



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO DE PLAN DE MIGRACIÓN Y SEGURIDAD DE IPV4 A
IPV6 PARA REDES DE EMPRESAS MEDIANAS Y PEQUEÑAS
A BAJO COSTO ORIENTADO A LA EMPRESA CHIFLES S.A”

INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

PAOLA ELENA CARRASCO ECHEVERRÍA

FREDDY JAVIER FRERE QUINTERO

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A Dios por permitirme alcanzar este objetivo, a mi familia por sus consejos, por la motivación constante y por ser ejemplo de perseverancia.

Freddy Frere Q.

Mis padres y hermanas por su apoyo y amor incondicional, a mis tíos Rita y Oswaldo por estar siempre junto a mí. A Luis por su ayuda y paciencia durante el desarrollo de este proyecto.

Paola Carrasco E.

DEDICATORIA

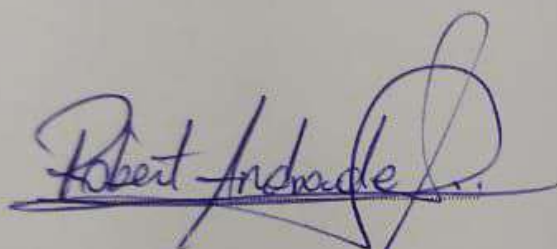
A Dios por ser quien guía mis pasos, a mis padres y a mis hermanos por ser mi apoyo incondicional y el pilar fundamental de mi vida.

Freddy Frere Q.

A Dios por bendecirme en todo tiempo, a mi familia por ser mi pilar y a Luis por ser mi apoyo en todo momento.

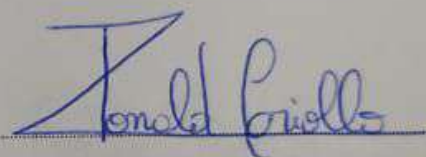
Paola Carrasco E.

TRIBUNAL DE EVALUACIÓN

A handwritten signature in blue ink, reading "Robert Andrade Troya". The signature is stylized with a large, looping flourish at the end.

MSc. Ing. Robert Andrade Troya.

PROFESOR EVALUADOR

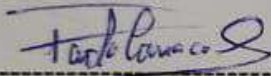
A handwritten signature in blue ink, reading "Ronald Criollo Bonilla". The signature is stylized with a large, looping flourish at the end.

Msig. Ronald Criollo Bonilla

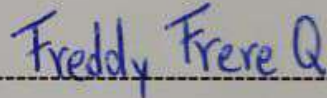
PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Paola Elena Carrasco Echeverría



Freddy Javier Frere Quintero

RESUMEN

En este proyecto se realizará el diseño del plan de migración de IPv4 a IPv6 de la empresa Chifles S.A, la compañía en mención presenta problemas en la comunicación entre sus trabajadores remotos y su servidor de pedidos.

En este trabajo analizaremos y dejaremos planteado que método de transición usará la empresa para llevar a cabo esta migración, teniendo en cuenta que la compañía desea mantener activo el funcionamiento de sus servicios de red durante la transición y espera que sean afectados lo menos posible.

ÍNDICE GENERAL

AGRADECIMIENTOS.....	ii
DEDICATORIA	iii
TRIBUNAL DE EVALUACIÓN	iv
DECLARACIÓN EXPRESA	v
RESUMEN	vi
ÍNDICE GENERAL.....	vii
CAPÍTULO 1	1
1. GENERALIDADES	1
1.1 Objetivo General.....	1
1.2 Objetivos Específicos.....	1
1.3 Antecedentes.....	1
1.4 Estado Actual de la Red	3
1.5 Fundamentos Teóricos	7
1.5.1 Funcionamiento Mobile IPv4.....	7
1.5.2 Seguridad en IPv6	9
1.6 Escenarios de migración.....	12
1.6.1 Escenario A: Router de Borde con Soporte IPv4 e IPv6.....	13
1.6.2 Escenario B: Router de Borde con Soporte Dual Stack.....	14
1.6.3 Escenario C: Servidores alojados en la red interna de la empresa	15
1.6.4 Escenario D: Trabajadores Remotos	16
CAPÍTULO 2.....	21
2. DISEÑO DE LA SOLUCIÓN	21
2.1 Plan de migración	21
2.2 Conexión a internet mediante IPv6	22
2.3 Configuración básica de los equipos en IPv6	22
2.3.1 Configuración de rutas estáticas en IPV6	23

2.4	Etapas de transición a IPv6	23
2.4.1	Etapa 1: Mantener IPV4 al mundo y tener IPV6 en la red local.....	24
2.4.2	Etapa 2: Tener IPV6 en el mundo y tener IPV6 en la red local.....	25
2.4.3	Resultados de la configuración de las etapas de la transición	27
2.4.4	Funcionamiento del Mobile IPv6	28
2.4.5	Funcionamiento de los Teléfonos IP	29
2.5	Direccionamiento de IPv4 en red Actual	29
2.6	Esquemas de los diagramas lógicos.....	32
2.6.1	Esquema de la topología de red IPV6	32
2.6.2	Diseño de las Vlans	32
2.6.3	Reglas de conectividad entre VLANS	36
2.6.4	Direccionamiento IPV6 en la red de la empresa Chifles S.A ..	37
2.6.5	Servicios de la Intranet Sobre IPV6	38
2.6.6	Evaluación del esquema lógico.....	41
2.7	Diseño del esquema físico.....	42
2.7.1	Evaluación del esquema Físico	42
CAPÍTULO 3.....		45
3.	IMPLEMENTACIÓN	45
3.1	Programación de Trabajo	45
3.2	Consideraciones generales pre-migración.....	47
3.3	Presupuesto del proyecto.....	48
CONCLUSIONES Y RECOMENDACIONES.....		49
BIBLIOGRAFÍA.....		51
ANEXOS		53

CAPÍTULO 1

1. GENERALIDADES

1.1 Objetivo General

El principal objetivo de este proyecto consiste en la elaboración de un plan de acción para la migración del protocolo de comunicaciones IPv4 al protocolo IPv6, en la red de una pequeña o mediana empresa (PYME). Definiendo así, todos los posibles procedimientos y requerimientos para garantizar la correcta funcionalidad de la red y los servicios que en ella se prestan.

1.2 Objetivos Específicos

Entre los objetivos específicos de este trabajo, se encuentran los siguientes:

- Analizar la situación actual de la infraestructura de red.
- Establecer los diversos métodos de transición de arquitecturas de red IPv4 a IPv6.
- Elaborar análisis de ventajas y desventajas de la transición.
- Realizar el diseño del plan de direccionamiento y VLAN's.
- Desarrollar el plan de migración de la red.
- Crear plantillas de configuración de los equipos.

1.3 Antecedentes

Chifles S. A. es una empresa dedicada a la producción y venta de chifles de plátano y tubérculos (yuca, camote y papa). Cuenta con 2 sucursales ubicadas en Quito y Guayaquil. La empresa consta de un cuarto de cómputo localizado en cada oficina, en los cuales se encuentra los servidores que alojan los servicios necesarios para el funcionamiento del negocio, tales como; el servidor web (www.chifles_ecuador.com) y el servidor de correo con su dominio chiflsecuador.com. La empresa además de ello cuenta con 2 servidores los cuales se encuentran alojados en una red externa de la compañía. El servicio de hosting es proporcionado por Inventio – ESPOL, estos servidores son de video conferencias y de recepción de pedidos respectivamente.

Además de ello para que su producto tenga mayor alcance cuenta con vendedores externos, ellos se dedican a ir a los puntos de venta del producto para ofertarlo y tomar los pedidos.

Esta empresa consta de las siguientes áreas:

- Área de producción y empaquetado
- Departamento de Sistemas
- Departamento de Recursos Humanos
- Departamento de contabilidad
- Gerencia
- Departamento de Ventas
- Departamento de Distribución

Chifles S. A. es una compañía catalogada como PYME (Pequeña y Mediana Empresa) debido a la limitada cantidad de usuarios con la que labora. Sin embargo; a causa del éxito que tienen sus productos en las ciudades donde se encuentran ubicadas sus oficinas, está por convertirse en una empresa de mayor jerarquía a causa de la creciente demanda de chifles en las localidades mencionadas anteriormente y en el resto de provincias del Ecuador.

Esta entidad considera que el estar a la vanguardia tecnológica corresponde a un pilar fundamental para continuar con el éxito empresarial que lleva hasta el momento. El departamento de sistemas de Chifles S.A. recibe capacitación constante en temas de networking, desarrollo y demás. Estos han escuchado los beneficios que ofrece la arquitectura de red IPv6 sobre su predecesora IPv4.

Dentro de 3 meses Chifles S.A. desea realizar la renovación total de su equipamiento activo de red, conociendo ya las bondades de IPv6, la entidad desea que los equipos y configuraciones a realizarse permitan ejecutar la implementación de la nueva arquitectura de red en ambas oficinas. Para ello, la empresa desea conocer de un plan de migración que considere y analice todas las metodologías y procesos necesarios a tomar en cuenta para la migración a dicha arquitectura.

Adicional a esto, a través del plan de migración a IPv6 será posible hacer un análisis del funcionamiento de este nuevo protocolo en la red de Chifles S.A y ver el impacto positivo que tendría en la comunicación que se realiza con sus vendedores externos.

Hay que recalcar que Chifles S.A en la actualidad sufre de algunos problemas de red, los cuales se mencionan a continuación:

- Servicio de video conferencia intermitente y poco confiable.
- Retardo elevado en conexión con servidor de pedidos.
- Problemas con servidor DHCP (en router).
- Movilidad limitada en usuarios remotos.

Si bien es cierto, Chifles S.A desea realizar la migración de su infraestructura a IPv6, es obvio suponer que la empresa quiere determinar la causa de estos problemas y a la vez mitigarlos para que no afecten a la nueva arquitectura.

