UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Analista de Operación y Mantenimiento en Empresa de Telecomunicaciones

INFORME DE ACTIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Hugo Fernando Luna Rodríguez

ASESOR(A) DE INFORME

Ing. Carlos Román Zamitiz

Ciudad Universitaria, Cd. Mx., 2018

Agradecimientos

A Dios y a mi familia

Por haber estado conmigo durante todo el camino para llegar al titulo de ingeniero, agradezco su apoyo, su esfuerzo y su amor, dedico a ustedes el fruto de nuestro trabajo de todos estos años.

A la Universidad Nacional Autónoma de México, Facultad de Ingeniería y Profesores

Por haberme abierto las puertas de la máxima casa de estudios y haberme ayudado a superarme a nivel intelectual y como persona. Marce, Gera agradezco el gran apoyo para ayudarme a entrar y a mantenerme en la UNAM. Profesor Carlos, gracias por el apoyo para culminar con el proceso de titulación.

ÍNDICE

INTRODUCCIÓN

Una empresa de telecomunicaciones es aquella que se dedica a ofrecer servicios de telefonía móvil, telefonía fija, servicios de banda ancha, entre otros servicios mediante la implementación de la ingeniería y la tecnología de punta para satisfacer al máximo al cliente, atraer a más clientes y hacer de su red la mejor y con mayor presencia en todo el país.

Debido a lo anterior las empresas de telecomunicaciones cuentan con un área especializada en la puesta en marcha de los equipos de la red y el mantenimiento en óptimas condiciones de funcionamiento de estos equipos así como garantizar la alta disponibilidad de los servicios de red tanto en condiciones normales como en caso de falla, todo esto con el objetivo de brindar a cualquiera de los tipos de cliente la seguridad y confianza de que sus servicios, comunicaciones y transacciones se realizarán de manera exitosa, segura y en el momento en el que lo requieran sin importar el día o la hora.

En el presente informe demuestro aplicar los conocimientos adquiridos en la carrera de Ingeniería en Computación de la Facultad de Ingeniería, en el área de Operación y Mantenimiento de la empresa de telecomunicaciones más grande y con mayor presencia en el país.

En el capítulo 1, muestro brevemente la estructura del área, así como su visión, misión, y las actividades cotidianas.

En el capítulo 2, muestro el marco teórico, conocimientos que adquirí en mi etapa como estudiante de la carrera de Ingeniería en Computación, mismos que apliqué en el capítulo 3, 4 y 5.

En el capítulo 3, muestro las actividades de inducción para obtener los conocimientos necesarios relacionados al puesto que ocupo actualmente en la empresa.

En el capítulo 4, muestro dos ejemplos de casos de falla en la red, así como su solución y la causa de los problemas que se presentaron.

En el capítulo 5, muestro el proyecto que me fue asignado, sus objetivos, implementación y los resultados.

CAPÍTULO 1: ORGANIZACIÓN Y ACTIVIDAD PROFESIONAL

1.1 Misión y visión de la empresa

1.1.1 Misión

Mejorar la vida de nuestros clientes, ayudando a personas, negocios y comunidades a estar más y mejor conectados con el mundo.

1.1.2 Visión

Ser líderes en el mercado de las comunicaciones de México, ofreciendo productos y servicios de excelencia, generando bienestar para nuestros clientes, equipo humano, inversionistas, socios de negocios y comunidad.

1.1.3 Valores

- Honestidad
- Respeto
- Servicio
- Austeridad
- Contribución social
- Desarrollo humano
- Creatividad

1.2 Dirección de Operación y Mantenimiento (O&M)

Operación y Mantenimiento, es una de las áreas que integra la empresa a la cual voy a referirme (véase figura 1.1), O&M asegura dentro de la empresa la disponibilidad de la infraestructura de la red, operando la red celular dentro de los estándares establecidos con el fin de brindar el mejor servicio a los usuarios.

1.2.1 Objetivo

Cumplir con la disponibilidad de los elementos de la red al 99.999%.

Se tienen como directriz los procesos generales de O&M: Recepción, Corrección, Rutinas y Mantenimientos preventivos, Mejorar la Red con Análisis Estadístico, Asegurar disponibilidad e integración de nuevas plataformas.

Figura 1.1 Estructura Organizacional

1.3 Subdirección O&M Red de Transmisión

La Subdirección O&M Red de Transmisión, desempeña un papel fundamental en toda la empresa, ya que se encarga de las siguientes actividades:

- Corregir las fallas de la red celular para mantener la disponibilidad del servicio dentro de los estándares de calidad establecidos.

- Prevenir fallas mediante rutinas de mantenimiento para garantizar la disponibilidad de la red.

- Mejorar la red celular a través del análisis estadístico para implementar acciones de mejora.

Figura 1.2 Subdirección O&M Red de Transmisión

1.4 Gerencia de la Red MPLS

La Gerencia de la red MPLS tiene como responsabilidad dentro de la Subdirección O&M Red de Transmisión lograr los siguientes objetivos:

- Mantener la disponibilidad de los equipos del CORE MPLS en 99.999% con un parámetro de desviación permisible de 0.004%.

- Mantener la disponibilidad en los perímetros de Seguridad IP de Tráfico Masivo y Acceso en 99.99% con un parámetro de desviación permisible de 0.05%.

- Mantener la disponibilidad de los equipos de IP de acceso en Edif Corp. y red LAN en Centrales de 99.99% con un parámetro de desviación permisible 0.05%.

- Mantener la disponibilidad en los equipos de la red de transporte IP RAN en 99.95% con un parámetro de desviación permisible de 0.5 %.

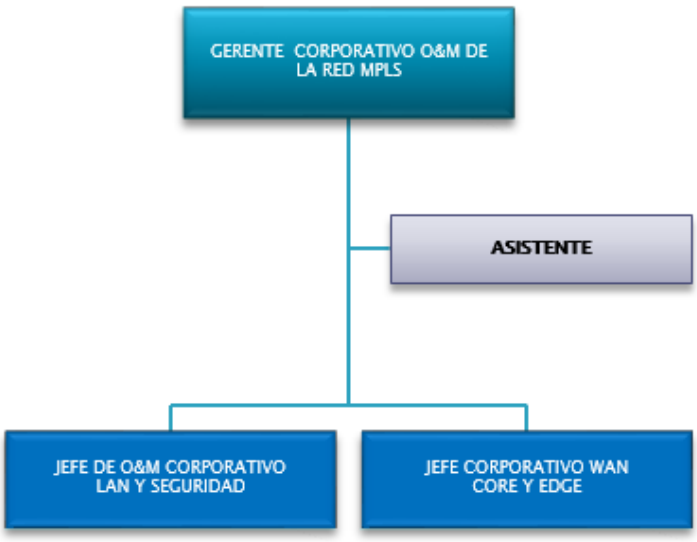


Figura 1.3 Gerencia de la red MPLS

1.5 Departamento O&M Wan, Core y Edge

El analista de O&M Wan, Core y Edge tiene como objetivo realizar un análisis estadístico para detectar fallas en la red MPLS, así como documentar los diferentes procesos, mantenimientos, acciones de mejora e información necesaria para la operación de la infraestructura de red MPLS.

Funciones principales:

- Administración y operación de equipos de datos y comunicaciones (routers, firewalls).
- Administración y diseño de redes MPLS.
- Clasificar alarmas para documentar la severidad y solución.
- Implementar las acciones de mejora para eliminar causa raíz del problema.
- Documentar la solución para tener registro de las acciones realizadas.
- Planear las rutinas de mantenimiento para seguir una estrategia de prevención.
- Documentar el plan de mantenimiento para tener un registro de las actividades a seguir durante su ejecución.

CAPÍTULO 2: MARCO TEÓRICO

2.1 Conceptos generales

Software

Software es el conjunto lógico de la computadora que cumple funciones específicas y que gracias a ellas es posible la realización de actividades, estas aplicaciones generan una interfaz o sistema de comunicación entre el usuario y la computadora.

Hardware

Corresponde a todas las partes físicas y tangibles de una computadora, sus componentes eléctricos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Sistemas

Un sistema es un conjunto de elementos de hardware, software, personas, procedimientos, herramientas, organizados de tal manera que lleven a cabo un objetivo en común.

Ingeniería en Sistemas

La ingeniería en sistemas, de acuerdo con la definición de Defense Systems Management College 1986, define el plan para gestionar las actividades técnicas del proyecto, identifica el ciclo de desarrollo y los procesos que serán necesarios aplicar. Desde la Ingeniería de sistemas se desarrolla la línea base técnica para todo el desarrollo, tanto de hardware como de software.

Las funciones que corresponden a la ingeniería en sistemas son:

- **Definición del problema:** Determina las expectativas hacia el producto, necesidades y restricciones obtenidas y analizadas en los requisitos del sistema. Trabaja cerca y constantemente con el cliente para establecer las necesidades operacionales del requerimiento.

- **Análisis de la solución:** Determina las opciones posibles para satisfacer los requisitos y necesidades del cliente, así como sus restricciones. Estudian y analizan las soluciones encontradas y eligen la mejor opción.

- **Planificación de procesos:** Determina grupos de tareas técnicas que se deben realizar, el esfuerzo requerido para cada una, su prioridad y los riesgos que implican para el proyecto.

- **Control de procesos:** Determina los métodos para controlar las actividades técnicas del proyecto y los procesos; la medición del progreso, revisión de los productos intermedios y ejecución de las acciones correctivas, cuando corresponda.

- **Evaluación del producto:** Determina la calidad y cantidad de los productos elaborados, a través de evaluaciones, inspecciones, pruebas, etc.

2.2 Redes de datos

Componentes de la Red

La infraestructura de red contiene tres categorías de componentes de red:

- Dispositivos

- Medios

- Servicios

Los dispositivos y los medios son los elementos físicos o el hardware, de la red. El hardware está compuesto por una PC, un switch, un router, un punto de acceso inalámbrico o el cableado que se utiliza para conectar esos dispositivos. A veces algunos componentes no son visibles como el caso de los medios inalámbricos.

Los componentes de red se utilizan para proporcionar servicios y procesos, que son los programas de comunicación (software), que se ejecutan en los dispositivos conectados en red. Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen hosting de correo electrónico y web hosting.

Dispositivos Finales

Los dispositivos de red con los que las personas están más familiarizadas se denominan “dispositivos finales” o “hosts”. Estos dispositivos forman la interfaz entre los usuarios y la red de comunicación subyacente. Un dispositivo host es el origen o el destino de un mensaje transmitido a través de la red.

Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Terminales de TelePresence
- Cámaras de seguridad
- Dispositivos portátiles móviles (como smartphones, tablets, lectores inalámbricos de tarjetas de débito y crédito, y escáneres de códigos de barras)

Dispositivos de Red Intermediarios

Los dispositivos intermediarios interconectan dispositivos finales. Estos dispositivos proporcionan conectividad y aseguran que los datos fluyan a través de la red. Los dispositivos intermediarios conectan los hosts individuales a la red y pueden conectar varias redes individuales.

Los siguientes son ejemplos de dispositivos de red intermediarios:

- Acceso a la red (switches y puntos de acceso inalámbrico)
- Internetworking (routers)
- Seguridad (firewalls)

Los dispositivos intermediarios utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red para determinar la ruta que deben tomar los mensajes a través de la red.

Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red.
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.
- Clasificar y dirigir los mensajes según las prioridades de calidad de servicio (QoS, Quality of Service).
- Permitir o denegar el flujo de datos de acuerdo con la configuración de seguridad

Tipos de Red

Red de área local (LAN, Local Area Network): Las redes de área local son infraestructuras de red que proporcionan acceso a los usuarios y a los dispositivos finales en un área geográfica pequeña.

Las características de las LAN incluyen lo siguiente:

- Las LAN interconectan dispositivos finales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.
- Por lo general, la administración de las LAN está a cargo de una única organización o persona. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.
- Las LAN proporcionan un ancho de banda de alta velocidad a los dispositivos finales internos y a los dispositivos intermediarios.

LAN inalámbrica (WLAN, Wireless LAN): Las LAN inalámbricas son similares a las LAN, solo que interconectan de forma inalámbrica a los usuarios y los extremos en un área geográfica pequeña.

Red de área extensa (WAN, Wide Area Network): Las redes de área extensa son infraestructuras de red que proporcionan acceso a otras redes en un área geográfica extensa.

Las características específicas de las WAN incluyen lo siguiente:

- Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes.

- Por lo general, la administración de las WAN está a cargo de proveedores de servicios de Internet (ISP).

- Normalmente, las WAN proporcionan enlaces de velocidad más lenta entre redes LAN.

Internet

Aunque el uso de redes LAN o WAN tiene ventajas, la mayoría de las personas necesitan comunicarse con un recurso ubicado en otra red, fuera de la red local del hogar, el campus o la organización. Esto se logra mediante el uso de Internet.

Internet es una colección mundial de redes interconectadas que colaboran para intercambiar información sobre la base de estándares comunes. A través de cables telefónicos, cables de fibra óptica, transmisiones inalámbricas y enlaces satelitales, los usuarios de Internet pueden intercambiar información de diversas formas.

Existen varias formas diferentes de conectar a usuarios y organizaciones a Internet:

- **Cable:** Servicio ofrecido por proveedores de servicios de televisión por cable. La señal de datos de Internet se transmite a través del mismo cable coaxial que transporta la señal de televisión por cable. Esta opción proporciona una conexión a Internet permanente y de un ancho de banda elevado. Se utiliza un módem por cable especial que separa la señal de datos de Internet de las otras señales que transporta el cable.

- **DSL:** Proporciona una conexión a Internet permanente y de un ancho de banda elevado. Requiere un módem de alta velocidad especial que separa la señal DSL de la señal telefónica. La señal DSL se transmite a través de una línea telefónica, que está dividida en tres canales. Uno de los canales se utiliza para llamadas telefónicas de voz. Este canal permite que una persona reciba llamadas telefónicas sin desconectarse de Internet. El segundo es un canal de descarga más rápido y se utiliza para recibir información de Internet. El tercer canal se utiliza para enviar o subir información.

- **Datos móviles:** El acceso a Internet por datos móviles se logra mediante una red de telefonía celular. Puede obtener acceso a Internet por datos móviles en cualquier lugar donde tenga cobertura de telefonía móvil. El rendimiento se verá limitado por las capacidades del teléfono y la torre de telefonía móvil a la que se conecte.

Modelo OSI

Es el modelo de referencia de internetwork más conocido. Se usa para diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

El Modelo OSI cuenta con las siguientes capas:

1) Física: Los protocolos de capa física describen los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits hacia un dispositivo de red y desde él.

2) Enlace de datos: Los protocolos de capa de enlace de datos describen los métodos para intercambiar tramas de datos entre dispositivos en un medio común.

3) Red: La capa de red proporciona servicios para intercambiar los datos individuales en la red entre dispositivos finales identificados.

4) Transporte: La capa de transporte define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones individuales entre dispositivos finales.

5) Sesión: La capa de sesión proporciona servicios a la capa de presentación para organizar su diálogo y administrar el intercambio de datos.

6) Presentación: La capa de presentación proporciona una representación común de los datos transferidos entre los servicios de la capa de aplicación.

7) Aplicación: La capa de aplicación proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana mediante redes de datos.

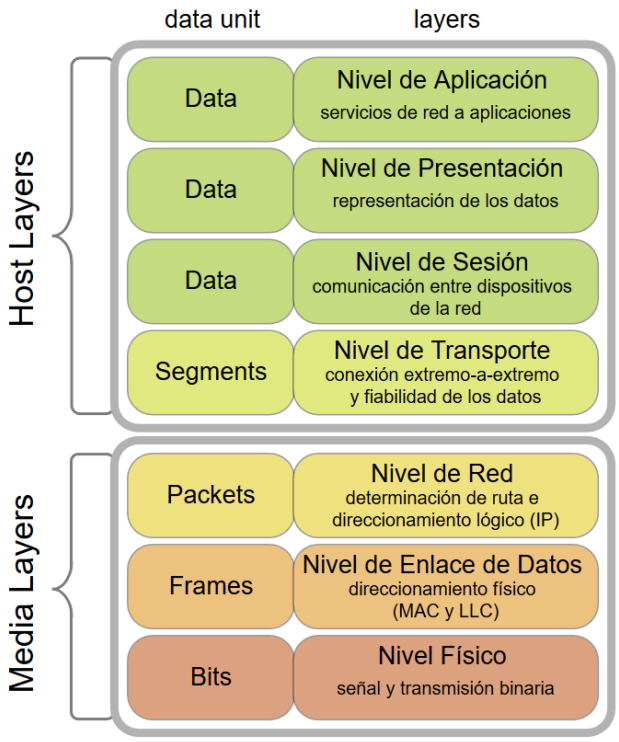


Figura 2.1 Modelo de Referencia OSI

Medios de Transmisión

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos:

- Hilos metálicos dentro de cables (Cobre)
- Fibras de vidrio o plástico (cable de fibra óptica)
- Transmisión inalámbrica

La capa física produce la representación y las agrupaciones de bits para cada tipo de medio de la siguiente manera:

- Cable de cobre: Las señales son patrones de pulsos eléctricos.
- Cable de fibra óptica: Las señales son patrones de luz.
- Conexión inalámbrica: Las señales son patrones de transmisiones de microondas.

Los criterios para elegir medios de red son los siguientes:

- La distancia por la que los medios pueden transportar una señal correctamente.
- El entorno en el que se instalarán los medios.
- La cantidad de datos y la velocidad a la que se deben transmitir.
- El costo del medio y de la instalación.

Opciones de conexión de Enlaces WAN

Existen diversas opciones de conexión de acceso WAN que los ISP pueden utilizar para conectar el bucle local al perímetro empresarial. Estas opciones de acceso WAN varían en términos de tecnología, velocidad y costo.

- **Infraestructura WAN privada:** Los proveedores de servicios pueden ofrecer líneas arrendadas punto a punto dedicadas, enlaces de conmutación de circuitos, como PSTN o ISDN, y enlaces de conmutación de paquetes, como WAN Ethernet, ATM o Frame Relay.
- **Infraestructura WAN pública:** El proveedor de servicios puede ofrecer acceso a Internet de banda ancha mediante una línea de suscriptor digital (DSL), cable y acceso satelital. Las opciones de conexión de banda ancha normalmente se usan para conectar oficinas pequeñas y trabajadores a distancia a un sitio corporativo a través de Internet. Los datos que se transmiten entre sitios corporativos a través de la infraestructura WAN pública se deben proteger mediante VPN.

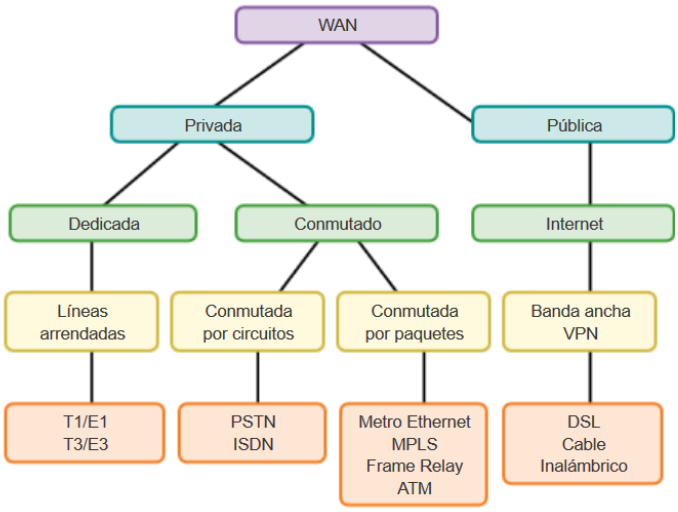


Figura 2.2 Opciones de Acceso WAN

Líneas Arrendadas

Cuando se requieren conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar una ruta de comunicaciones WAN preestablecida desde las instalaciones del cliente hasta la red del proveedor. Por lo general, un proveedor de servicios arrienda las líneas punto a punto, que se llaman “líneas arrendadas”.

El término “línea arrendada” hace referencia al hecho de que la organización paga una tarifa mensual de arrendamiento a un proveedor de servicios para usar la línea. Hay líneas arrendadas disponibles con diferentes capacidades y, generalmente, el precio se basa en el ancho de banda requerido y en la distancia entre los dos puntos conectados.

En América del Norte, los proveedores de servicios usan el sistema de portadora T para definir la capacidad de transmisión digital de un enlace serial de medios de cobre, mientras que en Europa se usa el sistema de portadora E. Por ejemplo, un enlace T1 admite 1.544 Mb/s, un E1admite 2.048 Mb/s, un T3 admite 43.7 Mb/s y una conexión E3 admite 34.368 Mb/s.

Un enlace E1 puede llevar 32 canales de 64 Kbps cada uno, de los cuales treinta y uno son canales activos simultáneos para voz o datos y uno más para señalización. Los E1 operan sobre dos juegos separados de cable, usualmente es un cable coaxial.

Propiedades del cableado UTP

El cableado de par trenzado no blindado (UTP) consta de cuatro pares de hilos codificados por color que están trenzados entre sí y recubiertos con un revestimiento de plástico flexible.

Los cables UTP dependen exclusivamente del efecto de anulación producido por los pares de hilos trenzados para limitar la degradación de la señal y proporcionar un autoblindaje eficaz de los pares de hilos en los medios de red.

El cableado UTP cumple con los estándares establecidos en conjunto por la TIA/EIA. Específicamente, TIA/EIA-568A estipula los estándares comerciales de cableado para las instalaciones de LAN y es el estándar más utilizado en los entornos de cableado LAN. Algunos de los elementos definidos son:

- Tipos de cables
- Longitudes del cable
- Conectores

- Terminación de los cables

- Métodos para realizar pruebas de cable

El Instituto de Ingenieros en Electricidad y Electrónica (IEEE) define las características eléctricas del cableado de cobre. IEEE califica el cableado UTP según su rendimiento. Los cables se dividen en categorías según su capacidad para transportar datos de ancho de banda a velocidades mayores. Por ejemplo, el cable de Categoría 5 (Cat5) se utiliza comúnmente en las instalaciones de FastEthernet 100BASE-TX. Otras categorías incluyen el cable de categoría 5 mejorada (Cat5e), la categoría 6 (Cat6) y la categoría 6a.

Los cables UTP se terminan generalmente con un conector RJ-45 especificado por el estándar ISO 8877.

