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.

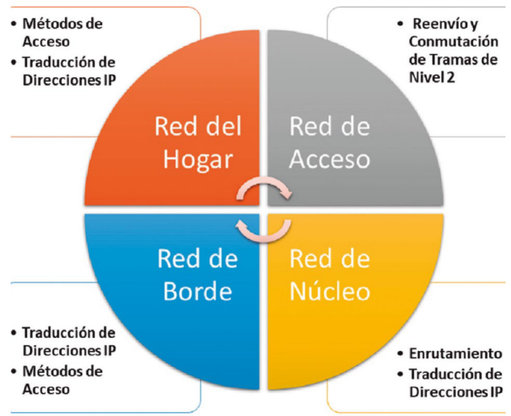

Figura 1. Modelo de Red de Datos para Servicios de Suscripción

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

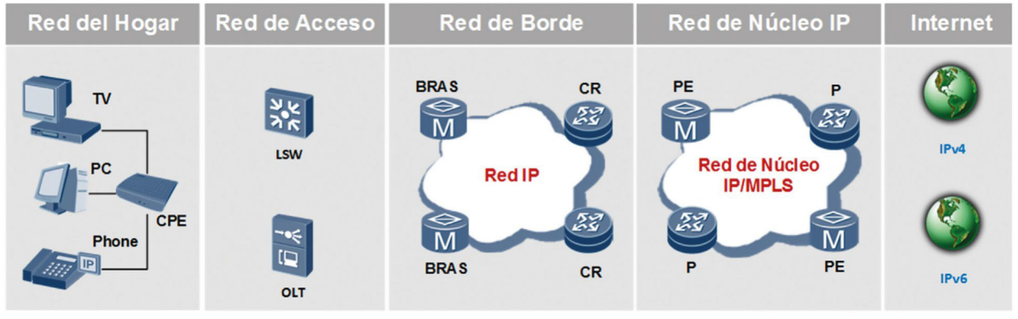

Figura 2. Red de Banda Ancha de un Operador de Telecomunicaciones Genérico

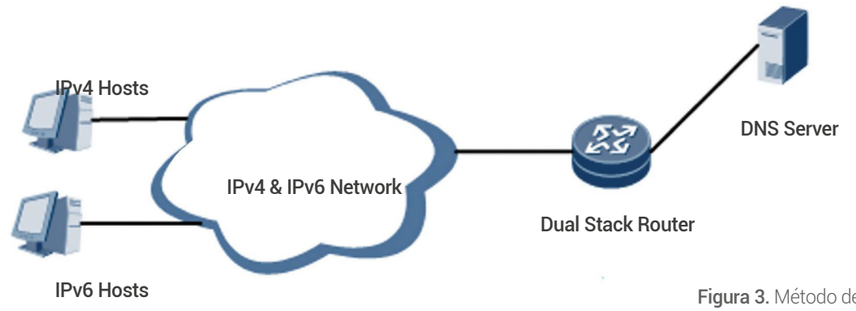

Figura 3. Método de Pila Dual

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*

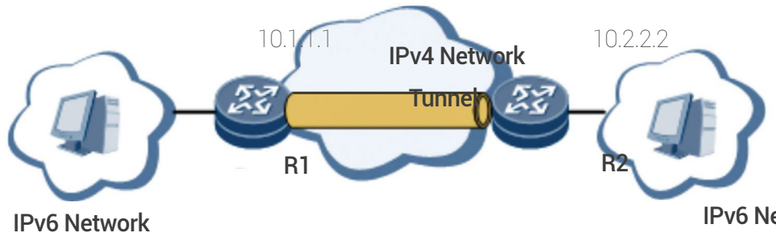

Figura 4. Método de Tunelización

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.