1.4 Estado Actual de la Red

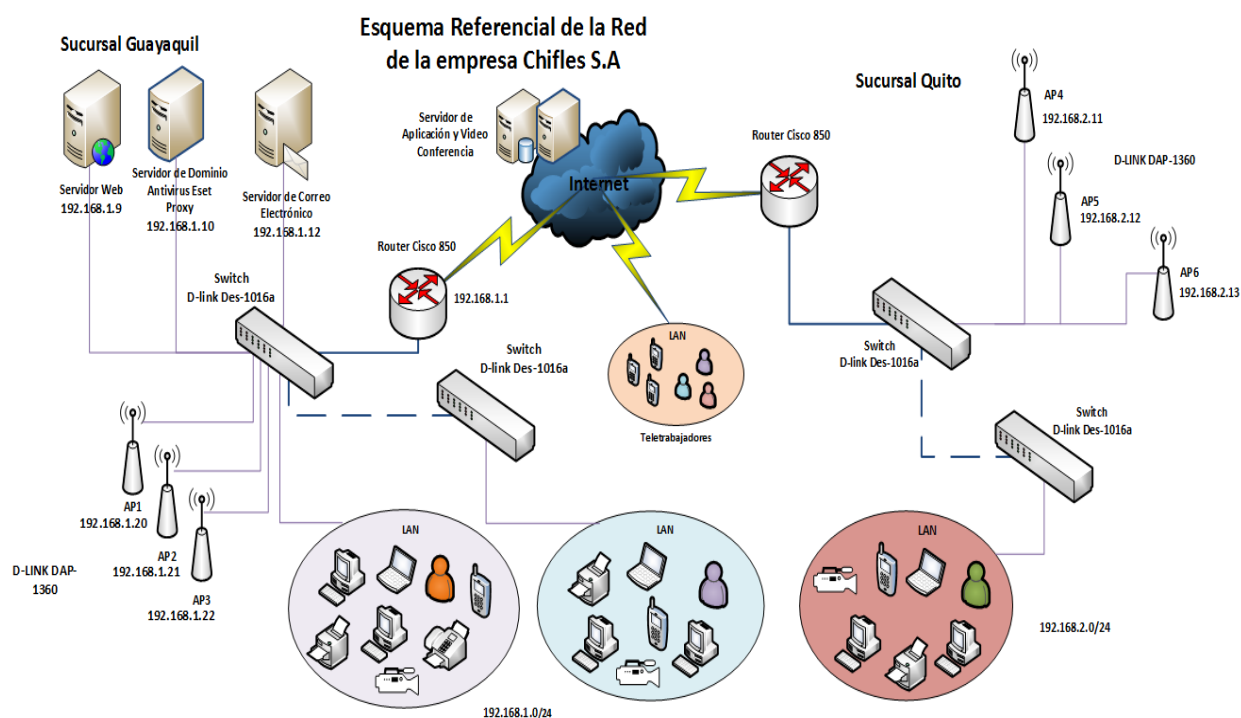


Figura 1.1: Topología actual de la red

La red de Chifles S.A se divide en dos estructuras: la LAN de Quito y la LAN de Guayaquil (ver Figura 1.1), las mismas se detallan según las especificaciones presentadas a continuación:

Guayaquil: Esta es la matriz de Chifles S.A (ver Figura 1.2) cuenta con un ISR (Router de servicios integrados) Cisco 850 el cual sirve para brindar los servicios de conectividad hacia internet a los equipos y servidores que se encuentran ocultos “detrás” de él. Adicionalmente facilita la conexión remota que realizan los vendedores que laboran en el exterior de la compañía, con los servidores internos de la red y externos de la misma. Cabe mencionar que estos equipos están discontinuados y ya cumplieron su tiempo de vida útil. A este router se conecta un switch no administrable de 16 puertos, el cual a su vez se interconecta con otro switch de 16 puertos no administrable; para de esta manera permitir que los usuarios finales, servidores y access points se comuniquen con el router mencionado anteriormente y así “salir” a internet.

La red inalámbrica de Chifles S.A esta conformado por 3 access points autónomos DLink, DAP - 1360

La oficina de Chifles S.A en Guayaquil posee 3 servidores físicos, los cuales se detallan a continuación:

- **Servidor Web:** En este servidor se almacena la página web de la empresa. Permite almacenar imágenes, información en forma de páginas web y cuando el usuario realiza una petición para acceder a la página, este lo muestra con ayuda del protocolo HTTP en formato HTML.
- **Servidor de Correo:** Permite enviar, recibir y almacenar correos para los clientes de la red
- **Servidor de Dominio:** Permite administrar la autenticación de los usuarios y el acceso a los recursos compartidos de la red.

Como se mencionó con antelación esta oficina cuenta con un total de 50 colaboradores, de los cuales 20 son usuarios de red. Dichos empleados comparten el mismo segmento de red que se encuentra delimitado por el siguiente bloque de direcciones IP privadas: 192.168.1.0/24.

Además de ello la sucursal cuenta con 5 teléfonos IP y 5 cámaras IP, las cuales son utilizadas por seguridad y monitoreo.

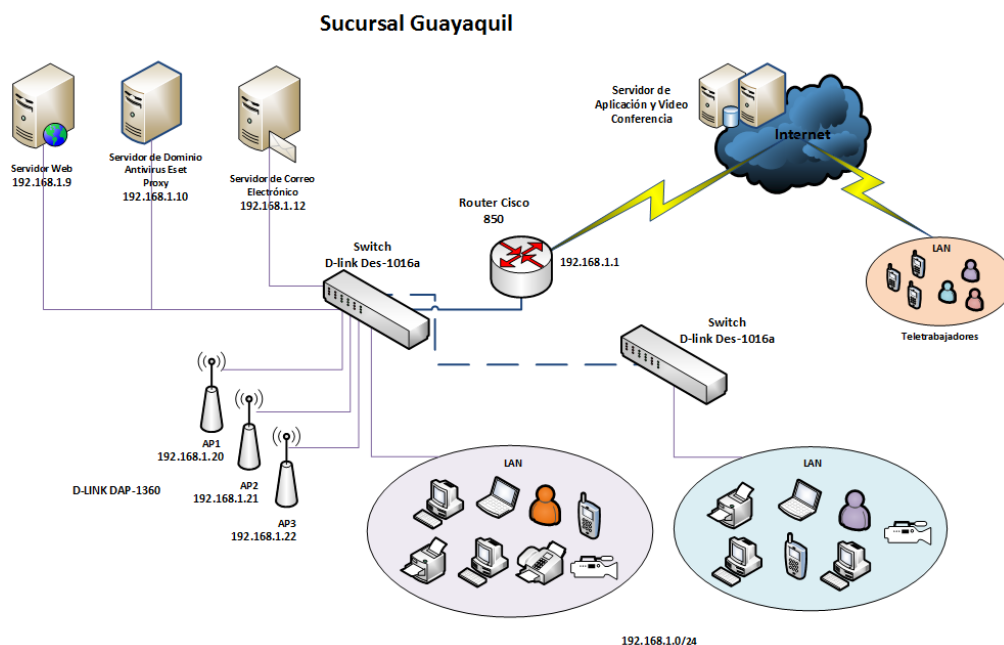


Figura 1.2: Topología actual Guayaquil

Quito:

La red de esta sucursal cuenta con un esquema similar a la LAN de Guayaquil que se detalló con anterioridad (ver Figura 1.3).

Tal como en Guayaquil, se cuenta con un ISR Cisco 850 el que brinda los servicios de conectividad hacia internet a los equipos y servidores que se encuentran ocultos “detrás” de él, permite la conexión remota que realizan los vendedores.

Cabe mencionar que estos equipos están discontinuados y ya cumplieron su tiempo de vida útil.

También se poseen 2 switches no administrables de 16 puertos que interconectan los usuarios finales con el router 850 y así contar con una ruta hacia internet.

La red inalámbrica de Quito posee las mismas características que la de la matriz de Chiffles S.A, con la diferencia de que solo existen 2 access points DLink.

En esta oficina laboran un total de 48 empleados, la red cableada de dicha sede se compone de 21 usuarios de red.

El segmento de red usado en esa sucursal es el: 192.168.2.0/24.

Además de ello la sucursal cuenta con 5 teléfonos IP y 5 cámaras IP, las cuales son utilizadas por seguridad y monitoreo.

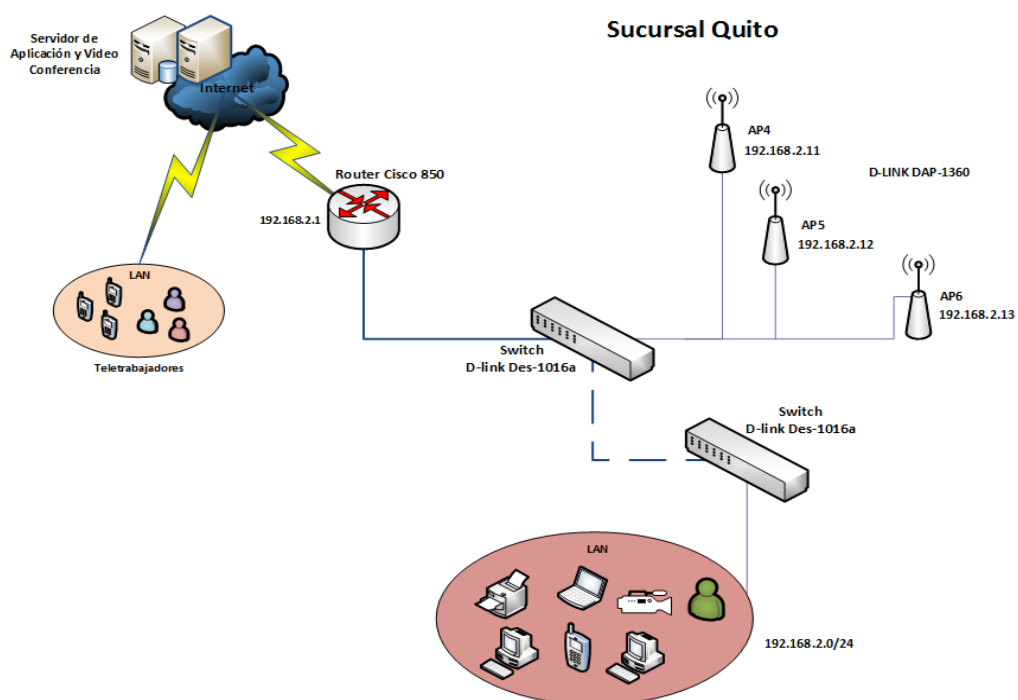


Figura 1.3: Topología actual Quito

Infraestructura externa

Adicionalmente la empresa cuenta con:

- **Servidor de inventario y pedidos:** En este servidor se almacena toda la información referente a inventarios, pedidos y venta de los productos que ofrece la compañía.
- **Servidor de conferencias:** Permite que los usuarios puedan realizar video llamadas o conferencias

Cabe recalcar que los servidores mencionados anteriormente están alojados en una red externa de la empresa Chifles S.A. El servicio de hosting es proporcionado por Inventio – ESPOL

Vendedores externos Quito y Guayaquil: Chifles S.A cuenta con un total de 54 vendedores externos que se dedican a ofrecer los productos que produce la compañía a las tiendas y despensas de cada una de las localidades mencionadas precedentemente. Estos usuarios se conectan a la red de Chifles S.A a través de conexiones “Mobile IPv4”, usando como dispositivo final un Handheld.

Situación actual de los trabajadores externos

Mobile IPv4 ofrece un mecanismo eficiente y escalable para nodos móviles dentro de Internet. Con Mobile IP, los nodos pueden cambiar sus puntos de acceso a Internet sin tener que cambiar su dirección IP. Esto permite mantener el transporte de datos y conexiones de alto nivel mientras el vendedor se moviliza. La movilidad del nodo es realizada sin la necesidad de propagar las rutas de los hosts a través del enrutamiento.

1.5 Fundamentos Teóricos

1.5.1 Funcionamiento Mobile IPv4

Mobile IP ofrece un mecanismo eficiente y escalable para nodos móviles dentro de Internet. Con Mobile IP, los nodos pueden cambiar sus puntos

de acceso a Internet sin tener que cambiar su dirección IP. Esto permite mantener el transporte y conexiones de alto nivel mientras se mueve. La movilidad del nodo es realizada sin la necesidad de propagar las rutas de los hosts a través del enrutamiento (ver Figura 1.4 y 1.5).

Agentes que intervienen en Mobile IPv4

- **Nodo móvil (MN):** Es un dispositivo móvil
- **Agente de Inicio (HA):** Un enrutador de la red propia que se encarga de tramitar la localización del MN
- **Agente extranjero (FA):** Es el enrutador de la red visitada que coopera con el HA para proporcionar movilidad.
- **Nodo Correspondido (CN):** Un nodo fijo o móvil con el que el MN se comunica.

Fases de Mobile IPv4

- **Detección de Agente:** En esta etapa el dispositivo móvil debe ser capaz de determinar si encuentra en su propia red o en una red nueva.
- **Registro:** El dispositivo después de determinar que no está en una red propia se registra con el Agente de Inicio con la nueva dirección dada por el Agente extranjero.
- **Enrutamiento y Túneles:** El dispositivo móvil se comunica con los diferentes nodos correspondidos, durante esta comunicación se forma un túnel entre el Agente de inicio y el Agente Extranjero.
- **Proceso de traspaso:** El nodo móvil cambia de subred. En este periodo se inicia nuevamente el proceso de detección de agente.

