UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA ELECTRONICA

TESIS DE MAESTRÍA

ESTRATEGIA DE IMPLEMENTACION PARA LA TRANSICIÓN DEL PROTOCOLO IPv4 A IPv6 EN LA RED DE LA UMSA

Tesis presentada para optar al título de
"Master de Ingeniería en Redes de Comunicaciones"

Autor: Lic. Hernán Adalid Pérez Gutiérrez

Tutor: M.Sc. Ing. Roberto Zambrana Flores

LA PAZ – BOLIVIA

2020

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

A mis padres Enrique y Julieta,
a mi esposa Neyda,
a mis hijos Hasmany y Hernán.

AGRADECIMIENTOS

Al M.Sc. Roberto Zambrana Flores, por su orientación y dirección.

A los Ing. Fabian Tito Luque e Ing. Ivan Caceres, por su colaboración.

Al Ing. Oscar Blass Chambi, por su apoyo incondicional.

A la Dirección del Instituto de Electrónica Aplicada, Ing. Wilber Flores Bustillo, y Personal Administrativo.

RESUMEN

La Universidad Mayor de San Andrés es la institución donde se implementará una tecnología acorde a los tiempos actuales en base a la interacción con otras empresas u instituciones con las que intercambia tráfico de datos bajo la modalidad de servicios como Internet o como sistema de gestión académica y administrativa financiera.

Los equipos de red que, permiten la conexión entre hosts, que podrían ser computadores de escritorio, portátiles, teléfonos inteligentes u otros; estos equipos de red cada vez se convierten en dispositivos con funcionalidades más sofisticadas por lo que también requieren una administración dispositivos de red más compleja como la necesidad de administrar vlans, puertos configurables como acceso, trunk, etc. y que deben soportar tanto Protocolos de Internet (IP) versión 4 (v4) como versión 6 (v6).

Por lo expuesto, se presenta la necesidad tecnológica, institucional y social de la implementación de la transición del protocolo IP4 a IP6 en la red da datos de nuestra Casa Superior de Estudios.

Respondiendo de esta manera a un desafío personal de brindar un aporte a la Institución que me cobija.

INDICE

CAPITULO I

ASPECTOS FUNDAMENTALES

CAPITULO II

FUNDAMENTACIÓN TEÓRICA

Pág.

CAPITULO III

RELEVAMIENTO DE INFORMACIÓN

CAPITULO IV

ANALISIS DE LA IMPLEMENTACIÓN

CAPITULO V

DISEÑO DE LA IMPLEMENTACIÓN

Pág.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

INDICE DE TABLAS

INDICE DE FIGURAS

Pág.

CAPITULO I

ASPECTOS FUNDAMENTALES

1.1 INTRODUCCION

El gran crecimiento experimentado en los últimos años por las tecnologías de la información, debido principalmente a la expansión de Internet, ha supuesto un considerable incremento tanto en el número de usuarios y volumen de tráfico generado en la red de la Universidad Mayor de San Andrés, así como en los servicios y aplicaciones que se ejecutan en esta red.

1.2 ANTECEDENTES

1.2.1 TEMÁTICOS

En la actualidad se dispone de una gran cantidad y diversidad de dispositivos, como teléfonos móviles, cámaras, lectores biométricos, sensores, lectores de tarjetas de proximidad, lectores de chip RFID y una infinidad de aparatos inteligentes que requieren conectividad para enviar y/o recibir información.

1.2.2 TECNOLÓGICOS

Los equipos de red que, permiten la conexión entre hosts, que podrían ser computadores de escritorio, portátiles, teléfonos inteligentes u otros; estos equipos de red cada vez se convierten en dispositivos con funcionalidades más sofisticadas por lo que también requieren una administración dispositivos de red más compleja como la necesidad de administrar vlans, puertos configurables como acceso, trunk, etc. y que deben soportar tanto Protocolos de Internet (IP) versión 4 (v4) como versión 6 (v6).

1.2.3 INSTITUCIONALES

La Universidad Mayor de San Andrés es la institución donde se implementara una tecnología acorde a los tiempos actuales en base a la interacción con otras empresas u instituciones con las que intercambia tráfico de datos bajo la modalidad de servicios como Internet o SIGEP como sistema de gestión administrativa financiera.

1.3 JUSTIFICACIÓN

1.3.1 TECNICA

Se debe considerar que el uso del Protocolo IPv4 al poseer una numeración ya agotada en la actualidad, se tuvo que recurrir a técnicas como el NAT (Network Address Translation), técnica que

permitió un paliativo pero que también contrajo una serie de inconvenientes como problemas en las comunicaciones extremo a extremo, en línea o la imposibilidad de acceder a un dispositivo desde la red externa.

El hecho actual y futuro del crecimiento exponencial de dispositivos que requieren ser parte de la red y requerirán aún más en el futuro, se ve como la solución técnica la implementación del Protocolo IPv6.

La implementación de nuevas tecnologías o tecnologías en franco crecimiento a nivel mundial hace que una institución tan importante en el contexto nacional como internacional como un líder en la formación de profesionales a nivel de pregrado como postgrado, permite que en el Internet sea visible y los usuarios dentro la red también se les permita acceder a contenidos mediante Protocolos IPv4 e IPv6.

1.3.2 SOCIAL

Los usuarios de la red de la UMSA que acceden a servicios TIC's provistos mediante su Departamento de Tecnologías de Información y Comunicación, dentro de la red LAN y acceden a contenidos en la nube requieren este acceso a sitios soportados por tecnologías camino a la obsolescencia como los más nuevos, siendo transparente este hecho para el usuario, y los usuarios que acceden a nuestros contenidos desde redes externas (Internet), también se debe garantizar su accesibilidad aun considerando el origen del acceso y las tecnologías que estos utilicen.

1.3.3 ECONOMICA

El adecuado empleo de las tecnologías de gestión de red permite mejorar la eficiencia, disponibilidad y el rendimiento de las redes, aumentar la relación calidad/costo en el diseño, implementación y explotación de las redes, así como aumentar la satisfacción de los usuarios por el servicio de red proporcionado.

1.4 PLANTEAMIENTO DEL PROBLEMA

El incremento exponencial de dispositivos inteligentes que requieren conectividad a la red y la deficiencia técnica que significa conectar esos equipos al Protocolo IPv4 tanto a nivel de direcciones públicas como las que tiene la UMSA asignado por LACNIC (Registro de Direcciones de Internet de América Latina y Caribe) misma que corresponde a una /20, hecho que obliga al uso de numeración de direcciones privadas con las consiguientes deficiencias lo que inevitablemente obliga a la transición del Protocolo IPv6.

1.5 OBJETO DE ESTUDIO

El estudio se enmarca en la implementación del Protocolo IPv6 de red perteneciente a la UMSA.

1.6 PREGUNTAS DE INVESTIGACIÓN

- ¿Es factible la transición del nuevo Protocolo de Internet, IPv6?
- ¿Qué tipo de mecanismos transición u coexistencia son los adecuados para la implementación del nuevo protocolo, IPv6, acorde a las necesidades y naturaleza de la institución?

1.7 OBJETIVOS

1.7.1 OBJETIVO GENERAL

Contrastar la teoría de transición del protocolo IPv4 al IPv6, a través del método experimentar, en base a la percepción de la necesidad de disponer una estrategia de implementación en la red de datos de Universidad Mayor de San Andrés en la gestión 2020 que permita verificar lo expuesto en dicha teoría.

1.7.2 OBJETIVOS ESPECIFICOS

- Revisar y analizar la teoría de transición del protocolo IPv4 a IPv6.
- Relevar y diagnosticar la infraestructura de red de la UMSA.
- Establecer los requerimientos necesarios para transición al protocolo IPv6.
- Elaborar el plan de la estrategia para la transición al protocolo IPv6.
- Implementar el plan de la estrategia de transición en la red inalámbrica.

1.8 LÍMITES Y ALCANCES

1.8.1 LÍMITES

- La implementación del nuevo protocolo no contempla a los servidores y servicios públicos que no lo soporten.
- La implementación del nuevo protocolo no contempla en unidades académicas que no lo acepten explícitamente.

1.8.2 ALCANCES

- Revisión de la teoría del protocolo IPv6 y la transición del protocolo IPv4 al IPv6.
- Evaluación de los equipos de red en sus tres niveles, núcleo, distribución y acceso; y la compatibilidad con el protocolo IPv6.
- Relevamiento de información de los servidores y servicios de red que se consideran en explotación.
- Relevamiento de información de hosts conectados en la red cableada e inalámbrica con cobertura en la red administrada por el DTIC.
- Establecer los requerimientos técnicos de equipamiento de hardware, licencias y RRHH para la transición al Protocolo IPv6.
- Planteamiento de la estrategia de transición más adecuada para su implementación
- Los mecanismos de transición a plantearse deben considerar las necesidades de conectividad de la Institución.
- El diseño del plan de transición del nuevo protocolo, IPv6, a servidores y servicios será lo bastante detallado para conseguir una forma de configuración sencilla y práctica.
- La ejecución del plan de transición considera la participación comprometida del personal técnico y ejecutivo de la Institución.
- La implementación del plan de la estrategia considera la configuración en equipos de red de borde, núcleo, distribución, administradores de ancho de banda, servidores y hosts de usuarios finales.

CAPITULO II

FUNDAMENTACIÓN TEÓRICA

2.1 INTRODUCCION

Las bases teóricas necesarias para la aplicación en el presente plan de implementación, se revisan en el presente capítulo, haciendo énfasis en temas relacionados con el IPv6, como ventajas, características, representación, encabezados, mecanismos de transición y enrutamiento.

2.2 IPV6

En la década de 1990 la fuerza de tareas de ingeniería de internet IETF (Internet Engineering Task Force) solicitó propuestas para un nuevo sistema de direccionamiento IP que remplazara al actual IPv4. Luego se recibió una respuesta del grupo IP de la próxima generación IPng (Internet Protocol Next Generation), los requerimientos a cumplir por el nuevo protocolo son:

- Manejo de millones de estaciones o hosts
- Reducción del tamaño de las tablas de enrutamiento
- Simplificación de la cabecera a fin de permitir un procesamiento rápido de paquetes
- Proporcionar mayor seguridad de datos que en IPv4
- Enfoque a la prestación de servicios en tiempo real
- Permitir movilidad de hosts sin necesidad de cambio de dirección
- Coexistencia con IPv4

2.2.1 CASOS DE USO DE IPV6

- Escasez de direcciones IP: IPv6 resuelve el problema de escasez de direcciones IPv4 ya que aporta direcciones IP prácticamente infinitas. En este sentido se indica que "Una dirección IPv6 posee 128 bits disponibles y soportará un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones (340 sextillones de direcciones) —cerca de 6,7 × 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la tierra"[1]
- El crecimiento de las tablas de enrutamiento: Actualmente existe saturación en los backbones de los routers debido al número de prefijos que los routers deben mantener en sus tablas de enrutamiento. IPv6 ofrece un direccionamiento jerárquico (TLA, NLA) permitiendo un procesamiento más rápido de los paquetes debido a que solo se debe leer una parte de la dirección para tomar una dirección de enrutamiento.
- Necesidad de conexión permanente a Internet: Los dispositivos móviles como computadoras portátiles, teléfonos inteligentes, tabletas y dispositivos fijos como computadoras, televisores, impresoras de red, necesitan conexión permanente a Internet para intercambiar información

[1] "Proyecto de Documentación de FreeBSD: Manual de FreeBSD" Capítulo 29. Networking Avanzado. URL: http://www.freebsd.org/doc/es/books/handbook/index.html

para ello requieren una dirección IP pública que no es siempre posible obtener. IPv6 dispondrá direcciones fijas para cada dispositivo que requiera conexión a Internet a un futuro muy lejano.

- Funcionalidad añadida: IPv6 incluye de forma nativa funcionalidades como Calidad de Servicio (QoS), seguridad (IPsec), movilidad IP y Multihomming.
- Mejor distribución de direcciones IP: Regiones como USA y Europa poseen en la actualidad cerca del 55% de las direcciones IP existentes dejando a zonas geográficas como Asia con un creciente problema de falta de direcciones. Un ejemplo es que a China se le han correspondido 9 millones de direcciones para una población de más de mil millones de habitantes mientras que a la Universidad de Stanford en Estados Unidos le han correspondido 17 millones de direcciones. La siguiente tabla muestra más claramente la necesidad de pasar a IPv6.

Región	Cantidad estimada de usuarios	Cantidad de direcciones asignadas
África	800.000.000	3.000.000
Norte América	500.000.000	125.000.000
América Latina y El Caribe	500.000.000	10.000.000
Europa	250.000.000	50.000.000
Asia	2.500.000.000	50.000.000

Tabla 2.1: Cantidad estimada de usuarios contra cantidad de direcciones asignadas en 2010.

- Nuevos servicios y ampliación de los actuales: Para las ISP la incorporación de IPv6 implica explotar nuevos servicios basados en la proliferación de los dispositivos móviles que se tiene hoy en día, en el caso de la UMSA, esta se vería beneficiada al ampliar sus servicios de Internet con servicios WiFi donde cada usuario puede estar conectado a Internet mediante su propia dirección IP y de forma permanente, esto no sería posible conseguir con el protocolo IPv4 ya que se usan actualmente mecanismos NAT que provocan lentitud en la comunicación.

2.2.2 VENTAJAS DE IPV6

IPv6 ofrece varios beneficios que motivan su utilización en todo entorno, estos de manera resumida son: un amplio espacio de direccionamiento a través de los 128 bits que conforman las direcciones, seguridad a través de IPsec, capacidades móviles, direccionamiento jerárquico para reducir el tamaño de las tablas de enrutamiento y una cabecera simplificada que permite un procesamiento simplificado.

2.3 CARACTERÍSTICAS DE IPV6

A continuación se muestran las características básicas de IPv6, estas características pueden incrementarse a futuro gracias a la escalabilidad que ofrece la estructura de este protocolo.

2.3.1 DIRECCIONAMIENTO IP

Extender el espacio de dirección de 32 a 128 bits permite:

- Soporte de más niveles de direccionamiento jerárquico y a la vez se obtiene enrutamiento más eficiente al reducir el tamaño de las tablas de enrutamiento.
- Más posibilidades de lograr una conexión y flexibilidad global
- Configuración automática de direcciones en un host incluyendo la dirección de capa de enlace en el encabezado.

- Multihomming o multiconexión que permite al host tener varias direcciones IP, un host puede conectarse a varias ISP.
- Redireccionamiento de extremo a extremo sin necesidad de traducción de direcciones permitiendo que enlaces entre host sean más fáciles de implementar.

Se elimina la necesidad de broadcast al implementarse solo multicast y anycast y también la necesidad de evaluar checksums.

2.3.1.1 ENCABEZADO SIMPLE

El eliminar ciertos campos del encabezado y hacer otros campos opcionales se logra:

- Mayor eficacia de enrutamiento y velocidad en procesamiento y reenvío de paquetes.
- Mejora de soporte de opciones IP que ahora son menos estrictos en cuanto a la longitud y con la posibilidad de incluir nuevas opciones en el futuro.
- Calidad de servicio (QoS) mediante la incorporación del control de flujo que permite etiquetar ciertos paquetes que pertenecen a cierto tipo de tráfico y gestionar el ancho de banda sin necesidad de abrir el paquete.

2.3.1.2 MOVILIDAD Y SEGURIDAD

La movilidad permite a las personas que tiene dispositivos móviles conectarse a diferentes redes a través de capacidades como la detección de movimiento que permite que los dispositivos puedan desplazarse sin necesidad de interrupciones en las conexiones de red establecidas con una única dirección IP y una dirección de respaldo en caso de ser necesario.

IPsec es una extensión que proporciona seguridad y su uso es obligatorio en IPv6, a través de la misma se agregan capacidades de autenticación, integridad y confidencialidad de los datos.

2.3.2 ENCABEZADO DE IPV6

El encabezado de IPv6 tiene 40 octetos, tres campos de encabezado heredados de IPv4 y cinco campos de dirección adicionales que se describen a continuación:

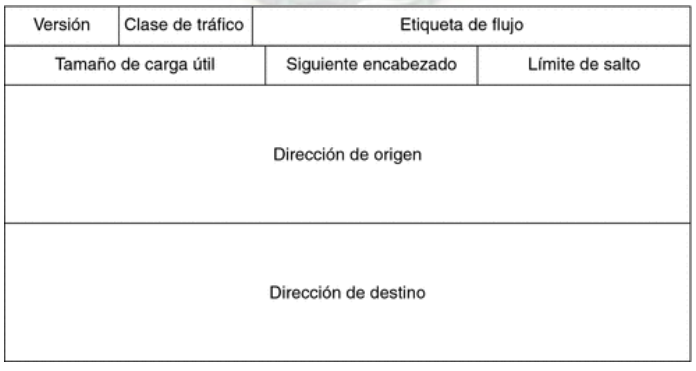


Figura 2.1: Encabezado IPv6.

Versión (4 bits): Contiene el valor 6 binario (0110) que identifica a IPv6.

- Clase de tráfico (8 bits): Especifica la forma en que un paquete debe ser manejado de acuerdo al RFC 24744.

- Identificador de Flujo (20 bits): Aquí se identifica los paquetes que requieren un mismo trato para facilitar el proceso de transmisión en tiempo real.
- Longitud de contenido o carga (16 bits): Representa el tamaño de la carga que trae el paquete, estos son los datos que siguen al encabezado.
- Siguiente encabezado (8 bits): Sirve para identificar al encabezado que viene inmediatamente después del encabezado IPv6.
- Límite de salto (8 bits): especifica el número de saltos que un paquete puede permanecer en la red antes de que se descarte. Este número va decreciendo hasta llegar a cero.
- Dirección de origen (128 bits): Contiene la dirección IPv6 que originó el paquete.
- Dirección de destino (128 bits): Contiene la dirección IPv6 del destino final del paquete.[2]

2.3.2.1 ENCABEZADOS DE EXTENSIÓN IPV6

En IPv6 los campos opcionales son codificados en campos separados que pueden ser colocados inmediatamente después del encabezado de IPv6, estos encabezados promueven mejoras en el procesamiento al otorgar información adicional de gestión del paquete.

2.3.3 DIRECCIONAMIENTO EN IPV6

El esquema de direccionamiento de IPv6 se define en el RFC 42915 el cual define el alcance de las direcciones, donde usarlas, tipos de direcciones y otros aspectos.

2.3.3.1 REPRESENTACION DE LAS DIRECCIONES

Al contener cada dirección 128 bits se necesita una representación diferente de la binaria a causa de su tamaño, es por eso que estas se representan en series de 16 bits hexadecimales, cada serie está separada por dos puntos según el esquema siguiente:

X:X:X:X:X:X:X:X

Donde "X" es un valor hexadecimal de 16 bits de la porción que corresponde a la dirección. Por ejemplo se tiene una dirección: 2031:0000:130F:0000:0000:09C0:876A:130B.
Los ceros al inicio son opcionales, por ejemplo 09C0 es igual a 9C0. • El campo 0000 es igual a 0.
Los campos sucesivos de ceros pueden representarse como doble dos puntos "::" que puede aparecer sólo una vez en una dirección IPv6.
De esta manera una dirección IPv6 puede escribirse de manera aún más corta, en el ejemplo anterior se puede acortar la dirección de la siguiente manera:

2031:0000:130F:0000:0000:09C0:876A:130B -> 2031:0:130F::9C0:876A:130B

Cada tipo de dirección IPv6 (unicast, anycast, multicast[3]) se identifica por los bits de mayor orden (izquierda) de cada dirección, dentro del campo denominado prefijo de formato FP (Format Prefix) cuyo tamaño es variable. La asignación de los prefijos se muestra a continuación:

[2] RFC 2474: Definición del Campo de Servicios Diferenciados (DS) y Cabeceras IPv4 e IPv6. URL: http://tools.ietf.org/html/rfc2474
[3] RFC 4291: IPv6 sobre redes de Acceso Múltiple sin Broadcast. URL: http://tools.ietf.org/html/rfc4291.

Tipo de Dirección	Prefijo Binario	Notación IPv6
Unspecified	00...0 (128 bits)	::/128
Loopback	0...01 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Global unicast	Resto	

Tabla 2.2: Prefijos asignados a direcciones IPv6.

2.3.3.2 TIPOS DE DIRECCIONES IPV6

Direcciones Unicast Locales: Estas direcciones también son conocidas como privadas e identifican a una sola interfaz dentro de un mismo segmento de red de área local LAN (Local Area Network), o dentro de un nodo. Estas se utilizan para configuración automática de dirección, descubrimiento de vecinos.

Direcciones Unicast Globales Agregables[4]: Estas direcciones están definidas en la RFC 23746 identifican a una sola interfaz en Internet pudiendo ser enrutadas en Internet, ya sea de manera nativa o por medio de túneles. Estas permiten agrupación ascendente hasta llegar al ISP y están normalmente compuestas por un prefijo de 48 bits y un ID de 16 bits para subredes permitiendo a cada ISP utilizar hasta 65.535 subredes.

La dirección global asignada por la Agencia de Asignación de números de Internet IANA (Internet Assigned Numbers Authority) comienza por el prefijo 001 (2000::/3). A partir de aquí, IANA asigna espacios de direcciones en los rangos 2001::/16 a los cinco registros (ARIN, RIPE, APNIC, LACNIC y AfriNIC).

Estas direcciones tienen además un mecanismo de agregación basada en intercambios lo cual permite un enrutamiento más eficiente al brindar más de una opción de conectividad a una u otra entidad o ISP de agregación (multihomming).

Una dirección agregable se organiza en una estructura jerárquica de 3 niveles los cuales son:

- Nivel de Topología Pública: Se refiere al espacio de dirección administrado por un conjunto de proveedores o “intercambiadores” de servicios públicos de tránsito de internet.
- Nivel de Topología de Sitio: Se refiere a la parte de la dirección que se utiliza para el enrutamiento interno de la organización. Aquí se manejan la renumeración y multihomming brindados por IPv6. Si una organización utiliza varios proveedores solo se intercambiarán el nivel de topología pública y se mantendrá el nivel de topología de sitio, este nivel es análogo al espacio de direccionamiento de red (ID de red) de la dirección en IPv4.
- Nivel de Identificador de Interfaz: Es la parte de dirección que identifica las interfaces reales de forma individual en los enlaces físicos, este nivel es análogo al espacio de direccionamiento de host (ID de host) en IPv4.

[4] RFC 2374 Formato de Direcciones Unicast Agregables Globales. URL: http://tools.ietf.org/html/rfc2374

El formato de las direcciones unicast globales agregables es el siguiente:

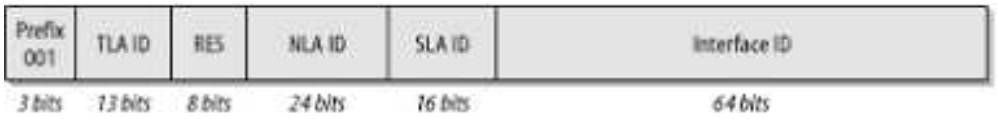


Figura 2.2: Formato de direcciones unicast globales agregables.

Dónde:

- FP corresponde al prefijo del formato (Format Prefix) con un tamaño de 3 bits.
- TLA ID corresponde al ID de agregación de nivel superior (Top Level Aggregation con un tamaño de 13 bits.
- RES corresponde a un espacio reservado (Reserved) con un tamaño de 8 bits.
- NLA ID corresponde al ID de agregación del siguiente nivel (Next Level Aggregation) con un tamaño de 24 bits.
- SLA ID corresponde al ID de agregación del nivel de sitio (Site Level Aggregation) con un tamaño de 16 bits.
- ID de la interfaz con un tamaño de 64 bits.

Los ISP también proporcionan direcciones públicas IPv6 y las organizaciones conectadas también reciben servicios de conectividad directa o indirecta a través de uno o varios proveedores de larga distancia.

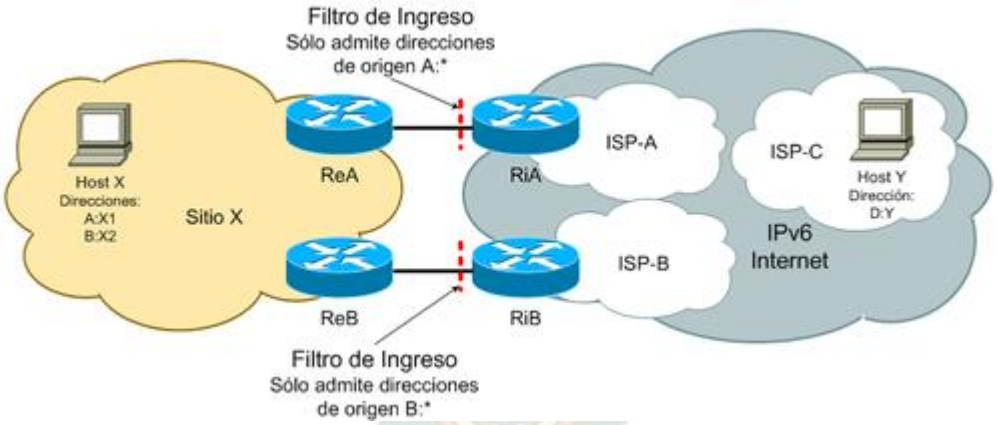


Figura 2.3: Direcciones agregables y conexión con ISP.

Como se ve en la Figura 2.3, una institución puede estar suscrita a uno o varios proveedores (multihoming) a través de un intercambiador sin necesidad de tener prefijos de direcciones para cada proveedor.

Direcciones Anycast: Estas direcciones identifican a múltiples interfaces, define una comunicación “uno a uno-entre-muchos” por lo cual no debe confundirse con un broadcast. Estas direcciones se usan para comunicación con el servidor más cercano, descubrimiento de servicios y movilidad. Estas direcciones se asignan dentro del espacio de las direcciones unicast y no es posible identificarlas observando sus bits.

Direcciones Multicast: Una dirección multicast identifica a un conjunto de interfaces que están descritas en la RFC 2375[5] y definen una comunicación "uno a muchos".

Dirección de Loopback: También conocida como dirección de retorno es una única dirección que se encuentra dentro de las direcciones unicast reservadas. Esta dirección es 0:0:0:0:0:0:0:1 que normalmente se escribe como "::1". Se utiliza para enviar paquete a uno mismo, por lo tanto puede asignarse a interfaces reales.

Dirección No Especificada: Esta dirección se encuentra dentro de las direcciones unicast reservadas y hace referencia a un mismo host y se utiliza sólo cuando un dispositivo no conoce su propia dirección. Esta dirección está compuesta únicamente por ceros, es decir 0:0:0:0:0:0:0:0 que normalmente se escribe como "::".

2.3.3.3 USO DE DIRECCIONES ANYCAST EN IPV6

La aplicación de las direcciones Anycast pueden ser útiles en:

- Redundancia, el servicio no depende de un solo servidor, de modo que si un equipo falla, los demás asumen sus funciones y el servicio continua disponible.

- Balanceo de carga, varios servidores se distribuyen la carga de trabajo, con la finalidad de no saturar un solo servidor y tener otros en ocio.

Con las consiguientes características:

- Al usuario final no le interesa a que servidor accede, simplemente le interesa acceder al servicio y que el mismo esté disponible.
- Las configuraciones basadas en direcciones Anycast permite dicho cometido cuando un host envía un datagrama a una dirección Anycast, la infraestructura de red buscará el camino más corto hasta uno, y preferentemente solo uno, de los equipos que acepta datagramas dirigidos a la dirección Anycast utilizada.
- La ventaja del Anycast es que simplifica la búsqueda del servidor más apropiado, que generalmente es el más cercano.
- Anycast se planteó en el RFC 1546 (1993) como especificación experimental para IPv4 y estaba destinado a ser utilizado para servicios tales como DNS y HTTP.
- Una forma de implementar Anycast es usando el método denominado "Dirección Unicast Compartido", que consiste en asignar direcciones Unicast "normales" a múltiples interfaces.
- En una red donde un grupo de routers puede proporcionar acceso a un dominio de enrutamiento común, se puede asignar una dirección única a todos los routers y cuando un cliente envía un paquete a esta dirección, será enviado al siguiente router disponible.
- Considerar, que, al utilizar direcciones Anycast, el emisor no tiene control sobre cuál será la interfaz a la que se entregará el paquete, ya que esta decisión se toma sobre el nivel del protocolo de enrutamiento.
- Puede darse errores si un emisor envía varios paquetes a una dirección Anycast y los paquetes llegan a diferentes destinos. Lo mismo ocurre si hay que establecer un diálogo con una serie de peticiones y respuestas o si hay que fragmentar el paquete.
- Las direcciones Anycast están dentro del espacio de las direcciones Unicast, por lo que, sintácticamente, no se puede distinguir una dirección Anycast de una Unicast.
- Cuando se convierte una dirección Unicast en dirección Anycast, asignando la dirección Unicast a más de una interfaz, los nodos que han recibido la dirección deben ser configurados de modo que reconozcan la dirección Anycast

[5] RFC 2375: Asignación de Direcciones Multicast. URL: tools.ietf.org/html/rfc2375

2.4 ESTRATEGIAS DE TRANSICIÓN A IPV6

El protocolo IPv6 ha sido diseñado desde el principio teniendo en mente el concepto de la transición que este implicaría, esto para mantener una completa compatibilidad en reversa con IPv4. Dado que no existe un día "D" para el cambio de protocolos en las redes de Internet, la transición se viene dando desde ya hace un tiempo y se prevé un largo periodo de transición.

IPv6 en la actualidad ya funciona en el núcleo de Internet y los proveedores de Internet de nivel superior, y en algunos proveedores de niveles inferiores, de esta manera la tarea de migrar a IPv6 es una obligación a mediano y a largo plazo para todos los proveedores de Internet en general.

Esto no significa que IPv4 vaya a desaparecer de manera inmediata, pues en realidad la transición total de Internet de IPv4 a IPv6 de un momento a otro es prácticamente imposible debido principalmente a la gran cantidad de usuarios que utilizan IPv4 y estos son cada vez más dependientes de todo tipo de actividades que se realizan en Internet.

En el caso de la red de la Universidad Mayor de San Andrés se ha pensado que esta transición debe realizarse de forma progresiva permitiendo a las unidades académicas y administrativas integrar el protocolo IPv6 en sus hosts y servicios de software de la red cuando estén en un estado estable. El protocolo IPv4 coexistirá durante un tiempo con IPv6 hasta un eventual reemplazo de IPv6 en todos los aspectos.

Los objetivos a alcanzarse con la transición a IPv6 son:

- Lograr la coexistencia entre IPv4 e IPv6 hasta que IPv4 desaparezca por completo.
- Uso de los switches de predio, routers, hosts y otros dispositivos de red con soporte de IPv6.
- Eliminar las interdependencias durante la transición.
- La implantación debe ser fácil tanto para el personal técnico encargado de las unidades TICs como para usuarios finales.

