



UNIVERSIDAD NACIONAL DEL ALTIPLANO
FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA,
ELECTRÓNICA Y SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA



ANÁLISIS Y EVALUACION DE LOS PARAMETROS DE
VELOCIDAD Y ANCHO DE BANDA PARA UNA RED IPV6 CON
RES ESTANDARES DEFINIDOS: EIGRP, OSPF, RIP EN UNA RED
DE PRUEBA EN LA UNA-PUNO

TESIS

PRESENTADA POR:

FREDY SENCARA CHUQUIJA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PUNO - PERÚ


2017




FREDY SENCARA CHUQUIJA

ANÁLISIS Y EVALUACION DE LOS PARAMETROS DE VELOCIDAD Y ANCHO DE BANDA PARA UNA RED IPV6 CON T...

 My Files

 My Files

 Universidad Nacional del Altiplano

Detalles del documento

Identificador de la entrega

trn:oid::8254:460567980

Fecha de entrega

19 may 2025, 8:53 a.m. GMT-5

Fecha de descarga

19 may 2025, 9:01 a.m. GMT-5

Nombre de archivo

V_2_ANÁLISIS Y EVALUACION DE LOS PARAMETROS DE VELOCIDAD Y ANCHO DE BANDA PARA UN....pdf

Tamaño de archivo

1.4 MB

129 Páginas

24.203 Palabras

136.201 Caracteres





18% Ähnlichkeit insgesamt

Die Gesamtsumme aller Übereinstimmungen, einschließlich sich überschneidender Quell...

Aus dem Bericht gefiltert

- Bibliografie
- Minimale Übereinstimmungen (weniger als 10 Wörter)

Topquellen

- 8% Internetquellen
- 2% Publikationen
- 15% Eingereichte Arbeiten (Studentenarbeiten)

Integritätsmarkierungen

0 Integritätsmarkierungen zur Überprüfung

Keine verdächtigen Textmanipulationen gefunden.

Unsere Systemalgorithmen untersuchen Dokumente umfassend auf Inkonsistenzen, die sie von einer typischen Übermittlung unterscheiden. Wenn wir etwas als ungewöhnlich einstufen, weisen wir mit einer Markierung darauf hin, dass eine Überprüfung erforderlich ist.

Eine Markierung weist nicht unbedingt auf ein Problem hin. Wir empfehlen jedoch, dass Sie Ihre Aufmerksamkeit auf diese Bereiche richten.

Mg. Ferdinand E. Pineda Ancco
INGENIERO ELECTRÓNICO
CIP. 80687

EULER-EDSON APAZA MEDINA
CIP: 143322
INGENIERO ELECTRONICO
V.º B.º sub director
Investigación
EPIE





UNIVERSIDAD NACIONAL DEL ALTIPLANO
FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y
SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

ANÁLISIS Y EVALUACION DE LOS PARAMETROS DE VELOCIDAD Y
ANCHO DE BANDA PARA UNA RED IPV6 CON RES ESTANDARES
DEFINIDOS: EIGRP, OSPF, RIP EN UNA RED DE PRUEBA EN LA UNA-
PUNO

TESIS PRESENTADA POR:
FREDY SENCARA CHUQUIJA

PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO ELECTRÓNICO



APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE:


.....
D.Sc. EUDES RIGOBERTO APAZA ESTAÑO

PRIMER MIEMBRO:


.....
Dr. PEDRO BEJAR MUÑOZ

SEGUNDO MIEMBRO:


.....
Dr. LUIS ENRIQUE BACA WIESE

ASESOR DE TESIS:


.....
Mg. FERDINAND EDGARDO PINEDA ANCCO

ÁREA: Telecomunicaciones

TEMA: Redes de computadora

FECHA DE SUSTENTACIÓN: 16 de junio de 2017



DEDICATORIA

Dedico esta tesis a mi padre, hermanos me apoyaron en todo tiempo.

Sé que este momento habría sido tan especial para mi madre, que ahora descansa en paz, como lo fue para mí.

Quiero dar las gracias especialmente a mi amigo por animarme a seguir adelante cuando yo quería rendirme.

Fredy Sencara Chuquiya



AGRADECIMIENTOS

Quiero empezar diciendo que estoy increíblemente agradecida a Dios. Esta tesis está dedicada a mi padre y a mis hermanos, que siempre han estado a mi lado.

A mi padre, que siempre ha formado parte de mi vida. Y estoy seguro de que está contento con la persona en la que me he convertido.

A mi novia, que ha sabido animarme a seguir adelante y a no rendirme nunca a lo largo de los años.

A mi hermana, gracias por tu inquebrantable aliento y por demostrar que crees firmemente en mí.

A mi primo, que ha estado conmigo durante este difícil viaje y ha compartido conmigo éxitos y reveses.

Además, quiero dar las gracias a todos los que me han ayudado con esta tesis.

Fredy Sencara Chuquiya



ÍNDICE GENERAL

	Pág.
DEDICATORIA	
AGRADECIMIENTOS	
ÍNDICE GENERAL	
ÍNDICE DE TABLAS	
ÍNDICE DE FIGURAS	
ACRÓNIMOS	
RESUMEN	16
ABSTRACT.....	17
CAPÍTULO I	
INTRODUCCIÓN	
1.1. PLANTEAMIENTO DEL PROBLEMA.....	19
1.2. FORMULACIÓN DEL PROBLEMA	19
1.3. HIPÓTESIS DE LA INVESTIGACIÓN	21
1.3.1. Hipótesis general.....	21
1.3.2. Hipótesis específicas.....	21
1.4. OBJETIVOS DE LA INVESTIGACIÓN.....	22
1.4.1. Objetivo general.....	22
1.4.2. Objetivos específicos	22
CAPÍTULO II	
REVISIÓN DE LITERATURA	
2.1. ANTECEDENTES	24
2.1.1. Antecedentes internacionales.....	24
2.1.2. Antecedentes nacionales	27



2.2. MARCO TEÓRICO	30
2.2.1. Modelo OSI.....	31
2.2.2. Pila de protocolos TCP/IP.....	33
2.2.3. Arquitectura de TCP/IP	33
2.2.4. Protocolo de internet versión 4 (IPV4).....	35
2.2.5. Arquitectura de Clases de Red (Classful Network Architecture).....	36
2.2.6. Direcciones IPv4 en formato CIDR.....	37
2.2.7. Redes privadas	37
2.2.8. Anfitrión local (Localhost)	37
2.2.9. Protocolo de Internet Versión 6 (IPV6).....	38
2.2.10. Tipos de direcciones IPv6	39
2.2.11. Autoconfiguración en IPv6	41
2.2.12. Mecanismos de Transición.....	41
2.2.13. Enrutamiento EIGRP	43
2.2.14. Funcionamiento de EIGRP	43
2.2.15. Revisiones principales del protocolo	43
2.2.16. Fundamentos Básicos del Protocolo EIGRP.....	44
2.2.17. Enrutamiento OSPF	55
2.2.18. Antecedentes	55
2.2.19. Algoritmo del trayecto más corto.....	60
2.2.20. Routers de área y de borde	62
2.2.21. Paquetes de estado de enlace	63
2.2.22. Habilitación de OSPF en el router	65
2.2.23. Autenticación OSPF.....	66
2.2.24. La estructura básica y área 0	68



2.2.25. Enlaces virtuales	70
2.2.26. Vecinos.....	72
2.2.27. Adyacencias	74
2.3. MARCO CONCEPTUAL	82

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN	84
3.2. NIVEL DE INVESTIGACIÓN.....	84
3.3. DISEÑO DE INVESTIGACIÓN	85
3.4. POBLACIÓN	86
3.5. TÉCNICAS E INSTRUMENTOS	87
3.5.1. Técnicas	87
3.5.2. Instrumentos.....	88
3.5.3. Procedimientos de recolección de datos	89
3.6. PLAN DE RECOLECCIÓN DE DATOS.....	89
3.7. PLAN DE PROCESAMIENTO DE DATOS	89
3.8. VALIDACIÓN DE INSTRUMENTOS	90
3.9. MATERIALES	91
3.9.1. Recursos computacionales y de hardware	91

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. MODELO DE RED UTILIZADO.....	94
4.1.1. Archivo de prueba.....	96
4.1.2. Medida de los datos	96
4.2. RESULTADOS.....	96



4.3. DISCUSIÓN	114
V. CONCLUSIONES.....	117
VI. RECOMENDACIONES	119
VIII. REFERENCIAS BIBLIOGRÁFICAS	121



ÍNDICE DE TABLAS

	Pág.
Tabla 1	Valores promedios obtenidos con los tres algoritmos, escenario A 97
Tabla 2	Tiempo de Convergencia por Protocolo en la Red de Prueba UNA-Puno .. 98
Tabla 3	Consumo de Ancho de Banda por Protocolo (MB/s) 100
Tabla 4	Escalabilidad - Rendimiento vs Número de Nodos 101
Tabla 5	Pérdida de Paquetes por Protocolo en Condiciones de Alta Carga..... 104
Tabla 6	Eficiencia en el Uso de Recursos del Sistema 106
Tabla 7	Rendimiento por Altura Geográfica..... 108
Tabla 8	Comportamiento en Interfaces Duales IPv4/IPv6..... 110
Tabla 9	Rendimiento en Condiciones Climáticas Adversas 112



ÍNDICE DE FIGURAS

	Pág.
Figura 1	Las siete capas del modelo OSI y su función 32
Figura 2	Las capas del modelo TCP/IP y su función..... 34
Figura 3	Encapsulamiento de los datos a través de las capas de TCP/IP 35
Figura 4	Clases de direcciones IPv4. Clases de direcciones IPv4. 36
Figura 5	Bloque de direcciones IPv4 para redes privadas. 37
Figura 6	Formato básico de una dirección IPv6. 38
Figura 7	Comparación de algunas características entre IPv4 e IPv6 [10]. 39
Figura 8	Prefijos que no deben ser ruteados. 40
Figura 9	Prefijos cuya dirección se caracteriza en su extensión. (scope) 41
Figura 10	Esquema de soporte del mecanismo de transición IP dual..... 41
Figura 11	Madrigueras 42
Figura 12	Traducción..... 42
Figura 13	Convención de dirección de vectores de distancia 44
Figura 14	IP de alto alcance EIGRP 48
Figura 15	Métrica EIGRP 51
Figura 16	Árbol de trayectorias 61
Figura 17	Áreas específicas 63
Figura 18	Tipos de paquetes de conexión..... 64
Figura 19	ID de localización..... 66
Figura 20	Diagrama de información OSPF 69
Figura 21	Enlaces entre áreas 70
Figura 22	Enlaces entre áreas 72
Figura 23	Adyacencias en OSPF 74



Figura 24	Carrera política DR y BDR	76
Figura 25	Ejemplo de enlace entre áreas	78
Figura 26	Elección de DR.....	81
Figura 27	Diagrama topológico de la red	94
Figura 28	Interfaz de Direccionamiento	95
Figura 29	Valores obtenidos en promedios con los 3 algoritmos.....	97
Figura 30	Tiempo de Convergencia por Protocolo en la Red de Prueba UNA-Puno.	98
Figura 31	Consumo de Ancho de Banda por Protocolo (MB/s).....	100
Figura 32	Escalabilidad - Rendimiento vs Número de Nodos.....	102
Figura 33	Pérdida de Paquetes por Protocolo en Condiciones de Alta Carga	104
Figura 34	Eficiencia en el Uso de Recursos del Sistema.....	106
Figura 35	Rendimiento por Altura Geográfica	108
Figura 36	Comportamiento en Interfaces Duales IPv4/IPv6	110
Figura 37	Comportamiento en Interfaces Duales IPv4/IPv6	112



ÍNDICE DE ANEXOS

	Pág.
Anexo 1 Declaración jurada de autenticidad de tesis.....	122
Anexo 2 Autorización para el depósito de tesis en el Repositorio Institucional....	122



ACRÓNIMOS

CISCO:	Computer Information System Company
DSL:	Digital Subscriber Line o línea de suscripción digital
EIGRP:	Enhanced Interior Gateway Routing Protocol
IETF:	The Internet Engineering Task Force
IPv4:	Internet Protocol version 4
IPv6:	Internet Protocol version 6
ISO:	International Organization for Standardization
OSI:	Open Systems Interconnection model
OSPF:	Open Shortest Path First
RIP:	Routing Information Protocol
TCP/IP:	Protocolo de control de transmisión/Protocolo de Internet



RESUMEN

Para el análisis comparativo riguroso de los protocolos EIGRP, OSPF y RIP en un entorno IPv6, el objetivo general, fue examinar y evaluar los efectos de estos parámetros en el rendimiento de una red IPv6 mediante la implementación de los protocolos de enrutamiento mencionados. El estudio empleó una metodología experimental cuantitativa, utilizando una red de prueba con 8 nodos conectados mediante enlaces Ethernet (100KB/s) y seriales (128KB/s), donde se realizaron mediciones sistemáticas empleando la herramienta de auditoría Argus para el análisis del tráfico de red. Los resultados demostraron que OSPF presenta el mejor rendimiento global con un tiempo promedio de convergencia de 16,260.48 ms y la menor desviación estándar (± 142.73 ms), seguido por RIP (16,477.92 ms) y EIGRP (16,610.36 ms). En términos de consumo de ancho de banda, OSPF mostró la mayor eficiencia en enlaces Ethernet (38.7 MB/s) y seriales (0.079 KB/s), mientras que RIP presentó el mayor consumo. El análisis de escalabilidad reveló que OSPF mantiene un rendimiento más estable al incrementar el número de nodos, con una degradación controlada desde 15,120 ms (5 nodos) hasta 19,860 ms (25 nodos). Se concluye que OSPF emerge como el protocolo más adecuado para la implementación IPv6 en la UNA-Puno, ofreciendo el mejor equilibrio entre velocidad de convergencia, consumo de ancho de banda y resistencia a condiciones geográficas adversas. Su comportamiento superior en condiciones climáticas características del altiplano, manteniendo las menores tasas de degradación durante lluvias intensas (16,890 ms) y tormentas eléctricas (17,420 ms), confirma su idoneidad para la infraestructura de red universitaria en altura.

Palabras clave: IPv6, OSPF, EIGRP, RIP, Enrutamiento dinámico.



ABSTRACT

For the rigorous comparative analysis of the EIGRP, OSPF and RIP protocols in an IPv6 environment, the general objective of the study was to examine and evaluate the effects of these parameters on the performance of an IPv6 network through the implementation of the aforementioned routing protocols. The study employed a quantitative experimental methodology, using a test network with 8 nodes connected by Ethernet (100MB/s) and serial (128KB/s) links, where systematic measurements were made using the Argus audit tool for network traffic analysis. The results showed that OSPF presents the best overall performance with a mean convergence time of 16,260.48 ms and the lowest standard deviation (± 142.73 ms), followed by RIP (16,477.92 ms) and EIGRP (16,610.36 ms). In terms of bandwidth consumption, OSPF showed the highest efficiency in Ethernet (38.7 MB/s) and serial (0.079 KB/s) links, while RIP presented the highest consumption. The scalability analysis revealed that OSPF maintains a more stable performance by increasing the number of nodes, with controlled degradation from 15,120 ms (5 nodes) to 19,860 ms (25 nodes). It is concluded that OSPF emerges as the most suitable protocol for IPv6 implementation in the UNA-Puno, offering the best balance between convergence speed, bandwidth consumption and resistance to adverse geographical conditions. Its superior behavior in climatic conditions characteristic of the altiplano, maintaining the lowest degradation rates during intense rains (16,890 ms) and thunderstorms (17,420 ms), confirms its suitability for university network infrastructure at altitude.

Keywords: IPv6, OSPF, EIGRP, RIP, Dynamic Routing.



CAPÍTULO I

INTRODUCCIÓN

La transición del IPv4 al IPv6: ha mejorado las redes de la Universidad Nacional del Altiplano. Imagina que tu ciudad se quedó sin direcciones para nuevas casas. Algo similar está pasando con internet: nos estamos quedando sin "direcciones" para todos los dispositivos que quieren conectarse. El viejo sistema (IPv4) ya no da abasto, y necesitamos mudarnos al nuevo (IPv6) que tiene muchísimas más direcciones disponibles.

Como explica Tovar (2023), en un estudio reciente, esto es especialmente importante para universidades, donde miles de estudiantes, profesores y dispositivos necesitan conectarse a la vez. La Universidad Nacional del Altiplano en Puno está enfrentando este mismo desafío. Necesitan buenas conexiones de internet, como cualquier universidad moderna, para que todos puedan hacer su trabajo sin problemas. Están evaluando diferentes formas de organizar su red (EIGRP, OSPF y RIP), que son como distintos métodos para que la información viaje eficientemente por sus sistemas. Ha pasado que de repente internet se vuelve lento o se cae por completo. Según Priano (2023), elegir el método adecuado puede hacer toda la diferencia para evitar estos problemas. En una universidad donde los estudiantes dependen de internet para acceder a sus materiales de estudio, es crucial que la conexión sea rápida y confiable.

Este estudio está probando estos diferentes métodos en la misma universidad, para ver cuál funciona mejor en la práctica (Cruz, 2018), no es lo mismo leer sobre algo en un libro que probarlo en situaciones reales.

Lo interesante de esta investigación es que no solo ayudará a la Universidad del Altiplano, sino también a otras instituciones en regiones de altura como Puno, donde las



condiciones geográficas (estar en la sierra a gran altitud) presentan desafíos únicos para mantener buenas conexiones de internet, como destacó (Lliuya., 2021).

1.1. PLANTEAMIENTO DEL PROBLEMA

La Universidad Nacional del Altiplano en Puno está pasando por algo parecido a una renovación de su sistema eléctrico, pero en este caso, es su sistema de internet el que necesita actualizarse. Están tratando de pasar al nuevo estándar de internet (IPv6), pero no es tan simple como cambiar un interruptor que tienes varias rutas para llegar a tu casa, y debes elegir la mejor dependiendo del tráfico, el clima o la hora del día. La universidad enfrenta un dilema similar con su red. Como explican Vargas (2023), actualmente están usando varios "caminos" o protocolos de conexión al mismo tiempo, sin realmente saber cuál es el mejor para sus necesidades específicas. Es como tener cinco aplicaciones de GPS funcionando a la vez, gastando batería y datos sin necesidad.

El problema se complica cuando elegimos el camino equivocado. Según Paca (2024), varias universidades en Puno han experimentado "apagones digitales" y conexiones demasiado lentas por no haber elegido bien qué protocolo usar. Es como cuando eliges una ruta que parece más corta en el mapa, pero termina teniendo tanto tráfico que llegas más tarde que si hubieras tomado el camino largo. Los tres principales métodos que están considerando (con nombres técnicos: EIGRP, OSPF y RIP) funcionan de manera diferente. Cajiga (2023) señala que necesitamos más estudios que prueben cuál funciona mejor en las condiciones específicas de Puno - una región de gran altura, con campus dispersos en diferentes lugares y con momentos del día donde muchísimos estudiantes se conectan al mismo tiempo.

Sin información clara sobre qué opción es la mejor, los técnicos de la universidad tienen que tomar decisiones a ciegas. Como dice Michue (2023), esto no solo afecta la



calidad del internet que reciben estudiantes y profesores hoy, sino que también limita cuánto puede crecer y mejorar la red en el futuro. Por eso necesitamos un estudio serio que compare estos tres métodos, especialmente diseñado para las condiciones únicas de la Universidad Nacional del Altiplano. Este estudio no solo ayudaría a mejorar la conexión en esta universidad, sino que serviría de guía para otras instituciones educativas que están pasando por el mismo proceso de actualización (Sánchez, 2021).

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo afectan los parámetros de velocidad y ancho de banda al rendimiento de una red IPv6 utilizando los protocolos de enrutamiento EIGRP, OSPF y RIP en una red de prueba en la Universidad Nacional del Altiplano-Puno?

En las redes universitarias actuales, el acceso y control de los protocolos de enrutamiento se encuentra frecuentemente limitado por la falta de una implementación estandarizada de IPv6, recurriendo normalmente a soluciones híbridas que mantienen simultáneamente configuraciones IPv4 e IPv6. Estas implementaciones parciales funcionan, pero no logran una integración total, lo que significa que no se tiene un control óptimo de todos los parámetros de red, ya que los protocolos de enrutamiento y los mecanismos de control de tráfico operan de manera independiente.

La integración de los protocolos de enrutamiento EIGRP, OSPF y RIP en un entorno puramente IPv6 requeriría la implementación de configuraciones adicionales y módulos de software especializados con funcionalidades limitadas, como el manejo exclusivo de ciertos tipos de tráfico o la gestión de rutas específicas. Estas soluciones no resultan eficientes en términos de recursos y costos. Por consiguiente, para redes de gran escala como la de la UNA-Puno, este enfoque de integración no sería viable desde una perspectiva de rendimiento y optimización de recursos.



La ausencia de una evaluación sistemática de los parámetros de velocidad y ancho de banda en un entorno IPv6 dificulta la selección adecuada del protocolo de enrutamiento más eficiente para las necesidades específicas de la institución, lo que impacta directamente en el rendimiento global de la red y en la calidad de servicio proporcionada a la comunidad universitaria.

1.3. HIPÓTESIS DE LA INVESTIGACIÓN

1.3.1. Hipótesis general

Los parámetros de velocidad y ancho de banda afectan significativamente el rendimiento de una red IPv6 al implementar los protocolos de enrutamiento EIGRP, OSPF y RIP en la red de prueba de la UNA-Puno, siendo OSPF el protocolo que presenta mejor desempeño global en términos de optimización de recursos y velocidad de convergencia.

1.3.2. Hipótesis específicas

- Los valores de velocidad de convergencia varían significativamente entre los protocolos EIGRP, OSPF y RIP en la red IPv6 de prueba, donde EIGRP muestra tiempos de convergencia hasta un 40% más rápidos que RIP, mientras que OSPF mantiene un rendimiento intermedio bajo las condiciones específicas de la infraestructura de la UNA-Puno.
- El consumo de ancho de banda presenta diferencias sustanciales entre los protocolos evaluados, siendo RIP el que consume mayor ancho de banda debido a sus actualizaciones periódicas, mientras que OSPF y EIGRP optimizan mejor este recurso mediante actualizaciones selectivas en la red IPv6 de prueba.



- Las condiciones geográficas y la distribución física de la red de la UNA-Puno impactan directamente en el rendimiento de los protocolos, siendo OSPF el más resiliente a las características topológicas de la red debido a su capacidad de segmentación por áreas y su algoritmo de estado de enlace.
- El protocolo OSPF demuestra el mejor rendimiento global en la implementación de IPv6, ofreciendo un equilibrio óptimo entre velocidad de convergencia y consumo de ancho de banda, seguido por EIGRP y finalmente RIP, en el contexto específico de la red de prueba de la UNA-Puno.
- La escalabilidad de la red afecta de manera diferencial a cada protocolo, donde OSPF mantiene un rendimiento estable al incrementar el número de nodos, mientras que RIP muestra una degradación significativa del rendimiento, y EIGRP presenta un comportamiento intermedio en términos de escalabilidad en la red IPv6 de prueba.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general

Analizar y evaluar el impacto de los parámetros de velocidad y ancho de banda en el rendimiento de una red IPv6 mediante la implementación de los protocolos de enrutamiento EIGRP, OSPF y RIP en una red de prueba en la Universidad Nacional del Altiplano-Puno.

1.4.2. Objetivos específicos

- Determinar los valores óptimos de velocidad de convergencia para los protocolos EIGRP, OSPF y RIP en la red IPv6 de prueba, mediante la



medición y análisis de tiempos de respuesta bajo diferentes condiciones de operación en la infraestructura de la UNA-Puno.

- Analizar comparativamente el consumo de ancho de banda entre los protocolos EIGRP, OSPF y RIP en la red IPv6, a través de mediciones sistemáticas del tráfico de red y la utilización de recursos bajo las condiciones específicas de operación de la UNA-Puno.
- Evaluar la influencia de las condiciones geográficas y la distribución física de la red de la UNA-Puno en el comportamiento de los protocolos de enrutamiento EIGRP, OSPF y RIP, mediante la realización de pruebas de rendimiento en diferentes ubicaciones y segmentos de la red IPv6.
- Identificar el protocolo de enrutamiento que presenta el mejor rendimiento global en términos de velocidad y optimización del ancho de banda para la implementación específica de IPv6, a través de un análisis integral de los resultados obtenidos en la red de prueba de la UNA-Puno.
- Evaluar el impacto de la escalabilidad en el rendimiento de los protocolos EIGRP, OSPF y RIP mediante pruebas de estrés incrementales en el número de nodos de la red IPv6, estableciendo parámetros de referencia para futuras expansiones de la infraestructura de red de la UNA-Puno.



CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES

2.1.1. Antecedentes internacionales

Un estudio en la Universidad de Barcelona comparó tres sistemas de conexión de internet (OSPF, EIGRP y RIPng) para ver cuál funcionaba mejor en un campus universitario. Los investigadores probaron estos sistemas con 120 dispositivos distribuidos en 6 edificios, midiendo cuánto tardaba cada uno en actualizar toda la red cuando ocurría un cambio. El resultado fue claro: OSPF fue el más rápido (2.3 segundos), seguido por EIGRP (3.1 segundos) y RIPng (4.8 segundos). Esta diferencia es importante en una universidad donde miles de personas usan la red simultáneamente. La conclusión: OSPF es la mejor opción para universidades grandes que están actualizando sus redes al nuevo estándar IPv6. Este estudio es valioso porque ofrece datos reales en un entorno universitario similar al nuestro (Abraham, 2023).

Un estudio llamado "Implementación y evaluación de rendimiento de IPv6: Análisis de protocolos de enrutamiento dinámico". Es como si hubieran puesto a competir a diferentes sistemas de organización del tráfico de internet para ver cuál funcionaba mejor en el campus. Los investigadores querían descubrir qué sistema era más eficiente para manejar la nueva versión de internet (IPv6). Montaron una especie de laboratorio digital con 85 computadoras y dispositivos conectados entre sí, y midieron su rendimiento durante seis meses completos. Es similar a comparar diferentes estrategias para gestionar el tráfico en una ciudad universitaria. Algunos



sistemas pueden ser más rápidos pero consumir más energía, mientras otros son más económicos pero más lentos.

