_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Diseño completo de una red de datos IPv6.

Rubén Olivares Herruzo.

Tutor: José Óscar 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 2013-14

Valencia, 24 de julio de 2014

Resumen

El proyecto propone el diseño y la configuración de una red empresarial genérica, flexible y modular basada en IPv6 que sirva para facilitar la implementación de esta tecnología, la cual está ya en proceso, en cualquier tipo de red independientemente del tamaño o localización geográfica.

En primer lugar, se estudiara el diseño topológico de la red, así como los componentes genéricos que serán utilizados y la interconexión entre estos. También se decidirá entre las diferentes tecnologías y protocolos disponibles en la actualidad y la distribución de los recursos disponibles y necesarios para cada una de las partes implicadas.

Finalmente, se procederá a configurar cada uno de los componentes de la forma más genérica y sencilla posible para el correcto funcionamiento de la red en su conjunto y se procederá a dejar registro de ellos para que con los mínimos cambios posibles su implementación sea sencilla en cualquier red funcional.

Resum

El projecte proposa el disseny i la configuració d'una xarxa empresarial genèrica , flexible i modular basada en IPv6 que serveix per facilitar la implementació d'aquesta tecnologia , la qual està ja en procés, en qualsevol tipus de xarxa independentment de la mida o localització geogràfica.

En primer lloc, s'estudia el disseny topològic de la xarxa, així com els components genèrics que seran utilitzats i la interconnexió entre aquests. També es decidirà entre les diferents tecnologies i protocols disponibles a l'actualitat i la distribució dels recursos disponibles i necessaris per a cadascuna de les parts implicades.

Finalment, es procedirà a configurar cadascun dels components de la forma més genèrica i senzilla possible per al correcte funcionament de la xarxa en el seu conjunt i es deixarà registre d'ells, per a què amb els mínims canvis possibles la seva implementació siga senzilla en qualsevol xarxa funcional.

Abstract

The project proposes the design and configuration of a generic, flexible and modular enterprise network based on IPv6 that facilitates the implementation of this technology, which is already underway, in any network regardless of size or geographic location.

First, the topological network design and generic components that will be used and the interconnection between them is considered. Decisions will also be made between different technologies and protocols available today and the distribution of resources available and required for each of the parties involved.

Finally each of the components will be configured the most generic and simple possible way for the proper functioning of the network as a whole and record of them will be left so as to get a simple implementation with minimal changes in any functional network.

Índice

Capítulo 1. Introducción al proyecto 3
1.1 Descripción del proyecto: 3
1.2 Objetivos 4
Capítulo 2. Tecnologías disponibles 7
2.1 Introducción a IPv6. 7
2.1.1 Necesidad de IPv6. 7
2.1.2 Características básicas 10
2.2 Introducción a las redes WAN. 11
2.3 VPN 12
2.3.1 GRE 13
2.3.2 Protocolo IPSec. 13
2.3.3 L2TP 15
2.4 VLAN 17
2.4.1 "Router-on-a-stick" 19
2.5 Protocolos de red disponibles. 20
2.5.1 RIPng 20
2.5.2 OSPFv3 21
2.5.3 EIGRP 25
2.6 DHCPv6 26
2.6.1 Formato de mensajes DHCPv6 27
2.6.2 Tipos de configuración DHCPv6 30
2.7 Listas de acceso (ACL) 32
Capítulo 3. Diseño de una red genérica de datos IPv6 35
3.1 Planificación de la distribución 35
3.2 Direccionamiento IPv6 35
3.2.1 Sede central o grande: 36
3.2.2 Sede mediana: 36
3.2.3 Sede pequeña: 37
3.3 Diseño topológico de los tipos de redes. 37
3.3.1 Diseño topológico de sede central o grande. 38
3.3.2 Diseño topológico de sede Mediana 39
3.3.3 Diseño topológico de sede Pequeña 41
3.4 Configuración de OSPFv3 42
3.5 Configuración de DHCPv6 45

3.5.1 Sede central: DHCPv6 con memoria de estado. 45
3.5.2 Sede mediana: DHCPv6 sin memoria de estado. 48
3.5.3 Sede pequeña: SLAAC. 50
3.6 Configuración de VLAN en la Sede central. 51
3.6.1 Swich 51
3.6.2 Router (router-on-a-stich). 54
3.7 VPN 56
3.7.1 Conexión VPN mediante túnel IPSec. 56
3.7.2 Servidor VPN para uso remoto con L2TP. 60
3.8 Bibliografía 63

Capítulo 1. Introducción.

1.1 Descripción del proyecto:

El Protocolo de Internet (IP) se desarrolló en 1973. Este permite el desarrollo y transporte de paquetes de datos, para esto, cada interfaz de la red necesita una dirección IP para poder ser contactado y contactar con el resto, en 1974 se desarrolló IPv4 el cual cuenta con 4 294 967 296 (232) direcciones de host diferentes de las cuales en 2010 quedaban menos del 10 % de IP sin asignar [1]. Debido a esto es necesario implementar el protocolo IPv6 el cual se desarrolló en 1996 para suplantar a este de forma paulatina el cual cuenta con exactamente 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones de host (2^128 o 340 sextillones). No contando solo con esta mejora sino también con otras diferentes para mejorar el proceso de los datos y su gestión.[7]

Este proyecto corresponde al diseño y configuración de una red corporativa genérica basada en IPv6, desarrollada en base a componentes cisco, la red ha de dar soporte a una gran variedad de empleados de diversas formas y en diferentes escalas y lugares, pudiendo aplicarse a empresas de diferentes tamaños y necesidades siendo el diseño escalable y genérico.

Esta red se apoyará en la infraestructura existente de los ISP`s que pueden encontrarse en el mercado de las telecomunicaciones.

Las sedes de la compañía tendrán un volumen de datos variable dependiendo de sus características, por lo que deberá crearse distintos tipos de redes diferentes para intercomunicarse, ofreciendo a las más grandes un ancho de banda mayor y más dedicado que a otras sedes más pequeñas donde las necesidades serán menores.

Parte del trabajo consistirá en hacer un estudio para determinar qué tecnología se adapta mejor a las necesidades individuales de cada oficina y qué equipamiento es necesario para llevarlo a cabo así como la configuración general de todos los elementos involucrados.

También, un aspecto importante a tener en cuenta es la seguridad ya que viajará información confidencial y sensible entre las diferentes oficinas.

Una vez finalizada la parte de estudio y diseñada de la red basada en IPv6 estaría disponible para su puesta en desarrollo donde las siguientes fases serían: petición de alta de

líneas y permiso del Ayuntamiento en caso de que sea necesario hacer obra para llegar a la sede, compra de equipos y materiales al proveedor y su posterior configuración.

1.2 Objetivos

El objetivo principal de este TFC es la creación, configuración e interconexión de las diferentes LAN de las sedes de una compañía utilizando el protocolo IPv6 así como la selección de los componentes implicados y diversos protocolos utilizados para su correcto funcionamiento.

Cada una de las sedes tendrá diseñada y configurada una red LAN propia que se conectará a la red WAN general y que dará servicio al número requerido de host requeridos de la forma más genérica y sencilla posible..

Cada una de las líneas pasará por la estructura de alguno de los ISPs nacionales que hay disponibles actualmente en el mercado dándole tanto acceso a internet como interconectándolas entre ellas.

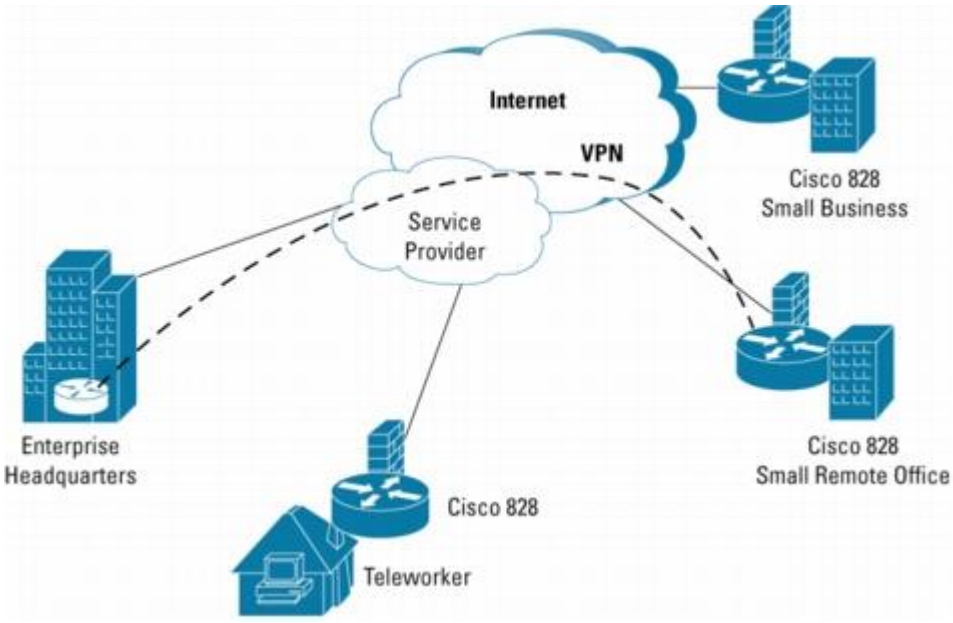

Ilustración 1. Ejemplo de interconexión de sedes a través de internet.

1.3 Distribución de tareas.

Este proyecto queda dividido en 3 fases: diseño de una red empresarial genérica y modular con la distribución de los distintos elementos que la componen, selección interconexión y montaje de los distintos elementos que componen la red y configuración de todos los elementos involucrados en la red.

1-Planificacion de la distribución.

Aquí queda comprendido el esquema inicial de la red a implementar así como la definición a grandes rasgos de todo lo que vamos a montar.

2-Documentacion.

Aquí queda comprendido todo lo necesario en lo que a crear una buena base teórica y bien fundamentada, además del estudio del manejo de las herramientas que se disponen para la elaboración del proyecto.

3-Direccionamiento IPv6.

En esta tarea se divide el rango de IP que ha sido asignado en las diferentes subredes necesarias para la red a crear.

4-Diseño topológico de las distintas redes.

A partir de todo lo anterior se selecciona los componentes de la red así como la distribución e interconexión óptima para que la red sea escalable, simple, modular y demás características quedando la estructura definida.

5-Configuracion OSPF.

Consta de la configuración del protocolo de encaminamiento de la red, el cual permitiría a los dispositivos conocer cuáles son sus cercanos y las rutas para comunicarse.

6-Configuracion DHCP.

Con la configuración de este protocolo cada dispositivo queda con su IP propia configurada.

7- Configuración VLAN.

Se crean y configuran las subredes o VLAN con las que trabaja la sede central proporcionándole cierto grado de seguridad y resto de características de las VLAN.

8-Configuracion VPN.

Se crean y configuran las VPN necesarias para la red, tanto interconexión de sus sedes como el servidor VPN de acceso remoto para los usuarios.

9-Conclusiones.

Fundamentar y argumentar los resultados obtenidos es la labor intrínseca en esta tarea, así como defender la configuración obtenida.

10- Redacción.

Preparar un documento que pueda ser presentado como un estudio riguroso y bien fundamentado en el que diseña, implementa y configura una red genérica, modular, flexible y escalable. Es el objetivo de esta última tarea del proyecto.

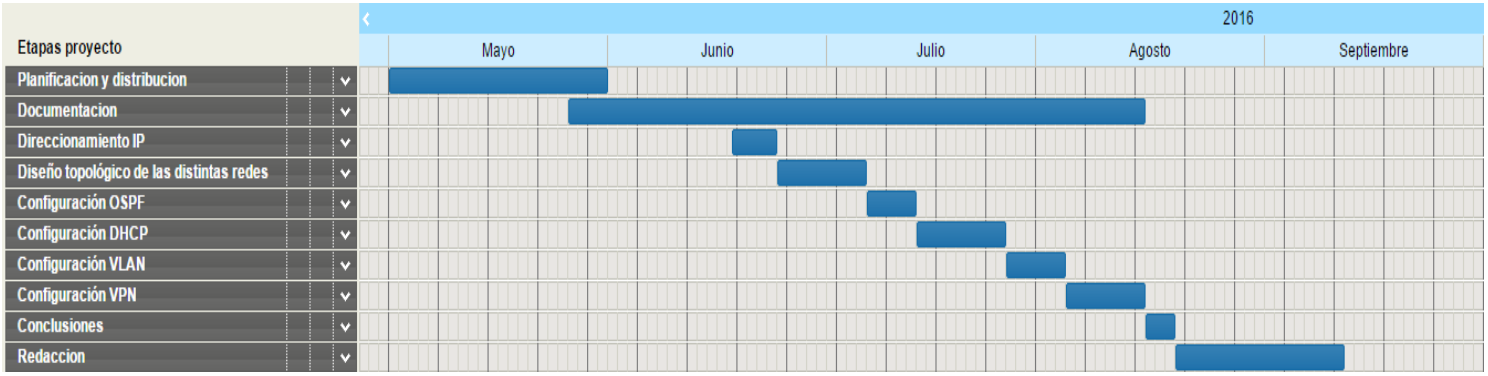

Ilustración 2: Diagrama de Grantt

Capítulo 2. Tecnologías disponibles.

2.1 Introducción a IPv6.

El Protocolo de Internet versión 6, en inglés: Internet Protocol version 6 (IPv6), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPv4) RFC 791.

2.1.1 Necesidad de IPv6.

El Protocolo de Internet versión 6, es una versión de IP, definida en el RFC 2460 y diseñada para reemplazar a Internet IPv 4 , RFC 791, el cual actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

IPv6 es el destinatario de sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso.