Para realizar la transición se han desarrollado mecanismos denominados Transición Simple de Internet o SIT (Simple Internet Transition), aquí se especifican reglas para simplificar la transición y sus características principales son:

- Transición progresiva donde cada elemento de red puede ser actualizado uno a la vez en lugar de todo al mismo tiempo.
- Se requiere solo de un servidor DNS (Domain Name Server) que soporte direcciones IPv6 para comenzar la actualización en los hosts.
- Cuando un elemento es actualizado a IPv6, aún puede utilizar IPv4 creando simplicidad de direccionamiento.
- Sin necesidad de trabajo preparatorio para iniciar la transición.

Según el SIT los requerimientos iniciales para realizar la transición son:

- Una estructura de direcciones IPv6 que permita la derivación de direcciones desde direcciones IPv4.
- Disponibilidad de pila doble o stack doble durante la transición, permitiendo la presencia de los dos protocolos al mismo tiempo y para que los nodos puedan trabajar con IPv4, con IPv6 o con ambos.
- Disponer de una técnica de encapsulación de paquetes IPv6 dentro de paquetes IPv4, esto permite enviar paquetes IPv6 a través de infraestructura que no soporta dicho protocolo.

- Una técnica opcional de traducción de encabezados IPv6 en encabezados IPv4 y viceversa para comunicar entre sí a los nodos con soporte con IPv6 e IPv4 en fases avanzadas de la transición.

Cumpliendo estos requisitos se garantiza por un periodo muy largo la conectividad entre hosts IPv6 y host IPv4 asegurando así la convergencia de la red. Para los ISP esto representa una protección de las inversiones de dinero realizadas en IPv4. Esto ocurrirá mientras existan dispositivos que no permitan la actualización al nuevo protocolo, por lo tanto la interacción ocurrirá con estos hasta que los dispositivos ya no se utilicen más.

2.4.1 REQUISITOS PARA UNA TRANSICIÓN MANEJABLE Y PROGRESIVA

Estos requerimientos son:

- Minimizar la resistencia: En la actualidad las organizaciones e ISPs de Bolivia aún no han aceptado la utilidad de IPv6, esto significa que existe una gran resistencia a adoptar el nuevo protocolo. Un factor importante para que la transición se complete exitosamente es que los mecanismos sean aceptados por la mayoría de usuarios y organizaciones que operan con Internet.
- Transición Progresiva: Se debe estar consciente de que el proceso de transición tomará un periodo de tiempo y no hay forma de sincronizar la transición en distintos sitios. El plan de transición debe elaborarse de manera singular para cada organización y debe estar realizado de forma de evitar en gran medida la existencia de interdependencias. También hay que tomar en cuenta que dentro de la infraestructura de red existen equipos y dispositivos que no pueden ser actualizados a IPv6 por lo tanto se debe seguir utilizando IPv4 hasta que estos dispositivos no se utilicen más.
- Coexistencia e interacción: La interdependencia significa que los nuevos equipos que se adopten tengan soporte integrado a IPv6, esto no implicará que se tenga que actualizar otros equipos antiguos de la red los cuales podrán seguir trabajando con IPv4, los equipos antiguos también deberán ser capaces de comunicarse con los nuevos equipos, es decir que debe haber soporte de IPv6 e IPv4 en todos los nuevos equipos y dispositivos de red.
- Flexibilidad en el mapeo de las direcciones: Es necesario realizar un mapeo de direcciones simple desde IPv4. El mapeo debe realizarse en un sitio específico sin asumir que las direcciones IPv4 son globalmente únicas.
- Herramientas de manejo inteligentes: Para el manejo de ambos protocolos, deben existir conjuntos de herramientas que sean capaces de separar las características de IPv4 e IPv6 por niveles, estas herramientas deben incluir la detección de rutas, implantación de puntos de traducción y mecanismos revisores de la capacidad de IPv6 en los hosts y dispositivos.

2.4.2 COMPONENTES DE LA TRANSICIÓN

Los principales componentes que se verán involucrados dentro de la transición al protocolo IPv6 son:

- Hosts o nodos de cliente: Se necesita que exista la interacción transparente entre los hosts que soporten IPv4 y los que soporten IPv4 e IPv6, además todos los hosts que soporten IPv6 deben ser capaces de comunicarse con la tecnología antigua.
- Routers y protocolos de enrutamiento: Estos dispositivos no pueden asumir que todos los vecinos con los que tiene interacción tienen soporte para IPv6 y los protocolos de enrutamiento establecidos deben estar basados en tráfico de origen y destino.
- Sistemas de denominación de dominio DNS (Domain Name System): DNS debe trabajar con direcciones IPv4 e IPv6 para que cualquier dispositivo pueda realizar consultas.

- Dependencias de los componentes: Los servidores DNS deben ser los primeros dispositivos físicos que se deben actualizar luego de asignar una dirección o un espacio de dirección IPv6 a cualquier dispositivo, así estos también podrán realizar y recibir consultas para direcciones IPv6. Mientras que el protocolo dual permite que IPv4 funcione sin inconvenientes.

2.4.3 MECANISMOS DE TRANSICIÓN A IPV6

Los equipos de trabajo de la IETF han diseñado herramientas, protocolos y mecanismos que pueden ser usados para permitir la transición de redes basadas en IPv4 hacia IPv6 desde el año 1996.

Los mecanismos permiten a las infraestructuras IPv4 utilizar IPv6 y también de forma viceversa. Se prevé que estos mecanismos tengan un uso prolongado. Cabe recalcar que para diferentes situaciones se requieren diferentes estrategias de transición.

Estos mecanismos de integración y coexistencia son los siguientes:

- Stack Doble o Pila Doble
- Túneles
- Traducción de protocolos

2.4.4 STACK DOBLE O PILA DOBLE

Este método es el preferido en la mayoría de los casos y este consiste en que un nodo tiene conectividad para redes IPv4 e IPv6 de manera simultánea, donde los dispositivos de red el router y switch se configuran para que puedan admitir ambos protocolos pero dando prioridad a IPv6 cada vez que se pueda.

En cada interfaz activa del nodo con Stack Doble existen configuraciones para los dos protocolos, es decir dos pilas, a partir de aquí el nodo pasa a denominarse “nodo IPv4/IPv6”, un nodo decide que stack utilizar en cada caso de acuerdo a la dirección del destino del paquete, prefiriendo utilizar IPv6 cada vez que esté disponible. Por ejemplo si se trabaja con direcciones IPv6 el nodo comunicará a través de paquetes IPv6 y si se elige la dirección IPv4 la conexión se realiza a través de paquetes IPv4. Esto no afecta a las aplicaciones y servicios antiguos que utilicen IPv4 que seguirán funcionando sin problemas, mientras que las nuevas aplicaciones tendrán la capacidad de operar aprovechando ambos protocolos.

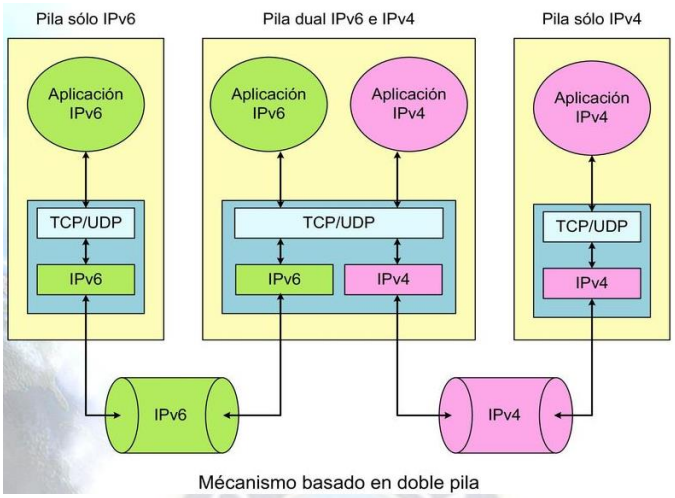


Figura 2.4: Funcionamiento de Stack Doble.

Para obtener su dirección singular IPv6 cada nodo puede utilizar mecanismos de configuración automática como DHCPv6 o configuración manual de IP.

No es necesario que las direcciones IPv4 e IPv6 estén directamente relacionadas pero en caso de que se requiera que tengan alguna relación ambas existen pasos para la obtención de direcciones IPv6 compatibles con IPv4 que son:

1) La dirección del Stack IPv4 se configura mediante DHCPv4, configuración manual de la dirección, uso del protocolo de arranque BOOTP, uso del protocolo RARP
2) El nodo antepone un prefijo de 96 bits con un valor de 0:0:0:0:0:0 a la dirección IPv4 configurada en el anterior paso y se usa esta nueva dirección como la dirección IPv6.

Cabe recalcar que las aplicaciones basadas en IPv4 deben ser actualizadas para que también soporten IPv6 pues en la mayoría de estas se usa API que solo soporta direcciones de 32 bits.

2.4.5 RESOLUCIÓN DE DNS

El servicio de nombres de dominio es un mecanismo que se utiliza para relacionar el nombre de un nodo con una dirección IP, debido a que este mecanismo fue diseñado para trabajar con direcciones IPv4 ahora este mecanismo debe ser actualizado para trabajar con direcciones IPv6, la actualización de DNS debe incluir los siguientes aspectos:

- El registro AAAA: anteriormente conocido como registro A que era usado para almacenar direcciones IPv4, ahora cumple la misma función admitiendo direcciones de tamaño de 128 bits.
- El dominio IP6.INT: usado para realizar la búsqueda inversa para los nodos, esto en base a direcciones IPv6.
- Redefinición de consultas existentes: esto implica que toda consulta debe soportar los registros A y AAAA para realizar cualquier procedimiento asociado a cada registro.

2.4.6 TÚNELES

Este es el segundo mecanismo de transición preferido para su implementación en redes, consiste en encapsular un paquete IPv6 dentro de IPv4 y así de esta forma un nodo IPv6 puede ser

localizado en infraestructuras IPv4 y de esta forma se permite por ejemplo que redes LAN que usan IPv6 pero que están en ubicaciones distintas puedan intercambiar información a través de túneles establecidos en infraestructuras IPv4.

Los túneles son generalmente utilizados sobre redes para permitir el intercambio de datos específicos o protocolos incompatibles sobre una red existente, por ejemplo IPsec y algunos mecanismos de redes privadas virtuales VPN (Virtual Private Network) usan protocolos de tunneling seguros para transferir datos sensibles sobre redes IP públicas.

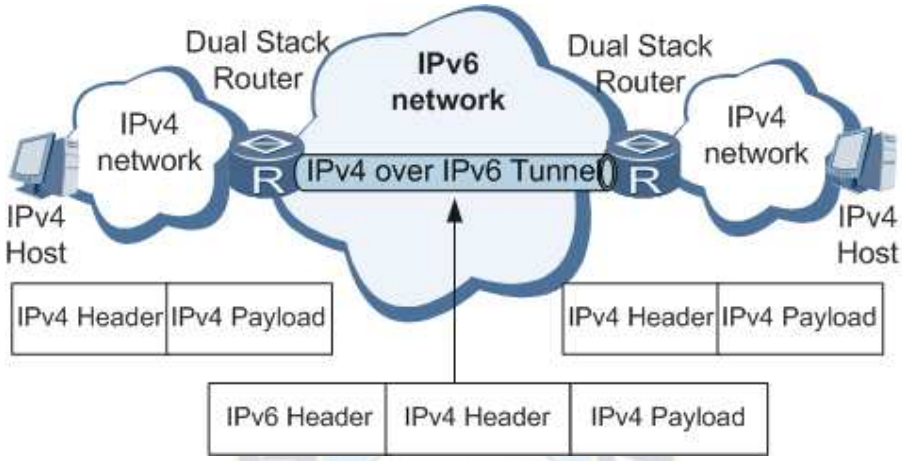


Figura 2.5: Túnel establecido sobre IPv4 entre dos islas con nodos IPv6.

Los túneles deben ser considerados como alternativas solamente cuando es imposible obtener conectividad de forma nativa sobre la infraestructura de red y los enlaces.

La comunicación por túneles entre nodos con soporte IPv6 es posible gracias al encapsulado de IPv6 dentro de IPv4 y a las infraestructuras que están basadas en IPv4 e IPv6 ya que en algunos casos se necesitarán pasar varias veces por infraestructuras que soportan IPv6 e IPv4, es por esto que para leer el contenido IPv6 se requiere de Stack Doble.

Los principales problemas que presenta el tunneling son:

- La unidad máxima de transmisión MTU (Maximum Transmission Unit) se ve reducida a solo incluir 20 octetos en el encabezado de IPv4 sin contener ningún campo opcional, esto se traduce en un aumento de tráfico de paquetes en la red.
- Dificultad que se presenta al resolver problemas en redes que implantan este mecanismo de transición.
- Existe un retardo adicional ocasionado por la encapsulación y desencapsulación de paquetes IPv6.

Es por esta razón que esta es considerada como una técnica de transición intermedia y no debe considerarse en ningún caso como una solución definitiva ya que el objetivo final es una arquitectura IPv6 nativa en toda la red.

Para poder configurar un túnel es necesario tomar en cuenta los siguientes aspectos:

- Habilitar el protocolo 41: Este es el valor utilizado en el campo “número de protocolo” en el encabezado de IPv4, este valor indica que el paquete IPv6 está encapsulado dentro de IPv4. Esto se describe en el RFC 2893[6].
- Manejo de Mensajes de error ICMPv4: Cada mensaje de error en IPv6 ocupa un espacio de 16 octetos a diferencia de los 8 octetos que ocupaba cada mensaje con IPv4.
- Traducción de Direcciones NAT: Es posible establecer túneles solamente si NAT está configurado en modo estático, en los modos de traducción dinámica de puerto y redirección de puerto no es posible establecer túneles. Esto se describe en el RFC 2766[7].

En el primer extremo del nodo se encapsulan los paquetes y en el segundo extremo se desencapsulan, bajo este concepto los túneles pueden ser construidos en los siguientes escenarios:

- Túneles de Router a Router: Mientras que los routers funcionen con Stack Doble es posible crear túneles para interconectar islas aisladas.
- Túneles entre Host y Router: En el caso de que los hosts funcionen con Stack Doble y que el router también admita Stack Doble. Si existe otra interfaz en el router con IPv6 nativa es posible realizar conexiones de extremo a extremo entre hosts de islas aisladas.
- Túneles de Host a Host: Aquí se requiere que ambos host tengan Stack Doble configurado y solo se permite establecer conexiones IPv6 de extremo a extremo entre ellos.

Los escenarios anteriormente descritos se muestran en la siguiente Figura:

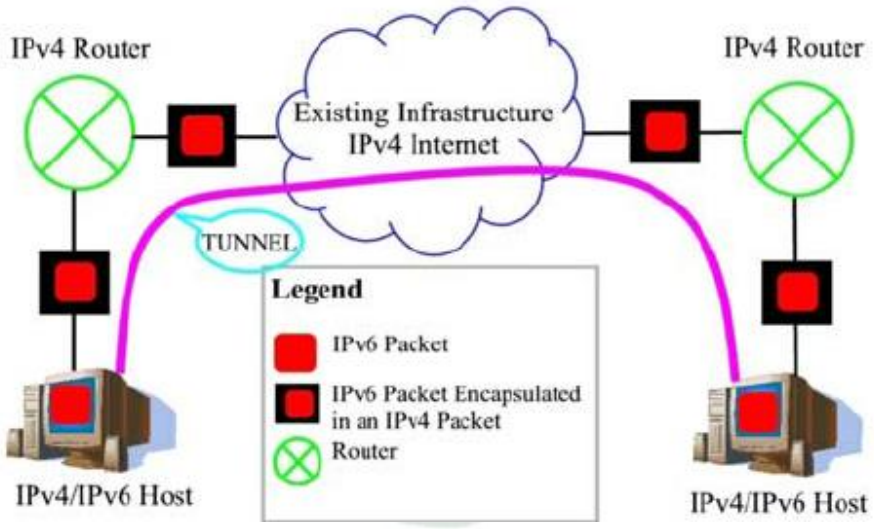


Figura 2.6: Escenarios para la creación de un túnel.

Y a partir de las configuraciones anteriores se definieron varias técnicas para establecer túneles entre nodos IPv4/IPv6, la siguiente lista muestra los protocolos y técnicas diseñadas para el establecimiento de túneles organizadas de las más prominentes a las menos prominentes:

- Túneles configurados
- Túnel broker

[6] RFC 2893: Mecanismos de transición a IPv6. URL: http://tools.ietf.org/html/rfc2893
[7] RFC 2766: Protocolo de Traslación - Traslación de Dirección de Red. URL: http://tools.ietf.org/html/rfc2766

- Túnel server
- Túnel 6to4
- Túnel GRE
- Túnel de protocolo de direccionamiento automático de túnel dentro de un sitio o ISATAP (Intransite Automatic Tunnel Addressing Protocol)
- Túnel automático compatible con IPv4

2.4.6.1 TÚNELES CONFIGURADOS

Los túneles configurados son permitidos y establecidos estáticamente (de forma manual) sobre nodos con Stack Doble previamente configurados, debido a que es uno de los primeros mecanismos de transición que soporta IPv6 por lo que son soportados por la mayoría de las implementaciones IPv6 hoy en día. Un túnel configurado es de interés para organizaciones que requieren control estricto sobre el establecimiento de túneles por las siguientes razones:

- Debido a que las direcciones IPv4 de origen y destino de cada túnel configurado son conocidas por las reglas de seguridad de firewalls o ACL (Access Control Lists), a diferencia que en mecanismos como túnel 6to4 que tiene control restrictivo.
- Cuando se implementan varios túneles sobre una red el personal puede deshabilitar el túnel en cualquier momento simplemente apagando la interfaz del túnel y afectando solo al tráfico sobre esa interfaz del túnel.

Un túnel configurado de forma manual es equivalente a un enlace permanente entre dominios IPv6 y comúnmente se usan en conexiones entre routers de extremo. Para realizar esto se configuran direcciones estáticas IPv6 e IPv4 en cada interfaz extremo del túnel. El túnel puede establecerse por ejemplo entre dos routers o entre un router y un host.

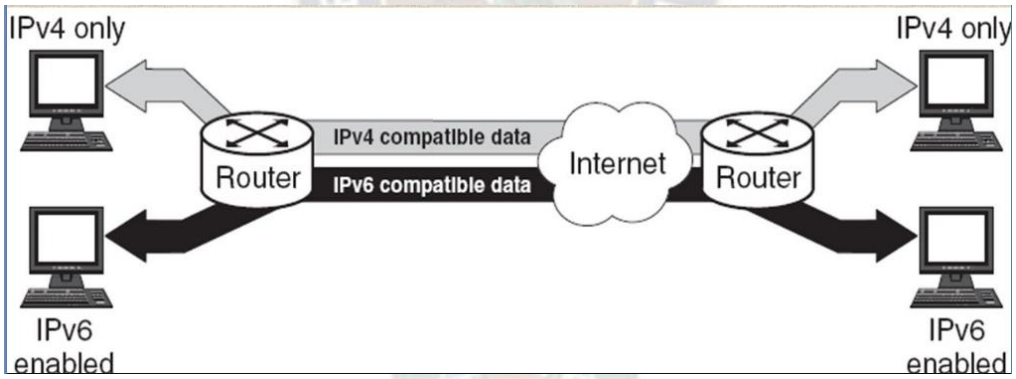


Figura 2.7: Topología con routers Stack Doble.

Se deben asignar las siguientes direcciones a las interfaces del túnel configurado:

- Dirección IPv4 local: Una dirección por la cual el nodo Stack Doble puede ser alcanzado sobre la red IPv4. Es usada como dirección de origen para el tráfico saliente.
- Dirección IPv4 global: Una dirección por la cual el nodo Stack Doble puede ser alcanzado sobre la red IPv4. Es usada como dirección de destino para el tráfico saliente.
- Dirección IPv6 local: Una dirección asignada localmente a la interfaz del túnel.

Luego de haber configurado todas las direcciones de cada interface del túnel, se debe configurar propiamente para permitir paquetes IPv6 entre dos redes IPv6 en cada extremo.

2.4.6.2 TUNEL BROKER

Tal como se vio en la anterior sección, el túnel configurado requiere de configuración manual en cada extremo, pero este mecanismo no es escalable si se lo maneja de forma estática. Para facilitar esto la IETF definió un mecanismo denominado Túnel Broker que está definido en la RFC 3053[8].

El Túnel Broker es un sistema externo que actúa como servidor en redes IPv4 y recibe solicitudes para tunneling de los nodos Stack Doble, o dicho de otra manera, las solicitudes son enviadas sobre IPv4 por nodos con Stack Doble al Túnel Broker utilizando HTTP de esta manera los usuarios finales pueden llenar una solicitud en una página web para solicitar un túnel configurado para sus nodos Stack Doble, luego se envía de regreso información sobre HTTP, la información incluye direcciones IPv4, direcciones IPv6 y rutas IPv6 por defecto a ser aplicadas en los nodos, opcionalmente se puede facilitar un archivo de comandos o script para facilitar la configuración del túnel en el sistema operativo. De esta manera los nodos Stack Doble quedan configurados remotamente.

Como requisitos además de tener configurados nodos Stack Doble también se requiere estar conectado a un dominio IPv6 y que el Túnel Broker y los nodos Stack Doble estén en redes IPv4 distintas. El proceso de establecimiento de Túnel Broker se muestra en la siguiente Figura.

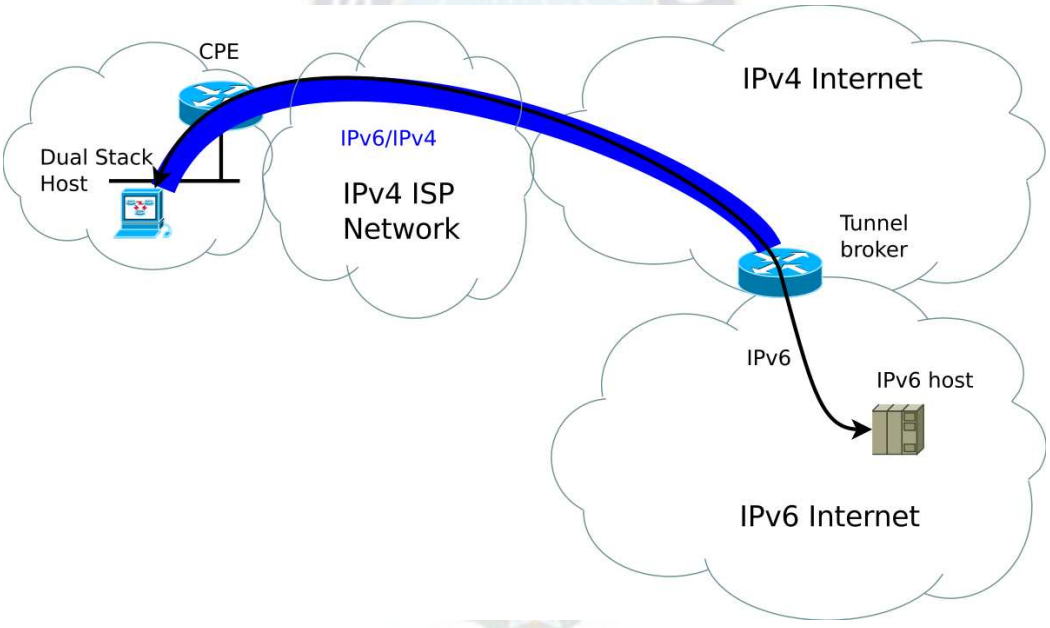


Figura 2.8: Host Stack Doble estableciendo un túnel configurado usando Tunnel Broker

2.4.6.3 TUNEL SERVER

El túnel server es un modelo simplificado del túnel broker. El túnel server combina el servidor de Túnel Broker y el nodo o host Dual Stack en el mismo sistema en lugar de tener dos sistemas separados, la forma de solicitar el túnel configurado es generalmente la misma que en Túnel Broker, tratándose así de solicitudes sobre HTTP en redes IPv4. La siguiente Figura muestra el funcionamiento de Túnel Server.

[8] RFC 3053: IPv6 Tunnel Broker. URL: http://tools.ietf.org/html/rfc3053

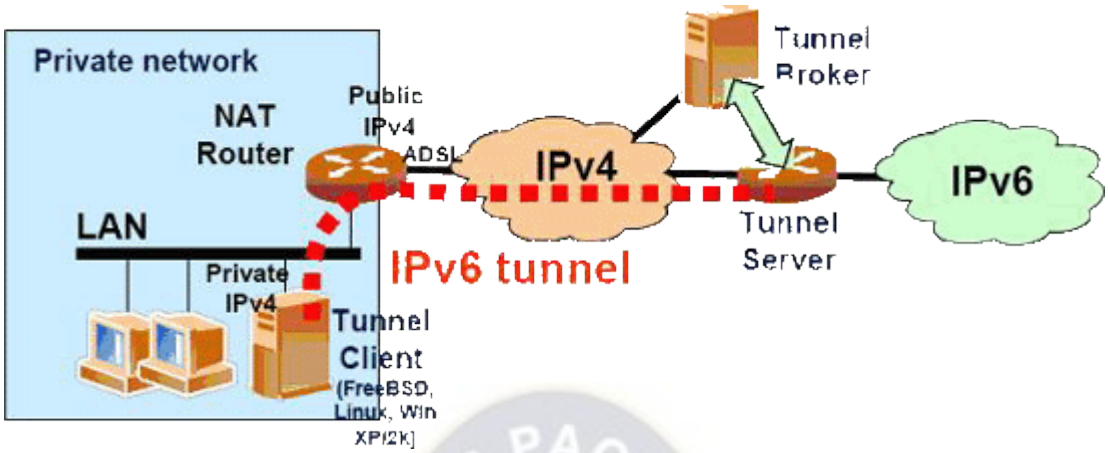


Figura 2.9: Host Dual Stack estableciendo un túnel configurado a través de Túnel Server.

2.4.6.4 TÚNEL 6T04

Al establecer, operar, administrar y mantener túneles configurados entre dominios IPv6 se requiere sincronización en al menos dos dispositivos. Para algunas organizaciones es aceptable manejar estáticamente algunos túneles pero para entidades más grandes esto es un problema y no es una práctica recomendada, para facilitar el proceso de último recurso se ha definido en la RFC 3056[9] otro mecanismo denominado Túnel 6to4.

Acá se establecen de forma automática islas funcionando con IPv6 sin necesidad de configurar direcciones de origen y destino para establecer túneles.

Entre las principales características de los túneles 6to4 están:

- Tunneling automático: los túneles se establecen dinámicamente de acuerdo a la dirección IPv6 de destino, de igual forma que en los túneles configurados, se encapsulan paquetes IPv6 en paquetes IPv4.
- Habilitado en los bordes: 6to4 debe estar habilitado en los routers de extremo o borde para que sea posible alcanzar otros sitios 6to4 usando la infraestructura IPv4.
- Posibilidad de implementar un prefijo único a cada isla IPv6 lo cual hace posible su rápida implementación en redes corporativas sin recuperar direcciones de los ISP o registros. Los prefijos 6to4 están todos basados en el espacio de direccionamiento 2002::/16 asignado por la IANA.
- Operación basada en la infraestructura IPv4: Para la configuración automática de las direcciones IPv6 se basan en las direcciones de la infraestructura IPv4 de los nodos de extremo donde se aplicará el túnel.

[9] RFC 3056: Conexión de Dominios IPv6 a través de Nubes IPv4. URL: http://tools.ietf.org/html/rfc3056.

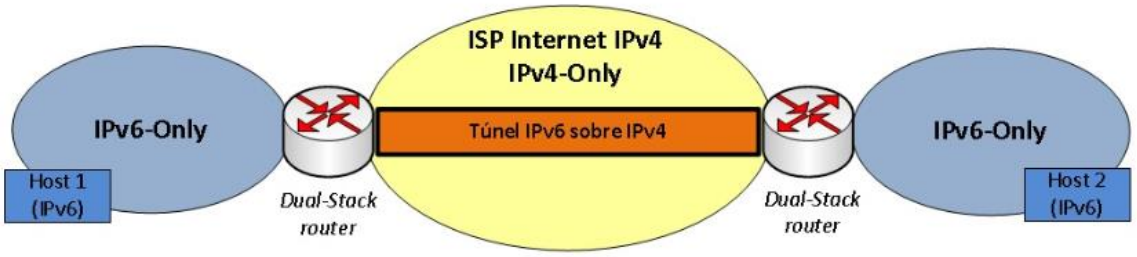


Figura 2.10: Conexión de extremo a extremo entre hosts IPv6 a través de un Túnel 6to4.

2.4.6.5 TÚNEL GRE

La técnica de transición por túneles GRE es bien conocida por ser estable y brindar conexiones seguras de punto a punto, este túnel proporciona beneficios adicionales para organizaciones que usan protocolo de enrutamiento IS-IS para IPv6 debido a que IS-IS necesita enviar mensajes de capa de enlace entre los routers adyacentes en una red, los túneles GRE son los únicos que pueden llevar este tipo de tráfico.

Un túnel GRE debe estar configurado estáticamente entre routers para permitir el transporte de paquetes IPv6 sobre IPv4.

2.4.6.6 TÚNEL ISATAP

Conocido por sus siglas en inglés ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), este es un mecanismo de capa superior automático que usa la red IPv4 subyacente como la capa de enlace para IPv6. ISATAP requiere routers con Stack Doble en funcionamiento, y permite que los host IPv6 se comuniquen entre sí mediante un enlace virtual, de esta forma se logra crear enlaces virtuales y redes IPv6 a través de la infraestructura IPv4. Entre sus funcionalidades están:

- Túneles automáticos: Estos se crean entre hosts, routers, o routers a hosts sin necesidad de aplicar configuraciones manuales.
- Formato de dirección ISATAP: Las direcciones que asigna ISATAP son hechas usando la concatenación de un prefijo unicast global IPv6 con el formado especial de la ID de interface, esto se muestra en la siguiente Figura.

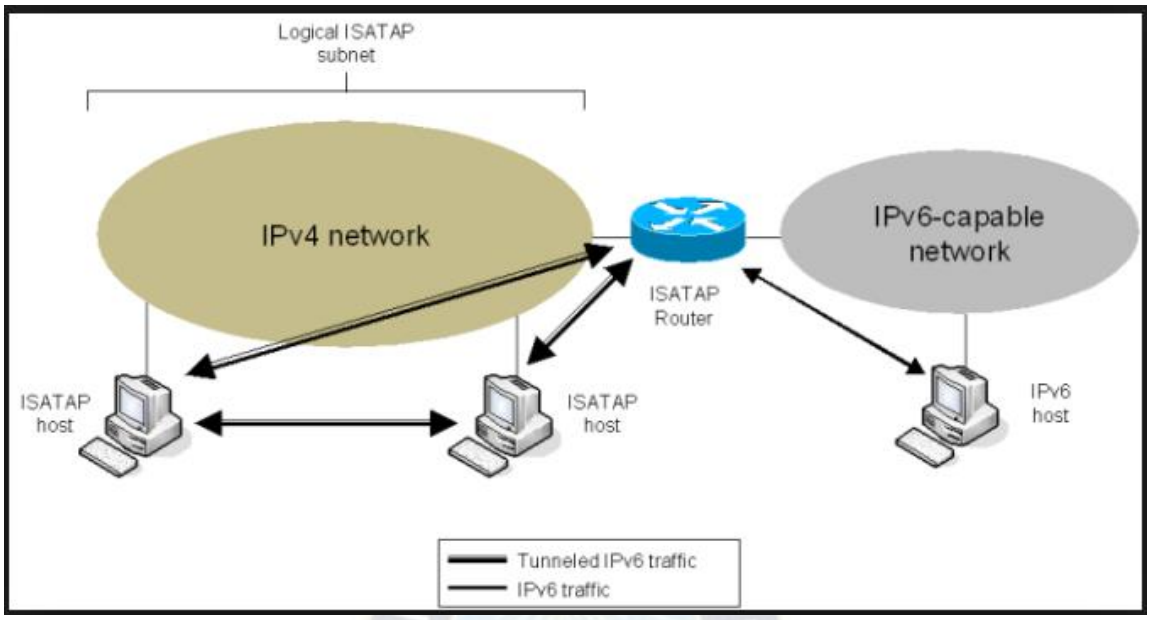


Figura 2.11: Asignación de dirección entre un host ISATAP y un router ISATAP.

