RESUMEN

PROPUESTA DE MIGRACIÓN DEL PROTOCOLO DE COMUNICACIÓN EN LA UNIVERSIDAD ADVENTISTA DE CHILE

por

Rodrigo Leiva Díaz

Asesor principal: Carlos Hernández Rentería

RESUMEN DE TESIS DE MAESTRÍA

Universidad de Montemorelos

Facultad de Ingeniería y Tecnología

Título: PROPUESTA DE MIGRACIÓN DEL PROTOCOLO DE COMUNICACIÓN EN LA UNIVERSIDAD ADVENTISTA DE CHILE

Nombre del investigador: Rodrigo Leiva Díaz

Nombre y título del asesor principal: Carlos Hernández Rentería, Maestría en Teleinformática

Fecha de terminación: noviembre de 2020

Problema

El protocolo de direccionamiento utilizado en el campus de la Universidad Adventista de Chile es IPV4. Se observa que la mayoría de los equipos de networking instalados, son compatibles con el protocolo IPV6. La institución tiene que migrar, dentro de los siguientes años, de IPV4 a IPV6. La Universidad Adventista de Chile no posee una metodología de migración y solución de problemas durante el proceso de transición al protocolo IPV6.

Método

El desarrollo de este proyecto se basa en etapas definidas que abarcan, primero, el análisis bibliográfico y del estado del arte, la investigación de las normas internacionales que dicta el IETF (Internet Engineering Task Force) y que desarrollan las RFC para el desarrollo de internet a nivel mundial. Segundo, la evaluación de las metodologías de migración existentes con sus ventajas y desventajas, el análisis del estado actual de la red analizada para el presente trabajo, el análisis del hardware existente, las configuraciones de los equipos en simulador y el análisis de los resultados. Tercero, el análisis del hardware actual de la red en la UnACh. Cuarto, el análisis de la situación de software que se utiliza en los diferentes departamentos para determinar que el cambio de protocolos no afecta su funcionamiento. Quinto, la simulación en software de la nueva configuración para la migración propuesta, y sexto, el análisis de los resultados.

Conclusiones

Al concluir este proyecto se pretende lograr la anticipación a eventos de cambio venideros en el ámbito de las tecnologías, y así, reducir los problemas con los que se afrontarán los administradores TI de las instituciones, como es el caso de la migración en la Universidad Adventista de Chile, que tiene que migrar del protocolo de internet IPv4 a IPv6. Planificar y simular escenarios con el software Packet Tracer ayuda a implementar los cambios de manera ordenada, respondiendo en forma eficiente al cambio tecnológico.

Universidad de Montemorelos

Facultad de Ingeniería y Tecnología

PROPUESTA DE MIGRACIÓN DEL PROTOCOLO DE COMUNICACIÓN EN LA UNIVERSIDAD ADVENTISTA DE CHILE

Tesis
presentada en cumplimiento parcial
de los requisitos para el grado de
Maestría en Ciencias Computacionales

por

Rodrigo Leiva Díaz

Noviembre de 2020

PROPUESTA DE MIGRACIÓN DEL PROTOCOLO DE COMUNICACIÓN EN LA UNIVERSIDAD ADVENTISTA DE CHILE

Proyecto

presentado en cumplimiento parcial de
los requisitos para el grado de
Maestría en Ciencias
Computacionales

por

Rodrigo Enrique Leiva Díaz

APROBADO POR LA COMISIÓN:

Mtro. Carlos Hernández Rentería Asesor principal	Mtro. Andrés Carballo Mendoza Asesor externo
Mtro. Saulo Hernández Osoria Miembro	Dr. Ramón Andrés Díaz Valladares Director de Posgrado e Investigación
Mtro. Daniel Gutiérrez Colorado Miembro	Fecha de aprobación 3 de diciembre de 2020

DEDICATORIA

A Dios, por su gran amor por mí y porque siempre está a mi lado, ayudándome y dándome fuerzas cuando lo necesito.

A mi esposa Verónica, por sus oraciones y paciencia en este desafío y siempre me apoya en todo.

A mis hijos Ismael, Silvana y Gabriel, en los cuales me veo reflejado. Sigo orando por ellos para que continúen adelante y se mantengan en los caminos del Señor.

A mis amigos, quienes me apoyaron y animaron en mis estudios, por brindarme su atención y aprecio.

En forma no menos especial, a todos mis mentores, quienes formaron parte de mi proyecto educativo en la Universidad de Montemorelos.

TABLA DE CONTENIDO

LISTA DE FIGURAS vii

LISTA DE TABLAS ix

RECONOCIMIENTOS x

Capítulo

I. DIMENSIÓN DEL PROBLEMA 1

Antecedentes 1
Estado actual 4
Planteamiento del problema 4
Justificación 4
Objetivos 5
Objetivo general 5
Objetivos específicos 5
Limitaciones 6
Delimitaciones 6
Metodología 6
Antecedentes generales 7
Marco filosófico. 8
La creación y el orden de Dios. 8
La oración, protocolo para hablar con Dios. 10
Definición de términos. 12

II. MARCO TEÓRICO 13

Introducción 13
Reseña histórica 13
Conceptos generales de IPv6 15
Unicast 17
Formato EUI64 18
Global unicast 19
Link-Local 19
Loopback 20
Unspecified 20
Unique Local 20
Embedded IPv4 20
Multicast 21

Direcciones de multicast reservadas 23
Anycast Addresses 24
Mejoras en el direccionamiento IPv6 24
Cabecera IPv6 simplificada 24
Proceso de migración IPv6 en Chile y México 27
Mecanismos de transición IPv4-IPv6 29
Comparativa de mecanismos de transición 30
Dual-Stack o doble pila IPv4 e IPv6 31
Tablas de enrutamiento en modo Dual-Stack 32
Configuración de direccionamiento en modo Dual-Stack 33
Solicitud de direccionamiento 33
Operación SLAAC en IPv6 34
DHCPv6 35
IPsec y seguridad en IPv6 43
¿Qué es IPsec? 43
Cabecera de autenticación AH 44
Cifrado seguro de la carga útil (Encapsulating Security Payload ESP) 44
Formato del paquete ESP 44
Algoritmos de Hash 47
Protocolo de intercambio de claves en internet (IKE, ISAKMP) 47
Ventajas y desventajas de los mecanismos de migración 48
Ventajas 49
Respuesta a cobertura inalámbrica 49
Desventajas 52
Resumen 52
Machine learning en IPv6 y blockchain 54
BlockChain 54

III. MARCO METODOLÓGICO 56

Planificación de la red para transición IPv4/IPv6 56
Metodología del proyecto 56
Situación actual de la red UnACh 59
Arquitectura de red data center UnACh 60
Arquitectura de red Lan UnACh 60
Servidores DHCP IPv4 actual 62
Diagrama general red UnACh 62
Planeamiento del direccionamiento IPv6 64
Configuración de escenarios 65
Configuración de red con SLAAC 65
Configuración VLan 66
Asignación de puertos 72
Configuración SLAAC 76

DHCPv6 sin estado, dual stack 77
DHCPv6 con estado, dual stack 84
DNSv6 88
Resultados Dual Stack 90
Configuración del router 92
Mediciones 95
Vlan 240 oficinas 95
Vlan 181 impresoras 96
Vlan 200 wifi oficinas 97

DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES 99

Introducción 99
Discusión 101
Conclusiones 102
Recomendaciones 102

REFERENCIAS….. 104

LISTA DE FIGURAS

1. Equipos wifi en el 2009 para el campus de la UnACh 8
2. Equipos wifi en el 2016 para el campus de la UnACh 9
3. Tipos de direcciones IPv6 (Graziani, 2017) 16
4. Estructura de las direcciones unicast globales (Graziani, 2017). 19
5. Cabecera IPv6 (Jiménez, Puerto y Payá, 2017).. 25
6. IPv6 campo de etiqueta de flujo (Graziani, 2017). 26
7. Páginas web nativas con IPv6 en Chile 27
8. Páginas web nativas con IPv6 en México 28
9. Estadística de usuarios que acceden a Google por IPv6 29
10. Resumen de técnicas de transición IPv4/IPv6 30
11. Enrutamiento en una red Dual-Stack 32
12. Configuración automática de direcciones IPv6 sin estado 34
13. Proceso de solicitud a DCHPv6 sin estado 36
14. Operación servidor DHCPv6 con estado 40
15. Implementación de NAT-PT 42
16. Cabecera ESP (Kent y Atkinson, 1998). 45
17. Rendimiento 50
18. Promedio de retardo punto a punto 50
19. Jitter promedio 51
20. Proporción de paquetes de entregados 51

21. Situación de conectividad del IPv6, ANUIES (Franco Reboreda y Rodríguez Elizondo, 2017) 59

22. Configuración esquemática de red data center UnACh 61

23. Topología lógica de la red de UnACh 64

24. Red data center a FAIN..... 66

25. Configuración automática IPv6 78

26. Configuración automática del host 80

27. Escenario Dual Stack..... 81

28. Configuración PC RedA en Dual Stack..... 83

29. Configuración PC RedB en Dual Stack..... 83

30. Topología utilizada para pruebas..... 84

31. Entradas para obtener DNS inverso de un nombre de dominio..... 89

32. Dual Stack Vlan 181 impresoras..... 91

33. Dual Stack Vlan 200 wifi..... 91

34. Dual Stack Vlan 240 oficinas..... 92

35. Resultados ping IPv6 Vlan 240 95

36. Resultados ping IPv4 Vlan 240 96

37. Resultados ping IPv6 Vlan 181 96

38. Resultados ping IPv4 Vlan 181 97

39. Resultados ping IPv6 Vlan 200 97

40. Resultados ping IPv4 Vlan 200 98

LISTA DE TABLAS

1. Analogía de la semana de la creación con el modelo de referencia OSI 10
2. Tipo de dirección IPv6 que se identifica por los bits de orden superior de la dirección 17
3. Resumen de los tres mecanismos de transición 53
4. Comparación de protocolos de transición IPv4/IPv6 60
5. Asignación de VLAn´s en la UnACh 63
6. Direccionamiento del pool´s DHPv4 85

RECONOCIMIENTOS

A Dios, por las oportunidades que ha provisto en mi vida y por guiarme continuamente en sus caminos en este proceso de perfeccionamiento profesional.

A mis profesores y maestros de la UM, Saulo Hernández, Daniel Gutiérrez, Carlos Hernández y German Harvey Alférez, quienes me dieron el conocimiento mientras estudiaba y se convirtieron en amigos en este proceso.

Un reconocimiento especial al profesor Ismael Castillo, quien por su gestión pude realizar los estudios de maestría. Gracias por su apoyo y que Dios le bendiga en su labor siempre.

CAPÍTULO I

DIMENSIÓN DEL PROBLEMA

Antecedentes

El protocolo de internet (IP, por su siglas en inglés) fue creado en la década de los ´70 para soportar las comunicaciones de la Agencia de Proyectos de Investigación Avanzada (ARPANET, por sus siglas en inglés) que fue la antecesora y precursora de lo que se conoce hoy como internet. La RFC 791 define la versión cuatro de este protocolo, siendo este el principal de los protocolos TCP/IP (Boronat Seguí y Montagud Climent, 2013).

La tecnología de redes de datos avanza a velocidades que no se pensaban en el pasado, es por esto que el sistema de direccionamiento IPV4 (internet protocolo versión 4) que se utiliza hoy en la mayoría de las instituciones, tienen que migrar en un futuro cercano a un sistema basado en IPV6 (internet protocolo versión 6). Las redes, para que se comporten eficiente, deben ser planificadas para que cumplan con los estándares más rigurosos de escalabilidad y disponibilidad (El Khadiri, Labouidya, Elkamoun e Hilal, 2018).

La Universidad Adventista de Chile (UnACh), actualmente está operando mediante un direccionamiento que utiliza el protocolo de internet versión 4 (IPV4), con un direccionamiento en subredes asignadas mediante un servidor Dynamic Host Configuration Protocol (DHCP, por su siglas en inglés). Este direccionamiento es sin clase y

cada subred está creada pensando en el grupo de trabajo al que corresponde cada usuario, por ejemplo, las facultades, los departamentos y la gerencia, entre otros.

Para realizar un mejoramiento de las comunicaciones y la seguridad de los datos, además de otras características importantes, se requiere migrar la red al protocolo de internet versión 6 (IPv6). El presente trabajo determina las opciones de configuración que deben seguirse para realizar la migración y las formas en que se puede llevar a cabo, sin que esto afecte a los usuarios y a los sistemas que funcionan actualmente, como los sistemas financieros y el software con licencias de red, entre otros sistemas instalados.

El avance en conectividad permite cada vez más dispositivos conectados a internet, siendo posible que prácticamente cualquier dispositivo esté en línea, llamado Internet of Things (IOT, internet de las cosas). Entre los dispositivos más comunes se encuentran computadores, teléfonos celulares, alarmas, cámaras IP, equipos domésticos, electrodomésticos, SmartTV, teléfonos IP, controler logic program (PCL, controladores lógicos programables) utilizados en la industria, sensores y muchos dispositivos datalogger que requieren conectividad para subir los datos recolectados. Estos últimos son lo que hoy están siendo introducidos en diferentes áreas, desde la industria hasta la agricultura de precisión (Franco Reboreda y Rodríguez Elizondo, 2017).

En cuanto a la definición de IoT, hoy en día no se tiene un concepto que contenga todas las características de esta tecnología emergente (Flores, Berón, Riesco y Rangel Henriques, 2018), que permita comprenderla del todo. Su interconexión a internet, permite aprovechar de mejor forma el rendimiento que cada equipo podría haber tenido por separado. Por ejemplo, una base de datos que es alimentada de forma local en

cada computador provoca inconsistencias entre la correlación de datos almacenados en un equipo y otro. Esto se puede solucionar instalando un equipo principal o servidor con una sola base de datos, siendo consultada por los usuarios desde distintos equipos conectados a la misma red. En otras palabras, es compartir recursos y la meta es que todos los programas, el equipo y, en especial, los datos estén disponibles para cualquier persona en la red, sin importar la ubicación física del recurso o del usuario. Otra visión más actual es que esta misma base de datos este distribuida en todos los nodos de la red, esto permite una mayor seguridad, dado que, si ataca la base de datos, tendrían que ser vulnerados todos los nodos de la red. Este sistema se conoce como Blockchain, que hoy en día está siendo utilizado en muchos campos, pero sus inicios fueron en las criptomonedas, descentralizando el almacenamiento de los datos (Jiang, Liu, Ren y Zhang, 2018).

Otro ejemplo, pero ya de una red corporativa y de uso popular, es el de un grupo de empleados de oficina que comparten un mismo servicio de impresión. Una impresora en red de alto volumen es más económica, veloz y fácil de mantener que una extensa colección de impresoras individuales, aunque, probablemente, compartir información sea aún más importante que compartir recursos físicos como impresoras y sistemas de respaldo. En los últimos años, el avance tecnológico ha permitido que las empresas e instituciones digitalicen toda su información, siendo el papel solo un respaldo a menor escala de ésta, lo que se ve reflejado en un aumento en la eficiencia de los procesos administrativos y productivos. Por ejemplo, el pago en línea de cuentas y facturas a través de bancos, la lectura del catálogo de libros, la base de datos con registro del personal que trabaja en las instituciones, controlando su asistencia y pago

de sueldos, el control de notas y asistencia de alumnos en las instituciones de educación y la venta y el stock de inventario en un negocio.

Estado actual

Cuando se realizó el diseño de internet se pensó en entregar números IP registrados, con los cuales cada organización tenía sus propias numeraciones y esto permitía que no se duplica. Esto funcionó, pero con el rápido crecimiento de internet en los años ‘90, quedó claro que las direcciones se agotaron rápidamente, situación que sucedió en el año 2011 en Latinoamérica, donde el Latin American Network Information Center (LANIC) entregó el último segmento disponible de IPv4. En lo particular de la red en la UnACh, cada subred tiene un campo de 24 bit para identificar el campo de red y ocho bit para el campo de host, lo que deja gran cantidad de direcciones que no se utilizan dentro de la red.

Planteamiento del problema

El protocolo de direccionamiento utilizado en el campus de la UnACh es IPV4. Se observa que la mayoría de los equipos de networking instalados son compatibles con el protocolo IPV6. La institución tiene que migrar, dentro de los siguientes años, de IPV4 a IPV6. La UnACh no posee una metodología de migración y solución de problemas durante el proceso de transición al protocolo IPV6.

Justificación

El agotamiento de direcciones en redes de datos ha preocupado desde los años ‘80. Por ello, se creó un grupo de trabajo en la Internet Engineering Task Force (IETF),

que desarrolló lo nuevo de internet llamado protocolo IP de nueva generación (IPng), posteriormente llamado IPV6. No solo este protocolo implica el aumento de direcciones, sino que también seguridad y otras mejoras. Las últimas direcciones IPV4 en Latinoamérica, se entregaron oficialmente el 3 de febrero de 2011, de acuerdo al anuncio de LANIC.

Objetivos

A continuación se presentan los objetivos del estudio:

Objetivo general

El objetivo principal del estudio fue diseñar una propuesta que permita a la UnACh, migrar del protocolo de comunicaciones de internet IPV4 a IPV6, entregando un diseño de la propuesta.

Objetivos específicos

Los objetivos específicos del estudio fueron los siguientes:

1. Analizar la situación actual de las redes en la UnACh.
2. Entregar hoja de ruta que permita llevar a cabo el cambio de protocolo de forma transparente para el usuario.
3. Determinar los beneficios al usar el nuevo protocolo IPV6.
4. Realizar configuraciones en diferentes escenarios.
5. Documentar configuración Dual Stack.
6. Realizar simulación en software Cisco Packet Tracer.
7. Crear Vlan con configuración Dual Stack.

8. Obtener resultados de conectividad.

Limitaciones

Para fines del presente estudio, se plantearon las siguientes limitaciones:

1. Falta de recursos financieros para la implementación de la propuesta.

2. Falta de recursos para adquirir software de alto costo para implementar la propuesta.

Delimitaciones

Para el presente estudio se fijaron las siguientes delimitaciones:

1. Se desarrolla solo estudio de direccionamiento IP optimizado.

2. Se trabaja con propuesta simulada en software.

3. No se desarrollan sistemas de seguridad en el núcleo de la red.

4. Se utiliza direccionamiento IP distinto al real por motivos de seguridad institucional.

5. Se pretende ingresar a la cobertura de las subredes, excluyendo data center institucional que está ligado a un contrato externo.

Metodología

La metodología que se utilizó está definida por los siguientes pasos: (a) investigación bibliográfica del estado del arte, de IPv6; (b) evaluación de las metodologías y alternativas de migración existentes; (c) investigación del estado de la red en la

UnACh; (d) análisis del hardware que existe y el necesario; (e) análisis de configuración de software que administra la red; (f) análisis de factibilidad, modelo simulado en pakect tracer y (g) análisis de resultados.

Antecedentes generales

En la UnACh se ha complejizado la administración de la red para poder cubrir las demandas de servicios de los funcionarios y los alumnos, lo cual ha llevado a que en el año 2012 el ancho de banda internacional fuera de 12 megabyte (Mb) de un enlace simétrico dedicado. En el año 2014 era de 50 Mb, ya que el anterior no era suficiente para las nuevas exigencias de los usuarios. En el año 2016, el ancho de banda internacional era de 130 Mb. En el 2019, se cuenta con tres enlaces de dos proveedores, siendo el primero con la empresa CLARO con 50-20 Mb, el segundo con la empresa ENTEL mediante microondas de 100-100 Mb y, el tercero también con la empresa ENTEL, pero en fibra óptica 100-100 Mb, simétrico.

Otro ejemplo, en junio de 2009 (ver Figura 1) existían 18 equipos de wifi instalados en el campus con los cuales se distribuía internet a los alumnos y funcionarios, con una capacidad máxima de 360 usuarios. A partir del año 2016 hay 54 equipos instalados de wifi con una capacidad máxima para 2160 usuarios, como se aprecia en la Figura 2; sin contar el aumento de los computadores fijos, las impresoras de red, el equipo de videoconferencia y los servidores.

El crecimiento sostenido de la red wifi en el tiempo se observa en las Figuras 1 y 2, pero solo teniendo en cuenta las necesidades de movilidad de los usuarios. Al ana-

lizar los sistemas operativos que coexisten en la institución, se pueden encontrar equipos con DOS, Windows XP, Windows 7 al 10, Linux en varias distribuciones e impresoras de red que solo soportan el protocolo IPv4, además de sistemas de licencia para software en red (licencia servidor, SPSS) que, al utilizar un puerto, podría tener problemas de conectividad si el cliente es IPv4 y el servidor nativo es IPv6. Dadas estas razones, la migración a un protocolo en la versión 6 en su totalidad debe ser cuidadosamente estudiada, para no perjudicar estos sistemas que aún se encuentran en operaciones en la red institucional.

Marco filosófico

La creación y el orden de Dios

EL relato de la creación en el libro de Génesis describe cómo Dios ordenó los días de la creación lo que permitió completar el plan trazado por la divinidad. Cada día tenía su propósito específico y, sin el anterior, el siguiente no pudo ser llevado a cabo, es decir, el orden que se sigue no puede ser alterado. De igual forma sucede en el modelo de referencia OSI, que ordena el proceso de comunicación en capas, cada una con sus protocolos y tareas específicas que interactúan con las capas superiores e inferiores.

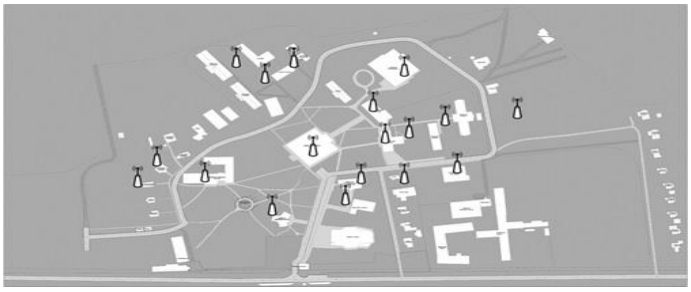


Figura 1. Equipos wifi en el 2009 para el campus de la UnACh.

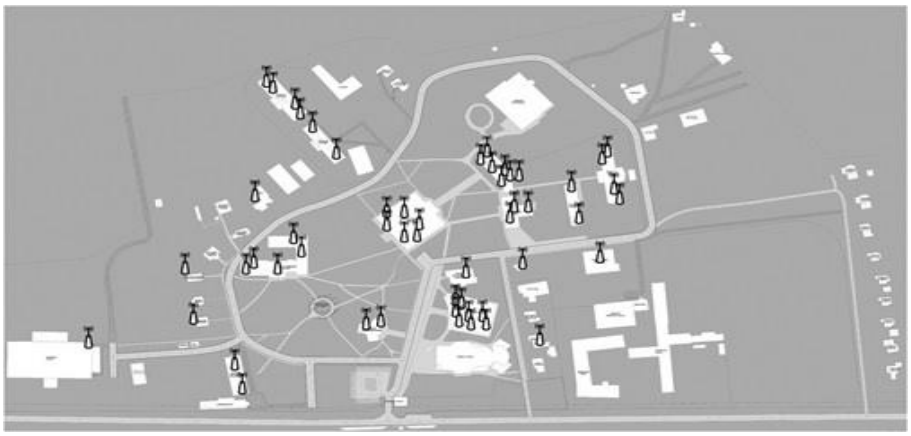


Figura 2. Equipos wifi en el 2016 para el campus de la UnACh.

El acto de creación de un día crea las condiciones para que el siguiente pueda ser ejecutado. Existe un orden perfecto que culmina con la creación del hombre el sexto día y con el descanso del sábado en el día séptimo. De igual manera, el sistema de referencia OSI, dividido en siete capas, como analogía a los días de la creación, comienza con la capa física y termina completando la visión total de la información enviada en la capa de aplicación, lo cual muestra al usuario final el resultado de lo realizado. Así mismo, Dios contempló y vio lo realizado el día séptimo (ver Tabla 1).

Cada día, se ejecutó un análisis y el relato bíblico así lo manifiesta: “Y vio Dios que era bueno en gran manera” (Génesis 1:4, 10, 12, 18, 21, 25 y 31). Lo mismo sucede en el modelo indicado, donde cada capa tiene su propio control que se manifiesta en el encabezamiento que coloca a la propia capa, ordenando así las PDU de cada capa, desde los datos provenientes de las capas superiores, segmentos, paquete, trama y bit que luego son enviados a través de la red.