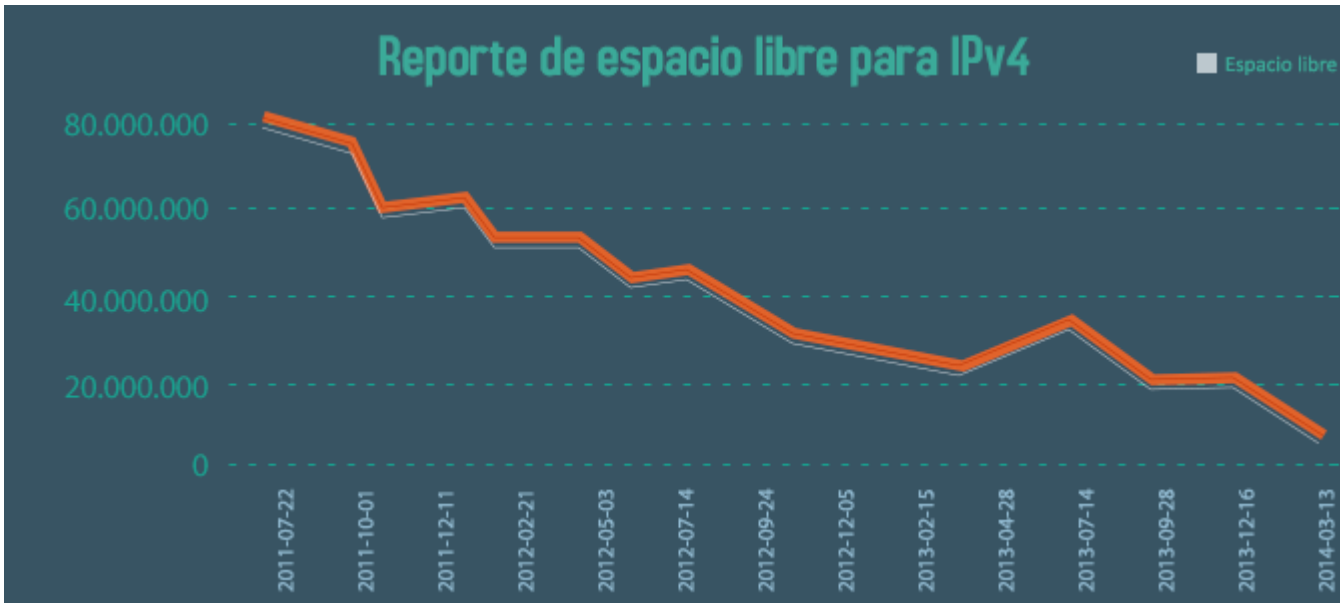

Ilustración 3: Espacio libre a través del tiempo de direcciones IPv4

A principios de 2010, quedaban menos del 10 % de IP sin asignar.1 En la semana del 3 de febrero de 2011, la IANA (Agencia Internacional de Asignación de Números de Internet) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IP`s en Asia.[7]

IPv4 posibilita 4 294 967 296 direcciones diferentes de host, un número demasiado pequeño para los dispositivos que necesitan ser direccionados. Por otro lado, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones de host diferentes.[7]

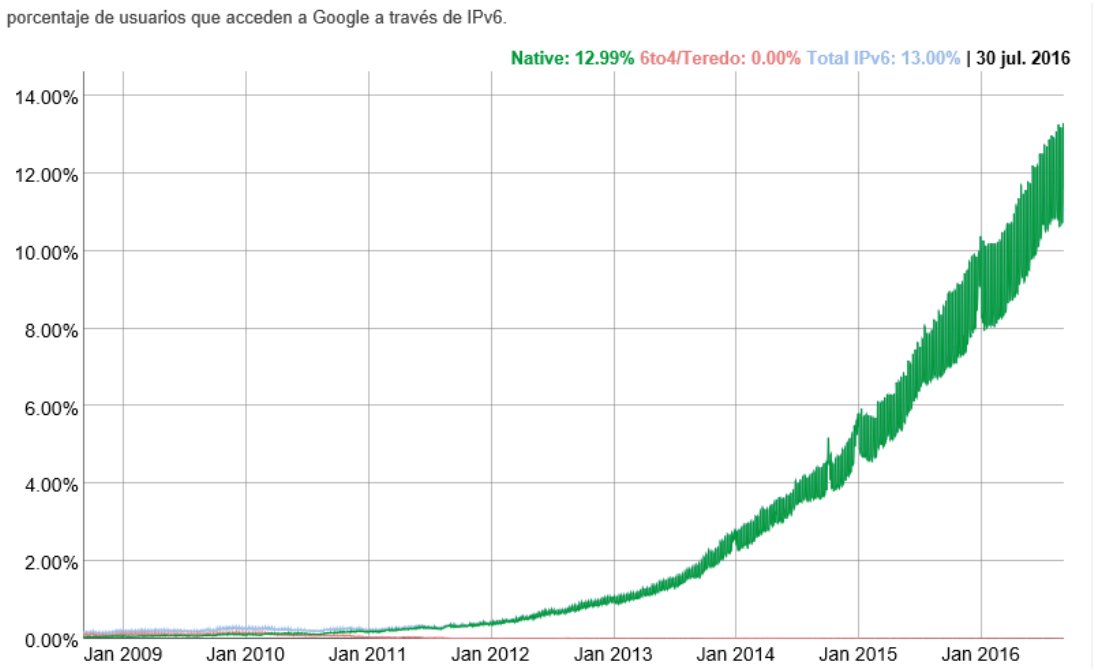

Ilustración 4: Porcentaje de usuarios que acceden a google a través de IPv6.

Debido a esto y puesto que IPv4 acabara por desaparecer en no demasiado tiempo es necesaria la actualización a IPv6 así como se recomienda en la creación de nuevas redes que estas utilicen el protocolo IPv6 y así evitar tener que actualizarlas. A parte de que desaparezca existen más razones para que IPv6 sea instalado como son:

-La posibilidad de que varias direcciones de red asignadas al mismo dispositivo. De esta manera se podrá estar conectado a varias redes a la vez lo que ofrece una gran flexibilidad todo ello desde el mismo dispositivo físico.

-Cifrado e IPSec integrados. IPv6 es un protocolo más seguro que su predecesor ya que de serie funciona cifrado, si se intercepta una comunicación, la información no podrá ser interpretada correctamente sin antes descifrarla.

-Multicast, la habilidad de enviar un paquete único a destinatarios múltiples es parte de la especificación base de IPv6 lo que simplifica mucho el broadcast así como la trasmisión de contenidos multiusuario como televisión vía IP.

-IPv6 permite el uso de jumbogramas, paquetes de datos de gran tamaño (hasta 64 bits).

-IPv6 incluye en su estándar el mecanismo “plug and play”, lo cual facilita a los usuarios estándar la conexión de a la red. La configuración puede ser realizada automáticamente. Esto permite que al conectar una máquina a una red IPv6, le sea asignada automáticamente una dirección IPv6.

-IPv6 incluye mecanismos de movilidad más eficientes y robustos.

-Al incorporar IPv6 una gran cantidad de direcciones, no será necesario utilizar NAT lo que simplificara todo el proceso de direccionamiento y creación de redes.

-Se hicieron varias simplificaciones en la cabecera de los paquetes, así como en el proceso de reenvío de paquetes para hacer el procesamiento de estos más simple y por ello más eficiente.[3]

Como podemos ver en el la siguiente figura en España se tiene aún más necesidad de implementar las redes IPv6 puesto que está muy por detrás de la media europea y la del resto de países desarrollados y esto solo supone más problemas en un futuro por la inadaptación de las redes, para las cuales las nuevas tecnologías se diseñan y llegara el punto en el que no sean compatibles con IPv4.

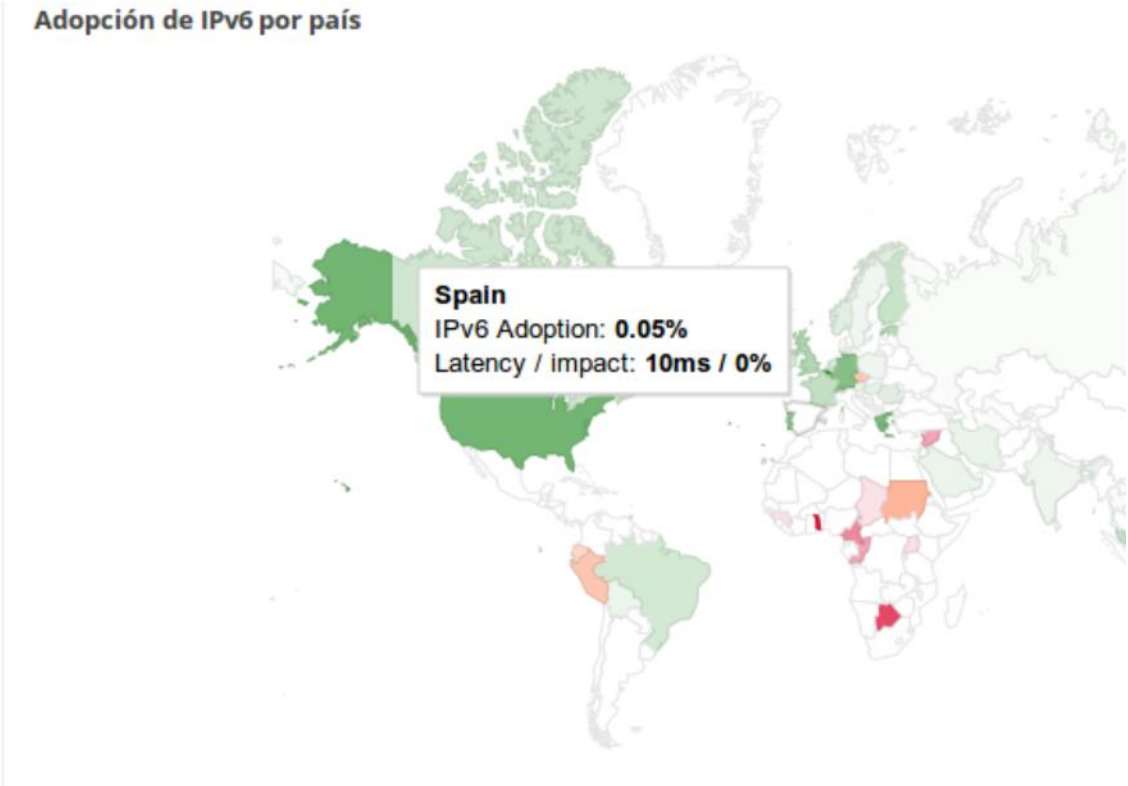

Ilustración 5: Adopción de IPv6 en España

2.1.2 Características básicas

Tipos de direcciones IPv6

Se clasifican en 3 categorías:

1) Direcciones unicast: es el identificador de un solo interfaz.

2) Direcciones multicast: es el identificador para un grupo de interfaces, que pueden ser incluso de diferentes nodos.

3) Dirección Anycast: el identificador para un set de interfaces que pueden pertenecer a diferentes nodos, a diferencia de multicast, los paquetes a esta dirección no se entregaran a todo el grupo sino a uno solo de sus integrantes.

Notación:

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales.

Si uno o más de dos grupos consecutivos son nulos, pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión solamente se permite en uno de ellos.

Direcciones especiales en IPv6

::/96 The zero prefix denota direcciones compatibles con IPv4

::/128 una dirección con todo ceros, dirección indefinida, usada para software.

::1/128 loop back address o dirección para local host.

2001:db8::/32 para documentación sobre IPv6.

fec0::/10 Prefijo para direcciones con solo acceso local.

fc00::/7 Unique Local Address (ULA

ff00::/8 multicast addresses. Todas las direcciones con este prefijo son multicast.

fe80::/10 link-local prefix. La dirección solo es válida en el link local físico.

En cuanto a mejoras con respecto a IPv4 se implementa de serie:

-Multicast, la habilidad de enviar un paquete único a destinos múltiples mediante grupos multicast.

-Seguridad: Internet Protocol Security (IPSec), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6.

-Simplicidad de procesado en routers: Se hicieron varias simplificaciones en la cabecera de los paquetes, así como en el proceso de reenvío de paquetes.

2.2 Introducción a las redes WAN.

Una WAN define la forma en que los datos se desplazan a través de una zona geográficamente extensa. Las WAN interconectan diferentes LAN's utilizando los servicios de un proveedor. Las tecnologías de señalización y transporte que utilizan estos proveedores de servicios suelen ser transparentes para los usuarios finales.

Dentro de la nube WAN se dan tres tipos de conexiones:

- Líneas alquiladas: también se llaman líneas punto a punto o líneas dedicadas. Ofrecen una comunicación por un medio exclusivo para el cliente. Estas líneas eliminan los problemas de conexión/desconexión de llamada y aportan mayor privacidad y seguridad. Suelen emplearse en conexiones serie síncronas manteniendo constante la utilización del ancho de banda. Son las líneas más costosas económicamente hablando.

-Circuitos conmutados: sólo se establece comunicación entre el emisor y el receptor durante el tiempo que dura la transmisión y las sucesivas conexiones pueden o no utilizar la misma ruta u otra diferente. Este tipo de conexiones suele emplearse para entornos que tengan un uso esporádico, enlaces de respaldo o enlaces bajo demanda. También es posible aprovecharse de los servicios de telefonía básicos mediante una conexión asíncrona conectada a un módem, como por ejemplo una línea RDSI.

-Paquetes conmutados: es un método de conmutación donde los dispositivos comparten un único enlace punto-a-punto o punto-multipunto para transportar paquetes desde un origen hacia un destino a través de una red portadora. Este tipo de redes utilizan circuitos virtuales para ofrecer conectividad de forma permanente o conmutada (PVC o SVC)

2.3 VPN

Una VPN (Red Privada Virtual) es utilizada principalmente para conectar dos redes privadas a través de una red pública de datos mediante túneles encriptados. Un túnel es un método para encapsular un protocolo en otro donde se aprovecha esta característica, principalmente cuando hay protocolos no enrutables y hacen que el uso de una VPN sea imprescindible para enviar tráfico.

Las organizaciones utilizan las redes privadas virtuales o VPN para crear una conexión de red privada de extremo a extremo a través de redes de otras empresas como a través de internet por ejemplo. El túnel elimina la barrera de distancia y permite a los usuarios remotos acceder a los recursos de red disponibles en el sitio central.

