

**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

FACULTAD DE INGENIERIA

**“OPTIMIZACIÓN FÍSICA Y LÓGICA EN RED MPLS EXISTENTE”**

TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN TELECOMUNICACIONES

PRESENTA:

**EDUARDO JUÁREZ VELÁZQUEZ**

DIRECTOR DE TRABAJO

DR. MIGUEL MOCTEZUMA FLORES



CIUDAD UNIVERSITARIA NOVIEMBRE 2013

# ÍNDICE

[ÍNDICE 2](#_Toc376859459)

[1. OBJETIVO 3](#_Toc376859460)

[2. DEFINICIÓN DEL PROBLEMA 4](#_Toc376859461)

[3. ANTECEDENTES 5](#_Toc376859462)

[Modelo OSI 6](#_Toc376859463)

[4. MARCO TEORICO 10](#_Toc376859464)

[AAA 10](#_Toc376859465)

[BGP 12](#_Toc376859466)

[Penalización. 16](#_Toc376859467)

[MPLS 17](#_Toc376859468)

[OSPF 20](#_Toc376859469)

[Ping. 23](#_Toc376859470)

[Traceroute 23](#_Toc376859471)

[SSH 23](#_Toc376859472)

[SNMP 25](#_Toc376859473)

[PPDIOO 26](#_Toc376859474)

[5. ANÁLISIS Y METODOLOGÍA EMPLEADA 29](#_Toc376859475)

[Validaciones Previas 30](#_Toc376859476)

[Validación de direccionamiento IP y conectividad 36](#_Toc376859477)

[Redundancia de fuentes de poder y apagado de equipo 39](#_Toc376859478)

[*PRP(Performance Route Procesor)* Redundancia de supervisora 42](#_Toc376859479)

[OSPF 44](#_Toc376859480)

[BGP 47](#_Toc376859481)

[Dampening 49](#_Toc376859482)

[MPLS 52](#_Toc376859483)

[Ruteo IP 55](#_Toc376859484)

[Convergencia 57](#_Toc376859485)

[Administración 59](#_Toc376859486)

[6. PARTICIPACIÓN PROFESIONAL 61](#_Toc376859487)

[7. RESULTADOS Y APORTACIONES 62](#_Toc376859488)

[8. CONCLUSIONES 63](#_Toc376859489)

[9. BIBLIOGRAFÍA 65](#_Toc376859490)

ÍNDICE DE FIGURAS Y TABLAS

[Figure 3.1. Capas del modelo OSI 6](#_Toc376862862)

[Figure 4.1. Funcionamiento de Dampening 16](#_Toc376862863)

[Figure 4.2. Trayectoria de un paquete en una red MPLS 18](#_Toc376862864)

[Figure 4.3. Ciclo de vida de la red de acuerdo al modelo PPDIOO 28](#_Toc376862865)

[Table 5.1. Objetivos de las pruebas a realizar 30](#_Toc376863821)

[Table 5.2. Captura de show redundancy en un Switch para validación previa 31](#_Toc376863822)

[Table 5.3. Captura de show module en un Switch para validación previa 32](#_Toc376863823)

[Table 5.4. Captura de show diagbus en un Enrutador para validación previa 33](#_Toc376863824)

[Table 5.5. Captura de show power status all en un Switch para validación previa 34](#_Toc376863825)

[Table 5.6. Captura de show environment table en un Enrutador para validación previa 36](#_Toc376863826)

[Table 5.7. Resumen de resultados de la prueba 1 38](#_Toc376863827)

[Table 5.8. Captura de show ip interface brief en un Switch para comparación. 39](#_Toc376863828)

[Table 5.9. Resumen de resultados de la prueba 2 41](#_Toc376863829)

[Table 5.10. Captura de show power estatus all en un Switch para comparación. 42](#_Toc376863830)

[Table 5.11. Resumen de resultados de la prueba 3 44](#_Toc376863831)

[Table 5.12. Resumen de resultados de la prueba 4 46](#_Toc376863832)

[Table 5.13. Captura de los comandos de validación de OSPF en un Enrutador para comparación. 47](#_Toc376863833)

[Table 5.14. Resumen de resultados de la prueba 5. 48](#_Toc376863834)

[Table 5.15. Captura de show ip bgp vpnv4 all summary para comparación. 49](#_Toc376863835)

[Table 5.16. Resumen de resultados de la prueba 6 51](#_Toc376863836)

[Table 5.17. Captura de show interface dampening en un Enrutador para comparación. 52](#_Toc376863837)

[Table 5.18. Resumen de resultados de la prueba 7. 55](#_Toc376863838)

[Table 5.19. Captura de comandos de validación de MPLS en un Enrutador para comparación. 56](#_Toc376863839)

[Table 5.20. Resumen de resultados de la prueba 8. 57](#_Toc376863840)

[Table 5.21. Resumen de resultados de la prueba 9. 59](#_Toc376863841)

[Table 5.22. Resumen de resultados de la prueba 10. 61](#_Toc376863842)

# OBJETIVO

Realizar las pruebas necesarias para determinar el correcto funcionamiento de la red de *Conmutación Multi-Protocolo mediante Etiquetas* (MPLS, por sus siglas en inglés), que se encuentra funcionando en condiciones óptimas y que en caso de presentarse fallas se puedan corregir de manera proactiva.

# DEFINICIÓN DEL PROBLEMA

Actualmente la red del cliente utiliza infraestructura y tecnologías independientes para el tráfico de voz y datos tanto para el cliente como para usuarios internos. El propósito de este proyecto es construir una red convergente basada en la tecnología MPLS para transportar todo el tráfico de una manera eficiente, administrable y confiable.

Las pruebas estarán enfocadas en la verificación de redundancia física y lógica de la red, la revisión de la configuración, depuración de comandos innecesarios así como la aplicación de las mejores prácticas en la red.

El propósito de este documento es definir la información y los escenarios de prueba requeridos para verificar la correcta configuración de desempeño de los equipos que pertenecen a la parte nueva de MPLS de la red del cliente. Este *Plan de Pruebas de Aceptación* (*ATP)* comprende principalmente la verificación de las capas de distribución y acceso, estará enfocado en todos los sitios pertenecientes al Núcleo de MPLS y el principal objetivo es que el cliente pueda verificar y estar de acuerdo con la configuración y desempeño del equipo utilizado simulando fallas en un ambiente controlado.

# ANTECEDENTES

Día a día es más grande la cantidad de equipos que se conectan a la internet y más las redes locales que se crean en empresas, negocios y hogares. Para que una Red de Área Local (LAN) sea funcional, se requiere que se encuentre bien estructurada, jerarquizada y que cumpla con los objetivos de cada cliente.

### Modelo OSI

El modelo de *Interconexión de Sistemas Abiertos* (OSI) define claramente cómo la información es transferida entre los distintos componentes de red hasta llegar al usuario, la mayoría de los componentes de red funcionan dentro de las 3 ó 4 primeras capas de dicho modelo.

En 1984, la Organización Internacional para la Estandarización (ISO) desarrolló el modelo OSI para describir como la información es transferida de un componente de red a otro, desde el momento en que un usuario introduce información a través de cualquier interface hasta el punto en que se convierten en señales eléctricas.

El modelo OSI resulta muy útil para la explicación de cómo “platica” un dispositivo de red con otro además de ser de gran utilidad para la solución de problemas.



Figure 3.1. Capas del modelo OSI

El modelo OSI se resume en 7 capas, cada una con distintas funcionalidades, esto ayuda a los vendedores a entender cómo la información es manejada y transportada entre equipos de red así también sirve como guía para la implementación de nuevos estándares y tecnologías.

Capa 7, Aplicación.

Define la interface que un usuario utiliza para interactuar con la aplicación, dicha interface puede ser gráfica o línea de comandos. También se incluyen las aplicaciones que reaccionan de acuerdo a las necesidades de la red sin la necesidad de la intervención del usuario, aplicaciones inteligentes.

Capa 6, Presentación.

La capa de presentación es la responsable de definir cómo la información es transmitida y presentada al usuario en la interface que se esté utilizando. Define como es que las diferentes formas de textos, gráficos, video y/o audio son transmitidas al usuario de manera correcta por la capa de aplicación. Por ejemplo ASCII para presentación de textos o los diferentes formatos (GIF, JPEG, TIFF) que existen para la presentación de imágenes

Capa 5, Sesión.

En la capa de sesión se inician y terminan las conexiones entre componentes de red para eso debe determinar si los datos se pueden obtener de manera local o si se requiere hacer alguna consulta a algún servicio de red y es así que inicia la sesión. También es responsable de diferenciar entre los distintos tipos de conexión asegurando que los datos son enviados a través de la conexión correcta y enviados a la aplicación correspondiente

Capa 4, Transporte.

La cuarta capa del modelo es la capa de transporte, aquí se llevan a cabo los mecanismos para configuración, mantenimiento y cierre de una conexión de manera confiable o no confiable, en una conexión confiable, en caso de error el paquete se reenvía, en una conexión no confiable, sólo se envía un mensaje de error.

La diferencia con la capa de sesión es que esta última se encarga de lidiar con detalles como la duración de la sesión, notificaciones, paquetes de monitoreopara determinar el estatus de la conexión, mientras que la capa de transporte se encarga de los mecanismos para el movimiento de la información entre los dispositivos de red, segmentación y retransmisión de datos, así como definición del tamaño de las ventanas de transmisión para evitar saturar algún otro componente de la red.

Capa 3, Red.

La capa de red es donde se define la topología lógica de red mediante el uso de direcciones IP y permite la comunicación entre dispositivos que se encuentren en distintos segmentos de capa 2, es aquí donde se lleva a cabo la convergencia de las diferentes tecnologías de la capa de enlace como Ethernet, Anillos de Fibra (FDDI), Serial y *Anillo de símbolos* (Token Ring).

Para mover los paquetes entre dispositivos de diferentes redes se utilizan los *enrutadores*, que son los encargados de tomar las decisiones de cómo se llevará el tráfico, estos dispositivos crean sus tablas de ruteo mediante protocolos que les ayudan a conocer redes que se encuentran en otros dispositivos o bien, mediante rutas estáticas definidas de forma manual.

Capa 2, Enlace.

En la capa 2 del modelo OSI es donde se lleva a cabo la entrega de datos a través de direcciones físicas o de *Control de Acceso al Medio* (MAC addresses). Se define también como un componente de red accederá al medio y define el tipo de trama y el método de transmisión. Aquí también es donde se transforman las señales eléctricas (1 y 0) en tramas de datos además de realizarse una inspección y descartar las tramas dañadas.

Los equipos conectados al mismo segmento de red mediante el mismo tipo de acceso al medio se pueden comunicar entre sí, para comunicación entre distintos segmentos se utiliza un *enrutador.*

Capa 1, Física.

La capa física define las propiedades físicas para la conexión y comunicación, es también la responsable de los mecanismos físicos para la conexión de red como:

* + El tipo de interface y cables utilizados para la conexión de los dispositivos
  + Los conectores utilizados en cada extremo de los cables
  + El acomodo de los cables dentro de los conectores
  + El tipo de codificación usado para transmitir la representación de bits de acuerdo al tipo de medio, señal eléctrica en cobre, luz en fibra y ondas de radio para Dispositivos Inalámbricos (Wireless)

# MARCO TEÓRICO

Durante la aplicación de las pruebas, se hará uso de distintos protocolos y funcionalidades, algunos propietarios y algunos estándares, para poder entender el resultado esperado se anexa una breve explicación de cada uno de los protocolos y funcionalidades utilizadas.

