Diseño de una red IPv6 en la empresa Siete24 LTDA.

Deisy Tatiana Bello Mosquera, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Ingeniería en Telecomunicaciones, CC 1.022.366.746

Jorge Eliecer Salamanca Urrego, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Ingeniería en Telecomunicaciones, CC 1.015.407.908

Gustavo Adolfo Higuera Castro, Universidad Distrital Francisco José de Caldas, Facultad Tecnológica, Ingeniería en Telecomunicaciones, CC 1.024.461.077

En este artículo, se da a conocer información que es útil y veraz para el diseño de la red IPv6 en la empresa Siete24 LTDA y así realizar la transición del protocolo actual IPv4. Se identifican las características de las variables abordadas en el estudio, se muestran los beneficios derivados del cambio, en donde se asemejan las fortalezas y debilidades de proponer el cambio del protocolo IPv4 a IPv6 que funciona actualmente en la compañía, generando una posible propuesta para la migración del protocolo actual, donde no afecta la seguridad ni la calidad en el servicio que se brinda. Se dan a conocer las ventajas y dificultades que se presentan durante el uso del protocolo IPv4 que actualmente emplea la entidad, con el fin de mejorar su desempeño con la posibilidad de usar el protocolo IPv6, la compañía contará con mayor nivel de seguridad ya que IPv6 cuenta con IPSec que permite la autenticación y encriptación de la información extremo a extremo, ofrece autoconfiguración e direcciones IP, en su red, podrá gestionar de forma más ágil, fácil y segura toda la topología, tendrá la facilidad de escalar tanto en forma lógica como física.

Palabras Clave

Diseño de redes, topología lógica, IPSEC, migración de redes, protocolo de internet IPv6 IPv4, VLANs.

Abstract

In this article, information is provided that is useful and truthful for the design of the IPv6 network in the company Siete24 LTDA and thus make the transition of the real IPv4 protocol. The characteristics of the variables addressed in the study are identified, the benefits derived from the

change are found, where the strengths and weaknesses of the proponent of the change from IPv4 to IPv6 protocol migration are found in the current protocol, where it does not affect safety and quality in the service provided. The advantages and advantages that are presented during the use of the IPv4 protocol currently used by the entity are disclosed, in order to improve its operation with the possibility of using the IPv6 protocol, the company counter with the highest level of security since IPv6 has IPsec that allows the authentication and encryption of the information from end to end, offers auto configuration and IP addresses, in red, manage the easiest, easiest and most secure topology, have the facility to scale both logically as physical.

Key Words

Network design, logical topology, IPSEC, network migration, Internet protocol IPv6 IPv4, VLANs.

Introducción

En la actualidad, la importancia del Internet ha generado un gran crecimiento de uso por parte de las personas y esto ha forjado un rápido agotamiento de las direcciones IPv4, lo cual ocasionará el cambio a IPv6, así como lo dijeron los autores Deering &Hinden en 1998.

En Colombia, se ha llevado a cabo la implementación gracias a la promoción del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el cual tiene objetivo principal ampliar el número de usuarios de Internet banda ancha de 2.2 a 8.8 millones de suscriptores en el periodo comprendido entre el 2010 y 2014 (MinTIC, 2011). En este momento ya está implementado en muchas otras en instituciones públicas del orden nacional definido previamente por el Ministerio el IPv6, como por ejemplo Colciencias, Coldeportes, Archivo General de la Nación, Ministerio de Cultura, Ministerio de trabajo y la Universidad Distrital Francisco José Caldas, entre otras (MinTIC, 2015). Por todo este desarrollo se ve la importancia de una actualización a una versión que está en crecimiento en el mundo y a la cual tarde o temprano se tendrá que adaptar, no solo por el hecho de su gran direccionamiento, sino por los muchos beneficios que trae consigo.

Ahora, ¿Por qué la implementación de IPv6 en una empresa?, es una carta de presentación

hacia la innovación tecnológica y permitirá tener una red actualizada, lo cual hablará muy bien de la compañía. Además, permitirá el crecimiento de las redes para la conexión de toda la empresa y no tendrá limitaciones en el momento en el que se presente un crecimiento notable de la red garantizando los requerimientos de seguridad y operatividad. Esta propuesta de IPv6 le permitirá contar a la compañía con un planeamiento eficaz para el desarrollo de la empresa sin ninguna complicación en el tema de redes.

Se tomó como base la red actual que está en funcionamiento en la empresa Siete24 LTDA. Se ve la oportunidad de proponer a la empresa la migración de forma paulatina al nuevo protocolo IPV6, con el fin de fortalecer la red actual y a su vez segmentar la red actual en las áreas que permiten el funcionamiento de la empresa en su día a día, para proteger la información y que solo las personas interesadas puedan conectarse entre sí.

Esta propuesta se lleva a cabo analizando la topología actual tanto física como lógica y se busca corregir las fallas actuales como el agotamiento de direcciones IP debido al segmento actual en el que está configurada la red, este direccionamiento privado ya no es suficiente debido al crecimiento de la compañía ya que solo utilizan un segmento LAN con capacidad para 253 direcciones IP.

Además de las políticas de seguridad ya que no cuenta con protocolos propios que protejan la información que se maneja ya que cualquier equipo que se conecté a la red actual podría sustraer información valiosa, se aumenta y se garantiza el ancho de banda de la compañía con la capacidad de soportar aplicaciones como video en tiempo real ya que este es uno de los servicios que presta al monitorear cámaras de vigilancia.

