_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DISEÑO MODULAR DE UNA RED IPv6 INTEGRAL

Hugo Morellá Soler

Tutor: Jose Oscar Romero Martínez

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2015-16

Valencia, 11 de septiembre de 2016

Resumen

El presente proyecto pretende realizar una red corporativa sobre una compañía ficticia con dos sedes interconectadas utilizando exclusivamente el protocolo IPv6.

Para ello se hará uso del direccionamiento IPv6, entendiendo las diferencias con IPv4 y los diferentes tipos de direcciones que aporta IPv6, y de los protocolos de encaminamiento propios de este protocolo, tales como RIPv6, OSPFv3 y IS-IS. Además se utilizará direccionamiento dinámico (DHCPv6) para poder poner en servicio un equipo simplemente conectándolo a la red.

Se aplicarán unas determinadas políticas de seguridad para proteger la información corporativa y permitir que esta sea accesible desde las distintas sedes. Para ello se hará uso de elementos de seguridad perimetral como son los firewalls.

Se permitirá la movilidad de los usuarios instalando puntos de acceso en ambas sedes.

Por último se utilizaran los protocolos de aplicación como HTTP que permitan acceder a las herramientas corporativas asumiendo que estas estarán en un front-end web.

Resum

El present projecte pretén realitzar una xarxa corporativa sobre una companyia fictícia amb dues seus interconnectades utilitzant exclusivament el protocol IPv6.

Per a això es farà ús de l'adreçament IPv6, entenent les diferències amb IPv4 i els diferents tipus d'adreces que aporta IPv6, i dels protocols d'encaminament propis d'aquest protocol, com ara RIPv6, OSPFv3 i IS-IS. A més es farà servir adreçament dinàmic (DHCPv6) per poder posar en servei un equip simplement connectant-lo a la xarxa.

S'aplicaran unes determinades polítiques de seguretat per protegir l'informació corporativa i permetre que aquesta sigui accessible desde les diferents seus. Per a fer-ho es farà ús d'elements de seguretat perimetral com són els firewalls.

Es permetrà la mobilitat dels usuaris instal·lant punts d'accés a les dues seus.

Finalment s'utilitzaran els protocols d'aplicació com HTTP que permetin accedir a les eines corporatives assumint que aquestes estaran en un front-end web.

Abstract

This project aims to conduct a corporate network on a fictitious company with two locations interconnected using only the IPv6 protocol.

To do this it will use IPv6 addressing, understanding the differences between IPv4 and the different types of addresses provides IPv6, and routing protocols own this protocol, such as RIPv6, OSPFv3 and IS-IS. In addition dynamic addressing (DHCPv6) will be used to commission a computer by simply connecting to the network.

Certain security policies apply to protect corporate information and to allow that this to be accessible from different locations. For it will make use of elements of perimetral security such as firewalls.

The mobility of users on both sites will be allowed by installing access points .

Finally will be used the application protocols such as HTTP that allow access corporate tools assuming that these will be in a front-end web.

Índice

Capítulo 0. Introducción

En el presente capitulo introduciremos el proyecto de diseño modular de una red IPv6 integral. Para el desarrollo del mismo se realizará una integración teórica son los conceptos elementales para poder desarrollar satisfactoriamente el diseño de la red y su posterior puesta en servicio.

0.1 Objetivos

El objetivo de este proyecto es realizar el diseño de una red corporativa utilizando IPv6 en su totalidad. Tanto nivel de direccionamiento, routing, seguridad, protocolos de aplicación y movilidad.

0.2 Metodología

La metodología empleada para el desarrollo del proyecto ha sido el estudio teórico de las bases de IPv6, así como los diferentes protocolos específicos de esta versión de IP. Tras ello se ha realizado un diseño de la red a nivel esquemático y implementado en el programa Cisco Packet Tracer 6.2 para realizar las configuraciones pertinentes.

0.2.1 Gestión del proyecto

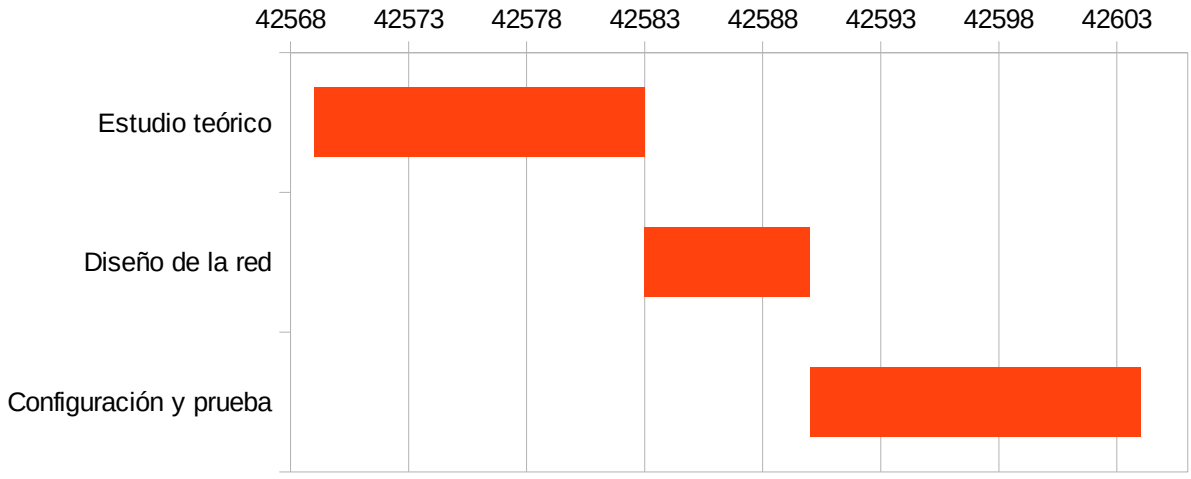
La gestión del proyecto se ha realizado planteando un marco de estudio con el que sería posible implementar el diseño, tras lo cual, asumiendo unas condiciones cerradas, realizar las configuraciones y probar que es completamente funcional.

0.2. Distribución en tareas

Las tareas elementales en las cuales se ha estructurado el proyecto son las siguientes:

- Estudio teórico de las particularidades de IPv6 y sus protocolos.
- Diseño de la red dadas unas especificaciones.
- Configuración y prueba de la red diseñada.

0.2.3 Diagrama temporal



Capítulo 1. IPv6

IPv6 está diseñado para reemplazar a IPv4: incrementa los bits de dirección de red de 32 a 128 (es decir unas 6'7 x 10^{17} direcciones por milímetro cuadrado de la Tierra). La mayor longitud de IPv6 permite escalar las redes y proporcionar accesibilidad mundial.

Otra mejora a tener en cuenta es la cabecera principal simplificada y las cabeceras de extensión. Este formato de cabecera permite manipular paquetes mas eficientemente. La flexibilidad del espacio de direcciones IPv6 reduce la necesidad de direcciones privadas y el uso de NAT. Ademas habilita nuevos protocolos de aplicación pues no requieren un procesado especial de los routers frontera en el borde de las redes.

Las funcionalidades de IPv6, tales como la agregación de prefijo, simplificación de renumeración de redes y las capacidades multihoming, posibilitan que el enrutado sea mas eficiente. Como protocolos de enrutamiento cabe destacar que IPv6 soporta RIP, IS-IS, OSPF y BGP.

1.1 Formatos de dirección IPv6

Las direcciones IPv6 poseen 128 bits (16 bytes). La dirección se divide en 8 grupos de 16 bits hexadecimales separados por dos puntos (:) con el siguiente formato x:x:x:x:x:x:x:x. Por ejemplo:

1234:4567:8910:1112:1314:1516:1718:1920

3003:0:0:0:1234:1234:5678:5678

Cuando las direcciones contienen consecutivos ceros en sus grupos de 16 bits, estos se pueden sustituir por dos puntos dobles (::). Hay que tener en cuenta que solo se puede usar los dos puntos dobles una vez por dirección, pues si no podría dar lugar a engaño.

Así, por ejemplo, la dirección “3003:0:0:0:1234:1234:5678:5678” podría reescribirse como “3003::1234:1234:5678:5678”.

La dirección “1234:0:0:1112:0:0:0:1920” podría reescribirse como “1234::1112:0:0:0:1920” o como “1234:0:0:1112::1920”. Lo que daría lugar a engaño seria escribirla como “1234::1112::1920” pues no se podría saber, a priori, la serie de ceros que hay en cada sustitución.

Este formato de escritura se llama formato comprimido, mientras que al original se le llama formato preferido. Cabe destacar que las direcciones IPv6 no son sensibles a mayúsculas o minúsculas.

Cada interfaz puede tener configuradas múltiples direcciones IPv6, pero solo una dirección link-local.

El prefijo IPv6 esta descrito en la RFC 2373. La longitud del prefijo es un numero decimal que indica cuantos bits de la parte alta de la dirección comprenden el prefijo (la parte de red la dirección). Por ejemplo, 3003:85B8:865D:5265::/64 es un prefijo valido.

1.1.1 Direcciones Unicast

Las direcciones unicast IPv6 es un identificador para una sola interfaz en un nodo. Un paquete que fuera enviado a una dirección unicast es enviada a la interfaz identificado por esa dirección.

1.1.2 Dirección Global Agregable

Es una dirección de un prefijo global unicast agregable. La estructura de la dirección permite la agregación estricta de los prefijos de los prefijos enrutables lo que limita el numero de entradas de la tabla de enrutamiento en la tabla de enrutamiento global. Estas direcciones son usadas en redes que son agregadas hacia arriba a través de organizaciones y finalmente por los ISP.

Están definidas por un prefijo global, un subnet ID, y un interface ID. Excepto las direcciones que empiezan por el binario 000, todas las direcciones global unicast tienen una interface ID de 64 bits. Usan todo el rango de direcciones que empiezan por el binario 001 (2000::/3). La estructura de las direcciones se puede ver en la siguiente imagen.

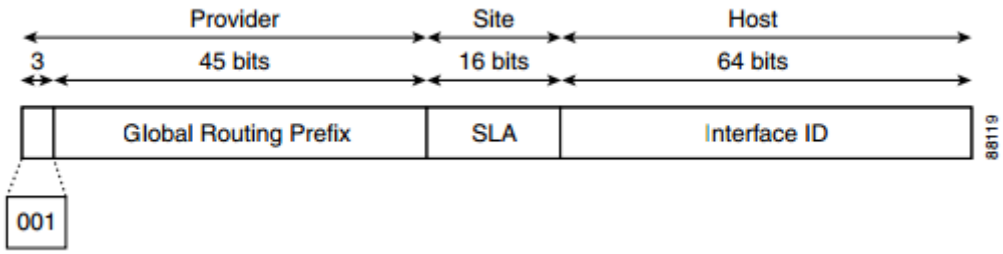


Figura 1. Estructura direcciones.

Las direcciones con el prefijo desde 2000::/3 (001) hasta E000::/3 (111) requieren tener un interface ID de 64 bits en el formato extendido universal de identificación (EUI-64). IANA (Internet Assigned Numbers Authority) asigna lasa direcciones del rango 2000::/16 a los registros regionales.

Las direcciones globales agregables consisten en 48 bits de prefijo y 16 bits de subnet ID o SLA (Site-Level Aggregator). Una subnet ID puede ser usada por organizaciones individuales para crear una jerarquía de direcciones y identificar subredes. Esto es similar a la subnet en IPv4, excepto que una organización con un subnet ID IPv6 puede crear 64.535 subredes individuales.

Un interface ID identifica las interfaces de un enlace. La interface ID es única para el enlace. En algunos casos la interface ID es la misma que, o se basa en, la dirección de la capa de enlace de datos del interfaz. Las interface IDs usadas tienen una longitud de 64 bits y están en el formato EUI-64.

Estas IDs se forman de una de las siguientes maneras:

- Para interfaces IEEE 802 (Ethernet, Fiber Distributed Data y otras), los primeros tres octetos (24 bits) son el OUI (Organizationally Unique Identifier) de la dirección MAC del interfaz, los octetos cuarto y quinto son el numero hexadecimal FFFE, y los últimos tres octetos son los tres últimos octetos de la dirección MAC. El bit Universal/Local (U/L), que es el séptimo bit del primer octeto cambia su valor de 0 a 1 o de 1 a 0.

- Para el resto de tipos de interfaces (serial, loopback, ATM, Frame Relay y interfaces de túnel) el interface ID es similar al usado en los interfaces IEEE 802. Sin embargo la primera dirección MAC de la pila de direcciones MAC en el router se usa como identificador (porque la interfaz no tiene dirección MAC).

Si no hay interfaces IEEE 802 en el router, las direcciones link-local se generan en las interfaces del router según los siguientes pasos:

1. El router pide una direccion MAC (de la pila de direcciones MAC del router).
2. Si no hay direcciones MAC disponibles, el numero de serie del router se usa para formar la dirección link-local.
3. Si el numero de serie del router no se puede usar para la dirección link-local, el router usa MD5 hash para determinar una direccion MAC del router a partir del hostname del router.

1.1.3 Direcciones Link-Local

Una dirección link-local es una dirección IPv6 unicast que puede ser configurada automáticamente en cualquier interfaz usando el prefijo link-local FE80::/10 (1111 1110 10) y el identificador de interfaz en el formato EUI-64 modificado. Las direcciones link-local son usadas por el protocolo neighbor discovery (NDP) y el proceso de autoconfiguración sin estado (SAP). Los nodos de un link local puede usar las direcciones link-local para comunicarse, no necesitan direcciones global unique para ello. Los routers IPv6 no pueden enrutar los paquetes que tengan como origen o destino una dirección link-local.

En la siguiente imagen se puede ver la estructura de las direcciones link-local.

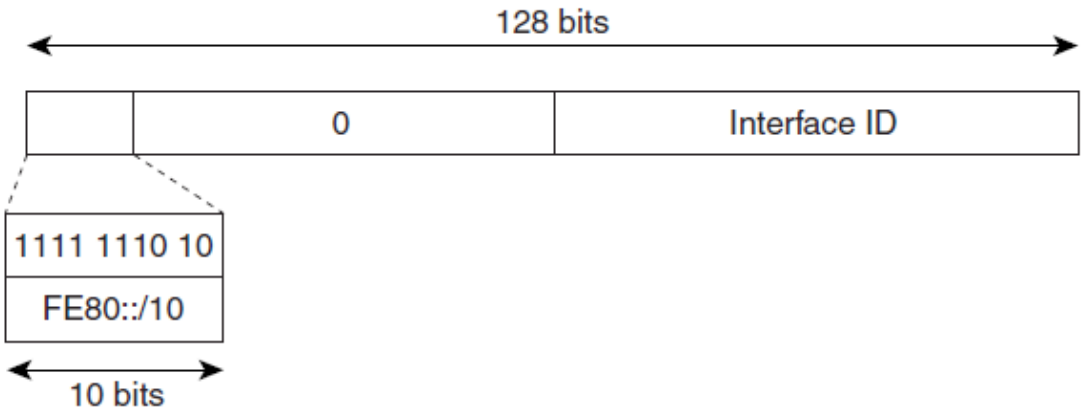


Figura 2. Estructura direcciones Link-Local.

1.1.4 Direcciones IPv4-Compatible IPv6 (Obsoleta por RFC 4291)

Una dirección IPv4- Compatible IPv6 es una dirección IPv6 unicast que tiene ceros en los 96 bits de parte alta de la dirección y la dirección IPv4 en los 32 bits de la parte baja de la dirección. El formato es 0:0:0:0:0:0:A.B.C.D o ::A.B.C.D. Las 128 bits son usados como una dirección IPv6 por el nodo, mientras que los ultimos 32 bits son usados como una dirección IPv4 por el nodo. Estas direcciones se asignan a los nodos que soportan tanto IPv4 como IPv6. La siguiente imagen muestra la estructura.

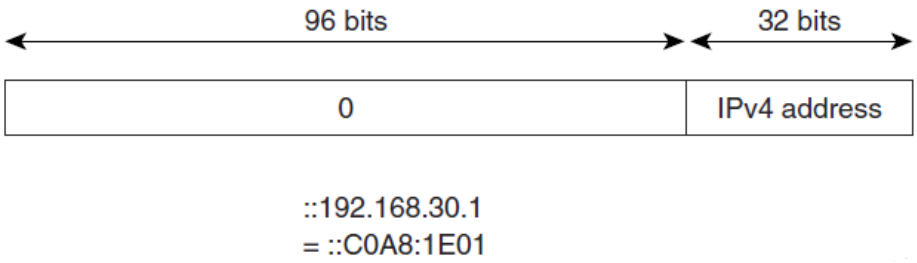


Figura 3. Estructura direcciones IPv4-Compatible IPv6.

1.1.5 Direcciones Unique Local

Una dirección unique local es una dirección IPv6 unicast que es global unique y está destinada para las comunicaciones locales. No se espera que se enrutable en Internet y es enrutable dentro de un area limitada, como un sitio y puede ser enrutada entre un numero limitado de sitios. Las aplicaciones pueden tratar estas direcciones como direcciones de ámbito global.

Tiene las siguientes características:

- Tiene un prefijo global unique (esto hace que sea muy probablemente única).
- Tiene un prefijo conocido para permitir un filtrado sencillo en los limites del sitio.

- Permite a los sitios ser combinados o interconectados privadamente sin crear ningún conflicto de direcciones o requerir la renumeracion de los interfaces que usen ese prefijo.

- Es independiente del ISP y puede ser usada para comunicaciones dentro de un sitio sin tener ninguna conectividad, permanente o intermitente, con Internet.

- Si es accidentalmente filtrado fuera del sitio por medio de enrutado o DNS, no hay conflicto con otras direcciones.

La siguiente imagen muestra su estructura:

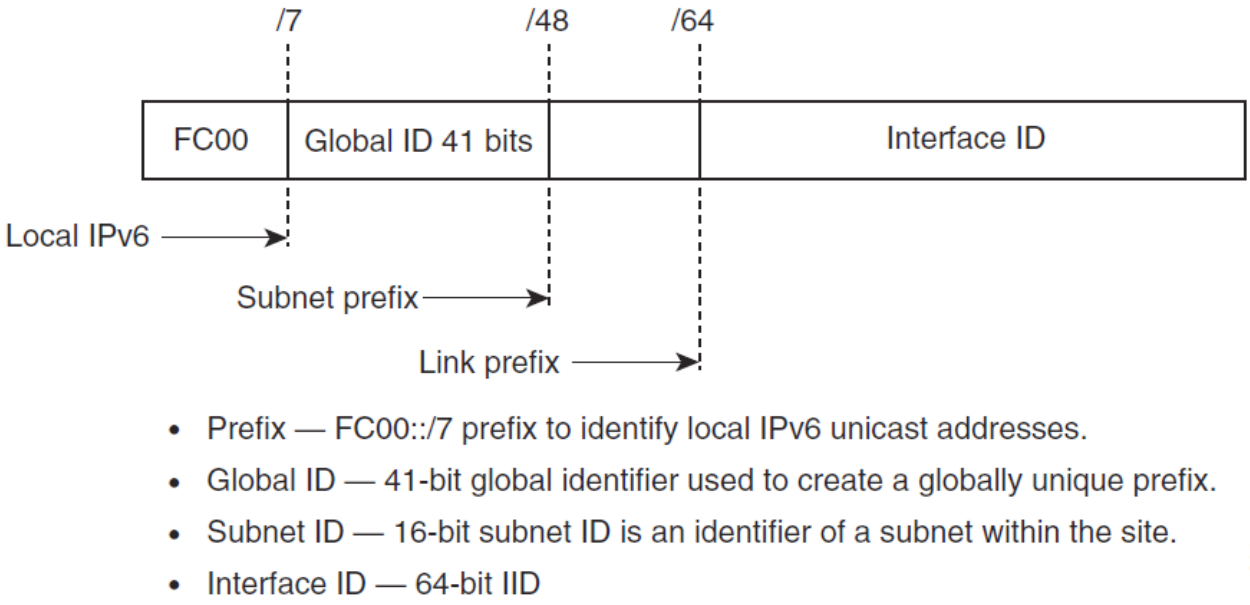


Figura 4. Estructura direcciones Unique Local.

1.1.6 Direcciones Anycast

Una dirección anycast es una dirección que es asignada para un grupo de interfaces que pertenecen a diferentes nodos. Un paquete enviado a una dirección de este tipo es enviado al interfaz mas cercano – como se define por el protocolo de enrutado en uso - identificado por la dirección anycast. Estas direcciones son indistinguibles sintácticamente de una dirección unicast porque las direcciones anycast están localizadas en el espacio de direcciones unicast. Asignando una dirección unicast a mas de un interfaz convierte una dirección unicast en anycast. Debes configurar los nodos que tienen una dirección anycast para reconocer que esa dirección es anycast.

Estas direcciones solo pueden usarse en un router, no en un host. Tampoco pueden ser usadas como dirección origen de un paquete IPv6.

La siguiente imagen muestra el formato de una dirección anycast de subred del router. La dirección tiene un prefijo concatenado por una serie de ceros (la interface ID). La dirección anycast de subred de router puede usarse para alcanzar otro router en el enlace que es identificado por el prefijo de la dirección.

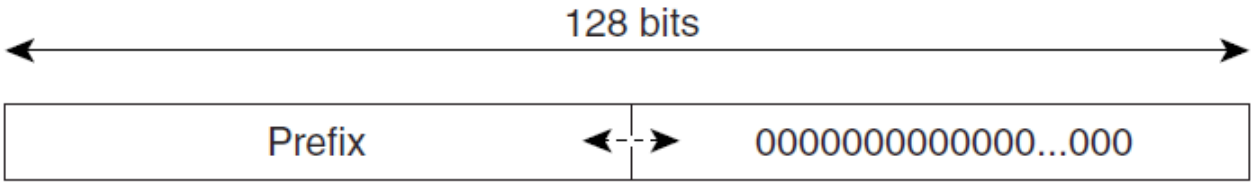


Figura 5. Estructura direcciones Anycast.

