UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

INGENIERÍA EN COMPUTACIÓN

"APLICACIÓN DE UNA METODOLOGÍA PARA EL ANÁLISIS DE DESEMPEÑO DE UNA RED"

T E S I S

QUE PARA OBTENER EL GRADO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

A L B E R T A M A R T Í N E Z Z Ú Ñ I G A

DIRECTOR DE TESIS: M.C. MARCO ANTONIO VIGUERAS VILLASEÑOR.

MÉXICO, D.F. 2008

Agradecimientos:

Gracias a la UNAM,

Gracias a todos los profesores por tener el corazón dispuesto a compartir lo que saben. Y en especial a Marco por su amistad y guía en este trabajo.

Gracias a Luís por estar a mi lado incondicionalmente compartiendo la vida

Gracias a Zabydel y Albert por haberme dado la oportunidad de trabajar a su lado dándome siempre su confianza y apoyo.

Gracias a mis amigos por compartir sus risas conmigo.

Introducción

La primera generación de redes se enfocaba en soportar conectividad básica entre dispositivos y en escalar las redes para soportar el crecimiento de usuarios.

La segunda generación de redes se enfocó en la interoperabilidad para expandir el alcance y escalamiento de redes, permitiendo conexiones entre múltiples y diversas redes.

Actualmente, en la tercera generación las redes, la entrega de servicios es la base para el éxito de usuarios y aplicaciones. Esta evolución ha llevado a la necesidad de contar con redes robustas que soporten diferentes servicios, aplicaciones, usuarios y dispositivos, con lo cual surge la necesidad de diseñar redes en base a una etapa de análisis.

Aún en la actualidad, la implementación de redes se basa pocas veces en una etapa de análisis, por el tiempo y costos que pueda implicar hacerlo. Esto origina la importancia de presentar un trabajo teórico y práctico, donde se muestre la aplicación de una metodología para analizar el desempeño de una red y con ello poder tomar decisiones asertivas al hacer reingeniería.

En este trabajo se analizará una red operativa de tercera generación, que provee diferentes servicios como enlaces ruteados, Internet y VPNs (Virtual Private Network - Red Privada Virtual). En particular se analizará el servicio de Internet que ofrece a sus clientes, por medio de una red de fibra óptica a nivel nacional, en tres principales ciudades: México D.F., Guadalajara y Monterrey.

Dentro de los tres objetivos que se detallan a continuación, el principal es presentar cómo la etapa de análisis de la metodología de sistemas tiene impacto a mediano y largo plazo, ya sea ayudando a disminuir los costos de operación, o bien, tomando en cuenta las interacciones y dependencias de los usuarios, de las aplicaciones, de los dispositivos y de la propia red.

A continuación se presentan los objetivos del presente trabajo.

Objetivos:

1. Presentar y aplicar una metodología para el análisis de desempeño de una red.
2. Obtener un análisis modular y completo del desempeño del conjunto de servicios que son ofrecidos por la red para el resto del sistema.
3. Realizar propuestas útiles para mejorar el desempeño de la red en caso de ser necesario.

Esta tesis está compuesta de cuatro capítulos. Los tres primeros capítulos exponen la parte teórica, y en el último un caso práctico con la aplicación de la metodología, estos se detallan a continuación:

Capítulo 1. La red y su análisis, introduce a los conceptos de la presente tesis, desde la metodología, los requerimientos, métricas de desempeño, hasta las tecnologías utilizadas.

Capítulo 2. Etapas del análisis del desempeño de la red, se describe detalladamente cada una de las etapas de análisis: requerimientos, flujo y seguridad.

Capítulo 3. Administración de la red, se presentan los elementos de la administración, los estándares, protocolos y herramientas.

Capítulo 4. Aplicación de la metodología, se presenta la aplicación de la teoría expuesta en los capítulos anteriores, el análisis, administración y conclusiones de la red en estudio.

Capítulo 1. La red y su análisis

1.1 Importancia del análisis, arquitectura y diseño de la red

La metodología de sistemas comprende tres etapas el análisis, la arquitectura y el diseño.[1]

Este trabajo se basa principalmente en la etapa de análisis y sólo se desarrollan los principales elementos de la arquitectura y diseño.

El análisis es la base teórica para realizar la arquitectura y diseño de la red, para que a su vez cumplan con los servicios y niveles de desempeño deseados, así como para elegir las estrategias de interconexión y las apropiadas tecnologías de red.

En la figura 1.1 se muestran los flujos de información entre el análisis, arquitectura y diseño de redes.

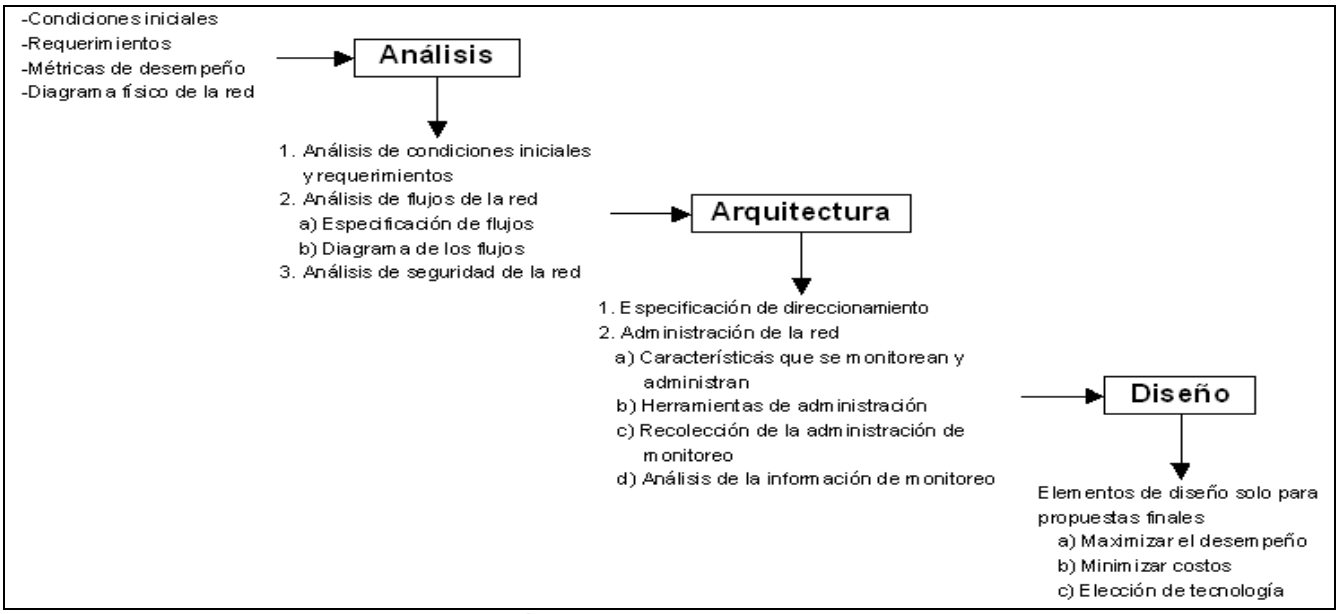


Figura 1.1 Análisis, arquitectura y diseño de redes.

Estas etapas toman en cuenta varios parámetros comunes: requerimientos, flujos de tráfico, objetivos de arquitectura, interacciones, dependencias y limitaciones. Estos parámetros son elegidos y analizados durante el análisis de red, además de priorizados y evaluados durante la arquitectura y diseño. Una vez completados estos procesos se debe contar con la documentación completa de la red que permita analizarla, en caso de que sea una red en operación, o continuar con la implementación, pruebas e integración, en caso de ser una red nueva.

1.1.1 Definición de análisis, arquitectura y diseño de red

Análisis. Es el estudio de los componentes de red, desde dispositivos (switches, routers, etc.), requerimientos y niveles de desempeño hasta el flujo de la información para entender el funcionamiento de la red bajo varias situaciones.

El análisis proporciona elementos para identificar y entender los requerimientos de desempeño dentro de la red, lo cual es tema de estudio de la presente tesis.

> NOTA: La presente tesis se basa principalmente en el análisis y sólo se desarrollan algunos elementos de la arquitectura y diseño, que se mencionan posteriormente.

Arquitectura. Es el desarrollo de las principales funciones de red, como son: direccionamiento, administración de la red, desempeño y seguridad.

Diseño de red. Provee detalle físico de la arquitectura. Durante el diseño se evalúan y eligen las tecnologías para cada área. También se establecen los objetivos de diseño tales como minimizar los costos o maximizar el desempeño, entre otros.

1.1.2 Principios de diseño

Es importante mencionar que dentro del diseño de redes, existe el concepto de ciclo de vida de la red llamado PDIOO, por las iniciales de planeación, diseño, implementación, operación y optimización. Este concepto nos ayuda a ubicar cómo la metodología de sistemas abarca cada una de las etapas del ciclo de vida de una red y que por ello permite presentar un análisis del desempeño y de acuerdo a éste realizar propuestas. **[2]**

Planeación. Los requerimientos de red son detallados y la red existente es analizada.

Diseño. La red es diseñada acorde a los requerimientos y a la información reunida durante el análisis de la red existente.

Implementación. La red es construida de acuerdo al diseño.

Operación. La red esta operativa y es monitoreada. Esta fase es la última dentro del diseño.

Optimización. Durante esta fase los problemas son detectados y corregidos, antes o cuando fueron detectados. Rediseñar la red debe requerirse si son demasiados los problemas que se están enfrentando.

1.2 Análisis

El proceso de análisis considera las bases de una red, desde sus requerimientos de implementación, pasando por los objetivos que debe cumplir, hasta el estado actual en el que se encuentra, esperando obtener como resultados: la descripción de cada uno de los requerimientos, flujos de la información y mapeos completos de toda la red, para que por medio de estos elementos en conjunto se pueda realizar un análisis completo y adecuado que permita ofrecer mejoras y soluciones a una red.

El análisis ayuda a entender cómo las tecnologías influyen en las redes, usuarios, aplicaciones y dispositivos, y viceversa. Por ejemplo, cuando nuevos elementos de estos son adicionados a la red, los requerimientos en la red pueden cambiar.

A lo largo de la presente tesis se mostrarán cada una de las etapas del análisis, y con ellas a detalle su importancia.

Si bien lleva más trabajo realizar el análisis, cuando se conocen los beneficios que proporciona, es probable que no se omita.

1.2.1 Etapas del análisis

Está dividido en tres secciones: análisis de requerimientos, análisis del flujo del tráfico y análisis de seguridad.

Antes de entrar a detalle en el análisis de requerimientos, flujo del tráfico y seguridad, es importante tener claro qué son los requerimientos, el flujo de datos, la seguridad, y su importancia, para ser analizados.

Requerimientos. Son las peticiones (de usuarios, aplicaciones, dispositivos) a la red, usualmente en términos de desempeño y función, las cuales son necesarias para el éxito de la misma; son fundamentales porque forman las expectativas de los clientes; pueden ser reunidos o entregados desde los clientes, aplicaciones, dispositivos y de los propios diseñadores de la red, y son usados por el flujo de datos.

Flujo del tráfico. Es el conjunto de datos que se transmiten y tienen atributos en común, como direcciones origen/destino, tipo de información y enrutamiento.

El análisis del flujo de datos permite analizar el desempeño de la red, por medio del flujo de la información de los servicios que ofrece la red para el resto del sistema.

Seguridad. En este contexto se pude definir como la protección de la red y sus servicios de accesos no autorizados, modificaciones o destrucción. Ésta garantiza que las funciones críticas no sean dañadas. De acuerdo a los objetivos planteados, no se desarrolla el tema de seguridad en el presente trabajo, sólo se realizará dentro del capítulo cuatro una revisión básica del estado actual de la seguridad en la red en estudio.

1.3 Metodología de sistemas aplicada a las redes

La metodología de sistemas considera a la red y a sus elementos (todo lo que interactúa o impacta sobre ella) como un sistema, y que asociado a éste hay un conjunto de servicios (niveles de desempeño y funciones) que son ofrecidos por la red para el resto del sistema. A continuación se definirán estos conceptos.

1.3.1 Definición de sistema

Un sistema es un conjunto de componentes que trabajan juntos para soportar o proveer conectividad, comunicaciones y servicios para usuarios del sistema. Los componentes del sistema incluyen usuarios, aplicaciones, dispositivos y redes. La figura 1.2 muestra los componentes genéricos de un sistema.

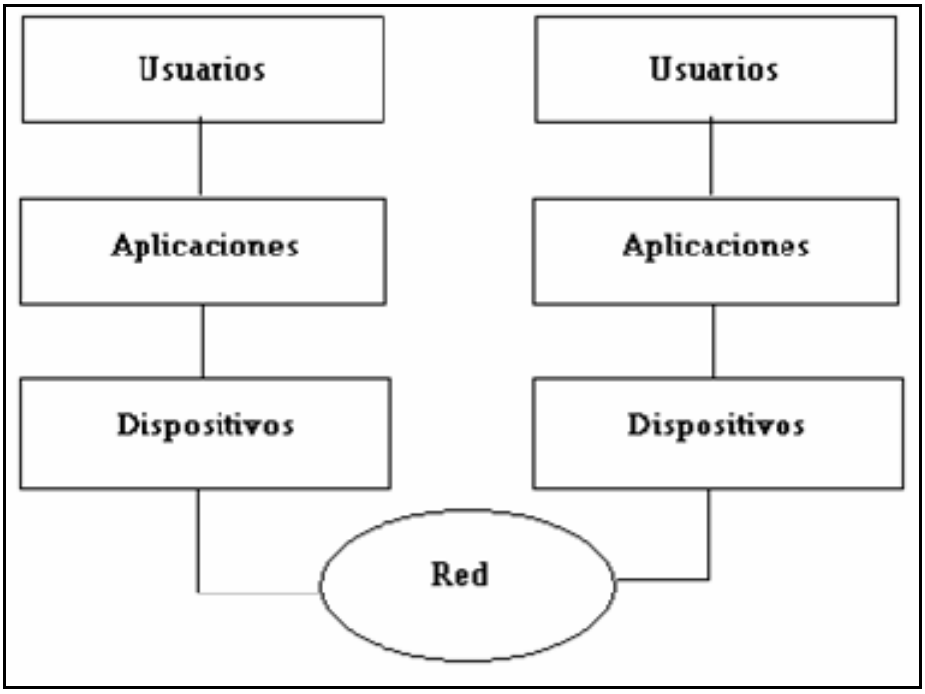


Figura 1.2 Componentes genéricos de un sistema

1.3.2 Componentes de un sistema

Los componentes de un sistema pueden ser subdivididos si es necesario, para enfocarse en una parte en particular del sistema. Por ejemplo, los usuarios de una red pueden ser descritos como personal de soporte, desarrolladores o clientes. En un caso similar, las aplicaciones pueden ser específicas para un usuario o genéricas para toda la red.

Comparando un Sistema con el modelo OSI (Open System Interconnection - Modelo de referencia de interconexión de sistemas abiertos), como se muestra en la figura 1.3, algunas capas del modelo OSI son modificadas. Esto muestra cómo múltiples protocolos pueden estar operando en un nivel del sistema. Por ejemplo, las capas: física, de enlace de datos y de red, pueden estar presentes en el nivel dispositivo y también algunas veces en el nivel de red (por ejemplo, switches y routers en la red).

- El Anexo B. Muestra a detalle las capas del modelo OSI y TCP/IP.

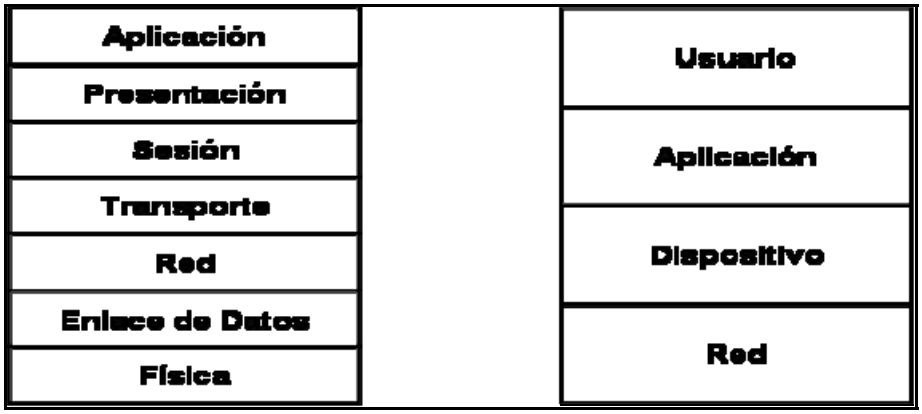


Figura 1.3 Comparación del modelo de referencia OSI con los niveles de un sistema.

La figura 1.4 muestra cómo los dispositivos pueden ser subdivididos de acuerdo a la función que realizan, tales como almacenamiento, cómputo, aplicaciones, etc.

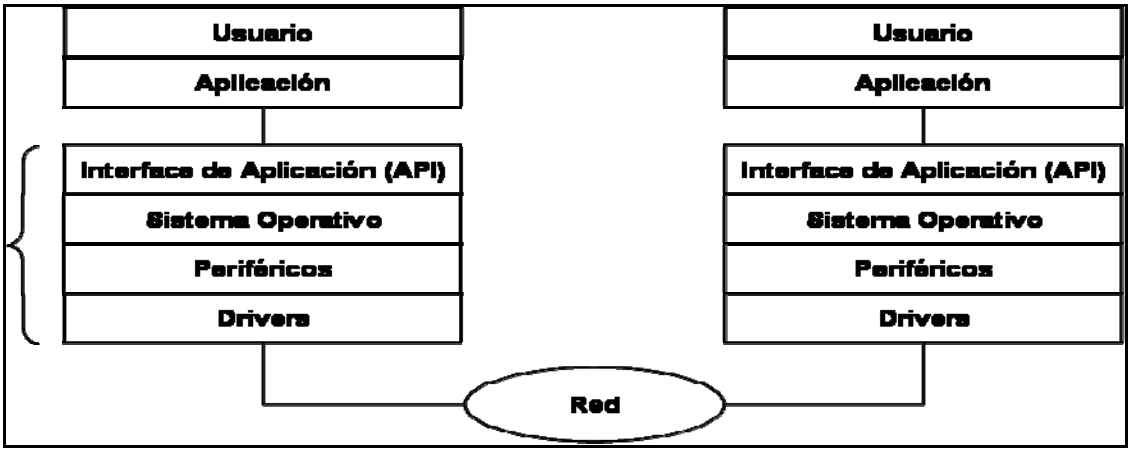


Figura 1.4 Dispositivos clasificados de acuerdo a la función que realizan.

Todos estos componentes trabajan juntos para proveer conectividad y comunicación a través del sistema. La conectividad y comunicación puede ser adaptada para necesidades específicas de usuarios y aplicaciones, tales como entrega de voz o datos en tiempo real, entrega no interactiva de datos de mejor esfuerzo (una red que no tiene implementadas herramientas de calidad de servicio se dice que ofrece un servicio de “mejor esfuerzo”), o entrega fiable de datos de misión crítica.

- NOTA: Se deben considerar descripciones más detalladas cuando es necesario identificar componentes que afectarán en la entrega de servicios a los usuarios.

1.3.3 Definición de servicio

En base a la definición que el IETF(Internet Engineering Task Force - Grupo de Trabajo en Ingeniería de Internet), hace de los servicios de red, como el conjunto de capacidades de red que pueden ser configuradas y administradas dentro de la red y entre redes, se tiene la siguiente definición:

Los servicios de red son los niveles de desempeño y funciones en la red.

Tipos de servicio

Los servicios pueden ser clasificados como:

1. Servicios ofrecidos por la red para el sistema (ver figura 1.5).
2. Servicios solicitados a la red por usuarios, aplicaciones y dispositivos (requerimientos)
3. Servicios fiables (entrega garantizada)
4. Servicios poco fiables (de mejor esfuerzo)

Debido a que los servicios también necesitan ser configurables, cuantificables y verificables dentro del sistema, para asegurar que los usuarios, aplicaciones y dispositivos obtengan los servicios que solicitan, también se pueden clasificar por el grado de desempeño, de acuerdo a las métricas de desempeño que se verán más adelante.

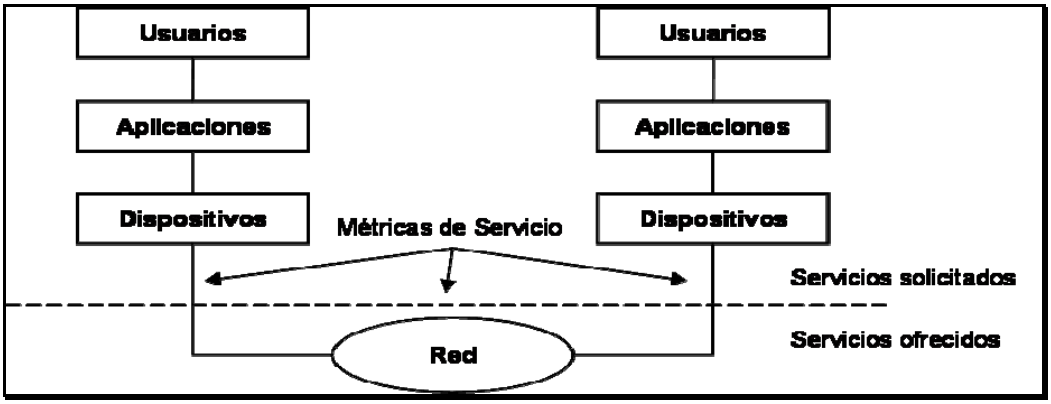


Figura 1.5 Tipos de servicio

1.4 Métricas de desempeño

Las métricas de desempeño son las medidas de los servicios en una red. Estas sirven para monitorearlos, verificarlos y administrarlos. En otras palabras, es la manera de cuantificar las características de desempeño que se toman en la red.

> NOTA: Es importante mencionar que las métricas de los servicios, en la presente tesis, serán las métricas de los servicios entregados desde la red para el resto del sistema.

Es importante definir las métricas de desempeño para la etapa de monitoreo y administración, como se verá en el capítulo cuatro.

La presente tesis se basa en reunir la información de los servicios, para posteriormente analizarlos de acuerdo a las métricas de desempeño definidas.

1.4.1 Características de desempeño

Los niveles de desempeño son descritos por las **características de desempeño**: Capacidad, Delay, Fiabilidad, Mantenimiento y Disponibilidad (las tres últimas por sus siglas en inglés se abreviarán posteriormente como RMA, Reliability, Maintainability, Availability), y se pueden describir en diferentes términos, de acuerdo a los servicios que se analicen.

Capacidad es la habilidad del sistema para transferir información (voz, datos y video, o la combinación de estos). Algunos términos están asociados con la capacidad, como son el ancho de banda y throughput.

Ancho de banda es la cantidad de información teórica que puede fluir por una conexión en un período de tiempo determinado. Teórica, significa que no toma en cuenta la perdida de desempeño relacionada por ineficiencias en el sistema.

Throughput es la cantidad de información real que puede fluir en el sistema o sus dispositivos de red. Sus valores varían dependiendo del diseño, tipos y configuración de los equipos y en que parte de la pila de protocolos se ha tomado la medida.