IPv6

Debido al gran crecimiento del Internet y el agotamiento de direcciones del Ipv4, el organismo que se encarga de la estandarización de los protocolos de Internet (*IETF, Internet Engineering Task Force*), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones con una longitud de 128 bits, es decir 340 sextillones de combinaciones. [1]

Dentro de las características más importantes del IPv6 se encuentran las siguientes:

- Cuenta con una mayor cantidad de direcciones, el cual pasa de 4 bytes que posee el IPv4 a 32 bytes del IPv6. Sin duda es una de las principales ventajas y diríamos que una de las razones más fuertes por las cuales cambiar de protocolo. Se habla de un número similar a 6.67126144781401e+23 direcciones IP por cada metro cuadrado sobre la superficie de la Tierra. [2]
- Otro aspecto importante es que cuenta con un nuevo formato de cabecera, lo cual permite realizar de una manera más eficaz el enrutamiento de los equipos cuando se procesa la información. [3]
- Su direccionamiento es más eficiente, ya que permite a los enrutadores principales contener tablas más pequeñas, dependiendo de la infraestructura que tenca cada IPS. [3] Adicionalmente, la dirección IPv6 se diseñó para ser subdividida en dominios de enrutamiento jerárquico que reflejan la topología del Internet actual. [2]
- En temas de seguridad el IPv6 cuenta con un protocolo llamado IPSec, del cual se hablará más adelante pero que entre sus principales características se encuentran: Limitar el acceso a sólo aquellos autorizados, certifica la autenticación de la persona que envía los datos, encripta los datos transmitidos a través de la red, asegura la integridad de los datos e invalida la repetición de sesiones, para evitar que no sean repetidas por usuarios maliciosos. [2]
- IPv6 permite configurar las direcciones manualmente o de forma automática, esto aun en la ausencia de un router, ya que los hosts pueden configurarse automáticamente con enlaces de direcciones locales, sin necesidad de una configuración manual. [3]

IPv4 frente a IPv6

Luego de ver las características que tiene IPv6 es importante mencionar las diferencias más notables de esta versión del protocolo en comparación con IPv4, las cuales son: el modelo de capas, redes conmutadas de paquetes, direcciones IP de origen y destino, VLSM (*Variable Length Subnet Mask),* también cambian servicios como el DNS y DHCP; funciones que eran usadas en muy pocas ocasiones o no eran usadas han sido eliminadas, como por ejemplo el protocolo NAT es eliminado

por completo debido al gran espacio de direcciones ofrecidas. [4]

Son muchas las ventajas que presenta el IPv6, pero para poder fijarse en la importancia de una actualización es importante realizar una comparación con el IPv4, las diferencias principales entre IPv4 e IPv6 se muestran en Tabla 1 a continuación:

IPv4	**IPv6**
Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
La implementación de IPSec es opcional.	La implementación y soporte para IPSec es obligatorio.
Ninguna identificación de flujo de paquete para QoS es manejada por los routers en la cabecera de IPv4.	La Identificación de flujo de paquete para QoS está presente en la cabecera IPv6 usando el campo "*flowLabel*"
La fragmentación es realizada en IPv4 involucra tanto al host como el router, de modo que este proceso produce retardos en el rendimiento del router.	El proceso de fragmentación en IPv6 solamente involucra al host ya que el paquete es procesado solo en el nodo final de destino.
No tiene ningún requisito para el tamaño de un paquete de capa de enlace y debe ser capaz de reensamblar un paquete de 576 bytes.	La capa de enlace de soportar un paquete de 1280 bytes de tamaño y debe ser capaz de reensamblar un paquete de 1500 bytes.
La cabecera incluye el *checksum.*	La cabecera no incluye *Checksum.*
La cabecera incluye campos llamados opciones.	Todos los datos opcionales son movidos a las cabeceras extendidas que tiene IPv6.
ARP envía tramas broadcast para realizar peticiones ARP de modo que se pueda resolver una dirección IPv4 en una dirección de capa física.	Las tramas para solicitar peticiones ARP son reemplazadas con mensajes *multicast* "Neighbor Discovery".
IGMP (*Internet Group Management Protocol*) es usado para manejar grupos de subredes locales.	IGMP es reemplazado por MLD (*MulticastListener Discovery*) que es un set de mensajes que son intercambiados por los routers para descubrir direcciones *multicast*.
ICMP Router Discovery es usado para determinar la dirección IPv4 del mejor "*Gateway*" y es opcional.	ICMPv4 es reemplazado por mensajes ICMPv6 y es necesariamente requerido.
Las direcciones de broadcast son utilizadas para enviar tráfico a todos los nodos en una subred.	No existen direcciones IPv6 de broadcast, en su lugar los enlaces locales echan una mirada en todos los nodos en donde direcciones *multicast* son usadas.
Las direcciones deben ser configuradas manualmente o mediante DHCP.	Las direcciones IPv6 no requieren configuración manual o DHCP.

Usa recursos de registros de direcciones de host in DNS para asignar nombres a direcciones IP.	Usa registros AAAA in DNS para asignar nombres a direcciones IPv6.

Tabla 1. Diferencias entre IPv4 e IPv6.

Protocolo DHCPv6

El protocolo de configuración dinámica de host DHCPv6 (siglas en inglés *Dynamic Host Configuration Protocol*) busca reducir esfuerzos en la instalación de dispositivos en una red con IPv6. El DHCP funciona primero cuando un equipo es conectado a nuestra red, entonces un servidor DHCP recibirá la solicitud de este equipo y le asignará una dirección y otra información a este y por último se realiza una verificación bidireccional entre el cliente y el servidor. [5]

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

- **Asignación manual:** El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP.
- **Asignación automática:** Al cliente DHCP se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.
- **Asignación dinámica:** El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al *clientServer* que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra. [6]

Enrutamiento *RIPng*, (*Routing Information Protocol new generation*)

Con el cambio de IPv4 a IPv6 también es necesario el cambio de protocolos de enrutamiento, que intercambian información de direccionamiento. Así que RIPng es una actualización de la que funciona actualmente en IPv4, pero que esta sea compatible con IPv6 y es definida por sus creadores como: RIPng está pensado para permitir a los routers intercambiar información para computar rutas a través de una red basada en IPv6. [7]