2.4.6.7 TÚNEL AUTOMATICO COMPATIBLE CON IPV4

Este fue uno de los primeros mecanismos de transición definidos por la IETF, y consiste en configurar túneles de forma automática permitiendo conectar redes y hosts IPv6 aisladas con otras redes y hosts, acá se usa el prefijo ::/96 que es el compatible con IPv4, se usa para asignar las direcciones de origen y destino de los puntos finales de la red.

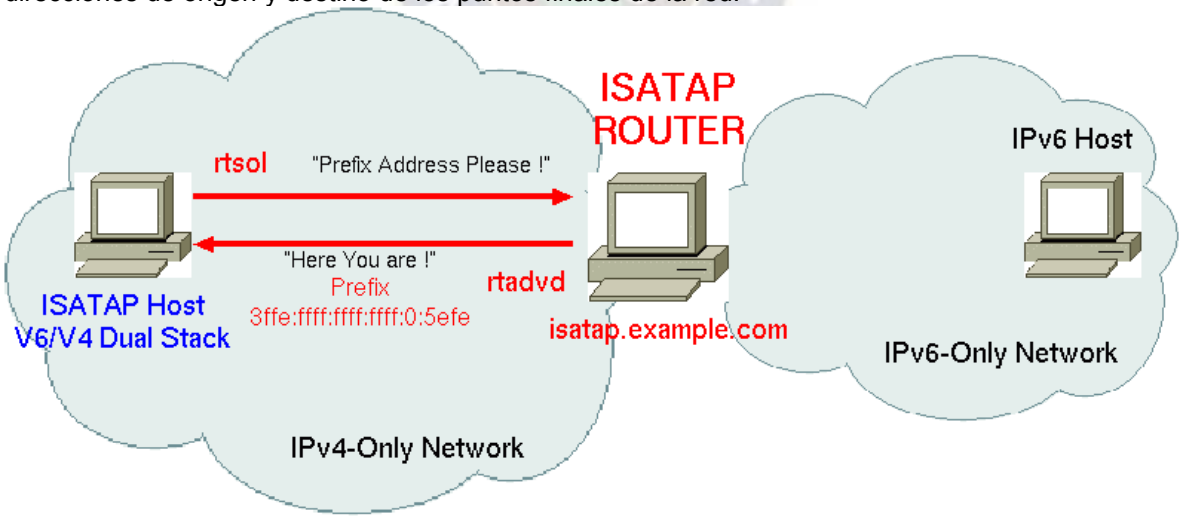


Figura 2.12: Implementación de un túnel automático compatible con IPv4.

Aunque esta es una manera simple de proveer de conectividad IPv6 en las redes, esta tiene varias limitaciones:

- Homogeneidad: Las comunicaciones siempre se realizan sólo mediante direcciones compatibles con IPv4, más aun, este mecanismo se limita a túneles entre hosts, un router puede actuar como un hosts para algunas aplicaciones.
- Limitaciones de espacio de direccionamiento: Debido a que este mecanismo está establecido en base a direcciones IPv4.
- Escalabilidad: Este mecanismo requiere de una dirección IPv4 única para cada host para permitir el establecimiento de IPv6 a la larga.

2.4.6.8 TUNNELING TEREDO

Este método también es conocido como "shipworm" y es uno de los nuevos mecanismos diseñados por la IETF para implementar la transición de las redes, la principal característica de este mecanismo es la habilidad de entregar paquetes IPv6 a redes que se encuentran detrás de dispositivos funcionando con NAT en dominios IPv4, esto es posible gracias a la encapsulación de paquetes sobre datagramas UDP. El mecanismo Teredo requiere además de los siguientes componentes:

- Servidor Teredo
- Relay Teredo
- Cliente Teredo

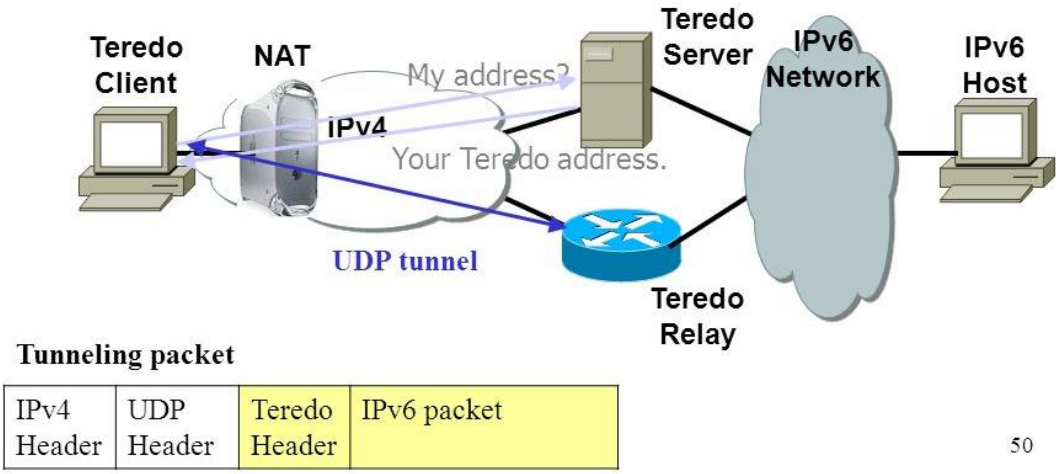


Figura 2.13: Modelo de túnel Teredo.

2.4.6.9 SOBRE EL MECANISMO DE TUNNELING APROPIADO

Hasta esta sección, se ha visto que existen túneles de host y túneles de sitio a sitio. Hay varios mecanismos de tunneling que permiten transportar paquetes IPv6 sobre la infraestructura IPv4, se debe recordar que el Túnel Configurado, el Túnel GRE y el Túnel 6to4 pueden ser usados para interconectar sitios. ISATAP puede ser usado para interconectar hosts. Los mecanismos Túnel Server y Túnel Broker también deben ser usados para implementar conectividad IPv6 a larga escala y en nodos aislados (Redes IPv4 Stub), el Túnel Teredo proporciona conectividad a nodos detrás de dispositivos que operan con NAT, y el Túnel Automático Compatible por lo general no es usado debido a sus limitaciones; en la sección de recomendaciones se indica el uso pertinente de un tipo de túnel en situaciones tipo en la institución.

2.4.7 TRADUCCIÓN DE PROTOCOLOS NAT

Este mecanismo es también conocido por sus siglas en inglés NAT-PT (Network Address Translation - Protocol Translation), está definido en la RFC 2766[10] y consiste en un algoritmo que traduce los encabezados de los paquetes IPv4 e IPv6, incluyendo los encabezados ICMP; esto permite comunicaciones directas entre dispositivos que usan diferentes versiones del protocolo IP y que se encuentran en redes distintas a través de traducciones similares a las que realiza NAT, pero fundamentalmente más complejas, esta técnica es la opción menos favorable y debe usarse como método de último recurso para su implementación en cualquier tipo de infraestructura de red.

Entre sus características se encuentran:

- NAT-PT provee de un enrutamiento interno IPv6 y uno externo IPv4 de forma similar que lo hace NAT en IPv4.
- Para realizar las traducciones de paquetes IPv4 a IPv6 y viceversa se utilizan dispositivos dedicados denominados traductores de direcciones IPv6.
- El algoritmo usado por NAT-PT es el SIIT (Stateless IP/ICMP Translator) que está definido en la RFC 2765[11]. Este es considerado como el traductor de protocolo. • Requiere por lo menos una dirección IPv4 pública para cada red IPv6 que desea comunicación con IPv4.
- Se utiliza una tabla de mapeo que contiene vínculos de las direcciones IPv6 de los nodos internos de la red IPv6 con las direcciones IPv4 de los nodos externos a la red y viceversa, de esta forma se brinda un enrutamiento transparente.
- Este mecanismo también implementa extensiones para ofrecer transparencia en la capa de aplicación denominada ALG, estas son: DNS-ALG y FTP-ALG.

En el siguiente diagrama de topología se muestra una aplicación de NAT-PT:

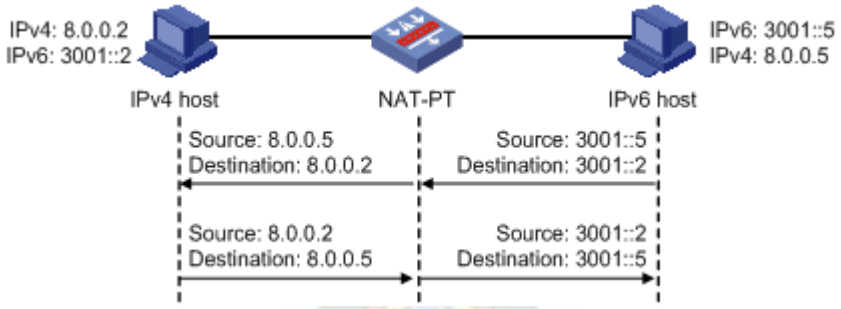


Figura 2.14: Comunicación entre nodos a través de NAT-PT

Aunque actualmente las redes de las organizaciones tienen implementado NAT y eso brindaría de bastante experiencia en la administración de NAT-PT, aun así se tienen varias desventajas entre las cuales están:

- Administrar NAT implica un alto costo.
- El proceso NAT-PT consume bastantes más recursos en los dispositivos en comparación con la implementación de Stack Doble o túneles.
- Es necesario agregar las extensiones DNS-ALG o FTP-ALG según sea el caso para lograr la convergencia de la red.

[10] RFC 2766: Protocolo de Traslación - Traslación de Dirección de Red. URL: http://tools.ietf.org/html/rfc2766
[11] RFC 2765: Algoritmo de Traducción sin Estado IP/ICMP (SIIT). URL: http://tools.ietf.org/html/rfc2765

2.5 ENRUTAMIENTO EN IPV6

Las redes que trabajan con IPv4 en la actualidad son muy complejas y cada red se hace única al contener características distintas una de otra como la topología, tamaño, extensión, número de hosts, etc.

Todas estas tienen en común que hacen uso de enrutadores, comúnmente denominados routers, para realizar comunicaciones con otros dispositivos como con un ISP, y para comunicarse con otros dispositivos de otras redes, es por esto que se necesita de configurar además de protocolos de enrutamiento. Estos protocolos trabajan en la capa 3 del modelo OSI, la capa de Red, aquí es donde las direcciones IP toman importancia para determinar la ruta para el encaminamiento de los diversos paquetes IP que circulen mientras exista interacción dentro de una red o entre múltiples redes.

Igualmente como ocurre con el enrutamiento sin clase CIDR (Classless Interdomain Routing) en IPv4, IPv6 usa enrutamiento de concordancia con el prefijo más largo. Acá se implementan versiones modificadas de los protocolos de enrutamiento comunes para administrar direcciones IPv6 que son más largas y con diferente estructura de encabezado. En otras palabras los protocolos de enrutamiento son simplemente extensiones lógicas de los protocolos usados en IPv4.

Gracias al mayor espacio de dirección, se permiten asignar cantidades más grandes de direcciones a los ISP y organizaciones. Ahora los ISP pueden agrupar a todos sus clientes y su red corporativa con un único prefijo y anunciarlo en Internet.

Más adelante en el desarrollo de este documento se detalla cual sería el impacto operativo en aplicar IPv6 a los routers y dispositivos de red mostrando si en este caso específico es factible o no.

2.5.1 DISTANCIAS ADMINISTRATIVAS

El valor de la distancia administrativa representa la fiabilidad que representa un protocolo de enrutamiento, gracias a este valor se han priorizado los protocolos desde el más fiable al menos fiable. Durante el proceso de selección de rutas que realiza el router, este usa la distancia administrativa para elegir la mejor ruta cuando existen distintas rutas con distintos protocolos de enrutamiento hacia una misma red o destino. En IPv6 los valores de las distancias administrativas no cambian respecto a sus equivalentes en IPv4 y estos valores se muestran en la siguiente tabla:

Routing Technique	Preference
Connected Interface	0
Static Route	1
EIGRP Summary Route	5
EBGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
ISIS	115
RIP	120
EGP	140
ODR	160
External EIGRP	170
Internal BGP	200
Unknown	255

Tabla 2.3: Distancias administrativas de los protocolos IPv6.

A continuación se describen los distintos protocolos de enrutamiento existentes para IPv6.

2.5.2 ENRUTAMIENTO ESTÁTICO

Al igual que en IPv4, el enrutamiento estático IPv6 es el tipo de enrutamiento más sencillo que se puede implementar, consiste en introducir las distintas rutas de forma manual dentro de cada router, por lo cual el administrador de red tiene la tarea de calcular las rutas, así como definir cuál es la más efectiva para realizar el envío de los datos, según sea la topología de red a manejar.

Entre sus ventajas se encuentra la simplicidad para manejarlo en redes pequeñas, el empleo reducido de ancho de banda para servicios de transmisión y además del bajo uso de CPU que el router emplea al administrar rutas estáticas.

2.5.3 BGP+ PARA IPV6

El protocolo de puerta de enlace de borde BGP4 (Border Gateway Protocol) es usado para realizar comunicaciones entre sistemas autónomos AS (Autonomous Systems).

BGP4 es un protocolo vector distancia que usa el puerto 179 de TCP para establecer conexiones con otros routers BGP vecinos. Los routers BGP intercambian la información de las redes alcanzables a través de mensajes de actualización enviados entre vecinos, estos mensajes contienen información acerca de la adición o la eliminación de una ruta.

Durante su operación se operan rutas a distintos sistemas autónomos para alcanzar rutas particulares. Este protocolo ha sido diseñado para ser altamente escalable y redes de tamaño inmenso como la Internet global.

BGP4+ es una versión extendida de BGP4 que es también conocida como multiprotocolo BGP, esta extiende las capacidades ya existentes de BGP4 para incluir soporte para IPv6, IPX y VPN, y aun así seguir teniendo soporte para IPv4. Este protocolo está definido en el RFC 4760[12]. En la siguiente Figura se muestra el establecimiento de BGP4+ con IPv6.

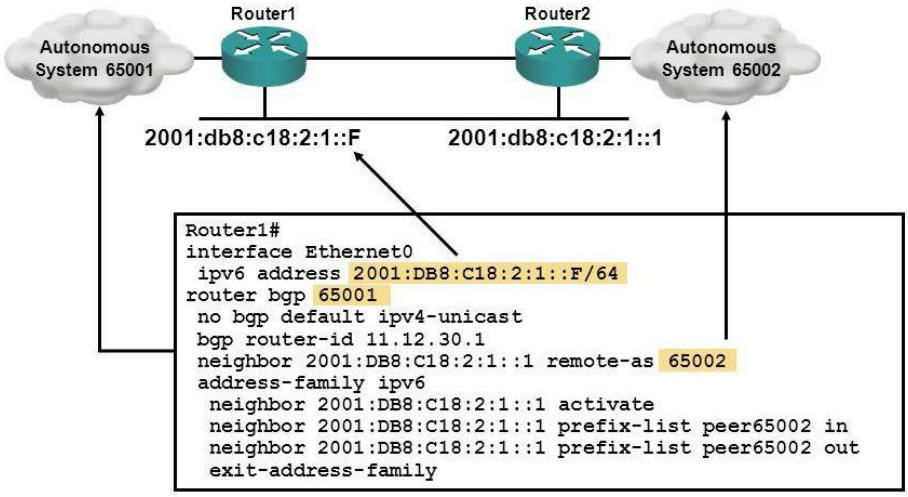


Figura 2.15: Conexión de dos routers utilizando BGP4+.

2.5.4 RIPng

Es parte de la familia de protocolos IGP (Interior Gateway Protocol) y la RFC 2080[13] define el protocolo de información de enrutamiento de siguiente generación RIPng (Routing Information Protocol Next Generation) como un protocolo de enrutamiento simple como una contraparte a RIP versión 2 (RIPv2) proporcionando una manera sencilla de crear redes IPv6 pues no se requiere de ningún conocimiento global de la red debido a que solo se intercambia información entre vecinos mediante mensajes locales.

Este protocolo al igual que su predecesor RIPv2, tiene un vector distancia con un límite de 15 saltos con actualizaciones de envenenamiento en reversa y horizonte dividido para evitar bucles de enrutamiento (routing loops). Y entre otras características RIPng incluye:

- Transporte para IPv6.
- Incluye el prefijo IPv6 y la dirección IPv6 del siguiente salto, (basadas en 128 bits). • Usa la dirección de enlace local FE80::10 para actualizaciones de enrutamiento entre routers vecinos.
- Se usa la dirección multicast estándar FF02::5 para “todos los routers” en un ámbito de enlace local.
- Envía actualizaciones de enrutamiento por el puerto UDP 521.

Si se desea implementar Stack Doble deben habilitarse RIP y RIPng en las interfaces.

[12] RFC 4760: Extensiones Multiprotocolo para BGP4. URL: http://tools.ietf.org/html/rfc4760
[13] RFC 2080: RIPng para IPv6. URL: http://tools.ietf.org/html/rfc2080

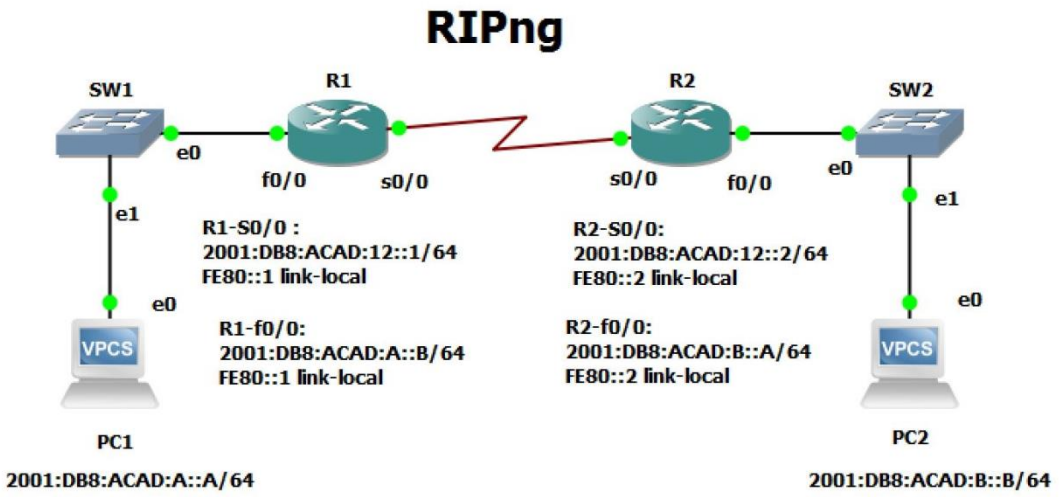


Figura 2.16: Conexión de dos routers utilizando RIPng.

2.5.5 IS-IS PARA IPV6

El protocolo de Sistema Intermediario a Sistema Intermediario IS-IS (Intermediate System to Intermediate System) es un protocolo de estado de enlace basado en el algoritmo Dijkstra[14] que ofrece una gran escalabilidad y un sistema jerárquico. Entre sus características están:

- El uso del costo de enlace para calcular la mejor ruta
- Tiempo menor de convergencia de la red.
- Basado en la estructura de dos niveles donde cualquier router IS-IS puede ser:

  1) Router de nivel 1 (L1): responsable del enrutamiento IPv6 en área interna
  2) Router de nivel 2 (L2): responsable del enrutamiento IPv6 entre distintas áreas.
  3) Router de nivel 1-2 (L1-L2): responsable del enrutamiento IPv6 tanto dentro del área interna como entre distintas áreas.
- Para IPv6 se añaden dos nuevos tipos de valor de longitud o TLV para añadir soporte para información relacionada con enrutamiento de esta nueva familia de direcciones que son: Accesibilidad IPv6 y Dirección de interfaz IPv6.

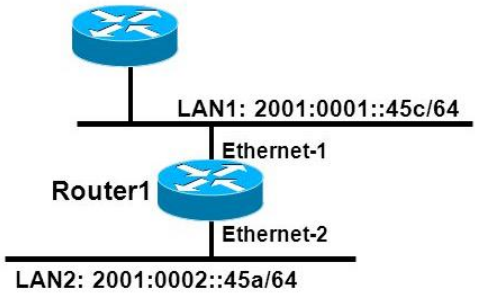
Al configurar routers con IS-IS se pueden obtener 3 arquitecturas distintas:

- IS-IS funcionando sólo con IPv4.
- IS-IS funcionando sólo con IPv6.
- IS-IS funcionando con IPv4 e IPv6.

Los routers IS-IS deben estar necesariamente contiguos a otros que operen con la misma versión IS-IS, de lo contrario se obtendrán “hoyos negros” en la topología. Los hoyos negros son routers IPv4 que se encuentran en medio de una ruta entre routers IS-IS IPv6, donde el router IS-IS IPv4 no podrá enviar ni recibir información IPv6 al no ser capaz de comprenderla. Por esto es

[14] Algoritmo Dijkstra comúnmente llamado algoritmo del primer camino más corto SPF (shortest path first), este algoritmo acumula costos a lo largo de cada ruta desde el origen hasta el destino, con el objetivo de conseguir la ruta más corta entre dos puntos.

recomendable implementar routers IS-IS con IPv4 e IPv6 en funcionamiento. A continuación se muestran ejemplos de configuración de redes con el protocolo IS-IS.



Dual IPv4/IPv6 configuration. Redistributing both IPv6 static routes and IPv4 static routes.

```
Router1#
 interface ethernet-1
     ip address 10.1.1.1 255.255.255.0
     ipv6 address 2001:0001::45c/64
     ip router isis
     ipv6 router isis

  interface ethernet-2
     ip address 10.2.1.1 255.255.255.0
     ipv6 address 2001:0002::45a/64
     ip router isis
     ipv6 router isis

  router isis
      address-family ipv6
      redistribute static
      exit-address-family
      net 42.0001.0000.0000.072c.00
      redistribute static
```

Figura 2.17: Ejemplos de topologías de redes con configuraciones IS-IS en IPv4 e IPv6.

2.5.6 OSPFv3

Este protocolo es conocido como el protocolo de la primera ruta más corta, OSPF (Open Shortest Path First) se define en el RFC 5340[15] y es un protocolo de enrutamiento que está basado en OSPFv2 para IPv4, con el cual tiene varias similitudes como por ejemplo:

- El uso de los mismos paquetes básicos como hello, descripción de paquetes, solicitud de estado de enlace, actualización de estado de enlace y aviso de estado de enlace.
- Los mecanismos para descubrimiento de vecinos y formaciones de adyacencias son idénticos.
- Los tiempos predeterminados para los paquetes LSA se mantienen sin cambios con respecto a OSPFv2.

Las principales diferencias que se muestran entre OSPFv2 y OSPFv3 son:

- OSPFv3 procesa las rutas por enlace y no por red como en OSPFv2, se pueden agregar múltiples instancias por enlace.
- Se usan direcciones de enlace local IPv6 para identificar adyacencias entre vecinos OSPFv3. Es decir que se asumen que se han asignado direcciones unicast (FE80::) a las interfaces ente vecinos.
- Se utiliza la dirección multicast FF02::5 para identificar a todos los routers dentro un enlace local.
- Se utiliza la dirección multicast FF02::6 para identificar a todos los routers designados dentro un enlace local.
- Se utilizan los encabezados de extensión IPsec como mecanismos de autenticación.
- Se envían mensajes OSPFv3 como datagramas IPv6, lo cual permite la creación de túneles 6to4.

[15] RFC 5340: OSPFv3 para IPv6. URL: http://tools.ietf.org/html/rfc5340.

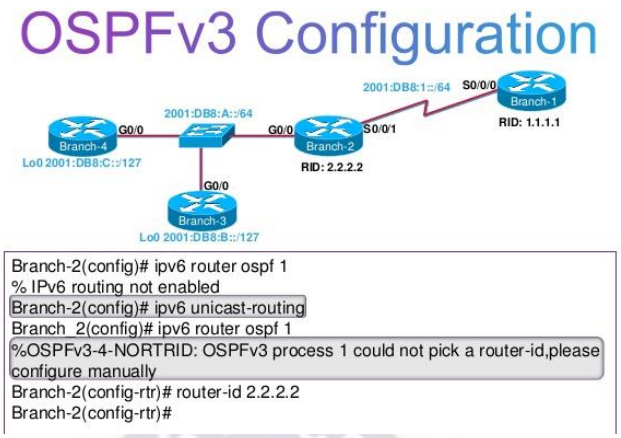


Figura 2.18: Ejemplos de topologías de redes con configuraciones OSPF en IPv4 e IPv6.

2.6 EL BACKBONE DE IPV6

Luego de haber descrito en las anteriores secciones el diseño de IPv6 así como la coexistencia con IPv4, los mecanismos de transición que pueden implementar así como los distintos protocolos de enrutamiento que operan con IPv6, en esta sección se presenta la arquitectura del backbone IPv6, además de cómo los espacios de direccionamiento IPv6 están alojados dentro de los registros regionales de Internet RIRs (Regional Internet Registers) y cómo estas direcciones son reasignadas a las ISP locales y sitios finales, finalmente se describen los criterios básicos para que la UMSA, pueda convertirse en un ISP IPv6 dentro de su área de red metropolitana(MAN).

2.6.1 6BONE

El 6bone es una red de redes IPv6 donde todos los enlaces entre las redes están constituidos usando IPv6, al referirse al 6bone debe entenderse como el núcleo de Internet IPv6; está red ha sido creada inicialmente como una red de prueba en 1996 por la IETF para crear un grupo de trabajo y validar los nuevos estándares que se han creado para las redes y servicios IPv6 entre todas las redes de transición de IPv4 a IPv6, además de recolectar reacciones frente a los nuevos procedimientos y mecanismos de transición hacia los desarrolladores y diseñadores de protocolos.

El 6bone es administrado y mantenido gracias a los esfuerzos colaborativos entre todos los participantes de este grupo de trabajo a nivel mundial. Hacia 2002 se obtuvieron más de 1100 nodos de conexión localizados en 57 países. En la actualidad gracias al lanzamiento mundial de IPv6 ocurrido en 2013 esta cifra es ser mucho más alta[16]. En la actualidad esta red está basada en enlaces IPv6 nativos en el núcleo de Internet, en stack doble y túneles en los nodos más exteriores que gradualmente deberán ser remplazados por enlaces nativos IPv6.

Cuando los administradores de redes de organizaciones como las ISP y otras compañías aceptan intercambiar su tráfico IPv6, esta operación es denominada “peering”, de la misma forma, los administradores deciden como se debe anunciarse sus redes.

[16] El departamento de cómputo de la Universidad de Lancaster en el Reino Unido provee de diferentes estadísticas acerca de localidades conectadas al 6bone, esta información es accesible en http://www.csipv6.lancs.ac.uk/ipv6/6Bone/Whois/bycountry.html.

En la siguiente Figura se muestra la topología del 6bone.

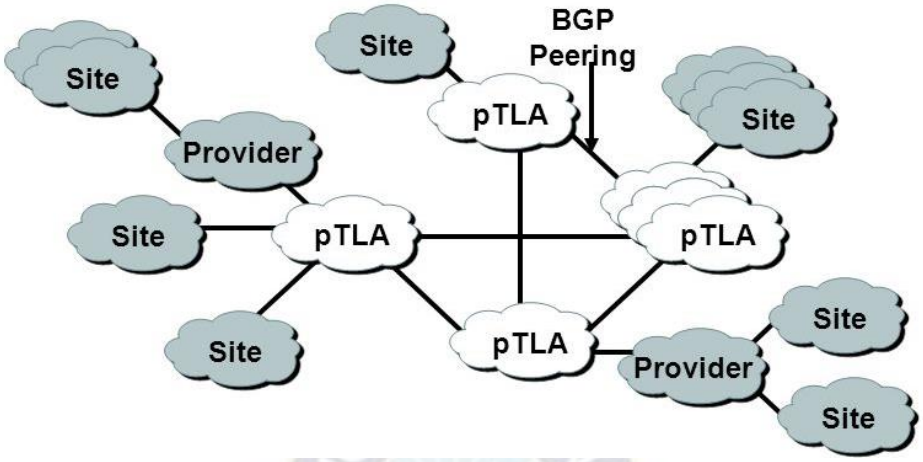


Figura 2.19: Relación de pTLAs con proveedores de nivel 1 (Tier 1 ISP) y sitios.

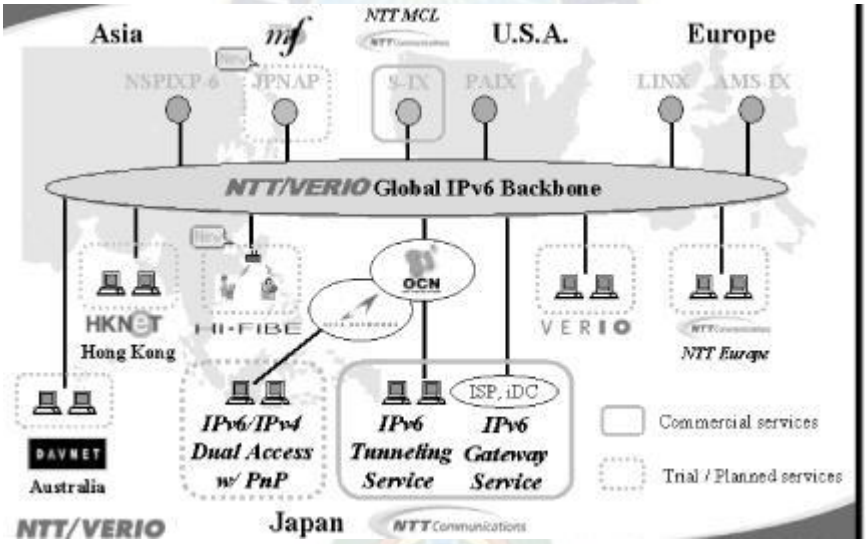


Figura 2.20: Topología jerárquica del 6bone mostrando el núcleo de internet (pTLA), proveedores de nivel 1 (Tier1 ISP) y sitios.