### AAA

El control de acceso es la forma en la que se controla quién está permitido a obtener acceso al servidor de red y los servicios que están autorizados a utilizar una vez que tienen acceso. Los servicios de seguridad de red de Autenticación, *Autorización y Contabilidad* (*AAA*) proporcionan el marco principal por el que se establece el control de acceso en el enrutador o servidor de acceso.

AAA es un marco arquitectónico para la configuración de un conjunto de tres funciones de seguridad independiente de una manera consistente. AAA ofrece una forma modular de realizar los siguientes servicios:

* Autenticación. La autenticación es la forma de identificar a un usuario antes de que pueda acceder a la red y los servicios de ella. Se configura la autenticación AAA mediante la definición de una lista con métodos de autenticación, y luego se aplica esa lista a diversas interfaces. En la lista de métodos se definen los tipos de autenticación que se realizan y la secuencia en la que se llevarán a cabo, debe ser aplicada a una interface específica antes de llevar a cabo cualquiera de los métodos de autenticación definidos. La única excepción es la lista de método por default. La lista de método por default se aplica automáticamente a todas las interfaces si no hay lista de otro método está definido. Una lista de métodos definidos anula la lista de método por defecto.
* Autorización. AAA trabaja por reunir a un conjunto de atributos que describen lo que el usuario está autorizado a realizar. Estos atributos son comparados con la información contenida en una base de datos de un usuario determinado y el resultado se devuelve a la AAA para determinar las capacidades reales del usuario y las restricciones. La base de datos se puede encontrar localmente en el servidor de acceso, en el equipo de comunicaciones o puede ser organizada de forma remota en un servidor de seguridad RADIUS o TACACS+. Servidores remotos de seguridad, tales como RADIUS y TACACS+, autorizan a los usuarios los derechos específicos mediante la asociación de atributos pares de valor (AV), que definen los derechos con el usuario apropiado. Todos los métodos de autorización deben ser definidos a través de AAA.
* Contabilidad. Proporciona el método de recepción y envío de información de seguridad del servidor utilizado para la facturación, auditoría y presentación de informes, tales como las identidades de usuario, inicio y fin, los comandos ejecutados, el número de paquetes, y el número de bytes. Permite realizar un seguimiento de los usuarios tienen acceso a los servicios, así como la cantidad de recursos de la red que están consumiendo. Cuando la contabilidad de la AAA se activa, el acceso a la red del servidor informa de la actividad del usuario al servidor de seguridad RADIUS o TACACS+ (según el método de seguridad que han puesto en práctica) en la forma de registros contables. Cada registro contable se compone de la contabilidad de los pares de AV y se almacena en el servidor de control de acceso. Estos datos pueden ser analizados para la gestión de la red, la facturación del cliente y/o auditoría. Todos los métodos de contabilidad deben ser definido a través de AAA. Al igual que con la autenticación y autorización, se configura la contabilidad AAA mediante la definición de una lista con nombre de métodos de contabilidad y luego se aplica esa lista a diversas interfaces.

### BGP

BGP es lo que se conoce como un *Protocolo de Puerta de enlaces Externa (EGP),* destinados a ser utilizados entre diferentes redes. Es el protocolo utilizado en Internet. Fue construido para la confiabilidad, la escalabilidad y el control, no la velocidad. Debido a esto, se comporta de forma diferente a *Protocolos de Puerta de Enlace Interna* *(*IGP).

Características

* BGP significa *Border Gateway Protocol* o Protocolo de Puerta de enlace de Frontera
* BGP utiliza el concepto de sistemas autónomos. Un sistema autónomo es un conjunto de redes bajo una administración común.
* Los sistemas autónomos ejecutan *Protocolos de Puerta de enlace Interior* (IGP) en el sistema y corren un *Exterior Gateway Protocol* (EGP) entre ellos.
* BGP versión 4 es el único EGP que se utiliza actualmente a nivel mundial como protocolo de ruteo para internet
* Los vecinos de BGP se llaman *peers* y se deben configurar de forma estática.
* BGP utiliza el puerto TCP 179.
* BGP es un protocolo *path-vector*. Su ruta a una red consiste en una lista de los sistemas autónomos en la ruta a esa red.
* El mecanismo de prevención de bucle en BGP es el número de sistema autónomo.

Cuando hay una actualización acerca de una red deja un sistema autónomo, el número de sistema autónomo que se antepone a la lista de sistemas autónomos que han manejado esa actualización. Cuando un sistema autónomo recibe una actualización, se examina la lista de sistema autónomo. Si encuentra su propio número de sistema autónomo en esa lista, la actualización se descarta.

Bases de datos BGP

BGP utiliza tres bases de datos. Las dos primeras que se mencionan son específicas de BGP, y la tercera es compartida por todos los procesos de enrutamiento en el equipo:

* *Base de datos de vecinos*. Es una lista de todos los vecinos BGP configurados. Para verla, se utiliza el comando ***show ip bgp summary***.
* *Base de datos de información de rutas (*RIB, R*outing Information Database*) Esta es una lista de redes conocidas por BGP, junto con sus caminos y sus atributos. Para verla, se utiliza el comando ***show ip bgp***.
* Tabla de Ruteo. Esta es una lista de las rutas de acceso a cada red utilizada por el enrutador, y el *siguiente salto* para cada red. Para verla, se utiliza el comando ***show ip route***.

Tipos de mensajes BGP.

BGP tiene cuatro tipos de mensajes:

* *Open*. Después de que un vecino se ha configurado, BGP envía un mensaje de *open* para tratar de establecer *vecindad* con ese equipo. Incluye información como el número de sistema autónomo, ID del enrutador y el tiempo de espera.
* *Update*. Mensaje utilizado para transferir información de enrutamiento entre *vecinos.*
* *Keepalive*. Los *vecinos* de BGP intercambian mensajes de actividad (Keepalives) cada 60 segundos. Estos mantienen la sesión de BGP activa.
* *Notification*. Cuando ocurre un problema que causa que un enrutador finalice la sesión BGP, un mensaje de notificación se envía al vecino de BGP y se cierra la conexión.

BGP Interno y Externo.

BGP interno (IBGP). Se refiere a la existencia de adyacencia BGP entre enrutadores dentro del mismo sistema autónomo. BGP externo (EBGP) se conoce cuando se tiene adyacencia BGP entre enrutadores de diferentes sistemas autónomos. BGP trata de manera diferente las actualizaciones de vecinosinternos a las actualizaciones de vecinos externos.

Selección de *siguiente salto* enBGP.

El siguiente salto (*next-hop)* para una ruta recibida de un vecino EBGP es la dirección IP del vecino que envió la actualización. Cuando un enrutador BGP recibe una actualización de un vecino EBGP, debe pasar a la actualización en sus vecinos IBGP sin cambiar el atributo del siguiente salto. La dirección del siguiente salto IP es la dirección IP de un enrutador de frontera que pertenece al sistema autónomo del siguiente salto. Por lo tanto, los enrutadores IBGP deben tener una ruta a la red conectando su sistema autónomo hacia el enrutador de borde.

Regla de Sincronización BGP

La regla de sincronización de BGP requiere que cuando un enrutador BGP reciba información sobre una red de un vecino IBGP, no use esa información hasta que una ruta coincidente se aprenda a través de un IGP o una ruta estática. También no anuncia esa ruta a un vecino EBGP a menos que exista una ruta coincidente en la tabla de enrutamiento.

BGP Peering

BGP asume que los vecinos externos están directamente conectados y que están generando vecindad con la dirección IP de la interface directamente conectada de su vecino. Si no es así, debe decirle a BGP para ver más de un salto de distancia de su vecino, con el comando ***neighbor ip-address ebgp-multihop number-of-hops***. Se puede utilizar este comando si se están generando vecindades con direcciones IP de bucle invertido (*loopback)*, por ejemplo. BGP asume que los vecinos de internos no pueden ser conectados directamente, por lo que este comando no es necesario con IBGP.

### Penalización.

La función de Penalización (Dampening) en los equipos, muestra un mecanismo de penalización exponencial configurable que permite suprimir los efectos que puede causar el hecho de cambios constantes de estado (apagado/encendido) en una interface, efectos como: cambios en las topologías de red, en los protocolos de ruteo, en la manera de aprender direcciones MAC, etc.

Esta funcionalidad permite al operador de la red configurar ciertos parámetros de penalización en una interface que se encuentra cambiando de estado de manera continua.

Cada vez que una interface cambia de estado, se dispara un contador, dicho contador aumenta de manera exponencial de acuerdo al número de veces y frecuencia con que ocurra el cambio, al rebasar cierto límite, la interface queda “penalizada” y no se permitirá que lleve tráfico. Una vez que la interface se estabiliza, dicho contador empieza a disminuir, hasta que, una vez alcanzado un umbral de operación óptimo, la interface se vuelve a habilitar.

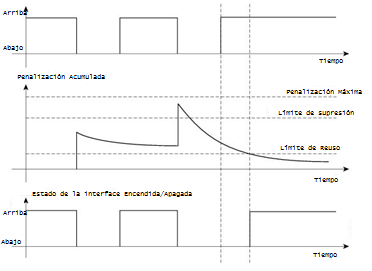


Figure 4.1. Funcionamiento de Dampening

### MPLS

La tecnología MPLS (MultiProtocol Label Switching) permite a las empresas y proveedores de servicio construir redes inteligentes de siguiente generación que permiten una amplia variedad de servicios avanzados (IP, Frame Relay, ATM o Ethernet) sobre una misma infraestructura. Clientes con diferentes enlaces de acceso se pueden agregar a la red ya que MPLS es independiente de las diferentes tecnologías de acceso.

MPLS es un método mejorado para el envío de paquetes a través de una red usando la información contenida en etiquetas contenidos dentro del paquete IP, dichas etiquetas se insertan entre los encabezados de capa 2 y 3. MPLS combina las tecnologías de *Conmutación* capa 2y de *Ruteo* en capa 3. El objetivo principal de MPLS es crear una red flexible que ofrezca estabilidad y buen desempeño, el cual incluye ingeniería de tráfico y Redes Privadas Virtuales (VPNs) que puedan brindar calidad de servicio (QoS) con múltiples clases de servicio.

En una red MPLS, los paquetes entrantes se etiquetan en el enrutador de frontera y son enviados a lo largo de un trayecto de enrutadores que basan sus decisiones de envío del paquete en el contenido de la etiqueta, en cada enrutador por el que pasa el paquete se cambia la etiqueta, indicándole al siguiente enrutador el camino a tomar, finalmente el paquete se desetiqueta en el último enrutador de frontera y entregado a su destino.

En la figura se observa el proceso de entrada de un paquete al *enrutador* de frontera (*Edge LSR*) el camino que sigue a través de la red y la entrega de dicho paquete ya sin etiquetas

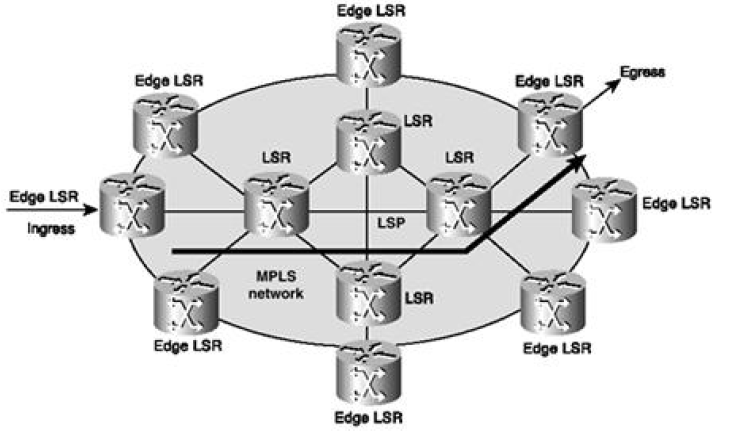


Figure 4.2. Trayectoria de un paquete en una red MPLS

Beneficios de MPLS.

