PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA
MAESTRÍA EN REDES DE COMUNICACIONES

SIMULACIÓN DE FUNCIONAMIENTO DEL PROTOCOLO IPV6 ENTRE UNA RED WAN Y LAN MEDIANTE EL SIMULADOR GNS3

PRIETO REYES LUIS MIGUEL

Quito, Junio 2014

ÍNDICE DE CONTENIDOS

CAPÍTULO I

1 Introducción IPv6

El protocolo IP ha sido uno de los mas exitosos protocolos a través de los tiempos de las redes, actualmente la versión IPv4 va teniendo limitaciones debido a que no ha tenido cambios substanciales desde RFC 791 en 1981. A pesar de proveer un protocolo robusto, y fácil de implementar, con el pasar de los años ha ido mostrando uno de sus más grandes problemas, el que se enfoca directamente en el número de IPs que puede proveer, al usar 32 bits da un número de combinaciones de 2^{32} los que resulta 4294967296 direcciones, que al parecer resulta un número grande, pero debido al crecimiento exitoso de Internet este número ha quedado pequeño. La solución actual sobre la limitante de la cantidad de direcciones IPs, es el protocolo IPv6 el cual maneja 128 bits por lo que resulta una cantidad aproximada 340 billones de billones de billones de direcciones IPs, solucionando el más grande problema que existe en la actualidad que es la escases de direcciones IPs.

1.1 Diferencias entre IPv4 e IPv6

Como ya se ha definido una de las mayores diferencias entre IPv4 e IPv6 es la cantidad de direcciones que pueden proveer pero además existen otras que a nivel de cabecera y estructura:

IPv4	IPV6
La longitud de dirección de origen y destino es de 32 bits.	Las direcciones de origen y destino tienen 128 bits.
IPsec es opcional.	IPsec fue creado para Ipv6 por lo tanto es requerido.
La cabecera incluye checksum para calcular la calidad del paquete.	El checksum fue removido para mejorar la velocidad de procesamiento.
La fragmentación es desempeñada por el host que envía los paquetes y el router disminuyendo el desempeño del router.	La fragmentación es desempeñada solamente por el host de envió.
El protocolo ARP usa broadcast para resolver direcciones IPv4.	El protocolo ARP es reemplazado con el protocolo ND.
Las direcciones Broadcast (255.255.255.255),son usadas para enviar tráfico a todos los nodos.	Las Direcciones multicast (FF02:1) son usadas para enviar tráfico a todos los nodos.
IPv4 necesita ser configurado manualmente o vía DHCP.	No necesita ninguna manera de configuración de IPv4, usa métodos de autoconfiguración.

La prioridad de entrega de paquetes no está presente en la cabecera IPv4.	Los routers manejan el flujo de prioridad de entrega de paquetes leyendo la cabecera en el campo de flujo.
IRDP es utilizados para determinar el mejor default gateway y es opcional.	ICMPv4 es reemplazado con ICMPv6 que envía mensajes de solicitud y anuncio.

Tabla 1.1 Comparación de IPv4 con IPv6, Autor: Luis Prieto

1.2 Estructura de IPv6

1.2.1 Formato Cabecera IPv6.

La cabecera IPv6 es más sencilla que la cabecera IPv4 y con mayor funcionalidad, además consta con un tamaño fijo de 40 bytes los cuales son ocupados por los 8 campos como se muestra en la figura.

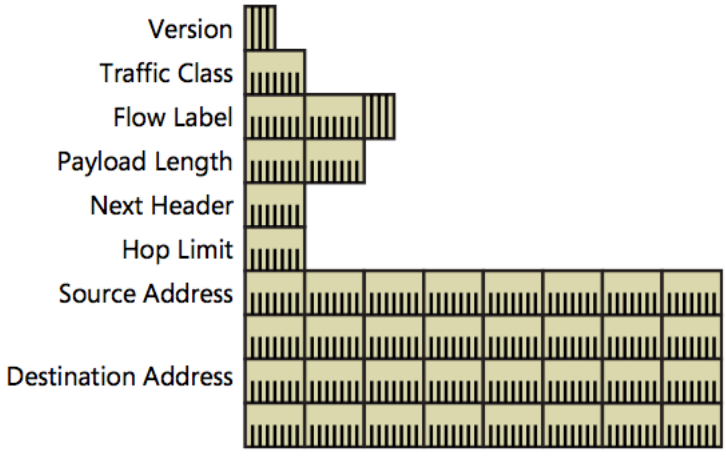


Figura1.1 Cabecera IPv6 , Fuente: Understanding IPv6, 3er Edition

- ***Versión*** Este campo indica la versión del protocola IP que se está utilizando, el espacio asignado es de 4 bits.
- ***Clase de tráfico*** Este campo indica la clase o prioridad del paquete, el tamaño de este campo es de 8 bits.
- **Campo de flujo** Indica si un paquete pertenece a una secuencia de paquetes entre el origen y el destino, son manejados por un router IPv6, usa 20 bits.
- ***Longitud del Payload*** Este campo indica el tamaño del payload del paquete es decir de la sección de paquete de datos, usa 16 bits, con este tamaño se puede usa hasta payload de hasta 65535 bytes.
- ***Siguiente cabecera*** Indica que tipo de protocolo se está usando de acuerdo a la capa del modelo en que se encuentre el paquete puede ser(TCP, UDP, ICMP)utiliza un espacio de 8 bits.
- ***Límite de saltos*** Indica el número de saltos que el paquete IPv6 puede dar antes de ser descartados, ocupa un espacio de 8 bits.
- ***Dirección de Origen*** Indica el host de origen del paquete IPv6 utiliza 128 bits.
- ***Dirección de Destino*** Indica la dirección de destino, generalmente si hay varios saltos la dirección no será la final sino la del siguiente salto.

  A continuación se muestra un ejemplo de la Cabecera IPv6:

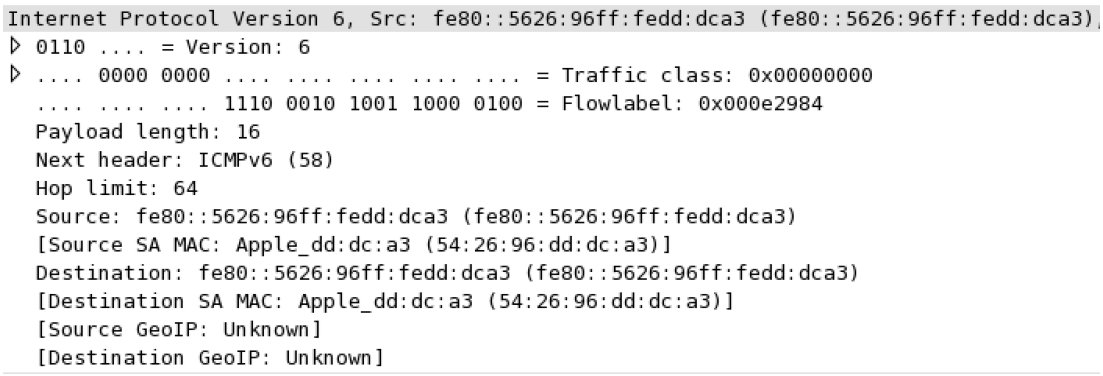


Figura1.2 Ejemplo cabecera IPv6, Autor: Luis Prieto

1.2.2 Tamaño del Paquete

Un paquete de datos IPv6 consiste en cabecera fija, cabecera de extensión y datos como se muestra a continuación:

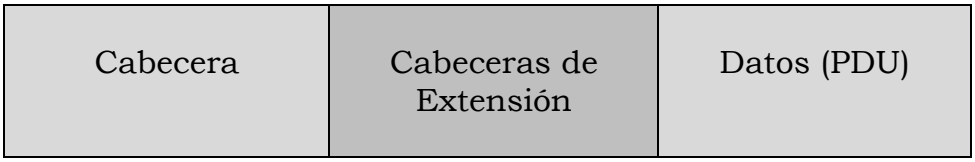


Figura1.3 Forma básica de un paquete IPv6, Autor: Luis Prieto

- *Cabecera*

  Como ya se definió la cabecera tiene un espacio fijo asignado de 40 bytes.

- *Cabeceras de extensión*

  Mueven la entrega y reenvío de paquetes, la única cabecera de extensión que es procesada por cada router es Hop-by-Hop Options, lo que mejora la velocidad de procesamiento en la cabecera, su tamaño es variable y los valores que pueden adquirir las cabeceras de extensión son:

Cabecera de Extensión	Valor
Hop-by-hop Options	0
Opciones de Destino	60
Encaminamiento	45
Fragmento	44
Autenticación	51
Encapsulación	50
Ninguna	59

Tabla 1.2 Valores de Cabecera de Extensión, Autor: Luis Prieto

- Datos PDU

  Llamado también carga útil tiene un tamaño como máximo de 60KB

1.2.3 Eficiencia

El Procesamiento IPv6 es más eficiente con relación al protocolo IPv4, a pesar de que el tamaño de los campos de dirección sea 4 veces más grande que IPv4, la cabecera solamente usa 40 bytes y es solamente 2 veces más grande con relación a la cabecera IPv4. Es decir la cabecera no ha aumentado en forma proporcional al direccionamiento, por lo que existe mayor eficiencia.

La mejoras de IPv6 son las siguientes:

- ***Ruteo más eficiente*** Debido a que IPv6 reduce el tamaño de las tablas de ruteo, el ruteo se realiza más eficientemente, los ISPs

agregan un único prefijo en las direcciones IPv6 de las redes de sus clientes, con lo que indican el acceso al internet, además la fragmentación es manejada por el equipo de origen en lugar del router, de modo que los routers pueden procesar más rápido debido a la disminución de carga.

- ***Procesamiento de paquetes más eficiente*** Al simplificar IPv6 la cabecera hace que el procesamiento de los paquetes sea más eficiente. IPv6 con relación a IPv4 no contiene campo checksum, debido a esto los routers no tienen que estar recalculando el checksum en cada salto. Eliminar este campo fue posible debido q a la mayoría de tecnologías de capa de enlace contienen capacidad de checksum de comprobación y de control de errores, además que la mayoría de capas de transporte que manejan conectividad punto punto tienen checksum para hacer esta verificación.
- ***Flujos dirigidos de datos*** IPv6 soporta multicast en vez de broadcast, el multicast permite que el flujo de paquetes sean enviados a destinatarios específicos por ejemplo la difusión multimedia, evitando que se envíen flujos de paquetes a destinatarios que no corresponden al grupo, reduciendo así el uso de ancho de banda.
- ***Configuración de red simplificada*** IPv6 integra configuración de direcciones automáticas, el router envía un prefijo de vínculo local en sus advertencias. Los host pueden generar sus propias

direcciones IP añadiendo su MAC Address de 48Bits, convertida en EUI-64, que equivale a una dirección hexadecimal de 64Bits y añade al prefijo que el router ha enviado, completando los 128 bits de la dirección válida IPv6.

- ***Soporta nuevos servicios*** IPv6 eliminó NAT debido a que ciertas aplicaciones no soportan los protocolos que utiliza NAT y las aplicaciones como video conferencia, VOIP no funcionan bien mediante NAT debido a que los protocolos como RTP y RTCP usan UDP con asignación dinámica de puertos y NAT no soporta esto. Con IPv6 se trabajara con redes Punto Punto debido a la eliminación de NAT por lo que los servicios multimedia, VOIP y calidad de servicio QoS son más robustas.
- ***Seguridad*** La seguridad es manejada por IPsec, que es un protocolo que asegura las comunicaciones sobre el Protocolo IP, autenticando y cifrando los flujos de datos. El protocolo ICMP IPv4 generalmente es bloqueado en la mayoría de empresas debido a los ataque maliciosos que existen, con ICMPv6 debido a que IPsec puede ser aplicada a los paquete ICMPv6.

1.2.4 Seguridad

La seguridad no solamente contempla solamente posibles amenazas o ataques de redes forañas, IPv6 considera también otros aspectos como los que se nombran a continuación:

- Conceptos de seguridad IT insuficientes.

- Incumplimiento de disposiciones IT
- Usurpación de derechos como robo de contraseñas
- Uso incorrecto o administración deficiente de los sistemas informáticos
- Abusos de derechos
- Debilidades en software
- Manipulación o destrucción de equipos IT
- Redes espías que duplican datos
- Troyanos, virus y gusanos
- Ataque de seguridad como enmascaramiento de IP

Estadísticas muestran que los ataque maliciosos fuera de la red son una pequeña fracción, muchos de los ataque maliciosos generalmente vienen del interior de la red, casi siempre es protagonizada por la mala conducta humana o por mala administración.

Podemos definir varios aspectos a tomar en cuenta para poder solventar el problema de seguridad:

- ***Confidencialidad*** La información almacenada o transmitida es accesible solamente para quien tenga los permisos.
- ***Integridad*** Las alteraciones de información pueden ser detectadas.
- ***Disponibilidad*** La información es accesible a usuarios autorizados.

- ***Autenticación*** Garantizar que el usuario quien accede a la información es quien dice ser.
- ***Autorización*** Dar los derechos apropiados al usuario que accede a la información.
- ***Contabilidad*** Recolección de información sobre el uso de los recursos.
- ***No rechazo*** Significa que la acción de envío, recibo o eliminación de información no puede ser denegada por ninguna de las partes involucradas

Estos requerimientos de seguridad son provistos por dos elementos:

- La encriptación que provee confidencialidad
- Checksums sumas de verificación que proveen integridad

La combinación adecuada de estos dos elementos suelen proveer autenticidad y no rechazo.

Tanto para IPv4 como para IPv6 existe IPsec que es el protocolos de seguridad que usa la combinación de algoritmos criptográficos simétricos y asimétricos.

IPsec describe un mecanismo general de seguridad que pueden ser usados tanto por IPv4 como IPv6, esto significa que IPv6 no es más seguro que IPv4, la diferencia radica que IPsec puede ser instalado separadamente en IPv4 mientras que en IPv6 es mandatorio y es parte integral dele protocolo.

IPsec define protocolos de autenticación de cabecera AH y de encapsulamiento de la cabecera de carga útil ESP, en IPv6 estas cabeceras son de cabeceras de extensión.

- ***Cabecera de Autenticación*** Esta provee integridad y autenticación para los datos transportados punto a punto, soporta varios mecanismos de autenticación, además está localizada entre la cabecera IPv6 y las cabeceras de capa superior como TCP, UDP, ICMP. Si los encabezados de extensión están presentes deben ser colocados después de las cabeceras Hop-by-hop, ruteo y fragmentación.

1.2.5 QoS

El desarrollo de IPv6 combinado con el crecimiento de la demanda de servicios en tiempo real, por lo tanto QoS calidad de servicio, ha sido una oportunidad para buscar otras soluciones, a pesar de los diferentes enfoques que existen la calidad de servicio todavía es un tema que se encuentra en investigación y hay muchas ideas en fase de desarrollo.

Los desarrolladores de IPv6 no se han enfocado en un solo mecanismo de calidad de servicio sino en tener mayor flexibilidad en los mecanismos utilizados en la calidad de servicio, a continuación se muestra las cabeceras de QoS para IPv6.

Existen dos campos para de la cabecera IPv6 que pueden ser usados para QoS y estos son:

- Traffic Class o Clase de tráfico
- Flow Label Field o Campo etiqueta de flujo

Clase de Tráfico

El los RFC se especifica un tamaño de bite para este campo y hace referencia al uso del campo DS para la clase de tráfico, en la figura se muestra como es utilizado este campo.

DSCP 6bits	ECN 2 bits

Figura1.4 Campo clase de tráfico, Autor: Luis Prieto

Se asignan los 6 bits mas significantes para DSCP dentro del campo DS y es usado para el PHB Per hop Behavior que especifica la política y prioridad aplicada. Existen 64 diferentes códigos especificados los que son divididos en 3 partes:

Pool	Código	Política
1	xxxxx0	Uso estándar
2	xxxx11	Uso experimental/ uso local
3	xxxx01	Experimental/ Uso Local/ uso futuro

Tabla 1.3 Tabla códigos QoS, Fuente: IPv6 Essentials, 2nd Edition

Los PBH especifican como los paquetes deben ser reenviados, por defecto este campo se usa 00000000, este código es provisto por el

router. Este PBH se define como best–effort, es decir los paquetes son reenviados sin ninguna política de prioridad, en otras palabras se deben entregar estos paquetes lo más pronto posible, basados en los recursos del router, los códigos para PBH son asignados por IANA y son en total 64, se pueden encontrar en http://www.iana.org/assigments/phdbis-codes. Los siguientes 2 bits proporcionan cuatro posibles puntos de congestión de 00 a 11, con el uso de estos códigos el router puede señalar sobrecarga antes de que exista pérdida de paquetes.

Campo de flujo

Los 20 bits asignados en la cabecera para este campo son utilizados para etiquetar a los paquetes y que el router les de un tratamiento especial, tales como QoS no predeterminados. Una etiqueta de flujo se le asigna a un flujo por nodo origen, entre el emisor y receptor puede haber varios flujos activos que intercambian paquetes sin necesidad e tener QoS, las etiquetas son elegidas aleatoriamente de la gamma 000001 FFFFF y se usarán como una clave a los routers para la búsqueda adecuada de un estado asociado al flujo.

1.2.6 Compatibilidad entre IPv4 e IPv6

La compatibilidad entre IPv4 e IPv6 se da debido a que el cambio a IPv6 es gradual y debe pasar un proceso de transición hasta que todos los equipos sean IPv6, a pesar de que esto es muy difícil que

pase ya que por muchos años se utilizarán estas tecnologías conjuntamente, para esto se definen dos mecanismos básicos:

- Dual Stack o Doble Pila que provee el soporte completo para IPv4 e IPv6, donde los nodos tienen la habilidad de enviar y recibir paquetes de los dos protocolos, los que son llamados nodos IPv6/IPv4, para que esto sea posible se necesita routers o nodos que manejen estas dos tecnologías, lo que no es una solución muy económica el momento de hacer la implementación.

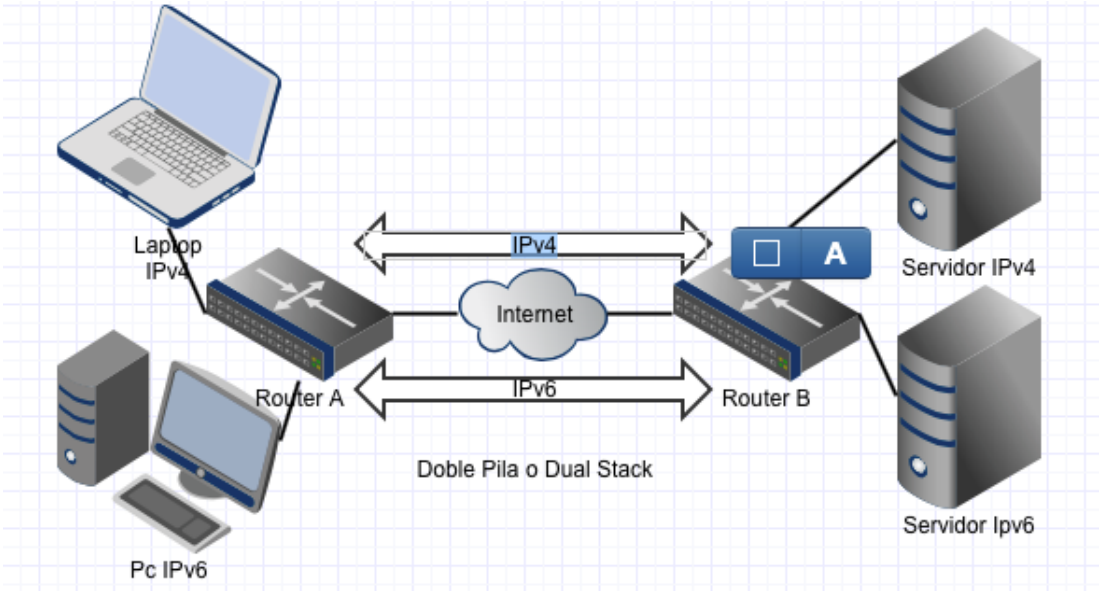


Figura1.5 Ejemplo de flujo Doble Pila o Dual Stack, Autor: Luis Prieto

Los paquetes pueden ser enviados desde los terminales tanto IPv4 como IPv6 son soportados por los routers por lo que comparten el mismo medio y son enviados desde router A a Router B o viceversa, estos se encargan de entregar a sus

destinatarios, así es como funciona la doble pila y permite que las dos tecnologías existan e interactuen.