En la zona libre por defecto está conformada el núcleo de Internet, en esta zona se intercambian tablas de enrutamiento de redes extensas entre los principales proveedores de internet o ISP, aquí no existen rutas IPv6 por defecto y solo están presentes las rutas agregadas.

Luego se encuentran los nodos de primer nivel (pTLAs, Primary Top Level Aggregation) o comúnmente llamados agregadores pues estos deben agregar todo el tráfico IPv6 hacia sus clientes y nodos inferiores que son los ISP de segundo nivel y además deben publicar solo algunos prefijos IPv6 en la zona libre. Como se analizó anteriormente, la agregación de rutas en IPv6 permite un enrutamiento eficiente y escalable hacia Internet. Entre distintos pTLAs se utiliza el protocolo BGP4+ para intercambiar información de enrutamiento. En la siguiente Figura se muestran las conexiones entre distintos pTLAs hasta 2002, La Figura 2.20: muestra las conexiones entre pTLAs en la 6bone.

2.6.2 ARQUITECTURA DEL 6BONE

La topología del 6bone es una vista conceptual del backbone, pero en realidad la arquitectura se ha realizado usando una diversidad de enlaces, es más las conexiones entre distintos pTLAs se realizan mediante una mezcla de enlaces nativos y túneles sobre la infraestructura IPv4. Para ejemplificar mejor esta idea, en la siguiente Figura se muestran ejemplos de los distintos tipos de enlaces usados entre las pTLAs.

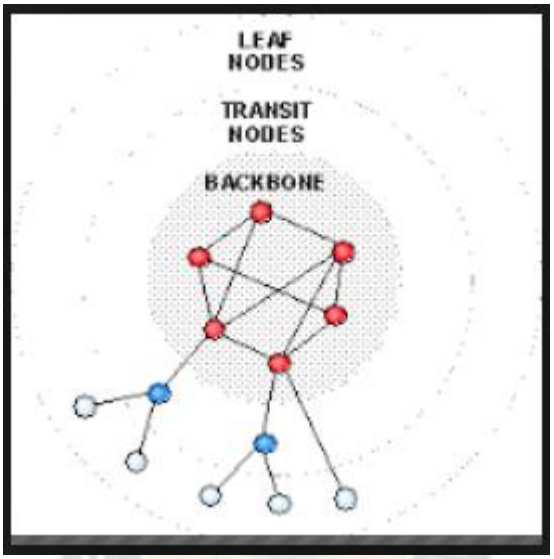


Figura 2.21: Ejemplo de interconexión entre 7 distintos pTLAs (A, B, C, D, E, F y G).

Una pTLA en la 6bone puede proveer de direccionamiento y conectividad a cualquier proveedor, proveedor intermediario o sitio que se encuentre directamente conectado, luego los proveedores puede asignar prefijos de las direcciones de los sitios directamente conectados mientras que los proveedores intermedios pueden asignar prefijos a otros sitios a un nivel inferior como se muestra en la siguiente Figura.

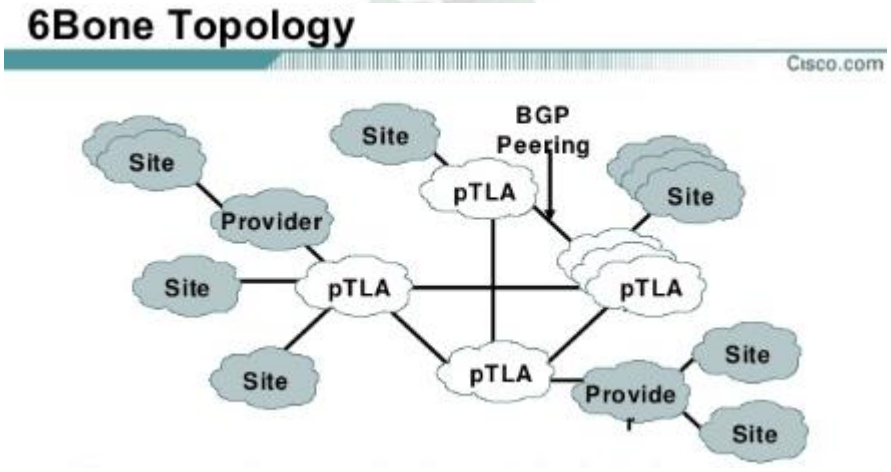


Figura 2.22: Asignación de prefijos y agregación entre un pTLA y sus proveedores inferiores.

Como se ha mencionado, el despliegue de IPv6 ha comenzado en 1999 y desde entonces las RIRs han asignado espacio de dirección IPv6 a los grandes proveedores. El núcleo actual de IPv6 ya está en pleno funcionamiento y es pequeño en comparación con el actual núcleo de la Internet IPv4, pero está creciendo considerablemente.

Los ISPs intercambian tráfico por medio de las NAP (Network Access Point) como ocurre en IPv4, y así proveen de conectividad a sus clientes.

2.6.3 IPV6 EN EL INTERCAMBIO DE TRÁFICO ENTRE PUNTOS DE ACCESO (NAPS)

Los puntos de acceso de la red o NAPs son lugares neutrales donde los proveedores pueden intercambiar tráfico y rutas. Los NAPs generalmente tienen infraestructura de alta velocidad para interconectar los enlaces de los proveedores y routers.

Todo ISP necesita estar conectado a una NAP para intercambiar tráfico con otros pares. Entre los ISP y las NAP se intercambian rutas, pero ninguna ruta por defecto es publicada entre ambos. Muchos puntos de acceso avanzados ofrecen servicios para optimizar la conexión y reforzar las políticas de enrutamiento.

Debido a que las NAPs generalmente están basadas en la capa 2 (Capa de Acceso) es posible para estas, establecer enlaces IPv6 nativos con otras infraestructuras con un esfuerzo mínimo y sin necesidad de modificar los acuerdos entre los pares y las NAPs pues el uso de IPv6 no introduce nuevos problemas.

Las NAPs que soportan IPv6 están emergiendo alrededor del mundo, en enero de 2003 existían 13 NAPs con conectividad IPv6 operacionales y que ofrecían servicios a ISP de nivel 1[20].

2.6.4 ESCENARIOS PARA ESTABLECER CONECTIVIDAD IPV6

A continuación se describen los escenarios para establecer conectividad entre los ISP IPv6 y las NAPs.

- Utilizando la dirección de enlace local para BGP4+: Los ISP dentro de una NAP no deberían usar los prefijos de otros ISP para configurar sus interfaces de rutas. Al configurar las direcciones en enlace local dentro de BGP4+ el ISP no necesita un prefijo IPv6 específico. En este escenario la conexión entre los dos ISP aparece como neutral. Debe tomarse en cuenta también que el uso de direcciones de enlace local requieren de una configuración específica en BGP4+.
- Utilizando el prefijo unicast global agregable registrado por la NAP: Las RIRs asignan prefijos /48 y /64 a las NAPs para restablecer conexiones entre ISPs vecinos. Este escenario puede también aparecer como neutral.
- Compartir prefijos entre ISPs: otro escenario consiste en compartir prefijos entre las ISPs vecinas a través de las NAP conectadas, esto es útil especialmente si la NAP no provee prefijos IPv6 globales unicast agregables a las USP.

2.7 CONCLUSIONES DE REVISIÓN TEÓRICA

La necesidad de implementar una estrategia de transición del protocolo IPv4 a IPv6 en la Universidad Mayor de San Andrés pasa por considerar los siguientes aspectos.

2.7.1 BENEFICIOS DEL USO DEL PROTOCOLO IPV6

El análisis de los aspectos teóricos brinda los siguientes beneficios en cuanto a la implementación de una estrategia de transición del protocolo IPv4 al IPv6:

- La posibilidad de disponer de las direcciones IP suficientes para todo dispositivo dentro la institución sin necesidad de uso de técnicas como el NAT que genera retardo en el tráfico, mayor procesamiento en los equipos de red y problemas en protocolos en tiempo real.

- Mayor agilidad en los procesamientos de enrutamiento debido a que se requiere leer una parte de la dirección para tomar la decisión de enrutar el tráfico.

- El uso de direcciones IPv6 permite la asignación de direcciones públicas y de esta manera posibilitar el intercambio de información a través de conexión de Internet con otros dispositivos o servicios.

- La capacidad de asignación de direcciones IPv6 a dispositivos móviles como teléfonos inteligentes, tablets, laptops, televisiones inteligentes y otros, brinda la oportunidad de desarrollar nuevos servicios de beneficio de la comunidad universitaria.

- Las direcciones IPv6 Unicast se podrá utilizar en hosts de usuarios finales, mediante el proceso de autoconfiguración y en servidores mediante la configuración estática; mientras que las direcciones IPv6 Anycast se podrá aplicar a servidores con los correspondientes beneficios como disponibilidad, balanceo y seguridad.

2.7.2 ELECCIÓN DEL MECANISMO DE TRANSICIÓN A IPV6

Luego de realizarse la revisión de los diferentes mecanismos de transición, y considerando:

- Que, tanto los equipos de los usuarios finales como servidores requieren convivir con las direcciones IPv4 e IPv6 de manera simultánea.
- Se debe garantizar la no afectación de los servicios antiguos, es decir, si se requiere traficar mediante IPv4 no se tiene ningún problema con esta necesidad.
- En el caso de requerirse traficar mediante IPv6, también, se garantiza éste, y de esta manera se explota los beneficios de proveedor del servicio de mejor modo.
- Los protocolos IPv4 e IPv6 al trabajar simultáneamente se prioriza el tráfico IPv6.

En base a las anteriores afirmaciones se puede inferir que el mecanismo de transición recomendado es el Stack Doble o también llamado Pila Doble.

2.7.3 ELECCIÓN DEL PROTOCOLO DE ENRUTAMIENTO PARA IPV6

El protocolo de enrutamiento dinámico dentro la red de la UMSA, debe ser elegido acorde a diferentes aspectos detallados a continuación:

- Debido a que se debe considerar que se utilizará los protocolos IPv4 e IPv6 simultáneamente, se debe elegir un protocolo que ente basado en uno de ellos y que use los mismos paquetes básicos de sincronización.
- En ambos protocolos, IPv4 e IPv6, los mecanismos de descubrimiento de vecinos y formaciones de adyacencia son idénticos.
- El procesamiento de rutas se debe realizar preferentemente por enlace y no así por red, por lo que se puede agregar múltiples instancias por enlace.

- Preferentemente, se debe utilizar direcciones multicast FF02::5 para identificar a todos los routers y FF02::6 para identificar a todos los routers designados dentro un enlace local.

Las anteriores aseveraciones hacen que se recomiende como un protocolo elegible para el enrutamiento dinámico al OSPFv3.

2.7.4 CONSIDERACIONES PARA EL 6BONE

Los proveedores del servicio de Internet locales deben ofrecer el servicio de “peering” con enlaces IPv6 nativo, y pueda publicar los prefijos IPv6 de la UMSA hacia la zona libre, por lo que también el ISP debe considerar la provisión de las direcciones IPv6 para los enlaces del protocolo BGP+; y la consideración del soporte para IPv4.

CAPITULO III

RELEVAMIENTO DE INFORMACION

3.1 INTRODUCCIÓN

La Universidad Mayor de San Andrés por su importancia dentro el área de los estudios superiores en Bolivia y la región, es poseedora de una infraestructura tecnológica considerable que durante el presente capitulo se detalla en cuanto al ámbito de redes y servidores.

3.2 HISTORIA DE LA INSTITUCIÓN

"La Universidad Mayor de San Andrés, (también conocida usualmente por la sigla UMSA) es la principal universidad pública del Estado Plurinacional de Bolivia, establecida desde 1830 en el departamento de La Paz (sede de gobierno) y desplegada a lo largo del mismo, en la ciudad capital y sus provincias en 4 Centros Regionales Universitarios (CRUs) y diversas Sedes Universitarias Locales (SULs). La UMSA es la segunda universidad más antigua de Bolivia, después de la Universidad San Francisco Xavier de Chuquisaca (1624) y la más representativa del Sistema de la Universidad Boliviana.

Es uno de los centros académicos superiores más prestigiosos del país, cuna de diferentes ideologías y partícipe de muchos movimientos sociales durante los diferentes periodos de gobierno en la historia de Bolivia, a la vez enseña y factum de la educación nacional. En el ámbito del alumnado, hasta el año 2016, la Universidad Mayor de San Andrés tenía en sus aulas alrededor de 74.391 estudiantes, de los cuales 4013 obtuvieron el título de licenciado o su equivalente (pregrado).

Cabe mencionar también que varios presidentes de Bolivia realizaron sus estudios superiores en esta universidad, egresando de sus aulas, así como también diferentes abogados, ingenieros, políticos, médicos y demás profesionales que llegaron a convertirse en personalidades destacadas dentro de la pluricomunidad boliviana durante el transcurso de los Siglos XIX, XX y XXI."[17]

3.2.1 HISTORIA DEL DEPARTAMENTO DTIC

El Departamento de Tecnologías de Información y Comunicación (DTIC) tuvo su origen en el programa UMSATIC, mismo que fue creado en el año 2001 en calidad de fase preparatoria y en el año 2003 inicia sus operaciones con la finalidad de montar la estructura tecnológica en el área de las Tecnologías de Información y Comunicación (TIC's), que la misma sea sostenible y sobre todo de apoyo a los pilares de la UMSA, que son la investigación, formación de profesionales y la interacción social.

[17] Fuente Universidad Mayor de San Andrés a traves de su sitio web https://www.umsa.bo

“Para dar continuidad e institucionalizar las tareas del programa UMSATIC se crea el Departamento de Tecnologías de Información y Comunicación (DTIC) mediante Resol. de H.C.U. Nº 096/07 en fecha 2 de abril de 2007 bajo la dependencia del Vicerrectorado, como unidad formalmente establecida tiene el objetivo de planificar, organizar, dirigir, coordinar y controlar la realización técnica y especializada en el procesamiento de datos, sistema de Tecnología de la Información y Comunicación, en los aspectos científico, académico, investigación, administrativo y financiero de la universidad, así como proveer a la UMSA, de los medios o recursos tecnológicos necesarios para apoyar, enriquecer y optimizar proceso de la Universidad.”[18]

3.3 ORGANZACION DEL DTIC

El DTIC está compuesto por dos divisiones, de acuerdo a la Resol. de H.C.U. Nº 096/07, bajo la siguiente estructura:

Figura 3.1: Organigrama del Departamento de Tecnologías de Información y Comunicación.

3.4 INFRAESTRUCTURA DE RED

La UMSA cuenta con una infraestructura de red basada en la marca Cisco, bajo el diseño de tres capas (Núcleo, Distribución Acceso), en la capa de distribución se cuenta con dos anillos de fibra óptica que brinda conectividad redundante a 22 predios dentro la mancha urbana, como se muestra en la siguiente figura.

[18] Fuente Departamento de Tecnologías de Información y Comunicación a traves de su sitio web https://dtic.umsa.bo

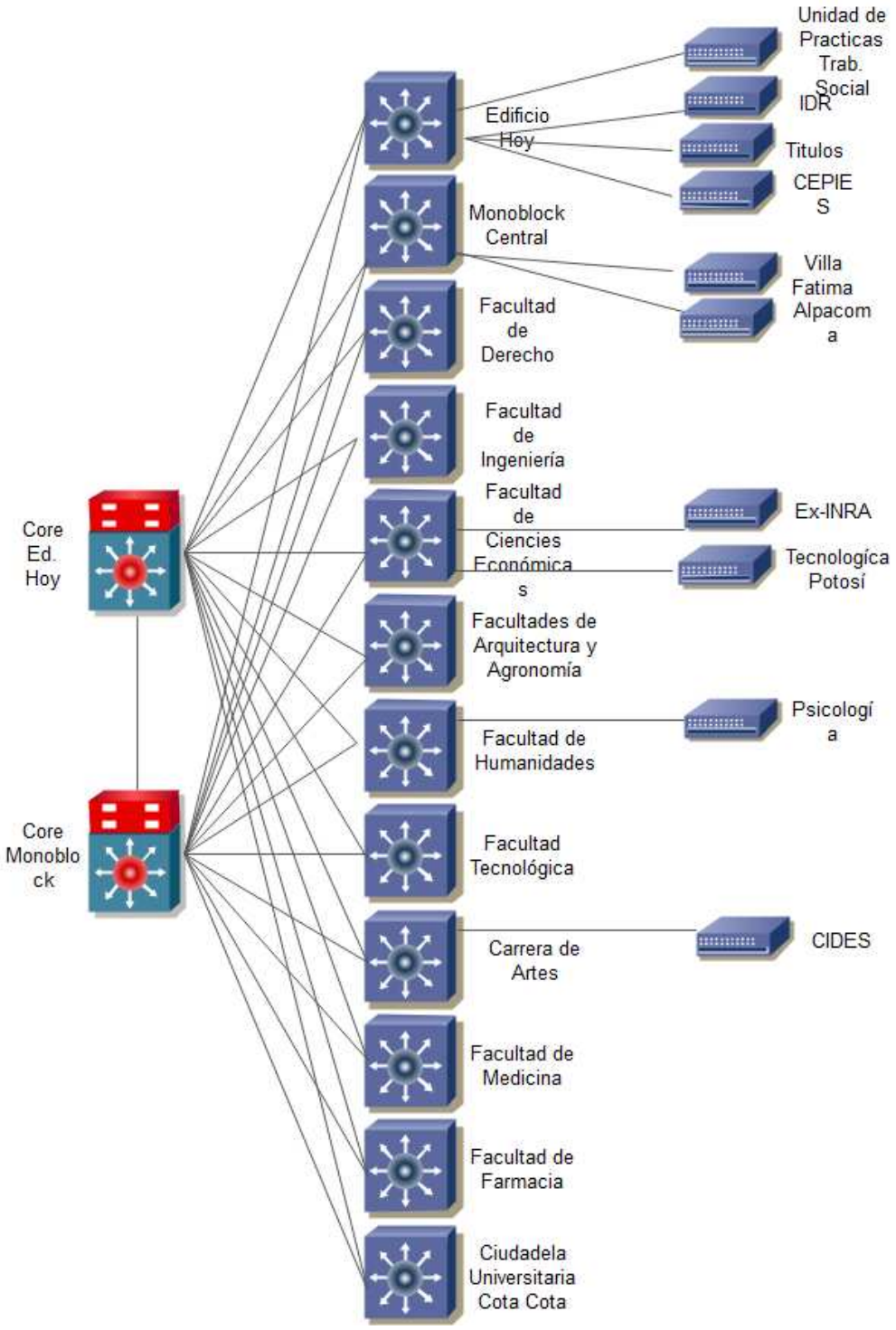


Figura 3.2: Esquema lógico de la red de la UMSA.

La red de la UMSA comprende, entre switchs de núcleo, distribución y acceso, más de 200 dispositivos.

3.4.1 NUMERACIÓN IPV4

La institución cuenta con un Número de Sistema Autónomo (ASN 27828) que incluye, en IPv4, el segmento de red 200.7.160.0/20. Se ha distribuido estos segmentos de la siguiente manera:

Red	Ubicación	Subredes identificables	Uso porcentual
200.7.160.0/24	Data Center	200.7.160.0/28 200.7.160.16/28 200.7.160.28/32 200.7.160.30/32 200.7.160.32/27 200.7.160.64/27 200.7.160.96/28 200.7.160.112/28 200.7.160.128/27 200.7.160.160/27 200.7.160.192/27 200.7.160.224/29 200.7.160.236/30	62%
200.7.161.0/24	Data Center	200.7.161.0/24	30%
200.7.162.0/24	Ed.Hoy Área Central	200.7.162.0/24 200.7.162.0/26 200.7.162.128/26 200.7.162.192/27 200.7.162.240/28	27%
200.7.163.0/24	Campus Cota Cota	200.7.163.0/24 200.7.163.0/26 200.7.163.64/26 200.7.163.128/26 200.7.163.192/26	30%
200.7.164.0/24	Ed.Hoy Adm. Central	200.7.164.0/24	64%
200.7.165.0/24	Monoblock	200.7.165.0/24	36%
200.7.166.0/24	Ed.Hoy Area Central	200.7.166.0/24	63%
200.7.167.0/24	Monoblock Autoridades	200.7.167.0/26 200.7.167.64/26	42%
200.7.168.0/24	FDCP	200.7.168.8/29 200.7.168.64/27 200.7.168.96/28 200.7.168.112/29 200.7.168.160/28 200.7.168.192/26 200.7.168.240/28	24%
200.7.169.0/24	FHCE	200.7.169.0/25	51%

		200.7.169.128/27 200.7.169.160/27 200.7.169.192/27 200.7.169.224/27	
200.7.170.0/24	DTIC ISP Servidores	200.7.170.0/29 200.7.170.8/29 200.7.170.16/29 200.7.170.24/29 200.7.170.32/28 200.7.170.48/29 200.7.170.56/29 200.7.170.64/29 200.7.170.72/29 200.7.170.80/28 200.7.170.112/28 200.7.170.200/29 200.7.170.208/28 200.7.170.224/29 200.7.170.232/29 200.7.170.240/29 200.7.170.248/29	28%
200.7.171.0/24	Monoblock	200.7.171.0/24	27%
200.7.172.0/24	Monoblock, Area descocentrada, Predios con SIU	200.7.172.32/28 200.7.172.48/29 200.7.172.64/26 200.7.172.128/26 200.7.172.192/29 200.7.172.200/29 200.7.172.208/29 200.7.172.216/29	25%
200.7.173.0/24	FAADU, FA	200.7.173.0/26 200.7.173.64/28 200.7.173.96/28 200.7.173.128/26	17%
200.7.174.0/24	FO, FCBF	200.7.174.0/25 200.7.174.128/26 200.7.174.224/27	53%
200.7.175.0/24	Arquitectura	200.7.175.0/26 200.7.175.64/27 200.7.175.96/27 200.7.175.128/25	54%

Tabla 3.1: Uso de direcciones IPv4 en la UMSA.

Siendo que el agotamiento es evidente en algunos segmentos se implantaron soluciones distintas para ser implementadas en corto plazo, entre ellas están: el espacio de direccionamiento privado[19] y la traducción de direcciones de red NAT (Network Address Translation) esto con el objetivo de preservar la cantidad de direcciones IP pública disponibles, pero estos esfuerzos no han sido suficientes.

3.5 SERVIDORES Y SERVICIOS

La División de Redes y Sistemas de Información dependiente del Departamento de Tecnologías de Información y Comunicación administra entre servidores dedicados, virtuales y en calidad de hosting se gestiona una cantidad superior a los doscientos servidores, mismos que albergan servicios y sistemas que se clasifican en:

Servicios básicos de red:
- DNS
- DHCP
- Monitoreo
- Seguridad
- Administradores de ancho de banda

Sistemas Académicos:
- Matriculación
- Sistemas Académicos
- Sistema de gestiones, admisiones y registro (GAR)
- Kardex estudiantil
- Otros

Sistemas de apoyo académico:
- Bibliotecas digitales
- Consultas y préstamos de libros

Sistemas Administrativos Financieros
- Contabilidad
- Presupuestos
- Tesorería y cajas
- RRHH
- Asistencia de personal Administrativo
- Planillas administrativas
- Planillas docentes
- Otros

Sistemas de apoyo a la gestión
- Ayni Sistema de Correspondencia
- Sistema de Títulos y Diplomas
- Sistema de archivo y documentación

Servicios TIC's
- Portal institucional
- Sistema de la cuenta institucional
- Correo electrónico

[19] RFC 1918 - Address Allocation for Private Internets - IETF Tools
URL:https://tools.ietf.org/html/rfc1918

- Plataformas de educación virtual

Plataformas de E-learning
- Moodle

Sistemas y servicios que se pueden clasificar, por el tipo de acceso en, de Internet, Intranet y Intranet-Internet; y otras características que se consideraran para la migración a IPv6.

3.6 USUARIOS

Los usuarios de los servicios brindados por el DTIC se pueden clasificar en los institucionales, mismos que se pueden cuantificar en estudiantes que superan los ochenta mil, docentes superior a los tres mil y administrativos que superan los dos mil; y los no institucionales que acceden a los portales mediante la Internet para interactuar con los diferentes servicios.

3.7 CONCLUSIONES DEL RELEVAMIENO DE INFORMACIÓN

3.7.1 CONCLUSIONES DE LA INFRAESTRUCTURA DE RED

El programa UMSATIC entre las gestiones 2002 y 2008, con financiamiento de la Cooperación Sueca, logro implementar una infraestructura de red basada en equipamiento de la marca Cisco y por consiguiente las recomendaciones en cuanto al esquema de red de tres capas (núcleo, distribución y acceso), considerando que algunos de los mismos aún se encuentran en explotación, equipos que se evaluarán en el siguiente capítulo con la finalidad de analizar la posibilidad del soporte para el protocolo IPv6.

3.7.2 CONCLUSIONES DE LA NUMERACIÓN IPV4 DE LA UMSA

LACNIC asignó a la UMSA el prefijo 200.7.160.0/20, junto al ASN 27828, que significa algo más de 4000 direcciones públicas de las que se tiene un 40% de uso aun cuando se asignó el 100% a diferentes funcionalidades y unidades académicas; pero la necesidad de la transición al protocolo IPv6 entre varios motivos se requiere que los usuarios finales puedan acceder a contenidos que en la actualidad se disponen en el nuevo protocolo a través de Internet y sobre todo que los contenidos que la UMSA genera se disponga en Internet en los protocolos en uso como IPv4 e IPv6.

3.7.3 CONCLUSIONES SOBRE SERVIDORES Y SERVICIOS

Los servidores entre virtuales y físicos, que superan los 200 tienen sistemas operativos sobre todo basados en Linux, entre los que se dispone de versiones compatibles con IPv6 y otros con características de obsolescencia que seguramente se recomendará la actualización de los mismos, y también se propondrá el procedimiento de configuración de la interfaz de red para los 3 sistemas operativos más utilizados en el área de servidores de la UMSA.

3.7.4 CONCLUSIONES SOBRE USUARIOS DE LA UMSA

La comunidad universitaria comprendida en más de 80.000 estudiantes, 3.000 docentes y 2.000 administrativos que acceden a los servicios de la UMSA con dispositivos que van desde equipos de computación de tipo escritorio, portátiles, tablets, teléfonos y televisiones inteligentes, etc. cuya configuración no debería ser complicada para el usuario final, por lo que un requerimiento técnico básico debería ser la configuración de los dispositivos de manera totalmente automática.

CAPITULO IV

ANALISIS DE LA IMPLEMENTACIÓN

4.1 INTRODUCCIÓN

La institución que es sujeto de estudio, en especial su área tecnológica, para el planteamiento de la implementación del protocolo IPv6 requiere un análisis y diagnóstico de sus recursos, para luego diseñar una solución acorde a sus necesidades.

4.2 REQUERIMIENTOS DE LA UMSA

Una institución de la importancia y prestigio, como la que goza la Universidad Mayo de San Andrés, tiene la necesidad de estar presente en el mundo virtual, Internet, y ser accesible mediante cualquier tecnología, vale decir, debe ser accesible a sus portales públicos mediante los protocolos IPv4 e IPv6.

Los usuarios finales que hacen uso de los servicios de red dentro la institución también requieren acceder a contenidos en Internet mediante los protocolos IPv4 e IPv6, siendo innegable la coexistencia de los mismos, por lo menos en los tiempos actuales.

Siendo la necesidad primordial de la institución, de la región y del mundo, dado el agotamiento de las direcciones IPv4, y el crecimiento exponencial de hosts que requieren el uso de direcciones públicas para el acceso directo desde y hacia la nube de Internet, la transición al protocolo IPv6.

4.3 CONECTAR LAS REDES DE LA UMSA A PROVEEDORES QUE SOPORTEN IPV6

Asumiendo que un usuario necesita de conectividad y direcciones IPv6, el primer paso para cualquier institución para obtener conectividad y direcciones es encontrar un proveedor IPv6 comercial. En el presente caso, se recomienda incluir en los Términos de Referencia de la contratación de servicios de Internet este punto especial.

Sin embargo, el objetivo de este proyecto principalmente es elaborar el plan de transición a IPv6 en la UMSA, para que en tanto y cuanto en que la Universidad cuente con una red convergente IPv6, se dispongan servicios IPv6 a los usuarios que lo requieran.

El plan de direccionamiento IPv6 para las redes de usuarios debe considerar las siguientes dos reglas:

- Determinar el número actual y futuro de las subredes a conectar.
- Asignar un prefijo /64 a cada subred de usuarios, tomando presente que no se debe variar el tamaño de la máscara de red como en el diseño de redes IPv4.

En la siguiente topología se muestra una ejemplo de una red de cliente donde el proveedor asigna el prefijo 2001:420:0100::/48 y el cliente asigna prefijos /64 a sus respectivas subredes.

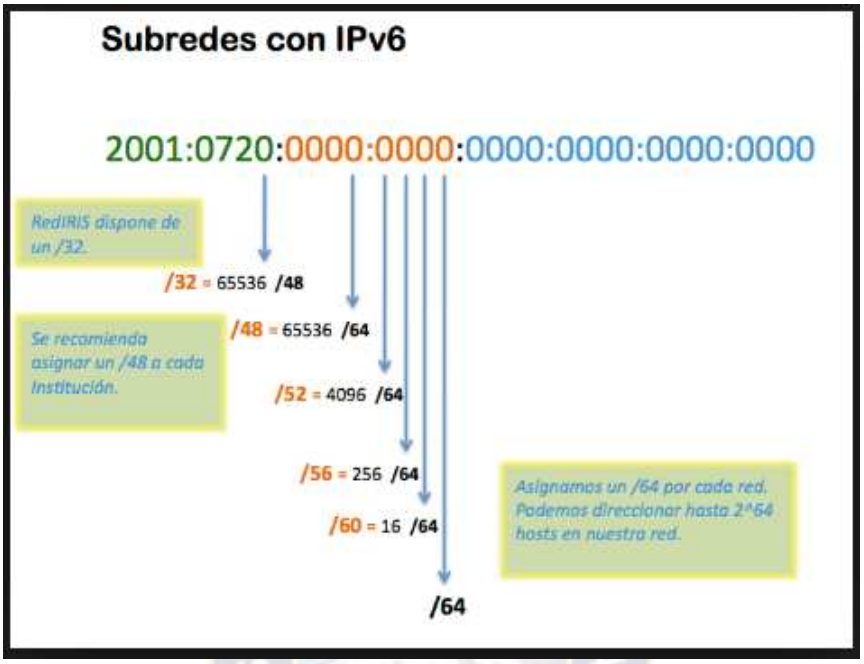


Figura 4.1: Asignación de prefijos /64 dentro de la red de usuario.

No hay guías claras para la reasignación de prefijos IPv6 dentro de la red de usuario, pero la IETF proporciona un documento que propone un método eficiente para ayudar a los usuarios finales y a los administradores de redes de usuarios a realizar sus planes de direccionamiento IPv6[20].

4.3.1 ENRUTAMIENTO Y AGREGACIÓN DE PREFIJOS IPV6 EN EL LADO DEL PROVEEDOR

La siguiente Figura muestra la misma topología de red ejemplificada en la Figura anterior pero ahora mostrando también la agregación de las rutas que realizan los proveedores de servicio de Internet.