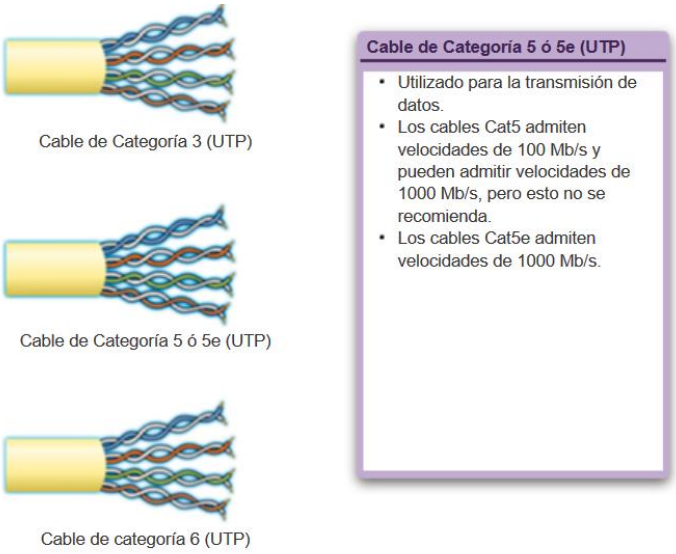
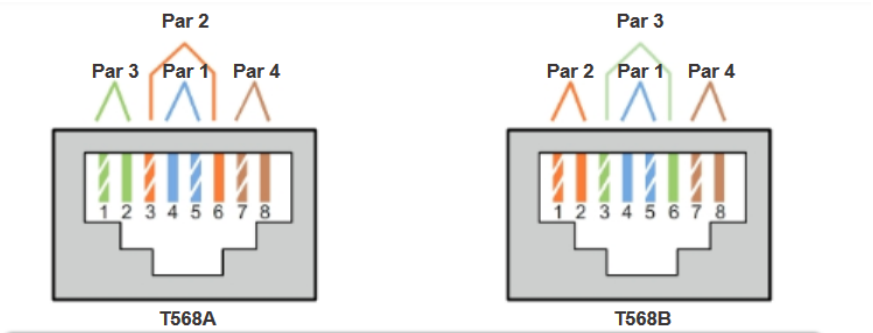


Figura 2.3 Cable Categoría 5

Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados. Esto significa que los hilos individuales del cable deben conectarse en diferente orden para distintos grupos de pines en los conectores RJ-45.



Tipo de cable	Estándar	Capa de aplicación
Cable directo de Ethernet	Ambos extremos son T568A o T568B.	Conecta un host de red a un dispositivo de red, como un switch o un hub.
Cruzado Ethernet	Un extremo es T568A, el otro extremo es T568B.	• Conecta dos hosts de red. • Conecta dos dispositivos de red intermediarios (un switch a un switch, o un router a un router).
De consola	Propietario de Cisco	Conecta el puerto serie de una estación de trabajo al puerto de consola de un router mediante un adaptador.

Figura 2.4 Cable UTP: Estándares Relacionados y Aplicación Típica

Half Duplex y Full Duplex

En las redes, los datos pueden fluir de dos maneras:

- **Comunicación Half-Duplex:** Ambos dispositivos pueden transmitir y recibir datos en los medios, pero no pueden hacerlo en forma simultánea.

- **Comunicación Full-Duplex:** Ambos dispositivos pueden transmitir y recibir datos en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para que ambos nodos.

Switch

Es el dispositivo de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

Los switches se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

Router

Un router es un dispositivo que proporciona conectividad a nivel de red o capa tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red o un switch), y que por tanto tienen prefijos de red distintos. También tiene la función de determinar la mejor ruta para enviar paquetes.

Dirección MAC

La dirección física de la capa de enlace de datos, o capa 2, tiene como propósito enviar la trama de enlace de datos desde una interfaz de red hasta otra interfaz de red en la misma red. Antes de que un paquete IP pueda enviarse a través de una red conectada por cable o inalámbrica, se debe encapsular en una trama de enlace de datos de modo que pueda transmitirse a través del medio físico.

El paquete IP se encapsula en una trama de enlace de datos para enviarse a la red de destino agregando las siguientes direcciones:

- **Dirección de enlace de datos de origen:** La dirección física del dispositivo que envía el paquete. Inicialmente, es la NIC que es el origen del paquete IP.

- **Dirección de enlace de datos de destino:** La dirección física de la interfaz de red del router del siguiente salto o de la interfaz de red del dispositivo de destino.

Dirección IP

La dirección lógica de la capa de red, o capa 3, contiene la información necesaria para enviar el paquete IP desde el dispositivo de origen hasta el dispositivo de destino. Una dirección IP de capa 3 tiene dos partes: el prefijo de red y la parte de host.

Los routers utilizan el prefijo de red para reenviar el paquete a la red adecuada. El último router de la ruta utiliza la parte de host para enviar el paquete al dispositivo de destino.

Los paquetes IP contienen dos direcciones IP:

- **Dirección IP de origen:** La dirección IP del dispositivo emisor.

- **Dirección IP de destino:** La dirección IP del dispositivo receptor. Los routers utilizan la dirección IP de destino para reenviar un paquete a su destino.

ARP (Protocolo de Resolución de Direcciones)

Un host emisor utiliza ARP para descubrir la dirección MAC de cualquiera de los hosts de la misma red local. El host emisor envía un mensaje de solicitud de ARP a toda la LAN. La solicitud de ARP es un mensaje de broadcast. La solicitud de ARP contiene la dirección IP del dispositivo de destino. Cada dispositivo en la LAN examina la solicitud de ARP para ver si contiene su propia dirección IP. Solamente el dispositivo con la dirección IP contenida en la solicitud de ARP responde con una respuesta de ARP.

La respuesta de ARP incluye la dirección MAC asociada con la dirección IP en la solicitud de ARP.

Protocolos de la Capa de Transporte

TCP (Protocolo de Control de Transmisión)

Es un protocolo de transporte confiable, lo que significa que incluye procesos para garantizar la entrega confiable entre aplicaciones mediante el uso de entrega con acuse de recibo y proporciona lo siguiente:

- **Conversaciones orientadas a la conexión mediante el establecimiento de sesiones:** TCP es un protocolo orientado a la conexión. Un protocolo orientado a la conexión es uno que negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y de destino antes de reenviar tráfico. El establecimiento de sesión prepara los dispositivos para que se comuniquen entre sí. Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente. La sesión se termina solo cuando se completa toda la comunicación.

- **Entrega confiable:** TCP puede implementar un método para garantizar la entrega confiable de los datos. En términos de redes, confiabilidad significa asegurar que cada sección de datos que envía el origen llegue al destino. Por varias razones, es posible que una sección de datos se corrompa o se pierda por completo a medida que se transmite a través de la red. TCP puede asegurar que todas las partes lleguen a destino al hacer que el dispositivo de origen retransmita los datos perdidos o dañados.

- **Reconstrucción de datos ordenada:** Los datos pueden llegar en el orden equivocado, debido a que las redes pueden proporcionar varias rutas que pueden tener diferentes velocidades de transmisión. Al numerar y secuenciar los segmentos, TCP puede asegurar que estos se rearmen en el orden correcto.

- **Control del flujo:** Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a cabo TCP, que regula la cantidad de datos que transmite el origen. El control de flujo puede evitar la pérdida de segmentos en la red y evitar la necesitad de la retransmisión.

UDP (Protocolo de Datagramas de Usuario)

Protocolo de transporte que proporciona solo las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos. Las siguientes características describen a UDP:

- **Sin conexión:** UDP no establece una conexión entre los hosts antes de que se puedan enviar y recibir datos.

- **Entrega no confiable:** UDP no proporciona servicios para asegurar que los datos se entreguen con confianza. UDP no cuenta con procesos que hagan que el emisor vuelva a transmitir los datos que se pierden o se dañan.

- **Reconstrucción de datos no ordenada:** En ocasiones, los datos se reciben en un orden distinto del de envío. UDP no proporciona ningún mecanismo para rearmar los datos en su secuencia original. Los datos simplemente se entregan a la aplicación en el orden en que llegan.

- **Sin control del flujo:** UDP no cuenta con mecanismos para controlar la cantidad de datos que transmite el dispositivo de origen para evitar la saturación del dispositivo de destino. El origen envía los datos. Si los recursos en el host de destino se sobrecargan, es probable que dicho host descarte los datos enviados hasta que los recursos estén disponibles. A diferencia de TCP, en UDP no hay un mecanismo para la retransmisión automática de datos descartados.

Direccionamiento de puertos TCP y UDP

Cuando se envía un mensaje utilizando TCP o UDP, los protocolos y servicios solicitados se identifican con un número de puerto. Un puerto es un identificador numérico de cada segmento, que se utiliza para realizar un seguimiento de conversaciones específicas y de servicios de destino solicitados. Cada mensaje que envía un host contiene un puerto de origen y un puerto de destino.

- **Puerto de destino:** El cliente coloca un número de puerto de destino en el segmento para informar al servidor de destino el servicio solicitado. Por ejemplo: el puerto 80 se refiere a HTTP o al servicio Web. Cuando un cliente especifica el puerto 80 en el puerto de destino, el servidor que recibe el mensaje sabe que se solicitan servicios Web.

- **Puerto de origen:** El número de puerto de origen es generado de manera aleatoria por el dispositivo emisor para identificar una conversación entre dos dispositivos. Esto permite establecer varias conversaciones simultáneamente. En otras palabras, un dispositivo puede enviar varias solicitudes de servicio HTTP a un servidor Web al mismo tiempo. El seguimiento de las conversaciones por separado se basa en los puertos de origen.

Gateway Predeterminado

Cuando un host necesita enviar un mensaje a una red remota, debe utilizar el router, también conocido como “gateway predeterminado”. El gateway predeterminado es la dirección IP de una interfaz de un router en la misma red que el host emisor.

Es importante que en cada host de la red local se configure la dirección de gateway predeterminado. Si no se define ninguna dirección de gateway predeterminado en la configuración de TCP/IP del host, o si se especifica un gateway predeterminado incorrecto, no se podrán entregar los mensajes dirigidos a hosts de redes remotas.

Routing Estático

Las rutas estáticas se configuran de forma manual. Estas definen una ruta explícita entre dos dispositivos de red. Las rutas estáticas no se actualizan automáticamente y se deben reconfigurar de forma manual si se modifica la topología de la red. Los beneficios de utilizar rutas estáticas incluyen la mejora de la seguridad y la eficacia de los recursos. Las rutas estáticas consumen menos ancho de banda que los protocolos de routing dinámico, y no se usa ningún ciclo de CPU para calcular y comunicar las rutas.

Existen dos tipos de rutas estáticas comunes:

- **Ruta estática a una red específica:** Se configuran para llegar a una red remota específica.

- **Ruta estática predeterminada:** Especifican el punto de salida que se debe utilizar cuando la tabla de routing no contiene una ruta para la red de destino.

Routing Dinámico

Los routers usan protocolos de enrutamiento dinámico para compartir información sobre el estado y la posibilidad de conexión de redes remotas. Los protocolos de routing dinámico realizan diversas actividades, como la detección de redes y el mantenimiento de las tablas de routing.

El descubrimiento de redes es la capacidad de un protocolo de enrutamiento de compartir información sobre las redes que conoce con otros routers que también están usando el mismo protocolo de enrutamiento. Los protocolos de routing dinámico permiten que los routers descubran las redes de forma automática a través de otros routers. Estas redes y la mejor ruta hacia cada una se agregan a la tabla de routing del router y se identifican como redes descubiertas por un protocolo de routing dinámico específico.

Los routers que usan protocolos de enrutamiento dinámico comparten automáticamente la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin que sea necesaria la participación del administrador de la red.

Ejemplos de protocolos de routing dinámico IPv4:

- **EIGRP:** Protocolo de Routing de Gateway Interior Mejorado

- **OSPF:** Open Shortest Path First

- **IS-IS:** Intermediate System-to-Intermediate System

- **RIP:** Protocolo de Información de Routing

BGP (Border Gateway Protocol)

BGP es el protocolo de encaminamiento EGP más utilizado en Internet. La versión 1 de este protocolo (RFC 1105) apareció en 1989 para sustituir a EGP. Posteriormente, salieron nuevas versiones como la versión 2 en 1990 (RFC 1163) y la versión 3 en 1991 (RFC 1267). Finalmente apareció la versión 4 (RFC 1771 y RFC 4271) que proporciona soporte para CIDR (Classless Interdomain Routing).

BGP es un protocolo que funciona sobre TCP por el puerto 179. BGP permite el encaminamiento de los paquetes IP que se intercambian entre los distintos AS (Autonomous System). Para ello, es necesario el intercambio de prefijos de rutas entre los diferentes AS de forma dinámica, lo cual se lleva a cabo mediante el establecimiento de sesiones BGP inter-AS sobre conexiones TCP. Este tipo de operación proporciona comunicación fiable y esconde todos los detalles de la red por la que se pasa.

Debido a que en cada AS se utiliza un protocolo IGP con una definición distinta para el coste de los enlaces, es imposible encontrar el camino más corto hacia cada destino. Por ello, una vez se han aplicado las restricciones sobre las rutas, BGP utiliza un algoritmo similar al tipo vector de distancia, llamado path-vector, para seleccionar aquellas rutas que impliquen el mínimo número de AS a atravesar.

Las tablas de encaminamiento de BGP almacenan rutas para alcanzar redes (indicadas mediante prefijos). Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado. El último número de AS de la ruta se corresponde con la organización que tiene registrado el prefijo, es decir, el AS donde se encuentra el destino. El principal motivo para almacenar la ruta completa es la detección y eliminación de bucles (loops) para evitar que los paquetes se envíen de forma infinita pasando varias veces por un mismo AS.

Sesiones BGP

En una sesión BGP participan sólo dos routers (peers). En cualquier momento una red puede tener muchas sesiones BGP concurrentes y también un mismo router puede participar en muchas sesiones BGP. En la sesión BGP se lleva a cabo el proceso denominado “peering”, que consiste en que un AS informa a otro sobre las redes que puede alcanzar a partir de éste.

Funcionamiento del proceso BGP

Cuando un router anuncia un prefijo a uno de sus vecinos BGP, esa información es considerada válida hasta que el primer router explícitamente anuncia que la información ya no es válida o hasta que la sesión BGP se pierde. Esto significa que BGP no requiere que la información de routing se refresque periódicamente.

De este modo, en un principio existirá un alto flujo de mensajes cuando se establece la sesión BGP, pero transcurrido un tiempo de estabilización los routers sólo necesitarán informar de los cambios que han ocurrido.

El proceso BGP consiste en 6 estados:

- **Estado libre.**
- **En conexión:** Uno de los extremos intenta una conexión TCP.
- **Activo:** Cuando uno de los extremos no puede establecer conexión y lo reintenta periódicamente.
- **OpenSent:** Un extremo envía un mensaje de identificación.
- **OpenConfirm:** Se recibe respuesta al mensaje de identificación.
- **Established:** Se aceptan las identificaciones. De aquí en adelante, la sesión se considera completamente activa.

Mensajes BGP

El tamaño de los mensajes puede variar entre 19 y 4096 octetos y éstos pueden enviarse de forma segura mediante la función de hash MD5.

Existen 4 tipos de mensajes:

- **OPEN:** Este mensaje es el primero que se envía tras el establecimiento de la conexión TCP. Su función es la de informar a los vecinos sobre la versión del protocolo BGP utilizado, el número de AS y el número identificador del proceso BGP. Además, este mensaje incluye un valor de tiempo durante el cual se va a mantener la sesión (90 segundos normalmente). Si se indica el valor 0 significa que la sesión no va a tener límite de duración. Una vez que se envía este mensaje, el proceso BGP se queda en espera de recibir un mensaje KEEPALIVE.
- **KEEPALIVE:** Este mensaje sirve como confirmación a un mensaje OPEN. Si el tiempo que se estableció para la duración de la sesión es limitado, es necesario que los procesos BGP envíen este mensaje cada cierto tiempo (30 segundos normalmente) para indicar que se mantiene la sesión. De este modo, en el caso de que no haya modificación de la tabla de ruteo, los routers BGP sólo intercambian este tipo de mensaje de forma periódica, lo cual genera un tráfico de unos 5bits/s en el nivel BGP.

- **NOTIFICATION:** Este mensaje sirve para cerrar la sesión BGP, cerrando también la conexión TCP. Además, se envía un código para indicar si hubo errores, como por ejemplo la recepción de un mensaje incorrecto, un problema del proceso BGP o la ausencia de mensajes KEEPALIVE durante 90 segundos (hello time). La consecuencia del cierre de la sesión BGP es la anulación de todas las rutas aprendidas en dicha sesión.

- **UPDATE:** Este mensaje sirve para intercambiar las informaciones de enrutamiento como las rutas a eliminar, el conjunto de atributos de cada ruta, las informaciones sobre los prefijos de redes accesibles (red y longitud de la máscara) y la longitud de cada ruta. Este mensaje se envía sólo cuando existe algún cambio y su recepción produce la activación del proceso BGP, que se encargará entonces de realizar las modificaciones y de emitir a su vez un mensaje UPDATE hacia los otros vecinos.

Atributos BGP

Dentro del mensaje UPDATE se distinguen una serie de atributos que indican una serie de informaciones adicionales asociadas al prefijo de la ruta. Estos atributos se codifican en forma de tripleta con los campos TIPO, LONGITUD y VALOR y son utilizados principalmente para elegir la mejor ruta hacia un destino y también para aplicar reglas de filtrado a los mensajes BGP recibidos y anunciados

Los atributos son los siguientes:

- **ORIGIN:** Indica la forma por la que se ha aprendido la ruta: i si la ruta ha sido aprendida por un protocolo IGP (ruta interior al AS del router origen que se ha configurado con comando **network** o **redistribute**), e si se ha aprendido por EGP (ruta exterior al AS), o **?** (INCOMPLETE) en el caso de que el origen sea desconocido o que se haya aprendido de una forma distinta (normalmente por redistribución en BGP de una ruta estática). La función de este atributo es también la selección de rutas, dando prioridad según los valores en el siguiente orden: IGP < EGP <INCOMPLETE.

- **AS-PATH:** Cada AS añade su número ASN en este atributo para cada una de las rutas que aprende antes de reenviarlas. Así, este atributo contiene una lista con los números de los AS que el anuncio de ruta ha atravesado para llegar al destino. Otra función de este atributo, además de indicar el camino de los AS a seguir para llegar al destino (algoritmo **Path Vector**), es también servir para la detección de bucles (un AS ignora un anuncio de ruta si éste ya contiene su propio ASN) y para el filtrado de rutas según las políticas de encaminamiento.

- **NEXT-HOP:** Cuando un nodo BGP anuncia un prefijo a otro nodo BGP indica en este atributo la dirección del nodo siguiente para llegar al destino. Este atributo es útil en el caso de que el siguiente nodo no utilice BGP. Así, en el caso de que un nodo BGP A anuncie a otro nodo BGP B una ruta cuyo nodo siguiente es C, si B recibe un paquete cuyo destino es la ruta aprendida, B lo envía directamente a C.

- **COMMUNITY:** Este atributo opcional permite agrupar los destinos en comunidades de destino (grupos de routers con unas mismas propiedades) para ayudar a escalar la aplicación de decisiones de enrutamiento (aceptar una ruta, preferir una ruta ante otra, redistribuir una ruta, etc). Cada destino puede ser miembro de varias comunidades.

ICMP (Protocolo de Mensajes de Control de Internet)

Es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Se usa para enviar mensajes de error, indicando por ejemplo que un router o host no puede ser localizado. También puede ser utilizado para transmitir mensajes ICMP Query.

Las herramientas **ping** y **traceroute** envían mensajes de petición **Echo ICMP** y reciben mensajes de respuesta **Echo** para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

Los mensajes de este protocolo se utilizan con fines de diagnóstico o control y se generan en respuesta a los errores en operaciones IP, estos errores del protocolo ICMP se dirigen a la dirección IP del paquete originario.

Ping

Es una utilidad de prueba que utiliza mensajes de solicitud y de respuesta de eco de ICMP para probar la conectividad entre hosts. Ping funciona tanto con IPv4 y con hosts IPv6.

Para probar la conectividad a otro host en una red, se envía una solicitud de eco a la dirección de host mediante el comando ping. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, ping proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Esta puede ser una medida del rendimiento de la red.

Ping posee un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, ping proporciona un mensaje que indica que no se recibió una respuesta. Generalmente, esto indica que existe un problema, pero también podría indicar que se habilitaron características de seguridad que bloquean mensajes ping en la red.

Una vez que se envían todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

Traceroute

Traceroute (tracert) es una utilidad que genera una lista de saltos que se alcanzaron correctamente a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la resolución de problemas.

Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

El uso de Traceroute proporciona el Tiempo de ida y vuelta (RTT) para cada salto a lo largo de la ruta e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta es el tiempo que le lleva a un paquete llegar al host remoto y el tiempo que la respuesta del host demora en regresar. Se utiliza un asterisco (*) para indicar un paquete perdido o sin respuesta.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

Traceroute utiliza una función del campo Tiempo de Vida (TTL) en IPv4. La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este router luego responde con un mensaje de ICMPv4. Traceroute ahora posee la dirección del primer salto.

A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes expiran el límite de tiempo a lo largo del camino. El campo TTL continúa aumentando hasta que se llega a destino o hasta un máximo predefinido.

Una vez que se llega al destino final, el host responde con un mensaje de puerto inalcanzable de ICMP o un mensaje de respuesta de eco de ICMP, en lugar de hacerlo con un mensaje de tiempo superado de ICMP.

Arquitectura Cliente/Servidor

Cliente: Los clientes son computadoras host que tienen instalado un software que les permite solicitar información al servidor y mostrar la información obtenida. Un explorador Web, como Internet Explorer, es un ejemplo de software cliente.

Servidor: Los servidores son hosts con software instalado que les permite proporcionar información, por ejemplo, correo electrónico o páginas Web, a otros hosts de la red. Cada servicio requiere un software de servidor diferente. Por ejemplo, para proporcionar servicios Web a la red, un host necesita un software de servidor Web.

Socket: La combinación del número de puerto de la capa de transporte y de la dirección IP de la capa de red del host identifica de manera exclusiva un proceso de aplicación en particular que se ejecuta en un dispositivo host individual. Esta combinación se denomina socket. Un par de sockets, que consiste en las direcciones IP de origen y destino y los números de puertos, también es exclusivo e identifica la conversación específica entre los dos hosts.

Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: 192.168.1.5:1099

El socket en un servidor Web podría ser el siguiente: 192.168.1.7:80

Protocolos de Administración Remota

Telnet (Telecommunication Network): Es un método para establecer una sesión de CLI de un dispositivo en forma remota, mediante una interfaz virtual, a través de una red. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de redes activos en el dispositivo. El dispositivo de red debe tener, por lo menos, una interfaz activa configurada con una dirección de Internet, por ejemplo, una dirección IPv4. Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como texto plano (cadenas de texto sin cifrar).

SSH (Secure Shell): El protocolo de Shell seguro (SSH) proporciona un inicio de sesión remoto similar al de Telnet, excepto que utiliza servicios de red más seguros. El SSH proporciona autenticación de contraseña más potente que Telnet y usa encriptación cuando transporta datos de la sesión. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.