Tabla 1

Analogía de la semana de la creación con el modelo de referencia OSI

Día de la semana de la creación	Capa del modelo OSI
Día siete: descanso y observación de lo creado	Capa 7: aplicación
Día seis: animales y la humanidad	Capa 6: presentación
Día cinco: mar criaturas incluyendo los peces y la aves.	Capa 5: sesión
día cuatro: estrellas, sol y luna	Capa 4: transporte
día tres: tierra y vegetación	Capa 3: red
Día dos: cielo y mar, separa las aguas	Capa 2: enlace de datos
Día uno: noche y día	Capa 1: física

La oración, protocolo para hablar con Dios

La oración es el medio que el hombre tiene para comunicarse con Dios, su Creador. La pregunta es: ¿cómo se ora y por qué? En Daniel 9:3 el profeta plantea: “Volví mi rostro a Dios, el Señor, buscándole en oración y ruego, en ayuno, ropas ásperas y ceniza”. De este texto se desprende que la actitud al orar es de humillar el espíritu, en sumisión y ruego. Esta es la forma correcta de orar a nuestro Señor. Se debe tener en claro qué es la oración y la forma en que se debe realizar. Contestando a esta pregunta, en 1 Samuel 1:1-18 se encuentra el relato de la oración de Ana por un hijo. En el relato ella está orando en el templo por ese hijo deseado y viendo el sacerdote Elí que solo movía sus labios, pensó que estaba ebria y yendo a donde ella estaba le pidió: “Digiere tu vino” (v. 14). Ana le contestó con una hermosa frase: “No, señor mío;

soy una mujer atribulada de espíritu. No he bebido vino ni sidra, si no que he derramado mi alma delante de Jehová". Este relato puede servir como una analogía con los protocolos de comunicación que el host debe ejecutar para comunicarse a través de internet. La oración, si no se realiza con fe y derramando el alma ante Dios, no es eficaz. De igual modo, en los protocolos de comunicación se deben cumplir requerimientos, es decir, un orden que permita la comunicación entre dos hosts. También se puede hacer referencia a que la oración en sí es una comunicación punto a punto, un enlace con el Creador. En redes de comunicación y datos, primero se tiene que establecer el circuito virtual para luego enviar el mensaje. Lo mismo ocurre con la oración, como lo plantea el profeta Daniel: volver el rostro a Jehová. Esto da paso a que el ser humano derrame su alma ante su Señor.

La oración permite tener una relación con Dios, la cual es un medio de recarga espiritual, desde donde se bajan los datos correctos que provienen del cielo y pasan a ser grabados en la mente y el corazón humano. De la oración, se obtienen los siguientes beneficios:

1. Da fortaleza al ser humano: vigoriza el alma y es un escudo para vencer en este mundo y enfrentar la adversidad.

2. Da energía: vitaliza el espíritu para pasar el día en largas jornadas de trabajo y aun en la enfermedad. Da fortaleza para lograr las cosas para las cuales el ser humano no tiene capacidad.

3. Da confianza y trae paz: elimina las preocupaciones y afanes. Gracias a la oración, el ser humano puede entregar las cargas delante de Dios y esperar en Él.

Toda la creación está conectada al ser humano. Por eso el profeta Jeremías dice: “Clama a mí, y te responderé; y te revelaré cosas grandes e inaccesibles que tú no conoces.” (Jeremías 33:3, RVA). La oración y su poder para conectar al ser humano con el inconmensurable y vasto Dios es una vislumbre de lo que las redes, a muy pequeña escala, hacen al conectar el mundo entero y el conocimiento que se genera a diario en la web.

Definición de términos

Para contextualizar al lector en los términos técnicos que se utilizan en este trabajo, se presenta una definición de términos más utilizados.

Dual Stack: protocolo de transición de dos estados que permite trabajar con los protocolos IPv4/IPv6 en una red.

Host: es un equipo que se puede conectar a internet traducido como anfitrión. Antes se definía a los computadores u ordenadores, pero hoy se ha extendido su uso a cualquier dispositivo que se conecta a la red.

Internet protocol o protocolo de internet: se trata del estándar utilizado para enviar y recibir información de una red.

Protocolo de control de transmisión o Control Protocol Transfer: es un protocolo orientado a la conexión, permitiendo el control de errores y el estado de la conexión.

Protocolo de datagramas de usuario: es un protocolo sin conexión utilizando redes de datos. Ofrece pocos servicios de corrección de errores, permitiendo mayor rapidez en las comunicaciones.

CAPÍTULO II

MARCO TÉORICO

Introducción

En este capítulo se detallan los fundamentos teóricos que son la base del estudio. Estos fundamentos dejan en claro ciertos conceptos básicos como los principios del funcionamiento de la tecnología de redes en el protocolo IPV6 y las redes Dual Stack.

Reseña histórica

Los inicios de internet comenzaron con la creación de ARPANET en el año 1969 como parte de una alianza entre el Departamento de Defensa de los Estados Unidos y algunas universidades como la Universidad de California, los Ángeles (UCLA), el Instituto de Investigación de Standford de San Francisco, la Universidad de California y la Universidad de Utah con el fin de compartir información de investigaciones. Primeramente, se interconectan cuatro IMPs (procesadores de la interfaz de mensajes) que estaban instalados en las universidades que participaban del proyecto. En cada una de estas universidades, se interconecta un computador a la naciente red y el envío del primer mensaje se realizó el 29 de octubre de 1969. Rápidamente, frente al éxito del proyecto, este plan creció dando el nacimiento a lo que hoy se conoce como internet (Andrada, 2017). En un principio, el protocolo de control fue el 1822. Este era básico y

permitía el envío de mensajes de un punto a otro entre IPMs. Después, fue reemplazado por el protocolo NCP (Network Control Protocol), porque IPMs no gestiona múltiples conexiones para varias aplicaciones, dentro de una misma máquina, lo que hoy se realiza con la asignación de puertos. En 1983, surgió el protocolo de internet TCP/IP, que llegó a ser el protocolo utilizado hasta el día de hoy. La versión IPv4 con 32 BIT (Jain, Tiwari, Singh y Sharma, 2018), contenía una cantidad de direcciones que para esos momentos era suficiente, pero el rápido crecimiento de la red y la cantidad de host conectados, en forma exponencial, con el paso de los años, produjo el agotamiento del bloque de direcciones IPv4 a nivel mundial .

El agotamiento sufrido por la dirección que utiliza el protocolo de internet IPv4 el 3 de febrero de 2011, entregados por la IANA (Internet Assigned Numbers Authority), al APNIC, de 33 millones de direcciones, tiene para los RIR's (Regional Internet registry) un punto en que no podrán entregar más direcciones de IP's públicas a las instituciones. Por lo tanto, se tendrá que enfrentar la migración al protocolo IPv6. La migración es gradual, pero no tiene retrocesos. A partir de esto ¿qué proceso se tiene que llevar a cabo y que funcionalidades y nuevos usos tiene el usar este nuevo protocolo?. Esta es la pregunta que esta investigación tiene que responder, enfocada a una institución como la UnACh, la cual es el objeto de estudio.

Las direcciones IPv4 se crearon para conectar a 4.294.967.296 millones de dispositivos a la red pública. En su creación, se pensó que esta cantidad de direcciones era suficiente, pero el avance de los dispositivos que se conectan a internet como teléfonos móviles, equipos industriales, Tablet y electrodomésticos, entre otros que requieren de una conexión vía web para supervisar y control de parámetros, ha hecho

que el protocolo IPv4 se agote (Ariganello y Barrientos Sevilla, 2015b). Además, en la actualidad, el internet de las cosas (IoT) ha fomentado que los dispositivos conectados aumenten considerablemente. Permitir que todos estos equipos se conecten a la red ha hecho que IPv4 no se dé abasto y la implementación de la nueva versión IPv6 sea necesaria.

Conceptos generales de IPv6

En este apartado se revisarán los fundamentos del protocolo de direccionamiento IP, versión 6, que es uno de los tópicos más nuevos del área de redes, ya que se trata de un protocolo importante porque viene a reemplazar al actual IP, versión 4. Es importante que se pueda entender paso a paso cómo funciona el protocolo que es un poco más complejo en su estructura respecto al proceso en la versión 4, pero mucho más simple en su configuración. También se ejemplifica cómo se configura siguiendo un ejemplo simple, además se estudian algunos conceptos importantes para formar una primera idea de cómo se diferencia este protocolo respecto a la versión IPv4 y cuáles son sus principales características. La idea de IP, versión 6, no es nueva, nació más o menos a mediados de los años noventa y se envió un primer borrador que se concretó en el RFC1550 y en ese tiempo se llamó IPpng de Nueva Generación (Ariganello y Barrientos Sevilla, 2015b), luego fue actualizado en la RFC2460 y actualizada por la RFC8200 (Deering y Hinden, 2017).

Respecto a la cantidad de direcciones en IP, versión 6, se tienen 128 bits para construir direcciones (ver Figura 3). Las direcciones de IPv6 tiene 128 bits de largo (Ariganello y Barrientos Sevilla, 2015b). En comparación a los 32 bits de longitud de

las direcciones IP, versión 4, y el tener 128 bits en el IP, versión 6, se tienen: 2^2 =340,282,366,920,938,463,463,374,607,431,768,211,456.

Son 340 sextillones de direcciones, hay algunos cálculos que dicen que una próxima versión 7, saldría dentro de los próximos 300 a 400 años. Se prevé, que los dispositivos conectados para el 2020 serán más de 35 billones solo en IoT (Llaneza González, 2018). Ya muchos equipos y sistemas operativos son totalmente compatibles con IPv6, como es Google Android, Apple iOS y Windows Mobile. En el segmento de telefonía celular, todos los equipos trabajan con IPv6 y utilizan una técnica de traducción de protocolo especial al comunicarse con dispositivos solo IPv4.

Los tipos de direcciones IPv6 que fueron definidos en la RFC4291 y actualizados por la RFC7346 (Droms, 2014), (IP version 6, Addressing Architecture), se muestran en la Tabla 2.

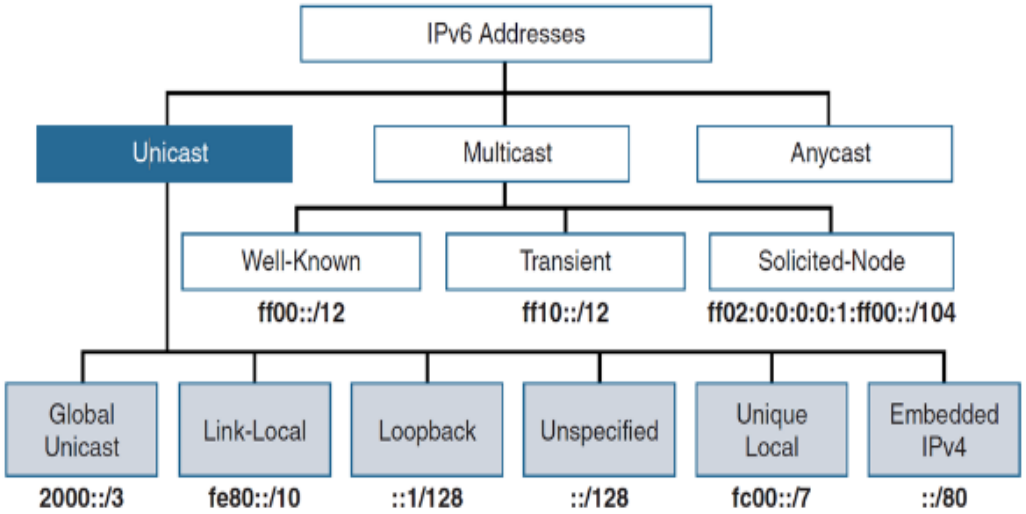


Figura 3. Tipos de direcciones IPv6 (Graziani, 2017).

Tabla 2

Tipo de dirección IPv6 que se identifica por los bits de orden superior de la dirección

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	111111010	FE80::/10
Global Unicast		(everything else)

Unicast

Unicast es una técnica de transmisión de datos donde se envían solamente los datos al nodo más cercano. Las direcciones de este tipo se pueden utilizar con prefijos de longitud de bits de forma arbitraria, de igual manera que se realiza en IPv4 con direcciones sin dominio entre clases (Deering y Hinden, 2017). Existen direcciones Unicast basadas en prefijos de multicast addresses que están definidas por la RFC3306 y actualizada en la RFC7371 (Boucadair y Venaas, 2014).

Hay varios tipos de direcciones unicast en IPv6 que a continuación se mencionan: (a) Unicast global, (b) Site-local unicast, (c) Link-Local Unicast y (d) Global Unicast, como las direcciones IPv6 con direcciones IPv4 incrustadas, que son un tipo especial de estos tipos de direcciones.

Se debe tener presente que, en este tipo de direcciones, a excepción de las que comienzan con el binario 0000, el ID de la interfaz debe tener una longitud de 64 bits y estar construidas en el formato EUI64, de acuerdo lo que establece el RFC4291.

El formato EUI64 está basado en construir el ID de la interfaz utilizando la dirección MAC de la misma.

Formato EUI64

El formato de construcción de una dirección IPv6 utilizando el protocolo EUI64, de acuerdo lo descrito en la RFC4291, es aquel que se establece a partir de la dirección MAC propia que identifica al host (Hinden y Deering, 2006) (Draves, 2003). Si en un router Cisco el comando para configurar la IP Address de la interfaz utilizando este protocolo es el siguiente:

IPv6 address dir ip /64 eui64

Siendo dir ip el número ip asignado a la interface con prefijo de 64 bits. La manera en que se forma esta dirección sigue pasos definidos. Primero, se divide la dirección MAC en dos partes iguales, por ejemplo:

Paso 1. 20-16-B9 48-6F-98

Paso 2. Se agregan 16 bits FFFE en medio de la dirección, quedando de las siguiente forma: 20-16-B9-FF-FE-48-6F-98

Paso 3. Se invierte el séptimo bits del primer bloque que identifica el host, para lo cual se debe transformar el 20 hex, en números binarios. 0010 0000.

El bit marcado con rojo se debe invertir quedando como 1, entonces este bloque queda de la siguiente forma: 0010 0010=22 HEX.

Finalmente, se transforma nuevamente a hexadecimal: 22-16B9-FF-FE48-6F98

Si el prefijo fuera FE80::/64 la dirección final quedaría de la forma siguiente: FE80::2216:B9FF:FE48:6F98/64

De esta forma quedan los 64 bits que identifican a la interfaz, utilizando el protocolo EUI64.

En la siguiente parte, se revisan cada uno de los tipos de direcciones que componen el direccionamiento IPv6, se describe brevemente cuál es su uso y el prefijo asignado a este tipo de dirección.

Global unicast

Las direcciones global unicast, son equivalentes a las direcciones IPv4 globales. Las direcciones GUA (Global Unicast Address) tienen el primer hexteto que comienza con el binario 001 de forma que su rango abarca desde 2000::/3 a 3fff, como se muestra en la Figura 4 (Graziani, 2017).

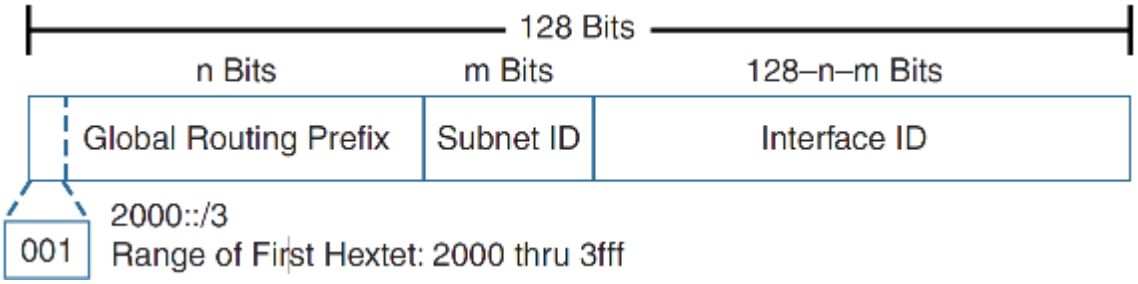


Figura 4. Estructura de las direcciones unicast globales (Graziani, 2017).

Link-Local

Las direcciones link local address son similares a las direcciones privadas en IPv4. Estas pueden trabajar en un ambiente sin conexión a un ISP (proveedor de servicios de internet). Si se requiere conexión externa a internet a través de un ISP, se requiere de NAT (Network address translation), IPv6 se ha resuelto creando las direcciones Link local (Molina Robles, 2015) que tienen la siguiente estructura: 1111111010 es el primer hexteto en binario FE80::/10, siendo la dirección con el prefijo asignado a este bloque.

Loopback

La dirección Loopback (Molina Robles, 2015) es similar a la dirección localhost de IPv4 127.0.0.1. En IPv6 la estructura de esta dirección es: ::1/128.

Unspecified

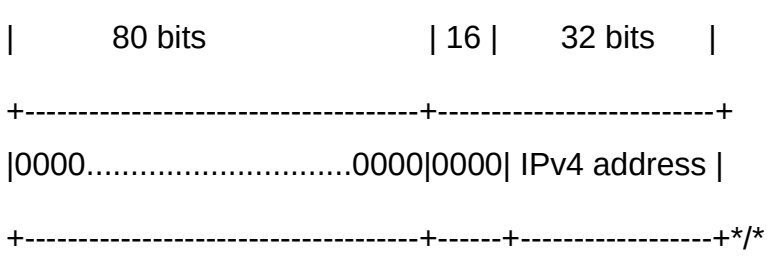
Esta dirección no especificada (Martínez Yelmo y Riaño Vílchez, 2015) se escribe solo con ceros los 128 bits y con un prefijo de igual número de bits. ::/128.

Unique Local

Unique local address son un tipo de direcciones especiales en IPv6. Una particularidad de estas direcciones es que no son enrutables en internet, son privadas, aunque si son enrutables dentro de una organización o dentro de un sistema autónomo (Praptodiyono et al., 2015). Esto no existe en IP, versión 4, aunque existe algo similar a las direcciones unicast link local address, que son aquellas redes APIPA. Ese Rango 169.254.0.0/16 es muy similar a las direcciones link-local address. La estructura de este tipo de direcciones, de acuerdo a la RFC4291, es: FE80::/10.

Embedded IPV4

Este formato de dirección IPv6 compatible con IPv4, se definió en la RFC4291 (Hinden y Deering, 2006) para facilitar el proceso de migración entre ambos protocolos. El formato es el siguiente:



En la actualidad, este método ya se encuentra en desuso, pero en los comienzos de la implementación de IPv6 fue un aporte a la migración. Ahora no está soportado por las nuevas tecnologías.

Multicast

Un concepto importante con IPv6 es que no existe el broadcast, sino que se reemplaza totalmente por multicast. Para realizar una comunicación multicast, se utiliza el rango de direcciones IPv6 FF00: :/8, el cual está reservado para realizar la multidifusión, siendo los primeros ocho bits 1. La razón de esto es bastante simple, el broadcast en una red IP, versión 4, es un tráfico muy poco optimizado porque si la red tiene 65,000 host, cada vez que se envía un mensaje de broadcast, va destinado a 65000 direcciones, incluso pueden ser muchas más. Se utiliza tráfico, recursos de red y ancho de banda para procesar en realidad datos que nunca van a llegar a ningún otro e igual son transmitidos por la red. Entonces, de manera más eficiente en IP, versión 6, se decidió eliminar broadcast y reemplazarlo totalmente por multicast, que es una tecnología que cumple con el mismo propósito. Es decir, transportar un paquete de datos a un grupo de usuarios de una red y ese grupo, por ejemplo, pueden ser todos, pero mucho más optimizado (Hinden y Deering, 2006). Las direcciones de este tipo poseen el siguiente formato:

```
| 8          |  4  |  4  |      112 bits                          |
+-----------+------+-------+----------------------------------------+
|11111111| flgs | scop |      group ID                           |
+-----------+------+-------+----------------------------------------+
```

El binario 11111111 identifica que es una dirección del tipo multicast. El siguiente Nibble FLGS es un Flag que se identifica con el siguiente formato: 0|R|P|T.

Los valores del bit T, P y R son definidos en la RFC3956, los cuales son los siguientes:

1. El flag de orden superior es reservado y debe estar en 0.

2. El T = 0 indica que es una dirección permanente, conocida y asignada por la Internet Assigned Numbers Authority (IANA).

3. El T = 1 indica que no es una dirección permanente ("transient" or "dynamically" assigned).

4. El P = 0 indica una dirección de multidifusión que no se asigna según el prefijo de red (RFC3306).

5. El P = 1 indica una dirección de multidifusión que se asigna en base a un prefijo de red (RFC3306).

6. Si P = 1, T debe establecerse en 1.

7. R = El 1 indica una dirección de multidifusión que incrusta la dirección en el RP (Rendezvous Point, punto de encuentro).

El SCOP es un valor de alcance de multidifusión de cuatro bits que se utiliza para limitar el alcance del grupo de multicast (RFC2373). Los valores son los siguientes: 0. Reserved, 1. Node-local scope, 2. Link-local scope, 3. Unassigned, 4. Unassigned, 5. Site-local scope, 6. Unassigned, 7. Unassigned, 8. Organization-local scope, 9. Unassigned, 10. Unassigned, 11. Unassigned, 12. E global scope y 13. F reserved.

Direcciones de multicast reservadas

EL siguiente grupo de direcciones multicast están reservadas para uso futuro no definido aún y nunca se deben asignar a un grupo multicast, de acuerdo a la RFC4291 (Hinden y Deering, 2006).

La Reserved Multicast Addresses son las siguientes:

FF00:0:0:0:0:0:0:0

FF01:0:0:0:0:0:0:0

FF02:0:0:0:0:0:0:0

FF03:0:0:0:0:0:0:0

FF04:0:0:0:0:0:0:0

FF05:0:0:0:0:0:0:0

FF06:0:0:0:0:0:0:0

FF07:0:0:0:0:0:0:0

FF08:0:0:0:0:0:0:0

FF09:0:0:0:0:0:0:0

FF0A:0:0:0:0:0:0:0

FF0B:0:0:0:0:0:0:0

FF0C:0:0:0:0:0:0:0

FF0D:0:0:0:0:0:0:0

FF0E:0:0:0:0:0:0:0

FF0F:0:0:0:0:0:0:0

Anycast Addresses

Este tipo de direcciones se asigna a más de una interfaz, pero en nodos distintos. El paquete que se envía a esta dirección se dirigirá al nodo más cercano, dependiendo del costo que se le asignó en el momento de configurar el enrutamiento. El formato de esta dirección es:

n bits	128-n bits
subnet prefix	00000000000000

Mejoras en el direccionamiento IPv6

El direccionamiento IPv6 incluye varias mejoras que los diseñadores incorporaron desde el conocimiento empírico que se desarrolló con IPv4.

Cabecera IPv6 simplificada

La cabecera IPv6 está definida por la RFC2460. En la Figura 5, se muestra el encabezado IPv6 que contiene 64 bits de longitud lo que permite un mejor procesamiento por las CPU´s actuales. La ventaja es que las CPU de 64 bits pueden leer una palabra de memoria de 64 bits a la vez (Graziani, 2017).

Cada uno de los campos que tiene el encabezado provienen de la versión anterior, pero se eliminaron varios que ya no serán usados. El significado de cada uno de ellos es el siguiente:

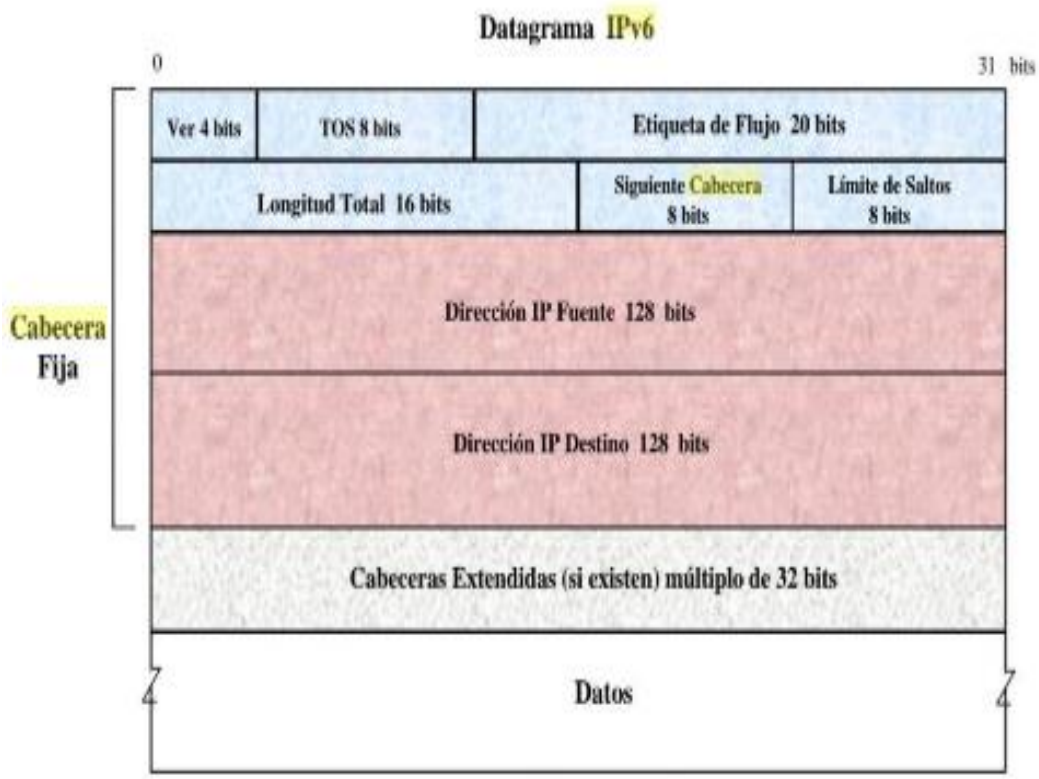


Figura 5. Cabecera IPv6 (Jiménez, Puerto y Payá, 2017).

