar como punto concentrador de los túneles GRE asociados a VRFs, eliminando las limitaciones existentes de escalabilidad punto-multipunto. Además, ofrece la posibilidad de mostrar una estadística referente al tráfico de datos en el uso de los enlaces.

En detalles, el acceso de las VPNs empresariales de los clientes se realiza mediante una instancia BGP proveniente del Backbone IP-MPLS —*Multiprotocol Label Switching*— por la cual se difunden las tablas de rutas de cada empresa y se agrupan por VRFs en el Router Virtual 2.

El Router Virtual 1 concentra el acceso a los CPE de cada entidad mediante el encapsulamiento con túneles GRE y los asocia con su VRF correspondiente, que comparten información de enrutamiento dinámico entre los dos Routers haciendo uso de una instancia BGP, de esta forma la solución es capaz de brindar interconexión entre los puntos de conectividad eLTE

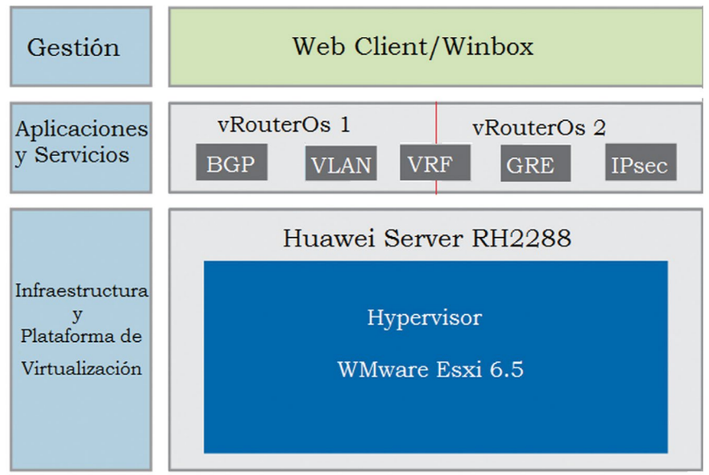


Figura 3. Esquema en capas de la solución de NFV

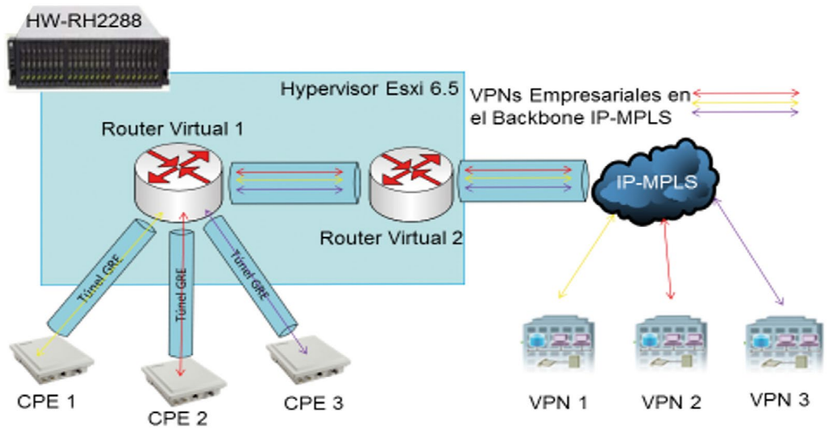


Figura 4. Arquitectura de la solución de conectividad

(CPEs) de los clientes y los que ya están conectados al Backbone IP MPLS del proveedor de servicios de su entidad (Figura 4).

Las funciones de red virtualizadas nos permiten incorporar funcionalidades para aumentar la seguridad de los enlaces, como el uso del protocolo IPsec para el cifrado de los túneles GRE, que es compatible con el terminal de datos EG860 de forma que se puede explotar al máximo las capacidades del sistema. Por otra parte, el EG860 como terminal de datos tiene limitaciones en las capacidades de enrutamiento y en la versión actual de su sistema no permite hacer uso de configuraciones de protocolos dinámicos para el aprendizaje de las rutas. Esto provoca que el operador tenga que agregar las tablas de rutas manualmente para garantizar la conectividad. El uso de otros protocolos para las VPNs, como la implementación de los túneles L2TP que puede ser una solución atractiva en algunos escenarios para mejorar la transparencia, pudiera verse afectado por el solapamiento de los rangos de direcciones IP de las empresas y el crecimiento de los puntos a conectar.

Existe una gama completa de soluciones de conectividad que se brindan como servicios por parte de algunos proveedores de infraestructuras de comunicaciones, dentro de estos servicios encontramos el Fixed Wireless Access (FWA), Acceso Inalámbrico Fijo, por su traducción al español. Este abre un mundo de oportunidades debido al gran número de sitios desatendidos en cuanto a conectividad, lo cual representa una oportunidad de crecimiento rentable de FWA para los operadores 3GPP —The 3rd Generation Partnership Project— actuales. FWA es una alternativa más rentable y eficiente para proporcionar banda ancha en áreas con acceso limitado a servicios de banda ancha fija como DSL —Digital Subscriber Line—, cable o fibra. La solución de conectividad desarrollada sigue un esquema similar al servicio FWA y puede tomarse como ejemplo de las aplicaciones que se pueden desarrollar para explotar la infraestructura al máximo brindando servicios de conectividad a distintos sectores empresariales.

Conclusiones

Aplicar soluciones de NFV y SDN en la red de MoviTel permitió optimizar el empleo de los recursos de cómputo de los que se disponía e incrementar la variedad de servicios a los clientes. Los trabajos realizados permitieron convertir la red de banda ancha eLTE desplegada en Cuba, en una red de transporte que garantiza servicios a múltiples empresas. El empleo de varios Routers Virtuales separando funcionalidades, posibilitó a MoviTel ofrecer mayor calidad en los servicios y una mejor gestión de los mismos. Durante el estudio de las soluciones implementadas se identificó un grupo de limitaciones que tiene el sistema y sus posibles soluciones. A finales de 2019, más de 50 empresas en Cuba hacen uso de estas soluciones. Por el impacto que han tenido las mismas en dar respuesta a solicitudes en lugares hasta el momento inaccesibles a las variantes ofrecidas por otros proveedores de conectividad, se considera que estas, han hecho un aporte en la Informatización de la Sociedad Cubana. El estudio e implementación de estas soluciones crea un precedente en la empresa para la asimilación de nuevas tecnologías.

Referencias

Agusti, R., Bernardo, F., Casadevall, F., Ferrús, R., Pérez-Romero, J., y Sallent, O. (2010). LTE: Nuevas Tendencias en Comunicaciones Móviles. España.

Costa-Requena, J.; Llorente, J.; Ferrer, V.; Ahokas, K.; Premsankar, G.; Luukkainen, S.; López, O.; Uriarte, M.; Ahmad, I.; Liyanage, M.; Ylianttila, M.; Montes de Oca, E. (2015). SDN and NFV integration in generalized mobile network architecture, *European Conference on Networks and Communications (EuCNC)*.Francia.

Gokani, N. (2018). *Software Defined Networking (SDN) and Network Function Virtualization (NFV) Market Landscape Assessment by Type, Opportunities and Higher Mortality Rates by 2027.* Obtenido de https://exclusivereportage.com: https://exclusivereportage.com/2018/11/21/software-defined-n

Huawei. (2017). *Huawei DBS3900 Product Documentation eLTE V100R003C00.* Obtenido de Huawei Enterprise: http://support.huawei.com/enterprise/portal/en/eLTE_Information_Service_Portal_en.html

McCann, S., y Shaw, H. (2016). *Learn About Network Functions Virtualization.* Obtenido de Juniper Networks: https://www.juniper.net/documentation/en_US/learn-about/LearnAbout_NFV.pdf

MikroTik. (2018). *Manual: Virtual Routing and Forwarding.* Obtenido de MikroTik Documentation: https://wiki.mikrotik.com/wiki/Manual:Virtual_Routing_and_Forwarding

Santana, C. (2018). *NFV y SDN: las redes del futuro y del presente*. Obtenido de t3chfest: https://t3chfest.uc3m.es/2018/programa/nfv-sdn-las-redes-del-futuro-del-presente/?lang=es

Plataformas para aplicaciones IoT basadas en Tecnologías Open Source

Platforms for IoT applications based on Open Source technology

Ing. Rainer Lester Ruiz Delgado[1]

Recibido: 07/2019 | Aceptado: 10/2019

Palabras clave

IoT
Arduino
Raspberry Pi
GSM
Monitoreo
Control Remoto
Programación Android

Resumen

En este artículo se realiza un análisis sobre la necesidad de implementar plataformas con tecnología Open Source como Arduino y Raspberry Pi para soluciones de IoT y se brinda una información teórica sobre estas. Se hace una breve exposición de las capacidades de cada plataforma, así como algunas aplicaciones que demuestran que fortalezas y debilidades tiene cada una.

Keywords

IoT
Arduino
Raspberry Pi
GSM
Monitoring
Remote Control
Android Programming

Abstract

This research analyzes the need to implement platforms with Open Source technology such as Arduino and Raspberry Pi for IoT solutions, and provides theoretical information about them. It is made a brief exposition of the capacities of each platform, as well as some applications that demonstrate which strengths and weaknesses each of them has.

Introduccion

Cuba actualmente vive un momento de transición hacia la digitalización de la sociedad en el cual ETECSA, como operador de telecomunicaciones, desempeña un rol muy importante. Este escenario permite a ETECSA identificar, innovar, expandir y crear nuevas oportunidades y modelos de negocio, incursionando por ejemplo en los ecosistemas de plataformas orientadas a la Internet de las Cosas (IoT) lo cual podrían ser en un futuro la base de las creaciones con valor añadido, y un motor para el desarrollo de aplicaciones innovadoras IoT para sus usuarios finales.

En este estudio se hace una breve exposición de las capacidades de las tecnologías de Open Source como Arduino y Raspberry Pi, así como algunas aplicaciones que demuestran las fortalezas y debilidades que tienen cada una. Se hace énfasis en la importancia de usar estas dos plataformas para desarrollar proyectos orientados a la IoT y como herramienta educativa en las universidades, como la Universidad Tecnológica de La Habana José Antonio Echeverría.

[1] Empresa de Telecomunicaciones de Cuba S.A. Vicepresidencia de Estrategia de Negocios y Tecnologías, La Habana, Cuba. rainer.lester@etecsa.cu

Materiales y métodos

Este trabajo se basó en el Método Descriptivo de la Investigación Cualitativa, para la reseña de plataformas con tecnología Open Source como Arduino y Raspberry Pi para soluciones de IoT. Para ello fueron consultados fundamentalmente sitios web oficiales de los propios proveedores, artículos científicos y tesis, con el ánimo de exponer la necesidad de implementar este tipo de soluciones en Cuba.

Internet de las Cosas (IoT)

Internet de las cosas (IoT) es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet. Es ampliamente usada en la ingeniería como en el monitoreo ambiental, ciudades inteligentes, y también en todas las industrias como la automovilística, agrícola, salud, domótica, gestión de alarmas entre otras, permitiendo monitorizar y controlar casi cualquier actividad, facilitando la toma de decisiones y aumentando la eficiencia en los procesos. En la logística se implementan estos sistemas para la gestión de almacenes y órdenes de distribución las cuales pueden ser accesibles desde los smartphones por medio de aplicaciones (Evans, 2011).

El desarrollo de IoT está compuesto por dispositivos enlazados a través de redes fijas e inalámbricas. Pueden ser cosas cotidianas como cámaras, sensores y demás, a los que se les puede asignar una dirección IP la cual permite acceder a ellos remotamente y recoger fácilmente los datos obtenidos para ser almacenados en una plataforma desde la cual se toman y se ejecutan decisiones (Evans, 2011).

Para facilitar el control del IoT se hace necesario diseñar y construir la interfaz del usuario en la cual se muestra de forma sencilla informes de la actividad que se monitorea y finalmente se potencia la plataforma integrando el internet con otros sistemas de información. En la figura 1 se observa la interacción del usuario con un panel de control, el cual permite gestionar diferentes dispositivos y recibir el estado de estos directamente de la nube.

Actualmente existen diversas tecnologías de bajo costo como las placas de Arduino y Raspberry PI que nos puedeN ayudar a la hora de implantar sistemas domóticos y automáticos usados en proyectos de IoT en los que confluyen sensores de diferente naturaleza con el objetivo de utilizar la comunicación de los dispositivos para informar sobre actividades que suceden a distancia, en la que se manda una señal de alarma al usuario, aunque se encuentre a kilómetros de su casa como podría ser la vigilancia remota de una casa inteligente conectada a internet.

Arduino

Arduino es una plataforma electrónica de código abierto —*open-source*— basada en software y hardware

Figura 1. El Internet de las cosas

muy fáciles de usar. Está pensado para diseñadores y desarrolladores, lo mismo en ámbitos educacionales o como hobby y para cualquier interesado en crear entornos interactivos. Los proyectos que se realizan pueden ser autónomos o se pueden comunicar con software en un ordenador. Arduino puede gestionar el entorno mediante la recepción de señales de entradas desde una variedad de sensores y puede afectar a su entorno mediante el control de luces, y a motores través del uso de actuadores (Arduino a, s.f.).

Arduino permite a un usuario con unos conocimientos básicos en programación programar el microcontrolador integrado en la plataforma y así realizar una multitud de proyectos que van desde encender un led hasta introducirse en el mundo de la robótica o incluso realizar proyectos más avanzados basados en comunicaciones inalámbricas o Ethernet incluyendo proyectos de IoT (Arduino a, s.f.).

Las placas Arduino están compuestas por un microcontrolador como eje central y una serie de componentes más encargados de apoyar y extender la funcionalidad de este. El microcontrolador de la placa se programa usando el —Arduino Programming Language— (basado en Wiring) y el —Arduino Development Environment— (basado en Processing). El entorno de desarrollo se puede descargar gratuitamente desde su sitio web. La programación de las placas es una tarea sencilla que solo requiere la conexión de la placa a uno de los puertos USB de la computadora y la carga del programa dentro del micro mediante la propia plataforma de desarrollo. Las placas pueden ser programadas infinidad de veces (Arduino a, s.f.).

