



PROYECTO WIFI INTEROPERABILIDAD

WIFI INTEROPERABILITY PROJECT

Elio R. Avila Rodríguez¹, Yussel Castrizano Jiménez², Eliezer Bravo Borrego³, Lesdier Duardo Liens⁴

1 ETECSA, Cuba, elio.avila@etecsa.cu, Ave. 1ro de Enero, Edif. 33, Apto. E-3, Rpto. Santos. Las Tunas

2 ETECSA, Cuba, yussel.castrizano@etecsa.cu

3 ETECSA, Cuba, eliezer.bravo@etecsa.cu

4 ETECSA, Cuba, lesdier.duardo@etecsa.cu

RESUMEN: *Entre los primeros servicios de Internet en nuestro país se encuentra el acceso WiFi en instalaciones hoteleras, aeropuertos y otros centros de servicios varios. En sus inicios se brindaban con soluciones diversas, en dependencia de las posibilidades de acceso que disponía ETECSA como proveedor de servicios en ese momento. Con el desarrollo de la infraestructura tecnológica de esta empresa, la intención de mejorar el servicio brindado, unido a los requerimientos de seguridad que imponen estos tiempos, se hizo necesario concebir un sistema que pudiera insertar en el modelo de red convergente de ETECSA aquellas soluciones aisladas, que incluye servicios de terceros, como solución integradora, escalable y segura para la provisión de los servicios de este tipo.*

En este trabajo se recogen los aspectos generales del proyecto denominado WiFi Interoperabilidad, que define las pautas a seguir por ETECSA para brindar el acceso WiFi a Internet en aquellos sitios de terceros, que comparten o no equipamiento con este proveedor y no están comprendidos en la solución WiFi ETECSA de espacios públicos. En el trabajo se recogen los antecedentes, los escenarios implementados en la solución y los principales resultados obtenidos hasta la fecha de confección de este artículo.

Palabras Clave: WiFi, Redes Convergentes, IP/MPLS

ABSTRACT: *Among the first Internet services in our country is WiFi access in hotel facilities, airports and other miscellaneous service centers. In the beginning, they were provided with various solutions, depending on the access possibilities available to ETECSA as a service provider at the time. With the development of the technological infrastructure of this company, the intention to improve the service provided, together with the security requirements imposed by these times, it became necessary to devise a system that could insert into the convergent network model of ETECSA those isolated solutions, which includes third party services, as an integrative, scalable and secure solution for the provision of services of this type.*

In this work the general aspects of the project called WiFi Interoperability are defined, which defines the guidelines to be followed by ETECSA in order to provide WiFi Internet access in third party sites, whether or not they are equipped with this provider and are not included in the ETECSA WiFi solution for public spaces. The work includes the background, the scenarios included in the solution and the principals results obtained up to the date of preparation of this article.

KeyWords: WiFi, Converging Networks, IP/MPLS.

1. INTRODUCCIÓN

A pesar de que nuestro país aún presenta bajos índices de penetración de Internet, lo cierto es que muestra un crecimiento sostenido en esta materia. Tal es así que en el último año el uso de las redes sociales aumentó un 346%; en los dos últimos años el número de puntos colectivos de navegación pasó de 155 a mil seis, entre salas cerradas y zonas WiFi; se duplicó el ancho de banda internacional; y el conjunto de personas usuarias aumentó un 50%, pasando de tres millones en 2014 a 4,5 en 2016 [1].

En este sentido ETECSA como proveedor de servicios de telecomunicaciones tiene una alta responsabilidad, al tener un peso significativo en toda la infraestructura tecnológica que se requiere para el desarrollo de este sector. Algunos de los avances que exhibe esta empresa en los últimos años, aparejado a lo anterior, son la apertura de un Centro de Datos en el 2014, la puesta en servicio del acceso a Internet en espacios públicos de conexión inalámbrica, con la apertura del Proyecto WiFi ETECSA en julio de 2015 [2], de 35 sitios en un inicio ya cuenta con 432 de ellos [3]. Más recientemente, la llegada de Internet a las casas a través del Proyecto Nauta Hogar con tecnología ADSL, cuya prueba piloto comenzó a finales del año 2016 en La Habana, el 29 de septiembre del 2017 sumó otras 5 provincias del país (Pinar del Río, Las Tunas, Holguín, Granma y Guantánamo).

