

Modelo de enlace punto a punto con direccionamiento IPv6 utilizando tecnología VPN entre una estación base y puntos de acceso inalámbrico.

Model point-to-point routing using IPv6 VPN technology between a base station wireless access points.

León Felipe Austria González

Gilberto Ortega Garcia

Alberto Corona Alejandro

Benito Canales Pacheco

Raymundo Sergio Noriega Loredo.

snoriegal@gmail.com

Resumen

Una de las necesidades más importantes en la actualidad para los gobiernos, empresas, instituciones y las personas, es mantener comunicaciones eficientes en puntos distantes. La evolución de las telecomunicaciones en los últimos años ha ocasionado cambios en la forma de mantener comunicación a grandes distancias, un ejemplo es el uso de internet como principal medio de comunicación, con esto las distancias geográficas no son obstáculo para la comunicación ya que con el uso de dispositivos electrónicos es posible llevar información desde un punto a otro; como es el caso de computadoras y dispositivo móviles principalmente

El transporte de datos mediante el uso de las redes genera beneficios como mantener comunicaciones a distancia en tiempo real, el problema de esta comunicación es que la información queda expuesta a terceros, lo cual puede ocasionar robo o alteración de datos, entre otros. Para poder ofrecer la seguridad que buscan los usuarios, en este proyecto se

propone utilizar tecnologías para mantener un nivel de seguridad deseable, esto se logrará mediante el uso de las Redes Privadas Virtuales (VPN Virtual Private Network por sus siglas en inglés) como una alternativa de solución y el ocultamiento del direccionamiento IPv6.

En este proyecto, se analiza la necesidad de implementar una VPN (Red Privada Virtual) sobre un enlace remoto Wi-Fi (Wireless-Fidelity) punto a punto para el transporte seguro de datos entre la red de la Universidad Tecnológica de la Sierra Hidalguense (UTSH) hacia los puntos de acceso definidos en las zonas de cobertura en el municipio de Zacualtipán, para ofrecer los servicios de internet a usuarios autorizados de la comunidad universitaria y con esto puedan tener acceso a la intranet de forma segura para el manejo de renuncias, gestos, consultas de información, envío de datos, que les permitan las comunicaciones electrónicas que demanda la comunidad universitaria en la actualidad.

Palabras claves: Telecomunicaciones, transporte de datos, VPN, IPv6, remoto Wi-Fi.

Abstract

One of the most important needs today for governments, businesses, institutions and individuals, is to maintain efficient communications in distant points. The evolution of telecommunications in recent years has led to changes in the way of maintaining communication over long distances, an example is the use of the Internet as a primary means of communication, this geographical distances are no obstacle to communication as the use of electronic devices may carry information from one point to another; such as computer and mobile device primarily

Data transport using networks generates benefits such as keeping distance communications in real time, the problem of this communication is that information is exposed to third parties, which may result in theft or alteration of data, among others. In order to provide the security that users are looking for in this project proposes to use technologies to maintain a desirable level of security, this will be achieved by using Virtual Private Networks (VPN Virtual Private Network for short) as an alternative solution and concealment of IPv6 addressing.

In this project, the need to implement a VPN (Virtual Private Network) over a Wi-Fi (Wireless-Fidelity) point remote link to point to the safe transport of data between the network of the Technological University of Sierra Hidalguense analyzed (UTSH) to the points defined in the coverage areas in the municipality of Zacualtipán to provide Internet services to authorized members of the university community users and that can access the intranet securely for handling renicaciones, registers, information queries sent data, enabling them to electronic communications that demand the university community today.

Key words: Telecommunications, data transport, VPN, IPv6, remote Wi-Fi.

Fecha recepción: Mayo 2016

Fecha aceptación: Julio 2016

Introducción

Objetivo

Diseñar y construir enlaces punto a punto para permitir una conexión segura entre la UTSH y puntos de distribución de servicio de internet mediante el uso de una red privada virtual.