1. Versión. En este apartado se coloca un 6, en binario 0110.

2. Traffic class. Este campo sirve para determinar el tratamiento que los router realizan al paquete de datos y permite proporcionar características de calidad de servicio QoS. El valor asignado a este campo se puede utilizar para determinar el tratamiento que se le otorgará al paquete y, además, el orden para la transmisión de los mismos.

3. Flow label. Este campo es nuevo en IPv6 y permite etiquetar con un número de secuencia los paquetes enviados desde una fuente a uno o más destinos, como se muestra en la Figura 6, donde el flow label permite un flujo a más de un destino.

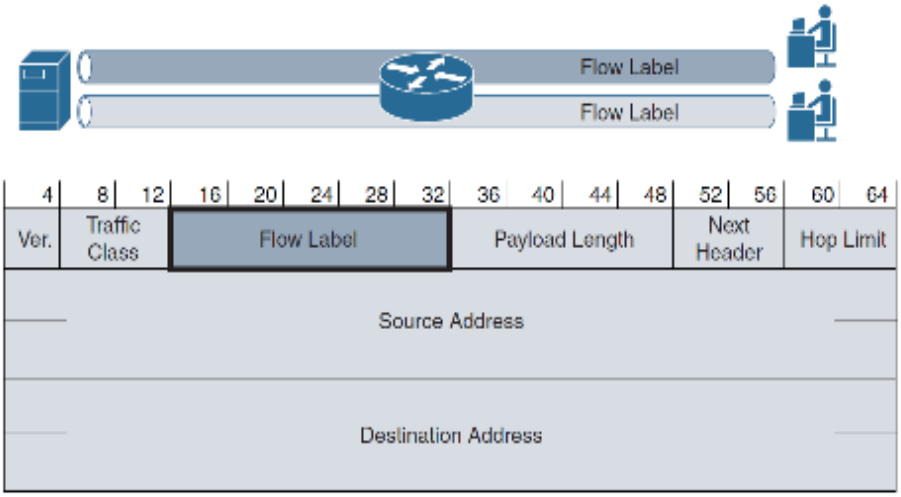


Figura 6. IPv6 campo de etiqueta de flujo (Graziani, 2017).

4. Payload Length field. Este campo es en el cual se indica la longitud de la carga útil en bytes que lleva el paquete luego del encabezado, es decir, el tamaño del contenedor que lleva la porción de datos útiles (Graziani, 2017).

5. Next Header. Este campo especifica el tipo de encabezado esperado después del encabezado principal del paquete IPv6 (Bautista et al., 2008). Este campo es similar en IPv4. Esta indicación permite saber si es un paquete TCP, UDP o ICMP6, entre otros. La IANA otorga números para cada uno de estos protocolos (IANA, 2017). Por ejemplo, si fuere TCP el número que llevaría será 6, UDP 17 e ICMP 1.

6. Hope limit. Este campo reemplaza al campo TTL de IPv4. Cada router va descontando una al valor de este campo, al llegar a cero se envía un ICMP al host emisor avisando que el paquete no llegó a su destino (Ariganello y Barrientos Sevilla, 2015a).

Proceso de migración IPv6 en Chile y México

El proceso de migración a una red mundial completamente trabajando en IPv6 es gradual y depende no solo de las implementaciones técnicas, sino que, además, de las políticas públicas de los estados. En el caso del presente trabajo, se analizan los niveles de implementación para Chile y México. Los estudios de Cisco, en su página de investigación y penetración de IPv6 (Cisco Systems, 2019) que monitorea la adopción a nivel mundial de IPv6, se observan las estadísticas de las páginas web habilitadas con el nuevo protocolo, entre otros datos. Para Chile, el porcentaje de sitios web habilitados para IPv6 es de un 57.1%, como se aprecia en la Figura 7, lo que indica un avance paulatino de implementación de esta nueva tecnología.

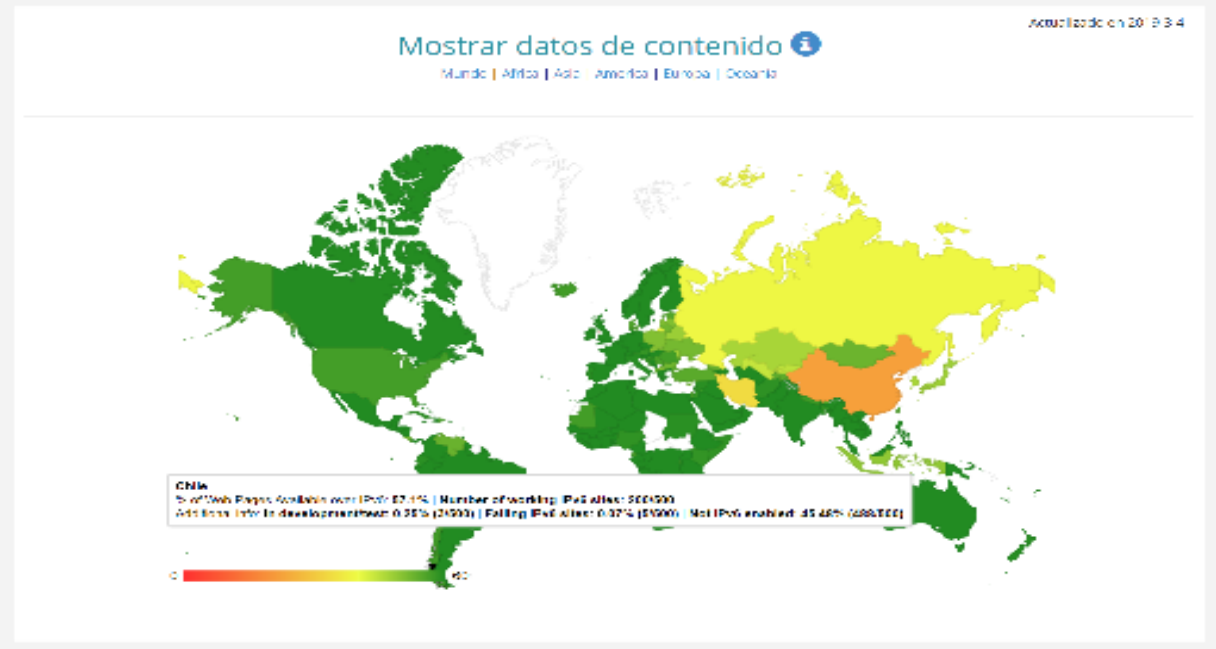


Figura 7. Páginas web nativas con IPv6 en Chile.

La penetración de IPv6 en México (ver Figura 8), en el número de sitios nativos de IPv6 es del 70.6%, más alta que lo que tiene Chile con solo el 57.1% de páginas web habilitadas para IPv6. Estas estadísticas facilitan la comprensión de cómo las páginas web pronto estarán siendo habilitadas en un 100% con IPv6. Lo que después viene es el proceso en que se eliminará el acceso desde redes IPv4, el cual es un proceso gradual, pero que no tiene vuelta atrás. Entonces las preguntas que surgen son: ¿qué sucederá con los hosts nativos en IPv4? ¿podrán acceder a las páginas web nativas en IPv6?

Para que ambos protocolos puedan tener comunicación entre sí, se requiere de técnicas y mecanismos como túneles, traducciones o Dual Stack que se verán en el siguiente apartado con más detalles.

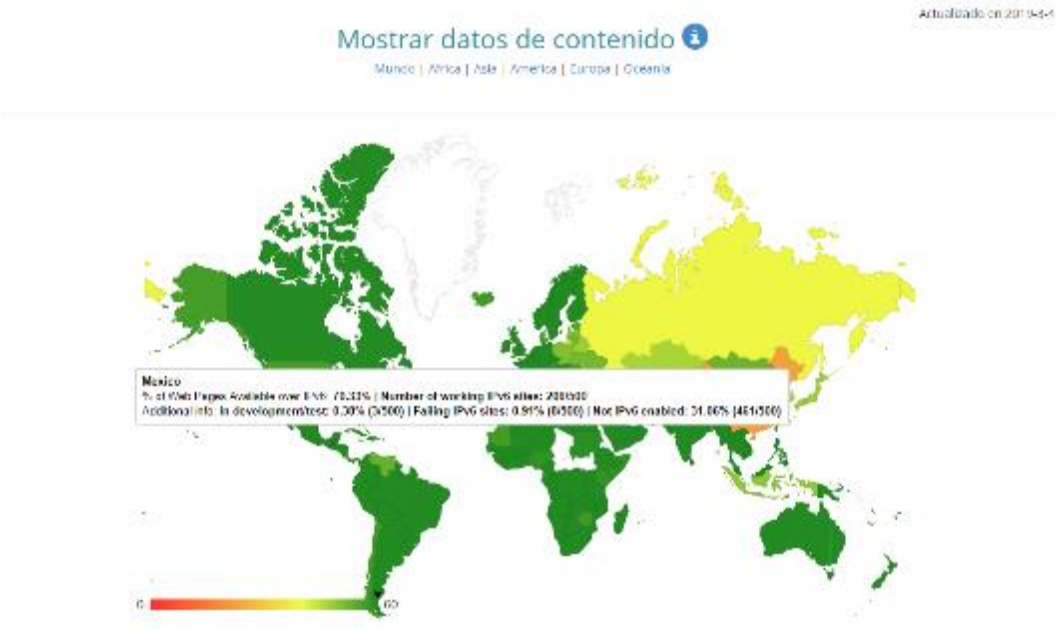


Figura 8. Páginas web nativas con IPv6 en México.

Mecanismos de transición IPv4-IPv6

A nivel mundial, la adopción de IPv6 ha tenido una curva exponencial a partir del 2011, año en que se agotó el direccionamiento IPv4. Desde esa fecha, se comenzaron a utilizar diferentes mecanismos que permiten la comunicación entre ambos protocolos. En la Figura 9, se muestra la estadística de adopción que Google realiza a nivel mundial (Google IPv6, 2017) en la cual se observa cómo a junio de 2019, los accesos desde host nativos IPv6 es de un 28,68% y que los mecanismos de traducción son prácticamente 0%, dado que en ellos siempre implica mayor procesamiento por parte de los router, e incluso, de algunos que no pueden procesar dado que son incompatibles con la nueva tecnología, lo que implica una inversión económica importante.

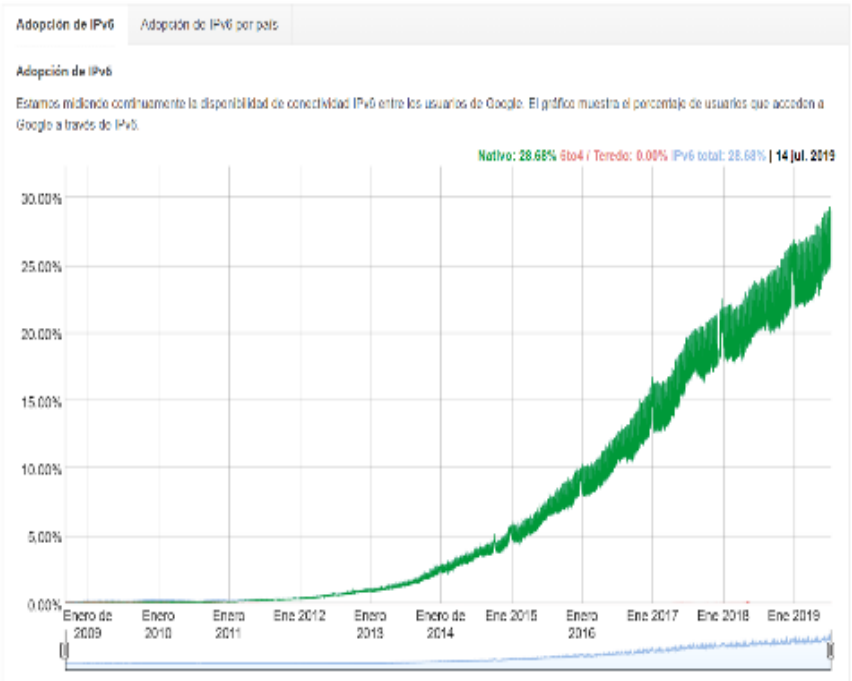


Figura 9. Estadística de usuarios que acceden a Google por IPv6.

Existen variados mecanismos para realizar la migración de forma paulatina entre los nodos IPv4/Ipv6. Cada uno de ellos busca solucionar temas puntuales y a su vez mejorar el rendimiento de la red, sin que el usuario final detecte dicho proceso. En la Figura 10, se aprecia un resumen de los principales mecanismos.

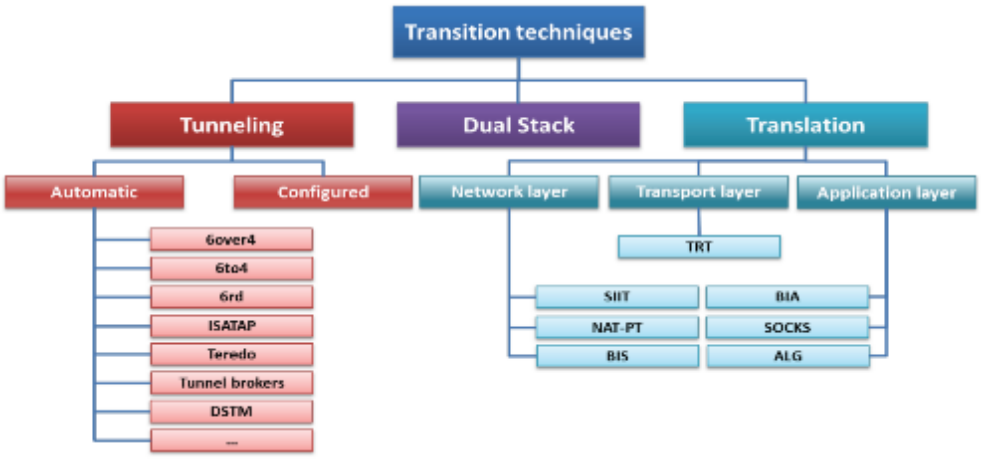


Figura 10. Resumen de técnicas de transición IPv4/IPv6.

Comparativa de mecanismos de transición

Primero se requiere entender cuando se comenzó a trabajar IETF en el desarrollo de los mecanismos de transición y coexistencia, es decir, cuál era el concepto. El concepto básicamente era que IPv6 se iba a desplegar antes de que se agotara IPv4 y con ese planteamiento es con el que el IETF diseñó los primeros mecanismos de transición. Por tanto, lógicamente, el objetivo inicial era mantener simultáneamente IPv4 e IPv6 y hoy en día es una situación totalmente diferente. Por eso, en primer momento, el mecanismo de transición obvio era la doble pila, mantener las redes IPv4 tal como están hoy en día en algunos casos con direcciones IPv4 públicas. Por ejemplo, en las

redes del IPS o los usuarios corporativos y en otro caso los usuarios residenciales con Nat y direcciones privadas en el interior de las redes, pero en todo caso la idea es tener direcciones IPv6 globales en toda la red. El primer mecanismo de los tres que existen es la doble pila o Dual Stack, como se le conoce en inglés. La recomendación hoy en día sigue siendo en las redes locales mantener doble pila, es decir, en ningún caso se va a deshabilitar IPv4, si se pretende que las aplicaciones actuales que todavía no soportan IPv6 sigan funcionando (Palet, 2016).

Dual-Stack o doble pila IPv4 e IPv6

El protocolo de doble pila o Dual-Stack permite implementar, de forma simple, las soluciones de interoperabilidad entre IPv4/IPv6 (Boronat Seguí y Montagud Climent, 2013). Esta solución está desarrollada en la RFC4213 (Nordmark y Gilligan, 2005), en la cual el ITF propone una solución para la operabilidad entre ambos protocolos. En Dual-Stack, los nodos que operan bajo esta modalidad poseerán dos direcciones IP, una para cada versión del protocolo. Esta es la forma más sencilla en que los nodos IPv6 sigan siendo compatibles con los nodos IPv4. Estos nodos pueden operar directamente con los nodos IPv4 usando dichos paquetes, al igual que con los nodos IPv6, utilizando paquetes IPv6.

Se debe considerar que, si bien los nodos soportan ambos protocolos, estos se pueden deshabilitar por razones operativas. Un Stack, IPv4 o IPv6, posee direcciones IP asignadas, pero no está definido qué aplicaciones están disponibles en cada Stack. En consecuencia, los nodos IPv4/IPv6 tienen tres modos de operación (Nordmark y Gilligan, 2005). Estos son los siguientes:

1. El Stack IPv4 habilitado y el Stack IPv6 deshabilitado.

2. El Stack IPv6 habilitado y le Stack IPv4 deshabilitado.

3. Ambos Stack deshabilitados.

Para el primer modo de operación, el nodo funcionará solo como nodo IPv4 nativo. Para el segundo modo de operación, el nodo funcionará solo como nodo IPv6 nativo. En el tercer modo de operación, el nodo funcionará para ambos Stack IPv4/IPv6, siendo este modo el que trabaja el modo Dual-Stack.

Tablas de enrutamiento en modo Dual-Stack

El problema de implementar el modo Dual-Stack en una red es que se requieren tablas de enrutamiento y procesos de enrutamiento separados para cada Stack (Boronat Seguí y Montagud Climent, 2013). Por lo tanto, el router de la red Dual-Stack (ver Figura 11) debe llevar ambas tablas, esto implica un mayor costo de procesamiento del mismo y, además, requiere que el router sea compatible con ambos protocolos.

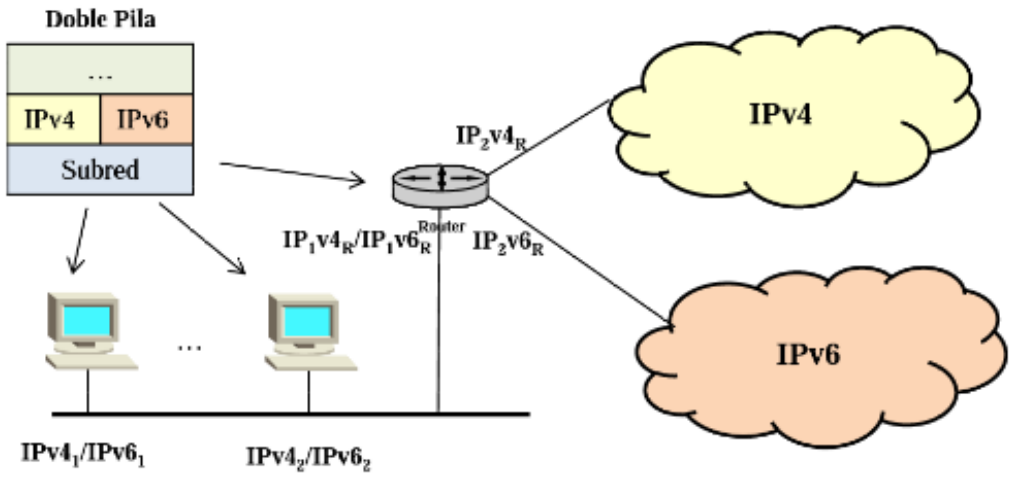


Figura 11. Enrutamiento en una red Dual-Stack.

Configuración de direccionamiento en modo Dual-Stack

Los nodos en modo Dual-Stack admiten ambos tipos de direcciones (IPv4/IPv6), pero la forma de configuración es distinta para nodos IPv4. Los mecanismos para adquirir una dirección son principalmente dos, el primero es configurar manualmente, de forma estática por el administrador, una dirección IPv4 en la Nic del nodo. Este método es largo y tiene sus desventajas dado que solo es eficiente en redes pequeñas. En el caso de grandes redes, la administración se torna compleja. El segundo método se adquiere desde un servidor DHCP (Dynamic Host Configuration Protocol, configuración dinámica de host) descrito por la RFC2131. Para nodos IPv6 también existen dos métodos, el primero es autoconfiguración automática (Thomson, Narten y Jinmei, 2007) de direcciones sin estado (SLAAC) que está descrita en la RFC4862, como se observa en la Figura 2 y no se requiere de un servidor para obtener el direccionamiento. El segundo es utilizando un servidor DHCPv6 descrito en la RFC3315, su operación es similar a DHCP en lPv4. En términos generales, donde un host a través de un puerto UDP que al realizar la solicitud de direccionamiento el host el puerto UDP es el 546 y la respuesta desde el servidor es por el puerto UDP 547 (Droms et al., 2003).

Solicitud de direccionamiento

Los hosts en IPv6 tienen dos posibilidades para obtener direccionamiento en una red, el primero es mediante la operación SLAAC (Stateless Address autoconfiguration) y el segundo es mediante un servidor DHCPv6. Este, además, posee dos modos, sin estado y con estado, los cuales se describen a continuación.

Operación SLAAC en IPv6

En modo SLAAC, descrito en la RFC4862, debe estar habilitado para responder las solicitudes de autoconfiguración del host en su red. En este modo no entrega direccionamiento, solo responde que está habilitado para operar con el Stack IPv6. El comando de habilitación en el caso de los router Cisco es:

Router(config)# ipv6 unicast-routing

Con este comando, el router está habilitado y comienza a enviar “mensajes de anuncio del router” (RA) a todos los clientes. Este mensaje permite al host configurar una dirección automática IPv6 sin estado en su MAC address. El router envía el prefijo de la red y su longitud, permitiendo al host crear su propia dirección de unidifusión global como se muestra en la Figura 12.

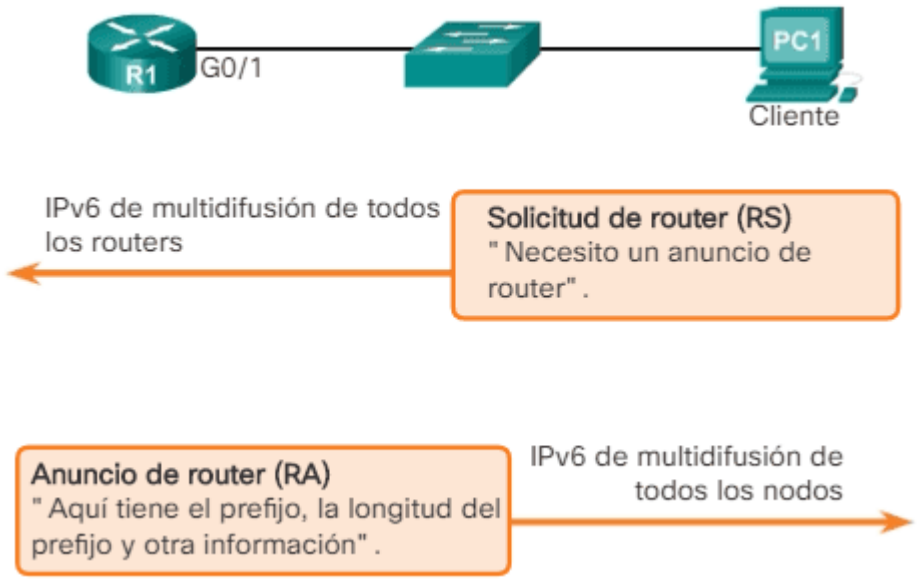


Figura 12. Configuración automática de direcciones IPv6 sin estado.

DHCPv6

El protocolo de configuración dinámica de host versión 6 (DHCPv6), como se le llama en español, funciona de la misma forma que en la DHCPv4 definido en la RFC2131, entregando los parámetros solicitados por un host como por ejemplo, direccionamiento, servidores DNS, proxy, etc., pero no son iguales en su funcionamiento. Se encuentra descrito por la RFC3315 para la v6 mientras que para la v4 está definido por la RFC2131.

DHCPv6 posee dos modos de operación, el primero sin estado y el segundo con estado.

DHCPv6 sin estado

El modo de DHCPv6 sin estado hace referencia a que el servidor no entrega direcciones, solo se limita a entregar los parámetros adicionales que el host solicita, pues este utiliza los mensajes RA para configurar su IPv6 y luego, mediante el aviso del router, solicita los parámetros faltantes al servidor DHCPv6 de la red. Cuando el host solicita mediante un mensaje RS (router solicitud) dirigido a las direcciones de multidifusión de todos los router, FF02::2, este responde con un mensaje RA a las direcciones de multidifusión de todos los nodos, FF02::1, el cual contiene el prefijo de la red y su longitud, al igual que en el modo SLAAC, el host crea su dirección IPv6, configurando de forma aleatoria mediante un IDD o utilizando EUI-64. El paquete de respuesta contiene dos indicadores M y O, ambos tienen el bit en 0 por defecto (modo funcionamiento SLAAC), pero en el caso de DHCPv6 sin estado O se cambia a 1, lo que le indica al host que debe solicitar parámetros adicionales a un servidor DHCPv6

existente en su red. Este indicador se puede configurar en los router CISCO mediante el siguiente comando:

Router(config-if)# ipv6 and other-config-flag

Enseguida el cliente se comunica con el servidor mediante el puerto UDP546, de modo de obtener direcciones del servidor DNSv6 de la red. El servidor responde a la solicitud, entregan los parámetros de configuración solicitados mediante el puerto UDP547, pero no guarda registro de las direcciones del host, esto es a lo que se llama sin estado, porque no guarda ningún registro de las asignaciones que poseen los host clientes en la red. En la Figura 13, se muestra el proceso descrito.