Delay también llamado latencia, es la medida de tiempo en transmitir una sola unidad de información (bit, byte, cell, frame o paquete) de una fuente a un destino.

El Delay tiene dos componentes, uno fijo y otro variable.

Delay fijo: son predecibles delays asociados con preparar y encapsular los datos, transmitir estos dentro de los cables y transportarlos hasta su destino. Los delays fijos son clasificados como:

Delay de procesamiento y empaquetado. Tiempo para crear los datos.

Delay de señalización. Tiempo que toma para transmitir los datos dentro del cable y está asociado con la velocidad del cable.

Delay de propagación. Tiempo que toman los datos para viajar en la red. En la mayoría de los casos es muy pequeño y puede ser ignorado.

Delay variable: Impredecibles delays que surgen de la espera de que otros paquetes encolados sean enviados por la interfaz. Entre más grandes sean los paquetes a enviar, este tipo de delay incrementa.

Jitter es la variación del delay presentada por los paquetes en la red. Este no tiene relevancia en la tranferencia de datos, pero en aplicaciones de voz es importatnte ya que son muy sensitivas a la diferencias de delay.

Loss. En casos extremos, los paquetes que ingresan a una red o con problemas serán tirados sin entrega. En TCP alguna cantidad de packet loss es aceptable y recuperable por el tipo de conexión que cuenta con retransmisión. Pero en UDP los paquetes tirados significan paquetes perdidos.

Fiabilidad (Reliability), es la media estática de la frecuencia de fallo de una red y sus componentes y representa caídas imprevistas del servicio. Las medidas de fiabilidad son: MTBFs (Mean Time Between Failures) y MTBCF (Mean Time Between Mission Critical Failures), usualmente expresadas en horas.

MTBF, considera todos los fallos sin tomar la importancia del tipo de fallo y es una aproximación muy usada en sistemas simples.

MTBCF, es usada en sistemas más complejos y/o con recursos limitados que restringen el grado de redundancia o compra de componentes de alta fiabilidad. Se utiliza en el análisis del desempeño de sistemas que cuentan con elementos de misión crítica.

Para que la red se considere fiable, la entrega de información debe ser en el tiempo establecido. Cuando el tiempo de entrega varía, los usuarios pierden confianza en el tiempo de entrega de la información.

Mantenimiento (Maintainability), es la medida estática de tiempo para restaurar el sistema a un estado de total operación después de que éste experimenta un fallo. Generalmente expresado como Mean-Time-To-Repair (MTTR).

Disponibilidad (Availability), también conocida como disponibilidad operacional, es la medida de la relación entre la frecuencia de fallas de misión crítica y el tiempo para restaurar el servicio. Es expresada en términos de MTBF dividido entre la suma del MTTR y el MTBF, como se muestra en la siguiente ecuación, dónde A es disponibilidad.

$$A = \frac{MTBF}{MTBF + MTTR}$$

Capacidad, Delay y RMA son dependientes entre ellas. Además los requerimientos de desempeño pueden ser combinados para describir un rango de desempeño para el sistema.

1.5 Etapa de soporte a la red

La etapa de soporte a la red es la habilidad del cliente para sostener un requerido nivel de desempeño durante todo el ciclo de vida de la red.

Esta etapa es a menudo olvidada, siendo un error el pensar que el éxito de la red sólo tiene que ver con la implementación, y que los futuros requerimientos y soporte son responsabilidad del cliente.

El 80% de los costos en el ciclo de vida del sistema se dan en la operación y soporte y únicamente el 20% es el costo para desarrollar, adquirir e instalar éste. Un buen diseño debe tomar en cuenta los principales factores que afectan la operabilidad y el soporte.

Las principales decisiones en la arquitectura y diseño que afectan los costos post-implementación son:

- Grado de redundancia de los componentes en rutas criticas en el diseño.
- Calidad de los componentes de red seleccionados para la instalación.
- Localización y accesibilidad de los componentes que requieren frecuente mantenimiento.
- Implementación de equipo de pruebas y técnicas para monitorear el sistema.

1.6 Elementos de la red

Una red es un conjunto de elementos dentro de un área, cuyo objetivo es comunicarse e intercambiar información.

1.6.1 Principales elementos

Estos elementos se pueden definir de acuerdo a las tres primeras capas del modelo referencia OSI (para más detalles ver Anexo B. El Modelo OSI y TCP/IP).**[3]**

Capa uno, que incluyen todo elemento físico y dispositivos tales como hubs, conectores, cableado.

Capa dos, incluye protocolos de enlace de datos: Frame Relay, PPP (Point-to-point Protocol - Protocolo Punto a Punto), DHCP (Dynamic Host Configuration Protocol - Protocolo Dinámico de Configuración de Clientes) y switches de capa dos. Múltiples switches de capa 2 interconectados forman un dominio de broadcast, por lo tanto cualquier mensaje de broadcast o multicast que se propague por toda la red es factor para tener un bajo desempeño.

- Broadcast es un dato dirigido a todos los dispositivos de la red. Este usa una dirección IP de broadcast por la que es identificado. Ejemplos que provocan trafico de broadcast son paquetes ARP y RIP versión 1.

  Multicast es un dato destinado para un grupo específico, también se identifica por el tipo de dirección. Trafico multicast incluye paquetes de protocolos como OSPF y aplicaciones de videoconferencia.

  Unicast es un dato destinado para un específico dispositivo.

  Directed Broadcast, es un dato destinado para todos los dispositivos en una IP subred, pero que se originó en un dispositivo en otra subred.

Capa tres, incluye direccionamiento, ruteo y dispositivos que soporten estas características tales como routers y switches de capa 3.

Los routers bloquean broadcast y multicasts por default y únicamente envían paquetes unicast y paquetes especiales llamados directed broadcasts

1.6.2 Tipos de switches

Los switches procesan más rápido la transferencia de datos que los routers porque la funcionalidad del switching esta implementada en hardware – en ASICs (Circuitos Integrados de Aplicación Específica) – en lugar de software**.**

Antes los switches estaban restringidos a examinar frames de capa 2. Ahora los switches procesan paquetes de capa 3. Por ello los principales tipos de switches que existen son dos:

Switches de capa 2: Envían los paquetes para el puerto correcto basados en la MAC address, de acuerdo a la tabla MAC (Medium Access Control Address - Dirección de Control de Acceso al Medio), que forman (de a cuerdo al siguiente proceso: empty, flooding, learning, filtering).**[4]**

Switches de capa 3: Son en realidad routers con algunas funciones implementadas en hardware para mejorar el desempeño por medio de las ASICs, tales como:

- Aprender rutas y mantener el mejor camino para cada una de ellas en la tabla de ruteo.
- Determinar el mejor camino que cada paquete debe tomar para llegar a su destino, comparando su dirección destino a la tabla de ruteo.
- Enviar el paquete a las apropiadas interfaces con el mejor camino. Esto es llamado switching the packet, el paquete es encapsulado en un nuevo frame, con la apropiada información, incluyendo la dirección MAC.
- Comunicarse con otros routers para intercambiar información de ruteo.
- Permitir la comunicación entre diferentes LANs.
- Bloquear broadcasts. Por default los routers no envían broadcasts, ayudando a controlar la cantidad de tráfico en la red.

Switches de capa 4: Son una extensión de los switches de capa 3, que también examinan el contenido de paquetes de capa 3. Por ejemplo, pueden examinar el tráfico de acuerdo a protocolos y números de puertos para dar prioridad a cierto tipo de tráfico.

1.6.3 Consideraciones de diseño con switches

1. El número de usuarios finales que deben ser soportados.
2. El número de switches.
3. Las aplicaciones que son usadas (estas definen algunas características que los switches deben tener para soportarlas, tanto en desempeño como en ancho de banda necesitado).
4. El uso de VLANs (acrónimo Virtual LAN – “Red de Área Local Virtual”), incluyendo las troncales que son requeridos entre los switches.
5. Requerimientos redundantes.
6. Interfaces requeridas.
7. En Switches de capa 3, determinar los protocolos de ruteo que serán soportados.

1.6.3 Direccionamiento IPv4 y Routing

Routing es el proceso que determina la ruta que tomarán los paquetes de un punto a otro. El elemento principal para del routing son los routers, que se encargan de reunir y mantener la información de routing para el envío de paquetes de datos y de voz.

Conceptualmente, la información de routing toma la forma de entradas en una tabla de routing. Existen dos formas para configurar las entradas de una tabla de routing: manualmente por el administrador de la red (routing estático), y/o usar un protocolo para crear y mantener la tabla de routing dinámicamente (routing dinámico).

El protocolo IP es un protocolo ruteable (es el protocolo que usa la ruta seleccionada por el protocolo de routing), es el más usado en todas las redes y el más importante. Además de ser más usado para la transferencia de datos, forma la base para otras tecnologías y soluciones como la telefonía IP y VoIP, que usa la red de datos para la transferencia de voz, eliminado así costos asociados con la larga distancia e introduciendo capacidades adicionales.

A continuación se describe ampliamente el concepto routing en las redes.

Routing es el proceso por el cual la información va de un lugar a otro. En redes, un router es el dispositivo usado para rutear tráfico

Para ser capaz de rutear algo, un router o cualquier entidad que lleve a cabo routing, debe hacer lo siguiente:

- Identificar la dirección destino. Determinar el destino (o dirección del paquete).
- Identificar las fuentes de la información. Determinar de cuales fuentes (otros routers) el router puede aprender los caminos para los destinos dados.
- Identificar las rutas. Determinar las rutas iniciales, posibles rutas o caminos, para el destino deseado.
- Seleccionar las rutas. Seleccionar el mejor camino para el destino deseado.
- Mantener y verificar la información de routing. Determinar si los caminos hacia el destino son los más actuales.

- La información que un router obtiene de otros routers es puesta en su tabla de ruteo. El router usará esta tabla para decidir cuales interfases usar para direccionar los paquetes. Si la red destino está directamente conectada, el router ya conoce cuál interfaz usar para enviar el paquete. Si la red destino no está directamente conectada, el router debe aprender la mejor ruta para enviar los paquetes.

Existen dos maneras de aprender la información para llegar a un destino:

Routing estático: La información de routing puede ser ingresada manualmente por administrador de red. Estas rutas deben ser actualizadas cada vez que exista un cambio en la topología de la red. Las rutas estáticas definen el camino específico que tomarán los paquetes desde la fuente al destino.

El ruteo estático es comúnmente usado sólo cuando se necesita rutear información de una red hacia una red Stub. Además las rutas estáticas pueden ser muy útiles para especificar un "gateway of last resort" para el cual todos los paquetes con destino desconocido serán enviados.

> NOTA: Una ruta estática es configurada para proveer conectividad para redes remotas, que no están directamente conectadas. Para conectividad entre elementos finales extremos (end-to-end) una ruta estática debe ser configurada en ambas direcciones.

Routing dinámico: La información puede ser colectada a través de un protocolo de routing dinámico, operando en los routers, que actualizará automáticamente las rutas conocidas si recibe una nueva información de la topología. El router aprende y mantiene rutas para los destinos remotos intercambiando actualización de routing con otros routers en la red.

Un protocolo de ruteo define las reglas que son usadas por un router para comunicarse con los routers vecinos. El ruteo dinámico se basa en un protocolo para difundir el conocimiento. En contraste, el ruteo estático define el formato y uso de los campos dentro del paquete.

Los tipos de protocolos de ruteo son los siguientes:

Interior Gateway Protocols (IGPs). Estos protocolos son usados para intercambiar la información de ruteo dentro de un sistema autónomo. Los protocolos RIPv1 y RIPv2, EIGRP y OSPF son ejemplos de IGPs.

Exterior Gateway Protocols (EGPs). Estos protocolos de ruteo son usados para comunicar sistemas autónomos (The Internet Assigned Numbers Authority (IANA) asigna números de sistemas autónomos para diversas jurisdicciones.). Un sistema autónomo es una colección de redes bajo una administración común y que comparten una estrategia común de ruteo. Un ejemplo de un protocolo EGP, es BGP (Border Gateway Protocol).

Los protocolos de ruteo pueden ser clasificados conforme a los siguientes algoritmos:

Distance vector. Los protocolos rutean de acuerdo a la dirección (vector) y la distancia (saltos) para cualquier enlace en la red.

Link state. Los protocolos que usan el algoritmo link state también son conocidos como SPF (Shortest Path First) y crean una abstracción exacta de la topología de toda la red, o al menos de la parte en donde el router está situado.

Balanced hyrbrid. Combina aspectos de link state y distance vector, como EIGRP.

> NOTA: Existen varios protocolos de ruteo, cada uno con sus ventajas y desventajas. Lo importante es entender los requerimientos de la red y como trabajan los protocolos de ruteo para elegir el apropiado a la red. En algunos casos será necesario contar con múltiples protocolos de ruteo. Entender cómo funcionan e interactúan es importante para el éxito de la red.

Múltiples protocolos de ruteo y rutas estáticas pueden ser usados al mismo tiempo. Debido a que estos pueden proveer diferentes caminos para rutear la información, existe un valor llamado distancia administrativa, que ayuda a determinar cuál ruta usar.

La distancia administrativa es un valor entero de 0 hasta 255. Un protocolo de ruteo con menor distancia administrativa es más confiable que otro con mayor distancia administrativa. Por ejemplo, si un router recibe al mismo tiempo una ruta de dos protocolos para la misma red como IGRP y RIPv1, debido a que RIP e IGRP usan diferentes métricas, el router usará la distancia administrativa para determinar qué IGRP es más confiable que RIPv1. El router adicionará la ruta de IGRP para su tabla de ruteo.

La tabla 1.1 muestra la distancia administrativa de los protocolos de ruteo de acuerdo a la cual se selecciona la fuente de ruteo.

Route Source	Default Distance
Connected interface	0
Static route ardes	1
EIGRP	90
IGRP	100
OSPF	110
RIPv1, RIPv2	120
External EIGRP	170
Unknown o unbelievable	255 (will not be used to pass traffic)

Tabla 1.1 Distancia administrativa de los protocolos de ruteo.

> NOTA: Si estos valores de distancia administrativa no son necesarios o no se desean, estos se pueden modificar, pero por lo general se recomienda los que están por default.

Otra característica de los protocolos de ruteo es que algunos pueden ser Classful (con clase) y otros classless (sin clase).

Classful

Los protocolos de ruteo classful son los que:

- No incluyen la subnet mask al anunciar la ruta.
- Dentro de la misma red, la consistencia de la subnet mask es asumida.
- Las rutas sumarizadas son intercambiadas entre las redes.

Sumarizar rutas es la representación de un conjunto de subredes por medio de una sola dirección IP a determinado número de bits.

Cuando es usado un protocolo de ruteo classful (como RIPv1 e EIGRP), todas las subredes de la misma red principal (clase A, B, o C) deben usar la misma subnet mask. Los routers que corren un protocolo classful realizan sumarización automática a través de los límites de la red. Sumarizar rutas es la representación de un conjunto de subredes por medio de una sola dirección IP a determinado número de bits.

Una vez que un router corriendo un protocolo classful recibe un paquete, hace algo de lo siguiente para determinar la porción de red de la ruta:

Si el paquete contiene información de la misma red principal como está configurada en la interfaz receptora, el router aplica la subnet mask que está configurada en la interfaz receptora.

Si el paquete contiene información de una red principal que es diferente de la configurada en la interfaz receptora, el router aplica la mask por default (por clase) como sigue:

Clase A, la mascara por default es 255.0.0.0

Clase B, la mascara por default es 255.255.0.0

Clase C, la mascara por default es 255.255.255.0

Classless

Los protocolos de ruteo classless:

- Incluyen subnet mask al anunciar la ruta.
- Soportan Variable-Length Subnet Mask *(VLSM).*
- La sumarización de rutas puede ser controlada manualmente en la red.

Los protocolos de ruteo classless (como RIPv2, EIGRP, OSPF, IS-IS) son llamados protocolos de segunda generación, porque están diseñados para mejorar algunas limitaciones de los primeros protocolos de ruteo.

La tabla 1.2 muestra la comparación de las características de los protocolos de ruteo.

Característica	RIPv1	RIPv2	IGRP	EIGRP*	IS-IS	OSPF
Distance vector	X	X	X	X		
Link state					X	X
Sumarización de rutas automática	X	X	X	X		
Sumarización de rutas manual		X		X	X	X
Soporte de VLSM		X		X	X	X
Propietario			X	X		
Tiempo de convergencia	Show	Slow	Slow	Very Fast	Fast	Fast
* EIGRP: Es un protocolo híbrido propietario de Cisco						

Tabla 1.2 Características de los protocolos de ruteo.

1.6.4 Consideraciones de diseño en el direccionamiento de una red

- Cantidad de direcciones IP requeridas.
- Tipo de direccionamiento privado o público.
- Subredes fijas (FLSM, Fixed-Length Subset Masks) o variables (VLSM).
- Protocolos de ruteo utilizados.

1.7 Seguridad en la red

En la actualidad las redes son una parte importante para el éxito de muchas empresas, por ello la seguridad de estas debe asegurar su disponibilidad, integridad y la privacidad de los datos. Pero de forma particular en este trabajo se determino no desarrollar el tema de seguridad de red, por no estar dentro de los objetivos que se plantean. Por ello sólo se hará referencia a los elementos fundamentales de seguridad en la red, de manera que se pueda determinar el estado actual de la seguridad en la red y propuestas para mejorarla, dentro del caso práctico.

A continuación se muestra la definición de algunos términos: los tipos de vulnerabilidades, amenazas y las tecnologías de seguridad, que se pueden usar dentro de una red.

1.7.1 Vulnerabilidades

Una vulnerabilidad es la característica del sistema disponible para que alguien malicioso la use y tome control total o parcial del sistema.

Las vulnerabilidades pueden ser de los siguientes tipos:

De diseño. Se refieren a problemas con la funcionalidad del sistema operativo, aplicaciones o protocolos.

Humanas. Se refieren a errores de los administradores y usuarios, como cuentas de usuarios inseguras o dispositivos inseguros.

De Implementación. Se refieren a la creación, configuración y puesta en marcha de políticas de seguridad, como políticas en la creación de claves, de acceso remotos, de usos de Internet y e-mail.

1.7.2 Amenazas

1) Ataques de reconocimiento

Los ataques de reconocimiento consisten en reunir inteligentemente información, a menudo usando herramientas como escáneres de red o analizadores de paquetes. Esta información puede ser usada para dañar a la red. Algunas formas de reunir la información para realizar este tipo de ataques son:

- Realizar Ping extendidos.
- Escáneres de red y puertos.
- Enumeración de direccionamiento.

2) Ataques de acceso

Durante el ataque de acceso se explotan las vulnerabilidades descubiertas en el ataque de reconocimiento. Algunos ataques comunes son:

- Entrar ilegalmente para cuentas de e-mail y bases de datos.
- Reunir información y passwords.
- Establecer puertas negras y que así se pueda regresar al sistema posteriormente.
- Elegir cuales y cuantos hosts se pueden atacar.
- Intentar cambiar system logs.

3) Ataques para descubrir información

Se caracteriza por la obtención de la información voluntaria de los usuarios que son engañados, y pueden ser:

- Social
- Phishing

4) Ataques de denegación de servicios (DoS)

Es el intento de dañar una red o un recuso de Internet, tal como un Web Server. Este consigue su objetivo enviando una gran cantidad de repetidas peticiones que paralizan a la red o al servidor.

1.7.3 Tecnologías de seguridad

Los ataques pueden ser tratados con sólidas políticas de seguridad así como con equipo y herramientas de seguridad:

- Defensas de amenazas
- Protección contra virus
- Filtrado de tráfico
- Detección y Prevención de Intrusos (IDS, IPS)
- Filtrado de Contenido
- Comunicación segura
- Redes Privadas Virtuales (VPN)
- Secure Socket Layer (SSL)
- Encriptación de archivos
- Confianza e identidad
- Authentication, Authorization and Accounting (AAA)
- Control de Admisión en la Red (NAC)
- Public Key Infrastructure (PKI)
- Mejores prácticas de seguridad en la red
- Administración de la red
- Valoración y auditorias
- Políticas

1.7.4 Calidad de servicio (QoS, Quality of Service)

Las primeras versiones de QoS tenían como objetivo proteger a los datos de otros datos. Cuando la voz sobre IP empezó a volverse una tecnología seria, herramientas de QoS fueron creadas para proteger la voz de los datos, ya las llamadas fueron enviadas sobre Internet, no sobre redes WAN privadas.

Actualmente diferentes tipos de aplicaciones, tales como voz, video y datos son soportados simultáneamente dentro de una sola infraestructura, lo que se conoce como *redes convergentes* **[5]**. Debido a la importancia que tiene el garantizar la calidad de servicio (de la voz y el video y los datos de alta criticidad) de estas redes surge el concepto de QoS, que se define como:

QoS es la habilidad de la red para proveer un mejor o especial servicio para un conjunto de usuarios o aplicaciones en perjuicio de otros usuarios o aplicaciones.

Antes de presentar los fundamentos de QoS, es importante mencionar que algunos proveedores de servicios implementan mecanismos de QoS para mantener un determinado nivel de calidad en los servicios (de voz y datos críticos) que ofrecen, de ahí proviene el concepto Acuerdo de Nivel de Servicio (ANS o SLA, Service Level Agreement), que regula la relación entre los clientes y el operador y que pueden incluir penalizaciones en el caso de que no se cumplan los niveles de calidad establecidos en dicho acuerdo.

En el caso del servicio de Internet del proveedor de servicios que se analiza dentro del caso práctico no tiene implementada QoS para este servicio, sólo se implementa ésta dentro del servicio de enlaces ruteados, cuando los clientes lo requieren. Para el caso del servicio de Internet sólo se mide el desempeño de los enlaces con métricas como la disponibilidad, capacidad (ancho de banda), round trip, packet loss y parámetros operativos como niveles de atención y tiempos de reparación en caso de fallas, como se verá dentro del capítulo cuatro.´

- Sólo se hace mención del tema de calidad de servicio ya que puede ser considerada en una red maneje servicios de voz y datos críticos, en dónde sea necesario aplicar ciertos niveles de calidad de servicio para garantizar la calidad de éstos

  Internet es conocido como un servicio de “mejor esfuerzo”: en general éste no soporta QoS.

Muchas aplicaciones de datos son basadas en TCP, lo que indica que cuentan con retrasmisión, si un segmento TCP es tirado, la fuente retransmite éste después de cierto periodo de tiempo o en caso de no recibir un aviso de que fue recibido, por lo que estas aplicaciones tienen cierta tolerancia a la perdida de paquetes. No así para el envió de paquetes de video y voz que presenta mínima tolerancia a la perdida de paquetes, para la transferencia de voz y video se utiliza el protocolo RTP (Real-Time Transport Protocol) que pertenece a UDP.

Un paquete de voz presentan una pequeña carga útil (payload) relativa a los encabezados – los encabezados IP(20 bytes), RTP(12 bytes), UTP(8 bytes) que adicionan arriba de 40 bytes. Para reducir estos encabezados existe una manera llamada cRTP que comprime el encabezado de 40 bytes a 2 o 4 bytes.