1.1.7 IPv6 Multicast Addresses

Una dirección IPv6 multicast es una dirección que tiene el prefijo FF00::/8 (1111 1111). Estas direcciones son un identificador de un grupo de interfaces que pertenecen a diferentes nodos. Un paquete enviado a una dirección multicast es enviado a todas las interfaces identificadas por esa dirección. El segundo octeto siguiente al prefijo define el tiempo de vida y el alcance de la dirección multicast. Una dirección permanente tiene el parámetro tiempo de vida igual a 0. Una dirección temporal, en cambio, lo tiene igual a 1. Una dirección multicast que tenga un alcance de un nodo, un enlace, un sitio, organización o alcance global, tiene el parámetro alcance igual a 1, 2, 5, 8, o E, respectivamente. Por ejemplo, una dirección multicast con prefijo FF02::/16 es una dirección multicast permanente con alcance de enlace. La siguiente imagen muestra el formato de estas direcciones.

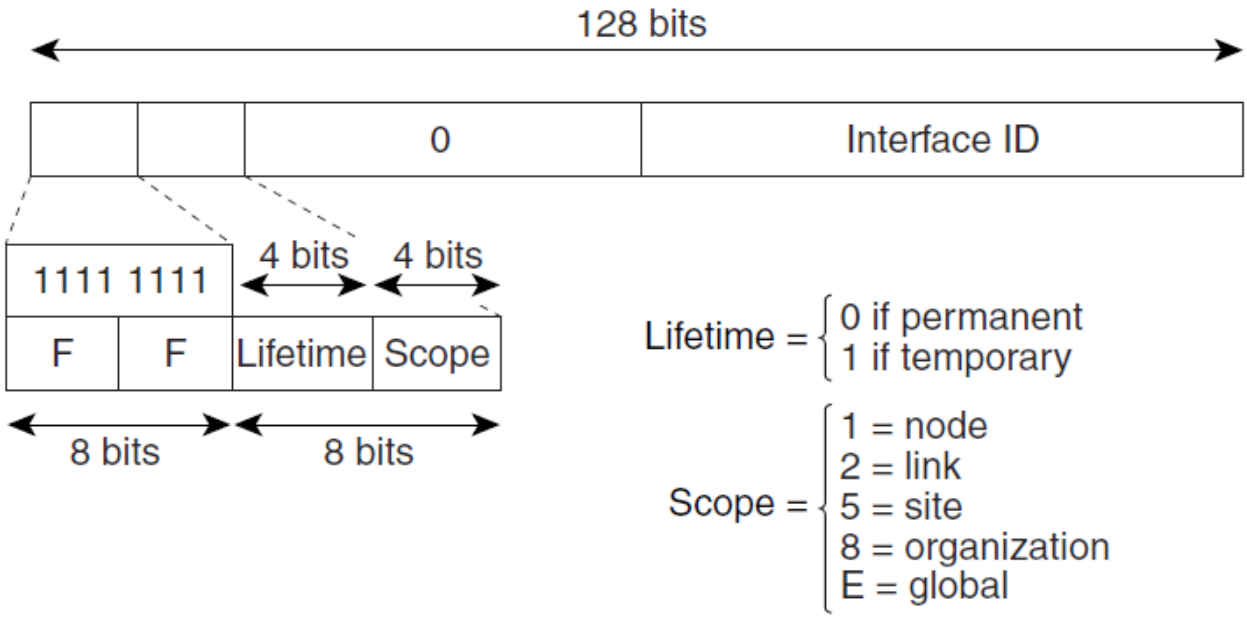


Figura 6. Estructura direcciones Multicast.

Los nodos IPv6 se deben unir a los siguientes grupos multicast:

- All-nodes: FF02:0:0:0:0:0:0:1 (el alcance es link-local).

- Solicited-node: FF02:0:0:0:0:1:FF00:0000/104 para cada una de sus direcciones unicast y anycast asignadas.

Los routers IPv6 deben también unirse al grupo multicast all-routers FF02:0:0:0:0:0:0:2 (el alcance es link-local).

La dirección multicast solicited-node es un grupo multicast que corresponde a una dirección unicast o anycast. Los nodos deben unirse a su grupo asociado para cada dirección unicast o anycast que tenga asignada. La dirección tiene el prefijo FF02:0:0:0:0:1:FF00:0000/104 concatenado con los 24 bits de la parte baja de la correspondiente dirección IPv6. Por ejemplo, la dirección solicited-node asociada a la dirección 2001::54:2122:4D4D:FEDC es FF02::1:FF4D:FEDC. Estas direcciones son usadas en los mensajes neighbor solicitation. En la siguiente imagen se puede apreciar como se construyen esta clase de direcciones.

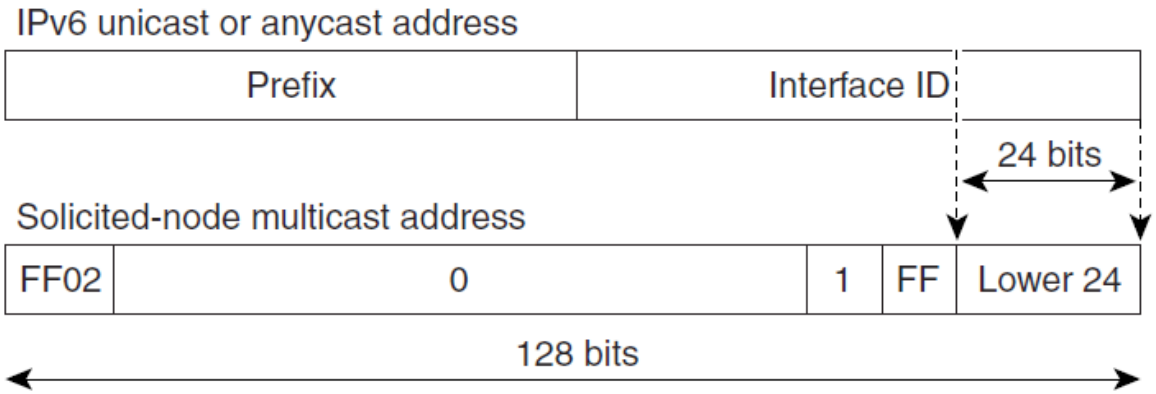


Figura 7. Estructura direcciones Solicited-node.

IPv6 no tiene direcciones broadcast, en su lugar se usan direcciones multicast (como all-nodes).

1.2 Cabecera del paquete IPv4

La cabecera basica de un paquete IPv4 tiene 12 campos con un tamaño total de 20 octetos (160 bits). Los 12 campos pueden ir seguidos de un campo de opciones, que es seguido por una porcion de datos que normalmente es un paquete de la capa de transporte. La longitud variable del campo de opciones se añade al tamaño total de la cabecera. En la siguiente imagen se puede ver su estructura. Los campos oscurecidos de la cabecera no estan incluidos en la cabecera del paquete IPv6.

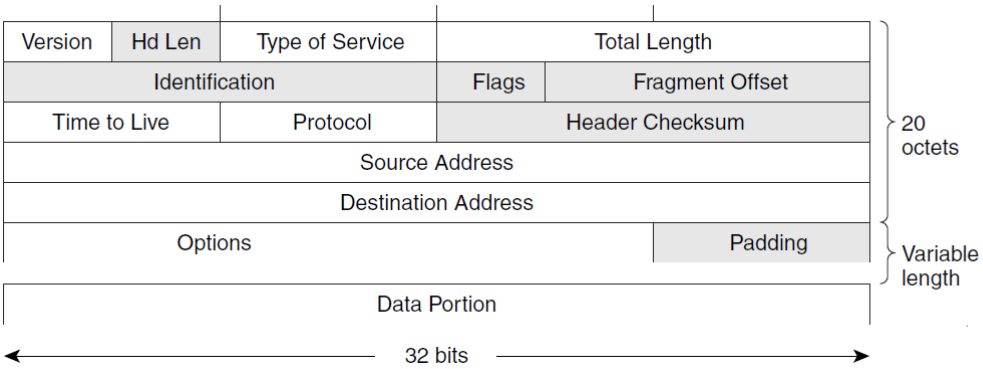


Figura 8. Estructura cabecera IPv4.

1.3 Cabecera IPv6 simplificada

La cabecera básica de un paquete IPv6 tiene 8 campos con un total de 40 octetos (320 bits). De la fragmentación se encarga el origen del paquete. Los checksums se usan en la capa de enlace de datos y de transporte. El checksum de UDP comprueba la integridad del paquete interior y la cabecera básica de IPv6. El campo de opciones se alinean a 64 bits, lo que facilita el procesado de los paquetes.

Campo	Descripción
Versión	Similar al campo de Version de IPv4, excepto que en lugar de ser 4 ahora es 6.
Clase de trafico	Similar al campo Type of Service de IPv4. Este campo etiqueta los paquetes con la clase de trafico que se usa en servicios diferenciados (DiffServ).
Etiqueta de flujo	Nuevo campo de IPv6. Este campo etiqueta los paquetes de un flujo especifico que diferencia los paquetes en la capa de red.
Longitud de la carga	Similar al campo Total Length en IPv4. Este campo indica la longitud total de la porcion de datos del paquete.
Siguiente cabecera	Similar al campos Protocol de IPv4. El valor de el campo siguiente cabecera determina el tipo de informacion que sigue a la cabecera IPv6. Ésta puede ser un paquete de la capa de transporte (TCP o UDP) o una cabecera de extensión.
Límite de saltos	Similar a Time to Live en IPv4. El valor del campo especifica el maximo numero de routers que el paquete puede transpasar antes de que sea considerado invalido. Cada router decrementa el valor en uno. Como no hay checksum en la cabecera de IPv6, el router puede decrementar el valor sin necesitar recalcularlo, lo que ahorra recursos de procesado.
Dirección origen	Similar al campo Source Address en IPv4, excepto que el campo contiene 128 bits en lugar de 32.
Dirección destino	Similar al campo Destination Address en IPv4, excepto que el campo contiene 128 bits en lugar de 32.

Tabla 1. Campos cabecera IPv6.

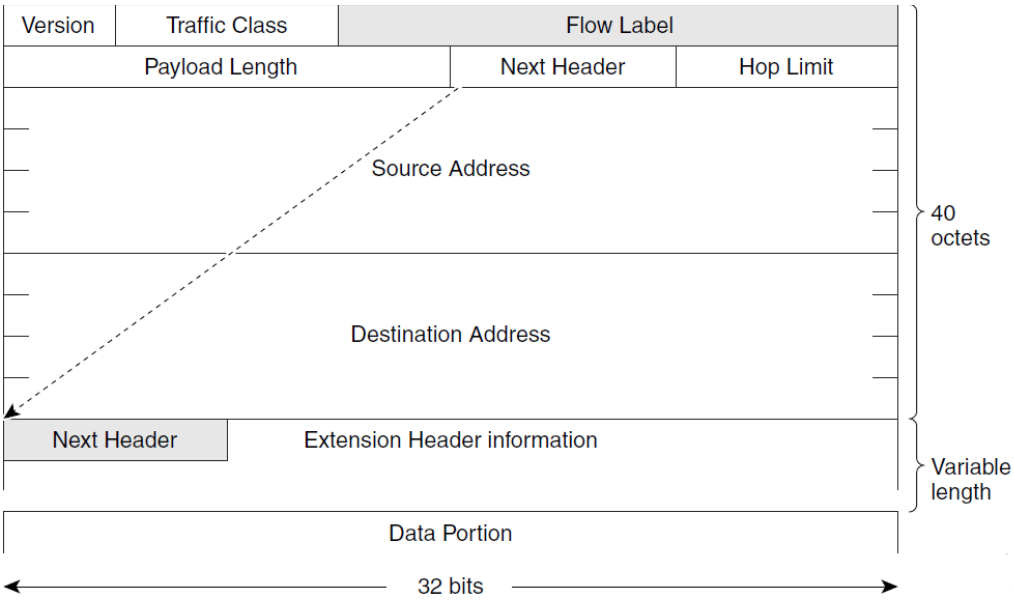


Figura 9. Estructura cabecera IPv6.

Las cabeceras de extensión opcionales y la porción de los datos del paquete van después de los ocho campos de la cabecera básica de IPv6. Si existe, esa cabecera de extensión se alinea a 64 bits. Cada cabecera de extensión se identifica por el campo Next Header de la cabecera anterior. Típicamente, la ultima cabecera de extensión tiene como campo Next Header TCP o UDP. La siguiente imagen muestra el formato de una cabecera de extensión.

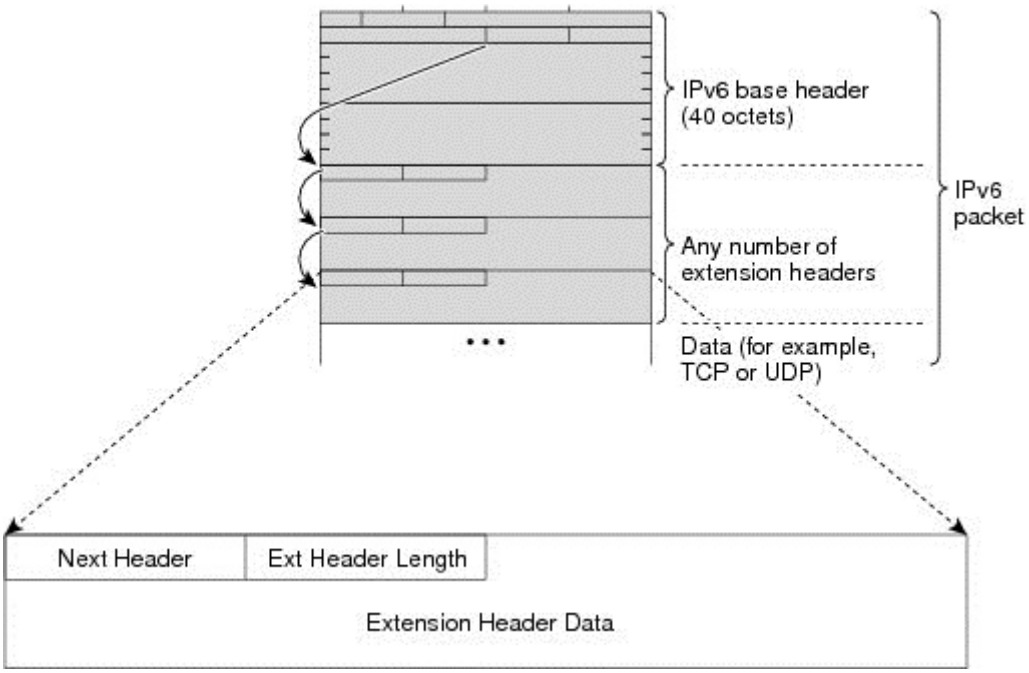


Figura 9. Estructura cabeceras de extensión IPv6.

Tipo de cabecera	Valor Next Header	Descripción
Hop-by-hop options header	0	Cabecera que es procesada por todos los saltos en el camino de un paquete. Cuando está presente, la cabecera siempre aparece después de la cabecera básica de IPv6.
Destination options header	6	Cabecera que puede ir detrás de cualquier Hop-by-hop options header. Es procesada en el destino final y en cada dirección visitada especificada en la cabecera de enrutamiento. Alternativamente, la cabecera puede seguir cualquier cabecera ESP (Encapsulation Security Payload). En este caso la cabecera solo es procesada en el destino final.
Routing header	43	Cabecera que es usada como fuente de enrutamiento.
Fragment header	44	Cabecera que es usada cuando una fuente fragmenta un paquete que es mas grande que la MTU para el camino entre ella y un destino. La cabecera es usada en cada paquete fragmentado.
Upper-layer headers	6 (TCP) 17 (UDP)	Cabeceras que son usadas dentro de un paquete para transportar los datos. Los dos principales protocolos de transporte son TCP y UDP.

Tabla 2. Valores del campo Next-header.

1.4 DNS para IPv6

IPv6 soporta los tipos de registro DNS que los procesos de búsqueda resuelven: nombre-dirección y dirección-nombre (reverse mapping). La siguiente table ilustra los tipos de registro:

Tipo de registro	Descripción	Formato
AAAA	Mapea un nombre de host a una dirección IPv6. (Equivalente a registro A en IPv4.)	f.in-addr-servers.arpa AAAA 2001:67c:e0::1
PTR	Mapea una dirección IPv6 a un nombre. (Equivalente a registro PTR en IPv4.)	1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.0.0.c.7.6.0.1.0.0.2.ip6.int PTR f.in-addr-servers.arpa

Tabla 3. Tipos de registro DNS para IPv6.

1.5 Path MTU Discovery para IPv6

Como en IPv4, se puede usar el descubrimiento de la MTU del camino en IPv6 para permitir a un host descubrir dinámicamente y ajustar las diferencias entre el tamaño de la MTU de cada enlace a lo largo de un camino de datos. Sin embargo en IPv6 la fragmentación la maneja la fuente del paquete cuando la MTU de un enlace a lo largo de un camino dado no es lo suficientemente grande para adaptar el tamaño de los paquetes. Siendo los host IPv6 los que controlan la fragmentación los routers ahorran recursos de procesado y ayuda a las redes a funcionar mas eficientemente. Una vez que la MTU es reducida por un mensaje ICMP Too Big, Cisco NX-OS retiene el valor mas bajo. La conexión no incrementara el tamaño del segmento periódicamente para ajustar el throughput.

1.6 ICMP para IPv6

Se puede usar ICMP en IPv6 para proveer información sobre la salud de la red. ICMPv6, la versión que funciona con IPv6, reporta error si los paquetes no pueden ser procesados correctamente y manda mensajes informativos sobre el estado de la red. Por ejemplo, si un router no puede retransmitir un paquete porque es demasiado grande para enviarlo a otra red, el router envía un mensaje al host origen. Ademas, los paquetes ICMP son usados en IPv6 neighbor discovery y el path MTU discovery.

El valor 58 en el campo Next Header identifica un paquete ICMP. Estos van detrás de todas las cabeceras de extensión y es el ultimo fragmento de información en los paquetes. Dentro de los paquetes ICMP los campos ICMPv6 Type y ICMPv6 Code identifican el tipo de paquete especifico así como el tipo de mensaje. El valor del campo Checksum se calcula por el emisor y se comprueba por el receptor desde los campos en el paquete ICMPv6 y en la pseudocabecera IPv6.

El campo de datos contiene información sobre errores o diagnósticos referidos al procesado del paquete IP. La siguiente imagen (3-11) muestra el formato de la cabecera de un paquete IPv6 ICMP:

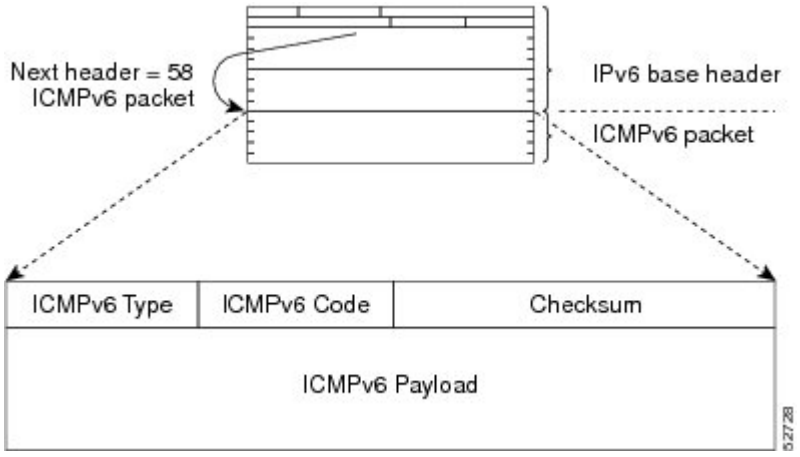


Figura 10. Estructura ICMP.

1.6.1 IPv6 Neighbor Discovery

Se puede usar IPv6 NDP (Neighbor Discovery Protocol) para determinar si un router vecino es alcanzable. Los nodos IPv6 usan NDP para determinar las direcciones de los nodos de la misma red (local link), para encontrar routers vecinos que puedan reenviar sus paquetes, para verificar si los routers vecinos son alcanzables o no y para detectar cambios en las direcciones de la capa de enlace de red. NDP usa mensajes ICMP para detectar si los paquetes son enviados a los routers vecinos que son inalcanzables.

1.6.2 IPv6 Neighbor Solicitation Message

Un nodo envía un mensaje de solicitud de vecino, el cual tiene el valor de 135 en el campo tipo de la cabecera del paquete ICMP, en el link local cuando quiere determinar la dirección de la capa de enlace de datos de otro nodo. La dirección origen es la dirección IPv6 del nodo que envía el mensaje. La dirección destino es la dirección multicast solicited-node del nodo destino. Además el mensaje incluye la dirección de la capa de enlace del nodo origen.

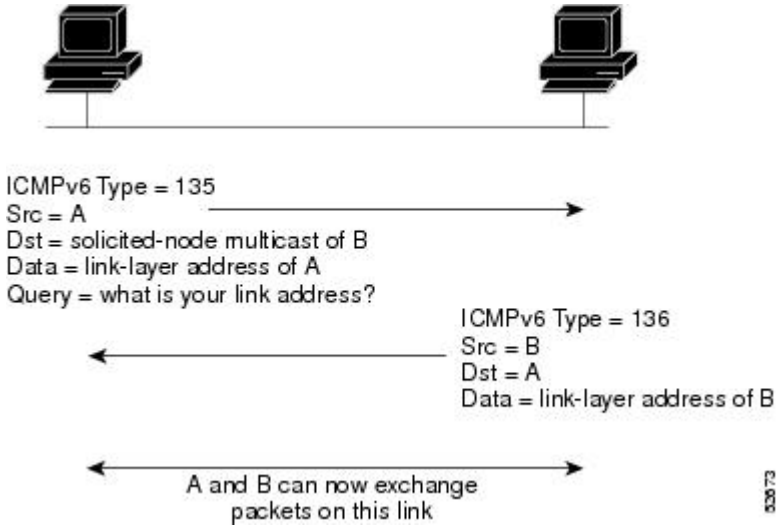


Figura 11. Funcionamiento Neighbor Solicitation.

Después de recibir el mensaje, el nodo destino responde enviando un mensaje neighbor advertisement, cuyo valor tipo de la cabecera ICMP es 136. La dirección origen es la dirección del nodo (que envía el mensaje neighbor advertisement) y además la parte de datos incluye la dirección de la capa de enlace de datos (MAC) del nodo. La dirección destino es la dirección del nodo que envió el mensaje neighbor solicitation.

Después de que el nodo origen reciba el mensaje neigbor advertisement, el origen y el destino se pueden comunicar. Estos mensajes pueden verificar si es alcanzable un vecino. Para ello, tras tener la dirección MAC, envía un mensaje neighbor solicitation a la dirección unicast del destino.