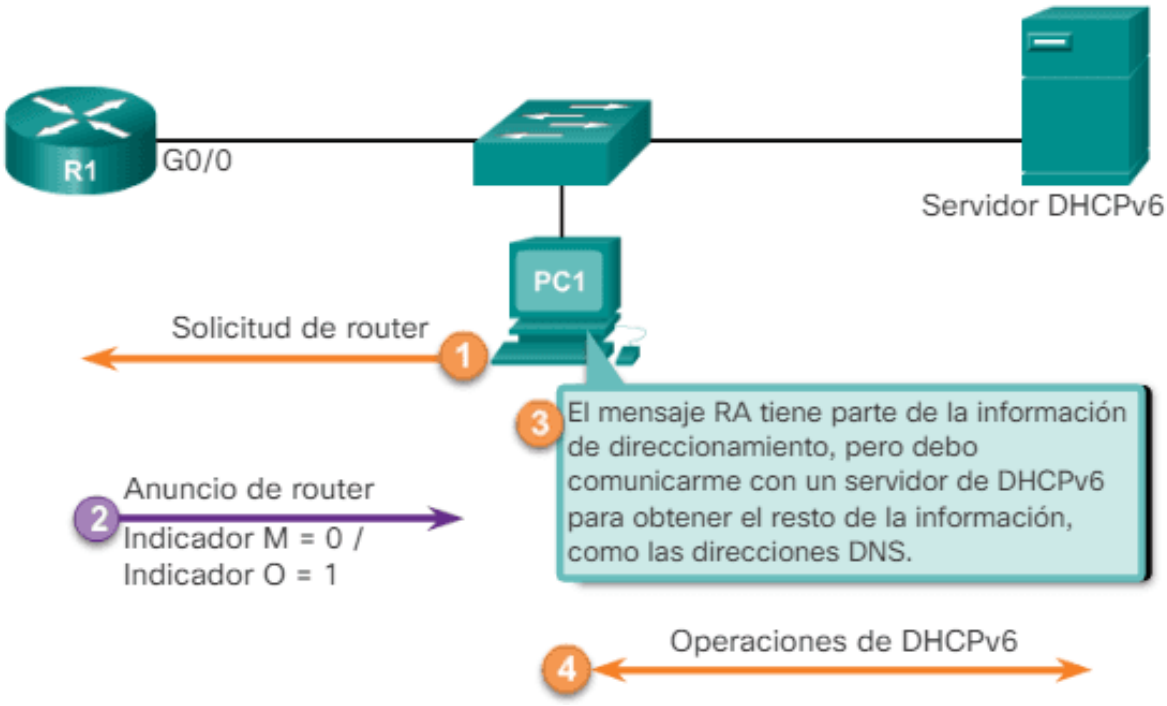


Figura 13. Proceso de solicitud a DCHPv6 sin estado.

DHCPv6 con estado

En este modo de operación el cliente envía una solicitud RS al router de la red, el router envía un mensaje RA (en el caso de los router CISCO envían mensajes RA cada 200 segundos), pero siendo el indicador M = 1, (el indicador O no interviene en este caso si el indicador M está en 1), el host entiende que debe realizar la consulta al servidor DHCPv6 de la red (Walton, 2018).

Para la comunicación entre el host y el servidor, se tienen una serie de mensajes definidos por la RFC3315, los cuales son los siguientes.

1. SOLICIT (1). Un cliente envía un mensaje de solicitud para localizar servidores.

2. ADVERTISE (2). Un servidor envía un mensaje de Publicidad para indicar que está disponible para el servicio DHCP, en respuesta a un mensaje de Solicitud recibido de un cliente.

3. REQUEST (3). Un cliente envía un mensaje de solicitud para solicitar los parámetros de configuración, incluidas las direcciones IP, desde un servidor específico.

4. CONFIRM (4). Un cliente envía un mensaje de confirmación a cualquier servidor disponible para determinar si las direcciones que se le asignaron siguen siendo apropiadas para el enlace al que está conectado el cliente.

5. RENEW (5). Un cliente envía un mensaje de Renovación al servidor que originalmente proporcionó las direcciones y los parámetros de configuración del cliente para extender la vida útil de las direcciones asignadas al cliente y para actualizar otros parámetros de configuración.

6. REBIND (6). Un cliente envía un mensaje de Rebind a cualquier servidor disponible para extender el tiempo de vida de las direcciones asignadas al cliente y para

actualizar otros parámetros de configuración; este mensaje se envía después de que un cliente no recibe respuesta a un mensaje de renovación.

7. REPLY (7). Un servidor envía un mensaje en respuesta que contiene las direcciones asignadas y los parámetros de configuración en respuesta a un mensaje de Solicit, Request, Renew, Rebind message recibido de un cliente. Un servidor envía un mensaje de respuesta que contiene los parámetros de configuración en respuesta a un mensaje de solicitud de información. Un servidor envía un mensaje de Reply en respuesta a un mensaje de confirmación que confirma o niega que las direcciones asignadas al cliente sean apropiadas para el enlace al que está conectado el cliente. Un servidor envía un mensaje de Reply para acusar recibo de un mensaje de Release o Decline.

8. RELEASE (8). Un cliente envía un Release al servidor que asignó las direcciones al cliente para indicar que ya no usará una o más de las direcciones asignadas.

9. DECLINE (9). Un cliente envía un mensaje de Decline a un servidor para indicar que el cliente ha determinado que una o más direcciones asignadas por el servidor ya están en uso en el enlace al que está conectado el cliente.

10. RECONFIGURE (10). Un servidor envía un mensaje de Reconfigure a un cliente para informarle que el servidor tiene parámetros de configuración nuevos o actualizados, y que el cliente debe iniciar una transacción de Renew/Reply o Information-request/Reply con el servidor en orden. Para recibir la información actualizada.

11. INFORMATION-REQUEST (11). Un cliente envía un mensaje Information-request a un servidor para solicitar parámetros de configuración sin la asignación de ninguna dirección IP al cliente.

12. RELAY-FORW (12). Un agente de retransmisión envía un mensaje de Relay-forward para retransmitir mensajes a los servidores, ya sea directamente o a través de otro agente de retransmisión. El mensaje recibido, ya sea un mensaje de cliente o un Relay-forward de reenvío de otro relay agent, se encapsula en una opción en el mensaje de Relay-forward.

13. RELAY-REPL (13). Un servidor envía un mensaje de relay-reply a un agente de retransmisión que contiene un mensaje que el relay agent envía a un cliente. El mensaje de respuesta de retransmisión puede ser retransmitido por otros relay agent para su entrega al relay agent de destino.

El servidor encapsula el mensaje del cliente como una opción en el mensaje relay-reply, que el agente de retransmisión extrae y retransmite al cliente (Droms et al., 2003).

La operación del servidor DHCPv6 con estado, se muestra en la Figura 14, donde en la primera etapa se realiza la operación SLAAC de forma normal cuando el host realiza una solicitud al router por direccionamiento. A continuación, se mencionan los siguientes pasos:

1. Paso 1. Este responde con su anuncio.

2. Paso 2. Con el indicador M=1 le da a entender que la solicitud debe ser atendida por el servidor DHCPv6 de la red, el host envía a través de un mensaje de SOLICIT a todos los servidores DHCPv6 de la red, utiliza para esto el puerto UDP546.

3. Paso 3. El servidor recibe la solicitud y envía la respuesta ADVERTISE como mensaje de unidifusión por el puerto 547.

4. Paso 4. El host responde de dos formas, para el caso de DHCPv6 con estado la respuesta es un REQUEST, donde se solicita al servidor todos los parámetros de la red, incluyendo el direccionamiento. El segundo INFORMATION-REQUEST se envía para el modo sin estado, donde el host ya tiene la dirección IP y solo solicita los parámetros adicionales al servidor, como por ejemplo, dirección de servidor DNS, proxy entre otros.

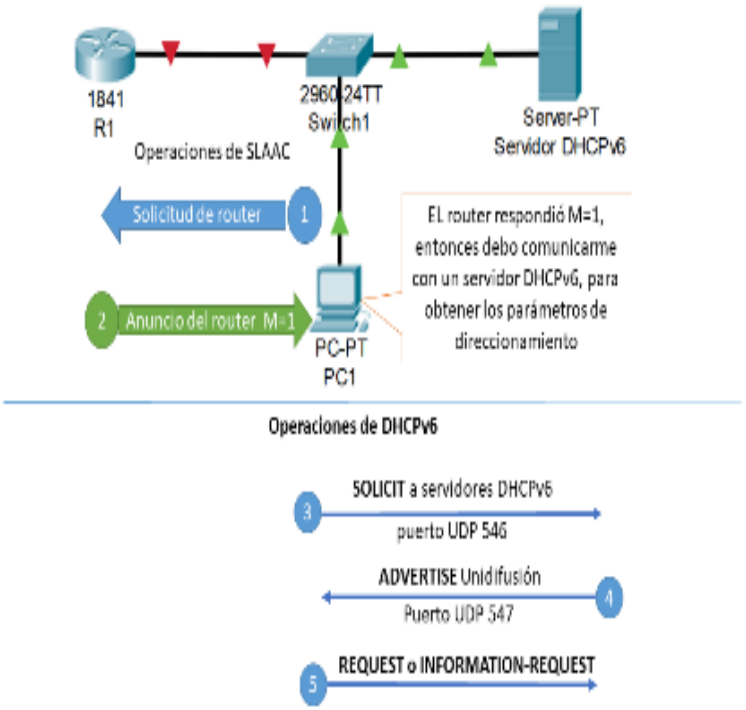


Figura 14. Operación servidor DHCPv6 con estado.

Túneles

Los túneles IPv6 es una técnica que permite la comunicación entre dos redes IPv6 a través de redes IPv4, definido en la RFC2893 (Gilligan y Nordmark, 2000) y que Carpenter y Moore (2001), en la RFC3056, explican cómo se implementa. Estas técnicas principalmente se ocupan para interconectar redes WAN, pero también pueden

ser utilizadas dentro de una gran empresa para interconectar Backbone que funcionan en IPv4. Existen varios tipos de túneles entre los cuales se pueden destacar los siguientes:

Manual

En este caso, se configuran todas las direcciones IPv4/IPv6 de forma manual en ambos lados del sistema que se desea comunicar (Boronat Seguí y Montagud Climent, 2013). Aquí los datos IPv6 se encapsulan en un encabezado IPv4. Posteriormente, se transmiten a través del túnel IPv4 y una vez en el destino son nuevamente desencapsulados y transmitidos a su destino final. La forma de determinar la dirección de punto final del túnel se realiza mediante la información que tienen los puntos de encapsulación y desencapsulación del túnel (El Khadiri et al., 2018). Este tipo de técnica puede operar en los siguientes modos: (a) de router a router, (b) de host a router, (c) de host a host y (d) de router a host.

Túnel automático 6-to-4

Este túnel permite la comunicación entre dos sitios IPv6 a través de una red IPv4 sin necesidad de un túnel configurado explícitamente o una dirección compatible IPv6-IPv4 (El Khadiri et al., 2018). Por lo tanto, la configuración del nodo final del túnel es mínima. Su operación se realiza a través de direcciones públicas que utilizan direcciones IPv6, las cuales enlazan a las direcciones 2001::/16 con la dirección IPv4 (32bits) (Boronat Seguí y Montagud Climent, 2013).

Traducción

La traducción de direcciones se realiza mediante el protocolo NAT-PT descrito en la RFC2766, que permite que un nodo IPv6 se comunique con un nodo IPv4 mediante la traducción de direcciones y protocolos, como se muestra en la Figura 15. En el modo tradicional de NAT-PT las sesiones que se establecen son unidireccionales, salientes desde los nodos IPv6. En el modo Bi-directional-NAT-PT, la comunicación de los nodos es, tanto de entrada como de salida (Tsirtsis y Srisuresh, 2000).

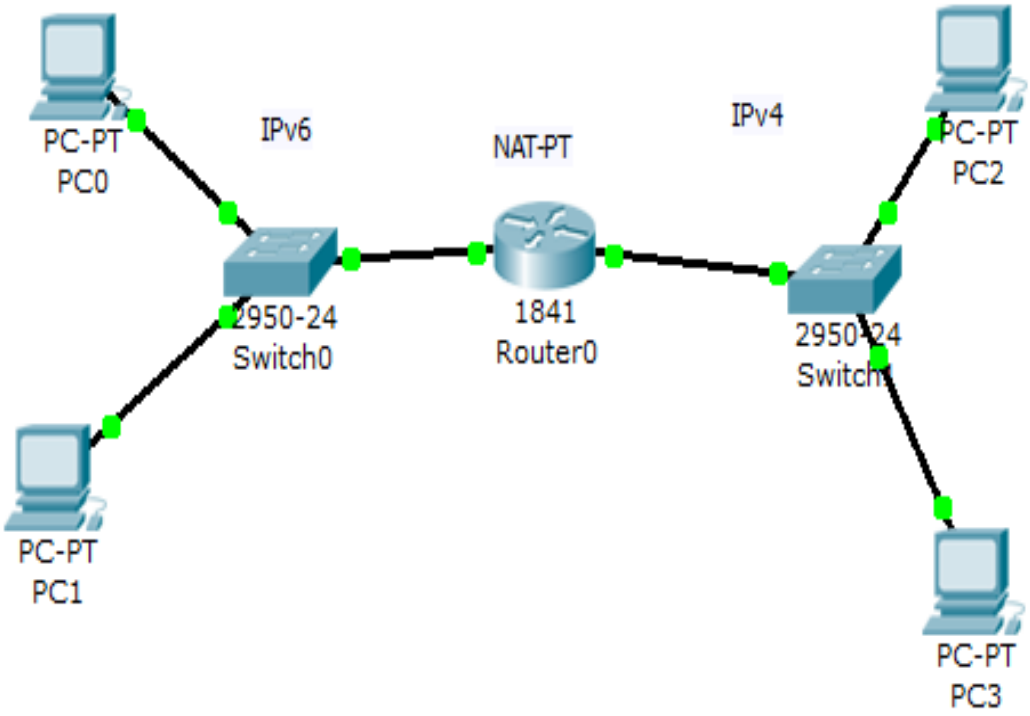


Figura 15. Implementación de NAT-PT.

IPsec y seguridad en IPv6

¿Qué es IPsec?

IPsec es el protocolo de seguridad que se implementó de forma opcional en el IPv4, pero que viene incorporado por defecto en IPv6. Está diseñado para proporcionar ser interoperable entre IPv4/IPv6, basado en técnicas de criptografías. Una descripción detallada de cada uno de los protocolos y algoritmos están definidos en la RFC4301 para IPsec (Droms et al., 2003) y la RFC4309 (Housley, 2005), que describe el uso de estándares de cifrado avanzados.

IPsec trabaja en la capa IP entregando seguridad a zonas que son protegidas. El tráfico que quiere atravesar este límite impuesto por el protocolo es revisado de acuerdo a las reglas y controles de accesos que el administrador de la red ha definido. Para esto, se ofrecen servicios de seguridad basados en ESP (cabecera de cifrado seguro de datos) o AH (cabecera de autenticación), ambos protocolos son cabeceras de extensión en el protocolo IPv6.

La cabecera de autentificación es la encargada de garantizar la integridad del tráfico IP, por lo que el receptor puede realizar la autenticación y verificación de los datos y que estos no han sido modificados en el trayecto de extremo a extremo. Se debe mencionar que con AH los datos viajan como texto plano, esto indica que pueden ser interceptados y leídos por intrusos.

La cabecera de cifrado seguro (ESP), complementa a la cabecera AH, permitiendo que los datos que viajan no pueden ser visualizados, aunque sean interceptados, esto se realiza a través de técnicas de cifrado.

Cabecera de autenticación AH

AH es una cabecera de extensión en IPv6 que permite entregar con integridad los datos al destino, mediante un proceso de autenticación. AH está basado en el algoritmo de encriptación HMAC (código de autentificación de mensajes en clave-hash), que se describe en la RFC2104 (Krawczyk, Bellare y Canetti, 1997).

Cifrado seguro de la carga útil (Encapsulating Security Payload ESP)

El encabezado ESP está descrito en la RFC2406 (Kent y Atkinson, 1998). Este puede ser usado de forma individual o en conjunto con otros protocolos, como por ejemplo el AH. Ese protocolo, a diferencia del ESP, no garantiza que los datos de un extremo a otro lleguen de forma correcta, sino que su uso permite encriptar la comunicación de extremo a extremo, es decir proporciona confidencialidad y autenticación de origen de datos sin conexión. Permite que sea un complemento para el protocolo ESP. La seguridad va a depender de las opciones seleccionadas en el momento que se estableció la Asociación de Seguridad (AS) y de la ubicación de la implementación. ESP opera en forma directa con el protocolo IP y su valor es 50.

Formato del paquete ESP

El encabezado del protocolo en IPv4 o extensión IPv6, inmediatamente anterior al encabezado de ESP contendrá el valor 50 en su campo Protocolo (IPv4) o encabezado xSiguiente (IPv6, extensión) para definir que tiene activo el protocolo ESP (ver Figura 16). El formato de la cabecera ESP es el siguiente:

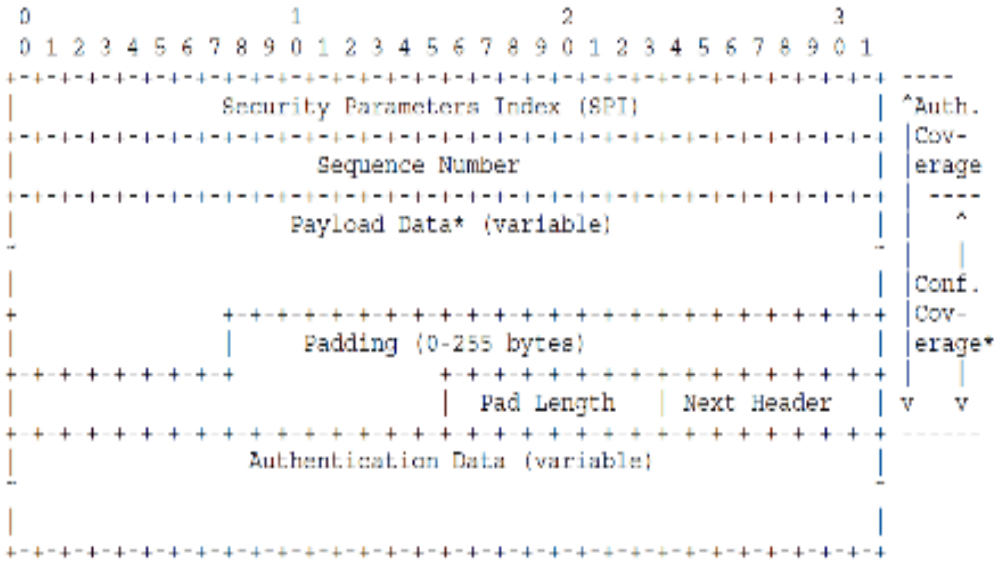


Figura 16. Cabecera ESP (Kent y Atkinson, 1998).

La descripción realizada por Kent y Atkinson (1998), de los campos del protocolo (ver Figura 16), son los siguientes:

1. Security Parameters Index SPI. Es un valor arbitrario de 32 bit, en donde se combina con la dirección IP del destino. Esto permite identificar de forma única para el AS de este datagrama. Los valores de este campo en el rango de 1 a 255 no se pueden utilizar porque están reservados por la IANA para uso futuro aún no definido. El valor 0 es de uso local y no se envía por medio de transmisión.

2. Sequence Number. Este campo de 32 bit es obligatorio, incluso en los casos en que el receptor no escoge habilitar el servicio de anti-replay. Contiene el incremento del número de secuencia. Siempre cuando se establece la SA, este número de secuencia se inicializa en 0 en ambos extremos.

3. Payload Data. Los datos de carga útil es un campo de longitud variable que contiene los datos descritos en el campo Next Header. Este campo es obligatorio y su longitud es un número entero de bytes.

4. Padding (for Encryption). El campo de relleno se usa por varios factores y se emplea un algoritmo de cifrado que requiere que el texto sin formato sea un múltiplo de algún número de bytes. También se puede requerir relleno, independientemente de los requisitos del algoritmo de cifrado, para garantizar que el texto cifrado finalice en un límite de cuatro bytes. Esto porque deben estar alineados con una palabra de cuatro bytes. También este campo se puede utilizar para ocultar la longitud real de la carga útil, como una medida adicional o de apoyo de la confidencialidad, eso sí esta medida tiene implicaciones no deseadas sobre el ancho de banda necesario para transmitir dicha carga adicional.

5. Pad Length. Este campo indica el número de bytes de PAD que lo preceden inmediatamente. El rango de valores válidos es de 0-255, donde el valor 0 indica que no hay bytes de relleno. Este campo es obligatorio.

6. Next Header. Es un campo de ocho bits que identifica el tipo de datos contenidos en el campo de Datos de carga útil, en el caso de un encabezado de extensión en IPv6 o un identificador de protocolo de capa superior. Este campo es de uso obligatorio.

7. Authentication Data. Es un campo de longitud variable que contiene un Valor de Verificación de Integridad (ICV) calculado sobre el paquete ESP menos los datos de autenticación. Este campo es opcional y solo se utiliza si el servicio se ha seleccionado para una SA.

Algoritmos de Hash

El algoritmo Hash es utilizado en IPsec para realizar la integridad de los datos. Esta función criptográfica es una función matemática que convierte un bloque de datos en una nueva serie de caracteres de longitud fija. Un problema que enfrentan este tipo de algoritmo son las colisiones porque los datos pueden tener un largo infinito y la salida que se obtiene con el algoritmo tiene una salida de bits de tamaño fijo. A pesar de esto, los mensajes que sufren colisiones pierden sentidos y son descartados por la red. En la red existen generadores online Hash o SHA, como se los conoce en inglés, que permiten generar las cadenas de bit correspondientes a las palabras ingresadas. Por ejemplo, en http://www.sha1-online.com/ se puede utilizar para comparar los distintos algoritmos de encriptación. Esto es muy útil en sistemas online porque las contraseñas son guardadas con esta encriptación lo que permite tener seguridad, dado que no son enviadas como texto plano por la red (Vivar Soto, 2008).

Protocolo de intercambio de claves en internet (IKE, ISAKMP)

El protocolo de intercambio de claves de internet permite el intercambio de secreto de claves al momento de establecer una SA en Ipsec y lo realiza mediante el intercambio secreto de tipo Diffie-Hellman sobre un canal inseguro. Está definido en la RFC2407 y la RFC2409, donde Oakley y SKEME, dos protocolos usados en IKE y definen un método para establecer un intercambio de claves autenticado. Esto incluye la construcción de la carga útil, la información sobre la carga útil, el orden en que se procesan y cómo se utilizan (Harkins y Carrel, 1998).

Mientras Oakley define "modos", ISAKMP define "fases". La relación entre los dos es muy sencilla e IKE presenta diferentes intercambios como modos que operan en una de dos fases siguientes:

La Fase 1 es donde los dos pares de ISAKMP establecen un canal seguro y autenticado con el cual comunicarse. Esto se llama la Asociación de Seguridad ISAKMP (SA). El "modo principal" y el "modo agresivo" realizan un intercambio de fase 1. El "modo principal" y el “modo agresivo" solo deben utilizarse en la Fase 1 (Harkins y Carrel, 1998).

La Fase es donde las asociaciones de seguridad se negocian en nombre de servicios como IPsec o cualquier otro servicio que necesite material clave y/o negociación de parámetros. El "modo rápido" realiza un intercambio de fase 2. El "modo rápido" solo debe usarse en la Fase 2 (Harkins y Carrel, 1998).

Ventajas y desventajas de los mecanismos de migración

En este apartado, se evalúan las ventajas de usar IPv6 en las redes, que en el presente trabajo es la red corporativa de la UnACh, pero se puede aplicar a cualquier institución con similar complejidad de su red.

Una de las ventajas más evidente es la autoconfiguración, esto permite que solo el host se conecte a la red para que reciba todos los parámetros y en caso de cambio de ISP (proveedor de servicios de internet), la migración se realice con transparencia para los usuarios, dado que solo se necesita el cambio de configuración dentro del router y/o del servidor DHCPv6, cabeceras más simples del paquete IPv6, lo que permite una mayor rapidez en el procesamiento. Una ventaja evidente es el aumento del

número de direcciones disponibles con el nuevo protocolo y se tiene que mencionar que en el IPv6, se eliminó el Broadcast reemplazado por direcciones Multicast. La seguridad implementada por defecto y no de forma opcional, permite al IPv6 ser más fuerte con el uso de IPSec (Vivar Soto, 2008).