En la figura 2 se puede ver una imagen de la plataforma Arduino y una ventana con un programa listo para ser compilado y ejecutado en el microcontrolador.

A través de Arduino se puede recopilar multitud de información del entorno sin excesiva complejidad. Gracias a sus pines de entrada, permite jugar con toda una gama de sensores (temperatura, luminosidad, presión, etc.). Estos módulos brindan la capacidad de controlar o actuar sobre ciertos factores del entorno que le rodean, como, por ejemplo: controlando luces, accionando motores, activando alarmas y muchos otros actuadores (Arduino a, s.f.).

Desde el momento de su creación, no han dejado de sucederse las innovaciones. Actualmente, existe una multitud de placas Arduino, y la mayoría de ellas están disponibles en distintas versiones, adaptables prácticamente a cualquier tipo de requisitos o necesidades para llevar a cabo un determinado proyecto. Algunos de los principales modelos de placas Arduino que se pueden encontrar en el mercado podrían ser los mostrados en la Tabla 1 donde se puede ver una comparación de los mismos (Arduino b, s.f.).

Como vemos Arduino nos proporciona todas las herramientas necesarias para programar el microcontrolador, para empezar a realizar nuestros proyectos. Además tiene dos grandes ventajas, la primera es que existe una comunidad muy numerosa que da soporte a esta plataforma, y la segunda que existen módulos de ampliación shields que permiten incorporar a la placa utilidades adicionales (comunicación WIFI, control de motores, etc.).

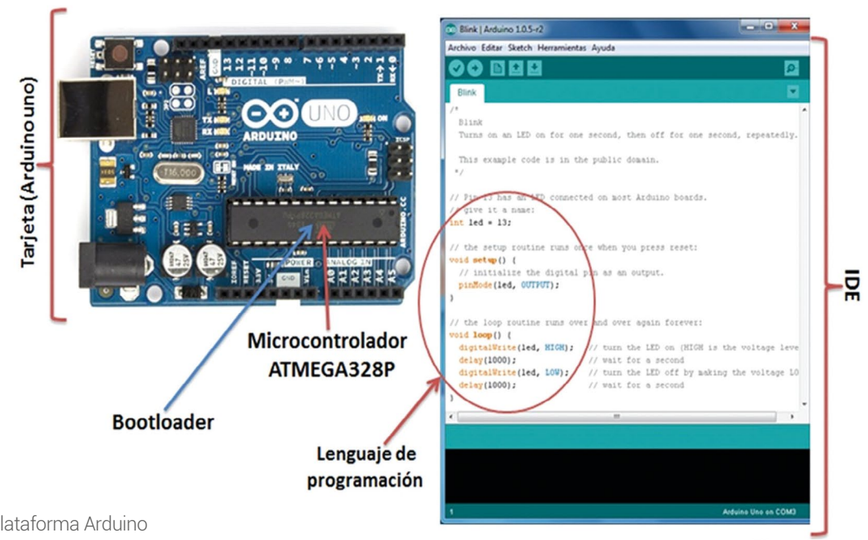


Figura 2. Plataforma Arduino

Tipo de Arduino	Mega2560 R3	UNO	Nano	Leonardo
Pines Digitales Entrada/salida	54 pines	14 pines	14 pines	20 pines
Pines de Entrada Analógicos	16 pines	6 pines	8 pines	12 pines
Procesador	ATmega 2560	ATmega 328P	ATmega 168	ATmega 32U4
Tamaño de Memoria Flash	256 KB	32 KB	32 KB o 16KB	32 KB
Velocidad de Reloj	16 MHz	16 MHz	16 MHz	16 MHz
Costo Aprox.	35.50€	20.50€	20.49€	18.00€

Tabla 1. Comparación entre módulos Arduinos

Placas de Extensión o *Shields*

Las placas de Arduino cuentan con una amplia gama de otras placas que extienden y dan riqueza a las funcionalidades de estas en cuestión. Se puede recurrir a una gran variedad de shields compatibles prácticamente con cualquiera de sus modelos. Unidades Bluetooth, WiFi, Modems GSM, sensores ultrasónicos, sensores de presencia, lectores de tarjetas de memoria SD, y muchas más (Aprendiendo Arduino, s.f.).

Un shield es un módulo de expansión en forma de placa impresa que se puede conectar a la parte superior de la placa Arduino para ampliar sus capacidades, permitiendo además ser apiladas unas encima de otras manteniendo un diseño modular, tal como se puede ver en la Figura 3 (Aprendiendo Arduino, s.f.)

Respecto a los shields, continuamente están saliendo nuevos modelos para Arduino que amplían las capacidades de las placas de Arduino. Todo esto enriquece la tecnología de hardware libre Arduino y permite desarrollar de una forma barata proyectos ambiciosos.

Los shields se pueden comunicar con el Arduino bien por algunos de los pines digitales o analógicos o

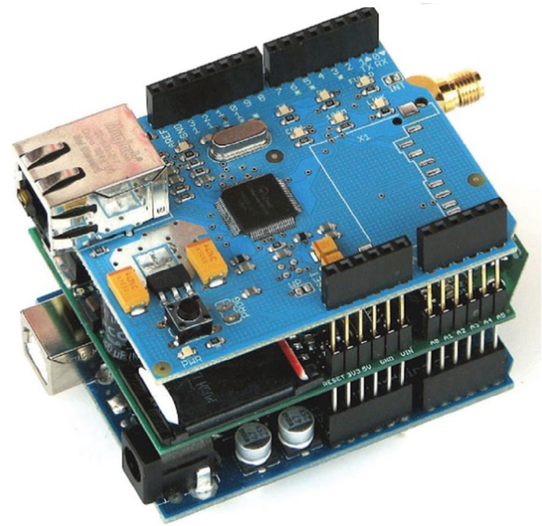


Figura 3. Shields conectados a una placa Arduino

bien por algún bus como el SPI, I2C o puerto serie, así como usar algunos pines como interrupción. Además, estos shields se alimentan generalmente a través del Arduino mediante los pines de 5V y GND.

A continuación, se muestran algunos de los shields más importantes de Arduino que describen la riqueza de este tipo de tecnología y todo lo que se puede hacer.

Arduino Ethernet Shield

El Arduino Ethernet Shield (Figura 4) permite a una placa Arduino conectarse a internet. Está basada en el chip Ethernet Wiznet W5100. El Wiznet W5100 provee de una pila de red IP capaz de utilizar los protocolos TCP y UDP. Soporta hasta cuatro conexiones de sockets simultáneas. Usa la librería Ethernet para escribir programas que se conecten a internet usando el Shield.

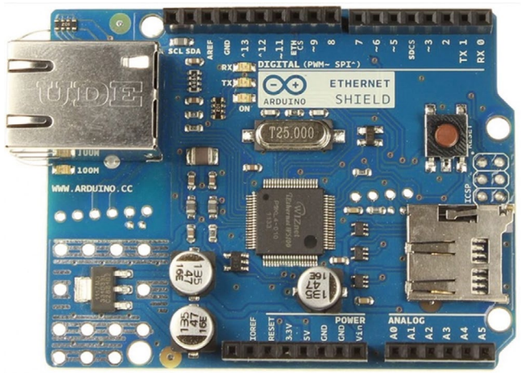


Figura 4. Arduino Ethernet Shield

Arduino Wireless SD Shield

El Arduino Wireless SD Shield (Figura 5) permite a una placa Arduino comunicarse de forma inalámbrica mediante un módulo inalámbrico. Se basa en los módulos XBee de Digi y puede ser utilizado como un reemplazo de serial / USB o puede ponerlo en un modo de comandos y configurarlo para una variedad de opciones de transmisión y redes de malla (Aprendiendo Arduino, s.f.).

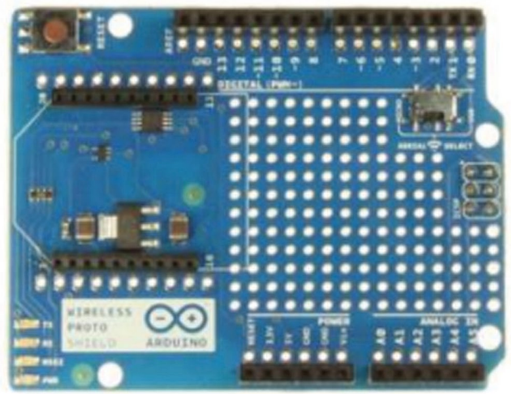


Figura 5. Arduino Wireless Proto Shield

Arduino WiFi Shield 101

El Arduino wifi Shield 101 (Figura 6) es una mejora de los anteriores wifi shield desarrollado junto con Atmel que usa el módulo WINC1500 y también añade funciones de cifrado hardware gracias al chip de cifrado ATECC508A. Usa una nueva librería llamada WiFi101 que también usan otros Arduinos con wifi integrado como el MKR1000. Esta librería es muy compleja y ocupa más del 60% de la memoria disponible en el Arduino UNO, dejando poco espacio para los programas. Si se van a realizar programas complejos, este shield es recomendable usarlo con Arduino Zero, Arduino 101 o Arduino Mega (Aprendiendo Arduino, s.f.)

Arduino Wireless Motor Shield

El Arduino Wireless Motor Shield (Figura 7) es un doble puente completo controlador diseñado para manejar cargas inductivas tales como relés, solenoides y motores de corriente continua paso a paso. Le permite manejar dos motores de corriente continua con su placa Arduino, el control de la velocidad y la dirección de cada uno de forma independiente. También se puede

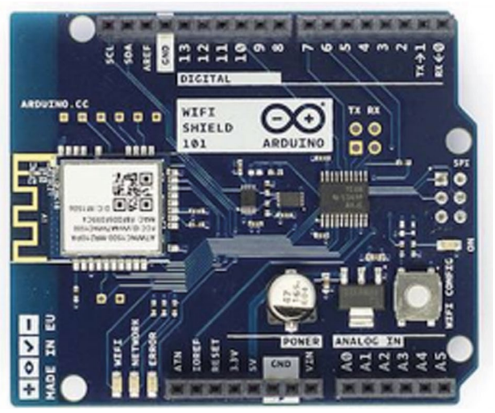


Figura 6. Arduino Wireless Proto Shield

fono ISSN: 1813-5056, RNPS: 0514, Vol. 15, No. 2 , julio-diciembre, 2019, pp. 42 - 55

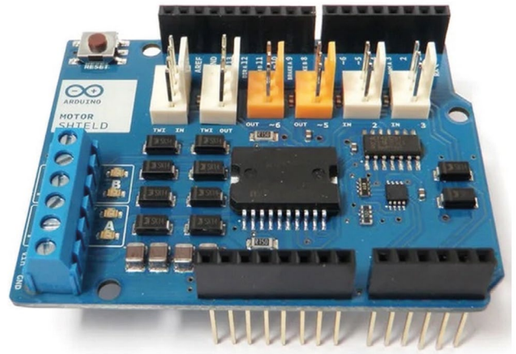


Figura 7. Arduino Wireless Motor Shield

Figura 8. Módulo GPRS+GPS Quadband para Arduino y Raspberry PI (SIM 908)

medir la absorción de corriente de cada motor, entre otras características (Aprendiendo Arduino, s.f.).

Existen otros tipos de Shields como son los shields de GSM que permiten conectar a internet mediante GPRS, usando una tarjeta SIM. También permiten enviar y recibir mensajes (SMS). Estos shields básicamente son módems GSM capaces de conectarse a una red GSM. Un cliente conectado a través de este modem, puede realizar todas las tareas habituales de los teléfonos móviles, desde conectarse a internet, hasta hacer llamadas. Dentro del grupo de shields GSM existen varios modelos que se muestran a continuación.

MÓDULO GPRS+GPS QUADBAND PARA ARDUINO/RASPBERRY PI (SIM908)

Este es uno de los tantos modelos de shield GPRS para Arduino. Cuenta con un módulo SIM908 integrado en la propia placa, ofrece la posibilidad de utilizar la tecnología GPS para posicionamiento en tiempo real, resultando muy útil para aquellas aplicaciones en las que necesitemos conocer la ubicación de nuestro dispositivo. En la figura 8 se aprecia una imagen de dicho shield (Aprendiendo Arduino, s.f.).

MÓDULO 3G/GPRS+GPS PARA ARDUINO/ RASPBERRY PI

Este es uno de los modelos más completo entre muchos shields GPRS disponibles. A parte del sistema GPRS, gracias a su módulo SIM5218, integra también servicios 3G y tecnología GPS. Admite más funcionalidades en comparación con el resto de los shields que se ha visto hasta ahora, incluso permite la conexión de una cámara para la toma de imágenes. En la figura 9 se

Figura 9. Módulo 3G/GPRS+GPS para Arduino/Raspberry PI

puede ver el aspecto que presenta este shield(Aprendiendo Arduino, s.f.).

Raspberry Pi

Esta plataforma empezó la revolución a nivel microprocesador. Usa lenguajes de alto nivel como Python, C++ y Java. El proyecto para su implementación se inició a partir del hecho de que los estudiantes no eran eficientes en detalles técnicos de computación, es decir, con fines didácticos. Fue así que se desarrolló esta computadora en miniatura de bajo costo y relativo alto desempeño que permite a una nueva generación de estudiantes interactuar con sus computadoras en una forma nunca antes imaginada, ofreciéndoles así un aparato con numerosas funcionalidades a un precio irrisorio fomentando y facilitando el estudio de las ciencias de la computación entre los jóvenes.

ISSN: 1813-5056, RNPS: 0514, Vol. 15, No. 2 , julio-diciembre, 2019, pp. 42 - 55 fono

A partir del año 2006 se realizaron varios diseños y prototipos de este dispositivo en la Universidad de Cambridge, Reino Unido. Aunque no fue hasta febrero de 2012 cuando se lanzó de forma comercial Raspberry Pi. Para entonces, ya se habían desbordado las expectativas de ventas, convirtiéndose en una herramienta ideal para el desarrollo de todo tipo de proyectos, no sólo de carácter didáctico sino también en el ámbito empresarial.