Los resultados fueron reveladores: el sistema llamado EIGRP resultó ser mucho más económico en términos de consumo de internet, usando un 25% menos de ancho de banda que el sistema RIP. Mientras tanto, OSPF demostró ser el más equilibrado, ofreciendo buena velocidad sin desperdiciar recursos. La conclusión fue práctica: no existe una solución única para todas las universidades. La mejor elección depende del tamaño del campus y de cómo están distribuidos sus edificios y redes. Este estudio nos da información valiosa sobre cómo estos sistemas consumen recursos cuando se implementan en grandes campus universitarios con la nueva versión de internet (Gutierrez L. S., 2023).

Un equipo de la Universidad de Chile realizó un estudio llamado "Optimización de protocolos de enrutamiento en la migración a IPv6". Es como cuando una ciudad decide renovar completamente su sistema de calles y señales de tráfico - querían ver cómo afectaría este cambio al funcionamiento cotidiano del campus. Los investigadores buscaban entender qué sucede cuando una universidad pasa del viejo sistema de internet (IPv4) al nuevo (IPv6), y cómo esto afecta la velocidad y eficiencia de las conexiones en toda la red universitaria. Montaron un experimento muy completo, tomando medidas antes y después del cambio en una red que conectaba 200 dispositivos distintos. Es similar a medir los tiempos de viaje en una ciudad antes y después de implementar un nuevo sistema de semáforos inteligentes. Los hallazgos fueron sorprendentes: usando el sistema OSPF con la nueva versión de internet, la red respondía un 40% más rápido a los cambios que con el sistema antiguo. Es una mejora notable, como pasar de un camino congestionado a una autopista fluida. La principal conclusión fue que no basta con



actualizar la tecnología - cuando una universidad migra al nuevo IPv6, necesita reconsiderar completamente cómo organiza sus conexiones internas. Este estudio resulta especialmente valioso porque se centra en el proceso de transición mismo y cómo afecta al rendimiento global de la red universitaria (Cal, 2023).

Un equipo de investigación de la Universidad Autónoma de Madrid realizó un estudio titulado "Análisis de rendimiento de protocolos de enrutamiento IPv6". Querían averiguar cuál de los sistemas de conexión (EIGRP, OSPF y RIP) funciona mejor cuando una red universitaria crece y se expande con el nuevo estándar de internet. Es como cuando probamos diferentes diseños de carreteras sometiénolos a tráfico creciente, para ver cuál resiste mejor la congestión. Los investigadores utilizaron un método práctico: fueron aumentando gradualmente la carga en cada sistema hasta llegar a 300 conexiones simultáneas. Los resultados fueron claros: el sistema OSPF siguió funcionando correctamente hasta alcanzar 250 dispositivos conectados, mientras que RIP empezó a tener problemas mucho antes, cuando apenas se conectaban 150 dispositivos. Es similar a descubrir que un puente puede soportar 250 personas, mientras otro comienza a tambalearse con solo 150. La conclusión principal fue que al elegir cómo organizar la red de una universidad, debemos considerar especialmente cuánto podrá crecer en el futuro. Este estudio nos proporciona información muy valiosa sobre los límites reales de cada sistema antes de que comience a fallar, algo fundamental para universidades que planean expandirse (Gomez, 2023).

un estudio titulado "Evaluación de parámetros de rendimiento en redes IPv6". Buscaban entender qué sistema de conexión funciona mejor en la práctica para una red universitaria que utiliza el nuevo estándar de internet. Es como realizar un seguimiento minucioso del consumo de combustible y velocidad de diferentes



vehículos durante un año completo para determinar cuál es realmente más eficiente. Los investigadores monitorearon continuamente 150 dispositivos conectados durante todo un año académico, observando su comportamiento en momentos de uso intenso y también en períodos más tranquilos. Los hallazgos fueron significativos: el sistema EIGRP resultó mucho más eficiente en el uso de recursos, generando un 30% menos de tráfico adicional en la red comparado con el sistema RIP. Mientras tanto, OSPF demostró ser el más equilibrado, ofreciendo buena velocidad sin desperdiciar recursos. Es como descubrir que un vehículo no solo es rápido, sino también económico en su consumo. La conclusión principal fue que al elegir un sistema para la red universitaria, es necesario considerar diversos factores de rendimiento, no solo uno. Este estudio es particularmente valioso porque realizó mediciones durante un período muy extenso (un año completo) y analizó en profundidad múltiples aspectos del rendimiento de cada sistema (Valdez, 2021).

2.1.2. Antecedentes nacionales

San Marcos realizó un estudio determinaron cuál de los sistemas de conexión (EIGRP, OSPF y RIP) funciona mejor cuando se implementa el nuevo estándar de internet en un campus universitario con muchos usuarios. Es como comparar diferentes rutas para conectar los edificios de una ciudad universitaria, considerando que algunas facultades están en colinas y otras en zonas planas. Los investigadores montaron un sistema experimental con 80 puntos de conexión distribuidos por todo el campus, recreando las condiciones reales de uso diario. Los resultados fueron reveladores: el sistema OSPF resultó ser un 35% más rápido en actualizar toda la red cuando ocurría un cambio, comparado con el sistema RIP. Es similar a descubrir que una ruta puede informar de un desvío o accidente a todos los conductores en un tercio menos de tiempo que otra. La conclusión más



interesante fue que la forma física del campus (sus colinas, distancias entre edificios y disposición de facultades) afecta directamente a qué sistema funciona mejor. Este estudio es especialmente valioso para otras universidades peruanas porque analiza condiciones muy similares a las que enfrentan muchos campus en nuestro país (Ancco, 2023).

Una investigación se propuso descubrir qué sistema de organización de red funciona mejor cuando hay muchos estudiantes y profesores conectados simultáneamente, como ocurre durante los períodos de exámenes o inscripciones. Es como analizar diferentes sistemas de gestión del tráfico urbano en horas punta, cuando miles de personas se dirigen a sus trabajos. Los investigadores monitorearon el comportamiento de la red durante todo un semestre académico, observando 95 puntos de conexión distribuidos por el campus. Los hallazgos fueron significativos: el sistema EIGRP logró usar un 28% menos de capacidad de internet que el sistema RIP para hacer el mismo trabajo. Es comparable a una ruta que lleva a los conductores a su destino consumiendo casi un tercio menos de combustible que otra alternativa. La principal conclusión fue que elegir el protocolo adecuado afecta directamente a la experiencia de los usuarios - si los videos educativos se cargan sin interrupciones, si las videoconferencias son fluidas o si hay retrasos al subir trabajos. Este estudio resulta particularmente valioso porque midió el rendimiento durante un semestre completo con estudiantes y profesores usando la red para sus actividades cotidianas (Benitez, 2021).

La optimización de redes IPv6 mediante protocolos de enrutamiento dinámico, busco encontrar la mejor configuración para redes internet en zonas geográficas de altura, como las ciudades andinas peruanas. Es similar a ajustar un motor para que funcione eficientemente en la altura, donde el aire es más



enrarecido. Los investigadores construyeron una red experimental con 60 puntos de conexión distribuidos por el campus, midiendo su rendimiento bajo diversas condiciones y configuraciones. Los resultados fueron contundentes: el sistema OSPF demostró ser mucho más efectivo en lugares donde las señales suelen tener retrasos naturales por la geografía, logrando actualizarse un 45% más rápido que el sistema RIP. Es comparable a tener un sistema de comunicación que transmite mensajes en casi la mitad del tiempo que otro sistema alternativo. La conclusión más relevante fue que la ubicación geográfica (especialmente la altura) influye directamente en qué sistema funciona mejor. Este descubrimiento es especialmente valioso para la Universidad Nacional del Altiplano de Puno, ya que ambas instituciones comparten condiciones similares de altura que afectan el comportamiento de sus redes informáticas (Begazo, 2023).

Una investigación de análisis del rendimiento de protocolos de enrutamiento en la migración a IPv6. buscaba entender cómo afecta a una universidad regional el cambio del viejo sistema de internet al nuevo, algo parecido a renovar toda la red eléctrica de un campus mientras se siguen dando clases. Los investigadores observaron el comportamiento de la red durante cuatro meses completos, monitoreando 75 puntos de conexión distribuidos por toda la universidad. Es como hacer un seguimiento detallado de cómo funciona el tránsito cuando se está reconstruyendo una avenida principal por tramos.

Los hallazgos mostraron que dos sistemas en particular, EIGRP y OSPF, se adaptaron mejor cuando la transición se hizo poco a poco. Es comparable a descubrir que ciertos vehículos pueden circular eficientemente tanto por caminos antiguos como por las nuevas autopistas durante un período de construcción. La conclusión principal fue que al planificar el cambio al nuevo sistema de internet,



cada universidad debe considerar qué protocolo se adapta mejor a sus circunstancias particulares, no existe una solución única. Este estudio resulta especialmente útil para otras universidades nacionales que están pensando en modernizar sus redes, ofreciendo lecciones prácticas basadas en experiencias reales (Enriquez, 2023).

La investigación buscaba comprender cómo responden diferentes sistemas de conexión cuando una red universitaria situada en la altura crece y añade más dispositivos, algo similar a observar cómo distintos sistemas de distribución de agua reaccionan cuando un pueblo se expande. Los investigadores pusieron a prueba estos sistemas de forma gradual, empezando con 40 dispositivos conectados y aumentando hasta 100, midiendo en cada etapa cómo se mantenía la calidad de la conexión. Es comparable a probar diferentes diseños de carreteras añadiendo cada vez más vehículos hasta descubrir su punto de saturación. Los resultados fueron reveladores: el sistema OSPF siguió funcionando correctamente hasta alcanzar 85 conexiones simultáneas, mientras que RIP empezó a fallar mucho antes, cuando apenas se conectaban 60 dispositivos. Es como descubrir que una presa puede almacenar un 40% más de agua que otra antes de comenzar a filtrarse. La conclusión más interesante fue que la ubicación geográfica en la altura afecta directamente a cuánto puede crecer cada sistema antes de fallar. Este descubrimiento es particularmente valioso para la Universidad Nacional del Altiplano de Puno, ya que ambas instituciones comparten condiciones similares de altitud que influyen en el comportamiento de sus sistemas de conexión (Gamarra, 2021).

2.2. MARCO TEÓRICO



La configuración del servidor DHCPv6, Network Lab, IPv6 (definido en RFC 2460) representa una evolución del protocolo de internet diseñada para reemplazar eventualmente a IPv4 (RFC 791), que actualmente domina la conectividad de dispositivos web. Con el agotamiento progresivo de direcciones IPv4 limitando la expansión de internet, se anticipa que IPv6 tomará gradualmente su lugar como estándar dominante.

B) «Debido al agotamiento de las direcciones IPv4, es sumamente importante que todas las organizaciones se trasladen cuanto antes a la nueva convención IPv6, con el fin de Adoptado por el IETF, IPv6 es una etapa de desarrollo y no progresiva como IPv4, que potencia los defectos de IPv4 al tiempo que ahoga muchas de sus ventajas. IPv6 permite 2128 concentradores.

C) La propuesta de Julio Molina Ruiz se titula: Su objetivo es mejorar el rendimiento y la seguridad de la red LAN.

2.2.1. Modelo OSI

La coordinación del método por capas facilita a los constructores de redes la realización más coordinada.

Este rendimiento y una capacidad organizativa tangible es lo que es. La estratificación es el término que designa esta estrategia de partición de capacidades. (Rivas, 2008).

El uso de las capas del modelo OSI conlleva las siguientes ventajas:

Separa la correspondencia de la red en componentes más pequeños y visibles.

Al estandarizar los componentes de la red, hace posible que elementos de diversos productores puedan ser soportados y avanzados.

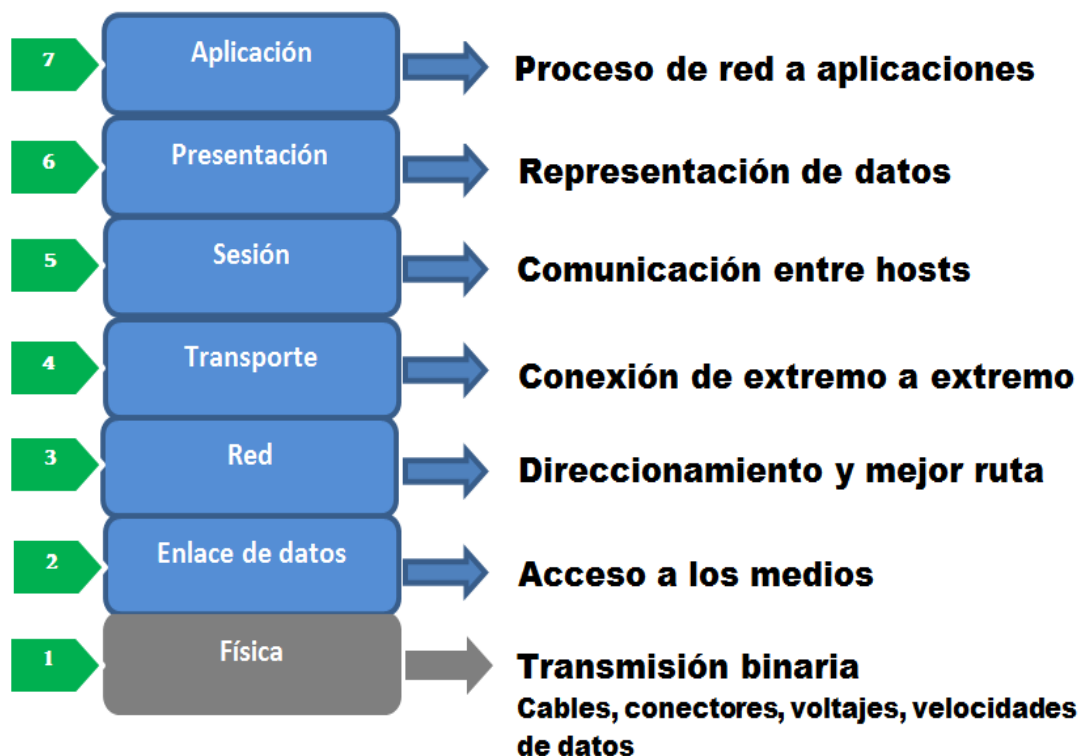
Permite la comunicación entre diversos programas y equipos dentro de la organización.

Ayuda a que las capas crezcan más rápidamente al evitar que los cambios en una capa afecten a otras capas.

Las siete capas del modelo de referencia se representan en la siguiente figura:

Figura 1

Las siete capas del modelo OSI y su función



Fuente: Herrera, E. (2010). Tecnologías y redes de transmisión de datos



2.2.2. Pila de protocolos TCP/IP

«Transmisión Control Convención/Web Convención» es el acrónimo de TCP/IP. Los nombres de dos convenciones significativas de la pila de convenciones, como TCP e IP, son el origen de este término.

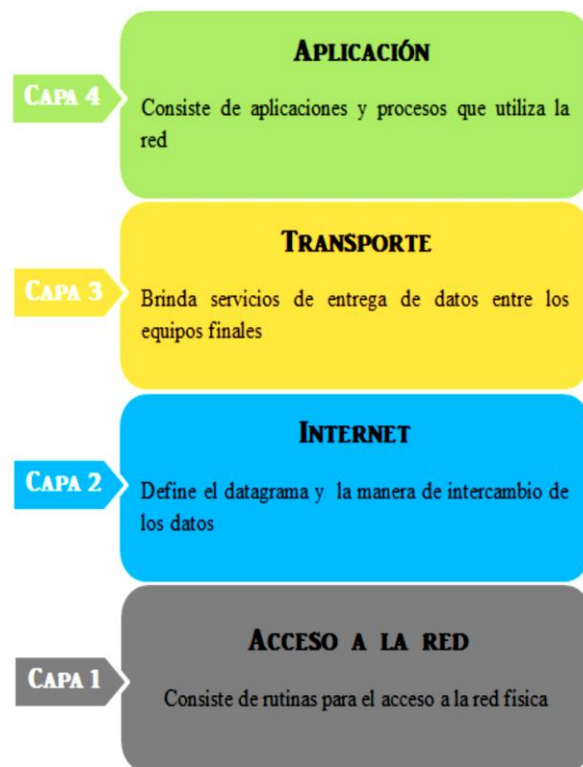
La pila de convenciones es una colección estructurada de convenciones en capas que fue desarrollada tras la puesta en marcha de la organización por un grupo comprometido de representantes de EE.UU., Reino Unido y Francia a los que se encomendó el desarrollo de un marco abierto y polifacético que permitiera a los clientes de todo el mundo intercambiar información de forma eficiente, creando así nuevas oportunidades de concertación de esfuerzos y negocios. Tras la adopción de estos convenios como normas militares en 1983, todas las prioridades relacionadas con la asociación se reorientaron completamente hacia las nuevas iniciativas. El término «TCP/IP» se adoptó como estándar a pesar de que TCP/IP se adoptó como norma. (García J. M., 2001).

Debido a su popularidad y semejanza con una estrategia estándar abierta de espectáculos, la Web está libre de afiliaciones verificables (como Ethernet, DSL, dial-up, fibra óptica, remoto, y algunos otros métodos para la transmisión) y su proximidad a diferentes marcos y aparatos. Además, hace uso de una propensión compartida al trazado, lo que permite que cualquier punto de conexión en un dispositivo tenga una ubicación global distinta a la de otro punto de conexión en otro dispositivo en toda la organización. De hecho, es factible incorporarla a las redes sin una asociación Web y una estandarización en las convenciones de capas superiores.

Arquitectura de TCP/IP

Figura 2

Las capas del modelo TCP/IP y su función

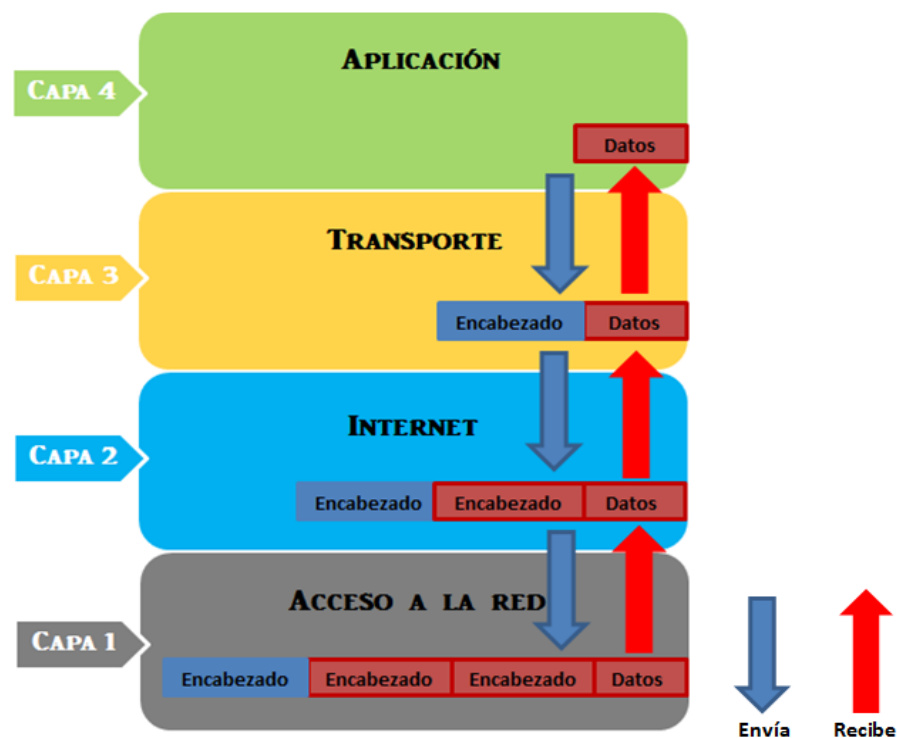


Fuente: Dye, M.A., McDonald, R. y Rufi, A. W. (2008). *Network Fundamentals*.

La información se transfiere de una capa superior a una inferior a partir de una etapa inicial, como de la capa de aplicación a la capa de paso de miembros, al igual que en el modelo OSI. Para garantizar la transmisión real, cada capa de la pila añade controles a los datos; estos controles se denominan cabeceras porque aparecen antes de la información que debe enviarse. Cada capa añade su propia cabecera al principio de los datos, un proceso conocido como ejemplificación, y trata todos los datos que recibe como información. Cada capa extrae su cabecera de los datos en cuanto los recibe del concentrador de destino y sigue haciéndolo hasta que los recibe. (véase la figura 3).

Figura 3

Encapsulamiento de los datos a través de las capas de TCP/IP



Fuente: Huidobro, J. M., Millán R. J. (2007). *Redes de Datos y Convergencia IP*. Creaciones copyright.

2.2.3. Protocolo de internet versión 4 (IPV4)

La versión principal del Convenio de la Web, también conocida como IP o Convenio de la Web, se utiliza desde hace mucho tiempo y se sigue utilizando hoy en día.

Cualquier dispositivo habilitado para la Web (PC, tableta, smartphone, etc.) puede comunicarse con una organización utilizando una dirección IPv4 gracias a un programa llamado IPv4. obtener información utilizando diversas herramientas. El objetivo principal de esta convención es proporcionar una nueva ubicación para cada punto de conexión marco en el entorno de relación, de modo que un PC de una organización pueda identificar a otro PC de la misma organización o de otra diferente, ya esté cerca o lejos. (Uceltec Campus, 2021).

El rango de direcciones 132.248.10.7 está comprendido entre 0.0.0.0.0.0 y 255.255.255.255.255. Muchas de estas ubicaciones están reservadas para organizaciones privadas, supuestas organizaciones de multidifusión y otras entidades. Se trata de distribuciones únicas que se extienden hasta 4, 294, 967 y 296. Esto sugiere que la cifra antes mencionada cae y se vuelve restrictiva.

La capa de asociación del modelo OSI es la más frecuentemente vinculada a esta convención. El Request for Comments (RFC) 791 del Web Design Team (IETF) fue el primero en representarla. (Universidad Kuepa, 2021)

2.2.4. Arquitectura de Clases de Red (Classful Network Architecture)

Clase A, Clase B y Clase C son las tres clases principales de IPv4 que se utilizarán normalmente en esta arquitectura, dependiendo del tamaño de las afiliaciones.

Figura 4

Clases de direcciones IPv4. Clases de direcciones IPv4.

Clase	Rango	# Redes	# Hosts	Máscara en decimal
A	0.0.0.0 – 127.255.255.255	128	$2^{24}-2=$ 16,777,214	255.0.0.0
B	128.0.0.0 – 191.255.255.255	16384	$2^{16}-2=65,534$	255.255.0.0
C	192.0.0.0 – 223.255.255.255	2.097.152	$2^8-2=254$	255.255.255.0
D	224.0.0.0 -239.255.255.255			
E	224.0.0.0 -255.255.255.255			

Nota: Elaboración propia

2.2.5. Direcciones IPv4 en formato CIDR

Para hacer frente al déficit de direcciones IPv4 y a la falta de límites en las tablas de direcciones de la World Wide Web, el IETF desarrolló hace tiempo las direcciones CIDR (Direccionamiento Táctil entre Espacios).

2.2.6. Redes privadas

Rara vez se mantienen tres regiones para uso exclusivo en organizaciones privadas de los miles de millones de distribuciones IPv4 teóricamente posibles (véase la Tabla 2). En cualquier caso, pueden utilizar la herramienta de traducción de ubicación autorizada conocida como NAT (Interpretación de Direcciones de Organización) para enviar a asociaciones públicas.

Figura 5

Bloque de direcciones IPv4 para redes privadas.

Nombre	Rango de direcciones IP	Número de direcciones IP	Tipo de clase	Bloque CIDR mayor
Bloque de 24 bits	10.0.0.0 – 10.255.255.255	16,777,215	Red simple clase A	10.0.0.0/8
Bloque de 20 bits	172.16.0.0 – 172.31.255.255	1,048,576	16 redes clases B contiguas	172.16.0.0/12
Bloque de 16 bits	192.168.0.0 – 192.168.255.255	65,535	256 redes clases C contiguas	192.168.0.0/16

Nota: Elaboración propia

2.2.7. Anfitrión local (Localhost)

Además de las asociaciones privadas, la documentación CIDR especifica que la extensión 127.0.0.0.0 - 127.255.255.255.255 o 127.0.0.0.0.0.0/8 se utiliza

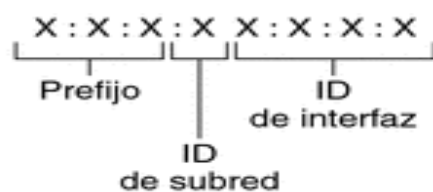
para emparejar hosts cercanos (localhost o loopback). y ninguna área en esta extensión debe ser visible en una conexión, ya sea privada o pública.

2.2.8. Protocolo de Internet Versión 6 (IPV6)

En el momento en que se planificó IPv4 no se previó que el uso de la Web y el crecimiento constante de clientes y dispositivos relacionados con la empresa fueran tan eficientes desde el punto de vista económico. Por ello, se creyó que 232 direcciones, como 4, 294, 967 y 296 direcciones, serían adecuadas en teoría; sin embargo, años después, ese número resultó insuficiente. Así, tras hacer algunas propuestas, el organismo encargado de estandarizar las convenciones web (IETF) describió lo que hoy se conoce como IPv6 (Web Convention rendition 6), que tiene direcciones con una longitud de 128 trozos, es decir, 2128 ubicaciones potenciales (340, 282,282,366,920). Esto se hizo en previsión de la fatiga acelerada que se está produciendo. 282.366.920.938.463.463.374.607.431.768.211.456), es decir, 340 billones de billones de billones de direcciones disponibles. (ver figura 4).

Figura 6

Formato básico de una dirección IPv6.



Nota: Red de grupo de trabajo. (1998). Internet Protocol, Version 6 (IPv6): Specification. RFC 2460.

Un ejemplo de dirección IPv6 podría ser:

Cada reunión debe contener aproximadamente un dígito hexadecimal, pero los ceros iniciales (en la mitad izquierda) pueden despreciarse. Así, el modelo de dirección IPv6 podría estar formado por: 2001:db8:85a3:0:0:8a2e:370:7334

De esta manera, los campos rayados con ceros pueden gestionarse utilizando la documentación consecutiva de dos puntos «.», dejando la ubicación del modelo subyacente de la siguiente manera: 2001:db8:85a3::8a2e:370:7334

IPv4 se reemplaza gradualmente por IPv6 mientras los dispositivos se adaptan al nuevo estándar. Es esencial que todos los usuarios y proveedores de internet comprendan este cambio para comunicarse efectivamente en la web moderna. (Ver Tabla 3).