La implementación de QoS en paquetes de datos se hace dentro de una parte de la cabecera del paquete de datos llamada ToS (Type of Service), en realidad pensada para llevar banderas o marcas. Lo que se hace para darle prioridad a un paquete sobre el resto es marcar una de esas banderas (flags). El detalle de los campos de un datagrama IP se puede consultar en el **Anexo B. El Modelo OSI y TCP/IP**

Algunas ventajas de implementar QoS en redes convergentes son las siguientes:

- Controlar cuales recursos de red están siendo usados (ancho de banda, equipo, etc.).
- Asegurar que los recursos son usados eficientemente principalmente por las aplicaciones de misión critica (tienen predecible, garantizado y/o alto desempeño de RMA).
- Crear las bases de una red convergente.

Modelos QoS

Los dos modelos QoS existentes usados para tráfico de redes end-to-end son: IntServ y DiffServ.

End-to-end QoS significa que la red provee el nivel de servicio requerido por el tráfico a lo largo de toda la red.

Con IntServ las aplicaciones solicitan servicios a la red, mientras los dispositivos de red confirman que cuentan con esos requerimientos antes que cualquier dato sea enviado. Los datos de las aplicaciones son considerados como el flujo de paquetes.

En contraste en DiffServ cada paquete es marcado cuando este ingresa a la red de acuerdo al tráfico que este contiene. El dispositivo de red usa esta marca para determinar cómo llevar el paquete a través de la red.

Herramientas QoS

Las herramientas disponibles para implementar políticas de QoS son:

Clasificación y marcado. Consiste en el análisis de paquetes y clasificación de estos dentro de diferentes categorías y en colocar su indicador del tipo de trafico en el encabezado del paquete.

Políticas. Herramientas que eliminan el exceso de tráfico o modificar su marcado.

Shaping. Herramientas que permiten almacenamiento extra de datos, hasta que estos pueden ser enviados, así estos se retrasan pero no son eliminados.

Exclusión de congestión. Técnica para monitorear la carga del tráfico de la red, así que esta congestión pueda ser evitada antes que se vuelva problemática.

Administración de congestión. Control de la congestión después de que ocurrió.

Herramientas de especificación de enlace. Son habilitadas en cada extremo de enlaces punto a punto WAN para reducir el ancho de banda requerido o el delay del enlace.

AutoQos. Es una característica que permite automáticamente habilitar QoS en Switches y Routers.

Importancia de QoS en los proveedores de servicios

El SLA puede incluir parámetros de calidad propios del servicio de telecomunicaciones, como la tasa de error, el tiempo de indisponibilidad y parámetros operativos, como la atención 24x7, el tiempo máximo de solución de problemas, por mencionar algunos.

Para controlar que se cumplan los acuerdos reflejados en el SLA para cada cliente, hay que procesar información técnica procedente de diversas fuentes. De ahí surgen los sistemas que gestionan y supervisan los servicios que se prestan a los clientes, llamados CRM (Customer Relationship Management).

1.8 Resumen

En este capítulo se definieron algunos de los conceptos que se manejarán a lo largo de la presente tesis, entre ellos los principales son los siguientes:

La metodología de sistemas consta de tres etapas, la primera la de análisis, la segunda la arquitectura y la tercera el diseño de la red. La presente tesis se basa principalmente en la etapa de análisis, y sólo se desarrollarán algunos elementos de la arquitectura y diseño.

Además, la metodología de sistemas puede ser aplicada para cualquier tipo de red y nos permite considerar las interacciones y dependencias de los usuarios, las aplicaciones, los dispositivos y de la red, lo que nos permite resolver los problemas que se dan cuando no se consideran las dependencias entre estos elementos.

También se hizo mención de los principales elementos de una red como tipo de dispositivos, direccionamiento y ruteo.

A continuación, en el siguiente capítulo se profundiza en cada una de las etapas del análisis.

Capítulo 2. Etapas del análisis del desempeño de la red

Las etapas del análisis de desempeño de la red son:

Etapa uno: Análisis de requerimientos.

Etapa dos: Análisis de flujo.

Etapa tres: Análisis de seguridad.

2.1 Etapa uno: Análisis de requerimientos

El proceso de análisis de requerimientos nos permitirá distinguir entre bajo o alto desempeño, los servicios y sus requerimientos, así como otros tipos de requerimientos usados para la arquitectura y diseño.

Antes de iniciar con la etapa de análisis de requerimientos, es importante mencionar que el tipo de desempeño de una red puede clasificarse en dos.

Múltiples niveles de desempeño. Cuando una o pocas aplicaciones, usuarios, grupos y/o dispositivos tienen requerimientos de desempeño significativamente más grandes que otros requerimientos.

Un nivel de desempeño. No hay diferencias significativas en los requerimientos de desempeño entre los elementos del sistema.

El análisis de requerimientos forma la base sobre la cual la arquitectura y diseño son construidos. Sin embargo es ignorado en la mayoría de los casos por el tiempo y costo que lleva realizarlo.

El análisis de requerimientos ayuda al diseñador a entender el probable funcionamiento de la red que se construirá y tiene los siguientes beneficios:

- Elección de la tecnología y servicios más objetiva e informada.
- La habilidad para combinar estrategias de interconexión de redes.
- Dimensionar redes y elementos para usuarios y aplicaciones.
- Un mejor entendimiento de dónde y cómo aplicar servicios en la red.

Los requerimientos son las descripciones de las funciones de red y desempeño necesarios para que la red soporte exitosamente sus usuarios, aplicaciones y dispositivos.

Parte del proceso de análisis de requerimientos, es darle prioridad a los requerimientos, determinar cuáles son realmente necesarios y cuáles son deseables (características).

En la figura 2.1, los requerimientos son separados en: fundamentales, características deseadas, rechazados (realmente no necesarios, no deseados, no realistas o no implementables) o de información. Las redes deben contar, como mínimo, con un conjunto de requerimientos fundamentales.

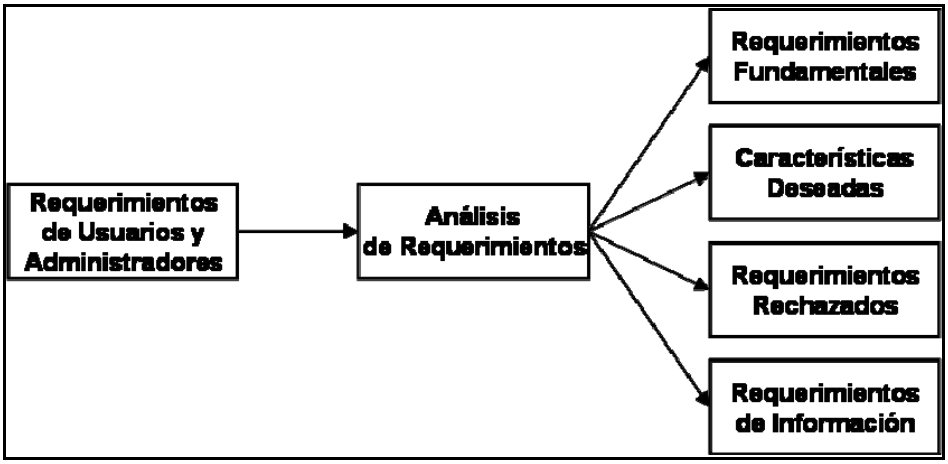


Figura 2.1 Separación de requerimientos.

Cabe mencionar que existe un método para categorizar los requerimientos que está basado en el RFC 2119 del IETF, en el cual se identifican palabras y frases que pueden ser usadas para describir la importancia de un requerimiento.

De acuerdo a los componentes que conforman al sistema (usuarios, aplicaciones, dispositivos y red), se inicia con los requerimientos de los usuarios, que son los menos técnicos y más subjetivos, después los requerimientos de las aplicaciones, dispositivos y red.

2.1.1 Requerimientos de usuarios

Los usuarios son la capa superior dentro del sistema. El termino usuario representa a los usuarios finales del sistema. Un usuario puede ser una red, otro sistema o dispositivo.

Los requerimientos de usuario, son el conjunto de necesidades de los usuarios, fundamentales para que realicen sus tareas dentro del sistema. Parte del trabajo de reunir y entregar los requerimientos, es hacerlo cuantitativos cuando sea posible.

En general, el sistema debe adaptarse a los usuarios y su ambiente, proveer acceso y transferencia de información rápida y confiable, así como ofrecer calidad de servicio.

Algunos requerimientos de usuarios son:

Límites de tiempo, la necesidad del usuario en acceder, transferir o modificar información dentro de un tolerable cuadro de tiempo. Por ejemplo, el tiempo para la descarga de archivos.

Interacción, es la medida del tiempo de respuesta de la red y el resto del sistema, cuando los usuarios requieren activa interacción. Por ejemplo, en acceso remoto, acceso web o visualización.

Fiabilidad, es la disponibilidad de los servicios desde la perspectiva de los usuarios. El usuario debe ser capaz de acceder a los recursos del sistema un alto porcentaje de tiempo con niveles de servicio consistentes (en términos de usos de aplicaciones o entrega de información).

Calidad de presentación, se refiere a la calidad de presentación que los usuarios reciben, ya sea en audio, video y/o pantallas. Las medidas de calidad incluyen a las características de desempeño.

Adaptabilidad, es la habilidad del sistema para adaptarse a los cambios en las necesidades de los usuarios. Por ejemplo, cuando un usuario necesita movilidad.

Seguridad, desde la perspectiva de los usuarios, es un requerimiento para garantizar la confidencialidad, integridad y autenticidad de la información y de los recursos físicos.

Adquisición y finanzas, se refiere a lo que los usuarios o administradores pueden permitirse comprar para la red como dispositivos, de manera que sea posible su adquisición. Aunque no es un requerimiento técnico, los costos y finanzas afectan al diseño de la red.

Funcionalidad, es cualquier requerimiento funcional del usuario al sistema. Las funciones que el sistema realiza son a menudo relacionadas con las aplicaciones que son usadas en el sistema. La funcionalidad implica determinar cuáles aplicaciones usan los usuarios actualmente.

Soporte, es el conjunto de características que describen cómo el cliente puede mantener la operación de la red, con el nivel de desempeño requerido en el proceso de análisis.

Futuro crecimiento, es determinar cuándo o si los usuarios necesitan y usan nuevas aplicaciones y dispositivos en la red.

2.1.2 Requerimientos de aplicaciones

Son requerimientos determinados desde la información de las aplicaciones, experiencia o pruebas como los siguientes.

1) Tipos de aplicaciones

Dentro del sistema, el componente aplicación es crucial. De este componente muchos requerimientos para la red son determinados.

Al inicio de las redes, las aplicaciones requerían conectividad básica y transferencia de datos a través de la red. Ahora además de esos requerimientos, requieren: alto desempeño, predecible o garantizado; funcionamiento para soportar los requerimientos de los usuarios: tiempo, interacción, fiabilidad, calidad, adaptabilidad y seguridad.

Basados en los requerimientos de desempeño, los tipos de aplicaciones son: aplicaciones de misión crítica, velocidad crítica, tiempo real e interactivas:

A continuación estas aplicaciones serán descritas por sus requerimientos y métricas de servicio:

Aplicaciones de misión crítica

Son las que presentan predecible, garantizado y/o alto desempeño de RMA (Fiabilidad, Mantenimiento, Disponibilidad).

Algunas de las pérdidas que se pueden dar en caso de que no se cumplan el desempeño establecido en estas redes son:

- Ingresos o clientes, aplicaciones que manejan transacciones y dinero. Por ejemplo: aplicaciones de bancos, para reservación, procesamiento de tarjetas de crédito.
- Información no recuperable como aplicaciones para teleconferencia o telemetría.
- Datos confidenciales, como ID o facturación de clientes.
- De la vida, como aplicaciones para monitorear la salud.

Aplicaciones de velocidad crítica

En términos de capacidad, estas aplicaciones requieren un predecible, seguro o alto grado de capacidad. Algunas de estas incluyen voz, video no almacenado y tele-servicios (tele conferencia, tele medicina, tele seminarios).

Aplicaciones de tiempo real e interactivas

La métrica de desempeño de estas aplicaciones es el delay. Éstas tienen una estricta relación de tiempo entre la fuente y el destino, con uno o más temporizadores en la recepción del destino. Si la información es recibida después de que el temporizador expira, la información es desechada. Por ejemplo aplicaciones basadas en VoIP se consideran de tiempo real, en dónde el delay end-to-end tiene varios factores que lo pueden conformar, entre ellos: la compresión, el encapsulado, propagación, procesamiento (switching) y descompresión, encolado (queuing), y serialización, Desde la perspectiva de servicio de una aplicación, optimizar el end-to-end delay (de extremo a extremo) y el round-trip (ida y vuelta), es más importante que enfocarse en diferentes fuentes de delay.

La figura 2.2 muestra los tipos de aplicaciones de tiempo real y no-tiempo real.

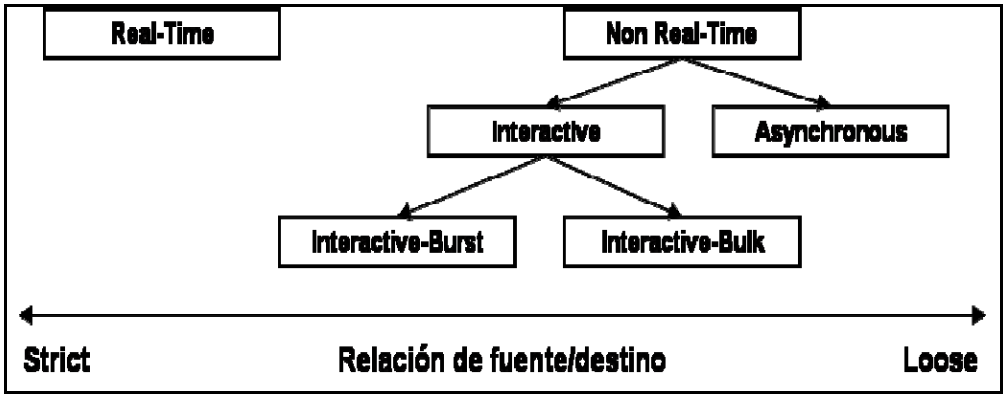


Figura 2.2 Ejemplo de la localización de los dispositivos en un campus.

Actualmente, la mayoría de las aplicaciones son consideradas Non-real-time.

Aplicaciones non-real-time

Las aplicaciones non-real-time, tienen varios requerimientos de delay end-to-end (en términos de la cantidad de delays). El destino espera hasta que la información es recibida de acuerdo a los temporizadores establecidos en las aplicaciones. Las aplicaciones de non-real-time pueden incluir asíncronos e interactivos delays.

Aplicaciones asíncronas

Las aplicaciones asíncronas son poco sensitivas a la relación de tiempo de entrega de información desde la fuente al destino, o al tiempo fuera de los límites de sesión de la aplicación, como el mail.

Debido a que no hay muchas aplicaciones que sean de tiempo real y asíncronas, la mayoría de las aplicaciones son del tipo interactivas.

Aplicaciones interactivas

Las aplicaciones interactivas asumen alguna relación de tiempo entre la fuente y el destino mientras la sesión de la aplicación sea activa. Sin embargo, la relación no es tan estricta como la de tiempo-real. Las aplicaciones interactivas son consideradas por muchas personas de tiempo-real, ya que entienden tiempo-real como “tan rápido como sea posible”. Algunas aplicaciones comunes interactivas son, telnet, FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos), Web.

Finalmente las aplicaciones interactivas pueden ser divididas en Burst y Bulk

Aplicaciones interactivas tipo burst

Aplicaciones interactivas tipo Burst, son sensitivas al delay de la red. Por ejemplo, aplicaciones de acceso remoto, como telnet.

Aplicaciones interactivas tipo bulk

Aplicaciones interactivas tipo Bulk, son en las que el delay del procesamiento o aplicación es el delay predominante. Por ejemplo, el uso de FTP en la transferencia de archivos grandes, debido al procesamiento en el receptor.

Es importante clasificar las aplicaciones para considerar si sus requerimientos afectan o influyen al diseño y arquitectura de la red.

2) Grupos de aplicaciones

Es útil reunir aplicaciones con características similares de desempeño, ya que esto ayudará en el mapeo las características de desempeño y en reunir y entender los requerimientos.

Los principales grupos de aplicaciones son:

Aplicaciones de control y de comandos/telemetría

Aplicaciones en las cuales los datos y comandos son transmitidos entre un dispositivo remoto y uno o más estaciones de control, para rastrear y determinar el estado del dispositivo remoto. Un dispositivo remoto puede ser un cajero automático, un vehículo piloteado remotamente, una nave espacial. Estas aplicaciones pueden ser caracterizadas de tiempo real y/o interactivas y de misión critica.

Aplicaciones de visualización

Incluye a las aplicaciones que usan objetos desde 2D hasta 3D, realidad virtual, inmersión y manipulación de objetos. Los ejemplos incluyen la visualización de simulaciones numéricas y de datos experimentales, como modelado de fluidos, simulaciones moleculares, etc.

Estas aplicaciones pueden ser caracterizadas como aplicaciones de velocidad-critica e interactivas tipo Burst.

Aplicaciones de cómputo distribuido

Incluye aplicaciones que son distribuidas a través de LANs, o WANs. Las aplicaciones pueden estar en dispositivos de cómputo que comparten el mismo bus local (paralelo), hasta las que han sido localizadas en la misma LAN (como en un cluster). Estas aplicaciones pueden ser caracterizadas de tiempo-real o interactivas tipo Burst.

Aplicaciones de acceso Web y uso

Las aplicaciones de acceso son las utilizadas para el acceso remoto. Las aplicaciones Web y de uso implican acceso remoto a dispositivos, así como descarga y actualización de la información. Esto es hecho con ayuda de interfaces gráficas. Estas aplicaciones son de tipo interactivas Burst y Bulk.

Aplicaciones de tipo bulk en el transporte de datos

Cuando la cantidad de información deseada es relativamente grande y las sesiones son menos interactivas (asíncronas), las aplicaciones pueden optimizar la velocidad de transferencia afectando la interacción. Estas aplicaciones no tienen requerimientos de alto desempeño.

Aplicaciones de tele-servicios

Estas aplicaciones proveen la entrega en conjunto de voz, video y datos, para grupos de personas en varias localizaciones. Algunos ejemplos incluyen: tele conferencia, tele medicina y tele seminarios. Estas aplicaciones pueden ser caracterizadas de tiempo-real e interactivas y son consideradas de velocidad y misión critica.

Aplicaciones OAM&P (Operations, Administration, Maintenance and Provisioning)

Son requeridas para la apropiada funcionalidad y operación de la red. Los ejemplos incluyen; DNS (Domain Name Service), Mail Services/SMTP (Simple Mail Transfer Protocol), ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones), de monitoreo, de administración y seguridad de la red, así como sistemas de contabilidad. Estas aplicaciones son consideradas de misión crítica e interactivas.

Aplicaciones cliente-servidor

En ellas el flujo de la información es entre el cliente y el servidor, tales como: ERPs (Enterprise Resource Planning), SCM (Suply Chain Management) y CRM (Customer Relationship Management). Estas aplicaciones son a menudo de misión crítica e interactivas.

3) Localización de las aplicaciones

Es también importante determinar la localización de las aplicaciones en la red. Hay aplicaciones que funcionan en todas partes y que todos usan. Sin embargo, hay aplicaciones que a menudo son utilizadas por un particular usuario, grupo de usuarios o servidores. Cuando sea posible, identificar tales aplicaciones y en dónde aplican, ayudará durante el análisis de flujo.

2.1.3 Requerimientos de dispositivos

Los requerimientos de los dispositivos que la red soportará se basan en el tipo de dispositivos, sus características y su localización.

Tipos de dispositivos

Los dispositivos pueden estar agrupados en tres categorías principalmente:

- Dispositivos de cómputo genéricos
- Servidores
- Dispositivos especializados

Características de desempeño de los dispositivos

Aunque la mayoría de componentes de un dispositivo son propietarios y la información de desempeño puede no estar disponible o ser impredecible, reunir la información para dispositivos estándares ayudará a identificar cómo cada uno de estos componentes afectan todo el desempeño del dispositivo.

Algunas características de desempeño a considerar son:

- Desempeño en el almacenamiento (disco duro, memoria flash, cintas)
- Desempeño del procesador (CPU)
- Desempeño de la memoria (tiempos de acceso)
- Desempeño del bus (capacidad)
- Desempeño del sistema operativo (pila de protocolos y APIs)
- Desempeño de los drivers

La información que se pueda reunir de las características de desempeño, será muy útil para estimar el desempeño del dispositivo o para identificar cualquier factor limitante.

Localización de dispositivos

La localización de existentes o esperados dispositivos genéricos, servidores y dispositivos especializados, puede ser de mucha ayuda para determinar la relación entre usuarios, aplicaciones y red. La localización de la información ayuda a determinar las relaciones entre los componentes del sistema, también a determinar las características del flujo de tráfico para el sistema, como se verá posteriormente en el análisis de flujo. La figura 2.3 muestra un ejemplo de la localización de los dispositivos en un campus.

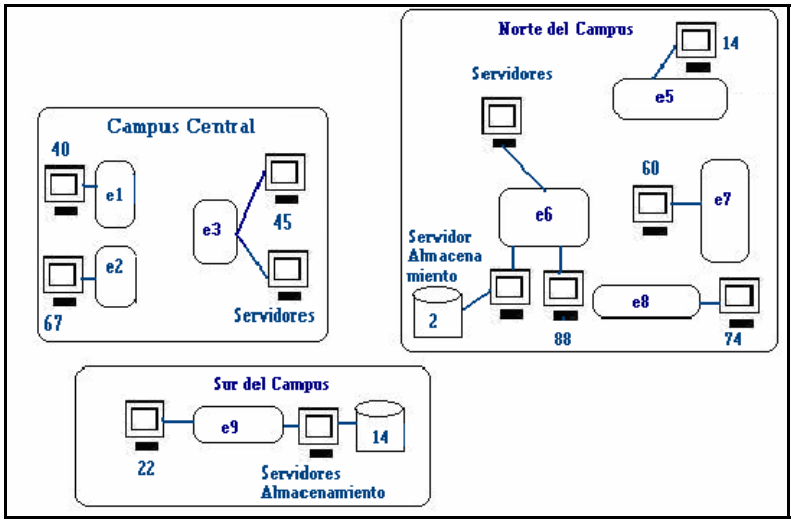


Figura 2.2 Ejemplo de la localización de los dispositivos en un campus.

Cuando la localización de los componentes del sistema cambia, es importante reevaluar los requerimientos del sistema para determinar si los requerimientos de los servicios han cambiado.

2.1.4 Requerimientos de red

Pocas redes son construidas desde cero, en la mayoría de los casos los requerimientos de la red son: adicionar nuevas aplicaciones para el sistema, migración de tecnología o protocolos, actualización de la infraestructura, reducción o expansión de los alcances del sistema.

Algunos de los requerimientos de la red se presentan como dependencias y limitantes cuando se incorporan cambios a la red o una nueva red:

Dependencias al escalar la red. La red existente puede afectar a las modificaciones de la nueva red. Por ejemplo, al adicionar cambios a la red existente puede afectar el tamaño y el alcance del sistema.