2.3 Conceptos generales de Seguridad Informática

Seguridad de la Información

Se refiere a los procesos y metodologías que son diseñadas e implementadas para proteger la información, impresa, electrónica o cualquier otro tipo de datos o información confidencial, privada y sensitiva de accesos no autorizados, uso, mal uso, divulgación, destrucción, modificación o intercepción.

Seguridad Informática

Subconjunto de la Seguridad de la Información encargada de la parte técnica. Protege los recursos de una organización como su información, hardware y software mediante la selección apropiada y aplicación de controles.

Objetivos de la Seguridad Informática

Disponiblidad: Significa proporcionar acceso oportuno y fiable a los datos y recursos a los individuos autorizados. Se proporciona la disponibilidad de los recursos implementado técnicas como Clustering, Balanceo de cargas y Respaldos.

Integridad: Exactitud y fiabilidad. Se proporciona integridad mediante Hashing, Control de Acceso y Control de Cambios.

Confidencialidad: Un sistema posee la propiedad de confidencialidad si los recursos manipulados por éste no son puestos al descubierto para usuarios, entidades o procesos no autorizados. La confidencialidad puede ser proporcionado por el cifrado de datos, ya que se almacena y se transmite cumpliendo un estricto control de acceso y clasificación de los datos.

Firewalls

El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios internos de la red contra amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas, además de evitar el acceso no autorizado. Los productos de firewall usan diferentes técnicas para determinar qué acceso permitir y qué acceso denegar en una red. Estas técnicas son las siguientes:

- **Filtrado de paquetes:** Evita o permite el acceso según las direcciones IP o MAC.
- **Filtrado de aplicaciones:** Evita o permite el acceso de tipos específicos de aplicaciones según los números de puerto.
- **Filtrado de URL:** Evita o permite el acceso a sitios Web según palabras clave o URL específicos.
- **Inspección de paquetes con estado (SPI):** Los paquetes entrantes deben constituir respuestas legítimas a solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques por denegación de servicio (DoS).

Además, los firewalls suelen llevar a cabo la traducción de direcciones de red (NAT). La NAT traduce una dirección o un grupo de direcciones IP internas a una dirección IP pública y externa que se envía a través de la red. Esto permite ocultar las direcciones IP internas de los usuarios externos.

Los productos de firewall vienen en distintos formatos:

- **Firewalls basados en aplicaciones:** Un firewall basado en una aplicación es un firewall incorporado en un dispositivo de hardware dedicado, conocido como una aplicación de seguridad.
- **Firewalls basados en servidor:** Un firewall basado en servidor consta de una aplicación de firewall que se ejecuta en un sistema operativo de red (NOS), como UNIX o Windows.
- **Firewalls integrados:** Un firewall integrado se implementa mediante la adición de funcionalidades de firewall a un dispositivo existente, como un router.
- **Firewalls personales:** Los firewalls personales residen en las computadoras host y no están diseñados para implementaciones LAN. Pueden estar disponibles de manera predeterminada en el OS o pueden provenir de un proveedor externo.

CAPÍTULO 3: ACTIVIDADES DE INDUCCIÓN AL PUESTO

3.1 Maqueta de esquema de configuración entre equipos de la red

En este capítulo se presenta las actividades de inducción que son asignadas al analista de O&M Wan, Core y Edge con el fin de que el empleado conozca y configure algunos esquemas de conectividad que tienen los servicios de la empresa así como para fomentar la práctica de los conocimientos de redes de datos como lo son los tipos de protocolos de enrutamiento dinámico y el concepto de alta disponibilidad implementando redundancia para los servicios, esto último indispensable para ofrecer una alta confiabilidad de la red para el caso de servicios críticos.

El esquema de conectividad que se solicita que el empleado nuevo en el área configure es el siguiente:

- Conectividad BGP con redundancia

Las maquetas fueron realizadas en el emulador de red GNS3 utilizando el software Cisco IOS Version 12.4(17a) perteneciente a un router Cisco 7206VXR, capaz de soportar BGP.

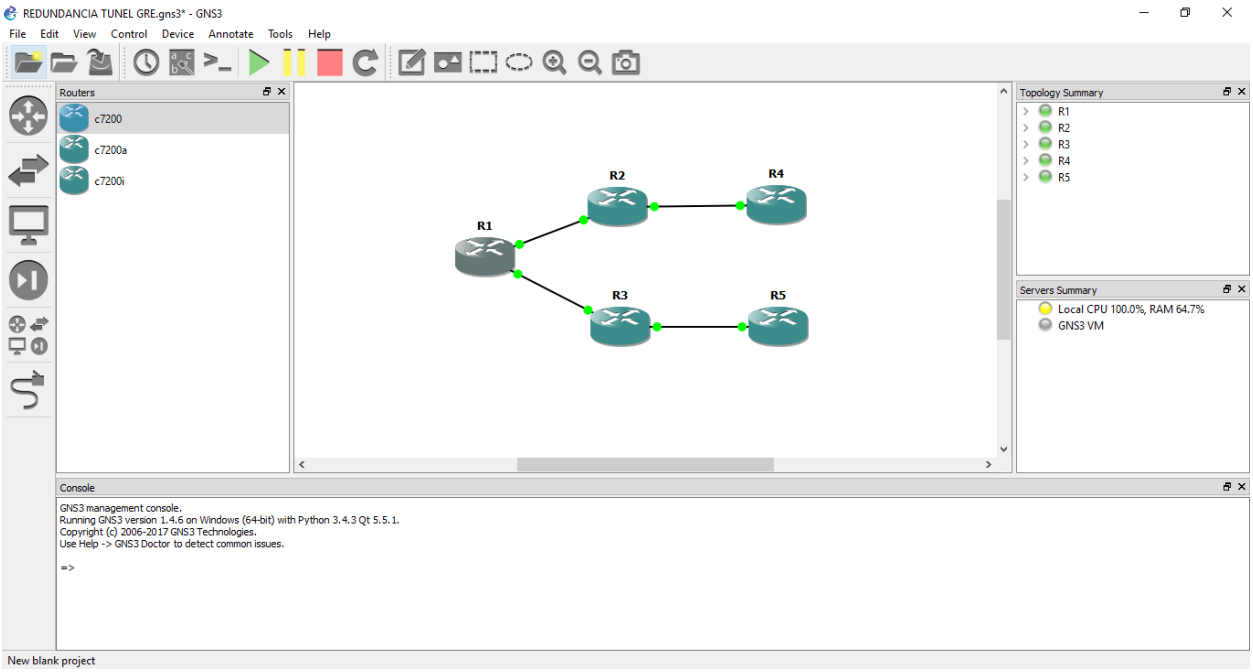


Figura 3.1 Emulador de red GNS3

3.2 Conectividad BGP con redundancia

Este esquema de conectividad consiste en configurar el protocolo de enrutamiento dinámico BGP entre los routers de la empresa y los dos routers del cliente con el fin de establecer la conectividad para el flujo de tráfico del cliente que contrato el servicio además de proporcionar una alta disponibilidad del medio de comunicación para garantizar la conectividad entre la empresa y el cliente aun cuando se presente una falla en algún router del path primario.

A continuación, se presenta el diagrama de configuración y la lista de comandos necesarios para realizar este tipo de conectividad en routers Cisco.

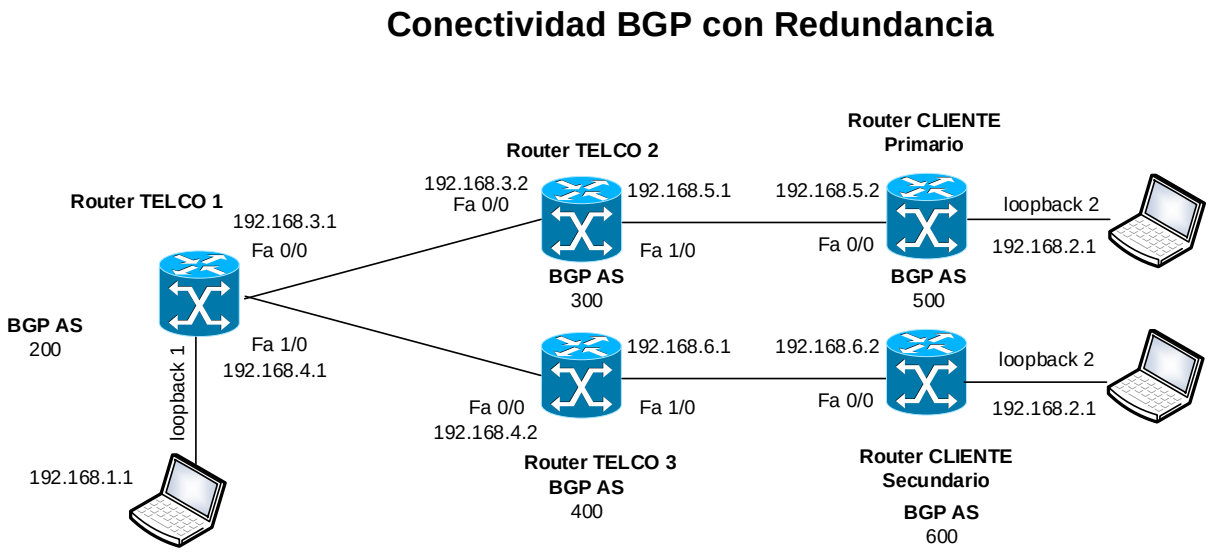


Figura 3.2 Diagrama de Conectividad mediante BGP

3.2.1 Configuración

Router TELCO 1

Interfaz Fa 0/0

```
Router>enable
Router#conf t
Router(config)#int fa0/0
Router(config-if)# ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shut
```

Interfaz Fa 1/0

```
Router(config)#int fa1/0
Router(config-if)# ip address 192.168.4.1 255.255.255.0
Router(config-if)#no shut
```

Loopback 1 Red

```
Router(config)#int loopback 1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
```

Configuración BGP

```
Router(config)#router bgp 200
Router(config-router)#bgp log-neighbor-changes
Router(config-router)#no synchronization
Router(config-router)#neighbor 192.168.3.2 remote-as 300
Router(config-router)#network 192.168.1.0 mask 255.255.255.0
Router(config-router)#neighbor 192.168.4.2 remote-as 400
Router(config-router)#network 192.168.1.0 mask 255.255.255.0
```

Router TELCO 2

Interfaz Fa 0/0

```
Router>enable
Router#conf ter
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#no shut
```

Interfaz Fa 1/0

```
Router(config)#int fa1/0
Router(config-if)#ip address 192.168.5.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
```

Configuración BGP

```
Router(config)#router bgp 300
Router(config-router)#bgp log-neighbor-changes
Router(config-router)#no synchronization
Router(config-router)#neighbor 192.168.3.1 remote-as 200
Router(config-router)#network 192.168.5.0 mask 255.255.255.0
Router(config-router)#neighbor 192.168.5.2 remote-as 500
Router(config-router)#network 192.168.3.0 mask 255.255.255.0
```

Router TELCO 3

Interfaz Fa 0/0

```
Router>enable
Router#conf ter
Router(config)#int fa0/0
Router(config-if)#ip address 192.168.4.2 255.255.255.0
Router(config-if)#no shut
```

Interfaz Fa 1/0

```
Router(config)#int fa1/0
Router(config-if)#ip address 192.168.6.1 255.255.255.0
Router(config-if)#no shut
```

Configuración BGP

```
Router(config)#router bgp 400
Router(config-router)#bgp log-neighbor-changes
Router(config-router)#no synchronization
Router(config-router)#neighbor 192.168.4.1 remote-as 200
Router(config-router)#network 192.168.6.0 mask 255.255.255.0
Router(config-router)#neighbor 192.168.6.2 remote-as 600
Router(config-router)#network 192.168.4.0 mask 255.255.255.0
```

Configuración Route Map AS-PATH

```
Router(config)#route-map PREPEND permit 10
Router(config-route-map)#set as-path prepend 150 150 150
Router(config-route-map)#router bgp 400
Router(config-router)#neighbor 192.168.4.1 route-map PREPEND out
```

Router CLIENTE Primario

Interfaz Fa 0/0

```
Router>enable
Router#conf t
Router(config)#int fa0/0
Router(config-if)# ip address 192.168.5.2 255.255.255.0
Router(config-if)#no shut
```

Loopback 2 Red

```
Router(config)#int loopback 2
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#exit
```

Configuración BGP

```
Router(config)#router bgp 500
Router(config-router)#bgp log-neighbor-changes
Router(config-router)#no synchronization
Router(config-router)#neighbor 192.168.5.1 remote-as 300
Router(config-router)#network 192.168.2.0 mask 255.255.255.0
```

Router CLIENTE Secundario

Interfaz Fa 0/0

```
Router>enable
Router#conf t
Router(config)#int fa0/0
Router(config-if)# ip address 192.168.6.2 255.255.255.0
Router(config-if)#no shut
```

Loopback 2 Red

```
Router(config)#int loopback 2
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#exit
```

Configuración BGP

```
Router(config)#router bgp 600
Router(config-router)#bgp log-neighbor-changes
Router(config-router)#no synchronization
Router(config-router)#neighbor 192.168.6.1 remote-as 400
Router(config-router)#network 192.168.2.0 mask 255.255.255.0
```

3.2.2 Estatus de configuración en routers

Información de Ruteo

Para establecer la conectividad se realiza la configuración de las vecindades de BGP entre los routers de la empresa y los routers del cliente, por lo que es necesario consultar en los equipos la información de ruteo.

Utilizamos el comando **show ip route** para consultar las tablas de ruteo de cada equipo en las cuales podemos encontrar la información de las rutas cargadas en los equipos y el protocolo por el que se conoce la ruta (estático o dinámico).

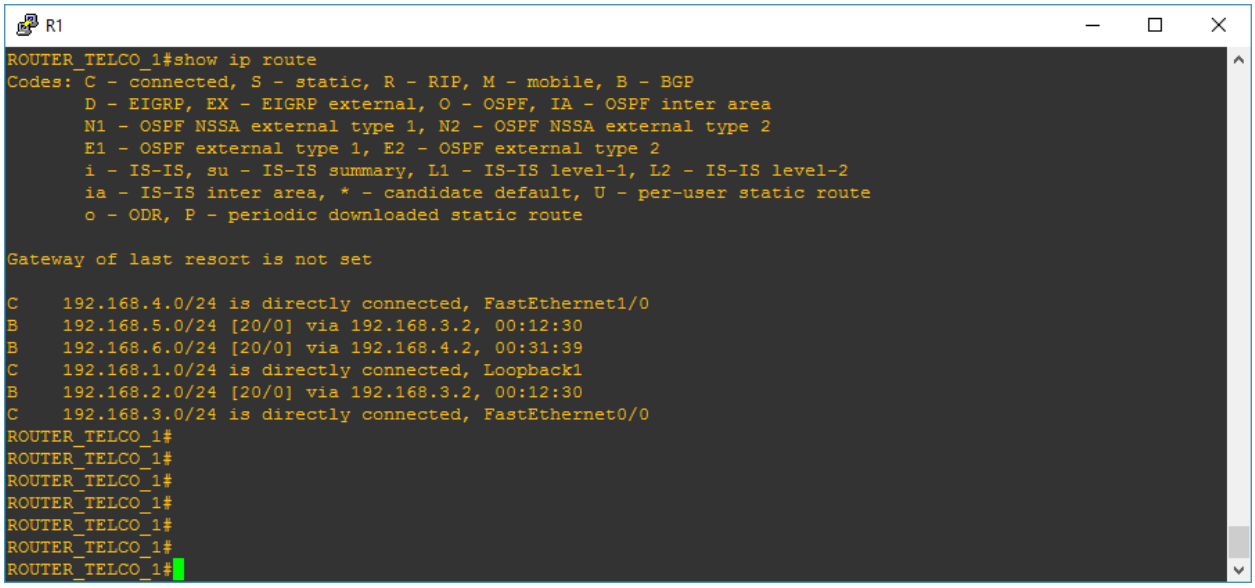


Figura 3.3 Salida del Comando **show ip route** en Router TELCO 1

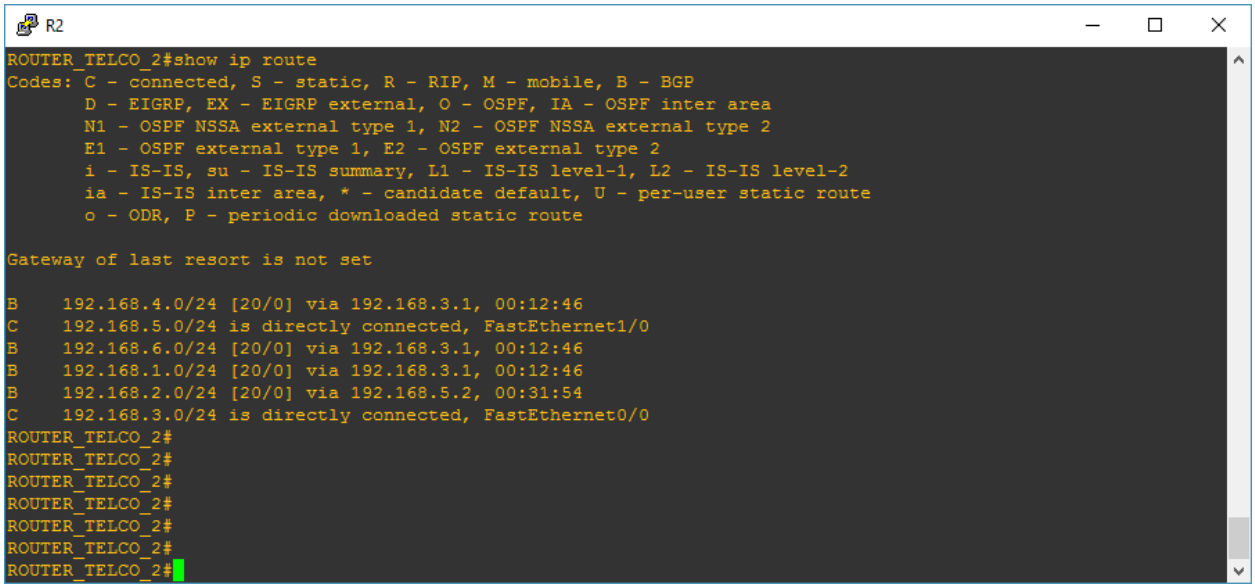


Figura 3.4 Salida del Comando **show ip route** en Router TELCO 2

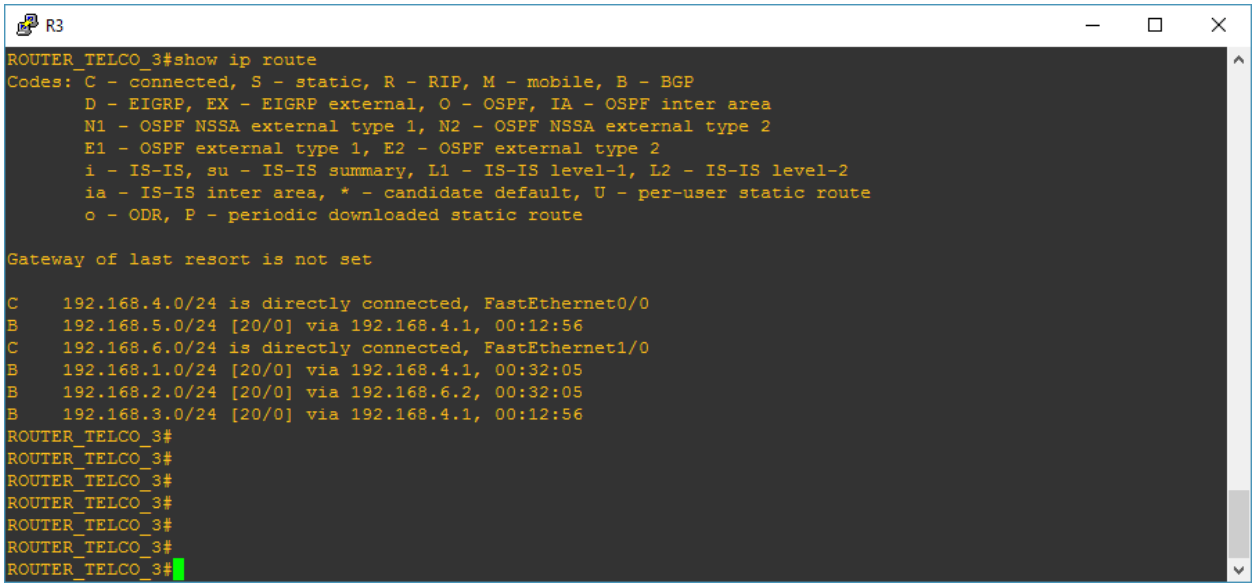


Figura 3.5 Salida del Comando **show ip route** en Router TELCO 3

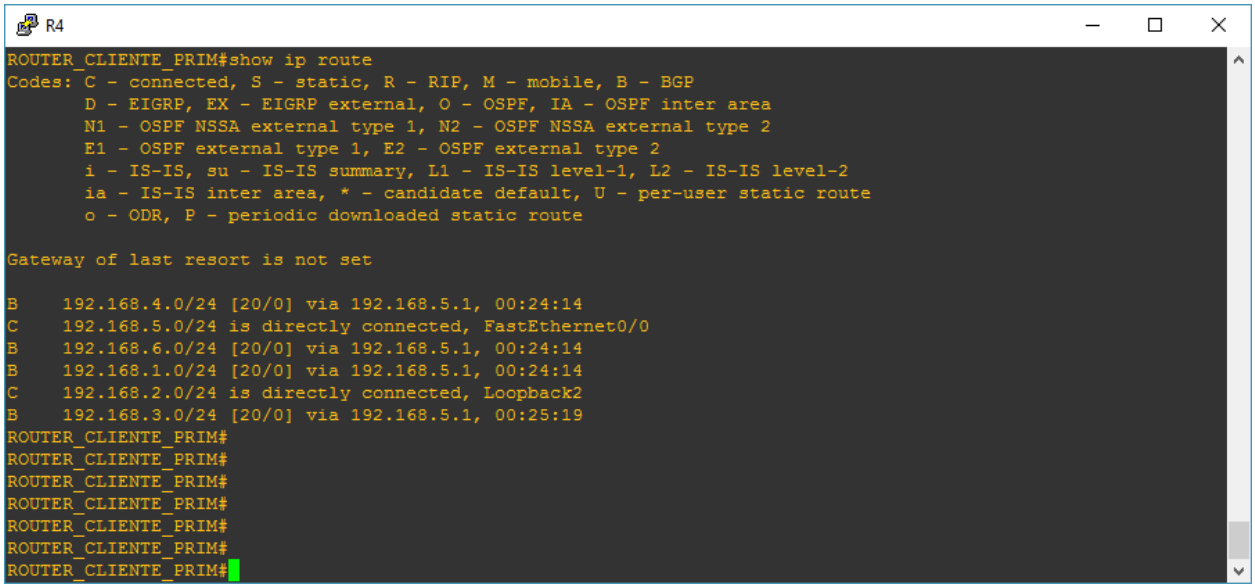


Figura 3.6 Salida del Comando **show ip route** en Router CLIENTE Primario

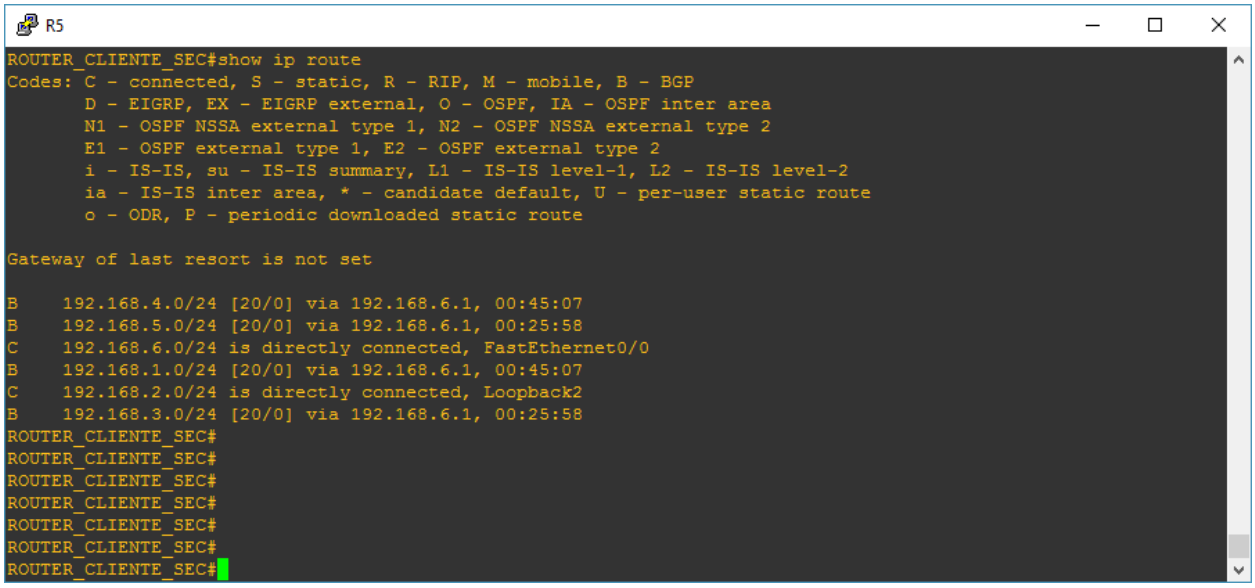


Figura 3.7 Salida del Comando **show ip route** en Router CLIENTE Secundario

Utilizamos el comando **show ip bgp** para conocer la información del protocolo de enrutamiento BGP así como las redes que se conocen mediante este protocolo.