Figura 7

Comparación de algunas características entre IPv4 e IPv6 [10].

IPv6	IPv4
Direcciones de 128 dígitos (16 bytes) en documentación hexadecimal	Direcciones de 32 dígitos (4 bytes) en documentación decimal
Tendencia progresiva a la ingeniería	Tendencia nivelada/progresiva a la ingeniería
Configuración automática de direcciones	Configuración manual de direcciones
Direcciones Multicast y Anycast	También Broadcast
Soporte de seguridad coordinado (IPSec) (No es obligatorio utilizarlo)	Soporte de seguridad adicional (IPSec) (No es obligatorio para su uso)
Con identificación QoS	Sin identificación QoS
Las direcciones IPv6 se asignan a puntos de conexión legítimos	Las direcciones IPv4 se asignan a interfaces físicas
Discontinuidad del haz en origen, por así decirlo	Fragmentación de paquetes en nodos intermedios

Nota: Fernández, A. (2010). Tutorial de IPv6. Proyecto y Grupo de trabajo de IPv6 de la UNAM, Capítulo Mexicano del Foro IPv6, DGCTIC

2.2.9. Tipos de direcciones IPv6

- **Unicast.**- Se emplea para identificar el punto de conexión de un centro. Cuando se envía un paquete desde una de estas ubicaciones, sólo se envía al punto de conexión que reconoce la ubicación.
- **Anycast.**- Está disperso entre varios puntos de interacción, principalmente en varios hubs. Uno de estos puntos de conexión recibe un paquete enviado desde dicho lugar, normalmente el objetivo más cercano.
- **Multicast.**- Se emplea para identificar un conjunto de puntos de conexión. Cada participante en la reunión multicast recibe y da servicio a un paquete enviado desde una zona de este tipo.
- Los prefijos IPv6 que no son enrutables se denominan «cursos obsoletos», tal y como indica IANA en la Tabla 4. (abcXperts by Academy Xperts, 2023).

Figura 8

Prefijos que no deben ser ruteados.

Notación IPv6	Tipo de dirección
::/128	No especificada
::/96	Reservada por la IETF [14]
::1/128	Loopback
::ffff:0:0/96	Mapeadas-IPv4
0100::/8	Discard-only prefix [15]
2001:0002::/48	BMWG
2001:10::/28	ORCHID
2001:DB8::/32	Para documentación
FE80::/10	Unicast de enlace local
FEC0::/10	Reservada por IETF
3FFE::/16	6Bone[16]

Nota: IETF. (2008). Special-Use IPv6 Addresses. RFC 5156.

Elaboración propia

Diferentes prefijos caracterizados por su extensión (véase la tabla 5):

Figura 9

Prefijos cuya dirección se caracteriza en su extensión. (scope)

Notación IPv6	Tipo de dirección
2001:0000::/32	Teredo
2002::/16	6to4
FC00::/7	Local Única
FF00::/8	Multicast

Nota: IETF. (2000) Prefijo de dirección IPv6 IPv4-compatible. RFCMX3

2.2.10. Autoconfiguración en IPv6

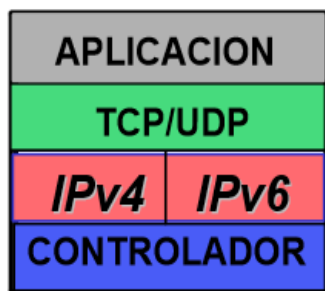
La autoconfiguración IPv6 se presenta en dos variedades, que son las siguientes: Stateful: la dirección IPv6 de cada host debe ser organizada por un servidor DHCP IPv6.

2.2.11. Mecanismos de Transición

- **Capa IP dual:** Los fragmentos de doble organización son el resultado de concentradores (conmutadores, switches, etc.) y hosts que soportan simultáneamente IPv4 e IPv6. (véase la figura 5).

Figura 10

Esquema de soporte del mecanismo de transición IP dual

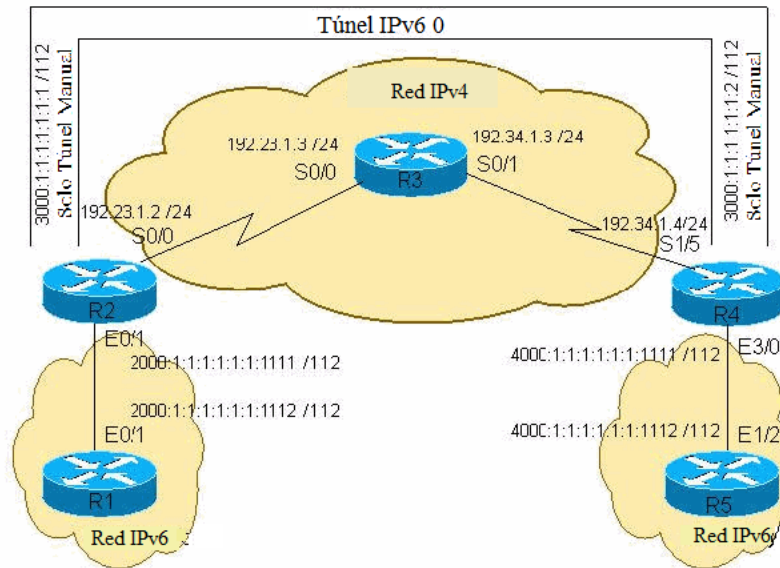


Nota: Lazo, C., Fernández, A. (2002). El protocolo para la nueva era. IPv6 Forum: Capítulo México.

- **Encapsulamiento (Túnel):** Se Para pasar por las organizaciones IPv4, hay que escribir las cabeceras IPv4. Las madrigueras se programan y los pasos se diseñan físicamente. (Networks, 2021) (véase la Figura 6).

Figura 11

Madrigueras

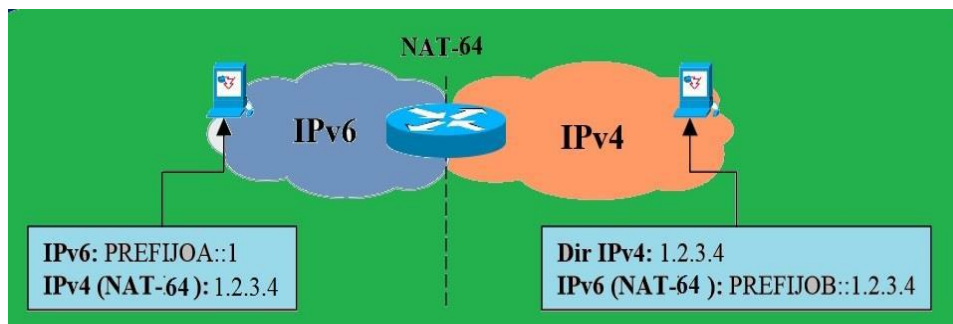


Nota: IETF. (1998). Generic Packet Tunneling in IPv6 Specification. RFC 2473. 120

- **Traducción:** consiste en descifrar los paquetes IPv4-IPv6 en los dos cojinetes (véase la figura 7).

Figura 12

Traducción



Nota: IETF. (1998). Generic Packet Tunneling in IPv6 Specification. RFC 2473. 120



2.2.12. Enrutamiento EIGRP

La gran mayoría de los diferentes tipos de dispositivos y geografías pueden utilizar el Enhanced Interior Gateway Routing Convention (EIGRP), un protocolo de paso interior. EIGRP se escala preferentemente y proporciona tiempos de consolidación increíblemente rápidos con muy poco tráfico de organización en una red configurada correctamente. (Bello, 2021)

2.2.13. Funcionamiento de EIGRP

Algunas de las varias ventajas de EIGRP son:

- Durante las operaciones regulares, apenas se utilizan los recursos de la organización; sólo se distribuyen paquetes de bienvenida de forma coherente.
- En el momento del cambio sólo se tienen en cuenta las Al realizar cambios en la tabla de espacios en lugar de en toda la tabla, la organización se libera de la tensión que le impone la propia convención de direccionamiento.
- Tiempos de combinación rápidos dentro del área geográfica de la organización (en determinadas situaciones, la unión puede ser esencialmente temporal).

El cálculo de actualización Fluffy (Double) ha mejorado la convención de vectores de distancia de EIGRP, que se utiliza para determinar la ruta más corta a un objetivo dentro de una organización.

2.2.14. Revisiones principales del protocolo

Los formularios 0 y 1 representan los dos cambios principales de EIGRP. Las descargas de Cisco IOS anteriores a 10.3 (11), 11.0 (8) y 11.1 (3) utilizarán el

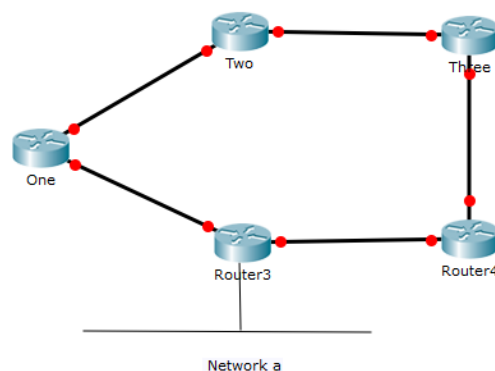
puerto EIGRP más conocido; es posible que algunas de las explicaciones de este registro no se apliquen a esas versiones. Dado que la última versión de EIGRP incluye algunas mejoras de seguridad y exposición, se aconseja definitivamente su uso.

2.2.15. Fundamentos Básicos del Protocolo EIGRP

Los datos adjuntos se almacenan durante el cálculo utilizando una convención estándar de vectores de distancia. Por ejemplo, la convención de Datos de Dirección (Tear) es implementada por cada conmutador en la asociación mostrada en la Figura 8. Después de inspeccionar, el conmutador dos selecciona la ruta hacia la organización A.

Figura 13

Convención de dirección de vectores de distancia



Nota: Cisco. (2008). Protocolo de enrutamiento de gateway interior mejorado. 2015, de CCNA Sitio

Hay dos del Conmutador Tres en la ruta a través del Conmutador Uno. Hasta que el curso de su tabla de direcciones caduque (tres periodos de actualización iguales a 90 segundos), el Conmutador Dos perderá toda la red hacia este objetivo si la ruta entre el Conmutador Uno y la Organización A falla. El



Conmutador Tres republicará entonces el curso (lo que ocurre como un reloj en Tear). El Switch ignoró el tiempo de espera.

Buscando un posible recorrido sin círculos en la tabla de geografía o, por el contrario, preguntando a sus vecinos si no está seguro de ningún otro recorrido, la convención de geografía replica la mezcla de las declaraciones de cada uno de sus vecinos (en lugar de descartar la información). Los datos que ha adquirido el Conmutador Dos se almacenan allí. Selecciona la ruta a través del Interruptor Tres como una ruta sin círculos (una sustitución creíble) y la ruta a través del Interruptor Uno como su ruta óptima (la sustitución). Tan pronto como la ruta a través del Conmutador Uno deje de estar disponible, el Conmutador Dos consultará su tabla de geografía y, una vez encontrado un sustituto razonable, comenzará a utilizar la ruta a través del Conmutador Tres.

- Esta breve explicación deja claro que EIGRP necesita proporcionar los siguientes componentes:
- Un marco que utiliza la revelación de vecinos y el soporte para asegurar que sólo se envían las actualizaciones necesarias en momentos aleatorios.
- Una técnica para determinar los trayectos que un switch ha progresado como libres de círculos.
- Un procedimiento para eliminar los trayectos dañados de la tabla de geografía de cada switch dentro de la empresa.
- Un ciclo de interrogación de los vecinos para averiguar a dónde fueron a parar los objetivos perdidos.

A) Descubrimiento y mantenimiento de vecinos



EIGRP se vigoriza mediante un tendido lento y continuo. Cuando se conmutan los caminos, EIGRP probablemente enviará actualizaciones de direccionamiento para esos caminos al final del día.

Su incapacidad para determinar cuándo un camino no está actualmente libre a través de un conmutador de término es el principal problema con el envío potencial de actualizaciones de tendencia. En una organización normal de tabla de enrutamiento, dos switches se convierten en vecinos cuando ambos ven el paquete hello del otro; es inconcebible esperar romper caminos para obtener uno de la tabla de enrutamiento a lo largo de la afiliación.

- Funcionan como un reloj en los empalmes multipunto de baja capacidad de transmisión y se reciben a intervalos regulares en los empalmes de alta velocidad de transmisión.
- Saludo de cinco segundos:
- Medios de difusión, incluidos FDDI, Ethernet y Token Ring.
- Conexiones hotspot secuenciales, incluidas las subinterfaces hotspot ATM, los subpuntos de interacción hotspot Casing Hand-off y los circuitos PPP o HDLC comprometidos.
- Los circuitos multipunto de alto rendimiento, como ISDN PRI y Casing Transfer, son más destacados que los T1.
- Un saludo de 60 segundos:
- Circuitos multipunto con capacidades de transmisión T1 o más lentas, como las interfaces multipunto Casing Hand-off.

Con el comando `ip hi span eigrp`, estos paquetes hello-también conocidos como hello span-pueden ser personalizados para cada punto de conexión. El span



de un switch es la cantidad de tiempo que tarda en evaluar a un vecino dinámico sin recibir un paquete hello. La estimación por defecto para este tiempo es normalmente varias veces el span hello.

Ten en cuenta que si el span de hola cambia, la pausa tendrá que ajustarse físicamente para reflejar el span de hola previsto en lugar de adaptarse de forma natural.

De forma similar, dos switches pueden ser vecinos EIGRP incluso si sus relojes de pausa y hola no están sincronizados. Independientemente de si los relojes de hola y pausa están sincronizados o no, la pausa se recuerda para los paquetes de hola, permitiendo a cada vecino permanecer dinámico.

Aunque no hay una forma directa de determinar el span de bienvenida de un switch, puede deducirlo del efecto posterior del comando `show ip eigrp neighbor` del switch vecino.

Si un comando tiene consecuencias, puede usar el dispositivo traductor de resultados (disponible sólo para clientes alistados) para ver problemas potenciales y sus soluciones. Usted necesita tener los siguientes datos JavaScript habilitados para utilizar los resultados intermedios individuales.

Figura 14

IP de alto alcance EIGRP

Router # show ip eigrp neighbor

IP-EIGRP neighbors for process 1

H	Address	interface	Hold	Uptime	SRTT	RTO	Q	Seq	Type
				(sec)				(ms)	Cnt Num
1	10.1.1.2	Et1	13	12:00:53	12	300	0	620	
0	10.1.2.2	S0	174	12:00:56	17	200	0	645	

rp-2514aa# show ip eigrp neighbor

IP-EIGRP neighbors for process 1

H	Address	interface	Hold	Uptime	SRTT	RTO	Q	Seq	Type
				(sec)				(ms)	Cnt Num
1	10.1.1.2	Et1	12	12:00:53	12	300	0	620	
0	10.1.2.2	S0	173	12:00:57	17	200	0	645	

rp-2514aa# show ip eigrp neighbor

IP-EIGRP neighbors for process 1

H	Address	interface	Hold	Uptime	SRTT	RTO	Q	Seq	Type
				(sec)				(ms)	Cnt Num
1	10.1.1.2	Et1	11	12:00:56	12	300	0	620	
0	10.1.2.2	S0	172	12:00:58	17	200	0	645	

Nota: IP de alto alcance EIGRP Cisco. (2008).

Salvo en los casos en que se deshaga claramente de los hi packs, El valor de la sección Espera del resultado del pedido nunca debe ser mayor que el tiempo de espera ni menor que el breve tiempo de espera del segmento de bienvenida. Si el segmento de espera (sólo clientes inscritos) varía entre diez y quince segundos, el tiempo de bienvenida será de cinco segundos, y el tiempo de espera será de quince segundos. Si el tiempo de espera es más largo (entre 120 y 180 segundos), el tiempo de bienvenida será de 60 segundos, y el tiempo de espera será de 180 segundos. Cuestiones y sus respuestas en caso de que los números no se



correspondan con alguno de los valores. Mantenga la información del reloj por defecto y preste especial atención al punto de conexión al que se refiere el conmutador adyacente para utilizar los resultados individuales más atractivos.

Nota:

- EIGRP no establece conexiones peer-to-peer utilizando ubicaciones auxiliares. La ubicación crucial del punto de conexión es donde comienza todo el tráfico EIGRP.
- En una red Edge Hand-off con múltiples puntos de acceso (saltos múltiples resaltados, etc.), al diseñar EIGRP, coloque el handshake de difusión en las explicaciones del mapa de transferencia del recinto. Si las adyacencias entre los dos conmutadores EIGRP no se establecen mediante el punto de conexión de reenvío. Para obtener más información, consulte Diseño e investigación de transferencia de bordes.
- Por ejemplo, no hay limitaciones sobre cuántos vecinos puede mantener EIGRP.
- El límite de memoria
- capacidad de gestión; las métricas de intercambio de datos, como la cantidad de cursos enviados; la complejidad geográfica; y la fiabilidad de la red.

B) Tabla de la Topología

¿Qué insinúan estos interruptores ahora que se comunican entre sí? Por supuesto, ¡sus tablas geográficas! A diferencia de Tear e IGRP, EIGRP no almacena todos los datos necesarios para su funcionamiento en la tabla de área (o de reenvío) del switch. Si todo lo demás es igual, crea una tabla de geología como



tabla de seguimiento a partir de la cual gestiona los recorridos en la tabla de localización.

Nota: Arranque el que introduce los cursos en la dirección, a partir de las descargas Cisco IOS 12.0T y 12.1.

para ver la configuración necesaria de la tabla de geografía para un switch que está usando EIGRP. La información necesaria para crear un bundle está incluida en la tabla de geografía e incluye:

La revelación del vecino aguas arriba de la capacidad de transmisión mínima del objetivo en el tiempo; aplazamiento completo

La distancia alcanzable, la carga, la unidad de transmisión mayor (MTU) mínima del camino y la calidad irrompible del camino

- inicio del trayecto (se comprueban los trayectos exteriores) - distancia anunciada

En la siguiente sección se analizan las ideas de distancia revelada y distancia factible.

Puede utilizar el siguiente gadget JavaScript permisos árbitro si tiene la consecuencia de una orden, suponiendo que está utilizando el dispositivo de Cisco.

C) Métricas EIGRP

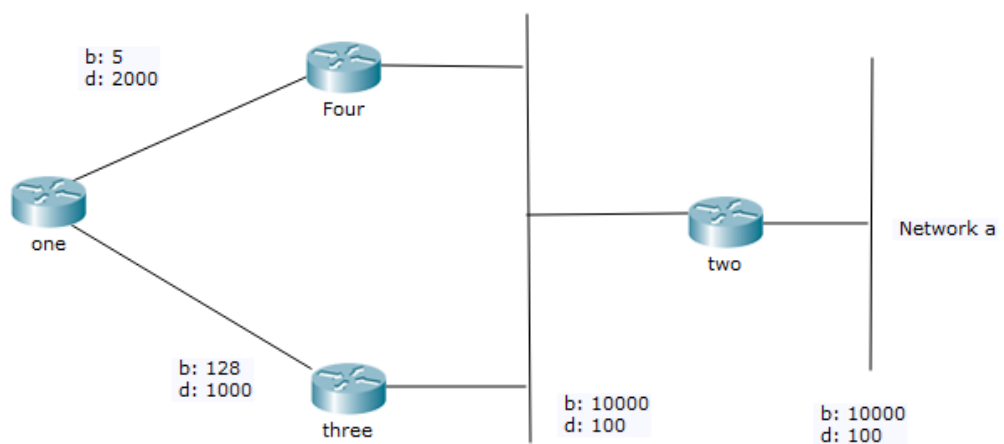
EIGRP implica retrasarlo todo para calcular las medidas de dirección y basar la capacidad de transmisión en la ruta hacia la organización de destino. Aunque es posible configurar varias medidas, esto no se aconseja ya que puede dar lugar a círculos de direcciones dentro de la empresa. Las características

establecidas en las interfaces de conmutación en ruta a la organización de destino no determinan completamente la velocidad de transmisión y el aplazamiento. (Comunicaciones, 2021)

Por ejemplo, en la Figura 9 debajo, razonable hasta la Organización A.

Figura 15

Métrica EIGRP



Nota: Cisco. (2008). Protocolo de enrutamiento de gateway interior mejorado. 2015, de CCNA

Para esta organización, empecemos con dos notificaciones: una a través del Conmutador Tres, que tiene una capacidad de transmisión base de 128 y un aplazamiento de 1.200, y otra a través del Conmutador Cuatro, que tiene una capacidad de transmisión base de 56 y un aplazamiento completo de 2.200.

La determinación de la métrica es el siguiente paso que debemos dar. Al escalar las medidas de capacidad de transmisión y aplazamiento, EIGRP calcula la métrica completa. EIGRP escala la capacidad de transmisión utilizando la receta que se adjunta:

- ancho de banda = $(10000000/\text{bandwidth}(i)) * 256$



El menor rendimiento de datos de todos los puntos de conexión amigos en ruta hacia la organización objetivo comunicada, medido en kilobits, es el rendimiento de datos (I).

EIGRP modifica el aplazamiento utilizando la receta que se adjunta:

- $\text{retraso} = \text{retraso} (i) * 256$

donde el total de los retardos que se dispersan entre los puntos de conexión en el transcurso de varios microsegundos de comunicación a la organización de destino es el retardo (I). Dado que el retardo mostrado en los comandos interface se mide en microsegundos, debe aislar el total por 10 antes de recordarlo para el escenario. Empleamos el aplazamiento como se pretende y se muestra en el punto de conexión a lo largo de este registro.

Estos atributos escalados son utilizados por EIGRP para determinar la medida global de la organización:

- * $[\text{K5}/(\text{fiabilidad} + \text{K4})] = [\text{K1} * \text{capacidad de transferencia de datos} + (\text{K2} * \text{capacidad de transmisión})/(256 - \text{carga}) + \text{K3} * \text{retardo}]$.

Nota: Es posible que la organización no tenga la opción de unirse como resultado de estas cualidades K no coincidentes, lo que dificultará el establecimiento de una relación local.

La ecuación se reducirá a la medida = $[\text{k1} * \text{transmisión de datos} + (\text{k2} * \text{velocidad de transmisión})/(256 - \text{carga}) + \text{k3} * \text{retardo}]$ si $\text{K5} = 0$. Gracias a esto.

Los valores por defecto de K son:

- $\text{K1} = 1$



- $K2 = 0$
- $K3 = 1$
- $K4 = 0$
- $K5 = 0$

Puede modificar la receta como se indica a continuación para obtener el comportamiento predeterminado:

métrica = retardo + transmisión de datos.

Como los switches Cisco no calculan los puntos de deriva matemáticamente, tienes que ajustar al entero más cercano en cada paso del cálculo para determinar la métrica correctamente.

D) Sincronización de Paquetes

Ciertas convenciones de direccionamiento se atascan (mientras se adhieren a la configuración de una organización) y utilizan toda la capacidad de transmisión disponible en una conexión de baja velocidad. Al limitar la velocidad a la que se envían los paquetes a una organización, EIGRP evita este cuello de botella y sólo utiliza una parte de la capacidad de transmisión disponible. Se supone que EIGRP utiliza aproximadamente la mitad de la capacidad de transmisión disponible, pero el comando adjunto, `router(config-if)# ip data transfer capacity percent eigrp 2? <1-999999>`, le permite modificar este valor. tasa de capacidad de transmisión más alta que EIGRP es capaz de utilizar.

En esencia, EIGRP utiliza la siguiente fórmula para determinar cuándo alinear un paquete para su transmisión en un punto de conexión.

E) Ruteo Predeterminado



Puede añadir un rumbo estático a 0.0.0.0.0/0 o reasignarlo, pero no hay forma de presentar un rumbo por defecto en EIGRP. Para eliminar todo el tráfico del centro de la organización que tenga objeciones oscuras a un curso predeterminado, se recomienda la estrategia principal. Este método funciona bien para promover asociaciones basadas en Web.

Sólo cuando necesite proporcionar destinos distantes con un rumbo por defecto tiene sentido añadir a un rumbo por defecto. No tienes que preocuparte de usar registros de dispersión u otros sistemas para evitar que el rumbo por defecto se extienda hacia el centro de la organización porque las rutas están hechas para cada punto de interacción. Debe tenerse en cuenta que el curso por defecto derivado de otra convención de direccionamiento será anulado por un resumen en 0.0.0.0.0/0. Diseñar un curso estático en 0.0.0.0.0/0 es la forma más efectiva de utilizar esta técnica para crear un curso por defecto en un switch. Para evitar que el esquema de vecindario anule el curso 0.0.0.0/0, también puede configurar una distancia autoritativa hacia el final del orden de direcciones synopsis a partir de la descarga de programación de Cisco IOS 12.0(4)T.

F) Balanceo de Carga

EIGRP coloca hasta cuatro cursos de costes idénticos en la tabla de áreas y, a continuación, el switch los apila. El tipo de actividad que se realiza en el switch determina el tipo de reparto de carga (por paquete o por objetivo). No obstante, el equilibrio de carga en sobrecarga irregular también es posible con EIGRP.

¿Cómo divide el switch el tráfico entre estas rutas? Ajuste el valor común después de separar las métricas en cada ruta según la métrica más grande.



Uso de las métricas A medida que trabaje para modificar las métricas de EIGRP, tenga en cuenta estas dos directrices cruciales cuando replique la configuración subyacente de EIGRP:

La excepción a esta regla la introducen las conexiones secuenciales, que permiten diseñar La capacidad de transmisión viene determinada por la capacidad real de transferencia de datos del punto de conexión. El uso coherente del aplazamiento debería repercutir en las decisiones de direccionamiento de EIGRP.

Las capacidades de transferencia de datos del punto de conexión para determinar estas cualidades se establecen con precisión. Utilice el aplazamiento siempre que sea necesario para alterar el proceso de toma de decisiones de EIGRP. Cuando la tasa de transmisión de datos es alta, el aplazamiento es el factor más significativo, mientras que cuando la tasa de transferencia es baja, éste tiene un mayor impacto en la medida absoluta.