Ventajas

Las ventajas son las siguientes: (a) mayor cantidad de direccionamiento, es decir, 128 bits, (b) seguridad incorporada Ipsec, (c) cabecera simplificada y (d) autoconfiguración.

Respuesta a cobertura inalámbrica

Una de las preocupaciones de los equipos IT empresariales es la movilidad creciente de los usuarios que quieren estar conectados a su red corporativa en todo lugar del campus, sin perder el acceso a los recursos que poseen. Diferentes estudios realizados con software, como el presentado por Jain et al. (2018), en el cual se realiza un estudio de red wifi, con protocolos 802.11a/g, 802.11b, fueron configurados 100 nodos. Dicho estudio permite evaluar los modos de operación y su respuesta a diferentes parámetros de la comunicación inalámbrica de los hosts. Se midieron los siguientes parámetros, el Throughput, Average End-to-End Delay, average Jitter y la Packet Delivery Ratio. Los casos utilizados fueron nodos IPv4, nodos IPv4 con interfaces duales, solo nodos IPv6, nodo IPv6 con interfaces duales y DualStack mode (Jain et al., 2018). El resultado del rendimiento (Throughput) se observa en la Figura 17 para los cuatro escenarios. El retraso medio de extremo a extremo se muestra en la Figura 18. El promedio de parpadeo de la red se muestra en la Figura 19. La proporción de entrega de paquetes se muestra en la Figura 20.

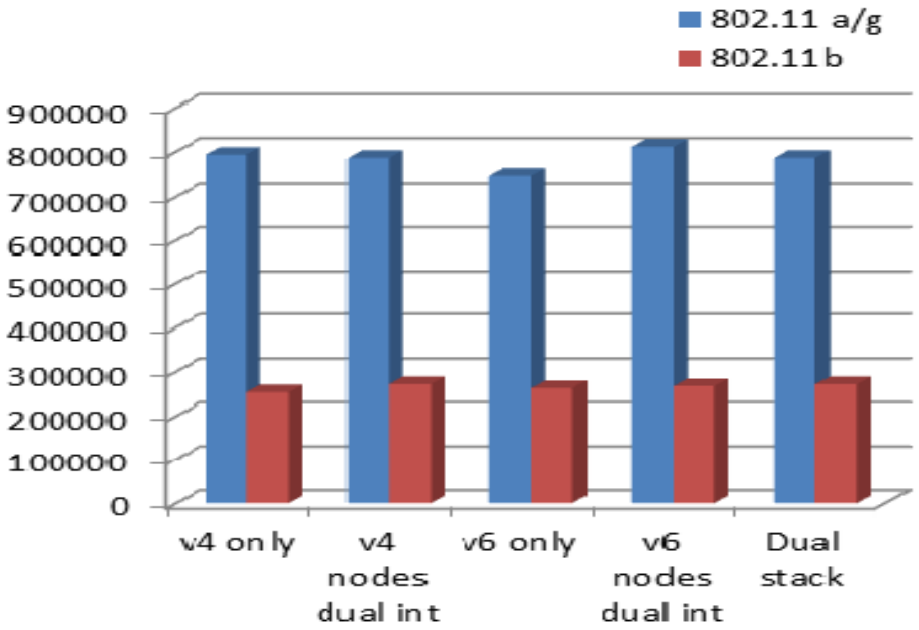


Figura 17. Rendimiento.

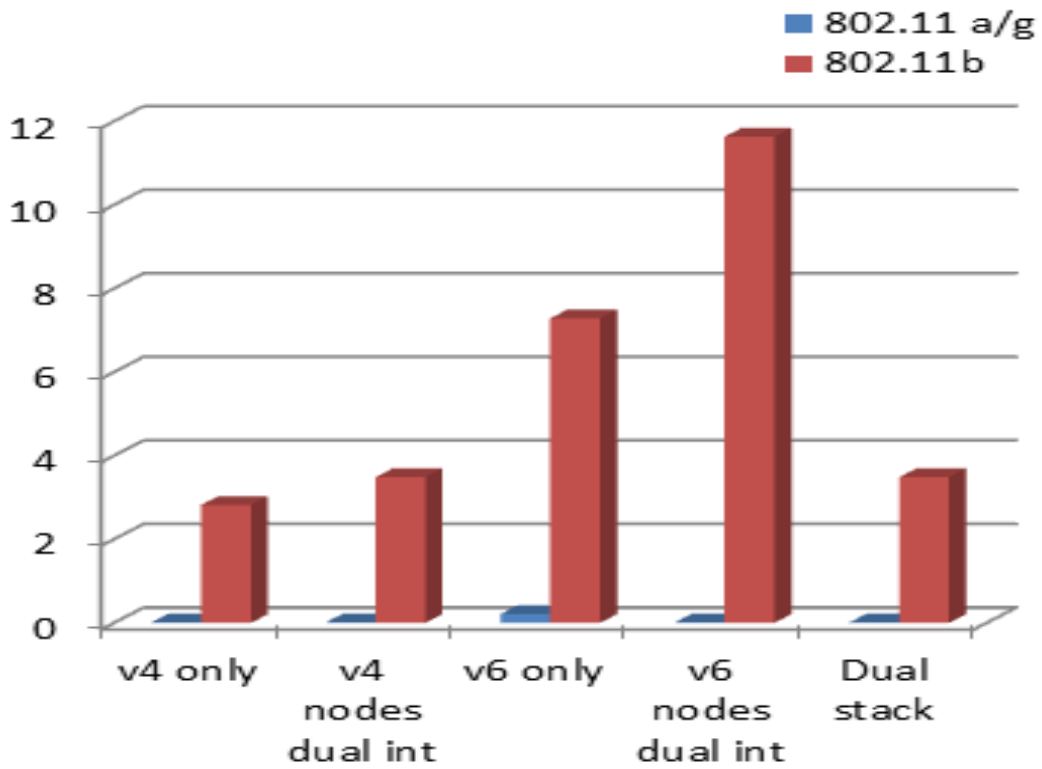


Figura 18. Promedio de retardo punto a punto.

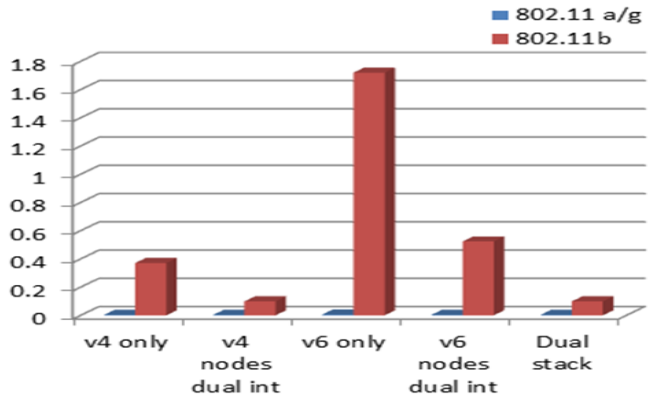


Figura 19. Jitter promedio.

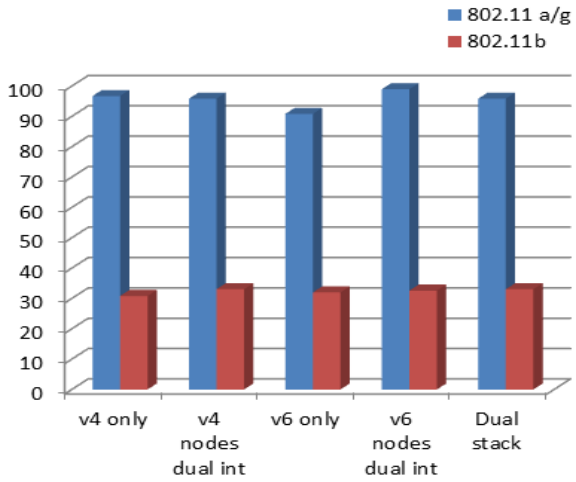


Figura 20. Proporción de paquetes de entregados.

En el análisis de los resultados se ve claramente que los mejores resultados son dados por una configuración IPv6 nativa, seguido muy de cerca por la implementación Dual Stack, todo esto en redes inalámbricas. Debido a esto, se ha decidido para el presente trabajo utilizar Dual Stack en la configuración propuesta para la red de la UnACh, que de igual forma sirve como referencia para otras instituciones de iguales características.

Desventajas

Una de las mayores desventajas es el amplio despliegue aún de infraestructura IPv4 lo que se traduce en la necesidad de tener sistemas intermedios que permitan la comunicación entre ambos protocolos. Otro factor es el mantenimiento, hoy los técnicos que dan soporte a las redes no están suficientemente capacitados para entregar soporte a redes con IPv6, debido a lo reciente que se comenzó a implementar esta tecnología. Por último, no se puede obviar el factor económico, debido a la gran cantidad de redes funcionando en IPv4. El cambio por parte de los ISP que mantienen aún direcciones IPv4 en sus stack, no les hace conveniente el comenzar a entregar masivamente direccionamiento IPv6 porque les afecta su modelo de negocio y en los cambios tecnológicos para dar soporte a este protocolo.

Resumen

Dual Stack, Tunelización y traducción son las tres grandes categorías en las que se agrupan los principales mecanismos que el IETF desarrolló para la transición entre IPv4/IPv6. Al realizar la migración, se debe tener claro las ventajas y las desventajas que cada uno de ellos posee, dado que no existe ninguno que cumpla con todo el requerimiento y que sea perfecto. El IPv6 es soportado por la mayoría de los sistemas operativos hoy en día. La Tabla 3 presenta un resumen de los tres mecanismos de transición.

Tabla 3

Resumen de los tres mecanismos de transición

Nombre	Tipo de mecanismo	Conectividad	Descripción	Ventajas	Desventajas
Pila Dual	Pila doble	Sólo entre sistemas del mismo tipo (IPv4-IPv4, IPv6-IPv6)	Trabaja en ambos protocolos. Procesa sólo los encabezados IP. Se basa en DHCP y Direcciones compatible para asignación de direcciones	Fácil de implementar. Una solución inmediata y accesible. Permite a los nuevos host IPv6 relacionarse rápidamente con el resto de los dispositivos	No trabaja en ambientes mixtos (IPv4 sobre IPv6 y viceversa). Si la red no es IPv6 no se ve beneficiada de las características de esta versión.
SIIT	Traducción	De IPv6-IPv4 de IPv4-IPv6	Para hacer dos protocolos compatibles, realiza la traducción de encabezados. Se necesita de un traductor que lleve a cabo la tarea de traducción.	Permite a nodos IPv4 comunicarse con nodos IPv6. Fácil de soportar por un dispositivo. No se afecta el checksum de capa de transporte. Puede manejar paquetes encriptados, ya que no modifica capas superiores.	Al realizar la traducción IPv6 a IPv4 se pierden muchos campos y con éstos, beneficios de IPv6. Se ignoran la mayoría la mayoría de los encabezados de extensión. Al manejar dos protocolos se necesitan dos tablas de ruteo. AL trabajar con IPv4 compatibles se reduce el campo de direccionamiento. Se reduce el tamaño de la MTU lo que resulta en fragmentación de los datos.
6over4	Tunneling	IPv6 a IPv6 sobre IPv4	Se comporta como una VPN	Permite la autoconfiguración. Conserva todas las características de IPv6.	Necesita soporte de ruteo multicast (IPv4 raramente cuenta con este soporte).
6to4	Tunneling	IPv6 a IPv6 sobre IPv4	Crea túneles automáticamente. Algoritmo más popular dentro de su clase.	Ayuda a conectar redes IPv6 aisladas entre si	

Machine learning en IPv6 y blockchain

Machinne Learning o aprendizaje de máquina es una tecnología que se está aplicando para seguridad, pero que no es propia del campo de las redes, más bien trabaja en las tres capas superiores del modelo de referencia OSI. Debido a sus bondades, ha permitido su utilización en otras áreas. Los algoritmos de esta tecnología no programan el software sino que, el software de acuerdo al aprendizaje que está realizando, se programa solo. Este es un nivel superior del desarrollo tecnológico y realiza un cambio de paradigma en el desarrollo de software (Weisman et al., 2018).

BlockChain

Una cadena de bloques es, esencialmente, una base de datos de registros distribuida, o libro de contabilidad público de todas las transacciones o eventos digitales que han sido ejecutados y compartidos entre las partes participantes. Cada transacción en el libro mayor público es verificada. Esta verificación se realiza mediante algoritmos de encriptación HASH, que permiten tener encriptadas y distribuidas las comunicaciones entre todos los nodos que componen la cadena. Cada nodo contiene una copia exacta de los bloques, por lo que es muy difícil por parte de un atacante cambiar la información de la transacción realizada, debido a que deberían intervenir todos los nodos al mismo tiempo, antes que estos hagan la verificación y se actualicen, es por esto que la tecnología BlockChain ha permitido un nivel de seguridad más avanzado y descentralizado (Jiang et al., 2018).

Esta tecnología es muy utilizada en el ámbito financiero y de las criptomonedas, pero poco a poco está ingresando en otros campos de la ciencia que poco a poco van

descubriendo sus ventajas y aplicabilidad en su área. Uno de estos campos es el IoT, el cual es importante para este estudio debido a que las comunicaciones encriptadas utilizan el mismo protocolo que en IPv6, mediante IPsec (Politou, Casino, Alepis y Patsakis, 2019).

CAPÍTULO III

MARCO METODOLÓGICO

Planificación de la red para transición IPv4/IPv6

Metodología del proyecto

Todo cambio en las instituciones debe tener una planificación, se puede llamar también gestión de procesos, dado que afectan a un proceso en particular o a todos los procesos de la institución, agregando o quitando valor al servicio entregado. En el caso del presente estudio, se utiliza el concepto de gestión de procesos para llevar a cabo el cambio tecnológico que se modela. Se propone que, al momento de decidir el cambio de tecnología, se realicen los siete pasos siguientes:

Primera etapa documental y revisión del estado del arte. Esta etapa se realizó en el capítulo II.

En la segunda etapa, se emplean las configuraciones de DHCPv6 con estado y sin estado, conjuntamente con DHCPv4 corriendo paralelamente (modo Dual Stack) como propuestas para realizar la migración. Los pasos son los siguientes:

Paso 1. Revisión de compatibilidad de hardware.

Paso 2. Planeamiento de direccionamiento IPv6.

Paso 3. Configuración de servidores DHCPv6 y DNSv6.

Paso 4. Configuración de enrutadores.

Paso 5. Configuración de switch´s.

Paso 6. Verificación de conectividad.

Paso 7. Toma de datos por tipo de red, IPv4 e IPv6.

Para el presente trabajo, la metodología que se realizó fue a partir del paso número dos, lo que permitió realizar la simulación de los diferentes escenarios posibles que la institución puede determinar cómo óptimos. De igual forma, se entregan los resultados obtenidos para que la toma de decisiones se realice en base a estadísticas técnicas. El paso uno, se realizó con antelación en consulta al departamento de tecnologías de la información DTI de la UnACh, informando que todos los equipos son compatibles con IPv6. Los dispositivos intermedios que utiliza la institución son los switch cisco modelo SF300-24, SF300-48, SF300-24PP y SF300-48PP. También se cuenta con un router Mikrotik CCR 1036, todos con compatibilidad IPv6 de acuerdo a las especificaciones de los fabricantes.

En lo expuesto en el capítulo dos, se tiene tres grandes bloques de mecanismos de transición, los cuales se mencionan a continuación:

1. Doble Pila o Dual Stack.

2. Túneles: Tunnel Broker (RFC3053), 6to4 (RFC3056), Teredo (RFC4380) y Softwires, 6RD.

3. Traducción: SIT, BIS, TRT, SOCKSv64, NAT-PT, NATPTIMPL, creados para HTTP.

Cuando se diseñaron los mecanismos de transición por parte del ITFE, el pensamiento era que se desplegaría IPv6 antes del agotamiento de las direcciones de IPv4, pero la realidad es completamente diferente. El objetivo fue mantener IPv4 e IPv6 simultáneamente.

La Tabla 4 muestra la comparativa de protocolos de transmisión más utilizados y las métricas que el grupo de trabajo del IETF utiliza para ver su aplicabilidad en una red. Es importante mencionar que esta tabla debe ser aplicada en el contexto de una red en particular y que podría variar de acuerdo al soporte que brinde el ISP de la institución. Según Palet (2016), los estudios realizados sobre los mecanismos de transición, la mayoría de ellos se centran en los ISP. Además, se debe tener en cuenta que los mecanismos de traducción fueron creados para trabajar en HTTP, es decir, en sistemas con soporte web, en este ámbito son eficaces, pero no se recomiendan para otras tareas, por esto la mejor solución en el caso de la UnACh, es Dual Stack en sus redes Lan y en combinación con un sistema que transporte el flujo IPv4 sobre IPv6, de acuerdo a la experiencias recogida de la Asociación Nacional de Universidades e Instituciones de Educación Superior de la República Mexicana, A. C. (ANUES). Estas instituciones asociadas avanzan en conjunto en diferentes temas de tecnologías de la información y en las cuales el mecanismo adoptado en Dual Stack (Franco Reboreda y Rodríguez Elizondo, 2017). Esto se basa en el estudio que realizaron sobre la penetración de IPv6 en las universidades, miembros de ANUIES, que para el 2017 un 11% de las instituciones poseen conectividad IPv6 con Dual Stack (ver Figura 21) y el 2018 sube el porcentaje a un 18% (Franco Reboreda y Rodríguez Elizondo, 2017). El ITFE también recomienda que en las redes locales el mecanismo sea doble pila (Palet, 2016). No se tienen cifras de comparación para instituciones de educación superior en Chile, así que con el antecedente y experiencia de las universidades mexicanas, se realiza el presente proyecto con Dual Stack para la red de la UnACh.

En la Tabla 4, se muestran las columnas agrupan los mecanismos de transición y los factores de estudio para cada mecanismo. Las casillas marcadas con color rojo indican que en el mecanismo el factor indicado no es compatible. Las casillas marcadas con verde indican que el mecanismo soporta completamente la funcionalidad y las casillas marcadas con naranja indican que no son ni buena ni malas y que deben ser evaluadas en su contexto (Palet, 2016).

Figura 21. Situación de conectividad del IPv6, ANUIES (Franco Reboreda y Rodríguez Elizondo, 2017).

Cuando se diseñaron los mecanismos de transición por parte del ITFE, el pensamiento era que se desplegaría IPv6 antes del agotamiento de las direcciones de IPv4, pero en realidad es completamente diferente. El objetivo fue mantener IPv4 e IPv6 simultáneamente.

Situación actual de la red UnACh

La arquitectura de la red en la UnACh se puede dividir en dos partes: (a) la red del data center corporativo y (b) la red Lan. En cuanto al data center, se encuentra bajo contrato a una empresa externa, por la compra mediante leasing del sistema completo de servidores, por lo que no se realizarán modificaciones en este proyecto a esta etapa de la red.

Tabla 4

Comparación de protocolos de transición IPv4/IPv6

Parametros	6RD	Sfotwires v2	NAT444	DS-Lite	Lw4o6	NAT64	464XLA	MAPE-E	MAP-T
Tunnel/Traducción (x)	T 6in4	T 6in4	x	T 4in6	T 4in6	x	x	T 4in6	x
Doble pila LAN	SI	SI	opcional	SI	SI	SI	SI	SI	SI
Multicast IPv4	SI	SI	SI	NO	NO	NO	NO	NO	NO
Red Acceso	IPv4	IPv4	IPv4/dual	IPv6	IPv6	IPv6	IPv6	IPv6	IPv6
Overhead	20 bytes	40 bytes		40 bytes	40 bytes	20 bytes	20 bytes	40 bytes	20 bytes
Impacto plan direccionamiento IPv6	SI	NO	NO	NO	NO	NO	NO	SI	SI
Requiere actualizaciones de los CPE	SI	SI	opcional	SI	SI	SI	SI	SI	SI
Traducción NAT44/NAPT, en el ISP o CPE o en ambos (CGN, carrier-grade NAT)	CPE	CPE	CPE y CGN	CGN	CPE	CPE	CPE	CPE	CPE
Donde se hace la traducción 46/64						ISP	ISP y/o CPE		CPE + ISP
Traducción ISP sin/con estado			CON			CON	CON	SIN	SIN
Escalabilidad	Alta	Media	Media	Media	Alta	Alta	Alta	Alta	Alta
Prestaciones	Alta	Baja	Baja	Baja	Alta	Media	Media	Alta	Alta
Requiere soporte de LGs	NO	NO	SI	SI	NO	SI	SI	SI	SI
Soporte otros vs sólo-TCP/UDP/ICMP	SI	SI	SI	SI	SI	NO	NO	NO	NO
Comparte "puertos"/IPv4	NO	NO	SI	SI	SI	NO	NO	SI	SI
Agregación IPv6	NO	NO	opcional	SI	SI	SI	SI	SI	SI
Mesh IPv4	SI	SI	SI	NO	NO	NO	NO	SI	SI
Mesh IPv6	Si	NO	opcional	Si	SI	SI	SI	SI	SI
Impacto en logging	NO	NO	SI	SI	NO	SI	SI	NO	NO
Facilidad HA (high availability)	Alta	Baja	Baja	Baja	Alta	Media	Media	Alta	Alta
Facilidad DPI (Deep Packet Inspection)	Baja	Baja	Alta	Baja	Baja	Alta	Alta	Baja	Alta
Soporte celular	NO	NO	SI	NO	NO	SI	SI	NO	NO
Soporte en CPEs (Equipo local del cliente)	SI	SI	SI	SI	SI	SI	SI	SI	SI

Arquitectura de red data center UnACh

La arquitectura de la sala de servidores está constituida por dos servidores Lenovo x3550s, dos switch de capa 3 a 10Gb y un storange EMC VNX 3200 con una capacidad de 12TB, tal como se muestra en la Figura 22.

Arquitectura de red Lan UnACh

La red lan de la universidad descrita en los antecedentes generales del capítulo uno, está compuesta por una red cableada y wifi para usuarios administrativos, docentes y alumnos. El crecimiento de la red, a lo largo de los años, ha creado la necesidad

de dividir administrativamente los segmentos de la red mediante el uso de redes virtuales o VLAN´s. Se tienen 19 vlan definidas para la red en general, las cuales son los siguientes:

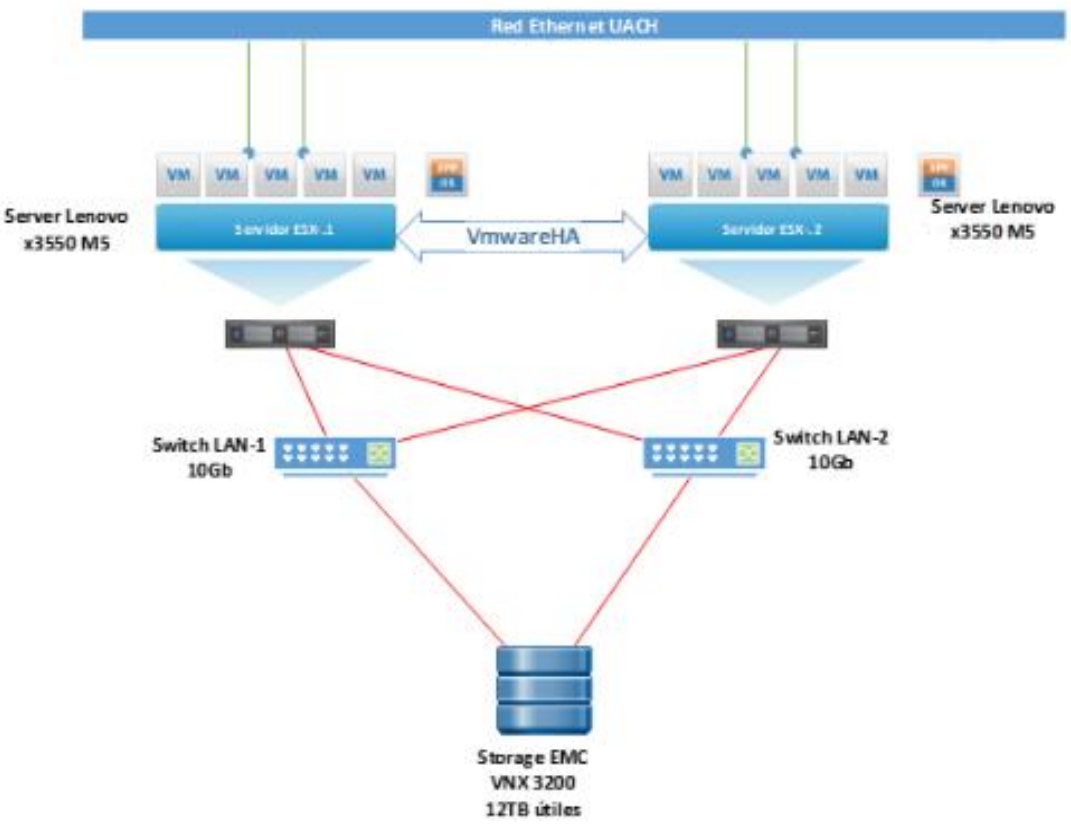


Figura 22. Configuración esquemática de red data center UnACh.