El método de Conmutación de etiquetas en el que está basado MPLS permite a los enrutadores tomar decisiones de acuerdo al contenido de una etiqueta en lugar de realizar una compleja búsqueda basada en la dirección IP de destino. Esta técnica provee varios beneficios a las redes IP:

* + - VPN. Los proveedores de servicios pueden crear VPN de capa 3 a lo largo del *núcleo* de la red para múltiples usuarios sin necesidad de encriptación para aplicaciones de cliente final.
    - Ingeniería de tráfico. Provee la habilidad de definir de manera explícita uno o varios caminos a través de los cuales puede viajar la información en la red. También provee la habilidad para definir el comportamiento de cierto tipo de tráfico con lo cual se optimiza el ancho de banda de los enlaces con menos carga.
    - Calidad de Servicio. Los proveedores de servicios pueden proveer múltiples clases de servicio con la calidad de servicio garantizada con sus clientes VPN.

MPLS combina el desempeño y capacidades de un modelo de capa 2, con la escalabilidad probada de capa 3. Esto permite a los proveedores de servicios enfrentar los retos de una red en crecimiento mientras ofrece la oportunidad de diferenciar entre los diferentes tipos de servicios sin sacrificar la infraestructura de red ya existente.

### OSPF

El protocolo OSPF o *Primero la Ruta Libre Más Corta* Es un protocolo de estándar abierto de rápida convergencia, de tipo *sin clase* que toma como base el ancho de banda para definir el costo que utiliza como métrica.

OSPF se basa en el algoritmo de primero camino más corto de Dijkstra para determinar el mejor camino a cada red, es responsabilidad del enrutador de estado del enlace crear la base de datos que refleje la estructura de la red. Los protocolos de ruteo del estado del enlace proveen más información de la estructura de la red que otros protocolos y permiten realizar mejores decisiones de ruteo.

Los enrutadores de OSPF intercambian *saludos* con todos sus vecinos en los cuales comparten su *Identificador* (ID) y el costo del enlace, la información de los vecinos se mantiene en la tabla de adyacencias.

Posteriormente el enrutador construye el *Anuncio del estado del enlace (LSA)* el cual incluye información como los Identificadores del *Enrutador (RID)* de cada vecino y el costo para alcanzarlo, posteriormente comparte dicho *LSA* con cada uno de los enrutadores y cada enrutador genera su propia base de datos de *LSA* conocida como *Base de Datos del Estado del Enlace (LSDB)*.

Existen diferentes tipos de LSA y se clasifican según su función:

* + - *Tipo 1, Router LSA*. Los LSA tipo 1 anuncian rutas intra-area, cada enrutador los genera y se propagan únicamente dentro del área.
    - *Tipo 2 Network LSA*. Anuncian rutas en un enlace multiacceso, se generan por un DR y sólo se propagan dentro del área.
    - *Tipo 3 Summary LSA*. Anuncian rutas inter-area, se generan por un ABR y se distribuyen en las áreas adyacentes.
    - *Tipo 4 Summary LSA*. Anuncian rutas a ASBR y se generan en el ABR distribuyéndose a las áreas adyacentes.
    - *Tipo 5 External LSA*. Anuncian rutas generadas en otro dominio de ruteo, se anuncian por un ASBR y distribuido a las áreas adyacentes.
      * *E1*. La métrica se incrementa en cada enrutador mientras pasa por la red.
      * *E2*. La métrica se mantiene, este es valor por default.
    - *Tipo 6 Multicast LSA.* Utilizado en operaciones multicast de OSPF.
    - *Tipo7 Not-so.stubby area (NSSA) LSA.* Anuncia rutas generadas en otro dominio de ruteo siempre y cuando el ASBR se encuentre dentro de una NSSA.
      * *N1.* La métrica se incrementa conforme pasa a lo largo de la red.
      * *N2.* La métrica se conserva durante la trayectoria.
    - *Tipo 8 External Attributes LSA.* Utilizado para convivencia entre OSPF y BGP.
    - *Tipo 9, 10, 11 Opaque LSA.* Utilizado para aplicaciones específicas como convivencia entre OSPF y MPLS.

El dominio de OSPF se divide en áreas para mejorar la eficiencia ya que con ello se logra minimizar el número de rutas aprendidas en cada enrutador, disminuir el flujo de *LSA*, minimiza el impacto de un cambio en la topología y refuerza el concepto de red Jerárquica.

Cualquier dominio de OSPF debe tener un área 0 y todas las áreas deben estar conectadas a dicha área ya que es un área de tránsito, la *LSDB*, deberá ser exactamente la misma en todos los enrutadores pertenecientes a un área y se recomienda no tener más de 100 enrutadores en un área.

Los tipos de áreas que se manejan en OSPF son los siguientes:

* + - Área Central. Área 0, área donde se conectan todas las demás áreas, área de tránsito.
    - *Área Regular.* Área diferente al área 0 cuya base de datos contiene rutas internas y externas.
    - *Área apéndice.* En su base de datos sólo tiene rutas internas y una ruta por Default
    - *Área Totalmente apéndice.* Designación de área propietaria del Proveedor, su base de datos sólo contiene rutas del área y una ruta por default.
    - *Área no tan Apéndice (NSSA).* En su base de datos se encuentran rutas internas, **rutas redistribuidas** de un proceso de ruteo y de manera opcional una ruta por default.
    - *Área Totalmente no tan Apéndice.* Designación de área propietaria del Proveedor, su base de datos sólo contiene rutas del área, **rutas redistribuidas** de un proceso de ruteo y una ruta por default.

Los enrutadores también se denominan de diferentes maneras según su lugar en la red.

* + - *Enrutadores internos*. Tienen todas sus interfaces dentro de la misma área.
    - *Enrutadores centrales*. Tienen al menos una de sus interfaces dentro del área 0
    - *Enrutador de frontera de área*. Tienen interfaces en 2 ó más áreas.
    - *Enrutador de Frontera de Sistema Autónomo.* Tienen interfaces fuera del dominio de OSPF, ya sea en otro protocolo de ruteo o en otro proceso de OSPF.

Cuando se lleva a cabo la planeación de una implementación de OSPF se debe tener en cuenta detalles como la topología exacta a la que se quiere llegar, las redes que se van a anunciar, números de proceso OSPF, equipos que se configurarán y los posibles cambios requeridos en las métricas de las interfaces.

### Ping.

El ping es un método muy común de solución de problemas y validación de conectividad dentro de una red, utiliza una serie de mensajes de *Protocolo de control de mensajes de Internet (*ICMP) para determinar si un cliente se encuentra activo, el tiempo de retraso en un enlace y la pérdida de paquetes.

El ping envía primero una solicitud hacia una dirección y posteriormente espera una respuesta, el ping es exitoso si la solicitud llega adecuadamente al destino y el destino es capaz de enviar la respuesta de regreso a la fuente dentro del tiempo de vida del mismo, por lo general 2 segundos.

### Traceroute

Herramienta de diagnóstico de red que sirve para determinar la ruta y los retrasos que se tienen para alcanzar un dispositivo destino a lo largo de una red.

Al ejecutar el comando traceroute, se envían paquetes hacia el destino con el *Tiempo de Vida* (TTL) incrementándose de manera continua hasta llegar al máximo de 30, cuando un enrutador en medio de la red encuentra un paquete con TTL=1, responde con un mensaje ICMP *time exceed* al origen el cuál le permite saber a la equipo origen que el paquete atravesó ese enrutador en particular.

### SSH

*Protocolo Secure Shell* Se define en los RFC 4250 (Asignación de número de protocolo), 4251 (arquitectura del protocolo), 4252 (el protocolo de autenticación SSH) y 4253 (El protocolo de capa de transporte SSH) de la IETF como un protocolo para acceso remoto seguro y otros servicios de red sobre una red no segura. Funciona a nivel de la capa de transporte y ofrece un túnel autenticado para la conexión con el protocolo SSH. También asume que las capas inferiores ofrecen protección de integridad y confidencialidad.

El protocolo SSH consiste de tres componentes mayores: el protocolo de capa de transporte que provee autenticación a nivel servidor, confidencialidad e integridad. El protocolo de autenticación de usuario que autentica al cliente con el servidor y el protocolo de conexión que multiplexa el túnel encriptado en varios canales lógicos.

El cliente envía una solicitud de servicio una vez que se ha establecido una conexión segura a nivel de la capa de transporte y se envía una segunda solicitud una vez que la autenticación de usuario está completa, esto permite a nuevos protocolos ser definidos y coexistir con los protocolos de SSH.

### SNMP

*Protocolo Simple de Administración de Red.* Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre equipos de red. Pertenece al conjunto de protocolos TCP/IP. SNMP permite a los administradores de red monitorear el desempeño de la red, encontrar y resolver problemas así como planear el crecimiento de la red.

SNMP comprende 3 elementos básicos:

* + - *Dispositivo Administrado (Managed Device).* Es el equipo de red que contiene el agente SNMP en una red administrada, dichos equipos colectan y almacenan información poniéndola disponible para su uso por SNMP.
    - *Agente.* Es un módulo de software que reside en un *managed device* y contiene la información recolectada de manera local y la traslada en un formato que sea compatible con SNMP.
    - *Sistema de Administración de Red(NMS).* Aplicación de administración SNMP que provee la cantidad de recursos de memoria y procesamiento requeridos para la administración de red. El NMS ejecuta aplicaciones que monitorean y controlan los *managed devices*.

SNMP consta de 3 versiones:

* + - SNMP Versión 1. Fue la primera implementación de SNMP, definía tablas altamente estructuradas que eran utilizadas para agrupar las instancias de objetos tabulares (objetos con múltiples variables). Las tablas están indizadas por lo que se puede modificar un renglón completo. En SNMPv1, el *NMS* realiza la solicitud y el *Managed Device* responde, el agente utiliza una operación de captura para informar, de manera asíncrona, al NMS de algún evento.
    - SNMP versión 2c. Basa su funcionamiento en SNMPv1, la diferencia radica en el hecho de que la captura generada tiene diferente formato para remplazar la captura de la versión 1, lo que permite que se pueda enviar y recibir información entre NMS.
    - SNMP versión 3. La versión 3 de SNMP provee algunas características de seguridad como autenticación, privacidad, autorización y control de acceso

### PPDIOO

El proveedor del equipo de comunicación define el ciclo de vida de una red en 6 fases:

* Preparación. La fase de preparación establece los requerimientos organizacionales y de negocio, desarrolla una estrategia de red y propone una arquitectura de alto nivel para soportar dicha estrategia. Se identifican las tecnologías soportadas por la arquitectura. Esta fase crea un perfil de negocio que permite establecer una justificación financiera para la estrategia de red.
* Planificación. La fase de Planificación identifica los requisitos de la red mediante la caracterización y evaluación de la red, realizando un análisis profundo de arquitecturas contra mejores prácticas y con miras al entorno operativo. Se desarrolla un plan de proyecto para administrar las tareas, responsables, metas, así como recursos para el diseño e implementación. Este plan de proyecto es seguido durante todas las fases del ciclo.
* Diseño. El diseño de la red se desarrolla sobre la base de los requisitos técnicos y de negocios obtenidos a partir de las fases anteriores. El diseño de la red proporciona una alta disponibilidad, confiabilidad, seguridad, escalabilidad y rendimiento. El diseño incluye diagramas de red y una lista de equipo. El plan del proyecto se actualiza con más información granular para su implementación. Después de que la fase de diseño es aprobado, la fase de Implementación se inicia.
* Implementación. El nuevo equipo es instalado y configurado en la fase de Implementación. Nuevos dispositivos reemplazan o aumentan la infraestructura existente. El plan del proyecto es seguido durante esta fase. Los cambios previstos en la red deben ser comunicado en las reuniones de control de cambios, con las autorizaciones necesarias para proceder. Cada paso en la implementación debe incluir una descripción, directrices detalladas de aplicación, el tiempo estimado para poner en práctica, los pasos del plan de retorno en caso de un fracaso, y cualquier otra información de referencia adicional. Se aplican los cambios, a la vez que son probados, antes de pasar a la fase de operación.
* Operación. La fase de operación mantiene el día a día de la salud operativa de la red. Operaciones incluyen la gestión y monitoreo de los componentes de la red, mantenimiento del ruteo, las actualizaciones de la administración, la gestión del rendimiento y **la identificación y corrección de fallas en la red**. Esta fase es la prueba final del diseño. Durante la operación, las estaciones de gestión de red deben supervisar la salud general de la red y generar *logs* cuando se alcanzan determinados umbrales.
* Optimización. La fase de optimización consiste en la gestión proactiva de la red mediante la **identificación y solución de los problemas antes de que afecten a la red**. La fase de optimización puede crear un diseño de red modificado si surgen demasiados problemas en la red, para mejorar los problemas de rendimiento, o para resolver problemas de aplicación. La exigencia de un diseño de la red lleva a modificar el inicio del ciclo de vida de la red.