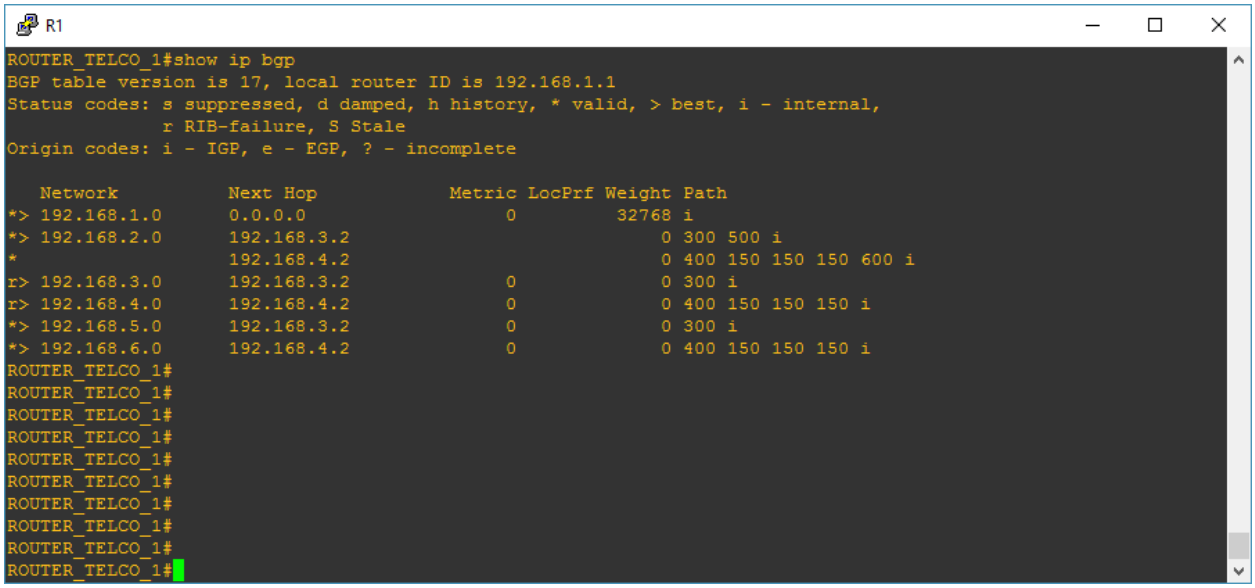


Figura 3.8 Salida del Comando **show ip bgp** en Router TELCO 1

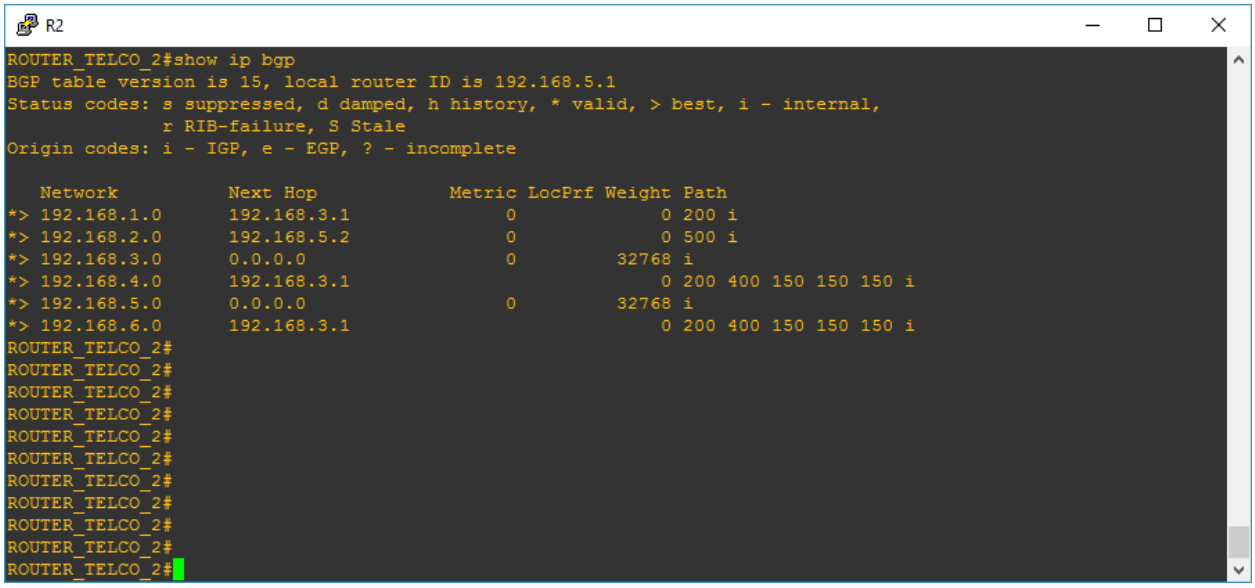


Figura 3.9 Salida del Comando **show ip bgp** en Router TELCO 2

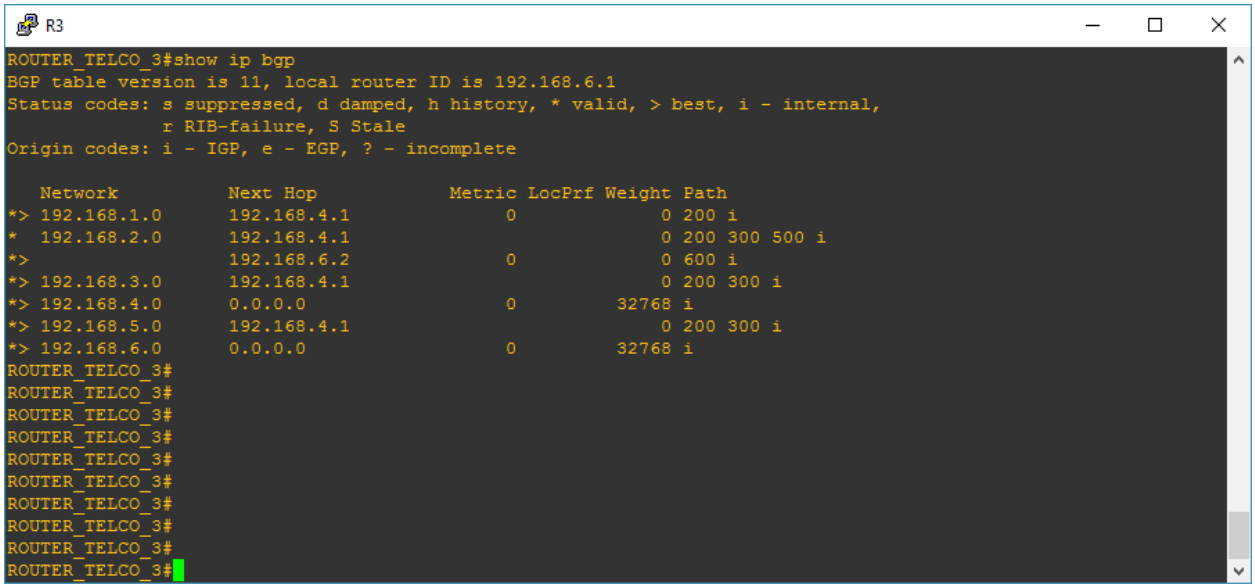


Figura 3.10 Salida del Comando **show ip bgp** en Router TELCO 3

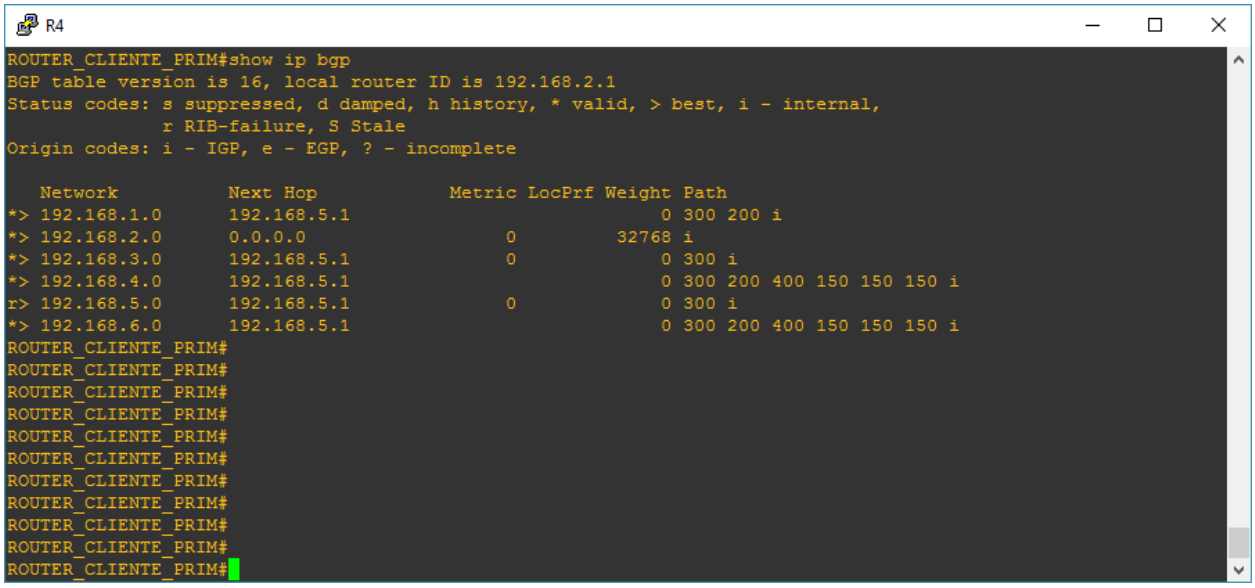


Figura 3.11 Salida del Comando **show ip bgp** en Router CLIENTE Primario

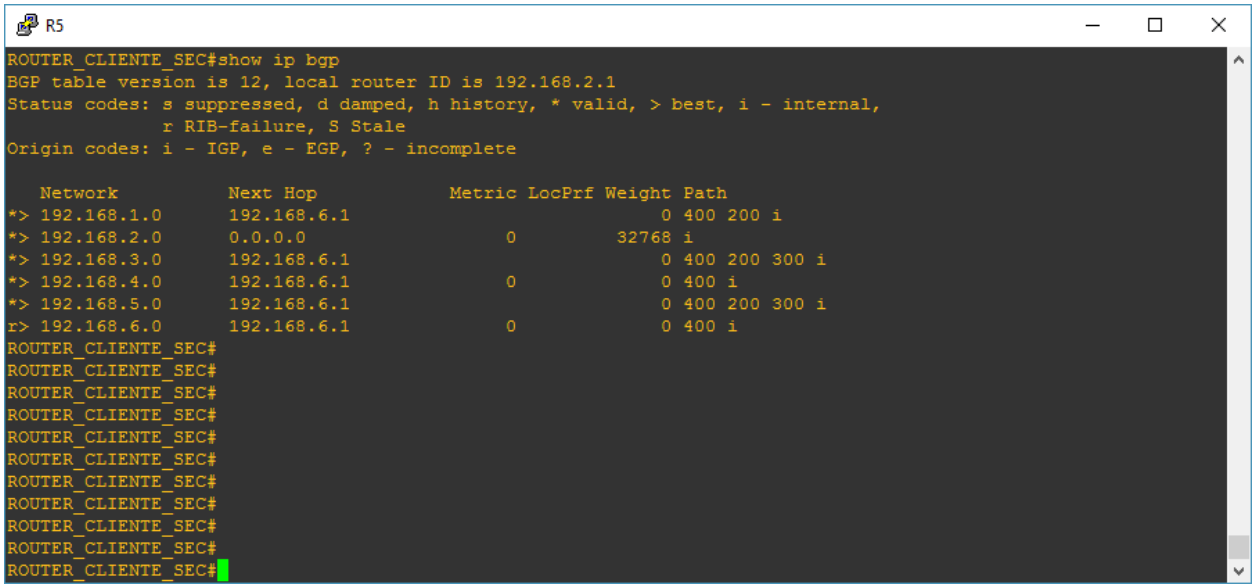


Figura 3.12 Salida del Comando **show ip bgp** en Router CLIENTE Secundario

3.2.3 Pruebas de conectividad y redundancia

Pruebas de Conectividad

Realizamos las pruebas de conectividad entre el **Router TELCO 1** y el **Router CLIENTE Primario** entre los cuales existe configurado el protocolo de enrutamiento dinámico BGP que permite la comunicación entre los hosts **192.168.1.1 (Empresa)** y **192.168.2.1 (Cliente)**.

Las pruebas consisten en probar la conectividad para estos routers utilizando el comando **ping** y **traceroute** que nos ayuda a validar la conexión y el correcto envío de datos entre los dos equipos además de validar el path que utilizan los paquetes para llegar a su destino.

Ejecutamos el comando **ping** en el equipo **Router TELCO 1** para validar que el host de la empresa **192.168.1.1** puede alcanzar al host del **Cliente 192.168.2.1**

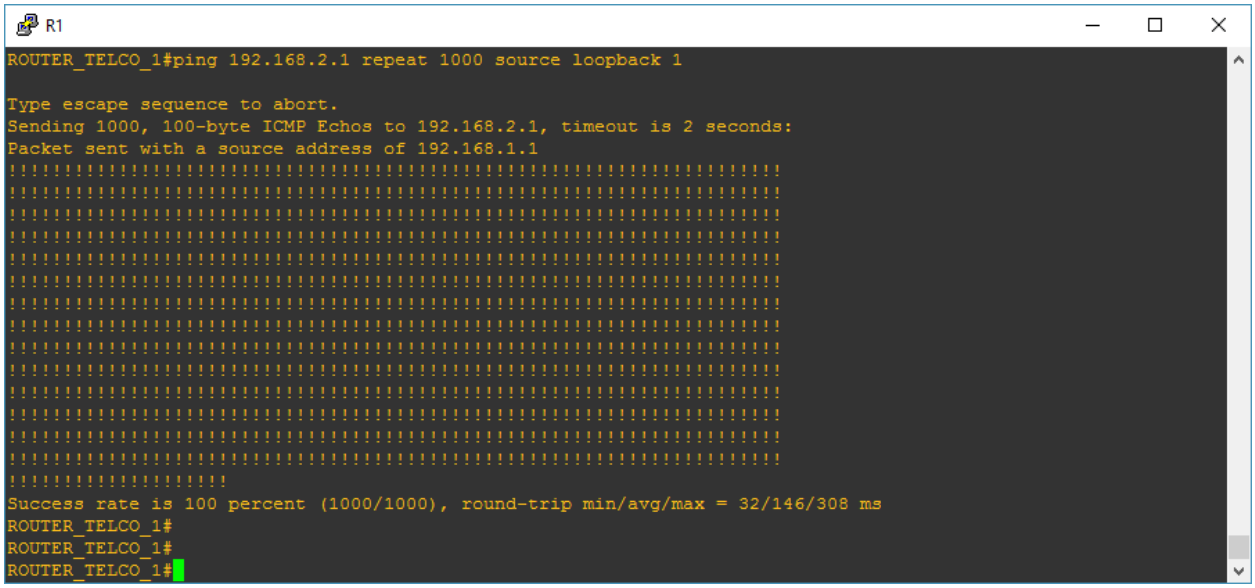


Figura 3.13 Salida del Comando **ping** en Router TELCO 1

Podemos observar que la red de la empresa **192.168.1.1** puede alcanzar la red del cliente **192.168.2.1** ya que se completa a un 100% el envío de paquetes, existiendo una correcta comunicación entre los equipos **Router TELCO 1** y el **Router CLIENTE Primario**.

Realizamos la validación anterior ahora ejecutando el comando **ping** desde el equipo **Router CLIENTE Primario** para validar que la red del **cliente 192.168.2.1** puede alcanzar la red de la **empresa 192.168.1.1**

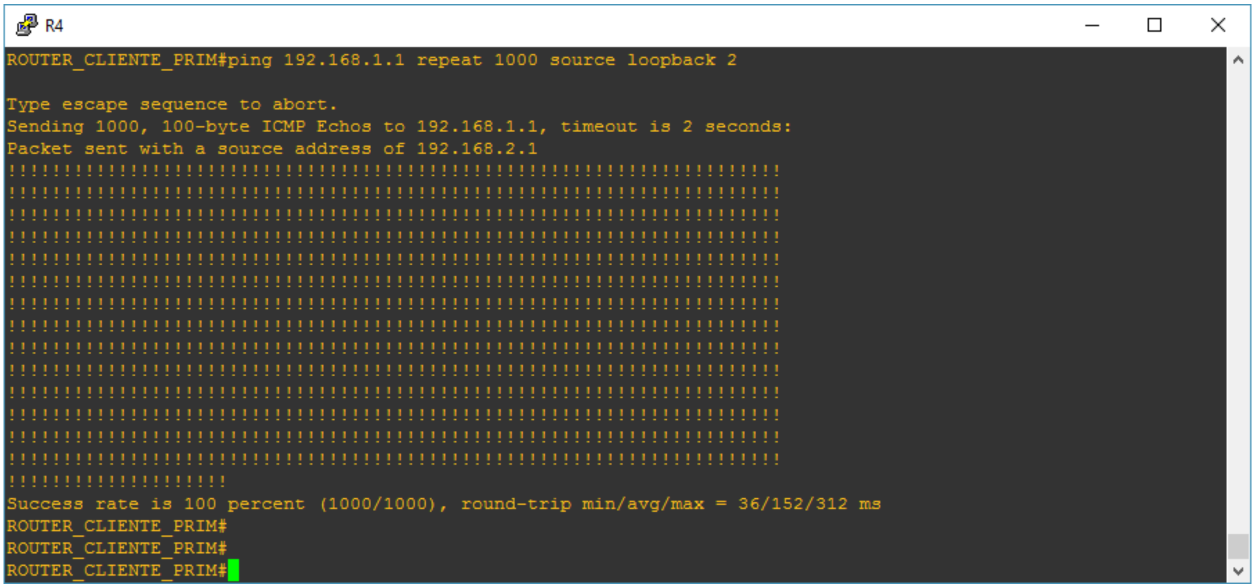


Figura 3.14 Salida del Comando **ping** en Router CLIENTE Primario

De igual manera observamos que la red del **cliente 192.168.2.1** puede alcanzar la red de la **empresa 192.168.1.1** ya que se completa a un 100% el envío de paquetes, existiendo una correcta comunicación entre los equipos **Router CLIENTE Primario** y **Router TELCO 1.**

Una vez que se valida la correcta comunicación entre la red de la empresa y la red del cliente, el siguiente paso es validar que efectivamente el tráfico entre ambas redes sea enrutado a través del path primario definido entre los equipos **Router TELCO 1** y el **Router CLIENTE Primario.** Para lo anterior se ejecutará en ambos equipos el comando **traceroute** para validar el path que utilizan los paquetes para llegar a su destino.

Ejecutamos el comando **traceroute** en el equipo **Router TELCO 1** para revisar el path que se utiliza para llagar a la red del cliente.