Desde el lanzamiento de la primera Raspberry Pi, el proyecto ha ido creciendo según los distintos usos que se comenzaron a darles a las placas. La mayoría de los componentes se mantienen en todas las versiones Raspberry Pi, pero han ido mejorando en potencia y alcances conforme fue pasando el tiempo. La Tabla 2 compara todos los modelos de forma exhaustiva (Maksimovic, Davidović,Vujović, Milošević, Perišić, 2014).

Cabe añadir que el diseño de la Raspberry Pi no incluye disco duro ni unidad de estado sólido para el almacenamiento permanente, para ello se hace uso de la ranura para las tarjetas de memoria. En la tarjeta de memoria se debe realizar la instalación del sistema operativo que deseamos que gestione la Raspberry Pi. A través de la página web oficial se puede acceder a distintas distribuciones: Raspbian, Pidora, OpenElec, ArchLinux Pi.

Actualmente, la Raspberry Pi Foundation ha lanzado la Raspberry Pi 4, la nueva versión del mini ordenador que llega con todo lo que los usuarios habían soñado.

Raspberry Pi 4 Modelo B (Figura 10) es el último producto de la popular gama Raspberry Pi de ordenadores. Ofrece incrementos innovadores en la velocidad del procesador, multimedia con muy buen rendimiento, memoria y conectividad en comparación con la generación anterior Raspberry Pi 3 Modelo B +, conservando la compatibilidad con versiones anteriores y similares en cuanto a consumo de energía. Para el usuario final, Raspberry Pi 4 Modelo B proporciona escritorio rendimiento comparable a los sistemas de PC x86 de nivel básico (Maksimovic, Davidović,Vujović, Milošević, Perišić, 2014)

Versión	**SoC** (System on Chip)	Velocidad	RAM	Puertos USB	Ethernet	Bluetooth
Raspberry Pi A+	BCM2835	700 MHz	512 MG	1	No	No
Raspberry Pi B+	BCM2835	700 MHz	512 MG	4	100 base T	No
Raspberry Pi 2 B	BCM2836	900 MHz	1 GB	4	100 base T	No
Raspberry Pi 3 B	BCM2837A0/B0	1200 MHz	1 GB	4	100 base T	4.1
Raspberry Pi 3 A+	BCM2837B0	1400 MHz	512 MB	1	No	4.2
Raspberry Pi 3 B+	BCM2837B0	1400 MHz	1 GB	4	100 base T	4.2
Raspberry Pi 4 B	BCM2711	1500 MHz	1 GB	2 USB-2 2 USB-3	100 base T	5.0
Raspberry Pi 4 B	BCM2711	1500 MHz	2 GB	2 USB-2 2 USB-3	100 base T	5.0
Raspberry Pi 4 B	BCM2711	1500 MHz	2 GB	2 USB-2 2 USB-3	100 base T	5.0
Raspberry Pi Zero	BCM2835	1000 MHz	512 MB	1	No	No
Raspberry Pi Zero W	BCM2835	1000 MHz	512 MB	1	No	4.1
Raspberry Pi Zero WH	BCM2835	1000 MHz	512 MB	1	No	4.1

Tabla 2. Comparación entre modelos Raspberry Pi

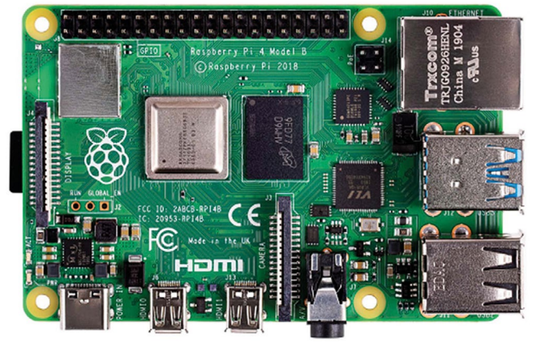


Figura 10. Raspberry Pi 4 Modelo B

Las características clave de este producto incluyen un quad-core de 64 bits de alto rendimiento procesador, soporte de doble pantalla en resoluciones de hasta 4K a través de un par de puertos micro-HDMI, decodificación de video de hardware hasta 4Kp60, hasta 4 GB de RAM, LAN inalámbrica de banda dual de 2.4 / 5.0 GHz, Bluetooth 5.0, Gigabit Ethernet, USB 3.0, y capacidad PoE —Power over Ethernet—.

El puerto GPIO sigue teniendo sus 40 pines, estos pines GPIO pueden emplearse para SPI —Serial Peripheral Interface—, estándar de comunicaciones, usado principalmente para la transferencia de información entre circuitos integrados en equipos electrónicos, I2C —Inter-Circuitos Integrados—, bus de comunicaciones en serie, UART —Transmisor-Receptor Asíncrono Universal—, control de puertos y dispositivos serie, generación de PWM —Modulación por Ancho de Pulso—, alimentación a 3.3V o 5V, GND y E/S.

Comparación entre las dos plataformas. ¿Cómo elegir la adecuada?

Si comparamos estas dos tecnologías nos vamos a dar cuenta que son diferentes, aunque a menudo escuchemos hablar de ellas para dar solución a los mismos problemas, como pueden ser proyectos sencillos de robótica o domótica. Cada una tiene sus fortalezas y debilidades, y una plataforma es mejor que otra para una determinada aplicación.

Microcontroladores vs microprocesadores: un microcontrolador es un circuito integrado diseñado con el propósito de tareas específicas. Es principalmente usado en productos que requieren un grado de control impuesto por el usuario. Los microprocesadores en cambio, son usados para ejecutar aplicaciones grandes y genéricas.

La Raspberry Pi y el Arduino fueron pensadas para propósitos muy diferentes, a pesar de que ambas son de software libre, para que cualquiera pueda revisarlo o modificarlo, solo el Arduino es de hardware libre, lo que significa que cualquiera puede tomar el diagrama eléctrico de la placa y fabricarse la suya propia, sin embargo, la Raspberry Pi esta única y exclusivamente bajo el control de la Raspberry Pi Fundation, siendo ellos los únicos que pueden fabricar y modificar dicha placa.

Arduino para principiantes y proyectos de propósito simple

Es la principal plataforma de la comunidad DIY —Do It Yourself—, ya que es open-source. Es fácil de desarrollar, consume poca energía y es muy simple de usar. Además, está especialmente diseñado para principiantes, de tal forma que cualquiera pueda jugar con el mismo y conectarlo a componentes externos. En esencia, el Arduino es una plataforma pequeña programable que acepta y almacena códigos de la computadora convencional. Es capaz de cosas simples como controlar luces o controlar sistemas de jardinería. La plataforma, el lenguaje de programación y muchos proyectos son de distribución libre, dispuestos a ser utilizados para adecuarse a las necesidades de muchos propósitos (Arduino.cl, s.f.), (Maksimovic, Davidović,Vujović, Milošević, Perišić, 2014)

Su uso es tan sencillo que cualquiera puede usarlo, es decir, no se precisa de conocimientos muy profundos de programación ni electrónica y es el punto perfecto de partida para cualquiera que busca iniciarse en proyectos de electrónica de tipo DIY debido a su simplicidad.

Ventajas: El Arduino es relativamente barato para disponer de varias unidades y explotar su uso. Además de su estandarte Arduino Uno, se disponen de muchas variaciones de modelos de Arduino para elegir. Como es de bajo consumo, es ideal para aplicaciones de usos de larga duración, o incluso para uso de baterías. Pero por, sobre todo, el Arduino tiene una popularidad muy alta, lo que conlleva a una gran facilidad de encontrar apoyo, documentación sobre proyectos particulares,

tutoriales, etc. Además, presenta flexibilidad para distintos tipos de interfaces (Arduino.cl, s.f.).

Desventajas: Si bien tiene una amplia proyección de uso y aplicaciones como se nombró en las ventajas, aún toma tiempo acostumbrarse a usar algo sin interfaz gráfica. Debido a lo barato y pequeño que es, normalmente el Arduino no puede manejar diferentes procesos al mismo tiempo, lo cual hace que no sea bueno para proyectos que requieren mayor poder de cómputo (Arduino.cl, s.f.).

El Arduino es mejor para proyectos de propósito simple donde no se necesite mucho poder de cómputo y sea necesario el uso de un microcontrolador con el objetivo de facilitar la tarea de recogida de los datos proporcionados por distintos sensores tantos los que proporcionan una señal de salida analógica como los que la ofrecen de manera digital sin excesiva complejidad. Por ejemplo, si se quiere hacer un proyecto donde solo quieras hacer el control de algunos actuadores, como encender un calefactor al detectar cierta temperatura, controlar un sistema de riego automatizado o realizar proyectos de monitoreo y control donde se realice lecturas de sensores y al mismo tiempo ejecutar, controlar o actuar sobre ciertos factores del entorno que le rodean como por ejemplo controlando luces, accionando motores, activando alarmas y muchos otros actuadores, podríamos utilizar un Arduino (Arduino.cl, s.f.).

Si la aplicación o proyecto que se requiere necesita de un sistema de vigilancia inteligente que pueda leer patentes de vehículos, calcular la cantidad de tráfico en una avenida, y toda esa información subirla algún servidor en la nube, lo ideal sería una Raspberry Pi no una placa de Arduino.

Raspberry Pi: Para proyectos de multimedia complejos o basados en Linux

El Raspberry Pi es una pequeña computadora que corre sobre Linux desde una tarjeta SD, de la que se puede correr todo tipo de proyectos DIY. En pocas palabras, es una computadora Linux de bajo consumo, de tal forma que en principio puede hacer lo que hace una maquina Linux a un costo más bajo. Con 2 puertos USB y la salida HDMI, puede usarse como cualquier computadora, lo cual significa que es perfecto para proyectos que requieran un sistema Linux. Es así que Raspberry Pi es ideal para requerimientos de pantalla y especialmente, proyectos que requieran conexión a internet (Arduino.cl, s.f.),

Ventajas: Una pequeña computadora trae toda clase de ventajas. El puerto HDMI puede usarse para conectarse a un televisor y los 2 puertos USB permiten operarlo como a una computadora con teclado y mouse fácilmente. Su procesador gráfico soporta 1080p. También tiene un puerto ethernet para fácil conexión a internet con leves dificultades. Ya que el sistema operativo corre desde una tarjeta SD, este puede cambiarse fácilmente con solo cambiar la tarjeta. Esto es muy útil considerando que se tienen varias opciones para el sistema operativo. Dado su precio, es poderoso y aun así de fácil uso para principiantes. En cuanto a capacidad de expansión, es importante mencionar que tiene grandes beneficios gracias a la placa que permite la compatibilidad con los shields de Arduino, ya que, sin incluir estas expansiones, el soporte exclusivo para el Pi es muy bajo (Arduino.cl, s.f.).

Aplicaciones

El eje central del IoT y su desarrollo son las aplicaciones. Las capacidades que aportan un procesador o microcontrolador, una memoria y otros recursos electrónicos, hacen que el Internet de las Cosas tenga aplicaciones en casi todos los campos que se puedan imaginar. Algunas de las aplicaciones con más interés son la domótica (smart home), el transporte inteligente (smart transport), aplicaciones industriales, las ciudades inteligentes (smart cities) o aplicaciones medicinales (smart health). En todas estas aplicaciones podemos encontrar la plataforma Arduino y Raspberry Pi como eje central en el desarrollo de muchos proyectos.

A continuación, se muestran algunos proyectos de ejemplos.

Proyectos con Arduino

La solución planteada en se realizó con el diseño de un Sistema Remoto de Supervisión y Control de Incendios, Humo y Fuga de Gas, que permite un ambiente más seguro para los residentes de una vivienda y que consta de diferentes sensores. (Villegas y Roa, 2017).

En este sistema remoto de seguridad en el hogar básicamente tienen la funcionalidad principal de la supervisión y control de variables especificadas como pueden ser (fuego, humo, fuga de gas y otras más) junto a la coordinación con el usuario a través de un mensaje por medio de un módulo GSM/GPRS.

El sistema está diseñado y desarrollado para encargarse de supervisar las variables establecidas continuamente en tiempo real, mediante sensores o detectores que están funcionando paralelamente entre ellos. En el momento que alguna de las variables ya establecidas esté por fuera de los parámetros, inmediatamente se manda un mensaje al usuario por medio del módulo GSM alertando que se ha presentado una situación de peligro en el lugar. En el momento que se envía dicho mensaje el sistema procede a activar el control para la respectiva variable activada.

En el mensaje enviado al usuario se le informará el tipo de suceso que se ha presentado en el lugar si la persona se encuentra fuera de la residencia en el momento que se presente dicho incidente y se le recomienda que se comunique con las autoridades correspondientes antes de dirigirse a su domicilio para evaluar los daños presentados.

En la Figura 11 se muestra el diagrama de bloques que está compuesto de los diferentes equipos para la realización de este proyecto de domótica de seguridad en el hogar con Arduino.

En (Biosca, Yera, Ruiz, 2018) se realizó el diseño de una plataforma de monitoreo y control remoto empleando la red celular GSM para estaciones de Telecomunicaciones no atendidas.

El sistema cuenta con un módulo de hardware que se instala en la estación en cuestión, que contiene el controlador de la estación basado en hardware libre Arduino y su set de sensores y actuadores asociados, así como un módulo de expansión GSM para la comunicación con la aplicación de control. El segundo elemento es la aplicación de control en sí, desarrollada para ser instalada en dispositivos Android y facilitar de esta forma el monitoreo y control de la estación de forma móvil desde cualquier tableta o teléfono móvil que porten los supervisores. El intercambio de información entre los terminales de administración y el módulo de control de la estación ocurre por medio del servicio de mensajes cortos o SMS propio de GSM.