[20] Este documento puede ser encontrado en http://www.ietf.org/internet-drafts/draft-ietf-ipv6-ipaddressassign-06.txt

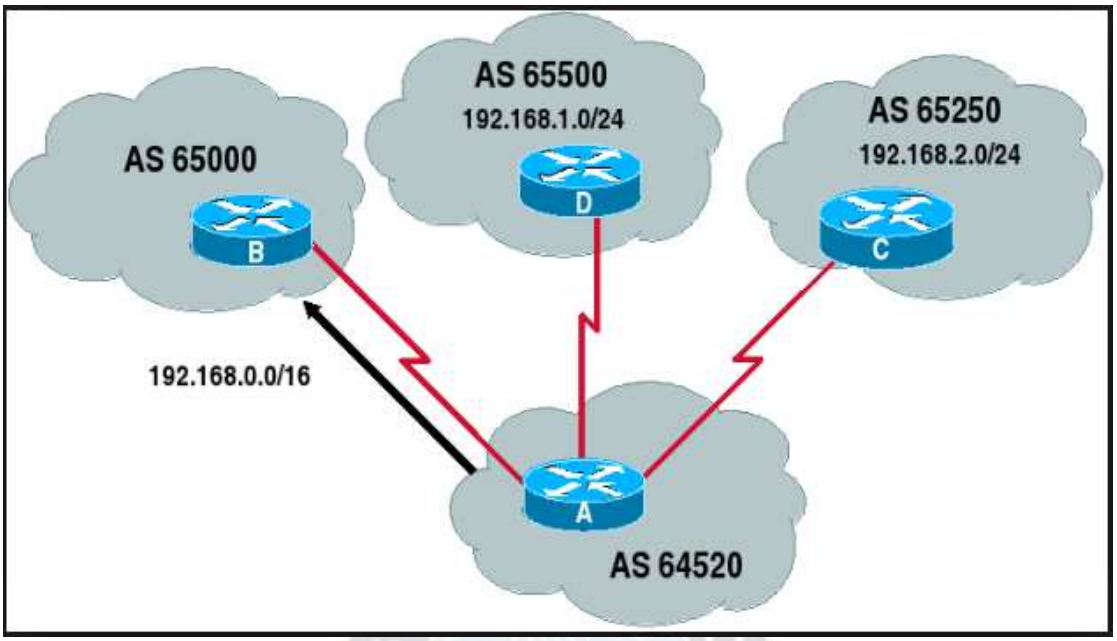


Figura 4.2: Agregación de la ruta realizada por los ISPs.

Ambos proveedores agregan rutas para sus clientes y publican cada uno una sola ruta a la IPv6 de Internet, es por eso que la tabla de enrutamiento global solo tiene las rutas agregadas de estos proveedores.

4.4 CONEXIÓN DE HOST USANDO MECANISMOS DE MIGRACIÓN Y COEXISTENCIA CON IPV4

Los hosts que están conectados a los enlaces actuales de internet IPv4 pueden migrar a IPv6 utilizando métodos de coexistencia y transición. Existen mecanismos como el túnel 6to4 que se explicó anteriormente que ayudan un solo host a conectarse a la red IPv6 mediante la infraestructura de red IPv4.

En el presente documento se incluye un anexo denominado “Conexión de usuarios finales a IPv6” donde se explican algunos métodos de configuración de clientes para la implementación de IPv6 en distintas plataformas.

4.5 SITUACIÓN DE LA TRANSICIÓN A IPV6 EN EL MUNDO

La transición de redes IPv6 en la actualidad no alcanza un punto significativo en la gran mayoría de los países del mundo, desde luego esto es causa de que este es un nuevo protocolo que recién empezó a desplegarse de forma oficial hace apenas hace algunos años, por lo cual aunque los grandes proveedores de servicios de Internet ya han migrado completamente a IPv6, aún no lo hacen el resto de proveedores de servicios e ISP que actualmente se encuentran en proceso de estudio y reestructuración de su infraestructura para soportar este nuevo modelo.

En la siguiente Figura se muestra un mapa estadístico acerca de la adopción IPv6 a nivel mundial[21].

[21] Estadísticas IPv6 de Google, URL: www.google.com/intl/ipv6. Consultado el 23 de mayo de 2014.

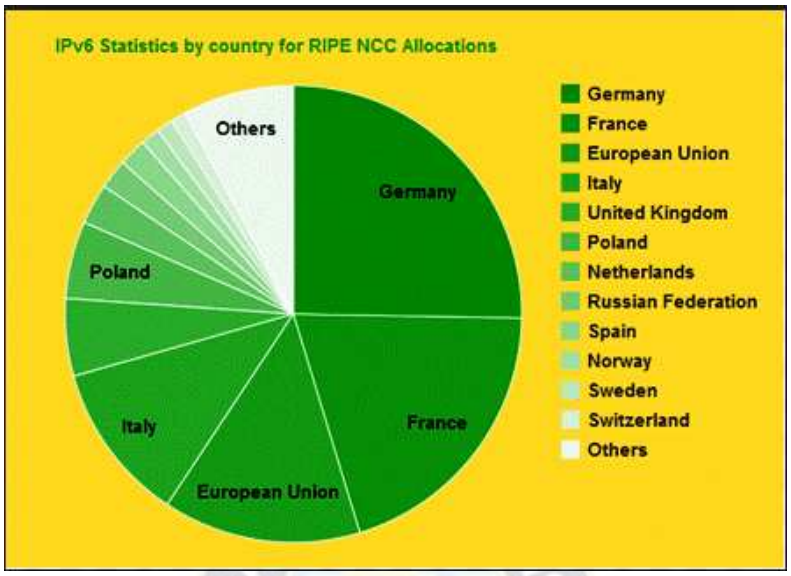


Figura 4.3: Mapa estadístico de la adopción de IPv6 a nivel mundial.

- Las regiones en verde intenso muestran los sitios donde IPv6 ha sido ampliamente desplegado (mientras más intenso sea el color, significa un mayor despliegue) y los usuarios no experimentan problemas para conectarse a sitios IPv6 de forma frecuente.
- Las regiones en verde muestran los sitios donde IPv6 ha sido ampliamente desplegado pero los usuarios experimentan dificultades y latencia al conectarse a sitios IPv6.
- Las regiones en verde claro muestran los sitios donde IPv6 no ha sido ampliamente desplegado y los usuarios experimentan dificultades y latencia al conectarse a sitios IPv6.
- Las regiones en blanco muestran los sitios donde IPv6 no ha sido desplegado.

Como se puede observar en la figura anterior y según los datos proporcionados por Google, Bolivia se encuentra aún sin despliegue de IPv6 por parte de los ISP, junto con la gran mayoría de países de Latinoamérica exceptuando a Perú que actualmente se encuentra con un importante despliegue de IPv6 en sus ISP locales que alcanza al 6% del total de conexiones.

En la siguiente Figura se muestran porcentajes de adopción a nivel mundial del protocolo IPv6 por parte de los usuarios finales[22].

Este gráfico muestra un crecimiento casi exponencial que está teniendo la adopción de este protocolo por parte de usuarios finales durante los últimos años, cabe señalar además que las conexiones nativas son las que más relevancia tienen con un 3.20% mientras que las conexiones por túneles 6to4 y túneles Teredo que son las de segunda mayor importancia alcanzan el 0.01%, es decir que son prácticamente nulas.

4.6 CONSIDERACIONES PARA EL PLAN DE IMPLANTACIÓN DEL PROYECTO

El presente proyecto está enfocado en evaluar la infraestructura de la red de la UMSA y generar un plan de transición acorde y expresa la viabilidad desde los aspectos técnico, económico y operativo, además debe satisfacer las necesidades y requerimientos de la Universidad y sus

[22] Estadísticas IPv6 de Google, URL: www.google.com/intl/ipv6. Consultado el 23 de mayo de 2014

usuarios, debiendo además lograr el equilibrio entre la seguridad y facilidad de uso dentro de la red y la transparencia en la transición que abarca desde los equipos de escritorio de los usuarios hasta los servidores de datos corporativos de la Universidad.

Para cumplir con los objetivos se deben realizar los siguientes pasos:

- Paso 1: Diagnóstico de la red de la UMSA
- Paso 2: Evaluación de las alternativas de migración o metodologías existentes
- Paso 3: Levantamiento de requerimientos dentro de la infraestructura actual
- Paso 4: Diseño del esquema IPv6 con los prefijos delegados por LACNIC
- Paso 5: Diseño del plan de transición al protocolo IPv6

El proyecto también contempla un estudio de factibilidad, dicho punto se analiza posteriormente.

4.7 DIAGNOSTICO DE LA RED DE LA UMSA

Es necesario diagnosticar el estado de la infraestructura de red actual antes de tomar cualquier decisión sobre la modificación del diseño de la topología de red o sobre la sustitución de equipos, esto con el fin de evitar problemas que afecten a los usuarios e impedir daños económicos a la Universidad.

Toda modificación del diseño con el fin de posibilitar la transición hacia IPv6 en el presente proyecto viene dado por los resultados del diagnóstico de la operatividad y la infraestructura de red actual de la UMSA

A partir de este diagnóstico efectuado se determinan los cambios que deben producirse antes de implementar IPv6.

4.7.1 DIAGNOSTICO ACERCA DE LA TOPOLOGÍA E INFRAESTRUCTURA DE LA RED ACTUAL

- La UMSA se conecta con todos sus predios mediante un backbone de fibra óptica, con su proveedor ISP de Internet a través de unas interfaces Ethernet cableadas por fibra óptica y cobre.
- Entre los sitios de distribución principal y los usuarios se utilizan topologías en estrella y estrella extendida.
- Entre los enlaces troncales de predio se utilizan topologías en anillo y estrella extendida hacia dos switches principales.
- Los equipos utilizan negociación full dúplex como modo de transmisión.
- La UMSA se interconecta en toda la red a través de enlaces cableados UTP o fibra óptica según sea la porción de la red.
- Se usa el medio de acceso CSMA/CD (Carrier Sense Multiple Access/Collision Detect).
- No están implementados los servicios NAT (Network Address Translation) dentro de la red de Internet, solamente en el borde de la red con el ISP.
- Hay servicios de DNS (Domain Name Server) no autoritativos y autoritativos dentro de la red de Internet de la Universidad, estos están ubicados dentro de la red de servidores de la UMSA.
- Dentro de la red se utiliza el protocolo de enrutamiento OSPF por defecto, existen redes virtuales VLAN (Virtual Local Área Network) para los distintos servicios de Internet e Intranet de la universidad y existe interconexión entre estas redes.
- Los equipos de núcleo de red y de borde son equipos modulares, lo cual permite una gran capacidad de adaptación a cambios que requieran como ampliación o actualización de conexiones. Estos también cuentan con elementos redundantes como fuentes de

alimentación con capacidad de distribución de carga y también soportan la característica de remplazo “en caliente” sin interrumpir el funcionamiento (Switch Multicapa Cisco Nexus 7000 line cards, routers Cisco de la linea ASR e ISR).

- El control de ancho de banda asignado por IP es centralizado y se usan dos equipos Traffic Shaper para este control basado en dirección IP. Este control se realiza siempre y cuando la comunicación sea hacia Internet. Dentro de la Intranet no hay control de ancho de banda, limitándose simplemente a la velocidad del puerto físico (cable) o virtual (uint16_t WiFi port) del dispositivo al que se conecte.

A continuación se muestra el diagrama de la conexión de las distintas redes y servicios que la UMSA tiene actualmente:

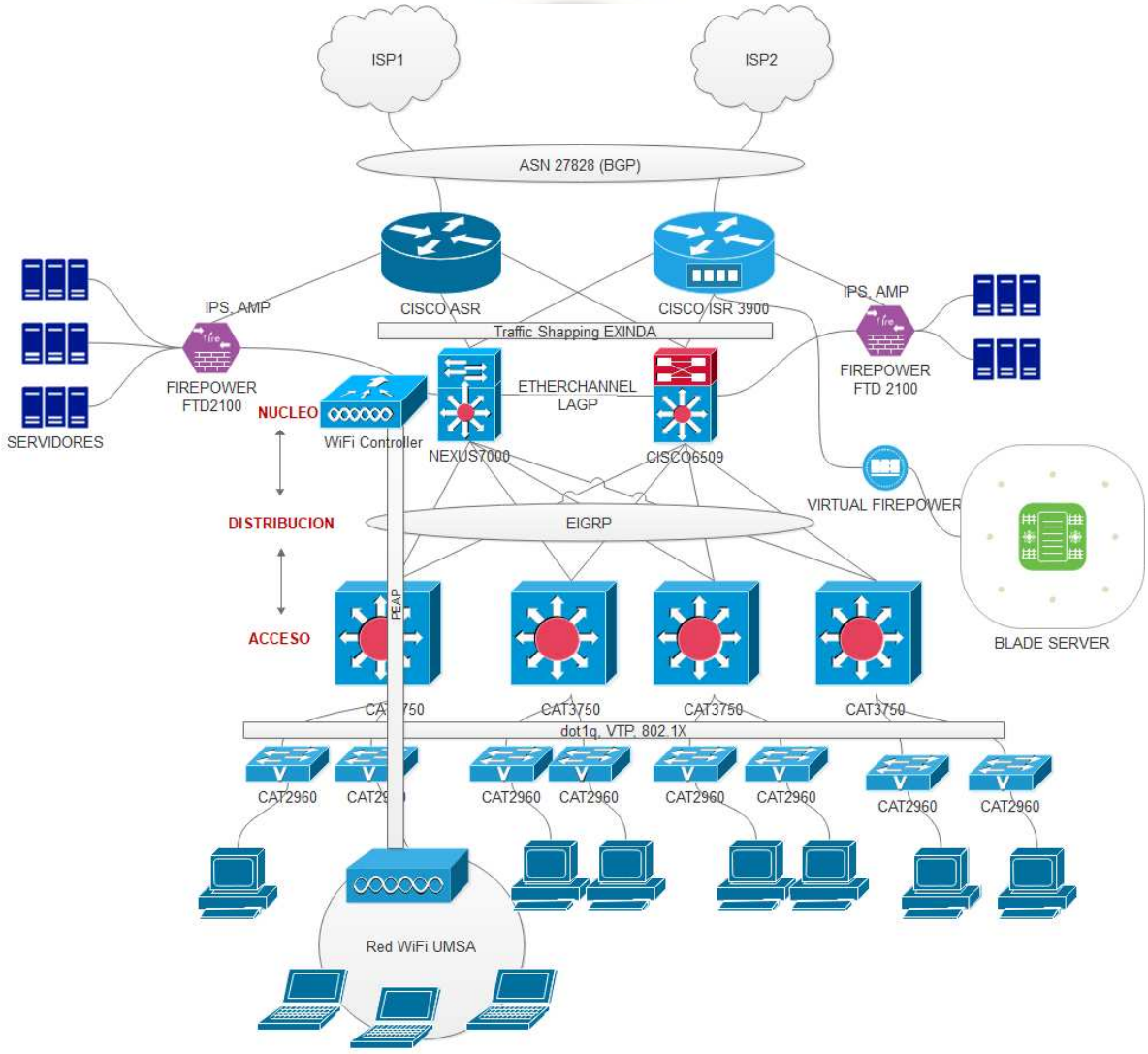


Figura 4.4: Diagrama de topología de la red de la UMSA.

La UMSA tiene una infraestructura de dos núcleos: uno ubicado en el Ed. Hoy y otro en el Monoblock Central.

La red posee de 12 nodos a nivel de la capa de distribución que operan en distintas áreas dentro la mancha urbana:

- Nodo Campus Cota Cota
- Nodo Carrera de Artes
- Nodo Facultad de Medicina
- Nodo Facultad de Ciencias Farmacéuticas y Bioquímicas
- Nodo Facultad de Derecho y Ciencias políticas
- Nodo Facultad de Ingeniería
- Nodo del Edificio Nava (Facultad de Ciencias Económicas y Financieras)
- Nodo Facultad de Arquitectura, Artes, Diseño y Urbanismo
- Nodo del Edificio Hoy
- Tres nodos en el Monoblock Central

El esquema actual de la red es jerárquico (basado en el modelo Cisco Campus Network) ya que los nodos poseen un nodo que a la vez puede poseer otros nodos antes de llegar al usuario final, está arquitectura de estrella extendida hace que la implementación de IPv6 pueda llevarse a cabo con mayor facilidad pues podrán asignarse prefijos de subredes y el plan de numeración será más claro.

En la siguiente Figura se muestra el diagrama lógico general de la red de Internet de la UMSA donde figuran los principales equipos como son routers, switches, firewalls, servidores y puntos de acceso.

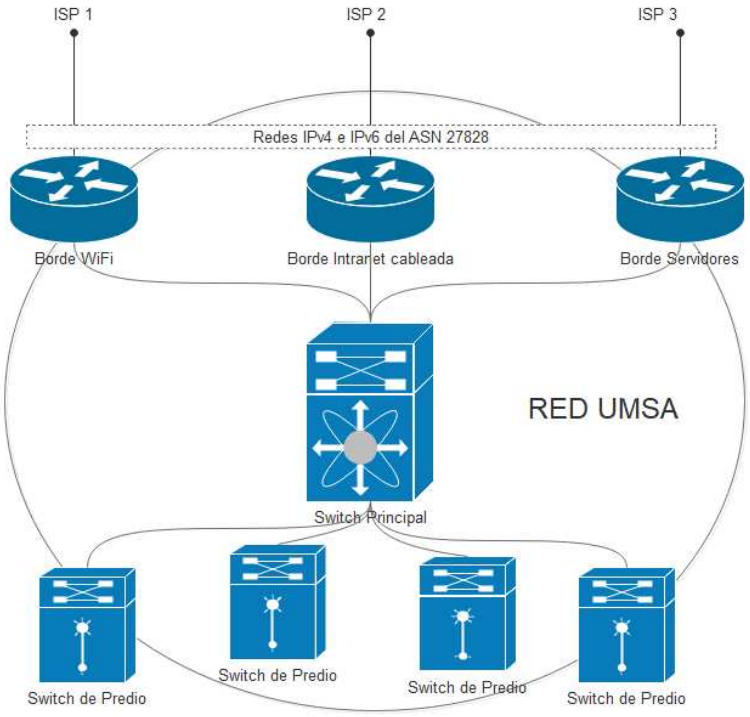


Figura 4.5: Diagrama general de la topología de la red de Nodo Internet de la UMSA.

Como se puede observar en las anteriores dos ilustraciones, el protocolo Ethernet es el usado para la interconexión de los principales equipos de red mediante conexiones por Giga Ethernet, Fast Ethernet y Ethernet, que además cuentan con la característica de soportar distintos medios físicos y un número ilimitado de nodos.

Estos nodos utilizan enrutamiento dinámico OSPF dentro del espacio de direccionamiento público asignado a la UMSA.

Se pretende también que al efectuar la transición a IPv6 los servidores se mantendrán y no serán remplazados sino actualizados en caso de ser necesario, lo mismo para servidores DNS y equipos de DMZ.

El monitoreo de toda la red se lo realiza empleando las herramientas de línea de comandos de consola que pueden ser usados por los distintos equipos como por ejemplo los routers, esto debido a las siguientes características presentes:

- Control de desempeño: es posible determinar el desempeño de la red y las tendencias de uso sin necesidad de afectar el ancho de banda.
- Control de múltiples instalaciones: se pueden obtener reportes desde múltiples consolas acerca del estado de red y monitorear múltiples redes desde una sola consola.
- Control de solución de problemas: se pueden resolver problemas en redes locales y remotas de forma eficaz y rápida.
- Control de información: permite la generación de reportes para justificar cualquier modificación de la red.

Además por ser de utilización libre con los equipos, estas herramientas ahorran dinero a la Universidad al prescindir de la compra de licencias para usar otras herramientas de monitoreo de red que se encuentran en el mercado.

En cuanto a los equipos de la infraestructura lógica de red que posee la UMSA, estos son la mayoría de reciente incorporación por lo cual el personal encargado afirma que están preparados para llevar a cabo la migración sin problemas, el análisis detallado de los equipos se efectúa más adelante dentro de este capítulo.

4.7.2 DIAGNÓSTICO ACERCA DE LA SITUACIÓN ACTUAL DEL SERVICIO DE INTERNET DE LA UMSA

La UMSA posee dos tipos de redes: cableadas e inalámbricas. La UMSA provee el servicio de Internet a más de 10 mil usuarios, distribuidos en sus más de 30 predios. Y provee Internet a sus tres estamentos Docentes, Estudiantes y Administrativos.

La UMSA, no utiliza direccionamiento IPv6 en ninguno de sus servicios de Internet; el servicio de Internet que actualmente tiene más usuarios en la institución es el de red cableada y es la base de todos los servicios de acceso a Internet que ofrece la Universidad.

Los servicios de Internet que utilizan sus usuarios tienen dos espacios de direccionamiento principales de IPv4 dentro del bloque 200.7.160/20 y 172.16.0.0/20, cuenta con un primer bloque de direcciones /20 que fue asignado a la Universidad, por LACNIC, y tiene un espacio de 4094 direcciones públicas y el segundo bloque corresponde a direcciones privadas, que, en total los dos espacios de direccionamiento suman 8188 direcciones IP disponibles para sus usuarios de los servicios de Internet.

La cantidad actual de usuarios del servicios de red de la UMSA es de aproximadamente 10000 usuarios.

Las direcciones públicas asignadas a la UMSA se han distribuido entre todas las Facultades y Áreas Administrativas, estas direcciones son asignadas a cada usuario de la red primordialmente de forma dinámica.

Como se puede observar, la red actual de la UMSA, tiene la suficiente cantidad de direcciones IPv4 públicas y privadas para proveer de conectividad a Internet a todos sus usuarios usando su bloque de direcciones públicas o privadas. La desventaja en el uso de direcciones privadas es la latencia y procesamiento que involucra utilizar NAT.

La UMSA, también tiene otros servicios de Internet que a pesar de estar implementados tienen poca cantidad de usuarios y tráfico de red, estos servicios son:

- WiFi
- Telefonía IP
- Red de Servidores

Estas redes y servicios adicionales también obtienen el direccionamiento apropiado compartiendo de esta forma la infraestructura de red.

4.8 EVALUACIÓN DE LAS ALTERNATIVAS DE TRANSICIÓN

Los mecanismos de transición, pueden agruparse en tres grandes categorías:

- Dual-Stack o doble pila: Coexistencia de IPv4 e IPv6 en los mismos dispositivos y redes. Estos mecanismos implican la utilización de ambos protocolos en paralelo en los dispositivos.
- Traductores: Traducción de IPv4 a IPv6 y de IPv6 a IPv4, para permitir la comunicación entre dispositivos IPv4 e IPv6.
- Tunneling: Transporte de paquetes IPv6 en túneles IPv4 y paquetes IPv4 en túneles IPv6. Ideal cuando el core no soporta IPv6.

Se han definido recomendaciones para lograr la coexistencia IPv4/IPv6, así como la transición a IPv6. Como ejemplo de mecanismos de migración se pueden mencionar Dual-Stack más NAT444, Stateful NAT64 + DNS64, 6rd, Dual Stack – Lite (DS-Lite), Gateway Initiated Dual Stack – Lite (GI-DS-Lite), 6PE y 6VPE. Los mecanismos definidos son herramientas que pueden combinarse y adaptarse a cada situación en particular. Cada implementación o predio debe decidir que mecanismo o grupo de mecanismos son más convenientes.

Se trata de determinar cómo es mejor desplegar la red IPv6 sin disrupciones, el análisis se hace con los datos expuestos en el diagnóstico para elegir la mejor alternativa que se ajuste mejor a la red de la Universidad y a partir de los resultados se podrá elaborar un diseño y plan de implementación de alto nivel que cumpla con los objetivos planteados.

Antes de elegir el método apropiado para la transición a IPv6 en la UMSA, deben tomarse en cuenta que:

- Que protocolos IPv4 e IPv6 son incompatibles a nivel de red.
- Existen algunos hosts que no generan ni reconocen IPv6. Los routers actuales descartan los paquetes IPv6.
- La principal dificultad consiste en actualizar la infraestructura de red.

- Durante la etapa de transición de Internet existirán redes con infraestructura mixta esto quiere decir que habrán redes con infraestructura IPv4 y otras con infraestructura IPv6.
- Con el fin de evaluar las distintas tecnologías se ha realizado una tabla comparativa entre los principales mecanismos para facilitar la elección de la alternativa de migración a implementar.

4.9 CONSIDERACIONES PARA LA INFRAESTRUCTURA DE RED IPV6

El diseño de la transición del protocolo IPv6 debe considerar los requerimientos de la UMSA, incluyendo consideraciones externas como la disponibilidad de prefijos e infraestructura de red de la Universidad, la infraestructura de seguridad, la conectividad con el/los proveedor(es) ISP, escalabilidad de la red, rendimiento de los equipos y mantenimiento de las redes de servicios.

Los factores más importantes que se deben tomar en cuenta en el momento de seleccionar la topología de red son los siguientes:

a. El tráfico de red, el tipo de servicios y aplicaciones que se van a ejecutar.
b. La capacidad de crecimiento de la red.
c. La capacidad y la distribución a equipos a interconectar.

Se presenta la información acerca de los equipos para determinar si requieren cambios, luego se determinan el direccionamiento apropiado para la red, y finalmente se elabora el plan que servirá como esquema por el cual el DTIC podrá regirse para la posterior implementación de este protocolo en la red universitaria.

4.10 EVALUACIÓN DE LA INFRAESTRUCTURA DE NÚCLEO DE RED

DISPOSITIVO	VERSION DE SOFTWARE	Soporte IPv6
ISR 3925	Cisco IOS Software, C3900e Software (C3900e-UNIVERSALK9-M), Version 15.2(4)M5, RELEASE SOFTWARE (fc2)	Si
ASR 1000	Cisco IOS XE Software, Version 16.06.03	Si
	Cisco IOS Software [Everest], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.6.3, RELEASE SOFTWARE (fc8)	Si
Nexus 7000	Software BIOS: version 2.12.0 kickstart: version 6.2(6a) system: version 6.2(6a) BIOS compile time: 05/29/2013 kickstart image file is: bootflash:///n7000-s2-kickstart.6.2.6a.bin kickstart compile time: 1/29/2014 15:00:00 [02/26/2014 08:19:34] system image file is: bootflash:///n7000-s2-dk9.6.2.6a.bin system compile time: 1/29/2014 15:00:00 [02/26/2014 10:27:32]	Si
FTD	Cisco Firepower 2110 Threat Defense (77) Version 6.2.2 (Build 81)	Si
FMC	Operating System 6.2.3 Operating System Version Cisco Fire Linux OS	Si
ASA 5550	Cisco Adaptive Security Appliance Software Version 8.4(4) Device Manager Version 6.4(9)	Si
3750	Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)	Si, es necesario cambiar al SDM dual-stack-ipv4-ipv6
2960	Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(50)SE5, RELEASE SOFTWARE (fc1)	Si, es necesario cambiar al SDM dual-stack-ipv4-ipv6

Tabla 4.1: Compatibilidad de equipos de la red Intranet de la UMSA

4.11 EVALUACIÓN DE SERVIDORES

En la figura siguiente se muestra el uso de los sistemas operativos y distribuciones en la UMSA:

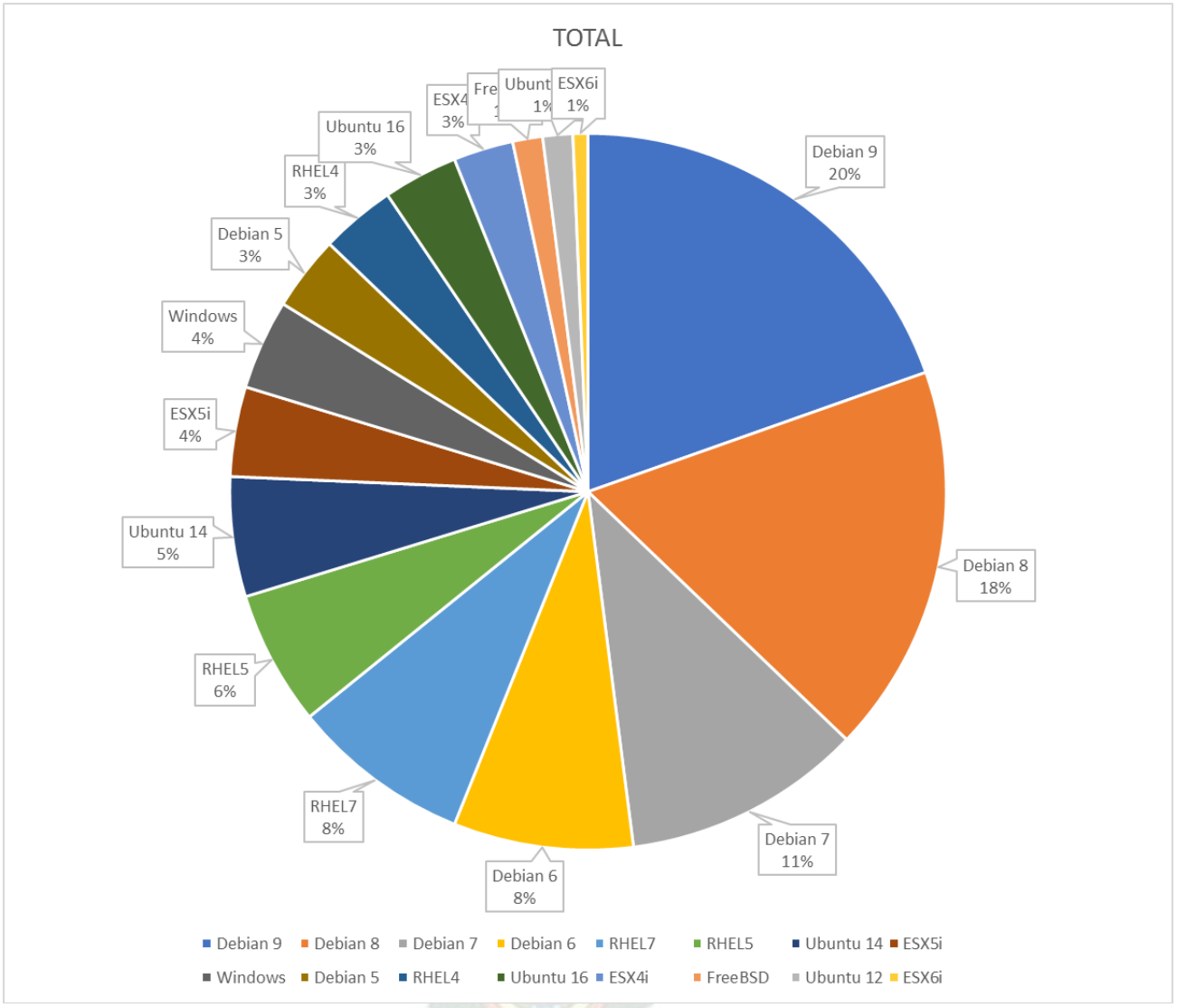


Figura 4.6 Sistemas Operativos y Distribuciones de los servidores de la UMSA (Marzo 2020).