A continuación, se citan las características de *RIPng*:

- Deja de usar definitivamente el protocolo UDP.
- Usa el algoritmo vector distancia para determinar una ruta óptima hacia el destino, usando la cuenta de saltos (*hop count*, número de routers entre un nodo de origen y uno de destino) como métrica.
- Selecciona a la ruta con la métrica más baja como la preferida para enviar paquetes.
- Los routers configurados con *RIPng* intercambian información acerca de la disponibilidad de la red mediante mensajes de actualización de ruta.
- Opera dentro de un Sistema Autónomo (AS), que es un conjunto de routers y redes controladas por un único administrador.
- Instala la mejor ruta en la tabla de enrutamiento.
- Usa actualizaciones de envenenamiento en reversa y horizonte dividido para evita *Routing Loops.*
- Soporta el *Simple Network Manager Protocol* (SNMO).
- Ayuda a una red IPv6 a entender la información IPv6 Configuración *RIP*.
- Se habilita *RIP* en cada interfaz con un número del proceso o dominio. [7]

Seguridad en IPV6

Dentro del campo de redes y más aún en las redes públicas hay un factor que se considera muy importante, y es la seguridad, la cual debe aplicarse en cada componente de una red y en cada sistema. Pero al hablar de seguridad se habla de un manejo de riesgos. IPv6 se desarrolló además de tener un mayor direccionamiento también tener una mayor seguridad que IPv4, en cuanto a eso se ha creado un protocolo de seguridad basado en IPv4 que se verá a continuación. [8]

IPSec (IP Security)

IPSec es un marco de estándares abiertos desarrollado por el por Internet Engineering Task Force (IETF) que proporciona seguridad para la transmisión de información confidencial sobre redes no protegidas como Internet. IPSec actúa en la capa de red, protegiendo y autenticando paquetes IP entre dispositivos IPSec participantes (*peers*), como enrutadores Cisco. IPSec

proporciona los siguientes servicios de seguridad de red opcionales. En general, la política de seguridad local dictará el uso de uno o más de estos servicios:

- Confidencialidad de datos: el remitente de IPSec puede cifrar paquetes antes de enviarlos a través de una red.
- Integridad de los datos - El receptor IPSec puede autenticar los paquetes enviados por el remitente IPSec para asegurarse de que los datos no se han alterado durante la transmisión.
- Autenticación de origen de datos - El receptor IPSec puede autenticar el origen de los paquetes IPSec enviados. Este servicio depende del servicio de integridad de datos.
- *Antireplay* - El receptor IPSec puede detectar y rechazar paquetes reproducidos. [9]

Transporte y Túnel en IPSec

Para poder observar un diagrama básico de lo que sería el transporte de información utilizando IPSec, en este la seguridad va de extremo a extremos, como se ve en la figura 1, en la cual los equipos N1 y N2 se comunican entre sí y utilizan seguridad bidireccional. [10]

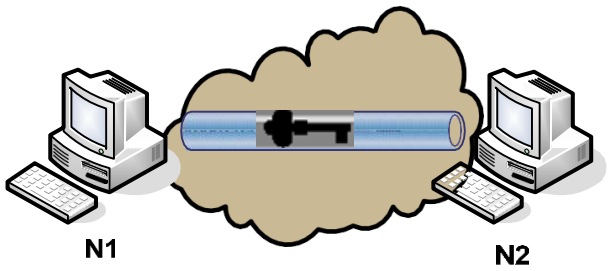


Figura 1. Modo trasporte de IPSec entre dos equipos [10]

En la siguiente figura se podrá observar la conexión de un equipo con una red privada virtual (VPN) que se encuentra en un servidor y también este mismo se encuentra conectado hacia otro equipo con el cual transmite información encapsulada en una conexión IP hacia el VPN y a esto se le conoce como conexión modo Túnel [10]

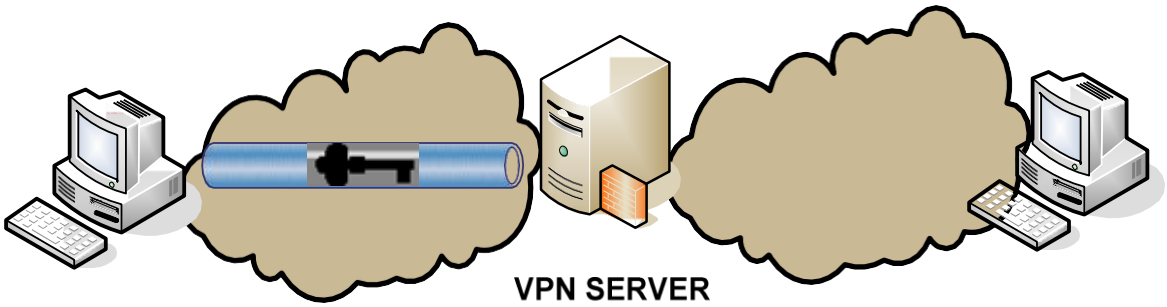


Figura 2 Modo Túnel de IPSec desde un nodo hacia un servidor VPN. [10]

Para realizar una conexión más segura se pueden combinar los modos Túnel y Transporte. En Figura 3 se muestra el modo túnel entre N1 y el servidor VPN y el modo transporte entre el servidor VPN y N2 haciendo esto que cada paquete que viene de N1 tenga dos diferentes encapsulaciones para IPSec; una para el servidor VPN y otra para N2. [10]

