



Universidad Nacional Autónoma de México
Facultad de Ingeniería

**“Implementación de solución de alta
disponibilidad de una red dorsal IP/MPLS”
TESIS**

Que para obtener el grado de:

Ingeniero en Telecomunicaciones

Presentan:

Aguilar Téllez Gustavo Alberto

Alfaro Flores Roberto Carlos

Asesor de tesis:

Ing. Cruz Sergio Aguilar Díaz



Ciudad Universitaria, abril 2014

ÍNDICE

ÍNDICE-----	i
INTRODUCCIÓN GENERAL-----	v
CAPÍTULO I: ANTECEDENTES -----	2
<i>Introducción</i> -----	4
<i>Objetivo General</i> -----	6
<i>Objetivos Particulares</i> -----	6
<i>Alcance</i> -----	6
CAPÍTULO II FUNDAMENTOS TEÓRICOS-----	8
2.1. Breve historia de las redes de datos -----	10
2.2. Estandarización de las telecomunicaciones-----	12
2.3. Modelos de referencia -----	14
2.3.1 Modelo OSI -----	14
2.3.2 Modelo TCP/IP-----	15
2.4. Dispositivos de red -----	16
2.5. Topologías de red -----	18
2.6. Direccionamiento IPv4-----	21
2.7. Métodos de ruteo -----	26
2.8. Protocolos de ruteo-----	27
CAPÍTULO III: ALTA DISPONIBILIDAD EN REDES IP/MPLS. -----	39
<i>Introducción</i> -----	41
3.1 Alta disponibilidad-----	42
3.2 Fundamentos de MPLS -----	43
3.3 Estrategias para lograr la alta disponibilidad en redes IP/MPLS -----	47
3.4 Descripción de técnicas para mitigar afectación en caso de fallas. -----	51
CAPÍTULO IV: ANÁLISIS Y DISEÑO DE LA RED. -----	56
<i>Introducción</i> -----	58
4.1 Diseño-----	58
4.1.1 Topología física -----	58
4.1.2 Topología Lógica -----	62
4.1.3 Planeación IP-----	74
4.2 Análisis de flujos -----	76
4.2.1 Funcionamiento en condiciones normales-----	76
4.2.2 Funcionamiento en caso de falla. Pérdida de poder en switch de acceso -----	80

4.2.3	Funcionamiento en caso de falla, pérdida de poder en ambos switch de acceso -----	81
4.2.4	Funcionamiento en caso de falla, pérdida de poder en router de acceso-----	82
4.2.5	Funcionamiento en caso de falla, pérdida de poder en ambos routers de acceso-----	84
4.2.6	Funcionamiento en caso de falla, pérdida de enlace entre equipos de backbone y acceso -----	85
4.2.7	Funcionamiento en caso de falla, pérdida de poder en router de backbone-----	87
4.2.8	Funcionamiento en caso de falla, pérdida de poder en ambos routers de backbone-----	89
4.2.9	Funcionamiento en caso de falla, pérdida de poder en Route Reflector -----	90
4.2.10	Funcionamiento en caso de falla, pérdida de poder en firewall de Internet-----	91
4.2.11	Funcionamiento en caso de falla, pérdida de poder en ambos firewall de Internet -----	93
4.2.12	Funcionamiento en caso de falla, pérdida de poder en router de Internet -----	95
4.2.13	Funcionamiento en caso de falla, pérdida de poder en ambos router de Internet-----	96
CAPÍTULO V: SIMULACIÓN Y RESULTADOS.-----		99
<i>Implementación</i> -----		101
5.1	Simulador GNS3-----	101
5.2	Simulación-----	102
5.3	Pruebas de simulación y resultados-----	106
5.3.1	Funcionamiento en condiciones normales-----	106
5.3.2	Pérdida de poder en switch de acceso -----	108
5.3.3	Pérdida de poder en ambos switch de acceso-----	111
5.3.4	Pérdida de poder en router de acceso -----	114
5.3.5	Pérdida de poder en ambos routers de acceso -----	116
5.3.6	Pérdida de enlace entre routers de backbone y acceso-----	118
5.3.7	Pérdida de poder en router de backbone -----	120
5.3.8	Pérdida de poder en ambos routers de backbone-----	122
5.3.9	Pérdida de poder en route reflector-----	123
5.3.10	Pérdida de poder en firewall de Internet -----	124
5.3.11	Pérdida de poder en ambos firewall de Internet-----	126
5.3.12	Pérdida de poder en router de Internet-----	128
5.3.13	Pérdida de poder en ambos router de Internet -----	130
RESUMEN DE RESULTADOS-----		132
CONCLUSIONES-----		133
ÍNDICE DE TABLAS-----		135
ÍNDICE DE FIGURAS-----		137
GLOSARIO -----		139
REFERENCIAS-----		147
ANEXO A: DIRECCIONAMIENTO IP-----		151

ANEXO B: CONFIGURACIONES -----	157
<i>a. Ciudad 1</i> -----	159
a.1. Configuración C1ACCESO1 -----	159
a.2. Configuración C1ACCESO2 -----	166
a.3. Configuración C1ACCESOSW1 -----	173
a.4. Configuración C1ACCESOSW2 -----	176
a.5. Configuración C1BACKBONE1 -----	180
a.6. Configuración C1BACKBONE2 -----	187
a.7. Configuración C1INTERNETFW1 -----	194
a.8. Configuración C1INTERNETFW2 -----	198
a.9. Configuración C1INTERNET1 -----	202
a.10. Configuración C1INTENRET2 -----	204
a.11. Configuración C1RR1 -----	206
a.12. Configuración C1RR2 -----	209
<i>b. Ciudad 2</i> -----	213
b.1. Configuración C2ACCESO1 -----	213
b.2. Configuración C2ACCESO2 -----	220
b.3. Configuración C2ACCESOSW1 -----	226
b.4. Configuración C2ACCESOSW2 -----	227
b.5. Configuración C2BACKBONE1 -----	227
b.6. Configuración C2BACKBONE2 -----	234
b.7. Configuración C2INTERNETFW1 -----	241
b.8. Configuración C2INTERNETFW2 -----	245
b.9. Configuración C2INTERNET1 -----	248
b.10. Configuración C2INTERNET2 -----	250
b.11. Configuración C2RR1 -----	252
b.12. Configuración C2RR2 -----	255
b.13. Configuración SERVICE PROVIDER -----	258
b.14. Configuración Servidor R27 (Emulación de un Host) -----	260

INTRODUCCIÓN GENERAL

Este trabajo tiene como objetivo proporcionar todas las herramientas teóricas necesarias para plantear el diseño de una red redundante, de nivel carrier¹, que pueda ofrecer alta disponibilidad en sus servicios. Para lograr lo mencionado anteriormente se ha organizado el presente trabajo en varios capítulos donde de manera general en los primeros se podrán obtener herramientas teóricas que pretenden dar el contexto necesario para entender los conceptos básicos y en base a ello poder emitir una solución, y la segunda parte del trabajo abarca capítulos donde se plantea una solución y el análisis de los resultados que arrojaron pruebas de laboratorio para la solución propuesta.

En el Capítulo 1, hablaremos de los objetivos y alcances que se tienen en este trabajo, que de manera general dan una visión de lo que se pretende con la realización de esta tesis y hasta donde está limitada.

En el Capítulo 2, hablaremos de los fundamentos teóricos que se requieren para poder entender la solución propuesta, dichos fundamentos abarcan desde un poco de historia hasta el detalle técnico de ciertos protocolos que se emplean en las redes de datos.

En el Capítulo 3, se explicara que es una red MPLS, en que escenarios es útil, así como los fundamentos teóricos que ayudan a comprender su funcionamiento y características principales, se abordara con mayor profundidad las ventajas de MPLS para el desarrollo de redes redundantes y de que protocolos se ayuda MPLS para dichos escenarios redundantes.

En el Capítulo 4, se propone una solución de red redundante, explicando el diseño de alto nivel y analizando el comportamiento de la red para los diversos flujos de información cuando la red se encuentra estable y en correcta operación, y el análisis cuando alguno de los elementos de la red presenta alguna falla.

En el Capítulo 5 se muestra la simulación del diseño propuesto y los resultados obtenidos que respaldan el objetivo del presente trabajo.

¹ En telecomunicaciones el término "carrier" se refiere a sistemas, hardware o software que son altamente confiables, y sus capacidades han sido comprobadas para cumplir con los estándares de alta disponibilidad y confiabilidad.

CAPÍTULO I: ANTECEDENTES

Introducción

En la actualidad los grandes proveedores de servicios de telecomunicaciones cuentan con su propia infraestructura para poder brindar los servicios que ofertan a sus clientes, una parte esencial y la más importante de su infraestructura es la red dorsal o también conocida comúnmente como "backbone", esta red está formada por los equipos más importantes de su red, y son importantes debido a que en estos equipos es donde se concentra la mayor cantidad de flujo de información, que es resultado de los servicios ofertados por el proveedor a sus clientes, como puede ser: Internet de banda ancha, servicios de voz, líneas rentadas, servicios de valor agregado, etc. En la actualidad las redes dorsales están basadas en IP, debido a que esta tecnología permite transportar y manipular diverso tipo de tráfico, sin necesidad de tener una infraestructura diferente para cada uno de los servicios que brinda, lo que conlleva a eliminar costos innecesarios y una operación más efectiva de la red.

En conjunto con las ventajas que brinda la tecnología IP en sí misma, ha surgido una nueva tecnología² que en conjunto con IP, han hecho que las redes de los prestadores de servicios mejoren en su desempeño, esta tecnología es MPLS, la cual surge como solución a los problemas que presentaban las redes basadas en capa dos o tres del modelo OSI, dichos problemas eran que en una red basada en capa dos se tenía alta velocidad de conmutación pero no se tenía la inteligencia para dirigir a los paquetes por la ruta más óptima; en redes basadas en capa tres se tenía la inteligencia para enviar a los paquetes por la mejor ruta pero no se contaba con alta velocidad de conmutación, así, MPLS surge como solución a lo anterior debido a que MPLS soluciona las deficiencias de las redes basadas en capa dos y capa tres.

Actualmente la mayoría de los prestadores de servicios cuentan con sus redes dorsales basadas en IP/MPLS, pero deben seguir trabajando en la optimización de su red con la finalidad de brindar a sus usuarios la mejor experiencia en lo referente a comunicaciones, un punto de mejora en las redes dorsales es la alta disponibilidad, es decir que la red cuente con una infraestructura que le permita tener falla en elementos de su red pero sin presentar afectación en los servicios brindados a sus clientes, la solución inmediata de muchos prestadores de servicios es incrementar su infraestructura a nivel de número de elementos de red, lo cual implica que si falla uno, pueda tener otro disponible, el problema surge debido a la alta demanda de los usuarios por una excelente calidad en el servicio, ya que un prestador de servicios puede tener elementos de red que trabajen de respaldo, pero sin una correcta implementación lo que sucederá es que si falla un elemento de la red, tomará unos minutos

² El Primer RFC de MPLS que creó la IETF fue el RFC 3031 en febrero del 2001. (IETF, RFC 3031).

en lo que el elemento de respaldo entra en acción, esto puede representar minutos de afectación a los usuarios, hoy en día debido a la alta competencia entre los prestadores de servicios, no se pueden dar el lujo de afectar el servicio de sus usuarios ni siquiera por un minuto, porque eso puede implicar la decisión de sus usuarios de cambiarse de compañía lo cual representa pérdidas monetarias para el prestador de servicios, si bien es cierto que la implementación de una red redundante puede incrementar los costos de diseño e implementación, también es cierto que en el mediano plazo se obtienen mejoras en la relación costo-beneficio, ya que una red redundante ofrece un servicio de calidad a los clientes del prestador de servicios, lo anterior llevaría a los prestadores a incrementar el número de sus clientes, lo cual se vería reflejado directamente en sus ingresos.

Con base en lo anterior se han creado protocolos denominados de alta disponibilidad que ayudan a que la afectación del servicio en caso de falla sea casi imperceptible para los usuarios, de la mano con estos protocolos de alta disponibilidad debe ir un buen diseño de implementación ya que si no se cuenta con un buen diseño, los protocolos se vuelven inútiles y la red se convierte en poco confiable. En el presente trabajo se plantea la realización de una investigación que dé como resultado un análisis de cómo se puede implementar una red considerando una solución de alta disponibilidad, de dicha investigación se obtendrá información suficiente para conocer qué tecnologías y protocolos han sido desarrollado en los últimos años para poder implementar una red redundante que brinde alta disponibilidad en sus servicios.

Objetivo General

Plantear un diseño de alto nivel³ para la implementación de protocolos de alta disponibilidad en una red IP/MPLS, que sea escalable, aplicable a cualquier red dorsal basada en MPLS con topología física redundante y que permita eventos de falla en elementos de la red sin que los usuarios perciban afectación en sus servicios.

Objetivos Particulares

- Mostrar la importancia de que una red cuente con una solución de alta disponibilidad
- Exponer las características que debe tener una red redundante
- Señalar algunos de los diversos protocolos y/o técnicas empleados para lograr tener alta disponibilidad en una red.
- Mostrar de manera general las consideraciones que se deben tomar al momento de estar diseñando una red.
- Mostrar un ejemplo de alta disponibilidad en una red basada en MPLS.

Alcance

Esta tesis está acotada a proponer un diseño de alta disponibilidad para una red dorsal basada en MPLS, dicho diseño se basa en fundamentos teóricos, y se trata de demostrar que dicho diseño es funcional pero debido a que es imposible formar un laboratorio debido a los costos que ello representaría, se empleará un simulador de redes (GNS3⁴), en el presente trabajo dicho simulador considera solo configuración en equipos CISCO⁵, y como todo simulador, se tienen limitantes debido a que para la implementación de ciertas funcionalidades se requiere de licenciamiento por parte de CISCO. Cabe aclarar que independientemente de que la simulación se basara en plataformas CISCO, la solución es

³ Un diseño de alto nivel, también conocido como HLD por sus siglas en inglés, tiene por objetivo brindar una visión general no detallada de alguna solución, mostrando solo sus aspectos generales.

⁴ GNS3 es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellas.

⁵ Cisco Systems es una empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

aplicable para cualquier otra marca de equipos de datos, debido a que la mayoría de los protocolos usados en el presente trabajo son estándares mundiales, la diferencia radicará en la forma de configuración y en que soporten las funcionalidades a implementar.

CAPÍTULO II FUNDAMENTOS TEÓRICOS

2.1. Breve historia de las redes de datos

Las redes de datos se fueron desarrollando como consecuencia de aplicaciones comerciales para microcomputadoras, en un inicio las microcomputadoras no tenían conexión entre ellas, lo que complicaba el compartir datos entre varios computadores. La solución inicial fue emplear dispositivos de almacenamiento como los disquetes para el intercambio de información, pero muy pronto se notó que esa no era una solución óptima para el desarrollo de las actividades empresariales que requerían ese intercambio de información. Poco a poco las empresas se dieron cuenta que la posible solución a sus problemas con el manejo de la información podía estar en el desarrollo de las redes de datos, este desarrollo de las redes se empezó a dar en pasos agigantados y a principios de la década de los 80's el desarrollo de redes era cada vez más notorio, pero debido al crecimiento sin organización, a mediados de la década de los 80's se empezó hacer presente un problema y fue que cada empresa dedicada a desarrollar hardware y software para redes empleaba sus propios estándares⁶ lo que se empezó a reflejar en la incompatibilidad entre redes, debido a lo anterior empezaron a surgir los estándares con la finalidad de hacer homogéneo todo el desarrollo de las redes y que las empresas pudieran desarrollar productos compatibles con otros de diferente marca.

En un inicio se empezó hablar de las redes LAN, que eran redes pequeñas, que se encargaban de interconectar a los dispositivos de una misma compañía, pero de inmediato surgió la necesidad de transmitir información no solo dentro de una misma empresa sino también poder hacerlo entre empresas, la solución a lo anterior fue la creación de las redes MAN y redes WAN. De esta manera se empezó a clasificar a las redes de datos de acuerdo con el área geográfica que podían cubrir.

Todo el proceso histórico del desarrollo de las redes es un poco complejo ya que han tenido participación miles de personas alrededor del mundo en los últimos 40 años, y cada aportación ha sido valiosa para que la humanidad hoy cuente con una red de redes que se ha vuelto en un pilar fundamental para el desarrollo social y económico de todos los países y que ha repercutido directamente en el estilo de vida de todas las personas.

La tabla 2.1 muestra un cronograma histórico de los eventos más relevantes en la historia de las telecomunicaciones.

⁶ En Telecomunicaciones, un estándar se puede definir como " *Conjunto de normas y recomendaciones técnicas que regulan la transmisión en los sistemas de comunicaciones*" (Eveliux, 2007)

Año	Evento
Antes de 1900	Comunicaciones de larga distancia a través de jinetes, señales de humo, palomas mensajeras, telégrafo.
Decada de 1890	Bell inventa el teléfono.
1901	Primera transmisión inalámbrica de Marconi.
Decada de 1920	Radio AM.
1939	Radio FM.
Decada de 1940	La segunda guerra mundial provoca el auge de la radio y el desarrollo de las microondas.
1947	Shockley, Barden y Brittain inventan el transistor de cátodo sólido (semiconductor).
1948	Claude Shannon publicó la "Teoría matemática de la comunicación".
Decada de 1950	Inención de los circuitos integrados.
1957	El departamento de defensa de los Estados Unidos crea ARPA.
Decada de 1960	Desarrollo de computadoras Mainframe.
1962	Paul Baran de "RAND" trabaja en redes de conmutación de paquetes.
1967	Larry Roberts publica el primer informe sobre ARPANET.
1969	ARPANET se establece en UCLA, UCSB, U-Utah y Standford.
Decada de 1970	Uso generalizado de circuitos digitales integrados; advenimiento de las PCs digitales.
1970	Universidad de Hawaii desarrolla ALOHANET.
1972	Ray Tomlinson crea un programa de correo electrónico para enviar mensajes.
1973	Bob Kahn y Vinton Cerf empiezan a trabajar en lo que posteriormente se transformaría en TCP/IP.
1981	Se acuña el término Internet a un conjunto de computadoras interconectadas entre sí.
1982	ISO lanza el modelo de referencia OSI.
	El protocolo TCP/IP se transforma en el lenguaje universal de INTERNET. ARPANet en sí mismo permaneció estrechamente controlado por el departamento de defensa hasta 1983 cuando su parte estrictamente militar se segmentó convirtiéndose en MILNET. El Pentágono se retira de Arpanet y crea MILnet. Internet ya dispone de 562 servidores. Se creó el sistema de nombres de dominios (.com, .edu, etc., más las siglas de los países), que prácticamente se ha mantenido hasta ahora.
1983	
1984	Se funda CISCO systems; comienza el desarrollo de gateways y Routers.
1987	La cantidad de hosts conectados a Internet supera los 10000.
1989	La cantidad de hosts conectados a Internet supera los 100000.
1990	ARPANET se transforma en la Internet.
1991	Se crea la WWW.
1992	La cantidad de hosts conectados a Internet supera el millón.
1994	Se presenta el navegador web "Netscape Navigator".
1996	La cantidad de hosts conectados a Internet supera los 10 millones.
1997	Internet 2 surge como propuesta para crear un espacio aparte y de más calidad de comunicaciones para instituciones de
2001	La cantidad de hosts en internet supera los 110 millones.
2004	Teléfono por Internet.
2005 a la actualidad	<p>6 son las claves del cambio en Internet y que nos han cambiado nuestra manera de verla.</p> <p>WEB2.0: Concepto que define toda una serie de aplicaciones de fácil manejo, de participación social y activa, que han permitido que al usuario interactuar de manera decisiva con la red.</p> <p>Blogs/Podcast: El blog aumento exponencialmente en 2004, pero es este año que se cierra el que le ha lanzado como medio de comunicación masivo y social, donde el espectador deja de ser consumidor de información para ser también generador de información. El podcast vendría a ser el hermano auditivo del blog, y este año se ha convertido en palabra de moda.</p> <p>iTunes: Con la guerra lanzada contra el P2P, el intercambio de archivos en Internet, Apple hizo su apuesta comercial para distribuir la música en Internet. En lo que parece ser el declive del modelo de negocio musical de las grandes multinacionales discográficas (el 85% de la música mundial es distribuida por solo 2 empresas), iTunes ha recogido el relevo de la venta de música.</p> <p>VoIP: Es posible transmitir voz mediante el protocolo IP. Con Skype como bandera, esta tecnología, conocida desde hace años, ha dado su salto definitivo. Google también se ha sumado a la VoIP con Google Talk.</p> <p>Internet sin cables: En este año se ha masificado el número de Hot Spots, lugares donde conectar tu portátil a Internet sin necesidad de hilos. A su popularización ha contribuido la aparición de consolas como la PSP (Play Station Potatil) que permiten navegar por Internet desde una consola de juegos portátil.</p> <p>Internet por satélite en vehículos: mediante una antena plana que mide tan solo dos pulgadas y es capaz de recibir programas de televisión satélite y dar conexión a Internet desde un vehículo. La antena se podrá instalar en coches particulares, trenes, autobuses y aviones y será comercializada en el mercado estadounidense por Audiovox.</p>

Tabla 0.1 Cronología de las telecomunicaciones⁷.

⁷ Información basada en el contenido de (Academy_Cisco_Networking, Versión 3.1).

2.2. Estandarización de las telecomunicaciones

En el mundo de las telecomunicaciones existen varios proveedores de dispositivos de comunicaciones y cada uno de ellos tiene su propia idea de cómo deberían hacerse las cosas, sin embargo, conforme se fue desarrollando el mercado de la comunicaciones se comenzaron a tener problemas de interoperabilidad entre las redes de telecomunicaciones, como cada vez más redes se interconectaban entre sí, se tenían que crear acuerdos entre los proveedores de tal manera que existiera interoperabilidad entre las diferentes marcas de equipos, y lo anterior no solo era para permitir la comunicación entre diferentes plataformas sino que también era un incentivo para el crecimiento del mercado de las telecomunicaciones, ya que un amplio mercado permite producción en masa, lo que impacta en el crecimiento de economías basadas en manufacturas y al final del día lo anterior se ve reflejado en disminución de precios en los equipos, lo que conlleva a una aceptación generalizada en los consumidores.

UIT (Unión Internacional de Telecomunicaciones)

En el mundo de las telecomunicaciones la necesidad de empezar a poner orden entre los proveedores de servicios y equipos de comunicaciones nació a partir del uso del telégrafo, donde se empezó a tener claramente la necesidad de tener compatibilidad a nivel mundial para asegurar comunicación entre diferentes países, derivado de lo anterior en 1865 representantes de varios gobiernos europeos se unieron para formar el antecesor de lo que hoy en día es conocido como ITU o UIT por sus siglas en español, dicha organización tiene varios sectores, el sector de estandarización de las telecomunicaciones normalmente es ubicado con las siguientes siglas ITU-T, el trabajo de este sector fue y sigue siendo, organizar conferencias mundiales sobre normalización de telecomunicaciones y de la dirección de los grupos de trabajo, cabe señalar que todo lo que emite la ITU es a nivel de recomendación.

ISO (International Standard Organization)

Otro organismo que forma parte de estandarización de las telecomunicaciones es la ISO, fundada en 1947, dicha organización está formada para producir y publicar estándares internacionales, hoy en día está formada por miembros de 164 países, cabe destacar que la ISO no solo publica estándares referentes a las tecnologías sino también en otros ámbitos ya que su objetivo es promover el desarrollo de estándares para facilitar el intercambio internacional de bienes y servicios. En lo referente a las telecomunicaciones ISO e ITU-T cooperan de manera conjunta, de hecho la ISO es un miembro de la ITU. De manera general se puede decir que la ITU y la ISO tienen gran impacto en acuerdos de relevancia internacional,

en los que regularmente participan organizaciones oficiales y de gobierno, ISO publica distintos tipos de documentos: estándares, guías técnicas, standard's handbook y boletines, la aportación más significativa de la ISO dentro de las redes de datos fue la publicación del modelo de referencia OSI.

IEEE: Institute of Electrical and Electronic Engineers

Es la organización profesional más grande del mundo, fundada en 1963 y de origen americano, cuenta en la actualidad con miembros de más de 130 países, se dedica a publicar numerosas revistas así como de programar numerosas conferencias técnicas a lo largo del año en diferentes partes del mundo relacionadas con computación, redes y comunicaciones, ha establecido un grupo dedicado al desarrollo de normas en el área de la ingeniería eléctrica y computacional, ejemplo de normas que han desarrollado son las normas 802 para redes LAN, que se volvieron clave para el desarrollo de las mismas, ej. 802.3 Ethernet.

IETF: Internet Engineering Task Force

Es el organismo que regula y normaliza protocolos y procedimientos en Internet, formado por voluntarios que estudian aspectos técnicos y recomendaciones para la adopción de estándares. Trabaja en problemas que necesitan de una resolución a corto plazo. En general la IETF es un pilar en el proceso de normalización en Internet y forma parte de las organizaciones que se ocupan de la coordinación de Internet y de las tareas de desarrollo dentro de la misma, el siguiente listado muestra dichas organizaciones.

- NIC (Network Information Center). Responsable de recibir y distribuir los protocolos de la red.
- NOC (Network Operation Center). Encargada de administrar los enlaces de telecomunicaciones y los ordenadores que actúan como sistemas de conmutación nodal y forman el núcleo de la red.
- IAB (Internet Architecture Board). Junta directiva de la arquitectura de Internet protocolos utilizados en la arquitectura TCP/IP. Supervisa dos grandes equipos de trabajo:
 - IETF (Internet Engineering Task Force). Trabaja en problemas que necesitan una resolución a corto plazo.
 - IRTF (Internet Research Task Force). Realiza tareas de investigación a largo plazo.
- IANA (Internet Assigned Numbers Authority). Responsable de la asignación de nombres y direcciones de red, así como también de los sistemas autónomos.

Encargada también de publicar los denominados solicitud de Comentarios RFC o Request For Comments determinantes en el proceso de desarrollo de normas de Internet.

2.3. Modelos de referencia

Hoy en día es prácticamente imposible no encontrar a una computadora que no soporte los mismos protocolos de red que cualquier otra computadora, pero cabe resaltar que no siempre fue así de fácil el tema de los protocolos de red, hubo un momento en que los protocolos de red no existían, inclusive no existía el famoso set de protocolos TCP/IP que es sobre lo que hoy en día se basan las comunicaciones en IP, los protocolos de red se fueron desarrollando conforme los Vendors⁸ iban desarrollando nuevos productos, lo anterior quiere decir que los mismos Vendors fueron desarrollando los protocolos, pero en consecuencia, el detalle de dichos protocolos no era dado a conocer de manera pública y se decía que los protocolos eran propietarios y solo podían ser utilizados por aquellos que los habían desarrollado, lo anterior influía en que prácticamente las grandes empresas eran las únicas que tenían el poder para ir maquilando el mundo de las comunicaciones a su manera y siendo ellos los más beneficiados, llegando a afectar el tema de la interoperabilidad con productos fabricados por otros Vendors.

2.3.1 Modelo OSI

La solución al problema planteado anteriormente, fue crear un modelo estándar que todos los Vendors pudieran soportar. La organización internacional para la estandarización (ISO, por sus siglas en inglés), tomó cartas en el asunto y en los años 70s comenzó a trabajar en lo que hoy se conoce como modelo OSI (Open System Interconnection), el cual tenía y sigue teniendo un objetivo muy claro, estandarizar los protocolos de las redes de datos de tal manera que se logre la comunicación entre todas las computadoras alrededor del mundo. ISO trabajó sobre ese objetivo, trabajando en conjunto con los grandes desarrolladores de tecnología alrededor del mundo, hasta que lograron la publicación del modelo más empleado alrededor del mundo como punto de referencia para la discusión de especificaciones de otros protocolos, el modelo OSI.

El modelo OSI consiste de 7 capas, cada capa define un grupo de funciones específicas de red, debido a esta estructura se puede estudiar cualquier protocolo de red, y de acuerdo con sus funciones se puede clasificar en alguna de las 7 capas del modelo OSI, por lo tanto a todos les

⁸ Término usado comúnmente para referirse a fabricantes de equipos de telecomunicaciones.

sirve el modelo OSI cuando tratan de describir las funciones de cierto protocolo o inclusive de cierto equipo de comunicaciones.

En general las capas del modelo OSI se pueden segmentar en 2 grupos, las capas superiores (5, 6 y 7) definen funciones enfocadas a la aplicación, y las capas inferiores (1, 2, 3 y 4) definen funciones enfocadas en la entrega de datos end to end.

En la siguiente tabla se muestra la descripción funcional de cada capa del modelo OSI:

Modelo OSI		
CAPA	DESCRIPCIÓN	UNIDA DE DATOS
7 APLICACIÓN	Proporciona la interfaz y servicios que soportan las aplicaciones de usuario. Se encarga de ofrecer acceso general a la red, ofrece los servicios de red relacionados con las aplicaciones de usuario, como la gestión de mensajes, la transferencia de archivos y las consultas a bases de datos. La capa de aplicación suministra cada uno de estos servicios a los distintos programas de aplicación con los que cuenta el usuario en su computadora.	APDU
6 PRESENTACIÓN	Su propósito principal es definir y negociar el formato de los datos, tal como: texto ASCII, texto EBCDIC, binario, BDC, JPEG, etc. La encriptación es también definida de acuerdo con el modelo OSI como un servicio de la capa de presentación.	PPDU
5 SESIÓN	Define como empezar, controlar y finalizar conversaciones (denominadas como sesiones), esto incluye el control y administración de múltiples mensajes bidireccionales .	SPDU
4 TRANSPORTE	Se enfoca a temas relacionados con la entrega de datos a otra computadora, por ejemplo corrección de errores y control de flujo.	Segmento
3 RED	La capa de red define 3 principales características: direccionamiento local, reenvío de paquetes y determinación de ruta. Los conceptos de ruteo definen como los dispositivos (generalmente routers), envían paquetes a su destino final, el direccionamiento lógico define como cada dispositivo puede tener una dirección que pueda ser usada para el proceso de ruteo, determinación de ruta se refiere al trabajo realizado por los protocolos de ruteo.	Paquete
2 ENLACE	Define los protocolos que determinan cuando un dispositivo puede enviar datos sobre un medio de Tx en particular, los protocolos de enlace de datos también definen el formato del encabezado que permite a los dispositivos enviar y recibir datos de manera satisfactoria. el trailer que maneja la trama de capa 2 define el campo FCS (Frame Check Sequence), que permite a los dispositivos detectar errores durante la transmisión.	Trama
1 FÍSICA	Esta capa típicamente hace referencia a estándares de otras organizaciones. Estos estándares tratan las características físicas del medio de transmisión, incluyendo conectores, pines, el uso de los pines, corriente eléctrica, codificación, modulación de señales, tipo de medio de Tx, etc.	Bit

Tabla 0.2 Capas del modelo OSI.

2.3.2 Modelo TCP/IP

El modelo TCP/IP nace como resultado de la implementación de la primera red, ARPANET, y dicho modelo se ha convertido en el estándar histórico y técnico del Internet. El Departamento de Defensa de Estados Unidos. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP, el cual se desarrolló como un estándar abierto, esto significaba que cualquier persona podía usar el TCP/IP.

El modelo TCP/IP cuenta con las siguientes capas: aplicación, transporte, Internet y acceso a la red. Aunque algunas de la capas tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta.

Modelo TCP/IP	
CAPA	DESCRIPCIÓN
4 Aplicación	La capa de aplicación brinda servicios al software de aplicación que está corriendo en cierta computadora, esto indica que la capa de aplicación no define a la aplicación en sí misma pero sí le ayuda en los servicios que la aplicación requiere. Por ejemplo, la aplicación de HTTP requiere de la transferencia de archivos, entonces en resumen la capa de aplicación provee una interfaz entre el software corriendo en una computadora y la red en sí misma.
3 Transporte	La capa de transporte se encarga de aspectos de calidad de servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Permite que la comunicación entre dos hosts se dé en una manera confiable. Dos protocolos de transporte son los que se han definido y son los que se pueden emplear como protocolos de transporte, dichos protocolos son TCP y UDP.
2 Internet	La capa de internet define un formato de paquete y protocolo llamado IP (Internet Protocol), el trabajo de la capa de internet es entregar los paquetes IP a donde estos pretendan llegar, el objetivo es que los paquetes lleguen a la red destino independientemente de la ruta que utilizaron para llegar allí. En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.
1 Acceso a la red	Esta capa guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles de tecnología de networking, y todos los detalles de las capas física y de enlace de datos del modelo OSI.

Tabla 0.3 Capas del modelo TCP/IP.

2.4. Dispositivos de red

Los equipos que se conectan de manera directa a un segmento de la red se denominan dispositivos, dichos dispositivos se pueden clasificar de manera general en dos grupos, el primero de ellos corresponde a los dispositivos de usuario final, comúnmente llamados "hosts", es decir aquellos dispositivos que brindan servicios directamente al usuario, por ejemplo; computadoras, impresoras, escáneres, etc. El segundo grupo se denomina dispositivos de red, este tipo de dispositivos se encargan de transportar los datos que se transfieren entre sí los dispositivos de usuario final, algunos ejemplos de estos dispositivos son los hubs, switches, routers, firewalls.

Para entender cómo funciona un red de datos es esencial tener claro cuál es la función de cada elemento de red; como se mencionó anteriormente estos elementos son los conocidos como dispositivos de red, el tener clara la función de cada uno de estos dispositivos ayuda para tener una adecuada visión al momento de plantear un diseño de red.

A continuación se presenta una descripción de los dispositivos de red más importantes.

Hub. Como su nombre lo indica, se encarga de concentrar conexiones, esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos, lo cual permite que en una red a un grupo de hosts se les trate como una sola unidad. Este equipo no tiene inteligencia para el análisis de paquetes. Este dispositivo trabaja dentro de la capa 1 del modelo OSI.

Switch. Es un dispositivo que renvía datos de acuerdo con la dirección MAC destino que se encuentra en la trama, se puede decir que permite la comunicación entre los elementos de red de un mismo segmento de red pero de una manera más ordenada que los hubs. En la actualidad se cuentan con switches denominados de capa 2 y capa 3, es decir que aparte de hacer sus funciones básicas de envío de datos basándose en la MAC destino, pueden hacer funciones de ruteo, teniendo más inteligencia para el tratamiento de los datos y reduciendo la necesidad de tener un router y un switch en equipos diferentes.

Router. Este dispositivo prácticamente puede hacer las funciones de los dispositivos mencionados anteriormente, puede regenerar señales, re-enviar paquetes, y su función más importante y por la que es reconocido es por el encaminamiento de paquetes, esta última parte explica el nombre del dispositivo, ya que tiene la inteligencia para indicar cuál es su siguiente salto del paquete de acuerdo con el destino al que quiere llegar el paquete, es por lo anterior que se dice que el router marca la ruta óptima para que el paquete llegue a su destino final.

Firewall. Un FW puede ser basado en software o hardware, y su función principal es ayudar a mantener la seguridad de la red, lo anterior lo lleva a cabo controlando el ingreso y egreso a la red de todos los paquetes, analizando cada uno y determinando, de acuerdo con su configuración, si deben pasar o deben ser bloqueados. Cabe mencionar que en las computadoras personales se cuenta normalmente con un firewall basado en software para proteger de ataques provenientes de usuarios externos, en el caso de los routers, algunos de ellos cuentan con funciones básicas de un firewall y un firewall cuenta con funciones básicas de un router.

Los dispositivos de red mencionados anteriormente cuentan con iconos particulares que permiten su identificación en un diseño de red, en la tabla 2.4 se muestra dicha simbología, cabe aclarar que existen variantes con respecto a los símbolos en la literatura, pero cada uno de ellos guarda la esencia básica de la simbología de las redes.

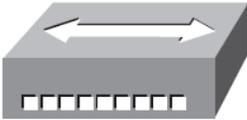
 <p style="text-align: center;">Router</p>	 <p style="text-align: center;">Switch</p>
 <p style="text-align: center;">Hub</p>	 <p style="text-align: center;">Firewall</p>

Tabla 0.4 Simbología de equipos de datos.

2.5. Topologías de red

La topología de una red define su estructura y muestra como es la interconexión entre los elementos que la conforman, la topología de una red se clasifica en física y lógica, la topología física define la disposición real de la conexiones físicas (cableado) entre los elementos de la red, la topología lógica define el flujo de datos entre los elementos de la red.

Las topologías más comúnmente usadas se muestran en la tabla siguiente.

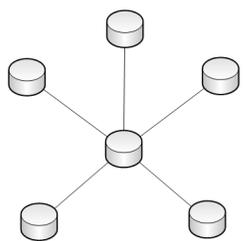
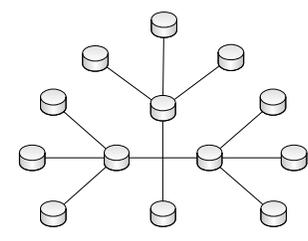
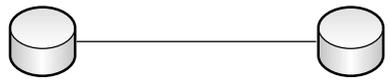
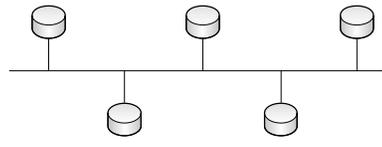
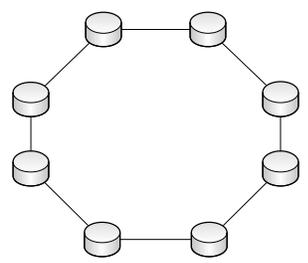
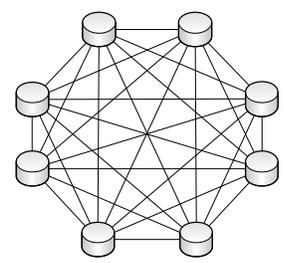
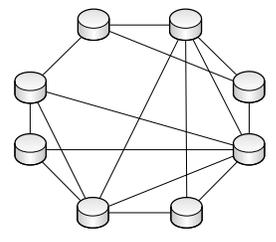
 <p>Estrella</p>	 <p>Estrella extendida</p>
 <p>Punto a punto</p>	 <p>Bus</p>
 <p>Anillo</p>	 <p>Malla completa (Full-Mesh)</p>
 <p>Malla parcial</p>	

Tabla 0.5 Topologías de Red.

Otra topología que resulta útil para poder interpretar la infraestructura de una red, es la topología jerárquica de una red o también conocida como modelo de red jerárquica, lo que

propone este modelo es dividir en capas discretas a la red de acuerdo con las funciones que realizan sus elementos, separando los elementos de acuerdo con su función se logra tener un diseño modular que facilita la escalabilidad y el desempeño.

El diseño jerárquico contempla 3 capas, que son las siguientes:

Acceso. Contempla usuarios locales y de acceso remoto

Distribución. Controla el flujo de datos entre las capas de acceso y backbone.

Backbone. Esta capa tiene varios nombres, se le puede también encontrar en la literatura como núcleo, red dorsal o core, pero en esencia es el mismo significado para todos esos diversos términos, esta capa se caracteriza por tener en ella los elementos más robustos de la red, dándole a esta capa las características de alta velocidad y alta disponibilidad (redundancia).

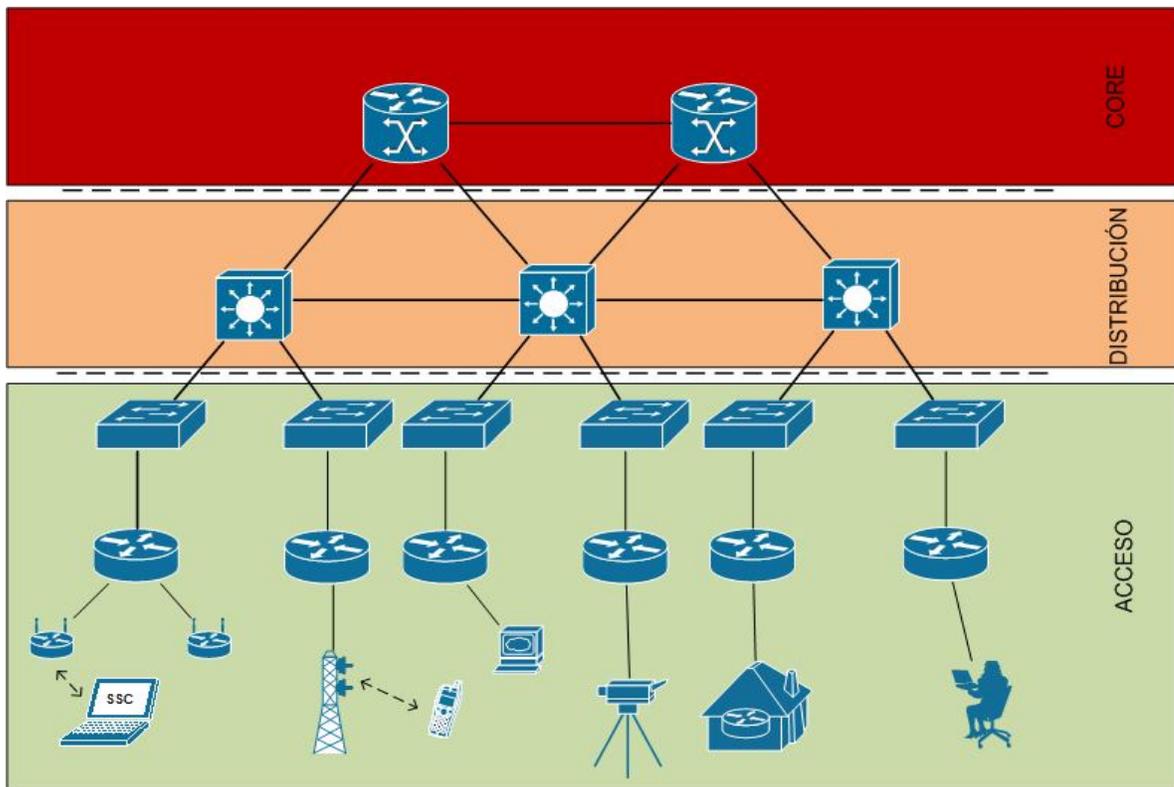


Figura 2.1 Topología Jerárquica.

2.6. Direccionamiento IPv4

Para facilitar el enrutamiento de paquetes en la red y la comunicación entre hosts, la suite de protocolos TCP/IP utiliza una dirección lógica de 32 bits conocida como dirección IP, esta dirección debe ser única para cada dispositivo dentro de la red, usualmente esta dirección está escrita en notación decimal, y en IPv4⁶ dicha dirección está formada por 4 octetos, es decir los 32 bits que forman la dirección son separados en 4 grupos de 8 bits, de allí el nombre de octetos, y en la representación decimal cada octeto es trasladado a su equivalente decimal, cada octeto es separado por un punto decimal ".", por ejemplo la dirección IP 100.1.1.1 es una dirección escrita en notación decimal que trasladada a notación binaria sería 01100100.00000001.00000001.00000001.

Cada paquete IP tiene 2 secciones básicas en su encabezado las cuales son la dirección IP fuente y la dirección IP destino, con esta información es como determina que ruta es la óptima para llegar a la IP destino que indica el paquete. En la figura 2.2 se muestra el encabezado del paquete IPv4.