Otro de los trabajos que vio la luz este año 2017, relacionado con el acceso a Internet, fue el denominado WiFi Interoperabilidad, cuyo propósito es hacer converger a la plataforma de control y autenticación NAUTA del modelo multiservicio de ETECSA (integra los proyectos antes mencionados), aquellos servicios WiFi de terceros no comprendidos en la solución WiFi ETECSA, que incluyen hoteles, aeropuertos, centros recreativos y de servicios varios, independientemente del fabricante y modelo de los equipos que éstos dispongan. Entre sus ventajas con respecto al sistema anteriormente empleado se encuentra la mejora en la calidad del servicio brindado, que incluyen aspectos relacionados con la seguridad y supervisión del sistema de forma global, el aumento del ancho de banda por usuario, la simplificación de la forma de desconexión, la posibilidad de personalizar los portales WEB por sitios, el ahorro de recursos de red, entre otras. Desde su apertura en abril del 2017 hasta finales de septiembre del mismo año habían migrado al nuevo

escenario o instalados nuevos servicios en más de 180 instalaciones.

El presente trabajo trata sobre este último proyecto, en él se recogen los principales elementos que intervienen en la solución y está organizado de la siguiente forma: luego de esta introducción se mencionan los aspectos básicos del sistema antes empleado, los escenarios desarrollados para el sistema integrador WiFi Interoperabilidad y por último las conclusiones, referencias bibliográficas, entre otros.

2. SOLUCIÓN WIFI INTEROPERABILIDAD

2.1 Elementos comprendidos en la solución

Una red WiFi cuenta de los siguientes componentes:

1. **Estación (STA):** Terminal de acceso, tal como una laptop, tableta o teléfono móvil inteligente.
2. **Punto de acceso (AP):** Cuenta con conexiones cableadas hacia los dispositivos del Upstream y acceso inalámbrico Downstream hacia las STA. Un AP interconecta las redes alámbricas e inalámbricas.
3. **Controlador de acceso (AC):** Gestiona la autenticación de los usuarios actuando como intermediario en el proceso de autenticación entre el usuario y el servidor de Autenticación, Autorización y Contabilidad (AAA), y en la contabilidad de la cuenta del usuario enviándole al mismo constantemente paquetes de actualización sobre el estado de su cuenta. Puede gestionar y monitorear a los AP, incluyendo las configuraciones de seguridad y radio de los APs, así como trabajar como servidor DHCP en el proceso de asignación de direcciones IP a los usuarios.

Otros elementos comprendidos en la solución son:

Switch de agregación:

Este dispositivo actúa como equipo de convergencia para transmitir paquetes de manera transparente, que contienen las etiquetas de las VLANs de cliente de los usuarios. Se conecta en bajada con los equipos de acceso y en subida con el PE o BRAS.

PE (Provider Edge) Router de Borde de la red IP/MPLS:

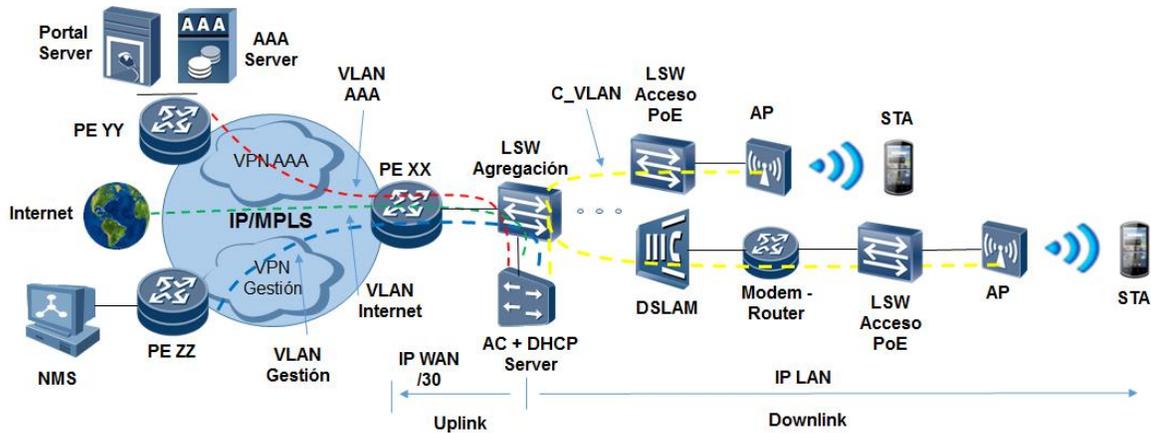


Fig. 1. Escenario típico WiFi terceros antes de la solución WiFi Interoperabilidad.