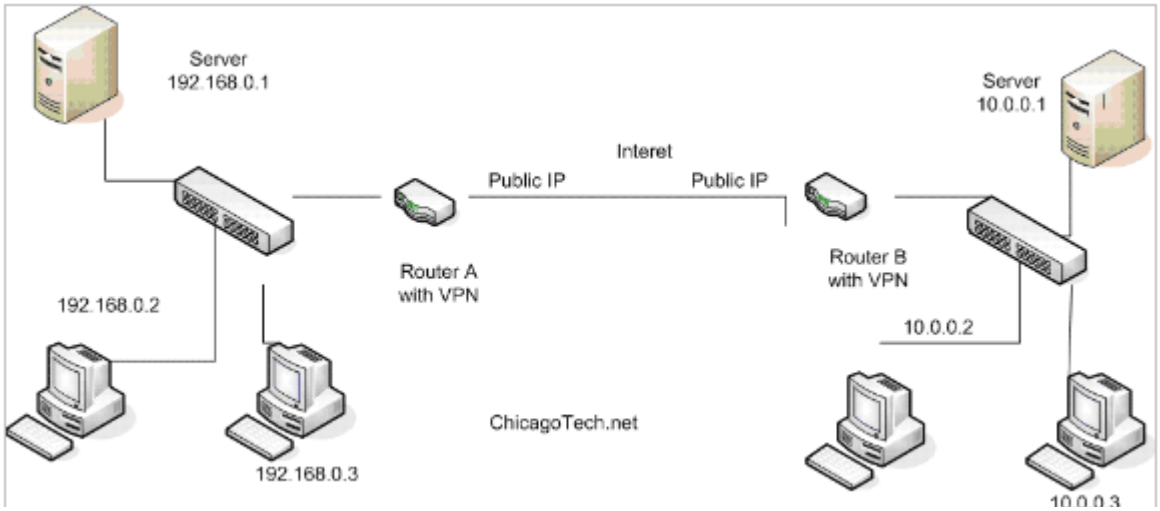

Ilustración 6: Ejemplo de conexión VPN.

Ventajas de las VPN

-Ahorro en costes: las VPN permiten que las organizaciones utilicen un transporte a través de internet proporcionado por otras empresas y rentable para conectar oficinas remotas y usuarios remotos a la sede central eliminando enlaces dedicados tipo WAN y bancos de modems.

-Escalabilidad: Las VPN permiten a las organizaciones utilizar una infraestructura de internet dentro de los ISP, lo que facilita la adición de nuevos usuarios.

-Compatibilidad con tecnologías de banda ancha: Las VPN permiten que los trabajadores móviles y los teletrabajadores aprovechen la conectividad de banda ancha de alta velocidad para acceder a las redes de sus organizaciones.

-Seguridad: Las VPN pueden incluir mecanismos de seguridad que proporcionan el máximo nivel de seguridad mediante protocolos de cifrado y autenticación que protegen los datos.

2.3.1 GRE

Un funcionamiento de las VPNs consiste en que los routers encapsulan los paquetes IP con la etiqueta GRE y los envía por la red al router de destino, en el otro extremo del router, que desencapsula los paquetes quitándoles la etiqueta GRE y dejándolos listos para enrutarlos localmente. Aunque el paquete GRE haya cruzado un gran número de routers a través de una gran red intermedia, para éste tan sólo ha efectuado un único salto a destino.

Las VPN deben proporcionar: confidencialidad, integridad y autenticación.

2.3.2 Protocolo IPSec.

Otra posibilidad para las VPN es el protocolo IPSec:

IPSec es un conjunto de protocolos y algoritmos de seguridad diseñados para la protección del tráfico de red de modo túnel. Su característica principal es la independencia algorítmica que le permite efectuar cambios de algoritmos si fuese necesario, por ejemplo, en el caso de un fallo de seguridad o si se tiene que encontrar un algoritmo más eficaz.

Este protocolo está diseñado para proporcionar seguridad sobre la capa IP lo que beneficia el transporte de protocolos o aplicaciones inseguras logrando un alto nivel de seguridad.

Las funcionalidades de IPSec son: encriptar el tráfico de manera segura para que no pueda ser visto excepto cada uno de los extremos, validar la integración de los datos asegurando que el tráfico no ha sido modificado, autenticar a cada uno de los extremos y anti-repetición evitando la repetición de la sesión segura.

IPSec utiliza dos protocolos importantes de seguridad:

• AH (Authentication Header) que incluye un sistema de autenticación criptográfico en el encabezado del paquete IP y que permite verificar que el tráfico no ha sido manipulado.

• ESP (Encapsulation Security Payload) que proporciona encriptación a la carga útil del paquete para el envío seguro de datos. Se utiliza para proteger tanto la conexión como los datos.

2.3.2.1 Fases para el establecimiento del túnel encriptado

Inicialmente se deben definir los parámetros que se usarán para establecer el túnel VPN.

Para establecer un túnel VPN es necesario que se lleven a cabo dos fases de negociación IKE (Internet Key Exchange) Fase 1 y fase 2.

1. IKE fase 1: Esta fase es la encargada de establecer un canal autenticado de comunicación. Para esto utiliza el Algoritmo de Diffie-Hellman el cual es asimétrico y permite el intercambio seguro de llaves simétricas como DES, 3DES, AES o SEAL que son utilizadas para encriptar el tráfico entre los pares en la fase 2.

La autenticación para este protocolo se puede realizar por medio de claves Pre-Compartidas (Pre-Shared Key) o de Certificados.

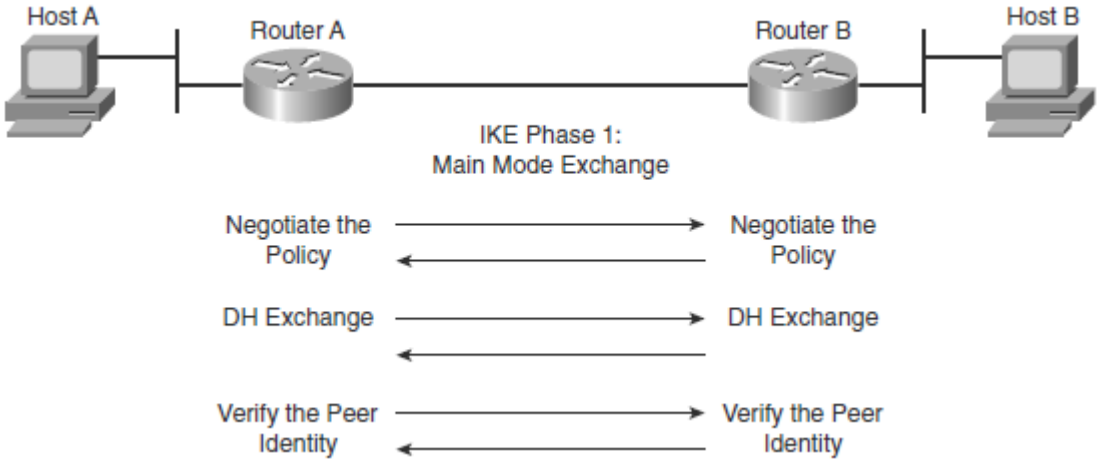

Ilustración 7: Fase 1 de IKE

2. IKE fase 2: En esta fase los pares hacen uso del canal seguro establecido en la fase 1 para compartir las claves simétricas con las cuales se encriptará el tráfico.

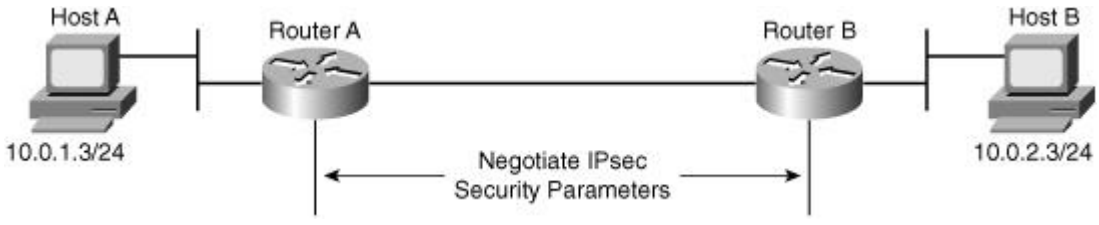

Ilustración 8: Fase 2 IKE

2.3.3 L2TP

L2TP es un protocolo que facilita el encapsulado en túnel de paquetes PPP a través de una red externa, lo más transparente posible a aplicaciones y usuarios finales.

A su vez, el protocolo PPP, (Point to Point Protocol), provee un método estándar el transporte de datagramas multiprotocolo sobre enlaces punto a punto.

PPP está comprendido por tres conceptos principales:

-Un método para el encapsulado de datagramas multiprotocolo

-Un Protocolo de control de enlace (LCP), usado para establecer, configurar y testear la conexión a nivel del enlace de datos.

-Una familia de protocolos de control a nivel de red, (NCP), para establecer y configurar diferentes protocolos de nivel de red.

PPP está diseñado para enlaces simples que transportan paquetes entre dos puertos. Estos enlaces proveen operación "Full Duplex" bidireccional simultánea, y se supone que transportan los paquetes en orden. PPP provee una solución común para hosts, bridges y routers.

El sistema de encapsulado PPP permite el multiplexado de diferentes protocolos de nivel de red en forma simultánea sobre el mismo enlace.

Protocolo de Control de Enlace, (LCP):

Es el protocolo de control de enlace de PPP. Es usado para establecer las opciones de formato de encapsulado, manejar el límite del tamaño de paquetes, detectar enlaces en estado de "loopback" y otras tareas de este tipo. Opcionalmente provee autenticación de identidad del puerto local, y determinación del estado de funcionamiento del enlace.

Protocolos de Control de Red, (NCP):

Cada protocolo de este tipo maneja las necesidades de su respectivo protocolo de nivel de red. Así se evitan dificultades respecto de enlaces punto a punto sobre circuitos conmutados.

L2TP:

Definido como Estándar en la RFC 1661, PPP encapsula paquetes de Nivel 2 en enlaces punto a punto. Los usuarios se conectan a las redes accediendo a un Network Access Server, (NAS). PPP funciona sobre esta conexión. El extremo de la conexión PPP y la terminación L2 residen en el NAS. L2TP extiende el modelo PPP permitiendo que los extremos L2 y PPP residan en diferentes dispositivos interconectados por una red de conmutación de paquetes. Con

L2TP, un usuario tiene una conexión L2 a un concentrador de acceso. El concentrador, tuneliza tramas PPP hacia el NAS. Esto permite que el procesamiento actual de Paquetes PPP sea independiente de la terminación del circuito L2. La ventaja es que en lugar de terminar la conexión L2 en el NAS, lo cual puede requerir costos de llamada de larga distancia, la conexión termina en un circuito concentrador local, el que extiende la sesión PPP sobre una infraestructura compartida, tal como un circuito Frame Relay , ATM, o la Internet. Todo esto ocurre sin cambios visibles para el usuario.[15]

L2TP permite la operación de Multienlaces. En este caso Multilink PPP, (múltiples canales o sesiones PPP) requieren terminar en un mismo NAS. Con L2TP se pueden agrupar Sesiones PPP provenientes de distintos NAS pues proyecta la sesión PPP.

L2TP Utiliza 2 tipos de Mensajes:

-Mensajes de Control

-Mensajes de Datos

Los mensajes de Control se utilizan para el establecimiento, mantenimiento, y cierre de túneles y llamadas. Los mensajes de datos son utilizados para encapsular las tramas PPP siendo transportadas en el túnel.

Los Mensajes de Control utilizan un "Canal de Control Confiable" dentro de L2TP a fin de garantizar el transporte. Sin embargo Mensajes de Datos no son retransmitidos cuando hay pérdida de Paquetes.

Entre un LAC y un LNS pueden existir múltiples túneles. A su vez, dentro de un túnel pueden coexistir múltiples sesiones. A partir de estos conceptos, se presenta la operación del protocolo. Son necesarios dos pasos para "tunelizar" una sesión PPP con L2TP:

-Establecer la conexión de control (Connection Control) para armar el Túnel

-Establecer una sesión la cual será iniciada por un "call request" entrante o saliente.

Es importante recalcar, que el túnel y su correspondiente conexión de control debe estar establecido antes de que una Llamada.

La primera conexión que se establece entre un LAC y un LNS es la conexión de control, llamada "Control Connect". A través de la misma se asegura la identidad del puerto, se identifica su versión de L2TP, y los atributos de la conexión. Un intercambio de 3 mensajes establece la conexión de control.

Se pueden crear sesiones múltiples individuales, las cuales se corresponde con flujos de tramas PPP individuales entre el LAC y el LNS. A diferencia de la conexión de control, el establecimiento de una sesión es direccional respecto del LAC y del LNS. El pedido de sesión

de un LAC a un LNS se denomina "Incomming Call", mientras que el de un LNS a un LAC es llamado "Outgoing Call".

Una vez establecido el túnel y la correspondiente sesión, el LAC recibe desde el sistema remoto las tramas PPP. Extrae el CRC, el "link framing" y los bytes de transparencia, para luego encapsular en L2TP el contenido de la trama restante y enviarlo por el túnel. El paquete recibido por el LNS es desempaquetado y procesado como lo hubiese sido una trama PPP entrante por la interfaz local.[12]

Cada puerto, mantendrá números de secuencia individuales para la conexión de control y para cada sesión individual.

Cualquiera de los dos extremos puede iniciar el cierre de una sesión, (LAC o LNS). Se ejecuta mediante el mensaje de control CDN.

2.4 VLAN

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).[14]

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware.

Clasificación:

- VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador;

- VLAN de nivel 2 (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación;

-VLAN de nivel 3: existen diferentes tipos de VLAN de nivel 3:

- VLAN basada en la dirección de red conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.

- VLAN basada en protocolo permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

Ventajas de la VLAN

La VLAN permite definir una nueva red por encima de la red física y, por lo tanto, ofrece las siguientes ventajas:

Mayor flexibilidad en la administración y en los cambios de la red, ya que la arquitectura puede cambiarse usando los parámetros de los conmutadores;

Aumento de la seguridad, ya que la información se encapsula en un nivel adicional y posiblemente se analiza;

Disminución en la transmisión de tráfico en la red. Puesto que la VLAN limita el dominio de difusión limitando así el tráfico de broadcast de difusión no deseado.

2.4.1 "Router-on-a-stick"

El enrutamiento tradicional entre distintas redes VLAN es por medio de interfaces físicas diferentes para cada una de estas, lo que presenta un importante problema y una gran limitación a la hora de un elevado número de VLAN puesto que los rutes tienen un número bastante limitado de interfaces físicas. Es más, a medida que el número de redes VLAN aumenta en la red es más difícil tener suficientes interfaces físicos en un router (encima su precio se encarecería mucho). Una alternativa a eso en redes de gran tamaño consiste en emplear subinterfaces y trunking de VLAN. Esto permite que en una única interfaz física del router enrutemos el trafico correspondiente a varias VLAN, estos subinterfaces son interfaces virtuales creados para evitar las limitaciones de hardware de las interfaces físicas del router.

Las subinterfaces son interfaces virtuales basadas en software que están asignadas a interfaces físicas. Cada subinterface se configura de manera independiente con una dirección IP y mascara de subred propia. Esto permite que una misma interfaz física forme parte simultáneamente de varias redes lógicas.[11]

Para que este modo de configuración funcione correctamente la interfaz física del router en cuestión ha de estar conectada a un puerto "trunk" en el "switch" adyacente.