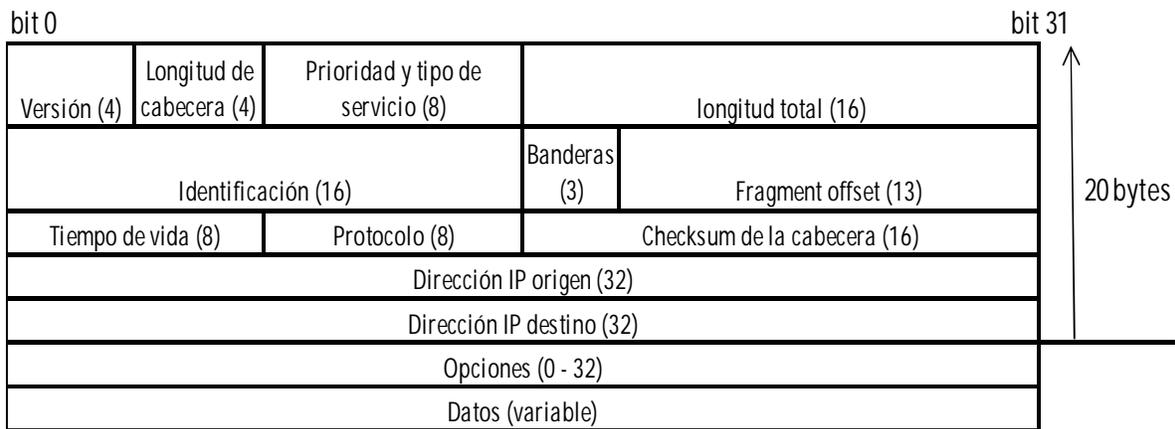


Figura 2.2 Encabezado del paquete IPv4.

Clases de direcciones

Desde un inicio, el direccionamiento IPv4 fue diseñado en una estructura de clases: Clase A, B, C, D y E. La clase D es empleada para direcciones de multicast y la clase E está reservada para experimentación. Clases A, B y C son direcciones que pueden ser asignadas a hosts, cabe mencionar que una dirección IP se divide principalmente en 2 partes, la parte que identifica a la red y la parte que identifica al host, considerando lo anterior las clases A, B y C presentan una estructura jerárquica, a continuación se observa la segmentación de las redes de acuerdo con la clase a la que pertenecen, véase tabla 2.6.

Clase	Rango del primer octeto, decimal	Rango del primer octeto, binario	Porción de red (R) y de Host (H)	Máscara de subred (Decimal y binario)	Número de posibles redes	Número de posibles hosts por red
A	0-127	00000000-01111111	R.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	$2^7-2=126$ *	$2^{24}-2=16777214$
B	128-191	10000000-10111111	R.R.H.H	255.255.0.0 11111111.11111111.00000000.00000000	$2^{14}=16384$	$2^{16}-2=65534$
C	192-223	11000000-11011111	R.R.R.H	255.255.255.0 11111111.11111111.11111111.00000000	$2^{21}=2097152$	$2^8-2=254$
D	224-239	11100000-11101111	No empleada para direccionamiento de hosts			
E	240-255	11110000-11111111	No empleada para direccionamiento de hosts			

*Dentro de la clase A, la red 0.0.0.0 (originalmente se planteó como una dirección de broadcast) y la 127.0.0.0 (Actualmente se sigue utilizando como dirección de loopback) están reservadas.

Tabla 0.6 Clases de direcciones IPv4.

Por definición todas las direcciones IP pertenecientes a la misma clase de red, A, B o C tienen exactamente el mismo valor en la porción de red de la dirección, el resto de la dirección IP es lo que se le conoce como la porción del host.

En un inicio esta definición de clases en las direcciones IP, permitió que las autoridades encargadas de asignar direcciones IP, pudieran asignar a los gobiernos, compañías, escuelas, ISP's, rangos de direcciones de acuerdo con el tamaño de su red, direccionamiento clase A para redes de gran tamaño, clase B para redes medianas y clase C para redes pequeñas. Con una autoridad central asignando todo el direccionamiento se lograba tener asegurada una única asignación de direcciones a nivel global, evitando conflicto con el direccionamiento, a cada organización se le asignaba una red clase A, B o C y dicha organización se encargaba de administrar ese direccionamiento con sus hosts internos. Cabe mencionar que este modo de asignación ha ido cambiando conforme ha pasado el tiempo y conforme ha crecido la red a nivel mundial, pero el término de clases sigue siendo útil para entender el direccionamiento IPv4.

IP Subnetting

El subnetting nació como una técnica para una mejor administración del direccionamiento IP dentro de las organizaciones, la idea principal del subnetting es tomar una red clase A, B o C y subdividirla en pequeños grupos de direcciones IP a los cuales se les denomina subredes o subnet que es como mejor se conoce en el mundo de las redes, este último término surge como abreviación de "subdivided network".

Para entender el concepto de subnetting nos referiremos a un ejemplo, supongamos que la autoridad de asignación de direcciones IP le da a una organización la red 200.1.1.0 /24, la cual corresponde a una red clase C, la organización deberá ser capaz de administrar esta red que le fue asignada para dar una IP a cada uno de sus elementos. Supongamos que la organización tiene la siguiente topología.

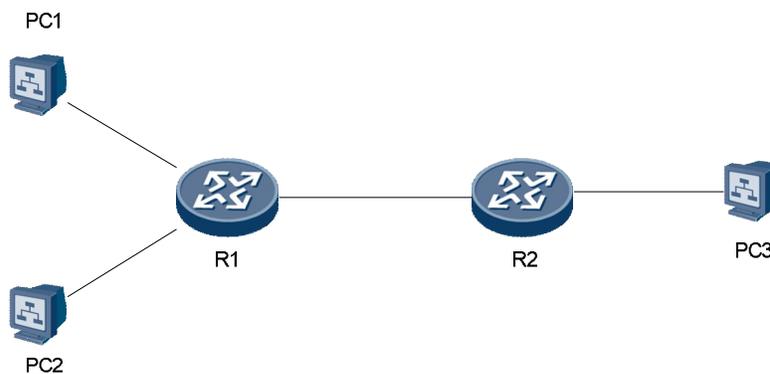


Figura 2.3 Ejemplo de subnet.

En la topología anterior se necesitan al menos de 4 segmentos de red, pero a la organización solo se le asignó el segmento 200.1.1.0 /24, con dicho segmento tendría hasta 254 direcciones IP, y en la imagen se ve que solo necesitaría 8 direcciones IP, pero debido a que hay routers presentes ocasionando la presencia de diversos dominios de broadcast, no se puede utilizar un mismo segmento en un dominio de broadcast distinto. Para resolver lo anterior es donde entra el subnetting, haciendo la división del segmento de red asignado.

Analizando la topología se observa que se requieren 4 diferentes segmentos y cada segmento requiere de al menos 2 IP's, para saber cuántos bits vamos a tomar prestados se tiene la siguiente fórmula:

$$2^{BP} - 2 = \text{IPs necesarias} \quad ; BP = \text{Bits Prestados}$$

$$BP = \sqrt{\text{IPs necesarias} + 2}$$

Por lo tanto, adecuándolo al ejemplo, tendríamos que $BP = \sqrt{2 + 2} = 2$

De lo anterior, la máscara de subred quedaría como /30, donde 30 es el resultado de, #bits de una dirección IPv4 – Bits prestados, en el caso del ejemplo sería 32-2=30.

Con lo cual tendríamos las siguientes subredes:

Subred	Host	Broadcast	Máscara
200.1.1.0	200.1.1.1-200.1.1.2	200.1.1.3	/30
200.1.1.4	200.1.1.5-200.1.1.6	200.1.1.7	/30
200.1.1.8	200.1.1.9-200.1.1.10	200.1.1.11	/30
200.1.1.12	200.1.1.13-200.1.1.14	200.1.1.15	/30
200.1.1.16	200.1.1.17-200.1.1.18	200.1.1.19	/30
.	.	.	.
.	.	.	.
.	.	.	.
200.1.1.252	200.1.1.253-200.1.1.254	200.1.1.255	/30

Tabla 0.7 Ejemplo de subneteo.

Cada una de esas subredes puede ser usada en los diversos dominios de broadcast que tiene la red.

Direccionamiento público y privado

Como se mencionó anteriormente la asignación de direccionamiento fue cambiando conforme se dio el crecimiento de las redes a nivel mundial, fue tanto el crecimiento que se volvió imposible asignar una IP a cada host en todo el mundo debido a que creció el número de hosts exponencialmente y la cantidad de direcciones IP's disponibles disminuía conforme pasaban los años, para contrarrestar este comportamiento se definió utilizar direccionamiento privado dentro de las organizaciones, lo que permitiría que diversas organizaciones podrían utilizar el mismo direccionamiento, pero con la condicionante de que este direccionamiento privado no iba a poder ser anunciado en la red pública, la asignación del direccionamiento privado quedó de la siguiente manera:

- Clase A: 10.0.0.0 /8 (10.0.0.0 – 10.255.255.255)
- Clase B: 172.16.0.0 /12 (172.16.0.0 – 172.31.255.255)
- Clase C: 192.168.0.0 /16 (192.168.0.0 – 192.168.255.255)

Este direccionamiento puede ser utilizado para las redes internas de una organización, si se requiere reenviar tráfico a la red pública que hoy en día se le conoce como Internet se requiere trasladar el direccionamiento privado a público, usando traslación de direcciones de red, mejor conocido como NAT por sus siglas en inglés (Network Address Translation).

2.7. Métodos de ruteo

El router es el dispositivo más importante en el reenvío de paquetes en una red de datos, ya que lleva a cabo las funciones de selección de ruta y conmutación de paquetes. Para el caso de selección de ruta, el router busca en su tabla de ruteo cuál es la ruta óptima para llegar a la dirección IP destino indicada en el paquete IP.

De acuerdo con la búsqueda del router en su tabla de ruteo cae en 3 posibles casos de determinación de ruta:

- **Red directamente conectada.** Si la dirección IP destino pertenece a un dispositivo que está directamente conectado a una de las interfaces del router, ese paquete es directamente enviado a tal dispositivo. Lo anterior indica que la dirección IP destino pertenecía a la misma red que la interfaz del router.
- **Red remota.** Si la dirección IP destino pertenece a una red remota, el paquete es enviado a otro router, y así será el envío consecutivamente hasta que el paquete llegue al router que tiene localmente a la red a la que pertenece la IP destino indicada en el paquete.
- **Red no determinada.** Si la IP destino indicada en el paquete no se encuentra en la tabla de ruteo del router, es decir que no pertenece a las redes directamente conectadas o a las redes remotas que conoce, entonces el router descarta el paquete debido a que no tiene información de donde enviar el paquete.

Existen 3 maneras en las que un router puede aprender rutas:

- **Rutas directamente conectadas.** Un router ingresa automáticamente a su tabla de ruteo aquellas redes a las que están asociadas sus interfaces, es decir, cada que se agrega una dirección IP a una de sus interfaces, el router interpreta a la red a la que pertenece la IP como una red directamente conectada.
- **Rutas estáticas.** Estas rutas, como su nombre lo sugiere, son rutas que son configuradas manualmente por el administrador de la red, prácticamente el administrador de la red mediante rutas estáticas indica el camino que seguirá el paquete IP para llegar a su destino.
- **Rutas dinámicas.** Para aprender rutas de manera dinámica se emplean los denominados protocolos de ruteo, si diversos routers quieren compartir rutas de manera dinámica, cada uno de ellos deberá tener configurado el mismo protocolo de ruteo, cabe mencionar que existen diversos protocolos de ruteo y cada uno de ellos

cuenta con sus particularidades, y de acuerdo con las necesidades de la red unos podrán ser más útiles que otros.

En muchos casos, la complejidad de la topología de la red, el número de elementos de red, y la necesidad de ajustar automáticamente a la red cuando esta sufre cambios, se requiere el uso de protocolos de ruteo, dichos protocolos tienen varias ventajas sobre el enrutamiento estático, pero hoy en día se siguen empleando ambos métodos de manera combinada.

La siguiente tabla muestra una comparación entre el método estático y el dinámico, y se puede observar que las ventajas de uno son las desventajas del otro.

Característica	Ruteo dinámico	Ruteo estático
Complejidad de configuración	Generalmente independiente del tamaño de la red	Incrementa con el tamaño de la red
Conocimiento requerido del administrador	Conocimiento avanzado requerido	No se requiere de conocimiento extra
Cambios de topología	Automáticamente se adapta a los cambios de topología	Se requiere intervención del administrador
Escalabilidad	Bueno para redes simples y complejas	Bueno solo para redes simples
Seguridad	menos seguro	más seguro
Uso de recursos	Usa CPU, memoria y ancho de banda	No se requiere de recursos extra
Predicción de ruta	Depende de la topología actual	La ruta al destino es siempre la misma

Tabla 0.8 Comparación entre ruteo estático y dinámico.

2.8. Protocolos de ruteo

Como anteriormente se mencionó, los protocolos de ruteo caen en la clasificación de método dinámico para determinar las rutas que seguirán los paquetes IP a su destino, durante el paso del tiempo se han desarrollado diversos protocolos; de acuerdo con las necesidades se han venido dando en las redes, lo anterior ha llevado a tener protocolos con características muy particulares, debido a tales particularidades podemos clasificarlos de la siguiente manera:

- IGP o EGP

- Vector distancia o estado enlace
- Classful o Classless

IGP y EGP

Para entender los conceptos de IGP y EGP es necesario introducir el concepto de AS (Autonomous System), un AS se define como una colección de redes que se encuentran bajo una misma administración, en la actualidad los sistemas autónomos públicos son asignados por la IANA⁹, mediante los registros regionales como por ejemplo; LACNIC, AFRINIC, APNIC, ARIN etc.

Un sistema autónomo sirve para distinguir en conjunto a toda una empresa o ISP y sirve como identificador cuando se interconectan entre ellos.

IGP (Interior Gateway Protocol). Usado para ruteo intra- AS, esto es, ruteo dentro del mismo AS.

EGP (Extended Gateway Protocol). Usado para inter-AS, esto es, ruteo entre diferentes AS's.

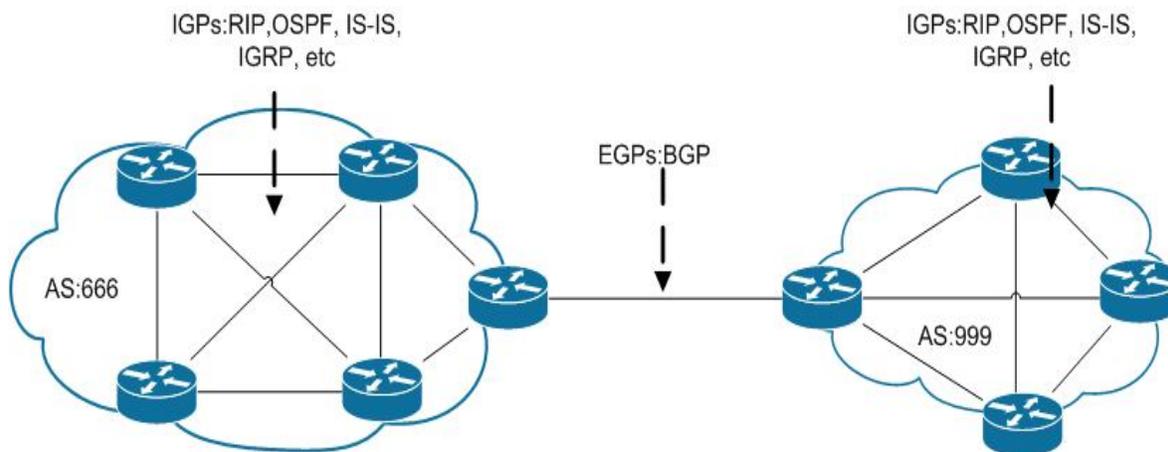


Figura 2.4 Protocolos de ruteo.

Protocolos de vector distancia

⁹ La Internet Assigned Numbers Authority (cuyo acrónimo es IANA) es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. Actualmente es un departamento operado por ICANN.

Vector distancia significa que las rutas son anunciadas como vectores de distancia y dirección, la distancia es definida en términos de una métrica de ruteo, como lo es el número de saltos y la dirección se define como el router al que se da el siguiente salto o la interfaz de salida del paquete.

Algunos protocolos de vector distancia periódicamente envían tablas de ruteo completas a todos sus vecinos, en grandes redes estas actualizaciones llegan a ser enormes causando afectación en el uso de ancho de banda de los enlaces.

Los protocolos de vector distancia típicamente emplean el algoritmo Bellman-Ford, el cual permite acumular en el router suficiente información para mantener la base de datos de las redes alcanzables, pero el mismo algoritmo no permite a un router tener el conocimiento de toda la topología de la red, el router únicamente conoce la información de ruteo que le es enviada por sus vecinos, la única información que conoce el router acerca de las redes remotas es la distancia o métrica para alcanzar a la red remota y la trayectoria o interfaz de salida para llegar a ella.

Los protocolos de vector distancia suelen ser útiles en los siguientes casos:

- Cuando la red es simple y no requiere de un diseño jerárquico
- Cuando los administradores no tienen suficiente conocimiento para configurar y analizar problemas de protocolos de estado enlace
- Cuando en el peor de los casos, el tiempo de convergencia de la red no es un tema importante.

Protocolos de estado enlace

En contraste con la operación de los protocolos de vector distancia, un router que tiene configurado un protocolo de estado enlace puede crear una “vista completa” o topología de la red gracias a la recopilación de información de los demás routers. Un protocolo de estado enlace emplea la información del estado de los enlaces para crear un mapa de la topología y seleccionar la mejor trayectoria a todas las redes destino que contemple la topología.

Otra diferencia con respecto a los protocolos de vector distancia, es que los protocolos de estado enlace no envían actualizaciones periódicas, después de que la red ha convergido, únicamente se envían actualizaciones cuando hay algún cambio en la red.

Los protocolos de estado enlaces trabajan de mejor manera en las siguientes situaciones:

- El diseño de la red es jerárquico, usualmente en redes grandes.

- El administrador tiene buen conocimiento de la implementación de protocolos de estado enlace.
- La rápida convergencia en la red cuando surge algún cambio es importante.

Protocolos Classful

La característica de estos protocolos es que no envían en sus actualizaciones la máscara de red, esto es debido a que el protocolo classful puede determinar la máscara de red basándose en el primer octeto de la dirección de red, lo anterior basado en la clasificación de direcciones A, B o C que ya se mencionaron en un tema anterior.

Este tipo de protocolos puede ser empleado hoy en día en las redes pero su gran desventaja es que no se puede contemplar para una red que ha sido dividida en varias redes (subnetting), en otras palabras los protocolos classful no soportan VLSM¹⁰.

Protocolos Classless

Los protocolos de ruteo que son classless incluyen en sus actualizaciones la dirección de red con su máscara, hoy en día son los más empleados y las redes ya no usan mucho el término de clases para la asignación de direccionamiento, estos protocolos soportan VLSM lo que ayuda a una mejor administración del direccionamiento.

Basada en las explicaciones anteriores, la tabla 2.9 muestra donde caen los protocolos de ruteo de acuerdo con las clasificaciones vistas previamente.

Protocolos de ruteo	IGP / EGP	Vector distancia / Estado enlace	Classless / Classful
RIP	IGP	Vector distancia	classful

¹⁰ Es el resultado del proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según se adaptan a las necesidades de hosts por subred.

RIPv2	IGP	Vector distancia	classless
RIPng	IGP	Vector distancia	N/A
IGRP	IGP	Vector distancia	classful
EIGRP	IGP	Vector distancia	classless
EIGRP para IPv6	IGP	Vector distancia	N/A
OSPF v2	IGP	Estado enlace	classless
OSPF v3	IGP	Estado enlace	N/A
IS-IS	IGP	Estado enlace	classless
IS-IS para IPv6	IGP	Estado enlace	N/A
BGPv4	EGP	Vector distancia	classless
BGPv4 para IPv6	EGP	Vector distancia	N/A

Tabla 0.9 Clasificación de los protocolos de ruteo.

De la tabla anterior cabe aclarar que los protocolos IGRP y EIGRP son protocolos propietarios, es decir solo equipos de la marca CISCO soportan dichos protocolos.

Métricas de ruteo

Existen casos donde un protocolo de ruteo puede aprender más de una ruta al mismo destino, para seleccionar la mejor trayectoria, el protocolo de ruteo debe ser capaz de evaluar y diferenciar entre las diversas trayectorias disponibles, una “métrica” es usada para este propósito, por ejemplo; dos diferentes protocolos de ruteo podrían seleccionar diferentes trayectorias hacia el mismo destino, lo anterior debido a que cada protocolo considera sus métricas para determinar la mejor ruta.

Algunas de las métricas empleadas por los protocolos de ruteo son las siguientes:

- **Número de saltos:** La mejor ruta es considerada entre menos saltos se requieran para llegar al destino.
- **Ancho de banda:** La mejor ruta es considerada entre más ancho de banda tenga.
- **Retardo (Delay):** La mejor ruta es considerada entre menos delay tenga.
- **Confiabilidad:** La mejor ruta es considerada entre más confiable sea
- **Carga:** La mejor ruta es considerada entre menos carga tenga.
- **Costo:** La mejor ruta es considerada entre menor costo tenga.

Distancia administrativa

Pueden existir situaciones donde mediante dos protocolos de ruteo se puede conocer una ruta diferente para llegar a un destino, es poco común que más de un protocolo de ruteo se implemente al mismo tiempo, pero en las grandes redes se puede dar esta situación, para determinar que protocolo tiene preferencia se emplea lo que se conoce como distancia administrativa, la cual es un valor entre cero y doscientos cincuenta y cinco, mientras menor sea el valor, la ruta tendrá mayor preferencia, es decir una ruta con distancia administrativa de cero será la preferida.

Cabe mencionar que cada Vendor maneja sus propias distancias administrativas por defecto y de hecho dichas distancias pueden ser modificadas por el administrador de la red conforme mejor le convenga, la tabla 2.10 es un ejemplo y muestra las distancias por defecto que maneja CISCO.

Tipo de rutas	Distancia administrativa
Directamente conectadas	0
Estáticas	1
ruta sumariada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Tabla 0.10 Distancia administrativa por defecto de los protocolos de ruteo, CISCO Systems.

OSPF (Open Shortest Path First)

Routers que están empleando un protocolo de estado enlace inundan de información detallada, de toda la red, a todos los demás routers, de tal manera que todos los routers cuentan con la misma información acerca de la red en la que se encuentran. Los routers emplean esta base de datos de estado enlace, mejor conocida como LSDB, para calcular las mejores rutas para cada subred.

OSPF, el protocolo de ruteo de estado enlace más popular, advierte información en mensajes de actualización de varios tipos, dichos mensajes son denominados LSA's. Después de que una

LSA's ha sido propagada, no se vuelven a enviar LSA's hasta después de 30 minutos o antes si es que ocurre un cambio en la red.

Algoritmo Dijkstra

La inundación de información de rutas entre routers no influye en un router para determinar que rutas agrega a su tabla de ruteo, los protocolos de estado enlace deben buscar y agregar rutas en su tabla de ruteo usando el algoritmo conocido como Dijkstra SPF.

La última actualización de OSPF se encuentra especificada en el RFC 2328, en dicha especificación de la IETF se encuentran todos los detalles técnicos del protocolo OSPF.

Un mensaje de OSPF es encapsulado en un paquete IP, hay 5 tipos de mensajes en OSPF los cuales son:

- **Hello:** El mensaje Hello es empleado para crear y mantener adyacencias con otros routers que estén corriendo OSPF.
- **DBD:** Hace referencia a las siglas de Data Base Description, y es un mensaje que contiene de manera abreviada una lista de los estados de enlace que son enviados por otros routers, y sirve para que el router que recibe este mensaje pueda compararlo con su base de datos sobre el estado de los enlaces.
- **LSR:** Hace referencia a Link State- Request, y sirve para que los routers soliciten más información acerca de cualquier dato que venga en el mensaje de DBD relacionado con los estados de los enlaces.
- **LSU:** Hace referencia a Link State-Update, y se emplean para responder a los LSRs, así como para anunciar nueva información. LSU's contienen 11 tipos de LSA's (Link State Advertisement), cabe mencionar que comúnmente al hablar de mensajes LSU's o LSA's se refiere a lo mismo, pero se debe tener claro que un tipo de LSA, está contenido en un mensaje LSU. Los tipos de LSA's son los siguientes:
- **LSAck:** Cuando un mensaje LSU es recibido el router envía un mensaje de notificación para confirmar la recepción de un mensaje LSU.

Tipo de LSA	Descripción
-------------	-------------

1	Router LSAs
2	Network LSAs
3 o 4	Summary LSAs
5	Autonomous system external LSAs
6	Multicast OSPF LSAs
7	Definido para áreas: Not so stubby
8	Atributos externos para BGP
9,10,11	Opaque LSAs

Tabla 0.11 LSA's OPSF.

Como se mencionó anteriormente, el funcionamiento de OSPF está basado en el algoritmo de "Dijkstra shortest path first" (SPF), lo que hace el algoritmo es acumular costos a lo largo de la trayectoria entre la fuente y el destino, y la trayectoria que tenga el menor costo hacia el destino será la óptima.

Normalmente los routers emplean una fórmula para determinar el costo del enlace, basándose en el ancho de banda de la interfaz física.

Tomando como ejemplo a CISCO, que es líder en el mercado de comunicaciones IP, sus routers emplean la siguiente fórmula para determinar el costo de una interfaz.

$$\text{Costo para ospf} = \frac{10^8}{\text{Ancho de banda}}$$

El valor de 10^8 es la referencia por defecto que usan los equipos de CISCO de acuerdo con su literatura, este valor está representando un BW de 100Mbps, es decir que una interfaz Fast Ethernet @100Mbps, tendría un costo de 1. Cabe mencionar que dicho valor de referencia puede ser modificado para interfaces que tengan una velocidad mayor a los 100Mbps, esta modificación se hace configurando manualmente los routers.

Un caso importante en los costos de OSPF se da cuando se da la importación de rutas de otros protocolos de ruteo o de otros procesos de OSPF, para este caso las rutas que aprende OSPF de esta manera se denominan rutas externas, y dichas rutas externas pueden caer en alguna de las siguientes categorías:

- **Tipo 1:** Indica que OSPF acumula los costos de la ruta cuando es propagada por el área de OSPF.
- **Tipo 2:** Indica que OSPF solo toma en cuenta el costo externo, no acumulando los costos de propagación en el área de OSPF.

BGPv4

La última versión del protocolo BGP es la BGPv4 publicada por la IETF en el RFC 4271, como protocolo EGP es ampliamente usado en las conexiones entre los ISPs, sus características principales son mencionadas a continuación:

- BGP es diferente de los protocolos IGP (OSPF, RIP, IS-IS, etc), ya que BGP se enfoca en controlar el anuncio de rutas y seleccionar la ruta óptima entre los sistemas autónomos, mientras que los protocolos clasificados como IGP se encargan de descubrir y calcular rutas.
- BGP utiliza como protocolo de la capa de transporte a TCP enviando sus mensajes al puerto 179, por lo tanto la confiabilidad de BGP es garantizada.
- BGP soporta CIDR.
- BGP únicamente envía mensajes de actualización cuando las rutas se actualizan, lo cual ayuda a reducir la ocupación de ancho de banda cuando BGP redistribuye rutas.
- BGP es un protocolo de vector distancia.
- BGP está diseñado para evitar los conocidos loops de ruteo:
 - Inter-AS: Las rutas de BGP contienen los AS que va atravesando a lo largo de la trayectoria, las rutas que contienen un AS local son descartadas, evitando loops del tipo inter-AS.
 - Intra-AS: BGP no advierte a sus peers las rutas que aprende dentro del AS, de esta manera se evitan loops del tipo intra-AS.
- Para hacer flexible la selección y el filtrado de rutas en BGP se pueden emplear políticas de ruteo.

Aunque BGP en lo general es considerado como un EGP, puede trabajar como iBGP o eBGP. Trabaja como iBGP si este corre dentro del mismo sistema autónomo, y es eBGP si corre entre diferentes sistemas autónomos. Cuando se trata de un eBGP, los vecinos son routers que están directamente conectados en diferentes sistemas autónomos, y cuando se trata de un iBGP los vecinos no necesariamente están directamente conectados, pueden estar alcanzables a través de rutas estáticas o de algún otro protocolo de ruteo, y se requiere que para evitar algún loop de ruteo dentro de un mismo sistema autónomo se tenga entre los vecinos lo que se denomina

BGP full-mesh, es decir, establecer sesiones de BGP entre todos los routers pertenecientes al mismo sistema autónomo.

Un término importante a la hora de estar hablando de BGP es el de "peer", dicho término es acuñado para referirse a los routers que "hablan" BGP entre ellos e intercambian mensajes de BGP, uno es el peer del otro y viceversa. BGP trabaja mediante el envío de mensajes entre los peers, hay 4 tipos de mensajes de BGP los cuales son: open, update, notification y keepalive.

Cuando entre peers de BGP se establece una sesión, pueden existir 6 estados en los que puede estar dicha sesión, dichos estados se dice que pertenecen a la maquina finita de estados de BGP, los estados pueden ser: Idle, Connect, Active, OpenSent, OpenConfirm, y Established. De los cuales durante el establecimiento de una sesión de BGP, los estados más significativos son:

- **Idle:** En este estado, BGP niega todas las solicitudes de conexión, este es el estado inicial de cualquier sesión de BGP.
- **Active:** En este estado, BGP intenta establecer una sesión TCP con el peer. Prácticamente este estado es el intermediario de BGP.
- **Established:** En este estado los peers de BGP pueden intercambiar mensajes de BGP.

Una sesión de BGP se dice que está establecida si en ambos peers se puede observar el estado como "Established".

Atributos de BGP

Un tema importante dentro de BGP es definir qué son los atributos de BGP, normalmente cuando BGP tiene que decidir por la ruta óptima, emplea a los atributos de ruta para poder tomar tal decisión, los atributos ayudan a BGP a filtrar y seleccionar rutas. De manera general los atributos de BGP se clasifican en bien conocidos (Well-Known) y opcionales (Optional), a su vez los bien conocidos se clasifican en mandatorios y discrecionales, y los opcionales en transitivos y no transitivos.

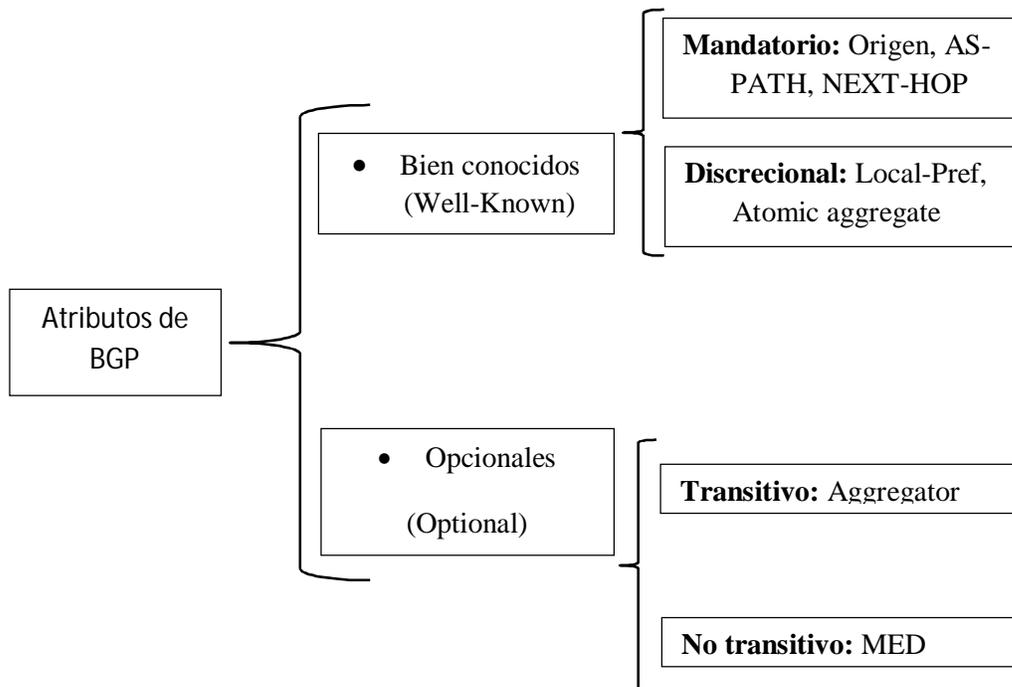


Figura 2.5 Atributos de BGP.

Atributos bien conocidos (Well-Known): Deben ser reconocidos en todas las implementaciones de BGP, son propagados a otros vecinos.

- **Mandatorio:** Deben estar presentes en todos los mensajes update.
 - *Origen:* Este atributo informa a todos los sistemas autónomos en la red como fue que los prefijos fueron aprendidos por BGP, puede tener 3 valores: IGP (i), EGP (e), incomplete (?).
 - *AS-PATH:* Es un atributo que va almacenando todos los sistemas autónomos por los que atraviesa una ruta.
 - *NEXT-HOP:* Indica la dirección IP local del siguiente sistema autónomo para alcanzar cierta red.

- **Discrecional.** Tal vez pueden estar presentes en los mensajes update, pero no necesariamente.
 - *Local-Pref.* Este atributo presenta un valor para determinar entre los routers de un mismo sistema autónomo cuál es la mejor trayectoria para salir del sistema

autónomo, entre mayor sea el valor de local-pref será la ruta preferida. Este atributo solo es intercambiado dentro de los routers del mismo sistema autónomo.

- *Atomic aggregate*. Este atributo indica que el prefijo a propagar es resultado de la sumarización de otros prefijos específicos, lo anterior ayuda a indicar que cierta información ha sido perdida durante la propagación debido a la sumarización y que probablemente dicha ruta no es la óptima.

Atributos opcionales (Optional). Son reconocidos en algunas implementaciones de BGP, pero se espera que no sean reconocidos por todos los routers que están corriendo BGP.

- **Transitivos:** Si no son reconocidos, de cualquier manera son propagados a los vecinos
 - *Aggregator*. El router que realiza la sumarización de rutas, puede agregar este atributo para indicar que él fue el que hizo la sumarización, dicho atributo contiene la IP con la que dicho router establece las sesiones de BGP con sus vecinos.
- **No transitivos.** Si no son reconocidos son descartados.
 - *MED (Multi Exit Discriminator)*. Este atributo es empleado para advertir a vecinos eBGP cuál es la ruta óptima para salir de su sistema autónomo hacia otra red que está dentro de otro sistema autónomo, obviamente esto se da cuando entre dos sistemas autónomos existen dos conexiones, es decir dos posibles rutas, el MED nos ayuda para determinar cuál es la mejor ruta. La ruta que tenga el menor valor en el atributo MED será la preferida.

CAPÍTULO III: ALTA DISPONIBILIDAD EN REDES IP/MPLS.

Introducción

Hasta hace no mucho tiempo, los proveedores de servicios mantenían y operaban por separado sus redes de conmutación de circuitos y conmutación de paquetes, esto debido a que en el inicio de las comunicaciones todo se manejaba en redes de conmutación de circuitos, que se usaba y se sigue usando para servicios de voz, años después vino todo lo que conocemos de IP dando lugar a la conmutación por paquetes, que se empleaba para servicios VPN entre empresas y otros servicios de datos, debido a este surgimiento no planificado, los proveedores de servicio decidieron mantener separadas sus redes de conmutación de circuitos y paquetes, con el paso del tiempo ambas redes fueron creciendo provocando aumento en costos de operación y mantenimiento de las mismas, aunado a lo anterior los proveedores se veían obligados a tener mano de obra especializada tanto para redes de conmutación de circuitos como para conmutación de paquetes. Hoy en día y ya desde hace algunos años los proveedores de servicio han enfocado sus esfuerzos en converger sus servicios en una sola red, lo anterior se pudo plantear debido al surgimiento de MPLS, dicha tecnología permite la convergencia de servicios de capa 2 y 3, haciendo referencia al modelo OSI, desde entonces los proveedores trabajan en el diseño de una red IP/MPLS que les permita la convergencia de todos sus servicios, de esta manera solo tener una red a la que tengan que operar y mantener, sumado a lo anterior todas las ventajas que trae MPLS son otro punto atractivo para pensar en su implementación dentro de cualquier red IP.

Un punto clave al que le deben poner peculiar atención los proveedores de servicios durante el diseño de sus redes es pensar en una red que sea confiable y que cuente con alta disponibilidad, lo anterior porque eso garantiza que en caso de alguna falla los servicios que le brindan a sus clientes no tendrán afectación, y la percepción del cliente acerca de un buen servicio es muy importante para que el proveedor de servicios pueda seguir operando con buenas ganancias económicas y siga teniendo la confianza de sus clientes, una falla en una red de algún proveedor de servicios, por breve que esta sea, representa pérdidas monetarias, debido a que durante el tiempo de falla puede dejar de facturar servicios en tiempo real como por ejemplo llamadas de voz, o puede ser multado por entidades gubernamentales, e inclusive puede ser acreedor a sanciones económicas por parte de sus clientes de acuerdo con los términos del contrato que hayan convenido.

3.1 Alta disponibilidad

El término “disponibilidad de un sistema”, en este caso de un elemento o una red en conjunto, denota la probabilidad (cuyo valor puede ir de 0 a 1), de que el sistema o la red puedan ser usados cuando se les necesita, y alternativamente se emplea también el término “disponible” para describir la fracción del tiempo en la que el servicio está disponible, como punto de referencia un equipo de red de clase carrier, requiere una disponibilidad en el rango de 0.99999¹¹, lo que significa que el servicio debe estar disponible un 99.999% del tiempo. Por otro lado el término “no disponible” denota la probabilidad de que el sistema o la red no pueden ser usados cuando se les necesita o como la fracción de tiempo en el que el servicio no está disponible, lo anterior se refleja en una expresión que mide la falta de disponibilidad en una red, la cual es “tiempo de inactividad por año”, si se hace el cálculo para un año tenemos que la probabilidad de “disponibilidad” es 0.99999 y la probabilidad de la “no disponibilidad” sería 0.00001, considerando que un año tiene 525600 min, el tiempo de inactividad por año permitido para una red carrier sería un máximo de 5.256 min, y si se hace el mismo ejemplo pero en lugar de considerar el tiempo se considera el intento de hacer llamadas, tendríamos que por cada millón de intentos de llamada solo 10 de ellos deberían fallar como máximo, de la manera anterior es como se determinan las expresiones para determinar la “disponibilidad” y la “no disponibilidad” en una red de clase carrier.

La disponibilidad de una red va muy de la mano con el término “confiabilidad” de la red, el cual se puede definir como la probabilidad de que la red pueda trabajar sin falla alguna en cierto lapso, por lo cual se concluye que si se mejora la confiabilidad de la red se mejoraría automáticamente la disponibilidad de la misma, es una relación que es directamente proporcional, y aunque la confiabilidad es un factor clave que influye en la disponibilidad de la red, la tolerancia a fallas de la red es un factor que también afecta directamente a la disponibilidad.

La tolerancia a fallas describe las características de un sistema, en este caso de una red, que cuenta con elementos que en caso de eventos de falla de alguno de ellos, un componente de la red conocido como “backup” puede tomar el trabajo que estaba realizando el elemento en falla, lo anterior da como resultado tener “redundancia” en una red. La tolerancia a fallas puede proveerse por hardware o software, o la combinación de ambas.

¹¹ Número de referencia tomado de (Hussain, 2004).

Se dice que una red es tolerante a fallas si puede mantener un nivel aceptable de servicio durante fallas en la red. Por lo anterior, contar con redundancia en la red se puede reducir el “tiempo de inactividad por año” significativamente, lo que da como resultado mejoría significativa en la disponibilidad de la red, el éxito de una red redundante en gran parte depende de la velocidad en la que se hace la conmutación de servicios entre el elemento en falla y el que está como backup.

En general, la redundancia es un elemento clave en las redes para alcanzar lo que se denomina “alta disponibilidad”, ya que la redundancia no solo protege a la red de fallas en alguno de sus elementos sino que también permite la realización de actividades programadas de mantenimiento o actualizaciones de los elementos de la red, sin afectar el servicio.

3.2 Fundamentos de MPLS

MPLS se mantiene como parte fundamental dentro de muchas redes de proveedores prestadores de servicio, es decir, actualmente MPLS se presenta como tecnología preferida en las redes tipo “carrier”, y lo anterior debido a la capacidad de MPLS de integrar voz, vídeo y datos de una forma común con garantías de calidad de servicio, sumándole las mejoras del rendimiento y disponibilidad que se obtienen con esta tecnología, así como su soporte de una amplia y escalable gama de servicios, debido a la topología que se maneja en redes MPLS, se ofrece a los administradores de red la flexibilidad para desviar tráfico sobre la marcha en caso de fallas de enlaces y congestión de red, además la ingeniería de tráfico y la precisión e inteligencia del enrutamiento basado en MPLS permite tener un mejor control sobre el ancho de banda disponible en la red y reducir los requerimientos de procesamiento a nivel del router, en general MPLS se traduce en una tecnología de red efectiva en costos, rápida y altamente escalable, los beneficios anteriores explican por qué se volvió tan popular la implementación de MPLS en las redes de proveedores de servicios.

En la parte técnica MPLS lo que ofrece es un nuevo paradigma de cómo los routers deben hacer el reenvío de paquetes, en lugar de enviar los paquetes basándose en la dirección IP destino, MPLS define como los routers pueden reenviar paquetes basándose en etiquetas, las cuales están asociadas a otros factores como pueden ser, ingeniería de tráfico, requerimientos de calidad de servicio así como requerimientos privados de los clientes que se conecten a la misma red MPLS.

En el reenvío IP convencional cada router basa su decisión de envío en lo que se conoce como next-hop (siguiente salto) y la información que tiene el router de la interfaz de salida, la información anterior la obtiene de la FIB (Forwarding Information Base), haciendo coincidir la dirección IP destino con algún prefijo de red contenido en la FIB, de la explicación anterior el proceso de reenvío de paquetes puede ser visto en los routers como un mapeo de la dirección IP destino a un next-hop.

Un concepto que vale la pena aclarar antes de entrar de lleno a MPLS es el de FEC (Forward Equivalence Class), este concepto surge cuando se da el caso de que a un router llegan paquetes desde un mismo subconjunto y coincide que el next-hop, para todos los paquetes de dicho subconjunto, es el mismo, y la fuente de los paquetes se vuelve indistinta para el router por lo cual se dice que dichos paquetes forman parte de una clase equivalente de reenvío, mejor conocido como FEC por sus siglas en inglés.

Todo el proceso anterior que realizan los routers en el reenvío convencional de paquetes IP, conlleva a requerir de alto nivel de procesamiento en los routers, lo que impacta en la velocidad de reenvío y recursos usados por los routers para esta tarea, para contrarrestar el proceso anterior se pensó en crear una forma para identificar las diversas FEC's que pudieran existir y asignar cada paquete a una FEC, con lo anterior los routers podrían basar su decisión de reenvío en otra información en lugar de estar buscando hacer coincidir la dirección IP destino con algún prefijo contenido en su FIB, una manera que se ideó para simplificar el proceso convencional de reenvío fue agregar información extra en el encabezado IP, dicha información adicional se le puso el nombre de "etiqueta", de la idea anterior es como surge MPLS ya que es la tecnología que permite tomar la decisión de reenvío basado en la información contenida en la etiqueta.

Una etiqueta es un valor de longitud fija (20 bits), que identifica a una FEC en particular, la asignación de un paquete IP a una determinada FEC se determina comúnmente por la dirección IP destino que lleva el paquete aunque cabe la posibilidad que sea determinado por otro factor.

El formato del encabezado MPLS es el siguiente:

20 bits	3	1	8
Label	EXP	S	TTL

Figura 3.1. Encabezado MPLS.

Donde;

Label: Es el campo de la etiqueta, donde con un valor decimal representa el identificador del LSP (Label Switch Path).

EXP: De la abreviación de "experimental", empleado para el marcado de QoS.

S: Del inglés "stack", sirve para el apilado estático de etiquetas, cuando S=0 indica que hay más etiquetas añadidas en el paquete, cuando S=1 se indica que dicha etiqueta es la única que precede al encabezado IP.