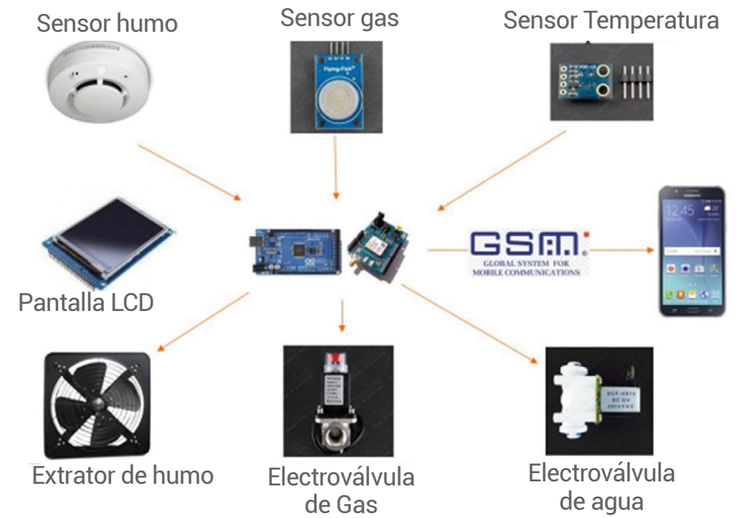


Figura 11. diagrama en bloques del sistema remoto de seguridad en el hogar

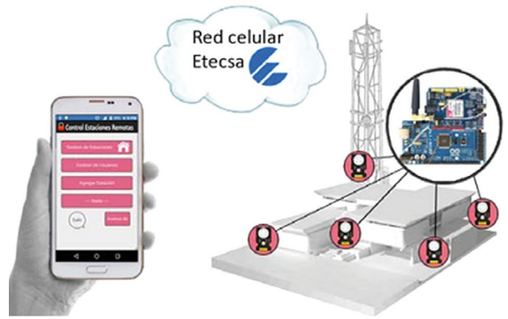


Figura12. Arquitectura de la plataforma de monitoreo y control

El sistema compuesto por dos partes fundamentales: el módulo de la estación, hardware y la aplicación de monitoreo y control, software, se aprecian en la figura 12.

El módulo de la estación, que se instala y se despliega en la instalación que se desea monitorear, está compuesto por un controlador Arduino Mega, al que se conectan cuantos sensores y actuadores como elementos se desee controlar y/o monitorear en la estación. Poniendo como ejemplo el caso de la figura 12 en la que se representa una estación de Telecomunicaciones, los

puntos de interés a monitorear pueden ser las puertas y ventanas de acceso a la instalación, el nivel de combustible en la planta de emergencia, la temperatura y la humedad en la sala tecnológica, entre otras variables.

La estructura del módulo de la estación se muestra en la figura 13 en un esquema en bloques.

El sistema electrónico que se puede observar en la figura 13, el cual es la parte inteligente colocada en la estación remota desatendida, está compuesto por un pequeño módulo Arduino Mega 2560 R3, un módulo SIM900 para comunicaciones GSM/GPRS, un lector de tarjetas Micro SD y una pantalla serie I2C de 4 líneas y 20 caracteres por línea. El microcontrolador de Arduino Mega 2560 R3 se comunica con el módulo SIM900 por medio del puerto serie y comandos AT. El módulo SIM900 es el encargado de la etapa de radiofrecuencia para el servicio de mensajes SMS. El programa en el microcontrolador desarrollado en lenguaje Arduino espera a recibir mensajes SMS para de ahí extraer el número de teléfono móvil que le envió el mensaje y el contenido del mensaje que le indicará la acción a ejecutar, como también generar mensajes SMS con información de monitoreo para el administrador como mensajes de alarmas. Dentro de las funcionalidades del sistema electrónico también se encuentra el monitoreo del estado de los sensores instalados en el local y la gestión de los procesos relacionados con registrar o dar baja a los usuarios administradores, hacer un historial con los logs generados por las sesiones de trabajo con el sistema.

El sistema se programó haciendo uso de dos leguajes de programación, Java del lado de la aplicación Android y lenguaje Arduino en el sistema electrónico a implementar. El intercambio de información entre la estación y la aplicación Android se realizó de la misma manera, pero se programa distinto para cada caso ya que son lenguajes de programación diferentes. Para lograr la comunicación en ambos sentidos se propuso

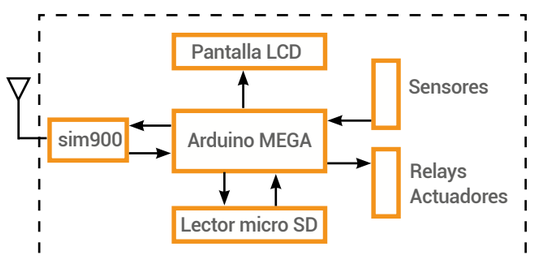


Figura 13. Estructura del hardware del módulo de la estación

implementar un protocolo de comunicación usando el servicio SMS de la red GSM realizado entre el terminal de administración (Aplicación Android) y el sistema electrónico en la estación no atendida.

Proyectos con Raspberry Pi

En el proyecto (Sedó, 2014) se realizó el desarrollo, tanto hardware como software, de un sistema domótico de bajo costo basado en el dispositivo Raspberry Pi, en un sistema capaz de gestionar elementos domésticos simples tales como sensores de presencia, bocinas de alarmas y encendido de luces. Además, se diseñó e implemento una interfaz web para facilitar la interacción del usuario con el sistema domótico instalado en su hogar.

En primer lugar, para poder acceder al sistema domótico del proyecto desde cualquier dispositivo con conexión a internet y así, interactuar con el mismo, se requiere de un servidor web propio que nos facilite esta acción. Raspberry Pi ofrece la posibilidad de trabajar como servidor web, realizando las configuraciones correspondientes.

Por otro lado, sobre el dispositivo Raspberry Pi se ejecuta un programa residente (daemon) encargado de la manipulación y almacenamiento del estado de las distintas señales discretas. En base a estos valores, se puede hacer uso de una placa de expansión PiFace Digital (Figura 14) en la que se conectarán los distintos dispositivos externos tales como luces, sensores de presencia y bocina. El estado de las señales correspondientes a estos dispositivos externos se almacena en una base de datos.

La placa de expansión PiFace Digital se trata de una placa diseñada para conectarse de forma directa sobre el conector GPIO de Raspberry Pi.

De este modo, el funcionamiento del sistema domótico se puede resumir según el esquema (Figura 15), cuya descripción es la siguiente:

1. El usuario accede a la interfaz web a través de su dispositivo móvil o de escritorio con la intención de modificar o consultar el estado de su hogar. Esta interfaz muestra el estado del sistema a través de una consulta a la base de datos, donde se almacena toda la información respectiva al sistema domótico.
2. Si se modifica algún dispositivo externo a través de la interfaz web, se actualiza la información de la base de datos.
3. El programa de gestión de señales, que se encuentra en continua ejecución en la Raspberry Pi, monitoriza los cambios solicitados por el usuario.
4. Una vez evaluada la información, se mandan las señales requeridas a los distintos dispositivos externos a través de la placa de expansión PiFace Digital.

De este modo, se consigue responder de forma rápida y sencilla a las diferentes peticiones del usuario acerca del sistema domótico de su hogar. No obstante, ésta se trata de una descripción general del sistema.

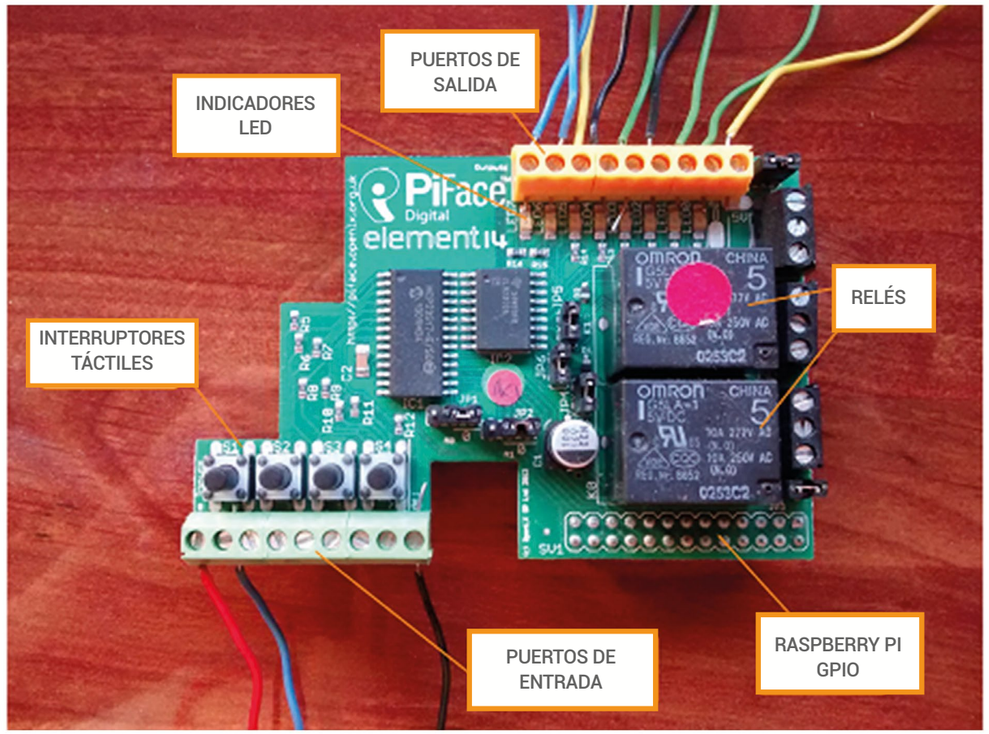


Figura 14. Placa de Expansión PiFace Digital

Desarrollo de la Solución de la Plataforma IoT Open Source en ETECSA

Etecsa debe fomentar la incorporación de las Plataformas Open Source Arduino y

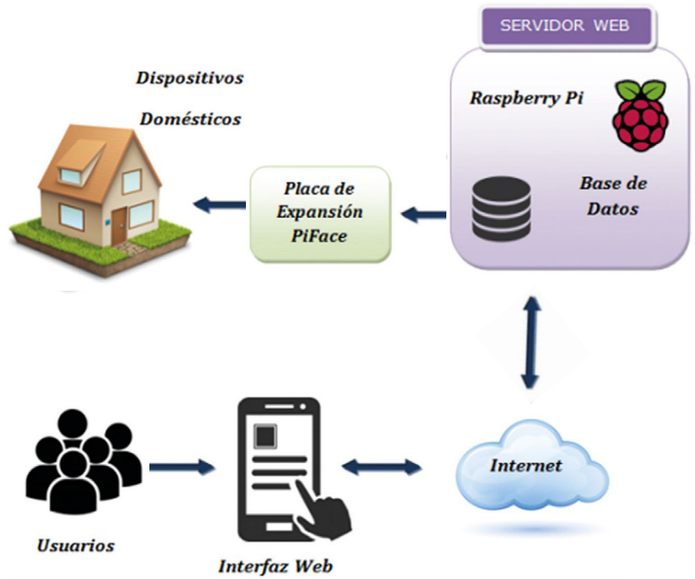


Figura 15. Diseño general del sistema domótico basado en Raspberry Pi

Raspberry pi como herramienta educativa en las universidades como la CUJAE en las carreras de Ingeniería Informática, Telecomunicaciones y Electrónica y Automática, con el objetivo de formar profesionales especializados en trabajar con proyectos de las áreas de programación y electrónica, donde los estudiantes puedan ir desarrollando habilidades a lo largo de la carrera y así en un futuro poder ser participe en proyectos complejos como crear una plataforma IoT Open Source. Es necesario crear una mano de obra especializada en este tema para afrontar la problemática de desarrollar plataformas IoT que puedan impulsar el proceso de digitalización de la sociedad que se está llevando a cabo en Cuba.

Teniendo en cuenta la situación socio-política de nuestro país, haciendo especial énfasis en las afectaciones provocadas por el embargo económico, se hace imposible en la práctica optar por comprar o utilizar una plataforma extranjera. Siendo la mejor solución desarrollarla en nuestro país, y ETECSA como único operador de Telecomunicaciones de nuestro país debería en un futuro poder contar con una plataforma IoT que pudiera brindar todas las bondades que ofrece esta tecnología y poder brindársela a sus usuarios y al país en ramas por ejemplo como la salud.

Trabajar con las universidades es la mejor manera de afrontar esta problemática, pues no solo contribuye a acelerar la salida al mercado de una solución de IoT cubana, también estaremos contribuyendo a formar profesionales especializados en el tema si financiamos sus proyectos de Tesis, ya que a veces los estudiantes no cuentan con la oportunidad de tener a mano las placas de Arduino o Raspberry o cualquier otro hardware necesario para desarrollar sus proyectos.

Es importante replantearse cómo podrían ser las relaciones universidad-empresa, en este contexto. Su importancia está dada por la medida en que dicha relación representa una estrategia eficaz para promover los procesos de innovación empresarial y para contribuir que las universidades hagan desarrollo de soluciones para el país. Para lograr se debe crear un ambiente de colaboración en el cual la empresa en este caso ETECSA y la universidad se comporten como socios:

- Los trabajos serán realizados en conjunto, supervisados por ambas partes.
- Las ganancias deberán ser repartidas mediante contrato previo.
- Programas de inserción laboral, formación y prácticas en la empresa enfocadas al desarrollo de soluciones técnicas para captar futuros especialistas en determinadas ramas de investigación.
- Incluir ofertas formativas optativas en las universidades, buscando la formación de expertos en áreas específicas como en IoT.
- Incluir áreas de trabajo pertenecientes a la universidad con todas las condiciones de software y hardware para desarrollar proyectos.
- La empresa debe crear concursos sobre ideas innovadoras enfocadas al desarrollo de soluciones de hardware o software en las universidades como recurso de innovación para la empresa.

Conclusiones

El presente trabajo se ha desarrollado con el fin de analizar la necesidad de implementar plataformas con tecnología Open Source para soluciones de IoT. Se presentaron algunas alternativas existentes en el mercado de placas de desarrollo de arquitectura Open Source como son Arduino y Rasberry Pi. Se compararon estas dos plataformas de desarrollo analizando sus ventajas y desventajas. Como también se evidencia la importancia de desarrollar una plataforma IoT teniendo en cuenta la situación socio-política de nuestro país relacionada con el bloqueo definiendo que es mejor desarrollarla en nuestro país y como las universidades juegan un papel muy importante en este escenario. Por tal motivo el autor encuentra que la utilización tanto del software código fuente abierto, como del hardware de arquitectura abierta tiene una ventaja competitiva trascendente, respecto a el software y hardware privativo.