En términos de funcionamiento, utilizar este método es lo mismo que utilizar el modelo tradicional de enrutamiento entre redes VLAN, pero en vez de emplear las interfaces físicas para realizarlo se utilizan subinterfaces.

2.5 Protocolos de red disponibles.

2.5.1 RIPng

Es la versión de RIP para IPv6, un protocolo de sencilla configuración aunque su utilización es escasa actualmente (redes pequeñas) , Se describe en el RFC 1058, fue basado en los protocolos de enrutamiento de Xerox PUP y XNS.

RIP es una implementación directa del enrutamiento distancia-vector para redes locales. La comunicación RIP usa UDP como protocolo de transporte, con número de puerto 520 como puerto de destino.

Operaciones Básicas

Cuando RIP comienza envía un mensaje para cada uno de sus vecinos (sobre el puerto UDP bien-conocido 520) solicitando una copia de la tabla de enrutamiento del vecino. Este mensaje es una pregunta (orden se pone a 1) con una familia de direcciones de 0 y una métrica de 16. Los routers de los vecinos devuelven una copia de sus tablas de enrutamiento.

Cuando RIP está en modo activo envía todo o parte de su tabla de enrutamiento a todos los routers de sus vecinos (mediante broadcasting y/o enviándolo sobre cualquier enlace punto-a-punto hacia sus vecinos). Esto se hace cada 30 segundos. La tabla de enrutamiento se envía como respuesta (orden es 2, incluso aunque no se solicite).

Cuando RIP descubre que una métrica ha cambiado, emite el cambio a otros routers.

Cuando RIP recibe una respuesta, el mensaje se valida y la tabla de enrutamiento local se actualiza si es necesario.

Para mejorar el rendimiento y la confiabilidad, RIP especifica que una vez que un router (o un host) aprende la ruta de otro router, debe mantener esa ruta hasta que aprenda la mejor (con un coste estrictamente bajo). Esto impide aquellas rutas oscilatorias entre dos o más caminos de igual coste.

El principal problema de este protocolo es que no está diseñado para redes grandes y cuando llega a un recuento de 15 o más saltos lo considera infinito (demasiado alejado);el router del decimoquinto salto no propagaría la actualización de enrutamiento al siguiente router.[2]

2.5.2 OSPFv3

Open "Shortest Path First" (OSPF), camino más corto primero, es un protocolo de red para encaminamiento jerárquico o “Interior Gateway Protocol” (IGP), que usa el algoritmo "SmoothWall Dijkstra", el cual se basa en enlace-estado para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo.

Su medida de métrica se denomina "cost", y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF construye además una base de datos enlace-estado idéntica en todos los routers de la zona.

2.5.2.1Desarrollo histórico de OSPF:

En 1987 se comenzó a desarrollar OSPF, siendo internet solo una red académica financiada por el gobierno de estados unidos.

En 1989 se publicó la especificación para OSPFv1 en la RFC 1131, Se escribieron dos implementaciones una para UNIX y otra para routers. OSPFv1 era un protocolo experimental y nunca se implementó.

En 1991 se introdujo OSPFv3 en la RFC 1247, y fue elegido como protocolo de gateway interior recomendado por el IETF.

En 1988 se actualizo la especificación de OSPFv2 en la RFC 2328 la cual sigue vigente en la actualidad.

En 1999 se publicó OSPFv3 para IPV& en la RFC 2740, la cual no es una nueva implementación del protocolo para IPv6 sino una re-escritura importante del funcionamiento del protocolo.

En 2008 se actualizo OSPFv3 en la RFC 5340 como OSPF para IPv6.

Una red OSPF se puede descomponer en regiones (áreas) más pequeñas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre

por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los routers en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los routers eligen a un router designado y un router designado secundario o de copia que actúan como "hubs" para reducir el tráfico entre los diferentes routers.

2.5.2.2 Características básicas

Sin clase: Por diseño, es un protocolo sin clase; por tanto, permite utilizar CLSM y CIDR

Eficiente: Los cambios de enrutamiento controlan las actualizaciones de enrutamiento (no hay actualizaciones periódicas). Utiliza el algoritmo SPF para elegir la mejor ruta.

Convergencia rápida. Propaga rápidamente los cambios que se producen en la red.

Escalable: Funciona bien en redes de tamaño pequeño y mediano. Los routers se pueden agrupar en áreas para dar soporte a un sistema jerárquico.

Seguro: Soporta la autenticación MD5. Si se habilita los routers OPF solo aceptaran actualizaciones de enrutamiento de sus interlocutores cifradas con la misma contraseña compartida previamente.

Componentes de OSPF

Los componentes básicos principales del protocolo de enrutamiento OSPF son 3

Estructuras de datos: OSPF crea y mantiene tres bases de datos:

-Base de datos de adyacencia. Crea la tabla de vecinos.

-Base de datos de estado de los enlaces. Crea una tabla de topología

-Base de datos de reenvió. Crea la tabla de enrutamiento.

Mensajes del protocolo de enrutamiento: OSPF intercambia mensajes para transmitir información de enrutamiento utilizando cinco tipos de paquetes:

-Paquete de saludo (HELLO)

-Paquete de descripción de base de datos

-Paquete de solicitud de estado del enlace.

-Paquete de actualización de estado de enlace.

-Paquete de acuse de recibo de estado del enlace.

Algoritmo: La CPU procesa las tablas de vecinos y de topología mediante el algoritmo SPF de "Dijkstra". El algoritmo SPF se basa en el coste acumulado para alcanzar un destino.

El algoritmo SPF crea un árbol SPF colocando cada router en la raíz del árbol y calculando la ruta más corta hacia cada nodo. A continuación, el árbol SPF se utiliza para calcular las mejores rutas. OSPF incluye las mejores rutas en la base de datos de reenvió, que se emplea para crear la tabla de enrutamiento.

En los comienzos de IPv6 muchos protocolos necesitaron actualizarse para poder soportar IPv6: ICMP, TCP, UDP y muchos otros incluido OSPF. Cuando el equipo de trabajo actualizo OSPF para trabajar con IPv6 lo llamo OSPFv3. De manera interesante OSPFv3 soporta IPv6 pero no IPv4. De esta manera OSPfv3 no intenta añadir soporte IPv6 a OSPFv2. OSPFv3 es similar a OSPFv2 en su funcionamiento y configuración pero son dos protocolos de enrutamiento diferente: un protocolo para enrutamiento IPv4 (OSPFv2) y un protocolo de enrutamiento para IPv6 (OSPFv3). Debido a que OSPFv3 solo publica rutasIPv6, un sitio que use "dual stack" necesitará utilizar ambos protocolos OSPFv2 y OSPFv3 (asumiendo que se utiliza OSPF en toda la red).[13]

2.5.2.3 Configuración de OSPFv3

OSPFv3 usa una configuración más directa habilitando el protocolo en cada interfaz mediante la adición de un subcomando en el modo de configuración de interfaz. De hecho, OSPFv3 no utiliza el subcomando "network" en el modo de configuración del router. En su lugar, OSPFv3 utiliza el subcomando de interface: ipv6 ospf <process-ID> area <#Area> Este comando habilita el proceso OSPFv3 en esa interfaz, y establece el área OSPFv3. El process-id identifica al proceso de OSPF (debe ser el mismo en toda las interfaces de un router para que se compartan las rutas). #area identifica el área a la que esa red pertenece.

OSPFv3 como protocolo de estado de enlace necesita conocer e identificar a sus vecinos. Para esto utiliza una importante configuración llamada Router ID (RID). Para revisar, OSPFv2 utiliza un RID de 32 bits, elegido durante el proceso de inicialización de OSPF. Es decir, cuando se configura OSPF por primera vez, o más tarde, cuando se vuelve a cargar el router. El proceso OSPFv2 elige su RID basado en los siguientes ítems:

1. Si el comando router-id de OSPF está configurado, utiliza este valor, e ignora las direcciones IPv4 de la interfaz.

2. Si el ID del router no está configurado con el comando router-id, comprueba las direcciones IPv4 de las interfaces loopback y que el estado de interface esté arriba. Entre ellos, escoge la más alta dirección IP numéricamente (En hexadecimal la que es mayor)

3. Si ninguna de los dos primeros puntos suministra un ID de router, el router elige la dirección IPv4 más alta de todas las interfaces cuyo estado de interface esté arriba. Curiosamente, OSPFv3 también utiliza un RID de 32-bit, utilizando las mismas reglas exactas de OSPFv2. Es decir, OSPFv3, que soporta IPv6, tiene un ID de router que se parece o es una dirección IPv4. Utilizando las mismas reglas de selección del RID por parte OSPFv3 y OSPFv2 se deja abierta la posibilidad de una mala y desafortunada configuración potencial: un router que no utilice el comando router-id OSPFv3, y no tiene ninguna dirección IPv4 configurada, no puede elegir un RID. Si el proceso OSPFv3 no tiene un RID, el proceso no puede funcionar correctamente, formar relaciones de vecindad, o rutas de intercambio.

Este problema se puede solucionar fácilmente. En la configuración de OSPFv3, si el router no tiene ninguna de las direcciones IPv4, asegúrese de configurar el RID utilizando el subcomando router-id. Más allá de esto, la configuración OSPFv3 es relativamente simple. A continuación se resumen los pasos de configuración y comandos de OSPv3:

Paso 1. Crear un número de proceso OSPFv3, y entrar en el modo de configuración OSPF para ese proceso, usando el comando global ipv6 ospf router <process-id> Paso 2 Asegúrese de que el router tiene un ID de router, ya sea porque:

A. Configuración con el subcomando router-id

B. Configuración de una dirección IPv4 en cualquier interface "loopback" cuyo estado esté arriba

C. Configuración de una dirección IPv4 en cualquier interface de trabajo cuyo estado esté arriba

Paso 3. Configure el comando ipv6 ospf <process-ID> area <#Area> en cada interfaz para permitir tanto OSPFv3 en la interfaz y establecer el número de área para la interfaz.[13]

2.5.3 EIGRP

"Enhanced Interior Gateway Routing Protocol" o Protocolo de enrutamiento de gateway interior) es un protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP. EIGRP al igual que IGRP usa el siguiente cálculo de métrica:

Métrica= [K1 * ancho de banda + ((K2 * ancho de banda)/(256-carga))+ (K3 * retardo)]*[K5/(confiabilidad + K4)]. (Nota: Debido a que EIGRP utiliza un campo de métrica de 32 bits, a diferencia de IGRP que es de 24, multiplica este valor por 256).

Los valores por defecto de las constantes son: K1=1, K2=0, K3=1, K4=0, K5=0. Cuando K4 y K5 son 0, la porción [K5/(confiabilidad+K4)] de la ecuación no forman parte del cálculo de la métrica. Por lo tanto, utilizando los valores por defecto de las constantes, la ecuación de la métrica es: Ancho de banda +retardo. [5].

Puesto que es un protocolo propietario de cisco y aunque trabajaremos con todo componentes cisco, al querer diseñar una red lo más genérica posible, desecharemos dicho protocolo como opción a implementar.

2.6 DHCPv6

Es un protocolo mediante el cual un servidor DHPv6 asigna direcciones IPv6 y otra información de configuración de red de forma dinámica, es una herramienta muy útil que ahorra mucho tiempo a los administradores de la red. Los parámetros de configuración incluyen la siguiente información:

- direccionamiento, de enrutamiento

- servidor de nombres (DNS)

- servicio de información de red (NIS)

El mecanismo de configuración automática con estado sigue un modelo de cliente-servidor y se basa en el uso de DHCPv6 como ocurre con DHCP para IPv4, aunque hay grandes diferencias en el código: DHCP en IPv4 no es más que una extensión del protocolo BOOTP, por lo que tiene una funcionalidad limitada. En cambio, el protocolo DHCPv6 permite establecer los parámetros de configuración de un servidor DHCP para un cliente IPv6.[6]

El cliente IPv6 representa un dispositivo que busca tener conectividad global IPv6 y solicita la información de configuración necesaria para poder establecer esta conectividad. El servidor DHCP constituye un punto central que reagrupa los parámetros de configuración. No necesariamente se ubica en el mismo enlace que el cliente, en cuyo caso, la información DHCP puede intercambiarse a través de un relevo. El servidor puede contener información de configuración para dispositivos ubicados en distintos enlaces. El cliente DHCP debe establecer una conexión directa ya sea con el relevo o con el propio servidor DHCP.[4]

El relevo funciona como un "proxy" DHCP que se limita a retransmitir los mensajes DHCP; es transparente a la información intercambiada y no modifica en absoluto los mensajes DHCP intercambiados entre el servidor y el cliente. El proxy encapsula los mensajes DHCP del cliente en un formato específico y realiza la operación inversa, es decir, desencapsula los mensajes provenientes del servidor para su entrega al cliente. El servidor forma el mensaje que

debe ser recibido por el cliente, y, si no tiene comunicación directa con él, lo encapsula en un mensaje DHCP dirigido al proxy.

Para conocer el estado de los recursos administrados (representados por los parámetros de configuración), el servidor DHCP mantiene una lista de asociaciones entre los parámetros asignados y el cliente. El cliente no puede ser identificado con su dirección unicast ya que ésta es parte de los parámetros otorgados por el servidor DHCP. Por ello, el servidor utiliza un identificador particular: el DUID (DHCP Unique IDentifier). El DUID es creado por el cliente y lo identifica a él, no a una interfaz. Se han propuesto varios esquemas para generarlo, por ejemplo, a partir de la dirección de enlace local, completada con un elemento que garantice la exclusividad, como un sello de tiempo. Una vez que el cliente genera un DUID, éste debe ser invariable, incluso si llegara a cambiar su dirección de enlace local.

2.6.1 Formato de mensajes DHCPv6

El protocolo DHCPv6 se describe en el RFC 3315. el protocolo de intercambio de información está desacoplado de la información en sí misma. La información intercambiada puede cambiar y evolucionar rápidamente sin afectar los mecanismos de este intercambio. Esta separación ofrece al protocolo una estabilidad y cierta capacidad para ser extendido.

En la terminología de DHCP, se le llama mensaje a una unidad del protocolo DHCPv6. Cada mensaje DHCP tiene un formato de encabezado idéntico. Desde este punto de vista, DHCP sigue los principios del segmento TCP: un formato único para todo el conjunto de funciones de TCP. Estos principios privilegian la simplificación en el proceso de desarrollo del protocolo.