TTL: Empleado para el mismo propósito que el campo TTL del encabezado IP.

A un router que soporta MPLS se le conoce como LSR (Label-Switching Router), y para solicitar o distribuir etiquetas, los LSR's usan procesos comúnmente referidos como protocolos de distribución de etiquetas, como pueden ser: LDP (Label Distribution Protocol), BGP y RSVP (Resource Reservation Protocol), los cuales se explicarán un poco más adelante.

Una red MPLS consiste de la interconexión de varios LSR's, dichos LSR's pueden caer en las siguientes variantes:

LSR (Label-Switching Router)	Cualquier router que puede poner o quitar etiquetas de un paquete, o que simplemente reenvía paquetes con etiquetas.
Edge LSR	Router que se encuentra en la frontera de la red MPLS, lo que significa que pone y quita etiquetas.
Ingress Edge LSR	Es aquel router que para un paquete en particular que no viene etiquetado, lo etiqueta.
Egress Edge LSR	Es aquel router que recibe un paquete etiquetado y se encarga de remover todo el etiquetado referente a MPLS y reenvía el paquete ya sin etiquetas.

Tabla 3.1. Variantes de LSR's.

La secuencia de LSR's por los que pasa un paquete, desde el ingreso E-LSR hasta el egress E-LSR se conoce como LSP, y cabe mencionar que dicho LSP es unidireccional, por lo tanto para tráfico bidireccional se requiere de un LSP para cada dirección, el LSP se puede establecer de 2 maneras, una estática y otra dinámica, la dinámica es haciendo uso de la información proporcionada por los protocolos de ruteo, la estática como su nombre lo sugiere es cuando mediante configuración en los edge LSR's se especifica explícitamente el path que seguirá dicho LSP, como se mencionó anteriormente para establecer LSP's, MPLS utiliza protocolos de distribución de etiquetas como son; LDP, BGP y RSVP, en particular para los LSP's formados de manera dinámica se emplea LDP y para los LSP's formados de manera estática se emplea RSVP.

En contraste con el reenvío de paquetes IP tradicional, el cual reasigna a cada paquete a una nueva FEC en cada salto, MPLS solo hace la asignación de FEC una sola vez, esto es en el ingreso edge LSR. Después de que el paquete es mapeado a una FEC en particular, todos los LSR's por los que cruza el paquete solo revisan la información de la etiqueta para tomar decisiones de reenvío, es por lo anterior que MPLS evita la búsqueda de direcciones IP en cada salto que tiene el paquete, con lo cual se mejora la velocidad de reenvío y se disminuye el procesamiento requerido en los routers, pero los verdaderos beneficios de MPLS son las aplicaciones que pueden habilitarse cuando una red está basada en MPLS, si solo se habilita MPLS en una red, realmente no tiene gran sentido ni mejoría en la red, los beneficios vienen ya que con MPLS las siguientes aplicaciones se pueden implementar: VPNL3, VPNL2, Traffic Engineering (TE), Fast ReRouting (FRR), estas aplicaciones avanzadas son las que hacen ver a MPLS una tecnología atractiva para construir redes seguras y escalables.

IP over MPLS. Se refiere a la forma natural de aplicar MPLS en una red, es decir indica el reenvío de paquetes capa 3 sobre LSP's que se han establecido usando LDP.

Traffic Engineering (TE). Permite el establecimiento de LSP's a través de trayectorias explícitas, las cuales pueden ser derivadas por la especificación directa del usuario o por protocolos de señalización basadas en la información proporcionada por los protocolos de ruteo.

Fast ReRoute (FRR). Es un mecanismo que provee de la creación de un túnel secundario, de tal manera que si falla el túnel primario el tráfico puede conmutar al túnel secundario inmediatamente, lo que garantiza que no se afecta el flujo de tráfico en caso de alguna falla en el path principal.

Layer 3 Virtual Private Network (L3VPN). Esta aplicación permite a los carriers compartir su red de transporte MPLS entre varios de sus clientes, lo más importante es que el carrier tiene tráfico de diferentes clientes pasando por su red, pero ese tráfico no se mezcla con el de otro cliente. MPLS VPN utiliza LDP o RSVP para establecer los LSP's entre los edge LSR's y emplea BGP para la distribución de las etiquetas respectivas a cada uno de los prefijos de red del cliente. Haciendo una analogía esta aplicación les permite a los clientes ver la red MPLS del carrier como un solo router, donde en una de sus interfaces conectan una parte de su red y en otra de sus interfaces, la parte lejana de su red a la que se quieren conectar.

Layer 2 Virtual Private Network (L2VPN). Esta aplicación permite la emulación de circuitos virtuales para transportar tramas (Ethernet, FR, ATM, y PPP) a través de la red MPLS, la información de los circuitos virtuales es intercambiada usando LDP, haciendo una analogía de esta aplicación, es como si los clientes vieran a la red MPLS del carrier como un solo switch virtual que une dos sitios a nivel capa 2 aunque geográficamente las conexiones puedan estar distantes, así, para los clientes sería como estar conectados a la misma LAN. En otros textos L2VPN también se conoce como AToM (Any Transport over MPLS).

3.3 Estrategias para lograr la alta disponibilidad en redes IP/MPLS

La confiabilidad y disponibilidad de una red IP/MPLS puede ser analizada desde 2 puntos de vista, el de servicio y el de red, el primero de ellos se refiere a satisfacer las expectativas del cliente en cuanto a la calidad y disponibilidad del servicio así como el cumplimiento de ciertas LSAs que se hayan acordado entre el carrier y el cliente, el segundo punto de vista se refiere a como poder reducir los costos de equipamiento y operación, pero hay que tomar en consideración que la principal tarea de una red es proveer de servicios a los usuarios, entonces los requerimientos de confiabilidad y disponibilidad son resultado del análisis hecho desde el punto de vista de servicio. Por lo anterior se podría resumir que un buen diseño de red debe satisfacer el objetivo de proveer servicios con alta confiabilidad y disponibilidad al menor costo operativo y de equipamiento.

Una red de conmutación de paquetes consiste de la interconexión de elementos de red como pueden ser; routers, switches y equipos de transporte, la confiabilidad de la red dependerá de la confiabilidad y disponibilidad de estos elementos de red, de hecho la tolerancia a fallas en elementos de red es crucial para cumplir con las SLAs acordadas entre los clientes y los

proveedores de servicio. Un elemento de red que es considerado de clase carrier debe cumplir con los siguientes requerimientos:

- Una falla de hardware en algún componente del equipo no debe dar por resultado pérdida o degradación del tráfico del usuario, tampoco se puede tolerar la pérdida del plano de control o de la administración del equipo.
- La falta de operación de un equipo no debe superar los 5.256 min por año.¹²
- Las tarjetas de servicio, conmutación y controladoras deben ser redundantes, es decir tener tarjetas trabajando en modo master y backup.
- El equipo debe ser capaz de recobrar el servicio ante fallas en los enlaces o en algún nodo.

Los requerimientos mostrados anteriormente regularmente se logran con una combinación de técnicas de tolerancia a fallas a nivel de red y a nivel de nodo.

TÉCNICAS DE TOLERANCIA A FALLAS A NIVEL DE NODO.

Mitigando fallas no planeadas relacionadas con hardware

La técnica más efectiva para reducir el impacto en el servicio en caso de alguna falla de hardware es contar con tarjetas redundantes en el equipo (Tarjetas de servicio, controladoras, fuentes, etc.), el nivel de redundancia en los equipos regularmente se expresa de la siguiente manera en sus especificaciones técnicas:

(1:N): Indica que hay un componente de respaldo por cada N componentes activos.

(1:1): Indica que hay un componente de respaldo por cada componente activo.

(1+1): Esto indica que los 2 componentes trabajan simultáneamente pero si uno de ellos falla el otro es capaz de soportar el trabajo que estaba haciendo el componente que falló.

Mitigando fallas no planeadas relacionadas con software

Aunque los equipos cuenten con redundancia en hardware, puede resultar ineficiente si no se cuenta con mecanismos que brinden redundancia al plano de control, los dos elementos más importantes que constituyen el software de un router son los protocolos de plano de control IP y los de MPLS. Los componentes del plano de control IP son protocolos de ruteo IP como

¹² Información basada en el contenido de (Hussain, 2004).

pueden ser OSPF, IS-IS, BGP, por otro lado, los componentes de plano de control MPLS, son protocolos de señalización como LDP, RSVP-TE y BGP.

Las tablas de reenvío IP y MPLS son referidas comúnmente como plano de reenvío, por la naturaleza de la criticidad de los tiempos en las operaciones de reenvío, generalmente las funciones de este plano son distribuidas en las tarjetas de servicio para mejorar el desempeño de reenvío. En contraste las tareas del plano de control son menos críticas y generalmente residen en la tarjeta controladora, también conocida como tarjeta central de procesamiento, se puede decir que el plano de control es como el cerebro del router ya que es la parte que brinda la inteligencia al router, es por eso que estas tarjetas normalmente cuentan con redundancia del tipo 1:1.

El comportamiento que existe en la conmutación o reinicio del plano de control resulta en la interrupción del servicio y pérdidas en el flujo del tráfico, lo anterior debido a que aunque la controladora tenga redundancia a nivel de hardware el plano de reenvío también se reinicia.

De lo anterior se concluye que no importa que se tenga redundancia de hardware se seguirá teniendo afectación en el servicio en caso de falla, para lograr minimizar el impacto se han creado varias técnicas para llevar el impacto del servicio al mínimo, dichas técnicas se reducen a 3 enfoques diferentes, los cuales se plantean en la siguiente tabla.

Descripción	Ventajas	Desventajas
Enfoque 1: Iniciar 2 copias idénticas del software del plano de control en las 2 controladoras (Active, Stand by), las dos instancias ejecutan de manera independiente	conmutación transparente para los vecinos, no se requieren cambios en los protocolos de control IP/MPLS	Procesamiento extra de la carga debido a la replicación de los paquetes de control necesariamente se requieren iniciar las 2 controladoras al mismo tiempo. No permite hacer upgrades o downgrades de software
Enfoque 2: Es similar al enfoque 1, la diferencia radica en que las instancias no se ejecutan de manera independiente sino en conjunto y de manera sincronizada	Tiempo rápido de recuperación, no hay necesidad de cambios en los protocolos.	Diseño complejo de la sincronía entre las instancias. No permite hacer upgrades o downgrades de software
Enfoque 3: Iniciar 2 copias idénticas del software del plano de control en las 2 controladoras (Active, Stand by), la instancia que está en stand by mantiene un estado parcial.	permite el upgrade de software	Necesidad de reestablecer sesiones y recuperar la información del estado del plano de control.

Tabla 3.2 Enfoques de técnicas para reducción de impacto en el servicio en caso de falla.

De los enfoques mencionados anteriormente cada proveedor de equipos maneja esta parte de manera particular, no hay un estándar que manejen todos los equipos, pero al final el resultado que ofrecen todos los proveedores de equipos es la menor afectación en caso de la conmutación de alguna de sus controladoras.

TÉCNICAS DE TOLERANCIA A FALLAS A NIVEL DE RED.

Mitigando fallas en la red ocasionadas por fallas en nodos o enlaces

El impacto causado por fallas en enlaces o en todo el equipo es mitigado empleando esquemas de protección/re-routing multicapa, en el caso de MPLS una solución es el TE-FRR (Traffic Engineering Fast Re-route), el cual permite el establecimiento de 2 LSP's, uno primario y uno de backup, otros esquemas de protección para la parte IP son el VPN FRR, IP-FRR, VRRP, OSPF

GR, IS-IS GR, BGP GR. Mientras que para MPLS se pueden también encontrar técnicas como BGP GR, LDP GR.

3.4 Descripción de técnicas para mitigar afectación en caso de fallas.

Como se ha comentado anteriormente, los proveedores de equipos han trabajado en los últimos años para crear protocolos que ayuden a mitigar la afectación de servicios en casos de falla, a continuación se describen algunas de esas técnicas.

IP FRR (Internet Protocol Fast Re-Route). En redes IP tradicionales cuando ocurre una falla en la capa inferior del enlace, la interfaz física del router pasa a estado "down", eso indica a las capas superiores iniciar el proceso de recalculación de rutas y hacer una actualización a sus tablas de ruteo, todo este proceso para seleccionar una ruta disponible puede llevar varios segundos, para servicios que no toleran alto delay y altas tasas de pérdidas de paquetes, el tiempo de convergencia de los protocolos de ruteo es intolerante ya que eso podría ocasionar interrupciones en el servicio. IP FRR asegura que el sistema de reenvío conmute inmediatamente a la ruta que queda disponible, lo cual hace que la interrupción del servicio en caso de falla sea imperceptible.

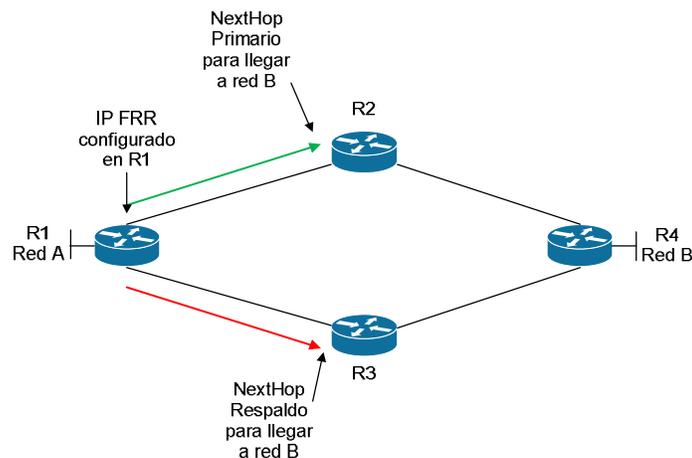


Figura 3.2. Técnica IP Fast Re-Route.

VRRP. Es un protocolo tolerante a fallas, y en general lo que hace es agrupar varios routers en un solo "router virtual"¹³, en el caso de que el router que está como primario falle, algún router restante del grupo puede tomar el procesamiento del tráfico inmediatamente lo cual asegura la continuidad y confiabilidad de una comunicación.

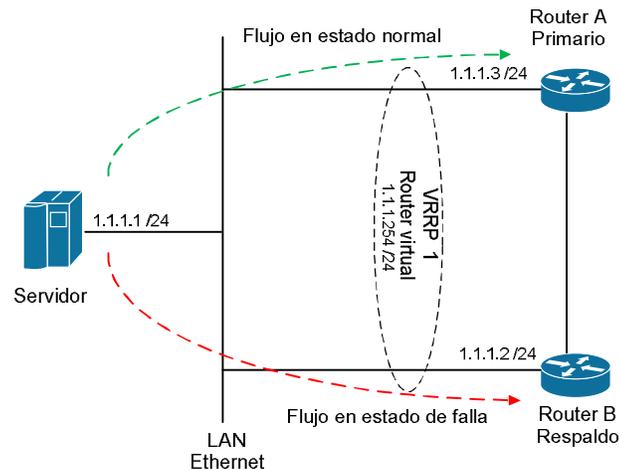


Figura 3.3. Técnica VRRP.

GR. Es una tecnología que se emplea para asegurar el reenvío normal de tráfico y NSF durante el reinicio de protocolos de ruteo, dichos protocolos llegan a reiniciarse cuando las controladoras de los equipos conmutan.

En modo GR, el plano de reenvío continúa con el envío de datos una vez que ha ocurrido un reinicio, y las acciones del plano de control, como el restablecimiento de las vecindades y el cálculo de rutas, no afectan al plano de reenvío. De esta manera la interrupción del servicio causada por la inestabilidad del ruteo es prevenida con lo que la confiabilidad de la red mejora.

Cabe mencionar que esta tecnología se maneja por separado para cada protocolo de ruteo; OSPF GR, IS-IS GR, BGP GR, LDP GR.

TE FRR. Es un mecanismo de protección local para proteger CR-LSP's contra fallas en enlaces o nodos, la idea de este mecanismo es la creación de CR-LSP's bypass para reenviar por allí el tráfico en caso de que el CR-LSP primario falle, las fallas que pueden afectar al CR-LSP primario

¹³ Es un dispositivo abstracto administrado con VRRP que funciona como puerta de enlace en una red LAN compartida

son: falla en enlace o falla en nodo, la creación de los CR-LSP's de bypass puede ser de manera manual o automática.

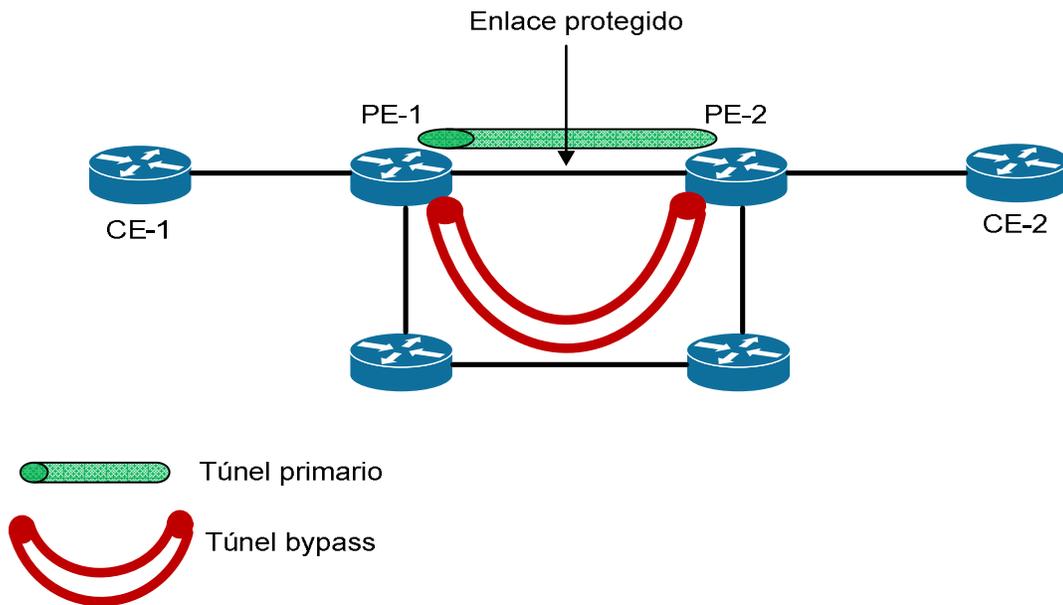


Figura 3.4. TE FRR protección de enlace.

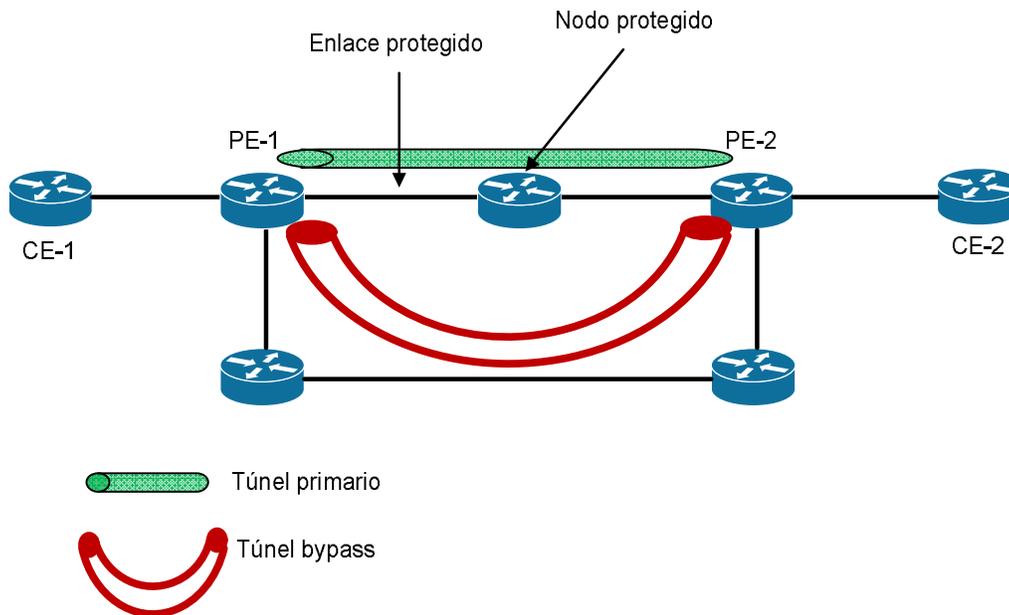


Figura 3.5 TE FRR protección de nodo.

VPN FRR. Actualmente muchos proveedores de servicios emplean VPN's en MPLS para aislar el tráfico de los diferentes servicios que cruzan por su red, si algo ocurre en la red el túnel por el que se establece la VPN se pierde y obviamente se afecta el tráfico, para evitar lo anterior se pensó en tener 2 rutas con un "path" totalmente diferente para cada VPN, emplear VPN FRR ayuda a conmutar rápidamente al túnel que se encuentra como backup, cuando se detecta que el túnel primario no está disponible, el plano de reenvío comienza a utilizar el túnel backup para reenviar tráfico, antes de que las rutas converjan en el plano de control, en general se dice que VPN FRR protege a los PE's ya que la solución de VPN FRR se presenta en escenarios donde los CE's tienen conexiones con dos PE's diferentes (dual-homed), en este escenario de dual-homed TE FRR no puede ayudar mucho cuando un PE falla, es por eso que surge VPN FRR como solución para conmutación rápida de tráfico en caso de falla en un PE, en la siguiente figura se muestra el escenario base donde aplica VPN FRR.

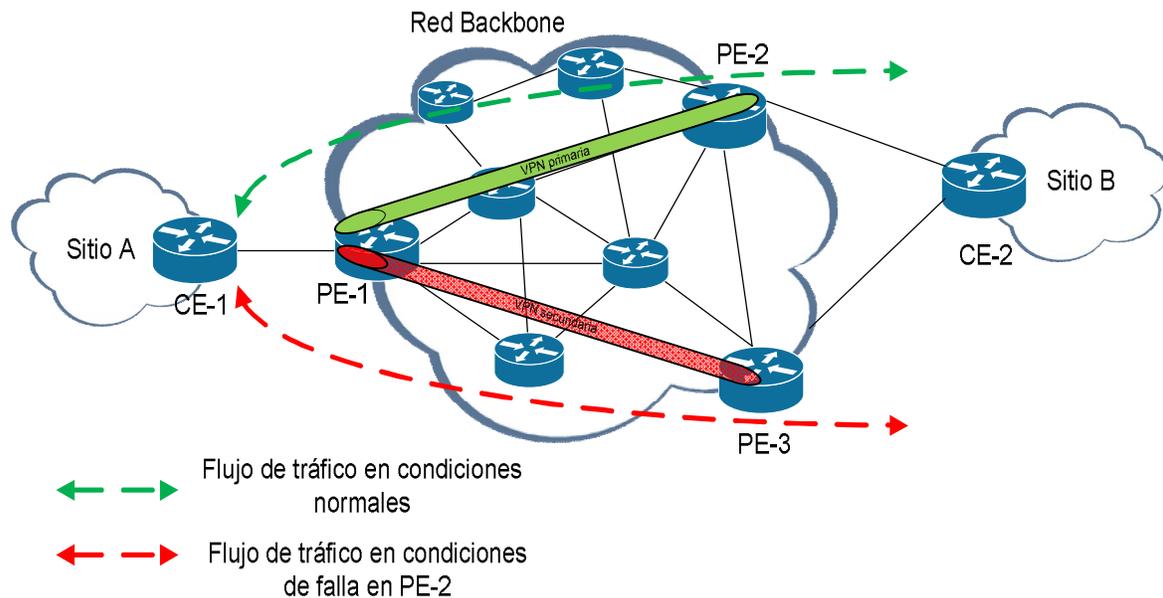


Figura 3.6. VPN FRR.

BFD. Es un mecanismo que detecta de manera rápida fallas en la comunicación entre 2 sistemas, e informa inmediatamente a los protocolos de capas superiores sobre la falla. Existen varios mecanismos detectores de fallas pero BFD se desarrolló para ser la mejor opción entre los mecanismos de detección de fallas, de manera general lo que hace BFD es crear una sesión entre los 2 sistemas que quiere monitorizar, si dicha sesión se pierde, BFD inmediatamente notifica a los protocolos de capas superiores para que estos ejecuten las acciones pertinentes antes de que se experimente interrupción en el servicio.

CAPÍTULO IV: ANÁLISIS Y DISEÑO DE LA RED.

Introducción

Tomando en cuenta el panorama teórico mostrado anteriormente se propone una solución para una compañía "X" de telefonía celular. Tomando como ejemplo uno de los servicios más brindados en la actualidad por los prestadores de servicios, la propuesta de diseño abarca solo la solución para brindar servicio de Internet, aunque cabe mencionar que dicha solución puede ser aplicada a una gran variedad de servicios.

El diseño mostrado se enfoca específicamente a la solución para la parte de datos IP y de los flujos de datos a partir de ser recibidos por parte de los equipos terminales a través de los equipos de PS.

4.1 Diseño

4.1.1 Topología física

Una red confiable debe contar con al menos dos puntos de presencia, localizados en dos lugares distintos apartados geográficamente, esto para poder implementar redundancia geográfica en caso de que suceda alguna eventualidad del tipo natural o accidente por el cual el lugar donde se encuentran los equipos que ofrecen servicios a una región determinada sean devastados total o parcialmente.

Por lo anterior se propone una topología basada en dos ciudades, pudiéndose ampliar a más de dos; siendo las topologías espejo una de la otra. Véase figura 4.1

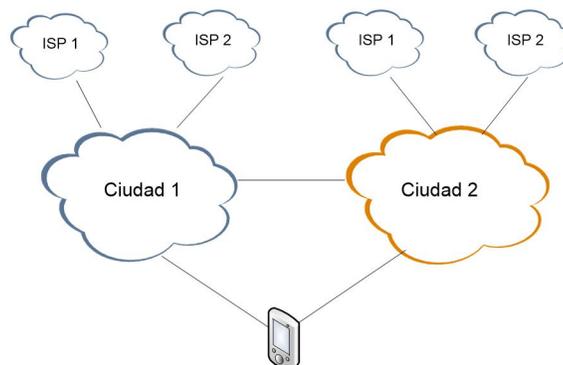


Figura 4.1. Redundancia geográfica.

Teniendo lo anterior en cuenta, si sucediera un siniestro en alguna de las ciudades, el servicio seguiría ofreciéndose a través de la otra ciudad.

Así, siendo la topología de ambas ciudades un espejo de la otra, procederemos a desglosar solo una de ellas.

La topología en cada ciudad cuenta con redundancia física local, es decir, se tienen dos equipos que se respaldan uno al otro en cada subsistema en caso de que alguno se dañe o deje de funcionar. Con lo cual encontramos que se tiene una red espejo local para redundancia dentro de la misma ciudad.

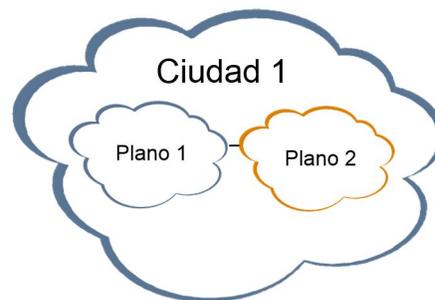


Figura 4.2. Redundancia Local.

Así dentro del diseño se cuenta con cuatro subsistemas los cuales se desglosan como se muestra en la siguiente figura mostrando para cada subsistema los dos equipos que componen la redundancia local.

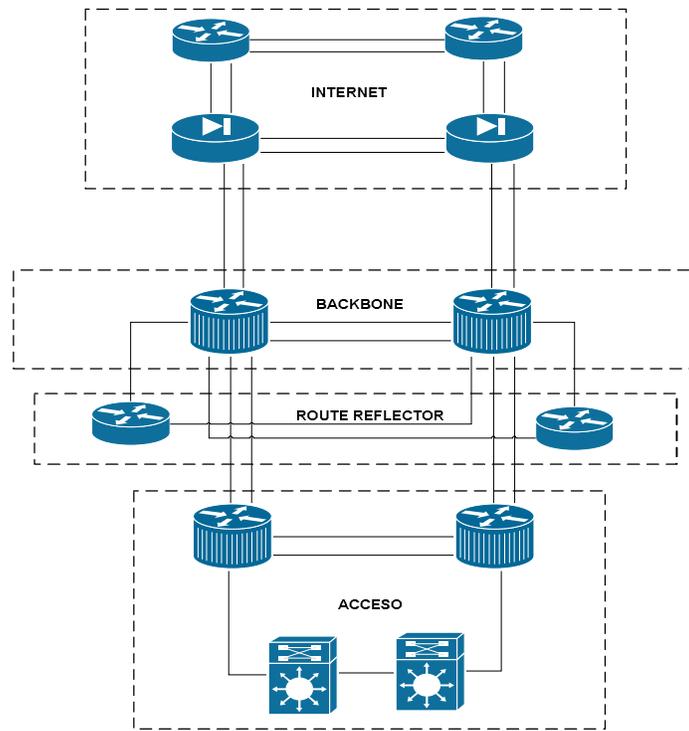


Figura 4.3. Desglose de subsistemas.

4.1.1.1 Acceso

Este subsistema está compuesto por dos routers y dos switches capa 3.

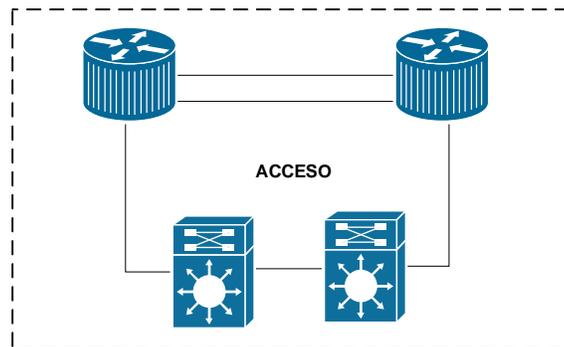


Figura 4.4. Subsistema de acceso.

Los dos switches son usados como punto de interconexión por lo cual deben contar con gran capacidad de puertos y de acuerdo con el número y el tipo de estos, la capacidad de conmutación deberá ser calculada; es recomendada la alta disponibilidad a nivel de hardware.

Los tipos de puertos pueden variar de acuerdo con las capacidades de los puertos de las plataformas que se conectan a ellos.

En cuanto a los dos routers al no ser estos los puntos de interconexión, deberán contar con pocas interfaces pero de gran capacidad; interfaces 10 Gigabitethernet se recomienda para ser conectados a los switches ya que a través de estas interfaces pasará todo el tráfico hacia el exterior recolectado por los dos switches. Debido a que estos routers tendrán que mantener la tabla de ruteo de toda la red se recomienda contar con una buena capacidad de procesamiento y memoria RAM además de contar con alta disponibilidad a nivel de hardware.

4.1.1.2 Backbone

Está compuesto por dos routers de gran capacidad en cuestión de procesamiento y de memoria, al igual que para el acceso se recomienda alta disponibilidad a nivel de hardware.

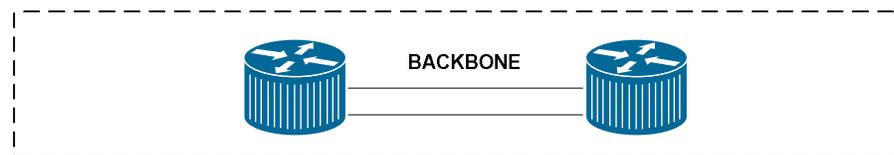


Figura 4.5. Subsistema de backbone.

La densidad de puertos debe ser lo suficiente para poder conectarse hacia los demás subsistemas más un margen de crecimiento, en cuestión de capacidad, se recomiendan interfaces 10 Gigabit Ethernet ya que es en este punto donde cruza la mayor cantidad de tráfico al ser este, el punto de convergencia de todos los demás subsistemas y punto también de interconexión con otras ciudades.

4.1.1.3 Route Reflector

Compuesto por dos routers conectados cada uno a su respectivo router de backbone, su densidad de puertos debe ser pequeña y su capacidad de nivel medio, interfaces fast ethernet puede usarse ya que la cantidad de tráfico no es grande sin ser por esto menos importante.

Ya que son estos equipos de vital importancia en la red, es muy importante contar con alta disponibilidad a nivel de hardware y una capacidad de procesamiento media ya que estos almacenan la tabla de ruteo de ambas ciudades para todas las instancias VRF.

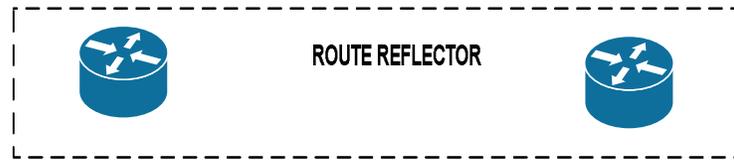


Figura 4.6. Subsistema de route reflector.

4.1.1.4 Internet

Este subsistema está compuesto por dos routers y dos firewall para dar salida a Internet a los usuarios de la red, la densidad de puertos de ambos debe ser la necesaria para poder conectarse a los demás elementos de red más un margen de crecimiento, para los routers conectados a los ISP la capacidad de procesamiento y memoria debe ser grande ya que ellos almacenarán la tabla completa de Internet para un ruteo óptimo, además de que a través de ellos saldrá todo el flujo destinado a Internet. En cuestión de los firewalls se recomienda gran capacidad de procesamiento y memoria debido a que estos elementos además de encargarse de encaminar el tráfico deben proteger la red ante posibles ataques del tipo aplicativo y del tipo DDoS por medio de políticas de seguridad, manteniendo además de esto una tabla de sesiones para cada conexión de cada usuario hacia la nube de Internet por lo que la capacidad de número de sesiones debe ser también alto.

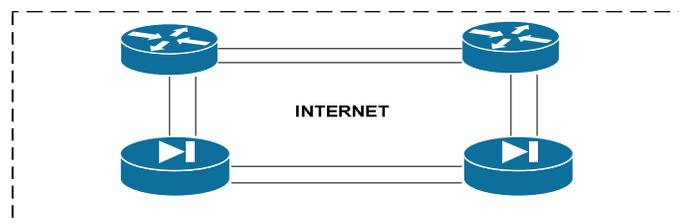


Figura 4.7. Subsistema de Internet.

4.1.2 Topología lógica

La red a nivel lógico se encuentra separada en varias capas que se sirven unas de las otras para proveer los servicios ofrecidos al cliente.

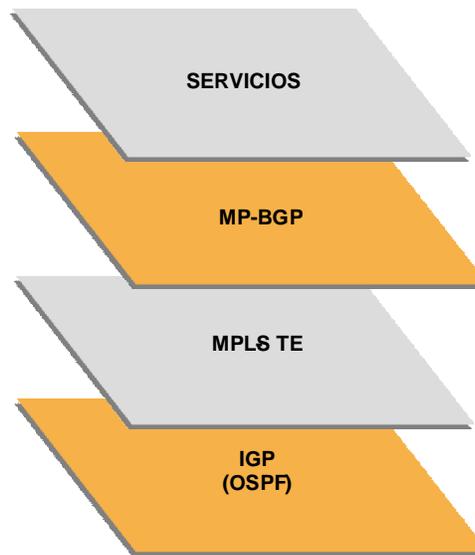


Figura 4.8. Capas lógicas.

A continuación se desglosa la red por subsistema mostrando los protocolos usados en cada uno de ellos.

4.1.2.1 Subsistema de acceso

Este subsistema tiene como tarea recibir las plataformas y equipos (PS, CS) que necesitan conectarse a la red MPLS así como añadirlos a la VRF correspondiente de acuerdo con el servicio proporcionado.

Los switches funcionan completamente en la capa de enlace del modelo OSI y solo funcionan a nivel capa de red para la operación y mantenimiento ya que necesitan tener una IP asociada a ellos de administración para poder ser gestionados.

Los mismos switches se encuentran fragmentados en VLAN's, las cuales se asignan a cada plataforma para aislarla del resto. Ya que la mayoría de plataformas cuentan con tarjetas redundantes, cada una de ellas se conecta a un switch diferente asociando el puerto a la misma VLAN asignada a la plataforma en cada switch.

Con el fin de permitir la comunicación de las VLAN usadas en ambos switches, entre los dos switches existe un troncal que usa el protocolo 802.1Q para etiquetado de las tramas Ethernet.

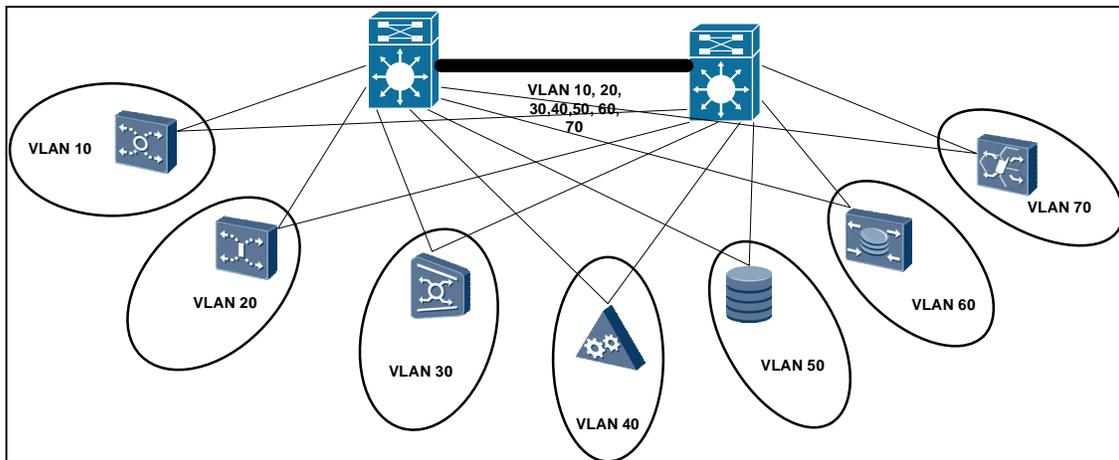


Figura 4.9. Segmentación en VLAN de switches de acceso.

Los dos routers funcionan como PE para la red MPLS recibiendo el tráfico de los dos switches a nivel capa de red y asociando cada flujo por medio de subinterfaces a las distintas VRF.

Los protocolos de alta disponibilidad implementados en este subsistema son:

- VRRP + BFD
- IP FRR
- VPN FRR + BFD

4.1.2.1.a VRRP

Como protocolo de alta disponibilidad a nivel de acceso se usa VRRP el cual funciona entre ambos routers para cada VLAN pasando a través de los switches de forma transparente para cada VLAN.

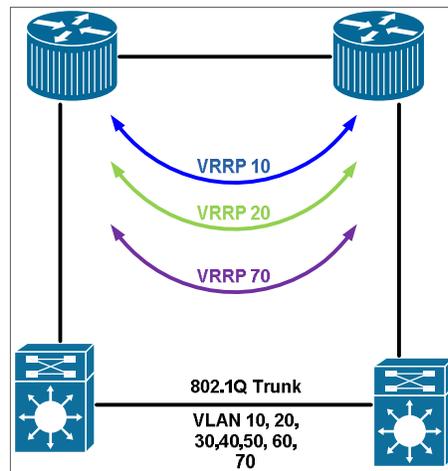


Figura 4.10. VRRP en routers de acceso.

Hacia las plataformas, los dos routers son vistos como un solo gateway para los equipos que no cuentan con capacidad de protocolos de ruteo dinámico y como vecinos OSPF para los equipos con capacidades de ruteo dinámico.

Con VRRP cuando algún router falle, el otro al no recibir más paquetes de señalización de VRRP dará por hecho que el router no está disponible y el tomará el puesto de MASTER asociándose a él mismo la IP virtual del grupo VRRP.

Con el fin de hacer más rápida la detección de alguna falla, es posible crear una sesión BFD entre ambos routers, así con este protocolo la detección es más rápida y por tanto la pérdida de información mínima.

4.1.2.1.b IP FRR

Entre los dos routers existe un enlace capa 3 el cual se usa para permitir alta disponibilidad por medio del protocolo IP FRR, a continuación se muestra el principio de funcionamiento.

En condiciones normales el flujo sigue la trayectoria en verde llegando por plano 1 y por plano 2.

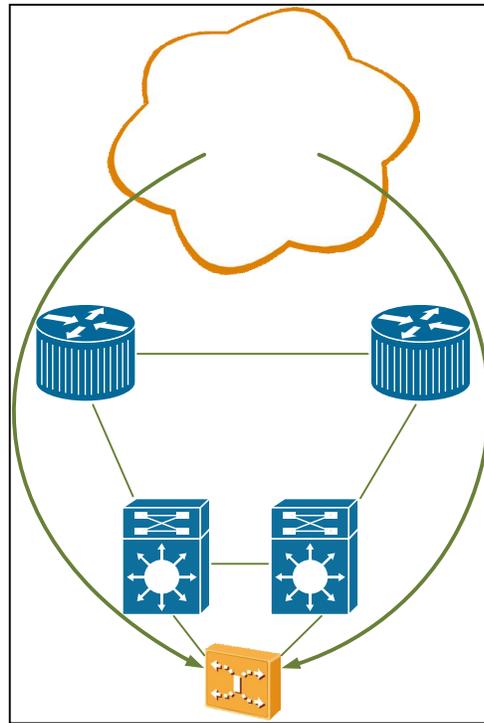


Figura 4.11. Flujo de datos en condiciones normales.

Sin embargo cuando alguna de las interfaces entre los router y los switches cambia a estado DOWN/DOWN, el tráfico es desviado al otro plano inmediatamente (trayectoria en rojo) mientras el IGP converge, esto con el fin de evitar, en lo posible, la pérdida de tráfico y servicio.

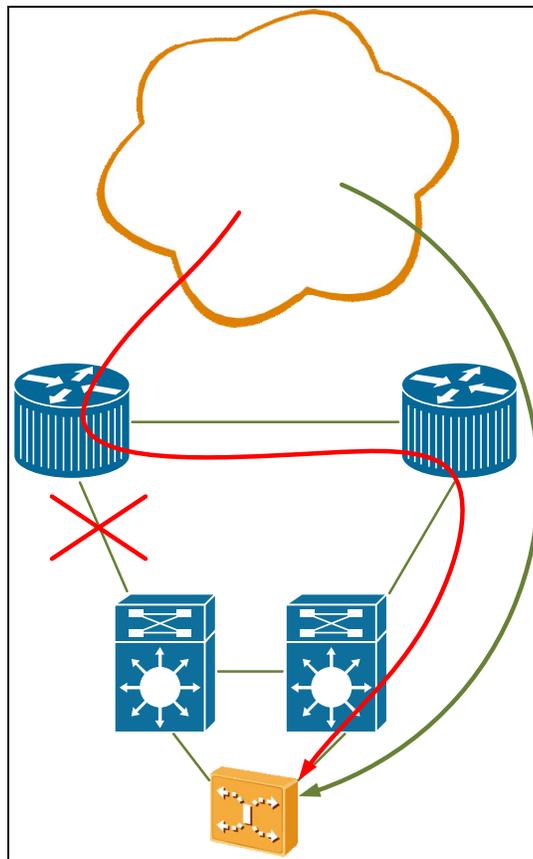


Figura 4.12. IP FRR - Flujo de datos en caso de falla.

Con lo anterior se tiene un desvío del tráfico inmediato, sin necesidad de esperar la convergencia del IGP lo cual nos da un tiempo de respuesta inmediato que resulta en mínima pérdida de información.

4.1.2.1.c VPN FRR

Con el fin de brindar protección extremo-a-extremo se implementa la solución VPN FRR la cual consiste en tener dos posibles NEXT-HOP en la tabla de ruteo de BGP hacia un destino, con uno de ellos como backup, así, en caso de que uno de los PE falle el tráfico se puede desviar a la IP NEXT-HOP del PE secundario.