De igual forma también se mostró a modo de ejemplo algunos proyectos realizados en tesis de estudiantes como muestra de la riqueza de este tipo de tecnología de desarrollo de la cual es menester destacar las comunidades que se forman a través de las redes sociales en donde estudiantes de ingeniería de diferentes naciones van incrementando y mejorando el conocimiento tanto tácito como explícito, para el desarrollo de proyectos de ingeniería escolares gracias a estas plataformas de desarrollo Open Source.

Referencias

Aprendiendo Arduino. (s.f.). Aprendiendo a manejar Arduino en profundidad. Shields. Obtenido de Aprendiendo Arduino: https://aprendiendoarduino.wordpress.com/category/shields/

Arduino b. (s.f.). Compare board specs. Obtenido de Arduino Products Compare: https://www.arduino.cc/Products/Compare

Arduino a. (s.f.). What is Arduino. Obtenido de Arduino Guide Introduction: https://www.arduino.cc/en/Guide/Introduction

Arduino.cl. (s.f.). Arduino vs Raspberry. Obtenido de Arduino.cl: https://arduino.cl/arduino-vs-raspberry/

Biosca Rojas, D.; Yera Pompa, J.I.; Riuz Delgado, R.L. (2018). Plataforma Iot para el Monitoreo Y Control Remoto de Estaciones no Atendidas Empleando Arduino+GSM. En XVII Convención y Feria Internacional Informática 2018, VIII Simposio de Telecomunicaciones. Obtenido de http://www.informaticahabana.cu/sites/default/files/ponencias2018/TEL17.pdf

Evans, D. (2011). Internet de las cosas: Cómo la próxima evolución de Internet lo cambia todo. CISCO: Informe Técnico.

Maksimovic, M., Davidović, N., Vujovic, V., Milosevic, V., y Perisic, B. (2014). Raspberry Pi as Internet of Things hardware: Performances and Constraints. Obtenido de ResearchGate: https://www.researchgate.net/publication/272175660_Raspberry_Pi_as_Internet_of_Things_hardware_Performances_and_Constraints

Sedó, R. (2014). Diseño de un sistema domótico de bajo coste basado en Raspberry Pi. Obtenido de ResearchGate: https://www.researchgate.net/publication/298214426_Diseno_de_un_sistema_domotico_de_bajo_coste_basado_en_Raspberry_Pi

Villegas Villada, D.; Roa Estrada, R. A. (2017). Prototipo de un sistema remoto de seguridad en el hogar. Universidad de San Buenaventura Colombia Facultad de Ingeniería, Ingeniería Electrónica. Tesis de Grado en Ingeniería Electrónica. Obtenido de: bibliotecadigital.usbcali.edu.co/bitstream/10819/4644/1/Prototipo_Sistema_Remoto_Villegasa_2017.pdf

Los Sistemas de Vigilancia Tecnológica en organizaciones cubanas. La experiencia del Ministerio de Comunicaciones

Technological Surveillance Systems in Cuban organizations. The experience of the Ministry of Communications

Lic. Leslie Carrodeguas Rodríguez[1]

Recibido: 06/2019 | Aceptado: 9/2019

Palabras clave

Sistemas de Vigilancia Tecnológica
Toma de Decisiones
Gestión de Información
Ministerio de Comunicaciones

Resumen

Se presentan los elementos teórico-conceptuales asociados a los Sistemas de Vigilancia Tecnológica (SVT) como parte de la gestión de información en las organizaciones y proceso estratégico para la toma de decisiones. Se puntualizan los componentes que integran los SVT, teniendo en cuenta los principales modelos, metodologías y normas vigentes. Se describe el estado del proceso de vigilancia en Cuba, profundizando en la experiencia del Ministerio de Comunicaciones.

Keywords

Technological Surveillance Systems
Decision-making
Information management
Communications Ministry

Abstract

The theoretical-conceptual elements associated with Technological Surveillance Systems (SVT, in its acronym in Spanish) are presented as part of the information management in organizations and decision-making strategic process. Components that make up the SVT are specified, taking into account the main models, methodologies and standards in force. The state of the surveillance process in Cuba is described, deepening in the experience of the Ministry of Communications.

Introducción

En la denominada sociedad del conocimiento y a raíz de los continuos cambios económicos, políticos, tecnológicos, sociales y culturales, la información se convierte en un factor estratégico para la generación de valor en las organizaciones, por tanto, si se gestiona adecuadamente contribuye al proceso de toma de decisiones estratégicas ágiles, precisas y con alto impacto social.

El análisis de la información interna permite identificar mejores prácticas, conocer el comportamiento de las relaciones con clientes, competidores y proveedores, así como el cumplimiento de las estrategias de la organización. Por su parte, la información externa aporta elementos que determinan el comportamiento de la economía, los adelantos científicos y tecnológicos, las regulaciones, buenas prácticas e información sobre competidores o productos sustitutos. De esta forma la vigilancia tecnológica se ha convertido a nivel internacional en un elemento importante de desarrollo competitivo en el entorno actual, del cual Cuba no se encuentra exento.

En el Ministerio de Comunicaciones (MINCOM) es fundamental contar con la información oportuna, eficiente y confiable durante los procesos de toma de decisiones, debido al desarrollo acelerado del sector de las Tecnologías de la Información y la Comunicación (TIC), y a las incesantes amenazas a las que se expone el país. De ahí la necesidad de replantearse sistemáticamente el funcionamiento de los componentes que conforman el Sistema de Vigilancia Tecnológica con vistas a su mejora continua. De ahí que la presente investigación se plantee el sistema de objetivos siguientes:

Objetivo General

Describir el Sistema de Vigilancia Tecnológica para el Ministerio de Comunicaciones con vistas a su actualización.

Objetivos específicos

Analizar los principales elementos teóricos conceptuales asociados a los Sistemas de Vigilancia Tecnológica.

Diagnosticar el estado actual de la vigilancia tecnológica en el Ministerio de Comunicaciones.

Proponer mejoras en la articulación de los componentes para el Sistema de Vigilancia Tecnológica del Ministerio de Comunicaciones.

Materiales y métodos

Análisis - síntesis: Se realizan análisis de todos los elementos que inciden en los sistemas de vigilancia tecnológica y se resume lo más significativo de los mismos.

Análisis documental: Consiste en el análisis y revisión de los documentos y fuentes de información relacionadas con los Sistemas de Vigilancia Tecnológica, fundamentalmente con sus definiciones y compontes.

Análisis de sistema: Está dirigido a modelar los procesos que integran el sistema mediante la determinación de sus flujos de información, así como las relaciones entre sus componentes. Esas relaciones determinan por un lado la estructura del sistema y por otro su dinámica.

Encuesta y entrevista: Se utiliza para la recolección de la información asociada a los componentes del Sistema de Vigilancia Tecnológica que se identifican en el Ministerio de Comunicaciones.

La Vigilancia Tecnológica, principales conceptos y características

Debido al crecimiento exponencial de la producción científica y las fuentes de información en general, el desarrollo acelerado de las tecnologías de la información y la comunicación y la evolución de campos de actividad interdisciplinares, se han generado nuevos retos organizacionales, la cuales encaminan sus acciones al uso de herramientas de gestión de información y el conocimiento.

Es decir, según Berges, Meneses y Martínez (2016) desde la década de los noventa las organizaciones, comenzaron a nutrirse de técnicas de captación y análisis del entorno con vistas a la generación de importantes ventajas competitivas, fundamentalmente en el ambiente empresarial, que en muchos casos denominaron como Inteligencia de Negocio, Inteligencia Empresarial, Inteligencia Competitiva, Vigilancia Tecnológica, entre otras terminologías.

Asimismo, Pérez (2019) apunta a la importancia del análisis profundo y sistemático de la competencia en el diseño de la estrategia de la organización, recomendando el empleo de sistemas formalizados de vigilancia e inteligencia.

En este sentido, la literatura especializada recoge diversas definiciones de la expresión Vigilancia Tecnológica como herramienta gerencial. A decir de Palop y Vicente "es el esfuerzo sistemático y organizado por la empresa de observación, captación, análisis, difusión precisa y recuperación de información sobre los hechos del entorno económico, tecnológico, social o comercial, relevantes para la misma por poder implicar una oportunidad u amenaza para ésta. Requiere una actitud de atención o alerta individual. De la suma organizada de estas actitudes resulta la función de vigilancia en la empresa" (Palop y Vicente, 1999).

Según Lesca, "la Vigilancia Tecnológica incluye los esfuerzos que la empresa dedica, los medios de que se dota y las disposiciones que toma con el objetivo de conocer todas las evoluciones y novedades que se producen en los dominios de las técnicas que le conciernen actualmente o son susceptibles de afectarle en el futuro" (Lesca, 1994).

Para Escorsa, "es la captura, el análisis, la difusión y la explotación de las informaciones técnicas útiles,

[1] Ministerio de Comunicaciones; Dirección de Gestión de Información, La Habana, Cuba. leslie.carrodeguas@mincom.gob.cu

para la supervivencia y el crecimiento de una organización" (Escorsa, 2014).

En 2006 y posteriormente en 2011 se publicó la norma UNE 166006:2011, que proporciona las directrices para optimizar, a través de la implantación de sistemas de Vigilancia Tecnológica e Inteligencia Competitiva (VT/IC), los procesos de monitoreo y análisis del entorno competitivo en el que se mueve la organización.

La UNE 166006:2011 define a la VT como "el proceso organizado, selectivo y sistemático, para captar información del exterior y de la propia organización sobre ciencia y tecnología, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento con el fin de tomar decisiones con menor riesgo y poder anticiparse a los cambios" (AENOR, 2011).

Esta norma define los requisitos generales de un sistema de VT/IC, establece tres grandes niveles de necesidades por parte de organizaciones y perfila, aunque sin ningún ánimo exhaustivo, los correspondientes productos de VT/IC para satisfacerlas: (Berges, Meneses y Martínez, 2016).

Según la Sociedad de Profesionales de Inteligencia Estratégica y Competitiva (SCIP), la VT/IC constituyen "el proceso ético y sistemático de recolección de información, análisis y diseminación pertinente, precisa, específica, oportuna, predecible y activa, acerca del ambiente de negocios, de los competidores y de la propia organización" (SCIP, 2019).

Al analizar las similitudes entre los conceptos de vigilancia e inteligencia, García (2019) refiere que, ciertamente existen coincidencias en los procesos y objetivos que integran dichas herramientas gerenciales. Sin embargo, según su criterio, la principal distinción se basa en que la vigilancia tiene como fundamento la observación y la inteligencia continúa su curso y centra en las actividades finales, de análisis de lo observado y agregación de valor a los resultados (García, 2019).

Actualmente en la literatura conviven diferentes versiones de sistemas de vigilancia e inteligencia, que comparten el núcleo del proceso y que ponen el acento en distintos puntos del mismo (AENOR, 2018). De esta forma, se evidencia una evolución en el concepto de la vigilancia tecnológica, que va más allá del monitoreo sistemático de factores críticos. Es decir, no es posible concebir a la Vigilancia como un proceso aislado de las variables: económica, comercial, competitiva, social, reguladora y jurídica. De ahí que las definiciones de Vigilancia Tecnológica, Inteligencia Competitiva e Inteligencia Empresarial están estrechamente relacionadas, por lo que en ocasiones se utilizan indistintamente para referirse a la misma actividad.

La versión de la norma UNE: 166006 publicada en 2018 considera el proceso de vigilancia e inteligencia como una suma de los dos, sin marcar sus diferencias sino reforzando este enfoque basado en procesos.

"Esta norma tiene por objeto facilitar el diseño y estructuración de los procesos de recogida, análisis y comunicación de información sobre el entorno de la organización, para apoyar la toma de decisiones a todos los niveles" (AENOR, 2018).

Esto se debe a la identificación de dos enfoques o paradigmas de la vigilancia: la primera que enfatiza en los análisis bibliométricos, cienciométricos y el análisis de la minería de texto; y la segunda escuela, que surge aproximadamente a principio de los años 2000, y profundiza en temáticas como el conocimiento, la estrategia, procesos inteligentes, inteligencia organizacional y las capacidades tecnológicas. Los principales ejes diferenciadores entre estas dos escuelas están dados por las capacidades, los pronósticos y el alcance de la innovación (Castellanos y Torres, 2010).

A los efectos de esta investigación, la Vigilancia Tecnológica se presenta desde un enfoque como proceso de inteligencia, en el cual están presente de los siguientes elementos:

Es un proceso organizacional sistémico, que transita por varias etapas.

Resalta el poder que posee la información como recurso estratégico.

Permite anticiparse a los cambios.

Incide en la competitividad de las organizaciones.

Su principal objetivo es tributar a la toma de decisiones.

Sus salidas fundamentales están dadas por servicios de inteligencia con alto valor agregado.

La vigilancia tecnológica está estrechamente relacionada con la gestión del conocimiento.

Según Orozco (2009) los recursos fundamentales de un SVT son: "personal preparado en gestión de información y en análisis de información, con conocimiento de los temas de interés a la empresa; acceso a muy variadas fuentes de información, ya sean bases de datos u otras; tecnología de información para el procesamiento más rápido y eficiente; contacto con personas en el entorno informativo de la empresa, ya sea local, nacional o internacional y una clara noción de la gestión de información en función de los intereses de la organización".

Por tanto, se entiende como SVT al conjunto de interrelaciones entre entidades y procesos de Vigilancia Tecnológica integrados al sistema de gestión de información. La entrada fundamental de los SVT es información relevante sobre el entorno y las condiciones internas de la organización, resultante del monitoreo sistemático de los factores críticos de vigilancia. Las salidas fundamentales del sistema, son servicios basados en el proceso de análisis y agregación de valor a la información estratégica de la organización, con el objetivo de contribuir a la adecuada toma de decisiones.