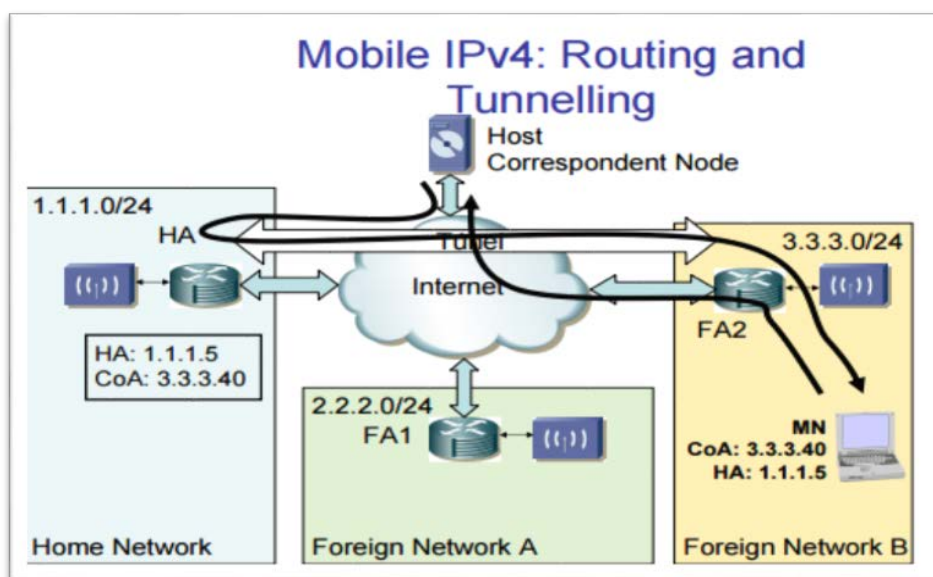


Figura 1.4: Fases de Mobile IPv4

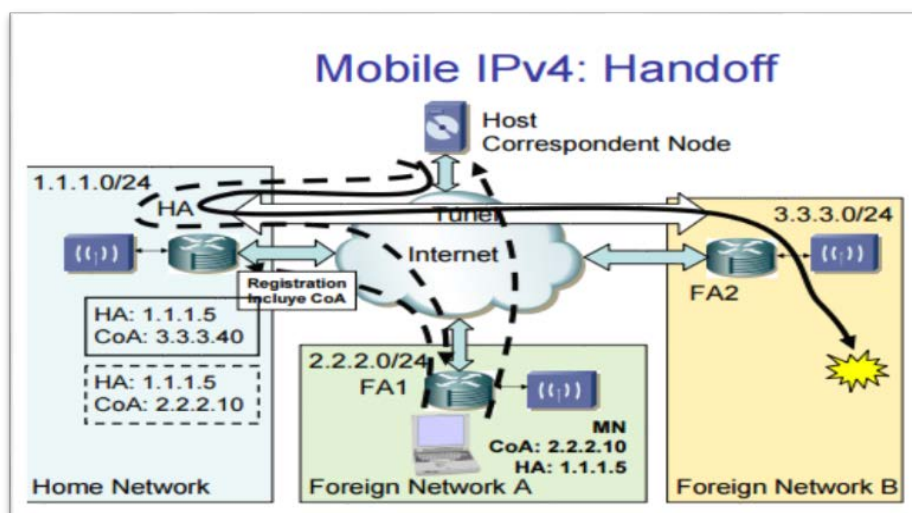


Figura 1.5: Fases de Mobile IPv4 en una red Diferente

1.5.2 Seguridad en IPv6

Además de los beneficios mencionados acerca del uso IPv6 mobile, una de las principales ventajas que obtenemos al implementar IPv6 es que podemos hacer uso del protocolo de seguridad IPsec. En el mismo se

definen políticas para asegurar la comunicación en la red. Adicional a esto, también describe como fortalecer esas políticas.

Al hacer uso de IPSec los nodos involucrados en la comunicación (computadoras o máquinas origen – destino) pueden garantizar la confidencialidad de los datos, la integridad de los mismos y la autenticación de la información en la capa de red. Otra de las ventajas que brinda IPsec es que:

- Soporta gran variedad de plataformas de sistemas operativos
- Brinda de manera integrada una solución de VPN si se desea la verdadera confidencialidad de los datos en la red.
- Es un estándar por lo que brinda interoperabilidad entre dispositivos diferentes
- La implementación del mismo es sencilla

El principal propósito de IPsec es el de proveer interoperabilidad, máxima calidad de la comunicación y seguridad cifrada de manera nativa. Este protocolo ofrece varios servicios de seguridad a la capa IP, además de ello brinda también protección a las capas superiores. Estos servicios de seguridad son, por ejemplo; control de acceso, integridad sin conexión, autenticación de datos desde el origen, protección en contra de la reproducción parcial o total de la información, confidencialidad (cifrado) y confidencialidad en el flujo del tráfico.

En las principales tecnologías embebidas dentro del protocolo de seguridad IPsec se encuentran:

- Data encryption standar (desk) de 56 bits y triple desk (3 desk) de 128 bits, los cuales son algoritmos de cifrado con claves simétricas para el cliente IPsec.
- Certificate authorities (CA) y Internet key exchange (IKE)
- Cifrado que puede ser desplegados en ambientes stand alone clientes, routers y firewalls

- Ambientes que pueden coexistir con el túnel L2TP

Modo de funcionamiento IPsec

IPsec tiene 2 modelos diferentes de funcionabilidad

- **Modo de transporte (transport mode, host-to-host):** En este modo la carga del paquete (payload) es encapsulado (mientras la cabecera se mantiene intacta) y el nodo remoto (a quien va dirigido el paquete) desencapsula el paquete.
- **Modo de túnel (Tunnel mode, Gateway-to-gateway / Gateway-to-host):** En este modo el paquete entero es encapsulado (se crea una nueva cabecera) y el host (o gateway) especificado en la nueva cabecera IP, desencapsula el paquete.

Entre las principales características de IPsec se encuentran los siguientes:

- **Authentication header (AH, cabecera de autenticación):** Esta cabecera provee autenticidad para los paquetes transportados, esto es hecho por medio de una suma de control (checksum) de los paquetes usando un algoritmo de cifrado.
- **Encapsulating security payload (ESP):** Mecanismo que provee cifrado a los paquetes.
- **IPcomp (IP payload compression):** Mecanismo que provee compresión antes del que el paquete sea cifrado.
- **IKE (Internet Key Exchange):** Mecanismo que provee (las opcionales) maneras de negociar las claves en secreto.
- **SPD (Security Police Database):** Sirve para manejar las políticas de seguridad y selecciona las co-relaciones entre dichas políticas y el tráfico actual de la red.
- **SAD (Security Asociation Database):** Brinda seguridad durante la asociación, parámetros necesarios para las conexiones de IPsec únicamente.

Aunque IPsec tradicionalmente provee conexiones remotas punto-punto por medio del uso de un túnel VPN, hay que recalcar que IPsec no es un mecanismo VPN como tal. De hecho, el uso de IPsec ha estado cambiando en los últimos años, desde que el mismo fue movido desde la WAN hacia la LAN para brindar seguridad al tráfico de la red en contra del espionaje y modificación de los datos.

Cuando dos computadoras desean comunicarse haciendo uso de IPsec, ellas se autentican mutuamente y negocian como cifrar y como firmar digitalmente el tráfico que ellos intercambian. Estas sesiones de comunicaciones IPsec son llamadas security associations (SAs)

1.6 Escenarios de migración

Aunque IPv6 es un protocolo de comunicaciones que no se encuentra implementado en la mayoría de las redes de empresas pequeñas o medianas, el origen del mismo data desde la década de los 90. Por ello, es común que gran cantidad de dispositivos en el mercado permitan realizar la implementación de dicho protocolo.

La principal desventaja de los equipos con este tipo de soporte consiste en que no se puede mantener una red híbrida (IPv4 e IPv6 trabajando de manera conjunta) y esto conlleva a un problema grave al momento de planear una migración de protocolos de comunicaciones.

Tal problema se origina debido a que la transición entre dichos protocolos o el tiempo en el cual ambas arquitecturas pueden coexistir juntas se ve afectado.

En conclusión, dependiendo de la topología se tendría que optar por:

- Realizar una migración completa a IPv6, lo cual elimina el proceso de transición y por ende afecta a la toda la infraestructura de la red.
- Realizar la migración implementando un proceso de transición con “artificios” lo cual añade complejidad a la configuración y administración de la infraestructura de la red.
- Abstenerse a realizar el cambio de protocolo de telecomunicaciones

A continuación en la Figura 1.6 la topología, en caso de realizar la implementación de un router con soporte IPv6:

1.6.1 Escenario A: Router de Borde con Soporte IPv4 e IPv6

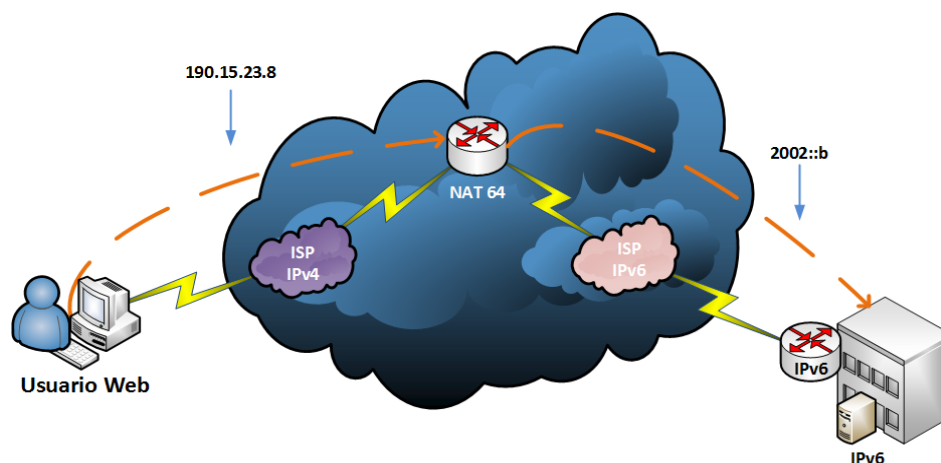


Figura 1.6: Topología con Router de borde con Soporte IPv4 e IPv6

Al realizar este tipo de implementación, el direccionamiento interno (LAN) de la red tiene que cambiar a IPv6, incluyendo a la granja de servidores de la compañía.

Es aquí donde se presentan mayores inconvenientes, debido a que; si bien es cierto, todos los usuarios (tanto internos como externos) de la red pueden continuar trabajando sin percibir ningún cambio en el uso de la red, los usuarios externos a la red que intenten acceder a un servicio (como el web), presentarán problemas de conexión debido a que se manejan con arquitecturas diferentes.

Como se detalla en el gráfico, se podría solventar el problema de la red por medio de la implementación de un servidor NAT64, el mismo mapeará una dirección IPv6 del pool perteneciente a la red, con una dirección IPv4 (perteneciente a la misma).

El problema con este escenario es que esa tarea la tiene que realizar un equipo externo a la red de la empresa o en consecuencia, adquirir un equipo adicional que cumpla con la función encomendada.