Para lograr esta tarea y al tener un esquema de dual-homed CE, es necesario tener dos diferentes RD en MP-BGP; uno por cada plano; al momento de advertir los prefijos aprendidos del CE a la red MPLS.

Con esto los PE remotos tienen la capacidad de añadir el mismo prefijo con dos NEXT-HOP diferentes dentro de la tabla de ruteo BGP, ver figura 4.13.

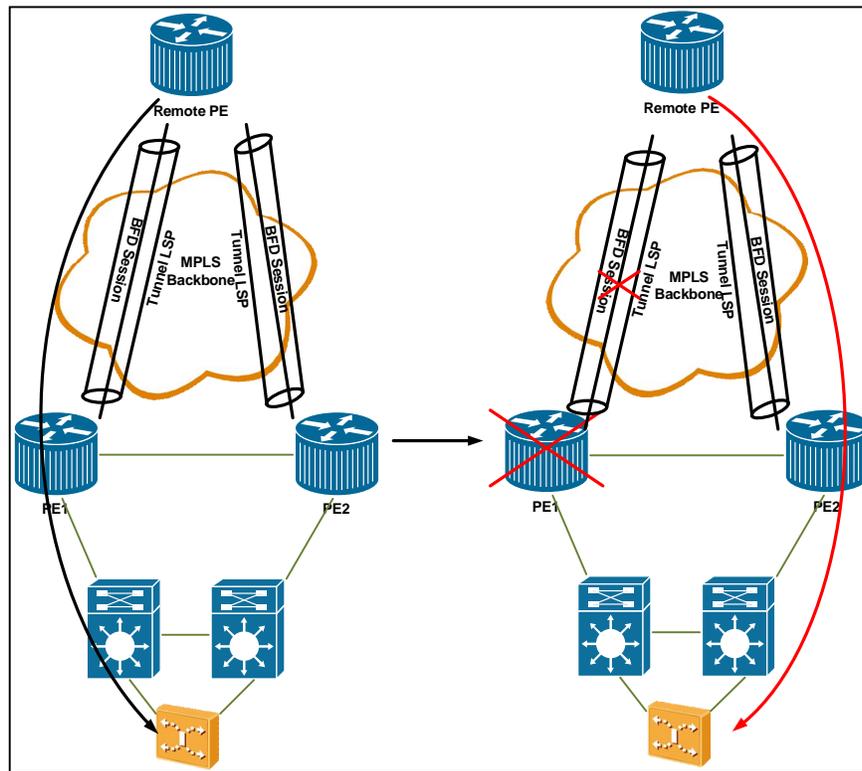


Figura 4.13. Funcionamiento de VPN FRR.

Con el fin de mejorar el tiempo de respuesta, es posible generar una sesión de BFD entre el PE remoto y los PE locales con el fin de monitorizar el status del PE; la sesión BFD pasa a través del LSP creado entre el PE remoto y el PE local. De esta forma cuando la sesión BFD falla, BGP da por hecho que el PE está inaccesible y usa su NEXT-HOP de backup.

4.1.2.2 Subsistema de backbone

Este subsistema es el encargado principalmente de interconectar ciudades y de recibir la ruta de default hacia Internet generada por el proveedor de servicios y advertida por los equipos del subsistema de ISP y/o subsistemas que requieran salir a Internet.

En este subsistema es necesario aplicar políticas de ruteo para marcado de comunidades en BGP para marcar la ruta de default recibida del subsistema de ISP, esto con el fin de balancear el tráfico hacia Internet en caso de falla.

Estos dos equipos por ciudad son de los elementos más importantes y podríamos llamarles el backbone de la red ya que si estos dos equipos fallan, el servicio entre ciudades es afectado completamente.

Entre este subsistema y el de acceso se corre un IGP; para el escenario propuesto en esta tesis, el IGP usado es OSPF, el cual sirve de fuente de información para el protocolo MPLS TE.

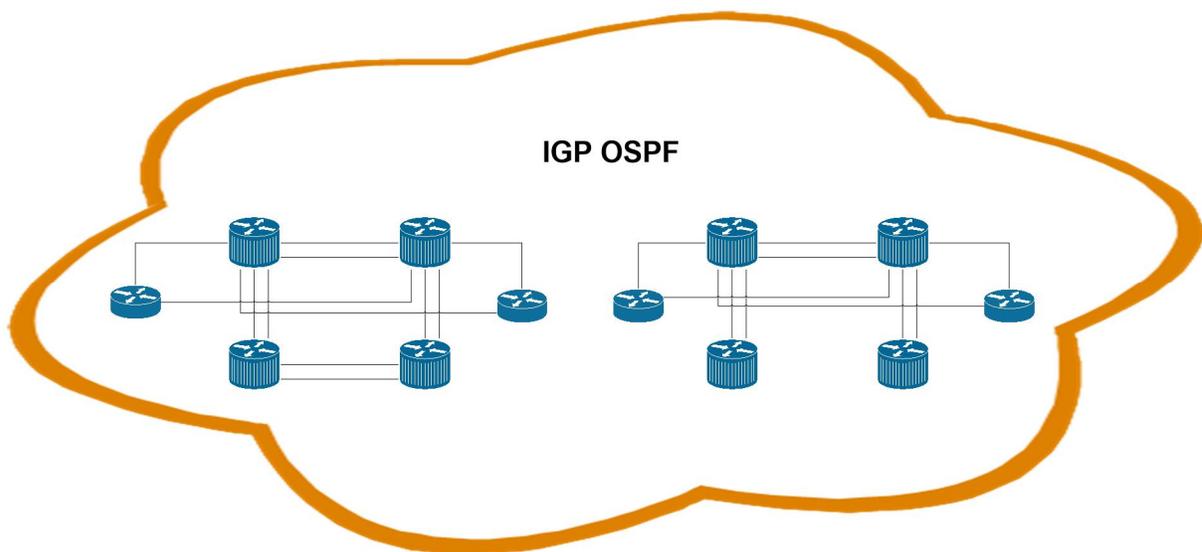


Figura 4.14. OSPF entre subsistemas backbone y acceso.

OSPF es el encargado de anunciar las Loopback de servicio de todos los routers, con el que se establecen vecindades iBGP hacia los BGP RR para intercambiar rutas VPN además de servir de fuente de información para MPLS TE. Es sobre estos dos últimos protocolos (BGP & MPLS TE) donde se implementan los mecanismos de alta disponibilidad.

Los protocolos de alta disponibilidad implementados en este subsistema son:

- BGP Route Policy para marcado de comunidades en BGP.
- MPLS TE FRR Link Protection

4.1.2.2.a BGP Route Policy

Empleado para marcado de comunidad en ruta de default para alta disponibilidad en la salida a Internet.

Cuando el firewall del subsistema de ISP advierte la ruta de default hacia el interior de la red, se tiene al igual que en el subsistema de acceso, un esquema Dual-homed CE por lo cual con el fin de proveer redundancia a nivel de salida a Internet es necesario asignar un RD distinto para cada plano.

Sin embargo, estas rutas al ser importadas a la VRF de Internet deben marcarse con comunidades para tener un criterio y punto de diferenciación al momento de escoger la salida primaria y la de backup a nivel de ciudad.

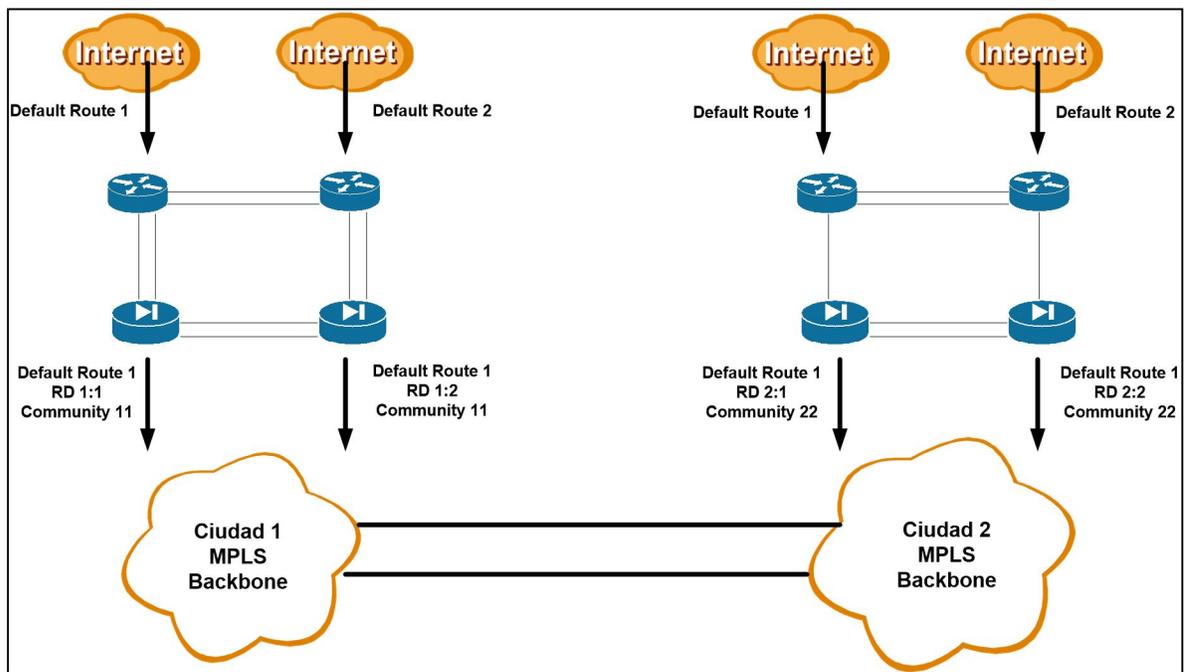


Figura 4.15. Marcado de comunidades y RD en backbone.

De esta forma los routers del subsistema de acceso reciben un total de 4 rutas de default agrupadas en dos grupos de comunidades, de esta forma al aplicar una política en BGP podemos definir cuál salida será la primaria y cual secundaria por medio del atributo LOCAL PREFERENCE de BGP asignando un valor mayor a las rutas de default locales basado en el valor de la comunidad con la cual han sido marcadas.

4.1.2.2.b MPLS TE FRR Link Protection

En el backbone es necesario tener un sistema de alta disponibilidad muy eficiente, ya que es donde cruza la mayor cantidad de tráfico y una falla en esta parte resulta en una afectación de servicio grave.

Además de tener un mecanismo de alta disponibilidad, es necesario manejar el ancho de banda de los enlaces inteligentemente para evitar enlaces ociosos dentro del backbone.

Tomando estas premisas como base, se toma MPLS TE como la mejor opción ya que cumple con ambas condiciones: Alta disponibilidad y uso inteligente del ancho de banda.

Así dentro del backbone MPLS se tiene una solución MPLS TE FRR con la cual se tiene protección a nivel de enlace, es decir, el tráfico es conmutado a un camino secundario de forma rápida en caso de que falle algún enlace protegido, reduciendo así la cantidad de tráfico afectado cuando un enlace falla. Ver figura 4.16.

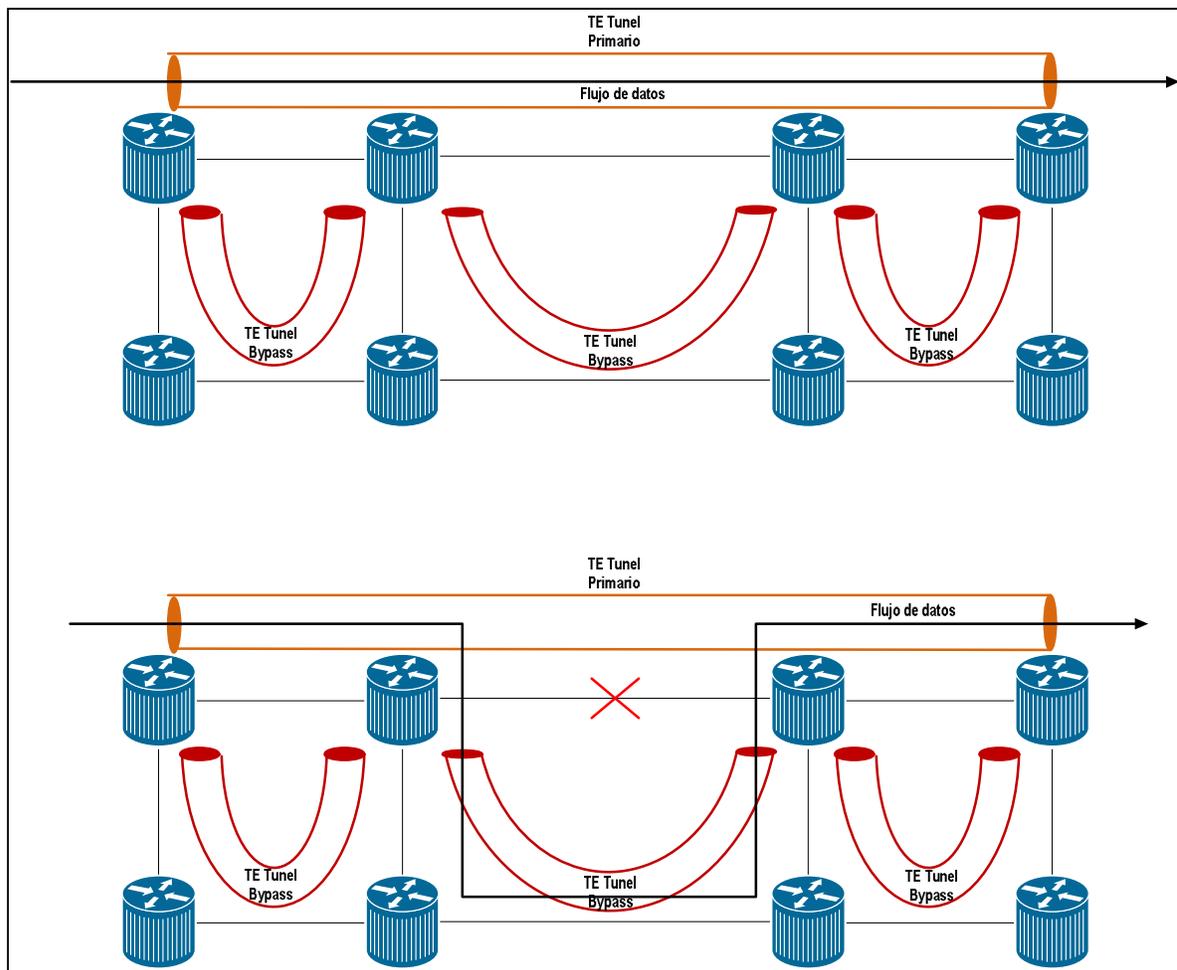


Figura 4.16. Funcionamiento MPLS TE FRR.

4.1.2.3 Subsistema route reflector

Este subsistema es el encargado de advertir las redes recibidas de la ciudad vecina y advertirlas a todos los equipos en la ciudad donde reside y viceversa, está compuesto por dos routers que establecen vecindad full-mesh con los RR de la ciudad vecina para recibir y advertir rutas, además establecen vecindades con cada elemento de la ciudad donde residen.

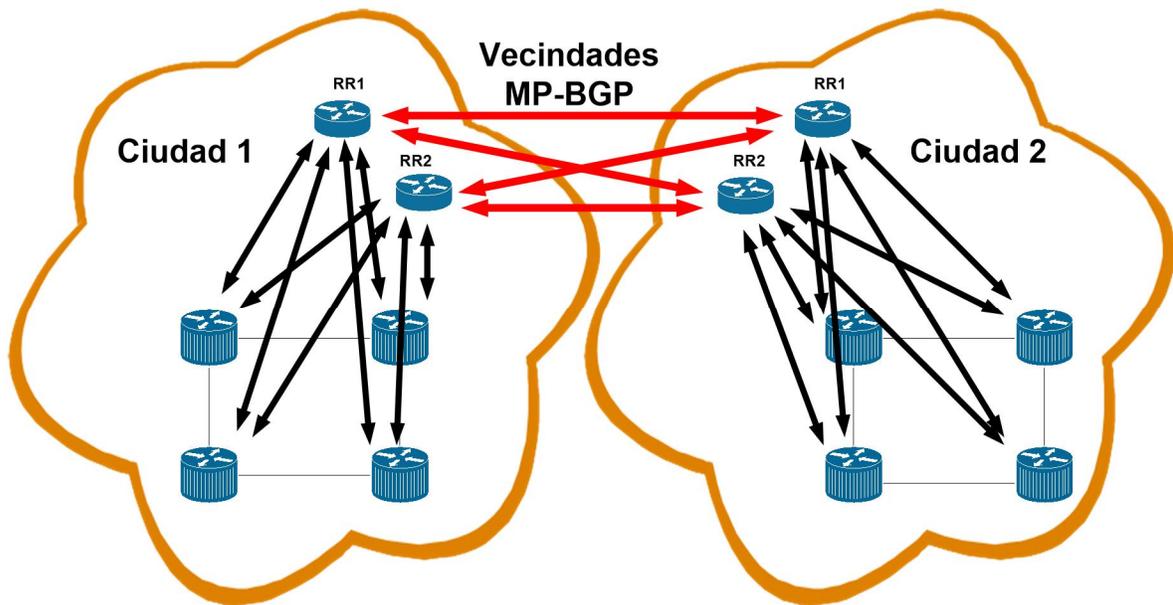


Figura 4.17. Vecindades MP-BGP.

4.1.2.4 Subsistema de ISP

Este subsistema es el encargado de dar salida al servicio de Internet de toda la red, sin este la red entera estaría aislada del resto del mundo.

Para tal propósito se tienen dos salidas redundantes cada una conectándose a un proveedor de servicio diferente.

Del proveedor se recibe la tabla completa de Internet con propósito de optimizar el ruteo además de una ruta de default la cual es inyectada a la red por medio de OSPF.

Los dos firewall son los encargados de realizar el filtrado de tráfico saliente y entrante (IPSEC o servicios que necesitan comunicarse desde el exterior) además de realizar NAT a las IP's públicas asignadas a la compañía.

Entre ellos se corre un protocolo propietario que se encarga de mantener la tabla de sesiones igual en ambos firewall, con el fin de que al haber una falla en uno de ellos la sesión no sea reiniciada, el protocolo en caso de Cisco es SSO (Stateful Switch Over).

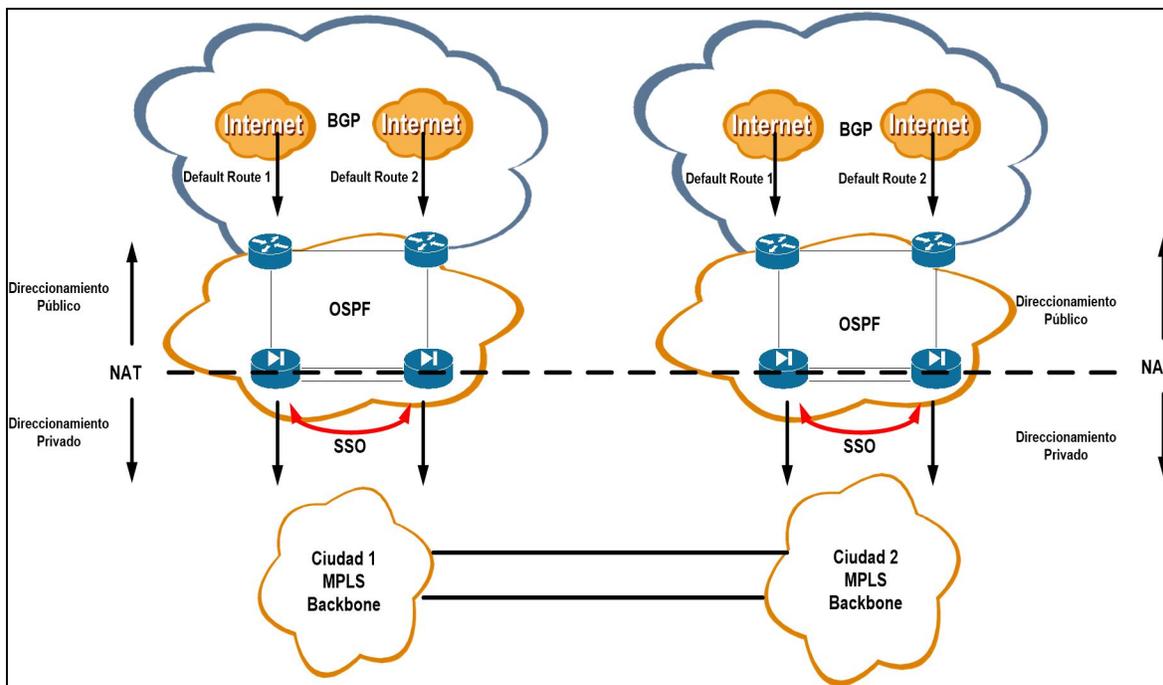


Figura 4.18. Subsistema ISP.

4.1.3 Planeación IP

Para la planeación IP de una red de tipo carrier, es necesario contar con un gran número de direcciones ya que cada elemento que compone la red debe tener al menos un par de ellas que son O&M y Servicio; de acuerdo con el RFC 1918 se tienen dos tipos de direccionamiento: público y privado.

Para la red planteada, se propone usar la red 10.0.0.0/16 la cual se encuentra dentro del espacio reservado Clase A de direccionamiento privado.

Esta red /16 debe dividirse de tal forma que se optimice el uso del direccionamiento.

Las redes tienen principalmente tres requerimientos con respecto al direccionamiento:

- Direccionamiento público.
- Direccionamiento privado de O&M.
- Direccionamiento privado de servicio.

El direccionamiento público es otorgado por los registros regionales que son administrados a su vez por la IANA.

Este tipo de direccionamiento, es usado para el servicio de Internet como "pool" de direcciones para NAT además de ciertas asignaciones directas a plataformas que necesitan comunicarse directamente hacia Internet desde el interior de la red.

El direccionamiento privado de O&M se le asigna a cada elemento con el fin de tener una IP a la cual conectarse remotamente para gestionar el elemento.

El direccionamiento privado de servicio se le asigna a cada elemento con el fin de usarse para comunicarse con otros equipos en la red para motivos de señalización en protocolos como MPLS, LDP, BGP, Etc.

Dentro del segmento privado deben reservarse ciertos rangos de direcciones que se usan para los equipos terminales (equipos de usuario) al momento de ofrecer el servicio de Internet, ya que al ser muchos suscriptores las IP's públicas no son suficientes por lo cual se les asigna una dirección IP privada la cual es NATeada (14) en los firewall para poder comunicarse hacia el exterior.

Así de lo anterior, por ejemplo, se tiene un router al cual se le asigna un direccionamiento privado de O&M el cual es configurado en una interfaz Loopback dentro de la VRF de O&M, y un direccionamiento privado de servicio el cual es configurado en cada una de sus interfaces en la VRF Pública con el fin de comunicarse con los routers adyacentes y remotos para señalización, en este caso OSPF, BGP, LDP, Etc.

Tomando en cuenta lo anterior se muestran las tablas de las asignaciones, en el anexo A de este trabajo, hechas tanto para direccionamiento privado como público.

¹⁴ Término común empleado en las redes de datos para indicar la acción de aplicar NAT a cierta dirección IP.

4.2 Análisis de flujos

Pues bien, después de repasar cada subsistema tanto a nivel físico como lógico, se muestra una explicación completa del funcionamiento general y ante falla de la red propuesta considerando los temas anteriores y las bases teóricas revisadas previamente.

4.2.1 Funcionamiento en condiciones normales

La figura siguiente representa los flujos más importantes dentro del proceso IP para tener funcionando en condiciones normales el servicio de Internet.

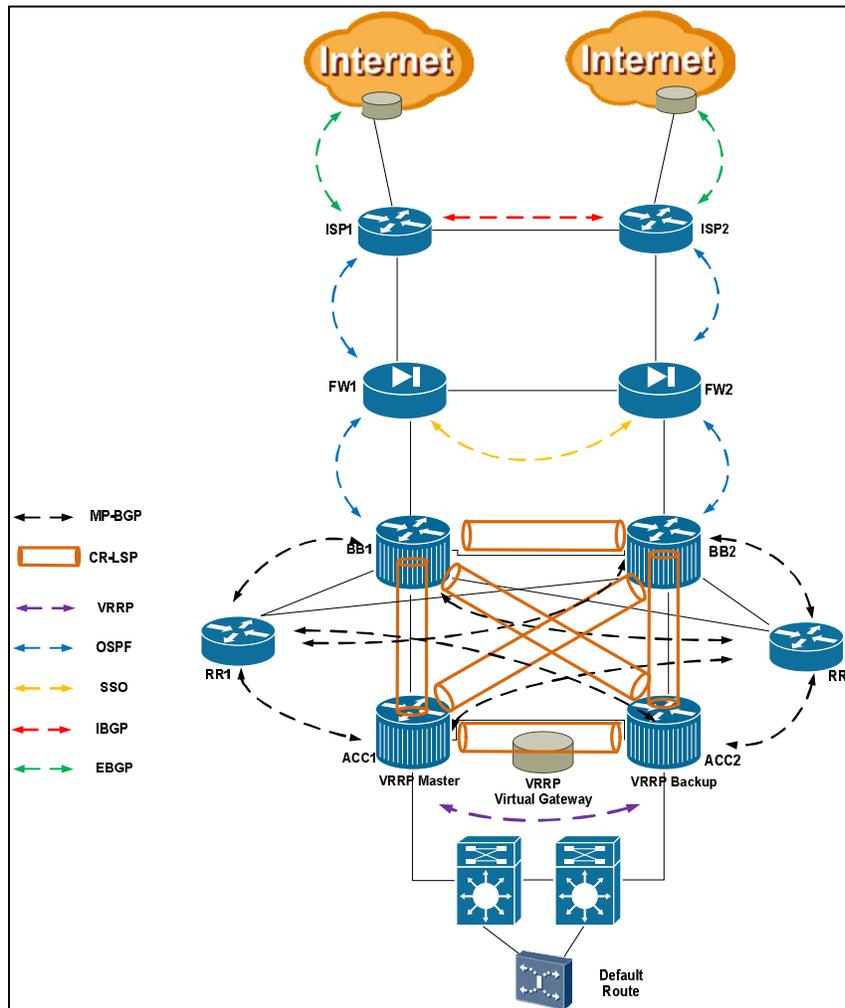


Figura 4.19. Flujos en condiciones normales.

Para fines de analizar el funcionamiento completo, revisaremos el comportamiento primero en dirección UPLINK (hacia Internet) y posteriormente en dirección DOWNLINK (desde Internet).

Dirección UPLINK.

El host envía el paquete.

En la plataforma, solo se configura una ruta de default a la IP del Virtual Gateway que está formado por los dos routers de acceso corriendo VRRP entre ellos.

Al enviar un paquete hacia su Gateway, el router de acceso con el rol de master recibe el paquete destinado a una IP ubicada en la nube de Internet.

El router de acceso busca en su tabla de ruteo y encuentra cuatro rutas publicadas por cada router de backbone; estando las rutas locales de salida a Internet marcadas con comunidad 1111 y las de la ciudad dos con comunidad 2222.

Para las rutas marcadas con comunidad 2222, el router de acceso reduce el atributo de BGP "LOCAL PREFERENCE" a ochenta, quedando las rutas locales con "LOCAL PREFERENCE" de cien, el cual es su default por lo que el router de acceso elige las dos rutas locales.

De las dos rutas preferidas, elige aquella con menor MED, este MED es heredado de la métrica con la que se importa de OSPF por lo que al advertir la ruta de default desde ambos firewall, la ruta advertida por el firewall uno es anunciada con menor métrica.

El router de acceso por tanto elige la ruta advertida por el backbone uno que a su vez fue importada de OSPF. Por lo que su tabla de ruteo muestra como NEXT-HOP la interfaz loopback del router backbone uno.

Sin embargo, al ser el paquete enviado por una VRF, este lleva consigo una etiqueta de VPN por lo que para poder llegar al router de backbone es necesario que exista un LSP entre el router de acceso y el router de backbone.

Este LSP es el CR-LSP creado entre ambos routers, acceso y backbone, y debe existir uno en cada dirección, por lo que para enviar el paquete, el router de acceso debe añadir la etiqueta de VPN y la etiqueta de MPLS TE.

El paquete por medio de la etiqueta de MPLS TE es enrutado hasta el router de backbone donde la etiqueta de MPLS es quitada quedando sólo la etiqueta de VPN la cual indica al router a que VRF corresponde y hacia qué interfaz debe enviar el paquete.

El router de backbone después de haber quitado las dos etiquetas revisa la dirección destino del paquete y lo envía hacia el firewall de ISP debido a que de este recibe la ruta de default por OSPF.

El firewall recibe el paquete y revisa la inter-zona correspondiente para confirmar si el paquete está o no permitido pasar, si está permitido, el firewall cambia la dirección IP de origen por medio de NAT y registra la sesión en su tabla de sesiones la cual se encuentra sincronizada con el FW2 por medio del protocolo SSO.

El paquete es enviado hacia los routers de ISP los cuales reciben la tabla completa de BGP de los routers del proveedor de servicio y que corren a su vez IBGP entre ellos.

Entre los dos routers de ISP se decide cual es la mejor salida basada en los atributos advertidos por el proveedor de servicios. El paquete sale a Internet.

Dirección DOWNLINK

Después de haber llegado el paquete hasta su destino, es necesario regresar una respuesta para que la comunicación se establezca, a esto se refiere esta sección.

Pues bien, la respuesta sale hacia Internet y observa que el segmento es anunciado por dos proveedores de servicios a la vez, de acuerdo con los atributos de BGP como AS-PATH, elige la ruta por alguno de los proveedores.

Ya estando en la red del proveedor, se tienen dos rutas para llegar al segmento, una por medio de la ciudad uno y la otra por medio de la ciudad dos, esto debido a la redundancia geográfica.

Elige la primera opción ya que esta cuenta con un AS-PATH menor y envía el paquete hacia el router de ISP de la ciudad uno.

Ya en el router de la ciudad uno, revisa su tabla de ruteo y ve que recibe dos rutas hacia el segmento del Pool para NAT, el firewall de ISP uno lo advierte con menor costo mientras que el firewall dos con costo mayor, ambos por OSPF.

El firewall uno al advertir el segmento con menor costo recibe el paquete, esta vez no se revisa la inter-zona ya que el paquete es la respuesta a una sesión anteriormente permitida e iniciada registrada en su tabla de sesiones.

El firewall uno revisa su tabla de translaciones NAT y modifica en este caso la IP de destino a la IP original, revisa su tabla de ruteo y lo envía al router de backbone.

Ya en el router de backbone, al recibir el paquete en la interfaz ligada a la VRF de servicio de Internet, revisa la tabla de ruteo de esta VRF y encuentra dos rutas, una por cada router de acceso, ambas con igual métrica (atributos), sin embargo por ser el router de acceso uno, el que tiene el menor costo en el IGP, toma esta ruta por medio de BGP siendo el next-hop la interfaz loopback del router uno.

Al ser un paquete de VRF, es necesario que exista un LSP que transporte el paquete hasta su destino, este LSP es el CR-LSP de MPLS TE que existe entre ambos equipos.

El router de backbone añade al paquete la etiqueta de VPN y la etiqueta de MPLS y lo envía por la interfaz que indica el LSP.

El paquete llega al router de acceso por medio de la etiqueta de MPLS y ahí se revisa la etiqueta de VPN para definir la VRF a la cual corresponde, el router de acceso revisa su tabla de ruteo y ve que la tiene directamente conectada así que lo envía por su subinterfaz conectada al Switch de acceso con el tag de la VLAN correspondiente.

El switch de acceso recibe el paquete con tag, revisa la VLAN a la que pertenece y lo transmite por el puerto correspondiente.

El host recibe la respuesta.

4.2.2 Funcionamiento en caso de falla. Pérdida de poder en switch de acceso

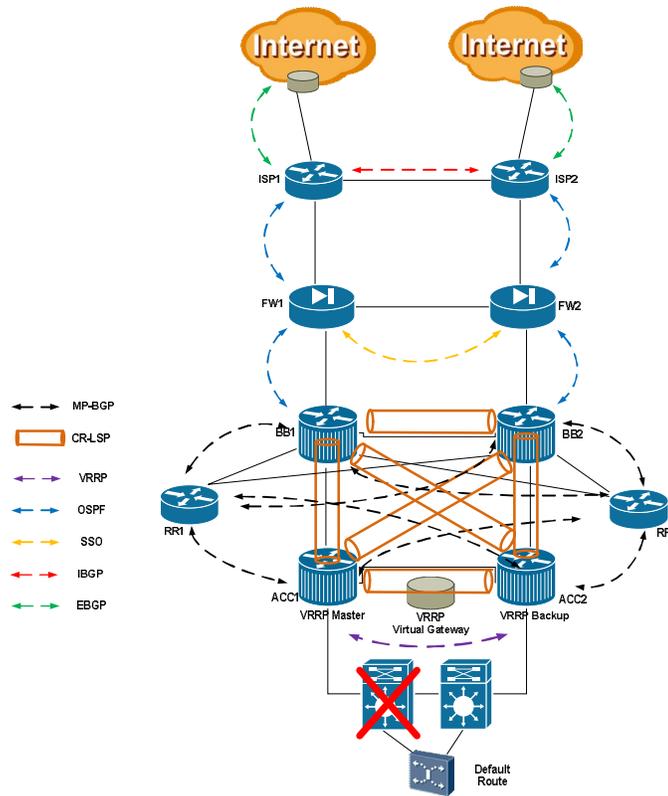


Figura 4.20. Pérdida de poder en switch de acceso.

Para el caso de pérdida de poder o falla en el switch de acceso, se tiene un escenario donde se requiere que el equipo terminal conectado al switch tenga un sistema de redundancia a nivel de hardware que sea capaz de detectar la pérdida de conexión física hacia el switch dañado y conmutar el tráfico hacia la tarjeta que conecta con el switch activo.

A nivel de capa dos, la pérdida de poder de un switch significa la fragmentación del dominio de broadcast y aislamiento entre ambos routers los cuales se comunican por medio del troncal que existe entre ambos switches.

Por tanto, al tener una falla en cualquiera de los dos switches, se tiene un corte en la señalización del protocolo de redundancia VRRP lo cual se refleja en la convergencia del protocolo tomando el router SLAVE el papel de MASTER dando salida al tráfico generado por el equipo conectado al switch.

Así en dirección UPLINK, el tráfico en el equipo conectado es conmutado al puerto secundario y entregado al switch activo el cual lo entrega al nuevo router MASTER que a partir de ese punto entrega el tráfico a la red MPLS siguiendo el mismo proceso descrito en el sub-capítulo 4.2.1.

Para la dirección DOWNLINK, la falla se refleja de inmediato, esto debido a que el router uno deja de advertir el segmento de red que se encontraba configurado en las interfaces conectadas al switch afectado, así, el tráfico DOWNSTREAM llega al equipo final por medio del router dos.

4.2.3 Funcionamiento en caso de falla, pérdida de poder en ambos switch de acceso

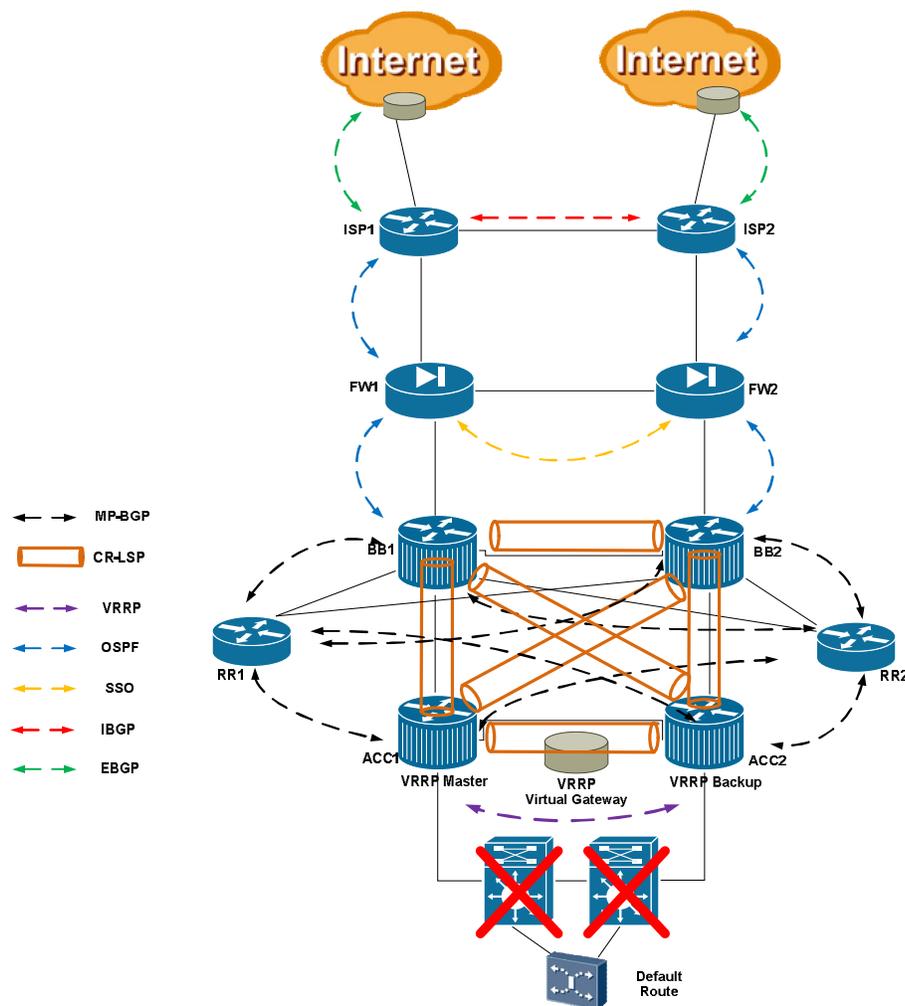


Figura 4.21. Pérdida de poder en ambos switches de acceso.

En el caso de falla de ambos switches, como se puede apreciar en la imagen, el equipo final queda completamente aislado de la red, por lo tanto la conexión es pérdida; sin embargo, este escenario al tener ambos switches con redundancia a nivel de hardware es poco probable que se presente.

4.2.4 Funcionamiento en caso de falla, pérdida de poder en router de acceso

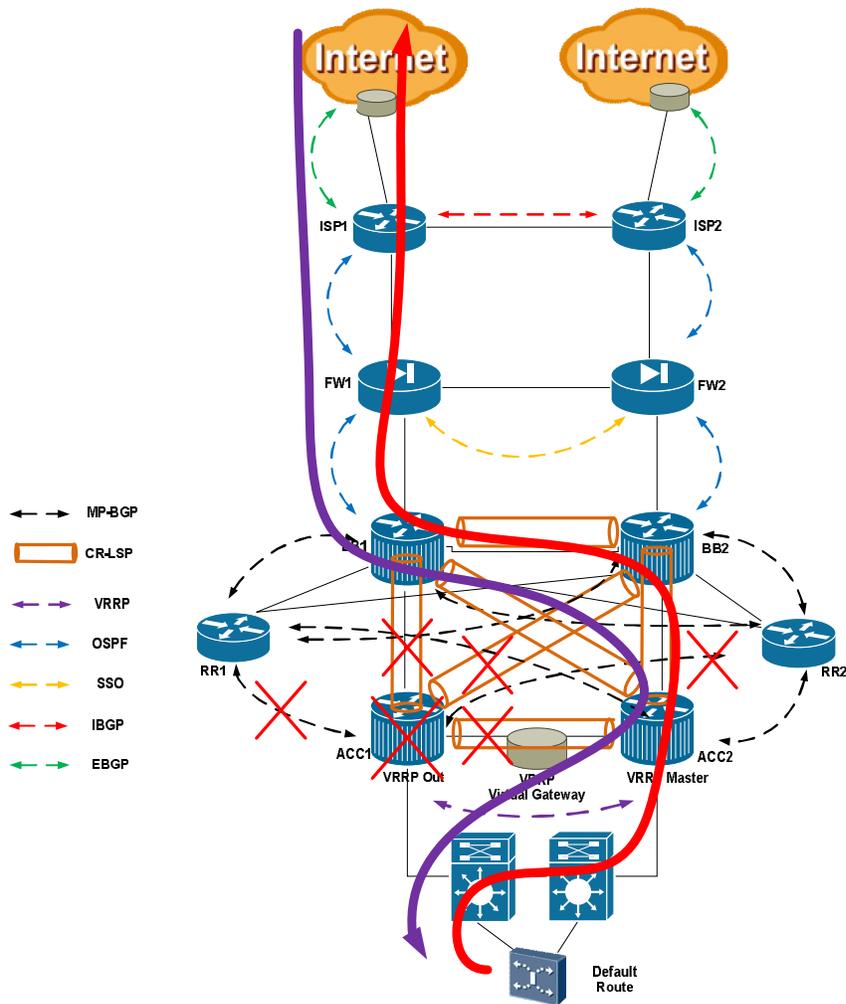


Figura 4.22. Pérdida de poder en router de acceso.

Al igual que para el caso anterior el análisis se dividirá en dos partes: Uplink y Downlink

Dirección UPLINK

El router de acceso uno pierde poder y se apaga.

Al apagarse, el equipo deja de emitir la señalización de VRRP que corre entre los dos routers de acceso.

El router de acceso número dos al detectar que el router uno no responde a los mensajes, asume que el equipo está fuera de servicio y toma el rol de MASTER, es decir, toma la IP virtual como propia y comienza a recibir el tráfico enviado por el equipo final hacia su GW.

El router de acceso número dos recibe el tráfico, revisa la dirección destino y al buscar en su tabla de ruteo encuentra que la opción más adecuada es la ruta de default, ruta para la cual tiene cuatro opciones, las dos advertidas localmente y las dos advertidas por los routers de backbone de la ciudad vecina.

Sin embargo las rutas anunciadas localmente cuentan con una LOCAL PREFERENCE mejor, debido a las políticas aplicadas sobre las rutas anunciadas por la ciudad vecina.

De las dos rutas con menor LOCAL PREFERENCE, elige aquella con menor MED, que es heredada de la métrica con la cual se importó del proceso de OSPF. De esta forma el router de acceso elige la ruta anunciada por el router de backbone uno y busca el túnel que lo lleve a este, en este caso tiene un túnel directo al router de backbone uno.

El router de acceso número dos toma el paquete y lo etiqueta con las dos etiquetas correspondientes: etiqueta de VPN y etiqueta de MPLS y lo envía.

El router de backbone uno recibe el paquete y lo envía hacia el firewall de Internet uno, ya que de este recibe la ruta de default.

El proceso desde este punto hacia la ubicación en Internet a la cual se desea llegar sigue el mismo esquema ya explicado con anterioridad en condiciones normales.

Dirección DOWNLINK

El análisis comenzará desde que el paquete llega al router de backbone uno, ya que el proceso hasta este punto sigue el mismo esquema explicado en el caso del funcionamiento normal.

Llegando el paquete al router de backbone uno, el router revisa su tabla de ruteo y encuentra que ya no existen dos rutas hacia este destino, puesto que uno de los routers de acceso está

fuera de servicio, lo cual implica que su relación de BGP con los route reflector está en estado de desconexión.

El router de backbone uno toma entonces la única opción que tiene por BGP hacia el NEXT-HOP que es router de acceso dos, revisa los LSP que tiene hacia ese NEXT-HOP y encuentra que tiene un túnel configurado hacia este destino.

El router de backbone uno toma el paquete IP y lo encapsula con dos etiquetas: etiqueta de VPN y etiqueta de MPLS y lo envía.

El paquete llega al router de acceso dos y al revisar la IP de destino se da cuenta que tiene el segmento directamente conectado a él, por lo cual el paquete es enviado hacia el switch con la dirección MAC de destino del host.

El paquete llega a su destino.