Modelos y procesos de la Vigilancia Tecnológica

En la literatura se describe un amplio conjunto de modelos, que integran los procesos de vigilancia tecnológica. Delgado en el artículo titulado: *Vigilancia tecnológica en una universidad de ciencias técnicas*, señala que las metodologías presentan como procesos comunes la búsqueda y análisis de la información. Mientras que el resto de los procesos varían en función del alcance y objetivo de la vigilancia y la difusión que se realiza sobre los resultados de la misma, incluyendo a los usuarios, así como el proceso de toma de decisiones. Enfatiza en que la implementación de un sistema organizado de vigilancia tecnológica exige enfoques multidisciplinarios horizontales y requiere su adaptación al entorno de la empresa y a su cultura, debiendo estar integrado en sus procedimientos habituales (Delgado, 2011).

Al respecto, se presenta un resumen de elaboración propia y de los autores Delgado(2011), San Juan y Romero(2016) y Moyares, Infante y Rodríguez(2018); que comprende los principales procesos de vigilancia tecnológica asumidos en las organizaciones a partir del uso de diferentes metodologías (Véase Tabla 1).

Los Sistemas de Vigilancia Tecnológica en Organismos de la Administración Central del Estado de Cuba

El desarrollo de la Vigilancia Tecnológica en Organismos de la Administración Central del Estado (OACE), tiene sus antecedentes en la década de 90' con la creación en 1992, de la consultoría de información Biomundi, cuya función principal era brindar servicios de consultoría y de Inteligencia Empresarial al Polo Científico del Oeste en función del desarrollo de la industria de biotecnología y la farmacéutica, alcance que fue extendido posteriormente a otros sectores.

Asimismo, desde hace casi dos décadas, existen organizaciones que utilizan los servicios de consultorías o mecanismos propios, para beneficiarse de estas técnicas en los sectores más importantes de la economía y la seguridad nacional.

El Ministerio del Interior (MININT), por ejemplo, cuenta con un Sistema de Vigilancia Tecnológica propio coordinado por el Centro de Investigación y Desarrollo Técnico (CIDT).

Este sistema constituye un instrumento de análisis y evaluación para la toma de decisiones, a partir de la detección temprana de oportunidades y amenazas tecnológicas, sirviendo como herramienta capaz de influir en la estrategia de desarrollo de la organización.

El sistema está organizado internamente en dos grupos de la forma siguiente:

Grupo de Observación tiene la función de captar información científico técnica, analizarla y elaborar productos informativos y de inteligencia, así como reproducir documentos seleccionados que considera necesario trasladar a los evaluadores.

Grupo de Evaluación tiene la función de analizar y evaluar los productos informativos y de inteligencia generados por el Grupo de Observación así como de la copia de documentos seleccionados y elaborará un informe conclusivo, el que contendrá evaluaciones, criterios, consideraciones y propuestas concretas (Tur, 2010).

En el Ministerio de las Fuerzas Armadas Revolucionaras (MINFAR) se establecieron las Indicaciones 308, en las cuales se define a la vigilancia tecnológica como "la actividad especializada y sistemática de búsqueda, seguimiento, análisis y entrega periódica de información, relacionada con los cambios tecnológicos y sus tendencias en aquellas esferas priorizadas, en el ámbito externo a una organización, con el objetivo de obtener conocimientos y elaborar recomendaciones para apoyar la adopción de decisiones a los diferentes niveles" (MINFAR, 2007).

En sentido general la vigilancia tecnológica en Cuba se ha extendido, a partir de la implementación de los Lineamientos de la Política Económica y Social del Partido y la Revolución, donde específicamente el lineamiento 228 plantea: la necesidad de fortalecer las

Mignogna (1997)	Sánchez y Palop (2002)	Morcillo (2003)	Porter et al. (2005, 2009)	Nossella et al. (2008)	Vázquez (2009)	MOVTUP (2013)
Planea e hipótesis	Planea/ Identifica necesidades FCV	Problema y objetivos	Define FCV Identifica recurso información/ Define plan de VT		Identifica problemas, factores críticos competitivos y tecnológicos	Diagnóstico de la situación de la VT/ Identificación de las necesidades, medios y fuentes de acceso a la información
Recopilación interna-externa	Búsqueda y Captura	Fuentes de información / Búsqueda de información	Búsqueda y Captación	Colección de datos	Identifica/ selecciona información / Busca información	Búsqueda, tratamiento y validación de la información
Evaluación/ Validación	Analiza y organiza/ Trata y Almacena	Análisis de información / Valida información	Tratamiento y Análisis	Análisis de datos	Analiza información	Puesta en valor de la información
	Inteligencia/ estrategia	Informe de inteligencia	Valida/ Explota	Organiza / Propósito/ Implementa	Inteligencia Competitiva	Elaboración del producto de VT
Diseminación	Comunica a directivos, difunde/ transfiere conocimiento	Organiza Información, difunde		Difunde la información	Distribuye resultados	Distribución de la información
Toma de decisión		Toma de decisión				Retroalimentación y mejora de los servicios

Tabla 1. Principales modelos y procesos de vigilancia e inteligencia

capacidades de prospección y vigilancia tecnológica y la política de protección de la propiedad industrial en Cuba y en los principales mercados externos (PCC, 2011).

De ahí que otros OACE en los cuales se ha identificado el desarrollo de esta actividad son el Ministerio de Educación Superior, el Ministerio de Energía y Minas, el Ministerio de Salud Pública, entre otros. Sin embargo, un elemento que dificulta la implementación de Sistemas de Vigilancia Tecnológica, es la no actualización de la Política Nacional de Información que oriente adecuadamente el desarrollo de esta actividad en el país.

Características del Sistema de Vigilancia Tecnológica implementado en el Ministerio de Comunicaciones. Propuesta de mejora

Como parte de la implementación de los cambios funcionales y estructurales que se desarrollan en el Ministerio de Comunicaciones, relacionados con las transformaciones del modelo económico cubano, se extinguió la unidad presupuestada: Consultoría de Información del Ministerio de la Informática y las Comunicaciones, Delfos, trasfiriendo sus funciones metodológicas a la Dirección de Gestión de Información del MINCOM.

En este contexto de cambio no ha sido posible continuar con el trabajo de los núcleos del SVT, que coordinaba la consultoría, debido a que muchas de las entidades a las que pertenecían los expertos y núcleos del sistema pasaron a ser atendidos por otros ministerios, a lo que se suma la separación de funciones estatales y empresariales llevada a cabo por los OACE y la creación de las OSDE (Organización Superior de Dirección Empresarial). Esto indica que las formas de integración establecidas en su momento para la vigilancia tecnológica no se mantienen vigentes y por ende deben ser actualizadas.

El Sistema de Vigilancia Tecnológica del Ministerio de Comunicaciones, en lo adelante SVT-MINCOM, se rige por la Resolución 152/2010 del Ministerio de Informática y Comunicaciones, Reglamento del Sistema de Vigilancia Tecnológica del Ministerio de Comunicaciones, en el cual se establece la estrategia del sistema, sus funciones, la estructura, así como las interrelaciones entre sus componentes.

Este sistema se desarrolla en el sector de las telecomunicaciones, las tecnologías de la información y la comunicación, y los servicios postales, con el objetivo de apoyar los procesos de decisiones del MINCOM, con información pertinente del entorno. Se concibe como un sistema abierto, flexible y adaptable a las características y modificaciones que en el mismo se realicen.

En este sentido, los servicios de información que brinda el SVT-MINCOM varían en su complejidad, en dependencia de las necesidades de los directivos y especialistas del MINCOM para el desarrollo de sus funciones, fundamentalmente en el desarrollo de estrategias y políticas públicas. Estos se clasifican en: *Alertas Tecnológicas, Boletines*, *Perfiles estratégicos*, *Estudios de Tendencia*, entre otros.

Sobre las funciones del SVT-MINCOM

Las líneas de trabajo establecidas a partir de las funciones del SVT cuentan con una vigencia práctica en el Ministerio. Sin embargo, se advierte que en la mayoría de los casos hacen referencia como punto focal a la identificación de riesgos y amenazas generados por el uso indebido o la introducción de tecnologías que atentan contra la seguridad nacional.

Si bien es cierto que la ciberseguridad se ha convertido en uno de los elementos de mayor relevancia en el ámbito de las TIC, el cual debe ir aparejado al proceso de informatización de la sociedad cubana; se considera que funcionamiento del SVT del MINCOM debe contemplar elementos propios de este sistema que garanticen la articulación de sus procesos así como la interrelación sinérgica de sus componentes.

Con lo cual se propone incorporar las siguientes funciones:

1. Identificar de manera sistemática las necesidades de información de los especialistas y decisores del MINCOM.
2. Difundir los resultados obtenidos del ejercicio de la vigilancia tecnológica a los distintos niveles de dirección, a los especialistas del MINCOM y a otras organizaciones, según corresponda.
3. Garantizar los recursos de información especializados para el uso de los decisores y para el propio desarrollo de la vigilancia tecnológica.
4. Incorporar expertos y organizaciones colaboradoras del sector de las comunicaciones, al Sistema de Vigilancia Tecnológica del MINCOM.
5. Propiciar el intercambio de experiencia y conocimiento entre decisores, expertos, colaboradores y especialistas que desarrollan la actividad de vigilancia tecnológica, a partir de información actualizada sobre las tecnologías estratégicas en el ámbito nacional e internacional.

Sobre la estructura de SVT-MINCOM

La estructura del SVT vigente comprende un grupo de actores tanto del ámbito presupuestado como empresarial, elemento que no se corresponde con el proceso de separación de funciones llevado a cabo en los OACE.

Según se muestra en la siguiente Figura 1 de la Resolución 152/2010 del MINCON, el sistema está integrado por diferentes componentes, como son: Coordinadores, Decisores, Asesores Estratégicos, Núcleos de Vigilancia Tecnológica y el Grupo de Gestión Tecnológica.

Esta estructura no se corresponde con los cambios estructurales y funcionales del Ministerio, por los que se propone eliminar a los Asesores Estratégicos, pasando las funciones fundamentales a la categoría de experto. Al mismo tiempo, se valora eliminar el grupo Gestión Tecnológica, debido a que

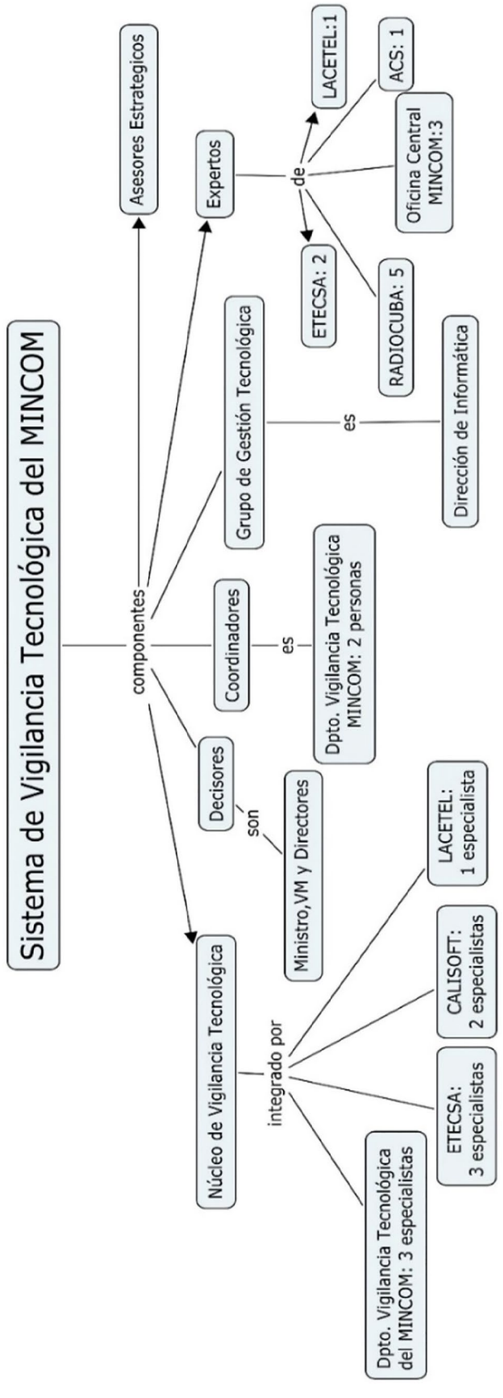


Figura 1. Estructura del SVT-MINCOM

sus funciones se garantizan desde el Centro de Comunicaciones del órgano central, que brinda soporte tecnológico al desarrollo de las funciones de las diferentes áreas del Ministerio. Con lo cual, se mantienen como actores del SVT-MINCOM a los Coordinadores, los Decisores, el Núcleo de Vigilancia y los Expertos.

Al respecto, el Artículo 15 del Reglamento Orgánico del Ministerio de Comunicaciones, establece las entidades adscritas al organismo, por lo que se considera que Núcleos de VT correspondientes a Lacetel y Calisoft, de conjunto con la OSRI, la UPTCER y Joven Club, deben construir subsistemas del SVT-MINCOM, donde los factores críticos estén relacionados directamente con el objeto social de estas entidades. (Véase Figura 2)

Cada uno de estos subsistemas se concibe atendiendo a la misión y características propias de las organizaciones que lo coordinan. Igualmente, los vínculos entre estos se consolidan a partir de la definición clara de los objetivos y el intercambio de los resultados del ejercicio de la vigilancia tecnológica.

Por otra parte, con la entrada en vigor en abril de 2018 del Decreto Ley 336/2017 del Consejo de Ministros, sobre las organizaciones superiores de dirección empresarial, se refuerzan las relaciones de atención del Ministro de Comunicaciones con las OSDE de Informática y Comunicaciones (GEIC), el Grupo Empresarial Correos de Cuba (GECC) y la empresa con tratamiento especial ETECSA. En este sentido, se propone que los Núcleos de ETECSA y la empresa perteneciente al GEIC no constituyan Núcleos del SVT-MINCOM. (Véase Figura 3)

Es decir, ETECSA y las OSDE atendidas por el Ministro de Comunicaciones contarán con sus sistemas independientes de VT, los cuales serán conducidos metodológicamente por el Ministerio, desde la Dirección de Gestión de Información.