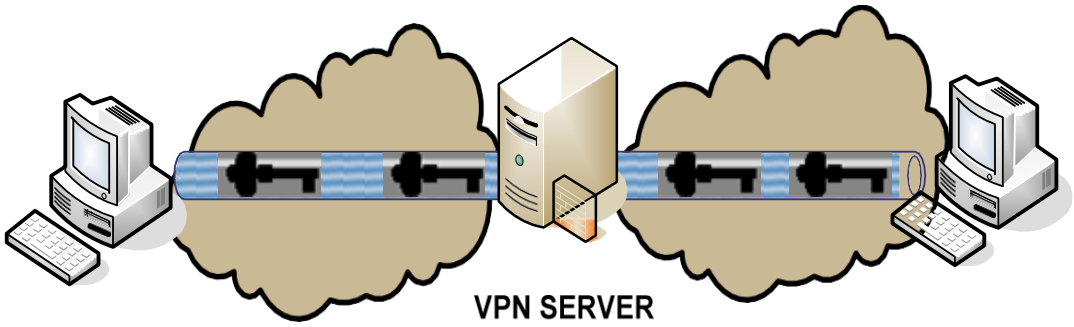


Figura 3 Modos IPSec Túnel y Transporte usados simultáneamente. [10]

Características protocolo TCP

El protocolo *TCP* (*Transmission Control Protocol*). está documentado en la *RFC* 793 de la *IETF*; es orientado a la conexión, y tiene una operación *full-dúplex*, contiene una revisión de errores por medio de una técnica de *checksum* que es usada para verificar que los paquetes no estén corruptos. Tiene acuses de recibo de uno o más paquetes, el receptor regresa un acuse de recibido, al transmisor indicando que recibió los paquetes. Si los paquetes no son notificados, el transmisor puede reenviar los paquetes o terminar la conexión si el transmisor cree que el receptor no está más en la conexión.

Protocolo *UDP*

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. [11] Básicamente este protocolo permite él envió de datos (datagramas IP) encapsulados sin necesidad de establecer una conexión previamente, esto con el fin de evitar de no crear y eliminar conexiones. [12]

Las características principales de este protocolo son:

- Como se mencionó anteriormente lo más destacado de este protocolo es que trabaja sin conexión, es decir, que no es necesaria la sincronización entre el origen y el destino.
- Posee una interfaz sencilla entre la capa de red y la capa de aplicación.
- Por otra parte, lo negativo de este protocolo es que no brinda garantía para la entrega de sus mensajes.
- Su uso, por ejemplo, cuando se necesita transmitir voz o vídeo y no importa si estos mensajes llegan, sino la velocidad de transmisión. [11]

ACL (*Access Control List*)

La ACL permite el filtrado de la información dentro de una red, permitiendo así el control de la información. Se trata de una serie de condiciones que permitirán el correcto manejo de la información.

Algunas de las condiciones de filtrado que permite la ACL son:

- Protocolo
- Números de puerto
- Valor de punto de código de servicios diferenciados (DSCP)
- Valor de precedencia
- Estado del bit de número de secuencia de sincronización (SYN) [13]

Infraestructura de la red actual de Siete24 LTDA.

Actualmente, la compañía cuenta con una red LAN con dos proveedores de servicio de internet (ISP). Los equipos que conecta esta red son: un router E900 marca LICKSYS, el cual permite tasas de transferencia de hasta N300Mbps y seguridad inalámbrica, y otro router 2811 marca Cisco, el cual es mucho más completo y cuenta con protección de firewall una memoria RAM de 256MB con opción de ampliar, protocolo *Fast Ethernet*, cifrado de hardware y además de soportar túneles por VPN. Los routers realizan el enrutamiento los ISP en la red de datos y en la red de telefonía IP. De allí también se derivan los servicios de telefonía IP, correo y WIFI. En este momento no se ha implementado una segmentación de la red, tampoco se cuenta con VLAN de telefonía creada, adicionalmente es necesario un balanceo de cargas y un mecanismo de seguridad, ya que es muy vulnerable.

Para la distribución de la red se cuenta con 2 *switch* HP v1910 de 48 puertos y 3 *switch* HP v1410 de 16 puertos los cuales no son administrados. Los primeros cuentan con una velocidad de hasta 1000Mbps y el segundo de hasta 100Mpbs, ambos con Fast Ethernet. Un diagrama de la infraestructura se puede observar en la figura 4.

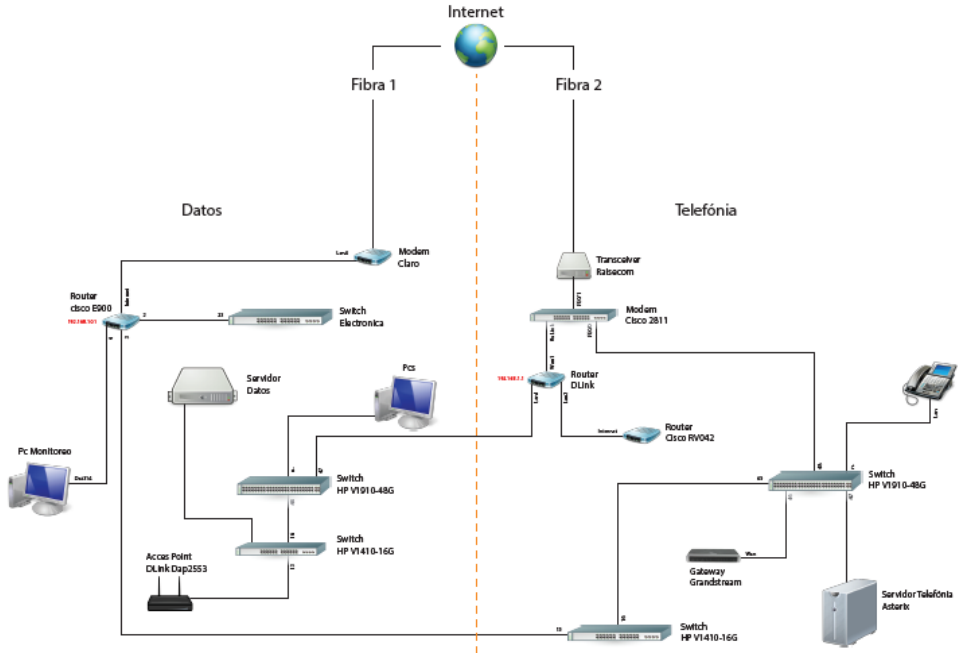


Figura 4. Infraestructura de la red de Siete24 LTDA

Metodología

Un diagrama para resumir la metodología de implementación del IPv6 se puede observar en la figura 2. Cabe resaltar que el alcance de este artículo es realizar la planificación y el diseño para el cambio de protocolos.