- Tunneling o Túneles los que encapsulan los Paquetes IPv6 en IPv4 para ser transportados dentro de una infraestructura IPv4 Estos mecanismos son usados por los host y routers IPv6 que necesitan interactuar con IPv4, lo que se hace es construir un enlace virtual llamado túnel, existen túneles configurados o automáticos.

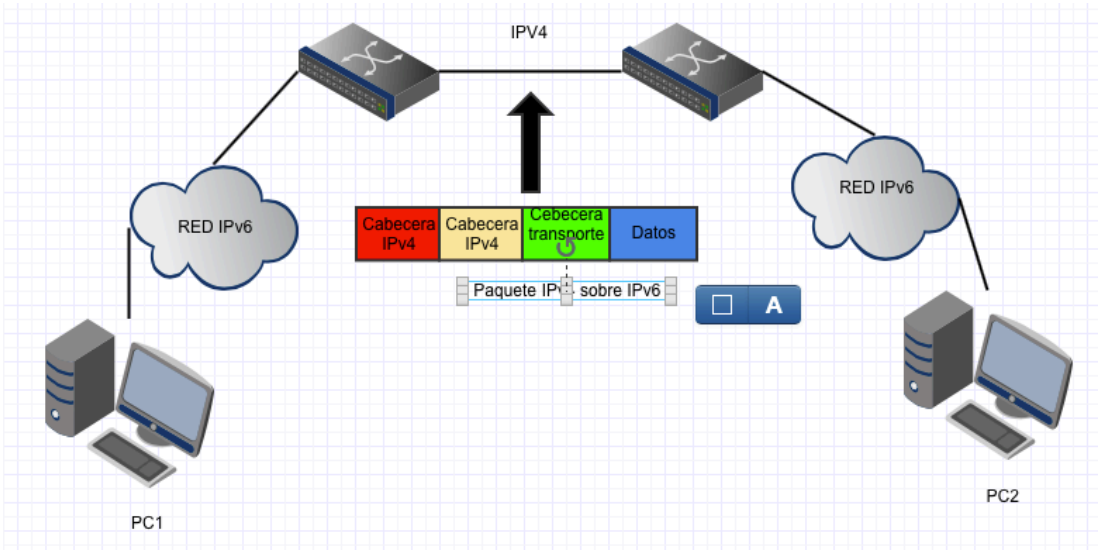


Figura1.6 Ejemplo de Túneles, Autor:Luis Prieto

CAPÍTULO II

2 Direccionamiento IPv6

El principal propósito de IPv6 es justamente incrementar la cantidad de direcciones, para eso se logró está nueva versión IP que es cuatro veces mas grande que IPv4. IPv6 está conformado de 128 bits, 2^{128}, para tener una idea de cuantas direcciones nos referimos sería aproximadamente 6,65 x 10^{23} direcciones por metro cuadrado de superficie en la tierra.

El uso de 128 bits permite múltiples niveles de jerarquía, flexibilidad en diseño de direcciones unicast y ruteo, lo que es una carencia de IPv4.

Los 128 bits distribuidos 64 bits para prefijo de la subred, que son suficientes para satisfacer los requerimientos de direcciones de los proveedores de internet (ISPs) entre tu organización, el backbone de internet, los 64 bits siguientes son usados como identificador de interface, que permite la identificar un host en la red.

2.1 Sintaxis de las Direcciones IPv6

Los 128 bits son divididos en bloques de 16 bits y cada bloque de 16 bits es convertido en 4 números dígitos hexadecimales y separados por dos puntos.

La forma binaria para IPv6 sería:

1111111011011100 1011101010011000 0111011001010100 0011001000010000

1111111011011100 1011101010011000 0111011001010100 0011001000010000

Convertido a formato Hexadecimal obtendríamos la siguiente dirección:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

Dentro de los bloques de 16 bits pueden existir únicamente ceros de este modo 1080:0000:0000:0000:8:800:200C:417A estos se puede abreviar únicamente dejando un cero

1080:0:0:0:8:800:200C:417A

En caso de que existan varios grupos de ceros conjuntos se los puede abreviar con el símbolo "::" de tal manera que la dirección quedará de la siguiente manera:

1080::8:800:200C:417A

A esto se le denomina compresión de ceros.

2.1.1 Prefijos IPv6

La manera de utilizar prefijos en Ipv6 es similar a la de IPv4 utilizando la CIDR, generalmente usada para determinar la subredes, interface que pertenece o rutas sumarizadas la notación usada para los prefijos es de la siguiente manera:

dirección/ lonjtud de prefijo.

La longitud del prefijo es cuantos bits más lejanos de la izquierda de la dirección son especificados para el prefijo, es decir, contando desde la izquierda a derecha los bits se especifica el número del prefijo.

La rutas sumarizadas encapsulan la red con un prefijo por ejemplo:

1111:2222:3333::/48

Esta dirección indica que los primeros 48 bits de la dirección equivalen a la red, y si queremos usar 16 bits para subredes, tendremos que el prefijo cambia a

1111:2222:3333::/64

donde el 64 nos indica las redes contenidas en la ruta sumarizada.

2.2 Tipos de Direcciones

Existen tres tipos de direcciones:

- **Unicast** Identifica la interface de un nodo IPv6, el paquete enviado a una dirección unicast es entregado a la interface que es identificada por la dirección.
- ***Anycast*** Se asignan múltiples interfaces, el paquete que se envía se entrega solo una de las interfaces generalmente a la más cercana.
- ***Multicast*** El paquete se entrega a un grupo de interfaces IPv6.

2.2.1 Direcciones Unicast

- ***Direcciones Unicast Globales***

  Están definidas por el prefijo 001, son equivalentes a las direcciones IPv4 publicas el formato es el siguiente:

Prefijo de ruteo global n bits (001)	Red ID 64-n bits	Identificador de interface 64 bits

Figura 2.1 Dirección Unicast, Autor: Luis Prieto

El prefijo global de ruteo es asignado por el ISP e indica que es una dirección unicast global, la red Id Identifica un link dentro de un sitio y el identificador de la interface identifica una interface o una sub red y debe ser única, identifica a un host ID.

- ***Direcciones de Enlace local***

Son usadas por los nodos cuando requieren comunicarse en el mismo enlace, se identifican con el prefijo de 64 bits 1111 1110 1000 0000 …. 0000, inician en formato FE80 . El formato es el siguiente

1111 1110 1000 0000 …. 0000 64 bits	Interface ID 64 bits

Figura 2.2 Dirección de enlace local, Autor: Luis Prieto

- ***Dirección Local Única***

Son direcciones privadas para una organización, se manejan dentro de la organización y la estructura es la siguiente:

7 bits 1111 110	ID Global 40 bits	ID Red 16 bits	Identificador de la interfaz 64 bits

Figura 2.3 Dirección Local Única, Autor: Luis Prieto

Los primeros 7 bits indica que es una dirección local, el ID global especifica la organización y es configurado aleatoriamente. El ID

de la red identifica la red en que esta la organización y el identificador de la interfaz que define los host asociados a la red.

- Direcciones Especiales
    - *Dirección sin especificar* Indica que no hay una dirección IPv6 equivale a "::" o 0:0:0:0:0:0:0:0.
    - *Dirección Loopback* Envía paquetes así mismo y es identificada por "::"1 o 0:0:0:0:0:0:0:1.

2.2.2 Direcciones Anycast

Las direcciones Anycast se usan para proveer redundancia y balance de carga, generalmente usa un método llamado, shared unicast address. El que asigna una dirección unicast múltiples interfaces, las entradas son creadas en la tabla de ruteo, así la capa de transporte asume que es una única dirección IP

En una red que este compuesta de un grupo de routers que provean acceso al dominio, se le asigna una dirección única, cuando los clientes envían paquetes a esta dirección este es enviado al router próximo resuelto por el tiempo de latencia y dependiendo de la topología de la red.

LA dirección anycast es definida en RFC 4291 con un prefijo de red y un identificador lleno de ceros de la siguiente manera:

Prefijo de red n bits	Longitud = 128 –n bits 0000….0000

Figura 2.4 Dirección Anycast, Autor: Luis Prieto

2.2.3 Direcciones Multicast

La dirección multicast es un identificador para un grupo de nodos, utiliza el valor mas alto en bytes FF o 1111 1111 en notación binaria, cuando se envía el paquete a una dirección multicast todos los miembros del grupo reciben el paquete en la figura se muestra como está estructurada una dirección multicast.

1111 1111 8 bits	Flags RPT 4 bits	Ámbito 4 bits	Grupo Identificador 112 bits

Figura 2.5 Dirección Multicast, Autor: Luis Prieto

La primera parte de la izquierda identifica la dirección multicast, el segundo bloque indica 3 banderas RPT valores el primero 0 es un valor reservado, cuando se utiliza T=0 indica que la dirección multicast será permanentemente asignada cuando utiliza T=1 indica que la dirección multicast será temporal, cuando P=0 la dirección no tiene prefijo, cuando P=1 la dirección está basado prefijo de red y cuando R=0 indica que no hay un punto de encuentro embebido y si R=1 existe punto de encuentro embebido. El tercer bloque indica en que ámbito de la red la red el paquete debe ser propagado, El valor

de 0 es reservado, 1 para ámbito de nodo local, 2 para el ámbito del link local, 5 para ámbito local del sitio, 8 para el ámbito local de la organización, E para ámbito global y F reservado. El bloque de identificación del grupo identifica el grupo concreto al que nos referimos en un determinado ámbito, además, estos son independientes el ámbito.

2.3 Equivalencia entre direcciones IPv6 e IPv4

Existe una equivalencia entre direcciones IPv4 e IPv6 en la siguiente Tabla podemos mostrar sus equivalente:

Concepto	IPv4	IPv6
Clases de Red	SI	No
Direcciones Multicast	224.0.0.0/4	FF00::/8
Direcciones Broadcast	Si	No
Dirección sin especificar	0.0.0.0	::
Dirección loopback	127.0.0.1	::1
Direcciones Públicas	Si	Direcciones unicast globales
Direcciones Privadas	10.0.0.0/8 172.16.0.0/12 192.168.0.0	Direcciones únicas locales FD00::/8

Tabla 2.1 Equivalencia entre IPv4 e IPv6, Fuente: IPv6 Essentials, 2nd Edition

CAPÍTIULO III

3 Coexistencia y Migración IPv4 e IPv6

La migración del protocolo IPv4 a IPv6 es algo un poco complicado, se debe tomar en cuenta que hay que cambiar la infraestructura de IPv4 a IPv6, verificando que todos los host, routers dentro de una organización tenga conectividad y sobre todo trabajen sobre IPv6, dentro de un ámbito de una pequeña y mediana organización esta migración sería algo más sencillo, pero si topamos en caso de una organización grande o inclusive en todo lo que es el internet sería una tarea demasiado complicada y costosa, mientras se va dando esta migración que tomará muchos años, se resolvió en el RFC 1752 que debía haber una coexistencia entre el Protocolo IPv4 e IPv6.

3.1 Técnicas de transición

Las técnicas de transición usadas son el:

- Dual Stack o doble pila
- Tunneling o tuneles

3.1.1 Dual Stack o Doble Pila

Es soportado por los dos protocolos y trabaja en modo IPv6/IPv4, cuando se envían paquetes IPv4 trabaja en modo IPv4-only que solo acepta paquetes de este protocolo y cuando se envían paquetes IPv6 trabaja en modo IPv6-only que también solamente acepta paquetes

de este tipo, además, cuando la pila IPv4 y la pila IPv6 son activados puede trabajar de ambos modos usando los dos protocolos.

Dual Stack es aplicado en compañías que necesitan dentro de su intranet el uso de IPv6, las empresas que empiezan con un plan piloto pera la transición a IPv6.

Los beneficios que Dual Stack provee son:

- No se necesita de túneles
- IPv4 e Ipv6 corren independientemente
- Dual Stack soporta una migración gradual de los puntos finales de las redes y sus aplicaciones.

A continuación se muestra la arquitectura Doble Pila y los modos que trabaja:

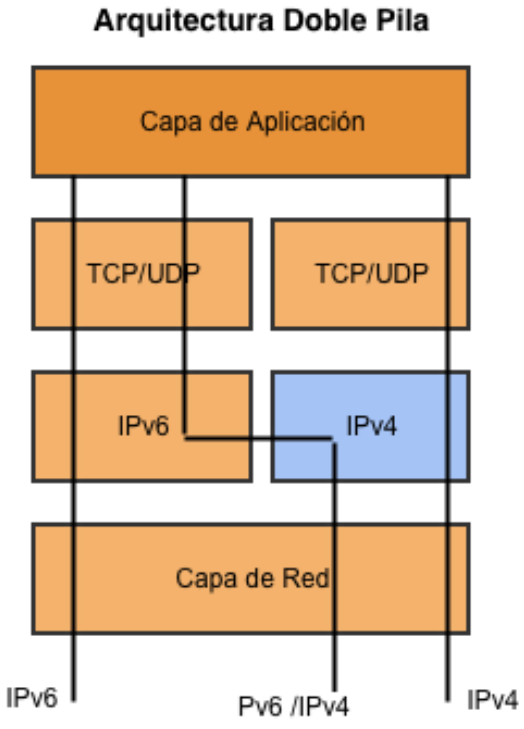


Figura 3.1 Arquitectura Doble Pila, Autor: Luis Prieto

3.1.2 Tunneling

El tunneling o túnel también llamado encapsulación donde un protocolo es encapsulado en otro, en este caso el protocolo IPv6 es encapsulado con una cabecera IPv4, para que una dirección IPv6 pueda subsistir en un entorno de red que trabaje con IPv4.

La encapsulación cumple con tres procesos

- Encapsulación en el punto de entrada del túnel
- Des encapsulación en el punto de salida del túnel
- Manejo del túnel estático o dinámico

A continuación se muestra un diagrama genérico de cómo los túneles se aplicarían:

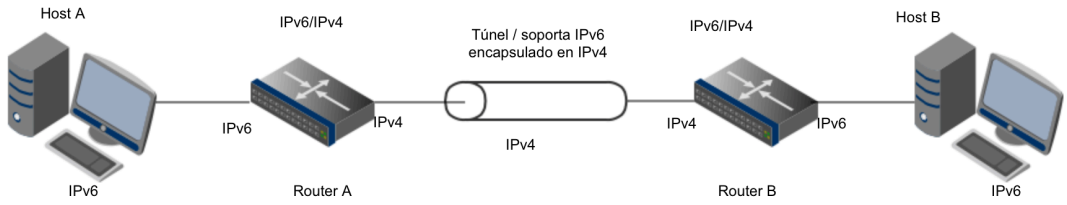


Figura 3.2 Diagrama genérico tunneling, Autor: Luis Prieto

Desde el Host A se envía información hacia el Host B, desde A sale con una dirección IPv6 llega hasta el Router A y este lo encapsula es decir pone una cabecera IPv4, continua su camino hacia el Router B el que desencapsula el paquete y nuevamente tendríamos una dirección y IPv6 que sería enviada a Host B. Los end point o puntos finales del túnel son donde el Router A encapsula al paquete IPv6 en un paquete IPv4, así mismo otro punto final es donde el Router B desencapsula el paquete IPv4 y lo convierte en IPv6.

El encapsulamiento se representa de la siguiente manera

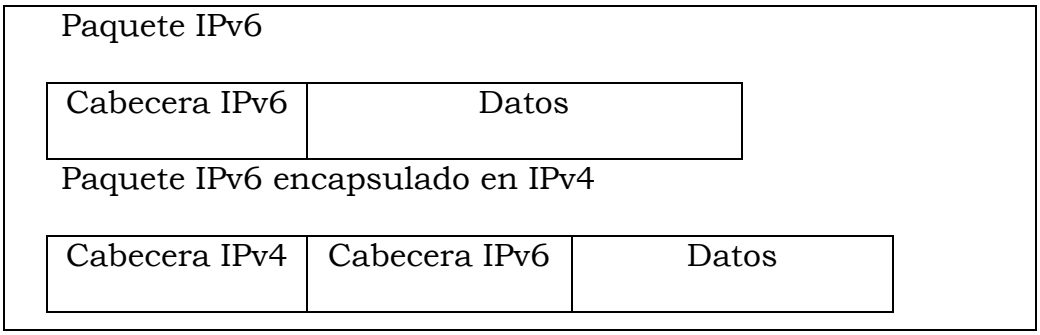


Figura 3.3 Representación de Encapsulamiento IPv4, Autor: Luis Prieto

- La longitud de la cabecera IPv4 equivale a la Cabecera IPv4 más las cabecera IPv6 más los datos.
- La dirección de origen será para este caso la del Router A
- La dirección de destino la del Router B

3.2 Tipos de túneles

3.2.1 Túneles configurados

Los túneles configurados trabajan en el modo IPv6-over IPv4, en el punto final del túnel las direcciones son determinadas por configuración, los routers son configurados con rutas estáticas manualmente, lo que se tiene son túneles configurados para el protocolo IPv6.

Los túneles configurados son:

- 6 in 4 IPv6 sobre IPv4 protocol 41
- GRE IPv6 sobre GRE sobre IPv4

GRE

Generic Routing Encapsulation es un protocolo desarrollado por Cisco usado para encapsular los paquetes IPv6 en IPv4, está diseñado para implementar cualquier esquema estándar de encapsulamiento de punto punto, los túneles GRE son utilizados para conexiones estables que requieren una comunicación. GRE encapsula el payload y puede transportar tráfico multicast,

6 in 4

Es un mecanismo de transición IPv4 a IPv6 que encapsula paquetes IPv6 en IPv4, los paquetes Ipv6 se envían a través de internet IPv4, poseen un encabezado de número de protocolo el 41, después del encabezado está el resto del paquete IPv6, es decir que se añade únicamente 20 bytes que corresponde a la cabecera IPv4.

3.2.2 Túneles Automáticos

Los Túneles Automáticos permiten que los nodos IPv6/IPv4 sin necesitar una pre configuración de los túneles se comuniquen, los puntos finales del túnel son determinados por el uso de las rutas, por las interfaces del túnel y por el siguiente salto de el destino de la dirección IPv6.