Estos equipos son los encargados de proveer los servicios de conectividad a las redes IP de los usuarios del Backbone IP/MPLS. Se encargan de las funciones PUSH/POP en la operación de etiquetas dentro de esa arquitectura.

Servidor de Acceso Remoto de Banda Ancha (Broadband Remote Acces Server, BRAS):

Este dispositivo está encargado, entre otras funciones, de terminar las sesiones IPoE implementando el control de acceso de los usuarios.

Servidor AAA:

El servidor de autenticación, autorización y contabilidad se comunica con el AC o BRAS, según sea el caso de acuerdo al escenario empleado, y realiza la funcionalidad AAA basada en el nombre de usuario y la contraseña enviada por estos equipos.

Portal Server:

El servidor portal actúa como un servidor web de autenticación para proveer autenticación web a los usuarios.

CGN:

Funcionalidad de servidor NAT, el mismo realiza la traslación de direcciones y puertos para navegación externa (IP reales), utilizando direcciones públicas o privadas.

2.2 Antecedentes

En un inicio el escenario típico implementado para el servicio WiFi de terceros se muestra en la Fig. 1, este cuenta con una arquitectura centralizada donde un Access Control (AC) (propiedad de ETECSA) gestiona los usuarios conectados a los Puntos de

Acceso (AP) de una o varias instituciones, según la capacidad del AC y los AP instalados, éstos últimos se enlazan capa 2 al AC por su Downlink, trazando convenientemente la VLAN de usuario (C_VLAN), ya sea por fibra óptica o equipos de transporte ETH/SDH hasta los switches de acceso, o por la red de cobre a través de DSLAMs. Los AP funcionan como conversores de medio, en el sentido Upstream convierten las señales de radio al protocolo Ethernet, mientras que en Downstream lo hacen a la inversa. El AC a su vez se enlaza vía Uplink al router de borde (PE) más cercano del backbone IP/MPLS, para ello utiliza 3 VLANs terminadas éstas en servicios capa 3 entre ambos equipos, los que utilizan subredes IP de enlace /30 (IP WAN). De esta forma el AC garantiza la conectividad enrutando el tráfico de los usuarios a los servidores AAA y Portal Captive para la autenticación de los usuarios, su salida a Internet una vez que ésta haya sido exitosa, o la gestión remota del AC y los APs, según sea el caso. En este escenario el AC realiza la función de servidor DHCP, de esta forma asigna automáticamente las IP LAN a los usuarios, las que por lo general son IP reales, la máscara de subred está en dependencia del número posible de usuarios concurrentes según los APs desplegados en la instalación.

Otra variante utilizada es cuando la institución contrata el servicio de Internet, y a través del despliegue de su red interna garantiza el servicio WiFi, utilizando para ello un AC u otro equipo que asuma la función de servidor DHCP, así como APs propios.

Entre las principales limitaciones de estos escenarios se encuentran:

1. Gestión engorrosa de los usuarios, que se realiza sobre los AC de forma independiente.
2. Interrupciones frecuentes por bajo desempeño de los AC propiedad de ETECSA, que provoca su bloqueo.