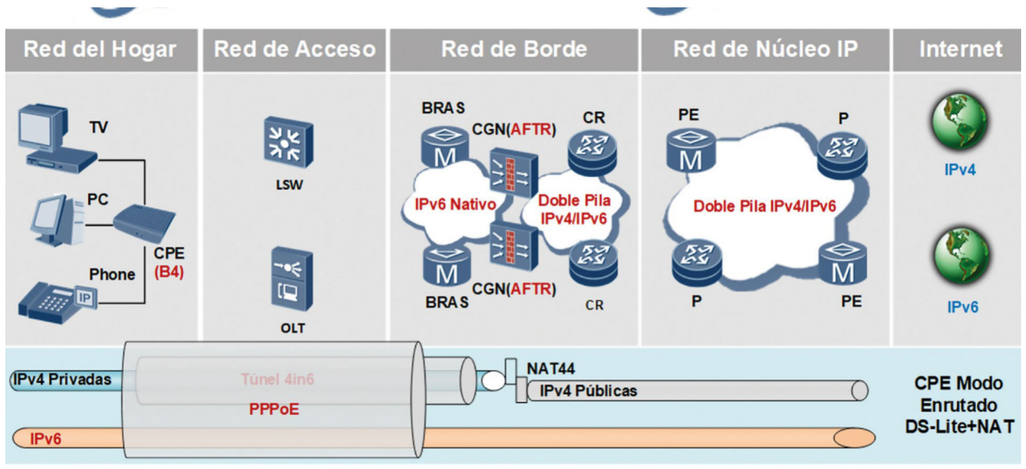

Figura 5. Mecanismo de Transición DS-Lite

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.