4.2.5 Funcionamiento en caso de falla, pérdida de poder en ambos routers de acceso

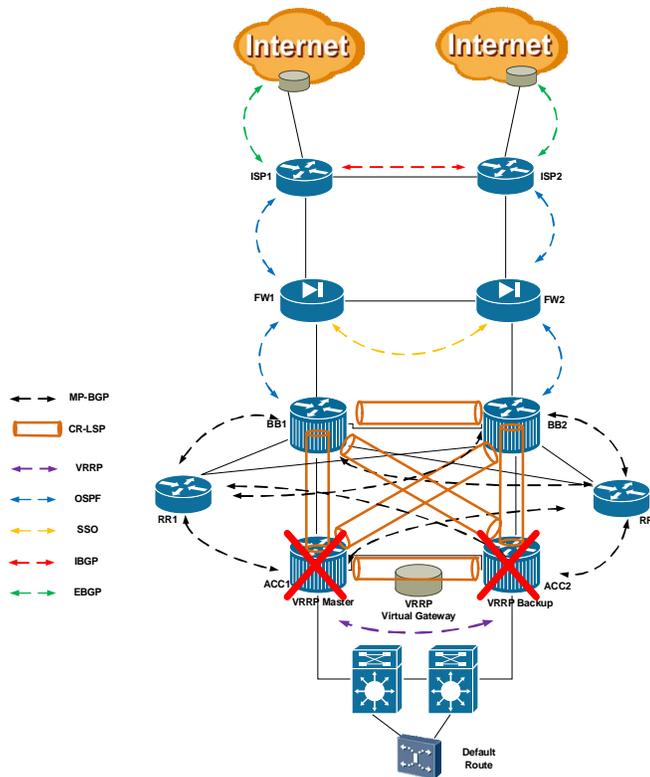


Figura 4.23. Pérdida de poder en ambos routers de acceso.

Al igual que el caso de falla en ambos switches de acceso, al fallar los dos routers de acceso, se tiene completamente aislada la parte de acceso lo cual implica una desconexión total e interrupción del servicio, igualmente este escenario es poco probable al contar con redundancia a nivel de hardware.

4.2.6 Funcionamiento en caso de falla, pérdida de enlace entre equipos de backbone y acceso

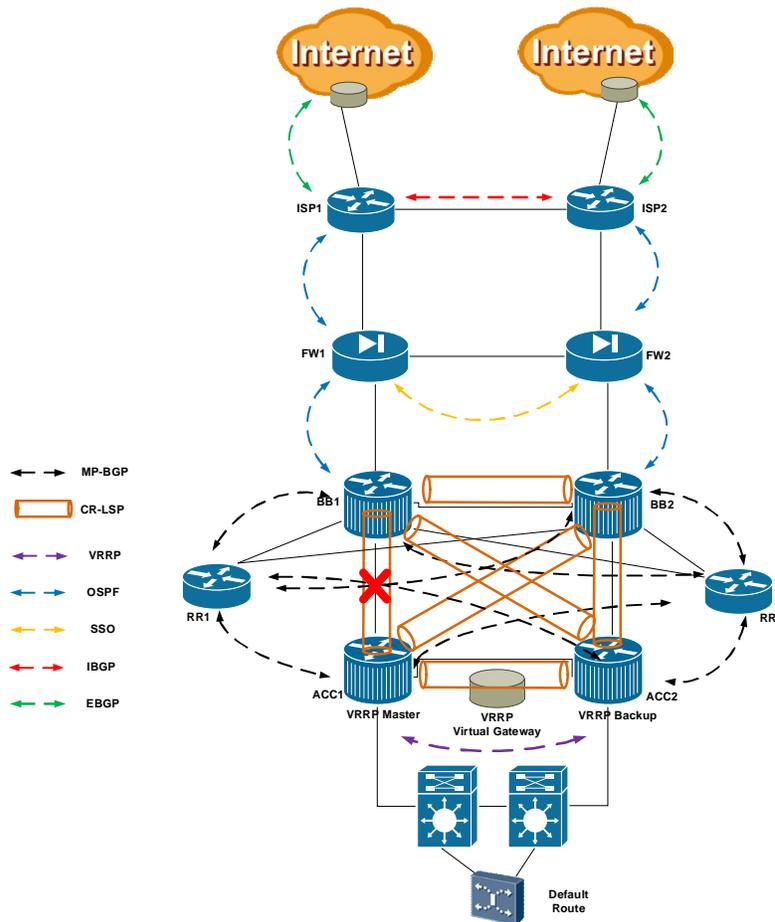


Figura 4.24. Pérdida de enlace entre equipos de backbone y acceso.

Dirección UPLINK

El host envía como cualquier otra ocasión su tráfico hacia su gateway esperando que éste llegue a su destino en Internet.

El router recibe el paquete, justo en ese momento la interfaz que une el router de acceso uno con el router de backbone uno deja de funcionar. Sin embargo, al existir un mecanismo de detección entre estos equipos (BFD), el router de acceso es capaz de detectar la falla en términos de decenas de milisegundos.

Al detectar la falla, el equipo de acceso uno hace la conmutación MPLS TE FRR y envía el tráfico por medio del túnel bypass (creado previamente por el protocolo MPLS TE), el cual puede no ser el mejor camino en cuestión de métrica, sin embargo protege el flujo de datos.

De esta forma el router de acceso no necesita tener que esperar hasta la convergencia del IGP para enviar el tráfico lo cual se refleja en una parte despreciable del tráfico perdido.

El router de backbone uno recibe el tráfico por la interfaz (túnel de bypass) que conecta al router de backbone dos y lo procesa como en caso normal enviándolo al firewall de ISP.

Dirección DOWNLINK

De igual forma al llegar el tráfico al router de backbone, este detecta la falla en el enlace por medio de BFD y dispara la conmutación hacia el tunel de bypass sin tener que esperar a que converja el IGP.

El router de acceso recibe el tráfico por una interfaz diferente y lo procesa como en condiciones normales hacia el switch de acceso.

De esta forma se protege la red ante falla en los enlaces usando mecanismos de detección que ayudan a detectar la falla en un periodo de tiempo corto con el fin de permitir al equipo reaccionar apropiadamente y proteger el flujo de datos.

4.2.7 Funcionamiento en caso de falla, pérdida de poder en router de backbone

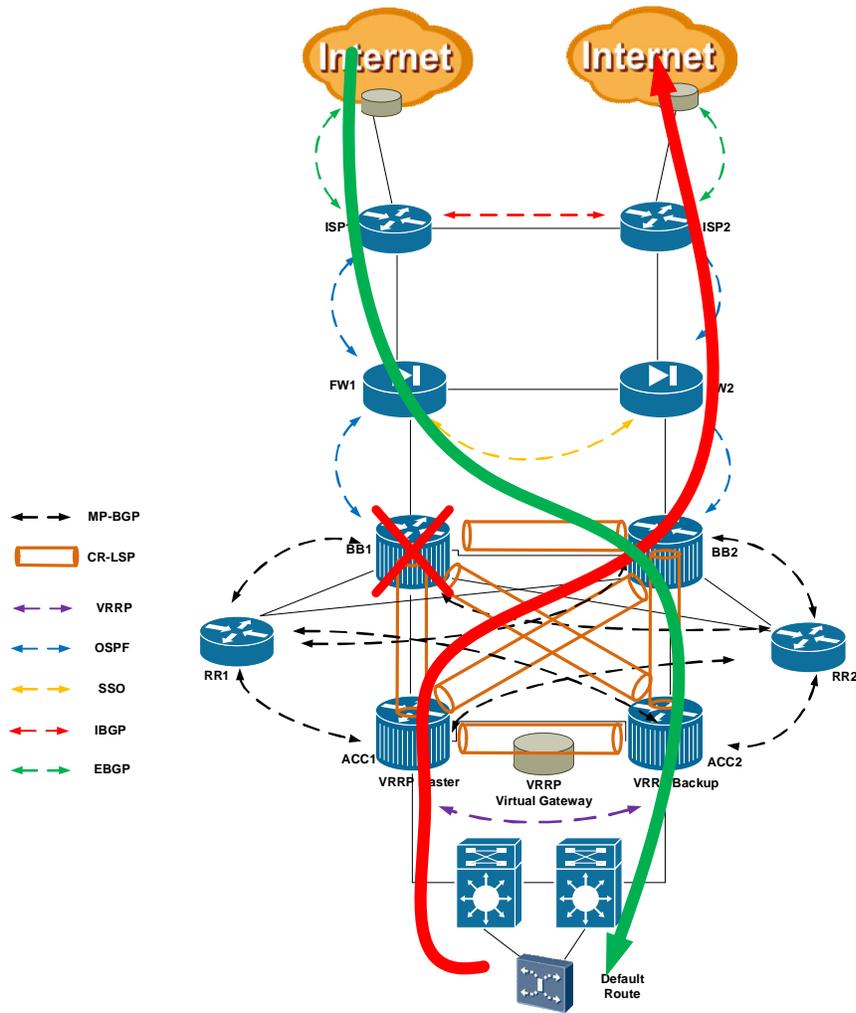


Figura 4.25. Pérdida de poder en router de backbone

El escenario muestra un ejemplo en el cual uno de los routers de backbone pierde poder o sufre una falla lo que ocasiona que deje de funcionar completamente.

Dirección UPLINK

El tráfico es generado desde el equipo conectado a los switches de acceso y enviado a su default gateway con el fin de que el tráfico llegue a su destino final.

El router de acceso MASTER en VRRP recibe el tráfico y revisa su tabla de ruteo con el fin de etiquetar el paquete y enviarlo a la red MPLS, sin embargo detecta que el router de backbone se encuentra fuera de servicio por medio de la sesión de BFD que existe entre ambos routers con el fin de detectar este tipo de fallas.

Al detectar la falla, el router de acceso revisa su tabla de ruteo y por medio del protocolo BGP VPN FRR, encuentra el NEXT-HOP alternativo que advierte el mismo segmento (ruta de default), en este caso, el router de backbone dos.

Sin esperar a la convergencia del protocolo de ruteo, el router de acceso envía el tráfico hacia el router de backbone dos por el CR-LSP previamente creado.

El router de backbone dos recibe el tráfico y lo procesa como en condiciones normales enviándolo al firewall de ISP dos, después esta hacia el router de ISP dos y de ahí hacia Internet.

Dirección DOWNLINK

El tráfico al llegar desde Internet encuentra que el firewall de ISP uno no advierte segmento interno alguno debido a que su fuente de información (router de backbone uno) ha fallado, por lo cual envía el tráfico hacia el firewall de ISP dos, que a su vez envía el tráfico hacia el router de backbone dos.

El router de backbone dos revisa su tabla de ruteo y encuentra que el router de acceso dos tiene la mejor métrica a nivel IGP y decide enviar el tráfico hacia este equipo.

El router de acceso recibe el tráfico y lo envía a nivel capa dos al equipo final.

El tráfico llega a su destino correctamente.

4.2.8 Funcionamiento en caso de falla, pérdida de poder en ambos routers de backbone

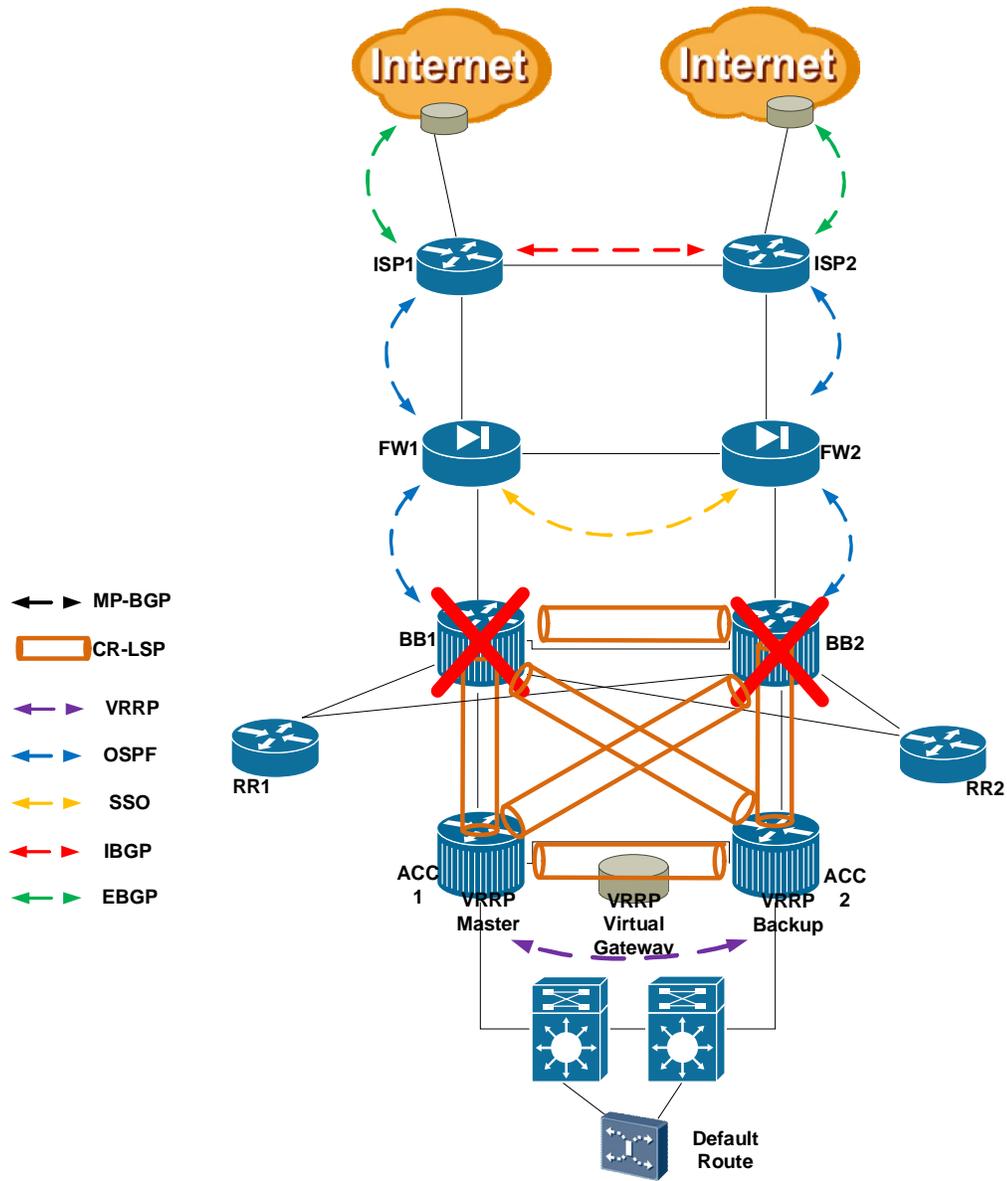


Figura 4.26. Pérdida de poder en ambos routers de backbone

Al presentarse una falla en ambos equipos de backbone, la red es segmentada aislando los route reflectors, de los routers de acceso y de los routers de backbone de la ciudad vecina, por lo cual el flujo de datos hacia y desde Internet es interrumpido. Sin embargo una falla de este

tipo es poco probable al tenerse fuentes redundantes en ambos equipos y bancos de baterías en las instalaciones que albergan los equipos.

4.2.9 *Funcionamiento en caso de falla, pérdida de poder en route reflector*

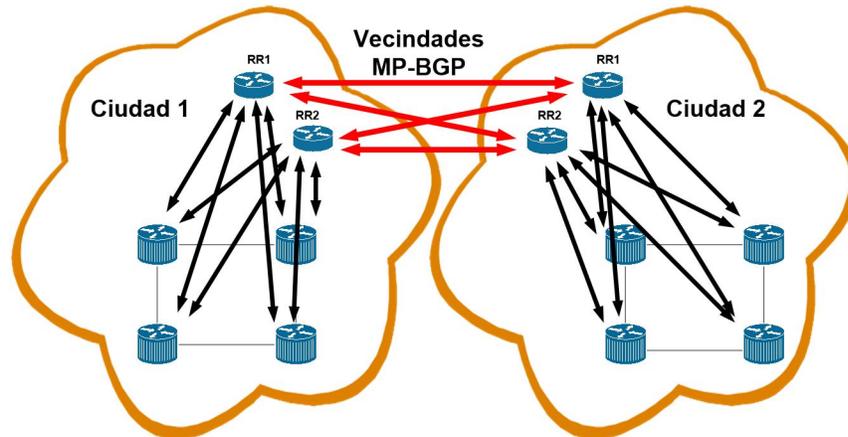


Figura 4.27. Pérdida de poder en route reflector.

En la red propuesta se cuenta con redundancia a nivel de equipo teniendo dos Route Reflector por cada ciudad.

Todos los elementos cuentan con sesiones de BGP hacia ambos route reflectors por medio de las cuales anuncian sus prefijos hacia la red y reciben los prefijos anunciados por otros equipos.

Estos dos route reflector tienen además de las sesiones con cada uno de los equipos de su ciudad, sesiones BGP con los dos Route-Reflector de la ciudad vecina por medio de las cuales se conocen los prefijos de una ciudad en la otra ciudad y viceversa.

Tomando en cuenta lo anterior, se tiene que al fallar un route reflector no se afecta el anuncio de los segmentos ya que el Route-Reflector dos sigue advirtiendo los segmentos de forma normal.

Sin embargo el tener una falla en ambos route reflector provoca una desconexión total a nivel lógico entre los elementos de la red de la misma ciudad y hacia la ciudad vecina, ya que los intermediarios que reciben y anuncian las rutas no están presentes.

Por lo anterior estos equipos junto con los de routers de backbone son de vital importancia para la red.

4.2.10 Funcionamiento en caso de falla, pérdida de poder en firewall de Internet

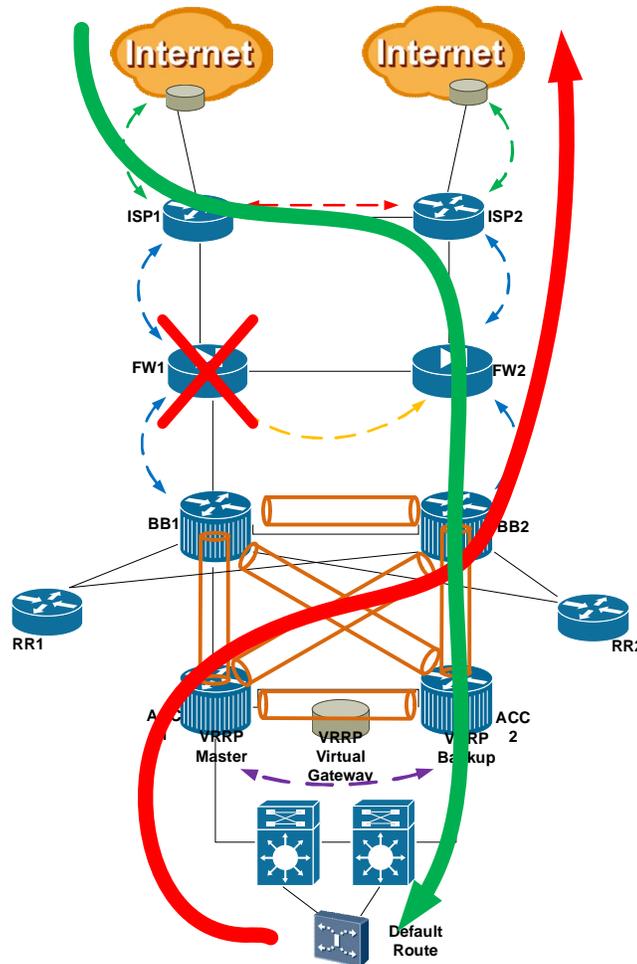


Figura 4.28. Pérdida de poder en firewall de Internet.

Dirección UPLINK

El tráfico llega a los routers de acceso desde el equipo conectado a los switches de acceso buscando lograr llegar a Internet.

El router de acceso revisa su tabla de ruteo y nota que el router de backbone uno, no anuncia más la ruta de default debido a que el equipo que se la anunciaba, el firewall de ISP uno, está fuera de servicio.

Por lo anterior el router de acceso envía el tráfico hacia la segunda opción que tiene para salir a Internet que es por medio del router de backbone dos el cual recibe todavía la ruta de default por medio del firewall de ISP dos el cual no ha sufrido afectación.

El tráfico llega al router de backbone dos y es procesado y enviado al firewall de ISP dos el cual a su vez lo envía al router de ISP dos y de ahí el tráfico sale a Internet.

Dirección DOWNLINK

El tráfico proveniente desde Internet llega a los routers de ISP los cuales solo tienen una ruta posible por medio del firewall de ISP dos ya que el firewall de ISP uno se encuentra fuera de servicio.

El tráfico es enviado al firewall de ISP 2 y este lo envía al router de backbone 2, este revisa su tabla de ruteo y observa que tiene dos posibles NEXT-HOP (router de acceso 1 y router de acceso 2), sin embargo por métricas de IGP elige el NEXT-HOP router de acceso 2.

El tráfico llega al router de acceso 2 y este al tener el segmento de destino directamente conectado lo envía a nivel capa 2 por la VLAN correspondiente hacia el equipo origen.

El flujo es completado correctamente.

4.2.11 Funcionamiento en caso de falla, pérdida de poder en ambos firewall de Internet

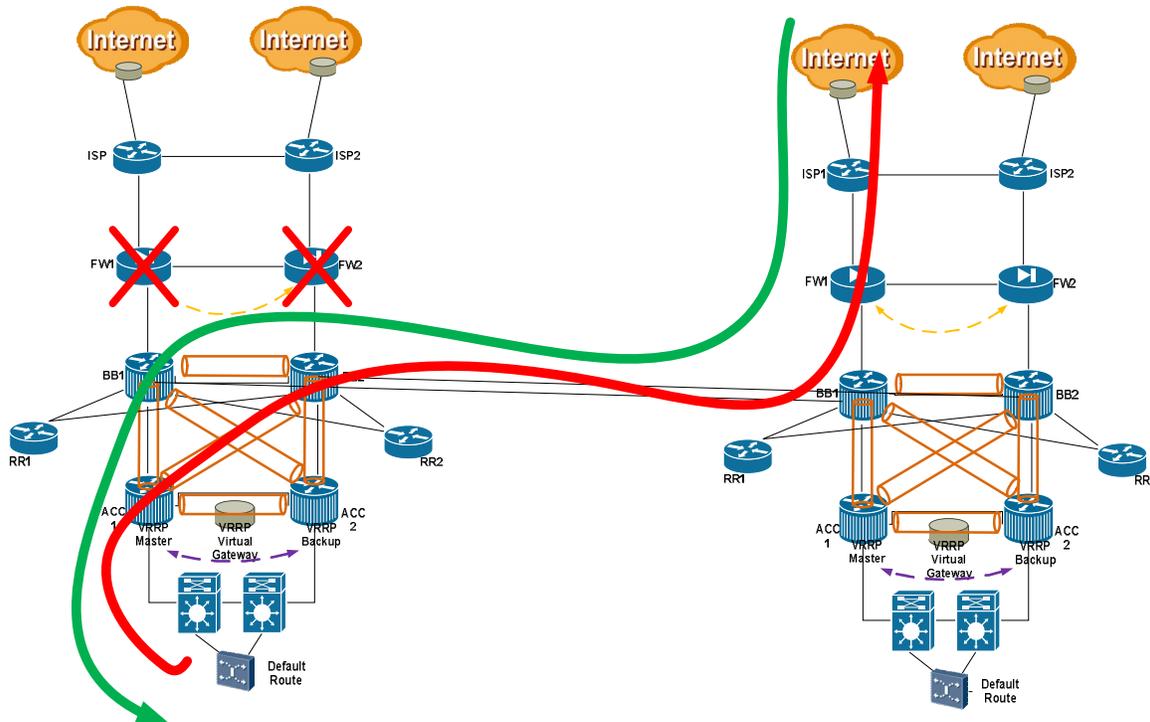


Figura 4.29. Pérdida de poder en ambos firewall de Internet.

A diferencia de los escenarios anteriores, la falla en ambos firewall de ISP no significa un aislamiento de la red o un corte en el flujo de datos.

Para este escenario se plantea una solución basada en el manejo de atributos de BGP y marcado de comunidades con lo cual el tráfico puede ser desviado a la ciudad vecina y "NATeado" usando el segmento advertido por dicha ciudad.

Dirección UPLINK

El tráfico llega a los routers de acceso los cuales han dejado de recibir la ruta de default por parte de ambos router de backbone de su ciudad debido a que ambos equipos que se las anunciaban (firewall de ISP 1 y firewall de ISP 2) se encuentran fuera de servicio.

Sin embargo los routers de acceso aun reciben dos rutas de default advertidas por los dos routers de backbone de la ciudad vecina pero con una "LOCAL PREFERENCE" menor.

De ambas rutas el router de acceso revisa cual NEXT-HOP representa una menor métrica y envía el tráfico al router de backbone 1.

El tráfico en el router de backbone 1 de la ciudad vecina es enviado usando la ruta de default advertida por el firewall de ISP de su misma ciudad.

El tráfico en el firewall de ISP de la ciudad 2 es "NATeado" con el segmento propio de la región y enviado a Internet.

Lo anterior protege el flujo de datos y evita la pérdida de servicio sin embargo también representa un aumento en el uso del ancho de banda y procesamiento en los equipos de la ciudad 2.

Dirección DOWNLINK

El tráfico al haber sido enviado a Internet con las IP's públicas de la ciudad 2, retorna por medio también de los routers de ISP de la ciudad 2.

El router de ISP de la ciudad 2 no se percató que el tráfico pertenece a la ciudad vecina ya que para el lo que pasa detrás del NAT es transparente así que envía el tráfico hacia el firewall de ISP 1.

Este revisa la IP de destino la cual coincide con los segmentos advertidos por el router de backbone 1 de su ciudad que pertenecen a la ciudad vecina.

Cabe mencionar que el router de backbone 1 de la ciudad 2 aprendió los segmentos de la ciudad 1 por medio de los Route-Reflectors mencionados anteriormente.

El tráfico recibido en el router de backbone 1 de la ciudad 2 es enviado al router de acceso de la ciudad 1 por medio del túnel TE que existe entre ellos esto después de haber revisado su tabla de ruteo y notar que el prefijo existía en su tabla con NEXT-HOP el router de acceso 1 de la ciudad vecina.

El tráfico llega al router de acceso 1 el cual de forma normal envía el tráfico al equipo origen cuyo segmento el tiene directamente conectado.

El tráfico se completa satisfactoriamente.

4.2.12 Funcionamiento en caso de falla, pérdida de poder en router de Internet

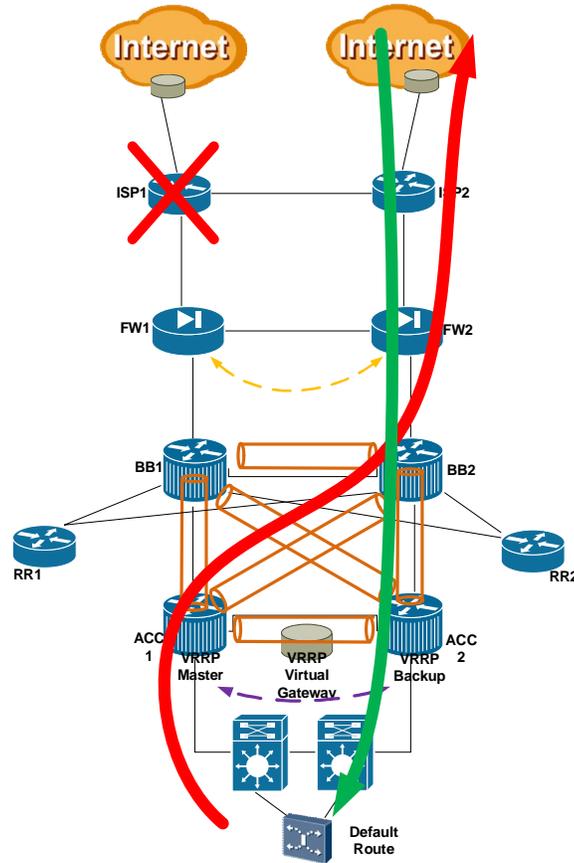


Figura 4.30. Pérdida de poder en router de Internet.

Dirección UPLINK

La convergencia es inmediata ya que al dejar de funcionar el router de Internet 1, la ruta por default advertida por el router 2 toma su lugar y el tráfico es desviado a la salida por el ISP2.

Dirección DOWNLINK

En este escenario se tiene una pérdida de servicio de duración corta la cual no puede ser evitada ya que es debido a la convergencia de las tablas de ruteo de Internet, es decir, el ISP conectado al router de Internet 1 deja de recibir el segmento público y comienza la convergencia en la nube de Internet para enviar el tráfico de retorno por la segunda opción que es el router 2 a través del ISP 2.

4.2.13 Funcionamiento en caso de falla, pérdida de poder en ambos router de Internet

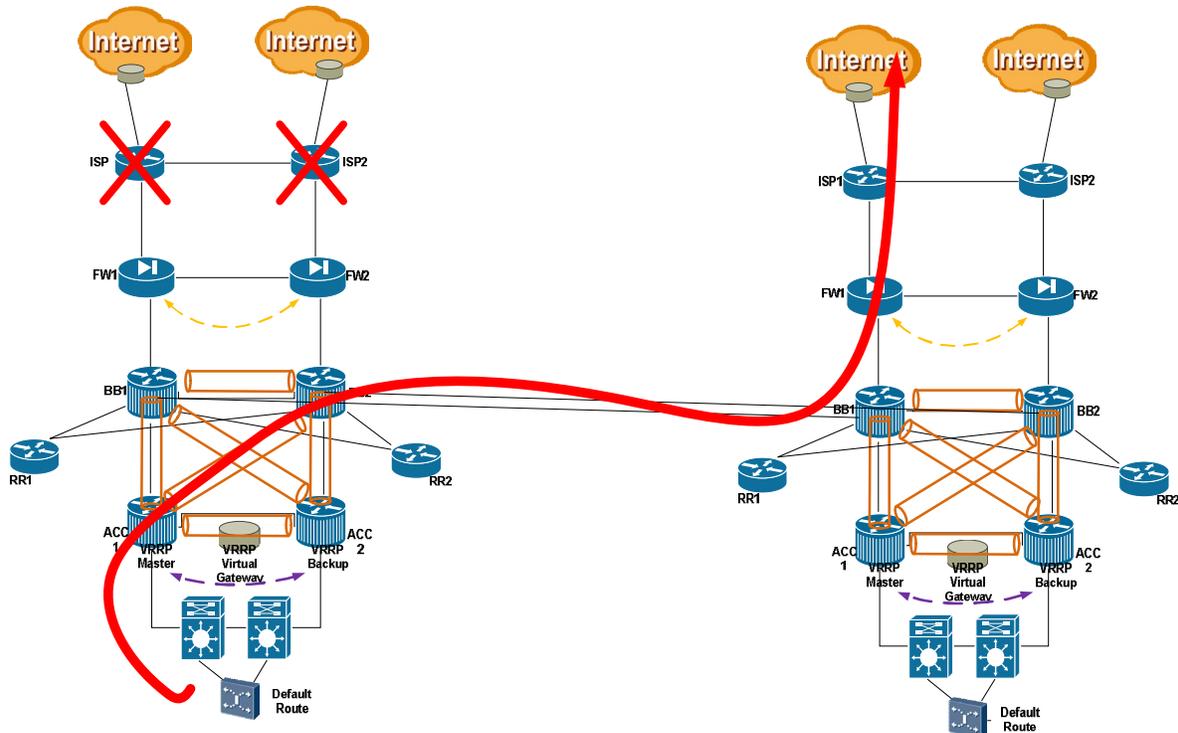


Figura 4.31. Pérdida de poder en ambos router de Internet.

En este escenario al tener fuera de servicio ambos routers de Internet se dejan de recibir del ISP las rutas por default y por consiguiente se dejan de advertir las rutas de default a los firewall de Internet.

Dirección UPLINK

El tráfico llega a los routers de acceso los cuales han dejado de recibir la ruta de default por parte de ambos router de backbone de su ciudad debido a que ambos equipos que se las anunciaban (firewall de ISP 1 y firewall de ISP 2) dejaron de recibirlas por parte de los routers de Internet.

Sin embargo los routers de acceso aún reciben dos rutas de default advertidas por los dos routers de backbone de la ciudad vecina pero con una "LOCAL PREFERENCE" menor.

De ambas rutas el router de acceso revisa cual NEXT-HOP representa una menor métrica y envía el tráfico al router de backbone 1.

El tráfico en el router de backbone 1 de la ciudad vecina es enviado usando la ruta de default advertida por el firewall de ISP de su misma ciudad.

El tráfico en el firewall de ISP de la ciudad 2 es "NATeado" con el segmento propio de la región y enviado a Internet.

Lo anterior protege el flujo de datos y evita la pérdida de servicio sin embargo también representa un aumento en el uso del ancho de banda y procesamiento en los equipos de la ciudad 2.

Dirección DOWNLINK

El tráfico al haber sido enviado a Internet con las IP's públicas de la ciudad 2, retorna por medio también de los routers de ISP de la ciudad 2.

El router de ISP de la ciudad 2 no se percató que el tráfico pertenece a la ciudad vecina ya que para el lo que pasa detrás del NAT es transparente así que envía el tráfico hacia el firewall de ISP 1.

Este revisa la IP de destino la cual coincide con los segmentos advertidos por el router de backbone 1 de su ciudad.

Cabe mencionar que el router de backbone 1 de la ciudad 2 aprendió los segmentos de la ciudad 1 por medio de los Route-Reflectors mencionados anteriormente.

El tráfico recibido en el router de backbone 1 de la ciudad 2 es enviado al router de acceso de la ciudad 1 por medio del túnel TE que existe entre ellos esto después de haber revisado su tabla de ruteo y notar que el prefijo existía en su tabla con NEXT-HOP el router de acceso 1 de la ciudad vecina.

El tráfico llega al router de acceso 1 el cual de forma normal envía el tráfico al equipo origen cuyo segmento el tiene directamente conectado.

El tráfico se completa satisfactoriamente.

CAPÍTULO V: SIMULACIÓN Y RESULTADOS.

Implementación

Con el fin de poner en práctica todos los fundamentos teóricos de redes IP aprendidos y mostrar la solución propuesta en los capítulos anteriores se ha creado una simulación la cual refleja el modo de funcionamiento de la red en condiciones reales, debido a los altos costos de implementarlo físicamente se ha decidido usar un simulador el cual emula equipos IP virtualmente.

Es importante señalar que la simulación, si bien refleja en gran manera el modo de operación de la red en condiciones reales, no refleja los requerimientos tanto de versión de software así como tampoco requerimientos a nivel de hardware, esto debido a que se realizó con las versiones disponibles debido a licenciamiento por parte del proveedor y en cuestión de hardware solo se utilizó el equipo soportado por el simulador, sin embargo pese a estas limitantes, la simulación puede considerarse confiable y funcional.

5.1 Simulador GNS3

GNS3 es un simulador de código abierto que simula redes complejas de una forma casi igual a las condiciones reales sin la necesidad de tener hardware especializado, como son routers o switches.

GNS3 provee una interfaz gráfica para diseñar y configurar redes virtuales, puede correr en cualquier PC con las capacidades requeridas y funciona en varios sistemas operativos como son Windows, Linux y MacOS X.

Para lograr una simulación precisa GNS3 usa emuladores como: Dynamips (Simulador de Cisco IOS), Virtual Box (Simulador de Servidores) y Qemu (Simulador de equipos como ASA, PIX e IPS)

Este software puede ser usado para simular nuevas soluciones antes de implementarse en la vida real con el fin de observar su comportamiento, también puede usarse para crear laboratorios para los interesados en obtener certificaciones CISCO o Juniper así como también para RedHat y Microsoft gracias a su emulador Virtual Box.

Para la simulación mostrada a continuación se usa la versión GNS3 Version 0.8.3.1

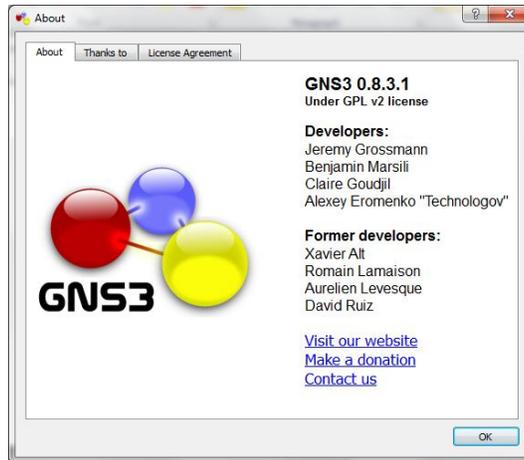


Figura 5.1.GNS3 Software versión.

5.2 Simulación

La simulación consta de dos ciudades interconectadas con fines de alta redundancia y con salidas a Internet independientes.

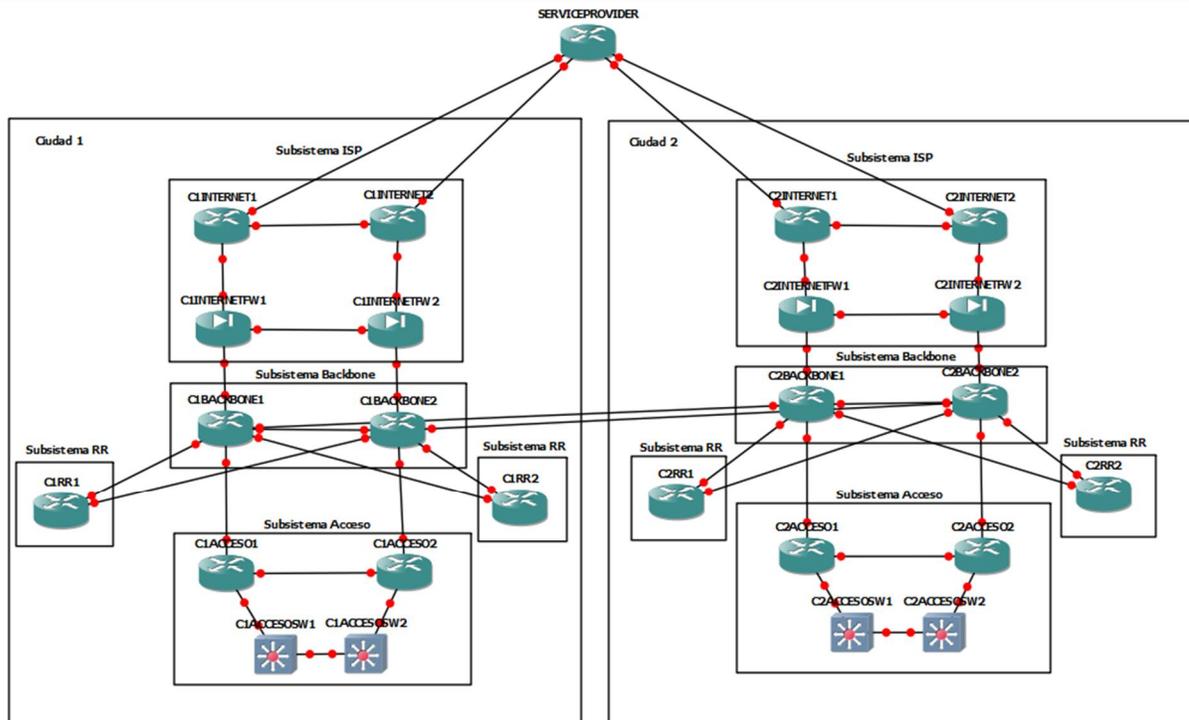


Figura 5.2. Topología de simulación.

Como se puede observar la simulación incluye un escenario con dos ciudades las cuales sirven de redundancia la una a la otra.

También se pueden observar los subsistemas mencionados en capítulos anteriores como son:

- a) Subsistema de acceso
- b) Subsistema de backbone
- c) Subsistema de route reflector
- d) Subsistema de ISP

Para la simulación se hizo uso de las siguientes imágenes de software y plataformas.

Sub-sistema	Nombre	Plataforma	Versión de Software
Acceso	C1AccesoSW1	Cisco 3745	c3745-advipservicesk9-mz124-15
	C1AccesoSW2	Cisco 3745	c3745-advipservicesk9-mz124-15
	C2AccesoSW1	Cisco 3745	c3745-advipservicesk9-mz124-15
	C2AccesoSW2	Cisco 3745	c3745-advipservicesk9-mz124-15
	C1Acceso1	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C1Acceso2	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C2Acceso1	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C2Acceso2	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
Backbone	C1Backbone1	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C1Backbone2	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C2Backbone1	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C2Backbone2	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
RR	C1RR1	Cisco 3660	c3660-telco-mz.124-25b
	C1RR2	Cisco 3660	c3660-telco-mz.124-25b
	C2RR1	Cisco 3660	c3660-telco-mz.124-25b
	C2RR2	Cisco 3660	c3660-telco-mz.124-25b
ISP	C1InternetFW1	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C1InternetFW2	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C2InternetFW1	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C2InternetFW2	Cisco 7206VXR NPE-400	c7200-adventerprisek9-mz.124-24.T5
	C1Internet1	Cisco 3660	c3660-telco-mz.124-25b
	C1Internet2	Cisco 3660	c3660-telco-mz.124-25b
	C2Internet1	Cisco 3660	c3660-telco-mz.124-25b
	C2Internet2	Cisco 3660	c3660-telco-mz.124-25b

Tabla 5.1. Imágenes de software y plataformas.

Información de las versiones:

Image Name	c7200-adventerprisek9-mz.124-24.T5.bin
Software	IOS
Release Number	12.4(24)T5
Platform Name	7200
Feature Set	ADVANCED ENTERPRISE SERVICES

Tabla 5.2. Version de IOS para Cisco 7200.

Image Name	c3660-telco-mz.124-25b.bin
Software	IOS
Release Number	12.4(25b)
Platform Name	3660
Feature Set	TELCO FEATURE SET

Tabla 5.3. Version de IOS para Cisco 3600.

Image Name	c3745-advipservicesk9-mz.124-16.bin
Software	IOS
Release Number	12.4(16)
Platform Name	3745
Feature Set	ADVANCED IP SERVICES

Tabla 5.4. Versión de IOS para Cisco 3700.

Las características específicas de cada versión pueden consultarse en: <http://tools.cisco.com/ITDIT/CFN/>

La topología muestra como se tienen dos ciudades con la misma estructura conectadas a un router que funge como emulador de un service provider anunciando una ruta de default y recibiendo los atributos por parte de los peer de BGP con el fin de tomar el mejor camino para el tráfico de entrada a la red.

Ambas ciudades se encuentran interconectadas por medio de conexiones directas, sin embargo en condiciones reales esta conexión puede hacerse por medio de anillos de fibra propios o por líneas rentadas siendo la primera opción la más confiable. Vease figura 5.2.

La simulación mostrada cuenta con todos los elementos descritos en el diseño así como también con las funcionalidades descritas. Sin embargo debido a licenciamiento y a recursos del sistema algunos de ellos fueron omitidos, por ejemplo la funcionalidad VPN FRR fue omitida ya que Cisco requiere un licenciamiento para poder añadir dicha funcionalidad, la otra funcionalidad omitida es BFD la cual consume muchos recursos del sistema haciendo que la simulación sea lenta y en casos se trabe por falta de memoria o uso excesivo de CPU.