También se envían mensajes neighbor advertisement cuando se produce un cambio en la dirección MAC de un nodo en un link local. Cuando se produce un cambio, la dirección destino del mensaje es la dirección multicast all-nodes.

La detección de nodo no alcanzable identifica un fallo del mismo o de la ruta a él y es usada en todos los caminos entre host y nodos vecinos (routers y hosts). Esto lo realizan los nodos a los cuales se están enviando solamente paquetes unicast y no aquellos a los que están siendo enviados paquetes multicast.

Un nodo se considera alcanzable cuando se recibe un ACK positivo del mismo. Un reconocimiento positivo de un protocolo de una capa superior (como TCP) indica que la conexión está alcanzando su destino. Si los paquetes están alcanzando al peer, también estan alcanzando el next-hop del origen y ,por lo tanto, alcanzar el destino confirma que el next-hop es alcanzable.

Para destinos que no estan en el link local, la retransmisión de paquetes implica que el primer salto del router es alcanzable. Cuando no se envian ACKs desde una capa superior, se usan mensajes neighbor solicitation para verificar que la ruta sigue funcionando (como un keep-alive). Los mensajes no solicitados confirman la ruta en una sola dirección (del origen al destino), mientras que los mensajes neighbor advertisement solicitados indican que el camino funciona en ambas direcciones.

El proceso de autoconfiguración sin estado (Stateless Autoconfiguration Process) utiliza los mensajes Neighbor Solicitation (NS) para verificar la unicidad de las direcciones unicast que asigna a un interfaz. Para ello ejecuta el proceso de detección de dirección duplicada antes de asignar. Mientras tanto se asigna una dirección tentativa a ese interfaz. Este envía un mensaje NS donde la dirección origen esta vacía y hay un campo con la dirección tentativa. Si algún nodo posee esa dirección envía un mensaje Neighbor Advertisement (NA) con la dirección tentativa. Si otro nodo envía un mensaje NS con la misma dirección tentativa, ese nodo también envía un mensaje NS. Si nadie envía un mensaje NA ni NS entonces envía el mensaje NS original considerando la dirección tentativa como única y la asigna al interfaz.

1.6.3 IPv6 Router Advertisement Message

Los mensajes Router Advertisement Message tienen son paquetes ICMP donde el campo tipo tiene el valor 134. Cada interfaz configurado de un router IPv6 los envía periódicamente a la dirección multicast all-nodes como se puede apreciar en la siguiente imagen:

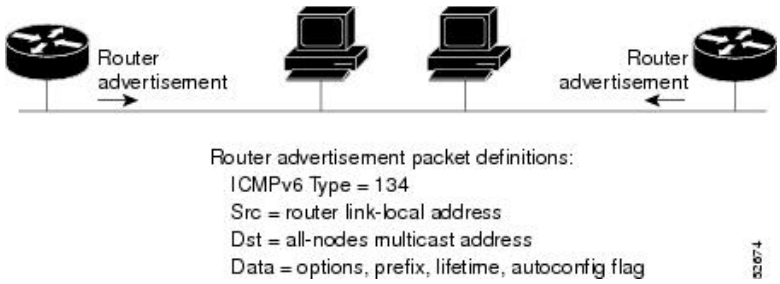


Figura 12. Funcionamiento Router Advertisement.

Estos mensajes contienen :

- Uno o mas prefijos de red que un nodo del link local puede usar para autoconfigurar la dirección IPv6.

- El tiempo de vida de los prefijos.

- Flags con el tipo de autoconfiguración (stateful o stateless).

- Información del router por defecto (si el que envía el mensaje es el router por defecto ademas debe enviar cuanto tiempo lo será).

- Otra información para hosts como el límite de saltos o la MTU de los paquetes que deben enviar.

Los mensajes RA también se envían como respuesta a los mensajes router solicitation (RS). Estos mensajes, que tienen en el campo Type de los paquetes ICMP el valor de 133, se envían por los hosts al iniciar el sistema con lo que pueden autoconfigurarse sin esperar al siguiente mensaje RA programado. La dirección origen es normalmente la dirección IPv6 unspecified (0::0). Si el host tiene configurada una dirección unicast se usa esta en el mensaje. La dirección destino es all-routers. Cuando se envía el mensaje RA en respuesta al mensaje RS la dirección destino es la dirección unicast del origen del mensaje RS.

Los parámetros configurables del mensaje RA son:

- Intervalo de tiempo entre mensajes.

- El tiempo de vida del router, que indica el tiempo que se puede utilizar el router como default router.

- El prefijo de red en uso en el enlace.

- El intervalo de tiempo entre la retransmisión de los mensajes NS.

- La cantidad de tiempo que un nodo considera un host alcanzable.

Los parámetros de configuración son específicos de un interface. El envío de mensajes RA (con los valores por defecto) se habilita automáticamente por los interfaces Ethernet. Para otro tipo de interfaces, se debe introducir el comando “no ipv6 nd supperss-ra” para enviarlos. Se pueden deshabilitar los mensajes RA de un interface introduciendo el comando: “ipv6 nd supperss-ra”.

1.6.4 IPv6 Neighbor Redirect Message

Los routers envían mensajes neighbor redirect (NR) para informar a los host de un mejor first-hop en la ruta para llegar al destino. Tienen en el campo Type de la cabecera de los paquetes ICMP el valor de 137.

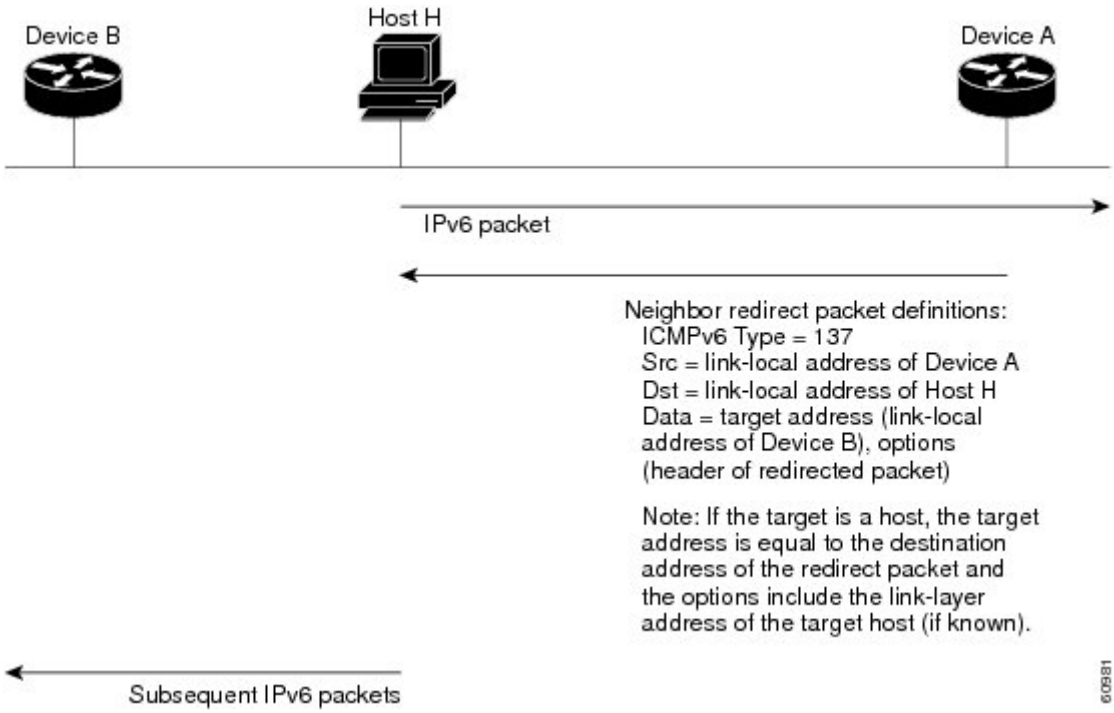


Figura 12. Funcionamiento Neighbor Redirect.

Después de reenviar un paquete el router envía un mensaje NR al origen del paquete bajo las siguientes circunstancias:

- La dirección destino del paquete no es una dirección multicast.
- El paquete no está en su tabla de routing.
- El paquete va a ser enviado por la interfaz que lo recibió.
- El router determina que hay un mejor first-hop para el paquete en el mismo enlace que la fuente del paquete.
- La dirección origen es una dirección IPv6 global de un vecino del mismo enlace o una dirección link-local. **[1]**

Capítulo 2. RIPv6

2.1 Formato de los mensajes y características de RIPng

Aunque RIPng (o RIPv6) es un protocolo nuevo se ha hecho un esfuerzo para que se parezca a sus predecesores. Su funcionamiento es prácticamente el mismo y usa en general el mismo algoritmo y operación que RIP. Además RIPng no presenta ninguna funcionalidad nueva comparado con RIPv2, exceptuando que permite implementar RIP en IPv6.

RIPng no presenta ninguna mejora con respecto a RIPv2. Las características que implementa RIPng son:

- Classless Addressing Support y Subnet Mask Specification: En IPv6 todas las direcciones son sin clase, y especificadas usando la dirección y la longitud del prefijo, en lugar de la mascara de subred. Por ello en lugar de enviar la mascara se envía la longitud del prefijo.

- Next Hop Specification: Esta característica se mantiene, pero se implementa diferente. Dada la longitud de las direcciones IPv6, incluir el campo Next Hop en el formato RTE (Routing Table Entry) de los mensajes RIPng incrementaría casi al doble de tamaño cada entrada. Hacer el campo Next Hop una característica opcional sería demasiado costoso. Por ello cuando se requiere el campo se especifica en una entrada distinta.

- Autentificación: RIPng no incluye un mecanismo de autentificación propio. Se asume que, si se requiere autentificación o encriptación, se realizará desde una capa inferior (en concreto desde el estándar IPSec definido para IPv6). Esto es mas eficiente que tener protocolos individuales como RIPng realizando autentificación.

- Etiqueta de la ruta: Este campo se implementa igual que en RIPv2.

- Uso de Multicasting: RIPng usa transmisión multicast, utilizando como destino la dirección FF02::9 (RIP routers).

2.2 RIPng Messaging

Hay dos mensajes RIPng básicos: RIP Request y RIP Response. Estos se intercambian usando UDP como en RIPv1 y RIPv2. Como es otro protocolo no puede usar el mismo numero de puerto que RIPv1 y RIPv2 (520), por ello usa el puerto UDP 521. Las reglas utilizadas son:

- RIP Request se envía al puerto 521. Puede tener como puerto origen el 521 o puede usar uno numero de puerto efímero.

- RIP Response se envía en respuesta a RIP Request enviado previamente. El puerto destino es igual al usado como puerto origen por RIP Request.

- Los mensajes RIP Response no solicitados se envían con los puertos origen y destino 521. **[2]**

2.3 Configurar RIP para IPv6

Antes de configurar RIPng en el equipo se debe habilitar el enrutamiento IPv6 usando el comando "ipv6 unicast-routing" en el modo de configuración global y habilitar IPv6 en cada interfaz que vaya a usarlo.

La secuencia de comandos para configurar un interfaz son los siguientes:

1) **enable**

2) **configure terminal**

3) **ipv6 unicast-routing**

4) **interface** *tipo número*

5) **ipv6 enable**

6) **ipv6 rip** *nombre* **enable**

No es necesario definir ningún proceso RIP ni las network del mismo a diferencia de RIP en IPv4. **[3]**

Capítulo 3. OSPFv3

3.1 Información sobre OSPFv3

OSPFv3 es un protocolo de enrutamiento de estado enlace del IETF. Los routers OSPFv3 envian un paquete especial llamado Hello Packet por cada interfaz con OSPF habilitado para descubrir routers OSPFv3 adyacentes. Cuando un router es descubierto, ambos routers comparan información del paquete Hello para determinar si tienen configuraciones compatibles. Los routers intentan establecer adyacencia, lo que significa que sincronizan sus bases de datos de estado de enlace para asegurarse que tiene información idéntica de routing OSPFv3.

Los routers adyacentes comparten Link State Advertisements (LSA) que incluyen información sobre el estado operacional de cada enlace, el coste y cualquier otra información del router. Cuando reciben un LSA por un interfaz los routers reenvían los paquetes por cada interfaz habilitado con OSPF para conseguir tener sus bases de datos de estado de enlace identicas. Cuando esto pasa la red converge.

Cada router usa el algoritmo de Dijkstra Shortest Path First (SPF) para construir su tabla de enrutamiento. Los routers pueden dividir las redes en areas. Esto reduce los requerimientos de CPU y memoria de los equipos, pues la mayoria de los LSA se envían dentro de su propia area. OSPFv3 soporta IPv6.

3.2 OSPFv3 vs OSPFv2

La mayor parte del protocolo OSPFv3 (RFC 2740) es la misma que OSPFv2. Las principales diferencias entre ambos son:

- OSPFv3 expande OSPFv2 para soportar los prefijos y la longitud de las direcciones IPv6.
- LSAs envían prefijo y longitud del prefijo, en lugar de dirección y mascara.
- El router ID y el area ID son numeros de 32 bits sin relación con las direcciones IPv6.
- Se usan las direcciones link-local para el neighbor discovery y otras características.
- Usa IPv6 para la autentificación (en concreto IPsec).
- Se redefinen los tipos de LSA.

3.3 Hello Packet

Los routers envían periódicamente paquetes Hello por cada interfaz habilitada con OSPFv3. El parámetro hello interval determina la periodicidad de los paquetes Hello y se configura por interfaz. Estos paquetes se utilizan para:

- Neighbor discovery.
- Keepalives.
- Comunicaciones bidireccionales.

- Elección del Designated Router (DR).

Los paquetes tienen información de la interfaz y del router que origino el mensaje, incluyendo el coste del enlace, el hello interval y las prestaciones opcionales del router. Cuando se recibe en una interfaz se determina si las configuraciones son compatibles. Cuando se da el caso se considera al router que envió el paquete vecino y se le añade a su tabla de vecinos.

Además estos paquetes incluyen una lista de router IDs con los que el router se ha comunicado. Si la interfaz que lo recibe ve su propio router ID se establece comunicación bidireccional entre las dos interfaces.

Por último los paquetes se envían como keepalive para determinar si un vecino sigue activo. Si no se recibe el paquete antes del dead interval configurado el vecino se borra de la tabla local.

3.4 Vecinos

Las interfaces OSPFv3 deben tener una configuración compatible con la interfaz remota antes de que se puedan considerar vecinos. Deben coincidir en los siguientes criterios:

- Hello interval.
- Dead interval.
- Area ID.
- Autentificación.
- Otras prestaciones.

Si coinciden la siguiente información se incluye en la tabla de vecinos:

- Neighbor ID: Router ID del router.
- Prioridad: Prioridad del router utilizada para la elección del DR.
- Estado: Indica si el router se ve, esta en proceso de configurar la comunicación bidireccional, esta compartiendo información del estado de enlace o es adyacente.
- Dead time: indica cuanto tiempo ha pasado desde el último paquete Hello recibido.
- Link-local IPv6 address: La dirección link-local del router.
- Designated Router (DR): Indica si el router es DR o Backup DR (BDR).
- Interfaz local: La interfaz por la que recibe los paquetes Hello del vecino.

Cuando el primer paquete Hello de un router nuevo, se pone en el estado de “initialization”. Cuando se establece la comunicación bidireccional pasa al estado “two-way”. Cuando empiezan

a intercambiar sus Link-State Database (LSDB) pasan a los estados “ExStart” inicialmente y “exchange” posteriormente. Cuando se completa el intercambio pasa al estado “full” que significa adyacencia completa. Si falla el envío de cualquier paquete Hello en el Dead Interval el router pasa al estado “down” y ya no se considera adyacente.

3.5 Adyacencia

No todos los vecinos establecen adyacencia. Dependiendo del tipo de red y el DR algunos routers pasan al estado de adyacencia completa y comparten LSAs con todos sus vecinos, mientras que otros no lo hacen.

La adyacencia se establece usando los paquetes Database Description, Link State Request (LSR) y Link State Update (LSU) en OSPFv3. El router envía cabeceras con su propía base de datos de estado de enlace y determina que LSAs son nuevos o actualizados. Ademas envía paquetes LSR por cada LSA nuevo que necesita. El destino responde con LSU. Esto se repite hasta que la información de la base de datos de ambos routers converge.

3.6 Designated Routers

Las redes con múltiples routers presentan una situación única para OSPFv3. Si cada router inunda la red con LSAs, la misma información se enviaría por múltiples fuentes. Dependiendo del tipo de red, OSPFv3 puede usar un router, el router designado (DR), para controlar el envío de LSAs y representar la red para el resto de routers de la misma área. Si el DR falla, se selecciona al router designado de reserva (BDR) para convertirse en DR.

Los tipos de red pueden ser:

- Punto a punto: Solo existe entre dos routers. Todos los vecinos de la red establecen adyacencia y no existe DR.

- Broadcast: Un red con múltiples routers que pueden comunicarse por un medio compartido que permite el trafico broadcast (como Ethernet). El DR y BDR controlan el flujo de LSAs en la red. Para ello se usan direcciones multicast como FF02::5 y una MAC de 0100.5300.0005 para comunicarse con sus vecinos.

El DR y el BDR se seleccionan de la información de los paquetes Hello. Cuando una interfaz lo envía rellena los campos prioridad, DR y BDR para saber quienes son los DR y BDR. Para ello OSPFv3 elige al router que tiene un ID mas alto como DR y BDR.

Todos los routers establecen adyacencia con el DR y el BDR y usan la dirección FF02::5 para enviar las actualizaciones de LSA. Esto se puede observar en la siguiente imagen:

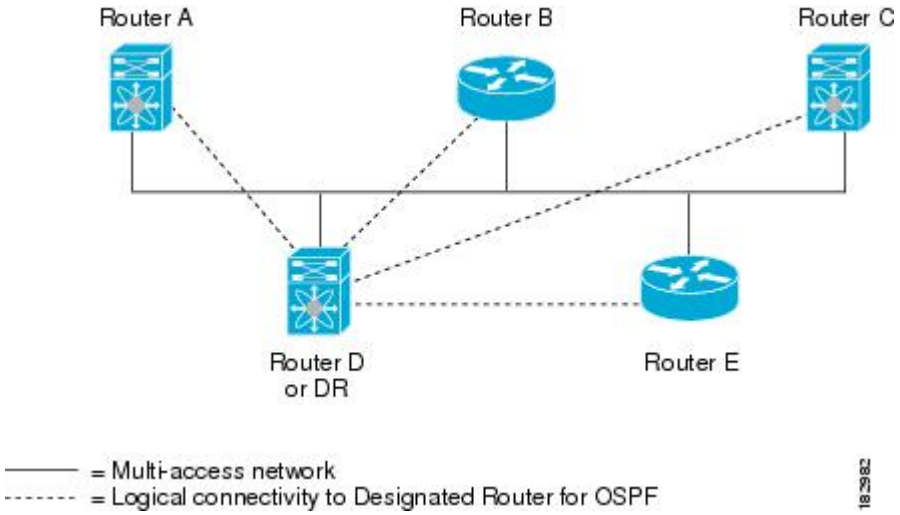


Figura 12. Adyacencia con el DR.

Cada subred posee un DR. Esto quiere decir que en una interfaz un router puede ser DR y en otra no serlo.

3.7 Areas

Se puede limitar los requerimientos de memoria y CPU que consume OSPFv3 en un router dividiendo la red en áreas. Un área es una división lógica de routers y enlaces dentro un dominio OSPFv3 dividiéndolo en subdominios. El flujo de LSAs se delimita a un área, al igual que la base de datos de estado de enlace. El ID del área es un valor de 32 bits que puede ser expresado como un numero o en decimal puntuado, como 10.175.221.50 (como una dirección IPv4).

Si se define más de un área en una red OSPFv3, también se debe definir el área de backbone, que tiene reservado el ID 0. Todas las áreas deben conectarse con el área de backbone. Si existe más de un área entonces uno o más routers se convierten en routers frontera del área (ABR). Un ABR conecta el área de backbone con una o más áreas. Un ejemplo se puede ver en la siguiente imagen:

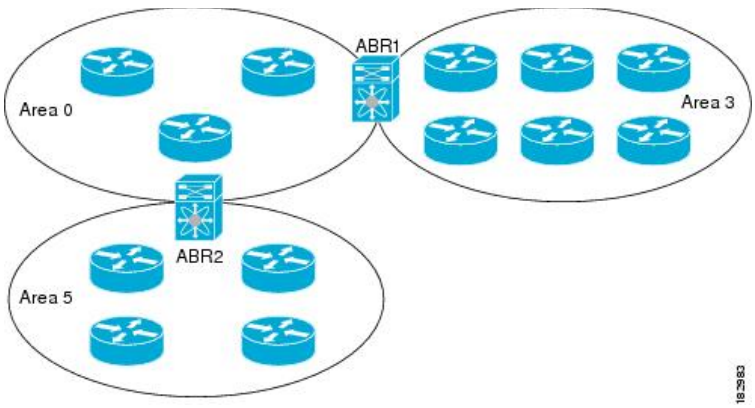


Figura 13. Áreas OSPFv3.

El ABR separa las bases de datos de cada área con la que esta conectado. Esté envía LSAs de tipo 3 con el prefijo Inter-Area para conectar un área con el área de backbone. En la figura anterior, el área 0 envía la información resumida a las áreas 3 y 5.

Además OSPFv3 define otro tipo de router: el router frontera de sistema autónomo (ASBR). Este conecta un área con otro sistema autónomo. Un sistema autónomo es una red controlada por una entidad técnica de administración única. OSPFv3 puede redistribuir su información de routing a otro sistema autónomo o redistribuir las rutas de otro sistema autónomo.

3.8 Link-State Advertisement

OSPFv3 utiliza LSAs para construir la base de datos de estado de enlace y con ello la tabla de enrutamiento.