La figura Estructura de los mensajes DHCPv6 muestra la estructura de un mensaje DHCPv6. La cabecera se divide en tres partes:

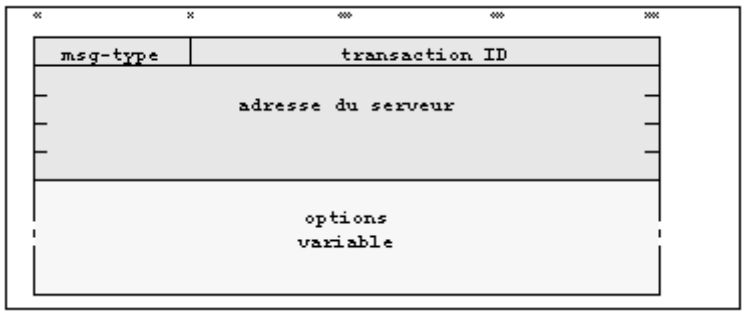

Ilustración 9: Estructura mensaje DHCPv6

La información de comando codificada en una palabra de 32 bits, designa la función DHCP relacionada con el intercambio. Esta parte contiene el tipo de mensaje y un identificador

del intercambio. El primer campo (de 8 bits) muestra el tipo de mensaje y define la función del mensaje en el protocolo. Como su nombre lo indica, el campo transaction-ID tiene por objeto identificar el intercambio desde el punto de vista del cliente. Le permite asociar las respuestas recibidas a las solicitudes que ha formulado.

La información de direccionamiento se utiliza para especificar la dirección IPv6 del servidor DHCP. Indica la dirección de la interfaz utilizada por el servidor en la transacción.

El campo de opciones se utiliza para transmitir las informaciones de configuración. Es un campo de longitud variable cuya codificación sigue el clásico esquema "TLV", es decir, el Tipo de la opción, la Longitud en octetos del elemento que le sigue, que es el Valor del parámetro. El tipo se codifica en dos octetos. El campo de longitud también ocupa dos octetos aún si valor del parámetro es nulo o si éste tiene una longitud fija.

Los mensajes utilizados para la comunicación entre el servidor y el proxy de relevo, son diferentes. Un mensaje de relevo encapsula como una opción, la información del mensaje DHCP del servidor al cliente. El mensaje de relevo tiene un prefijo de enlace que indica la interfaz del relevo a través de la cual se recibió el mensaje DHCP, o por la que debe ser enviado. La dirección de enlace local del cliente contiene la dirección de la interfaz a configurar en el cliente.

El protocolo DHCPv6 incluye 12 mensajes DHCP distintos:

Solicitud DHCP (DHCP Solicit): Mensaje de solicitud de presencia de servidores DHCP. Se transmite hacia un servidor o un proxy DHCP. Un cliente envía este mensaje para localizar los servidores DHCP.

Anuncio DHCP (DHCP Advertise): Mensaje de presencia de servidores DHCP. Se emite en respuesta a un mensaje de solicitud DHCP para comunicar la dirección IP de un servidor DHCP. El destinatario es el cliente si se encuentra en el mismo enlace que el servidor; de lo contrario, se envía al proxy del cliente.

Consulta DHCP (DHCP Request): Mensaje de solicitud de parámetros de configuración por un cliente sin dirección.

Confirmación DHCP (DHCP Confirm): Mensaje de solicitud de confirmación sobre la validez de los parámetros asignados al cliente.

Renovación DHCP (DHCP Renew): Mensaje de solicitud para prolongar el uso de la dirección IP asignada.

Reasignación DHCP (DHCP Rebind): Igual al mensaje anterior, pero puede ser otro servidor DHCP el que responde, y no necesariamente el que asignó la dirección IP.

Respuesta DHCP (DHCP Reply): Mensaje enviado por el servidor en respuesta a una petición del cliente. Contiene los valores de los parámetros de configuración solicitados.

Liberación DHCP (DHCP Release): Mensaje emitido por el cliente para notificar la liberación de las direcciones IP previamente asignadas por el servidor.

Denegación DHCP (DHCP Decline): Mensaje de un cliente indicando que una o varias de las direcciones asignadas ya están siendo utilizadas en su enlace.

Notificación de reconfiguración DHCP (DHCP reconfigure-init): Mensaje enviado por el servidor para notificar al cliente que existen nuevos valores para los parámetros de configuración. El cliente debe iniciar una nueva transacción para adquirir esta información.

Encapsulación de relevo (Relay-Forward): Mensaje del proxy para transportar los mensajes del cliente hacia el servidor. El mensaje del cliente se encapsula en este mensaje.

Encapsulación del servidor (Relay-Reply): Mensaje generado por el servidor hacia el proxy con información destinada al cliente. El proxy extrae el mensaje para el cliente y lo transmitirá sobre el enlace correspondiente.

El intercambio de información entre el cliente y el servidor DHCP se realiza por medio de opciones. La información se divide en tres categorías.

Información temporal. Se refiere a recursos de red solicitados por el cliente y asignados por el servidor por un período determinado. Actualmente, el único tipo de recurso temporal es la dirección IP, cuya gestión se realiza bajo el concepto de IA.

Información de carácter general. Se refiere al conjunto de parámetros normalmente presentados para la configuración de una máquina IPv6.[4]

2.6.2 Tipos de configuración DHCPv6

Las direcciones IPv6 de unidifusión global pueden configurarse manual o dinámicamente. Sin embargo, existen dos métodos en los que las direcciones IPv6 de unidifusión global pueden asignarse dinámicamente.

2.6.2.1 Configuración automática de direcciones sin memoria del estado (SLAAC).

La configuración dinámica de direcciones sin memoria del estado es un método mediante el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin utilizar los servicios d un servidor DHCPv6. En el núcleo de SLAAC esta ICPMv6, El cual es como ICMPv4 pero incluye funcionalidad adicional y es mucho más robusto. SLAAC utiliza mensajes ICMPv6 de solicitud al router y de anuncio de router para proporciona la información de direccionamiento y configuración que, normalmente, proporcionaría un servidor DHCP:

Mensaje de solicitud de router (RS): El cliente envía un mensaje RS a la dirección multidifusión a todos los routers FF02::2.

Mensaje de anuncio del router (RA): Proporcionan información de direccionamiento a los clientes. Los mensajes RA incluyen el prefijo y la longitud de este del segmento local. El cliente la utiliza para crear su propia dirección IP. Se envían a la dirección multidifusión de todos los nodos FF02::1.[10]

Al ser sin memoria de estado no existe ningún servidor que mantenga información de las direcciones de red.

2.6.2.2 DHCPv6 sin memoria de estado

La opción DHCPv6 sin memoria de estado informa al cliente de que debe utilizar la información contenida en el mensaje RA relativa al direccionamiento, pero que además hay disponibles parámetros de configuración adicionales en un servidor DHCPv6

Utilizando el prefijo y la longitud de este del mensaje RA, junto conEUI-64 o un IID agregado aleatoriamente, el cliente crea su dirección IPv6 de unidifusión global.

A continuación el cliente se comunica con el servidor DHCPv6 sin memoria del estado para obtener información adicional que no se proporciona en el mensaje RA. Puede tratarse, por ejemplo, de una lista de direcciones IPv6 del servidor DNS. Es decir este tipo de servidor solo proporciona parámetros de configuración para los clientes, no direcciones IP.

Para DHCPv6 sin memoria de estado el indicador O se configura en 1 y el indicador M se deja con la configuración predeterminada de 0.(RA)

2.6.2.3 DHCPv6 con memoria de estado

Requiere que el cliente obtenga toda la información de direccionamiento y configuración de un servidor DHCPv6 con memoria de estado. Por ello el servidor DHCPv6 mantiene información de estado de IPv6.

El indicador M informa de si se debe usar DHCPv6 con memoria de estado. El O no interviene.

2.7 Listas de acceso (ACL)

Una ACL es una lista secuencial de instrucciones permit o deny que se aplican a las direcciones o los protocolos de capa superior. Las ACL proporcionan una forma potente de controlar el tráfico que entra y sale de una red. Se pueden configurar listas ACL para todos los protocolos de la red enrutada.

Una ACL puede definirse también como una serie de comandos del IOs que controla si un router reenvía o descarta paquetes, basándose en la información disponible en la cabecera del paquete.

Cuando se configuran, las ACL realizan las siguientes tareas:

-Limitar el tráfico de la red para aumentar su rendimiento. Limitando los tipos de tráfico que la política de la empresa no considere oportunos.

-Proporcionar control de flujo de tráfico. Las ACL pueden restringir la entrega de actualizaciones de enrutamiento. Si no se requieren actualizaciones debido a las condiciones de la red, el ancho de banda se preserva.

-Proporcionar un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un acceda una parte de la red y evitar que otro host acceda a esa misma área.

-Filtrar el tráfico según el tipo de este. Por ejemplo permitir correo electrónico pero denegar el trafico telnet.

- Filtrar los hosts para permitirles o denegarles acceso a los servicios de la red. Las ACL pueden permitir o denegar a un usuario el acceso a determinados tipos de archivos, como FTP o HTTP.

Los router no tienen ACL configuradas de manera predeterminada; por tanto, no filtran el tráfico de manera predeterminada. El tráfico que entra en el router se enruta solamente en función de la información de la tabla de enrutamiento. Sin embargo cuando se aplica una ACL a una interfaz, el router realiza la tarea adicional de evaluar todos los paquetes de la red a medida que pasan a través de la interfaz, para determinar si el paquete se puede reenviar.

A demás de permitir o denegar el tráfico, las ACL se pueden utilizar para seleccionar el tipo de tráfico que se va a analizar, reenviar o procesar de otras formas, por ejemplo se pueden utilizar listas ACL para clasificar el tráfico, con el fin de permitir el procesamiento por prioridad.

Para evaluar el tráfico de la red la ACL extrae la siguiente información de la cabecera:

-Dirección IP origen.

-Dirección IP destino.

-Tipo de mensaje ICMP.

-Puerto origen.

-Puerto destino.

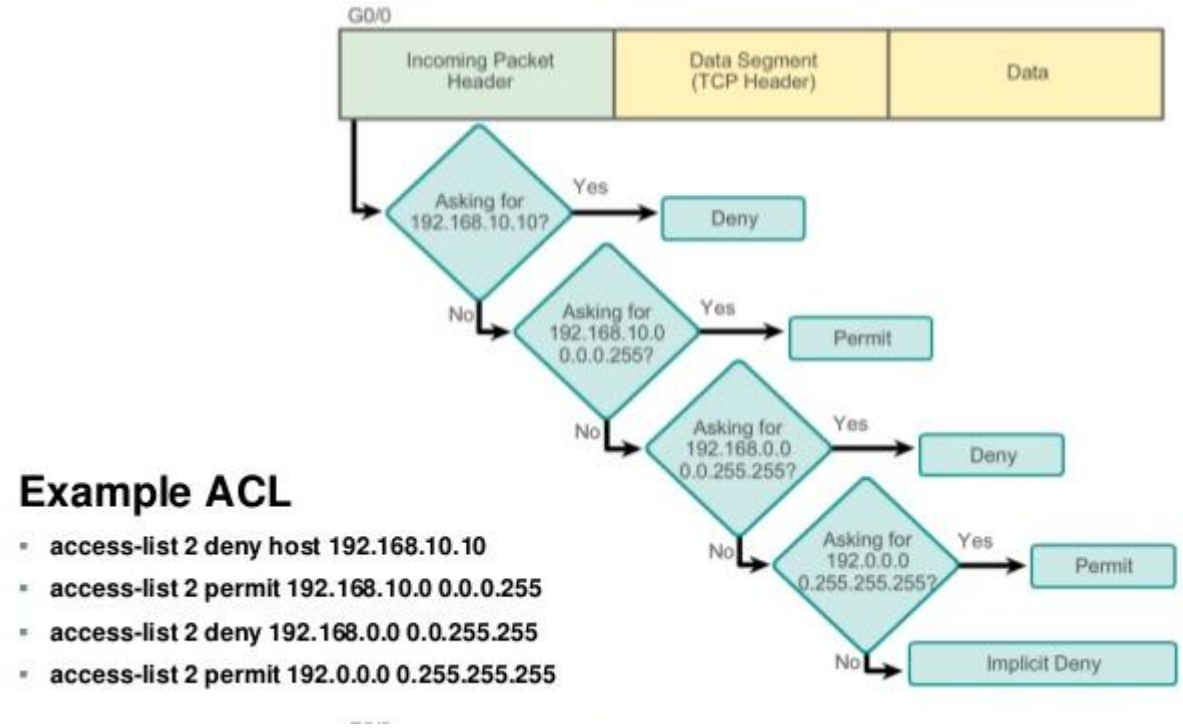

Ilustración 10: Ejemplo de lista de acceso.

Las ACL se configuran para aplicarse al tráfico de entrada o de salida.

ACL entrante. Los paquetes entrantes se procesan antes de enrutarse hacia la interfaz de salida. Las ACL de entrada son eficientes porque ahorran la sobrecarga de las búsquedas de enrutamiento si el paquete se descarta. Si las pruebas permiten el paso del paquete, entonces este se procesa para el enrutamiento. Son adecuadas para filtrar los paquetes cuando la red conectada a un interfaz de entrada es el único origen de los paquetes que se deben examinar.

ACL saliente. Los paquetes entrantes se enrutan hacia la interfaz de salida y luego se procesan a través de la ACL saliente. Las ACL salientes son adecuadas cuando se aplica el

mismo filtro a paquetes que proceden de varias interfaces de entrada, antes de salir por la misma interfaz de salida.

La última instrucción de una ACL siempre es una instrucción de denegación implícita. Esta instrucción se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esta denegación implícita, una ACL que no contenga al menos una instrucción permit bloqueara todo el tráfico.

Capítulo 3. Diseño de una red genérica de datos IPv6

Debido a que la escuela trabaja en su mayoría con material cisco y a que la herramienta paket tracer de esta compañía a pesar de sus errores y opciones no implementadas simula bastante bien el entorno que queremos realizar utilizaremos solo hardware de esta compañía aunque intentaremos hacer la red de todas formas lo más genérica posible y compatible con el resto de compañías con el menor número de cambiaos necesarios. Debido a la utilización del paket tracer se han limitado los componentes utilizados en el diseño a los que están disponibles en dicha herramienta.