Generalmente, después de que una red ha pasado de la fase de preparación hasta el final de la fase de operación y que es funcional, se inicia el apoyo a las actividades empresariales. Algún tiempo después, es necesario introducir nuevas funciones o nuevas políticas, o se tiene que escalar la red para soportar el crecimiento de los servicios y/o usuarios. En ese momento, la organización tiene que prepararse para anexar nueva tecnología y el ciclo de vida comienza de nuevo.

Siguiendo el ciclo de vida propuesto por el proveedor, se realizarán pruebas enfocadas en las fases 5 y 6 (Operación y Optimización) en una red ya implementada.

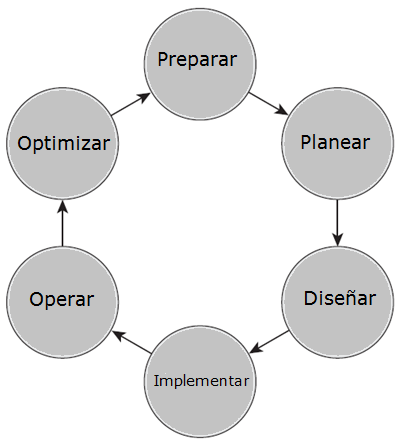


Figure 4.3. Ciclo de vida de la red de acuerdo al modelo PPDIOO

# ANÁLISIS Y METODOLOGÍA EMPLEADA

Plan de pruebas MPLS.

En la siguiente sección se describen los escenarios de prueba que se aplicarán para poder verificar la correcta operación y funcionamiento de la red así como sus elementos en los sitios de MPLS y medir el comportamiento y funcionamiento de la red y los protocolos de transporte.

En las siguientes pruebas se asegurará que las configuraciones de MPLS cumplen con lo estipulado en el documento de Bajo Nivel (LLD) así como asegurar que todo está configurado y funcionando como se espera

**Red MPLS**

Table 5.1. Objetivos de las pruebas a realizar

|  |  |
| --- | --- |
| **Objetivo** | El propósito de las pruebas a la red MPLS es verificar el rendimiento y métodos de recuperación de la solución interna MPLS. Las primeras pruebas consistirán en probar la red en condiciones regulares así como sus componentes. En las pruebas posteriores se someterá al equipo a diferentes pruebas de estrés para simular ambientes de falla para poder medir tiempos de recuperación y desempeño después de la falla. |
| **Resultados visibles.** | * Intercambio de Rutas. * Vecindades LDP/TDP. * Reenrutamiento en caso de falla * Convergencia IGP/EGP. |
| **Resultados Mesurables.** | * Retraso * Jitter * Tiempo de recuperación * Pérdida de paquetes * Tasa de transferencia   (con el uso de equipo analizador externo) |

Validaciones Previas:

Se utilizará el siguiente comando para validar en los Conmutadores (Switches):

* Ambas supervisoras cuentan con la misma versión de sistema operativo
* Una supervisora se encuentra en estado “active” y la otra en “standby hot”
* Se tiene el mismo valor de “configuration register” en ambas supervisoras

|  |
| --- |
| **#show redundancy** |
| Redundant System Information :  ------------------------------  Available system uptime = 15 weeks, 5 days, 14 hours, 12 minutes  Switchovers system experienced = 2  Standby failures = 0  Last switchover reason = user forced  Hardware Mode = Duplex  Configured Redundancy Mode = sso  Operating Redundancy Mode = sso  Maintenance Mode = Disabled  Communications = Up  Current Processor Information :  -------------------------------  Active Location = slot 5  Current Software state = ACTIVE  Uptime in current state = 15 weeks, 5 days, 13 hours, 49 minutes  Image Version = Cisco IOS Software, s72033\_rp Software (s72033\_ rp-ADVENTERPRISEK9\_WAN-M), Version 12.2(33)SXH5, RELEASE SOFTWARE (fc1)  Technical Support: http://www.cisco.com/techsupport  Copyright (c) 1986-2009 by Cisco Systems, Inc.  Compiled Thu 16-Apr-09 18:49 by prod\_rel\_team  BOOT = disk0:s72033-adventerprisek9\_wan-mz.122-33.SXH5.bin,1;  CONFIG\_FILE =  BOOTLDR =  Configuration register = 0x2102  Peer Processor Information :  ----------------------------  Standby Location = slot 6  Current Software state = STANDBY HOT  Uptime in current state = 15 weeks, 5 days, 13 hours, 48 minutes  Image Version = Cisco IOS Software, s72033\_rp Software (s72033\_rp-ADVENTERPRISEK9\_WAN-M), Version 12.2(33)SXH5, RELEASE SOFTWARE (fc1)  Technical Support: http://www.cisco.com/techsupport  Copyright (c) 1986-2009 by Cisco Systems, Inc.  Compiled Thu 16-Apr-09 18:49 by prod\_rel\_team  BOOT = disk0:s72033-adventerprisek9\_wan-mz.122-33.SXH5.bin,1;  CONFIG\_FILE =  BOOTLDR =  Configuration register = 0x2102 |

Table 5.2. Captura de show redundancy en un Switch para validación previa

Estatus (OK & PASS) de los módulos del switch

|  |
| --- |
| #sh module |
| Mod Ports Card Type Model Serial No.  --- ----- -------------------------------------- ------------------ -----------  1 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1010F3B4  2 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1012GWJA  3 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1010FFBY  4 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1009EPPC  5 2 Supervisor Engine 720 (Active) WS-SUP720-3BXL SAL09444JK2  6 2 Supervisor Engine 720 (Hot) WS-SUP720-3BXL SAD095003CM  8 4 CEF720 4 port 10-Gigabit Ethernet WS-X6704-10GE SAL1230YR02  Mod MAC addresses Hw Fw Sw Status  --- ---------------------------------- ------ ------------ ------------ -------  1 0016.c850.b438 to 0016.c850.b467 2.3 12.2(14r)S5 12.2(33)SXH5 Ok  2 0017.0eea.270c to 0017.0eea.273b 2.3 12.2(14r)S5 12.2(33)SXH5 Ok  3 0017.0e88.ef78 to 0017.0e88.efa7 2.3 12.2(14r)S5 12.2(33)SXH5 Ok  4 0017.0e88.bd14 to 0017.0e88.bd43 2.3 12.2(14r)S5 12.2(33)SXH5 Ok  5 0015.c69d.e234 to 0015.c69d.e237 4.3 8.1(3) 12.2(33)SXH5 Ok  6 0013.c3a7.cddc to 0013.c3a7.cddf 4.3 8.1(3) 12.2(33)SXH5 Ok  8 0022.55f7.f830 to 0022.55f7.f833 2.7 12.2(14r)S5 12.2(33)SXH5 Ok  Mod Sub-Module Model Serial Hw Status  ---- --------------------------- ------------------ ----------- ------- -------  1 Centralized Forwarding Card WS-F6700-CFC SAL1003AG3M 2.0 Ok  2 Centralized Forwarding Card WS-F6700-CFC SAL1005C2U6 2.0 Ok  3 Centralized Forwarding Card WS-F6700-CFC SAL1005C2U8 2.0 Ok  4 Centralized Forwarding Card WS-F6700-CFC SAL1005C6F3 2.0 Ok  5 Policy Feature Card 3 WS-F6K-PFC3BXL SAL09137G6P 1.6 Ok  5 MSFC3 Daughterboard WS-SUP720 SAL09412T6A 2.3 Ok  6 Policy Feature Card 3 WS-F6K-PFC3BXL SAD094004F0 1.6 Ok  6 MSFC3 Daughterboard WS-SUP720 SAD094608PL 2.3 Ok  8 Distributed Forwarding Card WS-F6700-DFC3CXL SAL1230Y3P1 1.1 Ok  Mod Online Diag Status  ---- -------------------  1 Pass  2 Pass  3 Pass  4 Pass  5 Pass  6 Pass  8 Pass |

Table 5.3. Captura de show module en un Switch para validación previa

* Estatus (OK) de los módulos y submódulos de los Routers

|  |
| --- |
| **#sh diags / sh diagbus** |
| SLOT 1 (RP/LC 1 ): Modular SPA Interface Card (10G)  MAIN: type 149, 68-3106-01 rev B0  Deviation: D092976  HW config: 0x60 SW key: 00-00-00  PCA: 73-10465-04 rev B0 ver 4  Design Release 1.0 S/N SAD122005ZF  MBUS: Embedded Agent  Test hist: 0x00 RMA#: 00-00-00 RMA hist: 0x00  DIAG: Test count: 0x00000000 Test results: 0x00000000  FRU: Linecard/Module: 12000-SIP-601=  Processor Memory: MEM-LC5-2048=(Non-Replaceable)  Packet Memory: MEM-LC5-PKT-512=(Non-Replaceable)  L3 Engine: 5 - ISE 10 Gbps  MBUS Agent Software version 2.69 (RAM) (ROM version is 3.4)  ROM Monitor version 255.255  Fabric Downloader version used 4.8 (ROM version is 255.255)  Primary clock is CSC 1  Board is analyzed  Board State is Line Card Enabled (IOS RUN )  Insertion time: 28w1d (21w6d ago)  Processor Memory size: 2147483648 bytes  TX Packet Memory size: 268435456 bytes, Packet Memory pagesize: 32768 bytes  RX Packet Memory size: 268435456 bytes, Packet Memory pagesize: 32768 bytes  0 crashes since restart  SPA Information:  subslot 1/0: SPA-1X10GE-L-V2 (0x50C), status is ok  subslot 1/1: SPA-2XOC48POS/RPR (0x46F), status is ok  subslot 1/2: Empty  subslot 1/3: Empty  High Speed SPA allowed in subslot 1/2 and 1/3: No  SUBSLOT 1/0 (SPA-1X10GE-L-V2): 1-port 10 Gigabit Ethernet Shared Port Adapter XFP based  Product Identifier (PID) : SPA-1X10GE-L-V2  Version Identifier (VID) : V02  PCB Serial Number : JAE1219HC03  Top Assy. Part Number : 68-2614-02  Top Assy. Revision : C0  Hardware Revision : 1.2  CLEI Code : IPUIA5VRAA  Insertion Time : 28w1d (21w6d ago)  Operational Status : ok |
|  |