Los SSOO de los servidores son predominantemente Debian Linux, la version de kernel más antigua es 2.6.9 de un RHEL4. GNU/Linux y tiene soporte de IPv6 desde 1996. Sin embargo el uso de IPv6 en las version 2.4 está desaconsejado. Sin considerar la obsolescencia de una minoría de servidores y sus sistemas operativos, un 99% por ciento de los servidores operativos soportan Dual Stack, lo que significa que la adopción de IPv6 en los mismos, es totalmente posible.

4.12 COMPATIBILIDAD DE HOSTS DE LA RED CABLEADA

En la siguiente figura se muestra el porcentaje de uso de sistemas operativos de los hosts en la red cableada.

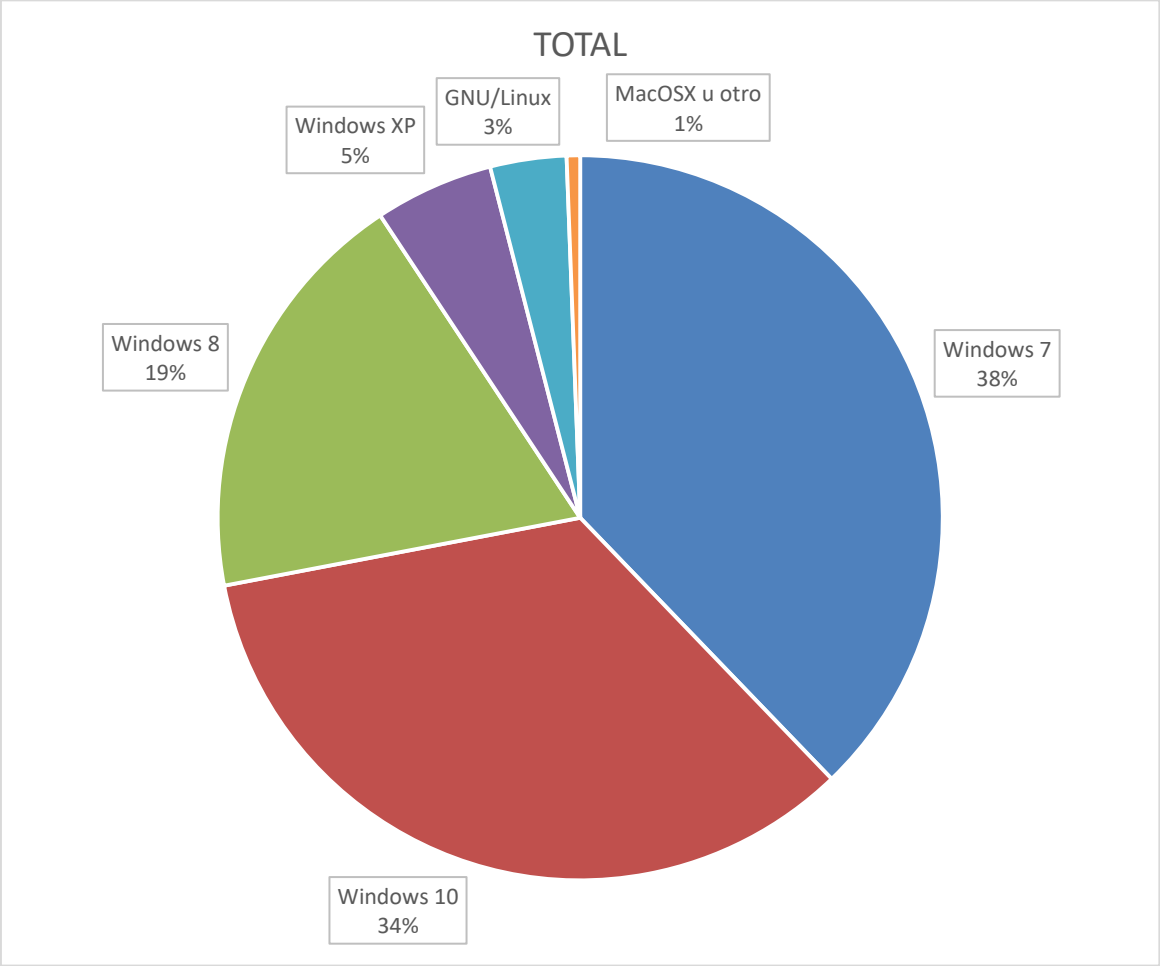


Figura 4.7: Sistemas Operativos de Usuarios Finales en la Red Cableada de la UMSA (Marzo 2020).

Una mayoría predominante usa Microsoft Windows como SSOO de escritorio en la red cableada. Windows ofrece compatibilidad con IPv6 desde la versión Windows XP. Sin embargo, hay que considerar que la compatibilidad total de Windows XP (~5% de los hosts) se consigue luego de un proceso de instalación de software y que las resoluciones DNS de Dual Stack no funcionan[23]. Considerando esto, se puede aseverar que un 95% de los hosts que se conectan a la red de la UMSA por cable están listos para la adopción de IPv6.

[23] https://sites.google.com/site/jrey42/Home/ipv6/winxp

4.13 COMPATIBILIDAD DE HOSTS DE LA RED INALAMBRICA (WiFi)

En la siguiente figura se ven los porcentajes de uso de los diferentes sistemas operativos de hosts y sus versiones en la red WiFi de la UMSA:

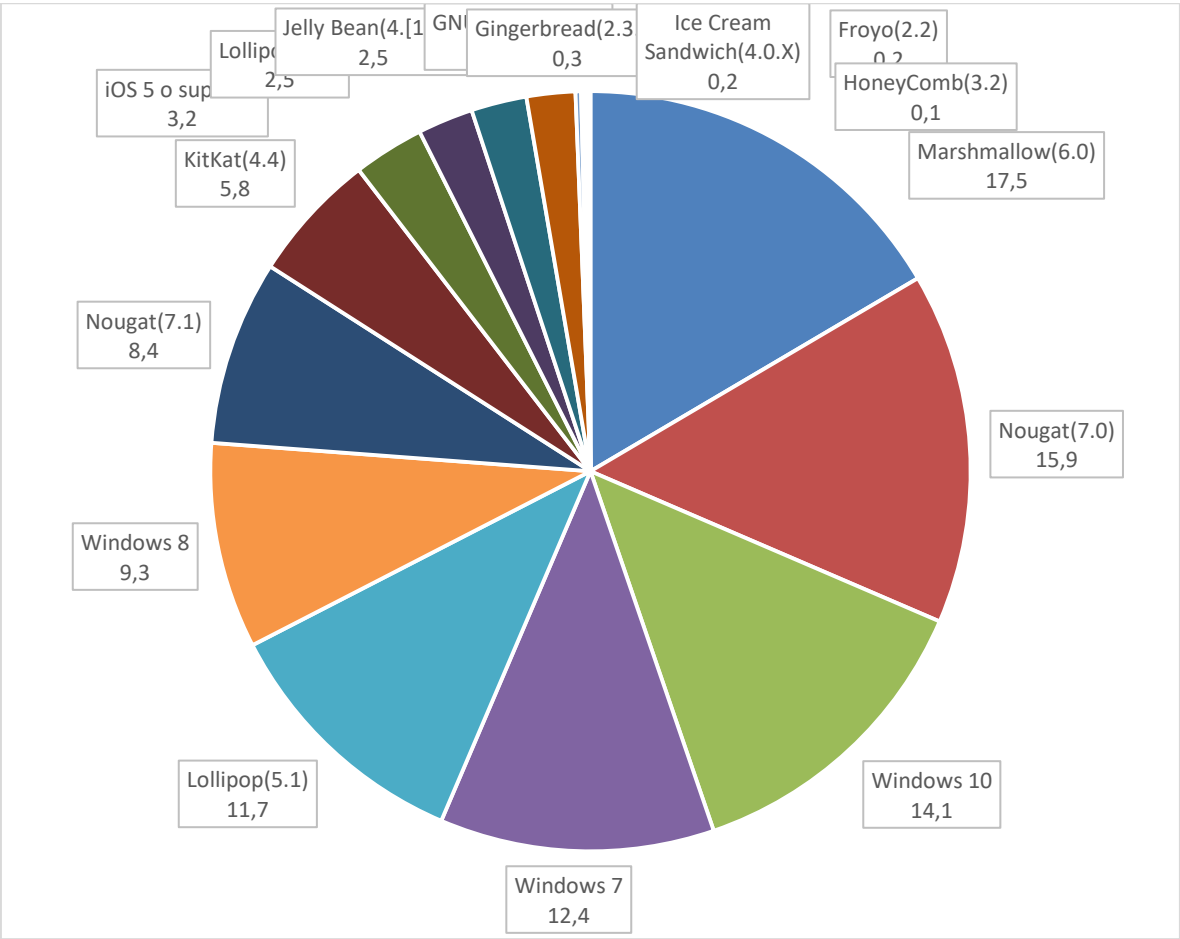


Figura 4.8: Sistemas Operativos de Usuarios Finales en la Red Inalámbrica de la UMSA (Marzo 2020).

Como se ve en la figura la mayoría de los usuarios móviles usan Android, las laptops preferentemente usan Windows 7 o superior. Con certeza se puede asegurar que un 99% de los usuarios de la red WiFi posee un dispositivo listo para la adopción de IPv6.

4.14 CONSIDERACIONES PARA LA CAPA DE ACCESO DE RED DE LA ARQUITECTURA TCP/IP

La Universidad utiliza el estándar Ethernet para todas sus redes que operan dentro de la topología física de la red y esta soporta IPv6 sin inconvenientes, este estándar se mantendrá durante la transición al nuevo protocolo y a la posible implantarse IPv6 de forma nativa.

Se estableció, además, no reubicar ningún equipo de la actual infraestructura pues una nueva ubicación puede afectar los patrones de tráfico, el uso de ancho de banda y la seguridad de la red.

Los dispositivos de núcleo son de reciente adquisición, por lo que la transición al protocolo IPv6 no debería presentar ningún problema, aunque estos se verán obligados a procesar tramas de mayor tamaño debido al aumento de tamaño del paquete IP con IPv6, tienen la capacidad necesaria para la adopción de IPv6.

4.15 CONSIDERACIONES PARA LA CAPA DE INTERNET DE LA ARQUITECTURA TCP/IP

Los cambios más significativos y de mayor impacto en la infraestructura de red de la UMSA, se realizan en la capa de Internet de la arquitectura TCP/IP o en la capa de red del modelo OSI debido a que deberá considerarse los cambios en las configuraciones de los distintos dispositivos de red y en la información de las distintas tablas de enrutamiento que se efectuarán en la transición a IPv6.

4.15.1 ESPACIO DE DIRECCIONAMIENTO IPV6

En nuestra región la encargada de administrar el espacio de direccionamiento IPv4 e IPv6 es el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), institución que aplica políticas propias para que las organizaciones de la región puedan solicitar espacio de direccionamiento. La UMSA cuenta con un número de sistema autónomo (ASN), sin embargo LACNIC no garantiza que una dirección global sea enrutable globalmente, esto dependerá del proveedor asociado y su infraestructura de conexión.

CAPITULO V

DISEÑO DE LA IMPLEMENTACIÓN

5.1 INTRODUCCIÓN

El diseño de la implementación de la solución planteada para el área tecnológica de la Universidad Mayor de San Andrés es el producto la revisión de las bases teóricas, relevamiento de la información y análisis de los recursos tecnológicos para en el presente capitulo hacer una propuesta de implementación.

5.2 PLAN DE NUMERACIÓN IPV6 Y DIRECIONAMIENTO DE LA RED

El esquema de direccionamiento en IPv6 es diferente a IPv4, en IPv4 la jerarquía de direccionamiento incluye los componentes de red, subred y host. En ipv6, con 128 bits, se provee un direccionamiento de jerarquía global única basada en prefijos en vez de clases de direcciones, lo que permite que el uso de recursos en las tablas de backbone sea más eficiente.

El formato es el siguiente:

global routing prefix	subnet ID	interface ID
n bits	m bits	128-(n+m) bits

En el caso de la UMSA el prefijo global asignado es 2801:104::/40. Entonces:

Global routing prefix=n=40

Y para definir el subnet ID, se propone una división por tipo de red

subnetID=m=5

con dos prefijos principales 2801:104::/45 para la red WiFi y 2801:104:8::/45 para la red cableada.

Sin embargo queda aclarar que cada uno de los prefijos es susceptible de organizarse, en el caso particular de la UMSA, por tipo de red, predio, facultad y unidad académica/administrativa, estructurándose de la siguiente manera:

Número de subredes requeridas=predio+facultad+unidades.

Considerando lo que en el futuro pasaría con la red de la UMSA se plantea:

Número de subredes requeridas=32+32+512

bits de subred necesarios=5+5+9 = /64

Por ejemplo:

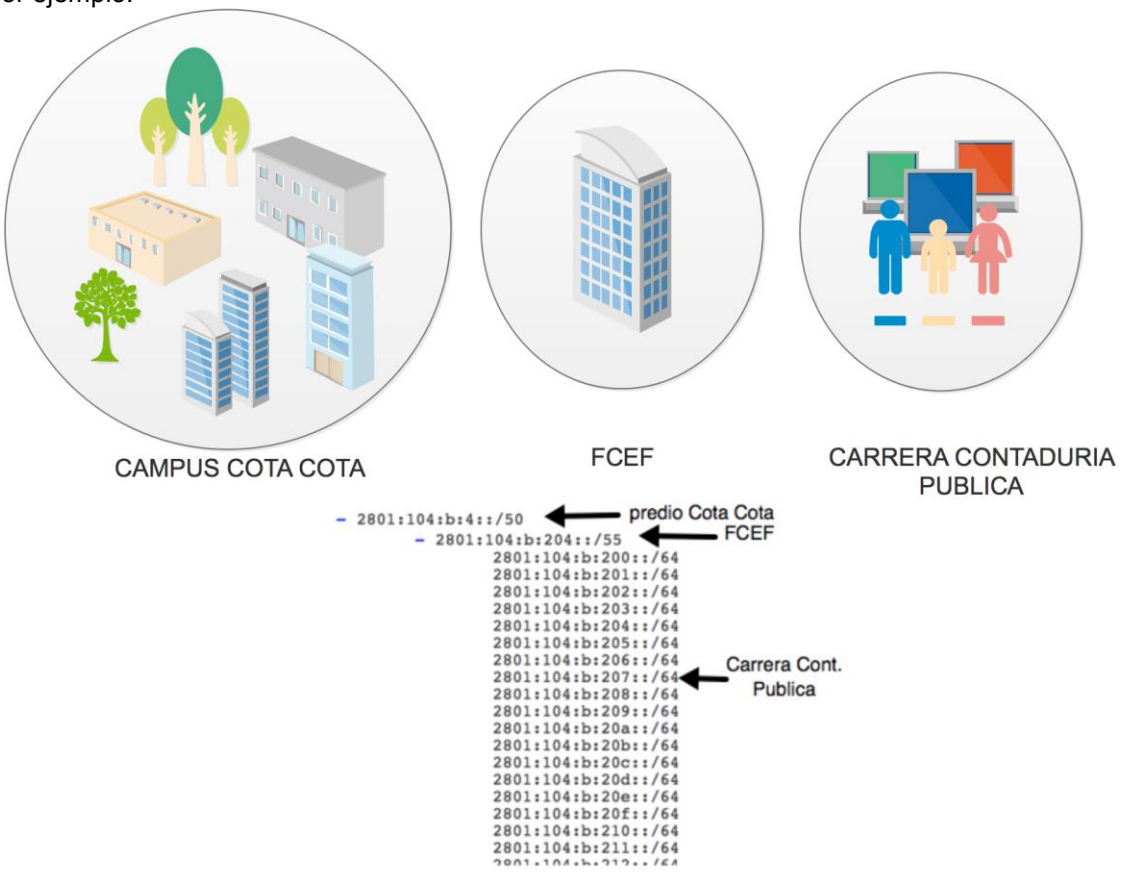


Figura 5.1 Distribución del SubnetID (16 bits).

LACNIC asignó a la UMSA el prefijo 2801:104::/40 de direcciones IPv6, misma se reasignó en base a servicios y las subredes o VLAN a implementarse, se creó el estándar de numeración para la red de la UMSA, como ejemplo se creará la numeración para la red del servicio de Intranet que utilizará el esquema mostrado en la siguiente tabla:

N° SEGMENTO	SUBRED	SERVICIO ASIGNADO
1	2801:104::/44	Servidores
2	2801:104:10::44	Servidores
3	2801:104:20::/44	Red cableada
4	2801:104:30::/44	Red cableada
5	2801:104:40::/44	Red Inalambrica
6	2801:104:50::/44	Red Inalambrica
7	2801:104:60::/44	
8	2801:104:70::/44	

9	2801:104:80::/44	
10	2801:104:90::/44	
11	2801:104:a0::/44	
12	2801:104:b0::/44	
13	2801:104:c0::/44	Enlaces 6 Bone
14	2801:104:d0::/44	
15	2801:104:e0::/44	
16	2801:104:f0::/44	

Tabla 5.1: Direccionamiento de la red de la UMSA, 2801:104::/40.

N° SEGMENTO	SUBRED	PREDIO
3-1	2801:104:20::/48	HOY
3-2	2801:104:21::/48	MONOBLOCK
3-3	2801:104:22::/48	COTA
3-4	2801:104:23::/48	MEDICINA
3-5	2801:104:24::/48	FARMACIA
3-6	2801:104:25::/48	TECNOLOGIA
3-7	2801:104:26::/48	INGENIERIA
3-8	2801:104:27::/48	DERECHO
3-9	2801:104:28::/48	ARTES
3-10	2801:104:29::/48	ARQUITECTURA
3-11	2801:104:2a::/48	NAVA
3-12	2801:104:2b::/48	TMONTES
3-13	2801:104:2c::/48	
3-14	2801:104:2d::/48	
3-15	2801:104:2e::/48	
3-16	2801:104:2f::/48	

Tabla 5.2: Direccionamiento de la red cableada, 2801:104:20::/44.

N° SEGMENTO	SUBRED	PREDIO
5-1	2801:104:40::/48	HOY
5-2	2801:104:41::/48	MONOBLOCK
5-3	2801:104:42::/48	COTA
5-4	2801:104:43::/48	MEDICINA
5-5	2801:104:44::/48	FARMACIA
5-6	2801:104:45::/48	TECNOLOGIA

5-7	2801:104:46::/48	INGENIERIA
5-8	2801:104:47::/48	DERECHO
5-9	2801:104:48::/48	ARTES
5-10	2801:104:49::/48	ARQUITECTURA
5-11	2801:104:4a::/48	NAVA
5-12	2801:104:4b::/48	TMONTES
5-13	2801:104:4c::/48	
5-14	2801:104:4d::/48	
5-15	2801:104:4e::/48	
5-16	2801:104:4f::/48	

Tabla 5.3: Direccionamiento de la red inalámbrica (WiFi), 2801:104:40::/44.

Bajo este esquema cada prefijo /44 puede convertirse en 16 prefijos /48, y a su vez cada prefijo /48 se puede convertir en 16 networks /52, luego cada prefijo /52 puede convertirse en 16 prefijos /56, y finalmente cada network /56 que serán asignados para usuarios este espacio permitirá por ejemplo que el servicio Intranet pueda tener 256 prefijos /64 para usuarios.

En caso de agotarse el espacio en cada prefijo podrá disponerse de otro para su utilización de la misma manera. Cada segmento /64 asignado a un grupo de usuarios puede tener hasta 2^{64} dispositivos conectados.

El bloque de direcciones 2801:104:c1::/56 se puede dividir en 256 subredes /64, para utilizarlas en los enlaces troncales de la infraestructura de red[24]. Se utilizó todo un bloque /56 para troncales para asegurar que la Universidad pueda cubrir todos los enlaces troncales existentes y por implementar en el futuro con el mayor margen de expansión posible sin que se tenga que recurrir a un nuevo plan de numeración en el futuro. De esta forma también se logra una manera más sencilla de identificar direcciones que correspondan a la red de enlaces troncales y facilitar las operaciones de mantenimiento y monitoreo.

En IPv4 se tenía presente el factor de dimensionamiento que era la forma de definir el tamaño apropiado para cada red según la cantidad de dispositivos que la conforman, el dimensionamiento en IPv6 no es un problema pues aunque asignar una cantidad grande de direcciones puede ser considerado un desperdicio de direcciones IP, esto no representa problema alguno considerando la cantidad de dispositivos que el usuario necesitará conectar y el espacio de direccionamiento de 128 bits que posee un número de direcciones prácticamente infinito.

N° SEGMENTO	SUBRED	ENLACE
13-1-1-1-1-1	2801:104:c0::/64	coreH-coreM
13-1-1-1-1-2	2801:104:c0:1::/64	coreH-300M
13-1-1-1-1-3	2801:104:c0:2::/64	coreH-650M
13-1-1-1-1-4	2801:104:c0:3::/64	coreH-1G

[24] El espacio /64 para enlaces troncales fue elegido basándose en las especificaciones del RFC3627: "Use of Prefix /127 Prefix Length between routers considered harmful". URL: tool.ietf.org/html/rcf3627.

13-1-1-1-1-5	2801:104:c0:4::/64	coreH-hoy
13-1-1-1-1-6	2801:104:c0:5:/64	
13-1-1-1-1-7	2801:104:c0:6::/64	
13-1-1-1-1-8	2801:104:c0:7::/64	coreH-mono1
13-1-1-1-1-9	2801:104:c0:8::/64	coreH-mono2
13-1-1-1-1-10	2801:104:c0:9::/64	coreH-mono3
13-1-1-1-1-11	2801:104:c0:a::/64	
13-1-1-1-1-12	2801:104:c0:b::/64	
13-1-1-1-1-13	2801:104:c0:c::/64	coreH-cota
13-1-1-1-1-14	2801:104:c0:d::/64	
13-1-1-1-1-15	2801:104:c0:e::/64	coreH-Farmacia
13-1-1-1-1-16	2801:104:c0:f::/64	coreH-Tecnologia
13-1-1-1-1-17	2801:104:c0:10::/64	coreH-Ingenieria
13-1-1-1-1-18	2801:104:c0:11::/64	coreH-Derecho
13-1-1-1-1-19	2801:104:c0:12::/64	coreH-Artes
13-1-1-1-1-20	2801:104:c0:13::/64	coreH-Arquitectura
13-1-1-1-1-21	2801:104:c0:14::/64	coreH-Nava
13-1-1-1-1-22	2801:104:c0:15::/64	coreH-Tmontes
13-1-1-1-1-23	2801:104:c0:16::/64	
13-1-1-1-1-24	2801:104:c0:17::/64	
13-1-1-1-1-25	2801:104:c0:18::/64	coreH-Rmed
13-1-1-1-1-26	2801:104:c0:19::/64	Rmed-medicina(3750)
13-1-1-1-1-27	2801:104:c0:1a::/64	
13-1-1-1-1-28	2801:104:c0:1b::/64	
13-1-1-1-1-29	2801:104:c0:1c::/64	
13-1-1-1-1-30	2801:104:c0:1d::/64	
13-1-1-1-1-31	2801:104:c0:20::/64	aristaM-Nexus
13-1-1-1-1-32	2801:104:c0:21::/64	aristaH-Nexus
13-1-1-1-1-33	2801:104:c0:22::/64	
13-1-1-1-1-34	2801:104:c0:23::/64	
13-1-1-1-1-35	2801:104:c0:24::/64	
13-1-1-1-1-36	2801:104:c0:25::/64	
…….	…….	
13-1-1-1-1-256	2801:104:c0:ff::/64	

Tabla 5.4: Direccionamiento para enlaces 6BONE núcleo Ed. Hoy, 2801:104:c0::/56.

N° SEGMENTO	SUBRED	ENLACE
13-1-1-1-2-1	2801:104:c1::/64	
13-1-1-1-2-2	2801:104:c1:1::/64	coreM-300M
13-1-1-1-2-3	2801:104:c1:2::/64	coreM-650M
13-1-1-1-2-4	2801:104:c1:3::/64	coreM-1G
13-1-1-1-2-5	2801:104:c1:4::/64	coreM-hoy
13-1-1-1-2-6	2801:104:c1:5:/64	
13-1-1-1-2-7	2801:104:c1:6::/64	
13-1-1-1-2-8	2801:104:c1:7::/64	coreM-mono1
13-1-1-1-2-9	2801:104:c1:8::/64	coreM-mono2
13-1-1-1-2-10	2801:104:c1:9::/64	coreM-mono3
13-1-1-1-2-11	2801:104:c1:a::/64	
13-1-1-1-2-12	2801:104:c1:b::/64	
13-1-1-1-2-13	2801:104:c1:c::/64	coreM-cota
13-1-1-1-2-14	2801:104:c1:d::/64	
13-1-1-1-2-15	2801:104:c1:e::/64	coreM-Farmacia
13-1-1-1-2-16	2801:104:c1:f::/64	coreM-Tecnologia
13-1-1-1-2-17	2801:104:c1:10::/64	coreM-Ingenieria
13-1-1-1-2-18	2801:104:c1:11::/64	coreM-Derecho
13-1-1-1-2-19	2801:104:c1:12::/64	coreM-Artes
13-1-1-1-2-20	2801:104:c1:13::/64	coreM-Arquitectura
13-1-1-1-2-21	2801:104:c1:14::/64	coreM-Nava
13-1-1-1-2-22	2801:104:c1:15::/64	coreM-Tmontes
13-1-1-1-2-23	2801:104:c1:16::/64	
13-1-1-1-2-24	2801:104:c1:17::/64	
13-1-1-1-2-25	2801:104:c1:18::/64	coreM-Rmed
13-1-1-1-2-26	2801:104:c1:19::/64	
13-1-1-1-2-27	2801:104:c1:1a::/64	
13-1-1-1-2-28	2801:104:c1:1b::/64	
13-1-1-1-2-29	2801:104:c1:1c::/64	
13-1-1-1-2-30	2801:104:c1:1d::/64	
13-1-1-1-2-31	2801:104:c1:20::/64	
13-1-1-1-2-32	2801:104:c1:21::/64	
13-1-1-1-2-33	2801:104:c1:22::/64	
13-1-1-1-2-34	2801:104:c1:23::/64	
13-1-1-1-2-35	2801:104:c1:24::/64	
13-1-1-1-2-36	2801:104:c1:25::/64	
…….	…….	
13-1-1-1-2-	2801:104:c1:ff::/64	

256		

Tabla 5.5: Direccionamiento para enlaces 6BONE núcleo Monoblock, 2801:104:c1::/56.

Por otra parte se debe considera también la numeración de los servidores, esta numeración debe ser estática y sin uso de opciones de autoconfiguración en los mismos, la razón es la de conseguir la máxima disponibilidad posible y evitar tener que realizar cambios ante problemas con la dirección de red, se recomienda colocar direcciones fáciles de recordar para una configuración rápida y elaborar estrictas medidas de seguridad para el control de acceso a los mismos. Mientras que para la red de usuarios deben tener direcciones asignadas dinámicamente a solicitud de los usuarios de la Universidad, actualmente ya se trabaja de este modo en IPv4 y se desea mantener la misma característica en IPv6 para que la Universidad pueda tener la mayor disponibilidad de direcciones IP para nuevos usuarios y evitar problemas de tráfico y seguridad. En este caso específico se hará uso de los servicios de asignación dinámica de direcciones DHCPv6 o SLAAC, que son compatibles con IPv6, específicamente se usará la numeración automática sin estado que permite configurar servidores DNS.

5.3 APLICACIÓN DEL PROCOLO DE ENRUTAMIENTO OSPFv3

OSPFV3 es el protocolo de enrutamiento OSPF para IPV6 establecido para la red de la UMSA, esta descrito en el RFC 2740. La configuración de OSPF para IPv6 consiste en:

1. Habilitar el protocolo de enrutamiento OSPFv3 para IPv6 en todos los dispositivos de red usando el área 0 para OSPFv3.
2. Habilitar CEF switching para IPv6.
3. Habilitar el proceso OSPFv3 que se ha configurado en el paso 1 en todas las interfaces donde existan prefijos ipv6 del dispositivo (excepto las interfaces de loopback), usando el área 0.

5.4 CONFIGURACIONES EN LOS EQUIPOS DE RED

Considerando que dentro la infraestructura de red se tiene a nivel de equipos de red y se dispone mayoritariamente de la marca Cisco y en particular los dispositivos de predio como son los switchs multicapa Cisco Catalyst 3750 se sigue el siguiente procedimiento:

Sistema operativo y otros datos:

Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 05-May-11 16:29 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(44)SE5, RELEASE SOFTWARE (fc1)

La característica llamada Switch Database Management (SDM). SDM ayuda al conmutador a administrar la asignación de recursos de cada característica. Esto significa que hay algunas características que están deshabilitadas en la plantilla predeterminada. Entonces, si queremos trabajar con estas características, debemos habilitarlas.