Estos sistemas podrán fungir como colaboradores eventuales del SVT-MINCOM, teniendo en cuenta que su objeto social está estrechamente relacionado con el desarrollo de la Informática, las Telecomunicaciones y los Servicios Postales, los cuales constituyen temáticas de atención rectora del Ministerio.

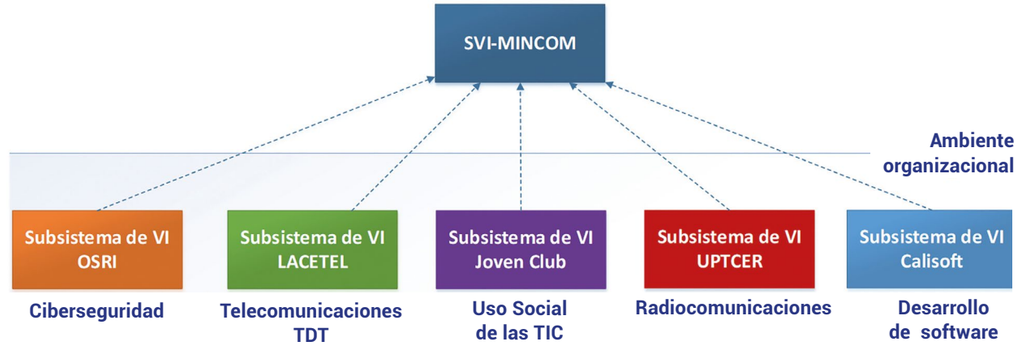


Figura 2. Definición de los subsistemas del SVT-MINCOM

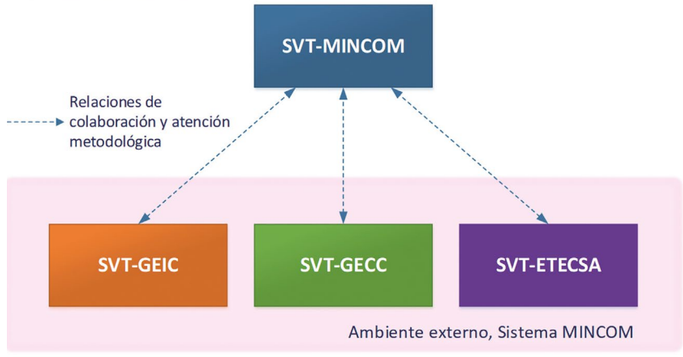


Figura 3. Relación entre los Sistemas de VT de las OSDE y el SVT-MINCOM

Conclusiones

A partir de la revisión de la literatura, se identifica que existen diferentes interpretaciones teóricas y académicas en relación con la Vigilancia Tecnológica, así como su relación con la Inteligencia Competitiva, Empresarial y Estratégica, entendida por muchos autores como procesos similares, que se distinguen por los niveles de análisis y valor agregado en los resultados.

El diseño de un SVT está condicionado por las características propias de cada organización. Es este sentido, no existe un modelo global para su implementación, aunque se percibe una tendencia en Cuba al diseño de SVT basados en la norma española UNE 166006:2006 y 2011 ajustada a las particularidades de las instituciones.

Se identifica que la mayoría de los referentes teóricos consultados, están enfocados al ámbito empresarial y científico, y en menor medida a las organizaciones gubernamentales.

La implementación de SVT se ha convertido en una herramienta de apoyo a la toma de decisiones estratégica en los OACE. Sin embargo, no constituye una práctica generalizada en todos los sectores.

El MINCOM dispone de un SVT implementado, que requiere de rediseño, debido a los resultados del proceso de perfeccionamiento estructural y funcional que atraviesa el organismo.

Recomendaciones

Desplegar estrategias nacionales que fortalezcan y generalicen la práctica de Vigilancia Tecnológica en Cuba.

Rediseñar el SVT-MINCOM en correspondencia con el perfeccionamiento del Ministerio de Comunicaciones.

Actualizar las normas y procedimientos de vigilancia tecnológica, que conducen el proceso de VT en el Ministerio de Comunicaciones.

Referencias

AENOR (2006-2011) *UNE 166006:2006 EX: Gestión de la I+D+i: Sistema de Vigilancia.* Madrid, España: AENOR

AENOR (2018) *Gestión de la I+D+i: Sistema de vigilancia e inteligencia.* Madrid, España: AENOR

Berges, A., Meneses, J. y Martínez, J. (2016) Metodología para evaluar funciones y productos de Vigilancia Tecnológica e Inteligencia Competitiva (VT/IC) y su implementación a través de la Web. El profesional de la Información, Vol. 25. Recuperado el 28 de mayo de 2019. Disponible en: https://recyt.fecyt.es/index.php/EPI/article/view/epi.2016.ene.10/25853

Castellanos, A. L. (2006). *Valoración, selección y pertinencia de herramientas de software utilizadas en vigilancia tecnológica*. Recuperado el 15 de julio de 2016, de: http://www.redalyc.org/articulo.oa?id=64326111

Castellanos, O., Torres, L & Jiménez, C. (2010) Valoración de los sistemas de inteligencia tecnológica. Ingeniería e Investigación, Vol 30, No.3. Recuperado el 14 de noviembre de 2019, Disponible en: https://revistas.unal.edu.co/index.php/ingeinv/rt/printerFriendly/18182/34013

Delgado, M. (2011). *Vigilancia tecnológica en una Universidad de Ciencias Técnicas*. Ingeniería Industrial, No.32

Escorsa, P (2014) *La Inteligencia Competitiva: factor clave para la toma de decisiones estratégicas en las organizaciones.* INTEC No.35, 11-12.

García, L. (2019) *Acercamiento a la Inteligencia Competitiva.* CRÍTICA.CL. Disponible en: https://critica.cl/otro/acercamiento-a-la-inteligencia-competitiva

Lesca, H. (1994). *Veille stratégique pour le management stratégique. État de la question et axes de recherche*. Paris: Economie Soc.

MINFAR (2007) *Indicaciones 308 sobre la Vigilancia Tecnológica del MINFAR*. La Habana

Moyares, Y., Infante, B. y Rodríguez, Y. (2018) *Diseño de un sistema de Vigilancia Tecnológica con la integración de tecnologías de la Web 2.0 en un observatorio tecnológico para un centro de desarrollo de software.* Revista Cubana de Información en Ciencias de la Salud. Vol.29, No.1 (2018), La Habana

Orozco, A. (2009). *Inteligencia empresarial: Qué y Cómo*. La Habana: IDICT.

Palop, F., y Vicente, J. M. (1999). *Vigilancia tecnológica e Inteligencia competitiva. Su potencial para la empresa española.* Madrid: Pearson Educación

PCC. (2011). Lineamientos de la Política Económica y Social del Partido y la Revolución. Recuperado el 14 de noviembre de 2019, Disponible en: http://www.granma.cubaweb.cu/secciones/6to-congreso-pcc/Folleto Lineamientos VI Cong.pdf

Pérez, N. 2019 Vigilancia Tecnológica e Inteligencia estratégica. Nuevas herramientas estratégicas para la gestión tecnológica y la innovación. CONCYTEC. Recuperado el 28 de mayo de 2019. Disponible en: https://portal.concytec.gob.pe/index.php/noticias/1753-vigilancia-tecnologica-e-inteligencia-estrategica-herramientas-claves-para-innovar

San Juan, Y y Romero, F. (2016) *Modelos y herramientas para la vigilancia tecnológica.* Ciencias de la información. Recuperado el 20 de agosto de 2019. Disponible en: www.researchgate.net/publication/32144299_Modelos_y_herramientas_para_la_vogilancia_tecnologica

SCIP (2019) *The SCIP Code of Ethics*. Recuperado el 15 de julio de 2019. Disponible en: www.scip.org/page/Ethic-Intelligence

Tur, L. (2010) *Propuesta estratégica para el análisis de información a partir de la Vigilancia Tecnológica. Estudio de caso.* Tesis de Licenciatura. Facultad de Comunicación. Universidad de la Habana.

NORMAS PARA LOS COLABORADORES

En la Revista Científico Técnica Tono**,** los especialistas y técnicos, tienen la posibilidad de publicar, luego de un riguroso proceso de revisión, artículos con información de contenido novedoso en ciencia y tecnología, con temas como la Electrónica, las Telecomunicaciones, la Informática, así como temas relacionados con la Empresa Moderna.

Los trabajos deben ser originales e inéditos y su envío a publicación supone el compromiso del autor de no someterlo a consideración de otras publicaciones. Deberán estar siempre en formato digital y se harán llegar directamente a la Dirección de Información y Vigilancia Estratégica remitidos a la Lic. Alena Bastos Baños, Editora ejecutiva de la publicación, a través del correo electrónico (tono@etecsa.cu/alena.bastos@etecsa.cu) o personalmente en cualquier dispositivo de almacenamiento.

Serán publicados, siempre que hayan sido aprobados por el Consejo Editorial de la Revista Científico Técnica Tono, los trabajos que se encuentren dentro del marco de la siguiente tipología:

Artículos de investigación: Comprende trabajos de Investigación, Desarrollo, Producción, y Servicios técnicos. Tienen por finalidad dar a conocer una contribución original de conocimientos empíricos al entendimiento teórico-práctico de una materia, al desarrollo investigativo de la misma o su aplicación, ya sea en el campo científico-técnico o docente. Tendrá una extensión de 10 a 15 cuartillas incluida la bibliografía y los anexos. Este tipo de contribución se somete a revisión por pares a doble ciego.

Artículos de revisión: Revisión bibliográfica, con valoración incluida sobre un tema dado. Puede abarcar períodos de tiempo largos o remitirse al estado actual en que se encuentra un tema en específico. Estará comprendida entre las 15 y 25 cuartillas sin contar bibliografía (que deberán ser más de 50 entradas bibliográficas) y anexos. Aunque existen dos modalidades: revisión descriptiva y revisión crítica, Tono solo aceptará la segunda, que implica una evaluación o valoración exhaustiva del aspecto tratado. Este tipo de contribución generalmente será realizado por un especialista de un tema dado a petición del Consejo Editorial y será sometida a revisión por pares a doble ciego.

Informe científico técnico: Documento que describe el proceso o los resultados de una investigación científica o técnica, o el estado del arte de un problema de esta índole. Generalmente forma parte de una serie de documentos numerados. Tendrá una extensión de más de 5 a 10 cuartillas incluida la bibliografía y los anexos. Se someterá a revisión por pares a doble ciego.

Estudios de casos: Son trabajos destinados a valorar experiencias, investigaciones, innovaciones, situaciones y resultados, ya sea de tipo científico, técnico, así como su tratamiento metodológico. Tono solo aceptará las modalidades de *Situación valoración* (Análisis y evaluación) y *Situación problema* (Descripción, análisis, esencia y causas, evaluación y toma de decisiones). Tendrá una extensión de 5 a 10 cuartillas y será sometido solo a revisión editorial.

Cartas al Editor: Cualquier tipo de comentario sobre la revista, temas de actualidad, eventos, cursos, etc., dirigidas al editor. Establecen un foro de opiniones e interpretaciones sobre tópicos nuevos en un campo específico. Deben ser revisadas por el Consejo Editorial con el fin de precisar el grado de interés para los lectores de la publicación. Es el canal de comunicación entre el equipo y los lectores, y su principal sistema de retroalimentación. Tendrán un máximo de 3 cuartillas.

Se entregará al autor(es) y coautor(es) un documento acreditativo de la publicación del trabajo.

NORMAS DE PRESENTACIÓN

Los trabajos que aspiren a ser publicados en Tono deberán prepararse utilizando el procesador de texto Microsoft Word. Los ficheros resultantes deberán tener por nombre el mismo título del trabajo y se presentarán a una sola columna dentro de los márgenes establecidos (tamaño de papel Carta, márgenes superior 3.0cm, inferior 2.0cm e izquierdo y derecho 2.5cm). No se deberá imprimir ningún marco alrededor del texto.

El tipo de letra a utilizar para el cuerpo del trabajo será Arial 11pt. y renglones con interlineado 1.15.

En el caso del Título y los subtítulos se utilizará Arial 12 en Negritas y Arial 11 en Negritas, respectivamente.

Las figuras deben ser de buena calidad y junto con las tablas deben estar intercaladas en el texto. En el caso de que por la calidad de las imágenes o por la cantidad utilizada dentro del texto el trabajo exceda los 15 Mb, se deberá entonces enviar las imágenes en una carpeta aparte, identificadas y numeradas en forma consecutiva, con el pie correspondiente, en ese caso también el autor deberá indicar dentro del texto (entre paréntesis) dónde debe colocarse cada imagen. Para las imágenes se utilizarán los formatos: JPG, TIFF, BMP en 300 DPI. En todos los caso se deberá indicar la procedencia de las fotos.

Los Pies de imagen o figura llevarán por formato Arial 9 y se representarán de la siguiente forma: **Figura 1. / Fig. 1.** Pie de figura.

Deben ser declaradas convenientemente toda la nomenclatura de los símbolos empleados y las unidades correspondientes.

Es obligatorio el uso del Sistema Internacional de Unidades.

La extensión de los trabajos dependerá del tipo de documento que se presente. Los artículos de reseña, investigación y revisión no deben exceder las 10, 15 y 20 cuartillas respectivamente, **incluida bibliografía y anexos**, las comunicaciones cortas deben comprender entre 2 y 5 cuartillas y para las cartas al editor solo se admitirá hasta un máximo de 3 cuartillas.

Las notas al pie de página deben quedar distribuidas a lo largo del texto, estas no deben ocupar más de la tercera parte de la página y si se excedieran han de continuar en la página siguiente, siempre deben identificarse con un número en el texto que remita al lector al inferior de la página. En cada página se permitirán solamente hasta tres notas.