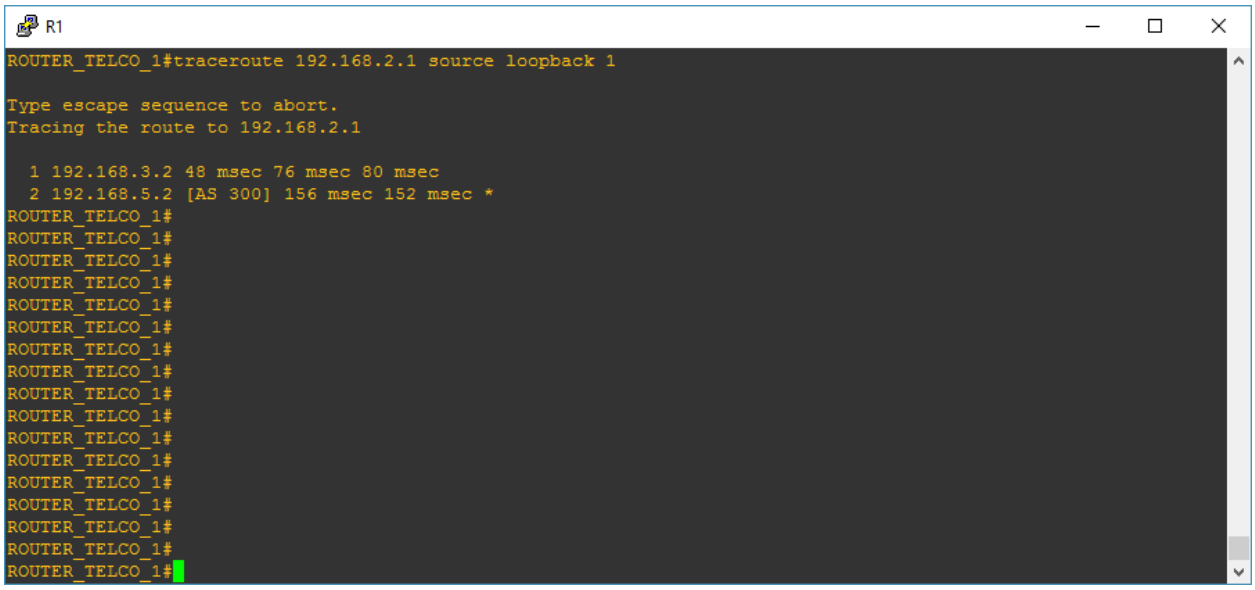


Figura 3.15 Salida del Comando **traceroute** en Router TELCO 1

De la salida del comando anterior podemos observar que se muestra en pantalla los saltos que tienen que dar los paquetes enviados desde la red de la **empresa 192.168.1.1** antes de llegar a su destino que en este caso es la red del **cliente 192.168.2.1**. El comando **traceroute** nos indica únicamente los saltos correspondientes al **Router TELCO 2 (192.168.3.2)** y al **Router CLIENTE Primario (192.168.5.2)**, con lo que confirmamos que el tráfico efectivamente está siendo enrutado sobre el path primario, dejando deshabilitada la ruta a través del **Router TELCO 3**.

Ahora ejecutamos el comando **traceroute** en el equipo **Router CLIENTE Primario** para revisar el path que se utiliza para llagar a la red de la empresa.

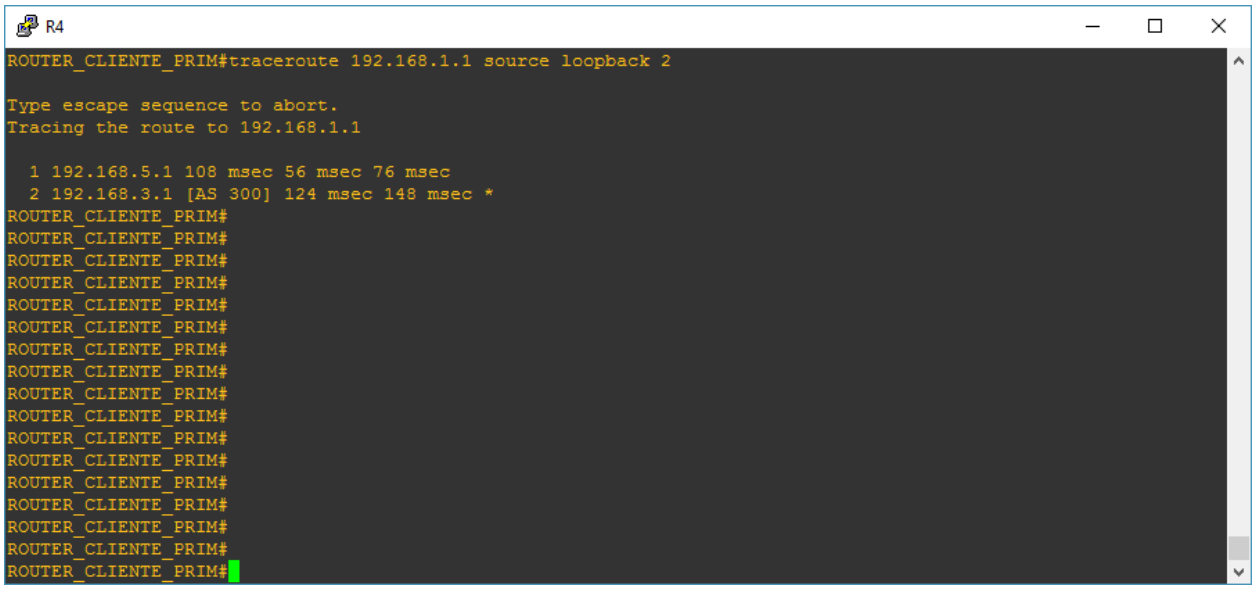


Figura 3.16 Salida del Comando **traceroute** en Router CLIENTE Primario

De igual manera que en el equipo de la empresa podemos observar que se muestra en pantalla los saltos que tienen que dar los paquetes enviados desde la red del **cliente 192.168.2.1** antes de llegar a su destino que en este caso es la red de la **empresa 192.168.1.1.**

El comando **traceroute** nos indica únicamente los saltos correspondientes al **Router TELCO 2 (192.168.5.1)** y al **Router TELCO 1 (192.168.3.1)**

Pruebas de Redundancia

Las pruebas de redundancia del servicio consisten en deshabilitar el path primario, apagando alguna de las interfaces del **Router TELCO 2**, con lo que podemos validar que efectivamente el path secundario se activa y ahora el tráfico viaja por esta segunda ruta. De esta manera estamos comprobando que se tiene un escenario de alta disponibilidad para el servicio del cliente ya que aun cuando se presente alguna falla en la red, el servicio no se verá afectado por dicha contingencia.

Se apagará la interfaz **fa0/0** del **Router TELCO 2** simulando una falla en ese equipo.

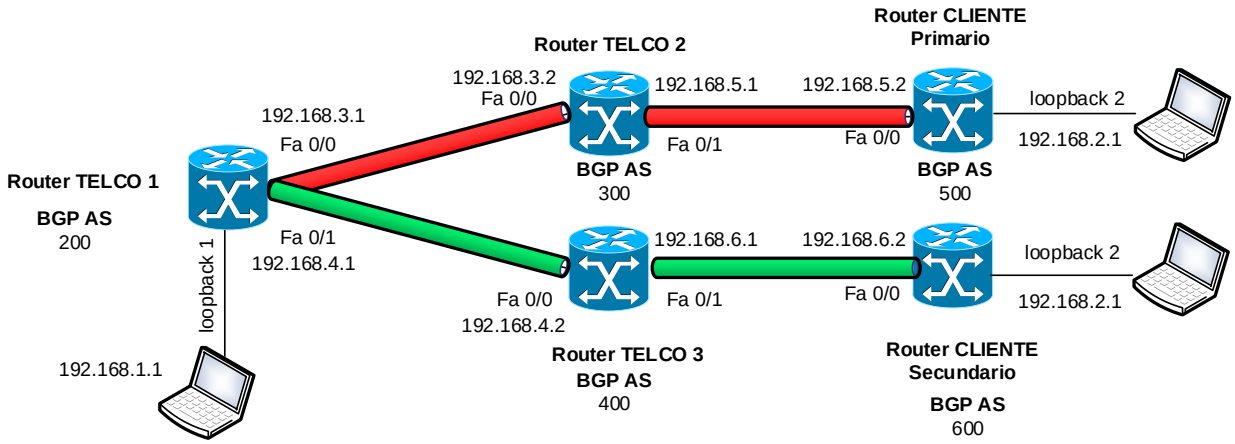


Figura 3.17 Simulación de falla en Router TELCO 2

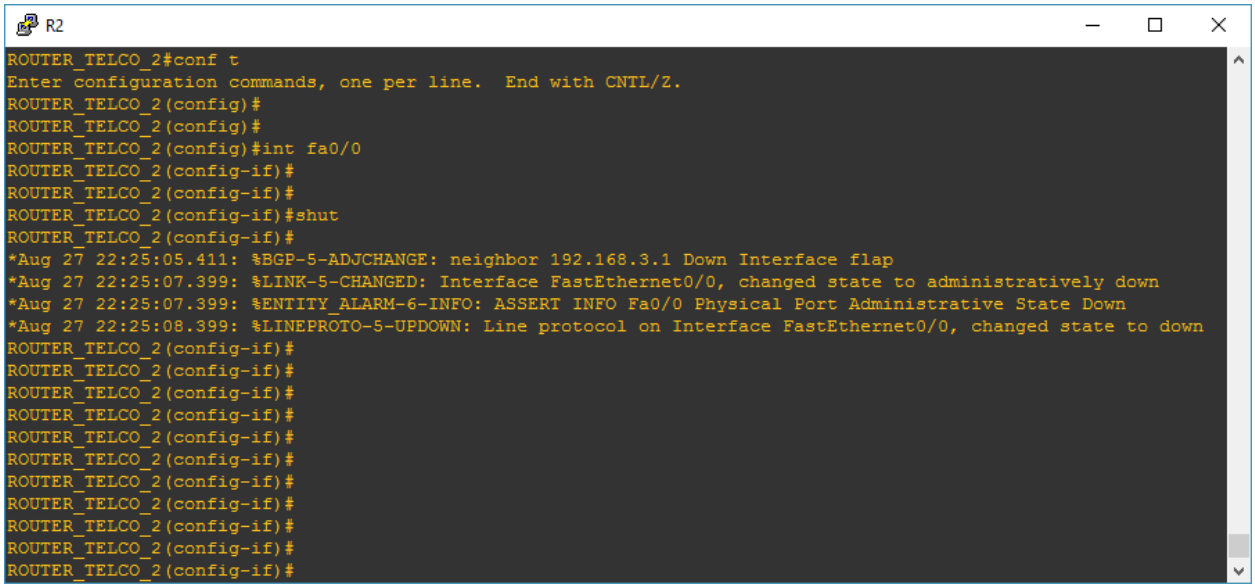


Figura 3.18 Apagado de interfaz fa0/0 en Router TELCO 2

A la salida del comando anterior podemos observar que al realizar el apagado de la interfaz **fa0/0** aparece en la pantalla un mensaje que indica que la interfaz fue apagada y esta administrativamente abajo y la vecindad de BGP que se tiene con el **Router TELCO 1** se encuentra abajo.

Momentos antes de deshabilitar el path primario, se ejecuta en el **Router TELCO 1** el comando **ping extendido** hacia la dirección IP de la red del **cliente 192.168.2.1**, para poder observar lo que sucede cuando el túnel primario se deshabilita.

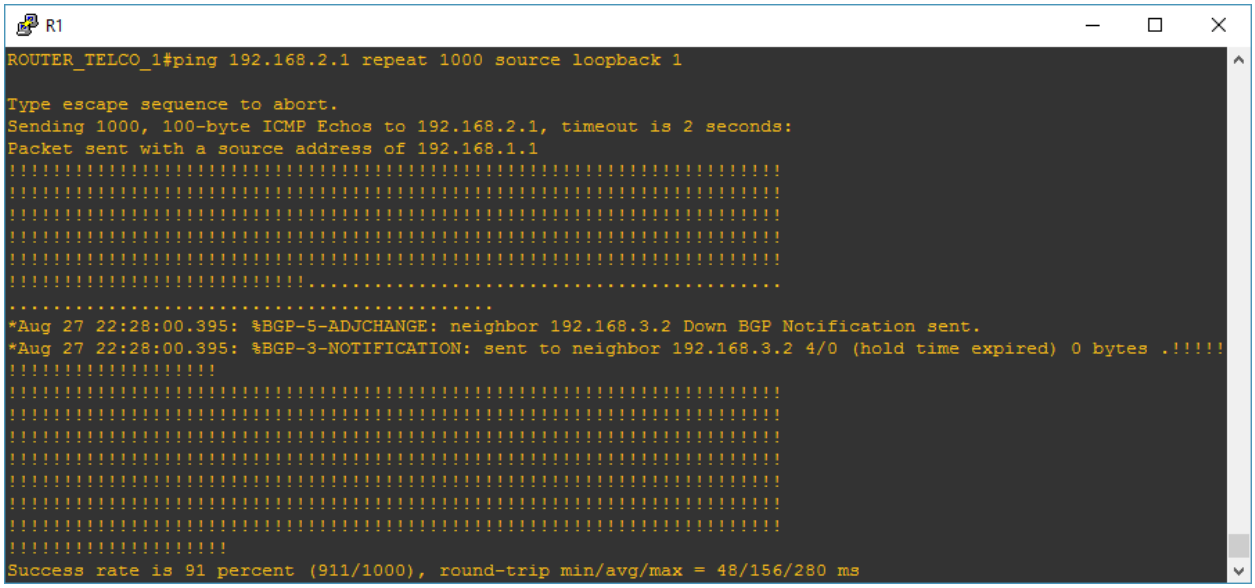


Figura 3.19 Ping Extendido en Router TELCO 1

A la salida del comando anterior podemos observar una pérdida de paquetes que se debe al apagado de la interfaz **fa0/0** en el **Router TELCO 2**, además observamos en pantalla un mensaje que indica que la vecindad con el **Router TELCO 2 (192.168.3.2)** se encuentra abajo. Pero después de un periodo de tiempo observamos que se restablece él envió de paquetes, esto debido a que se activa el path secundario a través del **Router TELCO 3** lo que permitió que el tráfico se conmutara hacia este enlace de respaldo de manera automática. Los contadores finales muestran que efectivamente hubo una pérdida de paquetes, pero gracias a que el segundo path fue configurado se puede ver que se completó él envió del resto de los paquetes permitiendo que el servicio continuara operando de manera normal.

Realizamos una prueba de trazado en el **Router TELCO 1** para comprobar que efectivamente el tráfico hacia el cliente se está enrutando a través de la ruta secundaria.

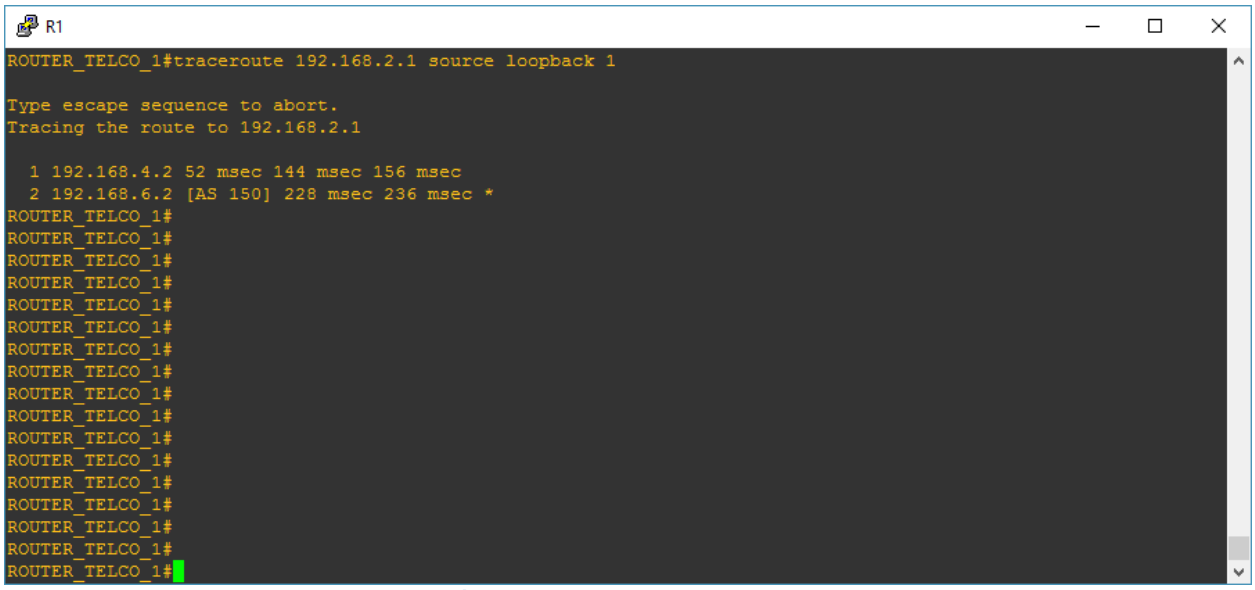


Figura 3.20 Ejecución de comando **traceroute** en Router TELCO 1

De la figura anterior observamos que se está enrutando el tráfico hacia el cliente a través de la ruta secundaria, ya que se observa solo los saltos correspondientes al **Router TELCO 3 (192.168.4.2)** y al **Router CLIENTE Secundario (192.168.6.2)**, con lo que validamos el correcto funcionamiento del esquema de configuración redundante.

Realizamos la ejecución del mismo comando en el **Router CLIENTE Secundario** y observamos que también el equipo del cliente enruta el tráfico hacia la empresa de telecomunicaciones a través del path secundario**.** Se observa que existe el salto del **Router TELCO 3 (192.168.6.1)** y del **Router TELCO 1 (192.168.4.1).**

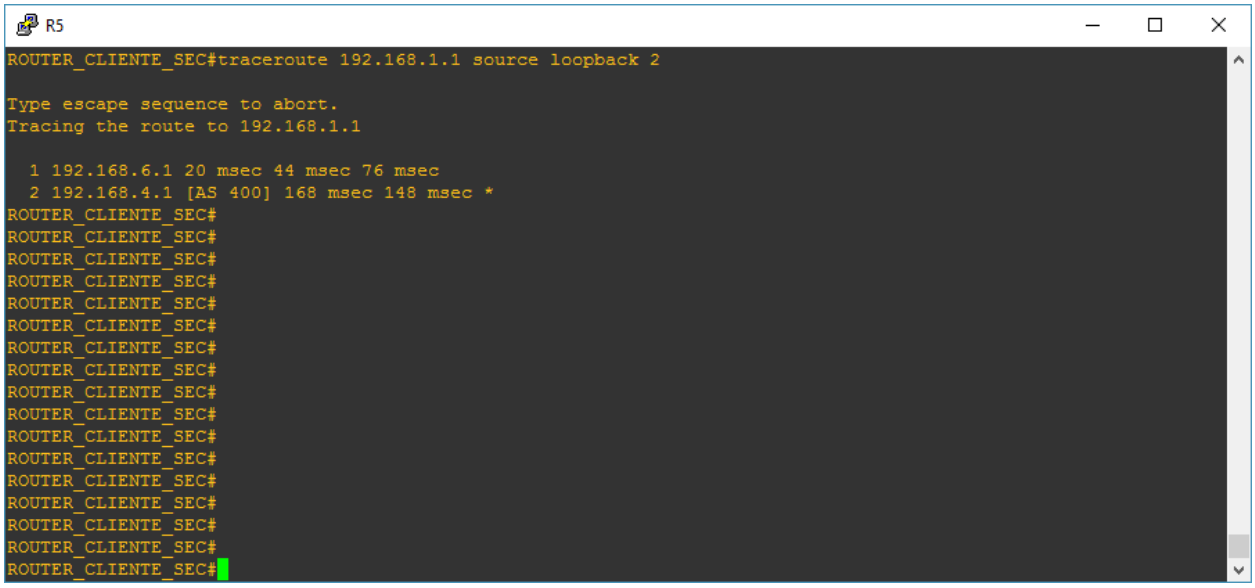


Figura 3.21 Ejecución de comando **traceroute** en Router CLIENTE Secundario

Conclusiones

Con este esquema de configuración en el cual implementamos dos rutas mediante BGP hacia dos diferentes equipos del cliente podemos asegurar una alta disponibilidad del servicio, lo cual nos ayuda a garantizar que las transacciones o envío de información que el cliente necesite realizar a través de nuestra red se realizaran sin ningún problema y en el momento en el que se requiera, sin tener algún impacto en las operaciones de nuestros clientes.

CAPÍTULO 4: CASO DE FALLA EN LA RED

4.1 Introducción

El cliente CJR tiene contratado con nuestra compañía un servicio corporativo que proporciona líneas telefónicas, así como navegación en Internet (Voz y Datos), todo esto mediante activación de tarjetas SIM que pueden ser usadas en diferentes dispositivos dependiendo el uso que el cliente le quiera dar. Existen dos principales usos:

- Llamadas y conexión a internet para dispositivos móviles (Celulares).

- Conexión a internet para envío de datos (Localización vehicular y terminales bancarias).

Como parte del servicio, se proporciona al cliente el detalle de los eventos generados por la línea activada como pueden ser llamadas o navegación en Internet. Se detalla la fecha y el usuario que generó el evento, así como la duración del mismo y datos adicionales como los números a los que se realizaron las llamadas. Lo anterior se realiza mediante un aplicativo alojado en un servidor interno que proporciona archivos llamados CDR con la información de los eventos generados por las líneas contratadas. La importancia de los CDR radica en el hecho de que sirven a nuestro cliente para poder tarificar el consumo de voz y datos de cada una de las líneas contratadas.

Dentro de las asignaciones de nuestra área se encuentra el segmento de la red por el que opera esta parte del servicio. Como administradores de los Routers y Firewalls de este segmento, es nuestro deber asegurar la disponibilidad de la red de transporte validando, modificando y/o agregando las siguientes configuraciones en los equipos:

- Ruteo: Configuración de rutas óptimas para el envío de datos entre cliente y empresa.

- Seguridad: Creación de políticas en FW (Direcciones IP, servicios y puertos).