Los túneles Automáticos son:

- 6to4 habilitado por defecto.
- ISATAP (intre-site Automatic Tunnel Addressing Protocol).
- TEREDO

6to4

Especifica un mecanismo para sitios IPv6 comunicándose entre ellos sobre una Arquitectura IPv4, se trata al área IPv4 como una capa unicast es decir un enlace punto punto y los dominios se comunican a través de routers 6to4, es decir los paquetes IPv6 se encapsulan dentro de la red IPv4 hasta llegar a su destino, esta configuración es la que se usa por defecto y es la que regularmente se hace referencia cuando hablamos de túneles, se ha asignado por IANA un prefijo especial para 6to4 este es 2002::/16, los 16 bits primeros son usados par ara el prefijo, los 32bits siguientes se asigna una dirección IPv4, luego los 32 bits siguientes se usa para el identificador de red es decir 65536 redes, los 64 bits restantes son asignados para los host de red es decir, 264 nodos por red a continuación se muestra en la figura el formato del prefijo para 6t4.

16 bits 2002	32 bits IPv4 dir.	16 bits Redes	64 bits Host

Figura 3.4 Formato 6to4, Autor: Luis Prieto

Cuando el paquete viaja de una red IPv6 a una IPv4 el router 6to4 encapsúlala dirección IPv6 y toma de los 32 bits la dirección IPv6 y la copia como dirección de destino, la dirección de destino se asigna desde el punto de partida del host o router que encapsula.

ISATAP

Intra-Site Automatic Tunnel Addressing Protocol está diseñado para proveer conectividad en nodos IPv6 e IPv4, estas direcciones tienen un prefijo de 64 bits que puede pertenecer a la gama unicast global los siguientes 32 bits contienen el identificador de red y es de la forma 00 00 5E FE el valor FE indica que tiene una dirección IPv4 embebida. Los últimos 32 bits contienen la dirección IPv4, se puede sumarizar esta dirección como:

2001:DB8::200:5EFE:62.2.84.115

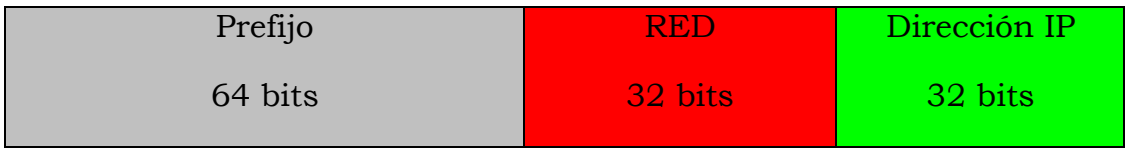


Figura 3.5 Formato ISATAP, Autor: Luis Prieto

Teredo

Este mecanismo es diseñado para proveer conectividad a host situados detrás de una o mas NATs, usa un túnel con protocolo UDP, el mecanismo consta de clientes y servidores Teredo. Teredo especifica muchos usuarios privados de internet situados detrás de NAT.

El prefijo Teredo es 2001:0000/32 tiene una longitud de 32 bits, el siguiente campo es una dirección IPv4 y contiene una dirección IPv4 de un servidor Teredo, el campo flags con 16 bits que especifica el tipo de dirección NAT en uso, el campo port contiene el puerto UDP

que es con que funciona Teredo, el campo dirección de cliente IPv4 contiene la dirección del cliente IPv4.

Prefijo 32bits	Dirección IPv4 de Servidor 32 bits	Flags 16 bits	Puerto 16 bits	Cliente IPv4 32 bits

Figura 3.6 Formato Teredo, Autor: Luis Prieto

CAPÍTULO IV

4 Ruteo IPv6

El ruteo es el proceso de mantener una tabla de ruteo asistidos por los protocolos de ruteo, cuando los paquetes llegan al router, son reenviados según la tabla de ruteo a su destino. En el ruteo IPv6 el los routers necesitan conocer las direcciones de los host o routers vecinos con esto construyen la tabla de ruteo, para auto configurar las direcciones IPv6, inicialmente los routers escuchan direcciones multicast con el prefijo (FF02::2) enviados por otros routers y este responde con el grupo de direcciones FF02::1, con la información de la tabla contenida en este, generalmente los routers envían esta información periódicamente a otros routers para mantener actualizadas las tablas de ruteo, básicamente los routers necesitan acceder a redes remotas.

Existen dos tipo de ruteo

- ***Ruteo Estático***

  En el caso de que la red IPv6 pequeña lo que se necesita en usar las rutas estáticas para alcanzar otros nodos, una red pequeña se considera aproximadamente entre 2 y 10 redes, las rutas estáticas indican que solamente se tiene una vía de acceso para que los paquetes viajes de extremo a extremo, además de limita a que la topología de la red no cambie con el tiempo.

  Las rutas estáticas están no soportan tolerancia a errores al no haber rutas alternativas si una ruta colapsa la red pierde el nodo y no tiene acceso.

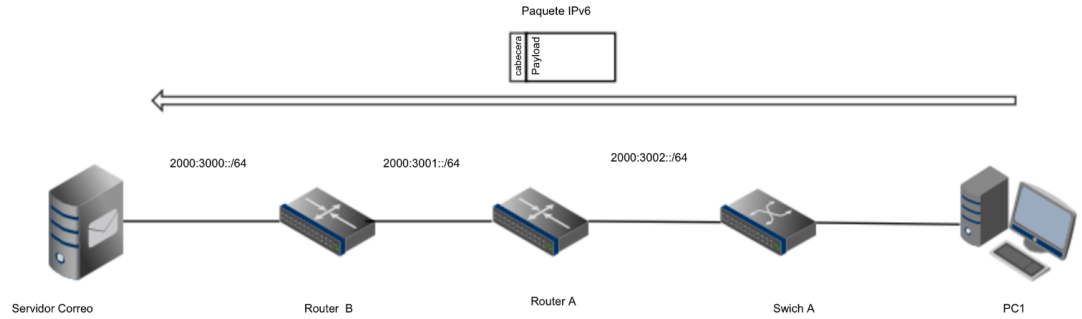


Figura 4.1 Ejemplo de Ruteo estático, Autor: Luis Prieto

- En la figura se muestra un paquete que parte del PC1 a Servidor de Correo para que esto suceda los Router A y Router B tiene que conocer todas las rutas. Para el Router A las rutas directa son 2000:3002::/64 y 2000:3001::64 y la ruta desconocida 2000:3000::64, estaría dentro de la configuración de la tabla de ruteo como ruta estática, de la misma manera el Router B tiene

conectado dos rutas directas 2000:3001::64 y 2000:3000::64 la ruta desconocida sería 2000:3002::/64 es la que aparecerá como ruta estática para la configuración y tabla de ruteo de el Router B.

- ***Ruteo Dinámico***

  Las rutas dinámicas se son usadas cuando la topología de red es muy complicada de tal forma que configurar manualmente cada ruta en cada router sería un proceso muy dificultoso además soluciona el problema de tolerancia a errores, ya que generalmente los nodos tienen rutas alternativas para llegar al mismo destino, cuando se configuran rutas dinámicas las redes son escalables y pueden crecer usando protocolos de ruteo que permiten a el router elegir la mejor ruta según el método establecido los protocolos de enrutamiento dinámico son:

  - RIPng
  - OSPFv3
  - IS-IS integrado
  - BGP-4

4.1 Ruteo entre IPv4 e IPv6

4.2 Protocolos de Ruteo

Los protocolos de ruteo son usados para facilitar el tráfico o las comunicaciones entre routers, actualizan las tablas de ruteo

automáticamente. Están basados en el vector distancia y protocolo de estado de enlace.

El vector distancia se basa en el conteo del número de saltos para tomar una decisión y el estado del enlace se basa en el costo del enlace donde el router envía un paquete ECHO y calcula el costo con el tiempo de ida y vuelta del paquete, eligiendo la mejor ruta.

4.2.1 RIPng

El protocolo RIPng Routing Information Protocol (next generation), utiliza el algoritmo del vector distancia, el número máximo de saltos que cuenta son 15 en este caso el salto 16 estaría fuera de alcance. Al Inicializar las tablas de ruteo RIPng envía un mensaje de solicitud a todos los host, dentro de los 3 minutos subsiguientes estarán las rutas dentro de la tabla de ruteo, luego serán actualizadas, una vez inicializado el router anuncia periódicamente cada 30 segundos las rutas apropiadas que están ubicadas en la tabla de ruteo.

RIPng está basado en el protocolo UDP, usa el puerto 521 y en el proceso de ruteo siempre escucha los mensajes que llegan por este puerto, el formato del mensaje RIPng es el siguiente:

Cabecera IPv6	Cabecera UDP	Cabecera RIPng	RTE 1	RTE 2	……	RTEn

Figura 4.2 Mensaje RIPng, Understanding IPv6, 3er Edition

La cabecera RIPng se le han asignado cuatro bytes, distribuidos en los campos

1. Command (Request o Response) 1 byte

   Request Un mensaje de solicitud requiere la respuesta del sistema para enviar todo o parte de su tabla de ruteo

   Response Un mensaje de respuesta contiene todo o parte de la tabla de ruteo del remitente. Puede ser enviado como respuesta a una solicitud o como una respuesta no solicitada en actualizaciones periódicas de tablas de enrutamiento.
2. Versión.- la versión es asignada con el valor de 1
3. Sin uso 2 bytes

El campo RTE es asignado con 20 bytes por cada entrada, 16 bytes para el prefijo IPv6 donde se encuentra la dirección del siguiente salto, 2 bytes para Route tag usado para llevar información adicional de una ruta aprendida de otro protocolo de enrutamiento, Prefix Length con un byte con el rango de 0 a 128 y el campo Metric de 1 byte el que se puede asignar de 1 a 16 dependiendo del número de saltos.

4.2.2 OSPFv3

OSPFv3 Open Shortest Path Fist está basa do en el algoritmo del estado del enlace, es una adaptación de OSPF versión 2 de IPv4. EL costo es un valor asignado pro el administrador de la red incluye valores de delay ancho de banda, este costo no puede superar 65535.

OSPFv3 toma sus decisiones basado en los estados de los estados que conectan las máquinas de origen y destino.

OSPFv3 tiene las siguientes diferencias con relación a la versión OSPFv2

- A estructura de los paquetes de OSPF han sido modificados para remover dependencias de las direcciones IPv4
- Se han definido nuevos LSAs para llevar direcciones y prefijos IPv6
- OSPF se ejecuta en cada enlace en lugar de cada subred.
- OSPF no provee autenticación en vez de ello depende de la autenticación de la cabecera (AH).

Cada Router tiene un estado de enlace (LSA) que describe su estado, el LSA de cada router con OSPF es propagado a través de la red OSPF, mediante una relación lógica entre vecinos y routers, cuando la propagación de todos los routers es completada se dice que la red OSPF ha convergido.

4.2.3 IS-IS integrado

IS-IS Intermediate Systems to Intermediate Systems es un protocolo similar a OSPF, utiliza un algoritmo de estado el enlace, llamado protocolo de enrutamiento interior. IS-IS fue desarrollado para soportar encaminamientos en grandes dominios.

Un dominio de enrutamiento puede dividirse en uno o mas subdominios y cada uno de estos se le asigna una dirección de área. El enrutamiento dentro de esta área se le conoce como nivel 1 de enrutamiento y el enrutamiento entre áreas de nivel 1 se conoce como nivel 2 de enrutamiento. Un router en terminología OSI se le conoce como un sistema intermedio IS, un IS puede operar en el nivel 1, nivel 2 o en ambos.

Los IS generan Link-state PDUs (LSPs) para avisar sus vecinos y el destino al que están directamente conectados.

Los Sequence Number PDUs (SNP) contiene una descripción sumarizada de uno o mas LSPs.

El IS es identificado por una dirección conocida como NET, esta dirección puede tener de 8 a 20 bytes de longitud y consiste en tres partes:

- Dirección de Área.- este campo consta de 1 a 13 bytes de longitud y está compuesto por los bytes de orden superior de la dirección.
- ID del sistema.- es un campo de 6 bytes que cuando IS opera en el nivel 1, nivel 2 o entre los dos, el ID del sistema será único para identificar a cada uno de ellos.
- NSEL.- el N-selector es un campo de un byte de longitud y el valor es 00.

Existen dos tipos de Circuitos soportados por IS-IS

Punto Punto.- los que constan dos IS en el circuito. Un IS forma una simple adyacencia a la otra IS en el circuito punto punto , esta adyacencia describe el nivel que es soportado en el circuito. Si los dos ISs soportan un nivel 1 en el circuito y se configuran con una dirección coincidente LSPs y SNPs de nivel 1 serán enviados dentro del circuito, los mismo se dará para nivel 2 y también cuando soporta nivel 1-2.

Circuitos de multiacceso.- soportan múltiples ISs, es decir dos o mas operando en el circuito. Tiene la capacidad de hacer frente a múltiples sistemas que utilizan una dirección multicast.

4.2.4 BGP para IPv6

EL BGP-4 Border Gateway Protocol Version 4 intercambia información usa el ruteo basado en vector distancia, fue diseñado para la interconexión de sistemas autónomos, usados para la conexión de sistemas grandes como proveedores de servicio como ISPs. Es compatible con las mismas características y funcionalidad de BGPv4 que fue creado específicamente para el protocolo IPV4. Las mejoras que se han incluido en BGP para IPv6 es el soporte de direcciones de familias y accesibilidad a información a nivel de Red y siguiente salto.

4.3 Tabla de Ruteo

La tabla de ruteo IPv6 almacena la siguiente información

- Un prefijo de dirección
- La interfaz a través de la cual se envían los paquetes que coinciden con el prefijo de dirección.
- La rutas directamente conectadas que son las direcciones de red que salen de las interfaces del Router.
- Las rutas remotas que son las direcciones de red que no están directamente conectadas, pero sin alcanzables
- Las rutas Host es una ruta específica a una dirección IPv6.
- Rutas por defecto son las rutas sumarizadas de todo el trafico IPv6.
- Una dirección de reenvío del siguiente salto

  A continuación se muestra un ejemplo de una tabla de ruteo:

ifIndex	RouteMetric	DestinationPrefix	NextHop	Store
12	256	ff00::/8	::	Active
1	256	ff00::/8	::	Active
12	256	fe80::c51d:624b:b276:6a03/128	::	Active
12	256	fe80::/64	::	Active
12	256	2001:db8::1:82e:9636:809e:2472/128	::	Active
12	256	2001:db8::/64	::	Active
1	256	::1/128	::	Active

Figura 4.3 Tabla de Ruteo IPv6, Fuente: Understanding IPv6

Las tablas de enrutamiento IPv6 se generan automáticamente y se basan en las configuraciones de ruteo del equipo, cuando se reenvían los paquetes, el router busca en su tabla de enrutamiento las entrada

más similar a la dirección de destino. La ruta predeterminada usa el prefijo ::/0 la que es utilizada para reenviar un paquete a un enrutador predeterminado de vínculo local.

CAPÍTULO V

5 Diseño Red en GNS3

Para la simulación se ha tomado en cuenta 3 redes LAN y una red WAN las que manejarán diferentes tipos de protocolos tanto IPv4 como IPv6 y se probará la conectividad entre host sin importar que protocolo sea el de destino.

La Herramienta de simulación que utilizaremos es GNS3, debido a que la herramienta permite varias maneras de hacer la simulación, se ha definido ciertos parámetros citados a continuación:

- IOS de cisco modelos 2621 y 3640 para routers.
- Los host serán simulados y configurados usando VPCS.
- Dos host configurados con virtual box con sistema operativo Ubuntu server 14.04.1.
- Switches con IOS 3640 de routers de cisco, permiten simular un switch configurable.
- Una WAN que soportará los túneles es decir permitirá el paso de paquetes de IPv6 a IPv4.
- Tres LAN distribuidas de la siguiente manera
    - LAN1 soporta el protocolo IPV4
    - LAN2 soporta el protocolo IPV6
    - LAN3 soporta el protocolo IPV6

- Los servidores utilizados para comprobar la conectividad y alcance entre las diferentes redes.
- Las direcciones IPv4 se configurarán de forma manual.
- Las direcciones IPv6 se configurarán de manera automática.
- Capturaremos paquetes con whireshark para monitorear sus cabeceras en diferentes puntos de la red.
- Dos host con Linux Ubuntu server 14.04 usando virtualización.

El diagrama de Red de acuerdo a estos parámetros se ha definido de la siguiente manera:

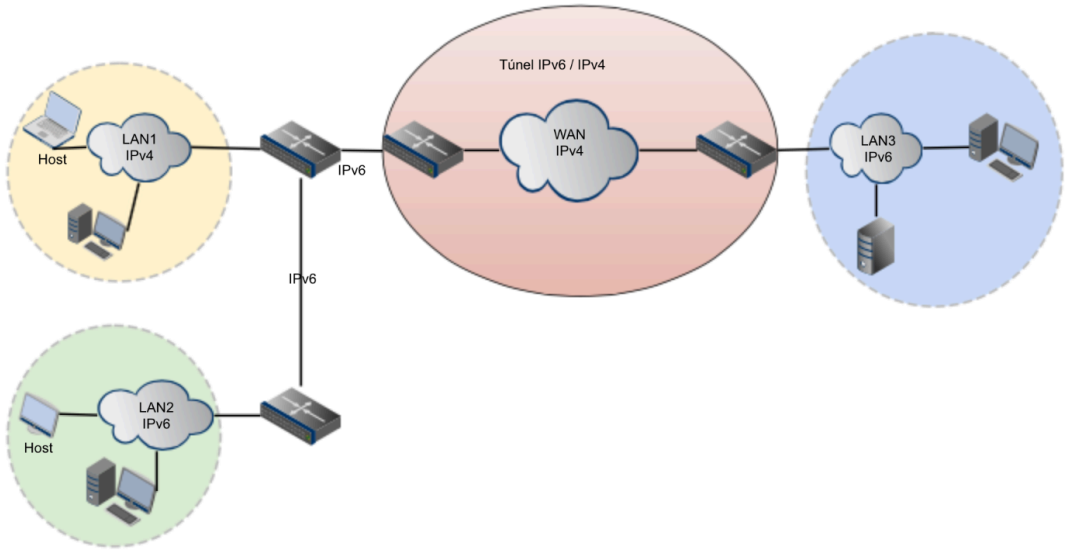


Figura 5.1 Diagrama de Red, Autor: Luis Prieto

LAN1 corresponde a nuestra red IPv4 la que se conecta a la WAN pero también muestra conectividad con LAN2.

LAN2 corresponde a la red IPv6 la que conecta directamente a la LAN1.

LAN3 corresponde a la red IPv6 la que se conecta directamente a la WAN.

WAN es la red hibrida recibe paquetes IPv6 de las redes LAN y los encapsula en IPv4.

5.1 Diseño de una Red WAN y LAN

La topología de la red en GNS3 muestra claramente las tres redes LAN que se van a conectar a la WAN como se muestra en la figura.