Table 5.4. Captura de show diagbus en un Enrutador para validación previa

* Estatus (OK & On) de las Fuentes de poder en los switches

|  |
| --- |
| **# sh power status all** |
| Power-Capacity PS-Fan Output Oper  PS Type Watts A @42V Status Status State  ---- ------------------ ------- ------ ------ ------ -----  1 PWR-4000-DC 3806.46 90.63 OK OK on  2 PWR-4000-DC 3806.46 90.63 OK OK on  Pwr-Allocated Oper  Fan Type Watts A @42V State  ---- ------------------ ------- ------ -----  1 WS-C6509-E-FAN 150.36 3.58 OK  Pwr-Requested Pwr-Allocated Admin Oper  Slot Card-Type Watts A @42V Watts A @42V State State  ---- ------------------ ------- ------ ------- ------ ----- -----  1 WS-X6748-GE-TX 325.50 7.75 325.50 7.75 on on  2 WS-X6748-GE-TX 325.50 7.75 325.50 7.75 on on  3 WS-X6748-GE-TX 325.50 7.75 325.50 7.75 on on  4 WS-X6748-GE-TX 325.50 7.75 325.50 7.75 on on  5 WS-SUP720-3BXL 328.44 7.82 328.44 7.82 on on  6 WS-SUP720-3BXL 328.44 7.82 328.44 7.82 on on  8 WS-X6704-10GE 362.46 8.63 362.46 8.63 on on |

Table 5.5. Captura de show power status all en un Switch para validación previa

* Estatus (OK) de las fuentes de poder en los Routers

|  |
| --- |
| **# sh environment table** |
| <Output Omitted>  Slot # Card Specifc Leds  16 MBUS-OK  17 MBUS-OK  18 MBUS-OK  19 MBUS-OK  20 MBUS-OK  24 MBUS-OK  25 MBUS-OK  28 BLOWER-OK  <Output Omitted>  Slot X: Card-type(96) = Performance Route Processor, Subtype(0) = None  Inlet temp sensor: Scanning is ENABLED  SHUT NA 700  CRIT NA 600  WARN NA 550  STATUS OK  RAW 24  ACTUAL 240  M/S/G 0 0 0x003DD400  Hotpoint temp sensor: Scanning is ENABLED  SHUT NA 750  CRIT NA 690  WARN NA 660  STATUS OK  RAW 28  ACTUAL 280  M/S/G 0 0 0x003DD3D8  Card 5v Hard disk supply: Scanning is ENABLED  SHUT NA NA  CRIT NA NA  WARN NA NA  STATUS OK  RAW 626  ACTUAL 5008  M/S/G 0 0 0x003DBBAC  Card 1.5v supply: Scanning is ENABLED  SHUT NA NA  CRIT NA NA  WARN NA NA  STATUS OK  RAW 374  ACTUAL 1496  M/S/G 0 0 0x003DBB3C  Card 1.6v supply: Scanning is ENABLED  SHUT NA NA  CRIT NA NA  WARN NA NA  STATUS OK  RAW 324  ACTUAL 1296  M/S/G 0 0 0x003DBA94  Card 1.8v supply: Scanning is ENABLED  SHUT NA NA  CRIT NA NA  WARN NA NA  STATUS OK  RAW 447  ACTUAL 1788  M/S/G 0 0 0x003DBAE8  Card 2.5v supply: Scanning is ENABLED  SHUT NA NA  CRIT NA NA  WARN NA NA  STATUS OK  RAW 620  ACTUAL 2480  M/S/G 0 0 0x003DBA40  Card 3.3v supply: Scanning is ENABLED  SHUT NA NA  CRIT 2900 3600  WARN 2950 3500  STATUS OK  RAW 814  ACTUAL 3256  M/S/G 0 0 0x003DB4C4  Card 5v supply: Scanning is ENABLED  SHUT 4400 5600  CRIT 4700 5200  WARN 4800 5150  STATUS OK  RAW 623  ACTUAL 4984  M/S/G 0 0 0x003DC1F8  MBUS 5V supply: Scanning is ENABLED  SHUT 4400 5600  CRIT 4500 5500  WARN 4700 5300  STATUS OK  RAW 630  ACTUAL 5040  M/S/G 0 0 0x003DB364 |

Table 5.6. Captura de show environment table en un Enrutador para validación previa

**Si todas las validaciones resultan exitosas, se procede a continuar con el ATP**

**Prueba No. 1**

Validación de direccionamiento IP y conectividad

**Propósito:** Asegurar que el equipo está configurado con el correcto direccionamiento IP y que tiene conectividad a otros equipos.

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1
* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2
* SWITCH\_ACCESO\_1
* SWITCH\_ACCESO\_2

**Procedimiento:**

* 1. Ingresar al equipo vía SSH.
  2. Entrar a modo privilegiado con el comando ***enable*.**
  3. Escribir el siguiente comandos para ver las direcciones IP de las interfaces así como el estatus de las mismas:
     + ***show ip interface brief.***
  4. Realizar Ping a los equipos conectados asegurando que se puedan alcanzar.
  5. Realizar conexiones SSH a todos los demás equipos para probar conectividad IP desde este equipo.

**Revisión:**

* Verificar la salida de los comandos ***show ip interface brief*** *y* comparar las direcciones IP configuradas contra las IP de la base de datos, verificar que cada dirección está correctamente asignada a la interface correspondiente y que el estado de la interface sea *up/up*.

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

Verificar que se pueden realizar conexiones SSH a todos los dispositivos.

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

**Resultados esperados:** Cada dirección IP está correctamente asignada a su interface y el estatus es up/up en las interfaces productivas y se llega por SSH al resto de los equipos.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.7. Resumen de resultados de la prueba 1

|  |
| --- |
| **Ejemplo** |
| Router#**sh ip int br**  Interface IP-Address OK? Method Status Protocol  GigabitEthernet0/0/0 10.224.150.1 YES NVRAM up up  GigabitEthernet0/0/1 10.255.248.1 YES NVRAM up up  GigabitEthernet0/0/2 unassigned YES NVRAM up up  GigabitEthernet0/0/2.9 192.168.199.13 YES NVRAM up up  Gi0/0/2.17 10.220.128.194 YES NVRAM up up  Gi0/0/2.18 10.220.128.210 YES NVRAM up up  Gi0/0/2.61 10.226.129.129 YES NVRAM up up  Gi0/0/2.62 10.255.19.34 YES NVRAM up up  Gi0/0/2.100 10.232.192.82 YES NVRAM up up  Gi0/0/2.101 10.232.200.162 YES NVRAM up up  Gi0/0/2.102 10.192.13.2 YES NVRAM up up  Gi0/0/2.103 10.192.14.2 YES NVRAM up up  Gi0/0/2.104 10.192.15.2 YES NVRAM up up  Gi0/0/2.105 10.192.17.2 YES NVRAM up up  Gi0/0/2.106 10.192.19.2 YES NVRAM up up  Gi0/0/2.107 10.192.22.2 YES NVRAM up up  Gi0/0/2.108 10.192.25.2 YES NVRAM up up  Gi0/0/2.109 10.192.3.2 YES NVRAM up up  Gi0/0/2.113 10.192.4.2 YES NVRAM up up  Gi0/0/2.114 10.192.5.3 YES NVRAM up up  Gi0/0/2.115 10.192.9.2 YES NVRAM up up  Gi0/0/2.116 192.9.200.2 YES NVRAM up up  Gi0/0/2.117 192.9.218.2 YES NVRAM up up  Gi0/0/2.119 10.192.39.3 YES NVRAM up up  Gi0/0/2.307 unassigned YES unset administratively down down  Gi0/0/2.331 10.192.7.2 YES NVRAM up up  Gi0/0/2.332 10.192.7.130 YES NVRAM up up  Gi0/0/2.345 10.192.38.2 YES NVRAM up up  Gi0/0/2.346 10.192.38.131 YES NVRAM administratively down down  Gi0/0/2.511 10.225.158.1 YES NVRAM up up  Gi0/0/2.521 10.225.133.3 YES NVRAM up up  Gi0/0/2.689 10.226.130.2 YES NVRAM up up  Gi0/0/2.701 10.192.1.1 YES NVRAM up up  Gi0/0/2.702 10.192.1.5 YES NVRAM up up  Gi0/0/2.703 10.192.1.9 YES NVRAM up up  Gi0/0/2.898 192.168.199.121 YES NVRAM up up  Gi0/0/2.900 10.220.128.6 YES NVRAM up up  Gi0/0/2.901 10.220.128.17 YES NVRAM up up  Gi0/0/2.904 10.220.254.1 YES NVRAM up up  Gi0/0/2.905 10.220.254.41 YES NVRAM up up  Gi0/0/2.906 10.220.254.49 YES NVRAM up up  Gi0/0/2.910 10.220.128.33 YES NVRAM up up  Gi0/0/2.912 10.220.128.89 YES NVRAM up up  Gi0/0/2.914 10.220.128.137 YES NVRAM up up  Gi0/0/2.916 10.220.128.121 YES NVRAM up up  Gi0/0/2.918 10.220.128.153 YES NVRAM up up  Gi0/0/2.920 10.220.254.33 YES NVRAM up up  Gi0/0/2.923 10.220.128.105 YES NVRAM up up  Gi0/0/2.925 10.232.211.33 YES NVRAM up up  Gi0/0/2.950 10.220.139.1 YES NVRAM up up  Gi0/0/2.952 10.220.67.33 YES NVRAM up up  Gi0/0/2.957 10.220.65.33 YES NVRAM up up  Gi0/0/2.959 10.202.35.241 YES manual up up  GigabitEthernet0/0/3 10.255.248.13 YES NVRAM up up  GigabitEthernet0/0/4 unassigned YES NVRAM administratively down down  GigabitEthernet0/0/5 10.255.248.21 YES NVRAM administratively down down  GigabitEthernet0/0/6 10.255.248.25 YES NVRAM administratively down down  Gi0/0/6.1116 unassigned YES unset deleted down  Gi0/0/6.1145 unassigned YES unset administratively down down  GigabitEthernet0/0/7 10.255.248.5 YES NVRAM up up  GigabitEthernet0/0/8 10.255.248.9 YES NVRAM administratively down down  GigabitEthernet0/0/9 unassigned YES NVRAM up up  Gi0/0/9.105 10.255.248.246 YES NVRAM up up  GigabitEthernet1/0/0 unassigned YES NVRAM up up  Gi1/0/0.1116 unassigned YES NVRAM deleted down  Gi1/0/0.1119 10.222.7.53 YES NVRAM up up  Gi1/0/0.1121 10.240.7.53 YES NVRAM up up  Gi1/0/0.1122 10.240.135.53 YES NVRAM up up  Gi1/0/0.1145 10.223.7.53 YES manual up up  GigabitEthernet1/0/1 unassigned YES NVRAM administratively down down  GigabitEthernet1/0/2 unassigned YES NVRAM administratively down down  GigabitEthernet1/0/3 unassigned YES NVRAM administratively down down  GigabitEthernet1/0/4 unassigned YES NVRAM administratively down down  Loopback0 10.255.9.36 YES NVRAM up up  Loopback1 10.255.254.191 YES NVRAM up up  Loopback678 10.192.35.2 YES NVRAM administratively down down  Ethernet0 unassigned YES NVRAM administratively down down  Ethernet1 unassigned YES NVRAM administratively down down  Ethernet2 unassigned YES NVRAM administratively down down  Router#telnet 131.108.28.9  login:user2  Password:  Router> |

Table 5.8. Captura de show ip interface brief en un Switch para comparación.