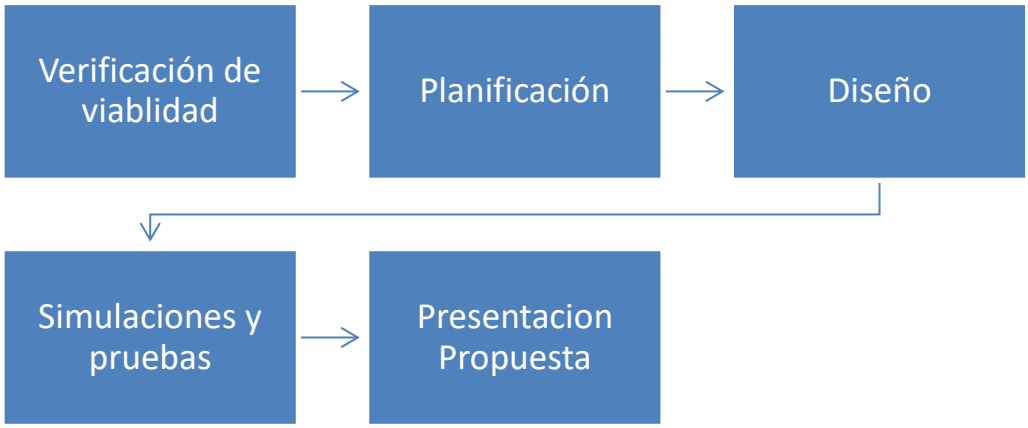


Figura 5. Metodología

Planificación

De acuerdo con los temas contemplados dentro del marco teórico de este artículo, que permite observar cada una de las ventajas y las formas de implementación de IPv6 para realizar el cambio del diseño de la red de IPv4 de la empresa SIE7E24. Razones como por ejemplo el agotamiento de IPv4 y también la importancia de una transición a tiempo a IPv6 para el adecuado crecimiento de la Banda Ancha.

Se puede observar que al empezar una transición IPv6 se evalúa las necesidades, se planifica su distribución, uso y gestión (Jordi Palet 2011). Para ello es necesario tener en cuenta las siguientes recomendaciones:

- Estimar las direcciones necesarias.
- Contemplar la asignación de direcciones a diferentes redes y subredes, tanto presentes como futuras.
- Redes en las que se implementará IPv6.

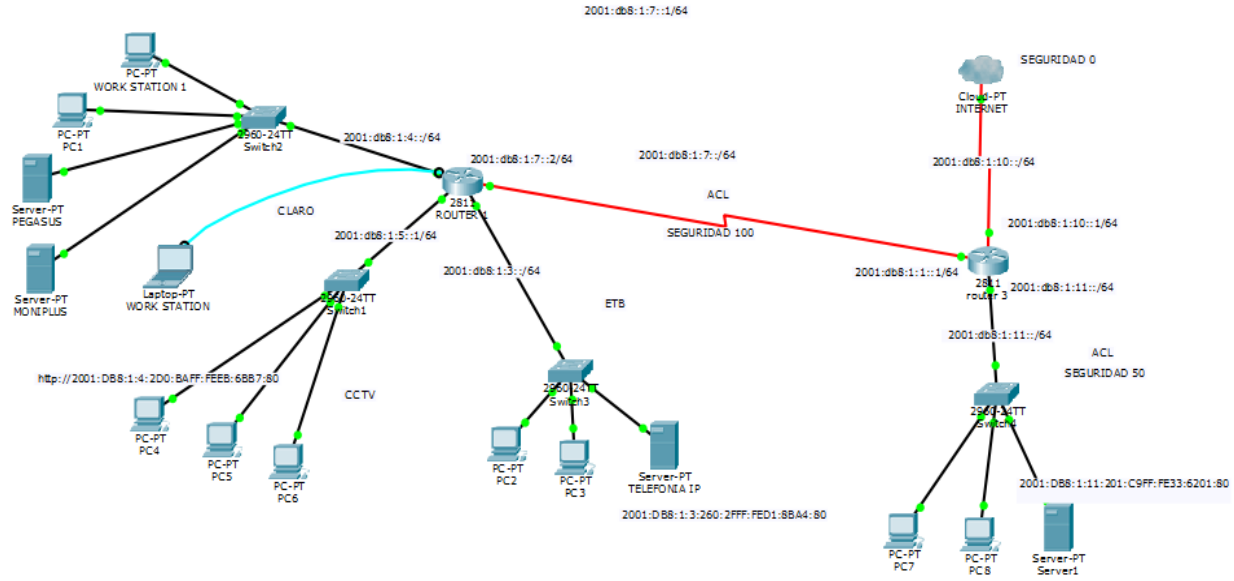
- Número y tipo de servicios ofrecidos.
- Distribución geográfica de la red.
- Estimación de las direcciones necesarias para uso interno.
- Criterios de asignación de prefijos a cada tipo de usuario y red.
- Topología de la red
- Protocolos de *Routing*

Diseño de la red por medio de IPV6

Para el diseño de la red se platea usar los equipos Cisco disponibles que pueden soportar IPv6, se verifican que la infraestructura soporte los respectivos cambios para la nueva red en IPv6 con equipos finales, buscar dispositivos de la red necesarios para la implementación y desarrollo: *Router*, *Switches*, Servidores, Cpe, Ordenadores, Sistemas Operativos (Windows, Linux, Mac).