3.8.1 Tipos de LSA

Tipo	Nombre	Descripción
1	Router LSA	Son los que envía cada router. Estos LSA incluyen el estado y el coste de cada uno de los links, pero no tiene información del prefijo. Los mensajes provocan la ejecución del algoritmo SPF y fluyen por cada área OSPFv3 local.
2	Network LSA	Son los enviados por los DR. Este LSA envía una lista de todos los routers de la red. También provocan la ejecución del algoritmo SPF.
3	Inter-Area Prefix LSA	Son los enviados por los ABR a cada elemento de un área externa. Incluye el coste desde el router hasta el destino.
4	Inter-Area Router LSA	Son los enviados por el ABR a un área externa. Solamente envia el coste del enlace al ASBR.
5	AS External LSA	Son los generados por el ASBR. Incluye el coste hasta el sistema autónomo externo de destino. Se envían hacia fuera del sistema autónomo.
7	Type-7 LSA	Son los generados por el ASBR dentro de una NSSA. Incluye el coste a un sistema autónomo externo. Solamente se fluyen dentro de una NSSA local.
8	Link LSA	Enviados por todos los routers, con alcance de enlace local. Incluye las direcciones link-local y los prefijos IPv6 para ese enlace.
9	Intra-Area Prefix LSA	Enviados por todos los routers. Incluye cualquier cambio en los prefijos o estado del enlace. Se envían dentro de un área local. No provocan la ejecución del algoritmo SPF.
11	Grace LSA	Enviados por un router reiniciado, con alcance de enlace local. Se envían para realizar un reinicio sencillo del proceso OSPFv3.

Tabla 4. Tipos de LSA.

3.9 Coste de enlace

Cada interfaz OSPFv3 tiene asignado un coste. El coste es un numero arbitrario. Por defecto se asigna un numero que es el ancho de banda de referencia entre el ancho de banda de la interfaz. El ancho de banda de referencia es 40 Gbps. El coste de cada enlace lo transportan los LSA de actualización.

3.10 Inundación y LSA Group Pacing

OSPFv3 manda actualizaciones a diferentes secciones de la red dependiendo del tipo de LSA. Utiliza los siguientes alcances:

- Link-local: Solo en el enlace local. (Link LSAs y Grace LSAs).

- Area-local: Dentro del un area OSPFv3. (Router LSAs, Network LSAs, Inter-Area-Prefix LSAs, Inter-Area-Router LSA y Intra-Area-Prefix LSAs).

- Alcance AS: Dentro de un dominio. (AS External LSAs).

La inundación es relativa a la configuración de áreas OSPFv3 y permite que una red tenga información idéntica de routing. Los LSAs se envían en base a el tiempo de actualización de estado de enlace (por defecto cada 30 minutos). Cada LSA tiene su propio tiempo de actualización.

Se puede controlar el flujo de LSAs de actualización usando la característica LSA group pacing. Esto puede reducir la utilización de la CPU o el buffer. Esta característica agrupa varios LSA con tiempos de actualización similares en un solo LSA de actualización.

Por defecto los LSA con tiempos de actualización parecidos (10 segundos de diferencia máximo) se agrupan. Se puede definir este valor más pequeño para tener bases de datos de estado de enlace más grandes o se puede definir más grande para bases de datos más pequeñas y optimizar la carga en la red del protocolo OSPFv3.

3.11 Base de datos de estado de enlace

Cada router almacena una base de datos de estado de enlace para cada red OSPFv3. Esta base de datos contiene todos los LSAs recibidos y incluye información de todos las rutas a través de la red. OSPFv3 utiliza esta información para calcular las rutas hasta cada destino y publica la tabla de routing con las mejores.

Los LSA se borran de la base de datos si no se reciben actualizaciones dentro del intervalo definido (llamado MaxAge que es un tiempo de vida). Los routers envían una repetición de los LSA cada 30 minutos para prevenir que la información se quede obsoleta.

3.12 OSPFv3 y la RIB unicast de IPv6

OSPFv3 ejecuta el algoritmo de Dijkstra SPF sobre la base de datos de estado de enlace. Este algoritmo selecciona la mejor ruta para cada destino basandose en la suma de todos los costes de enlace para cada enlace en un camino. El camino más corto para cada destino se introduce en la tabla de routing de OSPFv3. Cuando la red converge esta tabla se introduce en la RIB unicas de IPv6. OSPFv3 se comunica con la tabla de routing con los siguientes fines:

- Añadir o eliminar rutas.
- Manipular la redistribución de turas de otros protocolos.
- Proporcionar actualizaciones convergentes para eliminar rutas OSPFv3 obsoletas.

Además ejecuta el algoritmo de Dijkstra modificado para recalcular rapidamente la tabla con cambios en los LSAs Inter-Area Prefix, Inter-Area Router, AS-External, type-7 y Intra-Area Prefix. **[4]**

-

3.13 Ejemplo configuración OSPFv3

A modo de ilustrar los conceptos sobre OSPFv3 se realiza el siguiente ejemplo de diseño y configuración de una red integral IPv6 y enrutada con OSPFv3:

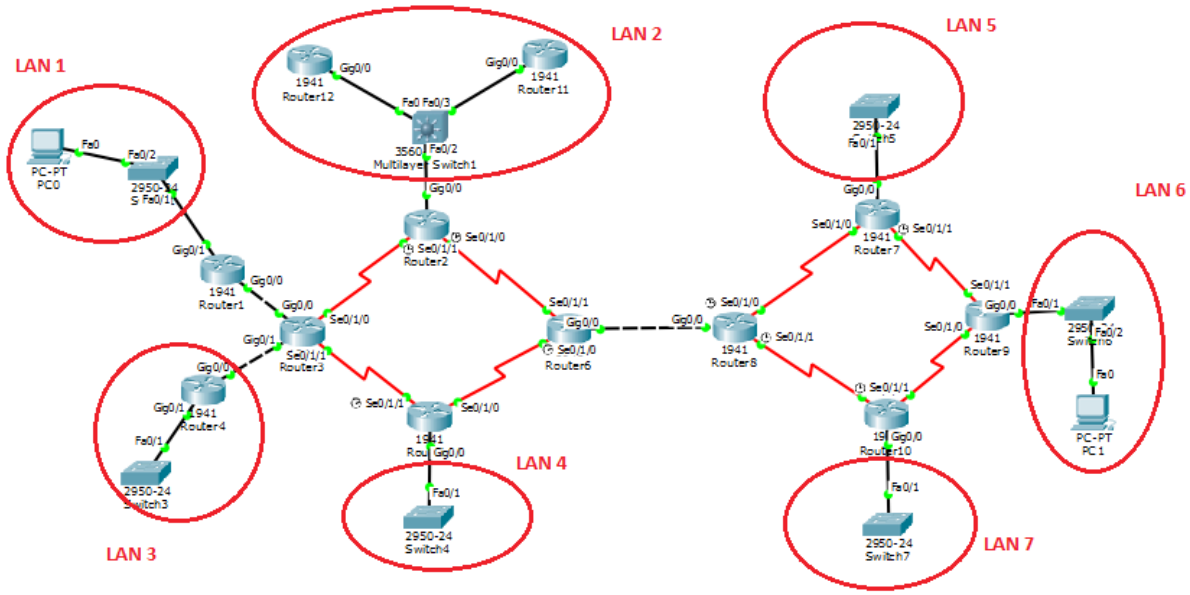


Figura 14. Red multiárea OSPFv3.

Se define 7 LANs corporativas con capacidad para 256 hosts internos por cada una. Se define una red de transporte redundada para comunicar las 7 sedes. El direccionamiento de las redes LAN se define según sigue para cumplir los requerimientos:

- LAN 1: 2001::/120
- LAN 2: 2001::100/120
- LAN 3: 2001::200/120
- LAN 4: 2001::300/120
- LAN 5: 2001::400/120
- LAN 6: 2001::500/120
- LAN 7: 2001::600/120

Por último sera necesario direccionar los enlaces punto a punto. En el siguiente esquema se puede ver los enlaces totales realizados:

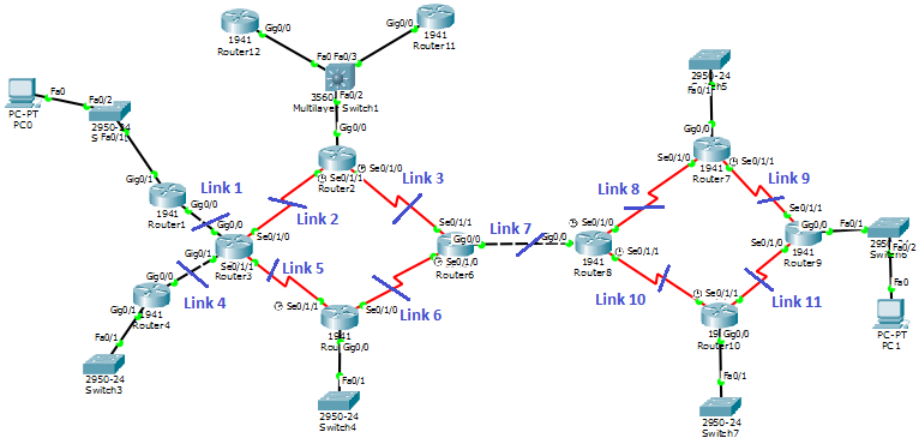


Figura 15. Enlaces ejemplo de configuración.

Cuyo direccionamiento se ha diseñado según sigue:

- Link 1: 2001::700/127
- Link 2: 2001::702/127
- Link 3: 2001::704/127
- Link 4: 2001::706/127
- Link 5: 2001::708/127
- Link 6: 2001::70A/127
- Link 7: 2001::70C/127
- Link 8: 2001::70E/127
- Link 9: 2001::710/127
- Link 10: 2001::712/127
- Link 11: 2001::714/127

Además para descargar la red de routers de alta inundación de LSAs, se definen dos areas OSPFv3 según sigue:

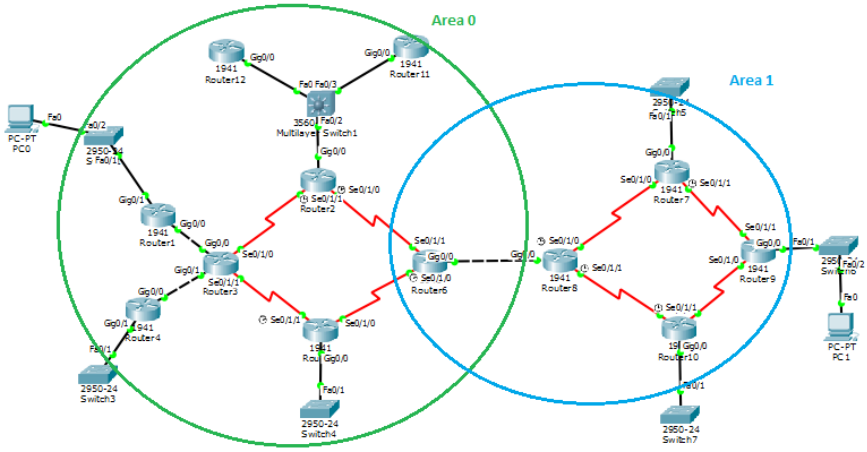


Figura 16. Áreas ejemplo de configuración.

Con el propósito de poner de ejemplo la configuración completa se ejemplificará con la configuración del **Router2**:

Router>enable

Router#configure terminal

Router(config)#ipv6 unicast-routing

Router(config)#no ip domain-lookup

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001::/120

Router(config-if)#ipv6 ospf 1 area 0

Router(config-if)#no shutdown

Router(config-if)#interface Serial0/1/0

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001::704/127

Router(config-if)#ipv6 ospf 1 area 0

Router(config-if)#ipv6 ospf cost 10 // Se prioriza este enlace

Router(config-if)#no shutdown

Router(config-if)#interface Serial0/1/1

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001::702/127

Router(config-if)#ipv6 ospf 1 area 0

Router(config-if)#no shutdown

Router(config-if)#ipv6 router ospf 1

Router(config-rtr)#router-id 0.0.0.2

Se decide priorizar en Link 3 y el Link 8 para poder lanzar trazas desde los PCs y que las rutas sean constantes.

También pondré la configuración del **Router6** para mostrar como es la configuración de un router con interfaces en distintas áreas.

Router>enable

Router#configure terminal

Router(config)#ipv6 unicast-routing

Router(config)#no ip domain-lookup

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001::70C/127

Router(config-if)#ipv6 ospf 1 area 1

Router(config-if)#no shutdown

Router(config-if)#interface Serial0/1/0

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001::70B/127

Router(config-if)#ipv6 ospf 1 area 0

Router(config-if)#no shutdown

Router(config-if)#interface Serial0/1/1

Router(config-if)#ipv6 enable

Router(config-if)#ipv6 address 2001::705/127

Router(config-if)#ipv6 ospf 1 area 0

Router(config-if)#ipv6 ospf cost 10 // Se prioriza este enlace

Router(config-if)#ipv6 router ospf 1

Router(config-rtr)#router-id 0.0.0.6

Con esta configuración la red diseñada esta completamente direccionada. Mostrando la tabla de enrutamiento de, por ejemplo, el Router2 se puede comprobar:

Router#show ipv6 route
IPv6 Routing Table - 22 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001::/120 [110/66]
via FE80::260:47FF:FE56:9801, Serial0/1/1
C 2001::100/120 [0/0]
via GigabitEthernet0/0, directly connected
L 2001::100/128 [0/0]
via GigabitEthernet0/0, receive
O 2001::200/120 [110/66]
via FE80::260:47FF:FE56:9801, Serial0/1/1
O 2001::300/120 [110/75]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::400/120 [110/22]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::500/120 [110/86]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::600/120 [110/76]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
O 2001::700/127 [110/65]
via FE80::260:47FF:FE56:9801, Serial0/1/1
C 2001::702/127 [0/0]
via Serial0/1/1, directly connected
L 2001::702/128 [0/0]
via Serial0/1/1, receive
C 2001::704/127 [0/0]
via Serial0/1/0, directly connected
L 2001::704/128 [0/0]
via Serial0/1/0, receive
O 2001::706/127 [110/65]
via FE80::260:47FF:FE56:9801, Serial0/1/1
O 2001::708/127 [110/128]
via FE80::260:47FF:FE56:9801, Serial0/1/1
O 2001::70A/127 [110/74]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::70C/127 [110/11]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::70E/127 [110/21]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::710/127 [110/85]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::712/127 [110/75]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
OI 2001::714/127 [110/139]
via FE80::290:CFF:FE1B:5801, Serial0/1/0
L FF00::/8 [0/0]

via Null0, receive

Con esto se comprueba que la configuración ha llegado al estado de convergencia en ambas áreas. Como último ejemplo se mostrara las rutas desde un PC de la LAN 1 a un PC de la LAN 6 y viceversa, teniendo en cuenta que se ha priorizado los Links 3 y 8.

Dirección PC0 (LAN1) = 2001::1/120

Dirección PC1 (LAN6) = 2001::501/120

Traza desde el PC0 al PC1:

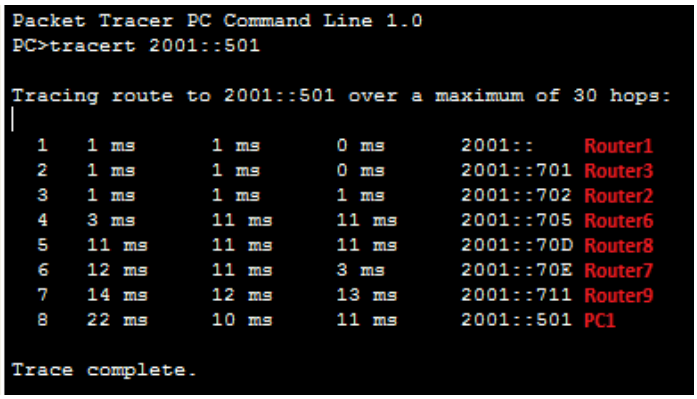


Figura 17. Prueba traza PC0 a PC1.

Traza desde el PC1 al PC0:

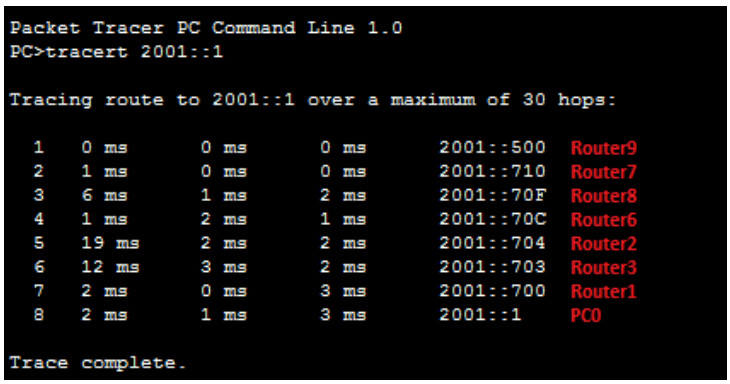


Figura 18. Prueba traza PC1 a PC0.

Con esto acaba el ejemplo de configuración de una red completa con OSPFv3.

Capítulo 4. IS-IS

El protocolo IS-IS (Intermediate System to Intermediate System) es un protocolo de estado de enlace que, al igual que OSPF, utiliza en algoritmo de Dijkstra para definir la mejor ruta a través de la red.

Las diferencias entre ambos protocolos se basan en el modo de funcionamiento. IS-IS asigna una dirección de area y de host a un router, en vez de a un interfaz. Cada router IS-IS de nivel 1 estará en una unica area y necesitara de un router de nivel 1-2 para interconectar areas. El router de nivel 1-2 es la ruta por defecto del area de nivel 1 y ve el sistema autonomo completo.

Los paquetes hello en IS-IS pueden ser de nivel 1 o nivel 2. En una red broadcast todos los routers son adyacentes. IS-IS opera en capa 2 y tiene su propio paquete de capa 3, con lo que la fragmentación es su responsabilidad. **[5]**

4.1 Configurar IS-IS

Para configurar IS-IS es necesario realizar dos configuraciones. Primero configurar el proceso IS-IS en el router. Segundo configurar IPv6 IS-IS en una interfaz. Los pasos son los que siguen:

Router>enable

Router#configure terminal

Router(config)#router isis *EtiquetaDelArea*

Router(config-router)#net *TituloDeLaEntidadDeRed*

Router(config)#interface *Tipo Numero*

Router(config-if)# ipv6 address *DireccionIPv6/LongitudDelPrefijo*

Router(config-if)#ipv6 router isis *EtiquetaDelArea*

Con esto es posible configurar IS-IS para una topología simple en IPv6. **[6]**

Capítulo 5. DHCPv6

IPv6 se diseño pensando en la asignación dinámica de direcciones. Teniendo en cuenta que las direcciones tienen 128 bits, realizar la asignación automática de direcciones es un aspecto importante dentro del diseño de redes. El tamaño de direcciones y la escritura de hexadecimales es un inconveniente para la asignación manual de direcciones en entornos medios y grandes, pues el formato no es intuitivo para el ojo humano. Para facilitar la asignación con poca o ninguna intervención humana se han desarrollado bastantes métodos y tecnologías para automatizar el proceso y los parámetros de configuración de los hosts IPv6.

Los métodos de asignación son los siguientes:

1) Asignación manual

Una dirección IPv6 se puede asignar manualmente por un operador humano. Esto esta abierto a errores y es excesivamente costoso realizarlo para cada elemento de red (recordemos que son direcciones de 128, es decir, 32 caracteres hexadecimales). Sin embargo para las interfaces de los routers y para elementos y recursos de red estáticos puede ser una solución apropiada.

2) Stateless Address Autoconfiguration (RFC2462)

SLAAC (por sus siglas en inglés) es uno de los métodos más convenientes para asignar direcciones a nodos IPv6. No requiere intervención humana para el usuario. Si se desea utilizar SLAAC el nodo debe estar conectado a una red con, por lo menos, un router. El router envía mensajes Router Advertisement que el nodo puede usar para autoconfigurarse con una dirección IPv6 y parámetros de enrutamiento, como especifica la RFC2462.

3) Stateful DHCPv6

DHCPv6 ha sido estandarizado por la IETF en la RFC3315. El protocolo capacita a los servidores DHCP a enviar los parametros de configuración, como la dirección de red, a los nodos IPv6. Esto posibilita la automatica asignación de direcciones reutlizables y flexibiliza la configuración. Este protocolo es el equivalente stateful de SLAAC.

4) DHCPv6-PD

DHCPv6 Prefix Delegation es una extensión de DHCPv6 especificada en la RFC3633. En general funciona como DHCPv6, pero permite delegar la asignación de una subred. Esto quiere decir que un cliente podría ser servidor de una subred mas pequeña y asignar dinámicamente el rango de direcciones recibido.

5) Stateless DHCPv6

Stateless DHCPv6 es una combinación de SLAAC y DHCPv6 especificada en la RFC3736. Básicamente es una configuración con SLAAC y la recepción de parámetros adicionales, como el servidor DNS o NTP, del protocolo DHCPv6. Esto puede ser útil para descargar la red de mensajes DHCPv6 en entornos inestables donde los cambios son bastante comunes.

El funcionamiento de DHCPv6 es similar al concepto cliente-servidor de DHCP para IPv4. Si un cliente quiere recibir los parametros de configuración enviará una petición a la red local. El servidor DHCPv6 le responderá con los parametros de configuracion solicitados como se ve en la siguiente imagen:

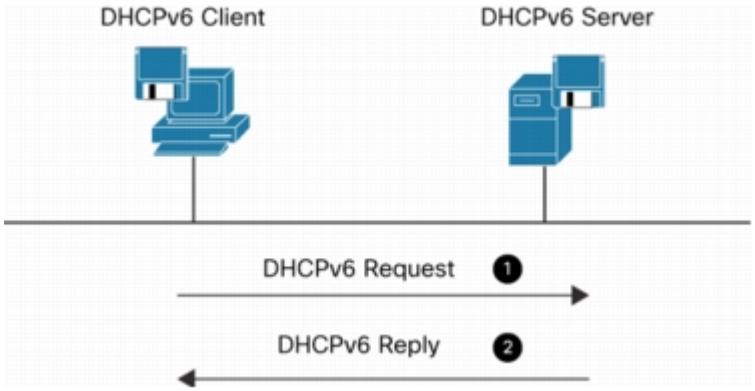


Figura 19. Funcionamiento DHCPv6.