**Prueba No. 2**

Redundancia de fuentes de poder y apagado de equipo

**Propósito:** Asegurar que las fuentes de poder funcionan correctamente de manera redundante y/o compartida

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1
* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2
* SWITCH\_ACCESO\_1
* SWITCH\_ACCESO\_2

**Procedimiento:**

1. Identificar las posiciones asignadas a las fuentes de poder en el Bastidor de fuerza.
2. Escribir el siguiente comando para validar el estatus de las Fuentes en los Switches:

***show power status all***

1. Escribir el siguiente comando para validar el estatus de las Fuentes en los Routers:

***show environment power-supply***

1. Apagar el breaker asignado a la fuente B del equipo que se está probando.
2. Verificar log de apagado de fuente y que el equipo siga funcionando correctamente.
3. Encender nuevamente el breaker y verificar que el equipo reconozca el encendido de la fuente de poder.
4. Repetir pasos 4 al 6 con la fuente A del equipo.
5. Reiniciar el equipo.

**Revisión:**

* Verificar en la salida del comando ***show ip interface brief***que el estado de las interfaces sea up/up, sin intermitencia en el equipo.

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

**Revisión:**

* El equipo inicia correctamente después del reinicio físico.

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

**Resultados esperados.** No se presentan intermitencias en los equipos, servicios ni interfaces durante una prueba de simulación de falla eléctrica. Todos los servicios levantan correctamente y no hay fallas de hardware.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.9. Resumen de resultados de la prueba 2

|  |
| --- |
| **Ejemplo** |
| Router# **sh power status all**  Power-Capacity PS-Fan Output Oper  PS Type Watts A @42V Status Status State  ---- ------------------ ------- ------ ------ ------ -----  1 PWR-4000-DC 3806.46 90.63 OK OK on  2 PWR-4000-DC 3806.46 90.63 OK OK on  Pwr-Allocated Oper  Fan Type Watts A @42V State  ---- ------------------ ------- ------ -----  1 WS-C6509-E-FAN 150.36 3.58 OK  Pwr-Requested Pwr-Allocated Admin Oper  Slot Card-Type Watts A @42V Watts A @42V State State  ---- ------------------ ------- ------ ------- ------ ----- -----  1 WS-X6548-GE-TX 142.80 3.40 142.80 3.40 on on  2 WS-X6548-GE-TX 142.80 3.40 142.80 3.40 on on  3 WS-X6148A-GE-45AF 112.56 2.68 112.56 2.68 on on  4 WS-X6548-GE-TX 125.16 2.98 125.16 2.98 on on  5 WS-SUP720-3BXL 328.44 7.82 328.44 7.82 on on  6 WS-SUP720-3BXL 328.44 7.82 328.44 7.82 on on  7 WS-X6704-10GE 362.46 8.63 362.46 8.63 on on |

Table 5.10. Captura de show power estatus all en un Switch para comparación.

**Prueba No. 3**

*PRP(Performance Route Procesor)* Redundancia de supervisora

**Propósito:** Asegurar que la redundancia opere correctamente en los equipos que tengan dos tarjetas supervisoras instaladas.

**Equipos donde se implementará:**

* SWITCH\_ACCESO\_1
* SWITCH\_ACCESO\_2

**Procedimiento:**

1. Escribir el siguiente comando para validar el estatus de las tarjetas supervisoras:

***show redundancy***

1. Abrir una ventana nueva en la terminal desde la que se están realizando las pruebas.
2. Desde la nueva ventana, realizar un ping continuo hacia la interface de *loopback* del equipo que se está probando.
3. Aplicar el siguiente comando en el equipo:

***redundancy force-switchover***

1. Verificar la cantidad de paquetes que se pierden en la ventana donde se está tirando el ping continuo.
2. Revisar de nuevo el estado de las supervisoras con el comando:

***show redundancy***

1. Una vez que la tarjeta que se forzó a reiniciarse tome el estado de “STANDBY HOT” repetir los pasos 4 al 6.

**Revisión:**

* Verificar que en las dos ocasiones que se realiza el *switchover*, la tarjeta redundante quede en estado ”*STANDBY* *HOT*” y que no haya afectación en el resto del equipo ni en sus conexiones.

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

**Resultados esperados.**

No se presentan intermitencias en los equipos, servicios ni interfaces durante una prueba de simulación de falla en tarjetas supervisoras.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.11. Resumen de resultados de la prueba 3

**Prueba No. 4**

OSPF

**Propósito:** Verificar el correcto funcionamiento y configuración del proceso de OSPF con la finalidad de validar IGP.

**Equipos donde se implementará:**

* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2

**Procedimiento:**

1. Escribir el siguiente comando para validar que existan rutas en el proceso de OSPF:

***show ip route ospf 65000***

1. Escribir el siguiente comando para validar la base de datos de OSPF

***show ip ospf 65000***

1. Escribir el siguiente comando para validar la vecindad y adyacencias de OSPF

***show ip ospf neighbor***

**Revisión:**

De lo desplegado por el comando ***show ip route ospf 65000*** asegurar que cada ruta está incluida en la tabla RIB (Routing Information Base)

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |

**Resultados esperados.**

* 1. Se debe tener un *next-hop­* para cada ruta aprendida por OSPF
  2. El *router\_id* del proceso de OSPF es la dirección de loopback del equipo
  3. La vecindad de OSPF debe estar en *FULL* en todos los equipos, presente y alcanzable a través de alguna interface.

|  |  |
| --- | --- |
| **Tabla de resultados de la prueba** | |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.12. Resumen de resultados de la prueba 4

|  |
| --- |
| **Ejemplo** |
| Router# **sh ip route ospf 65000**  10.0.0.0/8 is variably subnetted, 630 subnets, 8 masks  O 10.255.254.11/32 [110/91] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.249.12/30 [110/83] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.241.4/30 [110/106] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.248.12/30 [110/83] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.240.4/30 [110/100] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.220.40/30 [110/140] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.251.12/30 [110/81] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.250.12/30 [110/84] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.242.4/30 [110/96] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.249.8/30 [110/83] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.244.4/30 [110/102] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.32.208/30 [110/76] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.251.8/30 [110/80] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.247.4/30 [110/96] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.250.8/30 [110/88] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.246.4/30 [110/92] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.249.4/30 [110/89] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.245.8/30 [110/128] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.241.12/30 [110/166] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.226.128.96/27 [110/89] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.248.4/30 [110/89] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.244.8/30 [110/92] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.240.12/30 [110/90] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.251.4/30 [110/80] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.247.8/30 [110/106] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.243.12/30 [110/78] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.250.4/30 [110/88] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.246.8/30 [110/86] via 10.255.245.50, 01:06:08, POS0/1/0  O 10.255.249.0/30 [110/89] via 10.255.245.50, 01:06:08, POS0/1/0  Router# **sh ip ospf 65000**  Routing Process "ospf 65000" with ID 10.255.6.44  Start time: 00:00:36.552, Time elapsed: 1y14w  Supports only single TOS(TOS0) routes  Supports opaque LSA  Supports Link-local Signaling (LLS)  Supports area transit capability  Enrutador is not originating router-LSAs with maximum metric  Initial SPF schedule delay 50 msecs  Minimum hold time between two consecutive SPFs 50 msecs  Maximum wait time between two consecutive SPFs 5000 msecs  Incremental-SPF disabled  Initial LSA throttle delay 0 msecs  Minimum hold time for LSA throttle 20 msecs  Maximum wait time for LSA throttle 5000 msecs  Minimum LSA arrival 20 msecs  LSA group pacing timer 240 secs  Interface flood pacing timer 33 msecs  Retransmission pacing timer 66 msecs  Number of external LSA 5. Checksum Sum 0x31A46  Number of opaque AS LSA 0. Checksum Sum 0x0  Number of DCbitless external and opaque AS LSA 0  Number of DoNotAge external and opaque AS LSA 0  Number of areas in this enrutador is 1. 1 normal 0 stub 0 nssa  Number of areas transit capable is 0  External flood list length 0  IETF NSF helper support enabled  Cisco NSF helper support enabled  Reference bandwidth unit is 10000 mbps  BFD is enabled  Area BACKBONE(0)  Number of interfaces in this area is 4 (1 loopback)  Area has message digest authentication  SPF algorithm last executed 01:04:51.316 ago  SPF algorithm executed 274571 times  Area ranges are  Number of LSA 258. Checksum Sum 0x86763C  Number of opaque link LSA 0. Checksum Sum 0x0  Number of DCbitless LSA 0  Number of indication LSA 0  Number of DoNotAge LSA 0  Flood list length 0  Router#**sh ip ospf neig**  Neighbor ID Pri State Dead Time Address Interface  10.255.6.2 0 FULL/ - 00:00:33 10.255.245.58 POS0/1/0  10.255.6.44 0 FULL/ - 00:00:39 10.255.245.45 GigabitEthernet0/0/1  10.80.254.219 0 FULL/DROTHER 00:00:38 10.81.3.4 GigabitEthernet0/0/2.103  192.6.102.98 200 FULL/DR 00:00:36 10.81.3.2 GigabitEthernet0/0/2.103  10.80.254.219 0 FULL/ - 00:00:38 10.81.1.2 GigabitEthernet0/0/2.106  10.81.23.2 1 FULL/BDR 00:00:35 10.81.23.2 GigabitEthernet0/0/2.107  192.6.102.98 1 FULL/DROTHER 00:00:39 10.81.23.5 GigabitEthernet0/0/2.107 |

Table 5.13. Captura de los comandos de validación de OSPF en un Enrutador para comparación.

**Prueba No. 5**

BGP

**Propósito:** Verificar las configuraciones y funcionamiento de BGP.

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1
* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2

**Procedimiento:**

1. Escribir el siguiente comando para validar el funcionamiento de BGP:

***show ip bgp vpnv4 all summary***

**Revisión:**

* Verificar la salida de los comandos ingresados

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

**Resultados esperados.**

* 1. El *router\_id* del proceso de BGP es la dirección de loopback del equipo
  2. La vecindad de BGP debe estar mostrar el tiempo que lleva activa con todos los equipos, presente y con la IP del vecino.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.14. Resumen de resultados de la prueba 5.

|  |
| --- |
| **Ejemplo** |
| Router# **sh ip bgp vpnv4 all summary**  BGP router identifier 10.255.6.45, local AS number 64900  BGP table version is 8342798, main routing table version 8342798  8195 network entries using 1122715 bytes of memory  20293 path entries using 1379924 bytes of memory  3376 multipath network entries and 7081 multipath paths  1284/885 BGP path/bestpath attribute entries using 169488 bytes of memory  303 BGP rrinfo entries using 7272 bytes of memory  5 BGP AS-PATH entries using 120 bytes of memory  350 BGP extended community entries using 14084 bytes of memory  0 BGP route-map cache entries using 0 bytes of memory  0 BGP filter-list cache entries using 0 bytes of memory  BGP using 2693603 total bytes of memory  BGP activity 84835/76638 prefixes, 654969/634676 paths, scan interval 15 secs  Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd  10.255.0.191 4 64900 2128994 75356 8342798 0 0 4w6d 7219  10.255.0.192 4 64900 2251385 75356 8342798 0 0 4w6d 7146 |

Table 5.15. Captura de show ip bgp vpnv4 all summary para comparación.

**Prueba No. 6**

Dampening

**Propósito:** Verificar la configuración y correcto funcionamiento de la función de *dampening* en las interfaces.

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1
* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2

**Procedimiento:**

1. Seleccionar una interface para aplicar las pruebas, verificar que tenga los parámetros de dampening configurados y que el valor de  *Penalty* de la interface sea cero con los siguientes comandos.