Se plantea la opción de usar equipos Cisco por su optimo desempeño en redes industriales, el respaldo que se tiene al contar con un proveedor que ha estado de la mano con cada mejora hecha al estudio de las redes y ha participado activamente en los avances de IPV6.

Cisco cuenta con un programa de soporte técnico llamado Cisco Smart Net que permite soporte técnico las 24 horas del día en los dispositivos que cuentas con este servicio, reemplazo de hardware si es necesario en un plazo de 12 horas hábiles, esto brinda mayor confiabilidad a la hora de escoger el tipo de quipos que se proponen para la red de la compañía. Como se muestra en el Esquema 1. Topología propuesta en simulación de la red IPv6



Esquema 1. Propuesta diseño red IPv6 Siete 24 LTDA.

Método de diseño

Para el diseño de la red en IPv6 se implementó Método Flexible, se especifica en el RFC3531 como una manera flexible de asignar los bits de un prefijo que permite posponer al máximo la decisión del número de bits a asignar mediante el método de bits más significativos a la derecha se realiza la asignación de direcciones.

Si se divide una dirección IPv6 en N partes (p1, p2, pn), la asignación de direcciones de p1 se hará usando los bits más a la izquierda, la de pn usando los bits más a la derecha y para el resto (p2, …, pn) se fijará un límite arbitrario y se usarán los bits centrales de cada parte.

Segmentación de la red

Para el diseño de la red en IPv6 se implementó Método Flexible, se especifica en el RFC3531 como una manera flexible de asignar los bits de un prefijo que permite posponer al máximo la decisión del número de bits a asignar mediante el método de bits más significativos a la derecha se realiza la asignación de direcciones.

Si se divide una dirección IPv6 en N partes (p1, p2,…, pn), la asignación de direcciones de

p1 se hará usando los bits más a la izquierda, la de pn usando los bits más a la derecha y para el resto (p2, …, pn) se fijará un límite arbitrario y se usarán los bits centrales de cada parte.

Luego de segmentar la red se deben asignar las direccione IP a todos los dispositivos con que cuenta la compañía se propone hacerlo con HDCPV6 (*Dynamic Host ConfigurationProtocol*). El protocolo DHCPv6 se describe en la RFC 3315 de los autores, Droms, R, J.; Volz, B.; Lemon, T.; Perkins, C.; Carney, M (2003). La información intercambiada puede evolucionar y cambiar rápidamente sin afectar los mecanismos, esta separación ofrece al protocolo una estabilidad y cierta capacidad para ser extendido. Esta separación entre el protocolo y la información. Una unidad del protocolo DHCP sigue el patrón clásico de las estructuras protocolarias: una cabecera que contiene la información propia al protocolo, seguida de una carga útil que alberga la información aplicativa [9].

Cada mensaje DHCP tiene un formato de encabezado idéntico. Desde este punto de vista, DHCP sigue los principios que condujeron al diseño del segmento TCP: un formato único para todo el conjunto de funciones de TCP. Estos principios privilegian la simplificación en el proceso de desarrollo del protocolo.

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

- **Asignación manual:** El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC (*Media Access Control*) y procede a asignar la que configuró el administrador.
- **Asignación automática:** Al cliente DHCP (ordenador, impresora, etc.) Se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.
- **Asignación dinámica:** El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al *clientServer* que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

Distribución de direcciones por DHCP

Se crean diferentes *pools* para las diferentes áreas de la empresa como lo son: nomina, contabilidad, operaciones, recursos humanos, logística, tecnología, sistemas, asignándole un prefijo a cada una de ellas, esto permite una mejor organización de las direcciones y los permisos que requiera las subredes, con las siguientes líneas de código se puede generar el *pool* con su respectiva dirección

IPv6local pool claro 2001:DB8:1:4::/64 64

IPv6local pool contabilidad 2001:DB8:1:3::/64 6

Viabilidad

Esta fase comprende, primero, la simulación del modelo de la arquitectura; se recomienda el emulador *Cisco Packet Tracer*, que por su similitud con los equipos físicos en cuanto software y hardware puede funcionar como un equipo virtual, que permite ver la viabilidad del diseño de la red propuesta, con el fin de justificar la renovación tecnológica de la compañía. Todos los routers son marca Cisco y esto en parte representa una ventaja ya que Cisco, como parte activa del grupo que definió la estandarización de IPv6 y miembro fundador del "IPv6 *Forum*", ha implementado en sus equipos los principales mecanismos de transición a IPv6 para que puedan usarse a partir de la versión *Release* 12.2 (2) T del IOS que es la que admite las funcionalidades de IPv6.

Los routers de los enlaces troncales: Cisco 1750, Cisco 2509, Cisco 2511 y el router de la red local Cisco 1700 deben ser necesariamente reemplazados ya que tienen versiones inferiores a la 12.2(2) T del IOS y tampoco permiten una actualización del IOS. Existen 3 modelos de routers que podrían reemplazar a los equipos que no soportan IPv6, estos son: Cisco 1841, Cisco 3825 y Cisco 2821[9].

De estos tres modelos, el router Cisco 2821 tiene una memoria RAM de 256MB y expandible hasta 1GB, una memoria flash de 64MB expandible hasta 256MB y también incluye un firewall IPv6, de modo que este modelo puede reemplazar a los otro routers que no soportan IPv6. El router Cisco 1841 es recomendado para empresas pequeñas empresas y podría este

reemplazar al router Cisco 1700 que se encuentra en la red local del ISP y brinda servicios a los clientes del edificio, pero, dado que una migración a IPv6 puede representar el proveer nuevos servicios por parte del ISP, como las aplicaciones de VoIP, por ejemplo, el router Cisco 2821 posee un mejor soporte para estas aplicaciones. El router Cisco 3825 es usado para empresas grandes y su uso se basa principalmente en las aplicaciones de VoIP, además es demasiado costoso en relación a los equipos Cisco 1841 y 2821. Por estas razones el router Cisco 2821 sería el equipo que el proveedor puede usar para reemplazar tanto a los routers de los enlaces troncales como para el router usado en la red local. Además, este equipo es recomendado por Cisco para los proveedores de Internet que estén empezando a planificar su migración a IPv6 [9].