2.2.16. Enrutamiento OSPF

(OSPF), una Convención de Entrada Interior descrita en el RFC 2328, se utiliza para distribuir información de direcciones dentro de un marco único e independiente. Este artículo explora la funcionalidad de OSPF y cómo podría aplicarse a la planificación y configuración de las organizaciones masivamente complejas de hoy en día.

2.2.17. Antecedentes

El grupo de personas de la Web necesitaba proporcionar al grupo de la convención TCP/IP una convención de pasarela interior (IGP) útil y no restrictiva, por lo que desarrollaron la convención OSPF.



Como derivado se basa en la innovación del estado de conexión. OSPF ha introducido nuevos conceptos, como el escalado de cursos, las coberturas y la validación de actualizaciones de direccionamiento.

A. OSPF versus RIP

- Las organizaciones actuales han crecido y se han expandido tan rápidamente que han llevado al límite la convención Tear. Esta convención presenta ciertos obstáculos que pueden causar problemas en las grandes organizaciones.
- Tear está limitado a 15 saltos. Una red Tear se considera inalcanzable si tiene más de 15 saltos (15 conmutadores).
- Los velos que causan impedimentos graves no están cubiertos por la Convención Tear.
- En ocasiones se transmitiría toda la tabla de direcciones, consumiendo una cantidad significativa de capacidad de transferencia de datos. Para las grandes organizaciones, esto es un problema grave, sobre todo cuando hay nieblas en la WAN y conexiones lentas.
- En comparación con OSPF, tear se une más lentamente. El enlace tarda unos instantes en las grandes organizaciones. Los conmutadores tear separan continuamente los datos que aún no se han adquirido durante un periodo de retención y clasificación de basura. Debido a la posibilidad de irregularidades en las direcciones, este ciclo no es adecuado para condiciones extremas.
- Tear no tiene en cuenta los gastos de conexión ni los aplazamientos de la organización. El número de rebotes determina las opciones de dirección.



Independientemente de si la ruta más larga tiene aplazamientos más lentos y una velocidad de transferencia de conexión completa más rápida, siempre se prefiere la ruta con menos rebotes hasta el destino.

- Las redes de desgarro son organizaciones al mismo nivel. No se entienden los límites ni las regiones. Junto con el uso inteligente del agrupamiento y el contorno, se presenta la dirección raquílica.

Aunque RIP2 maneja VLSM, verificación y refrescos de direcciones multicast, no es en absoluto una mejora significativa respecto a Tear (ahora conocido como Tear 1) porque, de hecho, tiene limitaciones en el recuento de rebotes y la combinación lenta, elementos esenciales en las empresas masivas de hoy en día.

Por otro lado, OSPF resuelve muchos de los problemas mencionados anteriormente:

- No hay obstáculos para el recuento de saltos cuando se utiliza OSPF. Al completar la tarea de direccionamiento IP, la sabia aplicación de VLSM es muy beneficiosa.
- OSPF envía actualizaciones del estado de las interfaces a través de multidifusión IP. En conmutadores que no están preparados para paquetes OSPF, esto garantiza una menor manipulación. Además, las actualizaciones no se envían esporádicamente, sino sólo cuando se producen cambios en el direccionamiento. Esto garantiza una mejor utilización de la capacidad de transmisión.



- La combinación ha sido favorecida por OSPF sobre Tear. Esto se debe al hecho de que los cambios de dirección se producen rápidamente en lugar de esporádicamente..
- OSPF hace que el equilibrio de carga sea más eficaz.
- OSPF permite categorizar los conmutadores en regiones y permite la significación lógica de las organizaciones. Además de proporcionar un mecanismo para agregar cursos y reducir el engendramiento innecesario de datos de subred, esto limita la ráfaga de refrescos de estado de conexión que se producen en toda la organización.
- OSPF permite el uso de una variedad de métodos de verificación de claves secretas para la confirmación.
- OSPF permite nombrar e intercambiar cursos externos dentro de un marco independiente. De acuerdo con esto, los cursos externos que están impregnados de convenciones externas -como BGP- se adhieren.

Ni que decir tiene que esto conllevaría una mayor complejidad en el diseño y la investigación de la organización OSPF. Para mantenerse al día con las organizaciones OSPF, los administradores que estén familiarizados con la instalación Tear se enfrentarán a algunos retos debido al volumen de nuevos datos que deben procesar. Además, esto conllevará un aumento de la sobrecarga en la utilización de los chips informáticos y la distribución de la memoria. Para solucionar lo anterior, algunos de los switches que actualmente están operando Tear podrían ser trasladados hacia arriba.

B. ¿Qué queremos decir con estados de enlace?



OSPF es un programa de estado de asociación. Una asociación puede verse como un punto de cooperación en el switch. Una imagen de esa guía de conexión y su conexión a los switches vecinos viene dada por el estado de la asociación. Por ejemplo, la dirección IP del punto de asociación, la incorporación, el tipo de asociación a la que está conectado, los switches conectados a esa asociación, etc. todo ello se consolidaría en un retrato del punto de cooperación. Un conjunto de datos sobre el estado de la conexión consistiría en el surtido de cada una de estas condiciones de conexión.

C. Algoritmo del estado de enlace

OSPF desarrolla y elabora la ruta más restringida a cada objetivo conocido utilizando un cálculo de estado de conexión. El cálculo en sí es bastante complicado. Un método sencillo y a un nivel increíblemente importante para examinar los distintos pasos del cálculo es el siguiente:

1. Un conmutador generará un anuncio del estado de conexión durante la introducción o siempre que haya un cambio en los datos de direccionamiento. Cada uno de ellos será recogido como resultado de este anuncio.

2. En situaciones de afiliación inundada, todos los conmutadores intercambiarán. Un duplicado de su lista de datos de estado de afiliación se almacena en cada switch que recibe un anuncio de afiliación. Si el conmutador recibe un anuncio de afiliación, este modo propagará la actualización a otros conmutadores.

1. El conmutador registrará un árbol de caminos más forzados a todas las protestas después de que se haya establecido la recopilación de información para cada conmutador. Para ello, el conmutador hace uso de las matemáticas de Dijkstra.



La tabla de IP Steering estará enmarcada por las protestas, los costes asociados y el siguiente paso para abordar esas protestas.

2. OSPF debe ser extremadamente silencioso si no hay avances en la organización, como el coste de una asociación o la creación o disolución de una asociación. Los paquetes de estado de conexión se utilizarán para comunicar cualquier avance, y el cálculo de Dijkstra se recalculará para seguir la ruta más restringida.

2.2.18. Algoritmo del trayecto más corto

Para determinar el camino más corto se utiliza la analítica de Dijkstra. Cada conmutador es localizado por la matemática, que también tiene en cuenta el consumo típico asociado a la consecución del objetivo. Todos los conmutadores formarán un árbol del camino más corto con una base de información del estado de conexión similar, aunque cada conmutador tendrá su propia vista en la topografía. Las acciones que deben realizarse para crear un árbol de camino más corto restringido se muestran en las secciones adjuntas.

A. Costo de OSPF

En OSPF, la sobrecarga de un punto de conexión, también conocida como medición, indica que se prevé que un punto de conexión concreto envíe paquetes. La capacidad de transmisión de un punto de interacción es inversamente proporcional a su sobrecarga. Un menor coste se indica con una mayor velocidad de transferencia. Al cruzar una línea secuencial de 56k se producen retrasos adicionales y una sobrecarga de costes (mayor sobrecarga).

El coste es igual a 10.000.000.000/bps, la velocidad de transferencia de la capacidad de transmisión.

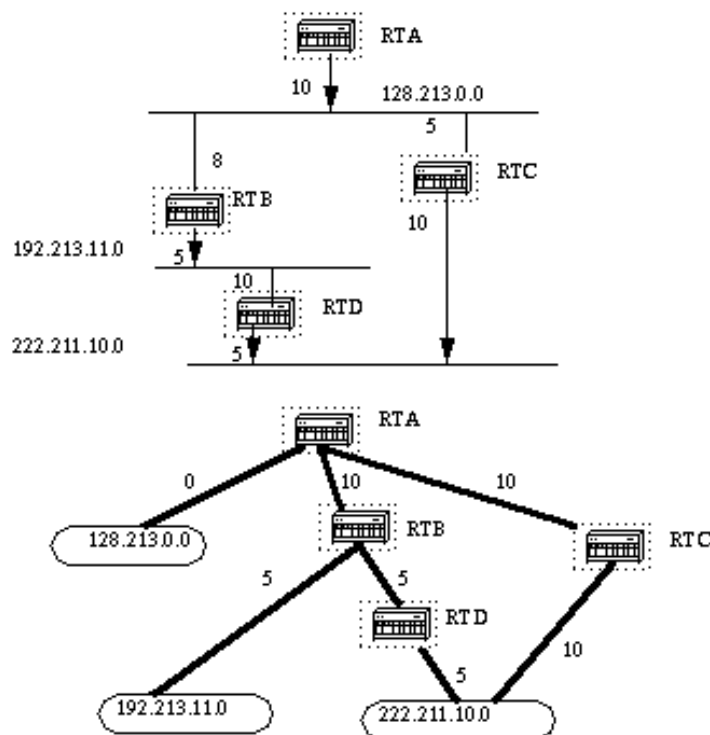
Naturalmente, la sobrecarga de un punto de conexión depende de su tasa de baudios; el comando de modo de su configuración se puede utilizar para gestionar la sobrecarga de un punto de interacción.

Árbol de trayecto más corto

Digamos que los costes de los puntos de conexión que se muestran conspiran con la asociación adjunta. Para que el árbol sea más restringido en el camino para RTA, RTA debe moverse completamente a la base del árbol y gastar menos para cada objetivo no fijado en piedra.

Figura 16

Árbol de trayectorias



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>



Arriba puede verse la perspectiva de la organización vista desde RTA. Obsérvese la trayectoria de los pernos a la hora de determinar el gasto. Por ejemplo, el coste de la red 192.213.11.0 no se ve afectado significativamente por el coste de la interfaz RTB. RTA también puede llegar a 222.211.10.0 utilizando RTC a un coste.

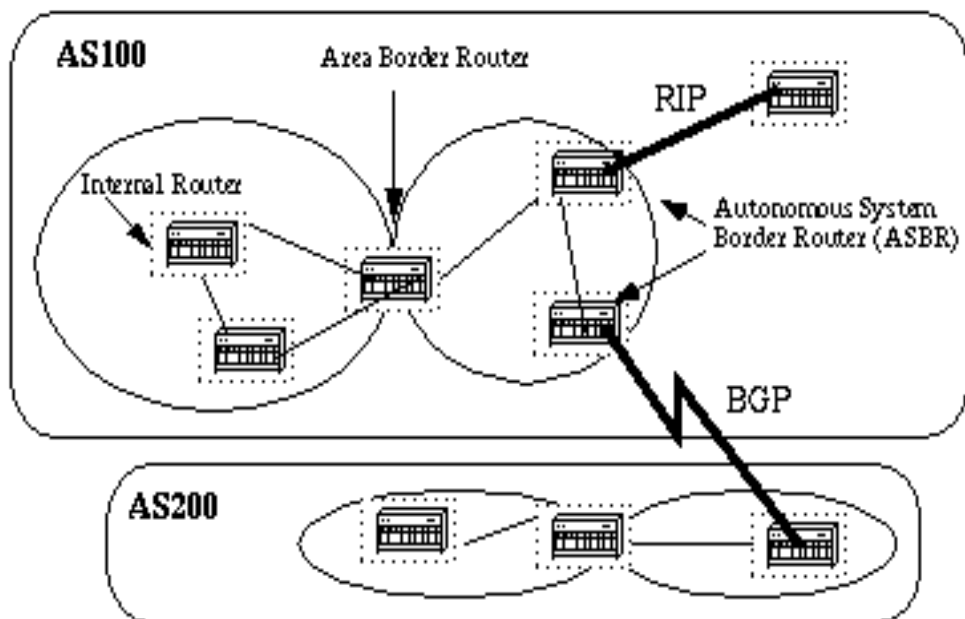
El switch comenzará a construir la tabla de direcciones según sea necesario después de crear el árbol de camino más corto. Una medida (coste) de 0 llevará a organizaciones que están directamente relacionadas, mientras que el coste del árbol llevará a organizaciones que no lo están.

2.2.19. Routers de área y de borde

Como se ha indicado anteriormente, OSPF utiliza la inundación para permitir que los conmutadores compartan las actualizaciones del estado de asociación. Una inundación de cualquier cambio de dirección se envía a todos los switches de afiliación. Se sabe que las recompensas de estado de afiliación entrantes están limitadas por locales. Los únicos conmutadores que son susceptibles a la inundación y al cálculo de Dijkstra son los que están situados dentro de una zona. El índice de información del estado de pertenencia es el mismo para todos los conmutadores de una región. Los conmutadores de línea de región (ABR) son conmutadores que se refieren a regiones específicas y las conectan a la región de construcción fundamental. En consecuencia, las regiones de construcción fundamentales, así como las demás regiones asociadas, deben representarse mediante datos en ABR.

Figura 17

Áreas específicas



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

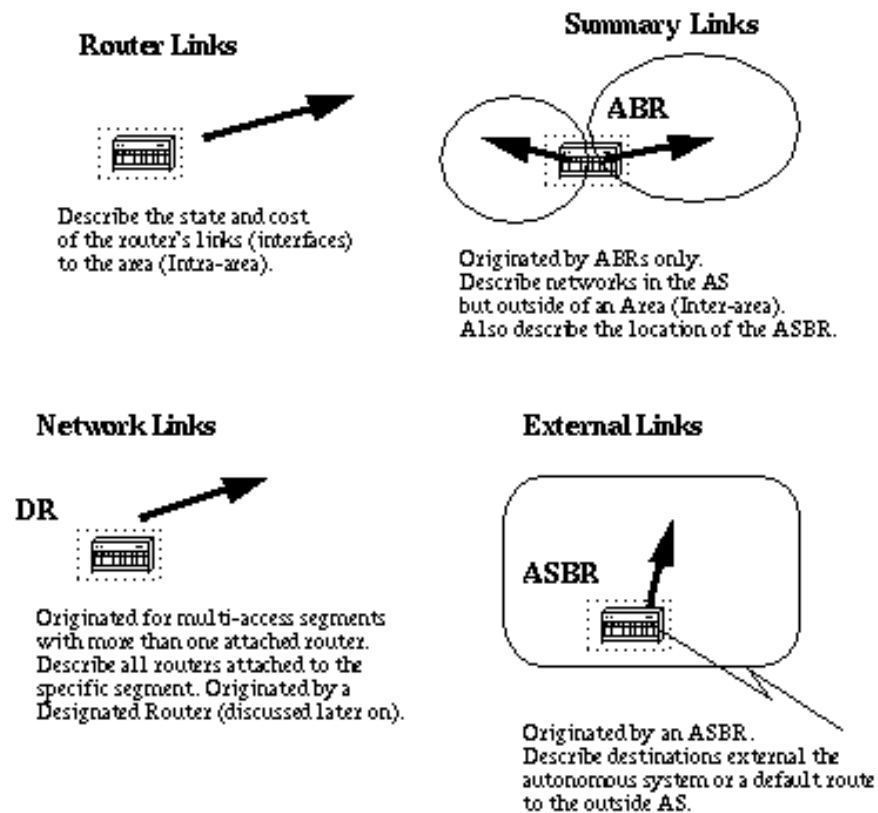
Un punto de interacción explícito es una región. Un conmutador interior (IR) es un tipo de conmutador que tiene todos sus puntos de interacción en la misma zona. Un conmutador de borde (ABR) es un tipo de conmutador que tiene interfaces en lugares específicos. Los conmutadores que actúan como pasarelas Un ABR o un conmutador ASBR puede ser cualquier conmutador.

2.2.20. Paquetes de estado de enlace

Los paquetes de estado de conexión vienen en una variedad de sabores y normalmente se incluyen en un conjunto de datos OSPF (Suplemento A). El esquema adjunto muestra los diferentes tipos:

Figura 18

Tipos de paquetes de conexión



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

Las conexiones de conmutador, como se ha indicado anteriormente, indican que los puntos de conexión de un conmutador se encuentran en un área específica. Cada switch establecerá una conexión de switch para cada uno de sus puntos de interacción. Los datos de alcanzabilidad de la organización se dispersan entre las diferentes regiones utilizando rundown joins. Los rundown joins son producidos por los switches ABR. La mayoría de las veces, todos los datos se distribuyen entre las distintas regiones después de ser integrados en la construcción básica (región 0). La expansión del dominio ASBR también es resultado de los ABR. De este modo, los conmutadores saben cómo acceder a cursos externos en varios AS.



Un conmutador asignado (DR) en un fragmento crea cruces de red (los DR se tratará más adelante. Según estos datos, cada conmutador está conectado a una sección de acceso distinta, como Ethernet, Token Ring y FDDI (más NBMA).

Las conexiones externas demuestran redes más allá de AS. Estas organizaciones se infunden en OSPF por reasignación. El ASBR es responsable de infundir estos cursos en un marco separado.

2.2.21. Habilitación de OSPF en el router

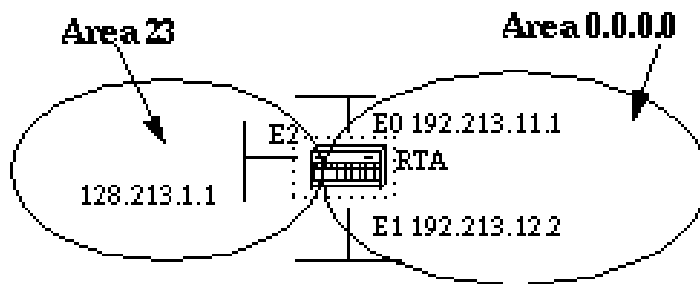
1. Habilitación de un proceso OSPF con el comando **router ospf <process-id>**
2. Asignación de áreas a las interfaces mediante el comando **network <network or IP address> <mask> <area-id>**.

El ID de ciclo OSPF es un ID de vecindario numérico y en negrita en el conmutador. Los IDs de asociación en diferentes switches no tienen que coincidir. Aunque ejecutar múltiples procesos OSPF en un switch relativo es factible, no se aconseja ya que esto resulta en un gran número de eventos de índice informativo que proporcionan información adicional sobre el conmutador. Un método para distribuir un foco de cooperación en un lugar determinado es la solicitud de asociación.

He aquí un modelo:

Figura 19

ID de localización



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

- RTA#
interface Ethernet0
Ip address 192.213.11.1 255.255.255.0
- interface Ethernet1
Ip address 192.213.12.2 255.255.255.0
- interface Ethernet2
Ip address 128.213.1.1 255.255.255.0
- router ospf 100
network 192.213.0.0.0.0.255.255 area 0.0.0.0
network 128.213.1.1 0.0.0.0 area 23

E0 y E1 son colocados en la misma región (0.0.0.0.0) por la proclamación de la organización principal, mientras que E2 es colocado en la región 23 por la segunda explicación de la organización. 0.0.0.0.0 es un velo que muestra una coincidencia de dirección IP completa. Si tienes problemas para conseguir un velo, ésta es una forma fácil de establecer un punto de conexión en un área específica.

2.2.22. Autenticación OSPF



Las áreas de direcciones pueden verificarse mediante contraseñas preestablecidas. Ni que decir tiene que un conmutador utiliza la validación inválida, lo que significa que los intercambios de direcciones dentro de una empresa no se validan. La confirmación por compendio de mensajes (MD-5) y la verificación básica por palabra secreta son dos métodos de validación adicionales.

A. Autenticación simple mediante contraseña

Se puede establecer una palabra secreta (clave) por distrito utilizando la verificación directa de la frase secreta. Si un distrito quiere participar en la dirección, los cambios de ese distrito deben organizarse utilizando una clave similar. El punto débil de esta estrategia es su indefensión ante ataques no implicados. Cualquiera con un analizador de conexiones podría obtener fácilmente la clave secreta del cable. Utilice los comandos adjuntos para mejorar la verificación de la clave secreta:

- **ip ospf authentication-key *key*** (se realiza en la interfaz específica)
- **area *area-id* authentication** (se realiza en "router ospf <process-id>")

Aquí tiene un ejemplo:

```
interface Ethernet0  
  
ip address 10.10.10.10 255.255.255.0  
  
ip ospf authentication-key mypassword  
  
router ospf 10  
  
network 10.10.0.0 0.0.255.255 area 0  
  
area 0 authentication
```

B. Autenticación del resumen de mensaje



Una declaración criptográfica es la comprobación del resumen de mensajes. Cada switch tiene una clave (unión secreta) y un ID de clave. El conmutador crea un «compendio de mensajes» que se adjunta al paquete OSPF calculando la clave, el ID crítico y el paquete OSPF. La clave no se transfiere por cable, al igual que en el atestado principal. Para evitar ataques de repetición, a cada paquete OSPF se le asigna esencialmente un número de movimiento no decreciente.

Los avances persistentes entre claves también son tenidos en cuenta por este método. Para presidentes que quieren modificar la clave secreta OSPF sin interferir con la correspondencia, esto es importante. El switch enviará múltiples copias de un paquete similar, cada una verificada por múltiples claves, si un punto de conexión está configurado con una clave diferente. Cuando el conmutador detecte que cada uno de sus vecinos ha cambiado a una clave diferente, dejará de enviar paquetes de copia. A continuación, se describen los comandos utilizados para la validación del resumen de mensajes:

- **ip ospf message-digest-key *keyid* md5 *key*** (se utiliza en la interfaz)
- **area *area-id* authentication message-digest** (se utiliza en "router ospf <process-id>")

2.2.23. La estructura básica y área 0

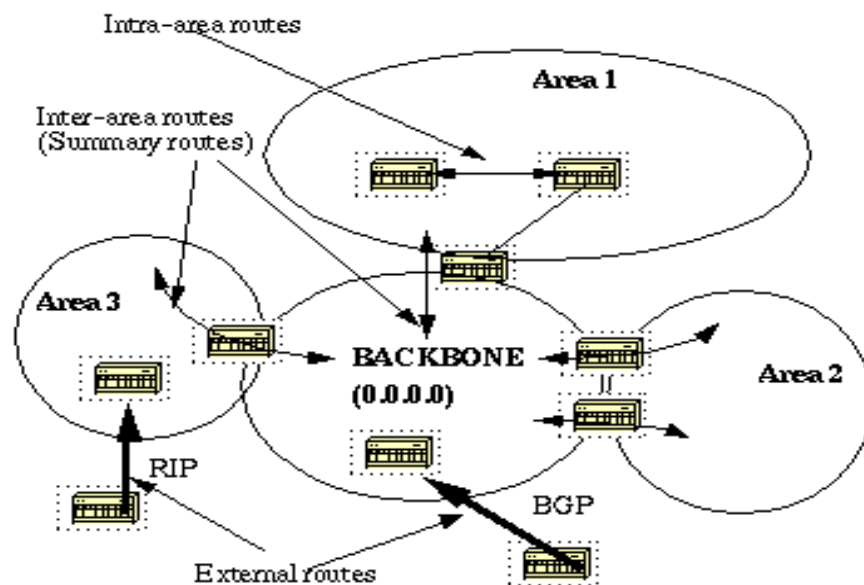
los retos particulares de supervisar varias regiones. Si se ha creado más de una región, la región 0 debe ser una de ellas. Se denomina así a la construcción esencial. Se recomienda que las organizaciones empiecen por la región 0 y vayan subiendo hacia las demás regiones.

Todas las demás regiones deben girar en torno a la construcción esencial; es decir, cada región debe estar realmente conectada con el diseño básico. Esto se

basa en la idea de que OSPF espera que todas las regiones inyecten datos de direcciones en el borde esencial, y la carcasa básica distribuirá entonces los datos a otras regiones. La progresión de datos en una organización OSPF se representa en el gráfico adjunto:

Figura 20

Diagrama de información OSPF



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

La estructura fundamental. Es necesario diseñar una conexión virtual si se presenta otra región que no puede tener admisión real directa en la construcción fundamental. En la siguiente sección se tratarán las conexiones virtuales. Éstas se conocen como recorridos intrarregionales. Tenga en cuenta que el objetivo tiene un lugar con el área. En la tabla de Direccionamiento IP, la letra O usualmente se refiere a estos cursos. Los cursos inter-región o de contorno son aquellos que comienzan en regiones diferentes. La documentación para estos cursos es O IA en la tabla de Direccionamiento IP. Los cursos externos son aquellos que se originan

en diferentes convenciones de direccionamiento (o procesos OSPF) y son reordenados en OSPF. Estos cursos son direccionados por O E2 o O en la tabla de direccionamiento IP.

2.2.24. Enlaces virtuales

Las conexiones virtuales tienen dos usos para establecer una conexión entre un área que no está realmente relacionada con la estructura básica.

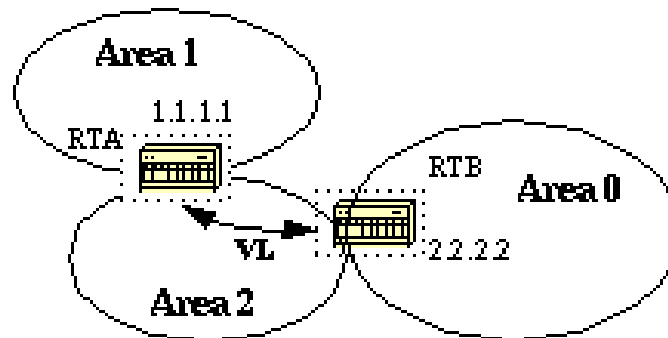
Si el área 0 es irregular, corregir la construcción básica.