***show run interface (número de la interface)***

***show interface dampening***

1. En modo de configuración de interface, aplicar de manera repetida el apagado y encendido de la misma y observar que se incremente el valor de *Penalty* hasta que el valor de *supp* cambie a TRUE y la interface quede apagada

***shutdown***

***no shutdown***

1. Revisar continuamente el valor de dampening hasta que se observe que el valor de *Penalty* sea menor al valor de *ReuseV* y el valor de *supp* regrese a *FALSE.*

***show interface dampening***

**Revisión:**

* La interface se bloquea cuando el valor de *Penalty* supera al valor de *SuppV*

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |

* La interface se desbloquea cuando el valor de *Penalty* es menor al valor de *ReuseV*

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

**Resultados esperados.**

1. La verificación inicial muestra los valores de *Penalty* en cero y los valores correctamente configurados
2. La interface se bloquea después de algunos reinicios de la misma debido a que se alcanzan valores de penalización
3. Transcurridos algunos minutos, se debe observar que la interface vuelve a trabajar de manera normal y que los valores de penalización disminuyen con el paso del tiempo.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.16. Resumen de resultados de la prueba 6

|  |
| --- |
| **Ejemplo** |
| Router# show interf dampening  GigabitEthernet1/0/1  Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart  0 0 FALSE 0 30 75 2000 240 19200 0  POS2/0/0  Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart  0 0 FALSE 0 30 75 2000 240 19200 0  Después de reiniciar 3 veces la interface POS2/0/0:  Router#show interface dampening  GigabitEthernet1/0/1  Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart  0 0 FALSE 0 30 75 2000 240 19200 0  POS2/0/0  Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart  3 2332 TRUE 150 30 75 2000 240 19200 0  Router# show run interface pos2/0/0  Building configuration...  Current configuration : 489 bytes  !  interface POS2/0/0  description “Enrutador 2”  dampening 30 75 2000 240  ip address 10.255.245.69 255.255.255.252  ip ospf message-digest-key 5 md5  ip ospf network point-to-point  <Se omiten algunos comandos para brevedad>  end**!** |

Table 5.17. Captura de show interface dampening en un Enrutador para comparación.

**Prueba No. 7**

MPLS

**Propósito:** Verificar que el etiquetado de MPLS se esté distribuyendo de manera correcta

**Equipos donde se implementará:**

* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2
* DISTRIBUCION\_SITIO\_1

**Procedimiento:**

1. Escribir el siguiente comando para validar que las interfaces involucradas en MPLS estén correctamente configuradas:

***show mpls interfaces***

1. Escribir el siguiente comando para verificar que el proceso de descubrimiento de rutas está activo y que se envían y reciben paquetes de forma correcta.

***show mpls ldp discovery***

1. Escribir el siguiente comando para validar que las interfaces conectadas se anuncien en cada vecino.

***show mpls ldp neighbor***

1. Escribir el siguiente comando para verificar el etiquetado de rutas.

***show mpls ldp bindings***

**Revisión:**

* Las interfaces están correctamente configuradas y corriendo LDP

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

* Se observan las interfaces en estatus “xmit/recv”

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

* Se observa que se establecen vecindades de LDP en las interfaces configuradas con LDP

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

* Se observan etiquetas en las rutas recibidas

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

**Resultados esperados.**

1. El estado de cada interface MPLS debe ser *Operational*
2. Las interfaces deben estar recibiendo y transmitiendo
3. La vecindad de MPLS debe estar en *up* en todas las interfaces.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.18. Resumen de resultados de la prueba 7.

|  |
| --- |
| **Ejemplo** |
| Router#**sh mpls interfaces**  Interface IP Tunnel Operational  GigabitEthernet0/0/1 Yes (ldp) No Yes  POS0/1/0 Yes (ldp) No Yes  Router#**sh mpls ldp discovery**  Local LDP Identifier:  10.255.6.45:0  Discovery Sources:  Interfaces:  GigabitEthernet0/0/1 (ldp): xmit/recv  LDP Id: 10.255.6.44:0  POS0/1/0 (ldp): xmit/recv  LDP Id: 10.255.6.2:0  Router#**sh mpls ldp neighbor**  Peer LDP Ident: 10.255.6.44:0; Local LDP Ident 10.255.6.45:0  TCP connection: 10.255.6.44.646 - 10.255.6.45.30059  State: Oper; Msgs sent/rcvd: 433498/433602; Downstream  Up time: 3w0d  LDP discovery sources:  GigabitEthernet0/0/1, Src IP addr: 10.255.245.45  Addresses bound to peer LDP Ident:  10.255.6.44 10.255.245.45 10.255.16.42 10.255.16.41  10.255.245.49  Peer LDP Ident: 10.255.6.2:0; Local LDP Ident 10.255.6.45:0  TCP connection: 10.255.6.2.646 - 10.255.6.45.62678  State: Oper; Msgs sent/rcvd: 292453/292589; Downstream  Up time: 2w0d  LDP discovery sources:  POS0/1/0, Src IP addr: 10.255.245.58  Addresses bound to peer LDP Ident:  10.255.6.2 10.255.220.89 10.255.245.58 10.255.245.18  Router#**show mpls ldp bindings**  10.34.0.0/8, rev 9  local binding: label: imp-null  remote binding: lsr: 10.155.0.55:0, label: 17  remote binding: lsr: 10.66.66.66:0, label: 18 |

Table 5.19. Captura de comandos de validación de MPLS en un Enrutador para comparación.

Ejemplo 5.11.

**Prueba No. 8**

Ruteo IP

**Propósito:** Verificar la conectividad a nivel de IP (capa 3) entre equipos de diferentes sitios.

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1

**Procedimiento:**

1. Realizar un ping extendido a la IP de *Loopback* de cualquier equipo remoto:

***hostname#****ping*

*Protocol [ip]:*

*Target IP address:* ***remote loopback0***

*Repeat count [5]: 1000*

*Datagram size [100]:*

*Timeout in seconds [2]:*

*Extended commands [n]: y*

*Source address or interface: loopback 0*

**Revisión:**

* Verificar que la *loopback* remota sea alcanzable por ping

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

**Resultados esperados.**

1. El equipo se debe alcanzar por ping, la latencia debe ser baja y no debe haber pérdida de paquetes

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.20. Resumen de resultados de la prueba 8.

**Prueba No. 9**

Convergencia

**Propósito:** Verificar que la pérdida en conectividad sea mínima en caso de falla de algún enlace o de pérdida total de algún equipo.

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1

**Procedimiento:**

1. Realizar un *traceroute* hacia la IP de *loopback* con la que se hizo la prueba de *IP Routing,* anotar la ruta obtenida.
2. Realizar un ping extendido hacía la *Loopback con la que se han estado realizando las pruebas*.

***hostname#****ping*

*Protocol [ip]:*

*Target IP address:* ***remote loopback0***

*Repeat count [5]: 1000*

*Datagram size [100]:*

*Timeout in seconds [2]:*

*Extended commands [n]: y*

*Source address or interface: loopback 0*

1. De acuerdo a lo obtenido en el traceroute, apagar el enlace por donde se está llevando a cabo el ruteo en el equipo de distribución mientras el ping está corriendo.
2. Observar la cantidad de pings perdidos durante la reconvergencia de servicios hacia el enlace de respaldo.
3. Encender el enlace apagado y verificar el tiempo que toma para que el tráfico se vuelva a establecer por el enlace original.

**Revisión:**

* Verificar que la reconvergencia a través del enlace de respaldo sea menor a 10 segundos

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

* Verificar que al restablecer el servicio principal, se vuelve a tomar como ruta principal

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |

**Resultados esperados.**

1. La reconvergencia hacia el enlace secundario se realiza en menos de 10 segundos
2. Cuando se restablece el enlace principal, todo el tráfico se va por dicho enlace

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.21. Resumen de resultados de la prueba 9.

**Prueba No. 10**

Administración

**Propósito:** Verificar que es posible realizar el monitoreo de enrutadores con políticas de AAA y utilizando SNMP

**Equipos donde se implementará:**

* DISTRIBUCION\_SITIO\_1
* ROUTER\_ACCESO\_1
* ROUTER\_ACCESO\_2
* SWITCH\_ACCESO\_1
* SWITCH\_ACCESO\_2

**Procedimiento:**

1. El cliente proporcionará 2 servidores, uno para TACACS+ y otro para SNMP.
2. Aplicar la configuración de SNMP y AAA en el equipo donde se realizará la prueba.

*aaa new-model  
aaa authentication login consola tacacs+ local  
aaa authorization exec default tacacs+ local  
aaa authorization commands 0 default tacacs+ local  
aaa accounting exec default start-stop tacacs+  
aaa accounting commands 1 default start-stop tacacs+  
aaa accounting commands 15 default start-stop tacacs+  
tacacs-server host x.x.x.x*

*tacacs-server key xxxxxxxx*

*ip tacacs source-interface Loopback*

*snmp-server community xxxxxxx*

*snmp-server trap-source Loopback1*

*snmp-server location "Mexico"*

*snmp-server enable traps xxxxxxxx*

*snmp-server host X.X.X.X*

1. Verificar en el servidor TACACS+ que el equipo se firma correctamente.
2. Verificar en el servidor SNMP que se obtienen traps del equipo.

**Revisión:**

* Confirmar que AAA funciona correctamente al conectarse a un servidor TACACS+

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

* Confirmar que se reciben *traps* de SNMP en el servidor de manera exitosa

|  |  |
| --- | --- |
| NOMBRE DEL EQUIPO | RESULTADO |
| **DISTRIBUCION\_SITIO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_1** | Pass:  Fail: |
| **ROUTER\_ACCESO\_2** | Pass:  Fail: |
| **SWITCH\_ACCESO\_1** | Pass:  Fail: |
| **SWITCH\_ACCESO\_2** | Pass:  Fail: |

**Resultados esperados.**

1. Los permisos de usuario se pueden administrar desde el servidor TACACS+
2. Se observan traps de SNMP en el servidor.

|  |  |
| --- | --- |
| Estado de la prueba | Exitosa/Parcial/Fallida |
| Falla | Descripción de la falla |
| Razón de la Falla | Motivo por el que se pudo haber presentado la falla |
| Notas |  |

Table 5.22. Resumen de resultados de la prueba 10.

# PARTICIPACIÓN PROFESIONAL

A lo largo de mis años como estudiante de la facultad de ingeniería de la UNAM, adquirí los conocimientos suficientes, así como las bases teóricas y conocimientos técnicos para poder entender, analizar y aplicar los diferentes métodos y protocolos utilizados en las redes de comunicaciones.

Otro de los ámbitos en el que se me ha permitido crecer es en la solución de problemas. Durante las pruebas hubo ocasiones en las que se presentaron fallas que había que resolver en el momento y gracias a la experiencia y las bases adquiridas, fue posible resolverlas de manera exitosa.

Además de los conocimientos técnicos adquiridos, he tenido gran desarrollo en las relaciones sociales gracias al perfil humanístico con el que me prepararon en la Facultad, el cual me ha sido de gran utilidad en el trato con el cliente incluso en las situaciones más delicadas.

Durante el desarrollo de las pruebas, se llevaron a cabo distintas correcciones tanto proactivas como reactivas, la aplicación de dichas correcciones y soluciones son parte de la lógica que, como ingeniero de la Facultad de Ingeniería de la UNAM, se me fue inculcada en las distintas materias que cursé durante mi estancia y fue, además, apoyada con la experiencia adquirida durante el tiempo que llevo laborando.

Otra de las oportunidades que se me presentó durante el desarrollo de las pruebas fue la de poder reafirmar los conocimientos teóricos para poder realizar los exámenes correspondientes para obtener la certificación de nivel profesional de red evaluada por proveedor (*Cisco Certified Network Professional CCNP*).