DHCPv6 ofrece la capacidad de asignación de direcciones reutilizables automatica y configuración adicional (por ejemplo servidor DNS, servidor NTP, etc.). El protocolo utiliza un concepto de arquitectura de “opciones” para transportar parametros adicionales y información. Estas opciones utilizan la estructura TLV (Type-Length-Value). Cada campo tipo y longitud tienen un tamaño de 16 bits, mientras que el campo valor tiene tamaño variable. Cada opcion debe aparecer solo una vez en el mensaje DHCPv6, aunque el estandar no lo restringe.

5.1 Componentes DHCPv6

Cada componente de DHCPv6 tiene un DUID (DHCPv6 Unique Identifier) que es utilizado por el equipo para intercambiar mensajes DHCPv6. El DUID se encuentra en el campo de opciones del mensaje debido a que su longitud puede ser variable y no es necesario en todos los mensajes. El DIUD debe ser unico y estable tanto en clientes como en servidores (por ejemplo, un DUID no debe cambiar por cambiar un elemento de hardware de un equipo).

Hay tres tipos definidos de DUID:

- Link-layer address plus time (DUID-LLT)
- Vendor-assigned unique ID basado en el Enterprise Number
- Link-layer address (DUID-LL)

El campo DUID-LLT se construye según sigue:

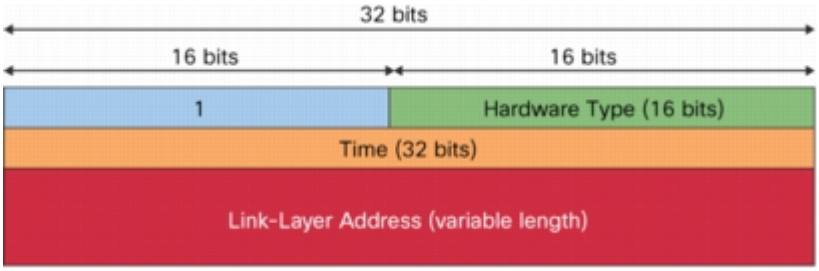


Figura 20. Construcción DUID-LLT.

Es decir:

- Dos octetos que contienen el valor 1.
- Dos octetos con el código del tipo de hardware.
- Cuatro octetos con un valor de tiempo.
- La dirección de la capa de enlace de red de cualquier interfaz conectado al equipo DHCP en el momento en que el DUID se genera.

5.2 Selección de una dirección por un servidor DHCPv6

El servidor selecciona una dirección para asignarla a una asociación de identidad según las politicas de asignación de direcciones determinadas por el administrador del servidor y por información especifica del cliente como:

- El enlace en el que esta el cliente.
- El DUID del cliente.
- Otra información suministrada por el cliente.
- Otra información suministrada por el relay agent.

5.3 Mensajes DHCPv6 cliente/servidor

Los mensajes se intercambian por los puertos UDP 546 y 547. Los clientes escuchan a traves del puerto 546 y los servidores y realy agents escuchan por el puerto 547. El formato basico del mensaje es el que sigue:

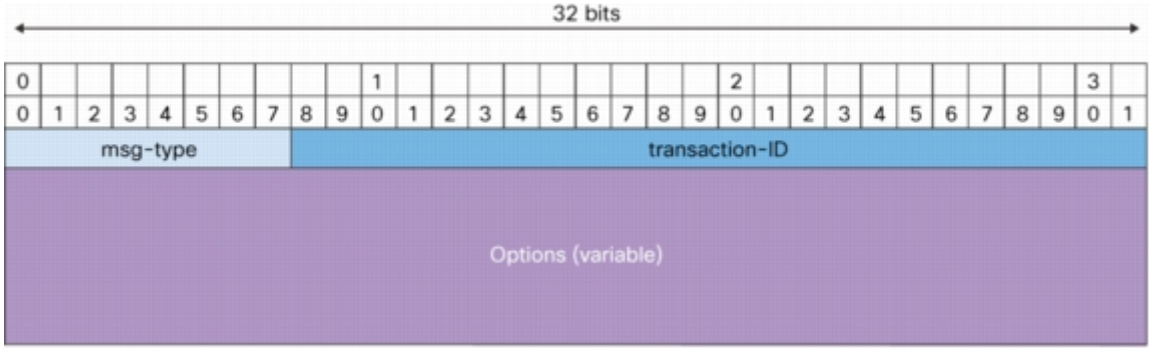


Figura 21. Estructura mensajes DHCPv6.

Mensajes cliente -> servidor:

Solicit, Request, Confirm, Renew, Rebind, Release, Decline, Information-Request.

Mensajes servidor -> cliente:

Advertise, Reply, Reconfigure.

Mensajes relay -> relay/server:

Relay-Forw.

Mensajes server -> Relay:

Relay-Reply.

Para recudir los requerimientos de campos fijos, cuando potencialmente no es necesario el uso de todos los campos, se utiliza una solución flexible basada en los campos de opciones de DHCPv6 en la capa de transporte. Por lo tanto, todos los datos se transportan con uso dinámico y selección de opciones.

Los posibles mensajes son los siguientes:

SOLICIT (1)

Un cliente DHCPv6 envía una solicitud a los servidores locales.

ADVERTISE (2)

El servidor envía este mensaje para indicar que está disponible para realizar el servicio de DHCP. Se envía en respuesta al mensaje SOLICIT recibido de un cliente.

REQUEST (3)

Un cliente envia este mensaje para pedir parámetros de configuración al servidor, lo que incluye direcciones IP o prefijos delegados.

CONFIRM (4)

Un cliente envía un mensaje Confirm a cualquier servidor disponible para determinar si la dirección asignada sigue siendo apropiada en el enlace en el que esta conectado. Este mensaje se enviará cuando el cliente detecte un cambio en la conectividad de la capa de enlace o si se enciende el equipo cliente y una o mas de las direcciones asignadas son validas. También se usa para saber si el cliente sigue en la misma red o ha sido conectado a otra. La actual asignación no se valida, solo el prefijo de la dirección o el prefijo delegado.

RENEW (5)

Un cliente envía un mensaje Renew al servidor que le proporcionó originalmente la dirección y los parámetros de configuración para extender el tiempo de vida de las direcciones asignadas al cliente y para actualizar otros parámetros de configuración.

REBIND (6)

Un cliente envía un mensaje Rebind a cualquier servidor disponible para extender el tiempo de vida de las direciones asignadas y actualizar otros parametros de configuración. Este mensaje se envía después de que el cliente no reciba respuesta a un mensaje Renew.

REPLY (7)

Un servidor envía en mensaje Reply que contiene las direcciones asingadas y los parametros de configuración en respuesta a los mensajes Solicit, Request, Renew o Rebind enviados por el cliente. También envía estos mensajes con parametros de configuración en respuesta a un mensaje Informatio-request. Además se envian en respuesta a un mensaje Confirm, confirmando o negando que las direcciones asignadas al cliente son apropiadas para en el enlace en el cual el cliente está conectado. Por último, el servidor enviará este mensaje como reconocimiento de un mensaje Release o Decline.

RELEASE (8)

Un cliente envía un mensaje Release al servidor que le asignó las direcciónes para indicar que no va a utilizar más una o más de las direcciones asignadas.

DECLINE (9)

Un cliente envía un mensaje Decline al servidor para indicar que ha determinado que una o más de las direcciones que le ha asignado están ya en uso en el enlace en el que esta conectado.

RECONFIGURE (10)

Un servidor envía un mensaje de Reconfigure al cliente para informarle que el servidor tiene nuevos o actualizados parámetros de configuración y el cliente puede iniciar una transacción Renew/Reply o Information-Request/Reply con el servidor para recibir la información actualizada.

INFORMATION-REQUEST (11)

Un cliente envía un mensaje Information-Request a un servidor para pedir parametros de configuración sin ninguna asignación de IP.

RELAY-FORW (12)

Un realy agent envía un mensaje Relay-forward para reenviar mensajes a los servidores conectados directamente o a traves de otro relay agent. El mensaje recibido de un cliente o otro el mensaje Relay-forward se encapsula como una opción dentro del propio mensaje.

RELAY-REPL (13)

Un servidor envía un mensaje Relay-reply a un relay agent conteniendo el mensaje que el relay agent debe entregar al cliente. Este mensaje puede ser retransmitido a través de otro relay agent hasta llegar al destino. El servidor encapsula el mensaje para el cliente como una opción dentro del mensaje Relay-reply, el cual extrae y retransmite al cliente. **[7]**

-

Capítulo 6. Firewall ASA 5505

Un Firewall es un dispositivo de seguridad perimetral que implementa distintas funciones tales como el bloqueo de accesos no autorizados o bloqueo de ataques. Al no disponer de más elementos en la versión 6.1 de Cisco Packet Tracer se utilizará el modelo ASA 5505 para probar su configuración y capacidades en IPv6.

6.1 Configurar DMZ

Para el entorno que nos ocupa, el diseño de una red corporativa, este elemento nos permitirá tener una DMZ (o zona desmilitarizada por sus siglas en inglés) para el acceso desde el exterior de la red a servidores en dicha zona.

Un ejemplo de configuración se puede ver en la siguiente imagen:

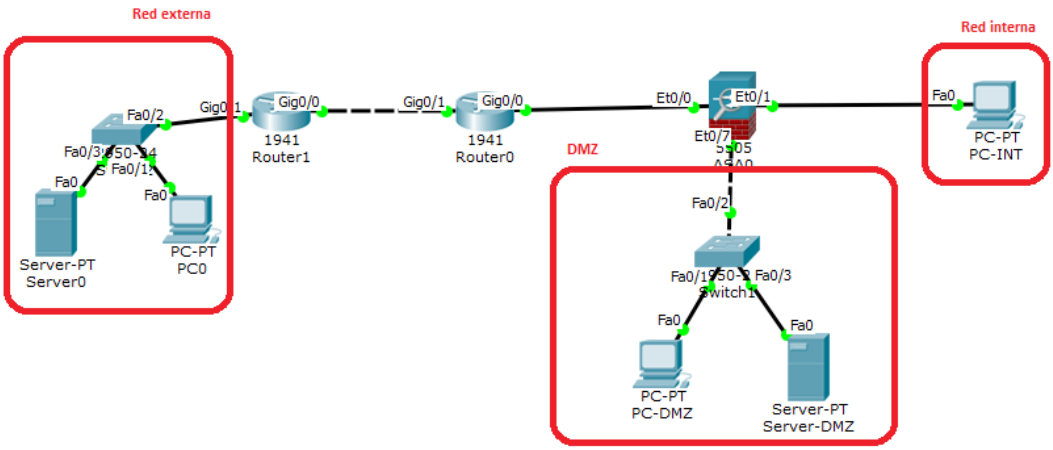


Figura 22. Estructura de la red con DMZ.

Con este ejemplo se intentá crear una zona que sea accesible desde la red externa y interna, pero que no comprometa la red interna desde la red externa o la misma DMZ.

Para ello se crean 3 VLANs según siguen:

interface Vlan1

nameif inside
security-level 100
ip address 192.168.1.0 255.255.255.0
ipv6 address 2001::/120
!
interface Vlan2
nameif outside
security-level 0
ip address 192.168.3.0 255.255.255.0

ipv6 address 2001::100/120
!
interface Vlan3
no forward interface Vlan1
nameif dmz
security-level 0
ip address 192.168.2.0 255.255.255.0
ipv6 address 2001::200/120

Nota: la existencia de direcciones IPv4 es una cuestión del software del Firewall, el cual daba problemas con la configuración en exclusiva de IPv6 (dejaba de funcionar con un simple reload).

Se puede apreciar que existen tres zonas: inside, outside y dmz. Los niveles de seguridad establecidos permiten la conectividad de dentro hacia fuera y no a la inversa. Además es necesario definir una ruta por defecto en el Firewall y una política de seguridad. Esto se realiza según sigue:

ipv6 route outside ::/0 2001::150 //Ruta estática

!
class-map INSPECCION
match any
!
policy-map POLITICA //Definición de política
class INSPECCION
inspect icmp
!
service-policy POLITICA global //Aplicación política

Para probar que estas reglas funcionan según hemos definido se prueba con pings y conexiones a los servidores. Las direcciones son según siguen:

- Servidores web: DMZ [2001::210], Exterior [2001::2010]
- PCs: Interno [2001::1], DMZ [2001::201], Externo [2001::2001]

En la siguiente imagen se puede ver la conectividad interna a nivel ICMP:

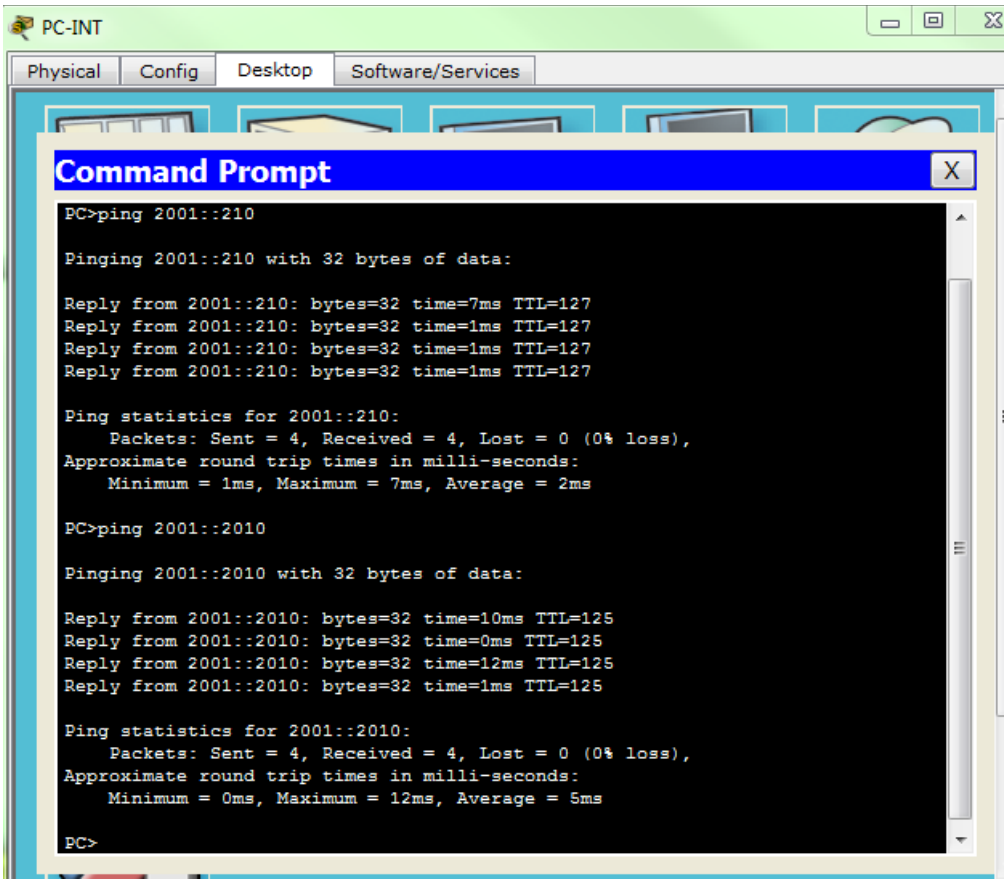


Figura 23. Conectividad ICMP.

Y a nivel HTTP:

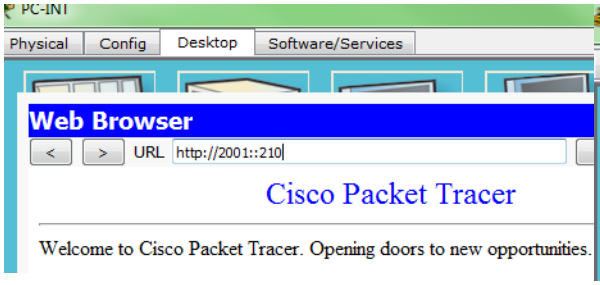


Figura 23. Conectividad HTTP 1.

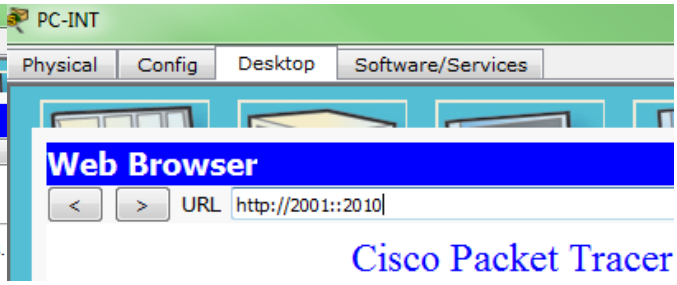


Figura 24. Conectividad HTTP 2.

En cambio ni desde el exterior, ni desde la DMZ, es posible acceder a la red interna:

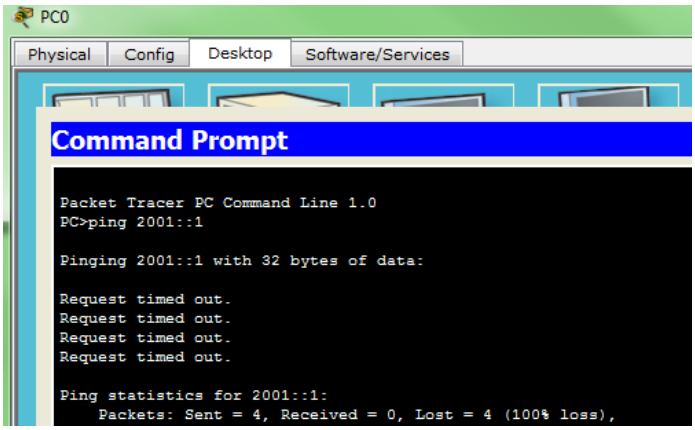


Figura 25. Conectividad DMZ 1.

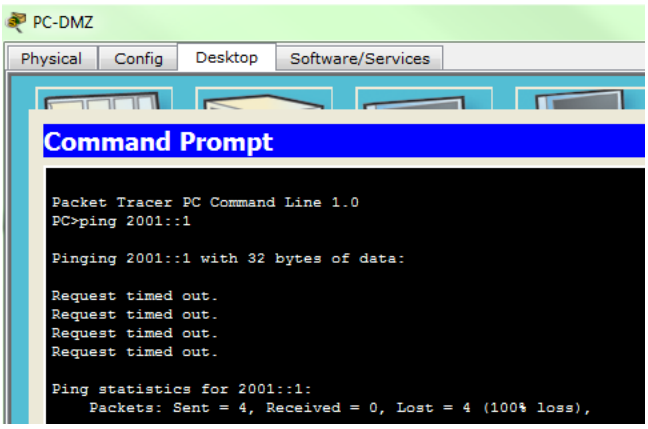


Figura 26. Conectividad DMZ 1

6.2 Creación de un túnel VPN entre dos ASA

Para que la conectividad sea completa entre dos sedes corporativas protegidas propiamente con un Firewall cada una es necesario crear un túnel entre ambos Firewalls. De esta manera no solo aseguraremos el poder conectar las sedes, si no que ademas esta conexión sea segura a través de un entorno hostil (por ejemplo internet).

Supongamos la siguiente configuración:

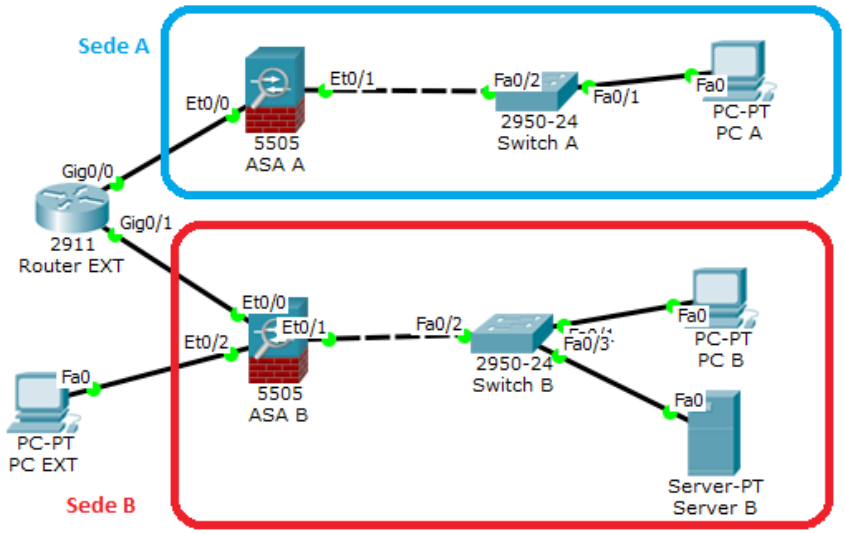


Figura 27. Ejemplo túnel VPN.

Donde el direccionamiento es el siguiente:

- Sede A: 2001:AAAA::/64
- De sede A a Router EXT: 2001:BBBB::/64
- De sede B a Router EXT: 2001:CCCC::/64
- Sede B: 2001:DDDD::/64

1) Primero configuraremos IKE con los mismos parámetros en ambos ASA y habilitaremos IPSEC. Para ello hay que introducir sendos comandos en los Firewall:

crypto ikev1 policy 10

encr aes

authentication pre-share

group 2

crypto ikev1 enable outside

crypto ipsec ikev1 transform-set cisco esp-aes esp-sha-hmac

Con esto habremos realizado la configuración general de IPsec.

2) Ahora es necesario definir ACLs en ambos ASA para que las utilice el túnel que posteriormente configuraremos:

En el ASA de la sede A:

ipv6 access-list IPv6-Lab permit icmp 2001:AAAA::/64 2001:DDDD::/64

ipv6 access-list IPv6-Lab permit tcp 2001:AAAA::/64 lt 65535 2001:DDDD::/64 lt 65535 established
ipv6 access-list IPv6-Lab permit udp 2001:AAAA::/64 lt 65535 2001:DDDD::/64 lt 65535
ipv6 access-list IPv6-Lab permit icmp6 2001:AAAA::/64 2001:DDDD::/64

En el ASA de la sede B:

ipv6 access-list VPN-Traffic permit icmp 2001:DDDD::/64 2001:AAAA::/64

ipv6 access-list VPN-Traffic permit tcp 2001:DDDD::/64 lt 65535 2001:AAAA::/64 lt 65535 established
ipv6 access-list VPN-Traffic permit udp 2001:DDDD::/64 lt 65535 2001:AAAA::/64 lt 65535
ipv6 access-list VPN-Traffic permit icmp6 2001:DDDD::/64 2001:AAAA::/64

3) Ahora es necesario realizar en mapeo de encriptación. Para ello necesitaremos definir: ACL, peer, IKE y interfaz.