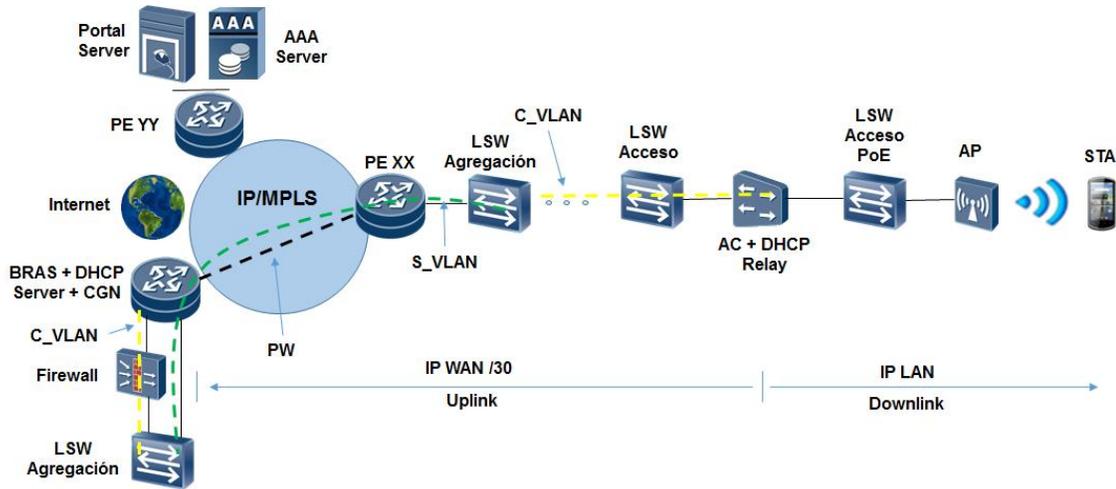


Fig. 2. Escenario capa 3 WiFi Interoperabilidad.

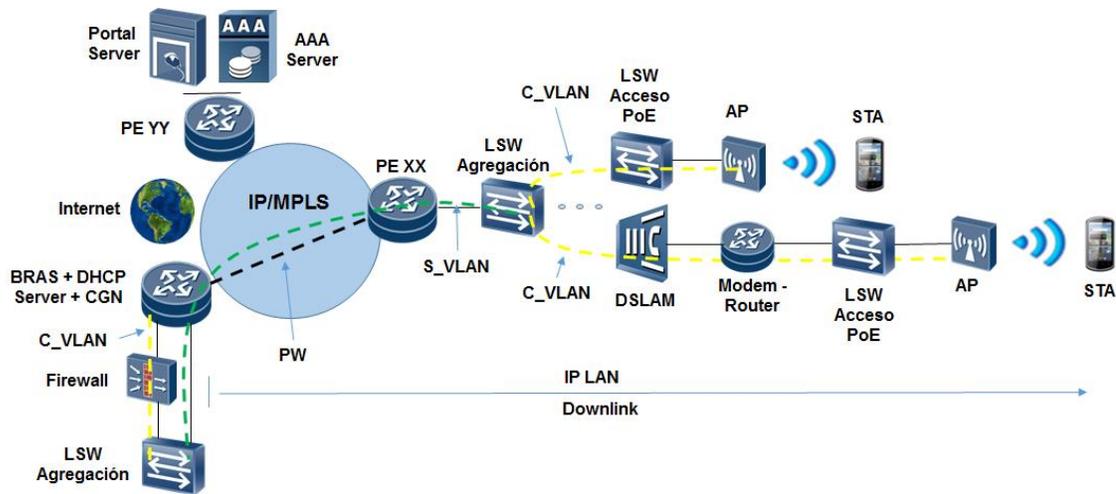


Fig. 3. Escenario capa 2 WiFi Interoperabilidad.

3. Imposibilidad de integrar los AC de fabricantes varios al Portal WEB y AAA del sistema convergente empleado por ETECSA.
4. Brechas de seguridad y supervisión deficiente.
5. Gasto elevado de direcciones IP reales.
6. Método incómodo de desconexión de los usuarios soportados sobre AC propiedad de ETECSA, direccionado a la URL (<http://1.1.1.1>).
7. Problemas con la desconexión aleatoria de usuarios soportados sobre AC propiedad de ETECSA, que al ejecutar el mecanismo de desconexión no detiene el consumo del crédito.

2.3 Escenario capa 3 WiFi Interoperabilidad

Este es el caso donde el cliente utiliza un AC y desea mantenerlo, requiere de un enlace con la red IP/MPLS con direccionamiento IP WAN y LAN de cara al BRAS (Ver Fig. 2). En este se emplea la

configuración "Layer 3 IPoE Access with Web Authentication" del fabricante HUAWEI, donde el AC está integrado, pero el control de usuario, la autenticación, entre otros, se hacen a través del BRAS, la plataforma AAA y el Portal Captive de HUAWEI, tal y como se emplea en la solución de sitios públicos WIFI ETECSA e Internet en las casas con ADSL Hogar. El AC trabaja en modo DHCP relay, este recibe la solicitud DHCP de la STA del usuario y reenvía la misma al BRAS, que opera como servidor DHCP. La STA del usuario recibe una dirección IP privada desde el BRAS, la cual se aplica en la solución CGN (NAT) en el propio BRAS para su posterior enrutamiento con IP reales hacia Internet.