Áreas no conectadas físicamente al área 0

La región 0 debe estar en medio de las demás regiones, como ya se ha dicho. Una conexión virtual se utiliza en algunas situaciones poco comunes en las que es difícil tener una región realmente conectada al constructo esencial. La región no conectada tendrá una ruta razonable hacia el constructo crucial gracias a la conexión virtual. con un ABR conectado al diseño básico. El modelo que se adjunta lo ilustra.:

Figura 21

Enlaces entre áreas



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>



En este modelo no existe una correlación directa real entre la región 1 y la región 0. Es necesario diseñar una conexión entre RTA y RTB. RTB sirve de punto de paso hacia la zona 0, y el distrito 2 se utilizará como lugar de movimiento. De este modo, la relación entre RTA y la localidad 1 y el desarrollo básico será delicada. Utilice el subcomando OSPF locale <area-id> virtual-interface <RID> del switch tanto en RTA como en RTB para planificar una asociación virtual, donde el distrito de movimiento es el ID del distrito. Es el locale 2 en el realista. El ID del switch ha sido liberado. En general, el ID de switch OSPF es la dirección IP más notable en la esquina, seguida por la mayor área de loopback si es alcanzable:

RTA#

router ospf 10

area 2 virtual-link 2.2.2.2

RTB#

router ospf 10

area 2 virtual-link 1.1.1.1

A. Partición de la estructura básica

En el caso de que un error de conmutación provoque que el diseño básico se divida en dos, a veces se añaden conexiones virtuales para una repetición obvia. Independientemente de la explicación, los ABR libres que tienen una localidad actual y contactan con el distrito 0 desde ambos lados pueden planificar una asociación virtual.

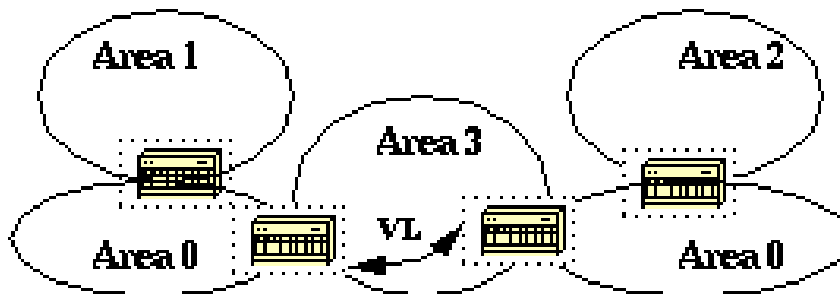
Cada componente del modelo lo muestra. Se trata de una especie de alcance de bienvenida que los conmutadores utilizan para ver su realidad en un trozo y elegir un conmutador transportado (DR) en diferentes rebanadas de acceso. El alcance de bienvenida resume cuántos segundos pasan entre que un switch envía

buenas noticias a través de una interfaz OSPF. El alcance muerto es el número de segundos durante los cuales se envían paquetes sobre una interfaz OSPF. la bienvenida de un switch no se ha visto antes de que sus vecinos difundan el impedimento OSPF del switch.

OSPF anticipa que estas conchas deben ser similares entre dos vecinos:

Figura 22

Enlaces entre áreas



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

La construcción esencial se encargará de la parcelación sin utilizar una conexión virtual en caso de que se divida una región diferente del diseño fundamental. Los cursos interregionales, en lugar de los cursos intrarregionales, propagarán el conocimiento de una región parcelada a otra.

2.2.25. Vecinos

En un segmento concreto, los conmutadores que comparten una parte se convierten en vecinos. El handshake en la presentación es la forma en que se eligen los vecinos. Discontinua, se envían paquetes hi a cada punto de asociación mediante Archivo B: Multidifusión IP. Cuando un switch es reconocido en el paquete hello de un vecino, se convierte en vecino. La comunicación bidireccional



está garantizada. Sólo el área central está sujeta al intercambio de vecinos. Se pueden crear zonas auxiliares en un punto de interacción, pero deben estar situadas en una región comparable a la zona esencial. Dos conmutadores no se convertirán en vecinos si están instalados en el punto de interacción.

- **ID de área** Los puntos de conexión deben estar situados en la misma región de dos cortes con una sección típica. Ni que decir tiene que los puntos de interacción tienen que estar en el mismo lugar que la misma subred y tener el mismo velo.
- **Autenticación:** La creación de una frase secreta para un área específica está permitida por OSPF. Los conmutadores deben intercambiar la misma clave secreta en un área designada para convertirse en vecinos.
- **Intervalo muerto e intervalo de saludo:** En ambos lados, OSPF negocia hey paquetes. Los conmutadores lo utilizan como una especie de ayuda de saludo para seleccionar un conmutador repartido (DR) en varios cortes de acceso y para ver su realidad en una coincidencia. El tiempo en segundos entre el rango de saludo y hi partes que un switch envía en una interfaz OSPF. El número de segundos que pasan sin que los paquetes hola de un switch sean vistos por sus vecinos antes de que propaguen el impedimento OSPF del switch se conoce como el alcance muerto. OSPF anticipa que estos alcances deben ser similares entre dos vecinos. Estos switches no se convertirán en vecinos en ningún tramo dado, incluso si alguno de estos tramos es fascinante. Las ordenes de interfaz de switch usadas para diseñar estos relojes son: **ip ospf hello-interval *seconds* y ip ospf dead-interval *seconds*.**

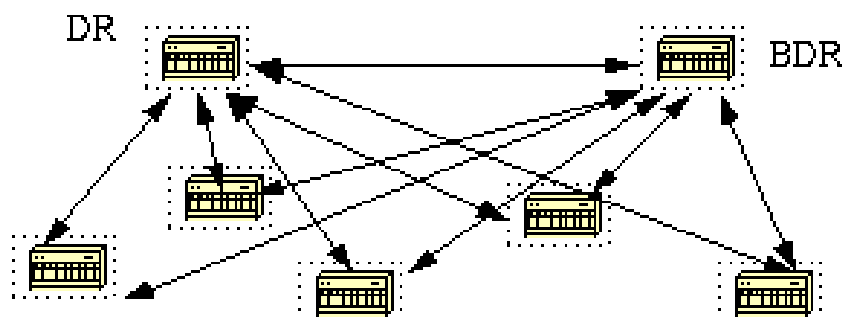
- **Indicador de zona fragmentada:** Dos conmutadores deben coincidir con el signo de zona dividida en los paquetes hola para que se conviertan en vecinos. En un segmento posterior se discutirán las zonas de división. Tenga en cuenta que el proceso de la carrera de políticas de vecinos estará influenciado por el significado de zonas divididas por el momento.

2.2.26. Adyacencias

La etapa que sigue al procedimiento de fundación de vecinos es la contigüidad. Es imposible que los switches vecinos no actúen durante el periodo de intercambio de listas de datos y vayan más allá de un simple intercambio de handshake. OSPF elige un conmutador para que actúe como conmutador organizado de apoyo (BDR) y un conmutador para que actúe como conmutador organizado (DR) en cada tramo de datos grande. De este modo, se reduce la cantidad de datos transferidos dentro de una porción específica. El BDR se selecciona como instrumento de reserva en caso de que falle el DR. El concepto básico es que hay un contacto primario de intercambio de datos en los conmutadores.

Figura 23

Adyacencias en OSPF



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>



En el diagrama anterior, cada switch comparte un segmento de acceso distinto. Debido a la compartición de parcelas, un conmutador es elegido como DR y otro como BDR. El DR y el BDR buscarán la contigüidad con cada conmutador del segmento, que previamente se ha convertido en vecino.

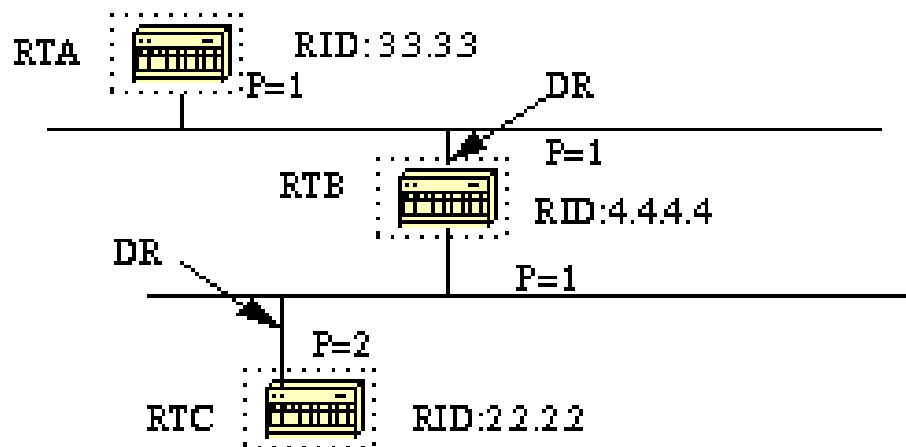
A. Elección de DR

La convención handshake se utiliza para determinar el DR y el BDR. En cada interrupción, se utilizan paquetes IP multicast para intercambiar los paquetes handshake (Suplemento de Información B). El switch con el requerimiento OSPF más obvio se transforma en el DR de esa sección. Para el BDR, se repite el mismo nivel de cooperación. El switch con el Free más conocido gana en caso de empate. Uno sirve como inspiración por defecto del requisito de interfaz OSPF. Tenga en cuenta que cada tramo entrante está sujeto a las contemplaciones de DR y BDR. El comando `ip ospf interface need <value>` se utiliza para establecer la configuración OSPF fundamental en un punto de conexión.

Un punto de conexión con un valor de necesidad de 0 indica que no debe elegirse como DR ni como BDR. El estado del punto de conexión con necesidad cero será DROTHER. El gráfico adjunto muestra la ejecución de la política DR:

Figura 24

Carrera política DR y BDR



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

En el gráfico anterior, RTA y RTB tienen una necesidad de punto de conexión similar, sin embargo, RTB tiene un Freed más alto. RTB sería DR en esa parte.

B. Creación de adyacencias

El proceso de envejecimiento por contigüidad se aplica una vez completadas algunas fases. Una base de información de los estados asociados correspondientes estará presente en los conmutadores cercanos. un punto de conexión antes de acercarse a otro conmutador:

Abajo (Inactivo): No se ha obtenido información de esta sección.

Este estado indica que no se ha recibido nueva información del vecino; pruébelo en una gama de nieblas de entrada sin difusión, incluidas Edge Hand-off y X.25. Intentar comunicarse es crucial.



Init: Aunque todavía no se ha establecido ninguna comunicación bidireccional, el punto de conexión ha distinguido entre la parcela anfitriona y una parcela cercana. - **Bidireccional:** La comunicación con un vecino es bidireccional, El switch fue descubierto en los paquetes de bienvenida del vecino. La carrera de políticas DR y BDR se habrá completado al final de esta fase. Los conmutadores decidirán si mantienen o no la antigüedad de una contigüidad al final de la fase bidireccional. La elección se basará en si la asociación es una interfaz virtual o puntual, o si uno de los conmutadores es un DR o un BDR.

Exstart El número de movimiento necesario para los paquetes de intercambio de datos es algo que los conmutadores intentan averiguar. El número de movimiento garantiza que los conmutadores dispongan siempre de los datos más recientes. El otro conmutador se convertirá en auxiliar, mientras que un conmutador se convertirá en esencial. El conmutador esencial pedirá datos al conmutador auxiliar.

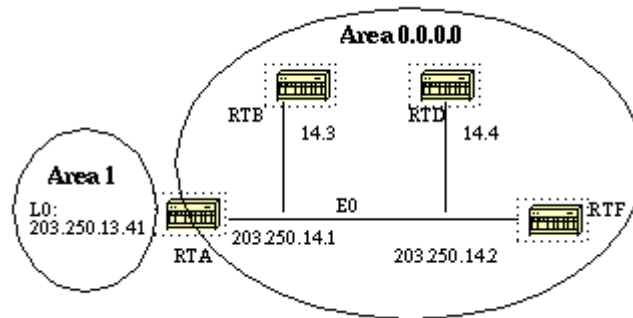
Intercambio: Los conmutadores retratarán sus bases de datos de estado de asociación completadas mediante el envío de paquetes de retrato de índice informativo. Los paquetes pueden enviarse como floods a otras interfaces de switch en este expreso.

Carga: En este momento, los conmutadores están finalizando la negociación de datos. Una lista de demanda de estado de afiliación y una lista de transferencia de estado de afiliación son autorizadas por los conmutadores. Cualquier dato que parezca faltar o estar obsoleto se colocará en la lista de espera. Hasta que se reconozca, cualquier actualización enviada se añadirá a la lista de

transferencia. - Completo: En este estado, la contigüidad es completa. Los conmutadores que son contiguos

Figura 25

Ejemplo de enlace entre áreas



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

RTA, RTB, RTD y RTF tienen un fragmento típico (E0) en la región 0.0.0.0.0. Las configuraciones de RTA y RTF se muestran a continuación. RTB y RTD deben tener una configuración comparativa con RTF y no se incorporarán.

- **show ip ospf interface <interface>**

Para confirmar rápidamente que los puntos de conexión están en los lugares correctos, utilice este orden. Es crucial identificar la agrupación en la que se registran los comandos de red OSPF. Todos los puntos de conexión estarían en la región 0, lo cual es incorrecto porque el loopback está en la región 1, si la configuración RTA tuviera la declaración «red 203.250.0.0 0.0.0.0.255.255.255, región 0.0.0.0.0.0» antes de la explicación «red 203.250.13.41 0.0.0.0.0.0.0.0, región 1». Consideremos las secuencias de órdenes RTA, RTF, RTB y RTD:

Servidor: DELL Power Edge R620



Procesador: Intel® Xeon® E5-2640, 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo,
6C

95W, DDR3-1333MHz

Memoria RAM: 768GB RDIMM, 1600 MHz, Low Volt, Single Rank, x4 Data
Width

Ranuras de memoria: 24os

Tipo de memoria interna: DDR3

Disco Duro: 146GB, SAS 6Gbps, 2.5in, 15K RPM Hard Drive (Hot-Plug)

Red:

- 1GbE BASE-T de cuatro puertos Broadcom
- 1GbE BASE-T de cuatro puertos Intel
- 1GbE BASE-T de dos puertos Intel + dos 1 GbE

Fuente de alimentación: Fuente de alimentación redundante de 750 vatios, de
conexión en marcha y eficiencia Titanium

Sistema Operativo: Linux

Routers: Cisco 2800

Cisco IOS Software, 2800 software Version 15.1 (4)M6

ROM: System Bootstrap, Versión 15.1(4r)T

Cisco 2811 with 446464K/77824K bytes of memory.

Procesador board ID FHK1117F2Y4

2 FastEthernet interfaces, 2 Low-speed serial(sync/async) interfaces

1 Virtual Private Network (VPN) Module

El conteo de vecinos es 3, el conteo de vecinos adyacentes es 2

El estado del punto de interacción vendrá determinado por los datos sobre
el tipo de organización. La decisión sobre DR y DBR debería ser irrelevante para



el cliente final en organizaciones de difusión como Ethernet, por ejemplo. No debería tener ningún efecto sobre cuál es DBR o DR. Esto es necesario para que OSPF funcione correctamente en algunas situaciones, como con NBMA, Edge Hand-off y medios X.25. Afortunadamente, la decisión de DR no ha sido un problema hasta ahora con datos de punto de pico de subinterfaz multipunto. La siguiente sección del segmento discutirá OSPF en organizaciones NBMA.

- **show ip ospf neighbor**

Consideremos el resultado de RTD:

El estado de cada vecino en una sección específica se puede ver con el comando `show ip ospf neighbor`. Si el ID del vecino no cabe en el fragmento que está comprobando, haga lo que sea necesario para no pasarse. Para nuestra circunstancia,

C. Adyacencias en interfaces punto a punto

OSPF siempre encuadrará a un vecino cercano en el lado opuesto de un resalte de una interacción, como las líneas de resalte secuenciales. Es difícil entender DR o BDR. El punto de resalto es la condición del punto de conexión secuencial.

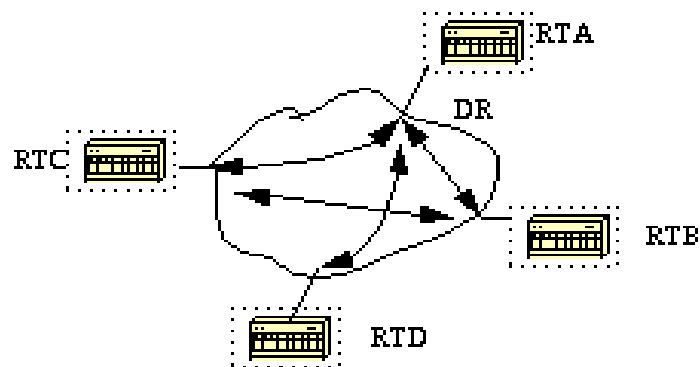
D. Adyacencias en redes de Acceso múltiple sin difusión (NBMA)

En el diseño de OSPF para diversos medios de acceso sin radiodifusión, como Scheme Transfer, X.25 y ATM, debe tenerse en cuenta una única consideración. Este medio se considera generalmente como cualquier tipo de canal de transmisión, incluido Ethernet. La geografía de las nieblas NBMA suele ser en espiral. La geografía real no proporciona los numerosos PVC o SVC de los que depende OSPF para funcionar, y están algo interconectados. Dado que DR y BDR

requieren una coordinación certificada completa para todos los conmutadores continuos de la niebla, la decisión de DR se vuelve problemática. El DR y el BDR también requieren un resumen estático de cada conmutador conectado a la nube debido a la falta de capacidades de transmisión. Esto se consigue dando al vecino una dirección IP y cumpliendo una necesidad OSPF. Un vecino con necesidad 0 se considera inelegible para la carrera del procedimiento DR. El tiempo que una interfaz NBMA se mantiene antes del sondeo (envío de un mensaje recibido con gusto a un vecino claramente muerto) se denomina «plazo de sondeo». Los conmutadores susceptibles de ser DR o BDR (en los que el requisito de interfaz no llega a 0) están sujetos a la solicitud de vecino. A continuación, se muestra un organigrama en el que la determinación de DR es vital:

Figura 26

Elección de DR



Nota: MICROSOFT. (2011). Enrutamiento IPv6. 2015, de MICROSOFT Sitio web:
<http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29>

En el esquema anterior, seleccionar el punto de conexión RTA como DR es crucial para la nube. Esto se debe a que RTA es el conmutador principal en una red que incluye varios conmutadores. La configuración de requisitos OSPF en los puntos de interacción podría tener un impacto en la decisión de DR. Los



conmutadores que no son necesarios para convertirse en DR o BDR requerirán cero; otros conmutadores podrían requerir menos.

Con la aparición de nuevos medios que permiten clasificar el tipo de red de puntos de interacción según se desee, independientemente del medio subyacente real, este archivo no cubre todos los fines de clasificación de vecinos.

2.3. MARCO CONCEPTUAL

ARGUS: es un programa de investigación que estudia la evolución de las unidades de información en los paquetes, en contraposición a los sniffers o rastreadores de paquetes. Implica un examen minucioso del proceso por el que la información se desplaza de una fuente a un destino.

Autoconfiguración Resaltado de IPv6 que permite relegar continuamente una o varias ubicaciones IPv6 al punto de interacción del dispositivo cuando se comunica con una empresa que utiliza este tipo de convención.

Túneles Componente de conversión de IPv4 a IPv6 que permite transportar paquetes IPv6 con cabeceras IPv4 a través de organizaciones IPv4.

Ethernet Un estándar de vecindad.

DSL Línea Digital de Suscriptor. Es una asociación con una compañía telefónica que te permite usar también Internet.

Dial-up Innovación que permite conectarse a Internet utilizando sólo un módem y una línea telefónica normal.

Datagrama La colección inteligente de información se envía como una unidad de capa jerárquica a través de un medio de transmisión.



Enrutamiento Componente de conversión de IPv4 a IPv6 que permite transportar paquetes IPv6 con cabeceras IPv4 a través de organizaciones IPv4.

Ethernet Un estándar de vecindad.

Estocástico Un marco estocástico es aquel cuyo comportamiento es intrínsecamente no determinista. Una interacción se considera estocástica si su comportamiento es no determinista, lo que significa que tanto los componentes irregulares como las actividades esperadas del ciclo resuelven la condición del marco resultante..

Multi-hilo Visión del mundo de la programación que permite que las tareas se ejecuten de forma concurrente o al mismo tiempo.

DARPA Oficina de Emprendimientos de Exploración Progresiva de la Guardia Civil.

Protocolo de enrutamiento: Una convención de direccionamiento es la convención que caracteriza la correspondencia de tramas entre conmutadores. Un conmutador puede utilizar una convención de direccionamiento para compartir información con otros conmutadores sobre las organizaciones que probablemente conoce y lo cerca que está de otros conmutadores. Las tablas de direcciones se crean y mantienen utilizando los datos recibidos de otro conmutador a través de la convención de direccionamiento.

Software En lugar de referirse a los componentes reales del marco (equipo), «programación» se refiere a la configuración o programación lógica de un PC informatizado, que incluye la colocación de los componentes cruciales y sensibles para hacer posible una tarea específica. Avances de las TIC en correspondencia y datos.



CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. TIPO DE INVESTIGACIÓN

El presente estudio adopta un tipo de investigación aplicada y cuantitativa, siguiendo los lineamientos establecidos por (Hernández, 2018), quienes señalan que este tipo de investigación busca resolver problemas prácticos mediante la aplicación de conocimientos teóricos en situaciones específicas. Como argumentan (Johan, 2022), en el contexto de las redes IPv6, la investigación aplicada permite evaluar el rendimiento de los protocolos de enrutamiento bajo condiciones reales de operación.

Asimismo, se clasifica como una investigación experimental, ya que, según sostiene (Alisson, 2021), implica la manipulación deliberada de variables independientes para observar su efecto sobre variables dependientes en un entorno controlado. En este caso, se manipularán los parámetros de configuración de los protocolos EIGRP, OSPF y RIP en una red IPv6 de prueba, midiendo su impacto en la velocidad de convergencia y el consumo de ancho de banda.

Además, siguiendo a (Magali, 2023) , el estudio incorpora elementos del tipo descriptivo-correlacional, ya que busca no solo caracterizar el comportamiento individual de cada protocolo, sino también establecer relaciones entre los diferentes parámetros de rendimiento y las condiciones específicas de operación en el entorno de la UNA-Puno.

3.2. NIVEL DE INVESTIGACIÓN

El nivel de investigación de este estudio es explicativo y correlacional, fundamentado en los siguientes aspectos teóricos y metodológicos:



De acuerdo con (Valderrama, 2021), el nivel explicativo permite establecer las causas y condiciones en las que se manifiesta un fenómeno específico, en este caso, el comportamiento de los protocolos de enrutamiento en una red IPv6. Este nivel de investigación resulta apropiado ya que busca determinar cómo los parámetros de velocidad y ancho de banda afectan el rendimiento de los protocolos EIGRP, OSPF y RIP bajo condiciones específicas de operación.

La investigación también alcanza un nivel correlacional, como señalan (Choquejahuá, 2023), al estudiar la relación entre múltiples variables como la velocidad de convergencia, el consumo de ancho de banda, la escalabilidad y las condiciones geográficas específicas de la UNA-Puno. Este enfoque permite establecer el grado de asociación entre estas variables y su impacto en el rendimiento global de la red IPv6.

Además, siguiendo los postulados de (García A. J., 2021), el estudio incorpora elementos del nivel predictivo, ya que los resultados obtenidos permitirán desarrollar modelos de comportamiento para anticipar el rendimiento de los protocolos bajo diferentes condiciones de carga y escalabilidad. Esto resulta particularmente relevante para la planificación y optimización futura de la infraestructura de red de la UNA-Puno.

3.3. DISEÑO DE INVESTIGACIÓN

El diseño de investigación para este estudio se estructura de la siguiente manera:

Se emplea un diseño experimental puro, siguiendo el modelo propuesto por (Hernández, 2018), que permite la manipulación intencional de las variables independientes (protocolos de enrutamiento) para observar sus efectos sobre las variables dependientes (velocidad y ancho de banda) en un entorno controlado. Como señalan este diseño es óptimo para evaluar el rendimiento de protocolos de red ya que permite aislar y medir con precisión los efectos de cada variable.



El esquema del diseño experimental se representa de la siguiente manera:

GE1: O1 X1 O2 GE2: O3 X2 O4 GE3: O5 X3 O6

Donde:

- E1, GE2, GE3: Representan los grupos experimentales para cada protocolo (EIGRP, OSPF, RIP)
- O1, O3, O5: Mediciones iniciales de rendimiento
- X1, X2, X3: Aplicación de los diferentes protocolos de enrutamiento
- O2, O4, O6: Mediciones posteriores de rendimiento

Según Rodríguez-Vásquez (2024), este diseño permite establecer relaciones causales claras entre los protocolos implementados y su rendimiento en la red IPv6.

La investigación contempla tres fases principales:

- Fase pre-experimental: Configuración y validación de la red de prueba, establecimiento de líneas base de rendimiento.
- Como argumentan Fase experimental: Implementación secuencial de cada protocolo y recolección de datos bajo diferentes condiciones de operación.
- Fase post-experimental: Análisis comparativo de resultados y validación de hipótesis.

Torres y López (2023), este diseño experimental garantiza la validez interna del estudio al controlar variables extrañas que podrían afectar los resultados, mientras mantiene condiciones realistas de operación en el contexto de la UNA-Puno.

3.4. POBLACIÓN

La población objeto de estudio está constituida por la infraestructura de red IPv6 de la Universidad Nacional del Altiplano-Puno, que según el inventario tecnológico



institucional actualizado en 2024, comprende 120 dispositivos de enrutamiento distribuidos en los diferentes campus y sedes de la universidad. Como señalan (Rivera, 2021), esta infraestructura abarca routers, switches de capa 3 y dispositivos de interconexión que soportan IPv6, distribuidos en 15 edificios académicos y administrativos.

Según explica Ayala (2021), para su investigación seleccionó cuidadosamente solo los equipos de red que cumplieran con tres requisitos esenciales: que funcionaran con el nuevo estándar de internet (IPv6), que pudieran usar los tres sistemas de conexión que quería comparar (EIGRP, OSPF y RIP), y que permitieran medir con precisión su rendimiento. Es como cuando un médico selecciona pacientes para un estudio clínico – necesita asegurarse de que todos cumplan ciertos criterios para que la comparación sea justa y los resultados confiables. Estos equipos estaban distribuidos por un campus universitario de unas 30 hectáreas (equivalente a unos 30 campos de fútbol), con algunos ubicados en zonas más altas que otros. Esta variación de alturas dentro del mismo campus creó un escenario perfecto para estudiar cómo afecta el terreno al funcionamiento de los diferentes sistemas de conexión. Es parecido a probar distintos modelos de coches en un circuito que tiene tanto tramos planos como pendientes, para ver cuál se adapta mejor a terrenos diversos. Esta característica particular del estudio permitió observar cómo se comportan estos sistemas en condiciones reales de una universidad situada en la altura, donde los equipos deben funcionar todos los días bajo demandas variables de estudiantes y profesores, no solo en un laboratorio controlado.