4.2 Topología del servicio Cliente CJR

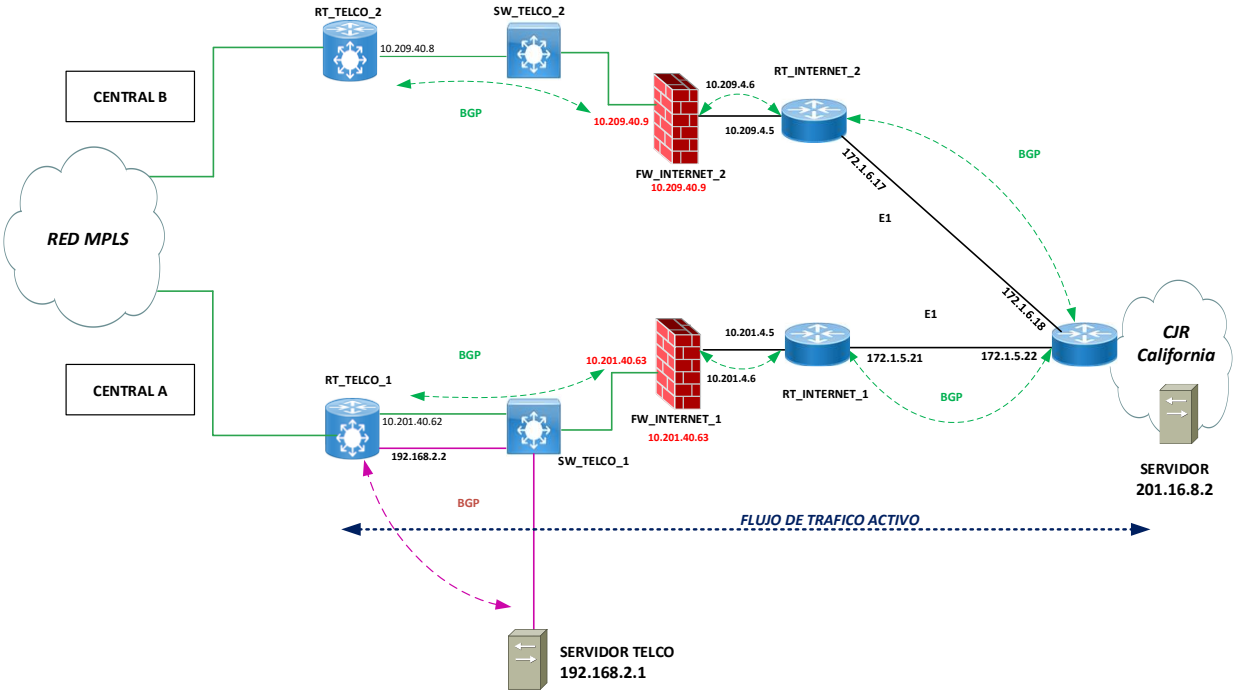


Figura 4.1 Topología Cliente CJR

El servicio del cliente CJR cuenta con un servidor ubicado físicamente en su Data Center de California, este equipo necesita establecer una conexión con el servidor interno TELCO de nuestra compañía para poder recibir los CDR generados por las líneas que tienen arrendadas.

Para esto se tienen dos enlaces dedicados que proporcionan el medio de transporte para el flujo de información entre estos dos servidores, proporcionando una alta redundancia para el servicio en caso de presentarse alguna falla. Del lado del cliente ambos enlaces se conectan a su Router Frontera y del lado de nuestra compañía se distribuyen en dos centrales diferentes, por lo que el enlace primario se conecta al Router RT_INTERNET_1 ubicado físicamente en la Central A y el enlace secundario se conecta al Router RT_INTERNET_2 ubicado en la Central B.

Siguiendo el flujo del tráfico hacia el interior de la red de nuestra compañía, podemos observar que detrás de los Routers de Internet 1 y 2 se encuentran los Firewalls FW_INTERNET_1 y FW_INTERNET_2 ubicados uno en cada Central. Estos equipos proporcionan seguridad al perímetro de la red, con lo que evitamos ataques de cualquier tipo a la red interna. En ambos equipos existen configuradas las políticas de seguridad que permiten la conexión entre las IP del servidor del cliente CJR de California y el servidor Interno TELCO de nuestra compañía, además de que se tienen habilitados los servicios y puertos que se requieren para establecer esta conexión.

Al interior de la red de nuestra compañía contamos con los Switches SW_TELCO_1 y SW_TELCO_2 que proporcionan el acceso a la red Interna y conectados a ellos tenemos los Routers RT_TELCO_1 y RT_TELCO_2 que son dispositivos de distribución que permiten alcanzar los diferentes servicios dentro de la red. Como se puede observar en la topología cada central cuenta con un Switch de acceso y un Router de distribución.

Por último, ambas centrales se interconectan gracias a una red MPLS externa que es la encargada de realizar el ruteo entre ambas centrales y así poder establecer la conectividad de los servicios entre la Central A y la Central B. Debido a lo anterior es posible establecer la comunicación entre el servidor CJR California y el servidor Interno TELCO de nuestra compañía utilizando el path primario y secundario.

4.3 Descripción de la falla del servicio

El cliente CJR reporta un problema de conectividad entre su servidor ubicado en California y el servidor interno TELCO en el cual está alojado el aplicativo que nuestro cliente consulta. Lo anterior provoca la interrupción del envío de los CDR generados por las líneas arrendadas.

El cliente CJR realiza la conmutación de la operación a su enlace secundario de manera automática para tratar de restablecer el servicio. Al tener un segundo enlace de respaldo se activa el path secundario para el flujo de información entre ambos servidores y con esto se logra reestablecer el servicio teniendo activo de nueva cuenta el envío de CDR hacia el cliente.

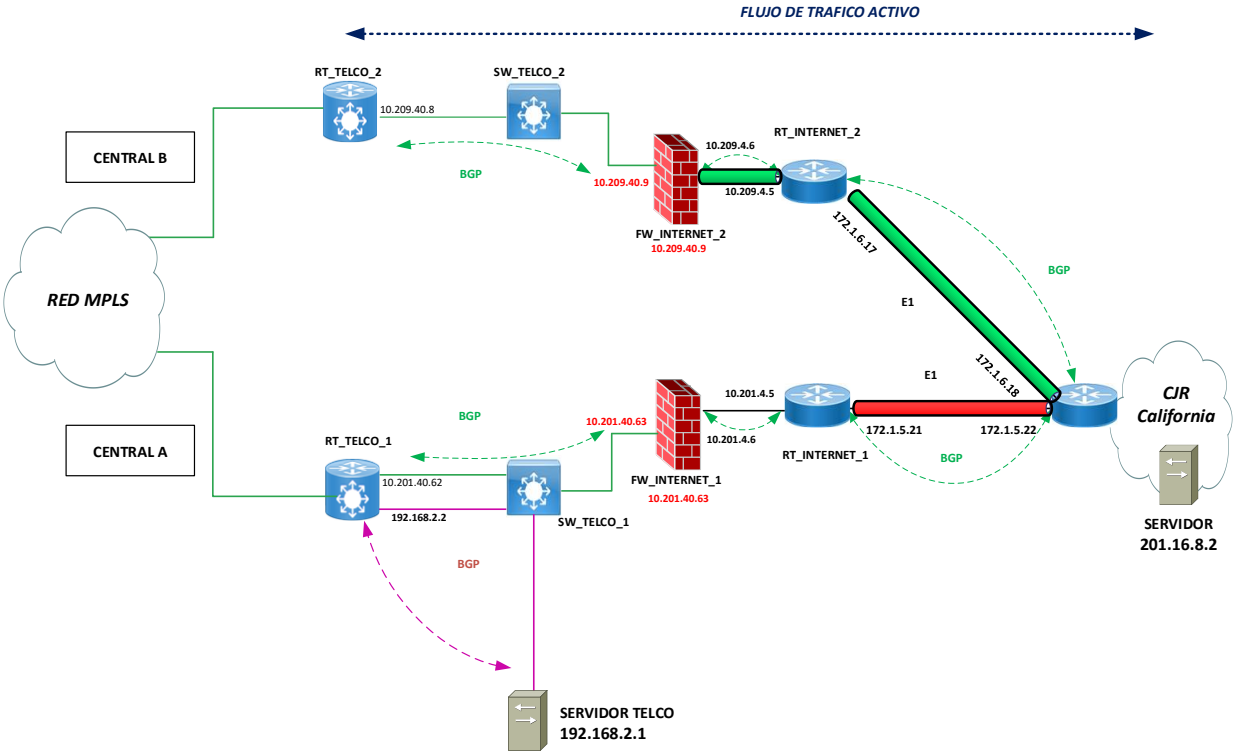


Figura 4.2 Falla del Servicio Cliente CJR

4.4 Troubleshooting

4.4.1 Falla en enlace dedicado

El primer paso dentro del Troubleshooting que se realiza para solucionar el problema de conectividad que presenta el servicio del cliente es la revisión de los enlaces dedicados para detectar alguna posible falla en esta parte de la trayectoria. Se realiza el siguiente procedimiento:

- Se verifica el estado de las interfaces que tienen conectados los enlaces dedicados en los equipos RT_INTERNET_1 y RT_INTERNET_2.

```
RT_INTERNET_1#show interface description | inc CJR
Interface                      Status         Protocol Description
Se1/0/0                        down           down     CONEXION CJR CALIFORNIA
```

```
RT_INTERNET_2#show interface description | inc CJR
Interface                      Status         Protocol Description
Se1/0/0                        up             up       CONEXION CJR CALIFORNIA
```

  De las salidas del comando **show interface description** ejecutado en ambos routers podemos observar que se tiene un problema con el enlace primario que se conecta en el router RT_INTERNET_1. Caso contrario del enlace secundario conectado en el router RT_INTERNET_2, en este equipo el enlace se encuentra operando correctamente y es debido a esto que el cliente pudo reestablecer su servicio.

- Se reporta el enlace caído con el proveedor externo de los enlaces dedicados, a fin de que se realice la corrección del problema.

- El proveedor del enlace dedicado realiza las correcciones necesarias dentro de su red con lo cual se reestablece en enlace principal del cliente.

```
RT_INTERNET_1#show interface description | inc CJR
Interface                      Status         Protocol Description
Se1/0/0                        up             up       CONEXION CJR CALIFORNIA
```

4.4.2 Falla por Ruteo Asimétrico

Una vez que se reestablece el enlace principal que se encontraba caído, se tienen ambos enlaces dedicados arriba, es decir, operando correctamente. Pero con esta corrección se presenta de nueva cuenta el mismo problema de conectividad y se interrumpe el envío de los CDR generados por las líneas arrendadas hacia el servidor ubicado en California.

Debido a lo anterior se decide realizar en los Firewalls un análisis del flujo de tráfico entre el servidor de CJR California y el servidor interno TELCO, esto nos ayudará a identificar algún problema que esté afectando la conectividad.

El análisis de tráfico se realiza utilizando la herramienta SmartView Tracker de nuestros Firewalls.

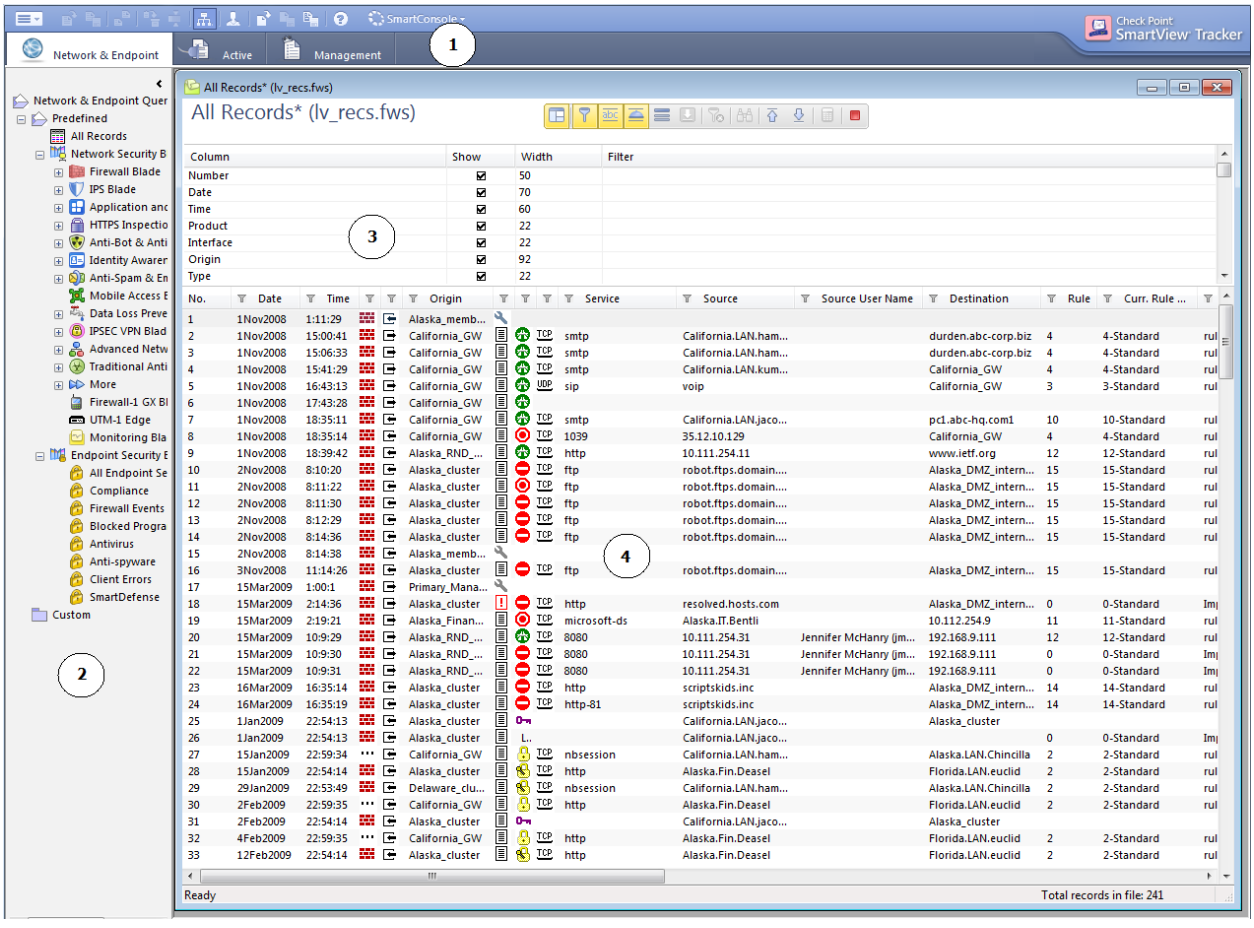


Figura 4.3 Captura de pantalla SmartView Tracker

Se realiza el análisis del flujo de tráfico en el firewall FW_INTERNET_2:

- Editamos el filtro del campo **“Destination”** agregando la IP del servidor interno TELCO (192.168.2.1). Se observa que las peticiones que vienen del servidor CJR California (201.16.8.2) hacia el servidor interno TELCO (192.168.2.1) son aceptadas por el firewall, es decir existe tráfico de entrada hacia la red interna.

- Editamos de nueva cuenta el filtro **“Destination”** agregando la IP del servidor CJR California (201.16.8.2). Se observa que no existe tráfico de respuesta a las peticiones generadas por el servidor CJR desde el servidor interno TELCO por lo que se sospecha que dichas respuestas podrían estarse enviando por el FW_INTERNET_1 generando así un problema de ruteo asimétrico.

Se realiza el análisis del flujo de tráfico en el firewall FW_INTERNET_1:

- Editamos el filtro **“Destination”** agregando la IP del servidor CJR California (201.16.8.2). Se observa que existe tráfico de respuesta a las peticiones generadas por el servidor CJR desde el servidor interno TELCO, con lo que se confirma el problema de ruteo asimétrico para este servicio.

- El FW_INTERNET_1 droppea el tráfico de respuesta hacia el servidor CJR California ya que como elemento de seguridad no permite acciones que no están definidas en sus políticas y para el caso del servicio CJR se establece en la política que únicamente el servidor CJR California es quien inicia la comunicación y para este caso de ruteo asimétrico el servidor interno TELCO es quien genera primero la conexión en este firewall para responder las peticiones recibidas, debido a esto el tráfico es bloqueado y se pierde la conectividad.

SOURCE	DESTINATION	PROTOCOL
CJR California (201.16.8.2)	TELCO (192.168.2.1)	UDP

Figura 4.5 Regla en Firewall para el Servicio CJR

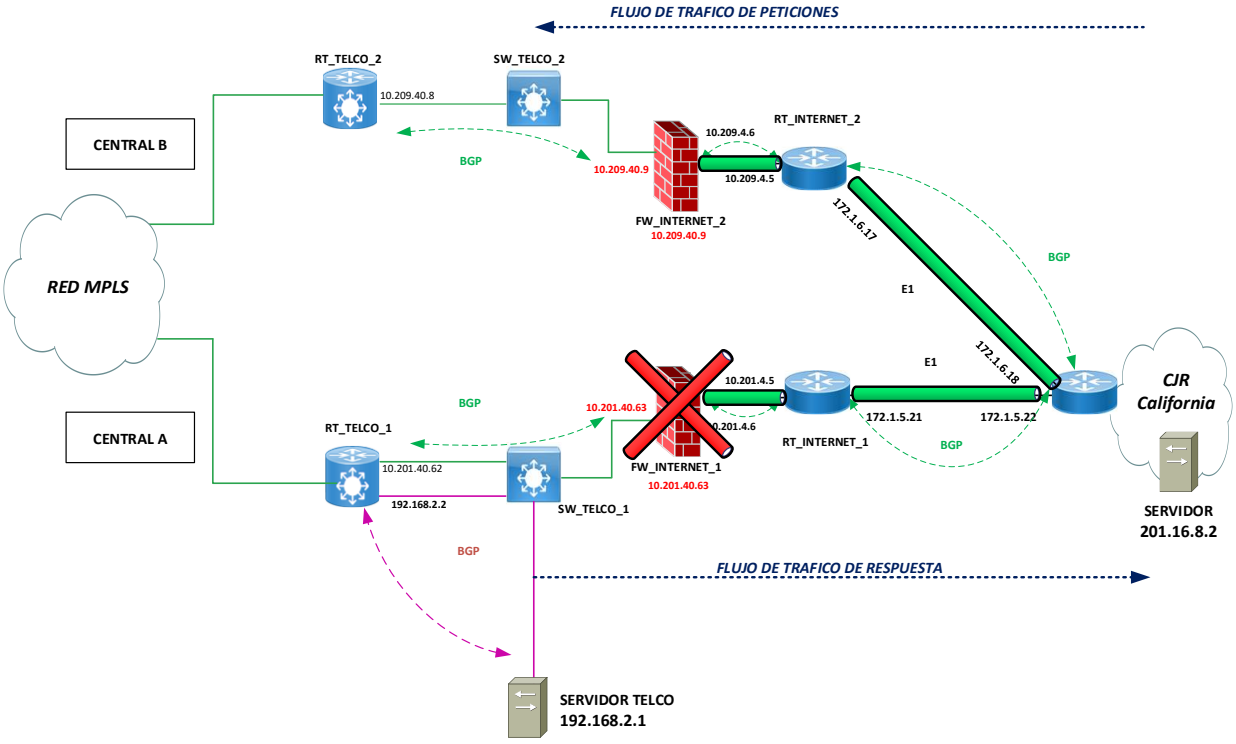


Figura 4.6 Falla por Ruteo Asimétrico

4.4.3 Solución del problema

Una vez detectados los drops generados en el FW_INTERNET_1 por ruteo asimétrico se procede a la corrección de este problema para reestablecer la conectividad del servicio y con esto también establecer la correcta configuración para contar con un escenario de alta disponibilidad ante otra posible falla de alguno de los enlaces dedicados.

1) Revisión de la configuración de rutas hacia Red Interna

Debido al problema de ruteo asimétrico que se presenta, podemos observar que el RT_TELCO_1 recupera su ruta principal cuando el enlace primario se reestablece, por lo tanto, existe una configuración adecuada de rutas primaria y secundaria hacia la red interna de la empresa.

Revisando la configuración del router RT_INTERNET_2 se encuentra lo siguiente:

- Prefix-List y Route-Map hacia FW TELCO

```
conf t
!
ip prefix-list SERVER_CJR seq 10 permit 201.16.8.2/32      //SERVIDOR CJR
!
!
route-map RM_CJR_CALIFORNIA permit 5
 match ip address prefix-list SERVER_CJR
 set as-path prepend 65001 65001 65001                     //SE AGREGAN 3 AS
!
exit
!
```

-Observamos que se encuentra creado el Prefix-List **SERVER_CJR** el cual tiene el objetivo de filtrar el tráfico interesante que en este caso es el tráfico que es enviado desde el servidor CJR California.

-Posteriormente se crea el Route-Map **RM_CJR_CALIFORNIA** que es una secuencia de instrucciones en el que se establece que se hará match con las direcciones IP definidas en el Prefix-List **SERVER_CJR,** además de agregar un **AS-Path Prepend** de 3 Sistemas Autónomos con lo cual se da un mayor peso a esta ruta convirtiéndola en un camino secundario.

- Configuración de BGP a Red Interna TELCO

```
router bgp 65001
neighbor 10.209.4.6 route-map RM_CJR_CALIFORNIA out
!
exit
!
Wr
```

-Se tiene aplicado el Route-Map **RM_CJR_CALIFORNIA** en la configuración de BGP hacia FW TELCO.

Esta configuración de rutas existente en el router RT_INTERNET_2 es propagada vía BGP hacia la red interna por lo cual con esta información el router RT_TELCO_1 es capaz de distinguir entre la ruta primaria y secundaria. En caso de presentarse una falla envía automáticamente los paquetes por el path secundario y al reestablecerse el enlace principal vuelve a enviar la información por su ruta primaria.

2) Configuración de Rutas Primaria y Secundaria hacia Cliente CJR

Del análisis anterior se determinó que se debía aplicar la misma configuración de rutas primaria y secundaria en el router RT_INTERNET_2 pero esta vez hacia el cliente CJR, ya que el problema de ruteo asimétrico se generó debido que a que su router frontera del cliente no es capaz de distinguir entre una ruta primaria y una secundaria.

- Prefix-List y Route-Map hacia ROUTER CJR

```
conf t
!
ip prefix-list SERVER_TELCO seq 10 permit 192.168.2.1/32      //SERVIDOR TELCO
!
!
route-map RM_TELCO_MX permit 10
 match ip address prefix-list SERVER_TELCO
 set as-path prepend 65001 65001 65001                        //SE AGREGAN 3 AS
!
exit
!
```

-Creamos el Prefix-List **SERVER_TELCO** el cual tiene el objetivo de filtrar el tráfico interesante que en este caso es el tráfico que es enviado desde el servidor TELCO.

-Posteriormente se crea el Route-Map **RM_TELCO_MX** que es una secuencia de instrucciones en el que se establece que se hará match con las direcciones IP definidas en el Prefix-List **SERVER_TELCO**, además de agregar un **AS-Path Prepend** de 3 Sistemas Autónomos con lo cual se da un mayor peso a esta ruta convirtiéndola en un camino secundario.

- Configuración de BGP a Red Cliente CJR

```
router bgp 65001
neighbor 172.1.6.18 route-map RM_TELCO_MX out
!
exit
!
wr
```

-Se aplica el Route-Map **RM_TELCO_MX** en la configuración de BGP hacia el Router Frontera del Cliente CJR.

Con esta configuración el Router Frontera del cliente podrá instalar una ruta primaria y una secundaria para alcanzar el servidor TELCO y en caso de presentarse una falla en alguno de sus enlaces el servicio no se verá interrumpido, cuando se reestablezca el enlace que falló ambas redes estarán preparadas para volver a enviar la información por el path primario garantizando así un escenario de alta disponibilidad.