La solución emplea una VLAN de cliente (C_VLAN) para cada sitio, la que se traza a través del switch de agregación del nodo más cercano y atraviesa los equipos involucrados del dominio IP/MPLS, pasa a través del Firewall (donde se aplican las políticas globales de seguridad) y termina en una sub-interface (BAS) del BRAS al que se asocia. En la

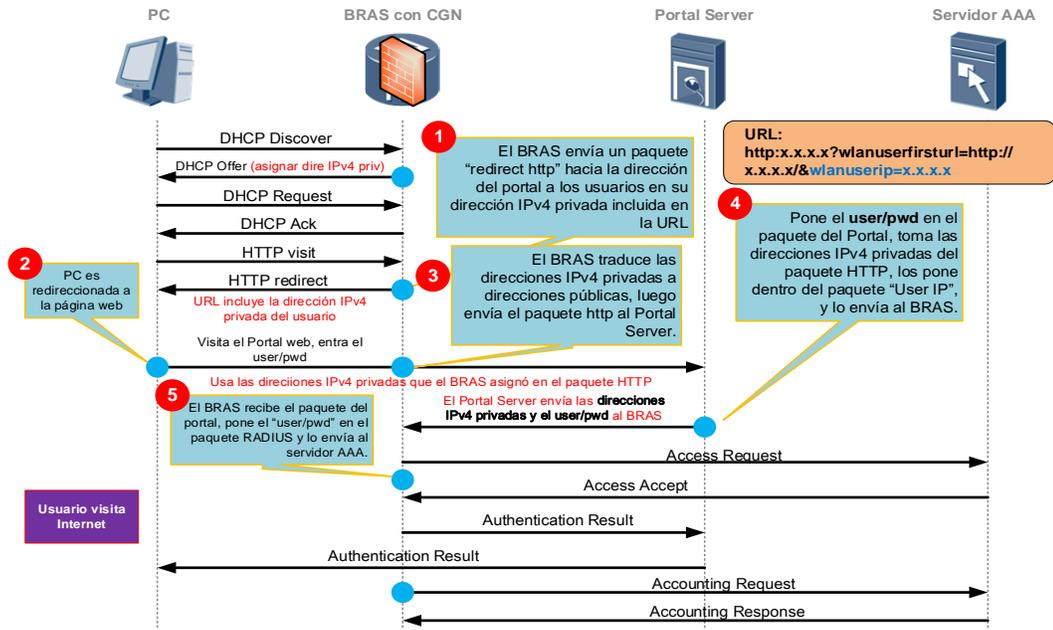


Fig. 4. Flujo de mensajes entre los equipos que conforman la solución WiFi Interoperabilidad.

sub-interface BAS se define el rango de direcciones IP privado, los dominios y las políticas de control de tráfico para cada sitio.

2.4 Escenario capa 2 WiFi Interoperabilidad

Este es el escenario mayormente empleado, en este caso se simplifica el esquema al eliminar el AC del extremo del cliente, requiere de un enlace con la red IP/MPLS que no demanda de direccionado IP, solo es necesario el trazado de una VLAN de cliente (C_VLAN) por los equipos de tránsito, que incluye los switches de agregación de ambos extremos, los equipos del dominio IP/MPLS y el Firewall, la C_VLAN termina en una sub-interface BAS del BRAS al que se asocia (Ver Fig. 3). En este caso se aplica la configuración "Layer 2 IPoE Access with Web Authentication" del fabricante HUAWEI, donde el BRAS opera como servidor DHCP y asigna dinámicamente las direcciones IP privadas a las STA que las demanden, en el propio BRAS se aplica la solución CGN (NAT) para su traslación a IP reales hacia Internet.

En ambas soluciones el cliente es responsable de administrar y proteger su red interna.

2.5 Flujo de mensajes en WiFi Interoperabilidad

En la Fig. 4 se muestra el flujo de mensajes que ocurre entre los equipos que intervienen en la solución WiFi Interoperabilidad.

2.6 Aplicación de la tecnología QinQ en WiFi Interoperabilidad [4]

Se debe señalar que en ambas variantes se ha aplicado la tecnología QinQ, que se utiliza para expandir el espacio de VLANs, ésta encapsula un paquete que transporta una etiqueta 802.1Q en otra etiqueta 802.1Q. El protocolo QinQ se basa en túneles capa 2 sobre la tecnología IEEE 802. Los paquetes transmitidos sobre una red de backbone contienen doble etiqueta 802.1Q (una etiqueta pública y otra privada), QinQ significa 802.1Q-in-802.1Q. La etiqueta pública se denomina VLAN Stacking (S_VLAN) y es la más externa en la trama Ethernet, la etiqueta privada se conoce como VLAN Cliente (C_VLAN) y es la más interna. Seguidamente se muestra el formato de la trama para este caso (Ver Fig. 5).