3.1 Planificación de la distribución

Para poder cumplir con el diseño de una red genérica lo primero es plantearla teóricamente, para el diseño de esta red se ha pensado en dividirlo todo en tres tipos de sedes, una central, la cual es la mayor, con capacidad para un numero grande de puntos de acceso físico a la red, cifra que rondaría los 140.000, el segundo tipo de sede genérica seria el mediano, con capacidad para unos 15.000 puntos de conexión a la red y un modelo de red pequeña adecuada para unos 600 puntos de acceso a la red.

Una vez diseñadas y configuradas nos dispondremos a interconectarlas con la red central, en el caso de que sea necesaria más de una red de uno de los tipos bastara con duplicarla con pequeñas adaptaciones.

3.2 Direccionamiento IPv6

Lo primero y necesario para poder poner en funcionamiento y poder planificar una red es conocer que rango tenemos en cuanto a direcciones IPv6 así como asignar a cada subred su rango particular, como el planteamiento de la red es genérico y no queremos complicar en exceso este con numero enrevesados utilizaremos una dirección genérica sencilla repitiendo el mismo número en toda ella. Puesto que el bloque mínimo adquirible es un /48 para usuarios

finales y esto supone un numero de direcciones IP = 1.208.925.819.614.629.174.706.176 por lo que no hay que preocuparse en cuanto a alcanzar el límite de direcciones que hay asignado.

Se usa la dirección inicial aaaa:aaaa:aaaa::/48 o en su forma sin abreviar aaaa:aaaa:aaaa:0000:0000:0000:0000:0000. A la hora de utilizar esta planificación para una red real bastaría con sustituir las a de nuestra dirección IP por la dirección que sea asignada desde el proveedor de direcciones.

Partiendo de esta dirección se divide el rango de direcciones en las distintas sedes que se han planificado:

3.2.1 Sede central o grande:

Para esta red debido a sus características y por si crece mucho (con el llamado internet de las cosas , el cual, lleva a que todo aparato que utilicemos acabe siendo conectado a la red sería posible un crecimiento inmenso) y puesto que se tienen muchas direcciones se ha decidido darle un tamaño /64 lo que dejaría la dirección de red como aaaa:aaaa:aaaa:0000:0000:0000:0000:0000/64 o aaaa:aaaa:aaaa::/64 el cual tendría como host inicial aaaa:aaaa:aaaa::1/64 y como host final aaaa:aaaa:aaaa:0000:ffff:ffff:ffff:ffff

Con un /64 se tendría un total de 18.446.744.073.709.551.616 direcciones IPv6

3.2.2 Sede mediana:

Se ha decidido que para este tipo de redes se utilizara un /80 lo que nos dejaría una dirección de red siguiendo a partir de la red anterior aaaa:aaaa:aaaa:0001::/80 en tipografía abreviada o aaaa:aaaa:aaaa:0001:0000:0000:0000:0000 si abreviar.

Lo que dejaría como host inicial la dirección aaaa:aaaa:aaaa:0001:0000:000:0000:0001 Y como host final aaaa:aaaa:aaaa:0001:0000:ffff:ffff:ffff

Se deja el espacio entero de un /64 por si a la hora de la implementación en una red no genérica hubiera más de una sede de este tamaño, fuera más fácil su asignación de rango de IP así como agruparlas por tipo mediano en una subred de conjunto.

Con un /80 tendríamos un total de 1.099.511.627.776 direcciones IPv6

3.2.3 Sede pequeña:

Para ese tipo de redes el tamaño que se asigna bastara con un /96 que siguiendo lo que se ha planteado anteriormente y se coloca a continuación del espacio reservado para bloques de direcciones destinados a sedes medianas, quedando una dirección de red aaaa:aaaa:aaaa:0002::/96 de forma abreviada o aaaa:aaaa:aaaa:0002:0000:0000:0000:0000/96 sin abreviar.

En cuanto a la dirección de host inicial seria aaaa:aaaa:aaaa:0002:0000:0000:0000:0001/96 y la dirección de host final quedaría con aaaa:aaaa:aaaa:0002:0000:0000:ffff:ffff/96.

Nuevamente se deja todo el resto del bloque /64 desde el que se ha iniciado esta partición en subbloques para posibles adiciones de más redes de este tamaño o sedes pequeñas.

Con un /96 se tendría un total de 4.294.967.296 direcciones IPv6

Como se puede comprobar la principal ventaja de IPv6 es que no hay problema con la sobreestimación es decir que no hay problema por diseñar bloques de redes muy grandes en previsión a que crezca la empresa o se necesite más puntos de acceso puesto que la cantidad de direcciones que se tiene es lo suficientemente grande para soportarlo.

3.3 Diseño topológico de los tipos de redes.

En este apartado se presentara la decisión así como su justificación en cuanto al diseño de la red a nivel lógico, es decir que cantidad de componentes y de que clase se ha decidido incluir en cada tipo de diseño para que la red sea lo más genérica posible y pueda adaptarse a cualquier necesidad.

3.3.1 Diseño topológico de sede grande.

Para este tipo de red como se dijo antes se ha estimado unos 140.000 puntos de conexión, por lo que se optó por una red jerárquica con un router de la serie 1941 como router central el cual solo requiere como característica especial un puerto Gigabit Ethernet como salida a nuestra red, después de este se ha pensado como red de distribución colocar un swich genérico modular e instalarle 2 salidas Gigabit Ethernet para conectarlo con el router principal (y con un posible router de respaldo) y con 8 puertos de fibra óptica también a velocidad Giga puesto que la sede es muy grande se ha pensado así disminuir los retardos producido por la red así como dar cobertura giga a las estaciones que la necesiten.

Después de esta capa vendrían 2 capas más de swich con 10 puertos de fibra a la misma velocidad conectando un nuevo swich a cada puerto de los antes mencionados, inmediatamente posterior a este se conectaría otro swich con 9 puertos Gigabyte Ethernet y uno de fibra óptica y para finalizar la distribución otro swich este de la serie Catalyst 2950 el cual contiene 24 puertos Ethernet comunes y dos puertos Gigabyte Ethernet uno de los cuales estaría destinado para conectar con el swich superior y el otro por si hay que ampliar la red o para terminales que requieran esa velocidad de conexión.

La conexión de red quedaría entonces en una configuración de árbol con 8*9*9*9*(24+1) conexiones. Siendo una simplificación la siguiente figura:

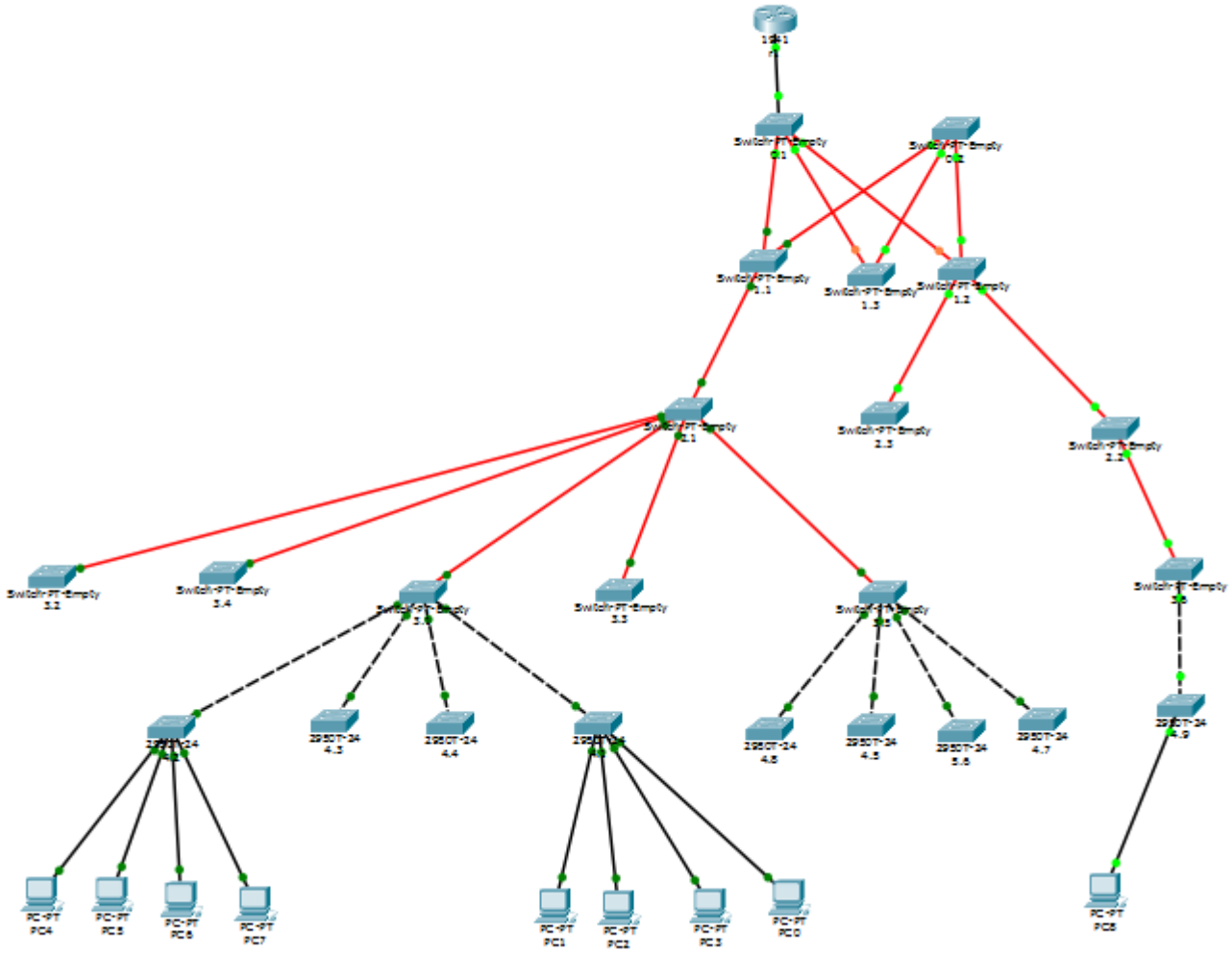

Ilustración 11: Maqueta de la sede grande

Con los enlaces de fibra óptica se persigue tanto la velocidad de la red, como disminuir el retardo de esta así como posibilitar múltiples implementaciones físicas puesto que esta tiene mucha menor limitación en cuanto a distancia que el cable Ethernet lo que posibilita que la sede principal sea de una topología expandida pudiendo ocupar varios pisos de un bloque o incluso una amplia extensión en un polígono o en el campo que al utilizar enlaces de fibra no habría prácticamente problemas con la separación entre los swiches principales.

3.3.2 Diseño topológico de sede mediana

Esta red ha sido diseñada estimando que el número de puntos de conexión ronda los 15.000 por lo que no se ha tenido en cuenta que estén muy separados topológicamente ni se ha pensado que fuera necesaria fibra óptica así como conexión gigabit aunque podría sustituirse en caso necesario por esta sin mayores complicaciones.

También aquí se ha optado por una configuración jerárquica con un router de la serie 1941 sin muchas características especiales y debajo de este tenemos 3 cascadas de swich de las serie Catalys2960 los cuales disponen de 24 puertos Ethernet y dos Gigabit Ethernet los cuales serán tratado como puertos estándar Ethernet.

Lo que deja una topología árbol 24*25*25 reservando un puerto del primer swich para la conexión con un router de respaldo. Siendo una simplificación la siguiente figura:

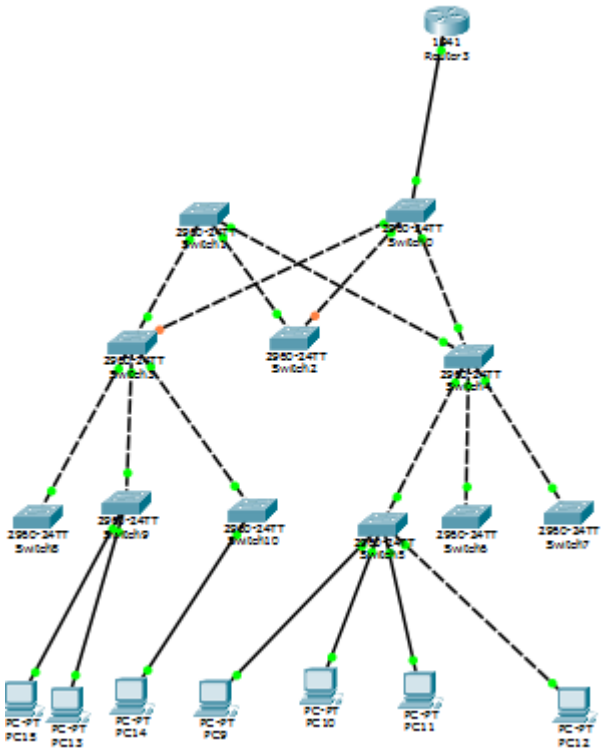

Ilustración 12: Maquete de una sede mediana.

3.3.3 Diseño topológico de sede pequeña

Esta red ha sido diseñada estimando que el número de puntos de conexión ronda los 600 por lo que no se ha tenido en cuenta que estén muy separados topológicamente ni se ha pensado que fuera necesaria fibra óptica así como conexión gigabit aunque podría sustituirse en caso necesario por esta sin mayores complicaciones.

De nuevo tenemos en el diseño una red jerárquica por ser la más cómoda y eficiente, es bastante similar a una red mediana pero con una capa menos de swiches ,es decir, quedarían dos capas de swiches Catalys2960 conectados a un router de la serie 1941 en forma de árbol reservando en el swich conectado al router un puerto de conexión para una posible conexión de respaldo.

Esto daría como resultado una topología en árbol 24*25 que se muestra simplificada en la siguiente figura:

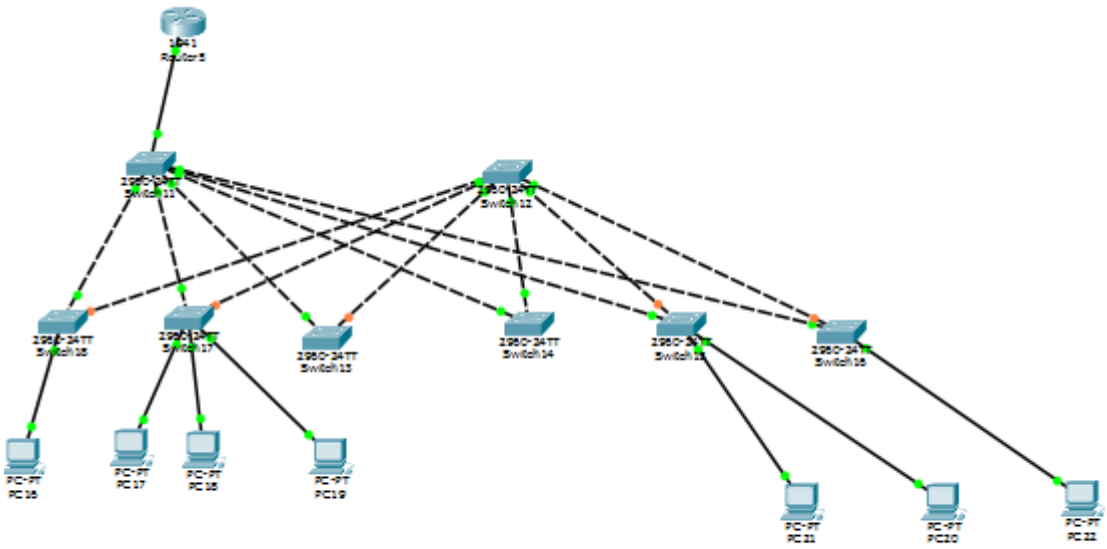

Ilustración 13: Maqueta de sede pequeña.