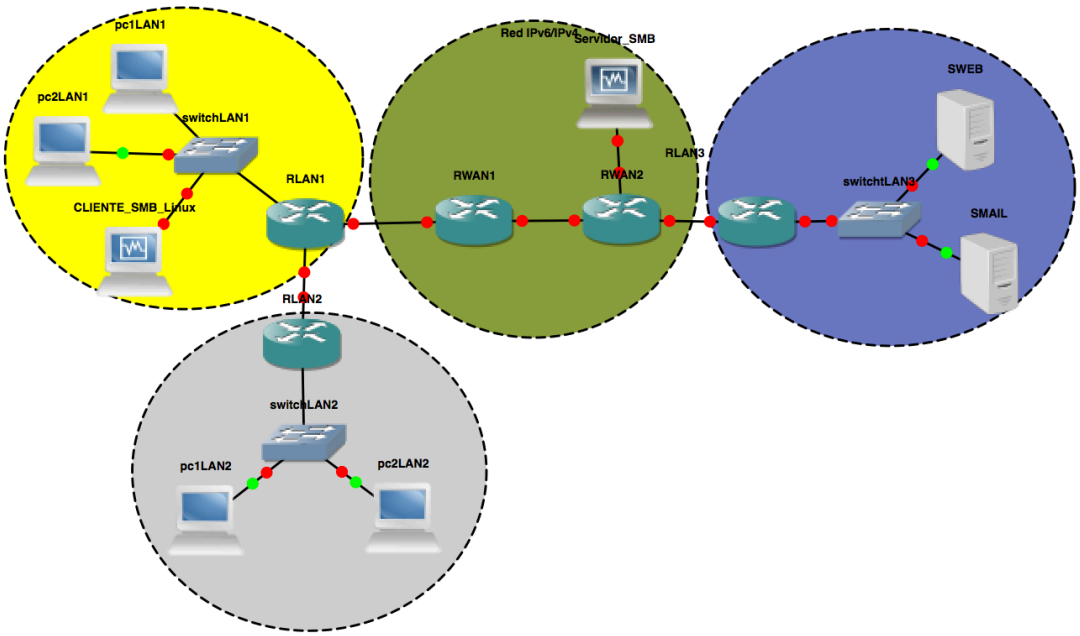


Figura 5.2 Distribución de la topología de red, Autor: Luis Prieto

Las PCs en la LAN1 tendrán direcciones IPv4 estáticas, las PCs en la LAN2 se configuraran con direcciones IPv6, donde el router de LAN2 está conectado directamente a en router de LAN1 antes de salir a la

WAN, por lo que este router de LAN1 deberá soportar los dos protocolos. Los servidores usarán direcciones IPv6 asignadas de manera automática y perteneces a la LAN3 que se conecta directamente con la WAN, lo que se desea simular es la conectividad entre estos tres tipos de redes y protocolos distintos, cualquier host o nodo está al alcance de cualquier dispositivo dentro de la red, el diseño final de la topología es el siguiente.

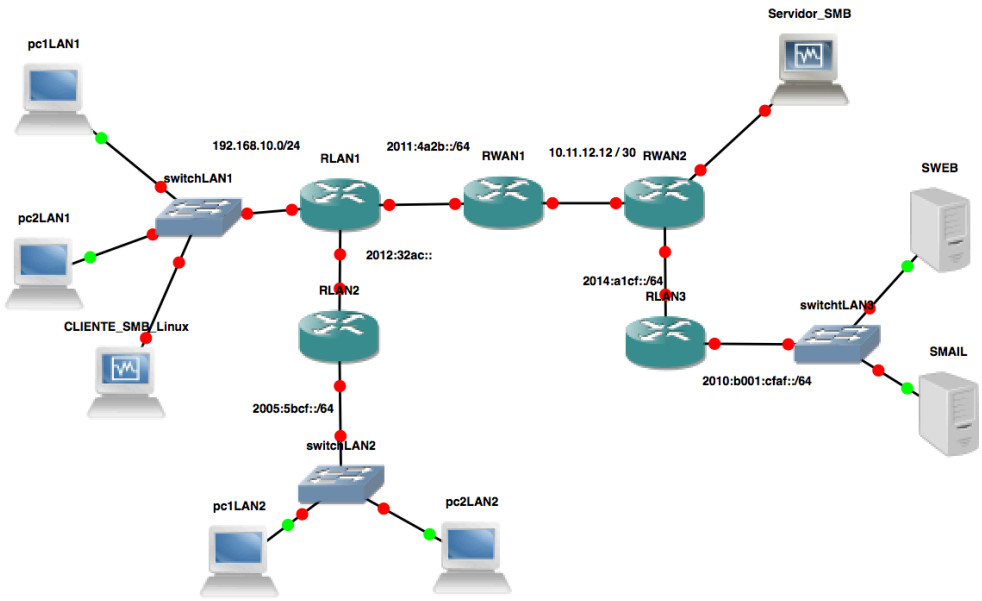


Figura 5.3 Topología de Red para la simulación en GNS3, Autor: Luis Prieto

5.2 Configuración de nodos

Los nodos serán configurados con los datos que se muestran a continuación:

Dispositivo	Interface	Protocolo	Dirección	Máscara
pc1LAN1	NIO_udp:30000:127.0.01:20000	IPv4	192.168.10.2	/24
pcLAN2	NIO_udp:300	IPv4	192.168.10.3	/24

	01:127.0.0.1:20001			
Cliente SMBLinux	e0	IPv4	192.168.10.4	/24
pc1LAN2	NIO_udp:30002:127.0.0.1:20002	IPv6	2005:5bcf::2050:79ff:fe66:6802	/64
pc2LAN2	NIO_udp:30003:127.0.0.1:20003	IPv6	2005:5bcf::2050:79ff:fe66:6803	/64
SWEB	NIO_udp:30004:127.0.0.1:20004	IPv6	2010:b001:cfaf:0:2050:79ff:fe66:6804	/64
SMAIL	NIO_udp:30005:127.0.0.1:20005		2010:b001:cfaf:0:2050:79ff:fe66:6805	/64
RLAN1	f 0/0	IPv4	192.168.10.1	/64
	f 0/1	IPv6	2011:4A2B::1F3F	/60
	f 1/0	IPv6	2012:4A2B::1F40	/60
RLAN2	f 0/0	IPv6	2005:5BCF::2A4A	
	F 0/1	IPv6	2012:4A2B::1F3F	/64
RLAN3	f 0/0	IPV6	2014:A1CF::CC62	
	f 1/0	IPV6	2010:B001:CFAF::BB2A	
RWAN1	f 0/0	IPv6	2011:4A2B::1F40	/64
	f 1/0	IPv4	10.11.12.13	/24
RWAN2	f 0/0	IPv4	10.11.12.14	/24

	f 1/0	IPv6	2014:A1CF::CC61	/64
	f2/0	IPv4	192.168.11.1	/24
Servidor SMB	e0	IPv4	102.168.11.2	/24

Tabla 5.1 Tabla de guía direcciones IP, Autor: Luis Prieto

Tenemos 5 routers con los siguientes IOS:

RLAN1	RLAN2	RLAN3	RWAN1	RWAN2
Cisco 2621	Cisco 2621	Cisco 3640	Cisco 3640	Cisco 3640

Tabla 5.2 Routers según modelo, Autor: Luis Prieto

Se ha elegido diferentes modelos de IOS debido a que con esto podemos mostrar que IPv6 puede ser habilitado en varios modelos de cisco. La configuración inicial de cada router se muestra a continuación:

RLAN1

RLAN1 pertenece a la LAN1 el que tiene 3 interfaces conectadas a las redes aledañas en la interfaz f0/0 se manejará el protocolo IPv4 y en la f1/0 y f0/1 el protocolo IPv6.

RLAN1 archivo de configuración
!   version 12.3   service timestamps debug datetime msec   service timestamps log datetime msec   no service password-encryption   !   hostname RLAN1

```
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
ip cef
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto

!
ip http server
ip classless
!
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Tabla 5.3 Configuración inicial RLAN1, Autor: Luis Prieto

RLAN2

RLAN2 pertenece a la LAN2 la que maneja en sus dos interfaces f0/0 y f0/1 el protocolo IPv6, aquí no se configurará ninguna interfaz con direcciones IPv4.

RLAN2 archivo de configuración

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RLAN2
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
ip cef
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
ip http server
ip classless
!
!
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
!
line con 0
line aux 0
line vty 0 4
 login
!
!
```

```
end
```

Tabla 5.4 Tabla de configuración RLAN2, Autor: Luis Prieto

RLAN3

RLAN3 es el router que se encuentra al otro lado de la WAN, este router maneja el protocolo IPv6 y las direcciones de red serán manejadas de manera automática por el router.

RLAN3 Archivo de configuración

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RLAN3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto

no ip http server
no ip http secure-server
```

```
!
ip forward-protocol nd
!
control-plane
!
line aux 0
line vty 0 4
 login
!
end
```

Tabla 5.5 Configuración inicial RLAN3, Autor: Luis Prieto

RWAN1

RWAN1 es el router que permite a los RLAN1 y RLAN2 salir a la WAN, en su interfaz f0/0 maneja el protocolo IPv6 esta conectado directamente a RLAN1, en su interfaz 1/0 maneja el protocolo IPv4, en esta interfaz se aplicara el tunneling IPV6 to IPv4.

RWAN1 Archivo de configuración

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RWAN1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
```

```
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
!
ip forward-protocol nd
!
!
log-adjacency-changes
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Tabla 5.6 Configuración inicial RWAN1, Autor: Luis Prieto

RWAN2

RWAN2 es el router que permite a la RLAN3 salir a la WANl, está directamente conectado vía f0/0 a el router RWAN1 mediante el protocolo IPv4, en esta parte se maneja el tunneling IPv6 to IPv4, cuenta con la interfaz f2/0 la que termina en un servidor Linux manejado con protocolo IPv4, el que nos permitirá transmitir archivos hacia el cliente que se encuentra en la LAN1.

RWAN2 Archivo de configuración

`version 12.4`
`service timestamps debug datetime msec`
`service timestamps log datetime msec`
`no service password-encryption`

```
!
hostname RWAN2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 general-prefix RWAN2 6to4 FastEthernet0/0
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 duplex auto
 speed auto
!

no ip http server
no ip http secure-server
!
ip forward-protocol nd
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Tabla 5.7 Configuración inicial RWAN2, Autor: Luis Prieto

5.3 Configuración Ip estática y dinámicas

Los host serán configurados dependiendo de la LAN a la que pertenecen en el caso de LAN1 tenderemos dos hosts pc1LAN1 y pc2LAN1, las direcciones serán configuradas IPv4 y con direcciones estáticas según la tabla de ruteo inicial, la dirección del cliente el que posee sistema operativo Linux server, será configurado con una dirección IPv4 estática, dentro de GNS3 usaremos VPCS para configurar los parámetros de red de los host .

Para configurar los host con VPCS Elegimos en el cuadro equipos terminales el equipo host, este tipo de equipo terminal será configurado con la consola VPCS más adelante

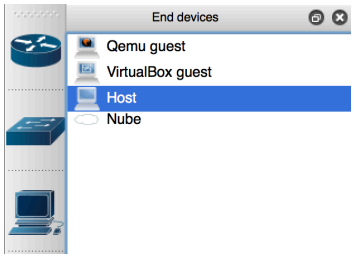


Figura 5.4 Host VPCS, Autor: Luis Prieto

Editamos el nombre del host que por defecto está en C1 editamos y lo configuramos con el nombre p1LAN1 y p2LAN1 y el resultado será el siguiente:

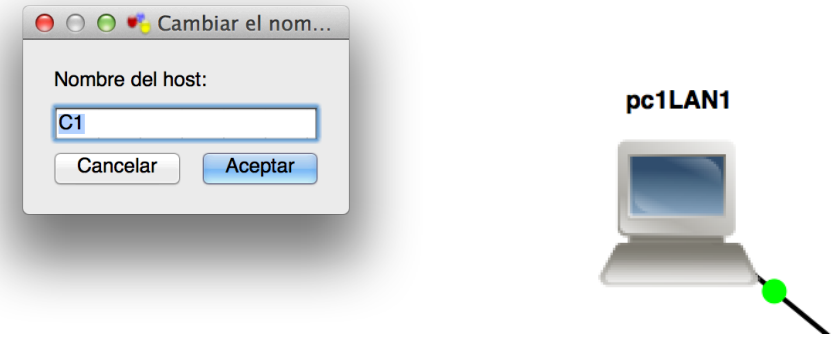


Figura 5.5 Asignación nombre de host VPCS, Autor: Luis Prieto

seguido a esto entramos a la configuración del host y elegimos la interfaz o la NIC que se va ha simular, este caso VPCS permite configurar la NIC mediante NIO_UD, un puerto local y un puerto remoto el que le va ha permitir identificarse al host dentro de la red, lo que debemos puntualizar es que cada host que se agregue no puede tener el mismo puerto local ni remoto de los que se encuentran dentro de toda la topología de la red.

En la figura se puede ver la manera de elegir el NIO_UDP, donde también podemos cambiar los puertos, GSN3 permite como máximo hasta 9 host para la simulación.

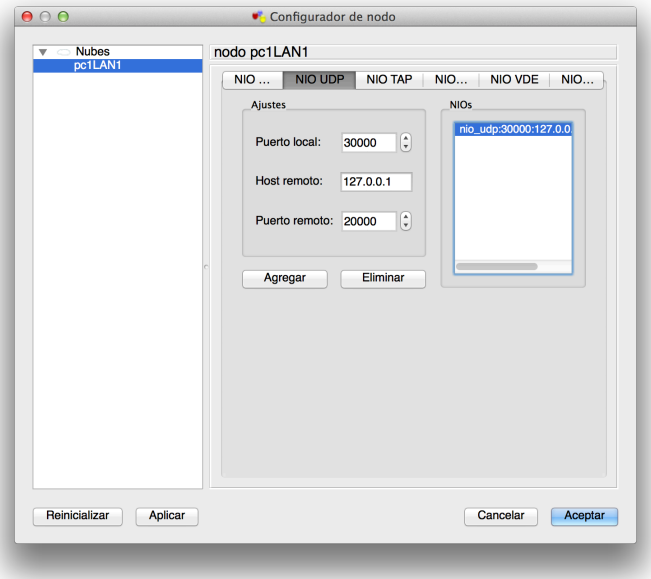


Figura 5.6 Configuración NIC del host, Autor: Luis Prieto

Luego de elegir los puertos y configurar el nombre del host que hace referencia a la topología abrimos el VPCS.

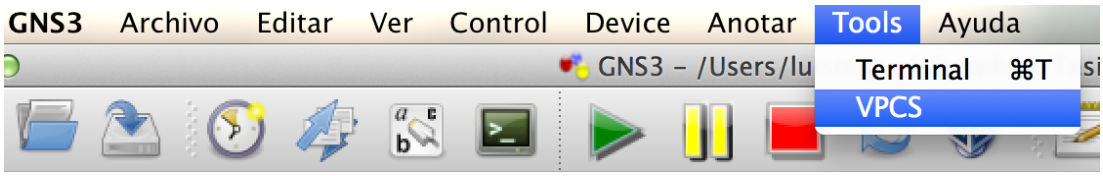


Figura 5.7 Terminal VPCS, Autor: Luis Prieto

Entonces obtenemos el terminal o el modo línea de comandos para la configuración de los hosts.

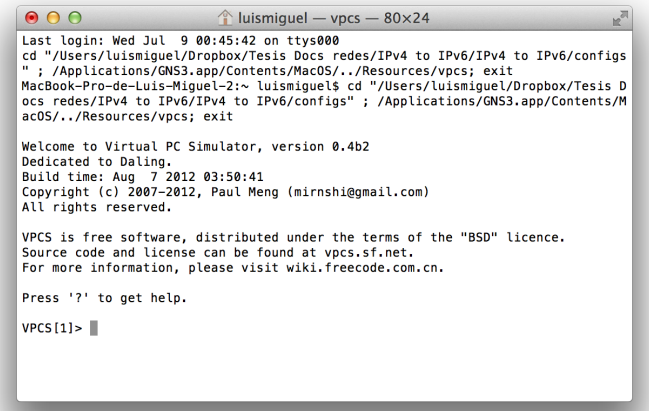


Figura 5.8 Terminal VPCS de GNS3 en el host, Autor: Luis Prieto

Dentro del terminal podemos configurar todos los parámetros correspondientes

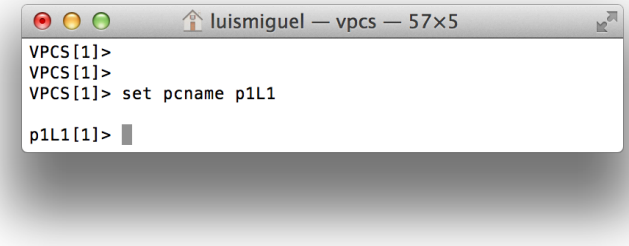


Figura 5.9 Configuración host 1 LAN1, Autor: Luis Prieto

Configuramos el pcname con el nombre p1L1, la IP, máscara y Gateway de este equipo de a acuerdo a la tabla de configuración de nodos, el cual corresponde a 192.168.10.2, 255.255.255.0 y Gateway 192.168.10.1. para mostrar la configuración usamos el comando “show ip” y obtenemos los siguiente:

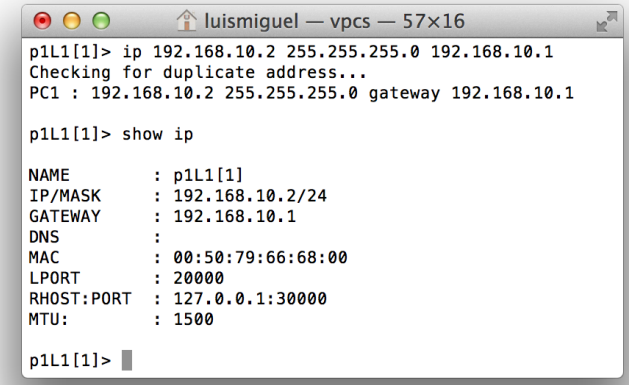


Figura 5.10 presentación de la configuración final p1L1, Autor: Luis Prieto

Para configurar el pc2LAN1 se seguirá los mismo pasos, solamente cambiaremos el nombre a p2L2 y la IP a 192.168.10.3.

El cliente SMB Linux es el host que contiene el sistema operativo virtual manejado por virtualBox, en el anexo podemos encontrar como se configura el virtualBox para el uso en GNS3, si ya lo tenemos configurado, debemos iniciar la simulación y dentro del terminal de Ubuntu Linux server configuramos la dirección Ip.

Usamos el comando gedit/network/interfaces, el que nos va ha desplegar una ventana con la configuración de las interfaces que contiene el sistema operativo simulado, en este caso existe una la eth0 que puede ser configurada como static o con dhcp, para identificar de mejor manera al host, utilizaremos una dirección Ip estática y el resultado del archivo de configuración de la interfaz se muestra en la figura

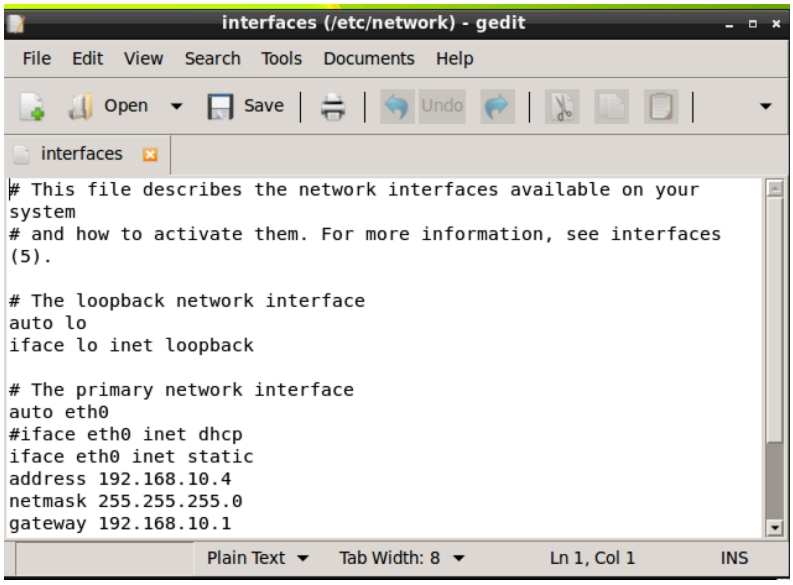


Figura 5.11 Archivo de configuración IPv4, Autor: Luis Prieto

En esta parte de la red se aplicará el uso de Dual Stack debido a que esta red intercambiará paquetes con otra pero con protocolo IPv6, también debemos configurar la interfaz eth0 con una dirección IPv6 global con un prefijo 2001:: el que nos permitirá identificar a los host IPv4 en las redes IPv6 y tener la conectividad deseada.