En el primer caso, el nivel de granularidad al cual podría llegar se ve afectado de manera directa, debido a que la administración del servicio es realizada por el proveedor de servicios de internet, esto es un problema si las políticas del mismo (configuración, seguridad y demás) son exhaustivas.

En el segundo caso, aunque la administración del servidor NAT64 se ejecutaría en las inmediaciones de la empresa, se realizaría la adquisición de otro equipo para que realice esta única tarea, esto conlleva a una inversión doble por parte de la compañía que lo desea implementar.

1.6.2 Escenario B: Router de Borde con Soporte Dual Stack

A continuación la topología en caso de realizar la implementación de un router con soporte Dual Stack:

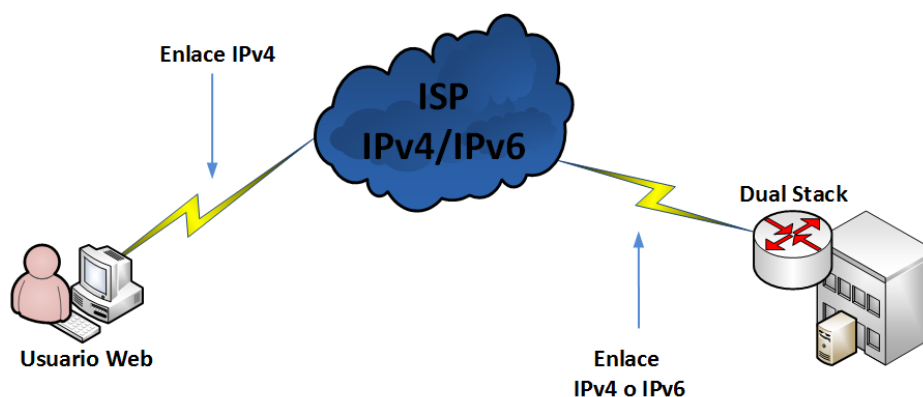


Figura 1.7 Topología con Router de borde con Soporte Dual Stack

Como se puede apreciar en la Figura 1.7, la solución es casi idéntica a cuando usamos un router en el escenario anterior. Difiere de que con un router con soporte dual stack, podemos hacer que ambos protocolos de comunicaciones coexistan en un mismo ambiente. Esto soluciona el

problema de los servidores, ya que los mismos podrían tener direccionamiento IPv4 e IPv6 y ser accesibles desde internet sin ningún problema. Otra forma de solventar dicho problema es con la traducción (NAT64) de estas direcciones, de tal manera que cuando se realice una consulta a la dirección IPv4 (anterior) de un servidor, el router de borde lo reenviará a la dirección IPv6 del servidor correspondiente.

Al realizar la implementación de un router con este tipo de soporte, incremento el nivel de granularidad (en cuanto a configuración) al cual se podría llegar, además de esto, la configuración de estas tecnologías no se verían limitadas por las políticas del proveedor de servicios de internet.

Otro beneficio es que por medio de esta solución, se evita realizar la adquisición de un equipo adicional para que realice las tareas especificadas anteriormente.

1.6.3 Escenario C: Servidores alojados en la red interna de la empresa

Una de las interrogantes que pueden surgir al ver el escenario A y B es: en el caso de tener los servidores en el interior de mi empresa, es decir, no en la nube aún se podría mantener la propuesta de migración a IPv6? La respuesta es que sí, IPv6 nos brindaría muchos beneficios en cuanto a seguridad se refiere sin tener la necesidad de adquirir o administrar equipos adicionales.

Además de los beneficios listados con anterioridad, una de las principales ventajas que obtenemos al implementar IPv6 es que podemos hacer uso del protocolo de seguridad IPsec. El mismo es un conjunto de estándares los cuales definen políticas para asegurar la comunicación en la red y describen como fortalecer esas políticas.

Al hacer uso de IPSec los nodos involucrados en la comunicación (computadoras o maquinas origen – destino) pueden garantizar la confidencialidad de los datos, la integridad de los mismos y la

autenticación de la información en la capa de red. Otras de las ventajas que brinda IPsec es que:

- Soporta gran variedad de plataformas de sistemas operativos
- Brinda de manera integrada una solución de VPN si se desea la verdadera confidencialidad de los datos en la red.
- Es un estándar por lo que brinda interoperabilidad entre dispositivos diferentes
- La implementación del mismo es sencilla

El principal propósito de IPsec es el de proveer interoperabilidad, máxima calidad de la comunicación y seguridad cifrada de manera nativa. Este protocolo ofrece varios servicios de seguridad a la capa IP, además de ello brinda también protección a las capas superiores. Estos servicios de seguridad son, por ejemplo; control de acceso, integridad sin conexión, autenticación de datos desde el origen, protección en contra de la reproducción parcial o total de la información, confidencialidad (cifrado) y confidencialidad en el flujo del tráfico.

En las principales tecnologías embebidas dentro del protocolo de seguridad IPsec se encuentran:

- Data encryption estándar (des) de 56 bits y triple des (3 des) de 128 bits, los cuales son algoritmos de cifrado con claves simétricas para el cliente IPsec.
- Certificate authorities (CA) y Internet key exchange (IKE)
- Cifrado que puede ser desplegado en ambientes stand alone clientes, routers y firewalls
- Ambientes que pueden coexistir con el túnel L2TP

1.6.4 Escenario D: Trabajadores Remotos

Anteriormente se detalló el funcionamiento de la red, tanto de manera interna como de manera externa (con IPv4 Mobile).

Al realizar la migración del router de borde, como era de esperarse, afectaría de manera directa a la forma por medio de la cual se conectan los usuarios remotos. Evidentemente, los mismos ahora realizarán sus funciones por medio del nuevo protocolo de comunicaciones, esto será transparente para ellos.

La primera gran diferencia con la topología de red original es que al realizar la implementación de IPv6, no podremos seguir haciendo uso de IPv4 Mobile, sin embargo esto representa un beneficio a la red, esto se debe a que con la nueva arquitectura de red, podremos hacer uso de IPv6 Mobile.

Este protocolo consta de muchas ventajas que eliminarán los problemas que actualmente presentan los trabajadores remotos.

IPv6 Mobile fue diseñado específicamente para brindar soluciones de movilidad real, integradas a IPv6, a diferencia de IPv4 mobile que solamente fue un parche para dicho protocolo (ver Figura 1.8).

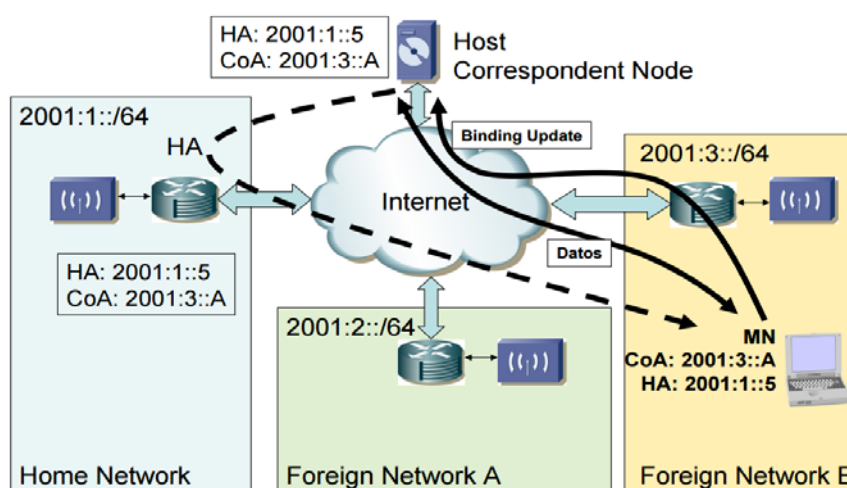


Figura 1.8: Funcionamiento IPv6 Mobile

Al hacer uso de IPv6 e IPv6 Mobile, se evita la necesidad de un "Foreign Agent", esto significa que no se requiere mantener la señalización con el router de la red remota, esto le resta delay al proceso de comunicación,

además de ello, evita que se tenga que declarar un pool de direcciones por cada Foreign Agent, estos beneficios ayudan a que se liberen recursos del router de borde.

Otro cambio importante en el nuevo protocolo de movilidad IP es que suprimo el "Triangle Routing" que sucedía con su predecesor. Esto significa que no habrá problemas de delay al comunicarse con los servidores virtualizados en el exterior de la compañía, simplificando así la administración de la infraestructura de la red debido a que se suprime el route optimization (usado como método de compensación para el triangle routing).

En conclusión, al hacer uso de IPv6 e implementar el protocolo de comunicaciones, se incrementa los niveles de movilidad a los cuales pueden llegar los trabajadores remotos.

Claro está que debido a que los trabajadores remotos recorrerán la ciudad o ciudades de manera constante, el alcance del direccionamiento IPv6 por parte del proveedor de servicios de la compañía será una limitante importante en cuestiones de movilidad. Como los dispositivos handhelds que usan los trabajadores remotos, soportan direccionamiento IPv6 e IPv4, a continuación una breve descripción de las posibilidades de comunicación con las que contarían los trabajadores remotos.

Trabajadores Remotos Haciendo Uso de IPv6:

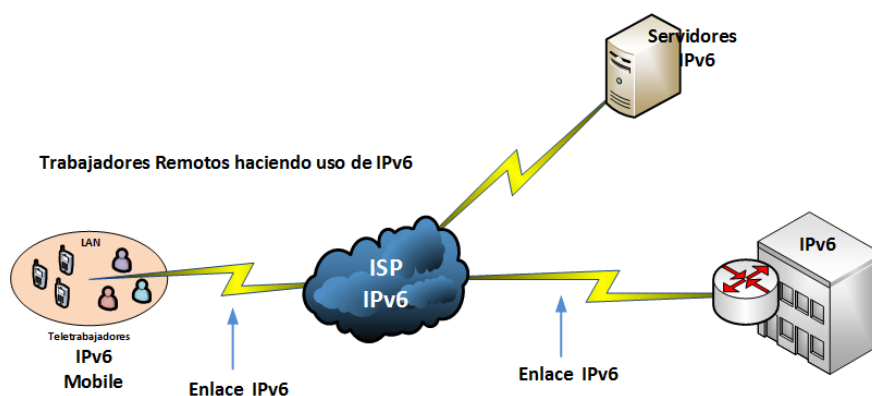


Figura 1.9: Topología de trabajadores Remotos Haciendo Uso de IPv6

Este es el típico caso en el que un trabajador remoto se encuentra laborando en un sector donde se puede trabajar con IPv6, este escenario es el ideal para la solución IPv6 a implementar. Esto se debe a que como la infraestructura LAN y de borde de la empresa, usará IPv6, la comunicación con los trabajadores remotos será totalmente transparente, compatible y no presentará problemas (ver Figura 1.9).