En el ASA de la sede A:

crypto map IPv6-L2L 1 match address IPv6-Lab

crypto map IPv6-L2L 1 set peer 2001:CCCC::2

crypto map IPv6-L2L 1 set ikev1 transform-set cisco

crypto map IPv6-L2L interface outside

En el ASA de la sede B:

crypto map IPv6-Lab 1 match address IPv6-Lab

crypto map IPv6-Lab 1 set peer 2001:BBBB::1

crypto map IPv6-Lab 1 set ikev1 transform-set cisco

crypto map IPv6-Lab interface outside

4) Y por último configurar el túnel:

En el ASA de la sede A:

tunnel-group 2001:CCCC::2 type ipsec-l2l

tunnel-group 2001:CCCC::2 ipsec-attributes
kev1 pre-shared-key cisco123

En el ASA de la sede B:

tunnel-group 2001:BBBB::1 type ipsec-l2l

tunnel-group 2001:BBBB::1 ipsec-attributes

ikev1 pre-shared-key cisco123

Con esto la configuración del túnel IPsec entre los dos Firewalls está realizada. **[8]**

Para comprobarlo realizaremos un acceso a portal web de la sede B desde el host de la sede A y desde el PC EXT:

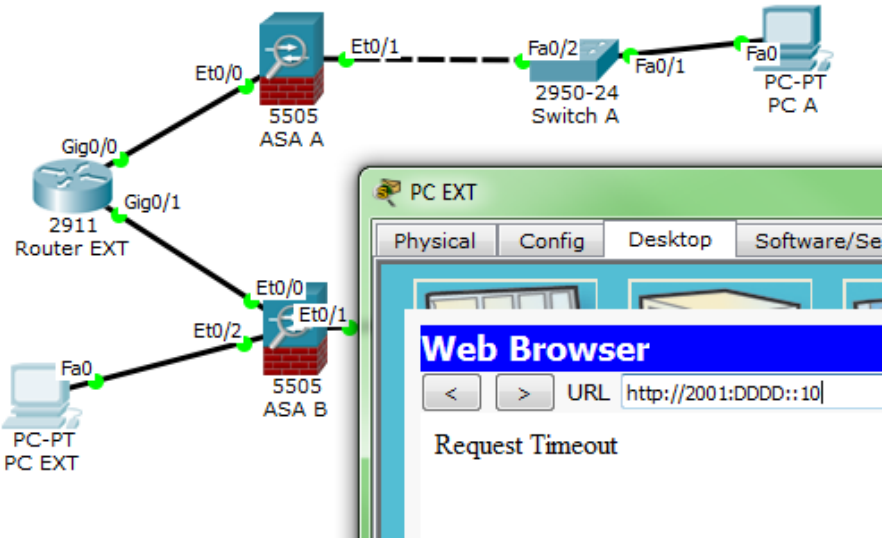


Figura 28. Comprobación túnel VPN (no visible desde el exterior).

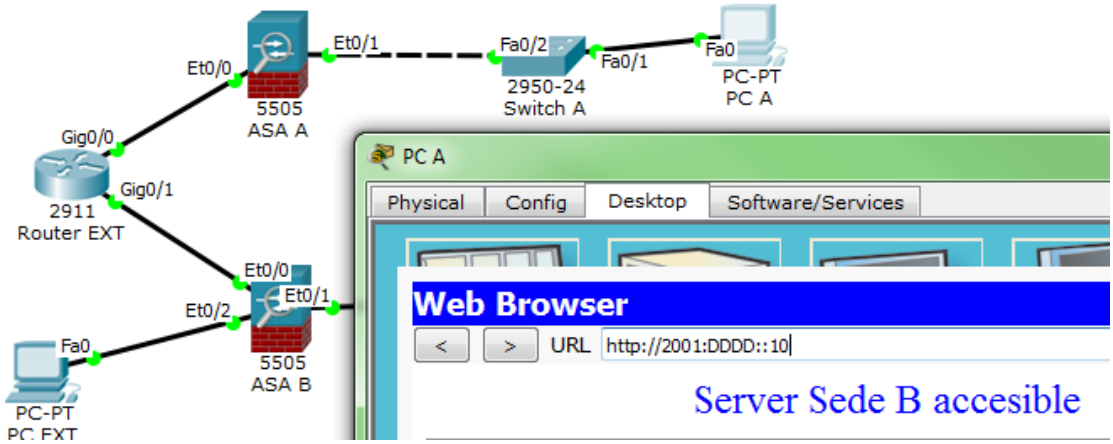


Figura 29. Comprobación túnel VPN (conectividad entre sedes).

Con ello queda demostrado en este ejemplo como configurar un túnel IPsec entre dos sedes.

Capítulo 7. Diseño de una red IPv6 integral

Con objeto de aplicar todos lo anteriormente detallado a nivel teórico y con determinados ejemplos prácticos se procederá al diseño de una red corporativa de una supuesta empresa compuesta de una sede central y una delegación. Supondremos unas condiciones de diseño cerradas, aunque siempre este tipo de diseño será escalable en caso de posible ampliación. Esto se puede ver en el siguiente esquema topológico:

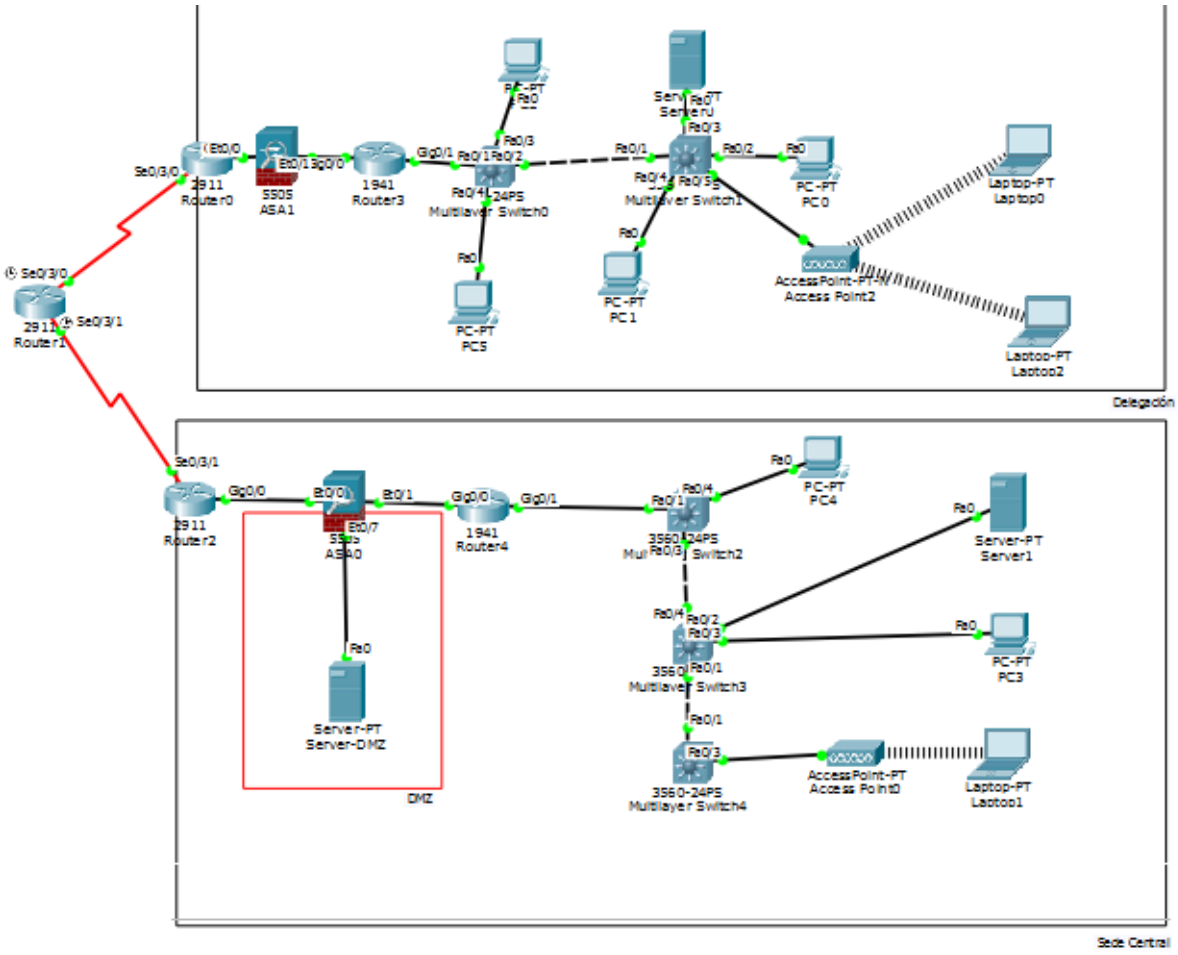


Figura 30. Diseño red IPv6.

7.1 Condiciones de diseño

Para el presente diseño se ha tomado el supuesto de dos redes corporativas. La primera la sede principal (o sede A) será la más grande y constará de 2000 hosts direccionables en su red interna y 500 en la DMZ (por si se quisiera utilizar a modo de red de invitados). Esto se realizará de esta manera para disminuir la vulnerabilidad de la red ante posibles atacantes en la red de invitados. Por último supondremos que la delegación regional unicamente constará de 500 hosts.

Los elementos de la DMZ deben ser accesibles tanto desde dentro de las redes internas de las dos sedes como desde cualquier red externa, pues dentro de ella tendremos un servidor web corporativo que permitirá a la empresa tener visibilidad en internet.

Cualquier elemento dentro de la red interna de cualquiera de las dos sedes no debe ser accesible desde fuera de la red ni desde la DMZ para evitar comprometer información corporativa. Para dicho fin se bloqueará a nivel de Firewall cualquier acceso no autorizado.

Por último ambas subsedes deben tener conectividad para poder compartir herramientas corporativas implementadas dentro de los servidores internos de ambas sedes. Supondremos que todas estas herramientas se crean como un front-end web, con lo que comprobando el acceso HTTP entre las dos subredes será suficiente para el funcionamiento de nuestra corporación.

7.2 Direccionamiento

Como hemos especificado antes en las condiciones de diseño los requerimientos y direcciones asignadas serán las siguientes:

- Sede Central:	2000 hosts	->	direcciones:	2001::/119
- Delegación:	500 hosts	->	direcciones:	2001::800/117
- DMZ:	500 hosts	->	direcciones:	2001::A00/117

Ademas requeriremos direccionamiento para nuestros enlaces punto a punto. En la siguiente imagen se puede ver la nomenclatura utilizada para los mismos:

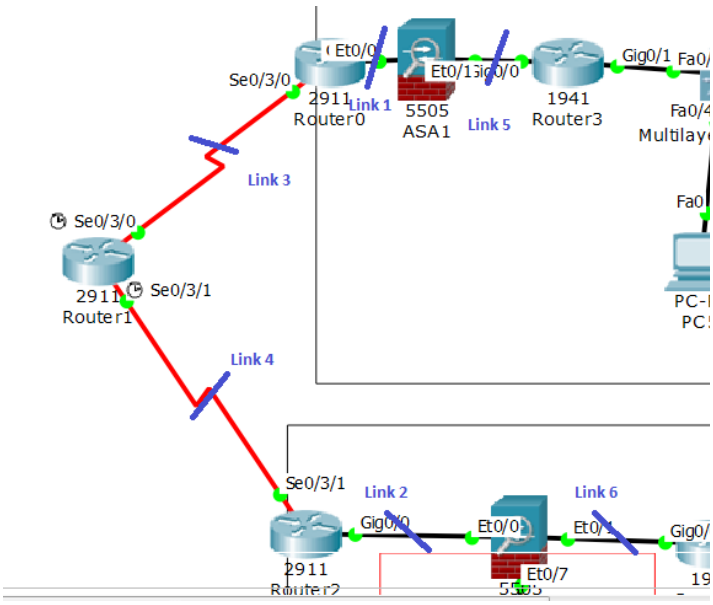


Figura 31. Enlaces punto a punto.

Con lo que el direccionamiento de esos enlaces queda según sigue:

- Link 1: 2001::C00/127
- Link 2: 2001::C02/127
- Link 3: 2001::C04/127
- Link 4: 2001::C06/127
- Link 5: 2001::C08/127
- Link 6: 2001::C0A/127

Con esto queda direccionada completamente la red de diseño. Se requerirá del prefijo 2001::/116 para el presente diseño. Se ha tomado dicho prefijo por simplicidad, pero es valido para cualquier prefijo /116 cambiando 2001:: por el prefijo público asignado XXXX:XXXX:XXXX...::/116. En total hemos utilizado 3084 de las 4096 direcciones posibles (12 bits). Se reservarán el resto para futuros usos.

7.3 Elementos de escalado interno

Para escalar internamente los 2000 equipos de la sede principal y los 500 de la delegación necesitaremos un árbol de switches. Por ello hemos necesitado poner en cascada switches de 24 puertos según sigue:

- Sede principal: 23 puertos (1er switch) x 23 puertos (2^{o} switch) x 23 puertos (3er switch) = 12.167 puertos de acceso.

De sobra para conectar los equipos de la sede principal con 3 niveles de switchs. Se elimina un puerto que será en el caso del primer switch el que conecta al router y en el resto el que conecta al switch por un enlace troncal:

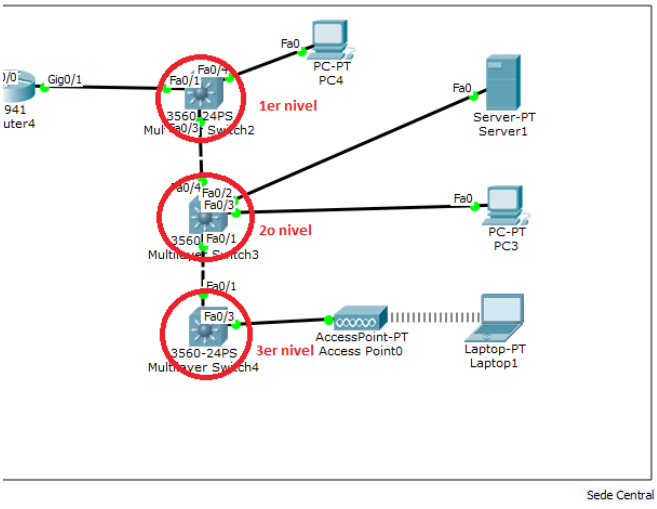


Figura 32. Switches sede central.

- Delegación: 23 puertos (1er switch) x 23 puertos (2o switch) = 529 puertos de acceso.

Suficiente para conectar los equipos de la delegación con dos niveles de switchs:

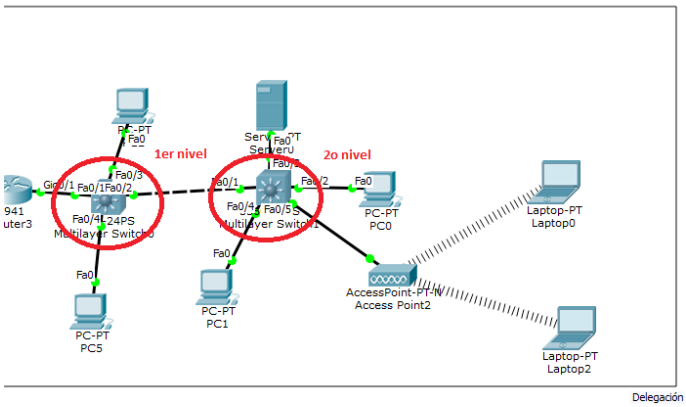


Figura 33. Switches delegación.

Con esto tenemos capacidad para conectar el número de equipos requeridos en las condiciones de diseño en ambas sedes.

7.4 Access Point

Para cumplir con los objetivo de movilidad dentro de nuestras sedes habilitaremos puntos de acceso WiFi conectados a los switches a través de cables Fast Ethernet.

Para la seguridad utilizaremos una autentificación WPA2-PSK con encriptación AES. Dicha configuración se realiza según sigue:

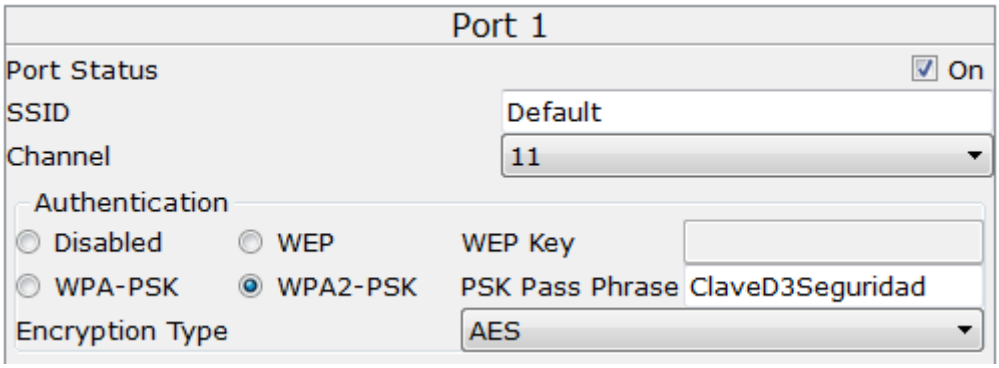


Figura 34. Configuración Access Point.

Existen otros esquemas de seguridad WiFi más robustos, pero como no presentan diferencias en la configuración con respecto a IPv4 no es objeto del presente diseño implantarlos.

7.5 Configuración Routers

Para explicar las configuraciones realizadas en los routers los dividiremos en dos tipos dado que sus configuraciones son similares. Los routers externos serán responsables de la interconexión y encaminamiento entre ambas sedes y serán gestionados por el ISP que nos suministré el servicio de acceso a internet. Los routers internos, ademas de encaminar los paquetes en caso de que se desee realizar más subredes en el futuro, serán los responsables de realizar la asignación dinamica de direcciones a través de DHCPv6. En la siguiente imagen se puede apreciar los elementos clasificados según su tipo:

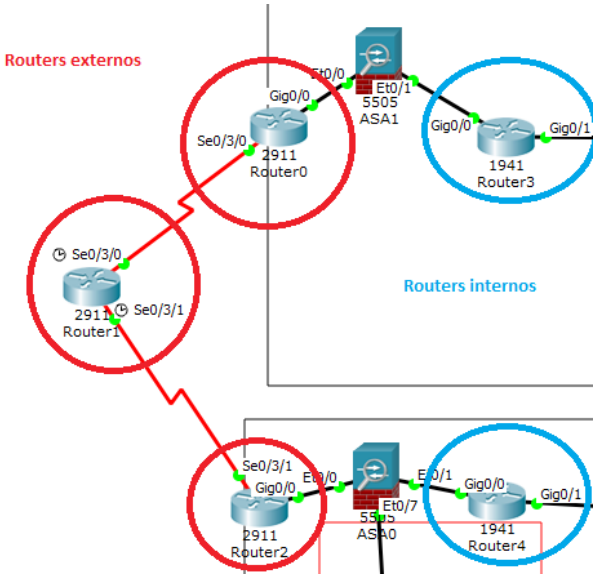


Figura 35. Clasificación de los routers.

Para todos los routers de la red utilizaremos los siguientes dos comandos:

ipv6 unicast-routing // Para permitir el enrutamiento unicast en IPv6

no ip domain-lookup // Para que no realicen búsquedas DNS

Empezaremos con la configuración de los tres routers externos: Router0, Router1 y Router2. Se ha decido utilizar el protocolo OSPFv3 para realizar el encaminamiento entre los routers de acceso a la red.

Router0:

interface GigabitEthernet0/0

no ip address

ipv6 address 2001::C01/127 // Dirección asignada del Link 1 punto a punto

ipv6 enable // Habilitamos IPv6 en la interfaz

ipv6 ospf 1 area 0 // Incluimos la interfaz en el proceso OSPFv3 (área 0)

```
!
interface Serial0/3/0
 no ip address
 ipv6 address 2001::C04/127          // Dirección asignada del Link 3 punto a punto
 ipv6 enable                         // Habilitamos IPv6 en la interfaz
 ipv6 ospf 1 area 0                  // Incluimos la interfaz en el proceso OSPFv3 (área 0)
!
ipv6 router ospf 1                   // Definimos el proceso OSPFv3
 router-id 0.0.0.1                   // Asignamos un router-id (en IPv6 no existe por
defecto)
 redistribute static                 // Para que redistribuya las rutas estáticas
!
ipv6 route 2001::800/119 GigabitEthernet0/0    // Red interna delegación
```

En el último comando hemos añadido una ruta estática para que enrute la red tras el Firewall. Dado que el firewall bloquea los paquetes OSPFv3 y queremos que esto sea así por motivos de seguridad. Se ha hecho lo mismo en el Router2 por lo que se omitirá esta explicación en su configuración.