5.3 Pruebas de simulación y resultados

5.3.1 Funcionamiento en condiciones normales

Prueba	Funcionamiento en condiciones normales.
Objetivo	Probar la simulación en condiciones normales.
Topología	
Procedimiento	Enviar un ping desde el Servidor R27 hacia la dirección 4.2.2.2 así como un trazado.
Resultados esperados	El ping debe completarse satisfactoriamente, el trazado debe salir por su salida a Internet local.
Resultados obtenidos	<p>Ciudad 1:</p> <pre>SERVER-C1#ping 4.2.2.2</pre> <p>Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 140/188/292 ms</p> <pre>SERVER-C1#traceroute 4.2.2.2</pre> <p>Type escape sequence to abort. Tracing the route to 4.2.2.2</p>

	1 10.45.0.2 68 msec 36 msec 44 msec 2 10.1.254.9 [MPLS: Label 23 Exp 0] 84 msec 48 msec 44 msec 3 10.1.254.10 56 msec 152 msec 92 msec 4 10.1.254.30 136 msec 148 msec 124 msec 5 200.139.131.1 184 msec * 148 msec
--	---

Tabla 5.5. Funcionamiento en condiciones normales.

5.3.2 Pérdida de poder en switch de acceso

Prueba	Pérdida de poder en switch de acceso.
Objetivo	Comprobar la alta disponibilidad cuando se pierde poder en un switch de acceso.
Topología	
Procedimiento	Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite el switch de acceso 1 mientras la ráfaga continuúa.
Resultados esperados	El servicio no debe interrumpirse o si se interrumpe debe recuperarse en un periodo corto de tiempo.
Resultados obtenidos	

	<pre>4 10.1.254.30 172 msec 132 msec 156 msec 5 200.139.131.1 212 msec * 216 msec SERVER-C1#traceroute 4.2.2.2 Durante la falla: Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.3 80 msec 80 msec 40 msec 2 10.1.255.5 [MPLS: Labels 34/23 Exp 0] 176 msec * 156 msec 3 10.1.254.9 [MPLS: Label 23 Exp 0] 104 msec 60 msec 112 msec 4 10.1.254.10 152 msec 152 msec 108 msec 5 10.1.254.30 184 msec 164 msec 172 msec 6200.139.131.1 256 msec * 332 msec</pre>
--	---

Tabla 5.6. Pérdida de poder en switch de acceso.

5.3.3 Pérdida de poder en ambos switches de acceso

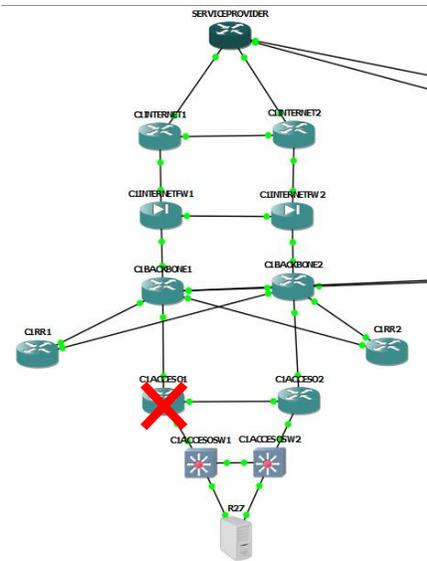
Prueba	Pérdida de poder en ambos switches de acceso
Objetivo	Comprobar pérdida de conectividad cuando ambos switches de acceso fallan.
Topología	
Procedimiento	<p>Desde el Server, enviar una ráfaga de pings hacia la dirección 4.2.2.2, mientras la ráfaga esta activa, apagar los dos switches de acceso.</p> <p>Verificar pérdida de conectividad, realizar un trazado antes y después de la falla.</p>
Resultados esperados	La conectividad se pierde completamente, el trazado no muestra salto alguno durante la falla.

<p>Resultados obtenidos</p>	<p>Antes de la falla:</p> <pre>SERVER-C1#ping ip 4.2.2.2 repeat 100000</pre> <p>Type escape sequence to abort. Sending 100000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !! !!!!!!.</p> <p>Success rate is 99 percent (146/147), round-trip min/avg/max = 96/169/328 ms</p> <pre>SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1#tracert 4.2.2.2</pre> <p>Type escape sequence to abort. Tracing the route to 4.2.2.2</p> <pre> 1 10.45.0.2 96 msec 44 msec 40 msec 2 10.1.254.9 [MPLS: Label 23 Exp 0] 92 msec 36 msec 84 msec 3 10.1.254.10 100 msec 120 msec 140 msec 4 10.1.254.30 164 msec 156 msec 216 msec 4 200.139.131.1 176 msec * 276 msec</pre> <p>Durante la falla:</p> <p>Se observa que la conectividad se pierde:</p> <pre>SERVER-C1#ping ip 4.2.2.2 repeat 100000</pre> <p>Type escape sequence to abort. Sending 100000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !!!!!!!!!!.....</p> <p>Success rate is 69 percent (79/113), round-trip min/avg/max = 96/164/340 ms</p> <p>El trazado no muestra salto alguno:</p> <pre>SERVER-C1#tracert 4.2.2.2</pre> <p>Type escape sequence to abort.</p>
------------------------------------	--

	Tracing the route to 4.2.2.2 1 * * * 2 * * * 3 * * * 4 * * * 5 * * * 6 * * * 7 * * * 8 * * * 9 * * * 10 * * * 11 * * * 12 * * * 13 * * * 14 * * *
--	---

Tabla 5.7. Pérdida de poder en ambos switch de acceso.

5.3.4 Pérdida de poder en router de acceso

Prueba	Pérdida de poder en router de acceso
Objetivo	Verificar la alta redundancia cuando uno de los routers de acceso pierde poder o es reiniciado.
Topología	
Procedimiento	<p>Desde el servidor, enviar una ráfaga de pings hacia la dirección 4.2.2.2, mientras la ráfaga se encuentra activa, deshabilitar el router de acceso 1.</p> <p>Capturar trazados antes y después de la falla.</p> <p>Verificar la cantidad de pings perdidos.</p>
Resultados esperados	<p>Se espera la pérdida del servicio cuando el router sea apagado, sin embargo el servicio debe reestablecerse en cuanto la tabla de ruteo converge.</p> <p>Vale la pena señalar que el tiempo que tarda la red en convergir puede mejorarse con el uso del protocolo BFD y el protocolo VPN FRR.</p>
Resultados obtenidos	<p>El trazado muestra la trayectoria por medio del router de acceso 1:</p>

	<pre>SERVER-C1#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 64 msec 56 msec 28 msec 2 10.1.254.9 [MPLS: Label 23 Exp 0] 116 msec 40 msec 64 msec 3 10.1.254.10 92 msec 120 msec 76 msec 4 10.1.254.30 124 msec 140 msec 216 msec 5 200.139.131.1 200 msec * 200 msec SERVER-C1# SERVER-C1# SERVER-C1#ping 4.2.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 140/170/204 ms Durante la falla: Se observa que el servicio se pierde momentáneamente debido a que el equipo es apagado, sin embargo en cuanto el IGP converge el servicio se restablece. En el trazado se observa que el camino es cambiado por medio del router de acceso 2. SERVER-C1#ping ip 4.2.2.2 repeat 100000 Type escape sequence to abort. Sending 100000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!!! !! !! !!!!!!!!!!!!!! Success rate is 88 percent (196/221), round-trip min/avg/max = 112/198/316 ms SERVER-C1#traceroute 4.2.2.2</pre>
--	---

	<p>Type escape sequence to abort. Tracing the route to 4.2.2.2</p> <pre> 1 10.45.0.3 36 msec 60 msec 28 msec 2 10.1.255.5 [MPLS: Labels 34/23 Exp 0] 120 msec 148 msec 132 msec 3 10.1.254.9 [MPLS: Label 23 Exp 0] 100 msec 132 msec 132 msec 4 10.1.254.10 128 msec 136 msec 120 msec 5 10.1.254.30 232 msec 192 msec 204 msec 5 200.139.131.1 236 msec * 236 msec </pre>
--	---

Tabla 5.8. Pérdida de poder en router de acceso.

5.3.5 Pérdida de poder en ambos routers de acceso

Prueba	Pérdida de poder en ambos routers de acceso
Objetivo	Verificar que la conectividad se pierde cuando ambos router de acceso fallan.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite ambos routers de acceso mientras la ráfaga continúa.</p> <p>Capturar trazados antes y después de la falla. Verificar la cantidad de pings perdidos.</p>
Resultados esperados	La conectividad debe perderse por completo.

<p>Resultados obtenidos</p>	<p>Antes de la falla:</p> <pre>SERVER-C1#ping ip 4.2. 2.2 repeat 100000</pre> <p>Type escape sequence to abort. Sending 100000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !! !!!!!!.</p> <p>Success rate is 99 percent (146/147), round-trip min/avg/max = 96/169/328 ms</p> <pre>SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1#tracert 4.2.2.2</pre> <p>Type escape sequence to abort. Tracing the route to 4.2.2.2</p> <pre> 1 10.45.0.2 96 msec 44 msec 40 msec 2 10.1.254.9 [MPLS: Label 23 Exp 0] 92 msec 36 msec 84 msec 3 10.1.254.10 100 msec 120 msec 140 msec 4 10.1.254.30 164 msec 156 msec 216 msec 6 200.139.131.1 176 msec * 276 msec</pre> <p>Durante la falla:</p> <p>Se observa que la conectividad se pierde:</p> <pre>SERVER-C1#ping ip 4.2.2.2 repeat 100000</pre> <p>Type escape sequence to abort. Sending 100000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !!!!!!!!!!!!.....</p> <p>Success rate is 69 percent (79/113), round-trip min/avg/max = 96/164/340 ms</p> <p>El trazado no muestra salto alguno:</p> <pre>SERVER-C1#tracert 4.2.2.2</pre> <p>Type escape sequence to abort.</p>
--	---

	Tracing the route to 4.2.2.2
	1 * * *
	2 * * *
	3 * * *
	4 * * *
	5 * * *
	6 * * *
	7 * * *
	8 * * *
	9 * * *
	10 * * *
	11 * * *

Tabla 5.9. Pérdida de poder en ambos router de acceso.

5.3.6 Pérdida de enlace entre routers de backbone y acceso

Prueba	Pérdida de enlace entre routers de backbone y acceso
Objetivo	Probar que el tráfico es enrutado vía el túnel de bypass por medio de MPLS TE FRR con pérdida mínima de tráfico.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite el link que une el router de acceso 1 al router de backbone1.</p> <p>Capturar trazados antes y después de la falla. Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico debe tomar otra ruta con mínima pérdida de tráfico.

<p>Resultados obtenidos</p>	<p>Antes de la falla:</p> <pre>SERVER-C1#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 76 msec 48 msec 28 msec 2 10.1.254.9 [MPLS: Label 23 Exp 0] 64 msec 56 msec 96 msec 3 10.1.254.10 164 msec 88 msec 80 msec 4 10.1.254.30 188 msec 196 msec 136 msec 5 200.139.131.1 224 msec * 168 msec SERVER-C1# SERVER-C1# SERVER-C1# SERVER-C1#ping 4.2.2.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 136/164/200 ms Durante la falla:<pre>SERVER-C1#ping ip 4.2.2.2 repeat 100000 Type escape sequence to abort. Sending 100000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !! !! !! !! !!!!!!!!!!!!!! SERVER-C1#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 96 msec 28 msec 32 msec 2 10.1.254.26 [MPLS: Labels 28/23 Exp 0] 172 msec 144 msec 184 msec</pre></pre>
--	--

	<p>3 10.1.255.5 [MPLS: Labels 37/23 Exp 0] 132 msec 152 msec 200 msec</p> <p>4 *</p> <p>10.1.254.9 [MPLS: Label 23 Exp 0] 104 msec 88 msec</p> <p>5 10.1.254.10 136 msec 192 msec 140 msec</p> <p>6 10.1.254.30 260 msec 292 msec 252 msec</p> <p>7 200.139.131.1 272 msec * 292 msec</p>
--	---

Tabla 5.10. Pérdida de enlace entre router de backbone y acceso.

5.3.7 Pérdida de poder en router de backbone

Prueba	Pérdida de poder en router de backbone
Objetivo	Comprobar alta disponibilidad cuando un router de backbone falla o es reiniciado.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación detenga el router de backbone1.</p> <p>Capturar trazados antes y después de la falla.</p> <p>Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico debe de usar el router de backbone 2 para salir a Internet.
Resultados obtenidos	<p>Antes de la falla:</p> <p>R27#traceroute 4.2.2.2</p> <p>Type escape sequence to abort.</p>

<pre>Tracing the route to 4.2.2.2 1 10.45.0.2 140 msec 68 msec 16 msec 2 100.0.0.1 [MPLS: Label 24 Exp 0] 260 msec 468 msec 312 msec 3 10.1.254.10 212 msec 368 msec 284 msec 4 10.1.254.30 584 msec 316 msec 252 msec 4 200.139.131.1 328 msec * * Durante la falla: R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !!!!!!!!!!!!!!!!!!!!!! !!!.....!!!!!! !! Success rate is 89 percent (198/221), round-trip min/avg/max = 104/257/504 ms R27#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 104 msec 84 msec 32 msec 2 10.1.254.26 [MPLS: Labels 27/31 Exp 0] 168 msec 112 msec 192 msec 3 10.1.255.9 [MPLS: Label 31 Exp 0] 168 msec 84 msec 60 msec 4 10.1.255.10 188 msec 152 msec 160 msec 5 10.1.255.30 192 msec 212 msec 200 msec 5 186.101.30.1 172 msec * 184 msec</pre>
--

Tabla 5.11. Pérdida de poder en router de backbone.

5.3.8 Pérdida de poder en ambos routers de backbone

Prueba	Pérdida de poder en ambos routers de backbone
Objetivo	Verificar pérdida completa de conectividad al fallar ambos router de backbone.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite ambos routers de backbone.</p> <p>Capturar trazados antes y después de la falla. Verificar la cantidad de pings perdidos.</p>
Resultados esperados	La conectividad debe perderse.
Resultados obtenidos	<pre>R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:U. U. U. U. U. Success rate is 0 percent (0/327)</pre>

Tabla 5.12. Pérdida de poder en ambos router de backbone.

5.3.9 Pérdida de poder en route reflector

Prueba	Pérdida de poder en route reflector
Objetivo	Verificar que la red puede trabajar con un solo RR en caso de que el otro falle.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite el router route reflector 1.</p> <p>Capturar trazados antes y después de la falla. Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico no debe verse afectado o la afectación debe ser mínima.
Resultados obtenidos	<p>Antes de la falla:</p> <pre>R27#ping ip 4.2.2.2 repeat 1000000</pre> <p>Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!</p> <p>Durante la falla:</p> <pre>R27#ping ip 4.2.2.2 repeat 1000000</pre> <p>Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !!</p>

Tabla 5.13. Pérdida de poder en route reflector.

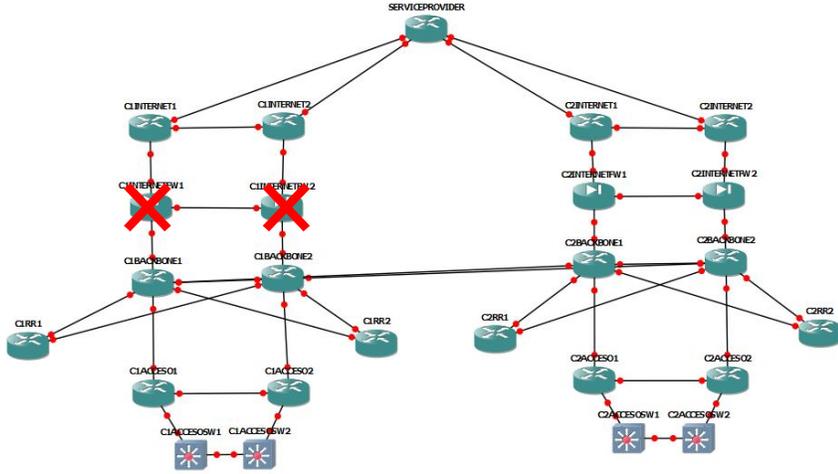
5.3.10 Pérdida de poder en firewall de Internet

Prueba	Pérdida de poder en firewall de Internet
Objetivo	Verificar que el tráfico no es afectado por la falla de un firewall de Internet.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite el firewall de Internet 1.</p> <p>Capturar trazados antes y después de la falla. Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico debe ser enviado por medio del firewall 2.
Resultados obtenidos	<p>Antes de la falla:</p> <pre>R27#traceroute 4.2.2.2</pre> <p>Type escape sequence to abort. Tracing the route to 4.2.2.2</p> <pre> 1 10.45.0.2 52 msec 56 msec 20 msec 2 10.1.254.9 [MPLS: Label 24 Exp 0] 72 msec 112 msec 76 msec 3 10.1.254.10 116 msec 112 msec 68 msec 4 10.1.254.30 168 msec 180 msec 172 msec 5 200.139.131.1 168 msec * 196 msec R27# R27# R27#</pre>

<pre>R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! Success rate is 98 percent (61/62), round-trip min/avg/max = 60/147/236 ms Durante la falla R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !!!!!!!!!!!!!!!!!!!!!!.....!!!!!! !! !! Success rate is 97 percent (266/272), round-trip min/avg/max = 68/182/420 ms R27# R27#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 124 msec 44 msec 76 msec 2 10.1.254.26 [MPLS: Labels 27/31 Exp 0] 112 msec 64 msec 28 msec 3 10.1.255.9 [MPLS: Label 31 Exp 0] 76 msec 92 msec 44 msec 4 10.1.255.10 96 msec 120 msec 132 msec 5 10.1.255.30 304 msec 164 msec 140 msec 6 186.101.30.1 204 msec * 180 msec</pre>
--

Tabla 5.14. Pérdida de poder en firewall de Internet.

5.3.11 Pérdida de poder en ambos firewall de Internet

Prueba	Pérdida de poder en ambos firewall de Internet
Objetivo	Verificar que en caso de falla de ambos firewall de Internet, el tráfico es desviado a la ciudad vecina con mínima afectación de servicio.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde el servidor R27, a continuación deshabilite ambos firewall de Internet.</p> <p>Capturar trazados antes y después de la falla.</p> <p>Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico se desvía a la salida de Internet de la ciudad 2.
Resultados obtenidos	<p>Antes de la falla:</p> <pre>R27#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 52 msec 56 msec 20 msec 2 10.1.254.9 [MPLS: Label 24 Exp 0] 72 msec 112 msec 76 msec 3 10.1.254.10 116 msec 112 msec 68 msec 4 10.1.254.30 168 msec 180 msec 172 msec 5 200.139.131.1 168 msec * 196 msec R27#</pre>

5.3.12 Pérdida de poder en router de Internet

Prueba	Pérdida de poder en router de Internet
Objetivo	Verificar que la pérdida de un router de Internet no impacta la conectividad a Internet.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde Servidor R27, a continuación deshabilite el router de Internet 1.</p> <p>Capturar trazados antes y después de la falla.</p> <p>Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico debe salir a Internet por medio del router de Internet 2.
Resultados obtenidos	<p>Antes de la falla:</p> <pre>R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !! !!!!!!.</pre>

<pre>Success rate is 98 percent (76/77), round-trip min/avg/max = 68/219/488 ms R27# R27# R27#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 88 msec 104 msec 280 msec 2 10.1.254.9 [MPLS: Label 58 Exp 0] 328 msec 192 msec 108 msec 3 10.1.254.10 160 msec 112 msec 60 msec 4 10.1.254.30 192 msec 276 msec 288 msec 5 200.139.131.1 260 msec * 252 msec R27# Durante la falla: R27# R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !! !!!!!!!!!!!!!!!!!!!!!! Success rate is 96 percent (152/157), round-trip min/avg/max = 84/222/628 ms R27# R27# R27#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 72 msec 76 msec 4 msec 2 10.1.254.26 [MPLS: Labels 27/50 Exp 0] 132 msec 216 msec 84 msec 3 10.1.255.9 [MPLS: Label 50 Exp 0] 68 msec 80 msec 96 msec 4 10.1.255.10 144 msec 136 msec 92 msec 5 10.1.255.30 200 msec 228 msec 172 msec 6 186.101.30.1 240 msec * 264 msec R27#</pre>
--

Tabla 5.16. Pérdida de poder en router de Internet.

5.3.13 Pérdida de poder en ambos router de Internet

Prueba	Pérdida de poder en ambos router de Internet
Objetivo	Verificar que en caso de falla de ambos router de Internet el tráfico es desviado a la ciudad vecina.
Topología	
Procedimiento	<p>Envíe una ráfaga de pings continuos hacia la dirección 4.2.2.2 desde R27, a continuación deshabilite ambos routers de Internet.</p> <p>Capturar trazados antes y después de la falla. Verificar la cantidad de pings perdidos.</p>
Resultados esperados	El tráfico es desviado a la ciudad vecina y el tráfico es recuperado con nula o mínima pérdida de tráfico.
Resultados obtenidos	<p>Antes de la falla:</p> <pre>R27#ping ip 4.2.2.2 repeat 1000000</pre> <p>Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!</p> <p>Success rate is 97 percent (39/40), round-trip min/avg/max = 84/238/432 ms</p> <pre>R27#traceroute 4.2.2.2</pre>

	<pre>Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 148 msec 36 msec 68 msec 2 10.1.254.9 [MPLS: Label 44 Exp 0] 112 msec 40 msec 52 msec 3 10.1.254.10 112 msec 200 msec 164 msec 4 10.1.254.30 244 msec 144 msec 308 msec 5 200.139.131.1 352 msec * 292 msec R27# Durante la falla: R27#ping ip 4.2.2.2 repeat 1000000 Type escape sequence to abort. Sending 1000000, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds: !!.....!!!!!!!!!!!!!!!!!!!!!!!!!!!! !! Success rate is 95 percent (119/125), round-trip min/avg/max = 80/213/684 ms R27# R27# R27#traceroute 4.2.2.2 Type escape sequence to abort. Tracing the route to 4.2.2.2 1 10.45.0.2 56 msec 24 msec 48 msec 2 10.1.254.5 [MPLS: Labels 30/29 Exp 0] 108 msec * 140 msec 3 10.2.254.9 [MPLS: Label 29 Exp 0] 176 msec * 128 msec 4 10.2.254.10 128 msec 88 msec 116 msec 5 10.2.254.30 120 msec 244 msec 140 msec 6 190.150.10.1 248 msec * 204 msec</pre>
--	--

Tabla 5.17. Pérdida de poder en ambos router de Internet.

RESUMEN DE RESULTADOS

Prueba	Paquetes perdidos durante la simulación de la falla
Funcionamiento en condiciones normales.	0
Pérdida de poder en switch de acceso.	1
Pérdida de poder en ambos switch de acceso	Se pierde totalmente conectividad
Pérdida de poder en router de acceso	25
Pérdida de poder en ambos routers de acceso	Se pierde totalmente conectividad
Pérdida de enlace entre routers de backbone y acceso	1
Pérdida de poder en router de backbone	23
Pérdida de poder en ambos routers de backbone	Se pierde totalmente conectividad
Pérdida de poder en route reflector	0
Pérdida de poder en firewall de Internet	6
Pérdida de poder en ambos firewall de Internet	5
Pérdida de poder en router de Internet	5
Pérdida de poder en ambos router de Internet	6

Tabla 5.18. Resumen de resultados en pruebas de simulación.

CONCLUSIONES

Por medio del presente trabajo se plasma gran parte de la teoría detrás de una red dorsal con mecanismos de alta disponibilidad, usada actualmente por los proveedores de servicio con el fin de asegurar la continuidad del servicio que ofertan a sus suscriptores.

Lo importante a destacar del presente trabajo es la gran cantidad de información que aporta para el diseño, implementación y operación de una red dorsal en alta disponibilidad para un proveedor de servicios; lo cual conlleva un alto marco teórico y experiencia en el uso del protocolo IP y los muchos protocolos que corren sobre él, y/o hacen uso del mismo.

Así, en el presente trabajo se logró pasar de lo general a lo particular, es decir, comenzando desde las bases teóricas del protocolo IP y temas avanzados de redes como MPLS, BGP, Traffic Engineering hasta el diseño, la simulación y las pruebas que avalan el correcto funcionamiento de las bases teóricas aplicadas correctamente, con el valioso complemento de la experiencia ganada en la implementación de redes complejas del tipo proveedor de servicio que los realizadores de la tesis han ganadó.

De esta forma, estamos seguros que el diseño mostrado es de gran valor al no ser solo un trabajo de investigación, sino más bien una guía para la implementación de una red en alta disponibilidad sustentando su funcionamiento por medio de pruebas semi-reales con resultados tangibles.

Con esto, empresas o instituciones que estén interesadas en asegurar la continuidad del servicio que ofrece a sus clientes hallaran en el presente trabajo información que le será útil para la correcta implementación de una red nueva que cuente con mecanismos de alta disponibilidad o bien para la optimización de una red existente que carezca de dichos mecanismos.

Vale la pena comentar que puede haber variantes en los diseños de redes con alta disponibilidad, esto en base al conocimiento y creatividad del ingeniero que las diseñe, así, se pueden lograr resultados similares de diferentes maneras, sin embargo, lo que nosotros intentamos plasmar en este trabajo es una solución estándar, la cual pueda servir de base para un diseño más específico.

Relativo a la simulación hecha y los resultados arrojados, es importante mencionar que se aprovecharon las bondades que existen hoy en día hablando de programas que te permiten simular redes complejas, que si bien aún tienen sus limitaciones, el poder realizar una simulación previa a la implementación de la red representa un gran valor como es poder obtener resultados y analizar el comportamiento esperado de la red con el fin de ahorrar tiempo y dinero.

Así, después de este trabajo concluimos un posible camino o metodología para la realización de una red como es:

- 1.- Planteamiento de diseño de alto nivel de acuerdo a los requerimientos del cliente.
- 2.- Simulación del diseño propuesto y evaluación de resultados.
- 3.- Implementación y puesta a prueba en un ambiente controlado como es un laboratorio.
- 4.- Implementación formal en campo.

Finalmente hay que comentar que aunque se hacen esfuerzos por tener una red de alta disponibilidad, siempre pueden existir factores de cualquier tipo que siempre tendrán alguna probabilidad de falla, sin embargo lo que intentamos con el presente trabajo es que dicha falla afecte el menor tiempo y al menor número de usuarios, y aunque sabemos que este tipo de diseños pueden tener un costo mayor al que podría tener una red sin alta disponibilidad, consideramos que la inversión se puede recuperar al mediano y largo plazo, por lo que los proveedores de servicios que cuidan la calidad de su servicio y que quieren la satisfacción del cliente, deberían considerar este tipo de diseños como una inversión ya que los clientes cada día son más exigentes y las regulaciones gubernamentales más estrictas.

ÍNDICE DE TABLAS

Tabla 2.1 Cronología de las telecomunicaciones.	11
Tabla 2.2 Capas del modelo OSI.	15
Tabla 2.3 Capas del modelo TCP/IP.	16
Tabla 2.4 Simbología de equipos de datos.	18
Tabla 2.5 Topologías de Red.	19
Tabla 2.6 Clases de direcciones IPv4.	22
Tabla 2.7 Ejemplo de subneteo.	25
Tabla 2.8 Comparación entre ruteo estático y dinámico.	27
Tabla 2.9 Clasificación de los protocolos de ruteo.	31
Tabla 2.10 Distancia administrativa por defecto de los protocolos de ruteo, CISCO Systems.	32
Tabla 2.11 LSA's OPSF.	34
Tabla 3.1. Variantes de LSR's.	45
Tabla 3.2 Enfoques de técnicas para reducción de impacto en el servicio en caso de falla.	50
Tabla 5.1. Imágenes de software y plataformas.	103
Tabla 5.2. Version de IOS para Cisco 7200.	104
Tabla 5.3. Version de IOS para Cisco 3600.	104
Tabla 5.4. Versión de IOS para Cisco 3700.	104
Tabla 5.5. Funcionamiento en condiciones normales.	107

Tabla 5.6. Pérdida de poder en switch de acceso.	110
Tabla 5.7. Pérdida de poder en ambos switch de acceso.	113
Tabla 5.8. Pérdida de poder en router de acceso.	116
Tabla 5.9. Pérdida de poder en ambos router de acceso.	118
Tabla 5.10. Pérdida de enlace entre router de backbone y acceso.	120
Tabla 5.11. Pérdida de poder en router de backbone.	121
Tabla 5.12. Pérdida de poder en ambos router de backbone.	122
Tabla 5.13. Pérdida de poder en route reflector.	124
Tabla 5.14. Pérdida de poder en firewall de Internet.	125
Tabla 5.15. Pérdida de poder en ambos firewall de Internet.	127
Tabla 5.16. Pérdida de poder en router de Internet.	129
Tabla 5.17. Pérdida de poder en ambos router de Internet.	131
Tabla 5.18. Resumen de resultados en pruebas de simulación.	132
Tabla A.1. Direccionamiento público y privado global.	153
Tabla A.2. Direccionamiento IP Ciudad 1.	154
Tabla A.3. Direccionamiento IP ciudad 2.	155

ÍNDICE DE FIGURAS

Figura 2.1 Topología Jerárquica.	21
Figura 2.2 Encabezado del paquete IPv4.	22
Figura 2.3 Ejemplo de subnet.	24
Figura 2.4 Protocolos de ruteo.	28
Figura 2.5 Atributos de BGP.	37
Figura 3.1. Encabezado MPLS.	44
Figura 3.2. Técnica IP Fast Re-Route.	51
Figura 3.3. Técnica VRRP.	52
Figura 3.4. TE FRR protección de enlace.	53
Figura 3.5 TE FRR protección de nodo.	54
Figura 3.6. VPN FRR.	55
Figura 4.1. Redundancia geográfica.	58
Figura 4.2. Redundancia Local.	59
Figura 4.3. Desglose de subsistemas.	60
Figura 4.4. Subsistema de acceso.	60
Figura 4.5. Subsistema de backbone.	61
Figura 4.6. Subsistema de route reflector.	62
Figura 4.7. Subsistema de Internet.	62
Figura 4.8. Capas lógicas.	63
Figura 4.9. Segmentación en VLAN de switches de acceso.	64
Figura 4.10. VRRP en routers de acceso.	65
Figura 4.11. Flujo de datos en condiciones normales.	66
Figura 4.12. IP FRR - Flujo de datos en caso de falla.	67

Figura 4.13. Funcionamiento de VPN FRR.	68
Figura 4.14. OSPF entre subsistemas backbone y acceso.	69
Figura 4.15. Marcado de comunidades y RD en backbone.	70
Figura 4.16. Funcionamiento MPLS TE FRR.	72
Figura 4.17. Vecindades MP-BGP.	73
Figura 4.18. Subsistema ISP.	74
Figura 4.19. Flujos en condiciones normales.	76
Figura 4.20. Pérdida de poder en switch de acceso.	80
Figura 4.22. Pérdida de poder en router de acceso.	82
Figura 4.23. Pérdida de poder en ambos routers de acceso.	85
Figura 4.24. Pérdida de enlace entre equipos de backbone y acceso.	85
Figura 4.25. Pérdida de poder en router de backbone.	87
Figura 4.26. Pérdida de poder en ambos routers de backbone.	89
Figura 4.27. Pérdida de poder en route reflector.	90
Figura 4.28. Pérdida de poder en firewall de Internet.	91
Figura 4.29. Pérdida de poder en ambos firewall de Internet.	93
Figura 4.30. Pérdida de poder en router de Internet.	95
Figura 4.31. Pérdida de poder en ambos router de Internet.	96
Figura 5.1. GNS3 Software versión.	102
Figura 5.2. Topología de simulación.	102

GLOSARIO

A

Acknowledge (en español: acuse de recibido). Tipo de mensaje en un protocolo que sirve para confirmar la recepción de un mensaje.

Active (en español: activo). Estado de un protocolo en el cual se encuentra realizando acciones varias que permitan converger la tabla de ruteo.

Aggregate (en español: agregado).

AS-PATH (Autonomous System Path; en español: Camino de Sistemas Autónomos). Atributo de BGP para evitar bucles de ruteo.

Autonomous System (en español: Sistema autónomo). Conjunto de equipos administrados por una misma entidad que se rige bajo sus propias normas y que en conjunto forman un sistema.

B

Backbone (en español: Red dorsal). Término empleado para referirse a la parte de la red donde se concentran los equipos más robustos.

Backup (en español: respaldo). Acción mediante el cual se tiene una replica de alguna configuración o de algún enlace para términos de poder usarlo en caso de que se pierda la copia original.

bfd (Bidirectional Forwarding Detection; en español: Detección de reenvío bidireccional). Protocolo que permite la detección rápida de pérdida de conectividad entre elementos de la red.

BGPv4 (Border Gateway Protocol Version 4; en español: Protocolo formterizo de puerta de salida, versión 4). Protocolo de ruteo empleado para intercambio de rutas entre dos sistemas autónomos diferentes.

Bypass (en español: desviación).

BW (Bandwith; en español: Ancho de banda). Término empleado para expresar la cantidad de información que se puede transmitir en un tiempo determinado.

C

CE (Customer Edge, en español: Frontera de cliente). Término en una arquitectura MPLS para definir el equipo que representa el borde del cliente.

CIDR (Classless Inter Domain Routing; en español: Enrutamiento entre dominios sin clases). Estándar de red que permite el uso de la técnica VLSM.

Classfull (en español: con clase). Término en redes usado para denotar un segmento de red IP que pertenece a las clases de direccionamiento A, B, C o D.

Classless (en español: sin clase). Término en redes usado para denotar que un segmento de red IP no pertenece a las clases de direccionamiento A, B, C o D.

CORE (en español: núcleo). Término relativo a la parte de la red esencial para su funcionamiento.

CPU (Central Process Unit; en español: unidad central de proceso). Componente físico de una computadora encargada de procesar la información.

CR-LSP (Constraint-based Routing Label Distribution Protocol; en español: Protocolo de enrutamiento de distribución de etiquetas basado en restricciones). Es un mecanismo que amplía las capacidades de LDP para cumplir con los requisitos de ingeniería de tráfico.

CS (Circuit Switching; en español: Conmutación de circuitos). Dominio en una red móvil que corresponde al procesamiento de circuitos de voz.

D

DBD (Database Description; en español: Descripción de la base de datos). Es un mensaje que contiene de manera abreviada una lista de los estados de enlace que son enviados por otros routers.

Default (en español: valor por defecto). Valor de una variable que viene seleccionada desde su fabricación o creación.

DDoS (Distributed Denial of Service; en español: Denegación de servicio distribuido). Ataque proveniente de diversas fuentes que afectan la disponibilidad de un servicio.

Dijkstra SPF (Dijkstra Shortest Path First; en español: Dijkstra trayectoria más corta primero). Es un algoritmo para la determinación de la trayectoria más corta, es empleado como algoritmo base en OSPF.

Downlink (en español: enlace descendente).

Downstream (en español: corriente abajo).

DOWN/DOWN (en español: abajo/abajo). Estado de una interfaz en el cual no tiene conexión tanto física como lógica hacia la red.

Dual-homed (en español: doblemente alojada). Término usado en redes de datos para referirse a escenarios donde se tienen dos enlaces de Internet para fines de recuperación ante fallas.

E

EBGP (External Border Gateway Protocol; en español: Protocolo externo de puerta de enlace fronterizo). Hace referencia al intercambio de rutas empleando BGP entre dos sistemas autónomos diferentes.

Edge (en español: borde).

EGP (External Gateway Protocol; en español: Protocolo exterior de puerta de enlace). Es un protocolo estándar usado para intercambiar información de enrutamiento entre sistemas autónomos.

Egress (en español: salida).

Established (en español: establecido). Estado en el que se encuentra un encaminador corriendo el protocolo BGP en el cuál ha intercambiado información de ruteo con otro encaminador.

EXP (abreviación de Experimental, en español: experimental). Conjunto de tres bits dentro del encabezado impuesto por el protocolo MPLS para fines de calidad de servicio.

F

FEC (Forwarding Equivalent Class; en español: clase equivalente de expedición). Término dentro del protocolo MPLS para denotar distintos flujos de tráfico que reciben el mismo tratamiento en cada enrutador habilitado para MPLS.

FIB (Forwarding Information Base; en español: Base de información de expedición). Tabla lógica dentro de un enrutador que guarda información acerca del tratamiento que se le dará a un paquete de información basado en sus características.

Firewall (en español: pared de fuego). Elemento de red dedicado a filtrar tráfico que pase a través de él entre segmentos de red basando su decisión en campos dentro de los encabezados de la pila TCP/IP.

FRR (Fast Re-Route; en español: Re-Enrutamiento rápido): Protocolo empleado en redes MPLS que permite enrutar el tráfico rápidamente por un camino alternativo cuando el principal por alguna razón ha dejado de funcionar.

Full-mesh (en español: malla completa). Tipo de topología que pueden seguir las redes de datos.

G

Gateway (en español: puerta de salida).

GR (Graceful Restart; en español: reinicio agraciado). Protocolo encargado de evitar pérdida de datos durante una falla en protocolos de ruteo que lo implementan además de ser un mecanismo que propicia la rápida convergencia del protocolo de ruteo ante una falla.

H

Hardware (en español: material físico informático). Componente físico de cualquier elemento de red.

Hello (en español: hola). En telecomunicaciones se usa comúnmente para referirse al mensaje usado por varios protocolos de ruteo con el fin de descubrir vecinos con los cuales formar vecindades para intercambiar rutas IP.

Host (en español: anfitrión). Término usado en redes de datos para denotar a un equipo terminal que posee solo una dirección IP.

Hub (en español: centro de actividad). Elemento de red que se emplea para conectar varios host a nivel físico.

I

IAB (Internet Architecture Board; en español: Dirección de Arquitectura de Internet). Junta directiva de la arquitectura de Internet protocolos utilizados en la arquitectura TCP/IP.

IANA (Internet Assigned Numbers Authority, en español: Autoridad de números asignada por Internet). Autoridad asignadora de direccionamiento de Internet a nivel mundial.

Idle (en español: Inactivo). Estado en el cual un protocolo de ruteo no se encuentra realizando ninguna actividad.

IEEE (Institute of Electrical and Electronics Engineers; en español: Instituto de Ingeniería Eléctrica y Electrónica). Asociación mundial de técnicos e ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas

IETF (Internet Engineering Task Force; en español: Grupo de trabajo de Ingeniería de Internet). Grupo de trabajo encargado de desarrollar y promover estándares para el desarrollo de Internet.

IGP (Interior Gateway Protocol; en español: Protocolo de Gateway Interior). Hace referencia a los protocolos utilizados dentro de un mismo sistema autónomo.

Ingress (en español: Ingreso, entrada).

IP (Internet Protocol; en español: Protocolo de Internet). Es el protocolo principal de Internet y la base de los demás protocolos empleados que se emplean para la comunicación entre dispositivos conectados en red. Su función principal es establecer la comunicación bidireccional entre dos dispositivos mediante la conmutación de paquetes.

IP-FRR (Internet Protocol Fast Re-Route; en español: desvío rápido del protocolo IP). Técnica de alta disponibilidad que funciona sobre IP para protección de flujos de tráfico.

ISO (International Organization for Standardization; en español: Organización Internacional para la Estandarización). Organización encargada de desarrollar y publicar estándares internacionales.

ISP (Internet Service Provider; en español: Proveedor de Servicios de Internet). Se refiere a cualquier empresa con la capacidad de brindar conexión de Internet a sus clientes.

ITU (International Telecommunications Union; en español: Unión Internacional de Telecomunicaciones). Es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación.

K

Keepalive (en español: sobrevivir). Tipo de mensaje intercambiado por los protocolos de ruteo encargados de advertir al equipo vecino que se encuentran aun presentes y funcionando.

L

L2VPN (Layer 2 Virtual Private Network; en español: Red Privada Virtual Capa 2). Aplicación que permite la emulación de circuitos virtuales para transportar tramas (Ethernet, FR, ATM, y PPP) a través de la red MPLS.

L3VPN (Layer 3 Virtual Private Network; en español: Red Privada Virtual Capa 3). Aplicación que permite la emulación de routers virtuales de tal manera que se puede manejar el tráfico de diversos clientes en un mismo router sin que se mezcle el tráfico de dichos clientes.

LAN (Local Area Network; en español: Red de Área Local). Se refiere a una red que interconecta dispositivos dentro de un área limitada.

Label (en español: etiqueta).

LDP (Label Distribution Protocol; en español: Protocolo de Distribución de Etiquetas). Protocolo empleado en redes MPLS para la distribución dinámica de etiquetas.

LOCAL PREFERENCE (en español: preferencia local). Atributo del protocolo BGP que influye en la decisión para la salida del tráfico del sistema autónomo.

LSA (Link State Advertisement; en español: Aviso de Estado Enlace). Hace referencia a los mensajes empleados por OSPF para anunciar información referente a los enlaces del router.

LSAck (Link State Acknowledge; en español: Notificación de Estado Enlace). Mensajes de notificación enviados por los routers para informar que ha recibido un mensaje LSU.

LSDB (Link State Data Base; en español: Base de Datos del Estado Enlace). Base de datos con la información de los enlaces de los routers, dicha información es empleada por los routers para calcular las mejores rutas.

LSP (Label Switched Path; en español: Intercambio de Rutas por Etiqueta). Nombre genérico que se le da al túnel MPLS establecido entre dos dispositivos, el LSP es unidireccional.

LSU (Link State Update; en español: Actualización del Estado del Enlace). Hace referencia a mensajes que se emplean para responder a los LSRs, así como para anunciar nueva información.

LSR (Link State Request; en español: Solicitud del Estado del Enlace). Mensajes utilizados por los routers para pedir información más detallada de los enlaces de sus vecinos.

M

MAN (Metropolitan Area Network; en español: Red de área metropolitana). Hace referencia a una red que interconecta LAN's dentro de una misma ciudad.

MASTER (en español: maestro). Término coloquial en redes de datos que se refiere al elemento o dispositivo que se encuentra en estado activo entre un conjunto de elementos que se encuentran pasivos.

MED (Multi-Exit Discriminator; en español: Discriminador de salida múltiples). Atributo de BGP propio al Sistema autónomo que influye en la decisión de envío de tráfico.

MPLS (Multi Protocol Label Switching; en español: Conmutación de etiquetas multiprotocolo). Mecanismo de transporte de datos estándar creado por la IETF que ha logrado colocarse como una solución para las nuevas redes convergentes ya que permite el manejo de diferente tipo de tráfico sobre el mismo medio.

MP-BGP (Multi-Protocol Border Gateway Protocol; en español: Protocolo fronterizo de puerta de enlace, multiprotocolo). Extensión del protocolo BGP para trabajar con MPLS y otros protocolos.

MPLS TE FRR (Multi Protocol Label Switching Traffic Engineering Fast Re-Route; en español: conmutación de etiquetas multiprotocolo, ingeniería de tráfico, re-enrutamiento rápido). Protocolo de alta disponibilidad usado en arquitecturas MPLS que provee protección ante fallas físicas en enlaces o equipos.

Multicast. Término usado para denotar un tipo de entrega de tráfico cuyo principio se basa en distribuir un mismo flujo de datos a varios receptores simultáneamente.

N

NAT (Network Address Translation; en español: Traslación de la dirección de red). Mecanismo empleado para trasladar direcciones IP, normalmente usado para trasladar direccionamiento privado a un direccionamiento público.

Network (en español: red). Término usado en redes IP para referirse a un conjunto de equipos terminales que se comunican entre ellos y comparten recursos.

NEXT-HOP (en español: siguiente salto). Término usado en BGP relativo al siguiente punto donde debe ser enviado el tráfico.

NIC (Network Information Center; en español: Centro de información de red). Responsable de recibir y distribuir los protocolos de la red.

NOC (Network Operation Center; en español: Centro de operación de red). Encargada de administrar los enlaces de telecomunicaciones y los ordenadores que actúan como sistemas de conmutación nodal y forman el núcleo de la red.

O

OSPF (Open Shortest Path First; en español: El camino más corto primero). Protocolo de ruteo que emplea la información del estado de los enlaces para calcular mediante un algoritmo la ruta más óptima.