Localización de dependencias. De acuerdo a los cambios hechos en la red existente, la localización y concentración de los componentes del sistema cambiarán.

Limitantes de desempeño. Se debe considerar cómo los cambios o la nueva red, afectarán el desempeño de la red existente. Las nuevas y las ya existentes características de desempeño tienen que integrarse en un conjunto.

Dependencias de soporte del servicio y red. Se debe tomar en cuenta los actuales y nuevos requerimientos como: estrategias de direccionamiento, elección y configuración de los protocolos de ruteo, el soporte del servicio, sistema de seguridad, contabilidad, monitoreo y administración.

Dependencias de interoperabilidad. Las dependencias de interoperabilidad entre la red existente y la red modificada, se dan entre los límites de las redes, en donde las diferentes tecnologías o medios son usados.

Red obsoleta. Algunos partes de la red existente pueden ser ya obsoletas cuando se desea modificar la red.

2.1.5 Financiamiento como requerimiento

Un requerimiento importante por mencionar es el **financiamiento** en la red.

El nivel de financiamiento es una limitante en la arquitectura y diseño de la red y es importante considerarlo desde el proceso de análisis, para evitar proyectos de redes económicamente no factibles. En el análisis de requerimientos se debe determinar si estos exceden o están dentro de los límites económicos.

Es recomendable contar con múltiples prototipos de arquitectura y diseños a elegir, con sus diferencias funcionales y financieras bien definidas.

2.1.6 Especificación de requerimientos

La especificación de requerimientos es un documento que lista y prioriza los requerimientos reunidos desde la arquitectura y diseño. La tabla 2.1 muestra un ejemplo de la forma en que se pueden especificar los requerimientos.

Especificación de requerimientos							
Id/Nombre	Fecha	Tipo	Descripción	Reunido / Entregado	Localización	Estado	Prioridad

Tabla 2.1 Especificación de requerimientos.

Los campos en esta plantilla son:

Id/name. Puede ser un número o nombre que identifique al requerimiento.

Fecha. Es la fecha cuando este requerimiento fue desarrollado.

Tipo. Representa el tipo de componente que lo originó (usuario, aplicación, dispositivo, red).

Descripción. Son los detalles de ese requerimiento.

Reunido / Entregado. Indicar de quien o dónde se obtuvo.

Localización. En dónde este requerimiento es aplicado, si se conoce.

Estado. Representa el estado actual de este requerimiento (fundamental, característica, futuro requerimiento, rechazado, o sólo de información).

Prioridad. Es un número de prioridad asignado de acuerdo al estado.

2.2 Etapa dos: Análisis de flujo

El análisis de flujo es el proceso de identificar el tráfico, su localización y los niveles de desempeño que requieren. El origen es llamado source y el destino sink.

Para el análisis de flujo se pueden presentar el mapeo de flujos de las aplicaciones, así como el mapeo de flujos con información de desempeño.

2.2.1 Flujos de datos

El flujo, también llamado tráfico, es un conjunto de tráficos de red (aplicación, protocolo e información de control) que tienen atributos en común, como direcciones destino y fuente, tipo de información, direccionamiento, y otra información end-to-end. Como se muestra en la figura 2.4, los atributos de los flujos aplican a través de la red o end-to end.

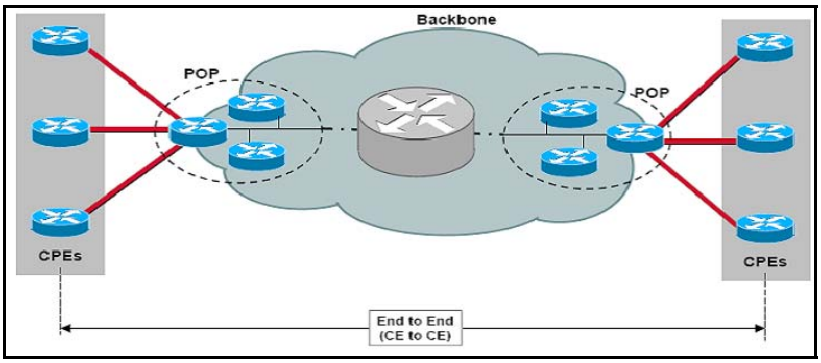


Figura 2.3 Flujos end-to-end.

2.2.2 Identificación de los flujos

Para identificar los flujos de las aplicaciones, se pueden seguir las siguientes consideraciones:

- Enfocarse de forma particular en determinadas aplicaciones, grupos de aplicaciones, dispositivo o funciones (por ejemplo: almacenamiento, procesamiento).
- Desarrollar un profile de las comunes o aplicaciones seleccionadas, usadas a través de la red.
- Elegir un número de aplicaciones importantes que se usan en toda la red.

2.2.3 Señalización del origen y destino de los flujos

La señalización del origen y término de los flujos, ayuda a identificar la dirección de estos. Al origen del flujo de llama fuente (source data), al termino del flujo se le llama destino (data sink). La figura 2.5 muestra la conexión de señalización usada para la fuente y destino.

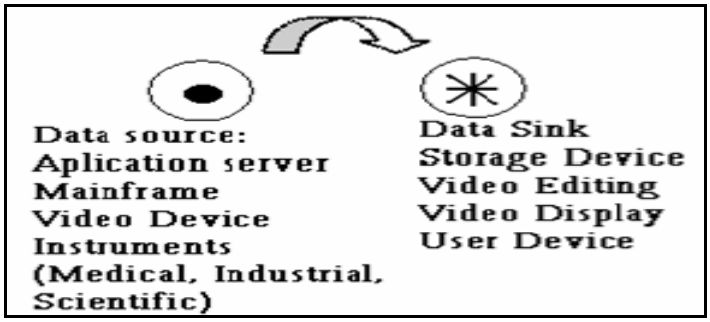


Figura 2.4 Señalización de fuente y destino de datos.

2.2.4 Clasificación de los flujos

Los flujos pueden clasificarse de acuerdo a los tipos que existen y/o sus características y también de acuerdo al modelo al que puedan pertenecer.

Individual, es el flujo de una sola sesión de una aplicación y se pueden determinar de la especificación de requerimientos o del conocimiento de las aplicaciones, usuarios y dispositivos y su localización.

Compuesto, es la combinación de múltiples flujos individuales que comparten enlaces comunes, caminos o red. La mayoría de los flujos en una red son compuestos.

Críticos, son aquellos tipos de flujos considerados más importantes que otros, como los de alto desempeño o de estrictos requerimientos o sirven a usuarios más importantes, aplicaciones y dispositivos. Ejemplos: misión critica, tiempo real, interactivos.

La tabla 2.2 muestra algunas características en común de los flujos que nos ayudarán a clasificarlos posteriormente:

Requerimientos de desempeño	- Bandwidth - Delay - Disponibilidad - Calidad de los Niveles de Servicio
Importancia / Niveles de prioridad	- Negocio/Empresa/Proveedor - Políticas
Otras	- Grupos con algo en común: Usuarios, Aplicaciones, Dispositivos. - Planeados (a una hora del día) - Protocolos usados. - Direcciones/Puertos - Seguridad/Requerimientos de Privacidad

Tabla 2.2 Características comunes de los flujos.

Modelos de los flujos

Los modelos de flujo son grupos de flujos que tienen específicas y consistentes características de funcionamiento.

Algunas de las características de los modelos de flujo son el direccionamiento, la jerarquía y conexión. Los flujos dentro de un modelo aplican para una sola aplicación.

Los modelos de flujo ayudan a describir el grado de jerarquía y conexión de los flujos de las aplicaciones. Ellos muestran en dónde se combinan los flujos, en dónde pueden ser agrupados y dónde ocurren los flujos entre iguales (peers) y cuales dispositivos están dentro del mismo nivel de jerarquía.

También ayudan a identificar cuales flujos son críticos, además de identificar y categorizar de forma rápida los flujos.

Los modelos de flujo son:

- Peer-to-peer
- Client-server
- Jerárquico Cliente-servidor
- Distributed computing

Modelo peer-to-peer (P2P)

Modelo Peer-to-Peer (entre iguales o de igual a igual) es donde los usuarios y aplicaciones son bastante consistentes a lo largo de la red y por lo tanto también el funcionamiento de su flujo. **[6]** En otras palabras, todos los nodos de una red P2P son iguales (no se distinguen servidores de clientes), cada usuario es un peer . Como se muestra en la figura 2.6.

El modelo de flujo peer-to-peer es el modelo por default, que se usa cuando no se tiene ninguna información acerca de los flujos de la red.

Este modelo tiene dos implicaciones importantes:

No se pueden distinguir tipos de flujos en este modelo. Sin embargo, todos o ninguno son flujos críticos. Además los flujos son equivalentes, así que pueden ser descritos por una sola especificación en un profile.

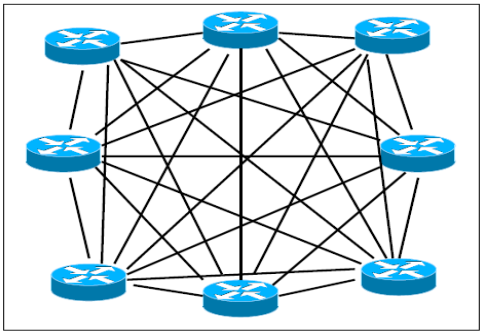


Figura 2.5 Ejemplo del modelo de flujo peer-to-peer.

Existe una clasificación para los sistemas peer-to-peer: centralizado y coordinado, jerárquico y descentralizado.

Modelo cliente-servidor

El modelo de flujo Cliente-Servidor es el modelo más conocido y aplicable. Los flujos en este modelo son bidireccionales, entre clientes y servidores, en forma de solicitudes (requests) y respuestas (responses). Los flujos son asimétricos y jerárquicos hacia el cliente. Los requests tienden a ser más pequeños comparados con los responses.

La figura 2.7 muestra el modelo de flujo cliente-servidor, en dónde el servidor es considerado la fuente y el cliente el destino del flujo, porque los flujos predominantes e importantes los origina el servidor para los clientes. Cuando existe el requerimiento de transmitir información para múltiples clientes concurrentemente, debe ser considerado proveer multicast en la red para optimizar los flujos de este modelo.

Algunos ejemplos son servidores con aplicaciones Web, aplicaciones ERP como SAP y aplicaciones de e-commerce.

En el siguiente modelo de flujo jerárquico cliente-servidor, pueden existir más de una capa dentro del modelo cuando existen servidores que a su vez son clientes de otros servidores.

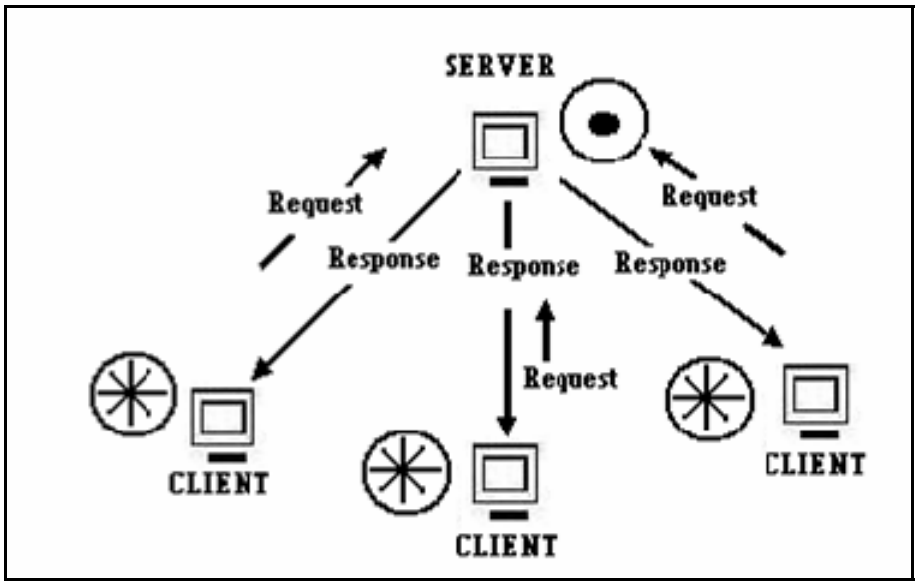


Figura 2.6 Modelo cliente-servidor.

Modelo jerárquico cliente-servidor

Cuando el modelo cliente-servidor cuenta con más capas para los flujos, este es considerado jerárquico, esto es, existen diferentes niveles o capas en las que los servidores atienden a su vez a otros servidores, que a su vez pueden atender a otros servidores y así repetidamente de acuerdo al numero de capas que se tengan. Así cada unos de los servidores pueden ser fuente y destino al mismo tiempo, como se muestra en la figura 2.8.

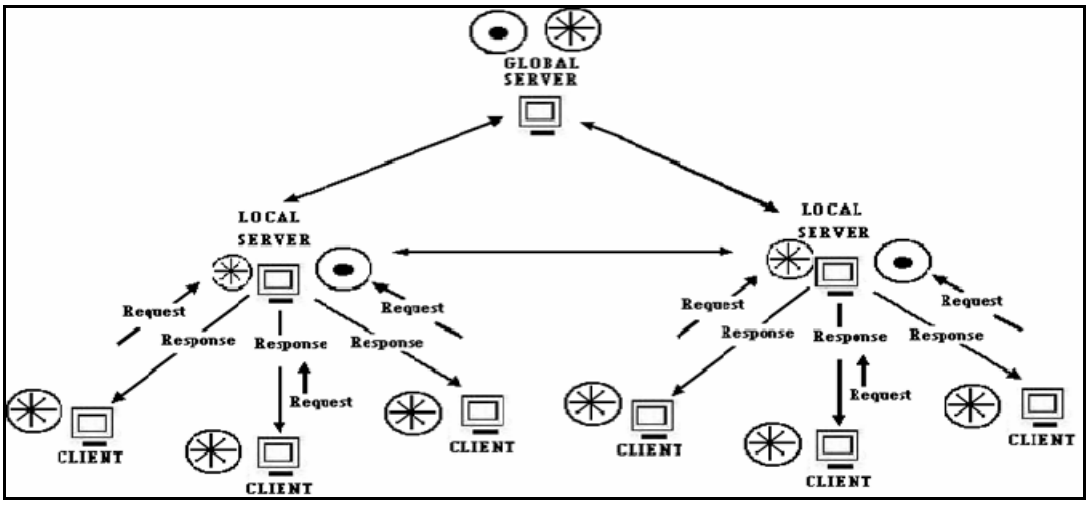


Figura 2.7 Modelo jerárquico cliente-servidor.

Algunos OSS (Operations Support System) que manejan algunas aplicaciones back-office, pueden ser modelados con este modelo de flujo.

Modelo de cómputo distribuido

El modelo de flujo de cómputo distribuido, mostrado en la figura 2.9, es el modelo más especializado. Este modelo puede tener características inversas del modelo cliente-servidor, o puede ser un híbrido: peer-to-peer y cliente-servidor. En este modelo los flujos pueden ser entre el dispositivo de administración de tareas y sus dispositivos de cómputo (como el modelo cliente-servidor) y/o entre dispositivos (como el modelo peer-to-peer).

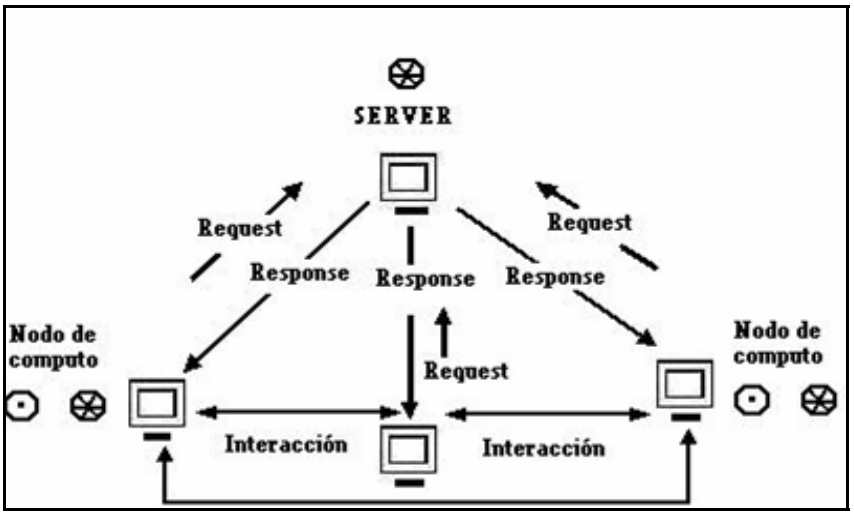


Figura 2.8 Modelo de computo distribuido.

En este modelo cada uno de los dispositivos tienen requerimientos más estrictos de desempeño, además se caracteriza porque las tareas pueden ser divididas entre los dispositivos o pueden llevarse a cabo de forma individual, de acuerdo a la disponibilidad de los dispositivos, además la transferencia de información puede ser poca o nula entre los dispositivos.

De acuerdo a la distribución de las tareas dentro del modelo de cómputo distribuido, los flujos se pueden identificar de dos formas: como **flujos en computing cluster** y como **flujos en parallel computing**.

Cuando las tareas entre los dispositivos (nodos de cómputo) son realizadas de forma individual y la relación entre ellos para realizar dicha tareas es nula, el modelo de cómputo distribuido toma la forma de **computing cluster** o **computing resource management system**, en donde las tareas son asignados a cada uno de los dispositivos de cómputo basados en la disponibilidad de sus recursos.

Flujos en computing cluster

Los flujos dentro de este tipo son similares a los flujos del modelo cliente-servidor. La diferencia es que la dirección de los flujos va desde los dispositivos de cómputo hacia el servidor, además los flujos son independientes entre ellos y son considerados como críticos.

Debido a que los flujos son asimétricos (no hay sincronización entre flujos individuales), el servidor (server) actúa como destino y los dispositivos de cómputo como fuente, como se muestra en la figura 2.10.

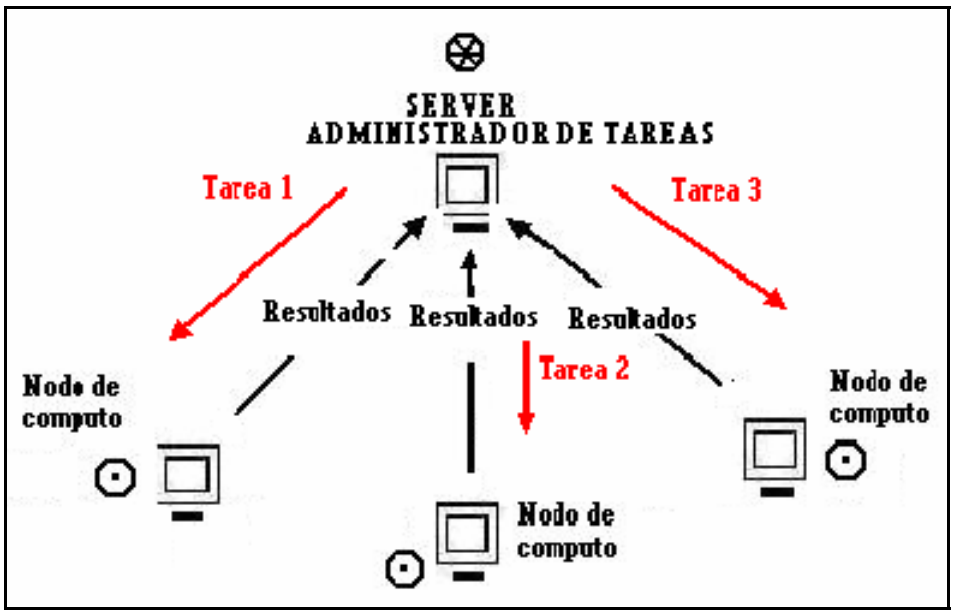


Figura 2.9 Flujos en computing cluster.

Flujos en parallel computing

El modelo de cómputo distribuido funciona como un sistema simplificado de procesamiento en paralelo, se da cuando una tarea es asignada a más de dispositivo y por tanto la relación entre ellos es muy estrecha, ya que trabajan en paralelo para realizar dicha tarea.

Cuando los dispositivos trabajan en conjunto intercambiando información con sus dispositivos vecinos, el flujo entre los dispositivos es considerado como crítico.

El servidor administrador de tareas configura a los dispositivos e inicia la tarea, como se muestra en la figura 2.11.

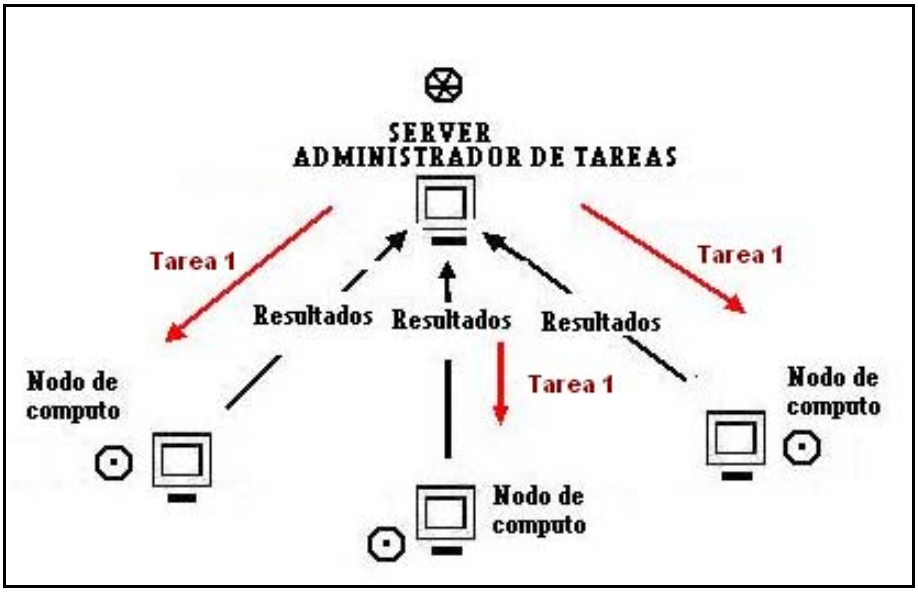


Figura 2.10 Flujos en parallel computing.

2.2.5 Prioridades de los flujos

Asignar prioridad a los flujos es importante ya que permite enfocarse a los aspectos que son más relevantes para el desempeño de la red. La prioridad se puede asignar acorde a la importancia de las características de los flujos.

Algunas asignaciones de prioridad se pueden hacer de acuerdo a:

- Los objetivos del negocio y el impacto del flujo en los negocios de los clientes.
- Política de la organización.
- Uno o más requerimientos de desempeño del flujo (capacidad, delay, RMA, QoS).
- Los requerimientos de seguridad de cada flujo
- El número de usuarios, aplicaciones y/o dispositivos que un flujo sirve.

El objetivo al asignar prioridad a los flujos es determinar los flujos que obtienen más recursos y cuáles flujos obtienen primero estos.

Se pueden usar más de un parámetro para asignar prioridad al flujo, creando múltiples niveles de prioridad.

2.2.6 Especificación de flujos

Los resultados de identificar, definir y describir los flujos conforman la especificación de flujos, también llamada **flowspec**. La especificación de flujo lista los flujos de una red, junto con sus requerimientos de desempeño y prioridad.