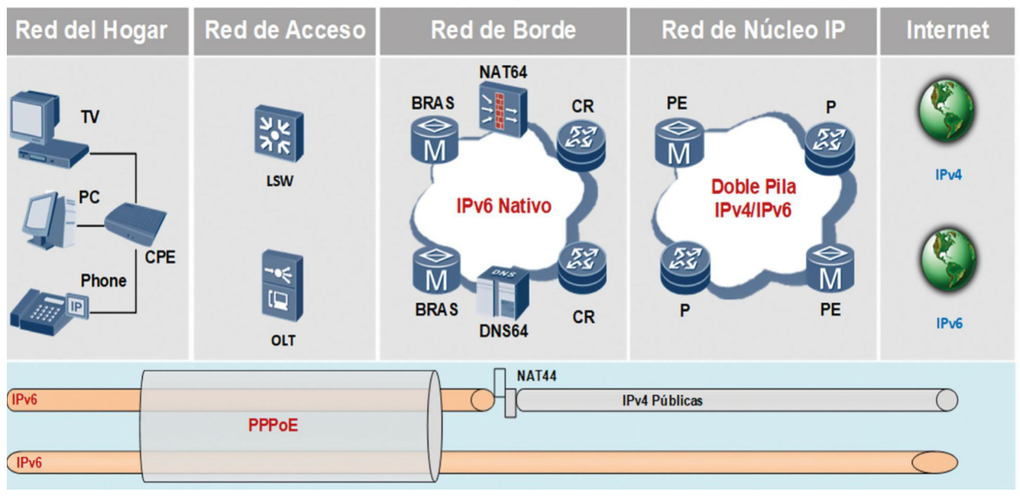

Figura 6. Técnica NAT64

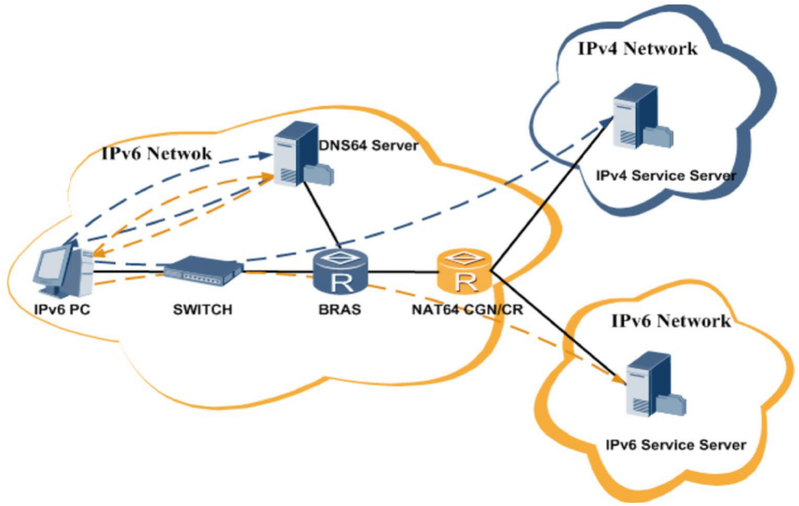

Figura 7. Principio de Operación Técnica NAT64

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

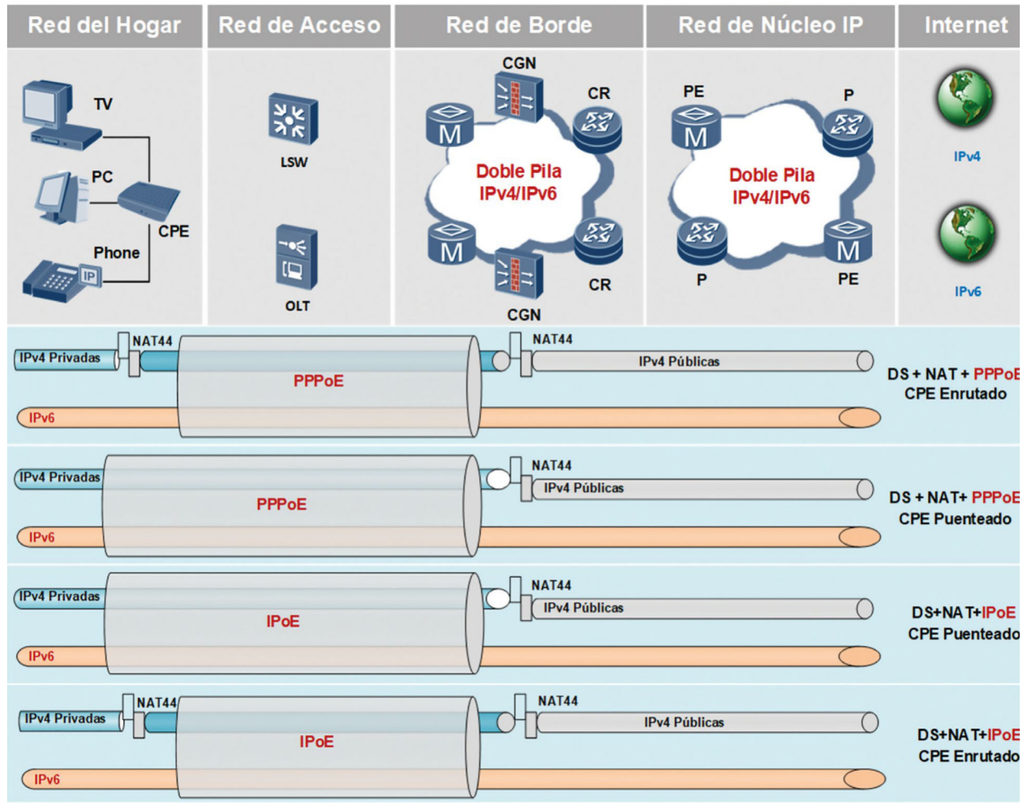

Figura 8. Técnica de Pila Dual+NAT444

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

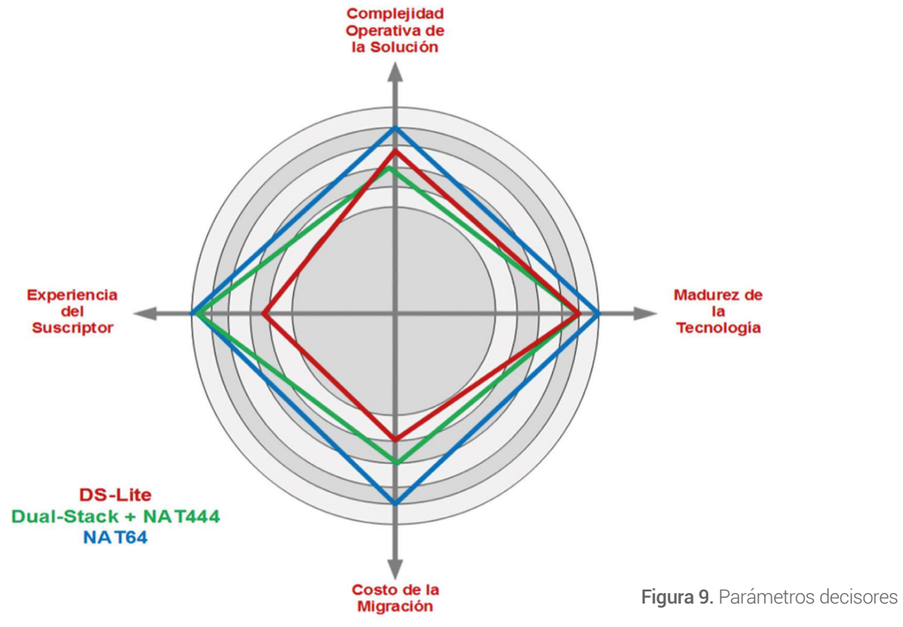

Figura 9. Parámetros decisores

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)