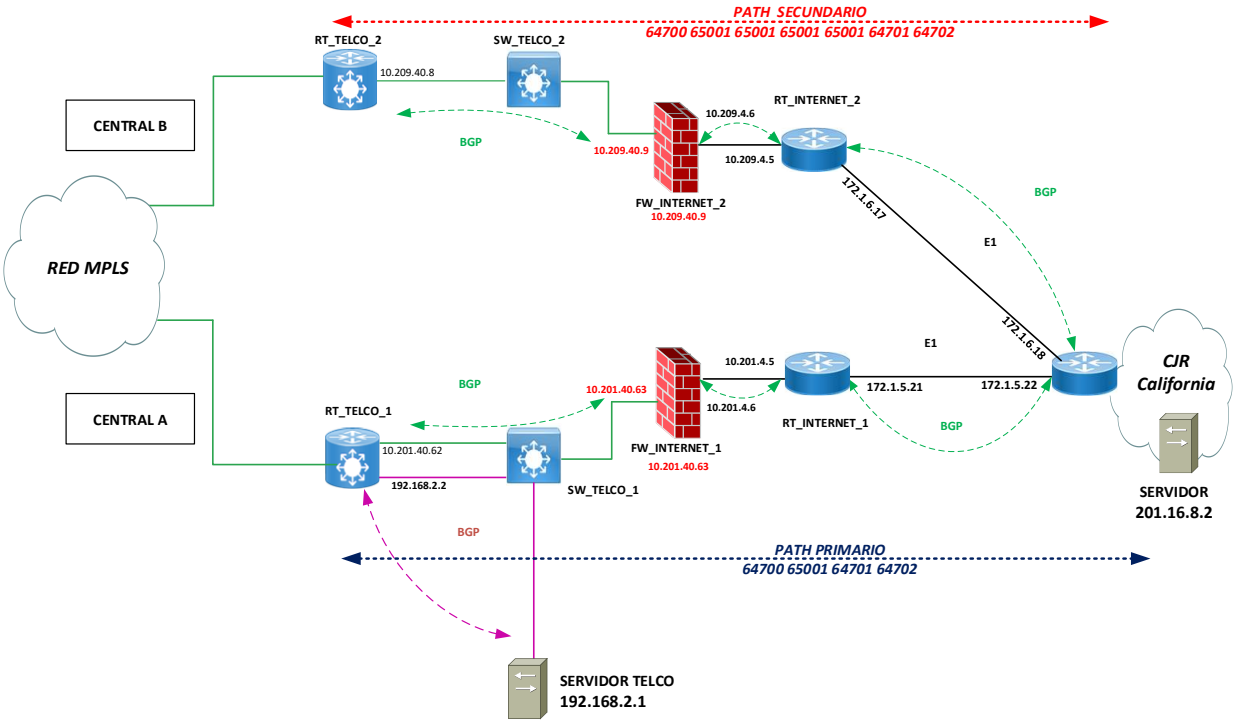


Figura 4.7 Topología Alta Disponibilidad Cliente CJR

4.5 Conclusiones

- Se presenta falla de conectividad por caída de enlace primario hacia el servidor CJR California, se contacta al proveedor externo del enlace y reporta tarjeta en estado “down” en uno de los equipos de la trayectoria del enlace. Se realiza cambio de tarjeta en equipo con lo que se recupera el enlace, al recuperar el path primario se genera ruteo asimétrico por lo que el FW droppea los paquetes de respuesta enviados por el servidor Interno TELCO hacia el cliente CJR.

- Se revisa la configuración del Router RT_INTERNET_2 y se observa que se encuentra la configuración adecuada para que el RT_TELCO_1 pueda distinguir entre su ruta primaria y secundaria por lo tanto este dispositivo envía la información de nueva cuenta por su path primario una vez que se reestablece el enlace caído.

- Revisando el mismo Router RT_INTERNET_2 encontramos que no existe configuración de ruta secundaria hacia el Router Frontera del Cliente el cual cuenta con una sesión de BGP activa hacia nuestra red, pero no distingue las rutas primaria y secundaria. Se configura el atributo de BGP AS-PATH Prepend para dar un mayor peso a la ruta del equipo RT_INTERNET_2 convirtiéndolo así en el path secundario hacia el servidor TELCO.

- Se realizaron las correspondientes pruebas de redundancia en conjunto con el cliente, se apagaron ambos enlaces, uno a la vez y se pudo validar el correcto funcionamiento de la configuración aplicada en el RT_INTERNET_2 para proporcionar el escenario de alta disponibilidad que el cliente necesita para su operación diaria.

CAPÍTULO 5: PROYECTO MIGRACIÓN DE ENLACES DE CADENAS COMERCIALES

5.1 Introducción

Nuestra empresa de telecomunicaciones ofrece diferentes servicios al público en general como lo son telefonía, mensajería SMS y datos (Navegación en internet, streaming, Apps, etc) mediante la red celular 4G que tiene desplegada a lo largo de México.

Existen dos formas de adquirir los servicios de telecomunicación celular que ofrece nuestra empresa:

- Planes de renta mensual: Incluyen una bolsa de determinado número de minutos para llamadas, mensajes SMS y MB de navegación en Internet. Al inicio de cada mes se vuelve a otorgar al cliente la bolsa incluida en su paquete.

- Prepago: Mediante recargas de diferentes costos se ofrece al cliente un determinado número de minutos para llamadas, mensajes SMS y MB de navegación en Internet. Al termino del crédito el cliente debe realizar otra recarga para volver a contar con el servicio.

Figura 5.1 Servicios proporcionados por la red 4G

5.2 Objetivo y alcance del proyecto

La forma de adquirir los servicios por parte del cliente que más ingresos aporta a nuestra empresa es el Prepago, es decir la recarga de tiempo aire para contar con minutos de telefonía, mensajes SMS y MB para navegar en Internet. Por tal motivo se tiene una infraestructura dedicada para asegurar la disponibilidad, seguridad e integridad de las transacciones que se realizan para la venta de tiempo aire de nuestra empresa a las diferentes cadenas comerciales que cuentan con terminales de recarga de saldo en sus establecimientos.

Debido a la importancia de esta infraestructura se realizó un análisis con el objetivo de detectar problemas y corregirlos además de encontrar posibles fallas y prevenirlas, y por último realizar mejoras a la arquitectura de este servicio para poder llevar a cabo la venta de tiempo aire por parte de las cadenas comerciales sin contratiempo alguno.

Se realizó el análisis de la siguiente arquitectura que se tiene para la conexión de las cadenas comerciales a los servidores de venta de tiempo aire alojados en nuestra empresa.

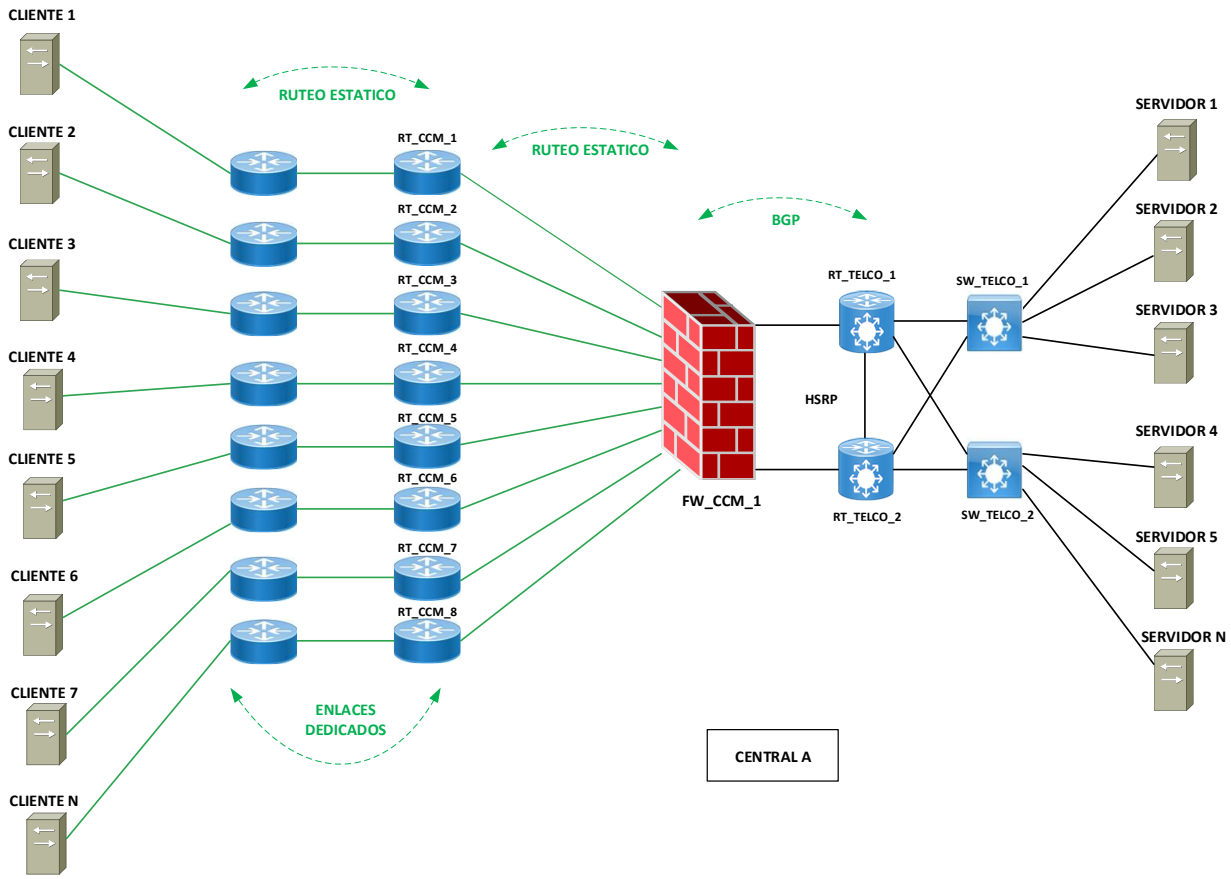


Figura 5.2 Topología Anterior Cadenas Comerciales

Como resultado del análisis realizado se detectaron los siguientes problemas:

- Los Routers frontera RT_CCM_1 al RT_CCM_8 donde se reciben los enlaces dedicados de las cadenas comerciales ya no cuentan con soporte en caso de falla por parte de Cisco.

- Los Routers CCM ya no soportan actualizaciones de software para corregir bugs o agregar nuevas funcionalidades útiles para implementaciones futuras, lo cual los convierte en equipos obsoletos.

- Ningún enlace dedicado cuenta con redundancia en caso de falla.

- Existe ruteo estático entre los Routers CCM y el Firewall FW_CCM_1.

- El cableado existente ya es muy viejo, por lo tanto, es vulnerable a presentar fallas.

Una vez que se tenían los resultados del análisis realizado por mi área se propuso a nuestra gerencia la siguiente arquitectura para solucionar los problemas encontrados y poder garantizar el correcto funcionamiento de la red.

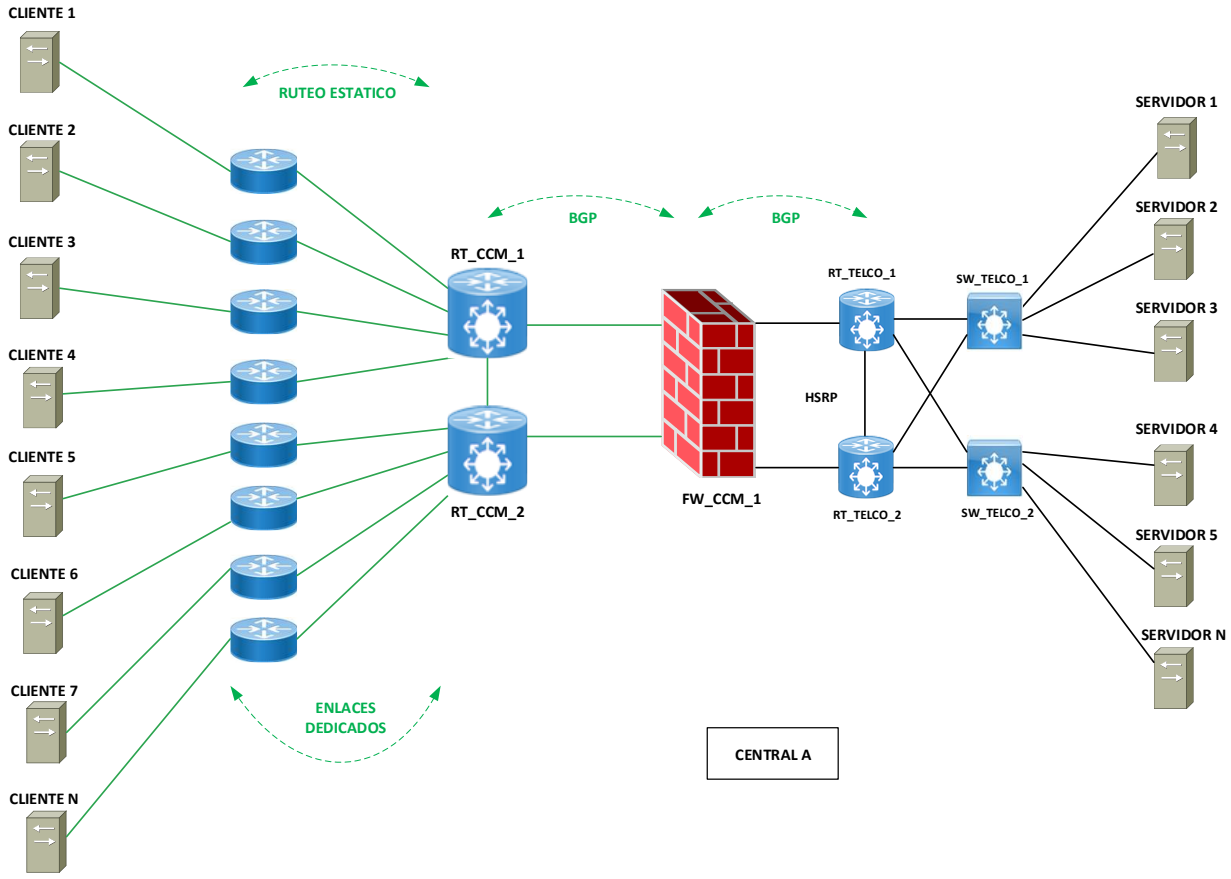


Figura 5.3 Topología Nueva Cadenas Comerciales

Se propone realizar las siguientes acciones para corregir los problemas encontrados:

- Cambiar los Routers CCM antiguos (Cisco 3800) por equipos carrier class con mayor capacidad y robustez (Cisco 7609-S).
- Instalar cableado nuevo UTP Categoría 5
- Implementar ruteo dinámico (BGP) para la conectividad entre los Routers CCM y el Firewall FW_CCM_1.
- Implementar redundancia para los clientes que lo soliciten.

Una vez que se aprobó el proyecto se definieron las siguientes fases para llevar a cabo los cambios propuestos anteriormente:

- **Fase I** Instalación de Routers y cables nuevos
- **Fase II** Conectividad vía BGP entre Routers CCM y Firewall
- **Fase III** Migración de enlaces a nuevos Routers CCM
- **Fase IV** Migración de enlaces con redundancia
- **Fase V** Apagado y desinstalación de equipos obsoletos

5.3 Fase I Instalación de routers y cables nuevos

En esta primer fase del proyecto se contempla la instalación de los nuevos Routers Cisco 7609-S los cuales cuentan capacidades de doble procesadora y doble fuente de poder para soportar los servicios que actualmente se conectan al equipos además de proporcionar escalabilidad ya que a futuro se seguirán agregando enlaces dedicados de nuevos clientes que requieran la conexión a los servidores de venta de tiempo aire, por otra parte estos equipos carrier class tienen características en su sistema operativo (IOS Version 12.2) que soportan el protocolo BGP, el cual es ampliamente utilizado a nivel de proveedor de servicios.

Figura 5.4 Router Cisco 7609-S

Por otra parte, se instaló cableado nuevo UTP Categoría 5 el cual soporta la velocidad de los enlaces dedicados E1 que son de máximo 2 MB, además se instaló un par de paneles balun que son necesarios para trasformar la señal de Tx y Rx del enlace (BNC) a un solo medio de transmisión que son los cables UTP y así poderlos conectar a los nuevos Routers.

Figura 5.5 Panel Balun

Se realizaron las siguientes actividades durante esta fase del proyecto:

- Se coordinó una primera ventana de mantenimiento en conjunto con personal de campo y proveedor para instalar los nuevos Routers en el site de la Central A; se colocaron en su lugar asignado dentro del site, se energizaron y se encendieron ambos equipos.

- Se realizó un site survey en conjunto con el proveedor del cableado para realizar el conteo de todos los enlaces dedicados de las cadenas comerciales para conocer el número de cables UTP Categoría 5 que serán requeridos, así como para determinar la cantidad y posición de los paneles balun que se utilizarán. Con esta información se realizó el pedido correspondiente al proveedor.

- Se realizó una segunda ventana de mantenimiento en conjunto con el proveedor del cableado y personal de campo para instalar los nuevos cables UTP y los paneles balun así como realizar las conexiones entre los Routers CCM y el Firewall y entre ambos Routers. Los cables para los enlaces dedicados de las cadenas comerciales se dejaron en punta únicamente para conectarlos en el momento de la migración.

5.4 Fase II Conectividad vía BGP entre routers CCM y firewall

En esta segunda fase del proyecto se implementó la conectividad vía BGP entre los Routers RT_CCM_1, RT_CCM_2 y FW_CCM_1 que sustituyó el ruteo estático en la anterior arquitectura por el ruteo dinámico entre los Routers que reciben los enlaces dedicados y el Firewall.

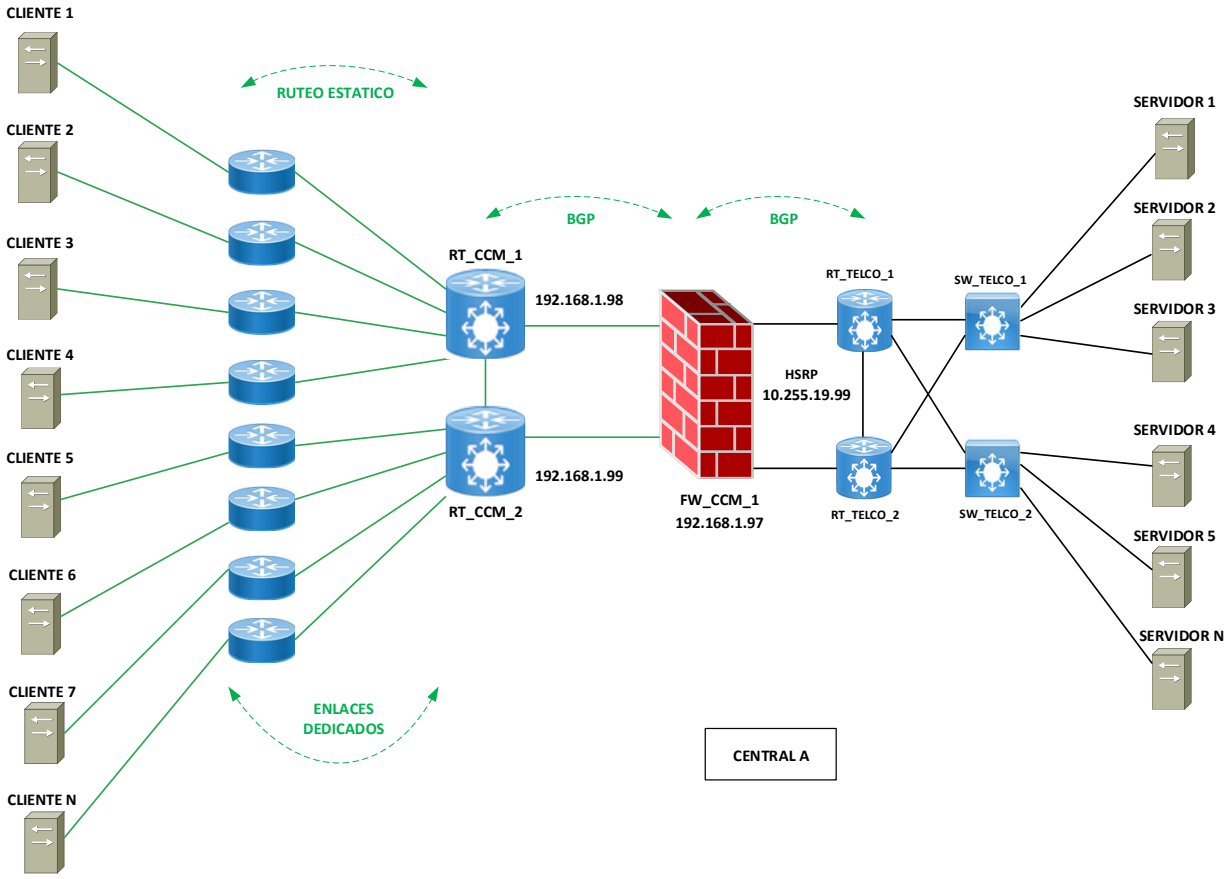


Figura 5.6 Topología Cadenas Comerciales

Se programó una ventana de mantenimiento para poder realizar las configuraciones necesarias para levantar las vecindades de BGP en los Routers RT_CCM_1, RT_CCM_2 y el firewall FW_CCM_1. A continuación se detalla los cambios aplicados en los tres equipos de red con el fin de establecer la conectividad vía BGP.

Se realizaron las siguientes tablas con la información que será utilizada para configurar BGP en los equipos.

ROUTERS	IP LOCAL	AS	PEER
RT_CCM_1	192.168.1.98	704	192.168.1.97
RT_CCM_2	192.168.1.99		192.168.1.97

Figura 5.7 Tabla de Información de BGP Routers CCM

FW	IP LOCAL	AS	PEER
FW_CCM_1	192.168.1.97	705	192.168.1.98
			192.168.1.99

Figura 5.8 Tabla de Información de BGP Firewall

Configuraciones en RT_CCM_1

- Route-Map hacia Router RT_CCM_2

```
conf t
!
route-map B2B-7601 permit 10
 set as-path prepend 704 704 704                    //SE AGREGAN 3 AS
!
exit
!
```

-Se crea el Route-Map **B2B-7601** que es una secuencia de instrucciones en el que se establece que deberá agregar un **AS-Path Prepend** de 3 Sistemas Autónomos con lo cual se da un mayor peso a esta ruta convirtiéndola en un camino secundario.

- Configuración de BGP

```
router bgp 704
bgp router-id 10.255.19.96                                  //IP DE GESTION
redistribute connected
redistribute static
neighbor 192.168.1.97 remote-as 705
neighbor 192.168.1.99 remote-as 704
neighbor 192.168.1.99 route-map B2B-7601 out
!
exit
!
```

-Se asigna el sistema autónomo (AS) al que corresponde el Router, que en este caso es **704** y se asigna la IP de gestión del equipo como un Router ID de BGP.