O&M (Operation & Maintenance, en español: Operación y Mantenimiento). Término usado en redes para referirse a la administración de los elementos de red en una red.

P

Path (en español: camino). Término usado en redes de datos para hacer referencia a la trayectoria que sigue la información dentro de una red de datos.

PE (provider edge; en español: borde del proveedor). Elemento que se encuentra en la frontera de la red del proveedor de servicios, generalmente se conecta a un equipo en la red del cliente llamado CE.

Peer (en español: par). Término usado en protocolos de ruteo para hacer referencia a un elemento de red con el cual se comunica otro elemento de red que corre el mismo protocolo de ruteo.

Pool (en español: estanque, piscina). Término en redes de datos usado para referirse a un conjunto de elementos lógicos como pueden ser direcciones IP's.

PS (Packet Switching, en español: Conmutación de paquetes). Dominio en una red móvil que corresponde al procesamiento de paquetes IP.

R

RD (Route Distinguisher, en español: Caracterizador de ruta). Atributo en BGP para definir una instancia de ruteo.

Route-Policy (en español: política de ruteo). Configuración hecha en un dispositivo de red con el fin de influenciar su comportamiento al momento de encaminar el tráfico.

Route-reflector (en español: reflector de rutas). Elemento dentro de una red de datos que implementa BGP y esta encargado de advertir rutas que recibe de ciertos clientes hacia otros.

Router (en español: encaminador). Elemento de red encargado de enrutar los paquetes de datos dentro de una red con el fin de que llegue a su destino desde la fuente. Trabaja en la capa número 3 de la pila de protocolos del modelo OSI.

RSVP (Reservation Protocol; en español: Protocolo de reservación). Protocolo encargado de reservar recursos como ancho de banda dentro de una red con el fin de garantizar cierta calidad de servicio a un flujo de datos.

Ruteo. Anglicismo usado para referirse a la acción de un encaminador al enrutar el tráfico de datos.

S

SLA (Service Level Agreement; en español: Acuerdo de niveles de servicio). Acuerdo que se firma entre dos partes para definir los niveles de servicio que proporciona un proveedor de servicio a sus clientes. Las variables pueden ser jitter, packet loss, delay, Etc.

SLAVE (en español: esclavo). Elemento dentro de un arreglo de equipos, dispositivos o elementos de red que obedece las instrucciones del elemento MASTER y que se puede encontrar en estado inactivo mientras el elemento MASTER se encuentre operando correctamente.

Software. Componente lógico de un dispositivo informático.

SSO (Stateful Switchover; en español: Conmutación de estado). Protocolo propietario de Cisco para la sincronización de tablas de sesiones entre dos firewall que se encuentran en alta disponibilidad.

Subnet (abreviación de las palabras en ingles "Subdivided Network"; en español: red subdividida).

Subnetting (expresión de acción proveniente de la abreviación de las palabras en inglés "Subdivided Network"; en español: red subdividida). Acción de dividir lógicamente un segmento de redes IP en varios segmentos más pequeños.

Summary (en español: resumen).

Stub (en español: colilla). Término en redes usado para denotar un segmento de la red que representa una rama o terminación de un conjunto de elementos de red.

Switch (en español: conmutador). Elemento de red encargado de conmutar paquetes de información entre distintos host basando su decisión en las direcciones físicas de destino dentro del encabezado.

Ethernet. Trabaja en la capa 2 de la pila de protocolos del modelo OSI.

U

Uplink (en español: enlace ascendente).

V

VLAN (Virtual Local Area Network; en español: Red de área local virtual). División lógica dentro de un switch con tablas de direcciones físicas independientes.

VLSM (Variable Length Subnet Mask; en español: Máscara de red de longitud variable). Es el resultado del proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según se adaptan a las necesidades de hosts por subred.

VPN FRR (Virtual Private Network Fast Re-Route; en español: Desvío rápido de red virtual privada). Mecanismo de alta disponibilidad que corre sobre BGP para escenarios donde se tiene doble puerta de enlace.

VRF (Virtual Routing and Forwarding; en español: Instancia de ruteo virtual). División lógica en un router que posee su propia tabla de ruteo.

VRRP (Virtual Router Redundancy Protocol; en español: Protocolo de redundancia de router virtual). Protocolo de redundancia que permite incrementar la disponibilidad de la puerta de enlace predeterminada en una misma subred.

W

WAN (Wide Area Network; en español: Red de área amplia). Red que se caracteriza por abarcar un área geográfica relativamente grande, un ejemplo de este tipo de redes es el Internet.

WWW (World Wide Web; en español: Red informática mundial). Normalmente se conoce solo como Web y es un sistema de distribución de documentos de hipertexto o hipermedios conectados vía Internet.

REFERENCIAS

Bibliografía

- Academy_Cisco_Networking. (Versión 3.1). *CCNA 1 & 2. Program*, Cisco Networking Academy.
- Alwayn, V. (2002). *Advanced MPLS Design and Implementation*. Indianapolis, USA: CISCO Press.
- Doyle, J. (2006). *CCIE Professional Development Routing TCP/IP Vol I*. Indianapolis, USA: CISCO Press.
- Doyle, J. (2006). *CCIE Professional Development Routing TCP/IP Vol II*. Indianapolis, USA: CISCO Press.
- Ghein, L. D. (2007). *MPLS Fundamentals*. Indianapolis, USA: CISCO Press.
- Hussain, I. (2004). *Fault-Tolerant IP and MPLS Networks*. Cisco Press.
- Odom, W. (2008). *CCENT/CCNA ICND1 Official Exam Certification Guide 2nd Edition*. Indianapolis USA: CISCO Press.
- Odom, W. (2008). *CCNA ICND2 Official Certification Guide 2nd edition*. Indianapolis, USA: CISCO Press.
- Odom, W. (2010). *CCIE Routing and Switching Certification Guide 4 edition*. Indianapolis, USA: CISCO Press.
- Odom, W. (2010). *CCNP Route 642-902 Official Certification Guide*. Indianapolis, USA: CISCO Press.

Mesografía

- Eveliux. (24 de julio de 2007). Recuperado el 14 de Febrero de 2013, de <http://www.eveliux.com/mx/estandares-y-organizaciones.php>
- CISCO. (s.f.). *BGP PIC Edge for IP and MPLS-VPN*. Recuperado el mayo de 2013, de Cisco Support: http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/xe-3s/irg-bgp-mp-pic.html
- CISCO. (s.f.). *CISCO Feature Navigator*. Recuperado el agosto de 2013, de CISCO Products & Services: <http://tools.cisco.com/ITDIT/CFN/>
- IEEE. (s.f.). *The Institute of Electrical and Electronics Engineers*. Recuperado el Diciembre de 2012, de <http://www.ieee.org.mx>

IETF. (s.f.). *Internet Engineering Task Force*. Recuperado el Diciembre de 2012, de <http://www.ietf.org/>

ISO. (s.f.). *International Organization for Standardization*. Recuperado el diciembre de 2012, de <http://www.iso.org>

UIT. (s.f.). *Unión Internacional de Telecomunicaciones*. Recuperado el diciembre de 2012, de <http://www.itu.int>

GNS3. (abril de 2013). *GNS3*. Obtenido de <http://www.gns3.net/>

ANEXO A: DIRECCIONAMIENTO IP

Planeación IP											
Direccionamiento Público											
		Rango Total		Segmento NAT							
		Segmento	Mascara	Segmento	Mascara						
Ciudad 1:		201.175.0.0	255.255.252.0	201.175.0.0	255.255.255.0						
Ciudad 2:		201.175.4.0	255.255.252.0	201.175.4.0	255.255.255.0						
Direccionamiento Privado											
				Rango Total							
				Segmento	Mascara						
				10.0.0.0	255.0.0.0						
		Rango Local		Segmento Servicio Loopback		Segmento O&M Loopback		Segmento Servicio Enlaces		Segmento APN Pool	
		Segmento	Mascara	Segmento	Mascara	Segmento	Mascara	Segmento	Mascara	Segmento	Mascara
Ciudad 1:		10.1.0.0	255.255.0.0	10.1.99.0	255.255.255.0	10.1.100.0	255.255.255.0	10.1.254.0	255.255.254.0	10.45.0.0	255.255.0.0
Ciudad 2:		10.2.0.0	255.255.0.0	10.2.99.0	255.255.255.0	10.2.100.0	255.255.255.0	10.2.254.0	255.255.254.0	10.46.0.0	255.255.0.0

Tabla A.1. Direccionamiento público y privado global.

Ciudad 1															
LOCAL								REMOTE							
Ciudad	Equipo	Slot	Port	Dot1q	VRRP VIP	IP	Mascara	Ciudad	Equipo	Slot	Port	Dot1q	VRRP VIP	IP	Mascara
Ciudad 1	C1BB1	0	0	N/A	N/A	10.1.254.1	30	Ciudad 1	C1BB2	0	0	N/A	N/A	10.1.254.2	30
Ciudad 1	C1BB1	1	0	N/A	N/A	10.1.254.5	30	Ciudad 1	C1ACC1	0	0	N/A	N/A	10.1.254.6	30
Ciudad 1	C1BB1	2	0	N/A	N/A	10.1.254.9	30	Ciudad 1	C1FW1	0	0	N/A	N/A	10.1.254.10	30
Ciudad 1	C1BB1	3	0	N/A	N/A	10.1.254.13	30	Ciudad 1	C1RR1	0	0	N/A	N/A	10.1.254.14	30
Ciudad 1	C1BB1	4	0	N/A	N/A	10.1.254.17	30	Ciudad 1	C1RR2	0	1	N/A	N/A	10.1.254.18	30
Ciudad 1	C1BB1	5	0	N/A	N/A	10.1.254.21	30	Ciudad 2	C2BB1	5	0	N/A	N/A	10.1.254.22	30
Ciudad 1	C1BB1	6	0	DISPONIBLE											
Ciudad 1	C1BB2	0	0	N/A	N/A	10.1.254.2	30	Ciudad 1	C1BB1	0	0	N/A	N/A	10.1.254.1	30
Ciudad 1	C1BB2	1	0	N/A	N/A	10.1.255.5	30	Ciudad 1	C1ACC2	0	0	N/A	N/A	10.1.255.6	30
Ciudad 1	C1BB2	2	0	N/A	N/A	10.1.255.9	30	Ciudad 1	C1FW2	0	0	N/A	N/A	10.1.255.10	30
Ciudad 1	C1BB2	3	0	N/A	N/A	10.1.255.13	30	Ciudad 1	C1RR2	0	0	N/A	N/A	10.1.255.14	30
Ciudad 1	C1BB2	4	0	N/A	N/A	10.1.255.17	30	Ciudad 1	C1RR1	0	1	N/A	N/A	10.1.255.18	30
Ciudad 1	C1BB2	5	0	N/A	N/A	10.1.255.21	30	Ciudad 2	C2BB2	5	0	N/A	N/A	10.1.255.22	30
Ciudad 1	C1BB2	6	0	DISPONIBLE											
Ciudad 1	C1ACC1	0	0	N/A	N/A	10.1.254.6	30	Ciudad 1	C1BB1	1	0	N/A	N/A	10.1.254.5	30
Ciudad 1	C1ACC1	1	0	N/A	N/A	10.1.254.25	30	Ciudad 1	C1ACC2	1	0	N/A	N/A	10.1.254.26	30
Ciudad 1	C1ACC1	2	0	2	10.1.1.1	10.1.1.2	25	Ciudad 1	C1ACCSW1	1	0	2,10	N/A	L2	L2
Ciudad 1	C1ACC1	2	0	10	10.45.0.1	10.45.0.2	16	Ciudad 1	C1ACCSW1	1	0	2,10	N/A	L2	L2
Ciudad 1	C1ACC1	3	0	DISPONIBLE											
Ciudad 1	C1ACC2	0	0	N/A	N/A	10.1.255.6	30	Ciudad 1	C1BB2	1	0	N/A	N/A	10.1.255.5	30
Ciudad 1	C1ACC2	1	0	N/A	N/A	10.1.254.26	30	Ciudad 1	C1ACC1	1	0	N/A	N/A	10.1.254.25	30
Ciudad 1	C1ACC2	2	0	2	10.1.1.1	10.1.1.3	25	Ciudad 1	C1ACCSW2	1	0	2,10	N/A	L2	L2
Ciudad 1	C1ACC2	2	0	10	10.45.0.1	10.45.0.3	16	Ciudad 1	C1ACCSW2	1	0	2,10	N/A	L2	L2
Ciudad 1	C1ACC2	3	0	DISPONIBLE											
Ciudad 1	C1FW1	0	0	N/A	N/A	10.1.254.10	30	Ciudad 1	C1BB1	2	0	N/A	N/A	10.1.254.9	30
Ciudad 1	C1FW1	1	0	N/A	N/A	10.1.254.29	30	Ciudad 1	C1INT1	0	0	N/A	N/A	10.1.254.30	30
Ciudad 1	C1FW1	2	0	N/A	N/A	10.1.254.33	30	Ciudad 1	C1FW2	2	0	N/A	N/A	10.1.254.34	30
Ciudad 1	C1FW2	0	0	N/A	N/A	10.1.255.10	30	Ciudad 1	C1BB2	2	0	N/A	N/A	10.1.255.9	30
Ciudad 1	C1FW2	1	0	N/A	N/A	10.1.255.29	30	Ciudad 1	C1INT2	0	0	N/A	N/A	10.1.255.30	30
Ciudad 1	C1FW2	2	0	N/A	N/A	10.1.254.34	30	Ciudad 1	C1FW1	2	0	N/A	N/A	10.1.254.33	30
Ciudad 1	C1INT1	0	0	N/A	N/A	10.1.254.30	30	Ciudad 1	C1FW1	1	0	N/A	N/A	10.1.254.29	30
Ciudad 1	C1INT1	0	1	N/A	N/A	10.1.254.37	30	Ciudad 1	C1INT2	0	1	N/A	N/A	10.1.254.38	30
Ciudad 1	C1INT1	1	0	N/A	N/A	200.139.131.2	30	Ciudad 1	SERVICE PROVIDER A	x	x	N/A	N/A	200.139.131.1	30
Ciudad 1	C1INT2	0	0	N/A	N/A	10.1.255.30	30	Ciudad 1	C1FW2	1	0	N/A	N/A	10.1.255.29	30
Ciudad 1	C1INT2	0	1	N/A	N/A	10.1.254.38	30	Ciudad 1	C1INT1	0	1	N/A	N/A	10.1.254.37	30
Ciudad 1	C1INT2	1	0	N/A	N/A	186.101.30.2	30	Ciudad 1	SERVICE PROVIDER B	x	x	N/A	N/A	186.101.30.1	30
Ciudad 1	C1INT2	2	0	N/A	N/A	N/A	30	Ciudad 1	C1INT2	0	0	N/A	N/A	N/A	30
Ciudad 1	C1RR1	0	0	N/A	N/A	10.1.254.14	30	Ciudad 1	C1BB1	3	0	N/A	N/A	10.1.254.13	30
Ciudad 1	C1RR1	0	1	N/A	N/A	10.1.255.18	30	Ciudad 1	C1BB2	4	0	N/A	N/A	10.1.255.17	30
Ciudad 1	C1RR2	0	0	N/A	N/A	10.1.255.14	30	Ciudad 1	C1BB2	3	0	N/A	N/A	10.1.255.13	30
Ciudad 1	C1RR2	0	1	N/A	N/A	10.1.254.18	30	Ciudad 1	C1BB1	4	0	N/A	N/A	10.1.254.17	30
Ciudad 1	C1ACCSW1	1	0	2,10	N/A	L2		Ciudad 1	C1ACC1	2	0	2,10	N/A	L2	
Ciudad 1	C1ACCSW1	1	1	10	N/A	L2		Ciudad 1	SERVIDOR	1	1		N/A	10.45.0.100	16
Ciudad 1	C1ACCSW1	1	15	2,10	N/A	L2		Ciudad 1	C1ACCSW2	1	15	2,10	N/A	L2	
Ciudad 1	C1ACCSW2	1	0	2,10	N/A	L2		Ciudad 1	C1ACC2	2	0	2,10	N/A	L2	
Ciudad 1	C1ACCSW2	1	1	10	N/A	L2		Ciudad 1	SERVIDOR	1	2		N/A	10.45.0.100	16
Ciudad 1	C1ACCSW2	1	15	2,10	N/A	L2		Ciudad 1	C1ACCSW1	1	15	2,10	N/A	L2	

Tabla A.2.Direccionamiento IP Ciudad 1.

Ciudad 2															
LOCAL								REMOTE							
Ciudad	Equipo	Slot	Port	Dot1q	VRRP VIP	IP	Mascara	Ciudad	Equipo	Slot	Port	Dot1q	VRRP VIP	IP	Mascara
Ciudad 2	C2BB1	0	0	N/A	N/A	10.2.254.1	30	Ciudad 2	C2BB2	0	0	N/A	N/A	10.2.254.2	30
Ciudad 2	C2BB1	1	0	N/A	N/A	10.2.254.5	30	Ciudad 2	C2ACC1	0	0	N/A	N/A	10.2.254.6	30
Ciudad 2	C2BB1	2	0	N/A	N/A	10.2.254.9	30	Ciudad 2	C2FW1	0	0	N/A	N/A	10.2.254.10	30
Ciudad 2	C2BB1	3	0	N/A	N/A	10.2.254.13	30	Ciudad 2	C2RR1	0	0	N/A	N/A	10.2.254.14	30
Ciudad 2	C2BB1	4	0	N/A	N/A	10.2.254.17	30	Ciudad 2	C2RR2	0	1	N/A	N/A	10.2.254.18	30
Ciudad 2	C2BB1	5	0	N/A	N/A	10.1.254.22	30	Ciudad 1	C1BB1	5	0	N/A	N/A	10.1.254.21	30
Ciudad 2	C2BB1	6	0	DISPONIBLE											
Ciudad 2	C2BB2	0	0	N/A	N/A	10.2.254.2	30	Ciudad 2	C2BB1	0	0	N/A	N/A	10.2.254.1	30
Ciudad 2	C2BB2	1	0	N/A	N/A	10.2.255.5	30	Ciudad 2	C2ACC2	0	0	N/A	N/A	10.2.255.6	30
Ciudad 2	C2BB2	2	0	N/A	N/A	10.2.255.9	30	Ciudad 2	C2FW2	0	0	N/A	N/A	10.2.255.10	30
Ciudad 2	C2BB2	3	0	N/A	N/A	10.2.255.13	30	Ciudad 2	C2RR2	0	0	N/A	N/A	10.2.255.14	30
Ciudad 2	C2BB2	4	0	N/A	N/A	10.2.255.17	30	Ciudad 2	C2RR1	0	1	N/A	N/A	10.2.255.18	30
Ciudad 2	C2BB2	5	0	N/A	N/A	10.1.255.22	30	Ciudad 1	C1BB2	5	0	N/A	N/A	10.1.255.21	30
Ciudad 2	C2BB2	6	0	DISPONIBLE											
Ciudad 2	C2ACC1	0	0	N/A	N/A	10.2.254.6	30	Ciudad 2	C2BB1	1	0	N/A	N/A	10.2.254.5	30
Ciudad 2	C2ACC1	1	0	N/A	N/A	10.2.254.25	30	Ciudad 2	C2ACC2	1	0	N/A	N/A	10.2.254.26	30
Ciudad 2	C2ACC1	2	0	2	10.2.1.1	10.2.1.2	25	Ciudad 2	C2ACC1	1	0	N/A	N/A	10.2.254.26	30
Ciudad 2	C2ACC1	2	0	10	10.46.0.1	10.46.0.2	16	Ciudad 2	C2ACCSW1	1	0	2,10	N/A	L2	L2
Ciudad 2	C2ACC1	3	0	DISPONIBLE											
Ciudad 2	C2ACC2	0	0	N/A	N/A	10.2.255.6	30	Ciudad 2	C2BB2	1	0	N/A	N/A	10.2.255.5	30
Ciudad 2	C2ACC2	1	0	N/A	N/A	10.2.254.26	30	Ciudad 2	C2ACC1	1	0	N/A	N/A	10.2.254.25	30
Ciudad 2	C2ACC2	2	0	2	10.2.1.1	10.2.1.3	25	Ciudad 2	C2ACC2	1	0	N/A	N/A	10.2.254.25	30
Ciudad 2	C2ACC2	2	0	10	10.46.0.1	10.46.0.3	16	Ciudad 2	C2ACCSW2	1	0	2,10	N/A	L2	L2
Ciudad 2	C2ACC2	3	0	DISPONIBLE											
Ciudad 2	C2FW1	0	0	N/A	N/A	10.2.254.10	30	Ciudad 2	C2BB1	2	0	N/A	N/A	10.2.254.9	30
Ciudad 2	C2FW1	1	0	N/A	N/A	10.2.254.29	30	Ciudad 2	C2INT1	0	0	N/A	N/A	10.2.254.30	30
Ciudad 2	C2FW1	2	0	N/A	N/A	10.2.254.33	30	Ciudad 2	C2FW2	2	0	N/A	N/A	10.2.254.34	30
Ciudad 2	C2FW2	0	0	N/A	N/A	10.2.255.10	30	Ciudad 2	C2BB2	2	0	N/A	N/A	10.2.255.9	30
Ciudad 2	C2FW2	1	0	N/A	N/A	10.2.255.29	30	Ciudad 2	C2INT2	0	0	N/A	N/A	10.2.255.30	30
Ciudad 2	C2FW2	2	0	N/A	N/A	10.2.254.34	30	Ciudad 2	C2FW1	2	0	N/A	N/A	10.2.254.33	30
Ciudad 2	C2INT1	0	0	N/A	N/A	10.2.254.30	30	Ciudad 2	C2FW1	1	0	N/A	N/A	10.2.254.29	30
Ciudad 2	C2INT1	0	1	N/A	N/A	10.2.254.37	30	Ciudad 2	C2INT2	0	1	N/A	N/A	10.2.254.38	30
Ciudad 2	C2INT1	1	0	N/A	N/A	200.139.131.2	30	Ciudad 2	SERVICE PROVIDER A	x	x	N/A	N/A	200.139.131.1	30
Ciudad 2	C2INT2	0	0	N/A	N/A	10.2.255.30	30	Ciudad 2	C2FW2	1	0	N/A	N/A	10.2.255.29	30
Ciudad 2	C2INT2	0	1	N/A	N/A	10.2.254.38	30	Ciudad 2	C2INT1	0	1	N/A	N/A	10.2.254.37	30
Ciudad 2	C2INT2	1	0	N/A	N/A	186.101.30.2	30	Ciudad 2	SERVICE PROVIDER B	x	x	N/A	N/A	186.101.30.1	30
Ciudad 2	C2INT2	2	0	N/A	N/A	N/A	30	Ciudad 2		0	0	N/A	N/A	N/A	30
Ciudad 2	C2RR1	0	0	N/A	N/A	10.2.254.14	30	Ciudad 2	C2BB1	3	0	N/A	N/A	10.2.254.13	30
Ciudad 2	C2RR1	0	1	N/A	N/A	10.2.255.18	30	Ciudad 2	C2BB2	4	0	N/A	N/A	10.2.255.17	30
Ciudad 2	C2RR2	0	0	N/A	N/A	10.2.255.14	30	Ciudad 2	C2BB2	3	0	N/A	N/A	10.2.255.13	30
Ciudad 2	C2RR2	0	1	N/A	N/A	10.2.254.18	30	Ciudad 2	C2BB1	4	0	N/A	N/A	10.2.254.17	30
Ciudad 2	C2ACCSW1	1	0	2,10	N/A	L2		Ciudad 2	C2ACC1	2	0	2,10	N/A	L2	
Ciudad 2	C2ACCSW1	1	1	10	N/A	L2		Ciudad 2	SERVIDOR	1	1		N/A	10.45.0.100	16
Ciudad 2	C2ACCSW1	1	15	2,10	N/A	L2		Ciudad 2	C2ACCSW2	1	15	2,10	N/A	L2	
Ciudad 2	C2ACCSW2	1	0	2,10	N/A	L2		Ciudad 2	C2ACC2	2	0	2,10	N/A	L2	
Ciudad 2	C2ACCSW2	1	1	10	N/A	L2		Ciudad 2	SERVIDOR	1	2		N/A	10.45.0.100	16
Ciudad 2	C2ACCSW2	1	15	2,10	N/A	L2		Ciudad 2	C2ACCSW1	1	15	2,10	N/A	L2	

Tabla A.3.Direccionamiento IP ciudad 2.

Ciudad 1		
Equipo	Servicio Loopback	Management Loopback
C1PMPLS1	10.1.99.1	10.1.100.1
C1PMPLS2	10.1.99.2	10.1.100.2
C1PEMPLS1	10.1.99.3	10.1.100.3
C1PEMPLS2	10.1.99.4	10.1.100.4
C1FW1	10.1.99.5	10.1.100.5
C1FW2	10.1.99.6	10.1.100.6
C1INTERNET	10.1.99.7	10.1.100.7
C1INTERNET	10.1.99.8	10.1.100.8
C1RR1	10.1.99.9	10.1.100.9
C1RR2	10.1.99.10	10.1.100.10

Tabla A.4.Direccionamiento IP O&M y Servicio ciudad 1.

Ciudad 2		
Equipo	Servicio Loopback	Management Loopback
C2PMPLS1	10.2.99.1	10.2.100.1
C2PMPLS2	10.2.99.2	10.2.100.2
C2PEMPLS1	10.2.99.3	10.2.100.3
C2PEMPLS2	10.2.99.4	10.2.100.4
C2FW1	10.2.99.5	10.2.100.5
C2FW2	10.2.99.6	10.2.100.6
C2INTERNET1	10.2.99.7	10.2.100.7
C2INTERNET2	10.2.99.8	10.2.100.8
C2RR1	10.2.99.9	10.2.100.9
C2RR2	10.2.99.10	10.2.100.10

Tabla A.5.Direccionamiento IP O&M y Servicio ciudad 2.

ANEXO B: CONFIGURACIONES

a.Ciudad 1

a.1. Configuración C1ACCESO1

C1ACCESO1
! ! upgrade fpd auto version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C1ACCESO1 ! boot-start-marker boot-end-marker ! logging message-counter syslog ! no aaa new-model ip source-route ip cef ! ! ip vrf Internet rd 65000:2 route-target export 65000:2 route-target import 65000:2 ! ip vrf O&M rd 65000:1 route-target export 65000:1 route-target import 65000:1 ! ! ! no ip domain lookup ip domain name lab.local no ipv6 cef ! multilink bundle-name authenticated

```
mpls traffic-eng tunnels
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
log config
hidekeys
!
!
!
!
!
I2 vfi vpls point-to-point
!
!
!
!
!
interface Loopback0
description SERVICE
ip address 10.1.99.3 255.255.255.255
!
interface Loopback1
ip vrf forwarding O&M
ip address 10.1.100.3 255.255.255.255
!
interface Tunnel1
description TO_C1PMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
```

```
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel2
description TO_C1PMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel201
description TO_C2PMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel202
description TO_C2PMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel203
description TO_C2PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
```

```
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel204
description TO_C2PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GE0/0
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE0/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C1PMPLS1
ip address 10.1.254.6 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
```

```
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C1PEMPLS2
ip address 10.1.254.25 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
no ip address
negotiation auto
!
interface GigabitEthernet2/0.2
encapsulation dot1Q 2
ip vrf forwarding O&M
ip address 10.1.1.2 255.255.255.240
vrrp 2 description O&M_GW_PROTECTION
vrrp 2 ip 10.1.1.1
vrrp 2 preempt delay minimum 1
vrrp 2 priority 110
!
interface GigabitEthernet2/0.3
encapsulation dot1Q 3
!
interface GigabitEthernet2/0.10
encapsulation dot1Q 10
ip vrf forwarding Internet
ip address 10.45.0.2 255.255.0.0
vrrp 10 ip 10.45.0.1
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
router ospf 2 vrf Internet
log-adjacency-changes
network 10.33.1.0 0.0.0.3 area 0
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
```

```
network 10.1.99.3 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
network 10.1.255.0 0.0.0.255 area 0
!
router bgp 65000
  bgp log-neighbor-changes
  neighbor C1RR peer-group
  neighbor C1RR remote-as 65000
  neighbor C1RR update-source Loopback0
  neighbor 10.1.99.9 peer-group C1RR
  neighbor 10.1.99.10 peer-group C1RR
!
  address-family ipv4
    neighbor C1RR route-map gi_preference in
    no neighbor 10.1.99.9 activate
    no neighbor 10.1.99.10 activate
    no auto-summary
    no synchronization
  exit-address-family
!
  address-family vpnv4
    neighbor C1RR send-community extended
    neighbor C1RR route-map gi_preference in
    neighbor 10.1.99.9 activate
    neighbor 10.1.99.10 activate
  exit-address-family
!
  address-family ipv4 vrf O&M
    redistribute connected
    no synchronization
  exit-address-family
!
  address-family ipv4 vrf Internet
    redistribute connected
    redistribute ospf 2 vrf Internet
    no synchronization
  exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip community-list standard C11 permit 11
ip community-list standard C12 permit 12
ip community-list standard C21 permit 21
ip community-list standard C22 permit 22
!
```

```
ip rsvp signalling hello
!
ip explicit-path name LP_GE0/0 enable
exclude-address 10.1.254.6
!
ip explicit-path name LP_GE1/0 enable
exclude-address 10.1.254.25
!
!
!
!
!
route-map gi_preference permit 10
match community C12
set local-preference 80
!
route-map gi_preference permit 20
match community C21
set local-preference 70
!
route-map gi_preference permit 30
match community C22
set local-preference 60
!
route-map gi_preference permit 40
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
```

```
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end
```

a.2. Configuración C1ACCESO2

C1ACCESO2
<pre>! ! upgrade fpd auto version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C1ACCESO2 ! boot-start-marker boot-end-marker ! logging message-counter syslog ! no aaa new-model ip source-route ip cef ! ! ip vrf Internet rd 65000:1002 route-target export 65000:2 route-target import 65000:2 ! ip vrf O&M rd 65000:1001 route-target export 65000:1 route-target import 65000:1 ! ! ! no ip domain lookup</pre>


```
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel2
description TO_C1PMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel201
description TO_C2PMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel202
description TO_C2PMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel203
description TO_C2PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
```

```
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel204
description TO_C2PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GEO/0
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GEO/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C1PMPLS2
ip address 10.1.255.6 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
```

```
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C1PEMPLS1
ip address 10.1.254.26 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
no ip address
negotiation auto
!
interface GigabitEthernet2/0.2
encapsulation dot1Q 2
ip vrf forwarding O&M
ip address 10.1.1.3 255.255.255.240
vrrp 2 description O&M_GW_PROTECTION
vrrp 2 ip 10.1.1.1
vrrp 2 preempt delay minimum 1
!
interface GigabitEthernet2/0.10
encapsulation dot1Q 10
ip vrf forwarding Internet
ip address 10.45.0.3 255.255.0.0
vrrp 10 ip 10.45.0.1
vrrp 10 priority 90
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
router ospf 2 vrf Internet
log-adjacency-changes
network 10.33.1.4 0.0.0.3 area 0
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.1.99.4 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
```

```
network 10.1.255.0 0.0.0.255 area 0
!
router bgp 65000
  bgp log-neighbor-changes
  neighbor C1RR peer-group
  neighbor C1RR remote-as 65000
  neighbor C1RR update-source Loopback0
  neighbor 10.1.99.9 peer-group C1RR
  neighbor 10.1.99.10 peer-group C1RR
!
address-family ipv4
  no neighbor 10.1.99.9 activate
  no neighbor 10.1.99.10 activate
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpv4
  neighbor C1RR send-community extended
  neighbor C1RR route-map gi_preference in
  neighbor 10.1.99.9 activate
  neighbor 10.1.99.10 activate
  exit-address-family
!
address-family ipv4 vrf O&M
  redistribute connected
  no synchronization
  exit-address-family
!
address-family ipv4 vrf Internet
  redistribute connected
  redistribute ospf 2 vrf Internet
  no synchronization
  exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip community-list standard C11 permit 11
ip community-list standard C12 permit 12
ip community-list standard C21 permit 21
ip community-list standard C22 permit 22
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE1/0 enable
```

```
exclude-address 10.1.254.26
!  
ip explicit-path name LP_GE0/0 enable
exclude-address 10.1.255.6
!  
!  
!  
!  
!  
route-map gi_preference permit 10
match community C12
set local-preference 80
!  
route-map gi_preference permit 20
match community C21
set local-preference 70
!  
route-map gi_preference permit 30
match community C22
set local-preference 60
!  
route-map gi_preference permit 40
!  
!  
!  
control-plane
!  
!  
!  
!  
!  
gatekeeper
shutdown
!  
!  
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
```

```
!  
end
```

a.3. Configuración C1ACCESOSW1

```
C1ACCESOSW1  
!  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C1ACCESOSW1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
ip cef  
!  
!  
!  
!  
no ip domain lookup  
ip domain name lab.local  
ip auth-proxy max-nodata-conns 3  
ip admission max-nodata-conns 3  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!
```

```
!  
!  
!  
!  
!  
!  
!  
vtp mode transparent  
archive  
log config  
hidekeys  
!  
!  
!  
!  
vlan 10  
!  
!  
!  
!  
interface FastEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet1/0  
switchport mode trunk  
!  
interface FastEthernet1/1  
switchport access vlan 10  
!  
interface FastEthernet1/2  
!  
interface FastEthernet1/3  
!  
interface FastEthernet1/4  
!  
interface FastEthernet1/5  
!
```

```
interface FastEthernet1/6
!
interface FastEthernet1/7
!
interface FastEthernet1/8
!
interface FastEthernet1/9
!
interface FastEthernet1/10
!
interface FastEthernet1/11
!
interface FastEthernet1/12
!
interface FastEthernet1/13
!
interface FastEthernet1/14
!
interface FastEthernet1/15
switchport mode trunk
!
interface Vlan1
no ip address
!
interface Vlan10
ip address 10.45.0.201 255.255.0.0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.45.0.2
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
```

```
!  
!  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login  
!  
!  
end
```

a.4. Configuración C1ACCESOSW2

C1ACCESOSW2

```
!  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C1ACCESOSW2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
ip cef  
!  
!  
!  
!
```



```
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
switchport mode trunk
!
interface FastEthernet1/1
switchport access vlan 10
!
interface FastEthernet1/2
!
interface FastEthernet1/3
!
interface FastEthernet1/4
!
interface FastEthernet1/5
!
interface FastEthernet1/6
!
interface FastEthernet1/7
!
interface FastEthernet1/8
!
interface FastEthernet1/9
!
interface FastEthernet1/10
!
interface FastEthernet1/11
!
interface FastEthernet1/12
!
interface FastEthernet1/13
!
interface FastEthernet1/14
!
interface FastEthernet1/15
switchport mode trunk
!
interface Vlan1
no ip address
!
interface Vlan10
ip address 10.45.0.202 255.255.0.0
!
ip forward-protocol nd
```

```
!  
!  
ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
!  
line con 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
line aux 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
line vty 0 4  
login  
!  
!  
end
```

a.5. Configuración C1BACKBONE1

```
C1BACKBONE1
!  
!  
upgrade fpd auto  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C1BACKBONE1  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
!  
no aaa new-model  
ip source-route  
ip cef  
!  
!  
ip vrf Internet  
rd 65000:2  
route-target export 65000:2  
route-target import 65000:2  
!  
ip vrf O&M  
rd 65000:1  
route-target export 65000:1  
route-target import 65000:1  
!  
!  
!  
no ip domain lookup  
ip domain name lab.local  
no ipv6 cef  
!  
multilink bundle-name authenticated  
mpls traffic-eng tunnels  
!  
!  
!  
!
```

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.1.99.1 255.255.255.255  
!  
interface Loopback1  
description O&M  
ip vrf forwarding O&M  
ip address 10.1.100.1 255.255.255.255  
!  
interface Tunnel3  
description TO_C1PEMPLS1  
ip unnumbered Loopback0  
tunnel destination 10.1.99.3  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng autoroute announce  
tunnel mpls traffic-eng forwarding-adjacency  
tunnel mpls traffic-eng path-option 10 dynamic  
tunnel mpls traffic-eng record-route  
tunnel mpls traffic-eng fast-reroute  
no routing dynamic  
!  
interface Tunnel4  
description TO_C1PEMPLS2
```

```
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel201
description TO_C2PMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel202
description TO_C2PMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel203
description TO_C2PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel204
```

```
description TO_C2PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE0/0
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE0/0
no routing dynamic
!
interface Tunnel2000
description Bypass_GE5/0
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE5/0
no routing dynamic
ip rsvp signalling hello refresh interval 500
!
interface Port-channel1
no ip address
hold-queue 300 in
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C1PMPLS2
```

```
ip address 10.1.254.1 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C1PEMPLS1
ip address 10.1.254.5 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
description TO_C1FW1
ip vrf forwarding Internet
ip address 10.1.254.9 255.255.255.252
ip ospf hello-interval 1
ip ospf dead-interval 2
negotiation auto
!
interface GigabitEthernet3/0
description TO_C1RR1
ip address 10.1.254.13 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
!
interface GigabitEthernet4/0
description TO_C1RR2
ip address 10.1.254.17 255.255.255.252
shutdown
negotiation auto
mpls traffic-eng tunnels
!
interface GigabitEthernet5/0
description TO_C2PMPLS1
ip address 10.1.254.21 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel2000
ip rsvp signalling hello
```

```
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet6/0
no ip address
shutdown
negotiation auto
channel-group 1
!
router ospf 2 vrf Internet
log-adjacency-changes
redistribute bgp 65000 metric-type 1 subnets
network 10.1.254.8 0.0.0.3 area 0
default-information originate
bfd all-interfaces
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.1.99.1 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
network 10.1.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp log-neighbor-changes
neighbor C1RR peer-group
neighbor C1RR remote-as 65000
neighbor C1RR update-source Loopback0
neighbor 10.1.99.9 peer-group C1RR
neighbor 10.1.99.10 peer-group C1RR
!
address-family ipv4
no neighbor 10.1.99.9 activate
no neighbor 10.1.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C1RR send-community extended
neighbor 10.1.99.9 activate
neighbor 10.1.99.10 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
```

```
exit-address-family
!
address-family ipv4 vrf Internet
 redistribute connected
 redistribute ospf 2 vrf Internet
 no synchronization
 network 0.0.0.0 route-map GI_Community
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE1/0 enable
 exclude-address 10.1.254.5
!
ip explicit-path name LP_GE0/0 enable
 exclude-address 10.1.254.1
!
ip explicit-path name LP_GE5/0 enable
 exclude-address 10.1.254.21
!
ip access-list extended default_route
!
!
!
!
!
route-map GI_Community permit 10
 set community 11
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
```

```
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
  stopbits 1  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
  stopbits 1  
line vty 0 4  
  login  
!  
end
```

a.6. Configuración C1BACKBONE2

C1BACKBONE2

```
!  
!  
upgrade fpd auto  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C1BACKBONE2  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
!  
no aaa new-model  
ip source-route  
ip cef  
!  
!  
ip vrf Internet  
  rd 65000:1002  
  route-target export 65000:2
```

```
route-target import 65000:2
!  
ip vrf O&M  
rd 65000:1001  
route-target export 65000:1  
route-target import 65000:1  
!  
!  
!  
no ip domain lookup  
ip domain name lab.local  
no ipv6 cef  
!  
multilink bundle-name authenticated  
mpls traffic-eng tunnels  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.1.99.2 255.255.255.255  
!
```

```
interface Loopback1
ip vrf forwarding O&M
ip address 10.1.100.2 255.255.255.255
!
interface Tunnel3
description TO_C1PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel4
description TO_C1PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel201
description TO_C2PMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel202
description TO_C2PMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
```

```
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel203
description TO_C2PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel204
description TO_C2PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE0/0
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE0/0
no routing dynamic
!
interface Tunnel2000
description Bypass_GE5/0
```

```
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE5/0
no routing dynamic
!
interface Port-channel1
no ip address
hold-queue 300 in
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C1PMPLS1
ip address 10.1.254.2 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C1PEMPLS2
ip address 10.1.255.5 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
description TO_C1FW2
ip vrf forwarding Internet
ip address 10.1.255.9 255.255.255.252
ip ospf hello-interval 1
ip ospf dead-interval 2
negotiation auto
!
interface GigabitEthernet3/0
description TO_C1RR2
ip address 10.1.255.13 255.255.255.252
```

```
shutdown
negotiation auto
mpls traffic-eng tunnels
!
interface GigabitEthernet4/0
description TO_C1RR1
ip address 10.1.255.17 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
!
interface GigabitEthernet5/0
description TO_C2PMPLS2
ip address 10.1.255.21 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel2000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet6/0
no ip address
shutdown
negotiation auto
channel-group 1
!
router ospf 2 vrf Internet
log-adjacency-changes
redistribute bgp 65000 metric 200 metric-type 1 subnets
network 10.1.255.8 0.0.0.3 area 0
default-information originate
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.1.99.2 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
network 10.1.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp log-neighbor-changes
neighbor C1RR peer-group
neighbor C1RR remote-as 65000
neighbor 10.1.99.9 peer-group C1RR
neighbor 10.1.99.10 peer-group C1RR
!
address-family ipv4
```

```
no neighbor 10.1.99.9 activate
no neighbor 10.1.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C1RR send-community extended
neighbor 10.1.99.9 activate
neighbor 10.1.99.10 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
exit-address-family
!
address-family ipv4 vrf Internet
redistribute connected
redistribute ospf 2 vrf Internet
no synchronization
network 0.0.0.0 route-map GI_Community
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE1/0 enable
exclude-address 10.1.255.5
!
ip explicit-path name LP_GE0/0 enable
exclude-address 10.1.254.2
!
ip explicit-path name LP_GE5/0 enable
exclude-address 10.1.255.21
!
!
!
!
!
route-map GI_Community permit 10
set community 12
!
```

```
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
gatekeeper  
shutdown  
!  
!  
line con 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
stopbits 1  
line aux 0  
exec-timeout 0 0  
privilege level 15  
logging synchronous  
stopbits 1  
line vty 0 4  
login  
!  
end
```

a.7. Configuración C1INTERNETFW1

C1INTERNETFW1
! ! upgrade fpd auto version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C1INTERNETFW1 ! boot-start-marker

```
boot-end-marker
!
!
redundancy inter-device
scheme standby NAT
!
!
redundancy
no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
association 1
no shutdown
protocol sctp
local-port 65000
local-ip 1.1.1.2
remote-port 65000
remote-ip 1.1.1.3
!
no aaa new-model
ip source-route
ip cef
!
!
!
!
no ip domain lookup
ip domain name lab.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
!  
class-map type inspect match-any APN-TO-INTERNET  
match access-group name APN-TO-INTERNET  
!  
!  
policy-map type inspect APN-TO-INTERNET  
class type inspect APN-TO-INTERNET  
pass  
class class-default  
drop  
!  
zone security gi_inside  
zone security gi_outside  
zone-pair security TO_INTERNET source gi_inside destination gi_outside  
service-policy type inspect APN-TO-INTERNET  
zone-pair security TO_NETWORK source gi_outside destination gi_inside  
service-policy type inspect APN-TO-INTERNET  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.1.99.5 255.255.255.255  
!  
interface Ethernet0/0  
no ip address  
shutdown  
duplex auto  
!  
interface GigabitEthernet0/0  
description TO_C1PMPLS1  
ip address 10.1.254.10 255.255.255.252  
ip nat inside  
ip virtual-reassembly  
zone-member security gi_inside  
ip ospf hello-interval 1
```

```
ip ospf dead-interval 2
duplex full
speed 1000
media-type gbic
negotiation auto
!
interface GigabitEthernet1/0
description TO_C1INTERNET1
ip address 10.1.254.29 255.255.255.252
ip nat outside
ip virtual-reassembly
zone-member security gi_outside
ip ospf hello-interval 1
ip ospf dead-interval 2
negotiation auto
!
interface GigabitEthernet2/0
description TO_C1FW2
ip address 10.1.254.33 255.255.255.248
negotiation auto
standby 0 ip 10.1.254.249
standby 0 priority 110
standby 0 preempt
!
router ospf 2
log-adjacency-changes
redistribute static metric-type 1 subnets
network 10.1.99.5 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
bfd all-interfaces
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat pool NATPOOL 201.175.0.0 201.175.3.255 netmask 255.255.252.0 add-route
ip nat inside source list APN-TO-INTERNET pool NATPOOL overload
!
ip access-list extended APN-TO-INTERNET
permit ip 10.45.0.0 0.0.255.255 any
permit ip 10.46.0.0 0.0.255.255 any
permit icmp any any
!
!
!
!
```

```
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
gatekeeper  
shutdown  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
  stopbits 1  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
  stopbits 1  
line vty 0 4  
  login  
!  
end
```

a.8. Configuración C1INTERNETFW2

C1INTERNETFW2
! ! upgrade fpd auto version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C1INTERNETFW2 !