La especificación de flujos se presentará en la parte dos, en el capítulo "Caso práctico".

2.2.7 Diagrama de flujos

El mapeo de los flujos se presentará en el capítulo cuatro "Caso práctico".

2.3 Etapa tres: Análisis de seguridad

De acuerdo a los objetivos que se buscan en este trabajo, el desarrollo del análisis de seguridad de la red se dejará como opción de trabajo futuro a esta tesis. A continuación solamente se hace mención de un modelo de referencia de los niveles de seguridad que se recomiendan, y de tres consideraciones (direccionamiento, administración y desempeño), a tomar en cuenta cuando se implementa la seguridad de una red:

El modelo de arquitectura Acceso/Distribución/Core de Cisco [7], puede ser considerado al momento de determinar los niveles de seguridad que pueden ser requeridos. Este modelo separa a una red en tres bloques basados en su función, lo que puede permitir aplicar diferentes niveles de seguridad. Como se muestra en la figura 2.12, la seguridad es incrementada desde el área de acceso a distribución y hasta el core, ya sea incrementando mecanismos de seguridad o mejorando los existentes en cada nivel.

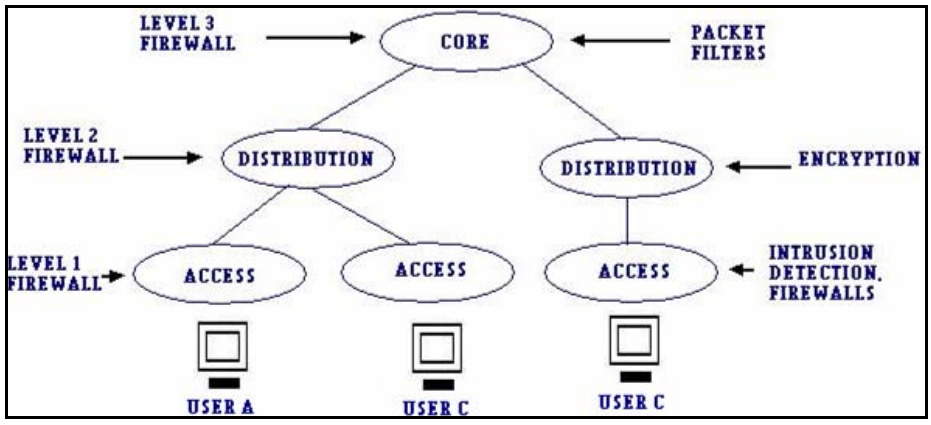


Figura 2.11 Modelo de arquitectura Acceso/Distribución/Core de Cisco,

Las zonas de seguridad están basadas en los requerimientos, determinados durante el proceso de análisis de requerimientos y deben ser descritas en el plan de seguridad.

Las siguientes consideraciones son importantes cuando se decide aplicar un mecanismo de seguridad:

La seguridad y el direccionamiento o ruteo

NAT es un mecanismo de direccionamiento que a menudo es usado para mejorar la seguridad. Sin embargo, cuando es aplicado para seguridad, este puede tener impacto en el direccionamiento de la red. Además el direccionamiento dinámico puede interferir con medidas de protección específicas y logging. Es más difícil controlar el intercambio de información ya que las direcciones cambian constantemente.

La seguridad y la administración

La seguridad depende de la administración de la red para configurar, monitorear, manejar y verificar los niveles de seguridad a través de la red. Adicionalmente, algunas veces se tiene necesidad de acceso para mantenimiento aún cuando haya ataques y si no se tiene disponible out-band access, se puede tener problemas, ya que no se tiene acceso a la red.

La seguridad y el desempeño

Los mecanismos de seguridad pueden afectar el desempeño de la red. Cuando la seguridad es de alta prioridad, los mecanismos de seguridad impactan en los flujos de tráfico y pueden restringir los mecanismos de desempeño que operan dentro de las zonas de seguridad minimizando el performance. Cuando el performance tiene alta prioridad, particularmente cuando es una necesidad para proveer desempeño end-to-end entre seleccionados usuarios, aplicaciones o dispositivos, los mecanismos de desempeño pueden incluir el uso de mecanismos de seguridad que no interfieran con esas áreas de la red.

2.4 Resumen

Dentro del capítulo dos se desarrollaron las tres etapas del análisis del desempeño de la red: las condiciones iniciales y el análisis de requerimientos, el análisis de flujo.

Las condiciones iniciales y los requerimientos de los usuarios, aplicaciones, dispositivos y de la red, nos permiten conocer las condiciones del sistema y el estado que se desea del sistema, además ayuda para una toma decisiones más objetivas e informadas en el diseño y arquitectura de la red.

El análisis de flujos ayuda a determinar el origen y destino de la información, así como sus características cuantificables como capacidad, delay, fiabilidad, calidad de los niveles de servicio, para efectos de poder medir el desempeño de los servicios que la red entrega al resto del sistema.

Por los objetivos planteados en este trabajo el tema de seguridad no se desarrolló, sólo se hizo mención de un modelo de referencia para implementarla, así como de las interacciones con el direccionamiento, administración y desempeño.

A continuación se presentan los principales estándares y elementos de administración de redes.

Capítulo 3. Administración de la red

3.1 Conceptos de administración de redes

Administración de red, es el conjunto de funciones para controlar, planear, asignar, desplegar, coordinar y monitorear los recursos de red.

El proceso de administración consiste en elegir cuáles características de cada tipo de dispositivo de red y/o datos se monitorean y administran principalmente, así como en determinar la instrumentación (dispositivos y utilidades) para colectar todos los datos necesarios, además de procesar y analizar estos datos para ser presentados y/o almacenados como conjunto de resultados.

Una efectiva administración es crucial para el éxito de las organizaciones con redes de datos y/o voz. Lo principal es cubrir las necesidades del negocio – los requerimientos.

Es importante conocer los requerimientos, para determinar cuáles de ellos son vitales para el negocio, así como la estrategia de administración, protocolos y herramientas que se usarán.

La definición de administración de redes anterior es proactiva, pero también existe la administración reactiva mencionada posteriormente en este capítulo.

3.1.1 Tareas principales de la administración de redes

La administración de la red puede ser dividida en dos funciones principalmente:

1. Administración de la información a través del sistema
2. Administración de los elementos de administración

Estas dos funciones consisten en una variedad de tareas, entre ellas las principales que se detallan más adelante son:

- Monitoreo para la notificación de eventos.
- Monitoreo para el análisis de tendencias y planeación.
- Configuración de parámetros de red.
- Troubleshooting de la red.

3.1.2 Dispositivos de red y características

Los dispositivos de red tienen características que se pueden medir. Estas pueden ser agrupadas en end-to-end, por-enlace, por-red o por-características de los elementos.

Características end-to-end, son las que pueden ser medidas a través de múltiples dispositivos en el camino de uno o más flujos y a través de la red o entre dispositivos.

Características por-enlace, por-red y por-elemento, son específicas para un tipo de elemento o conexión. Estas pueden ser usadas individualmente o combinadas para formar características end-to-end. Ejemplo de características por-enlace son: la propagación del delay y la utilización del enlace. Ejemplos de características por-elemento en un router son; velocidad de envío de paquetes, utilización de buffer, fallos de autenticación.

3.1.3 Terminología

Algunos de los términos relacionados con la administración de red son:

Dispositivo administrado. Dispositivo que tiene que ser administrado (Por ejemplo: un Router o Switch).

Información administrada. Datos usados y colectadas durante la administración de un dispositivo.

Sistema de administración de red. Incluye las aplicaciones y componentes que monitorean y controlan a los dispositivos administrados.

Agente de administración. Software en un dispositivo administrado que colecta y almacena información de administración.

Protocolo de administración. Protocolo que intercambia la información administrada entre el sistema de administración y los dispositivos administrados.

3.2 Modelos de referencia para la administración de redes

Existen estándares internacionales para la administración de sistemas que permiten contar con sistemas de administración y operen en un entorno de múltiples fabricantes. Estos sistemas ayudan al administrador de red a supervisar, monitorear y abastecer redes con tamaños, productos y fabricantes variables.

Los principales estándares que se mencionan son: el modelo TMN y el estándar FCAPS. **[8]** Estos modelos proveen un punto común de referencia entre proveedores, operadores y clientes. Una estrategia en común puede ser desarrollada siempre que los participantes estén de acuerdo en el alcance de la administración. La mayoría de los usuarios tienen un intuitivo punto de vista de la administración de la red, pero la intuición es subjetiva, de ahí la importancia de los estándares.

3.2.1 Estándar ISO para la administración de redes

La administración de redes, por ser vital para las organizaciones, ISO desarrolló un estándar conocido por sus siglas como FCAPS (Fault, Configuration, Accounting, Performance, Security Management).

Fault management - Consiste en el procesamiento de eventos y alarmas. Detecta, aísla, notifica y corrige las fallas que ocurren para retornar al estado operacional de la red.

Configuration management - Consiste en manejar y mantener la información de configuración, incluyendo inventario de dispositivos, archivos de configuración y software.

Accounting management - Cosiste en monitorear y manejar el uso de los recursos de la red, como los servicios contratados y su facturación.

Performance management - Consiste en implementar controles de desempeño basados en la arquitectura de servicios IP. Monitorea y colecta las métricas de desempeño de los dispositivos de red y analiza esta información de manera que el desempeño puede ser proactivamente manejado para cumplir con los requerimientos.

Security management - Consiste en implementar controles de seguridad. Controla el acceso a los recursos de red y da soporte a las políticas de seguridad.

ISO declaró que todas las redes necesitan considerar cada uno de estos aspectos de administración, pero no necesariamente implementar todos estos.

A medida que la aceptación del FCAPS inició, más detalles fueron necesarios y estos vinieron con el TMF (Telemanagement Forum). El TMF (originalmente conocido como el TMN -Telecommunication Management Network), fue un cuerpo establecido por los operadores y proveedores de equipo para implementar soluciones prácticas de administración.

3.2.2 El modelo TMN (Telecommunication Management Network)

El modelo TMN (Telecommunication Management Network) fue promovido por las operadoras de telecomunicaciones.

El modelo TMN esta basado en el modelo OSI y ha sido adoptado de forma generalizada por los operadores de servicios de telecomunicaciones como forma de estructurar lógicamente el soporte de las actividades necesarias para su negocio. El modelo TMN fue definido por la ITU-T y proporciona una arquitectura de referencia para el intercambio de información de gestión entre los sistemas de operación y/o los equipos.

El modelo TMN muestra como la administración de redes puede ser vista como una estructura de varias capas, como se muestra en la figura 3.1.

El modelo esta dividido en cinco niveles, cada uno con diferentes funciones de administración y con interfaces que vinculan a los niveles inferiores y superiores.

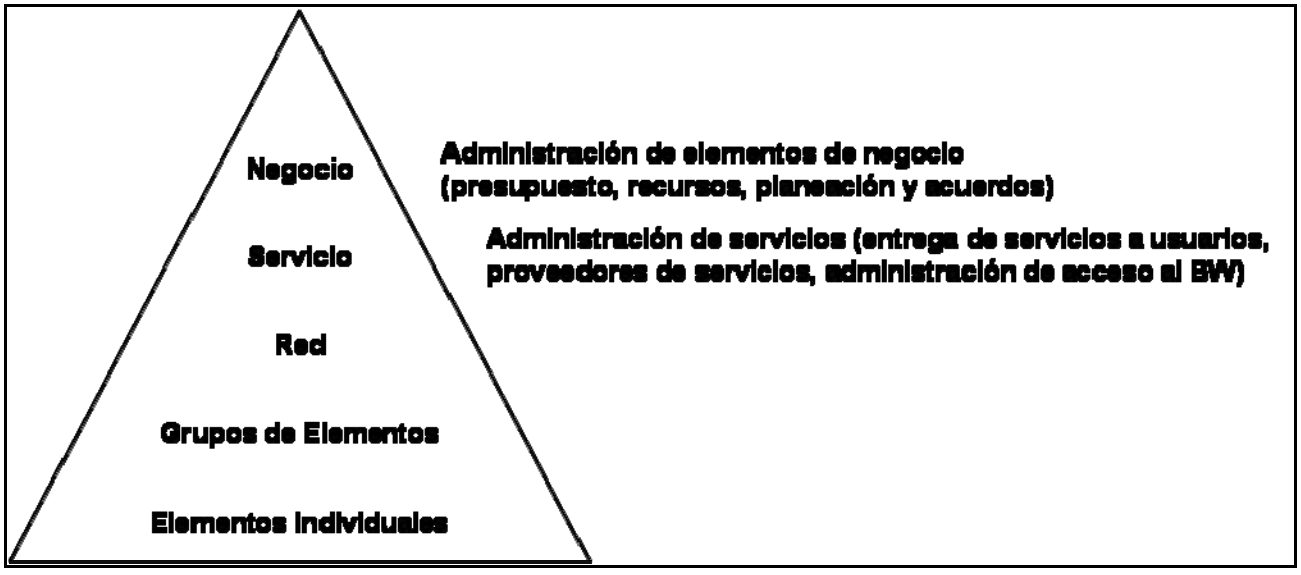


Figura 3.1 Niveles del modelo TMN.

Las principales tareas de administración en cada uno de los niveles del modelo TMN son los que se muestran en la figura 3.2.

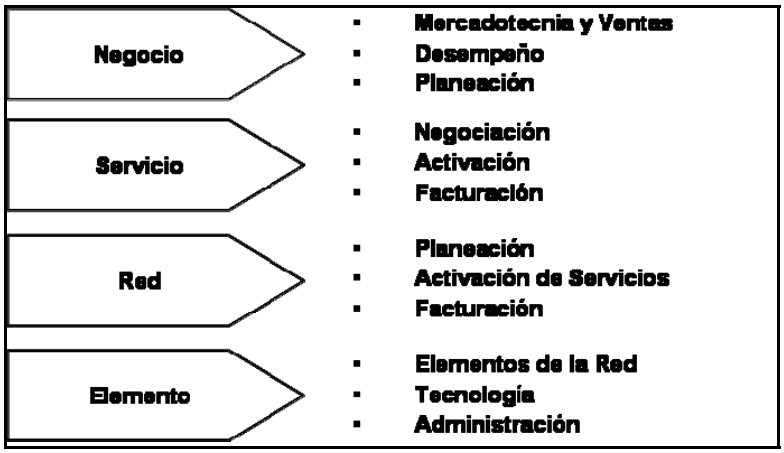


Figura 3.2 Principales tareas de administración del modelo TMN.

Para contar con más detalle de las actividades de administración dentro de las capas de servicio y red, se cuenta con las definiciones del Telecommunications Operations Map (TOM).

3.2.3 TOM (Telecommunications Operations Map)

El TOM define actividades específicas dentro de las capas de servicio y red. La definición exacta de las actividades y cómo se enlazan, es el primer paso en el diseño de la administración de la red.

La estructura del TOM es mostrada en la figura 3.3.

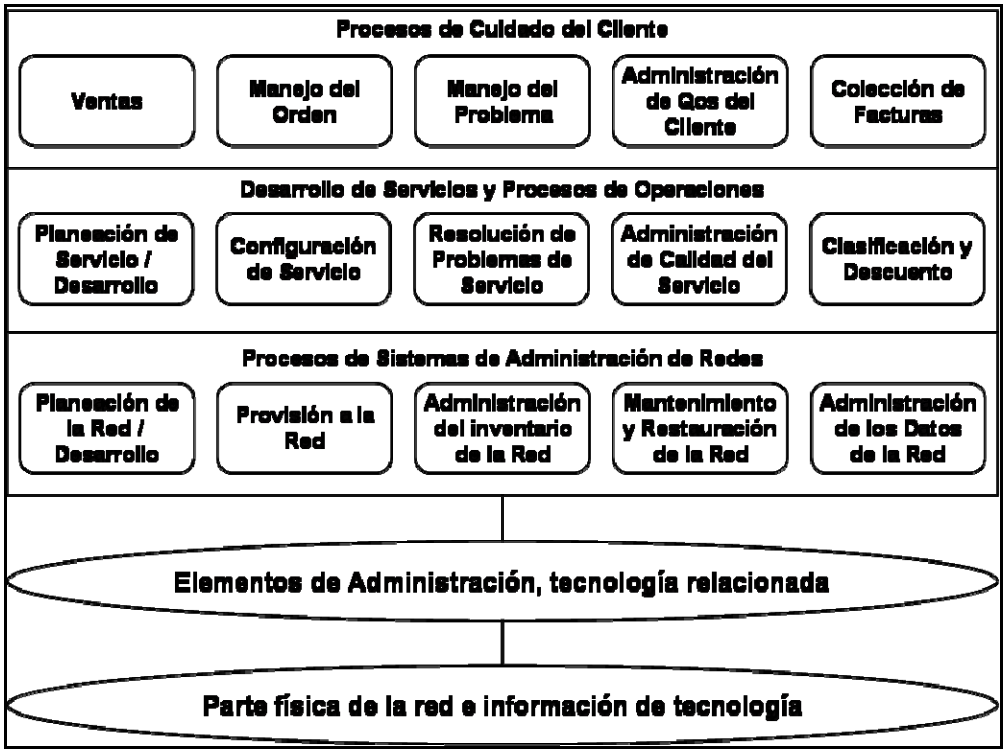


Figura 3.3 Estructura del TOM.

3.3 Tipos de administración

Existen dos tipos de administración de sistemas, la proactiva que “se adelanta a los hechos”, y la reactiva que “se encarga de las situaciones que ya se presentaron sin preverlas”.

3.3.1 Administración reactiva

La administración reactiva, o soporte, comprende la atención de los incidentes relacionados con la operación de la red que ya se presentaron. Incluye las tareas necesarias para identificar los problemas, así como las tareas necesarias para su corrección, además de las tareas de implementación de las medidas preventivas para evitar su repetición.

3.3.2 Administración proactiva

La administración proactiva, incluye las tareas de monitoreo, mejoramiento, prevención y corrección planificada, de acuerdo a las alarmas y reportes que se tienen de las herramientas y estrategias de administración de redes.

Debido a la importancia de anticiparse a los problemas que se puedan dar, a continuación se presentan algunos de los mecanismos que constituyen la administración proactiva como: protocolos y herramientas, monitoreo para la notificación de eventos y análisis de tendencias, instrumentación y configuración. Se dejará al final del presente capítulo, en la sección 3.10, los elementos de administración reactiva.

3.4 Mecanismos de administración proactiva

A continuación se presenta los dos principales protocolos para la administración de redes (SNMP y CMIP), así como algunas herramientas de administración.

3.4.1 Protocolos de administración de redes

Los protocolos principales que existen para la administración de redes son: SNMP y CMIP. Estos proveen los mecanismos para reparar, cambiar y transportar datos para administrarla.

a) Simple Network Management Protocol (SNMP)

SNMP es un protocolo que pertenece a la pila de UDP (User Datagram Protocol), ha sido ampliamente usado y forma la base de varios sistemas comerciales de administración de redes. Este provee facilidades para colectar, configurar y transportar información de administración.

Debido al auge que están teniendo las redes IP y sobre todo Internet, es uno de los protocolos de gestión más utilizados en la actualidad.

Las versiones existentes son SNMPV1, SNMPV2 y SNMPV3.

SNMPV1. Define cinco tipos de mensajes, entre la aplicación de administración y los agentes de administración:

Get request - Solicita una MIB especifica desde el agente (solicita el valor de un parámetro).

Get next request - Recupera la siguiente MIB desde una tabla o lista después del inicial get request (solicita el valor del siguiente parámetro en la lista).

Set request - Configura una variable MIB en un agente.

Get response - Una respuesta para un get request o get next request desde un administrador.

Trap message - Envía una alarma no solicitada para el administrador, cuando un dispositivo detecta un fallo.

SNMPV2. Incluye los siguientes nuevos tipos de mensajes.

GetBulk - Recibe una larga cantidad de datos (por ejemplo: tablas) en una petición así que múltiples mensajes get next request ya no son solicitados.

InformRequest - Similar al Trap message de SNMPv1.

SNMPV3. Esta basada en las versiones anteriores, provee más seguridad en la autenticación, la habilidad para manejar bloques de parámetros y la generación de traps para más parámetros.

Los parámetros accesibles vía SNMP están agrupados dentro de MIBs. Los parámetros pueden ser parte del estándar MIB (MIB-II); de otros estándares MIBs (basados en el tipo de dispositivo de red, tecnología o protocolo); MIBs de monitoreo remoto; o MIB específicos de una empresa (tienen parámetros que son específicos de un vendedor o producto en el mercado).

Management Information Base (MIB)

MIB es el estándar para colectar información de administración.

Una MIB es él o los parámetros que almacenan la información reunida por un agente de administración, localizado en un dispositivo administrado, para posteriormente sea utilizada por un protocolo de administración.

Cada objeto en una MIB tiene un identificador único. Las aplicaciones de administración especifican este identificador cuando desean utilizar un objeto específico.

Los estándares MIBs, son definidos en diferentes RFCs (Requests For Comments).

MIB-II está definido por el RFC 1213 ("Management Information Base for Network Management of TCP/IP-based Internets: MIB-II") y es una extensión del original MIB-I.

SNMP únicamente proporciona un marco o infraestructura para realizar el desarrollo de aplicaciones de gestión de red. Este marco consta del protocolo mediante el que los actores implicados (gestores y agentes) intercambian información de gestión, la estructura de dicha información, los tipos de datos que la soportan y la base de datos mantenida por los agentes en la que se almacena la información de gestión.

Como se ve en la figura 3.4, quedan fuera del estándar SNMP aspectos como la definición de las propias aplicaciones de gestión, el mecanismo concreto utilizado en el diálogo del agente con los recursos (objetos gestionados), los detalles de implementación, etc.

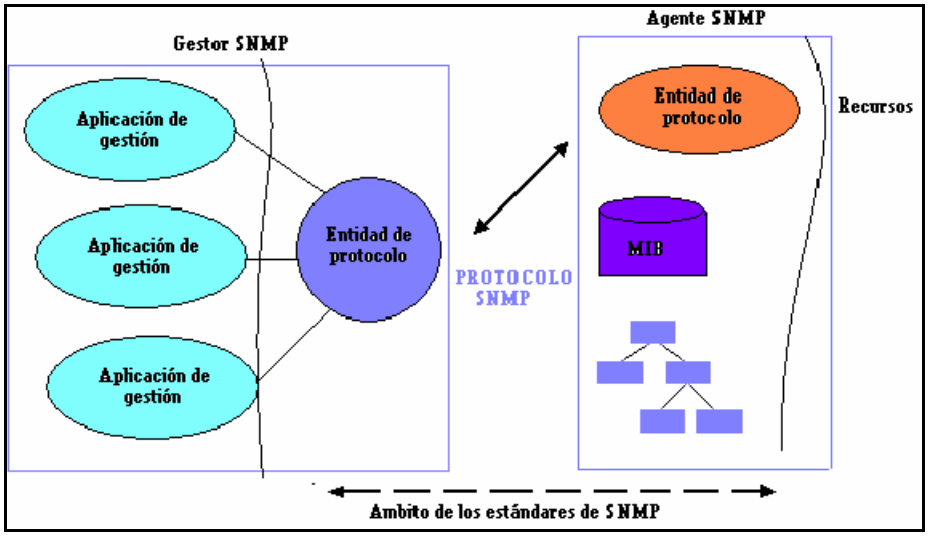


Figura 3.4 Ámbito de SNMP.