3.4 Configuración de OSPFv3

Se ha decidido configurar todo con ospfv3 puesto que el resto de protocolos planteados o no escalaban bien o eran propietarios lo que haría que el diseño fuera menos genérico y más complicado.

Para configurar este protocolo en la red se ha de hacer en los router involucrados y se tiene que seguir los siguientes pasos:

1. Habilitar el enrutamiento de unidifusión IPv6: ipv6 unicast-routing.
2. Configurar las direcciones locales de enlace.
3. Configurar un ID de router de 32 bits en el modos de configuración de router OSPFv3 mediante el comando router –id id.
4. Configurar parámetros opcionales de enrutamiento como el ajuste de ancho de banda de referencia.
5. Configurar los parámetros específicos de las interfaces OSPFv3, como el ajuste de ancho de banda de interfaz
6. Habilitar el enrutamiento IPv6 con el comando ipv6 ospf área.

Los siguientes comandos habilitan ospf en el router :(los comandos precedidos por! Son comentarios)

```
enable
configure terminal
!asignamos un nombre identificativo al router
hostname r1
! Habilitamos el enrutamiento de unidifusión
ipv6 unicast-routing
¡configuramos la dirección ipv6 de la interfaz de salida del router ascia nuestra red.
interface GigabitEthernet0/0
ipv6 address aaaa:aaaa:aaaa:0000:0000::1/64
```

no shutdown

ipv6 router ospf 10

router-id 1.1.3.1

interface gigabitEthernet0/0

bandwidth 1000000

! Añadimos el router al área 0

ipv6 ospf 10 area 0

En cuanto a la configuración de los otros dos router para tener configurado ospf en ambos solo se ha de cambiar la dirección IP por la correspondiente a cada uno de ellos perteneciente a su propia red, quedando:

Red mediana:

!asignamos un nombre identificativo al router

hostname r1

! Habilitamos el enrutamiento de unidifusión

ipv6 unicast-routing

¡configuramos la dirección ipv6 de la interfaz de salida del router ascia nuestra red.

interface GigabitEthernet0/0

ipv6 address aaaa:aaaa:aaaa:0001:0000::1/64

no shutdown

ipv6 router ospf 10

router-id 1.1.3.1

interface gigabitEthernet0/0

bandwidth 1000000

! Añadimos el router al área 0

ipv6 ospf 10 area 0

Red pequeña:

!asignamos un nombre identificativo al router

hostname r1

! Habilitamos el enrutamiento de unidifusión

ipv6 unicast-routing

¡configuramos la dirección ipv6 de la interfaz de salida del router ascia nuestra red.

interface GigabitEthernet0/0

ipv6 address aaaa:aaaa:aaaa:0002:0000::1/64

no shutdown

ipv6 router ospf 10

router-id 1.1.3.1

interface gigabitEthernet0/0

bandwidth 1000000

! Añadimos el router al área 0

ipv6 ospf 10 area 0

3.5 Configuración de DHCPv6

Como se explica en el apartado teórico, existen 3 tipos de configuración para una red en cuanto a DHCPv6, y puesto que se tiene 3 redes, se configura cada una de ellas con uno de estos adecuando cada tipo a la red que mejor lo asimila.

3.5.1 Sede central: DHCPv6 con memoria de estado.

Esta opción requiere que el cliente obtenga toda la información de direccionamiento y se configure un servidor DHCPv6 con memoria de estado, el cual guarda información sobre las IP otorgadas.

Se ha elegido esta opción para la red más grande puesto que al tener una alta tasa de usuarios evitamos que se generen IP repetidas que podría suceder con las otras opciones (aunque hay mecanismos que lo autocorrigen), aparte de esto esta opción es más segura puesto que mantienes un mejor control de la red y en la sede central es necesaria mayor seguridad.[8]

Los pasos para esta configuración serian

1. Habilitar el enrutamiento IPv6

Esto se puede hacer en el paso anterior a añadir ospfv6 que también lo necesita, DHCPv6 no lo necesita explícitamente pero como necesita enviar mensajes ICMPv6 RA es necesario implícitamente.

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

2. Configurar el conjunto de direcciones DHCPv6

El comando ipv6 dhcp pool nombre-del-conjunto-de-direcciones crea un conjunto de direcciones y pone al router en el modo de configuración de DHCPv6, el cual se identifica mediante el indicativo Router (config-dhcpv6) #:

```
Router (config)# ipv6 dhcp pool piscinasedecentral
```

3. Configurar los parámetros del conjunto de direcciones

Con DHCPv6 con memoria de estado, el servidor DHCPv6 debe asignar todos los parámetros de direccionamiento y de configuración. El comando address prefijo/longitud se usa

para indicar que el servido asigna el conjunto de direcciones. La opción lifetime específica, en segundos, el tiempo de arrendamiento valido y el preferido.

También suele proporcionar la dirección del servidor DNS y el nombre del dominio

Router (config-dhcpv6)# addres aaaa:aaaa:aaaa:0000:1000::/63 lifetime infinite

Router (config-dhcpv6)#dn-server aaaa:aaaa:aaaa:0000:0000::100/64

Router (config-dhcpv6)# ejemplo.com

Nótese que en la piscina de direcciones disponibles hemos reducido el rango de un /64 a un /63 para poder disponer de esas direcciones iniciales de nuestra red como direcciones estáticas, ósea, puestas por el personal de la red a diferentes maquinas como pueden ser los router, así como servidores y otras dispositivos los cuales las necesitan.

4. Comandos de interfaz

El comando de interfaz ipv6 dhcp server nombre-conjunto-direcciones asocia el conjunto de direcciones de DHCPv6 a la interfaz. El router responde a las solicitudes DHC&v6 sin memoria de estado recibidas en esta interfaz con la información contenida en el conjunto de direcciones. El indicador M se tiene que cambiar de 0 a 1 mediante el comando de interfaz ipv6 nd managed-config-flag. Esto informa al dispositivo de que no debe utilizar SLAAC y que debe obtener los datos de direccionamiento IPv6 y todos los demás parámetros de configuración del servidor DHCPv6 con memoria de estado:

Router (config)# interface gigabitEthernet0/0

Router (config)# dhcp server piscinasedesental

Router (config)# ipv6 nd managed-config-flag

La configuración hasta este punto de este router quedaría:

hostname r1

ipv6 unicast-routing

```
ipv6 dhcp pool piscinasedecentral
address prefix aaaa:aaaa:aaaa:0000:1000::/63 lifetime infinite
dns-server aaaa:aaaa:aaaa:0000:0000::100/64
domain-name ejemplo.com

ipv6 router ospf 10
router-id 1.1.1.1
interface gigabitEthernet0/0
bandwidth 1000000
ipv6 ospf 10 area 0


interface GigabitEthernet0/0
ipv6 unicast-routing
interface GigabitEthernet0/0

!description enlace principal a red troncal
ipv6 address aaaa:aaaa:aaaa:0000:1000:1/64
ipv6 dhcp server piscinasedecentral
!cambiar el indicador M de 0 a 1 para indicar DHCPv6 con estado
ipv6 nd managed-config-flag
ipv6 dhcp server piscinasedecentral
no shutdown
```

3.5.2 Sede mediana: DHCPv6 sin memoria de estado.

Esta opción informa al cliente de que tiene que se debe utilizar la información contenida en el mensaje RA relativa al direccionamiento, pero además hay disponibles parámetros de configuración adicionales en un servidor DHCPv6

Los pasos siguientes serían los de configuración en este modo:

1. Habilitar el enrutamiento IPv6

Para habilitar este se necesita el comando ipv6 unicast-routing visto anteriormente por los mimos motivos que en DHCPv6 con memoria de estado, es decir para trasmitir el mensaje RA.

Router (config)# ipv6 unicast-routing

2.Configurar un conjunto de direcciones DHCPv6

Este paso es igual que en la configuración de DHCPv6 con memoria de estado quedando los comandos:

Router (config)# ipv6 dhcp pool IPv6-r3

Router (config-dhcpv6)#:

3. Configuración de los parámetros del conjunto de direcciones:

Dentro del mensaje RA el cliente ya ha obtenido la información referente tanto a la Gateway predeterminada como la información necesaria para crear una dirección IPv6 de unidifusión global. Sin embargo, el servidor DHCPv6 sin memoria de estado se puede configurar para proporcionar otra información que no puede haber sido incluida en el mensaje RA, como, por ejemplo, la dirección del servidor DNS y el nombre del dominio:

Router (config-dhcpv6)# dns-server aaaa:aaaa:aaaa::100/64

Router (config-dhcpv6)# domain-name ejemplo.com

4. Configuración del interfaz de DHCPv6

El comando del modo de configuración de interfaz ipv6 dhcp server IPv6-r3 asocia el conjunto de direcciones DHCPv6 a la interfaz. El router responde a las solicitudes de DHCPv6

en esa interfaz con la información contenida en el conjunto de direcciones. Hay que modificar el valor del indicador O de 0 a 1 con el comando ipv6 nd other-config-flag- los mensajes Ra en esta interfaz indican que hay disponible información adicional procedente de un servidor DHCPv6 sin memoria de estado:

```
Router (config) # interface GigabitEthernet0/0
Router (config-if) # ipv6 dhcp server IPv6-r3
Router (config-if) # ipv6 nd other-config-flag
```

La configuración de este router hasta este punto quedaría:

```
hostname r3
ipv6 unicast-routing
ipv6 dhcp pool IPV6-r3
dns-server aaaa:aaaa:aaaa::100/64
domain-name ejemplo.com

ipv6 router ospf 10
router-id 1.1.2.1
interface gigabitEthernet0/0
bandwidth 1000000
ipv6 ospf 10 area 0

interface GigabitEthernet0/0
!description enlace principal a red troncal
ipv6 address aaa:aaa:aaa:0001::3/80
ipv6 dhcp server IPV6-r3
!cambiar el indicador o de 0 a 1 para indicar que hay disponible información adicional.

ipv6 nd other-config-flag
```

3.5.3 Sede pequeña: SLAAC.

La configuración dinámica de direcciones sin memoria de estado es un método mediante el cual un dispositivo puede obtener una dirección ipv6 de unidifusión global sin usar los servicios de un servidor DHCPv6. Por su simplicidad se ha elegido como medio de configuración de las sedes pequeñas puesto que pueden llegar a ser muchas y disponer de poco tiempo para configurarlas.

En SLAAC en el mensaje RA tanto el indicador O como el M toman el valor 0.

Indica al cliente que solo debe usar la información proporcionada por RA el cual incluye el prefijo, la longitud de prefijo, el servidor DNS, la MTU y la Gateway predeterminada y no hay más información. Para ello tenemos que poner ambos indicadores a 0

Router (config) # interface GigabitEthernet0/0

Router (config-if) # ipv6 noipv6 nd managed-config-flag

Router (config-if) #no ipv6 nd other-config-flag

La configuración del router implicado quedara de la siguiente forma:

hostname r5

ipv6 unicast-routing

ipv6 router ospf 10

router-id 1.1.3.1

interface gigabitEthernet0/0

bandwidth 1000000

ipv6 ospf 10 area 0

interface GigabitEthernet0/0

!description enlace principal a red troncal

ipv6 address aaaa:aaaa:aaaa:0002:0000::1/96

!cambiar el indicador o de 0 a 0 para indicar que no hay disponible información adicional.

no ipv6 nd managed-config-flag

no ipv6 nd other-config-flag

no shutdown

3.6 Configuración de VLAN en la Sede central.

3.6.1 Swich

En dicha sede se separa en dos grupos a los usuarios por seguridad, en un grupo se deja a la inmensa mayoría de los usuarios agrupándolos en la VLAN2 y en otro grupo se pondrá a los administradores de la red así como los puestos de trabajo que tengan que ver con información sensible de la empresa , los cuales se agruparan en la VLAN1 la cual físicamente se hará coincidir con los puertos que quedan gigabit Ethernet , pero que pueden extenderse a cualquier otro puerto de los swiches fácilmente de ser necesario.

Para conseguir esta distribución se tendrá que crear las dos VLAN y declarar todos los interfaces de los swich intermedios como troncales, luego se colocara cada puerto de los swich finales en su respectiva VLAN.

Para crear una VLAN en un swich se tendrá que seguir la siguiente secuencia:

-Acceder al modo de configuración global:

si#configure terminal

-crear una VLAN con un ID de VLAN valido:

s1 (config)#vlan 2

-especificar el nombre exclusivo del a VLAN en cuestión:

s1 (config-vlan)# name vlancomun

-y salimos del modo :

s1 (config-vlan)# end

-después creamos la segunda vlan

s1 (config)#vlan 1

s1 (config-vlan)#name vlanprivilegiada

s1 (config-vlan)#end

Una vez creadas las dos se tendrá que configurar cada puerto con su respectiva VLAN, en el caso de los swich intermedios es más sencillo puesto que todas sus interfaces son "trunk".