1. Vlan 160 Servidores-DTI
2. Vlan 180 CCTV
3. Vlan 181 Impresoras
4. Vlan 190 Servidores carrera Informática
5. Vlan 200 Wifi UnACh general

6. Vlan 201 Wifi UnACh aulas A

7. Vlan 202 Wifi UnACh aulas B

8. Vlan 203 Wifi UnACh biblioteca

9. Vlan 204 Wifi UnACh aulas C

10. Vlan 205 Wifi UnACh desarrollo estudiantil

11. Vlan 206 Wifi UnACh edificio administración

12. Vlan 207 Laboratorio de computación 3 y 4

13. Vlan 208 Wifi UnACh edificio facultad de salud

14. Vlan 240 Oficinas

15. Vlan 280 casas personal

16. Vlan 290 casas administradores

17. Vlan 300 Eventos

18. Vlan 501 Voz

19. Vlan 1181 Vpn Unión Chilena

Servidores DHCP IPv4 actual

Para entregar el direccionamiento en la red, actualmente está distribuido por una configuración DHCP que entrega un pool de direcciones a cada segmento configurado. El listado de la asignación DHCP se puede observar en la Tabla 5.

Diagrama general red UnACh

El diagrama de la red actual se ha desarrollado en el software Packet Tracer, versión 7.2.1.0218 de Cisco. Para cada una de las Lan que se muestran, se agrega un PC de escritorio, impresora de red, teléfono IP, wifi y un portátil, de forma genérica por

LAN, dado que el resto del host poseen características similares. Está simulación de red permite la realización de pruebas ping para medir el tiempo de respuesta en los distintos escenarios y de esta forma analizar los resultados obtenidos en la propuesta. La configuración lógica se observa en la Figura 23.

Tabla 5

Asignación de VLAn´s en la UnACh

Nombre	Interface
dhcp-voz	vlan 501
dhcp-dti	vlan 160
dhcp-cctv	vlan 180
dhcp-impresoras	valn 181
dhcp-datacenter-inf	ether 12-sw ServFain
dhcp-wifi-admin	vlan 206
dhcp-wifi-desarrollo-est	vlan 205
dhcp-lab 3	vlan 207
dhcp- wifi aulas A	vlan 201
dhcp-wifi-biblioteca	vlan 203
dhcp-wifi-aulas B	vlan 202
dhcp-wifi-aulas C	vlan 204
dhcp-wifi	vlan 200
dhcp-oficinas	vlan 240
dhcp-casas	vlan280
dhcp-casas admin	ether6-casas-admins
dhcp-evento	vlan 300
dhcp-vlan	bridge1

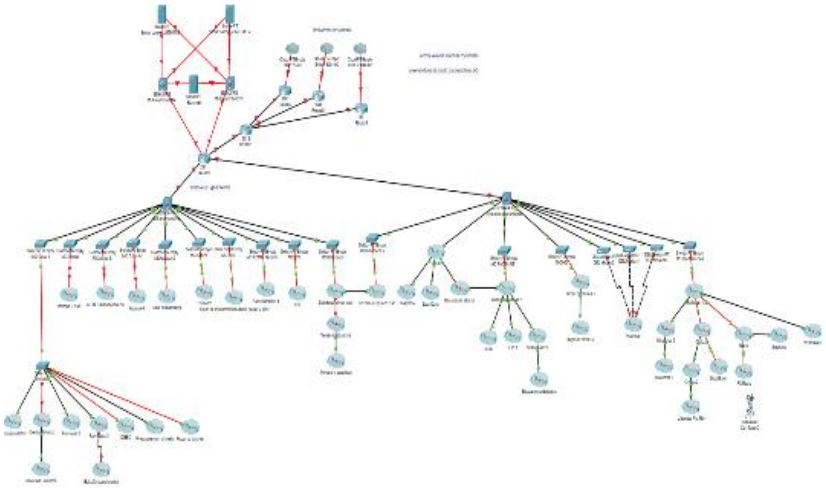


Figura 23. Topología lógica de la red de UnACh.

Planeamiento del direccionamiento IPv6

Para el presente estudio, se utiliza el siguiente direccionamiento:

1. Prefijos IPv6

Vlan 181 2001:1111:2222:181::/64

Vlan 200 2001:1111:2222:200::/64

Vlan 240 2001:1111:2222:240::/64

2. Direccionamiento IPv4

Vlan 181 172.20.181.0/24

Vlan 200 172.20.200.0/24

Vlan 240 172.20.240.0/24

3. Dirección servidor DHCP y DNS

IP address DHCPv4 172.20.10.11

IP address DNS4 172.20.10.10

4. IP address gateway IPv6

Vlan 181 2001:1111:2222:181::1/64

Vlan 200 2001:1111:2222:200::1/64

Vlan 240 2001:1111:2222:240::1/64

5. IP address gateway IPv4

Vlan 181 172.20.181.1 255.255.255.0

Vlan 200 172.20.200.1 255.255.255.0

Vlan 240 172.20.240.1 255.255.255.0

Configuración de escenarios

El sector más lejano del data center, es la Facultad de Ingeniería y Negocios (FAIN). Se elige esta localidad de la red por ser la peor condición de red debido a su distancia. El trazado de esta red va desde el data center, saliendo con un media converter (convertidor de medios, cobre-fibra multimodo), llegando al rack ubicado en el supermercado, donde se interviene la fibra en un ODF (cabecera de fibra óptica), enviando la señal nuevamente por fibra para las oficinas de la FAIN. En ese lugar, se cuenta con un rack que posee un ODF saliendo de este mediante un jumper de fibra LC al switch de distribución. Este trazado está realizado en fibra multimodo, subterránea de 50/125 con 3,5 dB/km de atenuación.

Configuración de red con SLAAC

Como se estudió en el capítulo II, SLAAC es una de las nuevas herramientas de autoconfiguración que IPv6 implementa, la que permite a los hosts configurar de forma automática una dirección de unidifusión global. En esta sección, se propone la configuración del router de la red para operar mediante SLAAC. La topología de la red que

aparece en la Figura 24, muestra el router principal el cual se configura para utilizar SLAAC en la red de la FAIN. La Vlan´s configuradas en el switch capa 3 del Core en el data center y enviadas a los switch de la capa de distribución, son las siguientes:

1. Equipos de oficina es la Vlan 240
2. Para el wifi Vlan 200
3. Impresoras de red Vlan 181

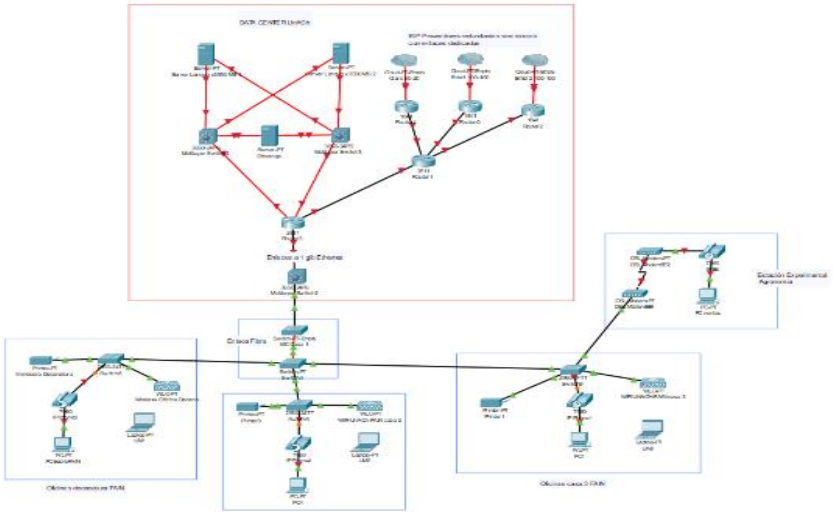


Figura 24. Red data center a FAIN.

Configuración VLan

La configuración de las Vlan en el switch de capa 3 en el nodo de Core, se realiza en modo VTP server, permitiendo reducir los tiempos de configuración en los nodos que pertenecen al mismo dominio. La configuración de las Vlan realizadas en los nodos del dominio son los siguientes:

Para nodos clientes:

vtp domain UnACh

vtp mode client

vtp password cisco

Para el nodo server:

vtp domain UnACh

vtp mode server

vtp password cisco

Para nodos que no intervienen, pero que se encuentran en la ruta desde el server a los clientes, estos se configuran en modo transparente.

vtp domain UnACh

vtp mode transparent

vtp password cisco

Una vez realizadas estas configuraciones, en el nodo server se realiza la creación de las Vlan en modo de configuración global. A continuación se mencionan:

VTPserver(config)#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

VTPserver(config)#vlan 240

VTPserver(config-vlan)#name Oficinas

TPserver(config)#vlan 200

VTPserver(config-vlan)# name WIFI

TPserver(config)# vlan 181

VTPserver(config-vlan)#name Impresoras

TPserver(config)# vlan 501

VTPserver(config-vlan)# name voz

TPserver(config)# vlan 99

VTPserver(config-vlan)# name Management

La siguiente configuración se muestra después de aplicar el comando show vtp status:

VTPserver#show vtp status

VTP Version capable: 1 to 2

VTP version running: 2

VTP Domain Name: UnACh

VTP Pruning Mode: Disabled

VTP Traps Generation: Disabled

Device ID: 0001.424B.7660

Configuration last modified by 0.0.0.0 at 3-1-93 06:15:18

Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:

VTP Operating Mode: Server

Maximum VLANs supported locally: 1005

Number of existing VLANs: 10

Configuration Revision: 6

MD5 digest: 0xE7 0x6E 0x9A 0x5D 0xEF 0x0D 0x26 0x83

0x48 0x0B 0xAB 0x48 0x2E 0x8B 0x19 0xED

En las dos líneas resaltadas se observa, primero el nombre de dominio que es el correcto y en la segunda línea resaltada, el modo de operación que en este caso es server.

En el nodo server, se configura el puerto giga 1/0/24 para que sea troncal y que pertenezca a la Vlan nativa 99, esto permite al puerto procesar el tráfico de todas las Vlan a los nodos clientes. Para verificar dicha configuración, se ingresa el comando show running-config siguiente:

interface GigabitEthernet1/0/24

switchport trunk native vlan 99

Se observa en la información que el puerto está efectivamente en modo troncal y que pertenece a la Vlan nativa 99.

En los nodos clientes, se debe configurar el mismo dominio y la clave para que estos reciban la información del VTP server. Los comandos ingresados en modo de configuración de terminal en todos los nodos son los siguientes:

1. Switch decanatura Fain1

Fain1(config)#vtp domain UnACh

Fain1(config)#vtp mode client

Fain1(config)#vtp password cisco

2. Switch casa 2 Fain2

Fain2(config)#vtp domain UnACh

Fain2(config)#vtp mode client

Fain2(config)#vtp password cisco

3. Switch casa 3 Fain3

Fain3(config)#vtp domain UnACh

Fain3(config)#vtp mode client

Fain3(config)#vtp password cisco

Para que la información del VTP server llegue a los clientes, se deben configurar los enlaces troncales de cada uno de los nodos del dominio que a continuación se hacen referencia:

1. Switch decanatura Fain1

Fain1(config)# interface GigabitEthernet0/1

Fain1(config-if)#switchport trunk native vlan 99

Fain1(config-if)#switchport mode trunk

2. Switch casa 2 Fain2

Fain2(config)#interface GigabitEthernet0/1

Fain2(config-if)#switchport trunk native vlan 99

Fain2(config-if)#switchport mode trunk

3. Switch casa 3 Fain3

Fain3(config)#interface GigabitEthernet0/2

Fain3(config-if)switchport trunk native vlan 99

Fain3(config-if)switchport mode trunk

Configurados todos los puertos de los switch y pasado el tiempo de convergencia, que por defecto son cinco minutos en switch cisco, se verifican en todos los nodos clientes la configuración de las Vlan´s. El comando para realizar la verificación es show vlan brief, el resultado en cada uno de los switch es el siguiente:

1. Switch decanatura Fain1

Fain1#show vlan brief

```
VLAN Name                              Status Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/2
99   Management                        active
181  Impresoras                        active
200  WIFI                              active
240  Oficinas                          active
501  voz                               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005et-default                         active
```

2. Switch casa 2 Fain2

Fain2#show vlan brief

```
VLAN  Name                             Status Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/2
99   Management                        active
181  Impresoras                        active
200  WIFI                              active
240  Oficinas                          active
501  voz                               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
  1005et-default                       active
```

3. Switch casa 3 Fain3

Fain3#show vlan brief

```
VLAN      Name      Status Ports
---- -------------------------------- --------- ---------------
---------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                   Gig0/1
99 Management           active
181 Impresoras          active
200 WIFI                active
240 Oficinas            active
501 voz                 active
1002 fddi-default       active
1003 token-ring-default active
1004 fddinet-default    active
1005 trnet-default      active
```

Asignación de puertos

Una vez configuradas las Vlan, se procede a la configuración de puertos. Esto se realiza individualmente por cada switch o nodo porque los requerimientos son diferentes en cada departamento. También es posible la configuración de Vlan dinámicas, esto se realiza mediante un software, como por ejemplo CiscoWorks 2000. El software de administración VMPS (VLAN Management Policy Server o Servidor de Gestión de Directivas de la VLAN) permite al administrador asignar puertos de forma dinámica por medio de la dirección MAC del dispositivo o por medio de usuario y contraseña en consulta a una base de datos Ldap (Lightweight Directory Access Protocol). Este método no es parte de este trabajo, por lo cual la asignación de puertos se realiza de

forma estática en los nodos.

Los comandos para asignar un puerto o grupo de puertos a una vlan por cada sector de la red, son los siguientes:

Nodo FAIN

Vlan 240 Oficinas:

Fain1(config)#interface range fastEthernet 0/1-15

Fain1(config-if-range)#switchport mode access

Fain1(config-if-range)#switchport access vlan 240

Fain1(config-if-range)#exit

Vlan 181 impresoras:

Fain1(config)#interface fastEthernet 0/24

Fain1(config-if)#switchport mode access

Fain1(config-if)#switchport access vlan 181

Fain1(config-if)#exit

Vlan 200 WIFI:

Fain1(config)#interface giga0/1

Fain1(config-if)#switchport mode access

Fain1(config-if)#switchport access vlan 200

Fain1(config-if)#exit

Verificación de asignación de puerto con el comando show vlan brief.

VLAN	Name	Status	Ports
1	default	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Gig0/2

```
99   Management          active
181  Impresoras          active    Fa0/24
200 WIFI                 active    Gig0/1
240 Oficinas             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15
501  voz                 active
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
     1005et-default      active
```

Nodo FAIN2

Vlan 240:

Fain2(config)#interface range fastEthernet 0/1-15

Fain2(config-if-range)#switchport mode access

Fain2(config-if-range)#switchport access vlan 240

Fain2(config-if-range)#exit

Vlan 181 impresoras

Fain2(config)#interface fastEthernet 0/24

Fain2(config-if)#switchport mode access

Fain2(config-if)#switchport access vlan 181

Fain2(config-if)#exit

Vlan 200 WIFI

Fain2(config)#interface giga0/2

Fain2(config-if)#switchport mode access

Fain2(config-if)#switchport access vlan 200

Fain2(config-if)#exit

Verificación de asignación de puerto con el comando show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
99   Management                        active
181  Impresoras                        active    Fa0/24
200  WIFI                              active    Gig0/2
240 Oficinas                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15
501  voz                               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
     1005et-default                    active
```

Nodo FAIN3

Vlan 240:

Fain3(config)#interface range fastEthernet 0/1-15

Fain3(config-if-range)#switchport mode access

Fain3(config-if-range)#switchport access vlan 240

Fain3(config-if-range)#exit

Vlan 181 impresoras:

Fain3(config)#interface fastEthernet 0/24

Fain3(config-if)#switchport mode access

Fain3(config-if)#switchport access vlan 181

Fain3(config-if)#exit

Vlan 200 WIFI:

Fain3(config)#interface giga0/1

Fain3(config-if)#switchport mode access

Fain3(config-if)#switchport access vlan 200

Fain3(config-if)#exit

Verificación de asignación de puerto con el comando show vlan brief.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
99   Management                        active
181  Impresoras                        active    Fa0/24
200  WIFI                              active    Gig0/1
240 Oficinas                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15
501  voz                               active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Configuración SLAAC

Para configurar SLAAC en el router, se debe habilitar en el router la configuración IPv6, con el comando IPv6 unicast-routing, el cual activa las funciones de IPv6.

R1(config)#ipv6 unicast-routing. Luego, se asigna una dirección a la puerta de enlace de la red, esto se realiza con los siguientes comandos:

R1(config)#interface fa0/1

R1(config-if)#ipv6 address 2001:1111:2222:3333::1/64

La dirección utilizada en la interface fast ethernet 0/1 del router es 2001:1111:2222:3333::1/64, lo que indica a la red el prefijo de la red para todos los nodos.

En los host, se debe elegir la opción autoconfiguración como se muestra en la Figura 25 que otorgará el direccionamiento mediante la respuesta de las RS (routing solicitation) emitidas por el host y la respuesta del router RA (router advertisement) emitidas a los host con la configuración solicitada. Estos, con la configuración EUI-64, configuran la dirección IPv6 propia. Esta es la funcionalidad nativa de IPv6 para obtener direccionamiento en una red, eliminando el concepto de DHCP (Dynamic Host Configuration Protocol).

DHCPv6 sin estado, dual stack

En este apartado, se configura un DHCPv6 sin estado para analizar la configuración como el tiempo de respuesta de la red. Un servidor DHCP sin estado puede ser configurado en un router, idealmente lo más cercano al cliente, permitiendo reducir el tráfico en la red.

Este servidor entrega los parámetros requeridos por el HOST al momento de ser solicitados, pero no guarda registros de a quien se le asignó dicho direccionamiento. En el router principal, se debe realizar la configuración del DHCPv6 sin estado, siguiendo los siguientes pasos:

El primer paso es activar el routing IPv6 en el router. No se necesita para el DHCPv6, pero sí para que el router genere las RA y se activa con el siguiente comando:

UnACh(config)#ipv6 unicast-routing

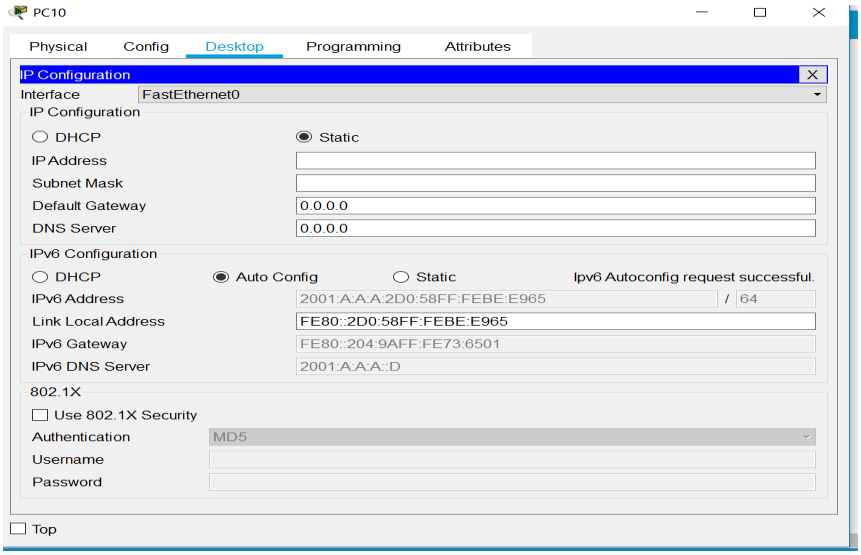


Figura 25. Configuración automática IPv6.

El segundo paso es activar el DHCPv6 pool con las direcciones o prefijo que asigna el servidor al host de la red. En el comando, luego de ingresados, debe aparecer la línea que indica config-dhcpv6 como indica en las siguientes líneas de comando ingresadas en el router:

UnACh(config)#ipv6dhcp pool UnACh1

UnACh(config-dhcpv6)#

El nombre del pool asignado para este ejemplo es UnACh1 y pueden existir varios pool´s para diferentes Vlan como sean necesarios. Para efectos prácticos, solo se realiza un ejemplo en el presente trabajo, dado que en los demás es solo repetir la misma secuencia.

Configurar el pool con los parámetros de la red

Durante el proceso de SLAAC, el host recibe la configuración para obtener una dirección de unidifusión global. Dentro de los parámetros recibidos está la dirección de

gateway que es la dirección de origen (source) de los mensajes RA, siendo esta la dirección link local que posee el router. En el caso del servidor DHCPv6, se puede configurar para entregar otros parámetros que no fueron enviados por la configuración automática SLAAC aplicada en el proceso anterior. En las siguientes líneas de comando, se ingresan el nombre de dominio y la dirección del DNS de la red:

```
UnACh(config-dhcpv6)#dns-server 2001:a:a:a::000d
UnACh(config-dhcpv6)#domain-name unach.com
```

Después se une la configuración del pool con la interface. Los comandos utilizados para vincular la interface, en este caso la fastEthernet 0/0, vinculan el dhcp server con el nombre del pool configurado. Esto se realiza con IPv6 dhcp server *nombre-pool*. Otra configuración que se debe realizar la cual marca la diferencia con SLAAC, es el cambio del indicador O de 0 a 1. Este le indica al host cuando recibe los mensajes RA que existe información adicional, la cual se encuentra en el servidor DHCPv6 sin estado y se realiza ingresando el comando ipv6 nd other-config-flag.