Para realizar las funciones de gestión, el gestor utiliza un mecanismo de sondeo (polling) para comunicarse con los agentes. El sondeo permite limitar la cantidad de información que debe procesar, así como los recursos gestionados. Del lado del agente se utilizan interrupciones, lo que hace que el tráfico sea poco predecible, lo que puede provocar situaciones de exceso de carga no deseadas.

SNMP utiliza un mecanismo intermedio (trap-directed polling) que se basa en el envío por parte del agente de un tipo especial de interrupción (trap), el cual desencadena en el gestor una operación de sondeo. Los traps sólo se envían ante situaciones de importancia.

Uno de los principales objetivos principales de SNMP es que sea sencillo, cualidad que se ha conseguido sacrificando algunos aspectos de gestión de redes y servicios. Por ejemplo, el mecanismo de envío de “Trap” no tiene la potencia de las notificaciones de CMIP utilizado en el modelo TMN, ya que la información en el “Trap” no permite al gestor distinguir la gravedad de los eventos que han ocurrido en la red. SNMP tampoco dispone de mecanismos con la potencia de filtrado y ámbito de CMIP. Otro aspecto débil de SNMP es el tema de seguridad, que no estaba tratado en la primera versión del protocolo y aunque se ha mejorado, no se ha llegado a una solución definitiva al respecto.

b) CMIP (Common Management Information Protocol over TCP / IP [CMOT])

Provee colección y configuración de parámetros, como SNMP, además permite otras operaciones. Algunas de las características de CMIP/CMOT son: nombrar globalmente a un objeto, clasificación de objetos, reportes de alarmas, pruebas de administración. Algunas características pueden ser implementadas con SNMP creando nuevas MIBs y herramientas.

SNMP es más simple en su configuración y uso que CMIP/CMOT, razón por la que es más usado. SNMP es usado en mecanismos de monitoreo, instrumentación y configuración, los cuales serán vistos a continuación.

3.4.2 Herramientas de administración de redes

Hay un gran número de sistemas de administración en el mercado, algunos que han permanecido y otros nuevos. Ciertos de los sistemas disponibles abarcan completamente el TOM, mientras otros sólo cubren una parte de éste. Algunos están optimizados de acuerdo a determinados vendedores e incluyen interfaces propietarias, mientras que otros son construidos para el mercado abierto y usan interfaces y protocolos estándares. Las capacidades y calidad de las herramientas de administración varían enormemente y al paso del tiempo aparecen o desaparecen algunos.

Dada la volatilidad de las herramientas en el mercado y larga lista de sistemas de administración, se presentarán las principales categorías de las herramientas y algunos ejemplos de estas.

Plataformas de administración total

A lo largo de los años han existido intentos para producir un sistema que abarque todas las funciones de administración. Algunos de los principales operadores y fabricantes de equipos, tales como IBM, AT&T y Nortel, han tratado de construir este tipo de sistemas.

NetView de IBM, es un ejemplo del peligro que se tiene al centralizar todas las funciones de administración. El NetView tuvo una fuerte orientación hacia manejar programas de monitoreo de transacciones (por ejemplo: CICS, IMS) y podía ser usado en sistemas IBM o compatibles y contaba con su propio protocolo SNA (Simple Network Architecture) de IBM. La complejidad del producto creció en el tiempo, volviéndose no rentable.

Herramientas de administración de clientes

Esta categoría de herramientas debe habilitar al operador de la red a tratar efectivamente las peticiones, órdenes y otras interacciones y por lo tanto proveer un buen servicio. Algunos proveedores en esta área son Siebel, Vantive, Clarify y Remedy. Las herramientas de estos proveedores son generalmente referidas como CRM (Customer Relationship Manager). Todas ofrecen facilidades para seguir las interacciones y progreso de las peticiones de los clientes (ejemplo: activación de servicios, ordenes, tiempo de solución de problemas), hasta que se completan. Algunos ejemplos dentro de esta categoría que proveen sistemas de facturación son: Kenan, Portal y Amdocs.

Herramientas de administración de servicios

Estas herramientas manejan los niveles de los servicios y son probablemente las menos maduras en establecer procesos específicos para manejar estos servicios. Hay un número razonable de este tipo de herramientas, que permite a un operador de servicios cumplir con las peticiones del cliente, como configuraciones apropiadas de los componentes de la red. Esta capacidad es referida como diseño de servicio y es soportada por herramientas de proveedores como Architel y Orchestream (se enfoca en la conectividad física) y Netscape iPlanet (el cual se enfoca en la configuración lógica, configurando políticas de ruteo). BEA Weblogic cae dentro de esta categoría.

Herramientas de administración de red

Este tipo de herramienta interactúa directamente con los elementos de la red, vía elementos de administración que están asociados con un específico equipo. Las principales características de esta categoría son la habilidad para enviar alarmas y recibir el estatus de la información del desempeño de los dispositivos de red. Los proveedores en este nivel son Micromouse y Smarts, los cuales han desarrollado adaptadores y software que trabajan juntos sobre cualquier tecnología; y Cisco con CiscoWorks, que optimiza la administración de una red implementada con equipo Cisco.

Herramientas de soporte

Adicional a las herramientas ya mencionadas, existe un grupo de herramientas que no tienen un especifico rol en la red, servicio y cliente, pero proveen soporte a estas. Por ejemplo, las herramientas de inventario además de almacenar las configuraciones, también la información de enlaces, servicios y clientes son almacenados. Algunos proveedores de herramientas de inventario son SmallWord, Cramer y Metasolv. Otras herramientas de soporte incluyen gateways de proveedores como Crosskeys, network planning de Netplan y reporting de Concord.

Integración de frameworks

Hay una amplia variedad de frameworks para administración en el mercado, las cuales se han venido integrando para ofrecer herramientas más completas y compatibles. HP OpenView Network Node Manager es probablemente el más usado. OpenView es generalmente usado por operadores que deben supervisar diversas tecnologías y proveer sistemas específicos. HP OpenView colecta información de varias fuentes y presenta esta información reunida, sin necesidad de implementar diferentes sistemas de administración.

NCRS StarSentry Manager, Compaq TeMIP, SunConnect SunNet Manager y Novell Network Management System (NMS), son algunos ejemplos de las soluciones de integración de sistemas de administración.

Herramientas de administración de sistemas

Son los sistemas que se encargan de supervisar la comunicación en las redes conocidos como OSS, deben ser manejados como otro software operacional. Hay un número de herramientas de administración, que tienen como objetivo monitorear el software operacional. BMC Patrol, Tivoli y CA Unicentre son ejemplos de estas herramientas.

Los OSS (Operations Support Systems) son sistemas de gestión usados para provisión, mantenimiento, monitoreo de eventos, facturación de los servicios, configuración, entre sus principales funciones. Existen varios paquetes OSS ahora disponibles en el mercado que se usan dentro de soluciones de administración.

Este tipo de sistemas son usados por los suministradores e integradores de sistemas, los cuales son motivados por la necesidad de encajar nuevos sistemas en estructuras de gestión existentes y por la necesidad de integración de sistemas como consecuencia de las adquisiciones y fusiones entre empresas que se están produciendo.

3.5 Mecanismos de monitoreo

Monitoreo es obtener los valores de las características de extremo a extemo por-enlace o por-elemento. El proceso de monitoreo involucra la colección de datos de las características deseadas, el procesamiento, el despliegue y almacenamiento de todos o algunos de estos datos.

Algunos valores son presentados como se obtienen y otros valores pueden ser modificados antes de presentarlos (adicionados, restados, simplificados). Esto es llamado procesamiento de datos.

Durante el proceso de monitoreo hay dos partes importantes: el despliegue y almacenamiento de los datos colectados durante el monitoreo.

Los datos pueden ser desplegados en diferentes tipos de displays como wide-screen o de pantallas de propósito especial. La elección es de acuerdo a las necesidades que se tengan.

El almacenamiento de la información colectada durante el monitoreo puede ser parcial, total o periódico. El almacenamiento primario consiste en conservar los datos por un corto periodo y puede hacerse en los dispositivos de administración; el almacenamiento secundario es agregar más dispositivos de almacenamiento para no saturar a los dispositivos de administración; el almacenamiento terciario consiste en almacenamiento permanentemente de los datos, es más lento y necesita de diferentes dispositivos de almacenamiento.

3.5.1 Tipos de monitoreo

Monitoreo para la notificación de un evento

Un evento es algo que ocurre y que amerita ser tomado en cuenta. Este pude ser un problema, un fallo de un dispositivo en la red, una característica que sobrepasa un límite, o una notificación para el usuario o administrador.

Los eventos pueden ser anunciados en un archivo, en un display o hasta con una alarma, de acuerdo a su prioridad.

La Figura 3.5 muestra un ejemplo de monitoreo para la notificación de un evento.

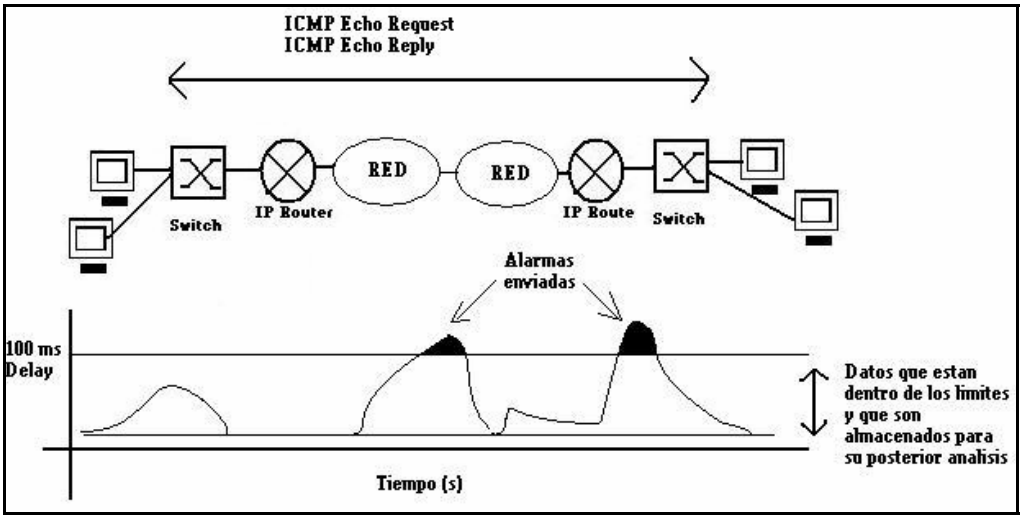


Figura 3.5 Monitoreo para la notificación de un evento.

Pueden establecerse umbrales y límites en características end-to-end, por-enlace, por-elemento, con corta o inmediata notificación de eventos (tiempo real).

Para el análisis en tiempo real es necesario determinar el número de características para analizar los dispositivos de administración, así como la cantidad de recursos (capacidad, CPU, memoria, almacenamiento).

Monitoreo para análisis de tendencias y planeación

El análisis de tendencias usa la información administrada para determinar el funcionamiento de la red por largos periodos de tiempo o las tendencias. Es muy útil para planear el futuro crecimiento de la red, así como para proponer mejoras o prevenir fallas. La figura 3.6 muestra un ejemplo de graficas de tendencias a largo plazo de algunas métricas de desempeño.

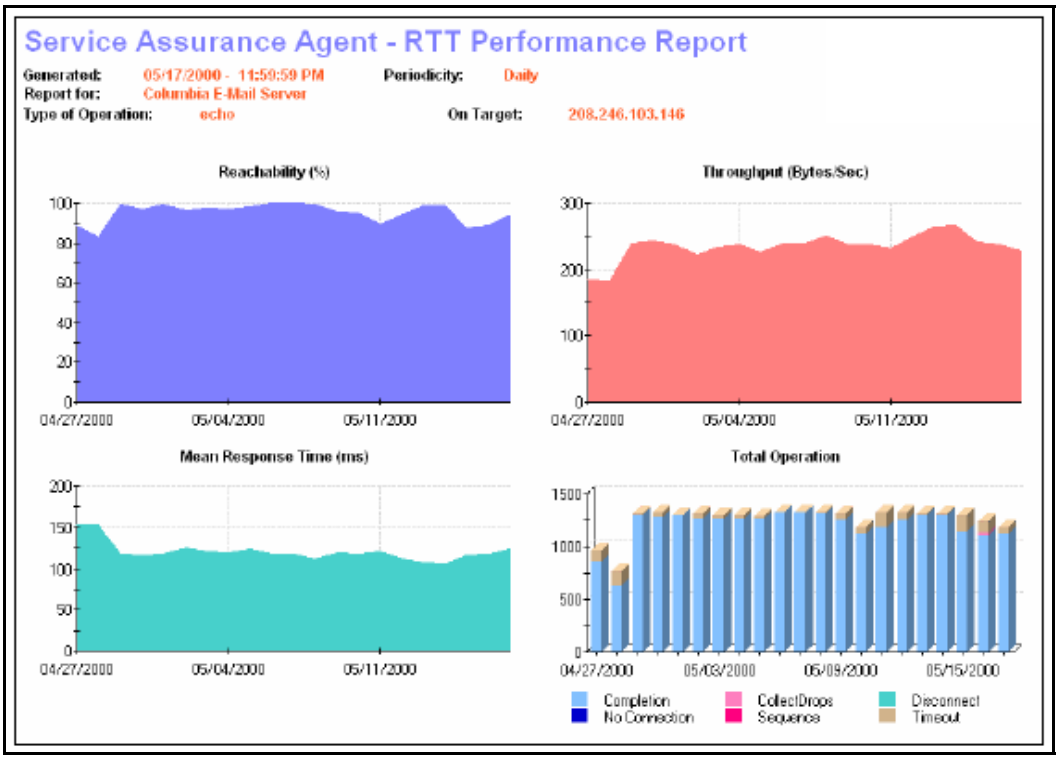


Figura 3.6 Monitoreo de métricas para análisis de tendencias.

Para realizar el monitoreo de las medidas de desempeño de la red, es importante saber que existen dos maneras de hacerlo, las que se mencionan a continuación:

3.5.2 Formas de tomar las medidas de desempeño

Existen dos formas para tomar las medidas de desempeño, como se muestra en la figura 3.7.

- Dentro de una ambiente de pruebas.
- En la red en funcionamiento.

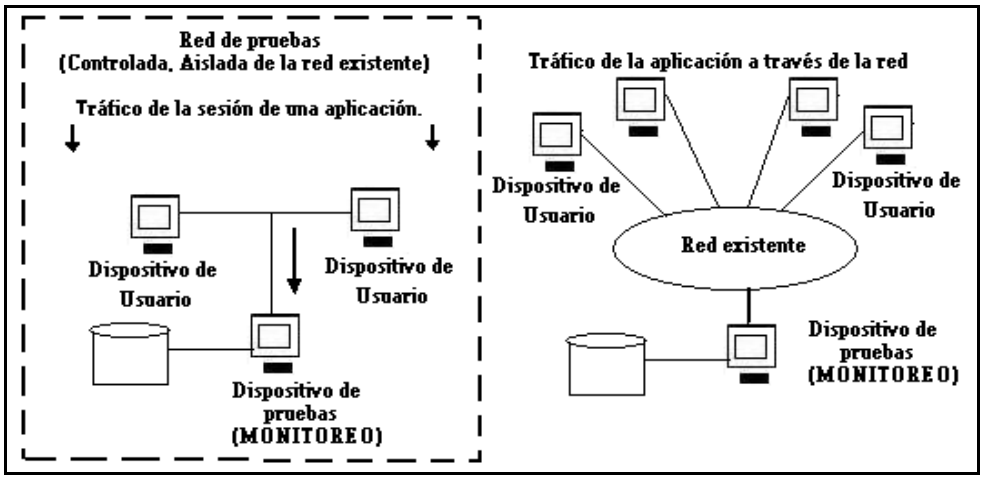


Figura 3.7 Formas de tomar las medidas de desempeño en una red de pruebas y en la red en funcionamiento.

En la primera se utiliza una red de pruebas con condiciones controladas, en dónde los dispositivos y aplicaciones son probados antes de ponerlos en la red de producción. La segunda consiste en medir los niveles de desempeño de una red en pleno funcionamiento, como se hará en este caso.

Cabe mencionar que en la mayoría de los casos, las empresas por cuestiones de costos, no cuentan con una red de pruebas, y sólo cuentan con la red operativa para tomar las medidas de desempeño de la red. En el caso práctico, se recolectarán los datos de desempeño de la red operativa en estudio.

3.5.3 Herramientas adicionales para monitoreo

Además de los protocolos de administración de red (CMIP y SNMP), existen herramientas comunes como el comando ping extendido (Packet InterNet Groper), el cual mide round-trip delay; el pathchar (disponible desde ee.lbl.gob), el cual combina el round-trip delay y per-peak capacity con trazado de los saltos, como con el comando traceroute. Otra herramienta para analizar tráfico es TCPdump.

3.5.4 Diagrama del sistema de monitoreo en la red

Ya que se analizará el desempeño de los servicios, las métricas serán aplicadas específicamente al trafico de los servicios que la red provee, la figura 3.8 muestra un ejemplo de una red con un sistema de monitoreo.

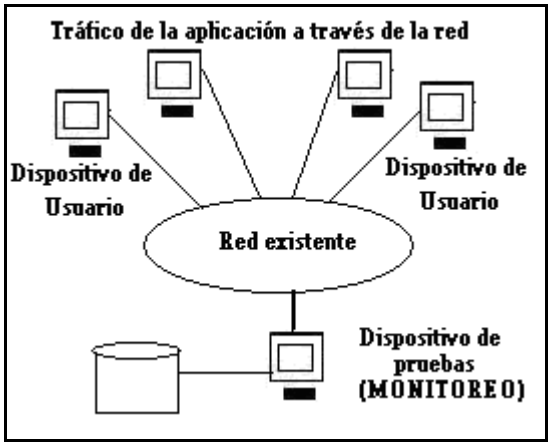


Figura 3.8 Ejemplo de una red con un sistema de monitoreo.

3.6 Mecanismos de instrumentación

La instrumentación es el conjunto de herramientas y utilidades necesarias para monitorear y llevar a cabo la administración de datos en la red. Los mecanismos de instrumentación incluyen el acceso para la administración de red vía SNMP, herramientas de monitoreo y acceso directo. La instrumentación puede ser usada junto con el monitoreo, el despliegue, el procesamiento y almacenamiento, para formar un completo sistema de administración.

Para que un sistema de administración trabaje apropiadamente, la instrumentación necesita ser precisa, fiable y simple. Para asegurar que es precisa, se puede probar y tomar medidas alternativas. Por ejemplo, si se cuenta con un laboratorio de pruebas, algunas condiciones de la red pueden ser replicadas y probadas.

Un sistema de administración es inútil si lo primero que falla cuando ocurren problemas en la red, son los mecanismos de instrumentación. Se puede contar con sistema de administración fiable, contando con redundantes componentes de administración distribuidos, así como con una jerarquía en la administración de flujos de datos, para así tener menos impacto cuando uno de estos falle.

3.7 Mecanismos de configuración

La configuración es establecer los parámetros en un dispositivo de red para su operación y control. Ver figura 3.9.

Los mecanismos de configuración incluyen:

- Conjunto de comandos SNMP.
- Telnet y acceso a la interfaz de línea de comandos (CLI).
- Acceso vía HTTP.
- Acceso vía CORBA (Common Object Request Broker Architecture).
- Descarga de archivos de configuración vía FTP o TFTP.

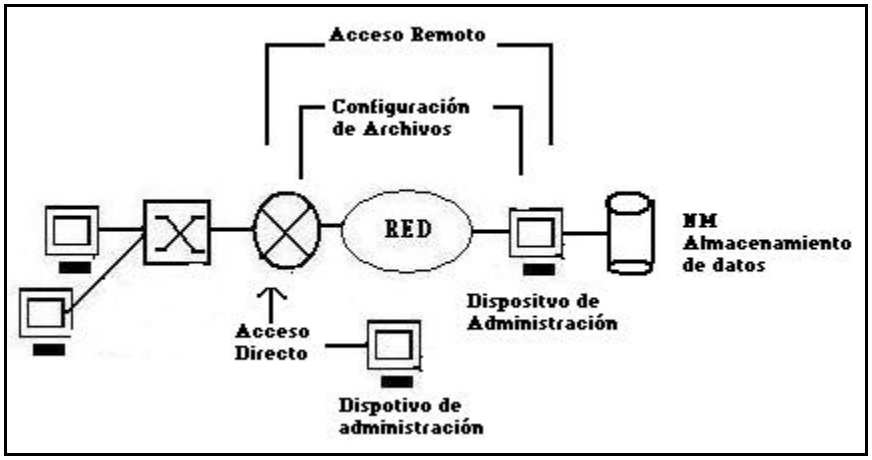


Figura 3.9 Mecanismos de configuración.

3.8 Estrategia de administración

Una estrategia para la administración permite obtener el detalle de la información que será colectada y analizada, así como los protocolos y herramientas que se pueden seleccionar.

Es importante trabajar de manera proactiva dentro de la administración de la red, por medio de alertas y reportes de las métricas de desempeño, antes de que se presenten fallos.

Algunas recomendaciones para tener mejores prácticas en la administración de la red son:

- Mantener una copia de los archivos de configuración y/o imágenes del sistema operativo.
- Mantener a la mano y actualizado un control de cambios del software.
- Monitorear parámetros críticos, incluyendo reportes del sistema (syslogs), SNMP traps y RMON statistics, que sean importantes para la red.
- Usar herramientas para identificar cualquier discrepancia de configuración.
- Determinar el número de sistemas de administración requeridos de acuerdo al número de usuarios finales y otros dispositivos; la cantidad de datos que serán colectados; y la capacidad del sistema.
- Tener en cuenta el ancho de banda requerido para la administración de datos. Por ejemplo, si varios mensajes syslogs son enviados a través de un enlace WAN, en ancho de banda pude ser saturado.

3.8.1 Service-Level Contracts (SLCs) y Service-Level Agreements (SLAs)

SLCs y SLAs son parte de la estrategia de administración además de ser elemento clave en la calidad de servicio.

Un SLC especifica la conectividad y los niveles de desempeño de los servicios entregados por los proveedores de servicio al usuario final.

SLA es la medida de desempeño de un servicio específico entre dos dispositivos. Por ejemplo, entre un router y un server.

Un SLCs puede incluir múltiples SLAs.

Un proveedor de servicio puede ser interno - un departamento de TI que provee de servicios a los usuarios, o externo - un ISP (proveedor de servicios de Internet).

3.9 Consideraciones en la arquitectura de administración

3.9.1 Administración In-band y Out-of-band

La administración **In-band** ocurre cuando el flujo del tráfico de administración sigue el mismo camino que el flujo de las aplicaciones de los usuarios. Esto simplifica la arquitectura de administración, ya que el mismo camino puede ser usado por ambos tipos de datos y no es requerido un camino adicional (y posible red).