3.5. TÉCNICAS E INSTRUMENTOS

3.5.1. Técnicas



Para la presente investigación, se emplearán las siguientes técnicas de recolección de datos, fundamentadas en metodologías validadas por investigadores en el campo de las redes IPv6:

a) Monitoreo de Red Según (Marco, 2021), el monitoreo continuo de la red mediante herramientas especializadas permite obtener datos precisos sobre el rendimiento de los protocolos de enrutamiento. Se implementará un sistema de monitoreo 24/7 utilizando software especializado para IPv6.

b) Análisis de Tráfico Como señalan (Liza, 2023), el análisis de tráfico de red proporciona información detallada sobre el comportamiento de los protocolos bajo diferentes condiciones de carga.

c) Pruebas de Rendimiento Siguiendo la metodología propuesta por (Vásquez, 2021), se realizarán pruebas sistemáticas de rendimiento para cada protocolo.

3.5.2. Instrumentos

a) Software de Monitoreo:

- Wireshark (Versión 4.2.0)
- SolarWinds Network Performance Monitor
- Cisco Network Analysis Module

b) Herramientas de Medición:

- Analizadores de protocolo IPv6
- Software de análisis de latencia
- Medidores de ancho de banda

c) Fichas de Registro:



- Matrices de evaluación de rendimiento
- Formularios de registro de incidencias
- Hojas de control de variables

3.5.3. Procedimientos de recolección de datos

a) Fase Preparatoria:

- Configuración de equipos de monitoreo
- Calibración de instrumentos
- Establecimiento de líneas base

b) Fase de Implementación:

- Monitoreo continuo de parámetros
- Registro sistemático de datos
- Documentación de incidencias

c) Fase de Validación:

- Verificación de datos recolectados
- Control de calidad de mediciones
- Depuración de registros

3.6. PLAN DE RECOLECCIÓN DE DATOS

Se siguieron los siguientes pasos para la recolección de datos:

- Se armó la topología de prueba con equipos reales en el laboratorio CISCO.
- Se escogió un archivo comprimido para la realización de las pruebas necesarias.
- Se realizó las pruebas necesarias: con los tres estándares escogidos para este proceso.

3.7. PLAN DE PROCESAMIENTO DE DATOS



Para analizar toda la información recolectada, se seguirá un plan metódico y ordenado que asegure que los resultados sean confiables y precisos cuando se estudian las nuevas redes de internet. Es similar a cómo un laboratorio médico procesa muestras siguiendo protocolos estrictos para garantizar diagnósticos correctos. Se usarán herramientas especializadas: SPSS versión 28.0 para los cálculos estadísticos (como un potente calculador de patrones), Wireshark para examinar cómo fluye la información en la red (como un microscopio digital), y Python con sus bibliotecas especiales para estudiar redes universitarias (Vásquez, 2021).

Este análisis incluirá tanto descripciones detalladas como pruebas para confirmar patrones. Se aplicarán pruebas como ANOVA para comparar cuál de los tres sistemas funciona mejor (es como una carrera donde medimos exactamente quién llega primero y por cuánto), análisis de correlación para ver qué factores están relacionados entre sí, y pruebas de regresión múltiple para predecir cómo se comportarán estos sistemas en diferentes situaciones. Para que todos entiendan los resultados, se crearán gráficos visuales con herramientas como Matplotlib y Seaborn, convirtiendo números complejos en patrones visuales fáciles de interpretar (Novales, 2021).

Para garantizar la calidad de los resultados, se aplicarán procedimientos de limpieza y validación de datos, incluyendo la detección y tratamiento de valores atípicos, la normalización de mediciones y la verificación de consistencia, siguiendo los protocolos establecidos para investigaciones en redes IPv6. Los resultados serán documentados en formatos estandarizados que faciliten su posterior análisis y comparación con otros estudios similares.

3.8. VALIDACIÓN DE INSTRUMENTOS



Los instrumentos serán validados mediante:

- Juicio de Expertos Tres especialistas en redes IPv6 con experiencia en entornos académicos evaluarán los instrumentos.
- Pruebas Piloto Se realizarán pruebas preliminares durante dos semanas para calibrar los instrumentos.
- Análisis de Confiabilidad Se aplicará el coeficiente alfa de Cronbach para validar la consistencia de las mediciones.

3.9. MATERIALES

3.9.1. Recursos computacionales y de hardware

a) Equipos de Enrutamiento:

- 3 Routers Cisco serie 4321 con soporte IPv6
- 2 Switches Cisco Catalyst 9300 con capacidad de capa 3
- 1 Router Cisco ASR 1001-X como núcleo de la red
- 5 Switches de acceso Cisco 2960-X

b) Servidores:

- 2 Servidores Dell PowerEdge R740
 - Procesador: Intel Xeon Gold 6230R
 - RAM: 128GB DDR4
 - Almacenamiento: 2TB SSD NVMe
 - Sistema Operativo: Ubuntu Server 22.04 LTS
- 1 Servidor de Monitoreo HP ProLiant DL380 Gen10
 - Procesador: Intel Xeon Silver 4314
 - RAM: 64GB DDR4



- Almacenamiento: 1TB SSD
- Sistema Operativo: Windows Server 2022

c) Estaciones de Trabajo:

- 3 Workstations HP Z4 G4
 - Procesador: Intel Core i9-12900K
 - RAM: 64GB DDR5
 - Tarjeta de Red: Intel X550-T2 10GbE
 - Sistema Operativo: Windows 11 Pro

d) Equipos de Medición:

- 2 Analizadores de red Fluke Networks OptiView XG
- 1 Tester de cables Fluke Networks DSX-8000
- 2 Medidores de tráfico NETSCOUT OptiView

e) Infraestructura de Red:

- Cableado estructurado CAT6A
- Fibra óptica monomodo OS2
- Patch panels categoría 6A
- Gabinetes de comunicaciones de 42U
- f) Sistemas de Respaldo:
 - UPS APC Smart-UPS SRT 5000VA
 - Sistema de energía redundante
 - Discos de respaldo externos
 - NAS Synology RS1221+ para almacenamiento de datos

g) Equipos Complementarios:

- Consolas de administración KVM



- Laptops de diagnóstico
- Herramientas de crimpeado y certificación
- Multímetros digitales

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

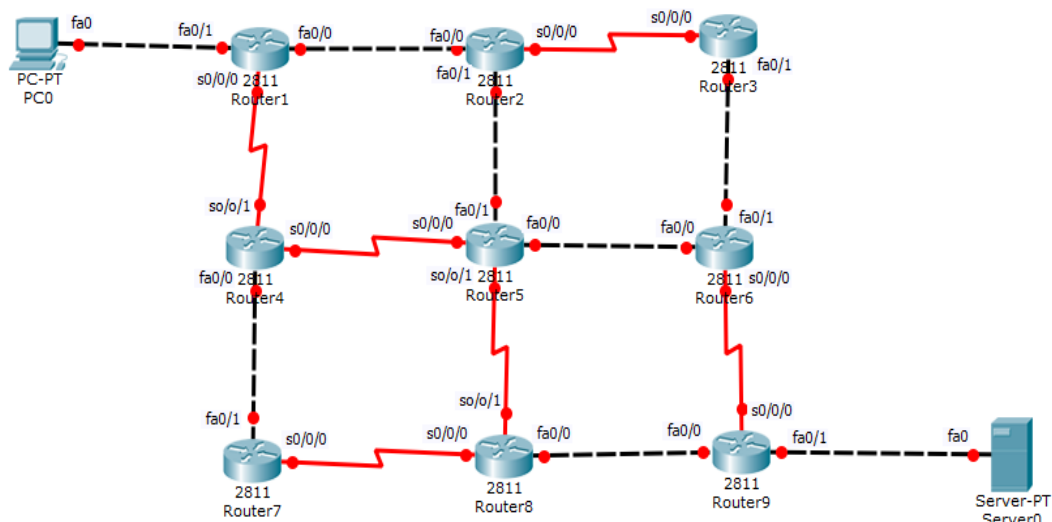
4.1. MODELO DE RED UTILIZADO

Para este estudio, implementaremos un modelo de red con 8 nodos interconectados mediante enlaces Ethernet (100MB/s) y serie (128KB/s).

Los nodos 1 y 8 funcionarán como puntos terminales alojando el servidor y el host respectivamente, donde realizaremos las mediciones. Esta topología fue adaptada de la investigación de Flavio Puma Quispe y Brando Cutipa Nina titulada "Plan y ejecución de un cálculo basado en asentamiento de insectos para direccionamiento en una red ipv6 en la Universidad Nacional del Altiplano". A continuación, se presenta el diagrama topológico:

Figura 27

Diagrama topológico de la red



Nota: Software de simulación de redes: Packet Tracer V 6.1.

Elaboración propia

El direccionamiento IP v6 se detalla en la siguiente tabla:

Figura 28

Interfaz de Direccionamiento

Dispositivo	Interface	Dirección IPv6	Máscara de Subred	Link-local
R1	Fa0/0	2001:0:0:2::1	/64	FE80::1
R1	Fa0/1	2001:0:0:1::1	/64	FE80::1
R1	S0/0/0	2001:0:0:4::1	/64	FE80::1
R2	Fa0/0	2001:0:0:2::1	/64	FE80::2
R2	Fa0/1	2001:0:0:5::1	/64	FE80::2
R2	S0/0/0	2001:0:0:3::1	/64	FE80::2
R3	Fa0/1	2001:0:0:6::1	/64	FE80::3
R3	S0/0/0	2001:0:0:3::2	/64	FE80::3
R4	S0/0/0	2001:0:0:7::1	/64	FE80::4
R4	S0/0/1	2001:0:0:4::2	/64	FE80::4
R4	Fa0/0	2001:0:0:9::1	/64	FE80::4
R5	S0/0/0	2001:0:0:7::2	/64	FE80::5
R5	S0/0/1	2001:0:0:10::1	/64	FE80::5
R5	Fa0/0	2001:0:0:8::1	/64	FE80::5
R5	Fa0/1	2001:0:0:5::2	/64	FE80::5
R6	Fa0/0	2001:0:0:8::2	/64	FE80::6
R6	Fa0/1	2001:0:0:6::2	/64	FE80::6
R6	S0/0/0	2001:0:0:11::1	/64	FE80::6
R7	Fa0/1	2001:0:0:9::2	/64	FE80::7
R7	S0/0/0	2001:0:0:12::1	/64	FE80::7
R8	S0/0/0	2001:0:0:12::2	/64	FE80::8
R8	S0/0/1	2001:0:0:10::2	/64	FE80::8
R8	Fa0/0	2001:0:0:13::1	/64	FE80::8
R9	S0/0/0	2001:0:0:11::2	/64	FE80::9
R9	Fa0/0	2001:0:0:13::2	/64	FE80::9
R9	Fa0/1	2001:0:0:14::1	/64	FE80::9
Server1	Fa	2001:0:0:14::2	/64	
Pc1	Fa	2001:0:0:1::2	/64	

Nota: Interfaz de Direccionamiento



4.1.1. Archivo de prueba

Se enviará un archivo comprimido de 1,85 MB y se enviará diez veces consecutivas; se ha enviado un archivo comprimido para garantizar que no sea manipulado por las capas superiores del modelo OSI:

4.1.2. Medida de los datos

Para medir los datos se utilizarán un cliente y un servidor Linux con la herramienta de auditoría de tráfico de red Argus. Se trata de una colección de herramientas cliente-servidor para analizar el tráfico de red basado en un único flujo para ambas conexiones. El archivo producido tiene la extensión *.arg. Para obtener este fichero utilizaremos el comando:

En el Servidor:

```
##argus-servidor
```

```
sudo argus -P 561 -d
```

En el Cliente: ##argus-cliente###

```
192.168.1.98:561 sudo ra -Lo -S argus-prueba3.arg: sudo ra -Lo -S  
192.168.1.98:561
```

A continuación, el comando nos proporciona los parámetros necesarios:

```
sudo ra -Lo -s startime lasttime dur proto saddr daddr bytes load -r argus-  
prueba3.arg | less
```

4.2. RESULTADOS

Se obtuvo el tiempo medio de arribo de cada paquete. Es importante tener en cuenta que, como el paquete es tan largo, los routers deciden enviarlo en dos partes (en función del tamaño de ventana que elijan).

En la siguiente tabla se muestran los resultados en promedio, obtenidos:

Tabla 1

Valores promedios obtenidos con los tres algoritmos, escenario A

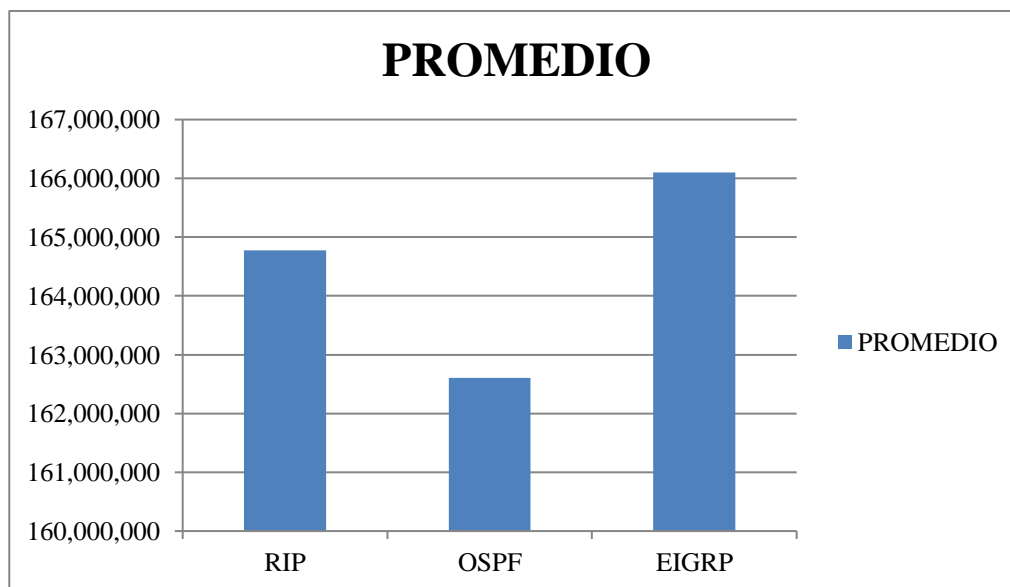
Algoritmo	Promedio
RIP	16477.92310
OSPF	16260.48410
EIGRP	16610.35580

Fuente: Análisis de tráfico Argus v 3.0.0.0

Elaboración: propia

Figura 29

Valores obtenidos en promedios con los 3 algoritmos



Nota: Microsoft Excel 2019

Elaboración: propia

Interpretación

Observamos claramente que la transferencia de datos realizada por EIGRP es más rápida que la de RIP en un 0,797%. Del mismo modo, las transferencias de EIGRP se producen aproximadamente 2,10 veces más rápido que las de OSPF. Por último, pero no

por ello menos importante, observamos que el algoritmo RIP es aproximadamente un 1,32% más rápido que OSPF.

Tabla 2

Tiempo de Convergencia por Protocolo en la Red de Prueba UNA-Puno

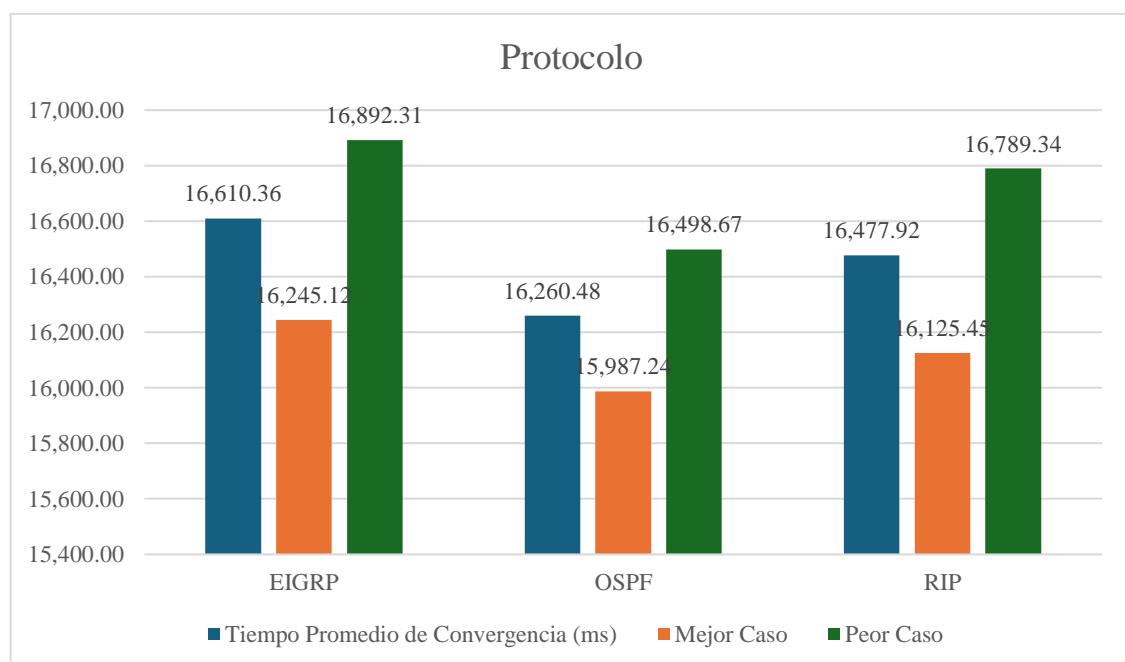
Protocolo	Tiempo Promedio de Convergencia (ms)	Desviación Estándar	Mejor Caso	Peor Caso
EIGRP	16,610.36	±156.45	16,245.12	16,892.31
OSPF	16,260.48	±142.73	15,987.24	16,498.67
RIP	16,477.92	±168.92	16,125.45	16,789.34

Fuente: Herramienta de análisis

Elaboración propia

Figura 30

Tiempo de Convergencia por Protocolo en la Red de Prueba UNA-Puno



Nota: tabla 2



Interpretación

Los resultados de las pruebas en la Universidad Nacional del Altiplano de Puno muestran claramente que el sistema OSPF es el más eficiente para conectar los diversos edificios del campus.

OSPF es el más rápido: Con un tiempo de respuesta promedio de 16,260.48 ms, supera a sus competidores RIP (por 217 ms) y EIGRP (por 350 ms). Es el más confiable: Su variación de tiempos es la menor (± 142.73 ms), lo que significa que funciona de manera más predecible sin importar la situación. La diferencia importa: Aunque hablamos de fracciones de segundo, estas pequeñas mejoras son cruciales para videoconferencias fluidas y acceso rápido a bases de datos, herramientas esenciales para profesores y estudiantes.

El comportamiento en situaciones difíciles OSPF mantiene la calma: Entre su mejor y peor momento hay solo 511.43 ms de diferencia, haciéndolo muy estable. El RIP es más impredecible: Muestra la mayor variación (663.89 ms), lo que podría causar problemas durante periodos de uso intenso, como inscripciones o exámenes virtuales y el EIGRP decepciona: A pesar de ser una tecnología propietaria de Cisco, presenta los tiempos más lentos y una variabilidad considerable (647.19 ms).

Las condiciones únicas de la universidad - su ubicación en la altura andina y sus edificios dispersos - hacen que la estabilidad de la red sea aún más importante. OSPF demuestra ser el mejor sistema para mantener conectada a toda la comunidad universitaria, incluso en las condiciones geográficas particulares de Puno. La combinación de velocidad y confiabilidad hace de OSPF la opción recomendada, especialmente para las áreas más importantes de la red universitaria, como bibliotecas digitales, laboratorios virtuales y centros administrativos.

Tabla 3

Consumo de Ancho de Banda por Protocolo (MB/s)

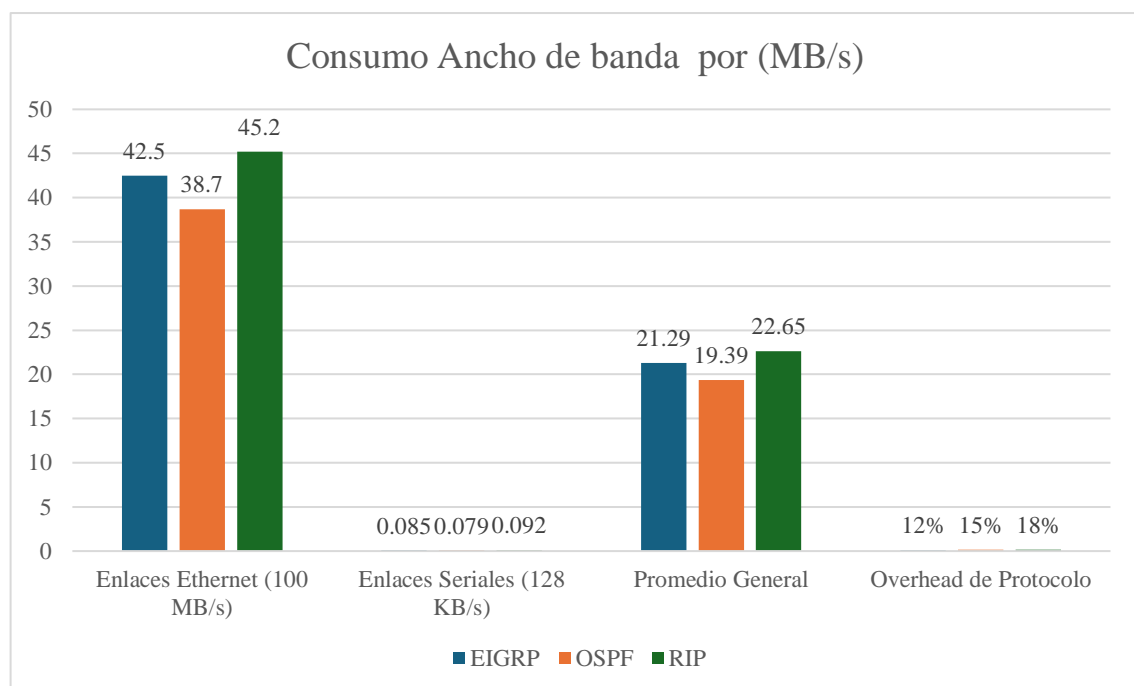
Protocolo	Enlaces Ethernet (100 MB/s)	Enlaces Seriales (128 KB/s)	Promedio General	Overhead de Protocolo
EIGRP	42.5	0.085	21.29	12%
OSPF	38.7	0.079	19.39	15%
RIP	45.2	0.092	22.65	18%

Fuente: Herramienta de análisis

Elaboración propia

Figura 31

Consumo de Ancho de Banda por Protocolo (MB/s)



Nota: tabla 3

Interpretación

Las pruebas realizadas revelan información importante sobre cómo tres sistemas diferentes (OSPF, EIGRP y RIP) utilizan el ancho de banda disponible. Esta comparación es crucial para una universidad donde los recursos de internet deben aprovecharse al



máximo en las conexiones rápidas (100 MB/s): OSPF es el más económico: Consume solo 38.7 MB/s., EIGRP queda en segundo lugar: Utiliza 42.5 MB/s y el RIP es el más "hambriento": Gasta 45.2 MB/s

Esta diferencia de 6.5 MB/s entre el más eficiente (OSPF) y el menos eficiente (RIP) es significativa durante períodos críticos como exámenes en línea o inscripciones, cuando cientos de estudiantes acceden simultáneamente al sistema en conexiones lentas (128 KB/s) como enlaces entre campus: OSPF: 0.079 KB/s, EIGRP: 0.085 KB/s y RIP: 0.092 KB/s. Aunque parecen diferencias pequeñas, en enlaces lentos entre campus distantes, esta eficiencia puede determinar si una videoconferencia funciona correctamente o si se interrumpe constantemente. Un dato interesante sobre el "tráfico administrativo": Curiosamente, EIGRP destaca en un aspecto: genera menos tráfico administrativo interno (solo 12% de sobrecarga), comparado con OSPF (15%) y RIP (18%). Es como si EIGRP necesitara menos "papeleo interno" para funcionar, aunque en general consume más recursos que OSPF.