Router1:

```
interface Serial0/3/0
 no ip address
 ipv6 address 2001::C05/127          // Dirección asignada del Link 3 punto a punto
 ipv6 enable                         // Habilitamos IPv6 en la interfaz
 ipv6 ospf 1 area 0                  // Incluimos la interfaz en el proceso OSPFv3 (área 0)
 clock rate 2000000                  // Ponemos la tasa de reloj porque es el DCE del serial
!
interface Serial0/3/1
 no ip address
 ipv6 address 2001::C07/127          // Dirección asignada del Link 4 punto a punto
 ipv6 enable                         // Habilitamos IPv6 en la interfaz
 ipv6 ospf 1 area 0                  // Incluimos la interfaz en el proceso OSPFv3 (área 0)
 clock rate 2000000                  // Ponemos la tasa de reloj porque es el DCE del serial
!
ipv6 router ospf 1                   // Definimos el proceso OSPFv3
 router-id 10.0.0.0                  // Asignamos un router-id (el más alto para que sea el
DR)
 redistribute static                 // Para que redistribuya las rutas estáticas
```

Router2:

```
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001::C03/127          // Dirección asignada del Link 2 punto a punto
 ipv6 enable                         // Habilitamos IPv6 en la interfaz
 ipv6 ospf 1 area 0                  // Incluimos la interfaz en el proceso OSPFv3 (área 0)
interface Serial0/3/1
 no ip address
 ipv6 address 2001::C06/127          // Dirección asignada del Link 4 punto a punto
 ipv6 enable                         // Habilitamos IPv6 en la interfaz
 ipv6 ospf 1 area 0                  // Incluimos la interfaz en el proceso OSPFv3 (área 0)
!
ipv6 router ospf 1                   // Definimos el proceso OSPFv3
 router-id 0.0.0.2                   // Asignamos un router-id
 redistribute static                 // Para que redistribuya las rutas estáticas
!
ipv6 route 2001::/117 GigabitEthernet0/0          // Red interna sede central
ipv6 route 2001::A00/119 GigabitEthernet0/0    // DMZ
```

La configuración de los routers internos (Router3 y Router4) serán distintas. No tendrán habilitado el protocolo OSPFv3 por motivos de seguridad. Además se utilizarán como servidores de DHCPv6 para sus redes internas. La configuración especifica de los routers será según sigue:

Router3:

```
ipv6 dhcp pool D1                    // Se define el proceso DHCPv6
 prefix-delegation pool client       // Se define el rango de prefijos de DHCPv6 en el
objeto client
 dns-server 2001::801          // Se define la dirección del servidor DNS
 domain-name D1.com            // Se le da un nombre de dominio al proceso
!
ipv6 local pool client 2001::802/119 119          // Rango de direcciones que utilizará DHCPv6
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001::C08/127          // Dirección asignada del Link 5 punto a punto
```

ipv6 enable // Habilitamos IPv6 en la interfaz

!

interface GigabitEthernet0/1

no ip address

ipv6 address 2001::800/119 // Dirección asignada de la red de la delegación

ipv6 enable // Habilitamos IPv6 en la interfaz

ipv6 dhcp server D1 // Definimos la interfaz como servidor DHCPv6

!

ipv6 route ::/0 GigabitEthernet0/0 // Se define la ruta por defecto en la interfaz del Firewall

Router4:

ipv6 dhcp pool D2 // Se define el proceso DHCPv6

prefix-delegation pool client // Se define el rango de prefijos de DHCPv6 en el objeto client

dns-server 2001::1 // Se define la dirección del servidor DNS

domain-name D2.com // Se le da un nombre de dominio al proceso

!

ipv6 local pool client 2001::2/117 117 // Rango de direcciones que utilizará DHCPv6

!

interface GigabitEthernet0/0

no ip address

ipv6 address 2001::C0A/127 // Dirección asignada del Link 5 punto a punto

ipv6 enable // Habilitamos IPv6 en la interfaz

!

interface GigabitEthernet0/1

no ip address

ipv6 address 2001::/117 // Dirección asignada de la red de la sede central

ipv6 enable // Habilitamos IPv6 en la interfaz

ipv6 dhcp server D2 // Definimos la interfaz como servidor DHCPv6

!

ipv6 route ::/0 GigabitEthernet0/0 // Se define la ruta por defecto en la interfaz del Firewall

Con esto queda definida la configuración en todos los routers necesarios para la construcción de la red corporativa. Con la configuración realizada hemos asegurado las comunicación entre las

dos sedes y además hemos habilitado internamente en cada sede la asignación dinámica de direcciones.

7.6 Configuración Firewalls

Para explicar las configuraciones realizadas en los dos Firewall dividiremos las explicaciones en 3 partes: configuración general de los Firewall, configuración de la DMZ y configuración del túnel VPN.

1) Para empezar describiremos la configuración general, para aclarar los equipos y los puertos a los que nos referiremos, incluyo la siguiente imagen:

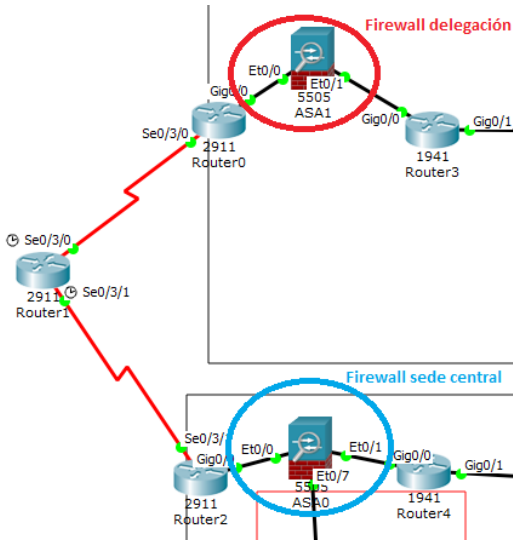


Figura 36. Firewalls de la red.

ASA0:

interface Ethernet0/0
switchport access vlan 2 // Asignamos el puerto E0/0 a la VLAN 2 (outside)
!
interface Ethernet0/1 // Puerto asignado a VLAN por defecto (VLAN 1 o inside)
!
interface Vlan1 // Definimos la interfaz VLAN 1
nameif inside // Nombre de la VLAN 1 = inside
security-level 100 // Le asignamos el nivel máximo de seguridad (100)
ip address 192.168.1.1 255.255.255.0 // Asignada por problemas de configuración
ipv6 address 2001::C0B/127 // Dirección asignada del Link 6 punto a punto

```
interface Vlan2                    // Definimos la interfaz VLAN 2
 nameif outside                    // Nombre de la VLAN 2 = outside
 security-level 0                  // Le asignamos el nivel mínimo de seguridad (0)
 ip address 192.168.3.0 255.255.255.0  //  Asignada por problemas de configuración
 ipv6 address 2001::C02/127        // Dirección asignada del Link 2 punto a punto
!
ipv6 route outside ::/0 2001::C03  // Ruta estática: default gateway
ipv6 route inside 2001::/117 2001::C0A // Ruta estática: red interna
ipv6 route outside 2001::800/119 2001::C00  // Ruta estática: red sede B
!
class-map INSPECCION               // Definimos la clase que mapeará la política
 match any
!
policy-map POLITICA                // Definimos la política a aplicar en el Firewall
 class INSPECCION                  // Insertamos la clase en la política
  inspect icmp                     // Definimos que paquetes se inspeccionarán (ICMP)
!
service-policy POLITICA global     // Aplicamos la política definida a todo el Firewall
```

ASA1:

```
interface Ethernet0/0
 switchport access vlan 2          // Asignamos el puerto E0/0 a la VLAN 2 (outside)
!
interface Ethernet0/1              // Puerto asignado a VLAN por defecto (VLAN 1 o
inside)
!
interface Vlan1                    // Definimos la interfaz VLAN 1
 nameif inside                     // Nombre de la VLAN 1 = inside
 security-level 100                // Le asignamos el nivel máximo de seguridad (100)
 ip address 192.168.1.1 255.255.255.0  //  Asignada por problemas de configuración
 ipv6 address 2001::C09/127        // Dirección asignada del Link 5 punto a punto
!
interface Vlan2                    // Definimos la interfaz VLAN 2
 nameif outside                    // Nombre de la VLAN 2 = outside
 security-level 0                  // Le asignamos el nivel mínimo de seguridad (0)
```

```
 ip address 192.168.5.0 255.255.255.0  //  Asignada por problemas de configuración
 ipv6 address 2001::C00/127            // Dirección asignada del Link 1 punto a punto
!
ipv6 route outside ::/0 2001::C01      // Ruta estática: default gateway
ipv6 route inside 2001::800/119 2001::C08          // Ruta estática: red interna
ipv6 route outside 2001::/117 2001::C02            // Ruta estática: red sede A
!
class-map INSPECCION                   // Definimos la clase que mapeará la política
 match any
!
policy-map POLITICA          // Definimos la política a aplicar en el Firewall
 class INSPECCION                      // Insertamos la clase en la política
  inspect icmp                         // Definimos que paquetes se inspeccionarán (ICMP)
!
service-policy POLITICA global         // Aplicamos la política definida a todo el Firewall
```

Con esto hemos finalizado la configuración general de los dos ASA.

2) Continuaremos con la definición de la DMZ en el ASA0, que será el único con esta zona, dado que con una única zona accesible desde el exterior es suficiente para el objetivo de la DMZ (visibilidad de la empresa).

ASA0:

```
interface Ethernet0/7            // El puerto E0/7 es el único conectado a esta zona
 switchport access vlan 3        // Asignamos el puerto a la VLAN 3 (dmz)
!
interface Vlan3          // Definimos la VLAN 3
 no forward interface Vlan1      // Asilamos la retransmisión entre la DMZ y la red interna
 nameif dmz                      // Nombre de la VLAN 3 = dmz
 security-level 0          // Le asignamos el nivel mínimo de seguridad (0)
 ip address 192.168.2.0 255.255.255.0  //  Asignada por problemas de configuración
 ipv6 address 2001::A00/119      // Dirección asignada de la red de la DMZ
```

Con esta simple configuración conseguimos una zona asilada, solo accesible a través del ASA0. En caso de restringir las políticas de seguridad se podrán implementar políticas más estrictas para la DMZ configurando el firewall.

Para nuestro caso, que desde la DMZ no se pueda acceder a ningún equipo de la red interna, pero que desde la red interna y desde el exterior esta zona sea accesible, con esta configuración es suficiente para cumplir con las especificaciones.

3) Finalizaremos la configuración de la VPN los firewall. Esto, como se ha explicado anteriormente, se realizará en tres pasos: definición ACLs, definición del túnel y creación del túnel.

ASA0:

ipv6 access-list SedeA permit icmp 2001::/117 2001::800/119

ipv6 access-list SedeA permit udp 2001::/117 lt 65535 2001::800/119 lt 65535

ipv6 access-list SedeA permit icmp6 2001::/117 2001::800/119

ipv6 access-list SedeA permit tcp 2001::/117 lt 65535 2001::800/119 lt 65535

// En esta ACL permitimos todo el tráfico generado desde la red interna (2001::/117) a la red externa // (2001::800/119), tanto ICMP, TCP como UDP.

crypto ikev1 enable outside // Habilitamos IKEv1 en la interfaz exterior

crypto ikev1 policy 10 // Definimos la politica a aplicar por IKEv1

encr aes // Encriptación: AES

authentication pre-share // Autentificación: pre-shared key

group 2 // Asignamos al grupo 2

crypto ipsec ikev1 transform-set cisco esp-aes esp-sha-hmac

// Con el anterior comando definimos el conjunto de transformación “cisco” que utilizará ESP-AES

// y ESP-SHA-HMAC

crypto map IPv6-L2L 1 match address SedeA // Definimos la ACL del túnel

crypto map IPv6-L2L 1 set peer 2001::C00 // Definimos el peer del túnel

crypto map IPv6-L2L 1 set ikev1 transform-set cisco // Asignamos el conjunto “cisco” al túnel

crypto map IPv6-L2L interface outside // Definimos en que interfaz se construirá el túnel

!

tunnel-group 2001::C00 type ipsec-l2l // Creamos el túnel contra el peer de tipo LAN to LAN

tunnel-group 2001::C00 ipsec-attributes // Definimos los atributos necesario del túnel

ikev1 pre-shared-key cisco123 // Definimos la pre-shared key “cisco123”

ASA1:

ipv6 access-list SedeB permit icmp 2001::800/119 2001::/117

ipv6 access-list SedeB permit udp 2001::800/119 lt 65535 2001::/117 lt 65535

ipv6 access-list SedeB permit icmp6 2001::800/119 2001::/117

ipv6 access-list SedeB permit tcp 2001::800/119 lt 65535 2001::/117 lt 65535

!

crypto ikev1 enable outside // Habilitamos IKEv1 en la interfaz exterior

crypto ikev1 policy 10 // Definimos la política a aplicar por IKEv1

encr aes // Encriptación: AES

authentication pre-share // Autentificación: pre-shared key

group 2 // Asignamos al grupo 2

crypto ipsec ikev1 transform-set cisco esp-aes esp-sha-hmac

// Con el anterior comando definimos el conjunto de transformación "cisco" que utilizará ESP-AES

// y ESP-SHA-HMAC

crypto map IPv6-L2L 1 match address SedeB // Definimos la ACL del túnel

crypto map IPv6-L2L 1 set peer 2001::C02 // Definimos el peer del túnel

crypto map IPv6-L2L 1 set ikev1 transform-set cisco // Asignamos el conjunto "cisco" al túnel

crypto map IPv6-L2L interface outside // Definimos en que interfaz se construirá el túnel

!

tunnel-group 2001::C02 type ipsec-l2l // Creamos el túnel contra el peer de tipo LAN to LAN

tunnel-group 2001::C02 ipsec-attributes // Definimos los atributos necesario del túnel

ikev1 pre-shared-key cisco123 // Definimos la pre-shared key "cisco123"

Con esto hemos finalizado tanto la configuración general de los firewall, de la DMZ y el tunel LAN to LAN entre los firewall.

7.7 Servidores DNS y HTTP

Como parte de las condiciones de diseño se ha conectado servidores HTTP en las dos sedes y en la DMZ. Los servidores de las redes internas además realizan la función de servidores DNS. Para ello se les ha puesto una dirección IPv6 estática (la cual se ha configurado en los servidores DHCPv6 para que sea entregada a los hosts).

La configuración del servidor en la sede central es según sigue en las siguientes imágenes:

HTTP:

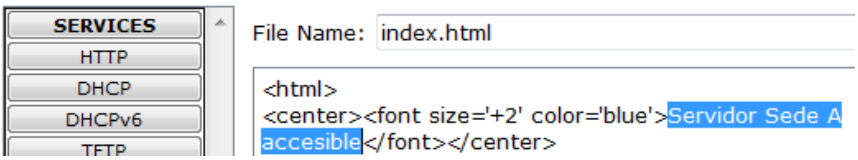


Figura 37. Configuración servidor sede central HTTP 1.

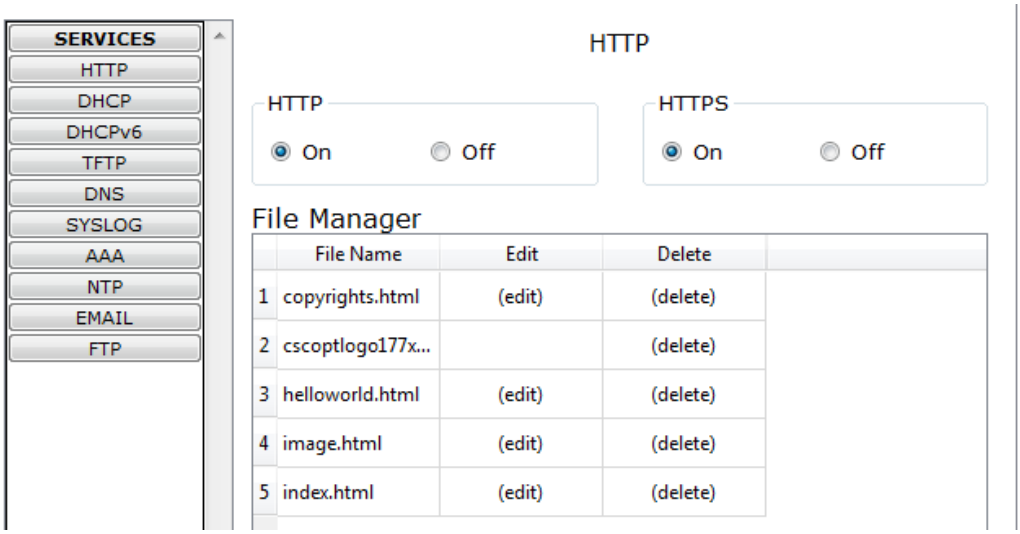


Figura 38. Configuración servidor sede central HTTP 2.

DNS:

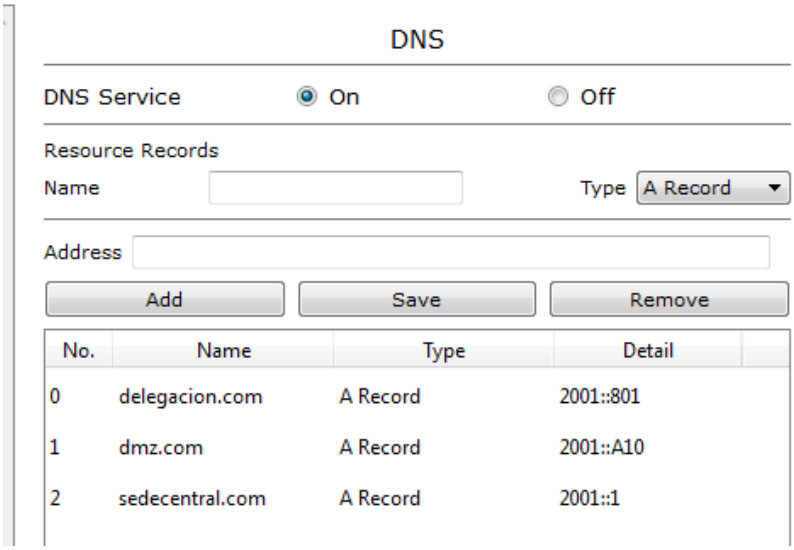


Figura 39. Configuración servidor sede central DNS.

IPv6 estática:

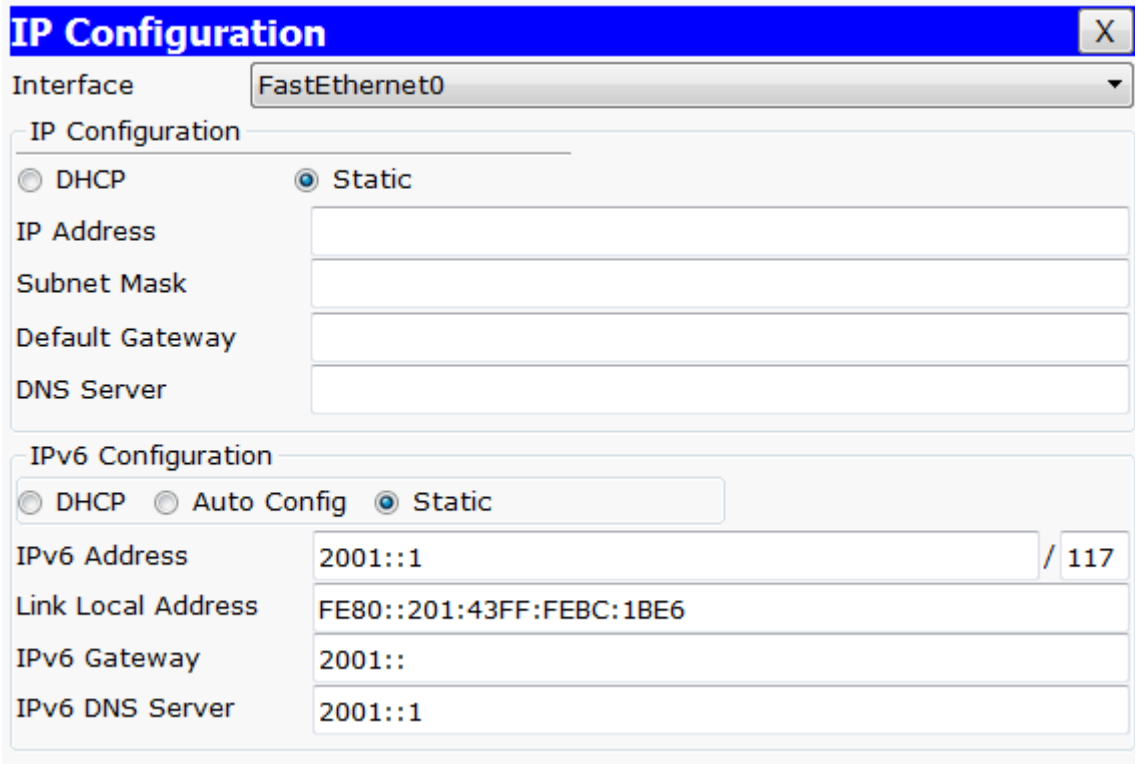


Figura 39. Configuración servidor sede central IPv6 estática.

Mientras que el servidor de la delegación será idéntica la configuración exceptuando las siguientes modificaciones:

HTTP:

Figura 40. Configuración servidor delegación HTTP.

IPv6 estática:

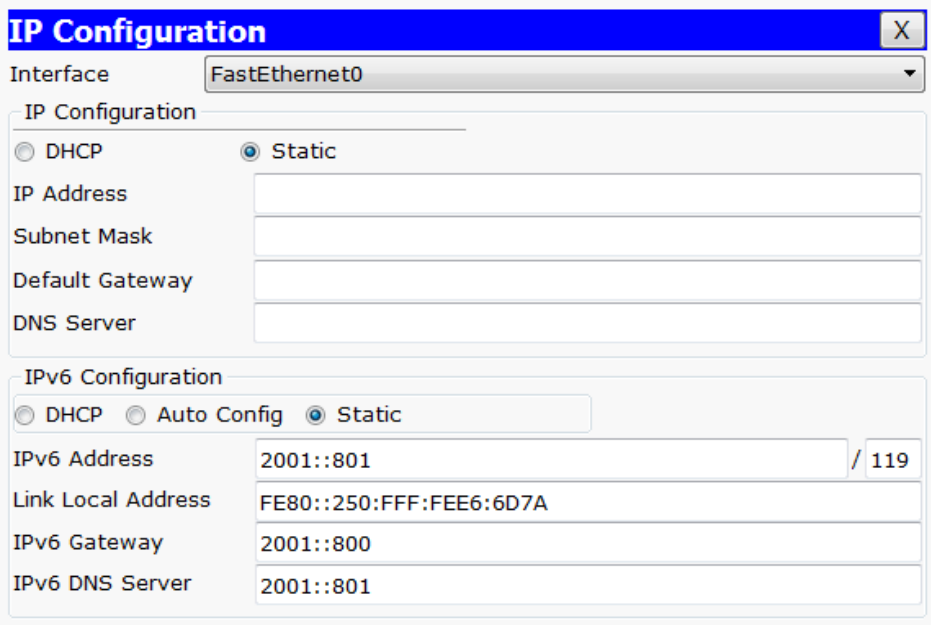


Figura 41. Configuración servidor sede central IPv6 estática.

Y por último la configuración del servidor de la DMZ (solo HTTP) sera así:

HTTP:

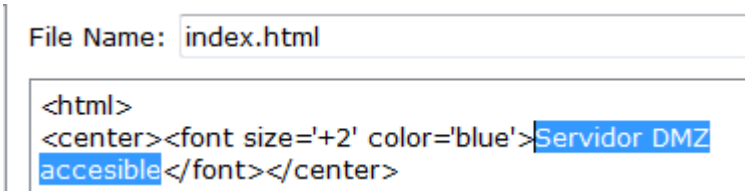


Figura 42. Configuración servidor DMZ HTTP.