Un problema que surge en la administración In-band, es que el flujo de administración puede ser afectado por los mismos problemas que impactan con el flujo de usuarios. Por ejemplo, cuando la red esta fallando y hay congestión de tráfico o riesgo en la seguridad, no será posible monitorearla ya que el flujo de administración también es afectado.

La administración **Out-of-band** ocurre cuando usan diferentes caminos el flujo de usuarios y el de administración, es implementada por medio de otra red, como Frame Relay, ATM o conexiones POTS (Plain Old Telephone Service).

Las ventajas de la administración Out-of-band:

- Permitir la administración de la red aún cuando surjan eventos que deshabiliten a la red, esto permite identificar la localización de la falla.
- Características adicionales de seguridad integradas en la red de administración, ya que esta red provee acceso para la mayoría de los dispositivos.
- Las conexiones out-of-band pueden ser usadas para la solución de problemas y configuración remota de dispositivos, lo que ahorra tiempo y dinero.

Una desventaja es la complejidad y costos adicionados.

Algunas redes combinan la administración In-band y Out-of-band, como se muestra en la figura 3.10, permitiendo que el flujo de administración use el mismo camino del flujo de datos cuando este no falle y usar un camino alternativo cuando falle.

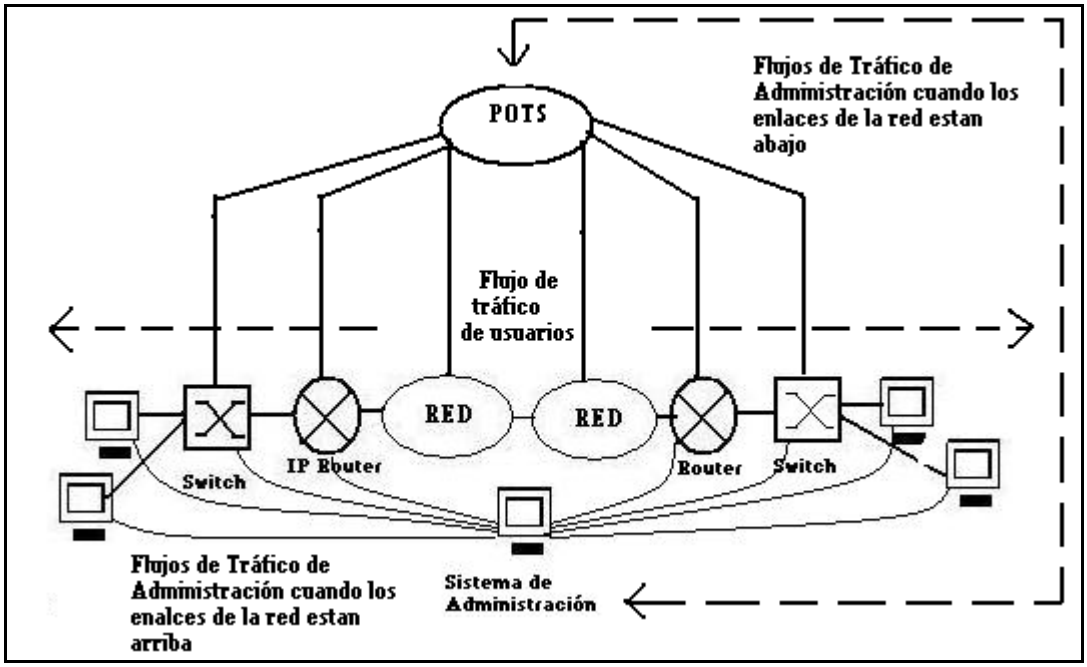


Figura 3.10 Combinación de la administración In-band y Out-of-band.

3.9.2 Administración centralizada y distribuida

Administración centralizada es cuando un sistema de administración de red es implementado en un punto.

Simplifica y reduce costos, pero tiene desventajas, como formar un punto de fallo y la convergencia de flujos en la interfaz del sistema de administración, potencialmente causando congestión o fallas.

Administración distribuida, es cuando múltiples componentes del sistema de administración se encuentran estratégicamente a lo largo de la red, distribuyendo las funciones de administración.

3.9.3 Tráfico de administración

Algunas recomendaciones que ayudan a determinar y optimizar la capacidad de los requerimientos del tráfico de administración son:

1) Para una LAN, se puede usar un dispositivo de monitoreo por subred. Hay que estimar los valores de las siguientes variables del tráfico:

- Número de dispositivos de red que serán monitoreados.
- Número promedio de las interfaces por dispositivo.
- Número de parámetros que serán colectados.
- Frecuencia de monitoreo (intervalo de monitoreo).

La combinación de estas variables, puede proporcionar un promedio de la cantidad de tráfico de administración por subred. Si el tráfico de administración es mayor al 10% de la capacidad de la red LAN, se debe considerar reducir la cantidad de tráfico de administración. Si el tráfico de administración es menor del 1% de la capacidad de la LAN, se pueden incrementar las variables a medir.

2) Para un ambiente WAN, se puede iniciar con un dispositivo de monitoreo para cada interfaz WAN-LAN.

Para la mayoría de los estándares de tecnologías LAN (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI), el tráfico de administración debe ser del 2 al 5% de la capacidad LAN:

10 Mb/s Ethernet	5% -> 500 Kb/s 2% -> 200 Kb/s
100 Mb/s Fast Ethetnet	5% -> 5 Mb/s
	2% -> 2 Mb/s
1000 Mb/s Giga Ethernet	5% -> 50 Mb/s 2% -> 20 Mb/s

3.9.4 Inspección y balance

La inspección y balance son métodos que duplican las medidas para verificar y validar la administración de la red. Es conveniente tener más de un método para colectar datos para la administración de la red, principalmente para datos que son considerados vitales para la apropiada administración. Los agentes SNMP y las MIB son implementaciones específicas en cada sistema de administración comercial, que no garantizan proporcionar datos que sean consistentes a través de toda la red.

Los objetivos de la inspección y balance son:

- Errores en el almacenamiento o presentación de los datos.
- Reiniciación de variables tipo contador sin notificación.
- Cambios de variables MIB de una versión de software a otra.
- Normalizar la administración de la red si está implementada con múltiples herramientas.

La colección de datos de administración debe ser verificada con precisión. Por ejemplo, cuando se utilizan variables SNMP para una interfaz, se puede considerar utilizar RMON para verificar estos datos. Se puede considerar usar un analizador de tráfico para verificar datos en períodos de tiempo aleatorios. También se pueden utilizar dispositivos generadores de tráfico y dispositivos para colectar datos.

3.9.5 Administración de la información administrada

Los flujos de administración de datos consisten en nombres, valores de los parámetros y resultados de queries de utilidades, como el ping o traceroute. Es importante para la arquitectura de administración de redes, entender cómo los datos son generados, transportados, procesados y almacenados, para determinar en dónde los componentes de administración deben ser colocados en la red. Algunas recomendaciones para administrar esta información son:

1) Elección del tipo de almacenamiento.

Determinar cuáles datos se necesitan mantener localmente y temporalmente almacenados, y cuáles deben ser almacenados externamente.

2) Copiar selectivamente los datos.

Cuando un parámetro de administración se utiliza tanto para notificación y análisis de tendencias, se debe considerar copiar y almacenar aparte ese parámetro cada N interacción. En donde la cantidad de interacciones debe ser lo suficientemente grande para mantener lo más pequeño posible el tamaño de los datos, y suficientes para el análisis.

Para evitar la perdida de datos al ser copiados, se debe considerar el uso de TCP para la transmisión y almacenamiento redundante.

3) Migración de datos.

Cuando los datos son colectados para análisis de tendencias y planeación, pueden ser almacenados localmente, y posteriormente almacenados en otros dispositivos una vez que no se afecte el tráfico de la red (en la noche).

4) Metadatos.

Los metadatos incluyen información adicional de los datos colectados, como referencias del tipo de datos, fechas de cuando fueron generados y marcas de identificación.

3.9.6 Selección de MIB

Determinar cuáles SNMP MIBs se usarán y aplicarán, así como las variables de cada MIB que sean apropiadas para la red. Puede ser toda una MIB (MIB-II), un conjunto de cada MIB o una MIB específica. Por ejemplo, un subconjunto de parámetros para el monitoreo de desempeño, que puede ser usado desde las interfaces MIB (RFC 2863), es: ifInOctets, ifInErrors, ifInUcastPkts, ifOutOctets, ifOutErrors, e ifOutUcastPkts. Estos seis parámetros pueden ser medidos en todas las interfaces de la mayoría de los dispositivos de red.

3.10 Administración reactiva

Aunque no es una buena práctica la administración reactiva (ó también llamada Troubleshooting), es importante mencionar los principales elementos de esta, ya que de ella se desprenden los elementos y procedimientos para detectar y solucionar los problemas que se generen.

Lo ideal es que la administración reactiva debe ser utilizada sólo en situaciones extraordinarias.

En general los puntos de la administración reactiva son:

- Detectar y/o tener el problema.
- Localizar el problema(s).
- Pruebas de diagnóstico (en caso de ser posible).
- Corrección de la falla.
- Implementación de herramientas para prevenir el mismo problema.

Dentro de la administración reactiva, el factor a controlar es el tiempo de la solución de la falla (MTBF), y en la mayoría de los casos, este depende principalmente del elemento humano, así como de los procedimientos y planes en caso de fallas que se manejen.

Principales elementos de la administración reactiva

El primer elemento que dentro de la práctica considero más importante, es el elemento humano, y de él, principalmente sus características y capacidades para ofrecer soluciones a las diversas situaciones que se presentan día a día.

El segundo elemento importante son los procedimientos y políticas con los que cuente la empresa, en caso de fallas.

El tercer elemento son las herramientas: equipo, acceso, passwords.

3.11 Resumen

Una vez puesta en marcha una red, es fundamental tener un plan de administración de la misma. Esto implica conocer los diferentes estándares y mecanismos de administración, que proporcionan un margen de referencia para administrar las redes de acuerdo a las necesidades y recursos de cada empresa, cumpliendo con los estándares definidos internacionalmente. Principalmente, la administración de red nos permite definir qué elementos se administran, qué herramientas de administración existen y cómo llevar a cabo esta administración, y con esto tener el control de la red día a día.

A continuación se desarrollará el caso práctico, objetivo de esta tesis.

Capítulo 4. Caso práctico: Aplicación de la metodología

Descripción de la metodología de sistemas aplicada a las redes

A continuación se menciona en que consiste la metodología de sistemas aplicada a las redes, y que es la base para el desarrollo del presente trabajo.

La metodología se fundamenta en que la red y todo lo que tenga relación o impacto sobre ella es un sistema, lo que permite ver las interacciones y dependencias entre la red, sus usuarios, aplicaciones y dispositivos. Asociado a este sistema hay un conjunto de servicios (niveles de desempeño y funciones) que son ofrecidos por la red para el resto del sistema. Analizar el desempeño de estos servicios que la red debe proveer y soportar, es el principal objetivo de esta tesis.

Este trabajo se basa principalmente en la etapa de análisis de una red en operación y sólo se desarrollan los principales elementos de la arquitectura y diseño.

Por último, la metodología de sistemas puede ser aplicada para una variedad de redes, desde pequeñas que proveen conectividad básica, hasta grandes y complejas, como plataformas de servicios (redes de tercera generación).

En base a lo anterior, la metodología de sistemas aplicada a las redes de datos se utilizará para analizar una red de la siguiente forma:

1. Obtener la red en funcionamiento.
2. Obtener las condiciones iniciales del sistema.
3. Especificar las medidas de desempeño de la red.
4. Reunir información de las medidas de desempeño de la red (por medio de una herramienta de monitoreo de red).
5. Realizar el análisis de la red en tres pasos:
   - Análisis de requerimientos.
   - Análisis de flujo de información.
   - Análisis de seguridad.
6. Presentación de resultados y propuestas.

El tipo de red que se presenta para el análisis es del tipo Internet Service Provider (ISP), esto es, la red de un proveedor de servicios de Internet.

Las etapas de análisis, arquitectura y diseño de una red, son desarrolladas de manera secuencial, de manera que la información en cada etapa será necesaria para la siguiente etapa.

Cabe mencionar que la presente tesis se basa, principalmente, en la etapa de análisis de red actualmente operando, y que sólo se desarrollan los principales elementos de la arquitectura y diseño.

El análisis de red esta dividido en tres secciones:

1. Análisis de requerimientos
2. Análisis de flujos
3. Análisis de seguridad

4.1 Análisis de requerimientos

A continuación se desarrollarán los elementos del análisis de requerimientos, entre ellos las condiciones iniciales, requerimientos, métricas y diagrama físico y lógico.

- NOTA: Los requerimientos fueron reunidos a partir de la información proporcionada por los usuarios, administradores y documentación de la organización.

En la tabla 4.1 se muestra el concentrado de condiciones iniciales y en la tabla 4.2, se muestran los requerimientos.

4.1.1 Condiciones iniciales y requerimientos de la red

Tipo de Proyecto	Análisis del desempeño de una red de un Proveedor de Servicios de Internet (ISP)
Alcance del proyecto	Determinar el desempeño de la red del ISP
Tipo de desempeño	Múltiples niveles de desempeño
Objetivos del Proyecto	Presentar y aplicar una metodología para el análisis de desempeño del backbone del ISP
	Obtener un análisis modular y completo del desempeño del conjunto de servicios que son ofrecidos por la red para el resto del sistema.
	Realizar propuestas útiles para mejorar el desempeño de la red en caso de ser necesario.
	NOTA: Se analizará el servicio de Internet que esta red de servicios provee.
Documentación	Si
Evaluación y Definición	Se aplicará la teoría expuesta en esta tesis y se dará la documentación y resultados obtenidos a la organización.
	La información de la organización será manejada de manera confidencial y se presentará como trabajo profesional de titulación.
Evaluación Técnica Inicial	
Tipo de red	De tercera generación y de un proveedor de servicios de Internet
Arquitectura	Jerárquica de acuerdo al modelo de CISCO (Core, Distribution y Access)
Tecnología	CISCO e IP
Número de usuarios (clientes)	2500
Tipos de usuarios	Clientes que pueden ser: Directores de empresas, Administradores de red, Ingenieros de red y Centro de HelpDesk.
Grupos de aplicaciones	Aplicaciones de acceso y web (estas pertenecen a los usuarios)
Cantidad de dispositivos de red	250 switches, 35 routers (core), 3 servidores DNS.
Tipo de cableado y capacidad	Fibra óptica, desde 128K hasta capacidad GigaBitEthernet.
Direccionamiento	WAN Público y Privado.
Numero de Vlans	1500
Tipo de ruteo	LINK-STATE,
Protocolo de ruteo	OSPF, BGP (IBGP, EBGP)
Tipo de herramientas de seguridad	Autenticación (TACACS), Listas de acceso, Encriptación (MD5), Firewalls
Servicios principales en la red y sus niveles de desempeño requeridos	Servicios de Internet de diferentes capacidades [desde 128Kbps hasta n E1's(2.048Kbps)]
	Los niveles de desempeño están definidos de acuerdo a la Arquitectura de red
	CORE y DISTRIBUCIÓN:
	Disponibilidad 99.95% de tiempo de un mes,
	Packet Loss 0.5% de extremo a extremo,
	Round Trip: 1) Nacional 20 ms, 2) Internacional 40 ms.
	ACCESS: Disponibilidad 99.85% del tiempo de un mes
	Dentro de los SLC firmados con los clientes, si se excede 20 minutos de indisponibilidad mensual, se reembolsa al cliente un día de servicio.
	La indisponibilidad existe cuando una conexión de Internet de un cliente, es incapaz de transmitir y recibir paquetes IP de la red de servicios. El cliente la puede medir por medio de herramientas ping y tracert.
	La indisponibilidad se mide a partir de que se genera un trouble ticket en el Network Operation Center (NOC), al recibir la llamada del cliente, o cuando una falla es detectada por medio de las herramientas de administración de red en el NOC.

Tabla 4.1 Condiciones iniciales

Tipo	Descripción	Estado	Prioridad
Usuario	Monitoreo y soporte las 24 horas 365 días del año.	Existente	Alta
	Implementación de seguridad en el tráfico de la red.	Deseable	Media
	Comprobar que se entrega la capacidad del enlace en términos de ancho de banda.	Probado	Alta
	Contar con la disponibilidad contratada.	Existente	Alta
	Contar con la latencia contratada (en términos de Round Trip Nacional e Internacional).	Existente	Alta
	Conocimiento del cliente de umbrales de latencia y disponibilidad de la red.	Deseable	Alta
	Conocimiento del cliente acerca del ISP para saber si cumple con sus expectativas.	Deseable	Alta
	Procedimientos de escalamiento dentro de la organización (1er, 2do, 3er Niveles).	Existente	Alta
	Conocimiento acerca del centro de datos para saber si soportan sus necesidades del servicio que contratan (físicas, de seguridad en la red, de administración de la red, de capacidad, de disponibilidad, de funcionamiento, de conectividad).	Deseable	Alta
	Adaptabilidad de la red para futuros crecimientos y/o cambios	Existente	Alta
	Atención administrativa para cambios, crecimientos, finanzas, contratos.	Existente	Alta
	Contratos con SLCs en donde quedan definidas las penalizaciones en caso de no cumplir con los SLAs.	Existente	Alta
Aplicación	No aplica, ya que sólo se ofrece en el servicio los enlaces de Internet a nivel de capa 3.	No aplica	No aplica
Dispositivos	Core Nacional equipos serie 7000, Core Internacional equipos 12000, equipos de distribución 3750.	Existente	Alta
	Cisco Internetwork Operating System Software (IOS Version 12.0 o mayor) en los equipos de core y distribución.	Existente	Alta
	2 Route Processor Cards por equipo.	Existente	Alta
	Fuentes de energía redundantes (2 UPS por cada área en común).	Existente	Alta
	Memoria de procesamiento 1 GB.	Existente	Alta
	Arquitectura modular de los dispositivos.	Existente	Alta
	Interfaces de acuerdo a uso y crecimiento	Existente	Alta
Red	Arquitectura de red jerárquica	Existente	Alta
	Disponibilidad del 99.95% en Core y Distribución	POR PROBAR	Alta
	Packet Loss 0.5% de extremo a extremo		
	Round Trip: 1) Nacional 20 ms, 2)Internacional 40 ms		
	Redundancia en enlaces de backbone	Existente	Alta
	Al 70% de uso de ancho de banda del enlace debe conmutar a enlace de backup	Existente	Alta
	Protocolos a usar como IGP es OSPF, y como EGP es BGP.	Existente	Alta
	Actualización de equipos periódica	Deseable	Media
	Sistema de gestión y monitoreo (con seguridad de acceso, control de cambios y actualizado)	Existente	Alta
	Documentación completa de toda la red (equipos, capacidades, redundancia, protocolos)	80%	Alta
	Conocimiento completo del backbone de todo el personal de soporte de primer nivel	70%	Alta
	Contar con personal de operaciones certificados	Deseable	Media

Tabla 4.2 Requerimientos

4.1.2 Métricas de desempeño

En la presente tesis, el tipo de métricas de desempeño permiten determinar los niveles de desempeño de los servicios ofrecidos por la red para el resto del sistema.

A continuación en la tabla 4.3, se muestran las métricas de los servicios en términos de disponibilidad, MTU, límites de utilización de enlaces y round trip y packet loss, los cuáles constituyen los SLAs establecidos con los clientes.

Posteriormente, en la etapa de monitoreo serán presentados las resultados de las métricas de la red de estudio. A continuación sólo son especificadas.

Métricas de servicio para RMA	
Fiabilidad	No aplica
Mantenimiento (MTTR)	Dentro del nivel de escalamiento se tienen tiempos de solución establecidos: Primer Nivel: 15 minutos Segundo Nivel: 1 hora Tercer Nivel: 2 horas
Disponibilidad	CORE: Disponibilidad 99.95% de tiempo de un mes DISTRIBUTION: Disponibilidad 99.95% de tiempo de un mes ACCESS: Disponibilidad 99.85% de tiempo de un mes
Métricas de servicio para capacidad	
Tamaño de paquetes máximo (MTU)	1500 bits que es un estándar por la IEEE
El límite de utilización de enlaces (BW):	70%
Métricas de servicio para delay	
Round-Trip Delay	1) Nacional 20 ms, 2) Internacional 40 ms
Packet Loss	0.5 % de la información de extremo a extremo
Service-Level Contracts (SLCs) y Service-Level Agreements (SLAs).	Los SLAs aplican para todos los clientes y estos incluyen solamente entrega de ancho de banda contratado, la indisponibilidad, el tiempo de soporte y solución de problemas
	La indisponibilidad se mide a partir de que se genera un trouble ticket en el Network Operation Center, al recibir la llamada del cliente o cuando una falla es detectada por medio de las herramientas de administración de red. Dentro de los SLC firmados con los clientes, si se excede 20 minutos de indisponibilidad mensual, se reembolsa al cliente un día de servicio, además se debe contar con soporte 24x7, con los tiempos de solución de problemas mencionados anteriormente. El 0.5% de Packet Loss se estableció considerando que las retransmisiones generadas en una conexión TCP, pueden ser demasiadas, de manera que sea inoperante si se tiene un packet loss mayor.

Tabla 4.3 Métricas de desempeño

A continuación son presentados el diagrama físico y lógico de la red de estudio.

La figura 4.1 muestra el diagrama de red generalizado, en donde se observa cómo la arquitectura de red es de acuerdo al modelo de CISCO (Core, Distribución y Acceso). Los equipos son etiquetados con la localidad – el tipo de equipo COR o DTB – y el número de equipo.

Se puede observar que del equipo de NMU-COR-R02, se conectan los principales enlaces, como los enlaces internacionales, los principales anillos de fibra en el D.F. y los enlaces hacia Monterrey y Guadalajara, las principales localidades que se analizarán por ser las localidades que tienen la mayoría de los clientes. Cabe mencionar que este equipo no cuenta con respaldo.