Los servidores en Linux no necesitan cambiarse pues las configuraciones requeridas para implementar IPv6 solamente deben hacerse en los archivos de configuración de los servidores; es decir, la configuración es hecha solamente a nivel de software, para la migración primeramente debe existir una coexistencia entre IPv4 e IPv6, razón por la cual todos los equipos, incluyendo al host, deben soportar esta coexistencia dual.

La mayoría de usuarios usan los sistemas operativos de Microsoft que es generalmente más popular que Linux, Windows XP, Windows Server 2003 y Windows Vista soportan una arquitectura dual de IPv4 e IPv6, pero la diferencia es que en Windows Server 2003 y Windows Vista IPv6 viene instalado y listo para configurar y usar.

El soporte para IPSec en Windows XP y en Windows Server 2003 es limitado, de modo que se requieren ciertas configuraciones adicionales para habilitar ciertos parámetros que sean requeridos. Hay que señalar que esto está más orientado a los hosts que utilizan Windows y con el uso de IPv6 la implementación de IPSec es obligatoria.

Teniendo en cuenta las recomendaciones de fabricante se siguen los siguientes pasos:

- Construir la red según las necesidades de la compañía.
- Realizar pruebas previas (prototipos, simulaciones).
- Proponer el diseño de la nueva red.
- Soporte de la Plataforma a IPv6.
- Soporte de las aplicaciones a IPv6.

- Direccionamiento *Unicast* IPv6.
- DHCPv6.
- Seguridad a nivel de *host* y tráfico IPv6.
- Priorización de entrega de tráfico de IPv6.
- Realizar pruebas de aceptación en el nivel del sistema (cumplimiento de objetivos).
- Coexistencia del protocolo ipv4 con el protocolo IPv6.
- Simular una red virtual de prueba para IPv6.
- Configurar la infraestructura de DNS.
- Actualizar equipos con IPv4 a IPv4/IPv6.
- Documentar los resultados.

Esta etapa comprende de analizar los datos que se realizaron con la simulación si son los esperados se procede a realizar la validar la aprobación del diseño de la red nueva en la actual la arquitectura física de la red.

Optimización de la red

- La integración de IPv4 e IPv6 no debe afectar a los servicios y aplicaciones existentes.
- No debe haber ninguna reducción en la seguridad de la red derivada de la migración hacia IPv6.
- Se reutilizará la infraestructura existente, capacidades, contenidos y entornos de aplicación siempre que sea posible.
- Redes y sistemas solo con IPv6 (Objetivo Final).

Conclusiones

- El espacio de 128 bits que IPv6 posee para las direcciones es cuatro veces más grande que el espacio para IPv4. Con tal cantidad de direcciones en IPv6 cada habitante de la tierra tendría su propia dirección y aun así seguirían existiendo direcciones IPv6 libres, se estima que habrían $6.65x10^{23}$ direcciones IPv6 por cada metro cuadrado

en la Tierra.

- La seguridad es uno de los principales requerimientos a la hora de plantear esta versión del protocolo beneficiando a las aplicaciones en cuanto a autenticación y encriptación de datos en forma transparente. Cabe señalar que IPv4 no poseía la seguridad ni menos encriptación de datos, para ello era necesario usar software de encriptación basados en varios estándares, uno de los más utilizados fue IPSec. Es precisamente en este que se basa la encriptación incluida en IPv6.
- La autoconfiguración de las direcciones en IPv6 es una nueva característica muy importante porque facilita el manejo de la red y la configuración por parte de los usuarios. La característica de autoconfiguración es un proceso flexible y permite generar una dirección IPv6 automáticamente a una PC local en ausencia de un servidor DHCPv6 *Router*.
- Al hacer la propuesta del diseño de la red IPV6 se encontraron muchos documentos de apoyo que facilitan la configuración y el diseño de la red, no es engorroso y es muy viable para cualquier empresa, esta migración no ha sido aceptada por el ingeniero de TI de la compañía Siete24 LTDA. Debido a que es claro que se necesita hacer una inversión en equipos que muchas veces las empresas no lo consideran necesario.
- Los cambios que actualmente se están dando en el desarrollo de la comunicación con la creación de dispositivos portátiles, de entretenimiento, y equipos tanto para el hogar como para la empresa hacen que IPv6 sea cada vez más requerido debido a los servicios que se pueden obtener y de allí la rentabilidad.

Bibliografía de consulta

[1]. ¿Qué es IPv6?, Ministerio de Energía, Turismo y Agenda Digital (Gobierno de España), Recuperado el 9 de octubre de 2017 de: http://www.ipv6.es/es-ES/introduccion/Paginas/QueesIPv6.aspx

[2]. Fundamentos de IPv6, IPv6 MX, IAR México, NIC México, Recuperado el 9 de octubre de 2017 de: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6#

[3]. Plan de migración de IPv4 a IPv6 para una red de un proveedor de servicios de internet (ISP), Ing. Remmy A. Llanos Gómez, (2016), Recuperado el 10 de octubre de 2017 de: http://www.revistasbolivianas.org.bo/scielo.php?pid=S2075-

89362016000100006&script=sci_arttext

[4]. Diseño e implementación de redes IPv6 en MIPYMES, Becerra Cobos Juan Camilo, Simbaqueva Buitrago Jerson Ricardo y Valenzuela Suarez Andrés Felipe, (2013), Recuperado el 10 de octubre de 2017 de: https://repositorio.escuelaing.edu.co/bitstream/001/222/1/FA-Ingeniería%20de%20Sistemas-1030580047.pdf