Los pasos serian: acceder al modo interfaz de los puertos específicos, forzar que sea “trunk”, especificar una VLAN nativa para las tramas no etiquetadas, configurar que VLAN están permitidas y salir del modo privilegiado.

s1 (config)# interface range gigabitethernet 0-9/0

s1 (config-if)#switchport mode trunk

s1 (config-if)#swichport native vlan 1

s1 (config-if)#swichport trunk allowed 1,2

s1 (config-if)#end

En cuanto a los router de final del árbol, los que conectan directamente con los usuarios la configuración sería algo distinta, primero se configura los puertos troncales que conectan con la red de swiches:

s1 (config)# interface range gigabitethernet 0/0

s1 (config-if)#switchport mode trunk

s1 (config-if)#swichport native vlan 1

s1 (config-if)#swichport trunk allowed 1,2

s1 (config-if)#end

Luego configuramos los puertos de la red de usuarios a la vlan 1:

s1 (config)# interface range fastethernet 0/0-24

s1 (config-if)#switchport mode access

s1 (config-if)#swichport access vlan 1

s1 (config-if)#end

Después se configuran los puertos de la red pertenecientes a los administradores y puertos de información sensible para la empresa.

s1 (config)# interface range gigabitethernet 1/0

s1 (config-if)#switchport mode access

s1 (config-if)#swichport access vlan 2

s1 (config-if)#end

De esta forma se tendrá dos tipos de configuración para swich, una para intermedio y otra para los finales de la red. Que habría que aplicar a cada uno.

3.6.2 Router (router-on-a-stich).

Para configurar adecuadamente el router en este modo de configuración se ha de configurar como si se usara la configuración tradicional puerto a puerto pero creando subinterfaces y encapsulándolos:

```
!creamos la subinterfaz
interface g0/0.10
!encapsulamos el trafico
encapsulation dot1q 10
!le asignamos direccion IP y mascara de subred.
ipv6 address aaaa:aaaa:aaaa:0000:1000:1/64
```

Y se repite esto para todas las interfaces que se quieran asignar, tantas como VLAN distintas se tengan.

En nuestro caso la configuración del router general quedaría de la siguiente forma:

```
hostname r1
ipv6 unicast-routing
ipv6 dhcp pool piscinasedecentral
address prefix aaaa:aaaa:aaaa:0000:1000::/63 lifetime infinite
dns-server aaaa:aaaa:aaaa:0000:0000::100/64
domain-name ejemplo.com
ipv6 dhcp pool piscinasedecentral2
address prefix aaaa:aaaa:aaaa:0000:2000::/63 lifetime infinite
dns-server aaaa:aaaa:aaaa:0000:0000::100/64
domain-name ejemplo.com
```

```
ipv6 router ospf 10
router-id 1.1.1.1
interface gigabitEthernet0/0
bandwidth 1000000
ipv6 ospf 10 area 0


interface GigabitEthernet0/0
ipv6 unicast-routing

interface GigabitEthernet0/0.1
!description enlace principal a red troncal
ipv6 address aaaa:aaaa:aaaa:0000:1000:1/64
ipv6 dhcp server piscinasedecentral
!cambiar el indicador M de 0 a 1 para indicar DHCPv6 con estado
ipv6 nd managed-config-flag
ipv6 dhcp server piscinasedecentral
no shutdown
interface GigabitEthernet0/0.2
!description enlace principal a red troncal
ipv6 address aaaa:aaaa:aaaa:0000:2000:1/64
ipv6 dhcp server piscinasedecentral
!cambiar el indicador M de 0 a 1 para indicar DHCPv6 con estado
ipv6 nd managed-config-flag
ipv6 dhcp server piscinasedecentral
no shutdown
```

3.7 VPN

3.7.1 Conexión VPN mediante túnel IPSec.

En la práctica, la implementación de IPSec como protocolo de VPN no es muy fácil de configurar. Requiere a priori un entendimiento muy detallado por parte del ingeniero de la dificultad técnica de este protocolo que, de por sí, es complejo.

Una VPN IPSec requiere del establecimiento de dos túneles. El primero llamado IKE Phase 1 ("Internet Key Exchange" Fase 1) que es utilizado para que los routers se comuniquen directamente entre ellos. Este túnel no es utilizado para el envío de paquetes IP de los usuarios, sino más bien, para el intercambio información de control. Para que el túnel IKE Phase 1 pueda establecerse con éxito, ambos routers deben de estar de acuerdo en las siguientes variables:

Hash algorithm

Encryption algorithm

Diffie-Hellman DH group

Authentication method

Lifetime

Después que ambos routers agotan con éxito la primera fase del IPSec — IKE Phase 1 —, sí y solo sí se establece la segunda fase — IKE Phase 2 — donde se establece el túnel por donde viaja la información de los usuarios de manera encriptada.

Entonces teniendo como trasfondo la información anterior, se ha de configurar una VPN Site to Site entre dos routers Cisco utilizando IPSec. Para hacer el proceso de configuración un poco más sencillo, se divide el proceso de configuración en dos etapas: ISAKMP 1; ISAKMP 2 tanto para R1 como para R5. A los túneles IKE también se les llama ISAKMP.

Con este proceso se configuran ambos router y se crea una VPN entre la sede pequeña y la central. Proceso que sería fácil duplicar para nuevas conexiones con otras sedes.

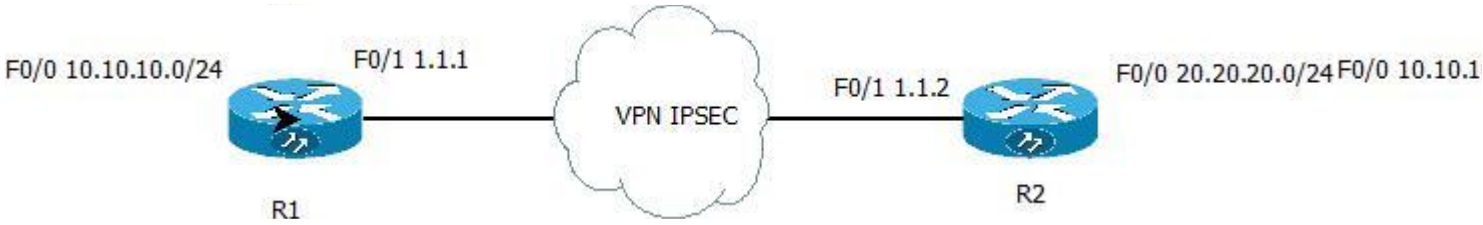

Ilustración 14: Ejemplo de túnel IPSec

se comienza con la configuración de R1.

IKE ISAKMP Phase 1

Paso 1: configuración de ISAKMP Policy.

R1 (config)#crypto isakmp policy 1

R1 (config-isakmp)#encr 3des

R1 (config-isakmp)#hash md5

R1 (config-isakmp)#authentication pre-share

R1 (config-isakmp)#group 2

R1 (config-isakmp)#lietime 86400

Paso 2: definir la contraseña a utilizar entre los R1 y R5 como pre-share key.

R1 (config)#crypto isakmp key Insertarcontraseña address 1.1.1.1

Paso 3: configuración de ACL

R1 (config)# ip Access-list extended VPN-TRAFFIC

R1 (config-ext-nacl)# permit ip ipv6 address aaaa:aaaa:aaaa:0000:1000:1/64

IKE ISAKMP Phase 2

Pasó 4: configurando IPSec.

R1 (config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

Paso 5: configuración de CRYPTO MAP

R1 (config)# crypto map CMAP 10 ipsec-isakmp

R1 (config-crypto-map)#set peer 1.1.1.1

R1 (config-crypto-map)#set transform-set TS

R1 (config-crypto-map)#match address VPN-TRAFFIC

Paso 6: aplicando Crypto MAP a una interface pública

R1 (config)# interface Fastethernet 0/1

R1 (config-if)#crypto map CMAP

El mismo procedimiento de configuración que aplicamos a R1 lo hacemos en R5 con ciertas modificaciones en cuanto a las direcciones IP.

Vamos a comenzar con la configuración de R5.

IKE ISAKMP Phase 1

Paso 1: configuración de ISAKMP Policy.

R5 (config)#crypto isakmp policy 1

R5 (config-isakmp)#encr 3des

R5 (config-isakmp)#hash md5

R5 (config-isakmp)#authentication pre-share

R5 (config-isakmp)#group 2

R5 (config-isakmp)#lietime 86400

Paso 2: definir la contraseña a utilizar entre los R1 y R5 como pre-share key.

R5 (config)#crypto isakmp key cisco address 1.1.1.1

Paso 3: configuración de ACL

R5 (config)# ip Access-list extended VPN-TRAFFIC

R5 (config-ext-nacl)# permit ip 2003:1973:1608:0001:0200::1/96

IKE ISAKMP Phase 2

Pasó 4: configurando IPSec Transform

R5 (config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

Paso 5: configuración de CRYPTO MAP

R5 (config)# crypto map CMAP 10 ipsec-isakmp

R5 (config-crypto-map)#set peer 1.1.1.1

R5 (config-crypto-map)#set transform-set TS

R5 (config-crypto-map)#match address VPN-TRAFFIC

Paso 6: aplicando Crypto MAP a una interface pública

R5 (config)# interface Fastethernet 0/1

R5 (config-if)#crypto map CMAP

3.7.2 Servidor VPN para uso remoto con L2TP.

Se configura un router cisco como servidor VPN para acceso remoto y que los trabajadores puedan hacerlo desde casa utilizando L2TP e IPSec a través de internet y puedan conectarse a la red privada de la empresa.

A continuación se detalla la configuración paso a paso:

1. habilitar la autentificaron aaa y crear el usuario:

aaa new-model

aaa authentication login default local aaa authentication ppp default local aaa authorization exec default local

user cisco password cisco

!usuario y contraseña quedan definidas como cisco, recomendable cambiarlas.

2. Habilitar VPDN y configurar el grupo VPDN:

vpdn enable ! vpdn-group L2TP ! Default L2TP VPDN group accept-dialin protocol l2tp virtual-template 1 no l2tp tunnel authentication

3. Configurar el método de autenticación utilizando claves pre-compartidas.

crypto isakmp policy 10 encr 3des authentication pre-share group 2 lifetime 3600 crypto isakmp key cisco address ::1/128 no-xauth crypto isakmp keepalive 3600

4. Configurar IPSec

crypto ipsec transform-set ipnetconfig esp-3des esp-sha-hmac mode transport ! crypto dynamic-map ipnetconfig-map 10 set nat demux set transform-set ipnetconfig ! ! crypto map cisco 10 ipsec-isakmp dynamic ipnetconfig-map

interface FastEthernet0/0 ip address aaaa:aaaa:aaaa:0000:0000:1/64 duplex auto speed auto crypto map cisco

5. Crear Vitrual_Template

interface Virtual-Template1 ip unnumbered FastEthernet0/0 peer default ip address pool poolipnetconfig ppp encrypt mppe 40 ppp authentication ms-chap-v2

6. Crear la piscina de direcciones IP para asignar a los usuarios del servicio.

ipv6 dhcp pool poolipnetconfig

address prefix aaaa:aaaa:aaaa:0000:2000::/63 lifetime infinite

Capítulo 4. Resultados del trabajo, conclusiones y propuesta de trabajo futuro.

En este proyecto se ha desarrollado el caso del diseño de una red genérica, modular, escalable y sencilla para una empresa cualquiera. Esta empresa un tamaño, topología y número de usuarios genérico por lo que se ha tenido que definir varios tipos de sedes así como la conexión entre ellas. Se han definido tres escenarios diferentes de diferentes tamaño y prestaciones: Sedes grandes con altas prestaciones en cuanto al número de usuarios así como una topología extensa en cuanto a terreno físico, sedes medianas con una cantidad de usuarios menor y menores necesidades y sedes pequeñas que podrían corresponder incluso con una pequeña sucursal u oficina.. Además, se ha todos los equipos involucrados en todas las redes de forma que puedan ser ampliadas o reducidas con facilidad, así como duplicadas si hubiera barias del mismo tamaño. Se ha optado por equipamiento Cisco por el amplio rango de hardware que ofrece, en su mayoría con posibilidad de obtener routers modulares y poder construir el dispositivo a medida, además del eficaz y consolidado funcionamiento para el tipo de redes que el cliente necesita como por la disponibilidad de su herramienta de simulación PaketTracer la cual posibilita la comprobación del correcto funcionamiento de lo configurado sin necesidad de montar la red físicamente.

.

Finalmente, como línea futura de la propuesta actual se puede ampliar la seguridad de la red(añadiendo dispositivos IPs o IDs para monitorizar el tráfico, firewall, zonas desmilitarizadas, protocolos de gestión de contraseñas….), tanto ampliando servidores dedicados para algunos de los diferentes procesos descargando de esta forma algo de trabajo de los router, también puede utilizarse el modelo diseñado para la red de alguna empresa, añadir puntos de conexión wifi y configurarlos con la consecuente seguridad, añadir QoS a la red e implementar algún sistemas de evaluación de las prestaciones de la misma.

4.1 Bibliografía

[1] http://web.archive.org/web/http://nro.net/media/less-than-10-percent-ipv4-addresses-remain-unallocated.html [Online] Agosto 2016.

[2] http://personales.upv.es/rmartin/TcpIp/cap03s02.html [Online] Junio 2016.

[3] http://ipv6.com/ [Online] Junio 2016.

[4] http://livre.g6.asso.fr/index.php/Protocolo_DHCPv6 [Online] Junio 2016.

[5] http://eltallerdelbit.com/eigrp/ [Online] Junio 2016.

[6] http://ipv6friday.org/blog/2011/12/dhcpv6/ [Online] Julio 2016.

[7] https://es.wikipedia.org/wiki/IPv6#Multicast [Online] Junio 2016.

[8] https://learningnetwork.cisco.com/thread/86214 [Online] Agosto 2016.

[9] https://supportforums.cisco.com/discussion/11372061/ipv6-dhcpv6-different-subnets [Online] Agosto 2016.

[10] http://www.ciscopress.com/articles/article.asp?p=2154680 [Online] Julio 2016.

[11] http://theosnews.com/2013/03/15409/ [Online] Agosto 2016.

[12] http://www.fiuba6662.com.ar/6648/presentaciones/tordillo/Informe-htm-Tordillo/L2TP.htm [Online] Julio 2016.

[13] https://rita.udistrital.edu.co/images/pdf/5OSPFv3.pdf [Online] Agosto 2016.

[14] http://es.ccm.net/contents/286-vlan-redes-virtuales [Online] Junio 2016.

[15] https://tools.ietf.org/html/rfc2661#section-1.0 [Online] Junio 2016.

[16] Cisco Press. “Curso CCNA R&S Modulo1. Introducción a las redes” Pearson education S.A 2014

[17] Cisco Press. “Curso CCNA R&S Modulo2. Fundamentos de enrutamiento y conmutación.” Pearson education S.A 2014

[18] Cisco Press. “Curso CCNA R&S Modulo3.Escalado de redes” Pearson education S.A 2014

[19] Cisco Press. “Curso CCNA R&S Modulo4.interconexion de redes” Pearson education S.A 2014