La Dirección de Información y Vigilancia Estratégica devolverá a sus respectivos autores los trabajos que no cumplan los requisitos de presentación antes establecidos.

Si los trabajos son aprobados con modificaciones, estos deberán ser reenviados con la señalización REV. en el nombre del fichero (Ejemplo: REV. Propuesta para la mejora…).

Trabajos con estructuras establecidas. Organización de la información

Artículos de investigación

Título y autores

En la primera página del artículo debe escribirse el título. Este deberá reflejar de manera clara y directa el contenido del artículo, ofrecerá la mayor cantidad de información específica con el mínimo de palabras, por lo que no debe exceder las 15 palabras y deben evitarse las abreviaturas a menos que estas sean muy reconocidas en el área específica que se piensa publicar.

Luego del Título deben presentarse los nombres de los autores organizados por: título académico, nombres completos y los apellidos (unidos por guión) alineados a la izquierda, con tipografía Arial 11pt.; sus filiaciones, cargo actual y correos electrónicos serán identificados apropiadamente con superíndices.

Ejemplo:

Autor(es):

Dr. Juan Alberto Pérez-García[1]

Lic. Claudia Pomares-Rodríguez[2]

[1] Empresa de Telecomunicaciones de Cuba S.A.; Especialista B en Telemática; Cuba. juan.perez@etecsa.cu

[2] Empresa de Telecomunicaciones de Cuba S.A.; claudia@etecsa.cu

Nota: *El autor principal lo define: grado de responsabilidad y contenido (más de 50%) y no el título académico.*

Resumen

De los diferentes tipos de resúmenes existentes, para esta revista se requiere el Indicativo, que consiste en una breve y exacta representación del contenido del trabajo. Debe tener entre 200-250 palabras y no debe contener referencias ni fórmulas. El contenido debe incluir los aspectos más importantes: propósitos del estudio o investigación, aportes, métodos y procedimientos básicos, resultados significativos y conclusiones; no debe incluir informaciones que no sean analizadas y discutidas en el artículo.

Palabras Clave

Reflejan la esencia del trabajo, los términos más empleados en la especialidad o los conceptos más relevantes. Deben utilizarse entre 4 y 8 palabras o frases cortas, organizadas por orden de prioridad, que ayudarán a clasificar el artículo para su futura recuperación. Deben estar en ALTAS separadas por punto y coma (;) y con Arial 11 pt.

Introducción

Será el primer acápite del artículo. En este momento debe precisarse ¿por qué y para qué la investigación o estudio? Se deben exponer los antecedentes, hipótesis y sistema de objetivos. Debe presentarse el propósito del artículo y resumir el fundamento lógico del estudio u observación; además debe hacer una mención breve sobre la metodología usada y el ámbito del estudio (local, nacional o internacional). Una página es suficiente para esta parte.

Materiales y métodos

Deben definirse ¿cómo y con qué se realizó la investigación o el estudio?; procedimientos estadísticos, diseño, evaluación de la información y de los datos. Esta parte del artículo debe dar respuesta a las siguientes interrogantes: ¿qué se estudió?, ¿cuándo se estudió?, ¿dónde se estudió?, ¿cuál método?, ¿cómo se estudió? Deberán escribirse correctamente las palabras técnicas, los términos específicos del tema y los nombres científicos de plantas, animales, microorganismos y otros.

Resultados

Deben ser breves y claros; dar respuesta a las interrogantes e hipótesis, siguiendo una secuencia lógica, así como aportar nuevas evidencias. Debe transitarse de lo desconocido a lo conocido y seleccionarse los resultados realmente significativos. Deben descartarse los hallazgos secundarios y destacarse o resumirse solo las observaciones importantes. Los gráficos y las tablas sirven de apoyo siempre que no repitan los datos expuestos en el texto.

Discusión

Es la parte donde deben ser analizados e interpretados los resultados, su significado, logros y limitaciones, además deben resaltarse los aspectos novedosos del estudio, sus aplicaciones prácticas y las conclusiones que se derivan de ellos. De ser necesario, en este apartado deben ser delimitados los aspectos no resueltos y los límites de las aplicaciones de los resultados. Si es necesario, además, se pueden proponer recomendaciones derivadas de los propios resultados que se presentan en el trabajo teniendo siempre en cuenta la diferencia entre las ideas que son apoyadas por los experimentos ya realizados (evidencia concreta) y las preguntas que podrían ser contestadas con experimentos aún por realizar (especulación).

Conclusiones

En este apartado deben exponerse las consecuencias de los resultados y establecerse el nexo de estas con los objetivos de la investigación o estudio. Deben evitarse las generalizaciones y verdades absolutas, así como extraer conclusiones que no se encuentren lo suficientemente respaldadas por los datos.

Recomendaciones

De ser necesario, se propondrán nuevas hipótesis o aspectos que sean objeto de ulterior investigación.

Bibliografía

Para la presentación tanto de las citas contextuales (o sea dentro del texto), como de la bibliografía utilizada para la conformación del artículo, debe emplearse el Estilo Bibliográfico APA de 5th Edición en adelante.

Libros

Apellidos, A. A. (Año). *Título*. Ciudad: Editorial.

Apellidos, A. A. (Año). *Título*. Recuperado de http://www.xxxxxx.xxx

Apellidos, A. A. (Ed.). (Año). *Título*. Ciudad: Editorial.

Formas básicas para un capítulo de un libro o entrada en una obra de referencia

Apellidos, A. A. y Apellidos, B. B. (Año). Título del capítulo o la entrada. En Apellidos, A.B. (Ed.), *Título del libro* (pp. xx-xx). Ciudad: Editorial.

Apellidos, A. A. y Apellidos, B. B. (Año). Título del capítulo o entrada. En Apellidos, A. A. (Ed.), *Título del libro* (pp. xx-xx). Ciudad: Editorial. Recuperado de http://www.xxxxxx

Publicaciones periódicas

Apellidos, A. A., Apellidos, B. B. y Apellidos, C. C. (Fecha). Título del artículo.

Título de la publicación, volumen(número), pp. xx-xx. doi: xx.xxxxxxx

Informe técnico

Apellidos, A. A. (Año). *Título*. (Informe Núm. xxx). Ciudad: Editorial.

Tesis

Apellidos, A. A. (Año). *Título*. (Tesis inédita de -especificar grado por el que se opta-). Nombre de la institución, Localización.

Leyes

Nombre de la ley, Volumen Fuente § sección (Año)

Sitios o páginas web

Nombre oficial del sitio web.Dirección electrónica. (acceso mes día, año).

[16] IEC. http:// webstore.iec.ch/ webstore/ webstore.nsf/ artnum/000022 (acceso diciembre 5, 2009).

Cita de un trabajo realizado por un autor, el cual no ha sido leído directamente, sino en una fuente secundaria (Cita de citas)

Se coloca dentro del texto el(los) apellidos del autor(es) original del trabajo, seguido de la información entre paréntesis: año del trabajo original, c.p. Apellidos de la fuente(s) secundaria, año de publicación de la fuente secundaria.

Ejemplos:

- Santisteban (1993, c.p. Santalla y Cañoto, 1994)...
- (Santisteban, 1993 c.p. Santalla y Cañoto, 1994).

tono
Revista Técnica de la Empresa de Telecomunicaciones de Cuba S.A.

Declaración de originalidad del trabajo escrito

Título del artículo

_____

_____

Mediante esta comunicación, certifico que el artículo enviado para posible publicación en la revista técnica *Tono*, es de mi entera autoría debido a que sus contenidos son producto de mi directa y auténtica contribución intelectual. Además, este trabajo es una investigación inédita, es decir, que no ha sido postulado a otro espacio de difusión —revistas o como partes de capítulo de libro, entre otros—.

Los datos y referencias a la literatura especializada ya publicados están debidamente identificados con su respectivo crédito e incluidos en las referencias bibliográficas al final del trabajo.

Por todo lo anterior declaro que todos los materiales presentados para posible publicación están totalmente libres de derechos de autor y, en consecuencia, me hago responsable de cualquier litigio o reclamación relacionada con Derechos de Propiedad Intelectual.

En caso de que el artículo sea seleccionado para ser publicado por la revista técnica *Tono*, manifiesto que cedo plenamente al Dirección de Información y Vigilancia Estratégica de ETECSA los derechos de reproducción, edición, distribución, exhibición y comunicación del mismo dentro y fuera del país, por medios impresos, electrónicos, CD ROM, Internet, etc., reconociendo siempre los derechos de autor correspondientes.

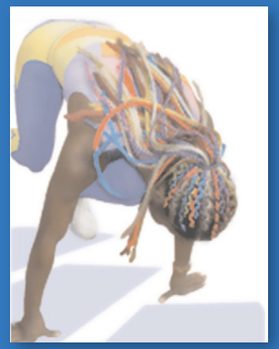
Para constancia de lo expuesto, firmo esta declaración a los _____ días, del mes de _____ del año _____, en la ciudad de _____.

Nombre y Apellidos del futuro colaborador

_____

No. Carnet de Identidad: ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Firma: _____

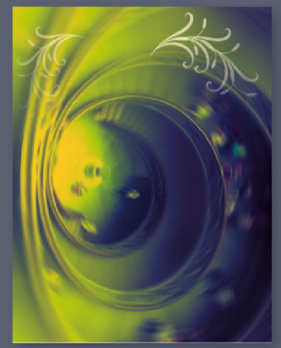


La arrancada

A la sombra de las redes en flor

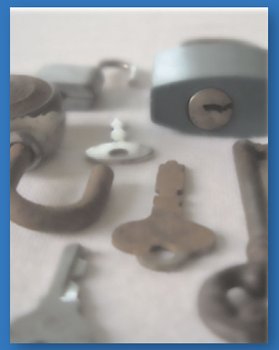
El éxtasis de la velocidad

La información como un océano...

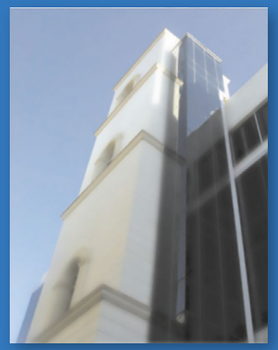


Escalera al futuro

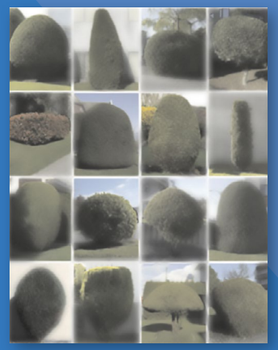
Ningún sofware es una isla



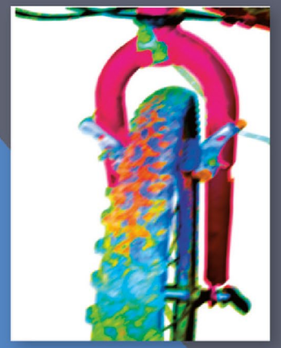
En busca de una seguridad razonable



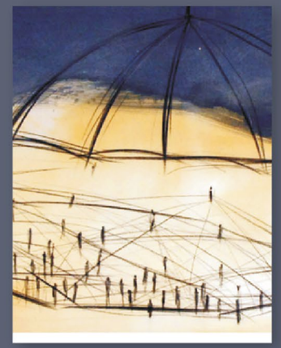
Arquitecturas convergentes



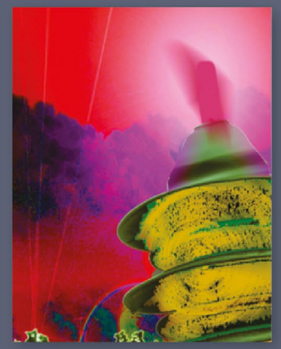
La educación regulatoria



Epur se mouve

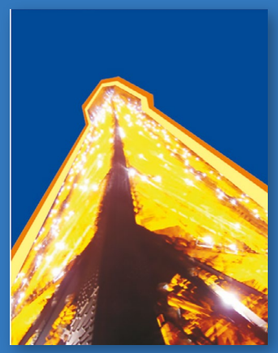


El secreto de las señales

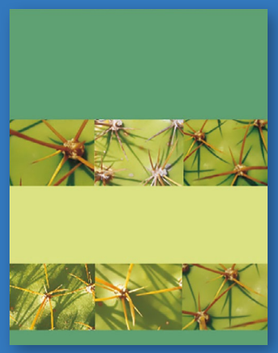


Si nunca pensamos en el futuro nunca lo tendremos

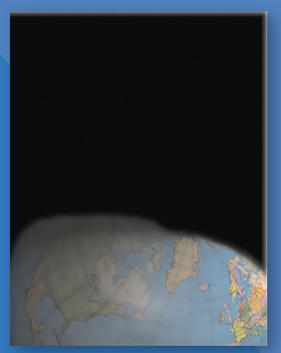
Cualquier tecnología avanzada es indistinguible de la magia



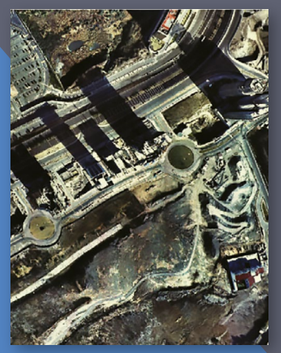
Conmovidos por el llamado de la luz



El entorno protector



En todas partes



El laberinto múltiple

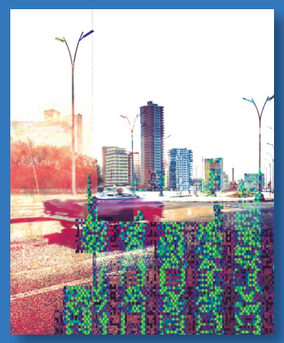
Redes sin límites

Regreso al Futuro

El futuro pertenece a quienes creen en la belleza de sus sueños

El verdadero progreso es el que pone la tecnología al alcance de todos

Todo es posible



CENTRO MULTISERVICIOS digital

Calle Obispo e/ Villegas y Aguacate

Informática 2020

XVIII CONVENCIÓN Y FERIA INTERNACIONAL

La Habana, Cuba
del 16 al 20 de marzo de 2020

POR LA TRANSFORMACIÓN DIGITAL