[5]. DHCPv6, Shane Kerr (ISC), Octubre 2006, Recuperado el 8 de octubre de 2017 de: http://meetings.ripe.net/ripe-53/presentations/dhcpv6.pdf

[6]. Protocolo DHCPv6, Association G6, Septiembre 2012, Recuperado el 8 de octubre de 2017 de: http://livre.g6.asso.fr/index.php/Protocolo_DHCPv6

[7]. RIPng, Villafán Canizares Juan Sergio, Recuperado el 8 de octubre de 2017 de:https://es.scribd.com/document/231489534/RIPng

[8]. 5 cosas que debes saber sobre la seguridad en IPv6, Carol Wilson, Oswaldo Aguirre, Recuperado el 8 de octubre de 2017 de: http://www.ipv6ve.info/sobre-seguridad/5-cosas-que-debes-saber-sobre-la-seguridad-en-ipv

[9]. IPv6 Implementation Guide, Cisco IOS Release 15.2S, 2012 Cisco Systems, Inc., Recuperado el 10 de octubre de 2017 de: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/xe-3s/ipv6-xe-36s-book/ip6-ipsec.pdf

[10]. Estudio para la migración de ipv4 a ipv6 para la empresa proveedora de internet milltec s.a., Nuñez David, (2009), Recuperado el 7 de octubre de 2017 de: http://studylib.es/doc/1265365/cd-2447.pdf

[11]. Protocolos de Transporte, Universidad Carlos III de Madrid (Grupo 2012-02), (2012), Recuperado el 7 de octubre de 2017 de: http://www.it.uc3m.es/lpgonzal/protocolos/transporte.php

[12]. El protocolo UDP, Networking and Emerging Optimization, Recuperado el 7 de octubre de 2017 de: http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/udp.html

[13]. IP de uso general ACL de la configuración, Cisco Systems, Inc., (2016), Recuperado el 7 de octubre de 2017 de: https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/26448-ACLsamples.html

[14]. Giira.udistrital.edu.co. (2016). Grupo de Investigación en Interconexión de

Redes Académicas, Recuperado el 7 de octubre de 2017 de http://giira.udistrital.edu.co/cvlac/

[15]. CCNA. (2014). Introducción al enrutamiento y reenvío de paquetes CCNA Exploration - Conceptos y protocolos de enrutamiento. Recuperado el 7 de octubre de 2017 de: https://sites.google.com/site/uvmredes2/1-introduccion-al-enrutamiento-y-reenvio-de-paquetes/1-3-construccion-de-la-tabla-de-enrutamiento

[16]. Diseño completo de una red de datos IPv6, Olivares H Rubén, (2012), Recuperado el 7 de octubre de 2017 de: https://riunet.upv.es/bitstream/handle/10251/80458/OLIVARES%20-%20Dise%C3%B1o%20completo%20de%20una%20red%20de%20datos%20IPv6.pdf?sequence=1&isAllowed=y

[17]. Despliegue de IPv6, Vives Alvaro, (2012), Recuperado el 7 de octubre de 2017 de: http://www.eslared.org.ve/walc2012/material/track2/DIA1-1-Consulintel_Curso-IPv6_WALC2012.pdf

[18]. Modelado específico de dominio para la construcción de learning objects independientes de la plataforma. Montenegro Marín, C E. (2011), Recuperado el 7 de octubre de 2017 de:https://dialnet.unirioja.es/servlet/tesis?Codigo=23791

[19]. Cisco IOS IPv6 Configuration Guide, Release 12.4, Estados Unidos: Cisco Systems, Inc., 648 pp., (2008) Recuperado el 7 de octubre de 2017 de: de.www.cisco.com

[20]. Migrating to IPv6: a practical guide to implementing IPv6 in mobile and fixed networks. Blanchet, Marc, (2006), Inglaterra: John Wiley &Sons Ltd

[21]. TCP/IP Tutorial and Technical Overview.8ª edición R, Lydia Parziale, David T. Britt, (2006), Recuperado el 7 de octubre de 2017 de: https://sites.google.com/site/ccna2redii/1-introduccion-al-enrutamiento.

[22]. Loshin, Pete (1999). IPv6 clearly explained. Estados Unidos: Morgan Kaufmann Publisher, Inc. 297 pp.

[23]. Miller, Mark A (2000). Implementing IPv6. 2a ed. Estados Unidos: M&T Books, 406 pp

[24]. Ramírez, Sergio, María Cervantes. Introducción al IPv6. Universidad de la República.

[25]. Waddingtin, Daniel G, Fangzhe Chang (2002). Realizing the Transition to

IPv6. IEEE Communications Magazine. Vol. 6, issue 3., pp.38-48

[26]. Mark A. Miller (2000), M&T Books Implementing IPv6, 2nd Edition.

Referencias

[1]. Ministerio de Tecnologías de la Información y las Comunicaciones (2011) Promoción del ipv6 en Colombia (Circular) http://www.mintic.gov.co/portal/604/w3-article-5932.html

[2]. Ministerio de Tecnologías de la Información y las Comunicaciones (2015) 40 Instituciones han comenzado el proceso de implementación de ipv6 en Colombia (Artículo) http://www.mintic.gov.co/portal/604/w3-article-5421.html.

[3]. Rodríguez J., y González R Robinsón. (2016). *Desarrollo de modelo para estandarizar la configuración DNS en routers de dos diferentes proveedores*. (Tesis de Pregrado). Recuperado de http://repository.udistrital.edu.co/bitstream/11349/5338/1/rodriguezchaparrojonathanandres2016.pdf

[4]. Araque J C., y Espinosa S L. (2015). *Desarrollo de un modelo para la configuración VLAN de switch de las plataformas Cisco y Huawei.* (Tesis de Pregrado). Universidad Francisco José de Caldas. Bogotá, Colombia.