```
UnACh(config)#interface fastEthernet 0/0
UnACh(config-if)#ipv6 address 2001:a:a:a::/64 eui-64
UnACh(config-if)#ipv6 dhcp server UnACh1
UnACh(config-if)#ipv6 and other-config-flag
```

Después se verifica en el host la obtención de los parámetros configurados, como se aprecia en la Figura 26.

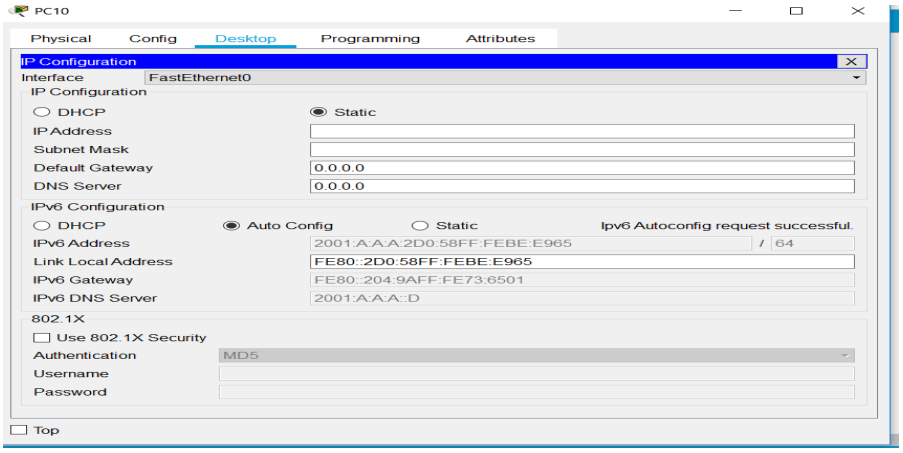


Figura 26. Configuración automática del host.

En la consola de comandos, se puede ingresar el comando IPv6config para ver por este medio lo parámetros de la red. El resultado es el siguiente:

C:\>ipv6config

FastEthernet0 Connection:(default port)

Link-local IPv6 Address.....: FE80::2D0:58FF:FEBE:E965

IPv6 Address.....: 2001:A:A:A:2D0:58FF:FEBE:E965/64

Default Gateway.....: FE80::204:9AFF:FE73:6501

DHCPv6 IAID.....: 32552

DHCPv6 Client DUID.....: 00-01-00-01-9A-CA-9A-94-00-D0-58-BE-E9-65

Para la configuración dual stack, se crea primeramente el Pool IPv4 para cada DHCPv4 en que son aplicados a cada LAN. En el ejemplo se configura un escenario que se representa por un router y dos redes distintas con un switch y un pc cada una, como se observa en la Figura 27, con las respectivas direcciones asignadas a las interfaces. Para este proceso se siguen los siguientes pasos:

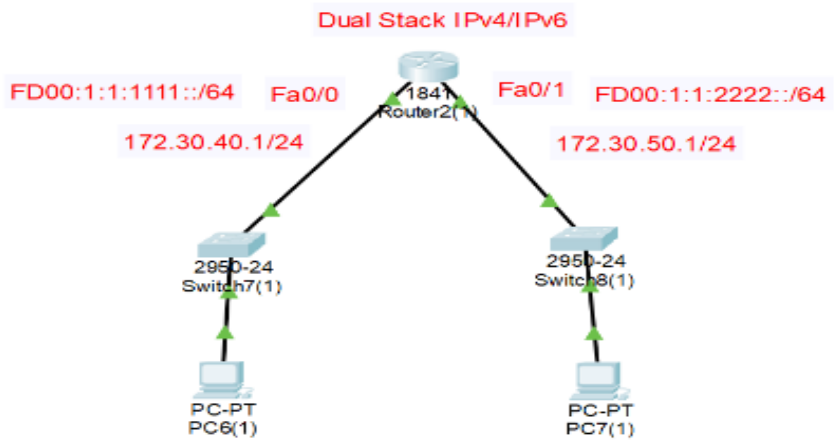


Figura 27. Escenario Dual Stack.

Paso 1. Se deben excluir las direcciones que son asignadas estáticamente en la red y que son parte del direccionamiento IPv4 de la red. En este caso son las direcciones del puerto gateway del router a la que se ha asignado una dirección estática y a servidores los cuales siempre deben tener direcciones estáticas. También se pueden excluir otras direcciones para guardarlas en uso futuro por parte de los administradores de la red. Los comandos para excluir las direcciones son los siguientes:

Router(config)#ip dhcp excluded-address 192.168.40.1 255.255.255.0

Router(config)#ip dhcp excluded-address 192.168.50.1 255.255.255.0

Se excluyeron las direcciones de los dos gateway.

Paso 2. Configurar el pool que el servidor DHCP tendrá para asignar direcciones a los hosts. Para la primera red se asignó el nombre RedA. Primero se crea el pool llamado RedA con el comando ip dhcp pool RedA. Luego se ingresa la dirección de red y la máscara que le indica al servidor el número total de direcciones asignables a

Host menos las excluidas con el comando network dir *red-máscara de subred*. En tercer lugar se ingresa una dirección de un servidor DNS. En este caso, se ingresa una dirección ficticia como por ejemplo, pero en una red real se debe ingresar la IP del servidor correspondiente y el comando es dns-server *ipaddress-servidor*. En el último paso se ingresa la dirección por donde la red se comunica con la WAN. En este caso, el gateway con el comando default-router address.

RedA:

Router(config)#ip dhcp pool RedA

Router(dhcp-config)#network 172.30.40.0 255.255.255.0

Router(dhcp-config)#dns-server 172.30.10.10

Router(dhcp-config)#default-router 172.30.40.R1

RedB:

Router(config)#ip dhcp pool RedB

Router(dhcp-config)#network 172.30.50.1 255.255.255.0

Router(dhcp-config)#dns-server 172.30.10.10

Router(dhcp-config)#default-router 172.30.50.1

Paso 3. Verificar la configuración del servidor DHCPv4 para las dos redes. Esto se puede hacer de dos formas: (a) la primera es en los hosts, ingresar y configurar para que obtengan direccionamiento por DCHP y (b) la segunda es en el router para verificar las direcciones entregadas. En la Figura 28 y en la Figura 29, se observa los dos PC configurados con sus respectivas direcciones obtenidas.

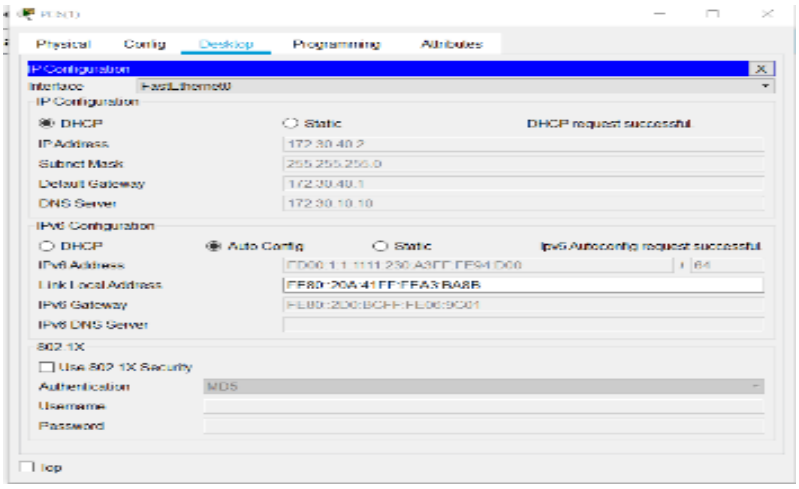


Figura 28. Configuración PC RedA en Dual Stack.

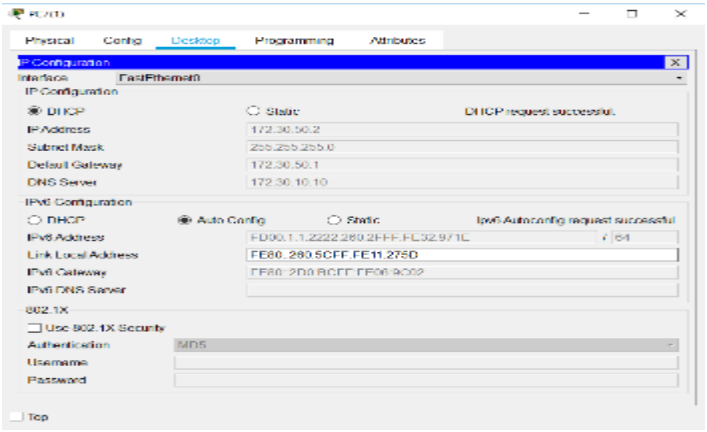


Figura 29. Configuración PC RedB en Dual Stack.

Para verificar en el servidor las direcciones entregadas, se realiza con el siguiente comando:

Router#show ip dhcp binding

IP address Client-ID/ Lease expiration Type Hardware address

172.30.40.2 000A.41A3.BA8B -- Automatic

172.30.50.2 0060.5C11.275D -- Automatic

Al observar las Figuras 28 y 29, la información obtenida del router, se observa que las direcciones son las correctas, por lo cual el servidor DHCPv4 está operando de forma correcta y la configuración Dual Stack es completamente operativa.

DHCPv6 con estado, dual stack

La topología usada para implementar el servidor Dual Stack junto con Vlan y el servidor DHCPv4 externo en otra red, de modo de poder mostrar la forma de configurar los relay UDP en el router (ver Figura 30), es la siguiente:

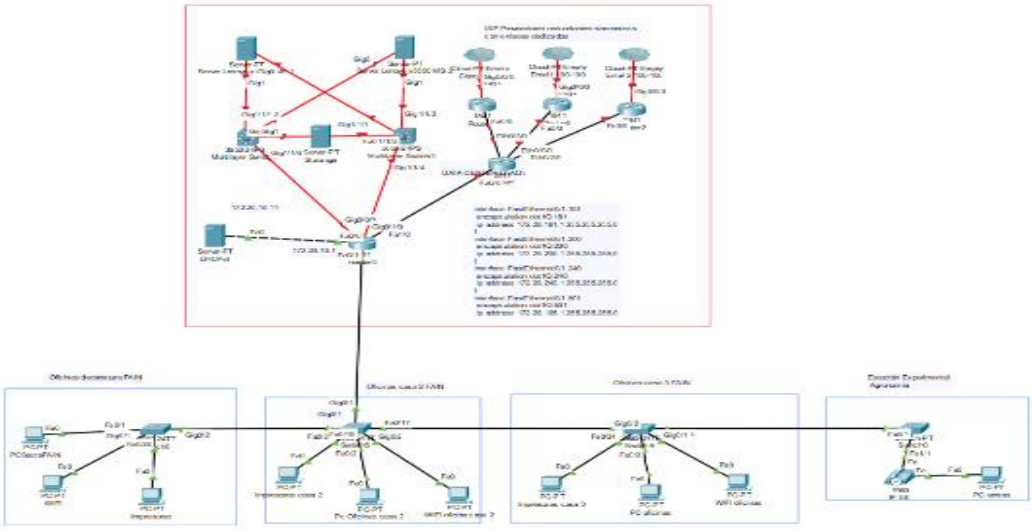


Figura 30. Topología utilizada para pruebas.

En la tipología de la Figura 30, se muestran los elementos que la red real de la universidad tiene. Por ejemplo, la sección del router que divide las redes lan de la lan de los servidores en el data center institucional, router 3. En esta zona de servidores se encuentra el servidor DHCPv4 que entrega el direccionamiento a las redes de los distintos departamentos de la institución. Se utiliza como ejemplo la FAIN, por ser la

más lejana. Además, enlaza la estación experimental de la carrera de agronomía y el laboratorio de micropropagación. La configuración de la Vlan ya realizada, se mantiene, solo que ahora se deben configurar los dos servidores DHCP para que entreguen direccionamiento a los distintos nodos de cada una de las Vlan. Para esto, se configura el servidor DHCPv4 y DHCPv6, con los pools´s de direcciones (ver Tabla 6) para cada una de las Vlan´s. La configuración del DHCPv4 es la siguiente:

Tabla 6

Direccionamiento del pool´s DHPv4

Pool Name	Default Gate-	Dns Server	Star Ip Address	Subnet Mask	Max user
4unach240	172.20.240.1	172.20.10.10	172.20.240.10	255.255.255.0	246
4unach200	172.20.200.1	172.20.10.10	172.20.200.10	255.255.255.0	246
4unach181	172.20.181.1	172.20.10.10	172.20.181.10	255.255.255.0	246
4unach501	172.20.105.1	172.20.10.10	172.20.105.10	255.255.255.0	246

Cada uno de los Pool v4 fueron configurados utilizando como puerta de enlace (gateway) la dirección IP de la subinterfaz del router 3. Esta configuración es las siguiente:

interface FastEthernet0/1.181

encapsulation dot1Q 181

ip address 172.20.181.1 255.255.255.0

```
ip helper-address 172.20.10.11
ipv6 address 2001:1111:2222:181::1/64
ipv6 dhcp server unach181
interface FastEthernet0/1.200
encapsulation dot1Q 200
ip address 172.20.200.1 255.255.255.0
ip helper-address 172.20.10.11
ipv6 address 2001:1111:2222:200::1/64
ipv6 dhcp server unach200
interface FastEthernet0/1.240
encapsulation dot1Q 240
ip address 172.20.240.1 255.255.255.0
ip helper-address 172.20.10.11
ipv6 address 2001:1111:2222:240::1/64
ipv6 dhcp server unach240
interface FastEthernet0/1.501
encapsulation dot1Q 501
ip address 172.20.105.1 255.255.255.0
ip helper-address 172.20.10.11
ipv6 address 2001:1111:2222:501::1/64
ipv6 dhcp server unach181
```

Para cada Vlan se creó una subinterfaz en el router, utilizando como troncal la FastEthernet 0/1. Una vez que se crea la subinterfaz, se debe configurar el tipo de

encapsulamiento IEEE 802.1Q, el cual permite compartir el mismo medio físico a diferentes redes lan, utilizando para esto el puerto principal como troncal (truck). Los comandos utilizados son los siguientes:

interface FastEthernet0/1.181

encapsulation dot1Q 181

Luego se les asigna una dirección IPv4 que es la gateway para cada una de las Vlan. El comando utilizado es el siguiente:

ip address 172.20.181.1 255.255.255.0

Hasta este momento, se tiene configurado el servidor DHCPv4 y todas las configuraciones en el router como subinterfaces con sus respectivas direcciones, pero el servidor DHCPv4 se encuentra en una red distinta a la de los hosts, por lo cual no podrán obtener los parámetros de configuración, debido a que el router no deja pasar los paquetes UDP 67 servidor y puerto UDP 68 cliente. Para que estos paquetes puedan pasar, el servidor debe configurar en el router este servicio mediante el siguiente comando para cada una de las subinterfaces:

ip helper-address “dirIp servidor DHCPv4”

Este comando habilita el reenvío de los paquetes UDP a la dirección especificada, la cual debe ser la del servidor DHCPv4.

Para el caso de los pools IPv6, se configuran en el router los pools de la siguiente forma:

ipv6 dhcp pool unach181

address prefix 2001:1111:2222:0181::/64 lifetime 172800 86400

dns-server 2001:1111:2222:3333::100

domain-name unach.com

Donde ipv6 dhcp pool name pool es el comando para crear el pool y el nombre unach181 corresponde al namel pool. En este ejemplo, se agrega el número de la Vlan en la cual se va a utilizar como forma de ordenar y recordar con facilidad a que Vlan pertenece el pool configurado.

Con el comando address prefix prfixIpv6/largo prefix liftetime duración, se configuran el prefijo IPv6 que tendrán las interfaces. Además del tiempo de vida que tendrá la asignación por parte del servidor, en este caso se utiliza el tiempo máximo permitido.

DNSv6

El comando dns-server estipula la dirección del servidor de resolución de nombre de dominio que se utiliza para la red IPv6, que no es el mismo servicio que IPv4, para lo cual se debe configurar un servicio distinto para IPv6 con registros A para IPv4/IPv6, los cuales deben ser idénticos. Por lo tanto, los registros AAAA para IPv6 deben ser ingresados con las mismas direcciones de dominio y su respectiva dirección IPv6. En el ejemplo siguiente se muestra una entrada de un servidor DNSv6 realizada en un servidor.

ejemplo-host EN AAAA 2830: 0: 1edf: j1ok: b25c :: 5

Al configurar una entrada DNSv6 en el servidor, se deben también configurar los registros PTR (DNS inverso necesario para resolver una dirección IP a un nombre de dominio). Existen servicios de DNS inverso. Por ejemplo, la página web http://rdns6.com/ es una de ellas que permite obtener los detalles para realizar las configuraciones correctas en el servidor de la institución. No todos los registros se

deben ingresar manualmente, sino que se debe realizar una sincronización con servidores DNS de orden superior de los ISP, lo que permite obtener los registros de forma automatizada, quedando solo los subdominios locales que la institución cree para ser registrados de forma manual.

En la página Invertir DNS v6, mencionada en el párrafo anterior, se generan los registros de forma automática, lo que permite al administrador generar la entrada para BIND de forma rápida (Al-Ani, Anbar, Manickam y Al-Ani, 2019). Aunque esta parte de la red está en contrato con una empresa externa y no es parte de este trabajo, se muestra un ejemplo a modo ilustrativo para que los lectores puedan utilizar este recurso que facilita el trabajo del administrador de servidores. La Figura 31 muestra las entradas ejemplo.

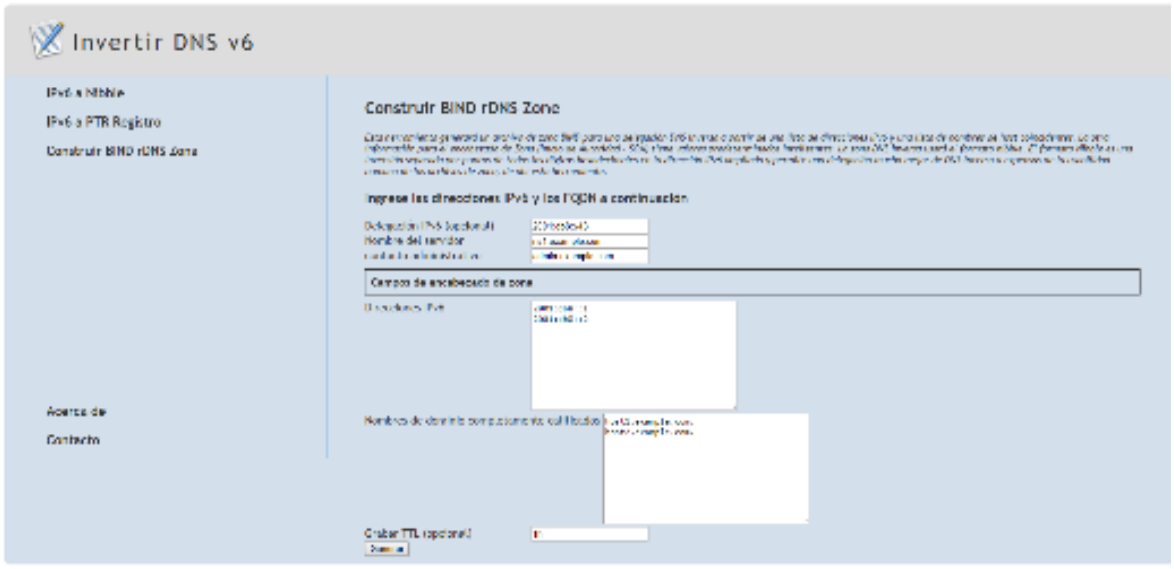


Figura 31. Entradas para obtener DNS inverso de un nombre de dominio.

Al generar la entrada se obtiene un código para ser ingresado en el registro BIND. A continuación se mencionan:

2001: db8 :: / 48

Archivo de zona creado con el generador de zonas DNS inverso de IPv6

http://rdns6.com/

$TTL 1h; TTL predeterminado

@ IN SOA ns1.example.com. admin.ejemplo.com. (

2019080401; de serie

1h; intervalo de actualización de esclavos

15m; intervalo de reintento de esclavo

1w; copia esclava expirar tiempo

1h; Tiempo de caché de NXDOMAIN

servidores de nombres de dominio

@ IN NS ns1.example.com.

Entradas de IPv6 PTR

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.bd0.1.0.0.2.ip6.arpa. EN PTR host1.example.com.

2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.bd0.1.0.0.2.ip6.arpa. EN PTR host2.ejemplo.com.

Resultados Dual Stack

En las Figuras 32, 33 y 34, se muestran los resultados finales de la configuración realizada para cada una de las Vlan, como se mostró en las secciones anteriores.

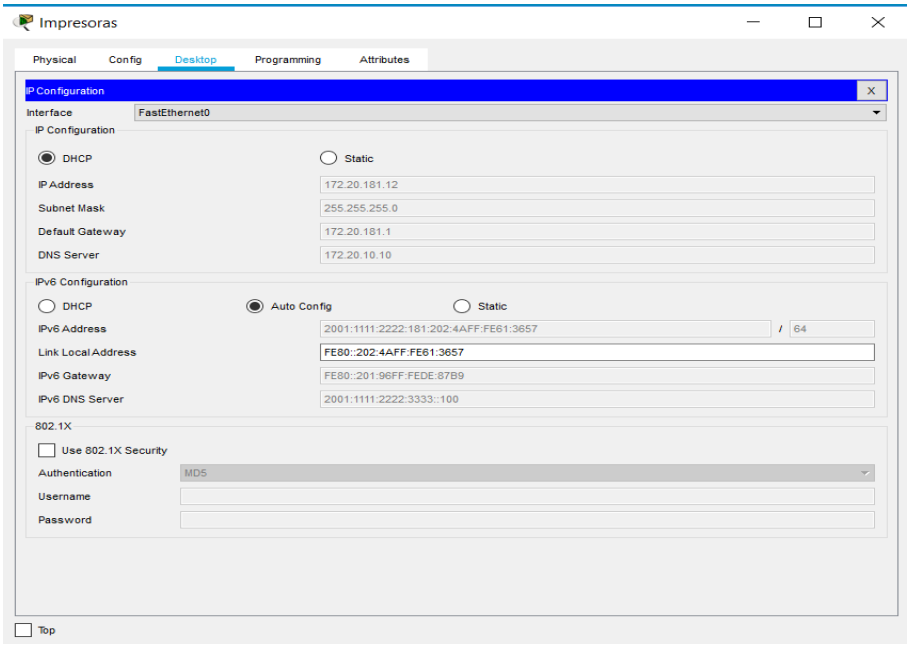


Figura 32. Dual Stack Vlan 181 Impresoras.

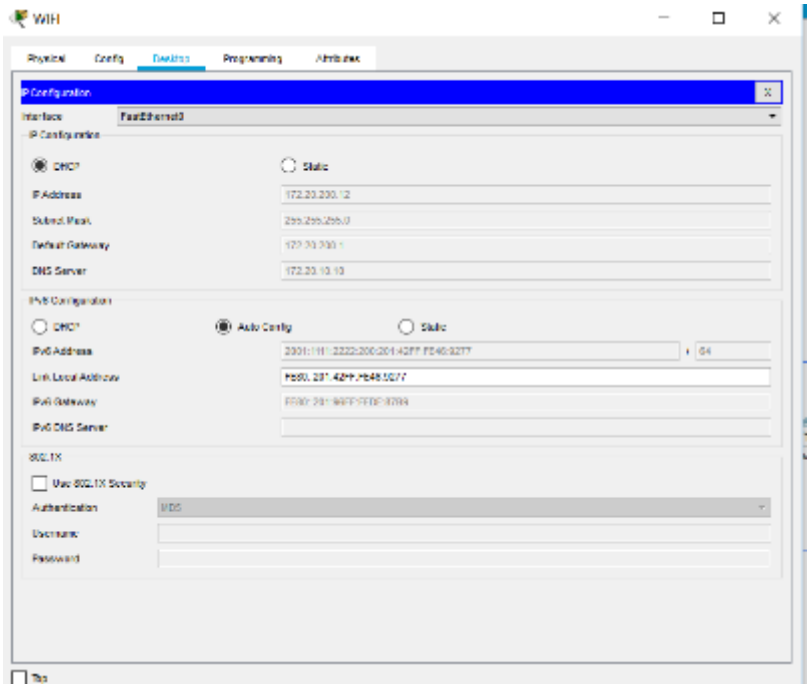


Figura 33. Dual Stack Vlan 200 wifi.

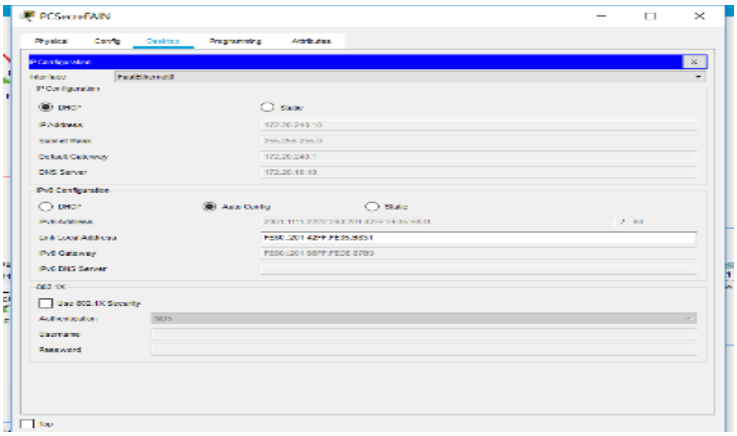


Figura 34. Dual Stack Vlan 240 Oficinas.

Configuración del router

La configuración completa del router, para que pueda funcionar con Vlan enrutamiento, DCHv6 y con DHCPv4 externo, es la siguiente:

ipv6unicast-routing

no IPv6 cef

ipv6dhcp pool unach181

address prefix 2001:1111:2222:0181::/64 lifetime 172800 86400

dns-server 2001:1111:2222:3333::100

domain-name unach.com

ipv6dhcp pool unach200

address prefix 2001:1111:2222:0200::/64 lifetime 172800 86400

dns-server 2001:1111:2222:3333::100

domain-name unach.com

ipv6 dhcp pool unach240

prefix-delegation pool unach240 lifetime 2592000 604800

address prefix 2001:1111:2222:0240::/64 lifetime 172800 86400

dns-server 2001:1111:2222:3333::100

domain-name unach.com

ipv6 dhcp pool unach501

address prefix 2001:1111:2222:0501::/64 lifetime 172800 86400

dns-server 2001:1111:2222:3333::100

domain-name unach.com

interface FastEthernet0/0

ip address 172.20.10.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

no ip address

ip helper-address 172.20.10.11

duplex auto

speed auto

interface FastEthernet0/1.181

encapsulation dot1Q 181

ip address 172.20.181.1 255.255.255.0

ip helper-address 172.20.10.11

ipv6 address 2001:1111:2222:181::1/64

ipv6 dhcp server unach181

interface FastEthernet0/1.200

encapsulation dot1Q 200

ip address 172.20.200.1 255.255.255.0

ip helper-address 172.20.10.11

ipv6 address 2001:1111:2222:200::1/64

ipv6 dhcp server unach200

interface FastEthernet0/1.240

encapsulation dot1Q 240

ip address 172.20.240.1 255.255.255.0

ip helper-address 172.20.10.11

ipv6 address 2001:1111:2222:240::1/64

ipv6 dhcp server unach240

interface FastEthernet0/1.501

encapsulation dot1Q 501

ip address 172.20.105.1 255.255.255.0

ip helper-address 172.20.10.11

ipv6 address 2001:1111:2222:501::1/64

ipv6 dhcp server unach181

interface Vlan1

no ip address

shutdown

router rip

version 2

network 172.20.0.0

Mediciones

Las mediciones se obtienen realizando ping desde los nodos de cada una de las Vlan a la dirección gateway correspondiente, lo que permite medir el tiempo de respuesta en cada una de las Vlan. En este apartado, se individualizan las mediciones a cada una de las Vlan.

Vlan 240 oficinas

Al ejecutar el comando ping hacia la puerta de enlace IPv6 de la Vlan 240 (ver Figura 35), se obtiene conectividad exitosa con un tiempo de respuesta de 1ms, con cuatro paquetes enviados y cuatro recibidos.

Al realizar ping a la gateway de la Vlan 240 en IPv4 (ver Figura 36), se obtiene un tiempo de respuesta de 1 ms, con cuatro paquetes enviados y cuatro recibidos.

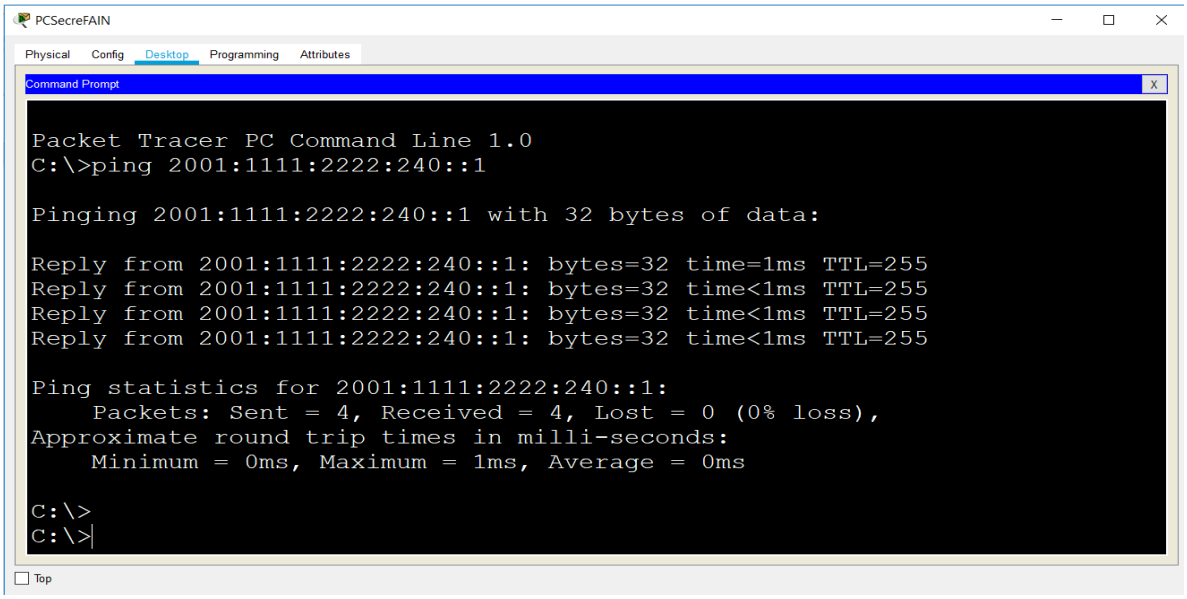


Figura 35. Resultados ping IPv6 Vlan 240.