Justificación

Dentro del proyecto “Red Convergente IPV6 de la UTSH” que consiste en ofrecer acceso y servicios de internet a la comunidad de la institución y público en general dentro y fuera de la misma; se requiere de un enlace seguro que brinde al usuario protección en el transporte de su información entre los diferentes puntos de acceso inalámbrico a la red local del campus, con el propósito de asegurar sus datos, en términos de: integridad, acceso, confiabilidad y resguardo de los mismos.

Impacto

Con la implementación de las redes privadas virtuales los usuarios y la comunidad en general que tengan acceso a la red, se verá beneficiada en el sentido de su tranquilidad ante el posible robo o pérdida de su información, con ello, elevar la confianza que se brinda para el manejo y transporte de datos. Gracias a las cualidades que ofrece la implementación de esta tecnología, como en la autenticación del acceso, la encriptación de datos y la codificación de la información, es como se garantiza la protección en el transporte de información.

Estado del Arte

En este apartado se describen las investigaciones más recientes y actuales sobre el tema de este trabajo. En inglés el "State of de Art", es referido al conocimiento o tecnología de punta o vanguardia (FLORES, 2011). En el caso específico en el que se escriben estas líneas, el periodo de indagación se delimitaría desde el 2013 al 2016. La descripción en este documento de investigación se expone los avances existentes acerca del tema y es de carácter más cualitativo. La presente investigación se incluye como parte importante para referir el grado de innovación que la investigación presenta y le da relevancia a la diferencia. La descripción gira en torno esencial a cuatro elementos: ¿Qué? ¿Quién? ¿Cuándo? ¿Qué características de seguridad?

Nombre del proyecto: Servicios de Tecnologías de la Información y Comunicación (STIC), Universidad de Chile.

Características: El Servicio VPN es un sistema que establece un canal seguro de comunicaciones entre su computador personal y la Red Corporativa de la Universidad. Utilizando el Servicio VPN, Académicos, Estudiantes y Personal de Colaboración de la Universidad de Chile pueden conectarse desde su hogar a los servicios en línea que han sido contratados por esta casa de estudios y cuyo acceso ha estado tradicionalmente circunscrito a computadores instalados dentro de la red corporativa (STIC, 2013).

Nombre del proyecto: Prototipo de enlace punto a punto utilizando tecnología VPN entre una estación y puntos de acceso inalámbricos (PEPP-VPN).

Descripción: Este prototipo parte del proyecto “Red Convergente IPV6 de la UTSH” que consiste en ofrecer acceso y servicios de internet a la comunidad de la institución y público en general dentro y fuera de la misma; es requerido un enlace seguro que brinde al usuario protección en el transporte de su información entre los diferentes puntos de acceso inalámbrico a la red local del campus, con el propósito de asegurar sus datos, en términos de: integridad, acceso, confiabilidad y resguardo de los mismos (GRUPO DE INVESTIGACIÓN, 2016). El diseño y la construcción de este prototipo debe permitir que los enlaces punto a punto, logren una conexión segura entre la UTSH y puntos de distribución de servicio de internet (localizados en escala pero que en proyección real debe ser la zona de cobertura de la cabecera municipal) mediante el uso de una VPN.

Tabla 1. Comparación del estado del arte.

¿Qué?	¿Quién?	¿Cuándo?	¿Qué características de seguridad?	Grado de innovación
STIC	Universidad de Chile	2013	Acceso de aplicaciones de manera remota autenticando y gestionando el perfil del cliente dentro de la aplicación con soporte a usuarios.	
PEPP-VPN	UTSH	2016	Políticas de seguridad orientadas al enlace bajo tres capas: direccionamiento físico, enlace a datos de la red, direccionamiento lógico.	Blindaje del túnel de la información orientado al enlace punto a punto asegurando la VPN. Integrando tecnologías WAN.