Inicialmente se verifica de la siguiente manera:

```
Switch#sh sdm prefer
 The current template is "aggregate default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                6K
  number of IPv4 IGMP groups + multicast routes:  1K
  number of IPv4 unicast routes:                  12K
  number of directly-connected IPv4 hosts:        6K
  number of indirect IPv4 routes:                 6K
  number of IPv4 policy based routing aces:       0
  number of IPv4/MAC qos aces:                    0.875k
  number of IPv4/MAC security aces:               1K
```

Para habilitar el dual stack en el switch:

```
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

Luego del reinicio:

```
Switch#sh sdm prefer
 The current template is "aggregate IPv4 and IPv6 default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                2K
  number of IPv4 IGMP groups + multicast routes:  1K
  number of IPv4 unicast routes:                  5K
  number of directly-connected IPv4 hosts:        2K
  number of indirect IPv4 routes:                 3K
  number of IPv6 multicast groups:                1.125k
  number of directly-connected IPv6 addresses:    2K
  number of indirect IPv6 unicast routes:         3K
  number of IPv4 policy based routing aces:       0
  number of IPv4/MAC qos aces:                    0.875k
  number of IPv4/MAC security aces:               1K
  number of IPv6 policy based routing aces:       0
  number of IPv6 qos aces:                        0.875k
  number of IPv6 security aces:                   0.5K
```

Entonces, ya es posible la configuración de direcciones IPv6 tanto para enrutamiento como dentro las vlans y asignación de direcciones IPv6 a los usuarios finales.

5.5 CONFIGURACIONES EN LOS HOSTS DE USUARIO FINAL

La asignación de direcciones IPv6 a usuarios finales, tanto en la red cableada como inalámbrica (WiFi) se plantea la aplicación del protocolo Stateless IPv6 ofrece una característica denominada Plug&Play Networking, esta permite que un host obtenga los siguientes parámetros:

- Prefijo(s) IPv6
- Puerta(s) de enlace
- Límite de saltos
- MTU
- Tiempo de validez de estos parámetros

Aunque la provisión en IPv6 de direcciones DNS está contemplada en el RFC5006, esta característica no está disponible en ningún sistema operativo.

a) Los hosts obtienen una dirección IPv6 automáticamente.
b) Los routers se pueden configurar manualmente o se puede usar la opción de Prefix Delegation descrita en el RFC 3633.
c) Los servidores DNS deben ser configurados manualmente. Las direcciones Link-local (a diferencia de las globales) se autoconfiguran en todos los hosts.

El proceso de autoconfiguración de direcciones IPv6 se describe en detalle en el RFC 4862:

1) El host escucha por RAs(mensajes de enrutador) que son enviados periódicamente en el link local(Dominio de broadcast) o pueden ser solicitados por el mismo host usando un Solicitation Message.
2) Cada RA provee información para la autoconfiguración.
3) Los hosts crean una dirección Global basada en el mac del host o un ID randomico(depende de la implantación del SSOO) que es la combinación EUI-64 más un Prefijo de enlace(provisto en el RA)

* Si el RA no incluye un prefijo, los hosts no autoconfiguran ninguna dirección global y solamente establecen la dirección de la puerta de enlace.

* Los mensajes RA contienen dos banderas:

El tipo de autoconfiguración stateful que debe realizarse (si hubiera) –la interpretación de ManagedFlag y OtherConfigFlag- es un poco ambigua y su implementación varia de un sistema operativo a otro.

La generación de EUIs IPv6 se basa en el uso de direcciones mac, que en teoría son únicas en un segmento de red, existe un acápite de seguridad usando Privacy Extensións descritas en el RFC4941.

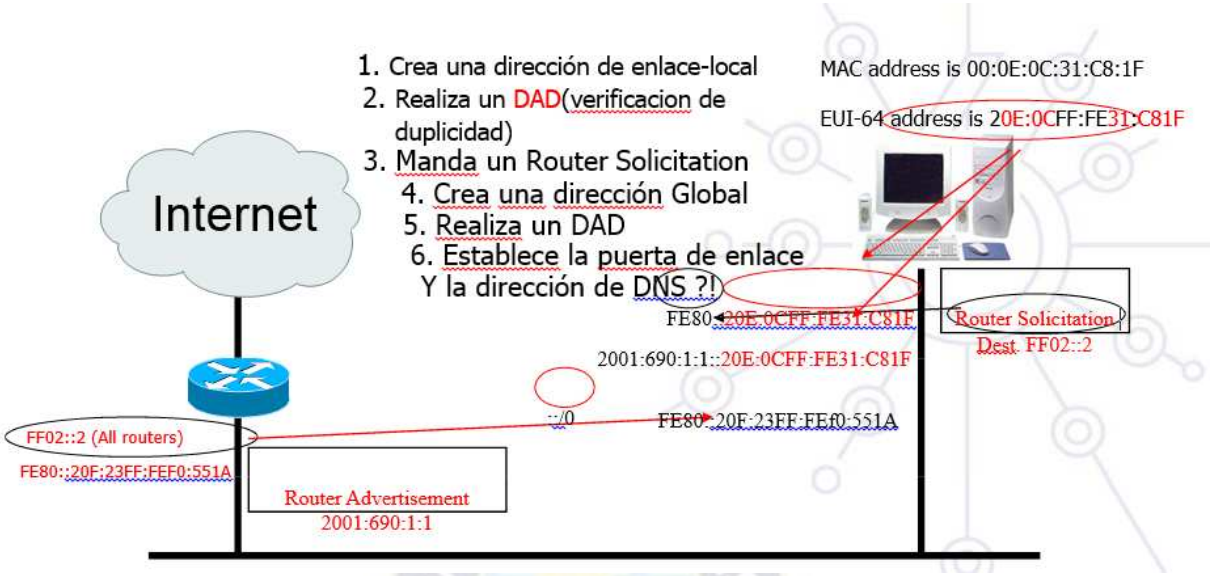


Figura 5.2: Esquema de funcionamiento del protocolo Stateless IPv6.

5.6 CONFIGURACIONES EN LOS SERVIDORES

Considerando que en el Capítulo 4 se evaluaron los servidores y se concluyó que las distribuciones mayoritariamente preponderantes son Debian, Red Hat y Ubuntu, a continuación se detalla la configuración de las interfaces para tales distribuciones, las mismas deben ser realizadas de manera estática debido a que estas direcciones están asociadas a registros en los servidores de DNS.

5.6.1 CONFIGURACIÓN PARA DISTRIBUCION LINUX DEBIAN

La distribución de Linux Debian se convierte en la más utilizada en los servidores del DTIC, con la finalidad de montar sobre éste servicios de interés de la comunidad, la instalación inicial del sistema operativo, a nivel de interfaz de red presenta únicamente la dirección IPv6 del tipo scope link, como se puede apreciar con el comando ip addr show:

```
root@usuario:~# ip addr show
…….
   inet6 fe80::20c:29ff:fe05:a87a/64 scope link noprefixroute
…….
```

La salida completa del comando ip addr show se puede revisar en (ANEXO 1).

El archivo de configuración de la interfaz de red tiene la dirección y nombre, /etc/NetworkManager/system-connections/Wired connection 1, de una instalación inicial en cuanto al protocolo IPv6 muestra:

```
……..
[ipv6]
method=auto
ip6-privacy=2
……..
```

Detalle completo del archivo /etc/NetworkManager/system-connections/Wired connection 1 se puede encontrar en (ANEXO 2).

La configuración de la interfaz de red comprende la modificación del archivo /etc/NetworkManager/system-connections/Wired connection 1, mediante la adición de las siguientes líneas:

```
.....
[ipv6]
addr-gen-mode=eui64
address1=2801:104:40:1::100/64,2801:104:40:1::1
dns=2001:4860:4860::8888;
dns-search=
ip6-privacy=2
method=manual
…….
```

El detalle completo del archivo /etc/NetworkManager/system-connections/Wired connection 1 luego de la configuración puede encontrarse en (ANEXO 3).

Luego de haberse realizado la configuración en la salida del comando ip addr show se puede resaltar:

```
…….
   inet6 2801:104:40:1::100/64 scope global
      valid_lft forever preferred_lft forever
   inet6 fe80::20c:29ff:fe87:7c9c/64 scope link
      valid_lft forever preferred_lft forever
…….
```

La salida completa del comando ip addr show luego de la configuración se puede revisar en (ANEXO 4).

5.6.2 CONFIGURACIÓN PARA DISTRIBUCION LINUX RED HAT

La distribución de Linux Red Hat se convierte en la segunda más utilizada en los servidores del DTIC, con la finalidad de montar sobre éste servicios de interés de la comunidad, la instalación inicial del sistema operativo, a nivel de interfaz de red presenta únicamente la dirección IPv6 del tipo scope link, como se puede apreciar con el comando ip addr show:

```
root@usuario:~# ip addr show
…….
   inet6 fe80::67e0:5e2e:4619:1037/64 scope link noprefixroute
…….
```

La salida completa del comando ip addr show se puede revisar en (ANEXO 5).

El archivo de configuración de la interfaz de red tiene la dirección y nombre, /etc/sysconfig/network-scripts, de una instalación inicial en cuanto al protocolo IPv6 muestra:

```
…….
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
```

IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
…….

Detalle completo del archivo /etc/sysconfig/network-scripts se puede encontrar en (ANEXO 6).

La configuración de la interfaz de red comprende la modificación del archivo /etc/sysconfig/network-scripts, mediante la adición de las siguientes líneas:

…….
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
IPV6ADDR=2801:104:40:1::100/64
IPV6_DEFAULTGW=2801:104:40:1::1
DNS2=2001:4860:4860::8888
IPV6_DOMAIN=umsa.bo
…….

El detalle completo del archivo /etc/sysconfig/network-scripts luego de la configuración puede encontrarse en (ANEXO 7).

Luego haberse realizado la configuración en la salida del comando ip addr show se puede resaltar:

…….
   inet6 2801:104:40:1::100/64 scope global noprefixroute
      valid_lft forever preferred_lft forever
   inet6 fe80::67e0:5e2e:4619:1037/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
…….

La salida completa del comando ip addr show luego de la configuración se puede revisar en (ANEXO 8).

5.6.3 CONFIGURACIÓN PARA LA DISTRIBUCION LINUX UBUNTU

La distribución de Linux Ubuntu se convierte en el tercer sistema operativo más utilizada en los servidores del DTIC, con la finalidad de montar sobre éste servicios de interés de la comunidad, la instalación inicial del sistema operativo, a nivel de interfaz de red presenta únicamente la dirección IPv6 del tipo scope link, como se puede apreciar con el comando ip addr show:

…….
   inet6 2800:cd0:2405:f400:a00:27ff:fea4:a032/64 scope global dynamic mngtmpaddr noprefixroute
      valid_lft 3234sec preferred_lft 3234sec
   inet6 fe80::a00:27ff:fea4:a032/64 scope link
      valid_lft forever preferred_lft forever
…….

La salida completa del comando ip addr show se puede revisar en (ANEXO 9).

El archivo de configuración de la interfaz de red tiene la dirección y nombre, /etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection, de una instalación inicial en cuanto al protocolo IPv6 muestra:

```
…….
[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=auto
…….
```

Detalle completo del archivo /etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection se puede encontrar en (ANEXO 10).

La configuración de la interfaz de red comprende la modificación del archivo /etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection, mediante la adición de las siguientes líneas:

```
…….
[ipv6]
addr-gen-mode=stable-privacy
address1=2801:104:40:1::100/64,2801:104:40:1::1
dns=2001:4860:4860::8888;
dns-search=
method=manual
…….
```

El detalle completo del archivo /etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection luego de la configuración puede encontrarse en (ANEXO 11).

Luego haberse realizado la configuración en la salida del comando ip addr show se puede resaltar:

```
…….
   inet6 2801:104:40:1::100/64 scope global noprefixroute
      valid_lft forever preferred_lft forever
   inet6 2800:cd0:2405:f400:a00:27ff:fea4:a032/64 scope global dynamic mngtmpaddr
noprefixroute
      valid_lft 3515sec preferred_lft 3515sec
   inet6 fe80::a00:27ff:fea4:a032/64 scope link
      valid_lft forever preferred_lft forever
…….
```

La salida completa del comando ip addr show luego de la configuración se puede revisar en (ANEXO 12).

5.6.4 SERVICIOS Y SISTEMAS

Se evalúan las de los servicios y sistemas para establecer la necesidad de plantear la migración hacia IPv6, sobre todo considerando que se tiene la obligación de mostrar nuestros contenidos a Internet bajo los protocolos IPv4 e IPv6

NOMBRE	TIPO	OBSERVACIONES	MIGRACIÓN
DNS	Internet/Intranet	DNS público - Cache	Obligatoria
DHCP	Intranet	Unicamente IPv4	No necesaria
Monitoreo	Internet/Intranet	Cacti/Prometheus	Obligatoria
Seguridad	Internet/Intranet	Todos los Firewall	Obligatoria
Adm. de ancho de banda	Internet	Exinda's	Obligatoria
Matriculación	Intranet		No necesaria
Sistemas académicos	Internet/Intranet	Módulos Internet	Obligatoria
Sistema GAR	Intranet		No necesaria
Kardex	Intranet		No necesaria
Bibliotecas digitales	Intranet		No necesaria
Prestamos de libros	Internet/Intranet	Módulos Internet	Obligatoria
Contabilidad	Intranet		No necesaria
Presupuestos	Intranet		No necesaria
Tesorería y cajas	Intranet		No necesaria
RRHH	Intranet		No necesaria
Asistencia personal	Internet/Intranet	Módulos Internet	Obligatoria
Planillas administrativas	Intranet		No necesaria
Planillas docentes	Intranet		No necesaria
Ayni	Internet/Intranet		Obligatoria
Sistema de títulos	Intranet		No necesaria
Sistema de archivo	Intranet		No necesaria
Portal Institucional	Internet/Intranet		Obligatoria
Cuenta institucional	Internet/Intranet	Módulos Internet	Obligatoria
Correo electrónico	Internet/Intranet		Obligatoria
Plataformas e-learning	Internet/Intranet		Obligatoria

Tabla 5.6 Sistemas y Servicios administrados por el DTIC

En el caso de presentarse inconvenientes en la migración de servidores a IPv6 siempre se dispondrá del acceso mediante IPv4, y en caso de tener problemas con el acceso u otro incidente de configuración, en la institución se cuenta con una solución de respaldo llamada Zerto que puede recrear en cualquier instante pasado cualquiera de los servidores que están protegidos por la solución ya mencionada.

5.6.5 APLICACIÓN DE LAS DIRECCIONES ANYCAST

Considerando los beneficios de las direcciones Anycast, a continuación se muestra parte del código para la implementación la interfaz de los routers mismos que están delante de los servidores que requieren ser parte de dichos beneficios:

```
interface GigabitEthernet0/0
no ip address
```

duplex auto
speed auto
ipv6 address 2001:22::2/64
ipv6 address 2345::/64 anycast
ipv6 ospf 1 area 2

5.7 CONSIDERACIONES PARA CAPAS DE TRANSPORTE Y APLICACIÓN DEL MODELO TCP/IP

A pesar de que los cambios más significativos se realizan en la capa de Internet del modelo TCP/IP, también es necesario tener en cuenta ciertos aspectos que pueden afectar el rendimiento de la red en las capas de transporte y aplicación de este modelo.

Como ya se ha mencionado anteriormente en este documento, el servicio de denominación de dominio es un mecanismo que se utiliza para relacionar el nombre de un nodo con una dirección IP, debido a que este mecanismo fue diseñado para trabajar con direcciones IPv4 ahora este mecanismo debe ser actualizado para trabajar con direcciones IPv6, la actualización de DNS debe incluir los siguientes aspectos:

- El registro AAAA: que cumple las mismas funciones que el registro A pero ahora cumple la misma función admitiendo direcciones de tamaño de 128 bits.
- El dominio IP6.INT: usado para realizar la búsqueda inversa para los nodos, esto en base a direcciones IPv6.
- Redefinir las consultas existentes: esto implica que toda consulta debe soportar los registros A y AAAA para realizar cualquier procedimiento asociado a cada registro.

Dentro de la red de servidores de la Universidad se debe configurar los servidores DNS para que estos sean capaces de resolver direcciones IPv6, así los usuarios con Stack Doble podrán realizar consultas y acceder a información IPv6, si un usuario realiza una consulta y recibe como respuesta una dirección de 32 bits, entonces se utilizará IPv4 para realizar la comunicación, si al contrario se recibe una respuesta de 128 bits se utilizará IPv6. También se debe tomar en cuenta que:

- No todas las direcciones podrán resolverse dentro del servidor DNS de la UMSA, existirán casos donde se tenga que resolver direcciones en otros servidores externos que probablemente no ha realizado la transición a IPv6, por lo cual no se garantiza del todo que la solicitud de una dirección IPv6 sea procesada con éxito. De ser necesario para el usuario se deben resolver estas direcciones a través de tablas locales configuradas manualmente.
- Las aplicaciones comúnmente utilizadas no tendrán que sufrir modificaciones para acceder al Stack Doble, la mayoría de aplicaciones de navegación HTTP, servicios de mensajería instantánea, streaming de audio, video y VoIP, pueden acceder a IPv6 de forma transparente al usuario. Solo en casos específicos donde aplicaciones de red que accedan a DNS deberán ser mejoradas para adquirir la capacidad de los nuevos registros de 128 bits.

La UMSA ha implementado el servidor DNS BIND que es una solución para realizar resoluciones de nombres bajo la plataforma de Linux, para que IPv6 funcione correctamente se debe contar con las versiones 8.1 o superiores para el soporte de registros AAAA, esta herramienta es gratuita y se la puede descargar desde los repositorios de GNU/Linux. En el caso de los servidores DNS internos se tiene un DNS Bouncer basados en NetBSD, cuyo soporte IPv6 es total.

5.8 CONSIDERACIONES DE SEGURIDAD

La seguridad es una consideración crucial al migrar a IPv6, pues este protocolo no es una actualización de IPv4 sino que implica el manejo de nuevos protocolos que conlleva nuevos desafíos de seguridad, específicamente la UMSA en el área de seguridad se maneja recursos de firewall y de prevención de intrusos que operan dentro de su red de servidores y en su red corporativa, estos equipos están preparados para la transición a IPv6 pero aun así pueden experimentar problemas cuando el tráfico atraviese el firewall.

Se debe verificar el soporte de IPv6 exista y que este permita configurar reglas de filtrado para IPv6 de similar forma que con IPv4, las reglas deben ser idénticas en ambos protocolos de lo contrario se tendrán políticas distintas de seguridad en ambos.

Además IPv6 tiene la posibilidad de añadir cabeceras de extensión para administrar distintos servicios como por ejemplo IPsec y movilidad, el uso de las cabeceras de extensión que no pueda ser reconocido por el firewall, el tráfico que no sea reconocido será bloqueado impidiendo la conectividad IPv6. Los dispositivos firewall deben estar configurados de forma que puedan evitarse fisuras en la conectividad en el momento que estos dispositivos procesen el tráfico IPv6, esta configuración se realiza modificando las reglas de seguridad de conexión de ser necesario el uso de extensiones en el tráfico manejado por las redes de la UMSA.

En cuanto a las configuraciones de seguridad en los routers o denominadas configuraciones perimetrales, es necesario configurar reglas que imiten a las ya existentes en IPv4 mediante las listas de acceso u otras configuraciones existentes. Igualmente las herramientas de seguridad perimetral como IDS y de análisis de logs, deben ser actualizadas para el soporte de IPv6. También, se debe considerar que los firewalls (Firepower de Cisco) están certificados para el uso el uso en Stack Doble como se documenta en el siguiente documento digital del fabricante[25], y es importante realizar las configuraciones y pruebas con las consideraciones de ventanas de trabajo y posibles cortes en los servicios en Intranet e Internet.

A continuación se muestra la regla en el firewall Firepower, relacionado con el control del tráfico desde y hacia Internet: el nombre de la regla, zona origen zona destino, red origen, red destino, puertos destino y la acción, que en este caso es permitir.

Figura 5.3: Regla del firewall para el tráfico IPv6.

La configuración detallada de firewall se muestra en el ANEXO 13.

5.9 CALIDAD DE SERVICIO SOBRE IPV6

La calidad de servicio – Quality of Service (QoS) – se define como la capacidad que tiene una red para sostener un comportamiento adecuado del tráfico que transita por ella, proporcionando diversos niveles de servicio a los distintos tipos de tráfico. Con ella, se asegura la entrega de información, dando prioridad a las aplicaciones de desempeño crítico, como el tráfico de video y voz en tiempo real.

[25] https:// www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/interfaces_for_firepower_threat_defense.html

Los enlaces de fibra óptica y UTP en la red LAN de la UMSA son de 1 y 10 Gbps; al momento se tiene una saturación del 20 al 30% y se tiene la proyección de subir los enlaces interbuilding a 10 Gbps por lo que se dispone de anchos de banda sumamente ociosos lo que desemboca en la inexistencia de la necesidad de aplicar políticas de configuración de calidad de servicio.

5.10 CUMPLIMIENTO DE ESTANDARES NACIONALES E INTERNACIONALES

La implementación de redes basadas en el protocolo IPv6 está regida internacionalmente por el RFC 2460, referida de la siguiente manera:

```
Network Working Group                                          S. Deering
Request for Comments: 2460                                          Cisco
Obsoletos: 1883                                                R. Hinden
Categoría: Track de Estándares                                     Nokia
                                                          Diciembre 1998


                          Especificación
                Protocolo Internet, Versión 6 (IPv6)
```

El RFC 2460 en detalle se puede revisar en (ANEXO 14).

El RFC 8200 respecto a la estandarización del protocolo IPv6, referida de la siguiente manera:

```
Internet Engineering Task Force (IETF)                         S. Deering
Request for Comments: 8200                                        Retired
STD: 86                                                        R. Hinden
Obsoletes: 2460                                    Check Point Software
Category: Standards Track                                      July 2017
ISSN: 2070-1721


Internet Protocol, Version 6 (IPv6) Specification
```

El RFC 8200 en detalle se puede revisar en (ANEXO 15).

A nivel nacional se revisaron los repositorios http://www.gacetaoficialdebolivia.gob.bo/, sitio oficial de publicación de leyes del Estado Plurinacional de Bolivia y https://www.att.gob.bo/ sitio oficial de la Autoridad en Transportes y Telecomunicaciones del Estado Plurinacional de Bolivia y no se encontraron normativas relacionadas con la implementación del protocolo IPv6 en Bolivia.

5.11 SIMULACION DE LA RED

Considerando la magnitud de la red de la UMSA, y los beneficios que se quiere lograr a nivel de servidores con las funcionalidades de la aplicación de direcciones Anycast de IPv6, por lo que se utilizó el simulador Packet Tracer de Cisco, donde se muestra la simulación de tres routers donde dos ellos Router1 y Router2 publican simultáneamente la subnet anycast 2001:23::/64, y el Router0 puede acceder a cualquiera de esos dos destinos, por lo que en condiciones normales se tiene disponible los servidores 0 y 1, como se muestra en la siguiente gráfica:

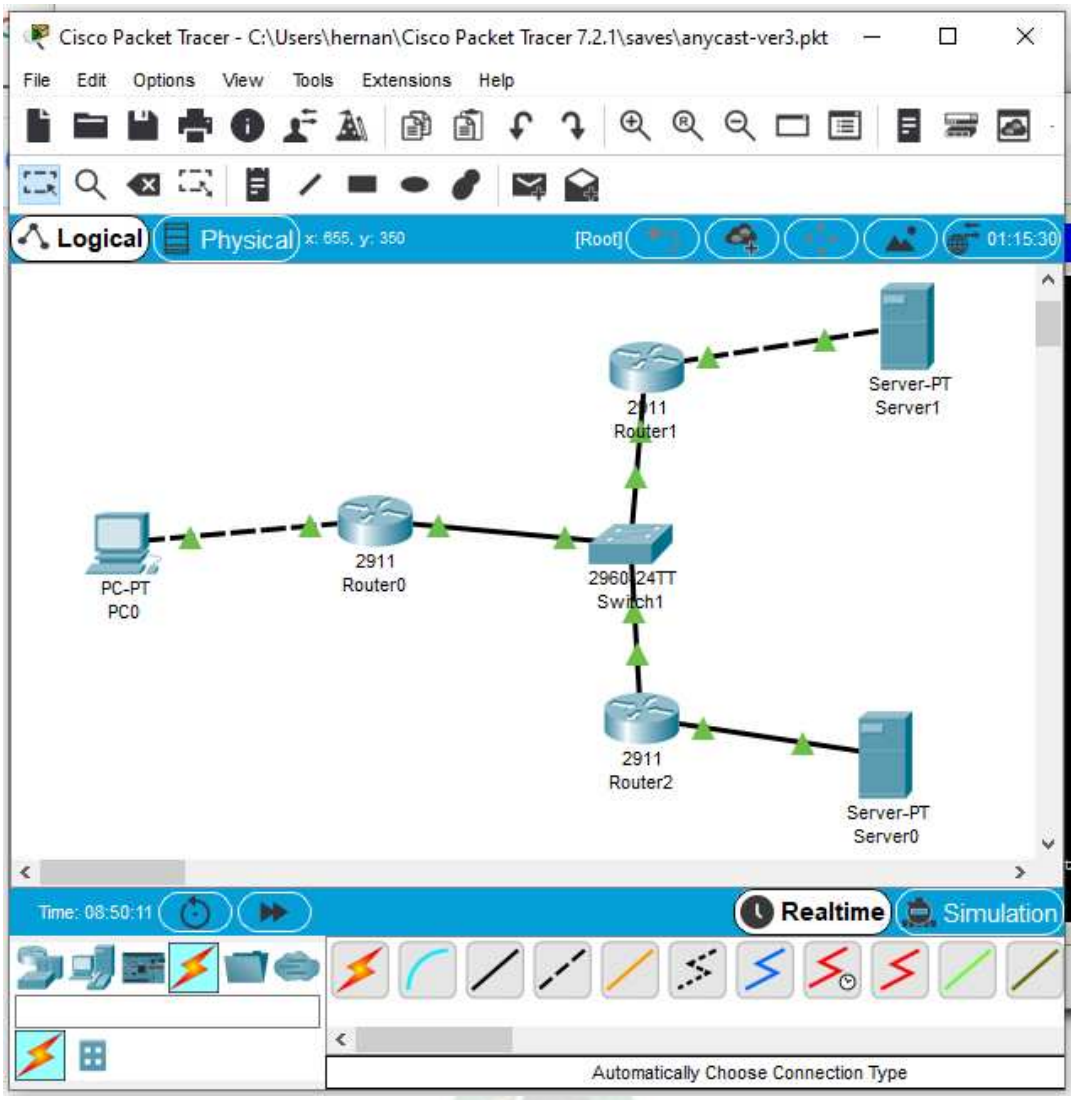


Figura 5.4: Esquema de funcionamiento direcciones IPv6 Anycast.

Código de configuración de las interfaces involucradas del Router 1:

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:22::2/64
ipv6 ospf 1 area 2
!
interface GigabitEthernet0/1
no ip address
duplex auto
```

```
speed auto
ipv6 address 2001:23::1/64 anycast
ipv6 ospf 1 area 2
```

Código de configuración de las interfaces involucradas del Router 2:

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
ipv6 address 2001:22::3/64
ipv6 ospf 1 area 2
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2001:23::1/64 anycast
ipv6 ospf 1 area 2
```

Salida del comando show ipv6 router del Router 1

```
R1#sh ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C       2001:22::/64 [0/0]
             via GigabitEthernet0/0, directly connected
L       2001:22::1/128 [0/0]
             via GigabitEthernet0/0, receive
O       2001:23::/64 [110/2]
             via FE80::20B:BEFF:FE4B:8801, GigabitEthernet0/0
             via FE80::260:2FFF:FEA5:5201, GigabitEthernet0/0
C       2001:24::/64 [0/0]
             via GigabitEthernet0/1, directly connected
L       2001:24::1/128 [0/0]
             via GigabitEthernet0/1, receive
L       FF00::/8 [0/0]
             via Null0, receive
```

Donde se puede observar que para la red 2001:23::/64 se dispone de dos destinos:

via FE80::20B:BEFF:FE4B:8801, GigabitEthernet0/0
via FE80::260:2FFF:FEA5:5201, GigabitEthernet0/0

Considerando la magnitud de la red de la UMSA, se presenta un modelo de esquema de red simplificada en cuanto a la cantidad de dispositivos de red pero no así en cuanto a los dispositivos que debe atravesar el tráfico de un usuario final tanto para llegar a los servidores como hacia Internet, como se muestra en la siguiente gráfica.

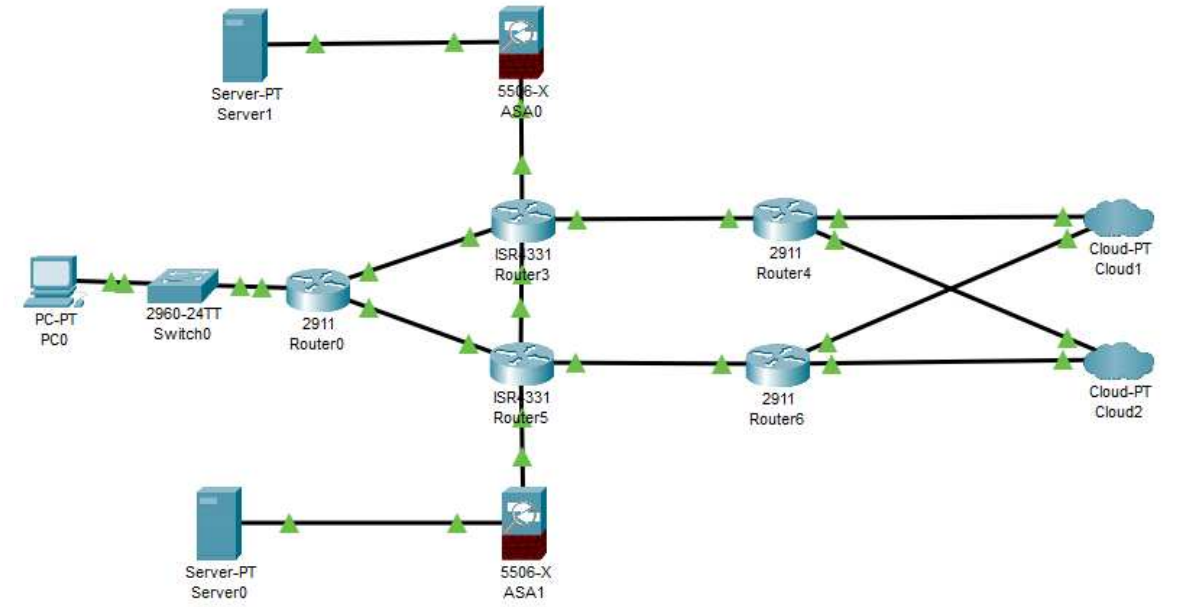


Figura 5.5: Esquema de funcionamiento de la red de la UMSA.

5.12 IMPLEMENTACIÓN DEL PLAN DE LA ESTRATEGIA DE TRANSICIÓN EN LA RED INALAMBRICA

A nivel de usuarios finales se dispone de dos medios de conectividad para el acceso a la red local, inalámbrica y cableada, siendo la solución inalámbrica basada en acceso protegido empresarial EAP/802.1X para la autenticación de usuarios (docentes, estudiantes y administrativos), y la asignación de ip se realiza a nivel MDF (Switch multicapa de edificio), mediante una configuración del tipo DHCPv6 - STATELESS IPV6 (SLAAC) configuradas a las Vlans correspondientes como se muestra en la siguiente configuración:

Configuración STATELESS:

…….
ipv6 dhcp pool WIFI6
 dns-server 2801:104:8::8
 domain-name UMSA.BO
…….

Configuración en la Vlan correspondiente a los usuarios finales:

…….