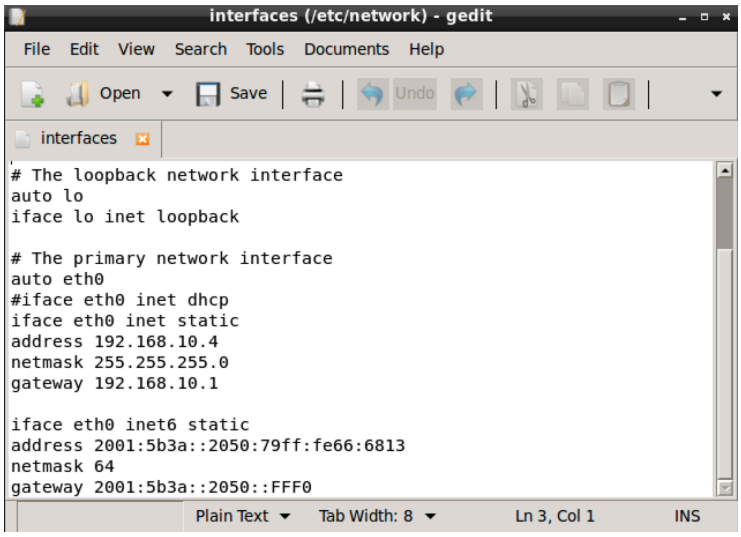


Figura 5.12 Archivo de configuración IPv4 e IPv6 Cliente Linux, Autor: Luis Prieto

Dentro de la LAN2 existen dos host que serán configurados de manera automática usando direcciones IPv6, para que esto necesitamos que el router LAN2 tenga el servicio activado de ipv6 autoconfig con la siguiente línea de comandos:

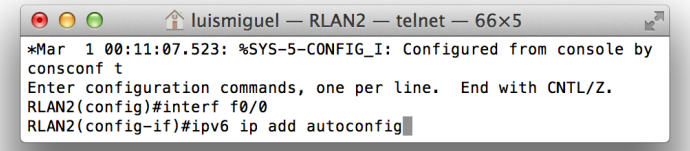


Figura 5.13 Configuración automática interfaz f0/0, Autor: Luis Prieto

Luego de este paso tendremos que en VPCS configurar la dirección IPv6 con el comando auto, de así el router será el encargado de designar la dirección IPv6 de acuerdo a la dirección que se haya configurado en el router y su prefijo.

En la LAN3 se ha designado el protocolo IPv6, de la misma manera las direcciones IPv6 serán configuradas de manera automática, y estarán basadas en prefijo de la red IPv6.

Como resultado de estas configuraciones tenemos que para los host que se manejan con VPCS las direcciones asignadas de la siguiente manera:

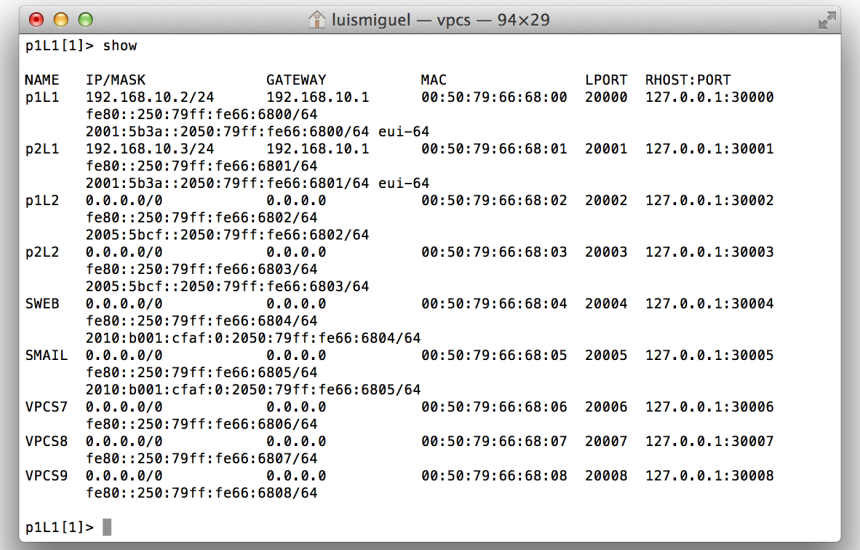


Figura 5.14 Tabla direcciones IP de los host, Autor: Luis Prieto

El comando show nos muestra todas las direcciones tanto IPv6 como IPv4 de cada uno de los host, para guardar la configuración utilizamos el comando save y el nombre de la configuración “save configuracion”. Cada vez que necesitemos guardar lo haremos con este método y si cerramos la consola VPCS simplemente haremos un “load configuracion” y obtendremos nuevamente todos nuestros parámetros configurados.

Los Routers también muestran cada uno su configuración de interfaces en las siguientes figuras:

RLAN1

Las direcciones IPv4

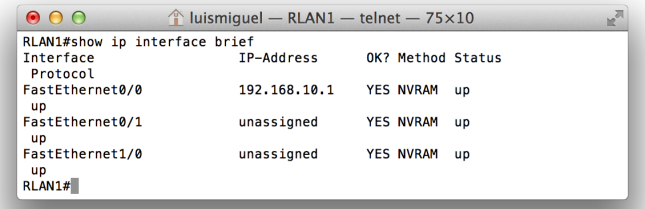


Figura 5.15 Interfaces IPv4 RLAN1, Autor: Luis Prieto

Las direcciones IPv6

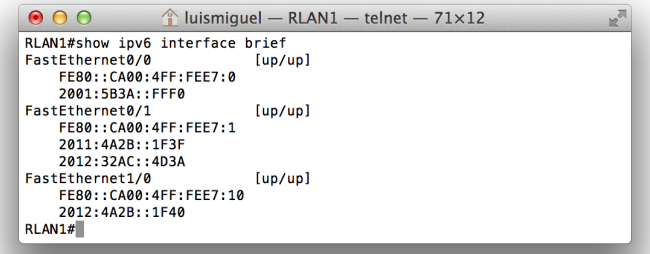


Figura 5.16 Interfaces IPv6 RLAN1, Autor: Luis Prieto

RLAN2

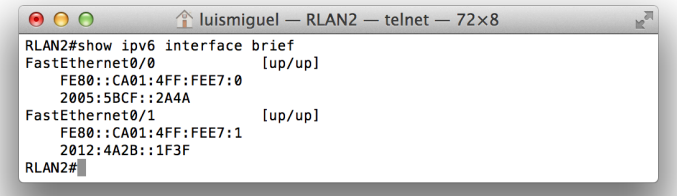


Figura 5.17 Interfaces IPv6 RLAN2, Autor: Luis Prieto

RLAN3

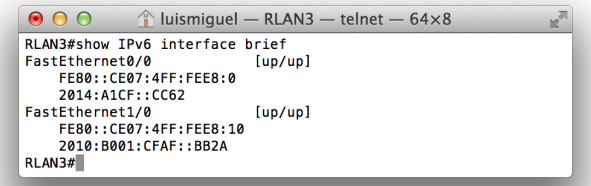


Figura 5.18 Interfaces IPv6 RLAN3, Autor: Luis Prieto

RWAN1

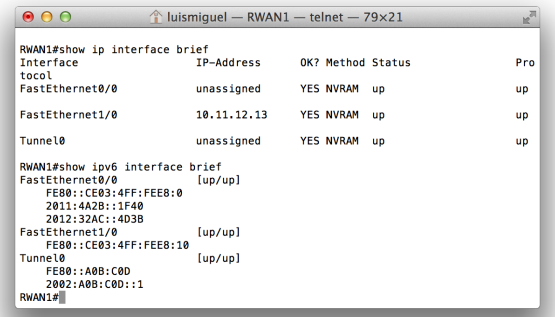


Figura 5.19 Interfaces IPv6 RWAN1, Autor: Luis Prieto

RWAN2

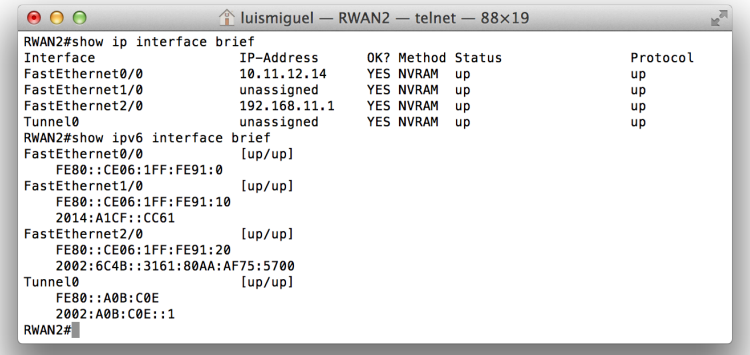


Figura 5.20 Interfaces IPv6 RLAN2, Autor: Luis Prieto

Otro paso importante de la simulación es configurar los switches que nos permitan tener mas de un host dentro de la LAN.

Se configuró un router con IOS cisco 3640, con el que vamos a emular un switch cisco añadiendo en la configuración las 16 interfaces.

Figura 5.21 Switch emulado desde router 3640, Autor: Luis Prieto

A este router cambiamos de nombre a switch LAN1 y procedemos a cambiar de ícono.

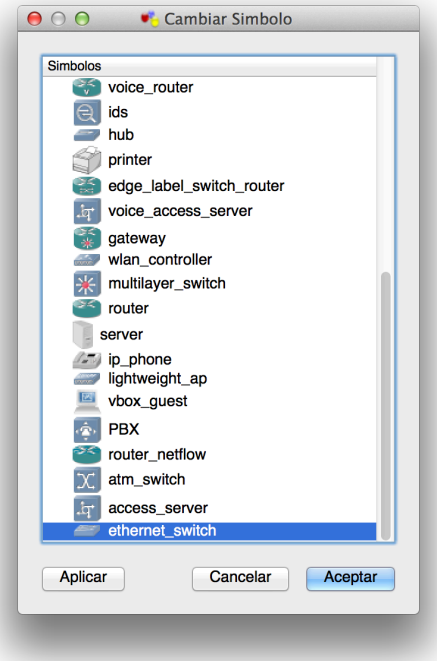


Figura 5.22 Cambio icono switch , Autor: Luis Prieto

Elegimos el ícono Ethernet switch y luego en la configuración en la pestaña slots seleccionamos el slot 0, y elegimos las interfaces NM-16ESW.

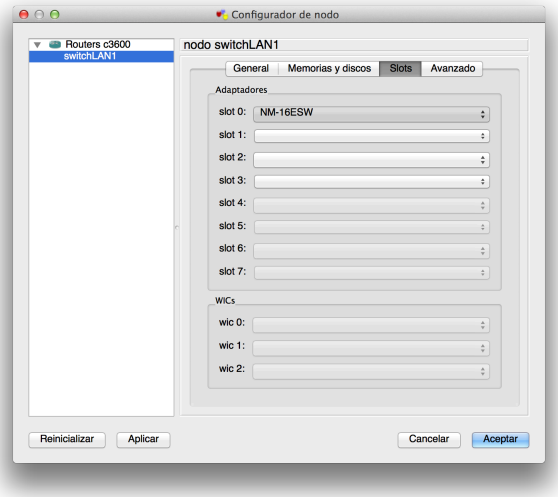


Figura 5.23 Elección de tarjeta de puertos Ethernet, Autor: Luis Prieto

Físicamente el switch está configurado, el siguiente paso es configurar el IOS para que la simulación quede completa. Donde simplemente con el command line haremos un “no shutdown” en las interfaces.

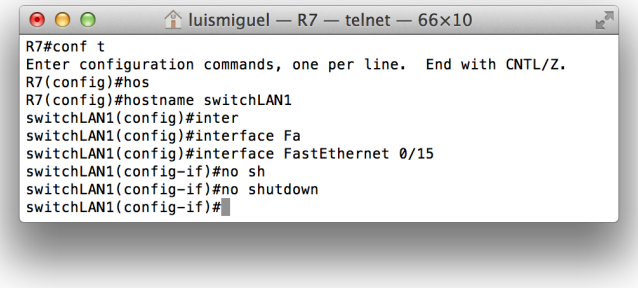


Figura 5.24 Habilita interfaces de switch, Autor: Luis Prieto

5.4 Configuración de Rutas dinámica y estáticas

En la configuración de rutas hay varios protocolos de enrutamiento de IPv6 , tanto como rutas estáticas como dinámicas, para la simulación hemos elegido el protocolo de enrutamiento OSPFv3, el que nos va ha permitir que exista conectividad en las rutas desconocidas para los routers, este protocolo se encarga de enviar cada 10 segundos un mensaje "hello" el que al tener respuesta indica el estado de la red y se puede mantener las mejores rutas para en envío de los paquetes.

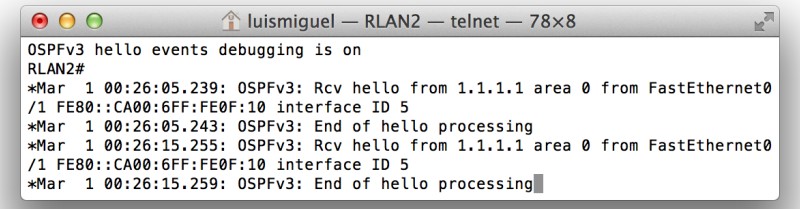


Figura 5.25 Modo debug en RLAN2 para OSPF, Autor: Luis Prieto

En cada router que maneje el protocolo se debe configurar el OSPFv3 el ID de OSPF en este caso es uno y el ID de cada router 1.1.1.1.

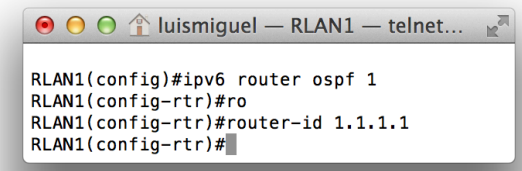


Figura 5.26 Configuración OSPF RLAN1, Autor: Luis Prieto

Todos los routers tienen que pertenecer a OSPF 1 para que se puedan comunicar, además de esto también a la misma área en este caso 0.

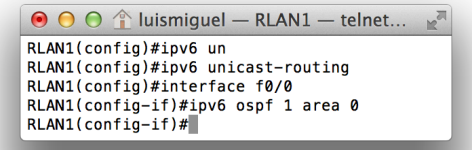


Figura 5.27 Configuración de OSPF para RLAN2 interfaz Ethernet, Autor: Luis Prieto

Configuraremos el protocolo OSPF en cada una de las interfaces que requiera que se conozca las rutas que no están directamente conectadas.

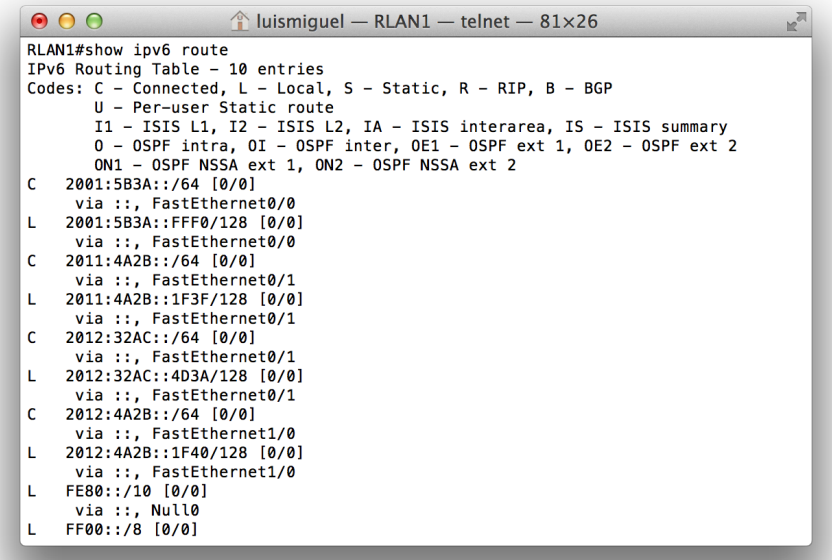


Figura 5.28 Tabla de inicial ruteo en RLAN1, Autor: Luis Prieto

Inicialmente cuando no se ha configurado OSPF, las rutas lucen de así, simplemente se muestra las rutas locales es decir, las interfaces que se conectan directamente a otras rutas, después de la configuración de OSPF, el resultado es distinto.

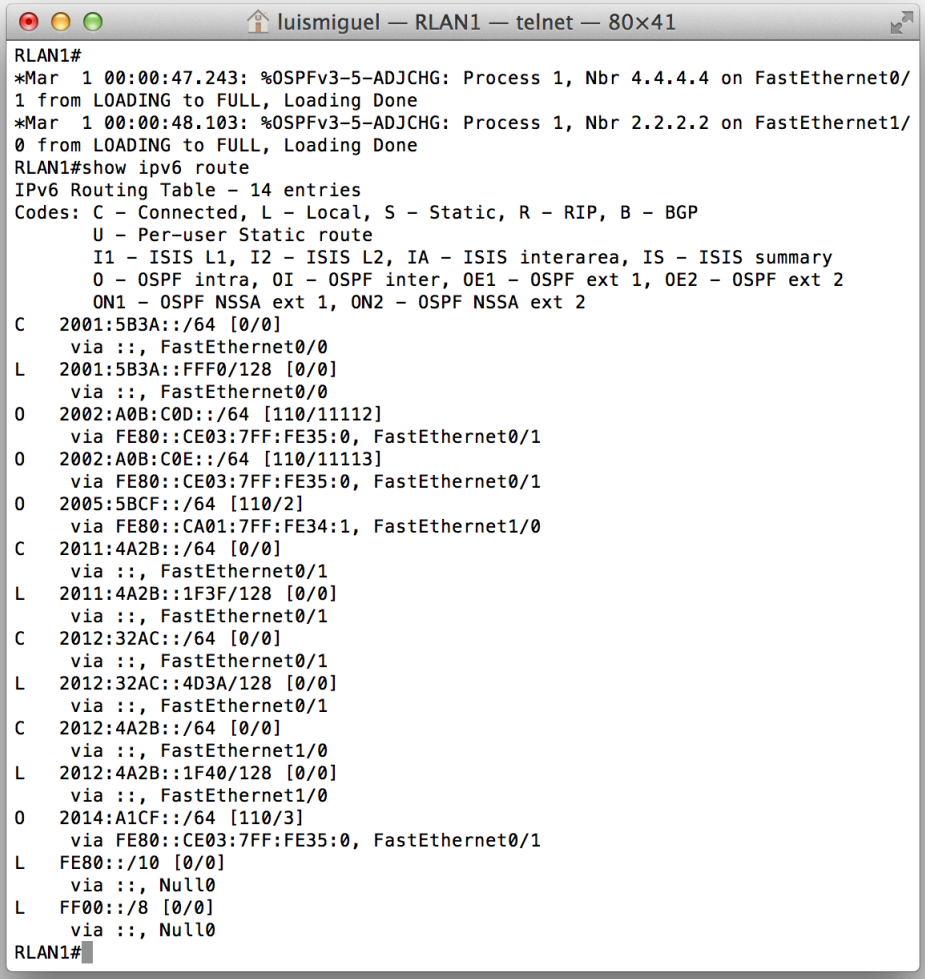


Figura 5.29 Tabla de ruteo configurado con OSPF en RLAN1, Autor: Luis Prieto

Ahora se muestran las rutas directamente conectadas y las de los siguientes saltos, por ejemplo en f0/1 la red 2012:32AC::4D3A/64 esta conectada localmente es decir es una red conocida pero se agrego la red con el protocolo OSPF 2014:A1CF::/64 vía f1 0/11 la que en la topología equivale a la red IPv6 en la interface f1/0. Lo que se ha logrado es que exista conectividad ahora con las redes que no estaban directamente conectadas a los routers.