```
C:\>ping 172.20.240.1

Pinging 172.20.240.1 with 32 bytes of data:

Reply from 172.20.240.1: bytes=32 time<1ms TTL=255
Reply from 172.20.240.1: bytes=32 time<1ms TTL=255
Reply from 172.20.240.1: bytes=32 time=1ms TTL=255
Reply from 172.20.240.1: bytes=32 time=1ms TTL=255

Ping statistics for 172.20.240.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figura 36. Resultados ping IPv4 Vlan 240.

Vlan 181 Impresoras

Al ejecutar el comando ping hacia la puerta de enlace IPv6 de la Vlan 181 (ver 37), se obtiene conectividad exitosa con un tiempo de respuesta de 1ms.

Al ejecutar el comando ping hacia la puerta de enlace IPv4 de la Vlan 181 (ver Figura 38), se obtiene conectividad exitosa con un tiempo de respuesta de 1ms.

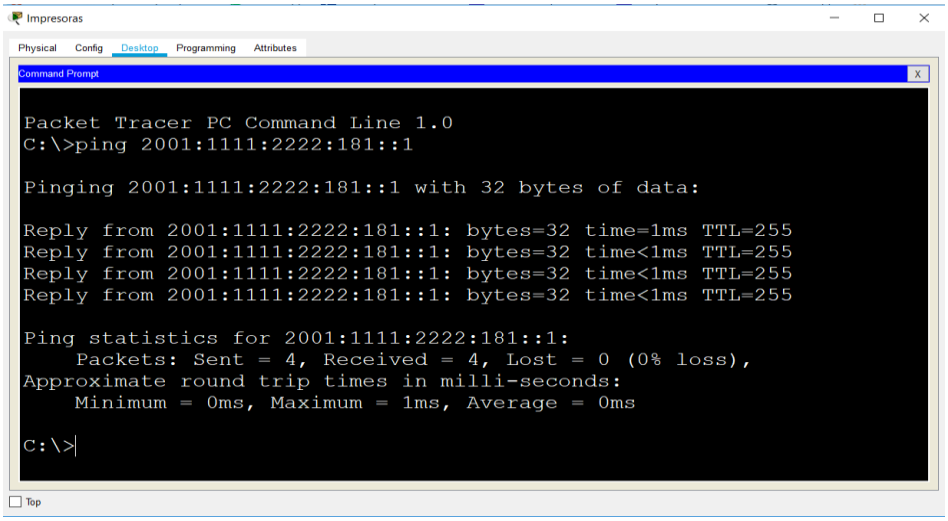


Figura 37. Resultados ping IPv6 Vlan 181.

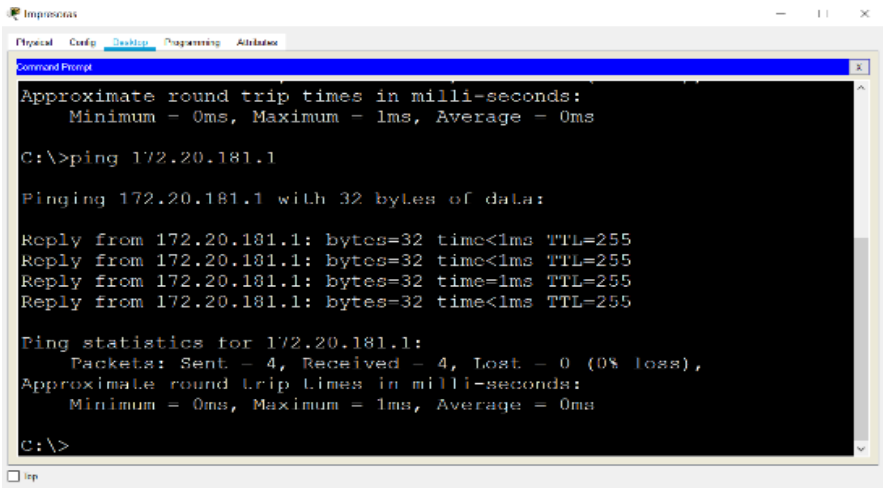


Figura 38. Resultados ping IPv4 Vlan 181.

Vlan 200 wifi oficinas

Al ejecutar el comando ping hacia la puerta de enlace IPv6 de la Vlan 200 (ver Figura 39), se obtiene conectividad exitosa con un tiempo de respuesta de 1ms.

Al ejecutar el comando ping hacia la puerta de enlace IPv4 de la Vlan 200 (ver 40), se obtiene conectividad exitosa con un tiempo de respuesta de 1ms.

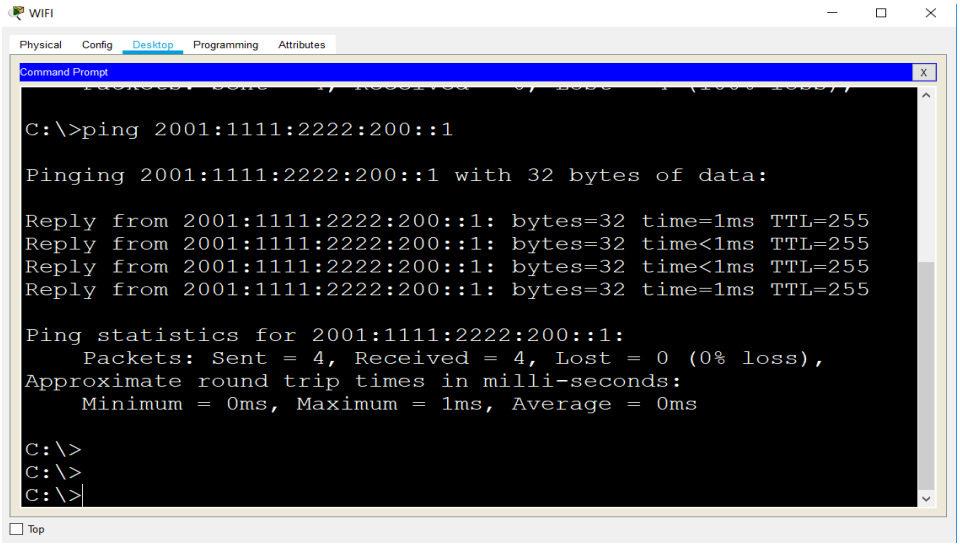


Figura 39. Resultados ping IPv6 Vlan 200.

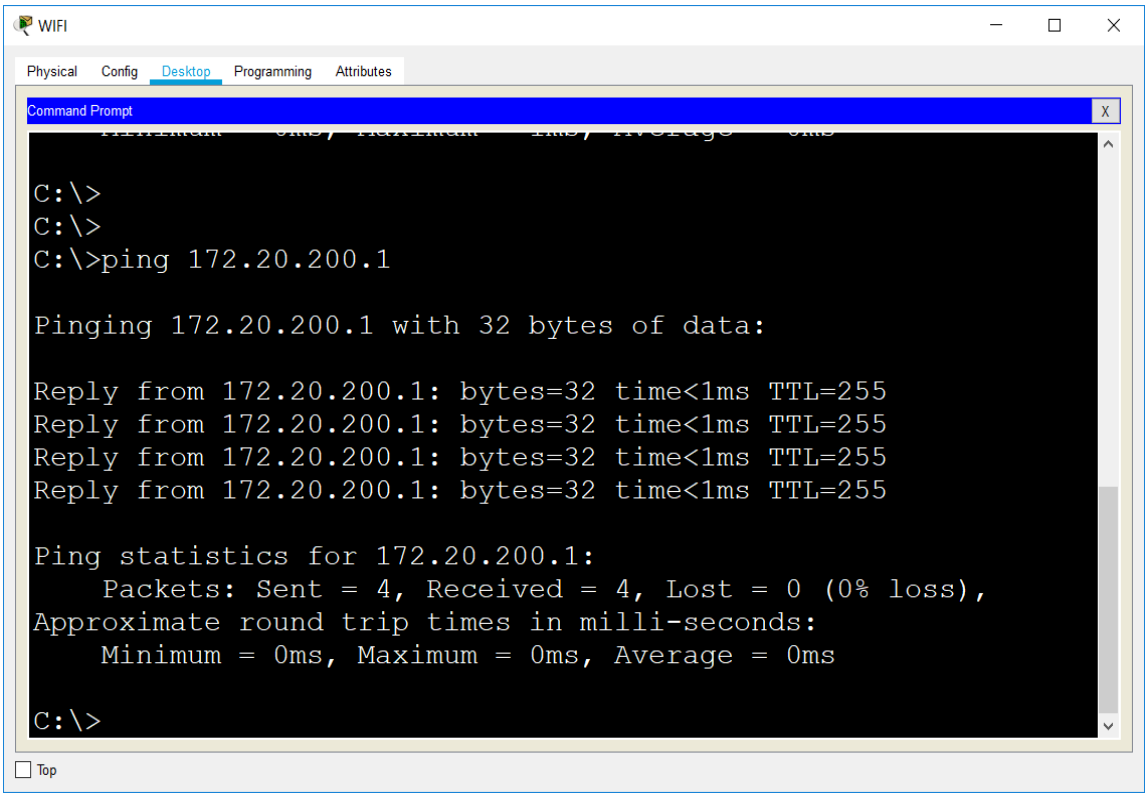


Figura 40. Resultados ping IPv4 Vlan 200.

CAPÍTULO IV

DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

Introducción

En el capítulo II se identifica la situación de las redes en general y cómo el agotamiento de IPv4, a nivel mundial, está produciendo un cambio a todo nivel, tanto de ISP como de las instituciones, y no todas están preparadas con protocolos definidos y configuraciones de pruebas establecidos para migrar de forma transparente para el usuario final. En este contexto, se plantea el problema que tiene la UnACh en sus redes, además de las ventajas de migrar al nuevo protocolo IPv6 y la justificación del presente proyecto basados en estadísticas a nivel mundial del proceso de migración y del contenido web exclusivo para el nuevo protocolo que no va a poder ser acceder desde IPv4. A partir de estos planteamientos, se proponen los objetivos; (a) análisis de la situación actual de las redes en una institución de educación superior, (b) entregar hoja de ruta que permita llevar a cabo el cambio de protocolo de forma transparente para el usuario, (c) determinar los beneficios al usar el nuevo protocolo IPv6, (d) realizar configuraciones en diferentes escenarios, (e) documentar configuración Dual Stack, (f) realizar simulación en Software Cisco Packet Tracer (g) crear Vlan con configuración Dual Stack y (h) obtener resultados de conectividad. Se realiza un estudio de las limitaciones y delimitaciones que afectan al proyecto como son: recursos financieros, hardware, software y alcances del proyecto, para enfocar el tema con mayor

precisión posible para no abarcar fuera del contexto que se pretende en los objetivos. Se plantea un marco filosófico sobre dos analogías que son la semana de la creación y el modelo de referencia OSI y la oración como modelo de comunicación con Dios y los protocolos de comunicación existentes hoy.

El capítulo II desarrolla el concepto general y profundo, en algunos puntos, del estado del arte en el ámbito técnico, analizando las normas que el IETF establece para el nuevo protocolo. Estas normas llamadas RFC hacen referencia a cada uno de los aspectos de cada una de ellas en lo particular, como es el IPv6, la seguridad IPsec, las cabeceras adicionales y el direccionamiento, entre otros. También se describen los comandos a ser utilizados en la plataforma CISCO y las ventajas y desventajas de los distintos protocolos de migración existentes.

En el capítulo III, se realizan la aplicación del proyecto propuesto, simulado en Packet Tracer, permitiendo tener diferentes escenarios de configuración posibles en el momento del cambio, como es la obtención de IP´s automáticas en IPv6, mediante el protocolo EUI-64, utilizando DHCPv6 sin estado y con estado. Además de plantear una red que tiene Vlan, el modelo Dual Stack establecido, debe funcionar en ese ambiente. Además de considerar que el servidor DHCPv4 no se encuentra en la misma red del host, por lo que se debió tener en cuenta todos estos parámetros en la configuración del escenario de trabajo.

En el capítulo IV, se presentan los resultados de los objetivos específicos plan-teados en el capítulo I y se ofrecen las conclusiones, las discusiones y las recomen-daciones para trabajos futuros que pueden ser abordados como nuevos trabajos de investigación.

Discusión

Ya obtenidos los resultados de las diferentes configuraciones y la propuesta de Dual Stack desarrollada en el capítulo III, se puede establecer que es posible realizar los cambios en la red de la UnACh y migrar al protocolo IPv6 sin dejar del todo en una primera fase el antiguo protocolo IPv4, que estará presente por varios años más con direccionamiento privado dentro de las instituciones. Las ventajas de tener IPv6 en la red permiten una mayor seguridad de los datos porque la transferencia de los datos se realiza de forma encriptada. Esto porque IPsec en IPv6 es obligatorio y no optativo como en la versión 4. Las configuraciones más complejas se dieron en el modelo que integra, no solo Dual Stack, sino que también Vlan, debido a que el servidor DHCPv4 no se encuentra en la misma Lan de los nodos finales (host). Al tener un router, el cual obstaculiza el paso del tráfico UDP, impedía que los hosts pudieran obtener direccionamiento, para ello fue necesario investigar la forma en que se debe realizar, pero la poca documentación existente sobre este caso se tornó difícil encontrar la solución que al final es simple, solo se debe autorizar el paso de los paquetes UDP a la dirección específica del servidor DHCP en el router. Finalmente, se estableció la configuración correcta que permite trabajar la red, con las Vlan que sean necesarias, que en el caso de este trabajo se utilizaron tres Vlan, la de impresiones, utilizada en la red de impresoras, la de wifi y la de oficinas. Otras Vlan solo deben seguir los mismos pasos, ya que es solo repetir los pasos de las anteriores, como es crear las Vlan, asignación de puertos, creación de Pool DHCP para IPv6/IPv4, creación de sub-interfaces, con la

asignación de las puertas de enlace y la encapsulación y por último los puertos troncales en cada dispositivo (switch) para que las comunicaciones de las Vlan se puedan realizar.

Conclusiones

Este trabajo presenta un desarrollo en el ámbito bibliográfico como una simulación del proyecto de migración de IPv4 a IPv6 en la UnACh. Se realizó un análisis de la red en la UnACh y se obtuvo información de la penetración a nivel mundial de los prefijos IPv6, de las páginas web nativas en IPv6 para Chile y México. Se desarrolló en las configuraciones que permite al administrador de la red, seguir los pasos necesarios para realizar la migración y, para poner en producción lo planteado en el presente trabajo. Se establecen las ventajas de migrar de forma paulatina a IPv6 con el mecanismo Dual Stack, de acuerdo al análisis bibliográfico realizado. Se configuraron los diferentes escenarios, los cuales se programaron en Packet Tracer, viendo su funcionamiento en este ambiente simulado. Se documentan las configuraciones del escenario Dual Stack. Se desarrollan los escenarios de simulación, aplicando Vlan y mostrando los resultados de conectividad.

Recomendaciones

En trabajos futuros, se recomiendan los siguientes aspectos:

1. Desarrollar estudios de seguridad en la red, aplicando Machinne learnig.

2. Implementar seguridad adicional en bases de datos, utilizando tecnología Blockchain.

3. Desarrollar estudio sobre aplicación de servidor de Vlan dinámicas.

4. Estudiar el comportamiento en un escenario real, utilizando herramientas de software como QNet o similares, para la simulación de tráfico en la red.

5. Ampliar el estudio de esta investigación a otras instituciones de diversos tamaños.

REFERENCIAS

Al-Ani, A. K., Anbar, M., Manickam, S. y Al-Ani, A. (2019). DAD-match; Security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network. *PLOS ONE*, *14*(4), 1-20. https://doi.org/10.1371/journal.pone.0214518

Andrada, A. M. (2017). *Nuevas tecnologías de la información y la conectividad/ nticx: Dispositivos, saberes y prácticas* (2a. ed.). Buenos Aires: Maipue.

Ariganello, E. y Barrientos Sevilla, E. (2015a). *Redes Cisco*. Madrid: RA-MA.

Ariganello, E. y Barrientos Sevilla, E. (2015b). *Redes Cisco: guía de estudio para la certificacion ccnp routing y switching* (3a. ed.). Madrid: RA-MA.

Bautista, R., Willmer, D., Cárdenas, M., Constanza, Y., Jaimes, S. y Marina, L. (2008). IPSec DE IPv6 en la Universidad de Pamplona. *Scientia Et Technica, 15*(39), 320–325.

Boronat Seguí, F. y Montagud Climent, M. (2013). *Direccionamiento e interconexión de redes basada en TCP/IP: IPV4, IPV6, DHCP, NAT, encaminamiento RIP y OSPF* (1a. ed.). Valencia: Universitat Politécnica de Valencia.

Boucadair, M. y Venaas, S. (2014). *Updates to the IPv6 multicast addressing architecture*. Recuperado de https://www.rfc-editor.org/rfc/rfc7371.txt

Carpenter, B. y Moore, K. (2001). *Connection of IPv6 domains via IPv4 clouds*. Recuperado de https://www.rfc-editor.org/rfc/rfc3056.txt

Cisco Systems. (2019). *6Lab*. Recuperado de https://6lab.cisco.com/

Deering, S. y Hinden, R. (2017). *Internet protocol, version 6 (IPv6) specification.* Recuperado de https://www.rfc-editor.org/rfc/rfc8200.txt

Draves, R. (2003). *Default address selection for internet protocol, version 6 (IPv6)*. Recuperado de https://www.rfc-editor.org/rfc/rfc3484.txt

Droms, R. (2014). *IPv6 Multicast Address Scopes.* Recuperado de https://www.rfc-editor.org/rfc/rfc7346.txt

Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. y Carney, M. (2003). *Dynamic Host Configuration Protocol for IPv6 (DHCPv6).* Recuperado de https://www.rfc-editor.org/rfc/rfc3315.txt

El Khadiri, K., Labouidya, O., Elkamoun, N. y Hilal, R. (2018). Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET modeler. *IJACSA: International Journal of Advanced Computer Science and Applications, 9*(4). https://doi.org/10.14569/IJACSA.2018.090454

Franco Reboreda, C. A. y Rodríguez Elizondo, T. (2017). *Estado actual de las tecnologías de la información y las comunicaciones en las instituciones de educación superior en México* (Vol. 1). México: ANUIES.

Flores, S. U., Berón, M., Riesco, D. E. y Rangel Henriques, P. (2018). *Diseño y construcción de sistemas de IoT seguros y escalables*. Conferencia presentada en el XX Workshop de Investigadores en Ciencias de la Computación. Universidad Nacional del Nordeste).

Gilligan, R. y Nordmark, E. (2000). *Transition mechanisms for IPv6 hosts and routers.* Recuperado de https://www.rfc-editor.org/rfc/rfc2893.txt

Google IPv6. (2017). *Estadística adopción IPv6*. Recuperado de https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption.

Graziani, R. (2017). *Ipv6 fundamentals* (1a. ed.). Indianapolis, IN: Cisco Press.

Harkins, D. y Carrel, D. (1998). *The Internet Key Exchange (IKE)*. Recuperado de https://www.rfc-editor.org/rfc/rfc2409.txt

Hinden, R. y Deering, S. (2006). *IP, version 6 addressing architecture*. Recuperado de https://www.rfc-editor.org/rfc/rfc4291.txt

Housley, R. (2005). *Using Advanced Encryption Standard (AES) CCM mode with IPsec Encapsulating Security Payload (ESP).* Recuperado de https://www.rfc-editor.org/rfc/rfc4309.txt

Jain, V., Tiwari, D., Singh, S. y Sharma, S. (2018). Impact of IPv4, IPv6 and dual stack interface over wireless networks. *International Journal of Computer Network and Information Security*, *10*(4), 65-71. https://doi.org/10.5815/ijcnis.2018.04.07

Jiang, H., Liu, D., Ren, Z. y Zhang, T. (2018). *Blockchain in the eyes of developers*. Recuperado de http://arxiv.org/pdf/1806.07080v1

Jiménez, L. M., Puerto, R. y Payá, L. (2017). *Sistemas distribuidos: arquitectura y aplicaciones*. Alicante: Universidad Miguel Hernández.

Kent, S. y Atkinson, R. (1998). *IP Encapsulating Security Payload (ESP)*. Recuperado de https://www.rfc-editor.org/rfc/rfc2406.txt

Krawczyk, H., Bellare, M. y Canetti, R. (1997). *HMAC: Keyed-Hashing for Message Authentication.* Recuperado de https://www.rfc-editor.org/info/rfc2104

Llaneza González, P. (2018). *Seguridad y responsabilidad en la internet de las cosas (Iot).* Barcelona: Editorial Bosch.

Martínez Yelmo, I. y Riaño Vílchez, P. I. (2015). *IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6*. Madrid: Universidad de Alcalá.

Molina Robles, F. (2015). *Planificación y administración de redes*. Madrid: RA-MA.

Nordmark, E. y Gilligan, R. (2005). *Basic transition mechanisms for IPv6 hosts and routers.* Recuperado de https://www.rfc-editor.org/rfc/rfc4213.txt

Palet, J. (2016). *Comparativa entre mecanismos de transición IPv6*. Recuperado de https://www.youtube.com/watch?v=skhwiPu1JKc

Politou, E., Casino, F., Alepis, E. y Patsakis, C. (2019). *Blockchain mutability: Challenges and proposed solutions*. Recuperado de http://arxiv.org/pdf/1907.07099v1

Praptodiyono, S., Murugesan, R. K., Hasbullah, I. H., Wey, C. Y., Kadhum, M. M. y Osman, A. (2015, octubre). S*ecurity mechanism for IPv6 stateless address autoconfiguration*. Conferencia presentada en International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), IEEE en Bandung, Indonesia. https://doi.org/10.1109/ICACOMIT.2015.7440150

Thomson, S., Narten, T. y Jinmei, T. (2007). *IPv6S Stateless address autoconfiguration.* Recuperado de https://www.rfc-editor.org/rfc/rfc4862.txt

Tsirtsis, G. y Srisuresh, P. (2000). *Network Address Translation - Protocol Translation (NAT-PT).* Recuperado de https://www.rfc-editor.org/rfc/rfc2766.txt

Vivar Soto, J. E. (2008). *Seguridad en IPv6 con IPsec* (Tesis de licenciatura). Universidad de Magallanes, Punta Arenas, Chile.

Walton, A. (2018). *SLAAC y DHCPv6: introducción y funcionamiento*. Recuperado de https://ccnadesdecero.es/slaac-dhcpv6-funcionamiento/

Weisman, M., Ritchey, P., Shearer, G., Colbert, E., Dauber, E., Knachel, L., . . . Greenstadt, R. (2018, marzo). Machine learning and data mining for IPv6 network defence. Conferencia presentada en la 13th. International Conference on Cyber Warfare and Security (ICCWS), en Washington, EUA.