```
interface VlanXX
 description VLAN-CLIENTES-WIFI
 ip address 172.24.56.1 255.255.248.0
 ipv6 address 2801:104:40::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server WIFI6
…….
```

Como protocolo de enrutamiento dinámico se utilizó OSPF, como se observa en la Vlan correspondiente a los usuarios finales:

```
…….
interface VlanXX
 description VLAN-CLIENTES-WIFI
 ip address 172.24.56.1 255.255.248.0
 ipv6 address 2801:104:40::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server WIFI6
 ipv6 ospf 1 area 0

ipv6 route ::/0 2801:104:C0:4::1
ipv6 router ospf 1
 router-id 6.6.6.6
 log-adjacency-changes
…….
```

El enrutamiento de tráfico para la salida a Internet, se aplicó en el enrutador asignado como “de borde”, con el uso del protocolo BGP mediante las siguientes configuraciones:

```
…….
set protocols bgp 27828 address-family ipv6-unicast network '2801:104:40::/44'
set protocols bgp 27828 address-family ipv6-unicast network '2801:104:c0::/48'
set protocols bgp 27828 neighbor 200.58.73.32 ebgp-multihop 255
set protocols bgp 27828 neighbor 200.58.73.32 remote-as 27839
set protocols bgp 27828 neighbor 200.58.73.32 soft-reconfiguration inbound
set protocols bgp 27828 neighbor 200.58.73.32 update-source 200.58.73.33
set protocols bgp 27828 neighbor '2803:9400:1:e::1' address-family ipv6-unicast
set protocols bgp 27828 neighbor '2803:9400:1:e::1' ebgp-multihop 255
set protocols bgp 27828 neighbor '2803:9400:1:e::1' remote-as 27839
set protocols bgp 27828 neighbor '2803:9400:1:e::1' soft-reconfiguration inbound
set protocols bgp 27828 neighbor '2803:9400:1:e::1' update-source '2803:9400:1:e::2'
…….
```

Configuraciones que permiten el funcionamiento del servicio de red inlamabrica (WiFi) en cerca de 30 predios de la UMSA a dispositivos móviles y portátiles de usuarios finales en la modalidad dual siendo una solución totalmente funcional y con la aclaración de que en Internet se prioriza el tráfico IPv6 sobre el tráfico IPv4.

5.13 PLAN DE IMPLEMENTACIÓN IPV6

Considerando la envergadura de la red de la UMSA y la cantidad de usuarios, se plantea una primera fase con alcance en el servicio de WiFi Institucional y generación de los procedimientos para el área de la red cableada y servidores; y desarrollo del plan de numeración de IPv6 en las tres áreas.

Se propone desarrollar los pasos que permitirán que se puedan realizar al menos las siguientes funciones, sin comprometer la capacidad de IPv4 o seguridad de la red:

- Transmitir tráfico IPv6 de Internet y pares externos a través del backbone y, a la LAN.
- Transmitir tráfico IPv6 de la LAN, a través del backbone, a Internet y pares externos.
- Transmitir tráfico IPv6 de la LAN, a través del backbone, a otra LAN (u otro nodo en la misma LAN).

Una implantación tipo consiste de las siguientes etapas:

- 1) IPv6 de planificación de transición (Cubierta por este proyecto)
- 2) la creación de redes y la infraestructura
- 3) configuración de dispositivos de red
- 4) configuración de la seguridad de red IPv6
- 5) los pilotos, pruebas y demostraciones
- 6) migración de hosts
- 7) desarrollo de normas de uso
- y 8) la formación

CRONOGRAMA DE IMPLEMENTACION

		TIEMPO ESTIMADO EN SEMANAS			
NRO. DE TAREA	DESCRIPCION DE TAREAS	1°	2°	3°	4°
1	Conf. y pruebas en equipos Core y borde	X			
2	Conf. y pruebas en equipos capa de distribución	X			
3	Conf. y pruebas en equipos capa de acceso		X		
4	Conf. y pruebas a los equipos de firewall (DMZ)		X		
5	Conf. y pruebas de servicios básicos de red			X	
6	Conf. y pruebas de asignación de ancho de banda			X	
7	Conf. de equipos de usuarios finales en Ed. Hoy				X
8	Conf. de equipos de usuarios finales en Monoblock				X
9	Conf. de equipos de usuarios finales en Cota Cota				X

Tabla 5.7: Cronograma de implantación de IPv6 en la UMSA en el servicio Inalámbrico (WiFi).

5.14 PROBABLES AMENAZAS EN EL PROCESO DE TRANSICIÓN A IPV6

Dentro de la factibilidad se consideran las siguientes amenazas:

- Complejidad del uso del protocolo IPv6: El personal del DTIC, sobre todo quienes trabajan en la unidad de nodo Internet son los que se involucran en el trabajo con el nuevo protocolo, a pesar de que el personal TIC de la Universidad tiene experiencia con el

manejo de IPv4, IPv6 implica que el personal tenga más conocimientos y capacidad para poder administrar ambos protocolos durante el periodo de coexistencia entre ambos protocolos y solamente IPv6 cuando se implemente de forma nativa.

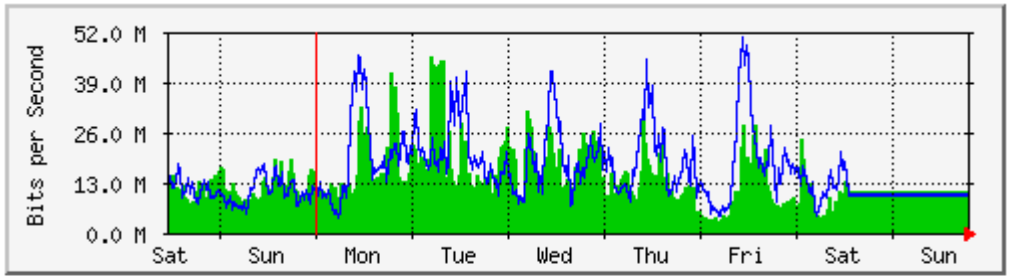
- Resistencia al cambio: En este proyecto la resistencia a usar el nuevo protocolo es inexistente ya que el nuevo protocolo está pensado principalmente para el uso del usuario final, la transición al nuevo protocolo se efectúa de forma transparente; el usuario final no experimenta ninguna dificultad para acceder a las mismas aplicaciones y servicios que accede normalmente con el nuevo protocolo. En algunos casos si el usuario experimenta problemas al usar los servicios el personal de soporte del DTIC o TIC Facultativo correspondiente es el encargado de ayudarlo para solucionar los mismos.
- Rapidez de la migración: IPv6 puede introducir cambios demasiado rápidos para permitir al personal adaptarse a él y aceptarlo, mientras que para los usuarios la transición es transparente, una aplicación rápida de este protocolo en toda la red puede ocasionar fallos en el funcionamiento de la red que a su vez puede ocasionar inestabilidad en los servicios que ofrece la UMSA, por esta razón el plan de migración se contempla en un periodo temporal que se considera suficiente y amplio para implementar el protocolo, se debe recordar que no hay una fecha de finalización impuesta para migrar todas las redes de IPv4 a IPv6 por lo que la migración puede realizarse ahora, o en un futuro cercano, además el mecanismo de transición elegido que es Stack Doble permite el despliegue progresivo de IPv6 en la red, pudiendo de esta forma implantarlo de forma parcial en algunos nodos primero e ir aplicando Stack Doble a toda la red paulatinamente sin estar limitados a implantar el nuevo protocolo en un determinado tiempo.
- Obsolescencia: La implantación de una tecnología que en la práctica pueda considerarse obsoleta en poco tiempo es impráctico, pero en este caso la aplicación de IPv6 no implica que vaya a ser un protocolo obsoleto en poco tiempo, IPv6 recién empezó hasta hace unos años, su despliegue a nivel mundial y es más está diseñado de tal forma que no se tenga que realizar otra actualización del protocolo de Internet en cientos de años debido a sus características que lo hacen flexible, seguro, estable y con capacidad de añadir una cantidad prácticamente infinita de nuevos usuarios con su respectiva dirección. Por lo que el problema de obsolescencia es prácticamente irreal.

Considerando que los aspectos anteriores se considera que el actual proyecto es factible operativamente.

5.15 MONITOREO DEL TRÁFICO IPV6 Y VALIDACION DE IPV6 VS. IPV4

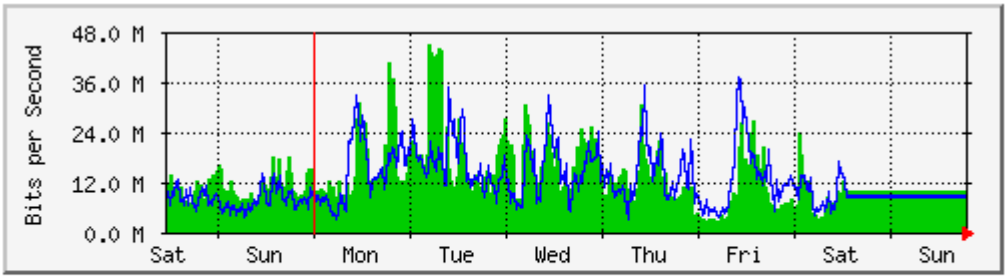
La red de datos de la Universidad Mayor de San Andrés cuenta con sistemas de monitoreo que permite dar seguimiento al tráfico de datos tanto del tipo IPv6 como IPv4, herramientas como Cacti, Prometheus, MRTG y Exinda, este último tiene la función primaria de la administración del ancho de banda contratado a los proveedores del servicio y que además cuenta con el servicio de monitoreo.

El proveedor del servicio de Internet, debe contar con el sistema de monitoreo con la finalidad de disponer de una herramienta para el seguimiento del ancho de banda contratado, como se muestra en la siguiente gráfica:



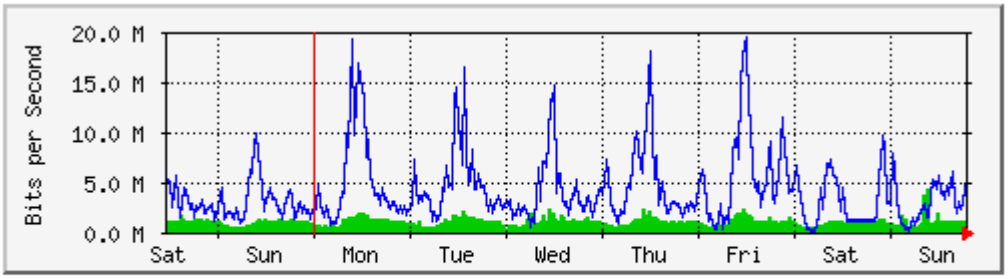
	Max	Average	Current
In	45.3 Mb/s (0.1%)	13.6 Mb/s (0.0%)	10.5 Mb/s (0.0%)
Out	50.1 Mb/s (0.1%)	15.8 Mb/s (0.0%)	9648.4 kb/s (0.0%)

Figura 5.6: Consumo total de ancho de banda de Internet de una semana.



	Max	Average	Current
In	44.8 Mb/s (0.4%)	12.6 Mb/s (0.1%)	9624.9 kb/s (0.1%)
Out	36.6 Mb/s (0.4%)	12.0 Mb/s (0.1%)	8605.6 kb/s (0.1%)

Figura 5.7: Consumo de tráfico IPv4 de Internet en una semana.



	Max	Average	Current
In	4325.9 kb/s (0.0%)	1035.9 kb/s (0.0%)	1145.4 kb/s (0.0%)
Out	19.2 Mb/s (0.2%)	4079.1 kb/s (0.0%)	4365.6 kb/s (0.0%)

Figura 5.8: Consumo de tráfico Ipv6 de Internet en una semana.

Como se verá se cuenta con las herramientas tecnológicas para el monitoreo de tráfico hacia Internet, tanto bajo el protocolo IPv4 como IPv6 y el total, herramientas que proveen las estadísticas de seguimiento, considerar también, que, cuando se implemente el protocolo IPv6 en la integridad de la red, a nivel de red cableada, inalámbrica y área de servidores se podrá disponer de un panorama fidedigno del tráfico hacia Internet clasificado en el protocolo IPv4 e IPv6.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

i. Se logró evaluar los distintos equipos y componentes de la actual infraestructura de red, con el objetivo de determinar los cambios a efectuar antes de iniciar el proceso de migración, donde se definió conservar la actual infraestructura realizando previamente actualizaciones al software de los activos de la Universidad.

ii. Mediante el análisis de los mecanismos de migración explicados, se estableció la mejor alternativa de migración para el caso de la UMSA, en base al diagnóstico realizado de la infraestructura de la red actual.

iii. Se propone un diseño para la nueva infraestructura de la red de servicios Intranet que será replicada al resto de servicios de Internet de la Universidad, creando un nuevo plan de numeración, verificando la disponibilidad del proveedor de servicios y las nuevas configuraciones a aplicar en los equipos considerando además que por tratarse de la migración de un ISP esta debe ser transparente para el usuario en todo momento.

iv. Se ha realizado el análisis y diseño de un plan de migración a IPv6 progresivo e integral para el ISP local en la UMSA, tomando en cuenta los periodos de tiempo más apropiados para efectuar la migración y asignando tareas a las distintas unidades TIC de la Universidad.

6.2 RECOMENDACIONES

v. La transición de Stack Doble permite la implementación por etapas en la red donde se aplique, se recomienda implementar los nodos dobles de forma progresiva comenzando por el núcleo de la red hasta expandirse a los puntos de distribución del usuario final. Este método es fundamental para la migración a IPv6.

vi. Aunque la Prueba de Concepto se ha realizado utilizando un Tunnel Broker y NPTv6, esto no es recomendable en un entorno de producción y se requiere configurar IPv6 BGP en el upstream del ISP.

vii. Se debe implantar RPKI en la publicación de prefijos IPv6.

viii. La UMSA debe adscribirse a un RIR para la gestión de publicación de sus prefijos en Internet mediante BGP.

ix. La implementación de servicios DHCP y DHCPv6 conjuntamente con agregación de prefijos permite el uso de mecanismos de autoconfiguración en los equipos de red y usuario final, al utilizarlos es posible desplegar la red más rápidamente. Sobre esto se requiere un dimensionamiento más acorde. Siendo que IPv6 orienta la red a un sistema globalmente jerárquico, es posible que los DNS deban estar distribuidos, para lo cual se debe implantar servidores locales de servicios de red en cada predio.

x. El tráfico de IPv6 sumado al tráfico de IPv4 puede crear sobrecargas en los componentes de red, es necesario obtener mediciones sobre el tráfico para determinar cambios en el ancho de banda empleado en cada enlace en caso de percibir retrasos y saturaciones.

xi. Es uno de los hitos en este proyecto proveerle conectividad de red a los usuarios del servicio WiFi, que actualmente opera con NAT444, situación que provoca retardos en la comunicación de los usuarios, que han tenido un crecimiento exponencial.

xii. Se debe programar talleres de capacitación y socialización al interior de la UMSA, siendo primordialmente necesario en el DTIC y en los TIC's de cada Facultad.

xiii. Asegurar que el personal TIC inmiscuido en el proceso de migración cuente con conocimientos suficientes acerca del nuevo protocolo IPv6, lo cual es fundamental para el desarrollo del proyecto, de no ser así es muy probable que la red no funcione correctamente.

GLOSARIO

- **CONMUTADOR** (en ingles "switch") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*).
- **DESIE** División de Sistemas y Estadistica.
- **DTIC** Departamento de Tecnologías de Información y comunicación
- **ENRUTADOR** es un dispositivo físico de red que facilita y establece una conexión entre una red local e Internet pasando información a y desde las redes de conmutación de paquetes.
- **PROTOCOLOS DE RED** Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.
- **MOVILIDAD IP** es la provisión de conectividad a Internet a dispositivos móviles inalámbricos, e incluso, que permanezcan conectados mientras se mueven, y los mismos tienen soporte IP.
- **MULTIHOMMING** se define como la conexión de un AS a más de un ISP a la vez. La forma más común de implementar multihoming es obtener un bloque de direcciones independientes del proveedor junto con un número de sistema autónomo (ASN) y anunciar el bloque de direcciones vía BGP a cada uno de los ISPs a los que se está conectado.
- **IPS** en inglés Internet Service Provider, es la empresa que brinda conexión a Internet a sus clientes.
- **WiFi** en inglés Wireless Fidelity, que significa fidelidad sin cables o inalámbrica, que comprende un conjunto de estándares para redes inalámbricas basados en las especificaciones IEEE802.11, lo cual asegura la compatibilidad e interoperabilidad en los equipos certificados bajo esta denominación.
- **BROADCAST** es la difusión amplia, difusión ancha o broadcast, es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.
- **CHECKSUM** permite la verificación de los datos que se envían a través de las tramas de TCP/IP. Si el 'checksum' que se genera al leer los datos no coincide con el que hay grabado al final, normalmente significa que ha habido un error de lectura. El 'checksum' es rápido de calcular, es transparente a la pérdida de bits (rotación de octetos aparentes de datos) y es efectivo ante los grupos de bits a ceros o a unos. Parecido al CRC.

- **IANA** en inglés Internet Assigned Numbers Authority, es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.
- **ARIN** en inglés American Registry for Internet Numbers, es el Registro Regional de Internet para América Anglosajona, varias islas de los océanos Pacífico y Atlantico.
- **RIPE** en francés Réseaux IP Européens Network Coordination Centre, es el Registro Regional de Internet para Europa, Oriente Medio y países del Asía Central.
- **APNIC** en inglés Asia pacific Network Information Centre, es el Centro de Información de Red de Asía y el Pacífico.
- **LACNIC** en inglés latin America & Caribbean Network Information Centre, es la entidad de Registro de Direcciones de Internet para Latinoamerica y el Caribe.
- **AfriNIC** en inglés African Network Information Centre, es la entidad de Registro Regional de Internet para África.
- **LOOPBACK** es una interfaz virtual cuyas direcciones IPv4 corresponden a al rango "127.0.0.0/8".
- **DNS** en inglés Domain Name System, es servidor encargado de traducir los nombres de dominio en direcciones númericas que las maquinas entienden.
- **HTTP** en inglés Hypertext Transfer Protocol, es el protocolo que permite las transferencias de información en la Internet.
- **MTU** en inglés Maximum Transmission Unit, es el tamaño máximo de los paquetes IP que se puede enviar a Internet.
- **CIDR** en inglés Classless Interdomain Routing, es el enrutamiento entre dominios sin clase que permite una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas.
- **AS** es un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de ruteo.
- **BACKBONE**, se denomina así a las conexiones troncales de Internet, las principales redes de comunicación que se encargan de conectar al resto de las redes.

BIBLIOGRAFÍA

Stallings, W. (2004). Comunicaciones Y Redes De Computadores 7 "Séptima" Edición.
Ubicación: Pearson Alhambra.

Archiex, J (2017). IPv6 Principios e implementación. 1 “Primera” Edición.

Cicileo G, (2009). IPv6 para Todos. 1 “Primera” Edición.

Acosta, A. (2014) IPv6 para operadores de redes. 1 “Primera” Edición.

Tanenbaum, A. (2003).Redes De Computadoras 4 "Cuarta" Edición.

Salsano, S.Listanti, M. &Sangregorio, E. (2003). COPS DRA: a protocol for dynamic Diffserv Resource Allocation.

Vázquez Gallo, E. (2007). Caracterización de Nuevos Servicios de Telecomunicaciones, 2006.
Recuperado de: http://www.dei.inf.uc3m.es/jspTSI2007/resumenes/TSI2005-07306-C02.pdf

Boyle, J.&Cohen, R.(2000). RFC 2748 (rfc2748) - The COPS (Common Open Policy Service) Protocol
Recuperado de : http:// www.faqs.org/rfcs/rfc2748.html

ANEXO 1

Salida del comando ip addr show de una instalación inicial de un sistema operativo Linux Debian:

root@usuario:~# ip addr show

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:05:a8:7a brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.133/24 brd 192.168.5.255 scope global dynamic noprefixroute ens33
       valid_lft 1340sec preferred_lft 1340sec
    inet6 fe80::20c:29ff:fe05:a87a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

ANEXO 2

Detalle del archivo /etc/NetworkManager/system-connections/Wired connection 1 de una instalación inicial de un sistema operativo Linux Debian:

```
[connection]
ip= Wired connection 1
uuid=140e4f35-c3ab-41e3-893e-6231ab55a2dd

[type=802–3–ethernet]

[ipv4]
method=auto

[ipv6]
method=auto
ip6-privacy=2
```

ANEXO 3

Detalle del archivo /etc/NetworkManager/system-connections/Wired connection 1 luego de la configuración de la interfaz de red de un sistema operativo Linux Debian:

/etc/NetworkManager/system-connections/Wired connection 1

```
[connection]
id=Wired connection 1
uuid=140e4f35-c3ab-41e3-893e-6231ab55a2dd
type=ethernet
permissions=
timestamp=1582807479

[ethernet]
mac-address-blacklist=

[ipv4]
address1=200.7.162.68/27,200.7.162.65
dns=198.18.19.20;
dns-search=umsa.bo;
method=manual

[ipv6]
addr-gen-mode=eui64
address1=2801:104:40:1::100/64,2801:104:40:1::1
dns=2001:4860:4860::8888;
dns-search=
ip6-privacy=2
method=manual
```

ANEXO 4

Salida del comando ip addr show luego de la configuración de la interfaz de red de un sistema operativo Linux Debian:

```
root@usuario:~# ip addr show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:87:7c:9c brd ff:ff:ff:ff:ff:ff
    inet 200.7.162.68/27 brd 200.7.162.95 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 2801:104:40:1::100/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe87:7c9c/64 scope link
       valid_lft forever preferred_lft forever
```

ANEXO 5

Salida del comando ip addr show de una instalación inicial de un sistema operativo Linux Red Hat:

```
[root@centos7 ~]# ip add show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 08:00:27:ec:d4:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global noprefixroute dynamic enp0s3
       valid_lft 7038sec preferred_lft 7038sec
    inet6 fe80::67e0:5e2e:4619:1037/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

ANEXO 6

Detalle del archivo /etc/sysconfig/network-scripts de una instalación inicial de un sistema operativo Linux Red Hat:

/etc/sysconfig/network-scripts

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
UUID=3c36b8c2-334b-57c7-91b6-4401f3489c69
```

ANEXO 7

Detalle del archivo /etc/sysconfig/network-scripts luego de la configuración de la interfaz de red de un sistema operativo Linux Red Hat:

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
UUID=3c36b8c2-334b-57c7-91b6-4401f3489c69
IPADDR=192.168.0.102
PREFIX=24
GATEWAY=192.168.0.1
DNS1=192.168.0.1
IPV6ADDR=2801:104:40:1::100/64
IPV6_DEFAULTGW=2801:104:40:1::1
DNS2=2001:4860:4860::8888
IPV6_DOMAIN=umsa.bo
```

ANEXO 8

Salida del comando ip addr show luego de la configuración de la interfaz de red de un sistema operativo Linux Red Hat:

```
[root@centos7 network-scripts]# ip add show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ec:d4:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 2801:104:40:1::100/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::67e0:5e2e:4619:1037/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

ANEXO 9

Salida del comando ip addr show de una instalación inicial de un sistema operativo Linux Ubuntu:

root@hernan:~# ip add show

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a4:a0:32 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.54/24 brd 192.168.100.255 scope global dynamic enp0s3
       valid_lft 258835sec preferred_lft 258835sec
    inet6 2800:cd0:2405:f400:a00:27ff:fea4:a032/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 3234sec preferred_lft 3234sec
    inet6 fe80::a00:27ff:fea4:a032/64 scope link
       valid_lft forever preferred_lft forever

ANEXO 10

Detalle del archivo /etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection de una instalación inicial de un sistema operativo Linux Ubuntu:

root@ubuntu:/etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection

```
[connection]
id=Ethernet connection 1
uuid=65a92a1c-016c-4ed1-a9e8-483831cc33c3
type=ethernet
permissions=

[ethernet]
mac-address-blacklist=

[ipv4]
dns-search=
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=auto

[proxy]
```

ANEXO 11

Detalle del archivo /etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection luego de la configuración de la interfaz de red de un sistema operativo Linux Ubuntu:

root@ubuntu:/etc/NetworkManager/system-connections/Ethernet connection 1. nmconnection

```
[connection]
id=Ethernet connection 1
uuid=65a92a1c-016c-4ed1-a9e8-483831cc33c3
type=ethernet
permissions=

[ethernet]
mac-address-blacklist=

[ipv4]
address1=192.168.100.54/24,192.168.100.1
dns=192.168.100.1;
dns-search=umsa.bo;
method=manual

[ipv6]
addr-gen-mode=stable-privacy
address1=2801:104:40:1::100/64,2801:104:40:1::1
dns=2001:4860:4860::8888;
dns-search=
method=manual

[proxy]
```

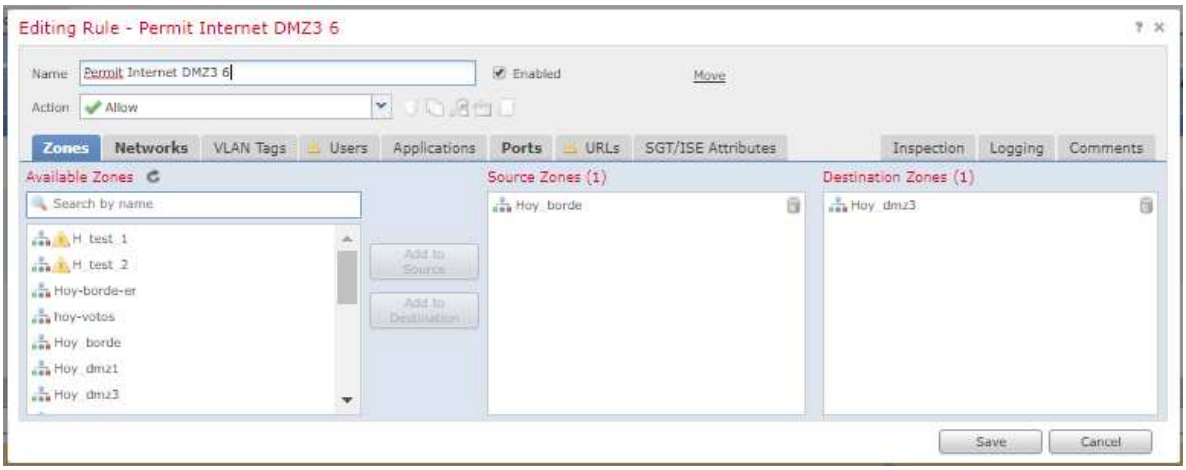
ANEXO 12

Salida del comando ip addr show luego de la configuración de la interfaz de red de un sistema operativo Linux Ubuntu:

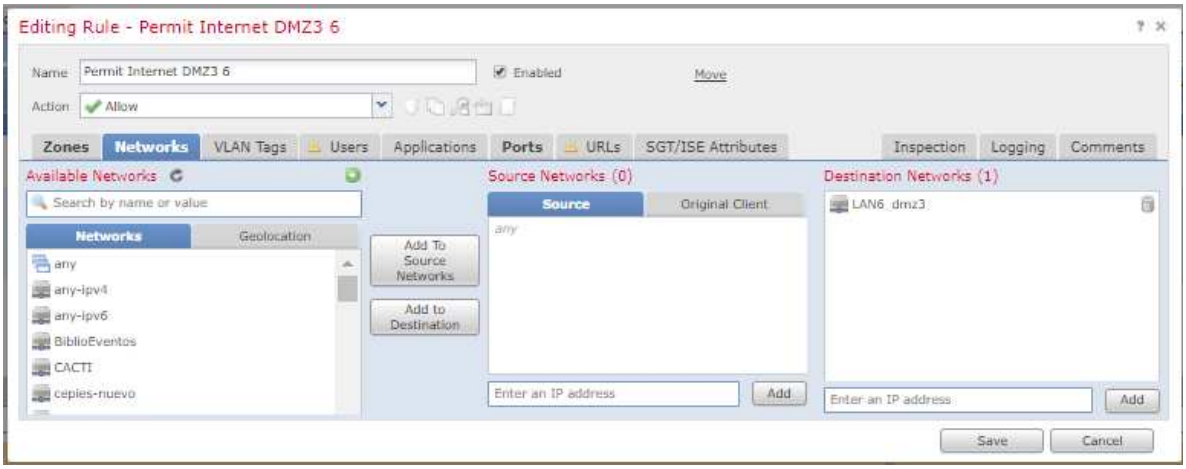
```
root@ubuntu:~# ip add show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a4:a0:32 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.54/24 brd 192.168.100.255 scope global dynamic enp0s3
       valid_lft 259065sec preferred_lft 259065sec
    inet6 2801:104:40:1::100/64 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 2800:cd0:2405:f400:a00:27ff:fea4:a032/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 3515sec preferred_lft 3515sec
    inet6 fe80::a00:27ff:fea4:a032/64 scope link
       valid_lft forever preferred_lft forever
```

ANEXO 13

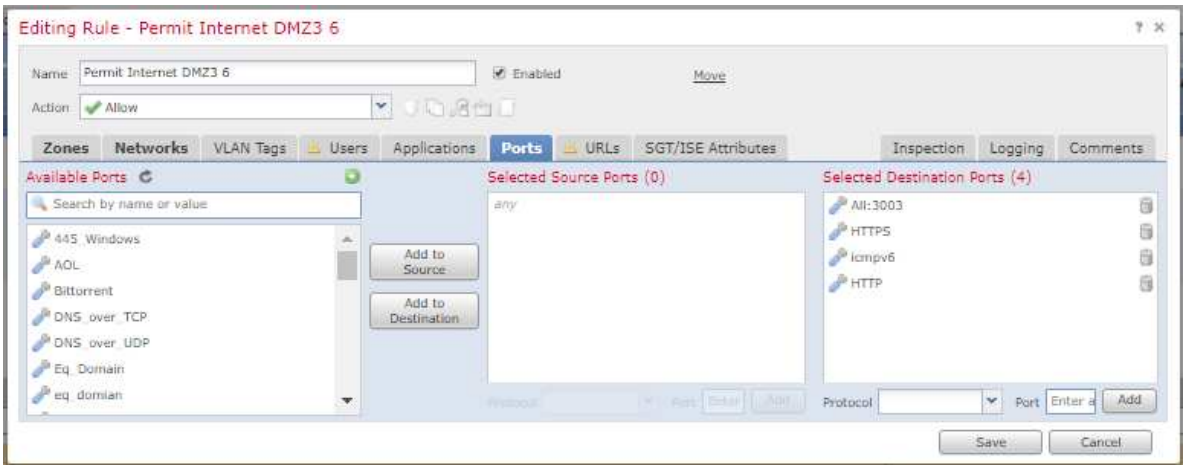
Detalle de las configuraciones del firewall, Firepower:



Detalle de las zonas involucradas en la regla.



Detalle de las redes involucradas en la regla.



Detalle de los puertos involucrados en la regla.

ANEXO 14

Detalle del RFC 2460, respecto a la implementación del protocolo IPv6:

Network Working Group — S. Deering
Request for Comments: 2460 — Cisco
Obsoletos: 1883 — R. Hinden
Categoría: Track de Estándares — Nokia
Diciembre 1998

Especificación
Protocolo Internet, Versión 6 (IPv6)

Estatus de este Memorándum

Este documento especifica un protocolo del track de estándares Internet para la comunidad Internet, y solicita debate y sugerencias para mejorías. Por favor remítase a la edición actual de los "Estándares de Protocolos Oficiales Internet" (STD 1) para el estado de estandarización y estatus de este protocolo. La distribución de este memorándum es ilimitada.

Aviso de Copyright

Resumen

Este documento especifica la versión 6 del Protocolo Internet (IPv6), algunas veces también referido como IP Siguiente Generación o IPng.

Lista de Contenidos

ANEXO 15

Detalle del RFC 8200, respecto a la estandarización del protocolo IPv6:

Internet Engineering Task Force (IETF)
Request for Comments: 8200
STD: 86
Obsoletes: 2460
Category: Standards Track
ISSN: 2070-1721

S. Deering
Retired
R. Hinden
Check Point Software

July 2017

Internet Protocol, Version 6 (IPv6) Specification

Abstract

This document specifies version 6 of the Internet Protocol (IPv6). It obsoletes RFC 2460.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8200.

Table of Contents