Resultados

Las pruebas se realizaron en dos etapas:

1.- Estudio de simulación; este estudio es efectuado con los cambios al modelo del sistema, para observar alteraciones al comportamiento del mismo y poder entender mejor la operación, anticipar los posibles resultados no previstos, y con ello mejorar el diseño.

2.- Construcción del modelo y experimentación; el armado se realiza en el laboratorio especializado dentro de la UTSH, en donde la topología propuesta, es probada y es vista desde el simulador (Figura 1), con los dispositivos en forma real (dispositivos de interconexión y finales) para poder observar e interpretar los resultados y así poder comprobar el grado de validez de la hipótesis de la solución propuesta.

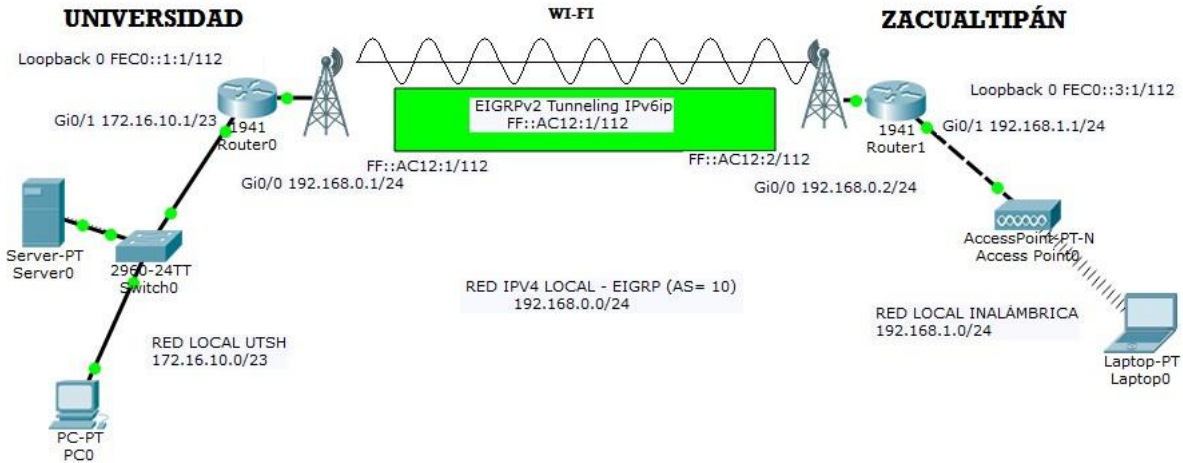


Figura 1. Topología de la red del enlace WI-FI punto a punto.

Conclusiones

La implementación de este proyecto en la Universidad Tecnológica de la Sierra Hidalguense dará grandes beneficios contribuyendo en gran medida al acceso de la información en distintos puntos geográficos de manera segura, creando una red metropolitana de acceso a la información, haciendo uso de la Intranet universitaria existente. Desde el punto de vista de innovación, el proyecto implementa niveles de seguridad mediante el uso de criptografía (cifrado de datos) en el enlace inalámbrico así como el ocultamiento del direccionamiento IPv6 del enlace a través de un túnel VPN, esto mejora la seguridad tradicional en un enlace Wi-Fi.

Bibliografía

GRUPO DE INVESTIGACIÓN, Tecnologías de la Información y Telecomunicaciones. (2016). “Aplicación del direccionamiento lógico para redes convergentes con base al protocolo de internet versión 6”. Acta No. 03/2016. Universidad Tecnológica de la Sierra Hidalguense, Zacualtipán de Ángeles Hidalgo.

STIC. (2013). “Servicios de Tecnologías de la Información y Comunicación”. Universidad de Chile. Disponible en: http://soporte.uchile.cl/mediawiki/index.php/Pol%C3%ADtica_de_Acceso_VPN

FLORES G. (2011). “Formando Investigadores”. Disponible en: <http://formandoinvestigadores-gft.blogspot.mx/2011/01/estado-del-arte.html>