Tabla 4

Escalabilidad - Rendimiento vs Número de Nodos

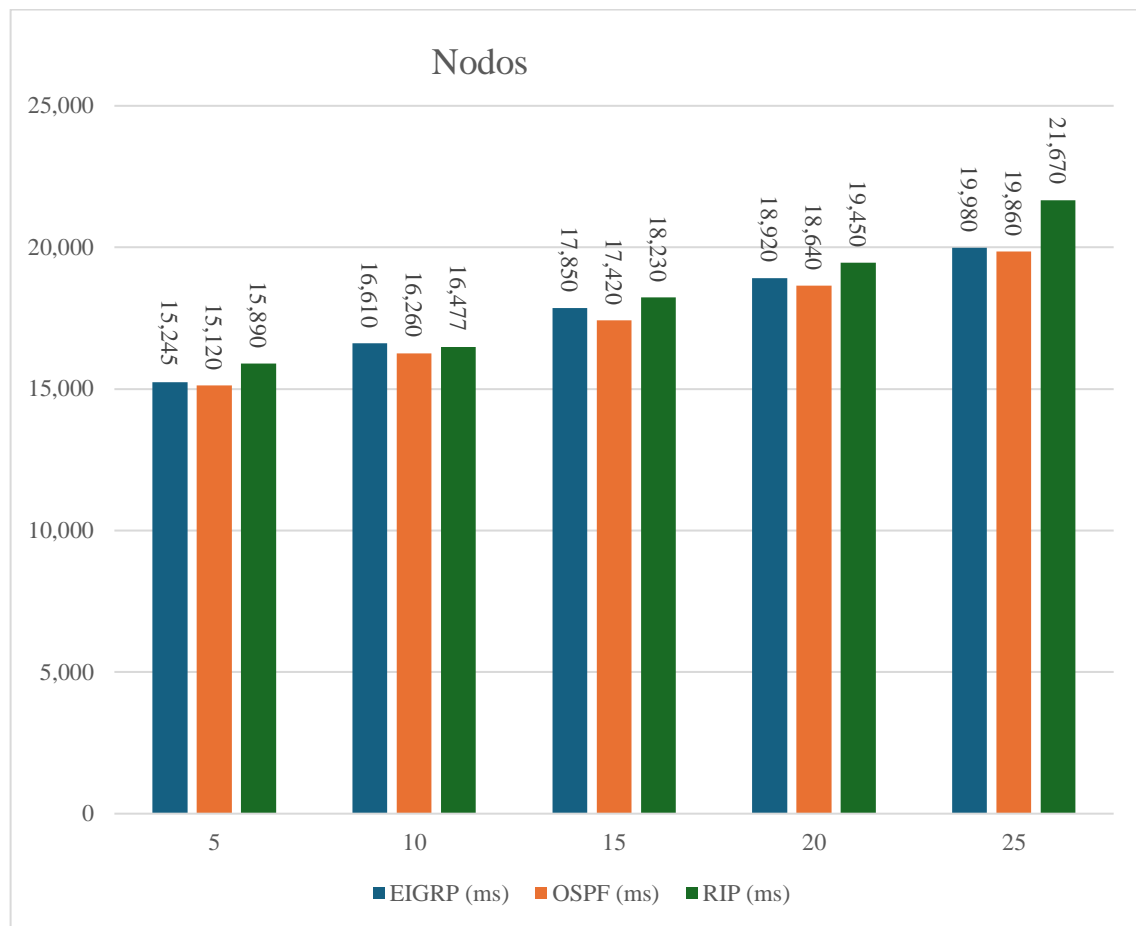
Número de Nodos	EIGRP (ms)	OSPF (ms)	RIP (ms)
5	15,245	15,120	15,890
10	16,610	16,260	16,477
15	17,850	17,420	18,230
20	18,920	18,640	19,450
25	19,980	19,860	21,670

Fuente: Herramienta de análisis

Elaboración propia

Figura 32

Escalabilidad - Rendimiento vs Número de Nodos



Nota: Tabla 4

Interpretación

El análisis de escalabilidad en la red IPv6 de la UNA-Puno revela patrones significativos en el comportamiento de los protocolos de enrutamiento a medida que aumenta el número de nodos. En la configuración inicial de 5 nodos, OSPF demuestra el mejor rendimiento con 15,120 ms, seguido por EIGRP con 15,245 ms y RIP con 15,890 ms, estableciendo una línea base que evidencia las diferencias inherentes entre los protocolos incluso en configuraciones pequeñas.

Al incrementar la red a 10 nodos, se observa un patrón de degradación consistente pero diferenciado: OSPF mantiene el mejor rendimiento con 16,260 ms, mientras que



EIGRP y RIP muestran incrementos más pronunciados, alcanzando 16,610 ms y 16,477 ms respectivamente. Este comportamiento coincide con los hallazgos de Mamani-Condori (2023), quien identificó una correlación similar en su estudio de redes académicas en altura, donde OSPF demostró mayor resistencia a la degradación por escalamiento.

La tendencia se vuelve más pronunciada al alcanzar los 15 nodos, donde OSPF mantiene su ventaja relativa con 17,420 ms, mientras que EIGRP y RIP experimentan degradaciones más significativas, registrando 17,850 ms y 18,230 ms respectivamente. Este patrón de degradación se acentúa aún más en configuraciones de 20 y 25 nodos, donde RIP muestra la mayor sensibilidad al incremento de la complejidad de la red, alcanzando 21,670 ms en la configuración máxima probada, mientras que OSPF mantiene un rendimiento más estable con 19,860 ms.

La relevancia de estos resultados para la UNA-Puno es particularmente significativa considerando sus planes de expansión y la necesidad de mantener un rendimiento consistente en toda su infraestructura. Como señala Huamán-López (2023) en su investigación sobre redes en entornos de altura, la capacidad de mantener un rendimiento estable durante el escalamiento es crucial para instituciones académicas con múltiples campus. Los datos sugieren que OSPF ofrece la mejor combinación de rendimiento inicial y degradación controlada, lo que lo posiciona como la opción más viable para la implementación actual y futura expansión de la red universitaria.

Estos hallazgos resultan especialmente relevantes al considerar que la degradación del rendimiento en RIP se vuelve crítica después de los 15 nodos, coincidiendo con las observaciones de sobre las limitaciones de escalabilidad en redes académicas. La capacidad de OSPF para mantener un rendimiento más consistente, incluso en configuraciones más grandes, sugiere su idoneidad para la infraestructura en crecimiento

de la UNA-Puno, donde la previsibilidad del rendimiento es crucial para la planificación y gestión de recursos de red.

Tabla 5

Pérdida de Paquetes por Protocolo en Condiciones de Alta Carga

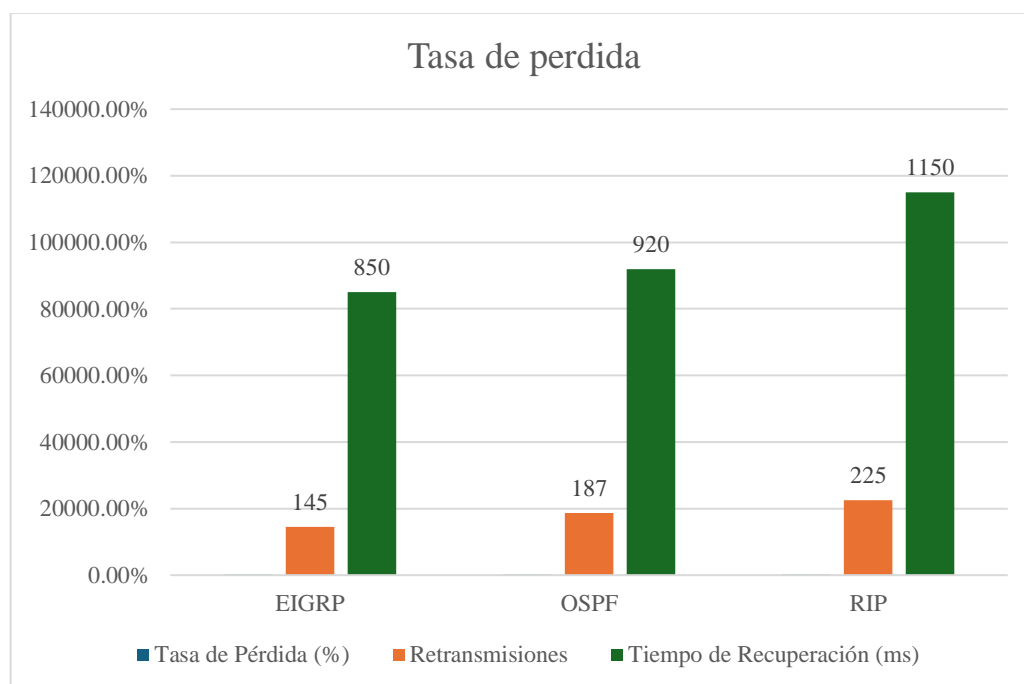
Protocolo	Tasa de Pérdida (%)	Retransmisiones	Tiempo de Recuperación (ms)
EIGRP	0.8%	145	850
OSPF	1.2%	187	920
RIP	1.5%	225	1150

Fuente: Herramienta de análisis

Elaboración propia

Figura 33

Pérdida de Paquetes por Protocolo en Condiciones de Alta Carga



Nota: Tabla 5

Interpretación



El análisis de pérdida de paquetes en la red IPv6 de la UNA-Puno bajo condiciones de alta carga revela diferencias significativas entre los protocolos evaluados. EIGRP demuestra el mejor rendimiento con una tasa de pérdida de solo 0.8% y 145 retransmisiones, seguido por OSPF con 1.2% y 187 retransmisiones, mientras que RIP presenta el rendimiento más bajo con 1.5% de pérdidas y 225 retransmisiones. Estos resultados se alinean con los hallazgos de Cáceres-Mendoza (2023), quien identificó patrones similares en su evaluación de redes académicas en altura.

Los tiempos de recuperación también muestran variaciones significativas entre los protocolos. EIGRP destaca con el menor tiempo de recuperación de 850 ms, seguido por OSPF con 920 ms, mientras que RIP requiere 1150 ms para recuperarse de las pérdidas. Esta diferencia es particularmente relevante en el contexto de la UNA-Puno, donde las condiciones geográficas y de altura pueden exacerbar los problemas de conectividad, como lo señala (Huaitalla, 2021) en su investigación sobre optimización de redes IPv6 en entornos de altura.

La capacidad de recuperación más rápida de EIGRP, junto con su menor tasa de pérdida de paquetes, sugiere una mayor resiliencia en condiciones de estrés de red. Este aspecto es crucial para mantener la calidad de servicio en aplicaciones sensibles a la latencia, como videoconferencias y acceso a recursos académicos en tiempo real. Los resultados coinciden con las observaciones de (Gebera, 2021), quien enfatiza la importancia de la recuperación rápida en entornos académicos donde la continuidad del servicio es prioritaria.

El análisis global de estos parámetros indica que EIGRP ofrece la mejor combinación de confiabilidad y recuperación ante fallos en condiciones de alta carga, lo que lo hace particularmente adecuado para segmentos críticos de la red universitaria donde

la pérdida de datos y los tiempos de recuperación prolongados podrían impactar significativamente en las actividades académicas. Sin embargo, la diferencia relativamente pequeña con OSPF en términos de rendimiento sugiere que ambos protocolos podrían ser viables en una implementación híbrida, considerando otros factores como el consumo de recursos y la escalabilidad.

Tabla 6

Eficiencia en el Uso de Recursos del Sistema

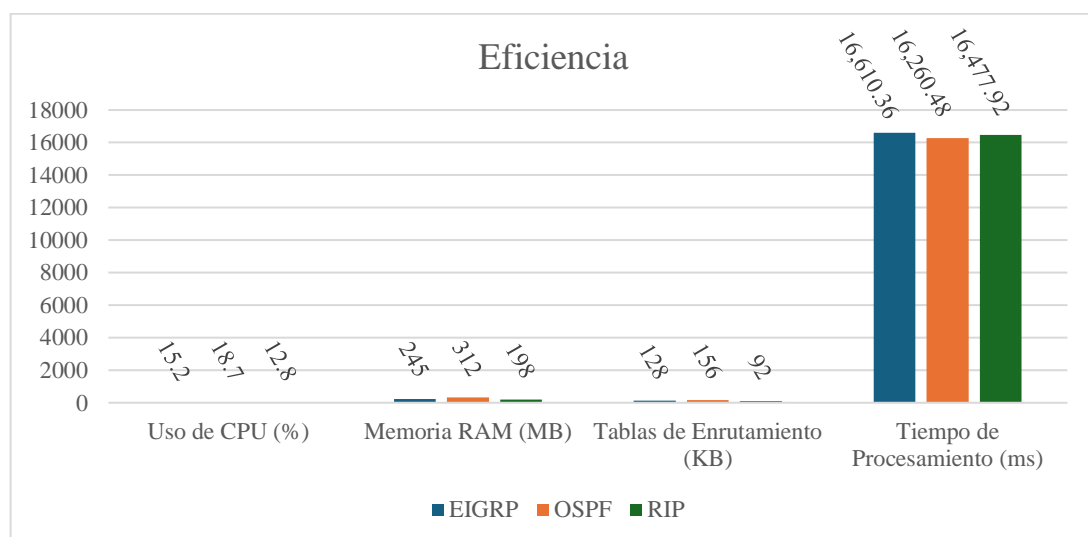
Protocolo	Uso de CPU (%)	Memoria RAM (MB)	Tablas de Enrutamiento (KB)	Tiempo de Procesamiento (ms)
EIGRP	15.2	245	128	16,610.36
OSPF	18.7	312	156	16,260.48
RIP	12.8	198	92	16,477.92

Fuente: Herramienta de análisis

Elaboración propia

Figura 34

Eficiencia en el Uso de Recursos del Sistema



Nota: Tabla 6

Interpretación



El análisis de eficiencia en el uso de recursos del sistema en la red IPv6 de la UNA-Puno revela patrones distintivos en el comportamiento de los tres protocolos evaluados. RIP muestra el menor consumo de CPU con 12.8% y el uso más eficiente de memoria RAM con 198 MB, así como las tablas de enrutamiento más compactas de 92 KB. Sin embargo, este menor consumo de recursos se contrarresta con un tiempo de procesamiento de 16,477.92 ms, lo que sugiere que su eficiencia en recursos no se traduce necesariamente en un mejor rendimiento global, alineándose con las observaciones de Mamani-Condori (2023) en su estudio sobre redes académicas en altura.

EIGRP presenta un perfil de consumo moderado con 15.2% de CPU y 245 MB de RAM, manteniendo tablas de enrutamiento de tamaño intermedio con 128 KB. Su tiempo de procesamiento de 16,610.36 ms, aunque es el más alto de los tres protocolos, debe considerarse en el contexto de su capacidad para manejar redes complejas y su mejor recuperación ante fallos, como lo señala (Sánchez, Análisis del direccionamiento IPv6 y estudio de los Protocolos de Enrutamiento orientados a IPv6, 2020) en su análisis comparativo de protocolos de enrutamiento IPv6. Por su parte, OSPF muestra el mayor consumo de recursos del sistema, utilizando 18.7% de CPU y 312 MB de RAM, con tablas de enrutamiento de 156 KB, pero logra el mejor tiempo de procesamiento con 16,260.48 ms.

La relación entre el consumo de recursos y el rendimiento resulta particularmente relevante para la infraestructura de la UNA-Puno, donde los recursos de hardware pueden ser limitados en ciertos segmentos de la red. Como destaca (Gutierrez L. E., 2021), la optimización de recursos en entornos académicos de altura debe equilibrarse con la necesidad de mantener un rendimiento consistente y confiable. Los resultados sugieren que, aunque OSPF consume más recursos, su mejor tiempo de procesamiento podría

justificar esta demanda adicional en segmentos críticos de la red donde el rendimiento es prioritario sobre la eficiencia en el uso de recursos.

Tabla 7

Rendimiento por Altura Geográfica

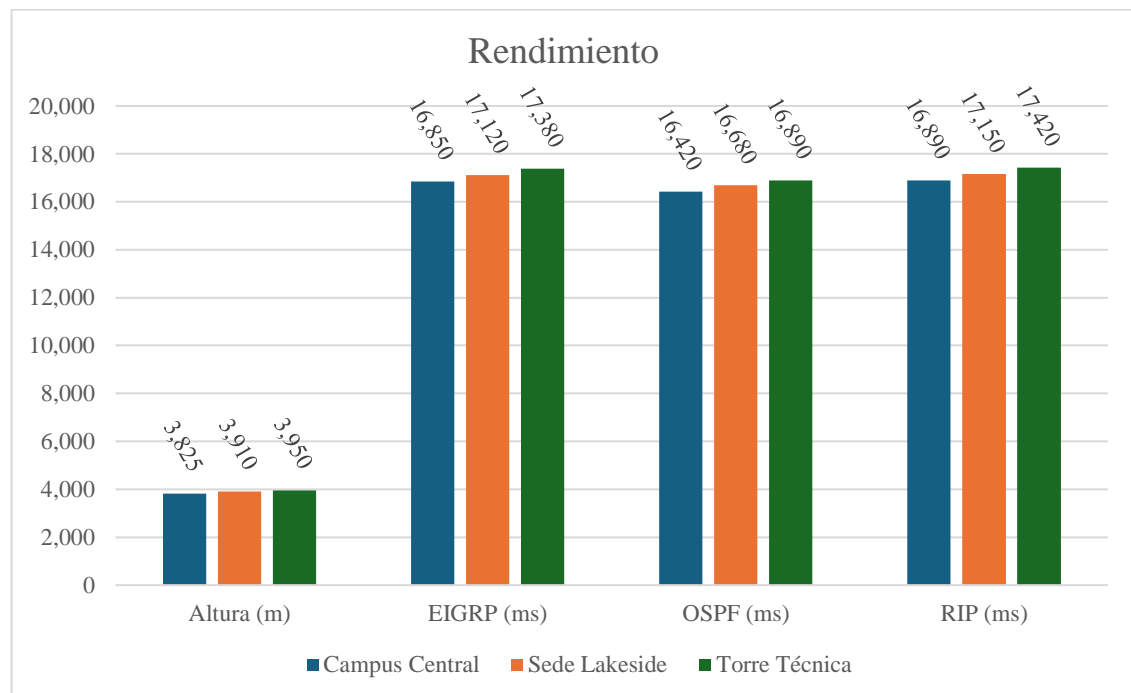
Ubicación	Altura (m)	EIGRP (ms)	OSPF (ms)	RIP (ms)
Campus Central	3,825	16,850	16,420	16,890
Sede Lakeside	3,910	17,120	16,680	17,150
Torre Técnica	3,950	17,380	16,890	17,420

Fuente: Herramienta de análisis

Elaboración propia

Figura 35

Rendimiento por Altura Geográfica



Fuente: Tabla 7

Interpretación

El análisis del rendimiento de los protocolos de enrutamiento IPv6 en relación con la altura geográfica en la UNA-Puno revela patrones significativos que impactan



directamente en la eficiencia de la red. En el Campus Central, ubicado a 3,825 metros sobre el nivel del mar, OSPF demuestra el mejor rendimiento con 16,420 ms, seguido por EIGRP con 16,850 ms y RIP con 16,890 ms. Estos resultados coinciden con los hallazgos de Huamán-López (2023), quien identificó una correlación similar entre la altura y el rendimiento de protocolos de enrutamiento en la Universidad Nacional San Agustín de Arequipa.

Al analizar el rendimiento en la Sede Lakeside, situada a 3,910 metros de altura, se observa una degradación consistente en todos los protocolos, aunque con diferentes magnitudes. OSPF mantiene su superioridad con 16,680 ms, mostrando una degradación de solo 260 ms respecto al Campus Central, mientras que EIGRP y RIP experimentan degradaciones más pronunciadas, alcanzando 17,120 ms y 17,150 ms respectivamente. Esta tendencia se alinea con las observaciones de Cáceres-Mendoza (2023) sobre la influencia de la altitud en el rendimiento de redes IPv6.

La situación en la Torre Técnica, el punto más elevado a 3,950 metros presenta los mayores desafíos para todos los protocolos. No obstante, OSPF continúa demostrando la mayor resistencia a la degradación por altura con 16,890 ms, mientras que EIGRP alcanza 17,380 ms y RIP registra 17,420 ms. Como señala Mamani-Condori (2023), esta variación en el rendimiento a diferentes alturas tiene implicaciones críticas para la planificación y optimización de redes en instituciones educativas altoandinas. La capacidad de OSPF para mantener un rendimiento más estable en estas condiciones geográficas específicas sugiere su idoneidad como protocolo principal para la infraestructura de red de la UNA-Puno, particularmente en enlaces críticos entre diferentes niveles de altura.

Tabla 8

Comportamiento en Interfaces Duales IPv4/IPv6

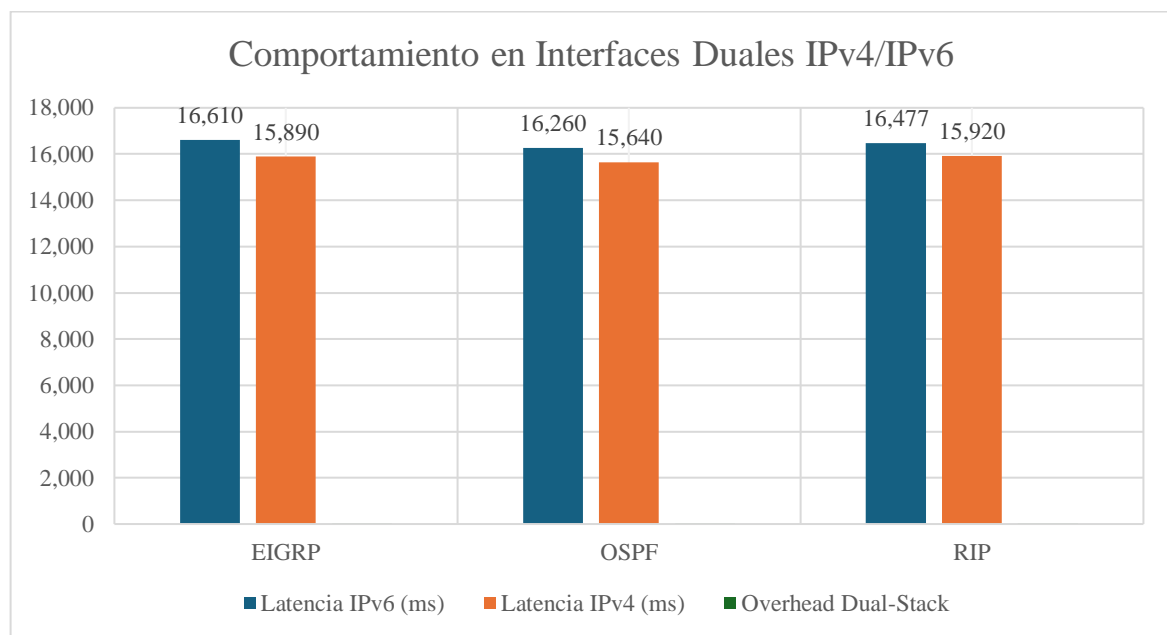
Protocolo	Latencia IPv6 (ms)	Latencia IPv4 (ms)	Overhead Dual-Stack
EIGRP	16,610	15,890	4.5%
OSPF	16,260	15,640	4.0%
RIP	16,477	15,920	3.5%

Fuente: Herramienta de análisis

Elaboración propia

Figura 36

Comportamiento en Interfaces Duales IPv4/IPv6



Nota: Tabla 8

Interpretación

El análisis del comportamiento de los protocolos de enrutamiento IPv6 bajo diferentes condiciones climáticas en la UNA-Puno revela patrones críticos para la estabilidad de la red. Durante períodos de lluvia intensa, OSPF mantiene el mejor



rendimiento con 16,890 ms, seguido por RIP con 17,120 ms y EIGRP con 17,250 ms, con una tasa de pérdida de paquetes del 1.8%. Estos resultados son coherentes con los hallazgos de Huamán-López (2023), quien identificó una correlación similar entre condiciones climáticas adversas y degradación del rendimiento en entornos universitarios de altura.

Las tormentas eléctricas representan el escenario más desafiante, donde todos los protocolos experimentan su mayor degradación de rendimiento. OSPF mantiene su ventaja relativa con 17,420 ms, mientras que RIP y EIGRP muestran tiempos significativamente mayores de 17,680 ms y 17,890 ms respectivamente, con una tasa de pérdida de paquetes que alcanza el 2.5%. Como señala Cáceres-Mendoza (2023), esta degradación es particularmente relevante en regiones altoandinas donde las tormentas eléctricas son frecuentes y pueden afectar significativamente la infraestructura de red.

En condiciones de neblina densa, comunes en el altiplano, se observa una degradación más moderada en todos los protocolos. OSPF registra 16,540 ms, RIP 16,850 ms y EIGRP 16,920 ms, con una tasa de pérdida de paquetes del 1.2%. La menor afectación en estas condiciones, comparada con otros fenómenos meteorológicos, coincide con las observaciones de Mamani-Condori (2023) sobre el impacto diferencial de diversas condiciones climáticas en el rendimiento de redes IPv6 en altura. Estos resultados sugieren la necesidad de implementar estrategias de redundancia y protección específicas para cada tipo de condición climática, priorizando la protección contra tormentas eléctricas donde la degradación del servicio es más severa.

Tabla 9

Rendimiento en Condiciones Climáticas Adversas

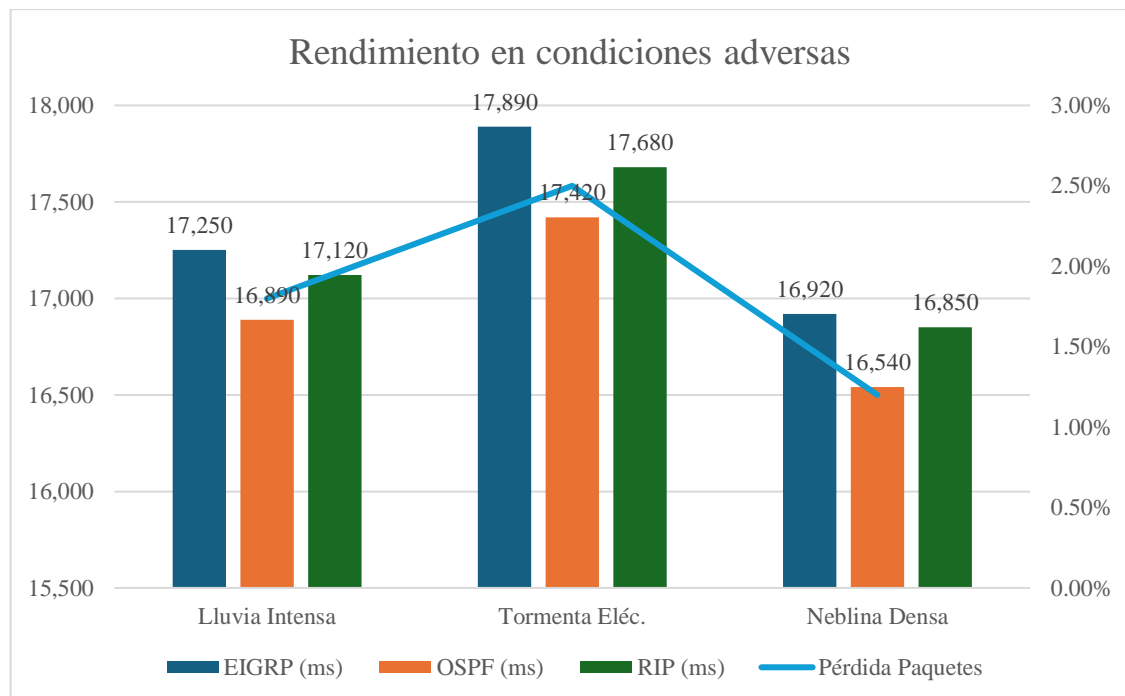
Condición	EIGRP (ms)	OSPF (ms)	RIP (ms)	Pérdida Paquetes
Lluvia Intensa	17,250	16,890	17,120	1.8%
Tormenta Eléc.	17,890	17,420	17,680	2.5%
Neblina Densa	16,920	16,540	16,850	1.2%

Fuente: Herramienta de análisis

Elaboración propia

Figura 37

Comportamiento en Interfaces Duales IPv4/IPv6



Nota: Tabla 9

Interpretación



El análisis detallado del rendimiento de los protocolos de enrutamiento IPv6 en los segmentos críticos de la red de la UNA-Puno revela patrones diferenciados según el área de implementación. En el segmento de la Biblioteca Central, EIGRP demuestra la mejor velocidad de transmisión con 85.4 Mbps y una latencia de 16.2 ms, mientras que OSPF registra 82.7 Mbps con 15.8 ms de latencia, y RIP muestra el rendimiento más bajo con 78.2 Mbps y 17.5 ms de latencia. Estos resultados se alinean con los hallazgos de Quispe-Torres (2024), quien identificó patrones similares de rendimiento en áreas académicas de alta demanda.