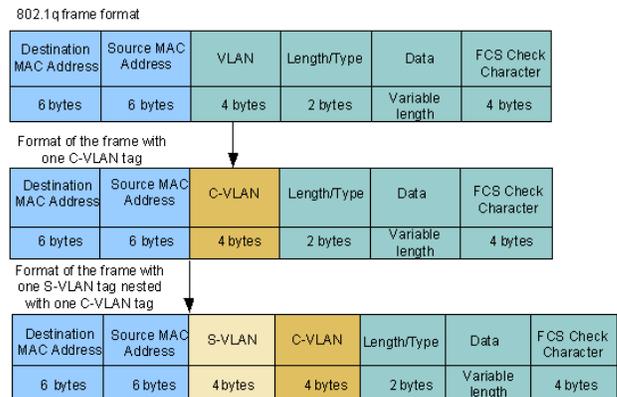


Fig. 5. Formato de la trama Ethernet.

Se ha previsto una VLAN Stacking por provincia, la

que se inserta en el sentido Upstream en el switch de agregación de origen en el sitio al que se conecta y se quita en el switch de agregación destino de cara al BRAS al que se asocia. En el sentido Downstream ocurre el proceso contrario. De esta forma las VLANs de clientes asignadas para cada institución se transportan sobre esta única VLAN (S_VLAN) entre los switches de agregación de los nodos de ambos extremos, atravesando así el dominio IP/MPLS. Con esto se optimiza el uso de recursos de red y se simplifica el proceso de provisión y atención a las interrupciones que puedan surgir. El empleo de VLANs independientes para cada cliente (C_VLAN) segmenta así los dominios de broadcast por institución.

2.7 Uso de los Pseudo-Wire en WiFi Interoperabilidad [4]

Otra de las funcionalidades que aprovechan las soluciones de WiFi Interoperabilidad es el uso de los Pseudo-Wire (PW) para el transporte capa 2 en la red IP/MPLS. Pseudo-Wire Emulation Edge to Edge (PWE3) es una tecnología de transmisión capa 2 extremo a extremo que emula los atributos esenciales de servicios de comunicaciones tales como ATM, FR, Ethernet, TDM y SONET/SDH en una red de conmutación de paquetes (PSN), como es el caso de IP/MPLS.

Los PW utilizan el Protocolo de Distribución de Etiquetas (LDP) sobre los PE de una red IP/MPLS para emular servicios capa 2 a través de túneles Multiprotocol Label Switch Protocol Label Switched Paths (MPLS LSPs) o Generic Routing Encapsulation (GRE). Los PW son conexiones virtuales que utilizan los VC-ID para identificar un Circuito Virtual (VC). El VC-ID de cada VC del mismo tipo debe ser único sobre todos los PE de la red (Ver Fig. 6).

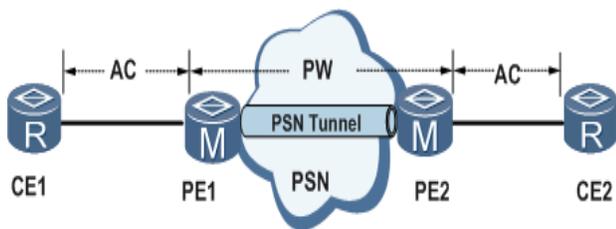


Fig. 6. Pseudo-Wire sobre una red IP/MPLS.

En aplicaciones de alta disponibilidad es posible garantizar redundancia de PW en aquellos escenarios donde un PE se conecta asimétricamente a otros 2 PE (Fig. 7). En ese caso se configuran 2 PW de un origen contra 2 destinos diferentes (primario/secundario), los que trabajarán en estado Master/Backup. Ante algún fallo del trayecto primario, el tráfico conmutará automáticamente hacia el secun-

dario, minimizando así su efecto sobre los usuarios finales.

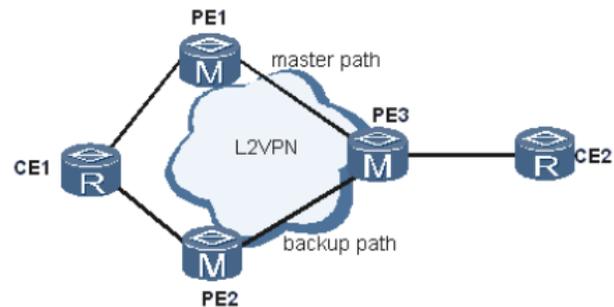


Fig. 7. Redundancia de PW en trayectos asimétricos.