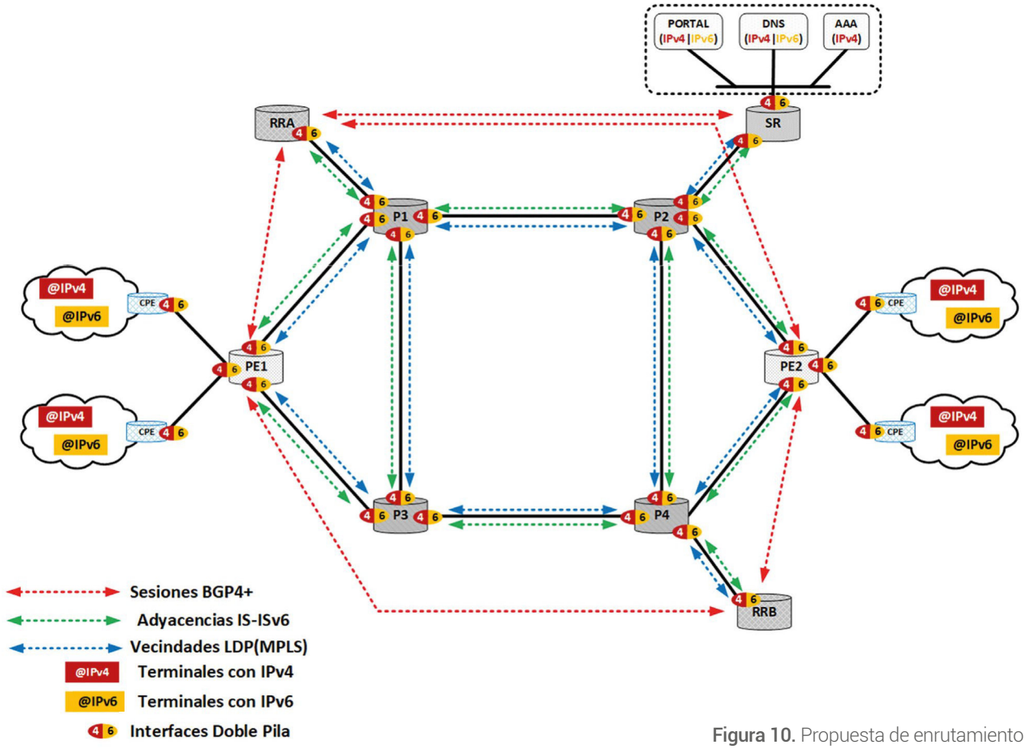

Figura 10. Propuesta de enrutamiento

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

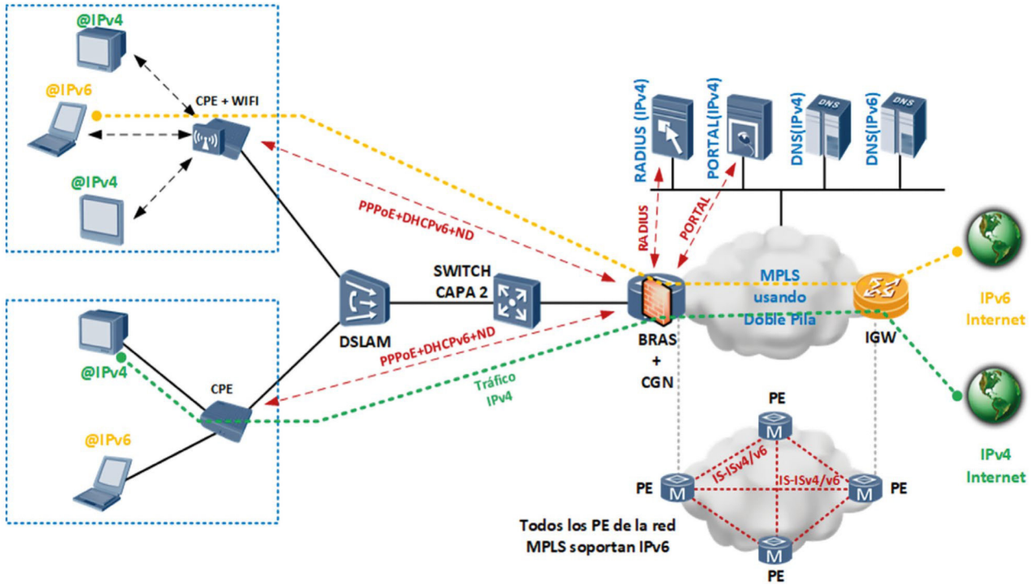

Figura 11. Interrelación entre elementos de la red