5.5 Configuración de Tunneling

EL Tunneling es el último paso para completar la conectividad en toda la topología de la red, dependiendo del segmento hemos elegido un tipo de túnel.

En el caso de la red LAN1 existen tres interfaces, la interfaz f0/0 es la que no tiene acceso a las demás ya que esta trabaja con el protocolo IPv4, para este caso específico trabajaremos con un túnel estático tipo Dual Stack. Para configurar esta técnica de transición de IPv4 a IPv6, debemos utilizar el comando “unicast-routing” el que permite activar el uso de IPv6 en cualquiera de la interfaces en el.

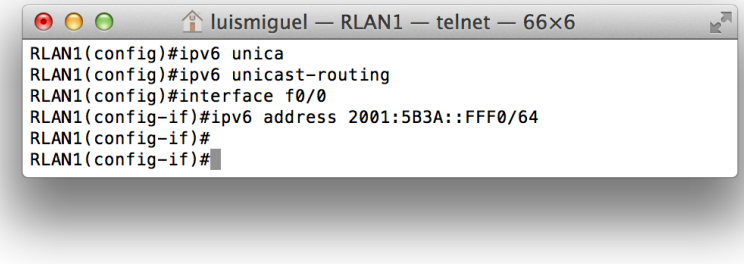


Figura 5.30 Configuración Dual Stack RLAN1, Autor: Luis Prieto

Activamos en los host las direcciones IPv6, en el momento que los paquetes se encuentren en un ambiente IPv4, se utilizarán las direcciones IPv4 y si un paquete necesita salir a otro ambiente utilizarán las direcciones IPv6 asignada a las interfaces, es decir que cada host tendrá asignado 2 direcciones de red tanto como una IPv4 como una IPv6.

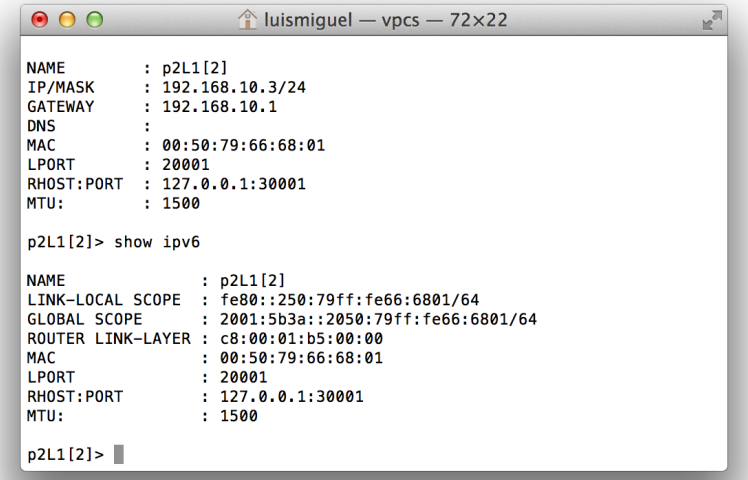


Figura 5.31 Tabla de configuración de la p2L1, Autor: Luis Prieto

En este caso el pc2LAN1 tiene asignado dos direcciones la IPv4 la 192.168.10.3/25 y la 2001:5B3A::FFF0/64, con las que podrá transmitir paquetes a todas las interfaces de la red. La dirección FE80::250:79FF:FE66:6801/64 utiliza un prefijo de enlace local la que únicamente es usada para las subredes

El otro segmento de red que necesita configuración de tunneling es entre el RWAN1 y RWAN2, estos están conectados entre si mediante

el protocolo IPv4 y tienen salida al protocolo IPV6. Utilizaremos el túnel automático IPv6 to IPv4 el que nos permitirá hacer un túnel IPv6 y que los paquetes viajen sin problema entre los dos routers.

El primer paso antes de que funcione el túnel debemos tener configurado OSPF para que luego de activado el túnel se conozcan todas las rutas aledañas y pueda haber conectividad entre los dispositivos de diferentes redes, este paso ya fue previamente preparado por lo que lo siguiente ha realizar es obtener una dirección IPv6 reservada para IPv6 to IPv4 con el prefijo 2002::/16, este prefijo es utilizado para direcciones 6to4. El router nos generará automáticamente la dirección IPv6, solamente hay que hacer la petición.

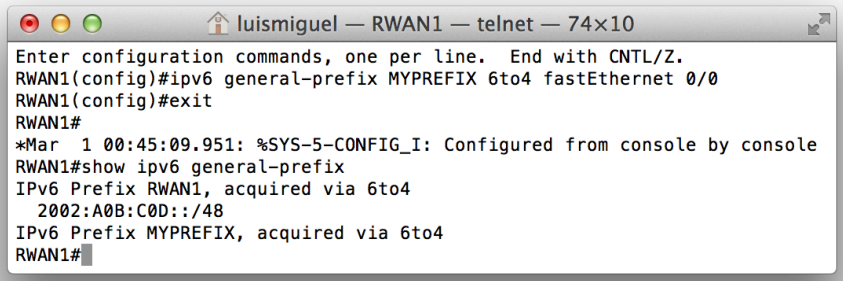


Figura 5.32 Configuración del prefijo en RWAN1, Autor: Luis Prieto

con el comando "ipv6 general-prefix MYPREFIX 6to4 fastEthernet 0/0" le decimos al router que genere una dirección única IPv6 con el prefijo 6to4, la dirección IPv6 se genera automáticamente y con el comando "show ipv6 general-prefix" obtenemos la dirección de red de

ese prefijo. Luego establecemos la misma configuración para el router RWAN2 y ya se ha establecido las direcciones IPv6 que utilizaremos para el túnel.

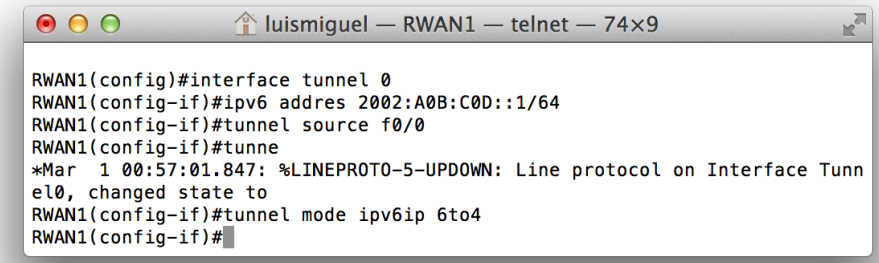


Figura 5.33 Aplicando tunneling a la dirección reservada, Autor: Luis Prieto

para configurar el túnel creamos una interfaz con su ID en este caso tunnel 0, asignamos una dirección IPv6 dentro de nuestra red con el prefijo 6to4 que el router nos ha asignado, luego le decimos al router que nos haga un túnel en la interfaz deseada con el comando “tunnel source f0/0” y terminamos el túnel asignando el tipo de túnel que vamos a configurar, para nuestro caso 6to4 con la línea de comandos “tunnel mode ipv6ip 6to4” así nuestro túnel es configurado, hacemos el mismo procedimiento para el otro router y ya podrán intercambiar los routers paquetes IPv6, para que toda la topología tenga conectividad se debe activar el protocolo OSPFv3 en la interfaz tunnel 0 de cada router WAN, para que propaguen todas las rutas que pertenecen a la RED.

El resultado final después de la configuración de las direcciones de red IPv4, IPv6, OSPF y tunneling se muestran en las siguientes tablas.

RLAN1

Archivo de configuración final

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RLAN1
!
boot-start-marker
boot-end-marker
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
ip cef
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:5B3A::FFF0/64
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2011:4A2B::1F3F/64
 ipv6 address 2012:32AC::4D3A/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
```

```
 ipv6 address 2012:4A2B::1F40/64
 ipv6 ospf 1 area 0
!
ip http server
ip classless
!
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Tabla 5.8 Configuración RLAN1, Autor: Luis Prieto

RLAN2

Archivo de configuración final

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
ip cef
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
no ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Tabla 5.9 Configuración RLAN2, Autor: Luis Prieto

RWAN1

Archivo de configuración final

```
Current configuration : 1086 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RWAN1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 general-prefix RWAN1 6to4 FastEthernet1/0
!
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A0B:C0D::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source FastEthernet1/0
```

```
 tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2011:4A2B::1F40/64
 ipv6 address 2012:32AC::4D3B/64
 ipv6 ospf 1 area 0
!
interface FastEthernet1/0
 ip address 10.11.12.13 255.255.255.252
 duplex auto
 speed auto
 ipv6 enable
 ipv6 ospf 1 area 0
!
ip http server
no ip http secure-server
!
ip forward-protocol nd
!
ipv6 router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Tabla 5.10 Configuración RWAN1, Autor: Luis Prieto

RWAN1

Archivo de configuración final

```
Current configuration : 1086 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RWAN1
```

```
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 general-prefix RWAN1 6to4 FastEthernet1/0
!
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A0B:C0D::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source FastEthernet1/0
 tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2011:4A2B::1F40/64
 ipv6 address 2012:32AC::4D3B/64
 ipv6 ospf 1 area 0
!
interface FastEthernet1/0
 ip address 10.11.12.13 255.255.255.252
 duplex auto
 speed auto
 ipv6 enable
 ipv6 ospf 1 area 0
!
ip http server
no ip http secure-server
!
ip forward-protocol nd
!
ipv6 router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
!
control-plane
!
line con 0
```

```
line aux 0
line vty 0 4
 login
!
!
end
```

Tabla 5.11 Configuración RWAN1, Autor: Luis Prieto

RWAN2

Archivo de configuración final

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RWAN2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 general-prefix RWAN2 6to4 FastEthernet0/0
interface Tunnel0
 no ip address
 no ip redirects
 ipv6 address 2002:A0B:C0E::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip 6to4
!
interface FastEthernet0/0
 ip address 10.11.12.14 255.255.255.252
 duplex auto
 speed auto
 ipv6 enable
 ipv6 ospf 1 area 0
!
```

```
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2014:A1CF::CC61/64
 ipv6 ospf 1 area 0
!
interface FastEthernet2/0
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2002:6C4B::3161:80AA:AF75:5700/64
 ipv6 ospf 1 area 0
!
no ip http server
no ip http secure-server
!
ip forward-protocol nd
!
!
ipv6 router ospf 1
 router-id 5.5.5.5
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Tabla 5.12 Configuración RWAN2, Autor: Luis Prieto

RLAN3

Archivo de configuración final
Current configuration : 835 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname RLAN3 !

```
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2014:A1CF::CC62/64
 ipv6 ospf 1 area 0
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2010:B001:CFAF::BB2A/64
 ipv6 ospf 1 area 0
!
no ip http server
no ip http secure-server
!
ip forward-protocol nd
!
!
ipv6 router ospf 1
 router-id 7.7.7.7
 log-adjacency-changes
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Tabla 5.13 Configuración RLAN3, Autor: Luis Prieto

5.6 Verificación de Conectividad de nodos en el simulador

Probaremos la conectividad con involucrando al host p1L2 y el host SWEB, los que pertenecen a la LAN2 y LAN3 respectivamente, estos host manejados con VPCS, por lo que solamente podremos probar la conectividad mediante el comando ping o enviando paquetes ICMP.

El simulador GNS3 tiene un sniffer incluido llamado Wireshark el que nos permitirá capturar paquetes en los diferentes nodos que existen en la topología. Ubicaremos el sniffer en la primera salida del paquete luego en el túnel 6to4 donde conectan RWAN1 y RWAN2, para terminar en el nodo terminal que sería SWEB.

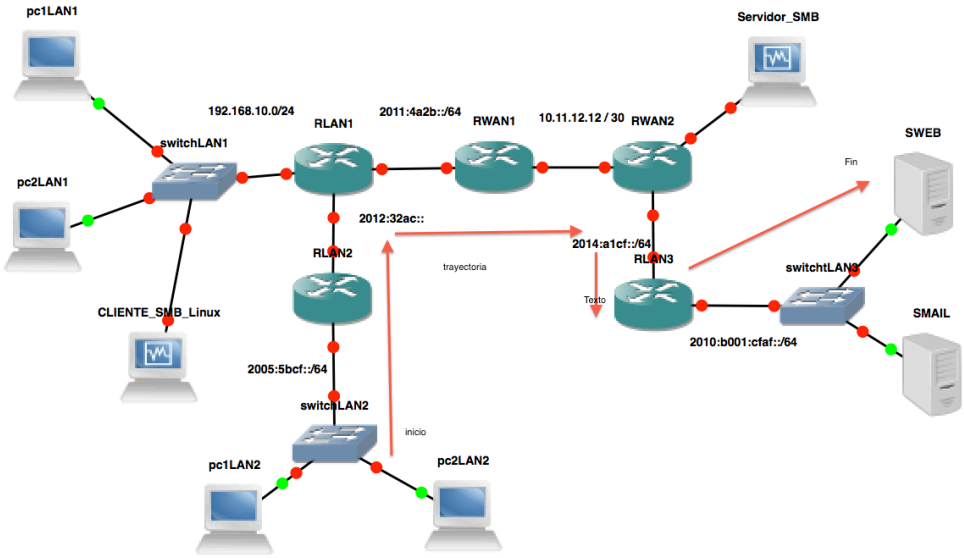


Figura 5.34 Trayectoria del paquete ICMPv6, Autor: Luis Prieto

En la figura 5.34 podemos ver la trayectoria del paquete, iniciando el la p1L2 que pertenece a la RLAN2, este segmento de red está configurado con direcciones IPV6.

Con el Comando ping iniciaremos la prueba de conectividad desde p1L2 hacia SWEB.

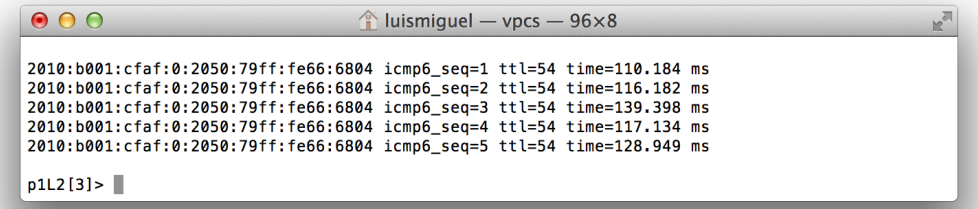


Figura 5.35 Ping p2L2 hacia SWEB, Autor : Luis Prieto

La prueba de conectividad realizada desde p1L2 a SWEB podemos concluir que fue exitosa, el paquete a completado su trayectoria en el analizaremos tres puntos sobre los nodos de la trayectoria.

El punto inicial se da en el router RLAN2 donde el router eviará a la dirección destino que es la de SWEB 2005:5bcf::2050:79ff:fe66:6802, el resultado del echo request es el siguiente:

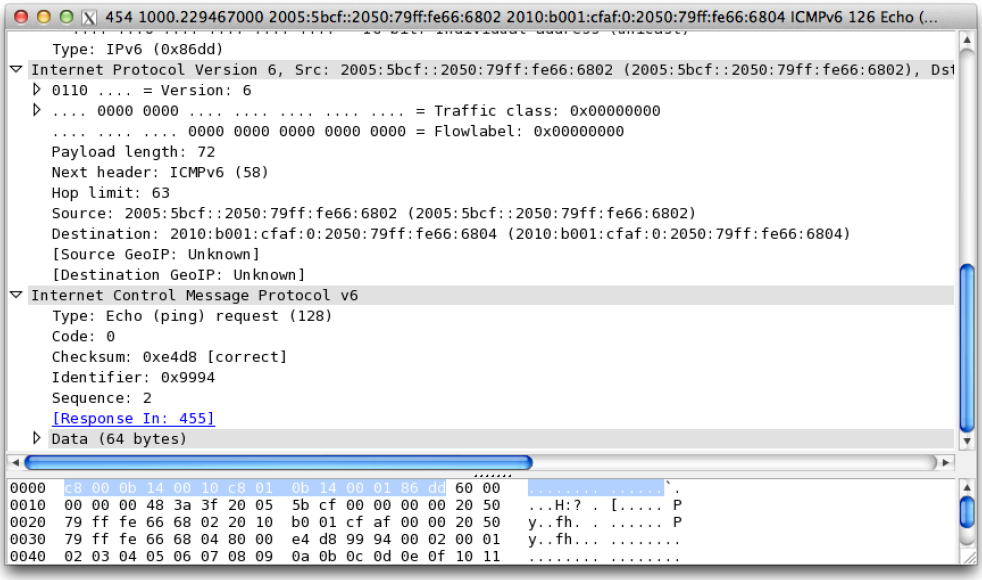


Figura 5.36 Captura paquete echo RLAN2, Autor Luis Prieto

Donde podemos ver el resultado para RLAN2 que la dirección de origen es 2005:5bcf::2050:79ff:fe66:6802 y la de destino la 2010:b001:cfaf:0:2050:79ff:fe66:6804 que corresponde a SWEB. El siguiente nodo que analizaremos donde hay cambio de red equivale a RWAN2.

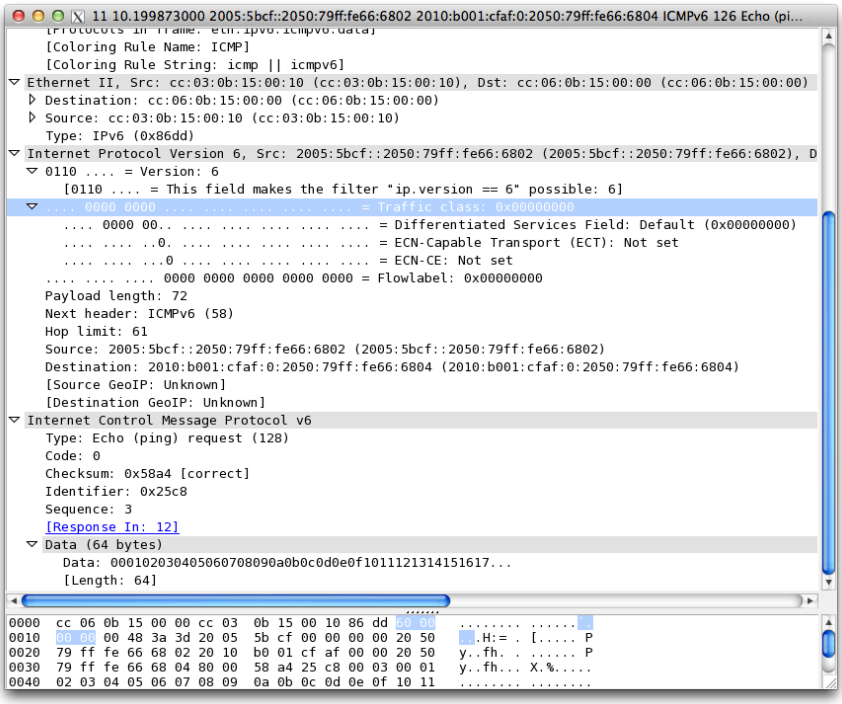


Figura 5.37 Captura paquete echo RWAN2, Autor Luis Prieto

Al igual que en el primer nodo también se presenta las direcciones de origen y destino, en este segmento de la red es donde se aplica 6to4, debido a que el protocolo que está funcionando entre los dos routers IPv4.