Trabajadores Remotos IPv6 en Red IPv4:

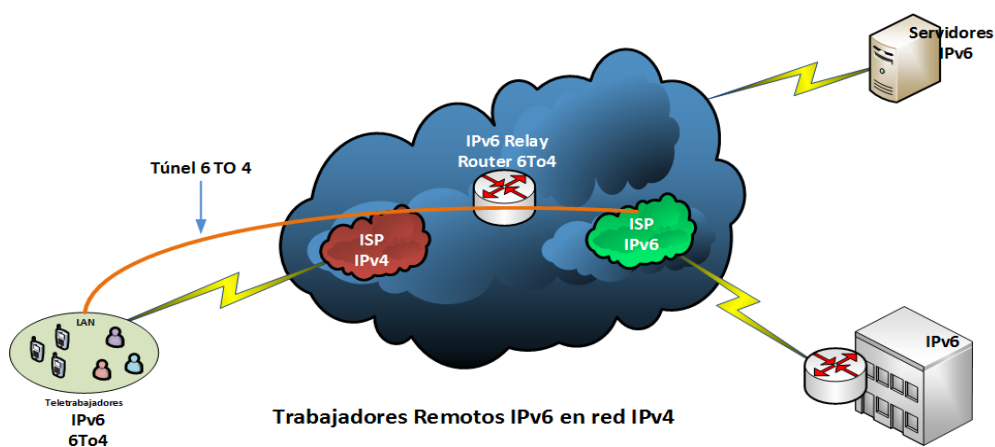


Figura 1.10: Trabajadores Remotos IPv6 en Red IPv4

En este escenario el trabajador remoto se encuentra en un sector en el cual por cuestiones de equipamiento activo, no se puede hacer uso del nuevo protocolo de comunicaciones. Como el servidor de pedidos (servidor mayormente utilizado por los trabajadores externos) haría uso de direccionamiento IPv6, el dispositivo handheld se configuraría con una dirección IP pública IPv6 6to4, de esta manera, el host del trabajador externo crearía un túnel 6to4 con un IPv6 relay router (configurado en el mismo), el cual le permitirá comunicarse con el servidor IPv6 a contactar. Esto será totalmente transparente para el usuario remoto. Cabe recalcar que esto agregaría un poco de retraso a la comunicación, sin embargo; no imposibilitaría al usuario remoto para comunicarse con la red de su empresa (ver Figura 1.10).

En conclusión, este método, incrementa la disponibilidad de conexión con los servidores de la compañía y la movilidad de los trabajadores externos.

Si bien es cierto, la solución anterior incrementa la disponibilidad de la comunicación con los servidores, para llevar a cabo una correcta ejecución del mismo, dependo del IPv6 Relay del ISP, en caso de que no haya disponibilidad de este equipo por parte del proveedor de servicios de internet, una solución de contingencia que se ha tomado en cuenta para el diseño WAN en el caso de que se presente un escenario de este tipo, es que se realice la implementación de un servidor VPN en la granja de servidores en la cual se encuentra el servidor de pedidos. De esta manera, en el peor escenario, el usuario podrá establecer manualmente una vpn (IPv4) con el servidor mencionado anteriormente y este equipo puede servir de gateway para permitir la comunicación entre el host handheld y el servidor o equipo de destino.

CAPÍTULO 2

2. DISEÑO DE LA SOLUCIÓN

2.1 Plan de migración

El propósito de este proyecto es el diseño de la migración la red de IPV4 a IPV6 de la empresa Chifles S.A, con el objetivo de brindarle mayor seguridad a la misma al momento que los tele trabajadores necesiten conectarse a la red asignándoles a los equipos de cada uno, una dirección IPV6 de la misma red.

El método que se utilizará para realizar este plan de migración es el Dual Stack, este permite que los computadores, servidores y routers puedan operar con una pila de ipv4 y una de ipv6 de forma paralela con el propósito de poder enviar y recibir los dos tipos de paquetes.

De una forma que al establecer un enlace con un nodo IPV6, este nodo IPV6/IPV4 funcione como uno solo, por lo tanto también el enlace con un nodo IPV4 actúe como un solo nodo.

La configuración de cada uno de los nodos está conformada con dos direcciones IP, se lleva a cabo a través de diferentes maneras por ejemplo tenemos para IPV6 el mecanismo de DHCP -v6 y para IPV4 el mecanismo de DHCP.

El mecanismo de Dual Stack, nos ayuda a agilizar el proceso del diseño de la migración de IPV6, porque su funcionamiento es de forma continua, significa que en el entorno de la red se pueden realizar configuraciones en pequeñas partes, si bien es cierto el propósito es que desaparezca el protocolo de IPV4, como solución se deshabilitará la pila IPV4 de cada nodo.

Concluyendo el proceso del Dual Stack, nos facilita la disminución de la reacción sobre el costo, tiempo y los servicios de las aplicaciones.

En la Figura 2.1 se detalla un diagrama del proceso del mecanismo de transición de Dual Stack:

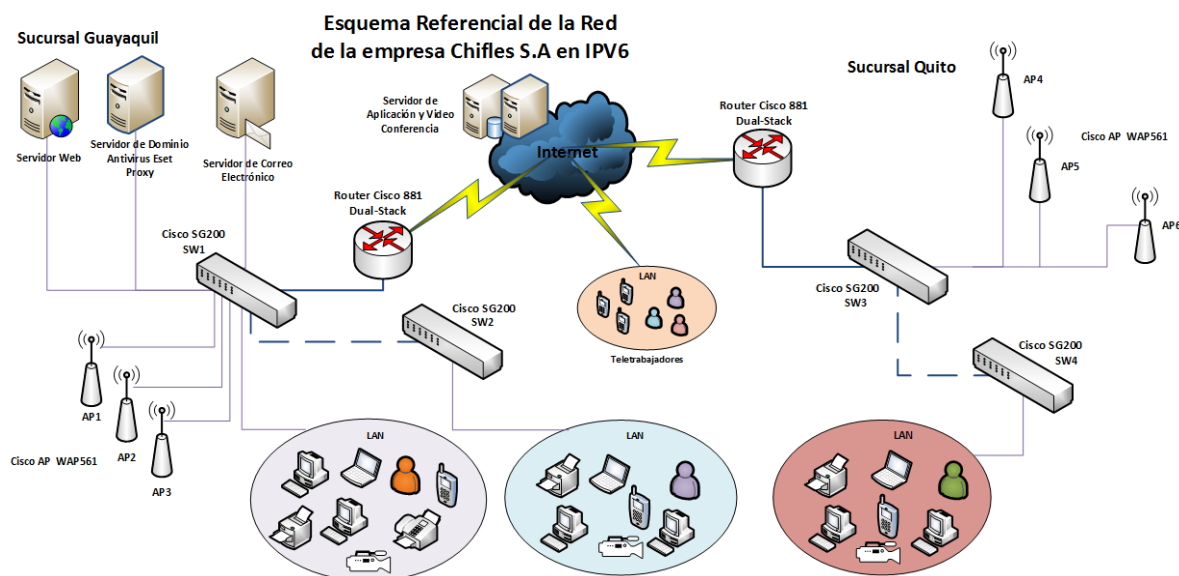


Figura 2.1 Mecanismo de Transición Dual Stack

2.2 Conexión a internet mediante IPv6

El servicio de internet de la empresa Chifles S.A es brindado por los proveedores ISP Telconet e ISP Claro, los mismos que cuentan con redes robustas que soporta el protocolo de IPV6, ofrecen una disponibilidad de internet del 99.6%, garantizando gran velocidad y alta calidad de servicio.

Mediante la información obtenida podemos definir que ambos proveedores de internet son aptos para que la empresa Chifles S.A pueda realizar el plan de migración al protocolo IPV6.

2.3 Configuración básica de los equipos en IPv6

```
Router> enable
Router# configure terminal
Router(config)# hostname <nombre_del_router>
```

Configuración del enrutamiento de paquetes IPV6

```
Router(config)# ipv6 unicast-routing
```

Configuración de IPV6 en la interfaz FastEthernet de un router

```
Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 enable
Router(config-if)#ipv6address <Dirección_IPv6>/<Longitud_del_prefijo>
Router(config-if)# exit
```

2.3.1 Configuración de rutas estáticas en IPV6

Habilitar rutas estáticas dentro de un Router

```
Router# configure terminal
Router(config)# ipv6 route <prefijo_IPv6>/<longitud_del_prefijo>
<interfaz_o_gateway>
```

En el caso de querer usar un Gateway por defecto:

```
prefijo_IPv6/longitud_del_prefijo= :: /0
```

Comando para verificar la lista de todas las rutas estáticas

```
Router# show ipv6 route static
```

2.4 Etapas de transición a IPV6

Para el desarrollo del plan de transición del protocolo IPV4 a IPV6, se debe tener en cuenta varios parámetros para que la comunicación sea estable entre la versión actual y el protocolo al que se desea migrar, porque el objetivo a alcanzar es el cambio completo a IPV6 sin que se vean afectados los servicios que ofrece la red con el protocolo IPV4.

El propósito del plan de transición es mantener los servicios de IPV4 y adaptarlos al plan de migración de IPV6, facilitando la comunicación entre los trabajadores externos y la red, mediante una conexión eficaz, eficiente y segura, ya que, en cada uno de sus dispositivos de trabajo se le asignará una dirección IPV6.

2.4.1 Etapa 1: Mantener IPV4 al mundo y tener IPV6 en la red local

El cuadro que se plantea es configurar en el Router de cada sucursal de la empresa Chifles S.A el protocolo de IPV6, el mecanismo de transición Dual Stack para tener acceso a la comunicación local de IPV6 a IPV4 y asignar direcciones IP a través de DHCP a todos los equipos que se encuentren conectados a la misma.

A demás se debe contar con la configuración de NAT para facilitar la traducción de las direcciones IPV4/IPV6.

En la Figura 2.2 se muestra el diagrama del primer escenario para el plan de migración a IPV6:

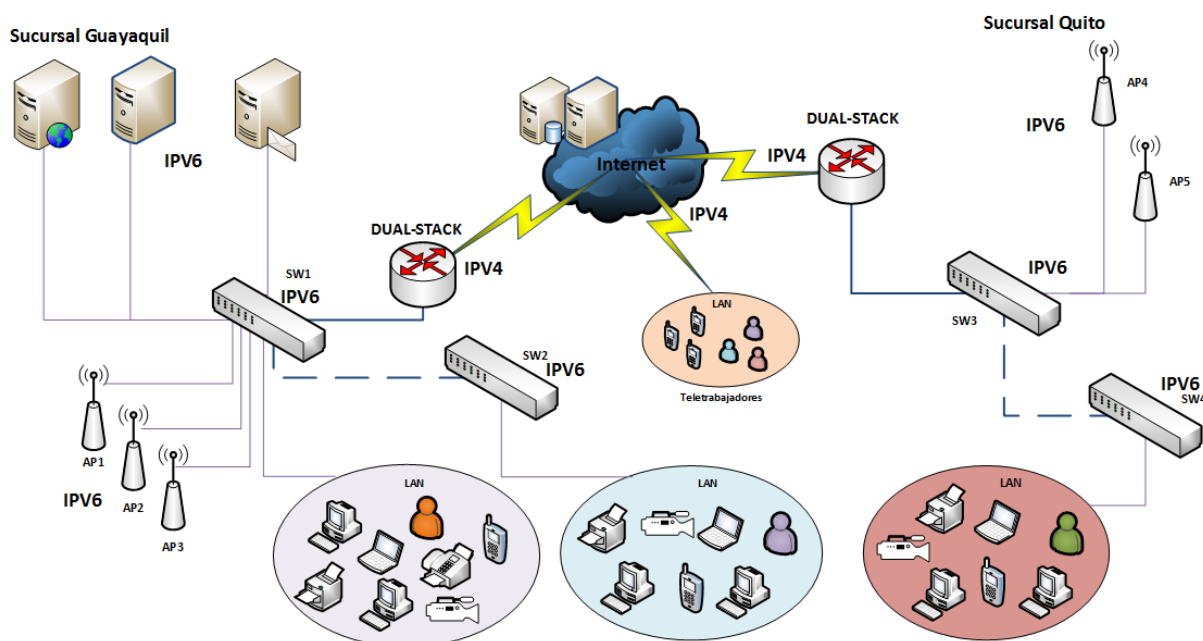


Figura 2.2 Mantener IPV4 al mundo y tener IPV6 en la red local.