Anterior a la puesta en servicio del Proyecto WiFi Interoperabilidad el transporte capa 2 sobre la red IP/MPLS de ETECSA se hacía utilizando las VPLS, con alto riesgo de ocurrencia de lazos que es proporcional al tamaño de la red, al estar todos los equipos involucrados en el mismo dominio de broadcast. La introducción de los PW combinados con el QinQ permite establecer enlaces únicos para cada provincia, lo que simplifica la atención a interrupciones que puedan ocurrir. Por otra parte, junto a la segmentación del tráfico por VLANs de cliente, reduce significativamente el efecto de la posible ocurrencia de lazos sobre la red.

3. CONCLUSIONES

En este trabajo se presentan los elementos básicos de las soluciones desarrolladas por ETECSA para brindar el servicio de acceso WiFi a Internet en espacios de terceros, que puede compartir o no equipamiento con el cliente. Los escenarios permitieron garantizar las condiciones técnicas necesarias para integrar en la misma arquitectura de red convergente NAUTA de ETECSA los despliegues ya existentes, con soluciones diversas en su implementación, independientemente del equipamiento empleado en éstas, así como establecer las pautas para la provisión de los servicios de este tipo en lo adelante.

Los escenarios comprendidos en WiFi interoperabilidad aprovechan las potencialidades del equipamiento disponible y brindan una solución integradora, escalable, robusta y segura. Entre sus ventajas se incluyen aspectos relacionados con la seguridad y supervisión del sistema de forma global con el uso del Firewall, el aumento del ancho de banda por usuario de 1 a 5 Mbps, la simplificación de la forma de desconexión, que ahora se reduce a la solo apagar el WiFi, la posibilidad de personalizar los portales WEB por sitios, el ahorro de recursos de red, (direcciones IP y VLANs), la facilidad del troubleshooting, entre otros.

Desde su apertura en abril del 2017 hasta septiembre de igual año se beneficiaron más de 180 sitios de todo el país, entre migraciones y nuevos servicios instalados, el 96% de ellos en instalaciones hoteleras.

4. AGRADECIMIENTOS

Los autores agradecen a todas aquellas personas que de una u otra forma se han visto involucradas en las tareas relacionadas con este trabajo, sin las cuales no hubiera sido posible su realización.

5. REFERENCIAS BIBLIOGRÁFICAS

1. **Manzaneda, J:** "Internet: ¿Cuál es la fuente para juzgar a Cuba?", Disponible en: <http://www.cubadebate.cu/opinion/2017/09/04/internet-cual-es-la-fuente-para-juzgar-a-cuba/#.WdefQjCJjQU>

2. **Lazo, L.:** "Proyecto WiFi ETECSA", Memorias VII Simposio Internacional de Telecomunicaciones, Ciudad de La Habana, 2016. Disponible en: <http://www.informaticahabana.co.cu/sites/default/files/ponencias/TEL61.pdf>

3. Espacios públicos de conexión inalámbrica (WIFI). Disponible en: http://www.etcscsa.cu/internet_conectividad/areas_wifi/.

4. Huawei ME60 Product Documentation V600R002C00. Disponible en: huawei.support.com.

6. SÍNTESIS CURRICULARES DE LOS AUTORES

Elio Ramón Avila Rodríguez. Camagüey, Cuba, 1967. Graduado de Ingeniero en Telecomunicaciones, Instituto Superior Politécnico Julio Antonio Mella, Santiago de Cuba, 1990. Graduado de Master en Automática, Universidad de Oriente, Santiago de Cuba, 2003. Ha desarrollado su labor profesional en las ramas de la electrónica, automática, docencia universitaria y las telecomunicaciones. Actualmente se desempeña como Especialista en Telemática en la División Territorial de ETECSA en Las Tunas y pertenece al grupo de profesores adjuntos al Centro Nacional de Capacitación de ETECSA. Sus líneas investigativas son las redes de Petri aplicadas a la automática y las comunicaciones, el empleo de los laboratorios virtuales en la educación y los sistemas de transmisión de datos, entre los que se encuentran: routing & switching, redes WLAN, sistemas de alta disponibilidad, IP/MPLS, etc. Ha participado como ponente en varios eventos internacionales, publicando en sus memorias y en revistas de corte técnico en temáticas relacionadas con sus líneas investigativas. Ha recibido varios reconocimientos y premios de Fórum en diversas categorías. Dirección postal: Ave. 1ro de Enero, Edif. 33, Apto. E-3. Rpto. Santos, Las Tunas, Cuba. Email: elio.avila@etcscsa.cu.