-Se aplican comandos para redistribuir las rutas que el equipo tenga configuradas de manera estática, así como aquellas que tenga conectadas directamente.

-Se levanta la sesión de BGP con sus dos vecinos que son el Router **RT_CCM_2** y el Firewall **FW_CCM_1.**

-Por último, se aplica el Route-Map **B2B-7601** hacia el Router **RT_CCM_2** para que dicho equipo pueda distinguir una ruta secundaria hacia el Firewall **FW_CCM_1.**

Configuraciones en RT_CCM_2

- Route-Map hacia Router RT_CCM_1

```
conf t
!
route-map B2B-7601 permit 10
 set as-path prepend 704 704 704                    //SE AGREGAN 3 AS
!
exit
!
```

-Se crea el Route-Map **B2B-7601** que es una secuencia de instrucciones en el que se establece que deberá agregar un **AS-Path Prepend** de 3 Sistemas Autónomos con lo cual se da un mayor peso a esta ruta convirtiéndola en un camino secundario.

- Configuración de BGP

```
router bgp 704
bgp router-id 10.255.19.97                              //IP DE GESTION
redistribute connected
redistribute static
neighbor 192.168.1.97 remote-as 705
neighbor 192.168.1.98 remote-as 704
neighbor 192.168.1.98 route-map B2B-7601 out
!
exit
!
```

-Se asigna el sistema autónomo (AS) al que corresponde el Router, que en este caso es **704** y se asigna la IP de gestión del equipo como un Router ID de BGP.

-Se aplican comandos para redistribuir las rutas que el equipo tenga configuradas de manera estática, así como aquellas que tenga conectadas directamente.
-Se levanta la sesión de BGP con sus dos vecinos que son el Router **RT_CCM_1** y el Firewall **FW_CCM_1.**

-Por último, se aplica el Route-Map **B2B-7601** hacia el Router **RT_CCM_1** para que dicho equipo pueda distinguir una ruta secundaria hacia el Firewall **FW_CCM_1.**

Configuraciones en FW_CCM_1

- Configuración de BGP

```
set as 705
set bgp external remote-as 704 on
set bgp external remote-as 704 peer 192.168.1.98 on
set bgp external remote-as 704 on
set bgp external remote-as 704 peer 192.168.1.99 on
!
save config
```

-Se asigna el sistema autónomo (AS) al que corresponde el Firewall, que en este caso es **705**.

-Se levanta la sesión de BGP con sus dos vecinos que son los Routers **RT_CCM_1** y **RT_CCM_2.**

- Configuración de Políticas

  Se creó la regla siguiente regla al principio de las reglas del Firewall:

  Name: BGP Service
  Source: RT_CCM_1, RT_CCM_2
  Destination: FW_CCM_1
  Service: BGP
  Action: Accept
  Log: None
  Comment: Regla para servicio de BGP Cadenas Comerciales

Figura 5.9 Ejemplo de Regla en Firewall

Con estas configuraciones aplicadas en los Routers RT_CCM_1 y RT_CCM_2 y el Firewall FW_CCM_1 se logró establecer la conectividad utilizando BGP como protocolo de ruteo dinámico y se tuvo listo el escenario para comenzar con la migración de servicios.

5.5 Fase III Migración de enlaces a nuevos routers CCM

Una vez establecida la conectividad vía BGP entre Routers y Firewall se inició la migración de los enlaces dedicados comenzando con aquellos que no se solicitó redundancia. Se programaron ventanas de mantenimiento para migrar los servicios de un Router a la vez.

Se realizó el siguiente proceso para migrar los enlaces dedicados de cada Router obsoleto a los nuevos Routers CCM.

1) Análisis de Información necesaria para configuraciones

Para llevar a cabo la migración de estos enlaces se realizaron las siguientes tablas que contienen la información para realizar la configuración de los equipos.

ROUTER OBSOLETO	ENLACE	SEGMENTOS	NEXTHOP CLIENTE
RT_CADENAS_COMER_I	CLIENTE A	10.25.19.0/24	10.20.12.46
	CLIENTE B	10.25.5.25/32	192.16.22.5
		10.25.5.26/32	
		10.25.5.27/32	
		10.25.10.3/32	
		10.25.10.4/32	
		10.25.10.5/32	
		21.94.37.4/32	
		21.94.37.5/32	
		21.94.37.6/32	
		21.94.37.7/32	
		21.94.37.46/32	
		21.94.37.47/32	
		21.94.37.48/32	

Figura 5.10 Tabla Prefijos del Cliente que anunciaran los Routers CCM al FW

EQUIPO ACTUAL	INTERFACE	SERVICIO	NUEVO EQUIPO	INTERFACE	PREFIJOS QUE ANUNCIARA EL FW
RT_CADENAS_COMER_I	Fa 0/1	CLIENTE A	RT_CCM_1	GigabitEthernet7/6	0.0.0.0/0
	Fa 0/2	CLIENTE B	RT_CCM_2	GigabitEthernet7/5	

Figura 5.11 Tabla Migración de Enlaces

-La primera tabla (Figura 5.10) se llena con los segmentos de los enlaces dedicados de nuestros clientes, los cuales serán cargados en los Routers **RT_CCM_1** y **RT_CCM_2** y una vez configurados serán anunciados vía BGP hacia el Firewall **FW_CCM_1.**

-La segunda tabla (Figura 5.11) se llena con las posiciones físicas en los antiguos Routers y las posiciones que ocuparan en los nuevos equipos los enlaces a migrar, así como el prefijo que estará anunciando el Firewall **FW_CCM_1** a los Routers **RT_CCM_1** y **RT_CCM_2.**

2) Configuraciones

Configuraciones en RT_CADENAS_COMER_I

- Apagado de Interfaces

```
conf t
!
int Fa 0/1
shut
!
int Fa 0/2
shut
!
exit
```

-Se apagan las interfaces que ya no se ocuparan para poder llevar a cabo la migración de los servicios.

Configuraciones en RT_CCM_1

- Encendido de Interfaces

```
conf t
!
interface GigabitEthernet7/6
description CLIENTE A
ip address 10.20.12.45 255.255.255.252
duplex full
speed 100
no cdp enable
no shut
```

-Se encienden y se asignan direcciones IP a las interfaces donde se conectarán los enlaces migrados. Las direcciones IP asignadas son las correspondientes a las interfaces de los equipos anteriores con el fin de que el cliente conserve el mismo Gateway por defatult (mismo Nexthop).

- Inyección de Rutas

```
conf t
!
ip route 10.25.19.0   255.255.255.0          10.20.12.46
```

-Se cargan los segmentos del cliente que el Router **RT_CCM_1** anunciará al Firewall **FW_CCM_1** mediante BGP.

Configuraciones en RT_CCM_2

- Encendido de Interfaces

```
conf t
!
interface GigabitEthernet7/5
description CLIENTE B
ip address 192.16.22.4 255.255.255.252
duplex full
speed 100
no cdp enable
no shut
```

-Se encienden y se asignan direcciones IP a las interfaces donde se conectarán los enlaces migrados. Las direcciones IP asignadas son las correspondientes a las interfaces de los equipos anteriores con el fin de que el cliente conserve el mismo Gateway por defatult (mismo Nexthop).

- Inyección de Rutas

```
conf t
!
ip route 10.25.5.25   255.255.255.255        192.16.22.5
ip route 10.25.5.26   255.255.255.255        192.16.22.5
ip route 10.25.5.27   255.255.255.255        192.16.22.5
ip route 10.25.10.3   255.255.255.255        192.16.22.5
ip route 10.25.10.4   255.255.255.255        192.16.22.5
ip route 10.25.10.5   255.255.255.255        192.16.22.5
ip route 21.94.37.4    255.255.255.255       192.16.22.5
ip route 21.94.37.5    255.255.255.255        192.16.22.5
ip route 21.94.37.6    255.255.255.255        192.16.22.5
ip route 21.94.37.7    255.255.255.255        192.16.22.5
ip route 21.94.37.46   255.255.255.255       192.16.22.5
ip route 21.94.37.47   255.255.255.255       192.16.22.5
ip route 21.94.37.48   255.255.255.255       192.16.22.5
```

-Se cargan los segmentos del cliente que el Router **RT_CCM_2** anunciará al Firewall **FW_CCM_1** mediante BGP.

Configuraciones en FW_CCM_1

Se realizaron las siguientes configuraciones en el Firewall con apoyo del proveedor del equipo:

- Se configuró el prefijo **0.0.0.0/0** para que sea anunciado vía BGP hacia los Routers **RT_CCM_1** y **RT_CCM_2** como ruta por default. Esto se debe a que por razones de seguridad el Firewall no debe propagar a los Routers CCM las rutas que aprende de la red interna.

- Se borraron las antiguas rutas estáticas hacia los Routers CCM para dejar operando únicamente el ruteo dinámico.

NOTA: NO se realiza ninguna configuración de reglas en el Firewall debido a que ya se tienen las reglas para los segmentos de todos los enlaces.

3) Ventana de mantenimiento

-Se programa una ventana de mantenimiento en conjunto con personal de campo y proveedores con el fin de migrar los enlaces dedicados de cada Router.

-Se realizó respaldos de la configuración de los equipos previo a la intervención de la red.

-Se aplicaron las configuraciones necesarias para migrar los enlaces en los equipos **FW_CCM_1, RT_CCM_1** y **RT_CCM_2.**

-Se realizaron validaciones de los servicios y aplicativos por parte de los clientes.

-Por último, se realizaban sesiones de Troubleshooting ya sea en el momento de la ventana de mantenimiento o a la mañana siguiente de la actividad, lo anterior solo en los casos en los que se presentaban fallas de conectividad de los aplicativos después nuestras actividades.

5.6 Fase IV Migración de enlaces con redundancia

Al concluir con la migración de los enlaces que no contaban con redundancia procedimos a realizar la correspondiente migración de los servicios que se solicitó redundancia con un segundo enlace. Se programaron ventanas de mantenimiento para migrar los servicios de un Router a la vez.

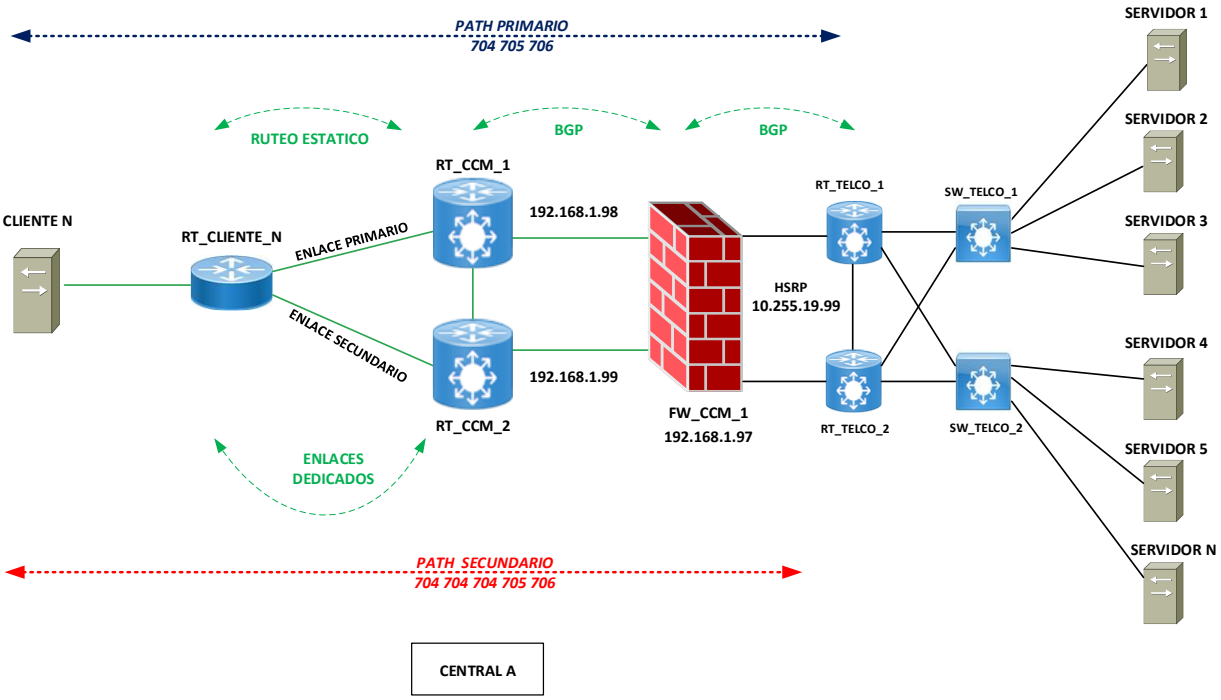


Figura 5.12 Topología Cadenas Comerciales – Servicios con redundancia

Se realizó el siguiente proceso para migrar los enlaces dedicados de cada Router obsoleto a los nuevos Routers CCM.

1) Análisis de Información necesaria para configuraciones

Para llevar a cabo la migración de estos enlaces se realizaron las siguientes tablas que contienen la información para realizar la configuración de los equipos.

CLIENTE	ENLACE	SEGMENTOS	NEXTHOP CLIENTE	COSTO
CLIENTE X	PRIMARIO	10.25.5.25/32	192.16.22.5	1
		10.25.5.26/32		
		10.25.5.27/32		
		10.25.10.3/32		
		10.25.10.4/32		
		10.25.10.5/32		
	SECUNDARIO	10.25.5.25/32	192.16.22.7	100
		10.25.5.26/32		
		10.25.5.27/32		
		10.25.10.3/32		
		10.25.10.4/32		
		10.25.10.5/32		

Figura 5.13 Tabla Prefijos del Cliente que anunciaran los Routers CCM al FW

EQUIPO ACTUAL	INTERFACE	ENLACE	NUEVO EQUIPO	INTERFACE	PREFIJOS QUE ANUNCIARA EL FW
RT_CADENAS_COMER_I	Fa 1/1	PRIMARIO	RT_CCM_1	GigabitEthernet5/1	0.0.0.0/0
	Fa 1/2	SECUNDAR	RT_CCM_2	GigabitEthernet5/1	

Figura 5.14 Tabla Migración de Enlaces

-La primera tabla (Figura 5.13) se llena con los segmentos de los enlaces dedicados de nuestros clientes, los cuales serán cargados en los Routers **RT_CCM_1** y **RT_CCM_2** y una vez configurados serán anunciados vía BGP hacia el Firewall **FW_CCM_1.**

-La segunda tabla (Figura 5.14) se llena con las posiciones físicas en los antiguos Routers y las posiciones que ocuparan en los nuevos equipos los enlaces a migrar, así como el prefijo que estará anunciando el Firewall **FW_CCM_1** a los Routers **RT_CCM_1** y **RT_CCM_2.**

2) Configuraciones

Configuraciones en RT_CADENAS_COMER_I

- Apagado de Interfaces

```
conf t
!
int Fa 1/1
shut
!
int Fa 1/2
shut
!
exit
```

-Se apagan las interfaces que ya no se ocuparan para poder llevar a cabo la migración de los servicios.

Configuraciones en RT_CCM_1

- Encendido de Interfaces

```
conf t
!
interface GigabitEthernet5/1
description CLIENTE X
ip address 192.16.22.4 255.255.255.252
duplex full
speed 100
no cdp enable
no shut
```

-Se encienden y se asignan direcciones IP a las interfaces donde se conectarán los enlaces migrados. Las direcciones IP asignadas son las correspondientes a las interfaces de los equipos anteriores con el fin de que el cliente conserve el mismo Gateway por defatult (mismo Nexthop).

- Inyección de Rutas

```
conf t
!
ip route 10.25.5.25   255.255.255.255        192.16.22.5
ip route 10.25.5.26   255.255.255.255        192.16.22.5
ip route 10.25.5.27   255.255.255.255        192.16.22.5
ip route 10.25.10.3   255.255.255.255        192.16.22.5
ip route 10.25.10.4   255.255.255.255        192.16.22.5
ip route 10.25.10.5   255.255.255.255        192.16.22.5
```

-Se cargan los segmentos del cliente que el Router **RT_CCM_1** anunciará al Firewall **FW_CCM_1** mediante BGP. Podemos observar que debido a que se trata del enlace primario no se configura costo alguno para las rutas, por lo tanto, el costo de las rutas estáticas es de 1.

Configuraciones en RT_CCM_2

- Encendido de Interfaces

```
conf t
!
interface GigabitEthernet5/1
description CLIENTE X
ip address 192.16.22.6 255.255.255.252
duplex full
speed 100
no cdp enable
no shut
```

-Se encienden y se asignan direcciones IP a las interfaces donde se conectarán los enlaces migrados. Las direcciones IP asignadas son las correspondientes a las interfaces de los equipos anteriores con el fin de que el cliente conserve el mismo Gateway por defatult (mismo Nexthop).

- Inyección de Rutas

```
conf t
!
ip route 10.25.5.25   255.255.255.255        192.16.22.7     100
ip route 10.25.5.26   255.255.255.255        192.16.22.7     100
ip route 10.25.5.27   255.255.255.255        192.16.22.7     100
ip route 10.25.10.3   255.255.255.255        192.16.22.7     100
ip route 10.25.10.4   255.255.255.255        192.16.22.7     100
ip route 10.25.10.5   255.255.255.255        192.16.22.7     100
```

-Se cargan los segmentos del cliente que el Router **RT_CCM_2** anunciará al Firewall **FW_CCM_1** mediante BGP. Podemos observar que debido a que se trata del enlace secundario se configura un costo de 100 para las rutas, con esto, el Firewall puede distinguir entre un path primario y un secundario ya aprende las mismas rutas por diferentes enlaces, pero es el parámetro del costo lo que hace la diferencia en la preferencia que tendrá el Firewall a la hora de elegir una ruta.

Configuraciones en FW_CCM_1

Se realizaron las siguientes configuraciones en el Firewall con apoyo del proveedor del equipo:

- Se configuró el prefijo **0.0.0.0/0** para que sea anunciado vía BGP hacia los Routers **RT_CCM_1** y **RT_CCM_2** como ruta por default. Esto se debe a que por razones de seguridad el Firewall no debe propagar a los Routers CCM las rutas que aprende de la red interna.

- Se borraron las antiguas rutas estáticas hacia los Routers CCM para dejar operando únicamente el ruteo dinámico.

NOTA: NO se realiza ninguna configuración de reglas en el Firewall debido a que ya se tienen las reglas para los segmentos de todos los enlaces.

3) Ventana de mantenimiento

-Se programa una ventana de mantenimiento en conjunto con personal de campo y proveedores con el fin de migrar los enlaces dedicados de cada Router.

-Se realizó respaldos de la configuración de los equipos previo a la intervención de la red.

-Se aplicaron las configuraciones necesarias para migrar los enlaces en los equipos **FW_CCM_1, RT_CCM_1** y **RT_CCM_2.**

-Se realizaron pruebas de redundancia de cada servicio, conmutando el tráfico entre los enlaces primario y secundario además de resolver los problemas que se presentaban, todo lo anterior en conjunto con el cliente.

-Se realizaron validaciones de los servicios y aplicativos por parte de los clientes.

5.7 Fase V Apagado y desinstalación de equipos obsoletos

Al término de la migración de todos los enlaces dedicados y una vez realizadas las pruebas de los correspondientes servicios del cliente, se procedió con el apagado y desinstalación de los equipos y el cableado obsoleto en coordinación con el área de Ingeniería que son los encargados de dar seguimiento a este tema.

Figura 5.15 Router Obsoleto Cisco 3800

Se realizaron las siguientes actividades:

- Se programó una ventana de mantenimiento para el apagado y desconexión de la fuente de energía de los Routers obsoletos con apoyo de personal de campo.

- Se realizó una segunda ventana de mantenimiento con apoyo de personal de campo para desinstalar los Routers y el cableado obsoleto.

- Por último, se enviaron a las bodegas de la empresa los equipos que se recogieron para que posteriormente se envíen al proveedor como parte de los convenios que se tiene del reciclado y recolección de equipos en desuso.

5.8 Conclusiones

Al término de las cinco fases de este proyecto podemos concluir que se lograron cumplir satisfactoriamente los siguientes objetivos planteados que dieron origen al proyecto.

- Se cambiaron los Routers CCM antiguos (Cisco 3800) por equipos carrier class con mayor capacidad y robustez (Cisco 7609-S).
- Se instaló cableado nuevo UTP Categoría 5
- Se implementó ruteo dinámico (BGP) para la conectividad entre los Routers CCM y el Firewall FW_CCM_1.
- Se implementó redundancia para los clientes que lo solicitaron.

Además de lo anterior podemos concluir lo siguiente:

- Se migró un total de 78 enlaces dedicados.
- Los 5 clientes con más ventas de tiempo aire cuentan con redundancia.
- Se llevaron a cabo un total de 14 ventanas de mantenimiento de las cuales, 8 ventanas fueron para migrar los enlaces de los Routers, 1 ventana para instalación de los nuevos equipos, 1 ventana para instalación de cables, 1 ventana para implementar BGP y 3 ventanas para implementar la redundancia de los clientes más importantes.
- El tiempo aproximado que duró el proyecto fue de 6 meses.

Las fallas más comunes que se presentaron durante la migración fueron las siguientes:

- Falta de conectividad debido a que se debe reiniciar aplicativo del cliente.
- Falta de conectividad debido a que no se cargaron en los Routers todos los segmentos del cliente.
- El Cliente agregó nuevas IP de servidores y no existían reglas en el Firewall.
- Falla de cableado nuevo.

REFERENCIAS

Bibliográficas

Odom, Wendell; **CCNA Routing and Switching 200-125 Official Cert Guide Library**; Cisco Press; 1st Edition; USA 2016

Zhang Randy, Bartell Micah; **BGP Design and Implementation**; Cisco Press; 1st Edition; USA 2003

Lasso Mesa, Mario; **Encaminamiento dinámico en Internet mediante BGP**; e-Reding Universidad de Sevilla; 1ra Edición; España 2015

Vázquez Gómez, Jesús; **Principios Fundamentales de Seguridad**; IPN; 2010

Harris, Shon; **CISSP. All in one Exam guide**; Mc Graw Hill; Sixth Edition; USA 2012

Digitales

Cisco Networking Academy - CCNA R&S Modulo 1-4
https://www.netacad.com/

BGP Commands
https://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfbgp1.html

Configuración y resolución de problemas half/full duplex para Ethernet 10/100/1000 Mb
https://www.cisco.com/c/es_mx/support/docs/lan-switching/ethernet/10561-3.html

SANS - Information Security Resources
https://www.sans.org/information-security/

Configuring HSRP
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html

IBM Knowledge Center - Conexiones T1/E1
https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_61/rzaiy/rzaiytone.htm