El último nodo para analizar es en RLAN3 donde podemos observar finalmente que el paquete contiene la dirección IPv6 de origen como la de destino.

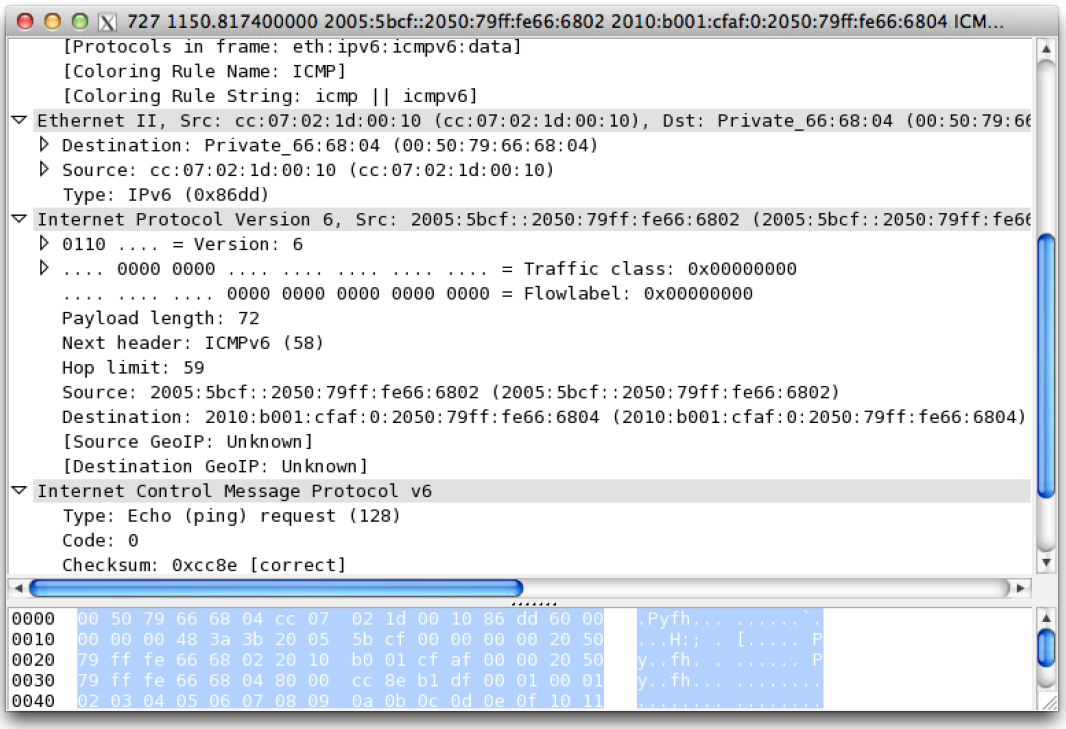


Figura 5.38 Ping a SWEB desde p1L2, Autor Luis Prieto

Claramente podemos observar que cuando se trabaja sobre el protocolo IPv6 se necesita necesariamente que todos los nodos funcionen sobre esos protocolos y se ha demostrado mediante el seguimiento de la trayectoria del paquete.

Otras de las pruebas de conectividad que analizaremos es mediante el envío de un archivo desde un servidor de archivos, para esto se ha configurado dos máquinas virtuales una que funciona como cliente y la otra como servidor, las dos máquinas están siendo manejadas dentro de virtualBox, además el sistema operativo es Ubuntu Server versión 14.04.

Los dos host se encuentran en diferentes LAN, el cliente pertenece a la LAN1 y el servidor es una terminal de RWAN2. El cliente maneja el

protocolo IPv4 con dirección 192.168.10.4, pero al mismo tiempo debido a que este segmento de red fue configurado con IPv6 para Dual Stack también maneja una dirección IPv6 la que corresponde a 2001:5b3a::2050:79ff:fe66:6813, la que nos permitirá salir hacia las redes externas que manejan IPv6. El servidor también maneja una dirección IPv4 y se ha asignado al mismo tiempo una dirección IPv6 global 2002:6c4b::3161:80aa:af75:5701 la que será usada cuando se necesite el alcance desde una dirección externa IPv6, es importante también recalcar que para que las redes IPv6 se propaguen dentro de toda la topología se ha usado OSPF el que nos mantendrá actualizadas las redes automáticamente dentro de cada router.

Para iniciar el análisis probaremos conectividad con el comando ping dentro del cliente terminal de Ubuntu Server hacia el Servidor.

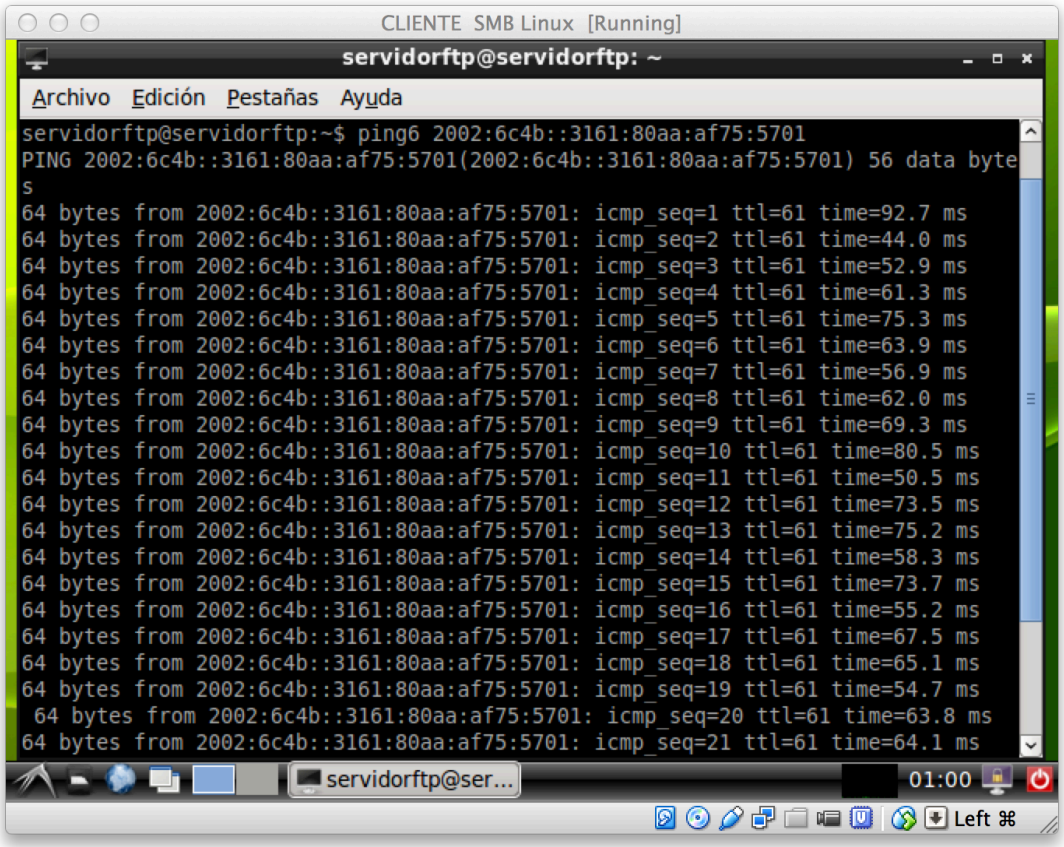


Figura 5.39 Prueba de conectividad Cliente Servidor, Autor: Luis Prieto

Haciendo ping hacia el servidor el resultado es que si existe conectividad, hacia la dirección 2002:6c4b::3161:80aa:af75:5701 que corresponde al servidor, luego de la verificación podemos iniciar a compartir archivos. Existen varias maneras de intercambiar archivos usando diferentes protocolos como SAMBA, FTP y SSH entre otros para nuestro ejemplo utilizaremos el SSH que funciona vía comandos y es sencillo de configurar, solo debemos tomar en cuenta que el puerto 22 debe estar habilitado es decir que en el firewall de Linux no

se encuentre cerrado este puerto ya que es por el cual escucha la conexión SSH.

De acuerdo a lo establecido podemos empezar a compartir archivos entre el cliente y el servidor.

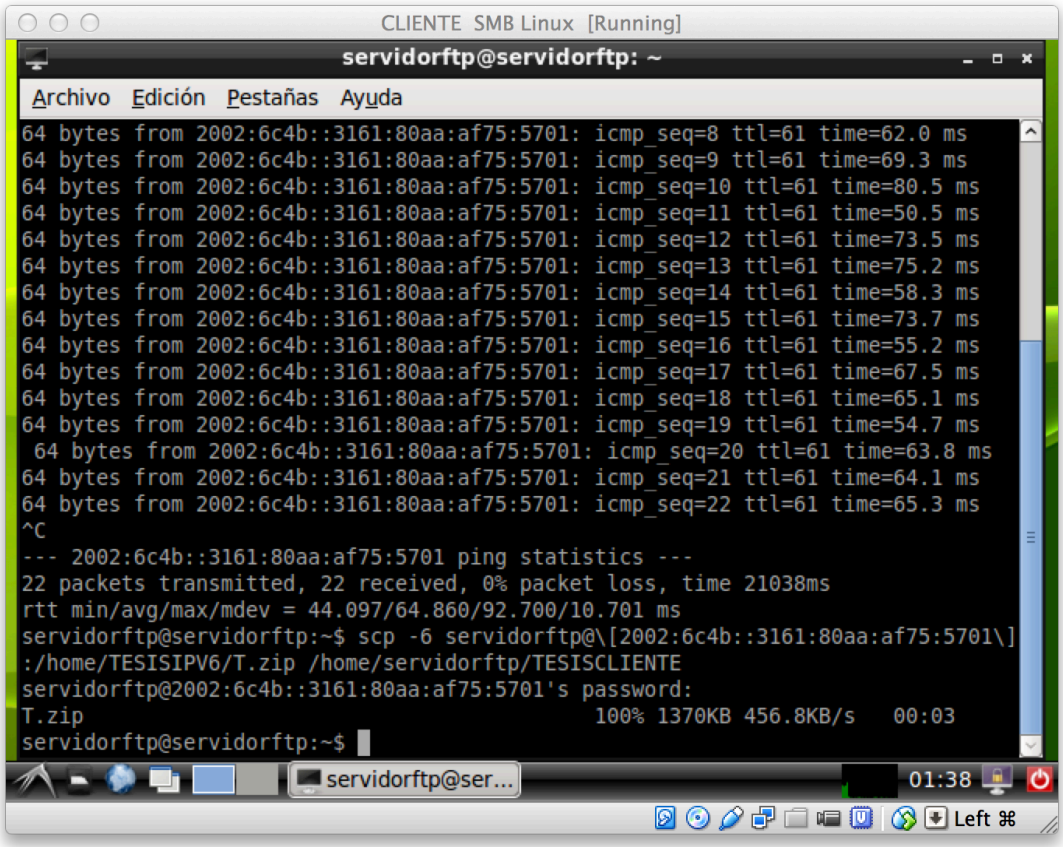


Figura 5.40 Comando SSH para compartir archivos, Autor: Luis Prieto

El comando scp es el que nos servirá para copiar el archivo desde el servidor, debe ir acompañado con -6 que nos hace referencia a que estamos usando una dirección IPv6, luego de ello establecemos la dirección de nuestro servidor 2002:6c4b::3161:80aa:af75:570, luego la carpeta de origen y la de destino. Si el proceso fue exitoso, tendremos como resultado un 100% de transmisión.

La herramienta de simulación tiene funcionalidades bastante poderosas que inclusive permite compartir archivos dentro de la simulación, debido a esta funcionalidad se ha podido completar el proceso de compartir archivos de diferentes LAN.

Hemos compartido el archivo T.zip desde el servidor al cliente, lo que demuestra que no solamente se puede hacer la simulación en GNS3 a nivel de conectividad sino también a nivel de servicio y sistemas operativos, dando así un resultado más apegado a la realidad.

CAPÍTULO VI

6 Conclusiones y recomendaciones

6.1 Conclusiones

- El protocolo IPv6 es totalmente compatible con su antecesor el protocolo IPv4, debido que existe varias maneras de establecer esta conexión, tanto como el Dual Stack como el tunneling, son las soluciones mas viables y económicas antes que se produzca la transición completa a IPv6.
- La configuración de equipos terminales se debe aplicar de manera automática debido a la complejidad de las direcciones IPv6, es muy complicado para un usuario común e inclusive para técnicos especializados que puedan configurar estas direcciones, por lo que se recomienda que el router se encargue de dar este servicio.
- Para establecer conectividad entre toda la red es necesario usar la configuración de las rutas, ya que cada router a pesar de saber las rutas directamente conectadas, desconoce las del siguiente salto, por lo que debemos configurar las rutas, para este caso se aplico modo OSPFv3 que es la que se aplica para Ipv6.
- IPv6 actualmente en Ecuador está tomando fuerza debido a la agotamiento de direcciones IPv4, no solamente en Ecuador sino

a nivel mundial, se espera según el ipv6tf IPv6 Task Force Ecuador en el 2016 el Ecuador ya tendrá un porcentaje considerable de penetrabilidad del protocolo.

- GNS3 es una herramienta de simulación muy poderosa y eficaz donde se puede mostrar resultados con redes altamente complejas sin necesidad de equipos físicos, además que el simulador permite crear situaciones reales como la conexión con máquinas virtuales, con el host que está manejado la simulación y por ende con equipos externos, por lo que la simulación puede tornarse más real al conectar también equipos físicos.
- GNS3 también nos da más opciones al momento de hacer simulaciones debido a que usa máquinas virtuales o se conecta directamente a host físicos, los que a su vez cargan sistemas operativos. En este caso la herramienta nos da la facilidad de usar todas las funcionalidades de los sistemas operativos, fácilmente podemos crear servidores de archivos, servidores web o manejar otro tipo de servicios según el sistema operativo, los que harán más real y consistente las simulaciones.

6.2 Recomendaciones

- Se recomienda usar un protocolo de enrutamiento dinámico, este nos va a permitir tener un control y acceso a las rutas de manera mas sencilla. En caso de que apliquemos un protocolo de red estático podríamos terminar cometiendo errores o se podría omitir rutas, lo que nos puede causar perdida de tiempo y que la conectividad y los accesos a los nodos se pierdan.
- Para que la simulación sea más apegada a la realidad es importante que se usen todas las herramientas de GNS3, el virtualBox, nos va permitir usa la virtualización de sistemas operativos con todas sus funcionalidades, de así tendremos más opciones al momento de probar conectividad entre los host.
- Es una buena opción cargar un sistema operativo con virtualBox liviano que no consuma muchos recursos al momento de inicial la simulación, se recomiendo utilizar Linux Server, el que nos da todas las potencialidades de un sistema operativo completo, pero con baja carga al momento de la simulación, si es necesario instalar el modo gráfico o manejar a nivel de consola y aplicar los comandos necesarios para que se ejecuten las operaciones.
- Las redes IPv4 dentro de las organizaciones empresariales tendrán mayor vigencia por lo que en estos casos debemos

decidir sobre cual es el mejor método para el intercambio de paquetes entre IPv4 e IPv6, tanto como el Dual Stack y la configuración de tunneling automáticos o manuales, serán importantes para dar solución a esta coexistencia.

Bibliografía

ILJITSCH VAN BEIJNUM. Running IPv6. Unites States of America.

Springer-Verlag. 2006.

TANENBAUM, A.S., Redes de Computadoras. 3a. ed. México. 1997.

JOSEP DAVIES. Understanding IPv6. United States of America. 2003

SILVIA HAGEN. IPv6 Essentials. 2da. ed. O'Reilly. 2006

(http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf)

Routing IPv6 Over IPv4
(http://www.cisco.com/web/about/ac123/ac147/ac174/ac197/about_cisco_ipj_archive_article09186a00800c830a.html)
Consultado: 2014-01-25.

Six Benefits of IPv6
(http://www.networkcomputing.com/networking/six-benefits-of-ipv6/d/d-id/1232791?)
Consultado: 2014-01-02.

R. Gilligan
RFC 2893
(http://www.ietf.org/rfc/rfc2893.txt)
Consultado:2013-12-12

Cisco
IP Routing: ISIS Configuration Guide, Cisco IOS Release 12.2SY
(http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/12-2sy/irs-12-2sy-book.pdf)
Consultado:2014-02-22.

RFC 2545
P. Marques
(http://tools.ietf.org/html/rfc2545)
Consultado:2014-02-22.

PEPJ
IPv4 to IPv6 converter

http://www.subnetonline.com/pages/subnet-calculators/ipv4-to-ipv6-converter.php
Consultado: 2014-04-23.

Anexos

Manual de Instalación GNS3

GNS3 es una herramienta de simulación gráfica que nos permite simular redes muy complejas que permite adaptar la virtualización de sistemas operativos como VirtualBox, de modo que permite manejar ambientes bastante reales, permitiendo la interconexión entre sistemas operativos como Linux, Windows y Mac OS en ambientes enfocados a la virtualización. La ventaja principal de esta compatibilidad con la virtualización de sistemas operativos, es que se puede trabajar con mayor precisión que una línea de comandos en VPCS, es decir, que tenemos acceso a más comandos que nos permitan más información de rutas y conectividad que un simple comando ping.

Requisitos para la Instalación

MacOS Snow Leopard o superior

GNS3 v0.8.2

VPCS virtual pc simulator

VirtualBox 4.3.10 o superior

Descarga GNS3 v0.8.2

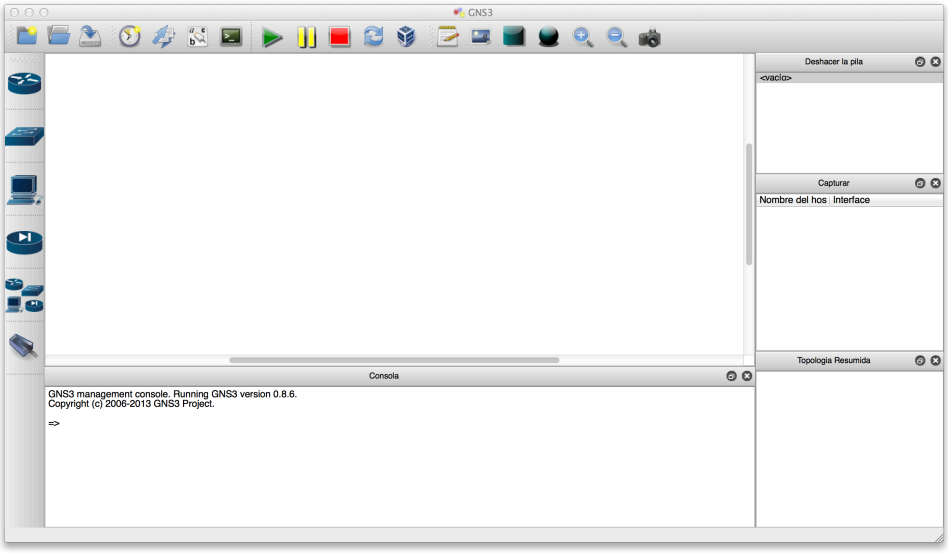
Para la descarga navegamos al siguiente link http://www.gns3.net/download/ y descargamos GNS3 V0.8.2 versión para mac

Mac OS X

- GNS3 v0.8.7 DMG package (OSX with Python2.7 only, includes Dynamips, Qemu and VPCS).
- GNS3 v0.8.2 Snow Leopard DMG package (OSX 10.6 Snow Leopard only, includes Dynamips).