Yussel Castrizano Jiménez, Cuba, 1979. Graduado de Ingeniero en Telecomunicaciones y Electrónica, Instituto Superior Politécnico José Antonio (CUJAE), 2005. Ha desarrollado su labor profesional en las ramas de la docencia universitaria y las telecomunicaciones. Trabajó en la Universidad de las Ciencias Informáticas como Profesor de Telemática entre 2005 y 2007, como Administrador de Red en el Instituto Central de Investigaciones Digitales (ICID) y en el Ministerio de la Industria Básica (MINBAS) entre los años 2007 y 2010, momento en el que ingresa en ETECSA como Especialista en Telemática, operando la red MPLS. Actualmente se desempeña como Jefe de Grupo de Agregación que maneja la capa de Backbone IP/MPLS de ETECSA. Sus líneas investigativas se encuentran asociadas al desarrollo y operación de la infraestructura y plataformas de las redes de transmisión de datos WAN en Cuba y los sistemas de transmisión de datos, entre los que se encuentran: routing & switching, sistemas de alta disponibilidad, IP/MPLS, etc. Ha recibido varios reconocimientos y premios de Fórum en diversas categorías. Dirección postal: Calle 52 # 4717, e/ 47 y 49, Rpto. Playa, La Habana. Email: yussel.castrizano@etcscsa.cu

Eliezer Bravo Borrego. La Habana, Cuba, 1972. Graduado de Ingeniero en Telecomunicaciones, Master en Radiocomunicaciones. Instituto Superior Politécnico José Antonio Echevarría (CUJAE), La Habana, Cuba, 2001 y 2003, respectivamente. Ha desarrollado su labor profesional en las ramas de la electrónica, la docencia universitaria y las telecomunicaciones. Actualmente se desempeña como Especialista en Telemática en la Dirección Central de Desarrollo y Tecnología de ETECSA y pertenece al grupo de profesores adjuntos al Centro Nacional de Capacitación de ETECSA. Sus líneas investigativas se encuentran asociadas al desarrollo de la infraestructura y plataformas de las redes de transmisión de datos WAN en Cuba, el empleo de los laboratorios virtuales en la educación y los sistemas de transmisión de datos, entre los que se encuentran: routing & switching, sistemas de alta disponibilidad, IP/MPLS, etc. Ha dirigido técnicamente los grupos que manejan la capa de Backbone de las redes de datos, tanto en variante ATM como IP/MPLS de ETECSA Cuba. Ha recibido varios reconocimientos y premios de Fórum en diversas categorías. Dirección postal: Ave. Factor, Edif. 821, Apto. D. Rpto. Nuevo Vedado, La Habana, Cuba. Email: eliezer.bravo@etcscsa.cu.

Lesdier Duardo Liens. La Habana, 1973. Graduado de Ingeniero en Telecomunicaciones y Electrónica, Instituto Superior Politécnico José Antonio Echevarría (CUJAE), La Habana, 2009. Ha desarrollado su labor profesional en las ramas de la electrónica y telecomunicaciones. Entre los años 1998-2012 se desempeñó como técnico en el centro de Gestión Nacional de Redes de Datos, operando redes (x.25, Frame relay, ATM, acceso e IP/MPLS. Actualmente se desempeña como Especialista en Telemática y pertenece a la Dirección Central de Desarrollo y Tecnología (DCDT) en la Dirección Estructura de Datos, específicamente en el desarrollo, planeamiento y diseño de redes de acceso, redes de agregación, VSAT, WLAN y Backbone IP/MPLS ETECSA. Sus líneas investigativas son las redes de las comunicaciones, el empleo de los laboratorios virtuales en los sistemas de transmisión de datos, entre los que se encuentran: routing & switching, redes WLAN, sistemas de alta disponibilidad, IP/MPLS, etc. Ha recibido varios reconocimientos por su participación en eventos internacionales como soporte en la infraestructura de transmisión de datos. Dirección postal: Calle 25 # 3403, Apto. 7, e/ 34 y 36. Rpto. Alturas de Almendares, Playa, La Habana. Email: lesdier.duardo@etcscsa.cu