Ejemplos de Comandos de configuración del Primer Escenario.

En el Router de cada sucursal se configura una dirección IPV4 e IPV6 de la siguiente forma:


```

Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)# interface fastEthernet 0/0
Router(config-if)#ipv6 enable
Router(config-if)#ip address 192.168.1.50 255.255.255.0
Router(config-if)#ipv6 address 2003:dc6:2e:10:1/64
Router(config-if)#no shut
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/1/0
Router(config-if)#ipv6 enable
Router(config-if)#ip address 200.0.0.1 255.255.255.252
Router(config-if)#ipv6 address 2001:db8:2f:40::1/64
Router(config-if)#clock rate 64000
Router(config-if)#no shut

```

Ejemplos de Configuraciones de rutas estáticas en el Router Principal de la siguiente manera:

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.20.3.224 255.255.255.240 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:35::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:2::/64 serial 0/1/0

```

2.4.2 Etapa 2: Tener IPV6 en el mundo y tener IPV6 en la red local

Este cuadro plantea algo parecido al primer escenario en donde lo que se desea es que la red de la empresa Chifles S.A pueda trabajar sobre el protocolo IPV6 asignando direcciones IP a través de DHCP en la red.

En este diagrama, el mundo ya está trabajando totalmente con el protocolo IPV6, gracias a esto para poder tener un acceso a internet desde la red local de la empresa Chifles S.A se tendría que configurar en los routers de cada sucursal un direccionamiento estático para protocolo de IPV6.

En la Figura 2.3 se muestra el diagrama del segundo escenario para el plan de migración a IPV6:

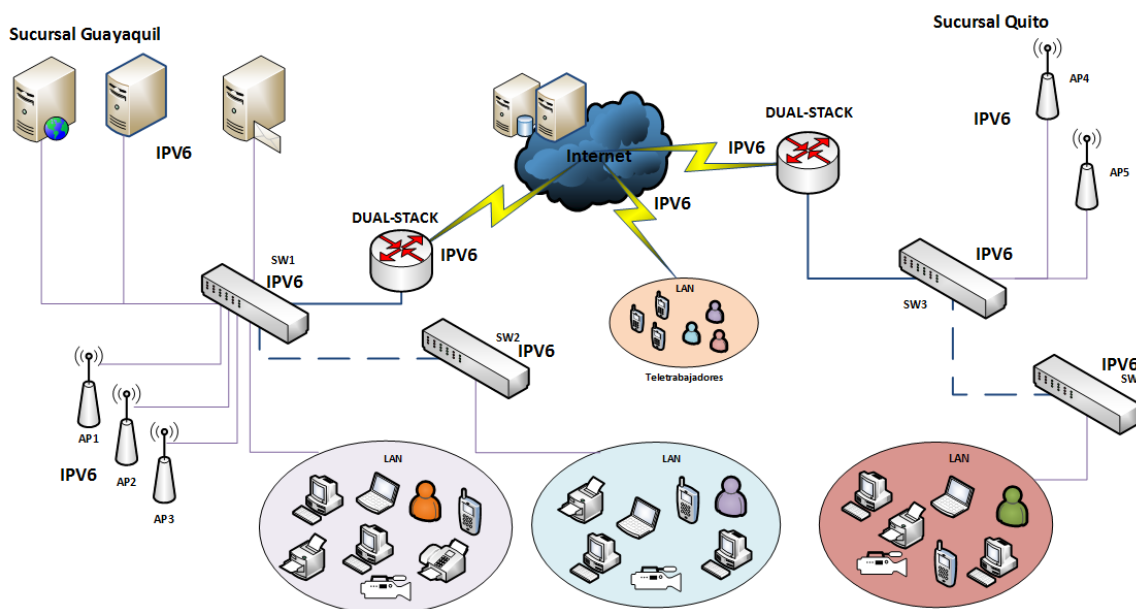


Figura 2.3 Tener IPV6 en el mundo y tener IPV6 en la red local.

Ejemplos de Comandos de configuración del Segundo Escenario.

En el Router de cada sucursal de la empresa Chifles S.A se debe configurar una dirección IPV6.

```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)# interface fastEthernet 0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2002:0DC6:2E:0::1/64
Router(config-if)#no shut
Router#configure terminal
Router(config)#interface serial 0/1/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2002:0DC6:2E:0::5/64
Router(config-if)#clock rate 64000
Router(config-if)#no shut
```

Ejemplos de Configuraciones de rutas estáticas en el Router de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 route 2001:db8:2f:50::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:4::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:5::/64 serial 0/1/0
Router(config)#
```

Ejemplos de Configuraciones de rutas estáticas en el Router Principal de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 route 2001:db85:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:2::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:3::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:1::/64 serial 0/1/0
```

2.4.3 Resultados de la configuración de las etapas de la transición

Protocolo DHCP:

Ya que no es posible establecer un rango de direcciones IPV6 dinámico para cada sub-interfaz del Router de las sucursales, se asigna a cada host una dirección estática para un mayor control y registro de cada dirección IP.

Ejemplos de Comandos de configuración de DHCP en cada sucursal.

```
ipv6 unicast-routing ipv6 cef
ipv6 dhcp pool Administrativo
prefix-delegation 2001:DB8:2f:1::/64 00030001C402068F0000 prefix-delegation
pool Administrativo
dns-server 2001:DB8:2f:35::10 domain-name cisco.com
ipv6 dhcp pool EdifRectorado
prefix-delegation 2001:DB8:2:2::/64 00030001C402068F0000 prefix-delegation
pool EdifRectorado
dns-server 2001:DB8:2f:35::1 domain-name cisco.com
```

```

ipv6 multicast-routing
interface FastEthernet0/0 no ip address
speed 100 full-duplex
interface FastEthernet0/0.10 encapsulation dot1Q 10
ipv6 address 2001:DB8:2f:1::1/64
ipv6 enable
ipv6 dhcp server Guayaquil
interface FastEthernet0/0.20 encapsulation dot1Q 20
ipv6 address 2001:DB8:2f:2::1/64
ipv6 enable
ipv6 dhcp server EdifRectorado

```

2.4.4 Funcionamiento del Mobile IPv6

Anteriormente se detalló el funcionamiento de la red actual de Chifles S.A., de manera interna y externa (con IPv4 Mobile).

Como se detalla en la Figura 2.4 al realizar la migración del Router de borde, como era de esperarse, afectaría de manera directa a la forma por medio de la cual se conectan los usuarios remotos. Evidentemente, los mismos ahora realizarán sus funciones del día a día por medio del nuevo protocolo de comunicaciones, esto será transparente para ellos.

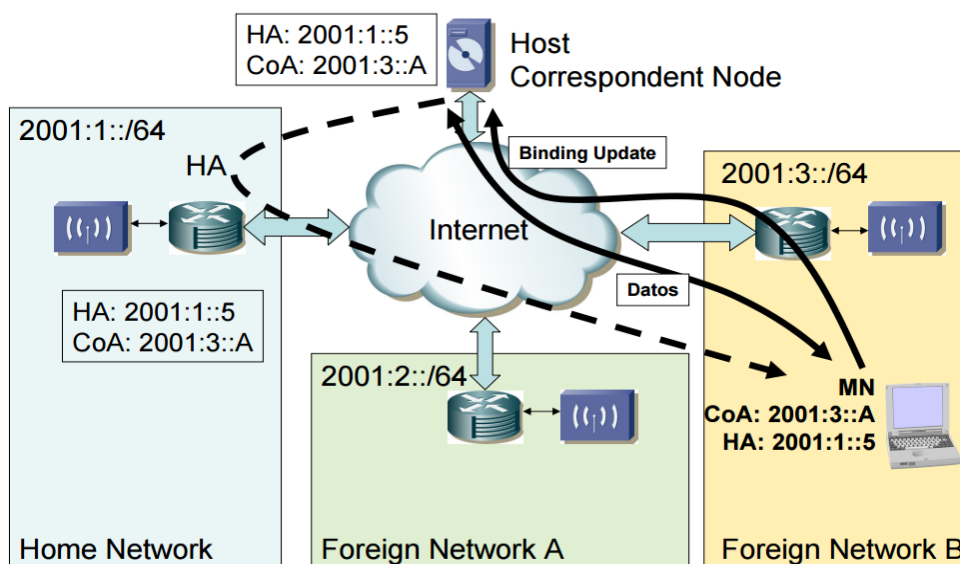


Figura 2.4 Fases de Mobile IPv6

2.4.5 Funcionamiento de los Teléfonos IP

Para que los teléfonos IP Cisco 7960G funcionen de manera adecuada en la red de la empresa Chifles S.A se debe realizar las siguientes configuraciones en el Router de cada sucursal:

```
dial-peer voice 1 voip
destination-pattern 5...
voice-class sip anat
session protocol sipv2
session target ipv6:[2001:db8:caf0:101:21b:78ff:fe7a:5d86]
session transport tcp
dtmf-relay rtp-nte
no vad
```

2.5 Direccionamiento de IPv4 en red Actual

En la empresa Chifles S.A se ha distribuido las direcciones IP de acuerdo al requerimiento de host y el porcentaje de crecimiento a futuro de la red.

A continuación se detalla en la Tabla 1 el requerimiento de host y el porcentaje de crecimiento a futuro para cada sucursal.

Sucursal	# de Host	% de crecimiento	Total
Guayaquil	20	100	40
Quito	21	100	42
Teletrabajadores	54	50	81

Tabla 1. Requerimientos de host y el porcentaje de crecimiento a futuro.

Por medio de la tabla anterior podemos analizar que la red de la empresa Chiffles S.A necesita 2 subredes para cubrir los requerimientos de ambas sucursales.

De acuerdo a los requerimientos se le asignó a la sucursal de Guayaquil el segmento de red 192.168.1.0/24 y a la sucursal de Quito el segmento de red 192.168.2.0/24.

En la Tabla 2, podemos observar la descripción de los equipos y dispositivos con sus respectivas direcciones IPV4 que se utilizan en cada sucursal.

Sucursal	Equipo	Dirección de Subred	Mascara de Subred
Guayaquil	Router	192.168.1.1	255.255.255.0
	Switch 1	192.168.1.2	255.255.255.0
	Switch 2	192.168.1.3	255.255.255.0
	Servidor WEB	192.168.1.9	255.255.255.0
	Servidor de Dominio Proxy y Antivirus	192.168.1.10	255.255.255.0
	Servidor de Correos	192.168.1.12	255.255.255.0

	AP1	192.168.1.20	255.255.255.0
	AP2	192.168.1.21	255.255.255.0
	AP3	192.168.1.22	255.255.255.0
	Host	192.168.1.30 – 70	255.255.255.0
	Cámaras IP	192.168.1.75 - 80	255.255.255.0
	Teléfonos IP	192.168.1.85 - 100	255.255.255.0
Quito	Router	192.168.2.1	255.255.255.0
	Switch 1	192.168.2.2	255.255.255.0
	Switch 2	192.168.2.3	255.255.255.0
	AP4	192.168.2.11	255.255.255.0
	AP5	192.168.2.13	255.255.255.0
	Host	192.168.2.20 - 70	255.255.255.0
	Cámaras IP	192.168.2.75 - 80	255.255.255.0
	Teléfonos IP	192.168.2.85 - 100	255.255.255.0

Tabla 2. Direcciones IPv4 para cada sucursal

2.6 Esquemas de los diagramas lógicos

2.6.1 Esquema de la topología de red IPV6

Mediante los estudios realizados se ha establecido que en toda la red de la empresa Chifles S.A, su proveedor de equipos es la empresa CISCO, los cuales trabajan con IPV6.

La empresa Chifles S.A cuenta con un personal especializado para brindar soporte a los equipos Cisco.

2.6.2 Diseño de las Vlans

El diseño de las Vlans dentro de la empresa Chifles S.A se llegará a implementar con la finalidad de obtener los siguientes beneficios en la red.

- Crear una división lógica por departamentos.
- Designar políticas de seguridad.
- Facilitar la administración y monitoreo de la red.

En la Tabla 3 se ha diseñado un total de 10 VLANS distribuidas de la siguiente manera:

#Vlan	Nombre de la Vlan
10	Servidores
20	Redes
30	Administrativo
40	Ventas
50	Distribución
60	Producción

70	Contabilidad
80	Wireless
90	Cámaras IP
95	Teléfonos IP
99	Nativa

Tabla 3. Nombre de VLANS

Distribución de las direcciones IP para cada VLAN

Proceso de configuración Inter-Vlan

Paso 1: Configuración del puerto del switch principal en modo trunk.

Paso 2: Configuración VTP

Paso 3: Creación de las Vlans en el Switch principal

Paso 4: Asignación de los puertos con sus respectivas Vlan en cada switch.

A continuación se detalla en la Tabla 4 las asignaciones de puertos de la configuración inter-VLAN en los switches de cada sucursal de la empresa Chifles S.A

Sucursal	Dispositivo	Puertos	Asignación
Guayaquil	Switch 1	Fa0/1 – 0/2	Enlace Troncal 802.1q (LAN 99 Nativa)
		Fa0/3 – 0/7	Vlan 10: Servidores
		Fa0/8 – 0/15	Vlan 20: Redes

		Fa0/16 – 0/20	Vlan 30: Administrativo
		Fa0/21 – 0/24	Vlan 40: Ventas
	Switch 2	Fa0/1- 0/2	Enlace Troncal 802.1q (LAN 99 Nativa)
		Fa0/3 – 0/5	Vlan 50: Distribución
		Fa0/5 – 0/6	Vlan 60: Producción
		Fa0/7 – 0/10	Vlan 70: Contabilidad
		Fa0/11 – 0/14	Vlan 80: Wireless
		Fa0/15 – 0/19	Vlan 90: Cámaras IP
		Fa0/20 – 0/24	Vlan 95: Teléfonos IP
Quito	Switch 1	Fa0/1 – 0/2	Enlace Troncal 802.1q (LAN 99 Nativa)
		Fa0/3 – 0/7	Vlan 10: Servidores
		Fa0/8 – 0/15	Vlan 20: Redes
		Fa0/16 – 0/20	Vlan 30: Administrativo
		Fa0/21 – 0/24	Vlan 40: Ventas
	Switch 2	Fa0/1- 0/2	Enlace Troncal 802.1q (LAN 99 Nativa)
		Fa0/3 – 0/5	Vlan 50: Distribución
		Fa0/5 – 0/6	Vlan 60: Producción
		Fa0/7 – 0/10	Vlan 70: Contabilidad

		Fa0/11 – 0/14	Vlan 80: Wireless
		Fa0/15 – 0/19	Vlan 90: Cámaras IP
		Fa0/20 – 0/24	Vlan 95: Teléfonos IP

Tabla 4. Asignación de Puertos en los Switches

Ejemplo de Configuración de las VLANS implementando el uso de IPV6

a) Creación de sub-interfaces en el router:

```
Router# configure terminal
Router(config)# interface fastEthernet 0/1.10
Router(config-subif)# description VLAN Servidores
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ipv6 address 2002:dc6:2e:1:1/64
```

b) Creación de VLANS en el Switch

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Servidores
Switch(config-vlan)# exit
```

Ejemplo de configuración de los puertos de cada Interfaz del Switch:

```
Switch# configure terminal
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch# configure terminal
Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

2.6.3 Reglas de conectividad entre VLANS

Las reglas de conectividad entre VLANS se han creado con el objetivo de permitir o denegar el acceso a entre los departamentos y los servicios que tiene la empresa Chifles S.A.

A continuación se presenta la Tabla 5 donde podemos identificar las reglas de acceso que se le ha configurado a cada VLAN en el diagrama de red de la empresa.

#Vlan / Nombre	Acceso de VLAN
10 / Servidores	20
20 / Redes	10
30 / Administrativo	40,50,60,70
40 / Ventas	50
50 / Distribución	40,60
60 / Producción	40,50
70 / Contabilidad	40,50
80/ Wireless	-----
90 / Cámaras IP	20
95/ Teléfonos IP	20
99/ Nativa	

Tabla 5. Reglas de Acceso entre VLANS

2.6.4 Direccionamiento IPV6 en la red de la empresa Chifles S.A

Para la creación del esquema de la red de la empresa Chifles S.A se ha seleccionado como origen para la sucursal de Guayaquil el siguiente direccionamiento IPV6:

- Formato de la dirección IPV6 en Hexadecimal:
2002:0DC6:002E:0000:0000:0000:0000
- Mascara de Red: /64
- Presentación alternativa de la dirección IPV6 de origen:
2002:0DC6:2E:0::/64

El direccionamiento origen para la sucursal de Quito es el siguiente:

- Formato de la dirección IPV6 en Hexadecimal:
2003:0DC6:002E:0000:0000:0000:0000
- Mascara de Red: /64
- Presentación alternativa de la dirección IPV6 de origen:
2003:0DC6:2E:0::/64

Para la asignación de direcciones IPV6 para cada host y equipo de red, se implementará el método de autoconfiguración a través de DHCP soportados por IPV6, a diferencia de los routers de cada sucursal que utilizará la configuración manual.

Distribución de direcciones IP para cada VLAN

A continuación se detalla en la Tabla 6 y 7 las direcciones IPV6 para cada VLAN de la red de la empresa Chifles S.A para sus diferentes sucursales.

Switches		Router	
#Vlan	Nombre de la Vlan	Sub- Interfaz	Dirección IPV6
10	Servidores	Fa 0/1.10	2002:dc6:2e:1:1/64
20	Redes	Fa 0/1.20	2002:dc6:2e:2:1/64
30	Administrativo	Fa 0/1.30	2002:dc6:2e:3:1/64
40	Ventas	Fa 0/1.40	2002:dc6:2e:4:1/64
50	Distribución	Fa 0/1.50	2002:dc6:2e:5:1/64
60	Producción	Fa 0/1.60	2002:dc6:2e:6:1/64
70	Contabilidad	Fa 0/1.70	2002:dc6:2e:7:1/64
80	Wireless	Fa 0/1.80	2002:dc6:2e:8:1/64
90	Cámaras IP	Fa 0/1.90	2002:dc6:2e:9:1/64
95	Teléfonos IP	Fa 0/1.95	2002:dc6:2e:10:1/64

Tabla 6. Asignación de las VLANS sobre IPV6 en la Sucursal de Guayaquil.

Switches		Router	
#Vlan	Nombre de la Vlan	Sub- Interfaz	Dirección IPV6
10	Servidores	Fa 0/1.10	2003:dc6:2e:1:1/64
20	Redes	Fa 0/1.20	2003:dc6:2e:2:1/64
30	Administrativo	Fa 0/1.30	2003:dc6:2e:3:1/64

40	Ventas	Fa 0/1.40	2003:dc6:2e:4:1/64
50	Distribución	Fa 0/1.50	2003:dc6:2e:5:1/64
60	Producción	Fa 0/1.60	2003:dc6:2e:6:1/64
70	Contabilidad	Fa 0/1.70	2003:dc6:2e:7:1/64
80	Wireless	Fa 0/1.80	2003:dc6:2e:8:1/64
90	Cámaras IP	Fa 0/1.90	2003:dc6:2e:9:1/64
95	Teléfonos IP	Fa 0/1.95	2003:dc6:2e:10:1/64

Tabla 7. Asignación de las VLANS sobre IPV6 en la Sucursal de Quito

2.6.5 Servicios de la Intranet Sobre IPV6

La empresa Chifles S.A brinda varios servicios en la red de datos los cuales son correos, base de datos, dominio, página web, proxy y antivirus.

Los servicios antes mencionados soportan IPV6 y funcionan sobre los Sistemas Operativos de Centos y Windows server 2012 R2 para facilitar su uso se realizarían cambios en la configuración de los archivos de direcciones IP.

❖ Configuración del Servidor web

En el rol del servicio WEB se debe configurar una dirección IPV6 que esté dentro del registro DNS de la empresa.

En apache web server encontramos el "httpd.conf", que es un archivo de configuración en el que se realizan las configuraciones de la dirección IP y el puerto por el cual el servidor web escucha.

Todas las direcciones IPV6 se realizan de la siguiente manera:

```
# cat httpd.conf
Listen [2001:db8:2f:0::25]
```

Así mismo se asignan al host virtual las direcciones IPV6:

```
# cat httpd.conf
NameVirtualHost 172.20.0.30
NameVirtualHost[2001:db8:2f:0::30]
```

Para que el dominio de Chifles.com se resuelva en IPV6 se tendría que configurar el JVM para elegir una pila IPV4 sobre IPV6:

```
-Djava.net.preferIPv4Stack=true
```

❖ Configuración del Correo Electrónico

Actualmente se está utilizando el protocolo IPV4, para poder realizar el plan de migración sin que se afecte el servicio es necesario que se trabaje con un ambiente mixto IPV4/IPV6 y posteriormente solo convivir con el ambiente IPV6.

La empresa Chifles S.A trabaja con el servicio de Zimbra versión 8.0 en la cual no todos los servicios y nodos soportan totalmente IPV6.

Si bien es cierto en este momento aún no se trabaja totalmente con IPV6 por este motivo se debe realizar las siguientes configuraciones:

- Contar con un Nodo Borde
- Instalar paquete zimbra-proxy
- Instalar zimbra mta
- Configurar Local Host en el nodo borde (127.0.0.1)
- Configurar la dirección IPV6

Después de ser instalado el nodo mixto se configura de la siguiente manera:

```
ipv6 - Only IPv6 address for the host
both - Use both IPv4 and IPv6 addresses for the host
```


La configuración del servidor **zimbralpMode** por medio de claves permite controlar el nodo ya sea en IPV4/IPV6 o solo en IPV6

En las configuraciones de zimbraMtaMyNetwork es necesario añadir el rango de las direcciones IPV6 vía zmprov.