IPv6 estática:

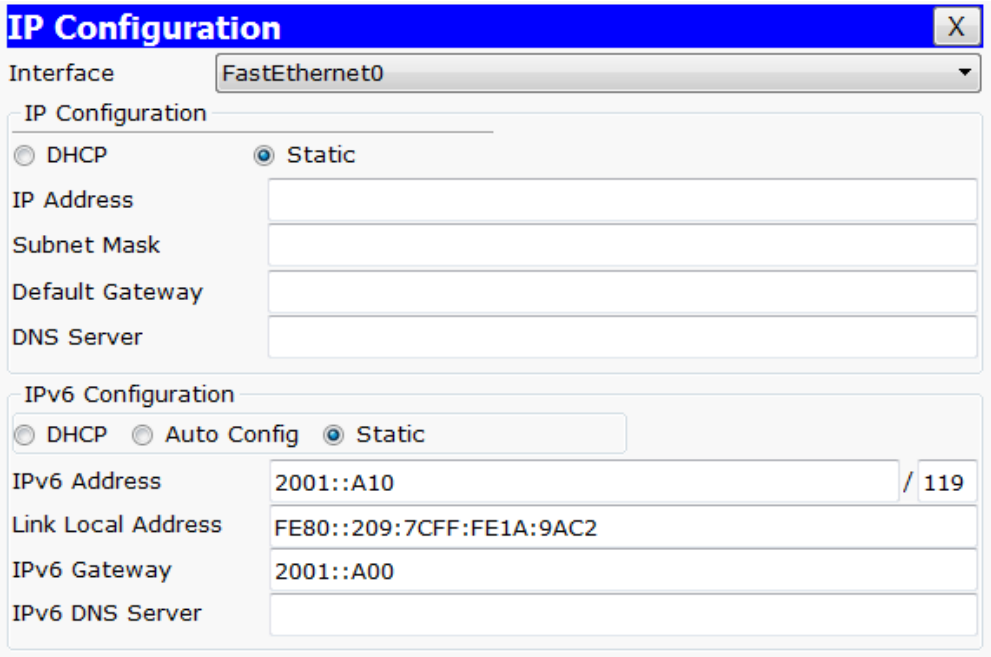


Figura 43. Configuración servidor DMZ IPv6 estática.

7.8 Comprobación de la configuración realizadas

A modo de comprobación de las configuraciones realizadas se conectará un PC a red de la sede central y se realizarán pruebas de asignación de dirección dinamica, conectividad con los servidores y acceso web a los serividores. Después se hará lo mismo desde la delegación. Por último se comprobará que desde el servidor de la DMZ no tenemos visibilidad sobre la red interna.

Sede central:

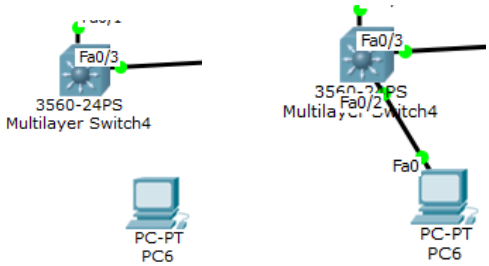


Figura 44. Conexión PC a sede central.

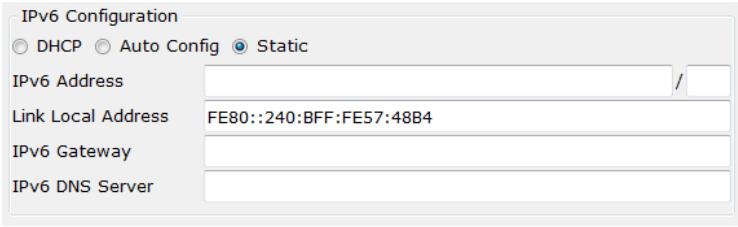


Figura 45. IPv6 desconfigurada.

Al activar DHCP en la configuración se asignará automáticamente la dirección al host:

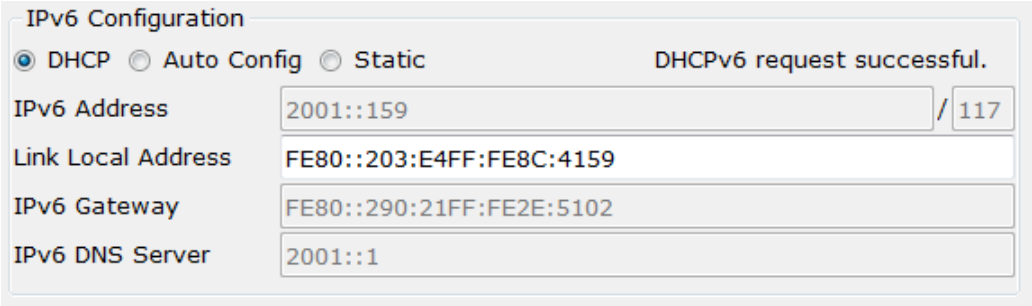


Figura 46. Autoconfiguración con DHCPv6.

Probando la conexión a los servidores:

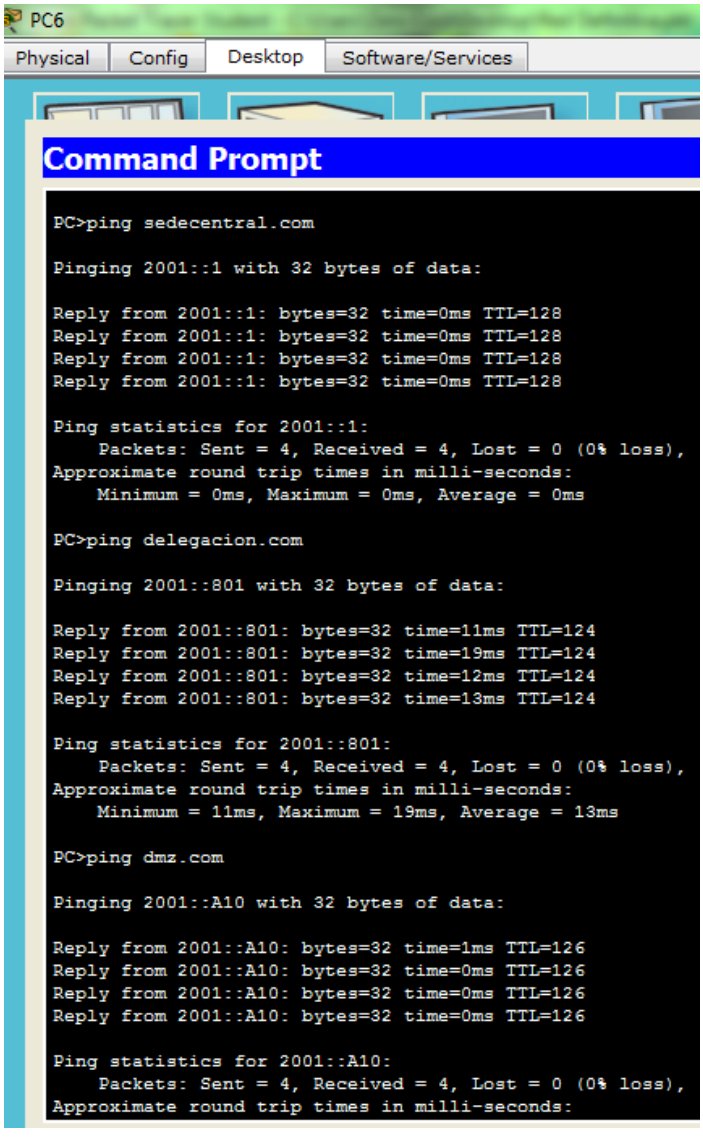


Figura 47. Conectividad ICMP desde sede central.

Figura 48. Prueba acceso sede central.

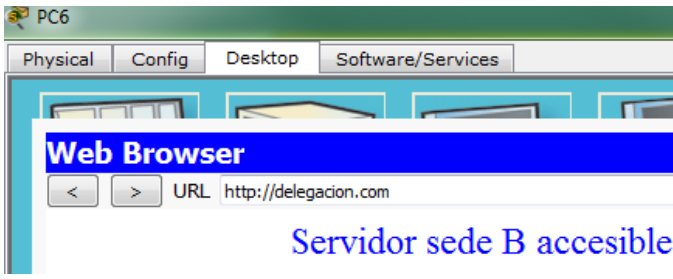


Figura 49. Prueba acceso delegación.

Figura 50. Prueba acceso DMZ.

Con esto hemos comprobado que un PC conectado a la red de la sede central se configura automáticamente gracias a DHCPv6 y ademas es capaz de acceder tanto a los servidores de su propia sede, como de la delegación y la DMZ.

Delegación:

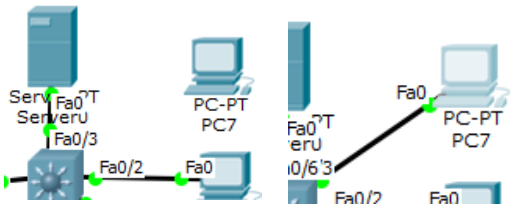


Figura 51. Conexión PC a delegación.

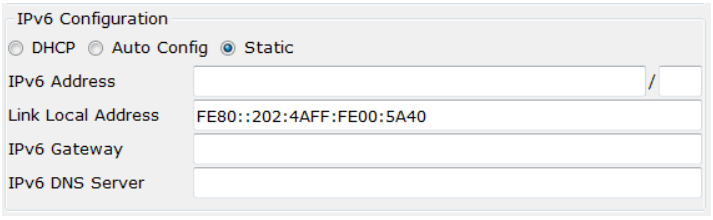


Figura 52. IPv6 desconfigurada.

Al activar DHCP en la configuración se asignará automáticamente la dirección al host:

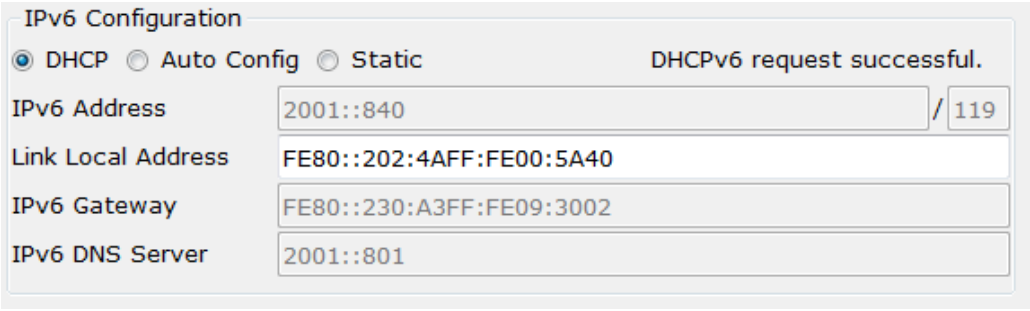


Figura 53. Configuración servidor DMZ HTTP.

Probando la conexión a los servidores:

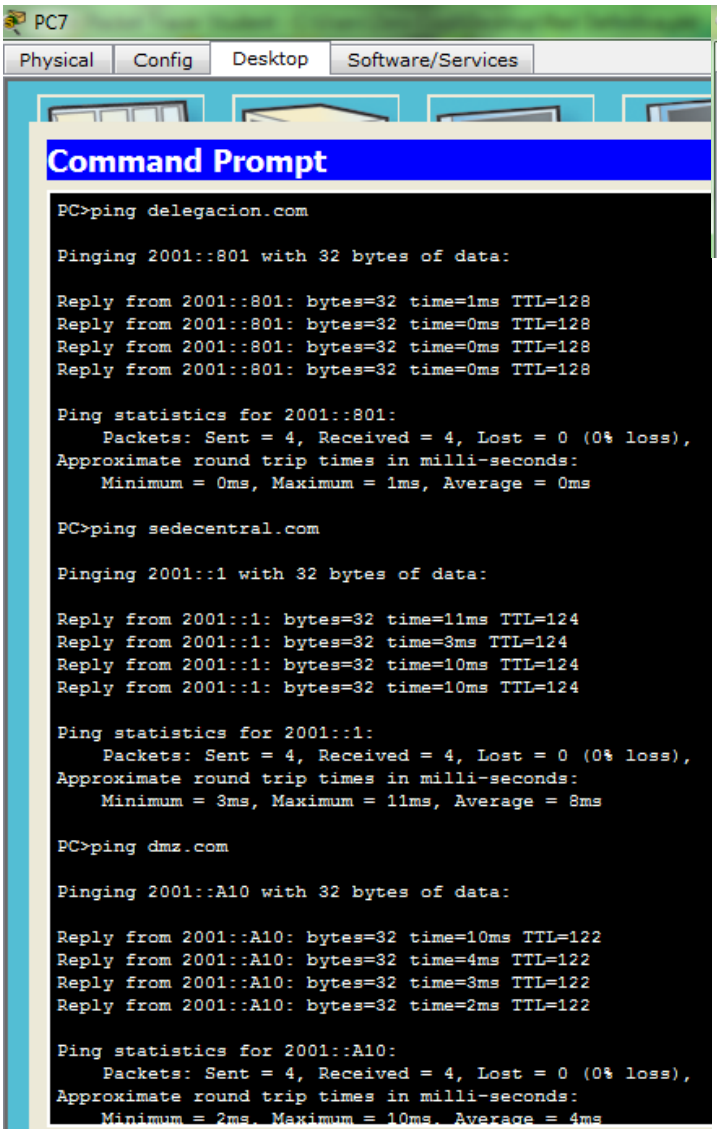


Figura 54. Conectivitat ICMP desde delegación.

Figura 55. Prueba acceso delegación.

Figura 56. Prueba acceso sede central.

Figura 57. Prueba acceso DMZ.

Con esto hemos comprobado que un PC conectado a la red de la delegación se configura automáticamente gracias a DHCPv6 y ademas es capaz de acceder tanto a los servidores de su propia sede, como de la sede central y la DMZ.

DMZ:

En cambio desde la DMZ no se debe poder acceder a la red interna de ninguna de las dos sedes. Como ejemplo realizaremos pings y accesos web a los servidores:

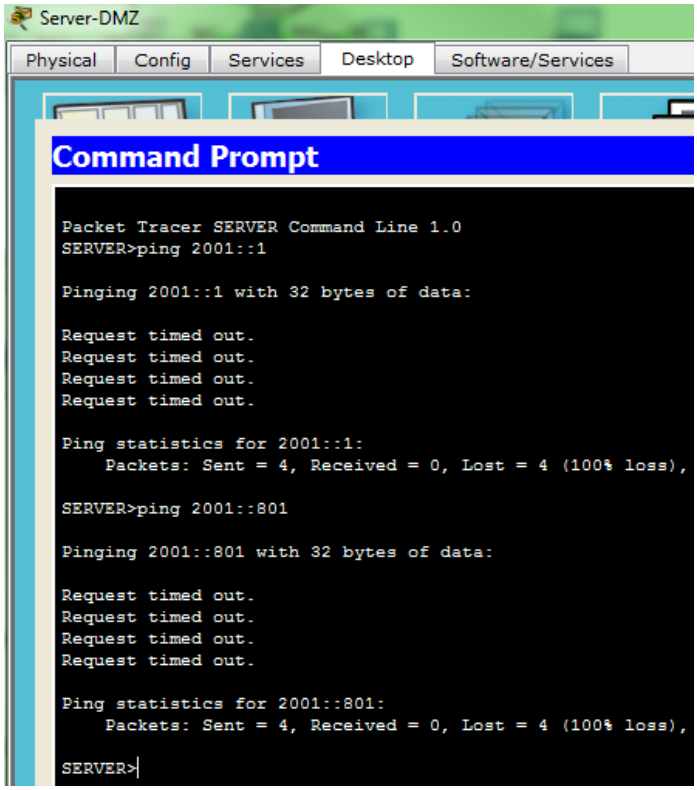


Figura 58. Conectividad ICMP desde DMZ.

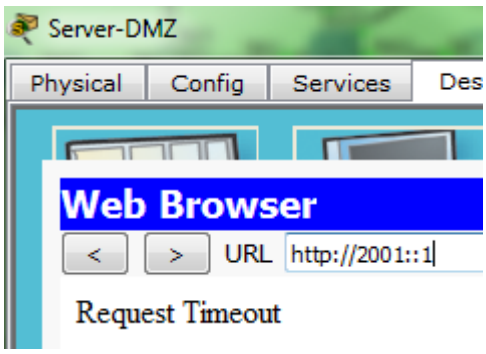


Figura 59. Prueba acceso sede central.

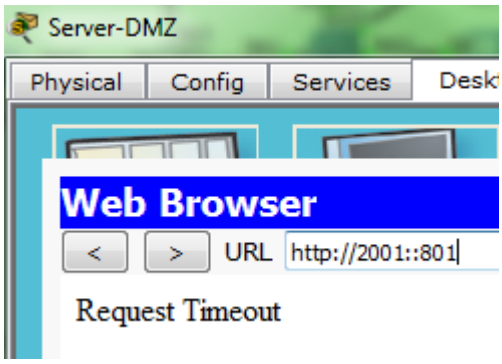


Figura 60. Prueba acceso delegación.

Con estas sencillas pruebas vemos que nuestra red interna esta protegida de cualquier acceso exterior.

Por lo tanto con estas pruebas hemos comprobado que se cumple con las condiciones de diseño planteadas en todos los casos.

Capítulo 8.
Conclusiones y propuesta de trabajo futuro

Como conclusión del proyecto podemos asumir que es completamente realizable el diseño, implementación y puesta en servicio de una red corporativa utilizando exclusivamente IPv6.

Para ello hemos realizado satisfactoriamente el direccionamiento de una red ante unas condiciones de diseño (escalable pensando en posibles ampliaciones), hemos utilizado los protocolo de routing específicos de IPv6 permitiendo la conectividad de distintas subredes, hemos implementado una política de seguridad y una conexión segura entre sedes, hemos hecho uso de los protocolos de aplicación sobre IPv6 y hemos permitido la movilidad de los usuarios habilitando puntos de acceso WiFi en ambas subsedes.

Como propuesta de trabajo futuro, al ser un campo cuya implantación no está extendida existen múltiples lineas de trabajo. Entre ellas hacer un estudio de calidades de servicio sobre IPv6 para videollamada o VoIP, estudiar su aumento de eficiencia con respecto a IPv4 o implantar redes híbridas para el uso de ambos protocolos sobre la misma red.

El siguiente paso es la implantación de IPv6 a nivel global, pues todavía tanto a nivel de redes como los mismos ISP se resisten a asumir su uso. Como todo, será cuestión de tiempo que este protocolo asuma fuerza en el mercado y se deje de utilizar IPv4.

Conclusions i proposta de treball futur

Com a conclusió del projecte podem assumir que és completament realitzable el disseny, implementació i posada en servei d'una xarxa corporativa utilitzant exclusivament IPv6.

Per això hem realitzat satisfactòriament l'adreçament d'una xarxa davant unes condicions de disseny (escalable pensant en possibles ampliacions), hem utilitzat els protocol de routing específics d'IPv6 permetent la connectivitat de diferents subxarxes, hem implementat una política de seguretat i una connexió segura entre seus, hem fet ús dels protocols d'aplicació sobre IPv6 i hem permès la mobilitat dels usuaris habilitant punts d'accés WiFi en totes dues subseus.

Com a proposta de treball futur, en ser un camp on la implantació no està estesa hi ha múltiples línies de treball. Entre elles fer un estudi de qualitats de servei sobre IPv6 per videotrucada o VoIP, estudiar el seu augment d'eficiència en comparació a IPv4 o implantar xarxes híbrides per a l'ús de tots dos protocols sobre la mateixa xarxa.

El següent pas és la implantació d'IPv6 a nivell global, ja que encara tant a nivell de xarxes com els mateixos ISP es resisteixen a assumir el seu ús. Com tot, serà qüestió de temps que aquest protocol assumeixi força en el mercat i es deixi d'utilitzar IPv4.

Conclusions and future work proposal

As conclusion of the project we can assume it is fully achievable design, implementation and commissioning of a corporate network using only IPv6.

So we've successfully completed the addressing of a network with design conditions (scalable considering possible extensions), we used the protocols routing of IPv6 allowing connectivity of different subnets, we have implemented a security policy and a secure connection between headquarters, we have made use of application protocols IPv6 and have allowed the mobility of users enabling WiFi access points in both subsites.

As a propose of future work, being a field whose implementation is not widespread there are multiple lines of work. Including a study of quality of service over IPv6 for video or VoIP, study their increased efficiency with respect to IPv4 or deploy hybrid networks to use both protocols on the same network.

The next step is the implementation of IPv6 globally, because the ISP resist to assume use. Like everything else, a matter of time that this protocol gets market strength and stop using IPv4.

Capítulo 9. Bibliografía

[1] Cisco Systems Inc, “Unicast Routing Configuration Guide, Cisco DCNM for LAN, Release 5.x”

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/dcnm/unicast/configuration/guide/l3-dcnm-book/l3_ipv6.html. [Online].

[2] Charles M. Kozierok, “The TCP/IP guide” http://www.tcpipguide.com/free/t_RIPngRIPv6MessageFormatandFeatures-2.htm. [Online].

[3] Cisco Systems Inc, “IP Routing: RIP Configuration Guide, Cisco IOS Release 15S”

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_rip/configuration/15-s/irr-15-s-book/ip6-rip.html. [Online].

[4] Cisco Systems Inc, “Cisco Nexus 5600 Series NX-OS Unicast Routing Configuration Guide, Release 7.x” http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/unicast/7x/unicast_n5600_config/l3_ospfv3.html. [Online].

[5] Wikipedia, “IS-IS” https://es.wikipedia.org/wiki/IS-IS. [Online].

[6] Cisco Systems Inc, “IP Routing: ISIS Configuration Guide, Cisco IOS XE Release 3S” http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/xe-3s/irs-xe-3s-book/ip6-route-isis-xe.html. [Online].

[7] Cisco Systems Inc, “DHCPv6 Based IPv6 Access Services” http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html. [Online].

pag 40

[8] Cisco Systems Inc, “Cisco Firewalls and Network Security” http://ciscofirewalls.weebly.com/create-a-lan-to-lan-vpn-tunnel-on-cisco-asa-with-ipv6.html. [Online].