Actualmente participo de manera activa en el monitoreo de la red en las que se realizaron las pruebas y los cambios, también busco aplicar los conocimientos en otras redes y de igual manera busco aplicar los conocimientos que voy adquiriendo con otros clientes.

El hecho de interactuar con distintos clientes y distintas topologías de red, me abre mucho el panorama respecto a las mejores prácticas a seguir en cualquier diseño, implementación u operación de red, así como mantenerme al tanto de las nuevas tecnologías en equipos de red y de centro de datos que surgen en el mercado.

# RESULTADOS Y APORTACIONES

Las pruebas se realizaron en más de 50 sitios con resultados satisfactorios en la gran mayoría de ellos, se realizaron correcciones mínimas y finalmente la red quedó operando de manera correcta, se mostró al cliente la viabilidad de realizar de manera constante un monitoreo proactivo de la red así como mantenimientos preventivos y correctivos de manera constante sin sacrificar funcionalidad ya que, con la pruebas, también se demostró que el esquema de red es robusto y cuenta con políticas de alta disponibilidad que permiten realizar este tipo de afectaciones en la red.

Las pruebas fueron ampliamente aceptadas y los resultados arrojados ofrecen al cliente la tranquilidad y seguridad de saber que cuentan con un servicio en óptimas condiciones a la vez que nos permite, como parte del área de proveedores, seguir ofreciendo nuestros servicios al cliente beneficiándonos de manera mutua.

Durante la realización de las pruebas, pude aportar mis conocimientos en la solución de problemas así como en la corrección de detalles que, aunque pudieran parecer mínimos, pueden causar problemas mayores si no se atienden de manera preventiva. La solución aportada con las pruebas, no sólo permite una mejora en la red del cliente donde se realizaron, sino también en las redes de cualquier cliente que tenga las mismas necesidades, bastaría con realizar las adecuaciones necesarias de acuerdo a la topología del cliente que así lo solicite. Es así como se integra y mejora la tecnología para cubrir las necesidades del mercado de comunicaciones.

# CONCLUSIONES

Las pruebas se realizaron en 53 sitios a lo largo de toda la república Mexicana; en 17 de los casos se presentaron fallas de hardware en algún módulo o fuente de poder al realizar el reinicio del equipo o las pruebas de redundancia en las tarjetas supervisoras, dichas fallas se corrigieron al solicitar la reposición de la pieza dañada con el proveedor por lo que todas las fallas de hardware fueron corregidas. Al realizar esta detección de piezas dañadas en un ambiente controlado, se evita que la falla se presente en un horario crítico que pueda causar una afectación en el negocio.

Se realizó también la corrección de las descripciones en las interfaces, lo cual permite identificar correctamente la conexión de cada enlace y que, en caso de contingencia, resulte más fácil conocer la topología de red y/o llevar a cabo la identificación y solución de la falla.

Para mejorar la seguridad de la red, se deshabilitaron por completo las interfaces que no tuvieran servicios productivos conectados y se validó que los servicios activos fueran los permitidos, esta “depuración” de conexiones, permite llevar un mejor control de los usuarios-servicios existentes evitando que usuarios malintencionados obtengan acceso a los recursos de la red.

Se detectó que había configuraciones que ya no eran funcionales o que causaba que los equipos tomaran rutas erróneas al transmitir y/o recibir tráfico de red, dichas configuraciones fueron corregidas y depuradas, permitiendo un mejor entendimiento de las mismas y un óptimo funcionamiento de la red.

Todos los sitios quedaron funcionando bajo un esquema de alta disponibilidad, por lo que en caso de falla de algún equipo, no se vería afectado el funcionamiento de la red en dicho sitio.

Finalmente se validó que todos los equipos fueran correctamente administrados desde una consola central y que todos los movimientos generados por los usuarios autorizados quedaran registrados para futuras referencias.

# GLOSARIO

* **Active/Standby Hot.** Estatus de las supervisoras de los equipos de red que cuentan con redundancia de hardware, la supervisora que se encuentre en estatus *Active* será la que esté realizando todos los proceso a nivel de plano de control, mientras que la supervisora en estatus *Standby Hot* estará sincronizada con la activa y en caso de falla, pasará a tomar el rol de *Active* disminuyendo el tiempo de afectación a unos cuantos segundos.
* **ATM.** Acrónimo de *Asynchronous Transfer Mode* o Modo de transferencia Asíncrona. Es un estándar que sirve para la transmisión de voz y datos en un modelo orientado a conexión para una transmisión de banda ancha en redes de Área Extendida (WAN) donde la velocidad de entrada o “bajada” es, generalmente, mayor a la velocidad de salida o “subida”, es por eso que se define como Asíncrona.
* **Broadcast.**  Difusión de una trama o paquete de datos a todos los equipos que se conectan al mismo dominio o segmento de red, se utiliza generalmente para la búsqueda de equipos conectados pero que aun no se les ha asignado una dirección IP o cuándo se requiere enviar una trama a todos los equipos en capa 2.
* **Calidad de Servicio.** Funcionalidad que sirve para separar el tráfico prioritario como la voz o paquetes de monitoreo de tráfico que no es prioritario, cada equipo asigna “colas” dentro de sus interfaces de Entrada/Salida con distintas prioridades, con esto es posible permitir que el tráfico que es más susceptible a retardos, llegue a tiempo a su destino sin importar si ya existe tráfico destinado a salir por la misma interface.
* **Conmutador.** Mejor conocido como *Switch*, es un equipo de comunicación que permite la comunicación de equipos dentro del mismo segmento de red asignando un dominio de colisión en cada una de sus interfaces con lo que se evitan las colisiones al tener la “inteligencia” para enviar y recibir los paquetes de manera independiente.
* **Dijkstra.** Algoritmo utilizado principalmente por el protocolo OSPF para realizar el cálculo de la mejor ruta para el envío de paquetes, se basa en el cálculo de parámetros como el costo del enlace y el ancho de banda del mismo.
* **Dirección IP (Internet Protocol).** Es la dirección o etiqueta de capa 3 utilizada por los equipos para su conexión hacia otras redes, es un número de 32 bits representado por 4 octetos que van del 0 al 255 cada uno, existen direcciones públicas que son las que permiten la navegación en internet, direcciones privadas que se utilizan dentro de un segmento limitado como oficinas u hogares. Actualmente se utiliza IP versión 4 (IPv4) para la comunicación a nivel mundial, sin embargo y debido a que el número de direcciones es limitado, se ha creado IP versión 6 cuyo número de direcciones es infinitamente mayor y que, paulatinamente, sustituirá a IPv4.
* **Enrutador.** Mejor conocido como Router. Es un equipo de Red que permite la comunicación entre equipos de distintos segmentos de red, es donde se configuran protocolos de ruteo como OSPF y BGP, la inteligencia es diferente a la del *Switch o* conmutador, ya que está enfocado a los paquetes de Capa 3.
* **Ethernet.** Familia de tecnologías estandarizadas de red para transmisiones a alta velocidad a través de un cable formado de 4 pares de hilos de cobre, las velocidades se han incrementado desde 10 megabits por segundo hasta 10 gigabits por segundo en sus últimas versiones. Esta tecnología se utiliza principalmente en la conexión de equipos dentro de una red de Área Local o LAN.
* **Frame Relay.** Tecnologia de red para transmisiones en la Red de Área Extendida (WAN) con una metodología de conmutación de paquetes en el medio, dicha tecnología especifica las capas físicas y lógicas de los canales de comunicación digitales y permite la comunicación entre sitios a un bajo costo.
* **Interface.** Se refiere al puerto físico Ethernet, Serial, óptico o inalámbrico, donde se lleva a cabo la conexión entre dos dispositivos de red a través del medio que el protocolo de interconexión defina.
* **IOS.** Acrónimo de Internetwork Operating System o Sistema de Interacción con la red. Es el sistema operativo de los equipos Cisco, se accede a él mediante el puerto de consola del equipo de comunicaciones o mediante algún protocolo que permita iniciar una sesión remota como Telnet o SSH. Sirve para realizar la configuración, monitoreo y verificación del equipo mediante líneas de comando.
* **IP.** Protocolo de Internet. Es el protocolo que define las reglas para el envío y recepción de paquetes en la red, su etiquetado y las rutas o caminos que deben tomar los datos para llegar a su destino con la mayor rapidez posible y, esencialmente, establece el internet.
* **LAN.** Local Area Network o Red de Área Local. Es el conjunto de dispositivos de red ubicados dentro de un área limitada como una oficina, una escuela o un hogar, a diferencia de la red de Área Extendida, no utiliza líneas rentadas y la comunicación es únicamente de manera local entre los dispositivos de la misma red. Se utiliza principalmente el protocolo Ethernet para la construcción de una red LAN
* **LLD.** Low Level Design o Diseño de bajo nivel. Es el documento de diseño que establece a nivel granular los componentes de red que se utilizarán, así como sus interconexiones y direccionamientos IP a utilizar, es el documento que se entrega previo a una implementación.
* **MPLS.** Mecanismo que permite la comunicación eficiente y de alto desempeño en redes de Área Extendida que permite la interacción entre distintos protocolos al etiquetarlos y unificarlos en un solo mecanismo de comunicación.
* **Multicast.** Direcciones IP enfocadas a entregar paquetes solamente a un grupo definido de equipos de red, cada equipo tendrá una dirección IP única, sin embargo, la misma dirección de multicast se configura en los equipos que se desea pertenezcan al mismo grupo y de esta manera es posible la comunicación entre los miembros del grupo.
* **Supervisoras.** Módulos de hardware donde se lleva a cabo la mayoría de los procesos dentro del equipo de red (*Router o Switch)* son las encargadas de realizar los diagnósticos, inicio, configuración, presentación al usuario y administración de los equipos, por lo general los equipos modulares cuentan con dos supervisoras para cuestiones de redundancia y alta disponibilidad.
* **Switchover.** Cambio de supervisora activa de manera física, al retirar o apagar la tarjeta activa; Lógica, al aplicar el comando ***redundancy forcé-switchover*** o por alguna falla en la tarjeta activa que provoca que ésta pierda la gestión y la tarjeta que se encontraba en  *standby hot* tome el rol de activa evitando pérdidas o interrupciones considerables de flujo de tráfico.
* **Vecindades.** En los protocolos de ruteo, ya sean externos como BGP o internos como OSPF, se configuran vecindades con los equipos con los que se desea intercambiar información acerca de rutas conocidas, esto con la finalidad de que cada equipo tenga un panorama de todas las redes existentes en el dominio de la red.
* **VPN.** Acrónimo de Virtual Private Network o Red Privada Virtual. Es el acceso que se realiza por parte de un equipo a una red LAN mediante una red WAN a través de un túnel virtual y que le permite al usuario o equipo, acceder de manera remota a la LAN.

# BIBLIOGRAFIA

**Anthony Bruno, Steve Jordan**. Official Certification Guide CCDA 640-864.

Cuarta Edición. Cisco Press 2011.

**Wendell Odom**. Official Certification Guide CCNP Route 642-902.

Primera Edición. Cisco Press 2011.

**Denise Donohue**. Quick Reference CCNP Route 642-902.

Primera Edición. Cisco Press 2010.

**Wendell Odom, Rus Healy, Denise Donohue**. CCIE Routing and Switching certificacion guide. Cuarta Edición. Cisco Press 2011.

Referencias electrónicas:

<http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfaaa.html>

<http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml>

<http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook>

<http://www.cisco.com/en/US/tech/tk364/technologies_tech_note09186a00801ae32a.shtml>

<http://tools.ietf.org/html/rfc4252>