```
zmprov ms edge.example.com zimbraMtaMyNetworks
"127.0.0.0/8 [::1]/128 x.x.x.x/x [xxxx:xxxx:xxxx::x]/x"
```

❖ Configuración de la DVR cámaras IP

Para que las cámaras IP funcionen correctamente con el protocolo IPV6, es necesario configurar en la DVR la dirección ipv6 que le corresponde a cada cámara.

2.6.6 Evaluación del esquema lógico

Se detalla en la Tabla 8 con el plan del proceso de migración hacia IPV6 con la finalidad de analizar las acciones.

Tema	Acción a realizar
Topología de la Red	Solo se modifica la configuración de los equipos con la versión actual. Ver detalle 2.1
Vlans	Se reconfiguran las Vlan implementando IPV6. Ver detalle 2.6.2
Direcciones IP	Se modifican las direcciones IPV4 a IPV6. Ver detalle 2.6.4
Direcciones IPV6 para las Vlans	Cambian las direcciones IPV4 a IPV6 con sus respectivas Vlans. Ver detalle 2.6.4

Intranet	Se debe actualizar y configurar las aplicaciones para que trabajen correctamente con ipv6. Ver detalle 2.6.5
-----------------	--

Tabla 8. Evaluación del esquema lógico

2.7 Diseño del esquema físico

2.7.1 Evaluación del esquema Físico

El esquema físico de la red de la empresa Chifles S.A no se va a modificar ya que se encuentran correctamente conectados los equipos de una forma jerárquica.

Se detalla el levantamiento de información del hardware y software que pertenecen a la empresa Chifles S.A.

- **Hardware**

El plan de migración de la empresa Chifles S.A necesita que todos los equipos trabajen correctamente con IPV6.

Se detalla en la Tabla 9 con los equipos que se recomiendan a la empresa, ya que cumplen con los requerimientos para poder realizar el plan de migración:

Equipo de Red	Marca & Modelo	Soporta IPV6	Actividad a ejecutar
Routers	CISCO 881	Si	Descargar actualizaciones del

			SO.
Switches	CISCO SG200	Si	Descargar actualizaciones del SO.
Access Point	WAP561	Si	Configurar soporte IPV6
DVR cámaras IP	HikVison DS-9016HFI-ST	Si	Descargar actualizaciones del S.O Configurar Soporte IPV6

Tabla 9. Estudio de los Equipos.

▪ **Software**

En las Tablas 10, 11 y 12 se detallan los sistemas operativos con los que actualmente cuenta la empresa trabajan con IPV6, se detalla el estudio de los sistemas operativos instalados en la empresa:

Servidor	S.O Instalado	Soporta IPV6	Actividad a ejecutar
Web	Centos	Si	Instalar el módulo IPV6
Proxy	Windows Server 2012 R2	Si	Configurar soporte IPV6
Base de datos	Windows Server 2012 R2	Si	Configurar soporte IPV6

Correo electrónico	Centos	Si	Instalar el módulo IPV6
Antivirus	Windows Server 2012 R2	Si	Configurar soporte IPV6
Dominio	Windows Server 2012 R2	si	Configurar soporte IPV6

Tabla 10. Estudio de los sistemas operativos de los servidores.

Equipo	S.O Instalado	Soporta IPV6	Actividad a ejecutar
Pc's	Windows 8.1	Si	Habilitar soporte IPV6

Tabla 11. Estudio de los sistemas operativos de las PC's

Equipo	S.O Instalado	Soporta IPV6	Actividad a ejecutar
Teléfonos IP	Cisco CallManager	Si	Habilitar soporte IPV6

Tabla 12. Estudio de los sistemas operativos de los Telefonos IP

CAPÍTULO 3

3. IMPLEMENTACIÓN

3.1 Programación de Trabajo

La calendarización de las tareas a efectuarse se lo realizará según el listado de procedimientos que se detallan a continuación:

Inicio del Proyecto: Una vez que se haya efectivizado la respectiva adjudicación del proyecto, será necesario establecer reuniones de carácter técnico/financiero, para de esta manera solventar cualquier duda, requerimiento o consideraciones generales a tomarse en cuenta para realizar la implementación futura (cuando así se lo desee) del proyecto.

Análisis de la red: Tal como su nombre lo indica, en esta etapa se realizará el levantamiento de información inicial de la red de Chifles S.A.

Las tareas a ejecutarse son las siguientes:

- Auditoría de servicios
- Auditoría de usuarios
- Análisis de la infraestructura física
- Análisis de las aplicaciones

Diseño de la nueva topología de red: En el tiempo que dure realizar esta tarea se realizarán los diseños lógicos de la “nueva” red de Chifles S.A., esto incluye, entre otros; Definición de tecnologías, plan de conexión y direccionamiento IP y VLAN

Inicio de la migración: Debido a que los equipos que se implementarían posteriormente no siempre se los encuentra en el mercado local, se tienen que considerar los tiempos de importación de los mismos en caso de suscitarse dicho evento. El tiempo estimado de importación de equipos es de 20 días. Además de lo mencionado anteriormente, se efectuarán las tareas que se mencionaran a continuación:

- Pre-comisionado: Pruebas en frío (sin energizar), las cuales garantizarán la integridad de los equipos a instalarse.
- Comisionado: Pruebas en caliente (equipos energizados), las cuales garantizarán el funcionamiento lógico del equipo a instalarse.

Periodo de transición: Como era de suponerse, para llevar a cabo la migración de este protocolo de comunicaciones, dicho proceso se tiene que realizarse paulatina y cuidadosamente, de tal manera que, se mantenga la continuidad en el negocio. Las tareas que se efectuarán en esta fase serán las de:

- Integración de nuevo equipamiento activo a la empresa
- Migración del equipamiento activo obsoleto (5 días)
- Pruebas de configuración en ipv4 (3 días)
- Pruebas de configuración de integración de ipv6 a red existente
 - Registro de eventos
- Migración de protocolos de comunicación a ipv6
- Pruebas de configuración ipv6
 - Registro de eventos

Documentación: Una vez culminadas las tareas de la fase anterior, se llevará a cabo la consolidación de información resultante de haber realizado dicha migración. Entre los principales entregables que se proporcionarán de manera física (impresa) y lógica (digital), se encuentran los siguientes:

- Bitácora consolidada de los eventos ocurridos
- Manuales
 - Configuración de red IPv4
 - Configuración de red en dual stack
 - Configuración de red en IPv6

Procedimientos de administración y mantenimiento

- Memoria técnica concerniente al proyecto.

3.2 Consideraciones generales pre-migración

Proceso de Importación (transporte de equipos en exterior, negociación de fletes, envío, obtención de seguros, desaduanización, etc.) 45 días.

Proceso de cambio de equipos 30 días, esto incluye:

- Instalación del nuevo equipamiento activo de red (no configuración) 1 día
- Pre-configuración de los equipos IPv4 (asignación de Vlans, direccionamiento, políticas, etc.) 4 días
- Switchover entre el equipamiento obsoleto y el nuevo equipamiento activo (se mantiene a los equipos obsoletos encendidos mas no funcionales, no forman parte de la red) 7 días.
- Pruebas de funcionamiento con nuevo equipamiento activo en IPv4 (no incluye hosts) 2 días
- Implementación de IPv6 en la red de la empresa (dual stack con IPv4, no incluye terminales) 3 días
- Pruebas de funcionamiento con IPv6 e IPv4 (incluyendo hosts) 2 días
- Migración de terminales (hosts) a nuevo protocolo de comunicaciones (20 días).

Consideraciones en equipos de acceso.

Arquitectura (hardware y software) del equipo debe soportar nuevo protocolo de comunicaciones, en este punto se deben tener ciertas consideraciones:

- Si el equipo no soporta IPv6, se debe mantener dual stack en la red. En el caso de que los recursos sean accedidos por usuarios externos a la compañía, se debe implementar DNS64 y NAT64 en los enrutadores de la empresa para que se realice el respectivo mapeo IPv4/IPv6
- Una vez se hayan realizado los preparativos mencionados en la fase anterior, se tiene que realizar la configuración de la dirección IPv6 en el dispositivo en cuestión.
- Pruebas de funcionamiento

3.3 Presupuesto del proyecto

Se detalla en la Tabla 13 el presupuesto.

Presupuesto 1				
Equipo	Cantidad	Descripcion	Precio	Total
Switch Cisco SG200	4	Dual Stack	\$ 1.700	\$ 6.800
Access Point Cisco WAP561	5		\$ 500	\$ 2.500
Router Cisco 881	2	Dual Stack	\$ 900	\$ 1.800
Total Valor Equipos				\$ 11.100
Diseño de migración				\$ 3.000
Configuración de red				\$ 2.000
Total Diseño/Migracion				\$ 5.000
Suma Total				\$ 16.100

Tabla 13: Presupuesto

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Mediante la elaboración de este proyecto se pudo realizar un análisis de los requerimientos para llevar a cabo una migración a IPv6, utilizando el mecanismo Dual Stack, con el cual se logrará mantener la conectividad de todos los servicios de la red.
2. La migración de la red hacia IPv6 es viable dentro de la empresa Chifles S.A, porque se llevó a cabo la verificación de las características de los equipos que la conforman, en donde se constató que el único cambio indispensable será el del router de borde de la compañía.
3. La seguridad de la red de la empresa aumentará considerablemente gracias al uso de IPSec que ofrece IPv6.
4. El proceso de migración a IPv6 tendrá que llevarse a cabo de manera gradual, por lo cual, será necesario mantener la coexistencia de ambos protocolos con el propósito de minimizar el impacto en la red.
5. La implementación de este protocolo permitirá mejorar la comunicación y el uso de movilidad que emplean los trabajadores externos en sus dispositivos de trabajo.
6. En los próximos años el uso de IPv6 trascenderá, por lo que el diseño de esta migración le permitirá a la empresa Chifles S.A estar preparada para necesidades venideras en cuanto al uso de IPv6 en su topología.

Recomendaciones

En base a los diferentes puntos analizados en los capítulos anteriores de este documento, se pueden brindar las siguientes recomendaciones:

1. Una vez migrada la red de Chifles S.A., se recomienda mantener la infraestructura de red anterior como respaldo, para que en caso de suscitarse algún problema, se pueda usar dicha red como contingencia mientras se realiza la depuración del problema y así mantener la continuidad del negocio.
2. Se debe realizar la optimización de la red (según se requiera) cuando se implementen nuevas soluciones a la “nueva red”.
3. Se debe monitorear constantemente el estado de los equipos (tanto de manera lógica como física), según los procedimientos establecidos en los manuales de administración a entregarse.
4. Luego que la empresa Chifles S.A haya migrado completamente a IPV6 es recomendable deshabilitar el protocolo de IPV4 en los Routers de cada sucursal.

BIBLIOGRAFÍA

[1] IPv6 Global Summit Moscow, (2013, Abril 19), Introduction to Mobile IPv6, [online]. Disponible en:

<http://www.free.net/NTL/IP6/presentation/mipv6english.pdf>

[2] Embedded Systems Conference, (2012, Enero 13), Mobile Internet Basics: Mobile IPv4 Tunnels, Bindings & Datagrams. [online]. Disponible en:

<http://www.embedded.com/design/connectivity/4234622/Mobile-Internet-basics--Mobile-IPv4-Tunnels--Bindings---Datagrams>

[3] Article IPv6, (2008), Network Address Translation (NAT) Pros & Cons, [online]. Disponible en: <http://ipv6.com/articles/nat/NAT-Pros-and-Cons>

[4] IPv6 Security, (2011, Noviembre), Análisis del protocolo IPsec: el estándar de seguridad en IP, [Online]. Disponible en: <http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPsec/ipsec.pdf>

[5] Portlipv6cuba, (2013, Enero), Tecnologías de Transición IPv4- IPv6, [Online]. Disponible en: <http://www.cu.ipv6tf.org/transicionipv6.htm>

[6] Transición a IPv6, (2011, Febrero), Lo que tu departamento de Mercadotecnia debe saber., [Online]. Disponible en: <http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/110>

[7] Protocolo IPsec, (2009), Protocolo IPsec, [Online]. Disponible en: http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

[8] Cisco, (2015), Cisco 880 Integrated Services Routers, [Online]. Disponible en: <http://www.cisco.com/c/en/us/products/routers/880-integrated-services-routers-isr/index.html>

[9] Cisco, (2015), Cisco Small Business 200 Series Smart Switches, [Online]. Disponible en: <http://www.cisco.com/c/en/us/products/switches/small-business-200-series-smart-switches/index.html>

[10] hikvision, (2015), DS-9000 Series Hybrid DVR, [Online]. Disponible en: http://www.hikvision.com/es/products_show.asp?id=6053

ANEXOS