Cuando la descarga esté completa obtendremos un archivo .dmg, el cual consta con un archivo que arrastramos y copiamos a nuestra carpeta aplicaciones, así tenemos ya instalado nuestro GNS3 en MACOS.

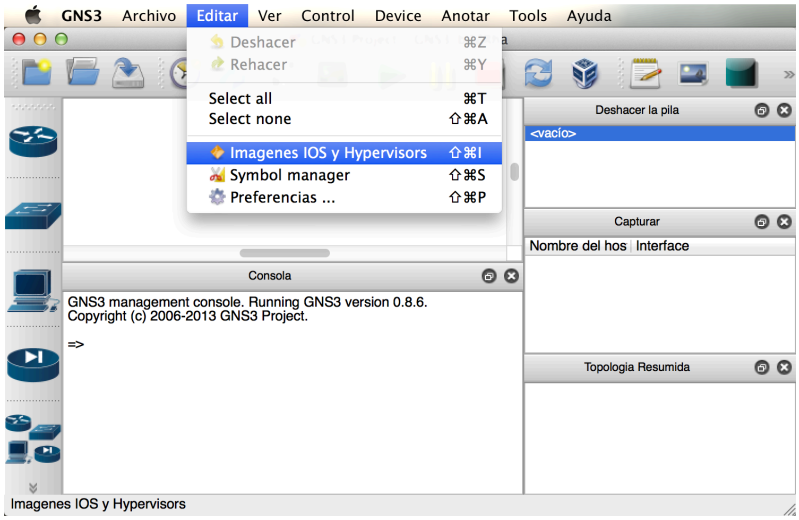
Ahora damos doble clic en la aplicación y se abrirá por primera vez lo que nos va como se muestra a continuación.



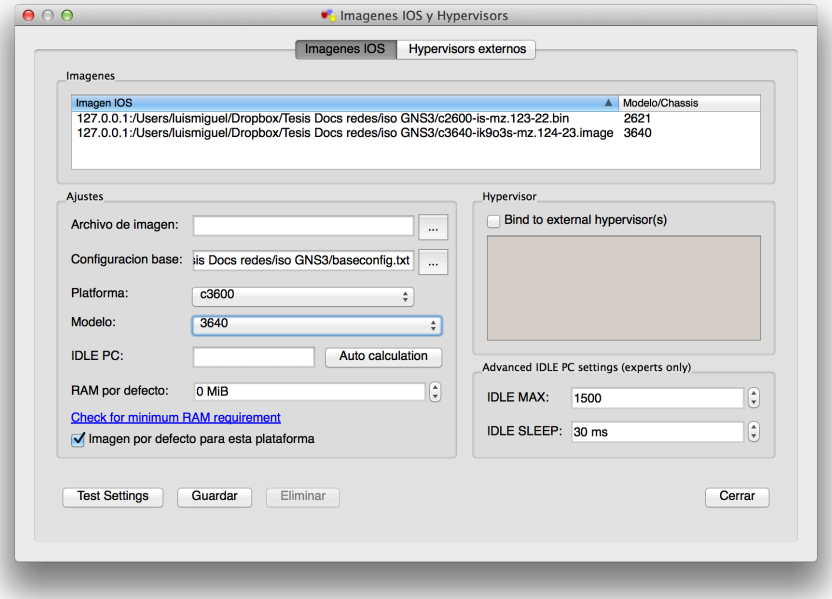
El primer paso a seguir para poner en marcha a nuestro GNS3, es descargar los IOS de los routers según el modelo que deseemos configurar. Debido a que GNS3 no incluye ningún IOS, primero debemos descargarlos, existen varios modelos en Cisco disponibles para realizar la simulación.

Primero descargamos de la página de GNS3 uno de los IOS de cisco, existen varios links, para este caso utilizaremos el IOS del router Cisco 3640.

En GNS3 damos clic en la ventana Editar y luego en imágenes IOS e Hypervisors.



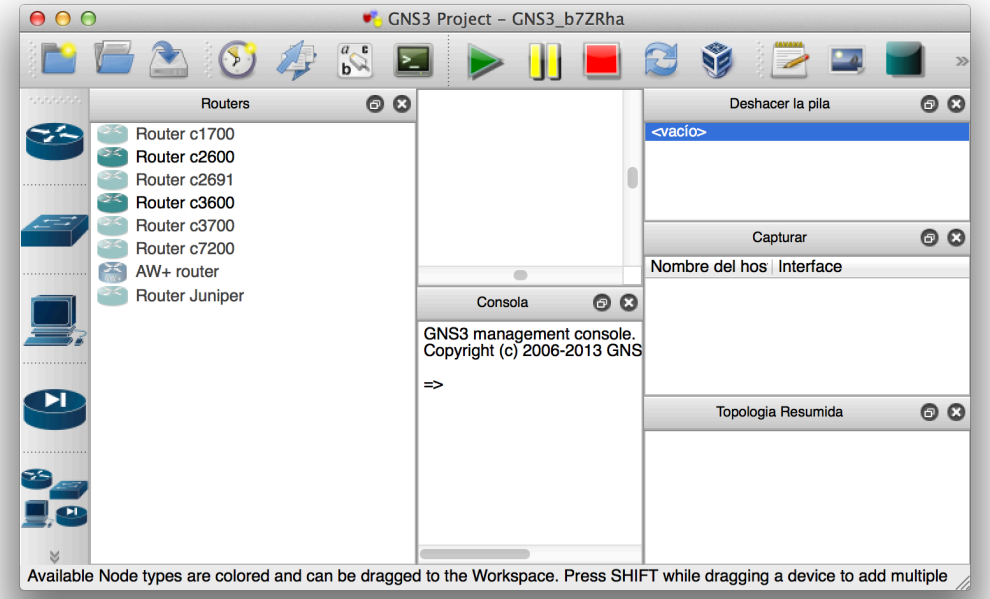
La que nos llevará a la ventana para agregar los IOS.



Damos clic en la configuración base, se abrirá el cuadro de búsqueda de la ruta donde se encuentra nuestra imagen, elegimos la ruta y por ende nuestro archivo de imagen que para este caso es el 3640. Los archivos pueden ser binarios .bin o archivos de imagen .img, en los dos casos serán válidos para cargar el IOS a nuestro router. Una vez cargado el IOS, se cargarán los parámetros por defecto en la pantalla,

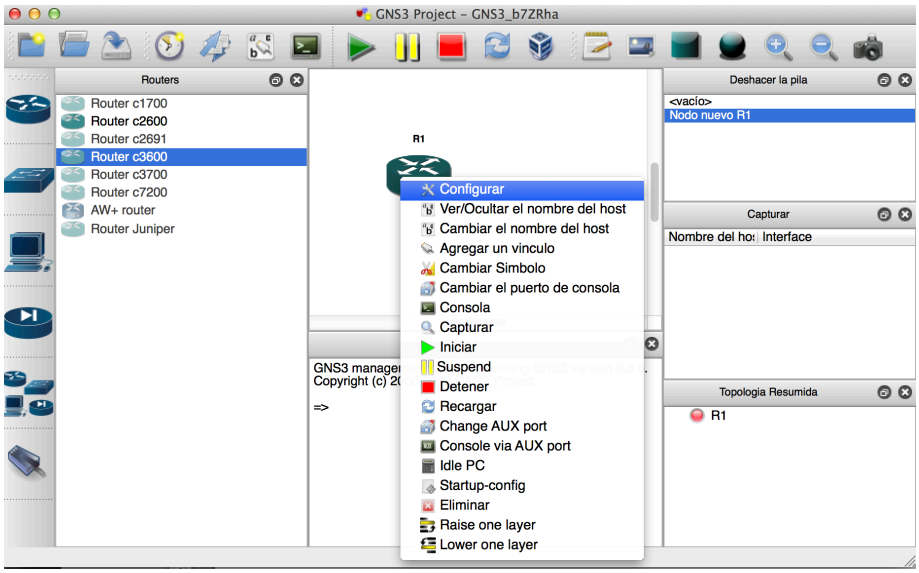
los que no es necesario cambiar ya que mas adelante los podemos configurar a nuestro gusto. Una vez agregado nuestro IOS está listo para ser usado en cualquiera de nuestros routers que están dentro del simulador GNS3, la mejor manera de aplicar el IOS es usando el router según el modelo de nuestro IOS, es decir que si descargamos un IOS 3640, utilicemos el case dentro de la plataforma los 3600 y aparecerá en el modelo el que necesitamos en este caso 3640 luego damos clic en guardar y cerramos el cuadro de diálogo.

Inicialmente si tratamos de arrastrar al área de trabajo el router, solamente será posible los que tengan configurados los IOS, los que no permanecerán inhabilitados hasta que se configure con algún IOS.

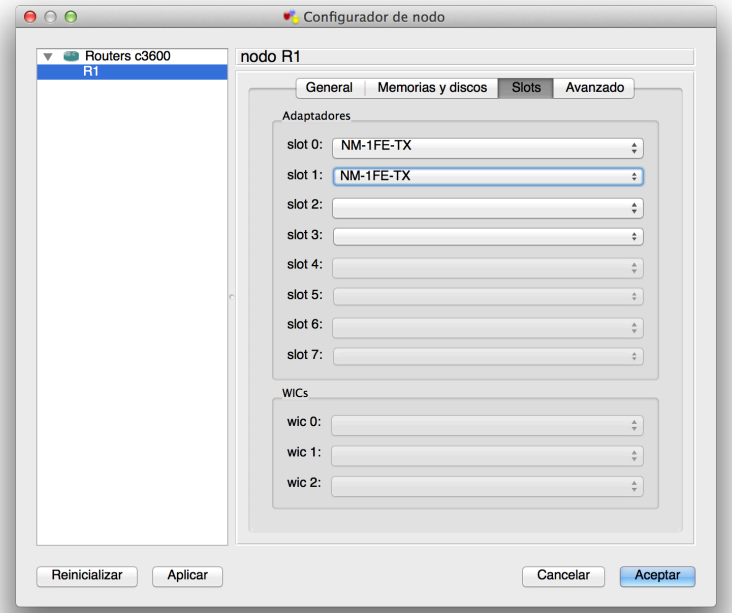


En este caso están habilitados los c3600 y los c2600. Para lograr este paso es necesario que al router le indiquemos que IOS va ha funcionar como predeterminado como lo hicimos en el paso anterior. Después de todo esto ya estamos listos para inicializar nuestro router de tal manera que tengamos una configuración inicial para todos los routers 3600 dentro del proyecto.

Para configurar el router 3600 lo arrastramos al área de trabajo, luego damos clic derecho y elegimos configuración y le damos clic.

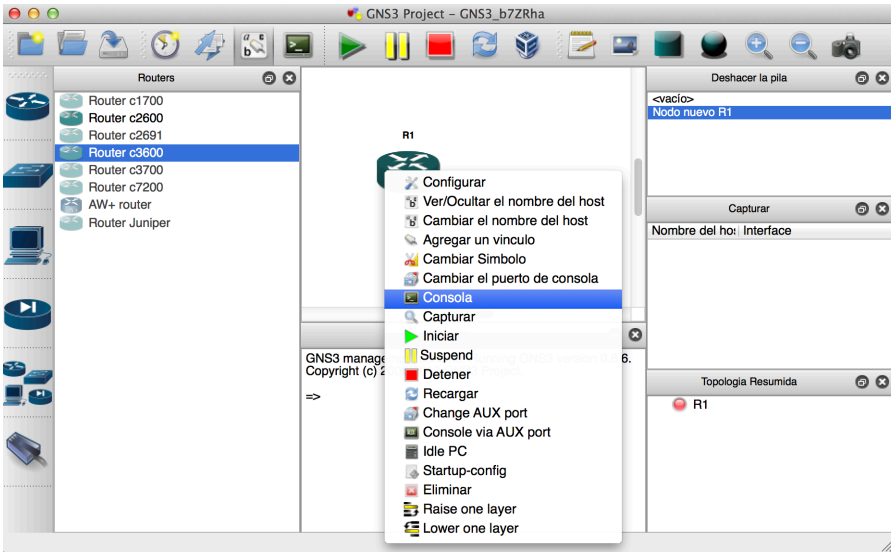


Dentro de la configuración debemos configurar los parámetros más importantes, para este caso debemos agregar las interfaces que queremos que el router contenga, de la misma manera que en los routers físicos se puede agregar interfaces seriales, Ethernet o FastEthernet, también se puede en los virtuales, para este ejemplo agregaremos dos interfaces FastEhternet de la siguiente manera.

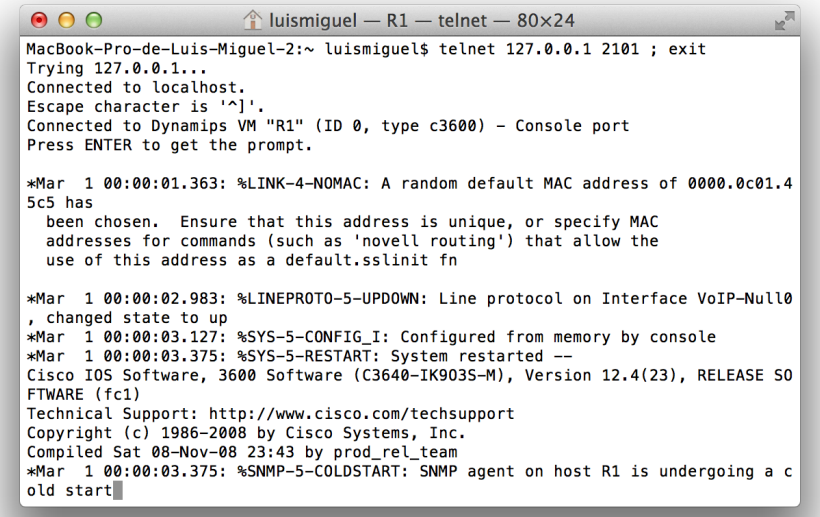


Las NM-1FE-TX equivalen a las interfaces FastEthernet. Una vez elegidas las interfaces deseadas aceptamos. Ahora es el momento para configurar el router con la configuración inicial.

En el paso siguiente damos clic derecho al router y elegimos consola el que nos va a desplegar el modo consola del router, el paso previo a la configuración de la consola es arrancar la simulación con el símbolo play.



una vez arrancado el router iniciará la consola y los comandos de arranque.



Al tratarse de un router cisco usaremos los comandos de cisco para configurar el router. De manera que ya tenemos inicializado el router 3640 y lo podremos utilizar una y otra vez en cada proyecto que creemos, podemos guardar en archivos las configuraciones iniciales

siempre que deseemos. Además de la misma manera que los routers físicos cisco debemos guardar la runnig-config en la startup-config es decir, la configuración que está corriendo en la de arranque, si omitimos este paso no se guardará ninguna configuración que hagamos en el router y cada vez que iniciemos nos pedirá que configuremos de nuevo.

Índice de Figuras y Tablas

Tablas

Figuras

Glosario

IPv6: Protocolo de Internet versión 6 que reemplaza a la versión 4.

Host: Computadoras que están conectadas a una red, que utilizan recursos y ofrecen servicios para el uso de la red.

IPv4: Protocolo de Internet versión 4, utiliza direcciones de 32 bits, es la versión actual usada en internet mientras se completa la transición a su sucesor el protocolo IPv6.

ICMPv4: Internet Control Message Protocol versión 4, es un protocolo de control de errores, que se usa para enviar mensajes de error, indica si un servicio no está disponible os si un host puede ser alcanzado o no.

ICMPv6: Internet Control Message Protocol versión 6, es la nueva versión de su antecesor ICMPv4, usado para detección de errores y diagnostico de redes.

RFC: Request for Comments es una publicación de la IETF y de la ISOC, con las principales con los principales desarrollos tecnológicos y estándares creados para Internet.

IETF: Internet Engineering Task Force, entidad que desarrolla y promueve estándares de internet.

ISOC: Internet Society, es una organización internacional que brinda liderazgo en estándares relacionados con Internet, educación y política

DHCP: Dynamic Host Configuration Protocol, es un protocolo de red que permite a todos los clientes de una red obtener una dirección y parámetros de configuración de manera automática y se pueda tener acceso a la misma.

IRDP: ICMP Router Discovery Protocol, permite a los host localizar routers que proveen conectividad IPv4 en una red.

TCP: Transmission Control Protocol**,** es un protocolo de internet de comunicación orientado a conexión fiable de transporte.

UDP: User Datagram Protocol, es un protocolo a nivel de capa de transporte que intercambia datagramas a través de una red sin que se haya establecido previamente una conexión, además no tiene confirmación ni control de flujo.

Payload: es la carga de datos, la parte transmitida de datos tiene la información del paquete.

PDU: Protocol Data Unit, información que es entregada como una unidad entre un par de entidades de red, contiene información de control como direcciones y datos de usuario.

MAC Address: Media Access Control Address, identificador de 48 bits que corresponde a una única tarjeta de red.

NAT: Network Address Translation, mecanismo que usan los routers para intercambiar paquetes entre dos direcciones que son incompatibles.

VOIP: Voice over IP, es un grupo de reglas que hace posible que la señal de voz viaje a través de internet sobre el protocolo IP.

RTP: Real-time Transport Protocol, protocolo utilizado para transmisión de información en tiempo real como audio y video

RTCP: Real Time Control Protocol, protocolo de comunicación que provee información de control sobre el flujo de datos de aplicaciones multimedia, la función principal es informar la calidad de servicio multimedia de RTP.

IPSec: Internet Protocol Security, conjunto de protocolos que aseguran las comunicaciones sobre el protocolo IP.

IT: Information Technology, es la aplicación de computadoras y equipos de telecomunicaciones para almacenar, recuperar, transmitir y manipular datos.

IANA: Internet Assigned Number Authority, es la organización responsable de la coordinación global de DNS Root, direcciones IP y otros protocolos de internet.

ISPs e ISP: Internet Service Provider, empresa que brinda conexión a internet a sus clientes.

CIDR: Classless Inter-Domain Routing, enrutamiento entre dominios sin clases, reemplaza la sintaxis previa para nombrar las direcciones IP, las clases de redes, se usa para asignación de prefijos de longitud arbitraria.

PHB: Per-hop behavior, termino usado para definir la prioridad

aplicada a un paquete cuando atraviesa un router en una red DiffServ.

DIFFSERV: Differentiated Services, arquitectura de red que sirve para el manejo y clasificación del trafico además provee calidad de servicio dentro de las redes IP.

RTE: Route Table Entry, describe la ruta anunciada por le uso del protocolo IPv6.

LSPs: Link State PDU, estos paquetes son responsables de distribuir información de ruteo entre nodos IS-IS.

LSAs: Link State Advertisement, anuncia el estado del enlace dentro del protocolo de enrutamiento OSPF.

GNS3: Graphical Network Simulator, simulador grafico para redes el que permite diseñar entornos de red en un ambiente simulado.

SSH: Secure Shell, es un protocolo seguro que permite acceder vía remota a los host y tomar el control de manera segura de un computador.