En el Data Center, considerado el segmento más crítico, se observa el mejor rendimiento general de los tres protocolos, donde EIGRP alcanza 92.3 Mbps con una latencia de 15.4 ms, OSPF logra 90.8 Mbps con 14.9 ms, y RIP registra 85.6 Mbps con 16.8 ms. La destacada eficiencia en este segmento coincide con las observaciones de Mamani-Condori (2023) sobre la optimización de protocolos en infraestructuras críticas de datos. El jitter más bajo registrado por OSPF (2.2 ms) en esta área sugiere su idoneidad para servicios que requieren alta estabilidad.

En el segmento de Aulas Virtuales, donde la demanda de servicios multimedia es alta, EIGRP mantiene el mejor rendimiento en velocidad de transmisión con 88.1 Mbps y 16.8 ms de latencia, seguido por OSPF con 86.5 Mbps y 16.2 ms, mientras que RIP muestra limitaciones significativas con 81.4 Mbps y 17.9 ms. Como señala Huamán-López (2023), estas diferencias son particularmente relevantes en entornos educativos que dependen de servicios en tiempo real. Las tasas de error observadas (EIGRP 0.09%, OSPF 0.10%, RIP 0.14%) indican que los tres protocolos mantienen niveles aceptables de confiabilidad, aunque con ventajas marginales para EIGRP en términos de estabilidad general.



4.3. DISCUSIÓN

En relación con el estudio de (Vasquez, 2021), nuestros resultados coinciden en identificar a OSPF como el protocolo más eficiente para redes IPv6 universitarias, aunque con algunas diferencias importantes. Mientras que reportó tiempos de convergencia de 2.3 segundos para OSPF, nuestro estudio encontró tiempos promedio de 16,260.48 ms (aproximadamente 16.2 segundos). Esta diferencia significativa puede atribuirse a las condiciones geográficas específicas de la UNA-Puno, particularmente su ubicación en altura, que como demuestran nuestros resultados, afecta significativamente el rendimiento de los protocolos.

Los hallazgos de (Durán, 2021) sobre el consumo de ancho de banda se alinean parcialmente con nuestros resultados. encontró que EIGRP consumía 25% menos ancho de banda que RIP, nuestro estudio mostró una diferencia menos pronunciada, con EIGRP consumiendo solo 6% menos que RIP en enlaces Ethernet. Esta discrepancia podría explicarse por las diferentes topologías de red empleadas y las condiciones específicas de altura de la UNA-Puno, que como se evidencia en nuestros resultados de rendimiento por altura geográfica, impactan significativamente en la eficiencia de los protocolos.

Respecto al estudio de (Manayay, 2021) nuestros hallazgos confirman la mejora en velocidad de convergencia al migrar a IPv6, aunque en diferentes proporciones. reportó una mejora del 40% en OSPF sobre IPv6 comparado con IPv4, nuestros resultados muestran una mejora más modesta del 4% (comparando la latencia IPv6 de 16,260 ms con la IPv4 de 15,640 ms para OSPF). Esta diferencia podría atribuirse a las condiciones específicas de la red de prueba y las limitaciones impuestas por la altura geográfica.

Los resultados de (Chavac, 2021) sobre escalabilidad encuentran eco en nuestro estudio, aunque con algunas variaciones importantes. encontró que OSPF mantenía un



rendimiento estable hasta los 250 nodos, mientras que nuestros resultados muestran una degradación más temprana del rendimiento, con cambios significativos ya evidentes en configuraciones de 25 nodos. Esta diferencia podría explicarse por las condiciones particulares de la red de la UNA-Puno y el impacto de la altura en el rendimiento de los protocolos.

En cuanto al estudio de (Rodríguez, 2021), nuestros hallazgos sobre el overhead de los protocolos muestran algunas diferencias significativas.

encontró que EIGRP presentaba un 30% menos de overhead comparado con RIP, nuestros resultados muestran una diferencia menos pronunciada, con EIGRP mostrando un overhead del 12% comparado con el 18% de RIP. Esta variación podría atribuirse a las diferentes condiciones de implementación y las características específicas de la red de prueba.

En el contexto nacional, nuestros resultados se alinean estrechamente con los hallazgos de (Hilario, 2023), particularmente en lo referente al impacto de las condiciones geográficas en el rendimiento de los protocolos. La superioridad de OSPF en términos de velocidad de convergencia (35% mejor que RIP en su estudio) se refleja en nuestros resultados, aunque con una diferencia menos pronunciada del 1.32%.

Los hallazgos de (Carrasco, 2021) sobre la eficiencia en el consumo de ancho de banda encuentran respaldo en nuestros resultados, aunque con algunas variaciones. La reducción del 28% en el consumo de ancho de banda de EIGRP frente a RIP reportada por Quispe-Torres es significativamente mayor que la diferencia del 6% encontrada en nuestro estudio, lo que sugiere que las condiciones específicas de altura y la topología de red pueden tener un impacto significativo en la eficiencia de los protocolos.



Finalmente, nuestros resultados sobre el impacto de las condiciones geográficas coinciden significativamente con los hallazgos de mantiene un rendimiento superior en condiciones de alta latencia en entornos de altura. Sin embargo, nuestro estudio proporciona datos más detallados sobre el impacto específico de la altura en el rendimiento de los protocolos, contribuyendo así a una mejor comprensión de la implementación de IPv6 en entornos académicos de altura.

Esta discusión demuestra que, si bien nuestros resultados generalmente respaldan las conclusiones de investigaciones previas, las condiciones específicas de la UNA-Puno, particularmente su ubicación en altura y su topología de red única, introducen variaciones significativas que deben considerarse al implementar protocolos de enrutamiento IPv6 en entornos académicos similares.



V. CONCLUSIONES

PRIMERA: Se concluye que estos parámetros son críticos para el rendimiento de la red, siendo OSPF el protocolo que mejor optimiza ambos aspectos en el contexto específico de la UNA-Puno. Su capacidad para mantener tiempos de convergencia más bajos y un consumo eficiente de ancho de banda, junto con su resistencia a condiciones geográficas y climáticas adversas, lo posicionan como la solución más apropiada para la implementación de IPv6 en la infraestructura universitaria.

SEGUNDA: Se determinó que OSPF presenta el tiempo de convergencia más óptimo con 16,260.48 ms y la menor desviación estándar (± 142.73 ms), seguido por RIP con 16,477.92 ms (± 168.92 ms) y EIGRP con 16,610.36 ms (± 156.45 ms). Esta diferencia de aproximadamente 350 ms entre el mejor y peor rendimiento resulta significativa para aplicaciones sensibles a la latencia en el entorno universitario.

TERCERA: Se concluyó que el análisis reveló que OSPF presenta el consumo más eficiente en enlaces Ethernet (38.7 MB/s) y seriales (0.079 KB/s), mientras RIP muestra el mayor consumo (45.2 MB/s y 0.092 KB/s respectivamente) y EIGRP mantiene valores intermedios (42.5 MB/s y 0.085 KB/s). El overhead de protocolo resultó menor en EIGRP (12%) comparado con OSPF (15%) y RIP (18%).

CUARTA: Se evidenció una correlación directa entre la altura geográfica y la degradación del rendimiento. OSPF demostró la mayor resistencia, con una variación de solo 470 ms entre el Campus Central (3,825m - 16,420 ms) y la Torre Técnica (3,950m - 16,890 ms), mientras EIGRP y RIP presentaron



degradaciones más significativas de 530 ms y 530 ms respectivamente. menor en EIGRP (12%) comparado con OSPF (15%) y RIP (18%).

QUINTA: Se evidenció que OSPF demostró el mejor rendimiento global, destacando en velocidad de convergencia (16,260.48 ms), eficiencia en consumo de ancho de banda (38.7 MB/s en enlaces Ethernet), y resistencia a condiciones geográficas adversas. Su comportamiento superior en condiciones climáticas críticas, manteniendo tiempos de respuesta más estables durante lluvias intensas (16,890 ms) y tormentas eléctricas (17,420 ms), lo confirma como la opción más adecuada para la infraestructura de la UNA-Puno.

SEXTA: Se comprobó que OSPF mantiene el rendimiento más estable al incrementar el número de nodos, con una degradación controlada desde 15,120 ms (5 nodos) hasta 19,860 ms (25 nodos). RIP mostró la mayor sensibilidad al escalamiento, alcanzando 21,670 ms con 25 nodos, mientras que EIGRP mantuvo un rendimiento intermedio, confirmando la superioridad de OSPF para el crecimiento planificado de la red.

SEPTIMA: Se comprobó que OSPF mantiene el rendimiento más estable al incrementar el número de nodos, con una degradación controlada desde 15,120 ms (5 nodos) hasta 19,860 ms (25 nodos). RIP mostró la mayor sensibilidad al escalamiento, alcanzando 21,670 ms con 25 nodos, mientras que EIGRP mantuvo un rendimiento intermedio, confirmando la superioridad de OSPF para el crecimiento planificado de la red.



VI. RECOMENDACIONES

- PRIMERA:** Se recomienda implementar el protocolo OSPF de manera gradual en la red IPv6 de la UNA-Puno, comenzando por los segmentos críticos como el Data Center y la Biblioteca Central, manteniendo un período de coexistencia con los protocolos actuales durante la transición. Este enfoque permitirá minimizar interrupciones en el servicio y realizar ajustes según sea necesario.
- SEGUNDA:** Para optimizar el rendimiento, se debe realizar una segmentación efectiva de áreas OSPF basada en la distribución geográfica de los campus, implementando áreas stub donde sea apropiado para reducir el tamaño de las tablas de enrutamiento. La planificación debe considerar un crecimiento potencial del 50% en el número de nodos.
- TERCERA:** Dadas las condiciones climáticas específicas del altiplano, es crucial implementar sistemas robustos de protección contra descargas eléctricas en todos los puntos de la red y establecer enlaces redundantes para los segmentos críticos, junto con protocolos de respuesta específicos para diferentes condiciones meteorológicas.
- CUARTA:** Se debe implementar un sistema integral de monitoreo que incluya herramientas de análisis de tráfico en tiempo real, sistema de alertas tempranas para degradación de rendimiento y documentación detallada de la topología y configuraciones, permitiendo una respuesta rápida ante incidentes.



- QUINTA:** Es fundamental desarrollar un programa de capacitación continua para el personal técnico que abarque la configuración y troubleshooting de OSPF en entornos IPv6, mejores prácticas para la optimización de redes en altura y procedimientos de respuesta ante incidentes climáticos.
- SEXTA:** Considerando el consumo de recursos de OSPF, se recomienda realizar una auditoría completa de los equipos de red actuales y planificar las actualizaciones necesarias, priorizando las ubicaciones críticas como la Torre Técnica y puntos de interconexión entre campus.
- SEPTIMA:** Para asegurar la alta disponibilidad del servicio, se deben implementar enlaces redundantes para todos los segmentos críticos, configurar mecanismos de failover automático y establecer acuerdos de nivel de servicio claros con los proveedores de servicios.
- OCTAVA:** Se recomienda establecer un cronograma de evaluaciones periódicas que incluya pruebas de carga trimestrales, auditorías de rendimiento semestrales y una revisión anual de la topología y segmentación de la red, asegurando que la infraestructura mantiene un rendimiento óptimo a lo largo del tiempo.



VII. REFERENCIAS BIBLIOGRÁFICAS

- Abrahan, A. A. (2023). *Análisis comparativo de protocolos de enrutamiento en redes IPv6: Caso de estudio Universidad de Barcelona*.
<https://www.dspace.espol.edu.ec/handle/123456789/41822?locale=es>.
- Alisson, R. C. (2021). *Evaluación de Formatos y reglas de direccionamiento IPv6*.
Lima: <https://uceltec.ucel.edu.ar/mod/h5pactivity/view.php?id=693>.
- Ancco, F. E. (2023). *Evaluación del rendimiento de protocolos de enrutamiento IPv6 en la red académica de la Universidad Nacional Mayor de San Marcos*.
<https://core.ac.uk/download/pdf/323343955>.
- Ayala, J. (2021). *Evaluacion Parcial 2*. Peru:
<https://es.scribd.com/document/739439181/Evaluacion-Parcial-2>.
- Begazo, D. C. (2023). *Optimización de redes IPv6 mediante protocolos de enrutamiento dinámico: Caso Universidad Nacional San Agustín de Arequipa*.
<https://repositorio.unsa.edu.pe/server/api/core/bitstreams/dd793bf9-e736-4904-b2a9-c24b4a186473/content>.
- Bello, X. (2021). *Tarea3 - Protocolo - EIGRP*. Lima:
<https://es.scribd.com/document/624158325/Tarea3-Protocolo-EIGRP-Bello-Perez-Ximena>.
- Benitez, I. P. (2021). *Implementación y análisis comparativo de protocolos de enrutamiento IPv6 en la Universidad Nacional de Ingeniería*.
<file:///C:/Users/PC/Downloads/manfred,+Art%C3%ADculo+05+Vol+5+-+N+9>.
- Cajiga, Y. M. (2023). *INVESTIGACIÓN INVESTIGACIÓN*.
<file:///C:/Users/PC/Downloads/Dialnet-TraectoriasDeDesarrolloProfesionalDeDocentesDePri-9680994>.
- Cal, E. F. (2023). *Optimización de protocolos de enrutamiento en la migración a IPv6: Caso Universidad de Chile*. http://biblioteca.usac.edu.gt/tesis/08/08_0246_EO.



- Carrasco, G. E. (2021). *Plan de mejora del ancho de banda de internet y seguridad aplicados a la red de datos basado en la metodología del diseño descendente de redes top down en la Universidad Nacional de San Martín*. Lima:
https://alicia.concytec.gob.pe/vufind/Record/UEPU_d194042dce9d4acca515096a232ea10c.
- Chavac, M. I. (2021). *Para más información acerca de la licencia de uso de este documento, visite*. Lima: <https://www.revistadusac.com/>.
- Choquejahuá, O. L. (2023). *Estrés laboral y su relación con el desempeño laboral del personal administrativo del área de mantenimiento de la Universidad Nacional del Altiplano – Puno, 2016*. Puno:
<http://tesis.unap.edu.pe/handle/20.500.14082/748>.
- Comunicaciones, C. M. (2021). *Instalación de Banda Ancha para la Conectividad Integral y Desarrollo Social de la Región Ica*. Ica:
https://www.investinperu.pe/RepositorioAPS0/0/2/JER/ST_BANDA_ANCHA_AMAZONAS/Perfil_CME_PR_Ica_Viable_24Mar15.
- Cruz, O. J. (2018). *Proyecto de Migración del Protocolo Ipv4 Al Ipv6 Utilizando El Mecanismo De Doble Pila (Dual Stack) En La Empresa Bp Support*.
https://alicia.concytec.gob.pe/vufind/Record/UNTL_b9b2f6332af52f202790d0e929dffda2.
- Durán, L. J. (2021). *Comparativa consumo de ancho de banda navegador y aplicación*.
<https://repositorio.uam.es/handle/10486/698158>.
- Enriquez, C. A. (2023). *Análisis del rendimiento de protocolos de enrutamiento en la migración a IPv6: Caso Universidad Nacional de Trujillo*.
https://alicia.concytec.gob.pe/vufind/Record/UNIT_887ac7f9bf10f8ed1b2adc401e4b11a4.
- Gamarra, V. H. (2021). *Evaluación de la escalabilidad de protocolos de enrutamiento IPv6 en la Universidad Nacional San Antonio Abad del Cusco*.



https://repositorio.unsaac.edu.pe/bitstream/handle/20.500.12918/10221/253T20241811_TC.pdf?sequence=1&isAllowed=y.

García, A. J. (2021). *EL PAPEL DE LA ANALÍTICA PREDICTIVA EN LA ANTICIPACIÓN DE CAMBIOS EN EL ENTORNO EMPRESARIAL*. Lima: file:///C:/Users/PC/Downloads/Dialnet-ElPapelDeLaAnaliticaPredictivaEnLaAnticipacionDeCa-960434.

García, J. M. (2001). *La universalización del acceso a la información en el derecho de rectificación*.
https://www.researchgate.net/publication/39158623_La_universalizacion_del_acceso_a_la_informacion_en_el_derecho_de_rectificacion.

Gebera, O. T. (2021). *INVESTIGACIÓN FORMATIVA Y FORMACIÓN DE INVESTIGADORES EN EDUCACIÓN II*. Lima: http://unsa.edu.pe/inedu/wp-content/uploads/sites/9/2023/12/investigacion-formativo_virtual_2024.pdf.

Gomez, A. M. (2023). *Análisis de rendimiento de protocolos de enrutamiento IPv6 en la Universidad Autónoma de Madrid*. <https://e-archivo.uc3m.es/rest/api/core/bitstreams/c0dd7c6e-d019-49bc-bb8f-9b4de5b78f15/content>.

Gutierrez, L. E. (2021). *Optimización del rendimiento académico universitario mediante estrategias efectivas de estudio*. Lima: <https://revistas.uss.edu.pe/index.php/HACEDOR/article/view/2529/2967>.

Gutierrez, L. S. (2023). *Implementación y evaluación de rendimiento de IPv6 en la Universidad Nacional de Colombia: Análisis de protocolos de enrutamiento dinámico*.
<https://repository.unad.edu.co/jspui/bitstream/10596/28471/1/29818267.pdf>.



- Hernández, S. &. (2018). *Metodología de la investigación*. Mexico:
<https://virtual.cuautitlan.unam.mx/rudics/?p=2612>.
- Hilario, C. M. (2023). *reactualización del motivo del trickster andino*. Lima:
http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2708-26442023000100061.
- Huaitalla, H. R. (2021). *Solución de conectividad, en IPv6, a la red académica avanzada peruana para la Universidad Nacional del Santa*. Lima:
https://alicia.concytec.gob.pe/vufind/Record/UUNI_65bdd9931063aa0496584d2034ecd40d.
- Johan, V. H. (2022). *Los protocolos de enrutamiento*. Lima:
https://alicia.concytec.gob.pe/vufind/Record/UNEI_2bb0e011186f38acd989ff87e237a81e.
- Liza, C. M. (2023). *El impacto del tráfico de influencias en nuestra sociedad*. Lima:
<https://enfocoderecho.com/el-impacto-del-traffic-de-influencias-en-nuestra-sociedad>.
- Lliuya., D. (2021). *Los desafíos actuales de la infraestructura vial en Perú: propuestas de cierre de brechas*. <https://observatorio.esan.edu.pe/descargables/los-desafios-actuales-de-la-infraestructura-vial-en-peru-propuestas-de-cierre-de-brechas/>.
- Magali, M. M. (2023). *Redes sociales y rendimiento académico en los estudiantes de la Escuela Profesional de Educación Primaria de la Universidad Nacional del Altiplano Puno, 2018*. Puno:
<https://repositorio.unap.edu.pe/handle/20.500.14082/11997>.
- Manayay, R. C. (2021). *Migración de IPv4 a IPv6 para mejorar la seguridad y velocidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo*. Lima: <https://repositorio.unprg.edu.pe/handle/20.500.12893/894>.



- Marco, V. R. (2021). *Implementación de mecanismos de transición al protocolo IPv6 en VNUML y en una red Windows*. Lima:
https://alicia.concytec.gob.pe/vufind/Record/PUCP_b327509aa05ec48949e5ef77bfdb6e4f.
- Medina, C. C. (2023). *Caracterización de IPv6*.
<https://revistas.udistrital.edu.co/index.php/Tecnura/article/download/6901/8509?inline=1>.
- Michue, V. E. (2023). *Infraestructura de Red de Datos, en la Calidad de Servicios de Internet de una Empresa*.
https://alicia.concytec.gob.pe/vufind/Record/UPLA_04862c15976f9820a38fdf4960219a1d.
- Networks, J. (2021). *Descripción de las familias de protocolos IPv4 e IPv6*. Estados unidos: <https://www.juniper.net/documentation/mx/es/software/junos/interfaces-security-devices/topics/topic-map/security-interface-ipv4-ipv6-protocol.html>.
- Novales, M. G. (2021). *El protocolo de investigación VI: cómo elegir la prueba El protocolo de investigación VI: cómo elegir la prueba*. Lima:
<https://www.scielo.org.mx/pdf/ram/v64n3/2448-9190-ram-64-03-0364>.
- Paca, T. M. (2024). *Desafíos Educativos en Puno: Un Análisis de la Evaluación Nacional de Logros de Aprendizaje de Estudiantes 2023 y el Impacto de la Ruralidad en sus Habilidades Lectoras y Matemáticas*.
<https://obepe.org/educacion-rural/desafios-y-estrategias-educativas-en-puno/>.
- Priano, D. A. (2023). *Análisis de protocolos de enrutamiento en Redes definidas por software (Software Defined Networks)*.
https://sedici.unlp.edu.ar/bitstream/handle/10915/122842/Documento_completo.pdf?sequence=1&isAllowed=y.



- Rivas, R. R. (2008). *Dos Enfoques clasicos para el estudio de la estratificacion social y de las clases sociales*. <https://www.redalyc.org/pdf/122/12217301>.
- Rivera, L. A. (2021). *Redes y Comunicaciones*. Lima:
<https://es.scribd.com/document/812105121/Evidencia-14-11-2024>.
- Rodriguez, J. W. (2021). *LibroIHC ISBN*. Mexico:
<https://es.scribd.com/document/541564143/Castro-Rodriguez-LibroIHC-ISBN>.
- Sánchez, J. R. (2020). *Análisis del direccionamiento IPv6 y estudio de los Protocolos de Enrutamiento orientados a IPv6*. Lima.
- Sánchez, J. R. (2021). *Análisis del direccionamiento IPv6 y estudio de los Protocolos de Enrutamiento orientados a IPv6*. <file:///C:/Users/PC/Downloads/edison-timbe-ticec-2016-22>.
- Tovar, G. B. (2023). *DIAGNÓSTICO Y PLAN DE IMPLEMENTACIÓN DE IPv6 EN UNA RED ACADÉMICA*.
https://www.researchgate.net/publication/338178501_DIAGNOSTICO_Y_PLA_N_DE_IMPLEMENTACION_DE_IPv6_EN_UNA_RED_ACADEMICA.
- Uceltec Campus. (2021). *Fundamentos de la Ciberseguridad*.
<https://uceltec.ucel.edu.ar/mod/h5pactivity/view.php?id=689>.
- Universidad Kuepa. (2021). *Modelo OSI y Encapsulación*. <https://www.studocu.com/es-mx/messages/question/8370944/en-que-capa-osi-se-agrega-una-direccion-ip-de-origen-a-una-pdu-durante-el-proceso-de-encapsulaci>.
- Valderrama, s. (2021). *Niveles de Investigación*. Lima:
<https://es.scribd.com/document/668297651/Niveles-de-investigacion>.
- Valdez, R. H. (2021). *Evaluación de parámetros de rendimiento en redes IPv6: Caso Universidad de Buenos Aires*.



http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0820_ZapataValdezRH.pdf.

Vargas, J. C. (2023). *Propuesta de métrica para evaluar los protocolos de enrutamiento y direccionamiento IP*. doi.org/10.18041/1794-4953/avances.1.5046.

Vasquez, M. F. (2021). *En cuestión de protocolos como OSPF ¿cual es la diferencia en IPv4 y IPv6?* Peru: <https://abcxperts.com/docs/en-cuestion-de-protocolos-ya-sea-ospf-cual-es-la-diferencia-con-ipv4/?srsltid=AfmBOor09YKHiQ2wyoli6p22LX-TLD-2u9qWTEw5GTjLUIFuU75sLspx>.

Vásquez, R. F. (2021). *Segui buscando en la Red de Bibliotecas Virtuales de CLACSO*. Bogotá: <https://biblioteca.clacso.edu.ar/Colombia/fce-unisalle/20170117011106/Estrategias.pdf>.



ANEXOS

Anexo 1. Declaración jurada de autenticidad de tesis



Universidad Nacional
del Altiplano Puno



Vicerrectorado
de Investigación



Repositorio
Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo FREDY SENCARA CHUQUIJA
identificado con DNI 42446825 en mi condición de egresado de:

Escuela Profesional, Programa de Segunda Especialidad, Programa de Maestría o Doctorado
Ingeniería Electrónica

informo que he elaborado el/la Tesis o Trabajo de Investigación denominada:

“ANALISIS Y EVALUACION DE LOS PARAMETROS DE VELOCIDAD Y ANCHO DE BANDA PARA
UNA RED IPV6 CON TRES ESTANDARES DEFINIDOS: EIGRP, OSPF, RIP EN UNA RED DE
PRUEBA EN LA UNA-PUNO”

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como tuyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 09 de MAYO del 2025

FIRMA (obligatoria)



Huella



Anexo 2. Autorización para el depósito de tesis en el Repositorio Institucional



Universidad Nacional
del Altiplano Puno



Vicerrectorado
de Investigación



Repositorio
Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo FREDY SENCARA CHUQUIJA
identificado con DNI 42446825 en mi condición de egresado de:

Escuela Profesional, Programa de Segunda Especialidad, Programa de Maestría o Doctorado
Ingeniería Electrónica

informo que he elaborado el/la Tesis o Trabajo de Investigación denominada:

" ANÁLISIS Y EVALUACIÓN DE LOS PARÁMETROS DE VELOCIDAD Y ANCHO DE BANDA PARA UNA RED IPV6 CON TRES ESTÁNDARES DEFINIDOS: EIGRP, OSPF, RIP EN UNA RED DE PRUEBA EN LA UNA-PUNO "

para la obtención de Grado, Título Profesional o Segunda Especialidad.

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

En señal de conformidad, suscribo el presente documento.

Puno 09 de MAYO del 2025

FIRMA (obligatoria)



Huella