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

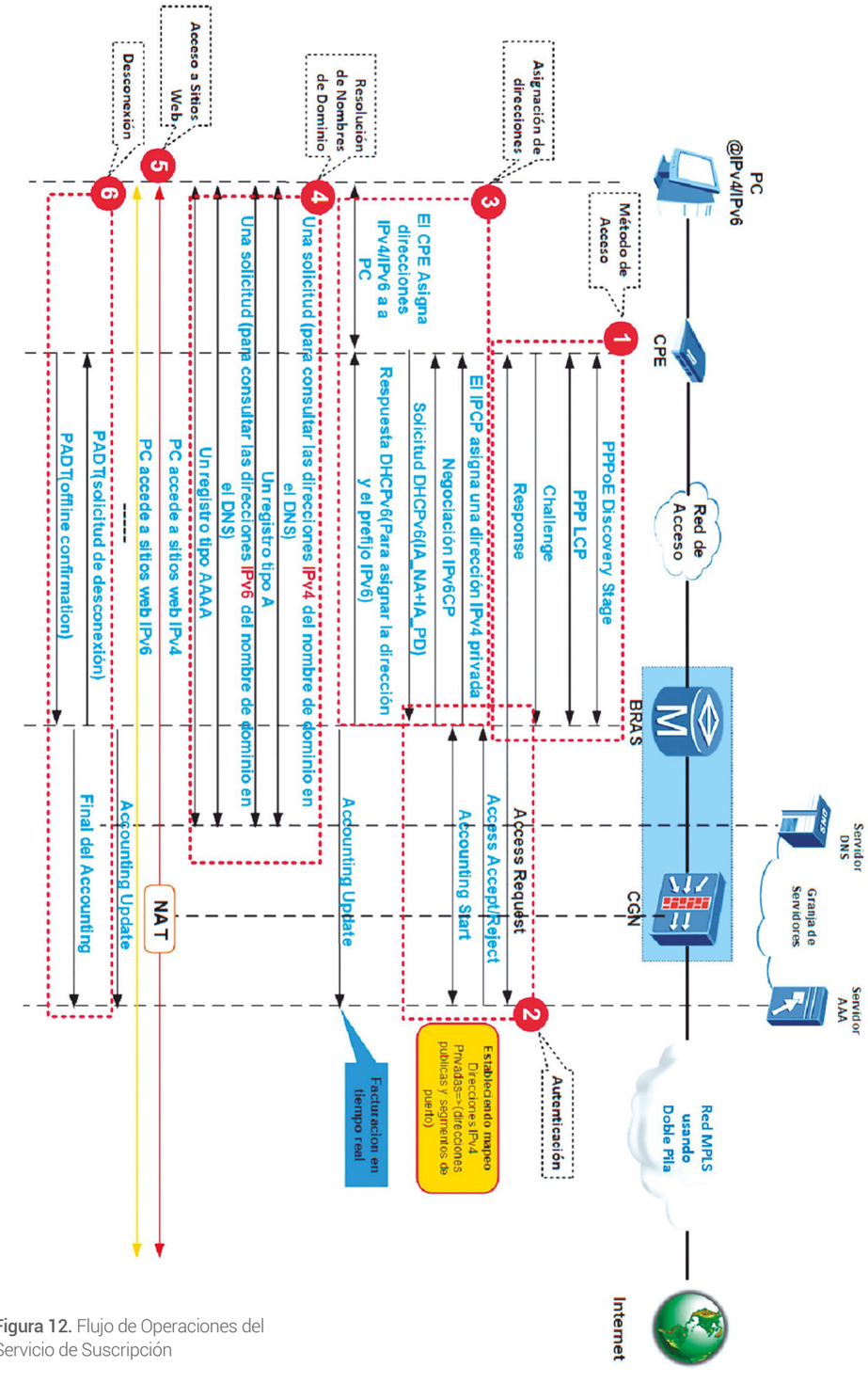

Figura 12. Flujo de Operaciones del Servicio de Suscripción

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