```
class type inspect APN-TO-INTERNET
  pass
class class-default
  drop
!
zone security gi_inside
zone security gi_outside
zone-pair security TO_INTERNET source gi_inside destination gi_outside
  service-policy type inspect APN-TO-INTERNET
zone-pair security TO_NETWORK source gi_outside destination gi_inside
  service-policy type inspect APN-TO-INTERNET
!
!
!
!
interface Loopback0
  description SERVICE
  ip address 10.1.99.6 255.255.255.255
!
interface Ethernet0/0
  no ip address
  shutdown
  duplex auto
!
interface GigabitEthernet0/0
  description TO_C1PMPLS1
  ip address 10.1.255.10 255.255.255.252
  ip nat inside
  ip virtual-reassembly
  zone-member security gi_inside
  ip ospf hello-interval 1
  ip ospf dead-interval 2
  duplex full
  speed 1000
  media-type gbic
  negotiation auto
!
interface GigabitEthernet1/0
  description TO_C1INTERNET1
  ip address 10.1.255.29 255.255.255.252
  ip nat outside
  ip virtual-reassembly
  zone-member security gi_outside
  ip ospf hello-interval 1
  ip ospf dead-interval 2
  negotiation auto
!
```

```
interface GigabitEthernet2/0
description TO_C1FW1
ip address 10.1.254.34 255.255.255.248
negotiation auto
standby 0 ip 10.1.254.249
standby 0 preempt
standby 0 name NAT
!
router ospf 2
log-adjacency-changes
redistribute static metric-type 1 subnets
network 10.1.99.6 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
network 10.1.255.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat pool NATPOOL 201.175.0.0 201.175.3.255 netmask 255.255.252.0 add-route
ip nat inside source list APN-TO-INTERNET pool NATPOOL overload
!
ip access-list extended APN-TO-INTERNET
permit ip 10.45.0.0 0.0.255.255 any
permit ip 10.46.0.0 0.0.255.255 any
permit icmp any any
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
```

```
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end
```

a.9. Configuración C1INTERNET1

```
C1INTERNET1
!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C1INTERNET1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
no ip domain lookup
ip domain name lab.local
!
!
!
!
```

```
interface Loopback0
description SERVICE
ip address 10.1.99.7 255.255.255.255
!
interface FastEthernet0/0
description TO_C1FW1
ip address 10.1.254.30 255.255.255.252
ip ospf hello-interval 1
ip ospf dead-interval 2
duplex auto
speed auto
!
interface FastEthernet0/1
description TO_C1INTERNET2
ip address 10.1.254.37 255.255.255.252
ip ospf hello-interval 1
ip ospf dead-interval 2
duplex auto
speed auto
!
interface FastEthernet1/0
description TO_ISP-1
ip address 200.139.131.2 255.255.255.252
duplex auto
speed auto
!
router ospf 2
log-adjacency-changes
network 10.1.99.7 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
default-information originate metric 100 metric-type 1
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
timers bgp 1 3
redistribute ospf 2 match external 1 external 2
neighbor 10.1.99.8 remote-as 65000
neighbor 10.1.99.8 update-source Loopback0
neighbor 200.139.131.1 remote-as 12300
no auto-summary
!
ip http server
ip forward-protocol nd
!
!
!
```

```
!  
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login  
!  
end
```

a.10. Configuración C1INTERNET2

C1INTERNET2

```
!  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C1INTERNET2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
!  
!  
ip cef  
!  
!  
no ip domain lookup  
ip domain name lab.local  
!
```

```
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.1.99.8 255.255.255.255  
!  
interface FastEthernet0/0  
description TO_C1FW2  
ip address 10.1.255.30 255.255.255.252  
ip ospf hello-interval 1  
ip ospf dead-interval 2  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
description TO_C1INTERNET1  
ip address 10.1.254.38 255.255.255.252  
ip ospf hello-interval 1  
ip ospf dead-interval 2  
duplex auto  
speed auto  
!  
interface FastEthernet1/0  
description TO_ISP-2  
ip address 186.101.30.2 255.255.255.252  
duplex auto  
speed auto  
!  
router ospf 2  
log-adjacency-changes  
network 10.1.99.8 0.0.0.0 area 0  
network 10.1.254.0 0.0.0.255 area 0  
network 10.1.255.0 0.0.0.255 area 0  
default-information originate metric 200 metric-type 1  
!  
router bgp 65000  
no synchronization  
bgp log-neighbor-changes  
timers bgp 1 3  
redistribute ospf 2 match external 1 external 2  
neighbor 10.1.99.7 remote-as 65000  
neighbor 10.1.99.7 update-source Loopback0  
neighbor 186.101.30.1 remote-as 12300  
neighbor 186.101.30.1 route-map AS-PATH out  
no auto-summary
```

```
!  
ip http server  
ip forward-protocol nd  
!  
!  
!  
!  
ip prefix-list AS-PATH seq 5 permit 201.175.0.0/22  
route-map AS-PATH permit 10  
  match ip address prefix-list AS-PATH  
  set as-path prepend 65000 65000  
!  
!  
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login  
!  
end
```

a.11. Configuración C1RR1

C1RR1
! ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C1RR1

```
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
!  
!  
ip cef  
!  
!  
ip vrf O&M  
rd 65000:1  
route-target export 65000:1  
route-target import 65000:1  
!  
no ip domain lookup  
ip domain name lab.local  
mpls traffic-eng tunnels  
!  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.1.99.9 255.255.255.255  
!  
interface Loopback1  
ip vrf forwarding O&M  
ip address 10.1.100.9 255.255.255.255  
!  
interface FastEthernet0/0  
description TO_C1PMPLS1  
ip address 10.1.254.14 255.255.255.252  
duplex auto  
speed auto  
mpls traffic-eng tunnels  
!  
interface FastEthernet0/1  
description TO_C1PMPLS2  
ip address 10.1.255.18 255.255.255.252  
duplex auto  
speed auto  
mpls traffic-eng tunnels  
!
```

```
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.1.99.9 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
network 10.1.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp cluster-id 1
bgp log-neighbor-changes
neighbor C1_PE&P peer-group
neighbor C1_PE&P remote-as 65000
neighbor C1_PE&P update-source Loopback0
neighbor C2_RR peer-group
neighbor C2_RR remote-as 65000
neighbor C2_RR update-source Loopback0
neighbor 10.1.99.1 peer-group C1_PE&P
neighbor 10.1.99.2 peer-group C1_PE&P
neighbor 10.1.99.3 peer-group C1_PE&P
neighbor 10.1.99.4 peer-group C1_PE&P
neighbor 10.2.99.9 peer-group C2_RR
neighbor 10.2.99.10 peer-group C2_RR
!
address-family ipv4
no neighbor 10.1.99.1 activate
no neighbor 10.1.99.2 activate
no neighbor 10.1.99.3 activate
no neighbor 10.1.99.4 activate
no neighbor 10.2.99.9 activate
no neighbor 10.2.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C1_PE&P send-community both
neighbor C1_PE&P route-reflector-client
neighbor C2_RR send-community both
neighbor C2_RR route-reflector-client
neighbor 10.1.99.1 activate
neighbor 10.1.99.2 activate
neighbor 10.1.99.3 activate
neighbor 10.1.99.4 activate
neighbor 10.2.99.9 activate
neighbor 10.2.99.10 activate
exit-address-family
```

```
!  
address-family ipv4 vrf O&M  
  redistribute connected  
  no synchronization  
exit-address-family  
!  
ip http server  
ip forward-protocol nd  
!  
!  
!  
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login  
!  
end
```

a.12. Configuración C1RR2

C1RR2
<pre>! ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C1RR2 ! boot-start-marker boot-end-marker ! !</pre>

```
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
ip vrf Internet
rd 65000:1002
route-target export 65000:2
route-target import 65000:2
!
ip vrf O&M
rd 65000:1001
route-target export 65000:1
route-target import 65000:1
!
no ip domain lookup
ip domain name lab.local
mpls traffic-eng tunnels
!
!
!
!
!
interface Loopback0
description SERVICE
ip address 10.1.99.10 255.255.255.255
!
interface Loopback1
ip vrf forwarding O&M
ip address 10.1.100.10 255.255.255.255
!
interface FastEthernet0/0
description TO_C1PMPLS2
ip address 10.1.255.14 255.255.255.252
shutdown
duplex auto
speed auto
mpls traffic-eng tunnels
!
interface FastEthernet0/1
description TO_C1PMPLS1
ip address 10.1.254.18 255.255.255.252
shutdown
duplex auto
speed auto
```

```
mpls traffic-eng tunnels
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.1.99.10 0.0.0.0 area 0
network 10.1.254.0 0.0.0.255 area 0
network 10.1.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp cluster-id 1
bgp log-neighbor-changes
neighbor C1_PE&P peer-group
neighbor C1_PE&P remote-as 65000
neighbor C1_PE&P update-source Loopback0
neighbor C2_RR peer-group
neighbor C2_RR remote-as 65000
neighbor C2_RR update-source Loopback0
neighbor 10.1.99.1 peer-group C1_PE&P
neighbor 10.1.99.2 peer-group C1_PE&P
neighbor 10.1.99.3 peer-group C1_PE&P
neighbor 10.1.99.4 peer-group C1_PE&P
neighbor 10.2.99.9 peer-group C2_RR
neighbor 10.2.99.10 peer-group C2_RR
!
address-family ipv4
no neighbor 10.1.99.1 activate
no neighbor 10.1.99.2 activate
no neighbor 10.1.99.3 activate
no neighbor 10.1.99.4 activate
no neighbor 10.2.99.9 activate
no neighbor 10.2.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C1_PE&P send-community both
neighbor C1_PE&P route-reflector-client
neighbor C2_RR send-community both
neighbor C2_RR route-reflector-client
neighbor 10.1.99.1 activate
neighbor 10.1.99.2 activate
neighbor 10.1.99.3 activate
neighbor 10.1.99.4 activate
exit-address-family
```

```
!  
address-family ipv4 vrf O&M  
  redistribute connected  
  no synchronization  
exit-address-family  
!  
address-family ipv4 vrf Internet  
  no synchronization  
exit-address-family  
!  
ip http server  
ip forward-protocol nd  
!  
!  
!  
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login  
!  
End
```

b.Ciudad 2

b.1. Configuración C2ACCESO1

C2ACCESO1
! ! upgrade fpd auto version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C2ACCESO1 ! boot-start-marker boot-end-marker ! logging message-counter syslog ! no aaa new-model ip source-route ip cef ! ! ip vrf Internet rd 65000:102 route-target export 65000:2 route-target import 65000:2 ! ip vrf O&M rd 65000:1 route-target export 65000:1 route-target import 65000:1 ! ! ! no ipv6 cef ! multilink bundle-name authenticated mpls traffic-eng tunnels ! ! ! !

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.2.99.3 255.255.255.255  
!  
interface Loopback1  
ip vrf forwarding O&M  
ip address 10.2.100.3 255.255.255.255  
!  
interface Tunnel1  
description TO_C2PMPLS1  
ip unnumbered Loopback0  
tunnel destination 10.2.99.1  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng autoroute announce  
tunnel mpls traffic-eng forwarding-adjacency  
tunnel mpls traffic-eng path-option 10 dynamic  
tunnel mpls traffic-eng record-route  
tunnel mpls traffic-eng fast-reroute  
no routing dynamic  
!  
interface Tunnel2  
description TO_C2PMPLS2  
ip unnumbered Loopback0
```

```
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel101
description TO_C1PMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel102
description TO_C1PMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel103
description TO_C1PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel104
description TO_C1PEMPLS2
```

```
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GEO/0
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GEO/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C2PMPLS1
ip address 10.2.254.6 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C2PEMPLS2
ip address 10.2.254.25 255.255.255.252
negotiation auto
```

```
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet2/0.2
encapsulation dot1Q 2
ip vrf forwarding O&M
ip address 10.2.1.2 255.255.255.240
vrrp 2 description O&M_GW_PROTECTION
vrrp 2 ip 10.2.1.1
vrrp 2 preempt delay minimum 1
vrrp 2 priority 110
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
router ospf 2 vrf Internet
log-adjacency-changes
network 10.35.1.0 0.0.0.3 area 0
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.2.99.3 0.0.0.0 area 0
network 10.2.254.0 0.0.0.255 area 0
network 10.2.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp log-neighbor-changes
neighbor C2RR peer-group
neighbor C2RR remote-as 65000
neighbor C2RR update-source Loopback0
neighbor 10.2.99.9 peer-group C2RR
neighbor 10.2.99.10 peer-group C2RR
!
address-family ipv4
neighbor C2RR route-map gi_preference in
no neighbor 10.2.99.9 activate
```

```
no neighbor 10.2.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C2RR send-community extended
neighbor C2RR route-map gi_preference in
neighbor 10.2.99.9 activate
neighbor 10.2.99.10 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
exit-address-family
!
address-family ipv4 vrf Internet
redistribute connected
redistribute ospf 2 vrf Internet
no synchronization
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip community-list standard C11 permit 11
ip community-list standard C12 permit 12
ip community-list standard C21 permit 21
ip community-list standard C22 permit 22
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE0/0 enable
exclude-address 10.2.254.6
!
ip explicit-path name LP_GE1/0 enable
exclude-address 10.2.254.25
!
!
!
!
!
route-map gi_preference permit 10
match community C22
set local-preference 80
```

```
!  
route-map gi_preference permit 20  
  match community C11  
  set local-preference 70  
!  
route-map gi_preference permit 30  
  match community C12  
  set local-preference 60  
!  
route-map gi_preference permit 40  
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
gatekeeper  
  shutdown  
!  
!  
line con 0  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  login  
!  
end
```

b.2. Configuración C2ACCESO2

```
C2ACCESO2
!
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2ACCESO2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
ip cef
!
!
ip vrf Internet
rd 65000:1102
route-target export 65000:2
route-target import 65000:2
!
ip vrf O&M
rd 65000:1001
route-target export 65000:1
route-target import 65000:1
!
!
!
no ipv6 cef
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
!
!
!
!
!
!
```

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
ip address 10.2.99.4 255.255.255.255  
!  
interface Loopback1  
ip vrf forwarding O&M  
ip address 10.2.100.4 255.255.255.255  
!  
interface Tunnel1  
description TO_C2PMPLS1  
ip unnumbered Loopback0  
tunnel destination 10.2.99.1  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng autoroute announce  
tunnel mpls traffic-eng forwarding-adjacency  
tunnel mpls traffic-eng path-option 10 dynamic  
tunnel mpls traffic-eng record-route  
tunnel mpls traffic-eng fast-reroute  
no routing dynamic  
!  
interface Tunnel2  
description TO_C2PMPLS2  
ip unnumbered Loopback0  
tunnel destination 10.2.99.2  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng autoroute announce  
tunnel mpls traffic-eng forwarding-adjacency  
tunnel mpls traffic-eng path-option 10 dynamic
```

```
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel101
description TO_C1PMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel102
description TO_C1PMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel103
description TO_C1PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel104
description TO_C1PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
```

```
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GE0/0
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE0/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C2PMPLS2
ip address 10.2.255.6 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C2PEMPLS1
ip address 10.2.254.26 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
```

```
interface GigabitEthernet2/0
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet2/0.2
encapsulation dot1Q 2
ip vrf forwarding O&M
ip address 10.2.1.3 255.255.255.240
vrrp 2 description O&M_GW_PROTECTION
vrrp 2 ip 10.2.1.1
vrrp 2 preempt delay minimum 1
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.2.99.4 0.0.0.0 area 0
network 10.2.254.0 0.0.0.255 area 0
network 10.2.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp log-neighbor-changes
neighbor C2RR peer-group
neighbor C2RR remote-as 65000
neighbor C2RR update-source Loopback0
neighbor 10.2.99.9 peer-group C2RR
neighbor 10.2.99.10 peer-group C2RR
!
address-family ipv4
neighbor C2RR route-map gi_preference in
no neighbor 10.2.99.9 activate
no neighbor 10.2.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpv4
neighbor C2RR send-community extended
neighbor C2RR route-map gi_preference in
neighbor 10.2.99.9 activate
neighbor 10.2.99.10 activate
```

```
exit-address-family
!
address-family ipv4 vrf O&M
 redistribute connected
 no synchronization
exit-address-family
!
address-family ipv4 vrf Internet
 redistribute connected
 no synchronization
exit-address-family
!
ip forward-protocol nd
 no ip http server
 no ip http secure-server
!
ip community-list standard C11 permit 11
ip community-list standard C12 permit 12
ip community-list standard C21 permit 21
ip community-list standard C22 permit 22
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE1/0 enable
 exclude-address 10.2.254.26
!
ip explicit-path name LP_GE0/0 enable
 exclude-address 10.2.255.6
!
!
!
!
!
route-map gi_preference permit 10
 match community C22
 set local-preference 80
!
route-map gi_preference permit 20
 match community C11
 set local-preference 70
!
route-map gi_preference permit 30
 match community C12
 set local-preference 60
!
route-map gi_preference permit 40
!
```

```
!  
!  
control-plane  
!  
!  
!  
gatekeeper  
shutdown  
!  
!  
line con 0  
stopbits 1  
line aux 0  
stopbits 1  
line vty 0 4  
login  
!  
end
```

b.3. Configuración C2ACCESOSW1

C2ACCESOSW1

```
!  
  
!  
hostname C2ACCESOSW1  
!  
no ip domain lookup  
ip domain-name lab.local  
!  
line con 0  
exec-timeout 0 0  
logging synchronous  
privilege level 15  
no login  
line aux 0  
exec-timeout 0 0  
logging synchronous  
privilege level 15  
no login  
!  
!  
end
```

b.4. Configuración C2ACCESOSW2

```
C2ACCESOSW2
!  
!  
hostname C2ACCESOSW2  
!  
no ip domain lookup  
ip domain-name lab.local  
!  
line con 0  
exec-timeout 0 0  
logging synchronous  
privilege level 15  
no login  
line aux 0  
exec-timeout 0 0  
logging synchronous  
privilege level 15  
no login  
!  
!  
end
```

b.5. Configuración C2BACKBONE1

```
C2BACKBONE1  
!  
!  
upgrade fpd auto  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C2BACKBONE1  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
!  
no aaa new-model  
ip source-route
```

```
ip cef
!  
!  
ip vrf Internet
rd 65000:102
route-target export 65000:2
route-target import 65000:2
!  
ip vrf O&M
rd 65000:1
route-target export 65000:1
route-target import 65000:1
!  
!  
!  
no ipv6 cef
!  
multilink bundle-name authenticated
mpls traffic-eng tunnels
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive
log config
hidekeys
!  
!  
!  
!  
!  
!  
!  
!
```

```
interface Loopback0
description SERVICE
ip address 10.2.99.1 255.255.255.255
!
interface Loopback1
description O&M
ip vrf forwarding O&M
ip address 10.2.100.1 255.255.255.255
!
interface Tunnel3
description TO_C2PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel4
description TO_C2PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel101
description TO_C1PMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel102
description TO_C1PMPLS2
```

```
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel103
description TO_C1PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel104
description TO_C1PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.2.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Tunnel1001
description Bypass_GE0/0
ip unnumbered Loopback0
tunnel destination 10.2.99.2
tunnel mode mpls traffic-eng
```

```
tunnel mpls traffic-eng path-option 1 explicit name LP_GE0/0
no routing dynamic
!
interface Tunnel2000
description Bypass_GE5/0
ip unnumbered Loopback0
tunnel destination 10.1.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE5/0
no routing dynamic
!
interface Port-channel1
no ip address
hold-queue 300 in
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C2PMPLS2
ip address 10.2.254.1 255.255.255.252
shutdown
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C2PEMPLS1
ip address 10.2.254.5 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
description TO_C2FW1
ip vrf forwarding Internet
ip address 10.2.254.9 255.255.255.252
negotiation auto
```

```
!  
interface GigabitEthernet3/0  
description TO_C2RR1  
ip address 10.2.254.13 255.255.255.252  
negotiation auto  
mpls traffic-eng tunnels  
!  
interface GigabitEthernet4/0  
description TO_C2RR2  
ip address 10.2.254.17 255.255.255.252  
shutdown  
negotiation auto  
mpls traffic-eng tunnels  
!  
interface GigabitEthernet5/0  
description TO_C2PMPLS1  
ip address 10.1.254.22 255.255.255.252  
negotiation auto  
mpls traffic-eng tunnels  
mpls traffic-eng backup-path Tunnel2000  
ip rsvp signalling hello  
ip rsvp signalling hello refresh interval 500  
!  
interface GigabitEthernet6/0  
no ip address  
shutdown  
negotiation auto  
channel-group 1  
!  
router ospf 2 vrf Internet  
log-adjacency-changes  
redistribute bgp 65000 metric-type 1 subnets  
network 10.2.254.8 0.0.0.3 area 0  
default-information originate  
!  
router ospf 1  
mpls traffic-eng router-id Loopback0  
mpls traffic-eng area 0  
log-adjacency-changes  
network 10.1.254.0 0.0.0.255 area 0  
network 10.2.99.1 0.0.0.0 area 0  
network 10.2.254.0 0.0.0.255 area 0  
network 10.2.255.0 0.0.0.255 area 0  
!  
router bgp 65000  
bgp log-neighbor-changes  
neighbor C2RR peer-group
```

```
neighbor C2RR remote-as 65000
neighbor C2RR update-source Loopback0
neighbor 10.2.99.9 peer-group C2RR
neighbor 10.2.99.10 peer-group C2RR
!
address-family ipv4
no neighbor 10.2.99.9 activate
no neighbor 10.2.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C2RR send-community both
neighbor 10.2.99.9 activate
neighbor 10.2.99.10 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
exit-address-family
!
address-family ipv4 vrf Internet
redistribute connected
redistribute ospf 2 vrf Internet
no synchronization
network 0.0.0.0 route-map GI_Community
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE5/0 enable
exclude-address 10.1.254.22
!
ip explicit-path name LP_GE0/0 enable
exclude-address 10.2.254.1
!
ip explicit-path name LP_GE1/0 enable
exclude-address 10.2.254.5
!
!
```

```
ip prefix-list default_route seq 5 permit 0.0.0.0/0
!
!
!
!
route-map GI_Community permit 10
set community 21
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
end
```

b.6. Configuración C2BACKBONE2

```
C2BACKBONE2
!
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2BACKBONE2
!
boot-start-marker
boot-end-marker
```

```
!  
logging message-counter syslog  
!  
no aaa new-model  
ip source-route  
ip cef  
!  
!  
ip vrf Internet  
rd 65000:1102  
route-target export 65000:2  
route-target import 65000:2  
!  
ip vrf O&M  
rd 65000:1001  
route-target export 65000:1  
route-target import 65000:1  
!  
!  
!  
no ipv6 cef  
!  
multilink bundle-name authenticated  
mpls traffic-eng tunnels  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!
```

```
!  
!  
!  
!  
!  
interface Loopback0  
  description SERVICE  
  ip address 10.2.99.2 255.255.255.255  
!  
interface Loopback1  
  ip vrf forwarding O&M  
  ip address 10.2.100.2 255.255.255.255  
!  
interface Tunnel3  
  description TO_C2PEMPLS1  
  ip unnumbered Loopback0  
  tunnel destination 10.2.99.3  
  tunnel mode mpls traffic-eng  
  tunnel mpls traffic-eng autoroute announce  
  tunnel mpls traffic-eng forwarding-adjacency  
  tunnel mpls traffic-eng path-option 10 dynamic  
  tunnel mpls traffic-eng record-route  
  tunnel mpls traffic-eng fast-reroute  
  no routing dynamic  
!  
interface Tunnel4  
  description TO_C2PEMPLS2  
  ip unnumbered Loopback0  
  tunnel destination 10.2.99.4  
  tunnel mode mpls traffic-eng  
  tunnel mpls traffic-eng autoroute announce  
  tunnel mpls traffic-eng forwarding-adjacency  
  tunnel mpls traffic-eng path-option 10 dynamic  
  tunnel mpls traffic-eng record-route  
  tunnel mpls traffic-eng fast-reroute  
  no routing dynamic  
!  
interface Tunnel101  
  description TO_C1PMPLS1  
  ip unnumbered Loopback0  
  tunnel destination 10.1.99.1  
  tunnel mode mpls traffic-eng  
  tunnel mpls traffic-eng autoroute announce  
  tunnel mpls traffic-eng forwarding-adjacency  
  tunnel mpls traffic-eng path-option 10 dynamic  
  tunnel mpls traffic-eng record-route  
  tunnel mpls traffic-eng fast-reroute
```

```
no routing dynamic
!
interface Tunnel102
description TO_C1PMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel103
description TO_C1PEMPLS1
ip unnumbered Loopback0
tunnel destination 10.1.99.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel104
description TO_C1PEMPLS2
ip unnumbered Loopback0
tunnel destination 10.1.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng record-route
tunnel mpls traffic-eng fast-reroute
no routing dynamic
!
interface Tunnel1000
description Bypass_GE1/0
ip unnumbered Loopback0
tunnel destination 10.2.99.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE1/0
no routing dynamic
!
interface Tunnel1001
```

```
description Bypass_GE0/0
ip unnumbered Loopback0
tunnel destination 10.2.99.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE0/0
no routing dynamic
!
interface Tunnel2000
description Bypass_GE5/0
ip unnumbered Loopback0
tunnel destination 10.1.99.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name LP_GE5/0
no routing dynamic
!
interface Port-channel1
no ip address
hold-queue 300 in
!
interface Ethernet0/0
no ip address
shutdown
duplex auto
!
interface GigabitEthernet0/0
description TO_C2PMPLS1
ip address 10.2.254.2 255.255.255.252
duplex full
speed 1000
media-type gbic
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1001
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet1/0
description TO_C2PEMPLS2
ip address 10.2.255.5 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet2/0
description TO_C2FW2
```

```
ip vrf forwarding Internet
ip address 10.2.255.9 255.255.255.252
negotiation auto
!
interface GigabitEthernet3/0
description TO_C2RR2
ip address 10.2.255.13 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
!
interface GigabitEthernet4/0
description TO_C2RR1
ip address 10.2.255.17 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
!
interface GigabitEthernet5/0
description TO_C2PMPLS2
ip address 10.1.255.22 255.255.255.252
negotiation auto
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel2000
ip rsvp signalling hello
ip rsvp signalling hello refresh interval 500
!
interface GigabitEthernet6/0
no ip address
shutdown
negotiation auto
channel-group 1
!
router ospf 2 vrf Internet
log-adjacency-changes
redistribute bgp 65000 subnets
network 10.2.255.8 0.0.0.3 area 0
default-information originate
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.1.255.0 0.0.0.255 area 0
network 10.2.99.2 0.0.0.0 area 0
network 10.2.254.0 0.0.0.255 area 0
network 10.2.255.0 0.0.0.255 area 0
!
router bgp 65000
```

```
bgp log-neighbor-changes
neighbor C2RR peer-group
neighbor C2RR remote-as 65000
neighbor 10.2.99.9 peer-group C2RR
neighbor 10.2.99.10 peer-group C2RR
!
address-family ipv4
no neighbor 10.2.99.9 activate
no neighbor 10.2.99.10 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C2RR send-community both
neighbor 10.2.99.9 activate
neighbor 10.2.99.10 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
exit-address-family
!
address-family ipv4 vrf Internet
redistribute connected
redistribute ospf 2 vrf Internet
no synchronization
network 0.0.0.0 route-map GI_Community
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip rsvp signalling hello
!
ip explicit-path name LP_GE1/0 enable
exclude-address 10.2.255.5
!
ip explicit-path name LP_GE0/0 enable
exclude-address 10.2.254.2
!
ip explicit-path name LP_GE5/0 enable
exclude-address 10.1.255.22
!
```

```
!  
!  
!  
!  
route-map GI_Community permit 10  
set community 22  
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
!  
gatekeeper  
shutdown  
!  
!  
line con 0  
stopbits 1  
line aux 0  
stopbits 1  
line vty 0 4  
login  
!  
end
```

b.7. Configuración C2INTERNETFW1

C2INTERNETFW1
! ! upgrade fpd auto version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C2INTERNETFW1 ! boot-start-marker boot-end-marker

```
!  
logging message-counter syslog  
!  
no aaa new-model  
ip source-route  
ip cef  
!  
!  
!  
!  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config  
hidekeys  
!  
!  
!  
!  
!  
class-map type inspect match-any APN-TO-INTERNET  
match access-group name APN-TO-INTERNET  
!  
!  
policy-map type inspect APN-TO-INTERNET  
class type inspect APN-TO-INTERNET  
pass  
class class-default  
drop
```

```
!  
zone security gi_inside  
zone security gi_outside  
zone-pair security TO_INTERNET source gi_inside destination gi_outside  
service-policy type inspect APN-TO-INTERNET  
zone-pair security TO_NETWORK source gi_outside destination gi_inside  
service-policy type inspect APN-TO-INTERNET  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.2.99.5 255.255.255.255  
!  
interface Ethernet0/0  
no ip address  
shutdown  
duplex auto  
!  
interface GigabitEthernet0/0  
description TO_C1PMPLS1  
ip address 10.2.254.10 255.255.255.252  
ip nat inside  
ip virtual-reassembly  
zone-member security gi_inside  
duplex full  
speed 1000  
media-type gbic  
negotiation auto  
!  
interface GigabitEthernet1/0  
description TO_C1INTERNET1  
ip address 10.2.254.29 255.255.255.252  
ip nat outside  
ip virtual-reassembly  
zone-member security gi_outside  
negotiation auto  
!  
interface GigabitEthernet2/0  
description TO_C1FW2  
no ip address  
shutdown  
negotiation auto  
!  
router ospf 2  
log-adjacency-changes
```

```
redistribute static metric-type 1 subnets
network 10.2.99.5 0.0.0.0 area 0
network 10.2.254.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat pool NATPOOL 201.175.4.0 201.175.7.255 netmask 255.255.252.0 add-route
ip nat inside source list APN-TO-INTERNET pool NATPOOL overload
!
ip access-list extended APN-TO-INTERNET
permit ip 10.45.0.0 0.0.255.255 any
permit ip 10.46.0.0 0.0.255.255 any
permit icmp any any
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
!
end
```

b.8. Configuración C2INTERNETFW2

```
C2INTERNETFW2
!  
!  
upgrade fpd auto  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C2INTERNETFW2  
!  
boot-start-marker  
boot-end-marker  
!  
logging message-counter syslog  
!  
no aaa new-model  
ip source-route  
ip cef  
!  
!  
!  
!  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
log config
```

```
hidekeys
!
!
!
!
!
!
class-map type inspect match-any APN-TO-INTERNET
  match access-group name APN-TO-INTERNET
!
!
policy-map type inspect APN-TO-INTERNET
  class type inspect APN-TO-INTERNET
    pass
  class class-default
    drop
!
zone security gi_inside
zone security gi_outside
zone-pair security TO_INTERNET source gi_inside destination gi_outside
  service-policy type inspect APN-TO-INTERNET
zone-pair security TO_NETWORK source gi_outside destination gi_inside
  service-policy type inspect APN-TO-INTERNET
!
!
!
!
interface Loopback0
  description SERVICE
  ip address 10.2.99.6 255.255.255.255
!
interface Ethernet0/0
  no ip address
  shutdown
  duplex auto
!
interface GigabitEthernet0/0
  description TO_C1PMPLS1
  ip address 10.2.255.10 255.255.255.252
  ip nat inside
  ip virtual-reassembly
  zone-member security gi_inside
  duplex full
  speed 1000
  media-type gbic
  negotiation auto
!
```



```
!  
gatekeeper  
shutdown  
!  
!  
line con 0  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  login  
!  
end
```

b.9. Configuración C2INTERNET1

C2INTERNET1

```
!  
  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C2INTERNET1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
!  
!  
ip cef  
!  
!  
no ip domain lookup  
ip domain name lab.local  
!  
!  
!  
!  
interface Loopback0
```

```
description SERVICE
ip address 10.2.99.7 255.255.255.255
!
interface FastEthernet0/0
description TO_C1FW1
ip address 10.2.254.30 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
description TO_C1INTERNET2
ip address 10.2.254.37 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet1/0
description TO_ISP-1
ip address 190.150.10.2 255.255.255.252
duplex auto
speed auto
!
router ospf 2
log-adjacency-changes
network 10.2.99.7 0.0.0.0 area 0
network 10.2.254.0 0.0.0.255 area 0
default-information originate metric-type 1
!
router bgp 65000
no synchronization
bgp log-neighbor-changes
redistribute ospf 2 match external 1 external 2
neighbor 10.2.99.8 remote-as 65000
neighbor 10.2.99.8 update-source Loopback0
neighbor 190.150.10.1 remote-as 12300
no auto-summary
!
ip http server
ip forward-protocol nd
!
!
!
!
!
control-plane
!
!
line con 0
```

```
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end
```

b.10. Configuración C2INTERNET2

C2INTERNET2

```
!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2INTERNET2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
no ip domain lookup
ip domain name lab.local
!
!
!
!
interface Loopback0
description SERVICE
ip address 10.2.99.8 255.255.255.255
```

```
!  
interface FastEthernet0/0  
description TO_C1FW2  
ip address 10.2.255.30 255.255.255.252  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
description TO_C1INTERNET1  
ip address 10.2.254.38 255.255.255.252  
duplex auto  
speed auto  
!  
interface FastEthernet1/0  
description TO_ISP-2  
ip address 181.156.237.2 255.255.255.252  
duplex auto  
speed auto  
!  
router ospf 2  
log-adjacency-changes  
network 10.2.99.8 0.0.0.0 area 0  
network 10.2.254.0 0.0.0.255 area 0  
network 10.2.255.0 0.0.0.255 area 0  
default-information originate metric-type 1  
!  
router bgp 65000  
no synchronization  
bgp log-neighbor-changes  
redistribute ospf 2 match external 1 external 2  
neighbor 10.2.99.7 remote-as 65000  
neighbor 10.2.99.7 update-source Loopback0  
neighbor 181.156.237.1 remote-as 12300  
neighbor 181.156.237.1 route-map AS-PATH out  
no auto-summary  
!  
ip http server  
ip forward-protocol nd  
!  
!  
!  
!  
ip prefix-list AS-PATH seq 5 permit 201.175.4.0/22  
route-map AS-PATH permit 10  
match ip address prefix-list AS-PATH  
set as-path prepend 65000 65000 65000  
!
```

```
!  
!  
control-plane  
!  
!  
line con 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line aux 0  
  exec-timeout 0 0  
  privilege level 15  
  logging synchronous  
line vty 0 4  
  login  
!  
end
```

b.11. Configuración C2RR1

C2RR1

```
!  
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname C2RR1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 5  
!  
!  
ip cef  
!  
!  
ip vrf O&M  
  rd 65000:1  
  route-target export 65000:1  
  route-target import 65000:1
```

```
!  
no ip domain lookup  
ip domain name lab.local  
mpls traffic-eng tunnels  
!  
!  
!  
!  
!  
interface Loopback0  
description SERVICE  
ip address 10.2.99.9 255.255.255.255  
!  
interface Loopback1  
ip vrf forwarding O&M  
ip address 10.2.100.9 255.255.255.255  
!  
interface FastEthernet0/0  
description TO_C2PMPLS1  
ip address 10.2.254.14 255.255.255.252  
duplex auto  
speed auto  
mpls traffic-eng tunnels  
!  
interface FastEthernet0/1  
description TO_C2PMPLS2  
ip address 10.2.255.18 255.255.255.252  
duplex auto  
speed auto  
mpls traffic-eng tunnels  
!  
router ospf 1  
mpls traffic-eng router-id Loopback0  
mpls traffic-eng area 0  
log-adjacency-changes  
network 10.2.99.9 0.0.0.0 area 0  
network 10.2.254.0 0.0.0.255 area 0  
network 10.2.255.0 0.0.0.255 area 0  
!  
router bgp 65000  
bgp cluster-id 2  
bgp log-neighbor-changes  
neighbor C2_PE&P peer-group  
neighbor C2_PE&P remote-as 65000  
neighbor C2_PE&P update-source Loopback0  
neighbor C1_RR peer-group  
neighbor C1_RR remote-as 65000
```

```
neighbor C1_RR update-source Loopback0
neighbor 10.1.99.9 peer-group C1_RR
neighbor 10.1.99.10 peer-group C1_RR
neighbor 10.2.99.1 peer-group C2_PE&P
neighbor 10.2.99.2 peer-group C2_PE&P
neighbor 10.2.99.3 peer-group C2_PE&P
neighbor 10.2.99.4 peer-group C2_PE&P
!
address-family ipv4
no neighbor 10.1.99.9 activate
no neighbor 10.1.99.10 activate
no neighbor 10.2.99.1 activate
no neighbor 10.2.99.2 activate
no neighbor 10.2.99.3 activate
no neighbor 10.2.99.4 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C2_PE&P send-community both
neighbor C2_PE&P route-reflector-client
neighbor C1_RR send-community both
neighbor C1_RR route-reflector-client
neighbor 10.1.99.9 activate
neighbor 10.1.99.10 activate
neighbor 10.2.99.1 activate
neighbor 10.2.99.2 activate
neighbor 10.2.99.3 activate
neighbor 10.2.99.4 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
exit-address-family
!
ip http server
ip forward-protocol nd
!
!
!
!
!
!
control-plane
!
!
```

```
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end
```

b.12. Configuración C2RR2

C2RR2
<pre>! ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname C2RR2 ! boot-start-marker boot-end-marker ! ! no aaa new-model memory-size iomem 5 ! ! ip cef ! ! ip vrf Internet rd 65000:1002 route-target export 65000:2 route-target import 65000:2 ! ip vrf O&M rd 65000:1001 route-target export 65000:1 route-target import 65000:1 !</pre>

```
no ip domain lookup
ip domain name lab.local
mpls traffic-eng tunnels
!
!
!
!
!
interface Loopback0
description SERVICE
ip address 10.2.99.10 255.255.255.255
!
interface Loopback1
ip vrf forwarding O&M
ip address 10.2.100.10 255.255.255.255
!
interface FastEthernet0/0
description TO_C2PMPLS2
ip address 10.2.255.14 255.255.255.252
shutdown
duplex auto
speed auto
mpls traffic-eng tunnels
!
interface FastEthernet0/1
description TO_C2PMPLS1
ip address 10.2.254.18 255.255.255.252
shutdown
duplex auto
speed auto
mpls traffic-eng tunnels
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
network 10.2.99.10 0.0.0.0 area 0
network 10.2.254.0 0.0.0.255 area 0
network 10.2.255.0 0.0.0.255 area 0
!
router bgp 65000
bgp cluster-id 1
bgp log-neighbor-changes
neighbor C2_PE&P peer-group
neighbor C2_PE&P remote-as 65000
neighbor C2_PE&P update-source Loopback0
neighbor C1_RR peer-group
```

```
neighbor C1_RR remote-as 65000
neighbor C1_RR update-source Loopback0
neighbor 10.1.99.9 peer-group C1_RR
neighbor 10.1.99.10 peer-group C1_RR
neighbor 10.2.99.1 peer-group C2_PE&P
neighbor 10.2.99.2 peer-group C2_PE&P
neighbor 10.2.99.3 peer-group C2_PE&P
neighbor 10.2.99.4 peer-group C2_PE&P
!
address-family ipv4
no neighbor 10.1.99.9 activate
no neighbor 10.1.99.10 activate
no neighbor 10.2.99.1 activate
no neighbor 10.2.99.2 activate
no neighbor 10.2.99.3 activate
no neighbor 10.2.99.4 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor C2_PE&P send-community both
neighbor C2_PE&P route-reflector-client
neighbor C1_RR send-community both
neighbor C1_RR route-reflector-client
neighbor 10.2.99.1 activate
neighbor 10.2.99.2 activate
neighbor 10.2.99.3 activate
neighbor 10.2.99.4 activate
exit-address-family
!
address-family ipv4 vrf O&M
redistribute connected
no synchronization
exit-address-family
!
address-family ipv4 vrf Internet
no synchronization
exit-address-family
!
no ip http server
ip forward-protocol nd
!
!
!
!
!
```

```
control-plane
!  
!  
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!  
end
```

b.13. Configuración SERVICE PROVIDER

SERVICE PROVIDER

```
!  
!  
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!  
hostname SERVICEPROVIDER
!  
boot-start-marker
boot-end-marker
!  
!  
no aaa new-model
memory-size iomem 5
!  
!  
ip cef
!  
!  
no ip domain lookup
ip domain name lab.local
!  
!  
!  
!
```

```
!  
interface Loopback1000  
ip address 4.2.2.2 255.255.255.255  
!  
interface FastEthernet0/0  
ip address 200.139.131.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
ip address 186.101.30.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface FastEthernet1/0  
ip address 190.150.10.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface FastEthernet2/0  
ip address 181.156.237.1 255.255.255.252  
duplex auto  
speed auto  
!  
interface FastEthernet3/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface FastEthernet4/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
router bgp 12300  
no synchronization  
bgp log-neighbor-changes  
timers bgp 1 3  
neighbor 181.156.237.2 remote-as 65000  
neighbor 181.156.237.2 default-originate  
neighbor 186.101.30.2 remote-as 65000  
neighbor 186.101.30.2 default-originate  
neighbor 190.150.10.2 remote-as 65000  
neighbor 190.150.10.2 default-originate  
neighbor 200.139.131.2 remote-as 65000
```

```
neighbor 200.139.131.2 default-originate
no auto-summary
!
no ip http server
ip forward-protocol nd
!
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end
```

b.14. Configuración Servidor R27 (Emulación de un Host)

Servidor R27 (Emulación de un host)

```
!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R27
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
```

```
!  
!  
!  
!  
no ip domain lookup  
ip domain name lab.local  
ip auth-proxy max-nodata-conns 3  
ip admission max-nodata-conns 3  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
vtp mode transparent  
archive  
log config  
hidekeys  
!  
!  
!  
!  
vlan 10  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
no ip address  
shutdown
```

```
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
!
interface FastEthernet1/1
switchport access vlan 10
!
interface FastEthernet1/2
switchport access vlan 10
!
interface FastEthernet1/3
!
interface FastEthernet1/4
!
interface FastEthernet1/5
!
interface FastEthernet1/6
!
interface FastEthernet1/7
!
interface FastEthernet1/8
!
interface FastEthernet1/9
!
interface FastEthernet1/10
!
interface FastEthernet1/11
!
interface FastEthernet1/12
!
interface FastEthernet1/13
!
interface FastEthernet1/14
!
interface FastEthernet1/15
!
interface Vlan1
no ip address
!
interface Vlan10
```

```
ip address 10.45.0.100 255.255.0.0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.45.0.1
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