4.1.3 Diagrama físico y lógico

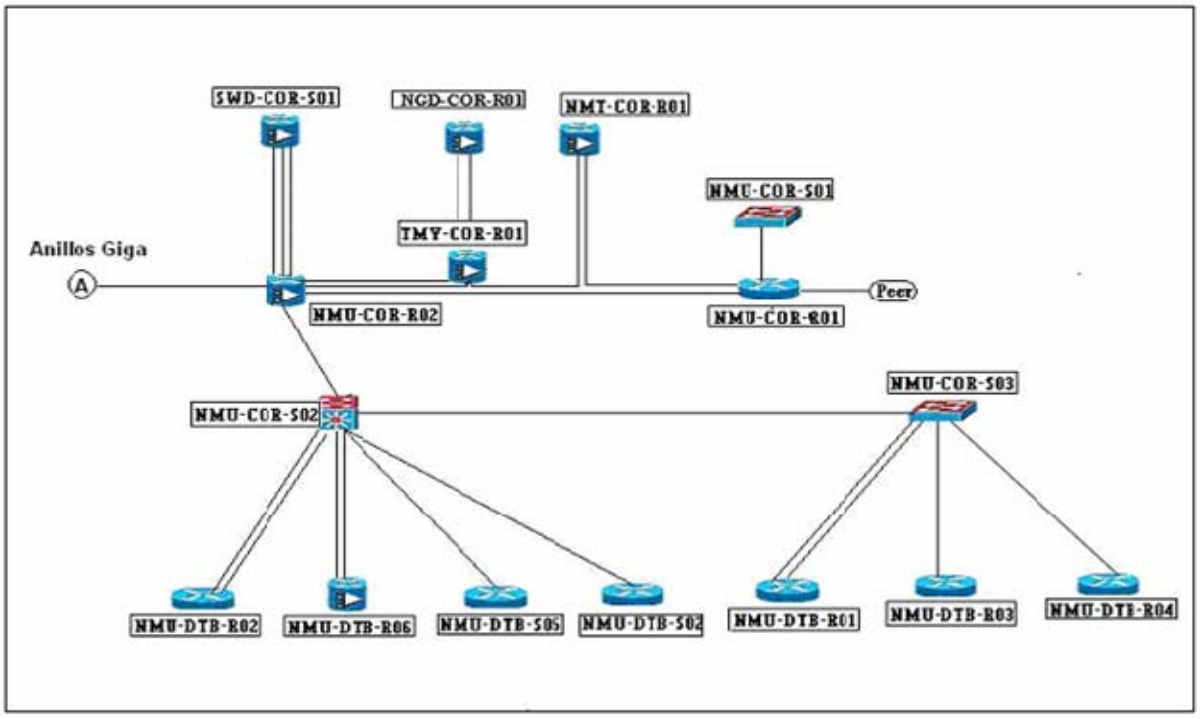


Figura 4.1 Diagrama de red físico generalizado.

La figura 4.2 muestra a detalle el diagrama de red con la capacidad de los enlaces y las interfaces de donde se derivan. Aquí nuevamente se pueden observar cómo el equipo de COR-R02, es el principal equipo dentro del Backbone.

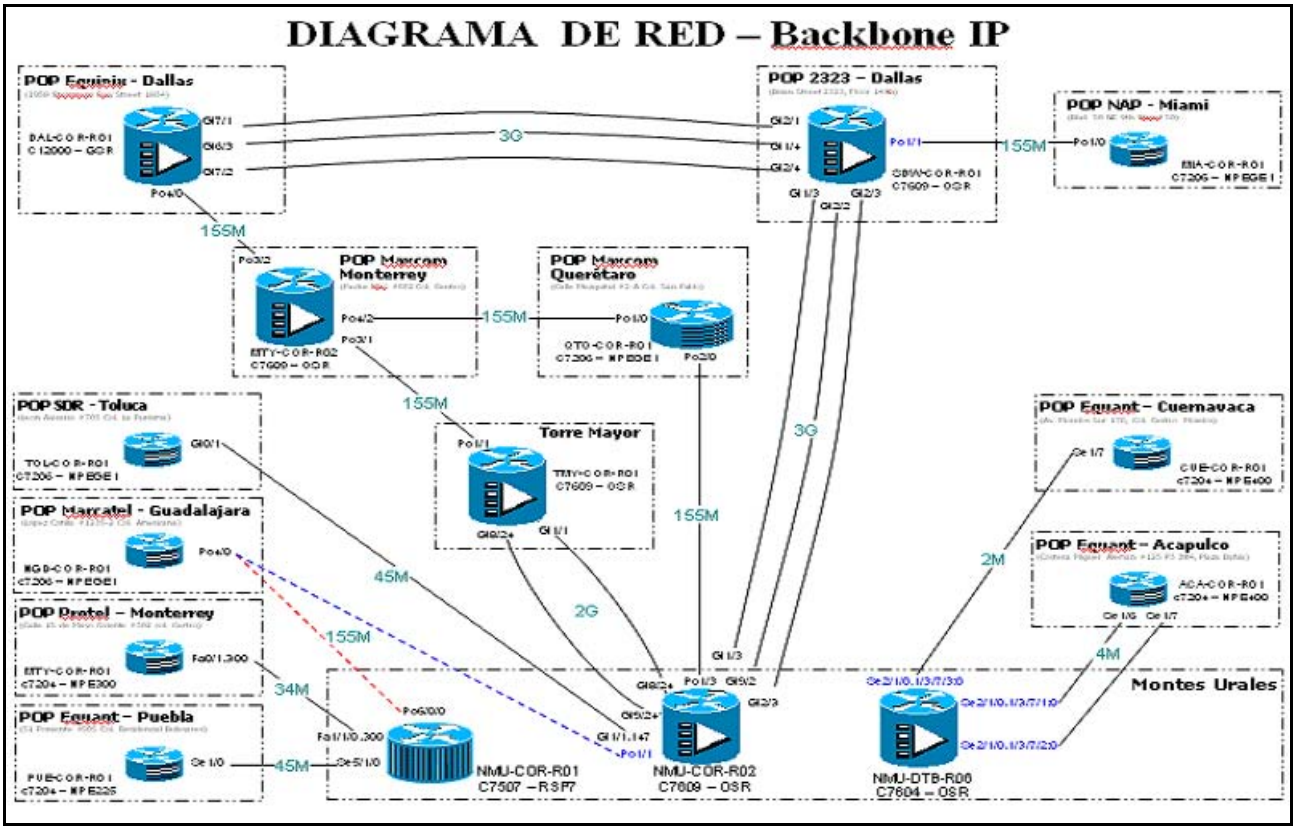


Figura 4.2 Diagrama de red físico detallado.

A continuación, la figura 4.3 muestra el diagrama lógico de la red. Aquí se puede observar que el principal protocolo IGP (Interior Gateway Protocol) es OSPF. Lógicamente, el backbone esta dividido por áreas, siendo el área 0 la encargada de rutear las redes a las demás áreas. El área 0 esta compuesta de equipos de CORE (series 7000), las demás áreas son conformadas por los equipos de distribución (series 3750 multicapa), que forman los anillos de fibra.

El protocolo EGP (Exterior Gateway Protocol) que se emplea, es BGP, y es implementado para el conocimiento de redes de los diferentes sistemas autónomos, además para implementar los servicios de routing entre empresas por medio de VPNs.

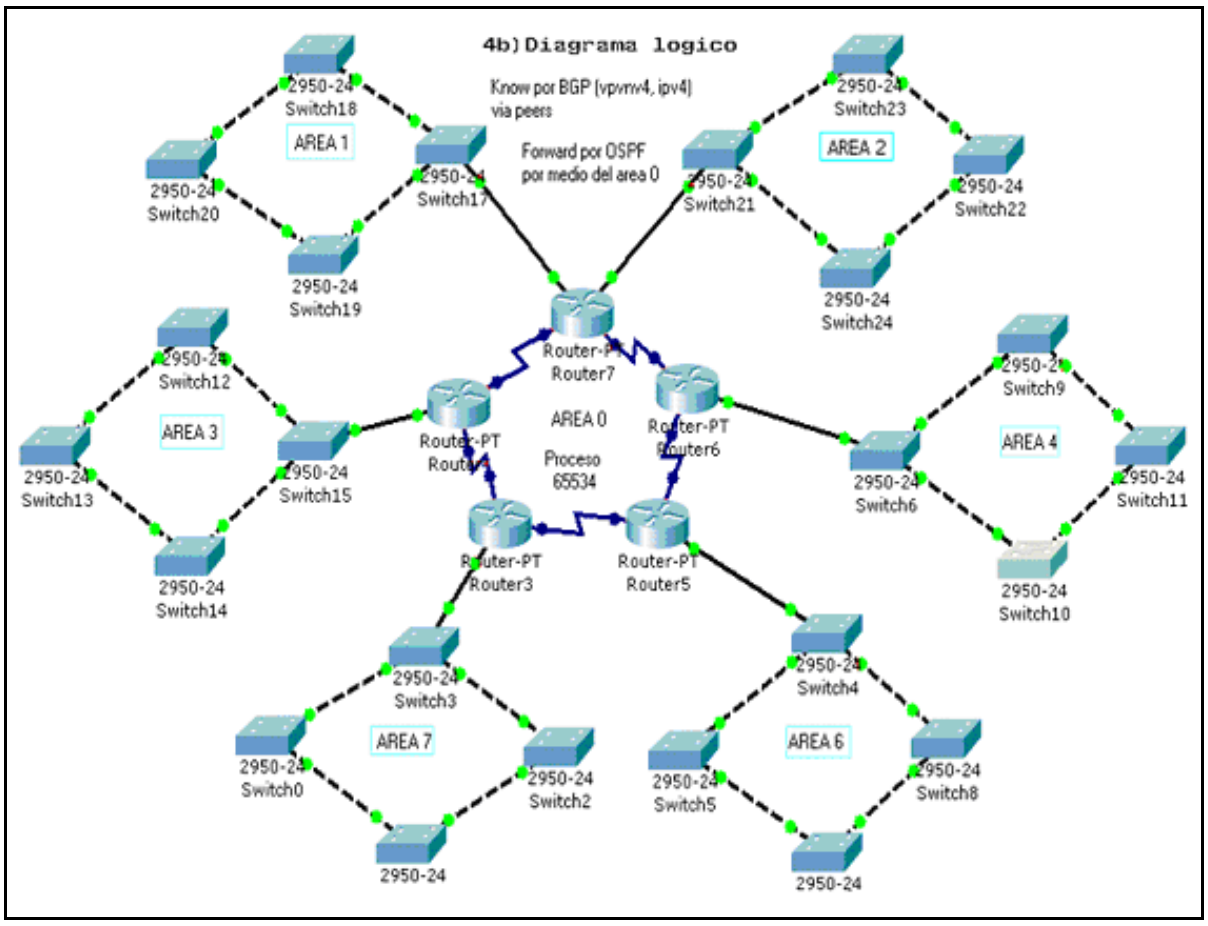


Figura 4.3 Diagrama lógico

4.1.4 Análisis de requerimientos

A continuación, en la tabla 4.4 se presenta el análisis comparativo de lo que se tiene y lo que se desea, de acuerdo a las condiciones iniciales y métricas de desempeño. Cabe mencionar, que esta información fue proporcionada principalmente por ingenieros que diseñaron la red, administradores e ingenieros de soporte.

Esta información dará la pauta para determinar si los requerimientos iniciales se cumplen y si las métricas que se tienen son logradas. Los resultados que se obtengan servirán a la empresa para una futura reingeniería de esta red

Estado Actual (Requerimientos Iniciales)	Lo deseable (Requerimientos)	Limitantes	Consecuencias
CORE y DISTRIBUCIÓN: Disponibilidad del 99.95% de tiempo de un mes; Packet Loss 0.5% de extremo a extremo. Round Trip: 1) Nacional 20 ms, 2)Internacional 40 ms	Que se cumplan al 100% estas métricas Por probar que se cumplan dentro del monitoreo	Falta análisis costo- beneficio, en donde se demuestre el beneficio de tener mayor redundancia antes de tener fallas por la carencia de esta.	Penalizaciones económicas, mayores costos de operación, cancelaciones de servicios
Monitoreo y soporte las 24 horas 365 días del año	Apoyo y solución de problemas desde la primera llamada Implementación de seguridad en la red.	Problemas que implican más áreas y/o tiempo de afectación a otros servicios Falta de trabajo en equipo entre las áreas de la empresa Control de implementación de servicios Mayores costos en adquisición de herramientas de seguridad	Mayores costos de operación y penalización. Mayores costos de operación y penalización.
Comprobar que se entrega la capacidad del enlace en términos de ancho de banda	Explicación al cliente del servicio que está contratando	Atención por parte del cliente y ejecutivo de ventas	Falsos reportes con reclamo de no tener el BW contratado
Conocimiento del cliente de umbrales de latencia y disponibilidad de la red Procedimientos de escalamiento dentro de la organización (1er, 2do, 3er Niveles)	Para todos lo clientes		Falsas expectativas del cliente acerca del servicio, por ejemplo reportar falta de servicio cuando el problema está dentro del sitio del cliente
Adaptabilidad de la red para futuros crecimientos y/o cambios.	OK		
Atención administrativa para cambios, crecimientos, finanzas, contratos.	Mejor comunicación entre áreas técnicas y administrativas	Jornadas de trabajo diferentes y falta de integración de áreas de la empresa	
Contratos con SLCs en donde quedan definidas las penalizaciones en caso de no cumplir con los SLAs	Para todos lo clientes		
Redundancia en equipos de backbone	Redundancia en todos los equipos de backbone	Mayores costos	Mayores costos de operación y penalización
Cisco Internetwork Operating System Software (IOS Versión 12.0 o mayor) en equipos de core	OK		
2 Route Processor Cards por equipo	OK		
Fuentes de energía redundantes (2 UPS por cada área en común)	OK		
Arquitectura de los dispositivos Modular	OK		
Interfaces de acuerdo a uso y crecimiento	OK		
Memoria de procesamiento 1 GB	OK		
Arquitectura de red jerárquica			
Redundancia en algunos enlaces de backbone	Redundancia en todos los enlaces de backbone	Mayores costos	Mayores costos de operación y penalización
Al 70% de uso de ancho de banda del enlace, debe conmutar a enlace de backup	OK		
Protocolos a usar como IGP es OSPF y como EGP es BGP	OK		
Actualización de equipos periódica	Administración proactiva de equipos (revisiones y actualizaciones periódicas)		Reducción de costos de soporte

Estado Actual (Requerimientos Iniciales)	Lo deseable (Requerimientos)	Limitantes	Consecuencias
Sistema de gestión y monitoreo (con seguridad de acceso, control de cambios y actualizado)	Ok		
	Documentación completa de toda la red (equipos, capacidades, redundancia, protocolos), así como etiquetado de los equipos		
	Conocimiento completo del backbone de todo el personal de soporte	Falta de capacitación por parte de la empresa, y auto- estudio.	Mejor apoyo para solución de problemas
No existe	Contar con personal de operaciones certificados	Falta de estimulación al personal	Mejor satisfacción del personal y beneficios para la empresa

Tabla 4.4 Análisis de requerimientos.

4.2 Análisis de flujo

A continuación, en la tabla 4.5, se mencionan los principales flujos que se presentan en la red, con los peerings entre las principales ciudades a nivel nacional (DF, Monterrey y Guadalajara), y los flujos a los proveedores internacionales que permiten la conexión con la nube de Internet, así como los requerimientos que estos deben cumplir.

4.2.1 Especificación de flujos

Requerimientos de flujos

- El direccionamiento en los enlaces punto a punto debe ser a 30 bits
- Comunicación debe ser dúplex.
- Los equipos conectados deben ser routers
- Conmutación a enlaces de backup en caso de fallas
- Redundancia en salidas nacionales e internaciones con diferentes proveedores,
- Crecimiento oportuno de los enlaces en base a las necesidades
- La capacidad de los enlaces debe ser Gigabit Ethernet.
- Limitar en todos los casos el ancho de banda contratado por el cliente
- La administración de la red puede ser del tipo out-bound
- El sentido de la información es contrario al de las manecillas del reloj
- La redundancia es implementada en anillos

PEERINGS NACIONALES	PEERINGS INTERNACIONALES
OC3 TELMEX (NMU-COR-R02)	CWIRELESS (2323)
OC3-II TELMEX (NMU-COR-R02)	PEERFABRIC (2323)
E3 (BW 34000 Kb) TELMEX (NMT-COR-R01)	YIPES (EQX)
OC3 ALESTRA (NMU-COR-R02)	COGENT (EQX)
MCM 35M (NMU-DTB-S01)	YAHOO (EQX)
IMPSAT (NMU-COR-R01)	SPRINT (EQX)
UNAM 10M (NMU-COR-R02)	PCW (EQX)

Nota: OCx: Optical Carrier levels; OC-1: 51.84 Mbps; OC-2: múltiplos de dos; OC-3: 155.52 Mbps; OC-12: 622.08 Mpbs; OC-24: 1.244 Gbps; OC-48: 2.488 Gbps; EQX=DAL-COR-R01.

La figuras 4.4 y 4.5 muestran de manera detallada los peerings nacionales e internacionales, que permiten el intercambio de redes a nivel nacional e internacional, respectivamente.

El flujo de información distribuída (redes intercambiadas) con los peerings, esta controlada por medio de reglas configuradas en los routers, y es conforme a los acuerdos pactados con estos ISPs.

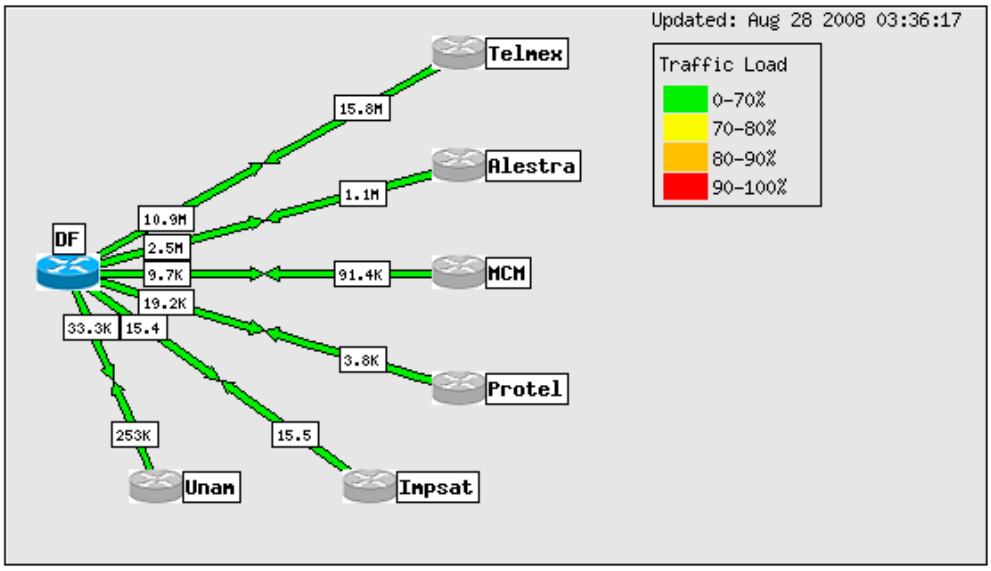


Figura 4.4 Flujos peers nacionales.

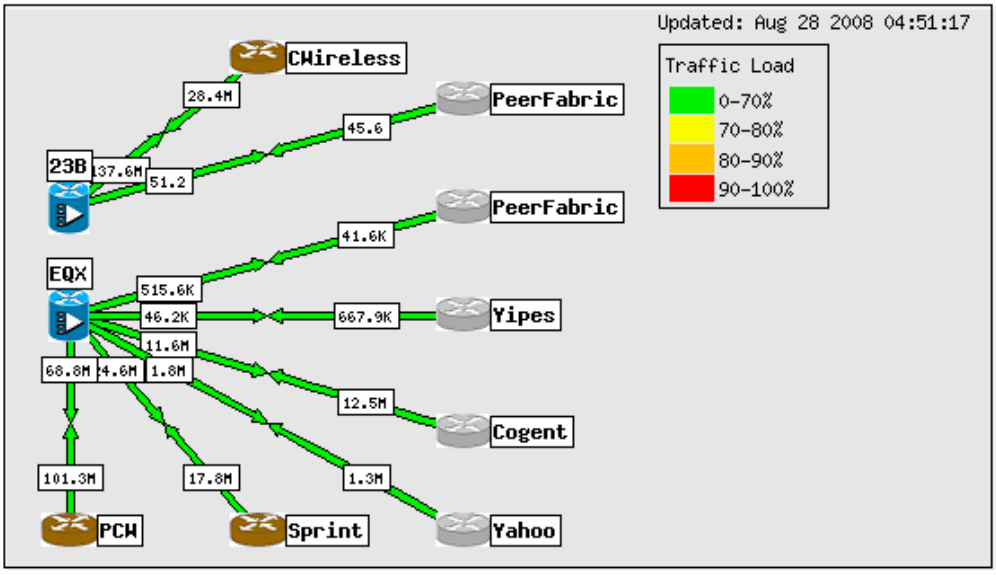


Figura 4.5 Flujos peers internacionales.

ENLACES INTERNACIONALES	ENLACES NACIONALES
2323=SWD-COR-R01	**DF**
TRK DF-2323 GIGA-I (to SWD-COR-R01 Gi1/3)	TRK GIGA I NMU-TMY (to TMY-COR-R01 Gi1/1)
TRK DF-2323 GIGA-II (to SWD-COR-R01 Gi4/3)	TRK GIGA II NMU-TMY (to TMY-COR-R01 Gi8/24)
TRK DF-2323 GIGA-III (to SWD-COR-R01 Gi2/2)	**MEXICO-GUADALAJARA**
TRK OC-3 III EQX-MTY (to NMT-COR-R02 PO3/2)	**(CAMBIOS EN IMPLEMENTACIONES)**
TRK EQX-2323 GIGA-I (to SWD-COR-R01 Gi1/2)	TRK OC-3 I :GUADALAJARA-DF (to TMY-COR-R01 Po ¼)
TRK EQX-2323 GIGA-II (to SWD-COR-R01 Gi1/4)	TRK OC-3 II : GUADALAJARA-DF (to TMY-COR-R01 Po 2/4)
TRK EQX-2323 GIGA-III (to SWD-COR-R01 Gi4/4)	**MÉXICO-MONTERREY**
TRANSIT GE PCCW – Giga I	TRK OC-3 DF-MTY (to NMT-COR-R02 PO3/1)
TRANSIT GE PCCW – Giga II	**QUERETARO-MONTERREY**
TRANSIT GE SPRINT (DAL-COR-R01)	TRK OC-3 QRO-MTY (to NMT-COR-R02 PO4/2)
	QUERETARO-DF
	TRK OC-3 QRO-DF (to NMU-COR-R02 Po1/3)
	TRK OC-3 DF-QRO II (to NMU-COR-R01 PO2/4)
	MÉXICO-SAN LUIS (IMPLEMENTACIÓN NUEVA)
	TRK OC-3 DF-SLP (to SLP-COR-R01_PO1/0
	ANILLOS GIGA DERIVADOS DEL NMU-COR-R02
	Anillo GIGA A,B,C)

4.2.2 Diagramas de flujos

La figura 4.6 muestra la ubicación de los flujos mencionados anteriormente. A nivel nacional se puede observar cómo fluye el tráfico entre el D.F. y las diferentes ciudades, como Guadalajara y Monterrey. A nivel internacional se observa el tráfico internacional con Dallas (etiquetado como 2323), y los diferentes proveedores de Internet como Sprint y Pccw.

Para Guadalajara, se puede observar cómo se tienen dos enlaces DF-Guadalajara, lo que permite la redundancia en caso de falla de alguno de ellos.

Para Monterrey, se tienen tres enlaces, dos por medio de un proveedor (Protel), y el tercero entregado por un proveedor diferente (Maxcom).

De las salidas internacionales por Dallas (2323), se tienen trabajando tres Gigas, dos de ellas por un proveedor, y la tercera por uno diferente. Para el caso de Monterrey y las salidas internacionales, se observa que se pueden presentar problemas, cuando el proveedor que entrega dos de los enlaces, tenga algún contratiempo, ya que sólo quedaría habilitado un enlace a Monterrey y un enlace hacia Dallas, por lo que la sugerencia, en este caso, es mayor redundancia por diferentes proveedores.

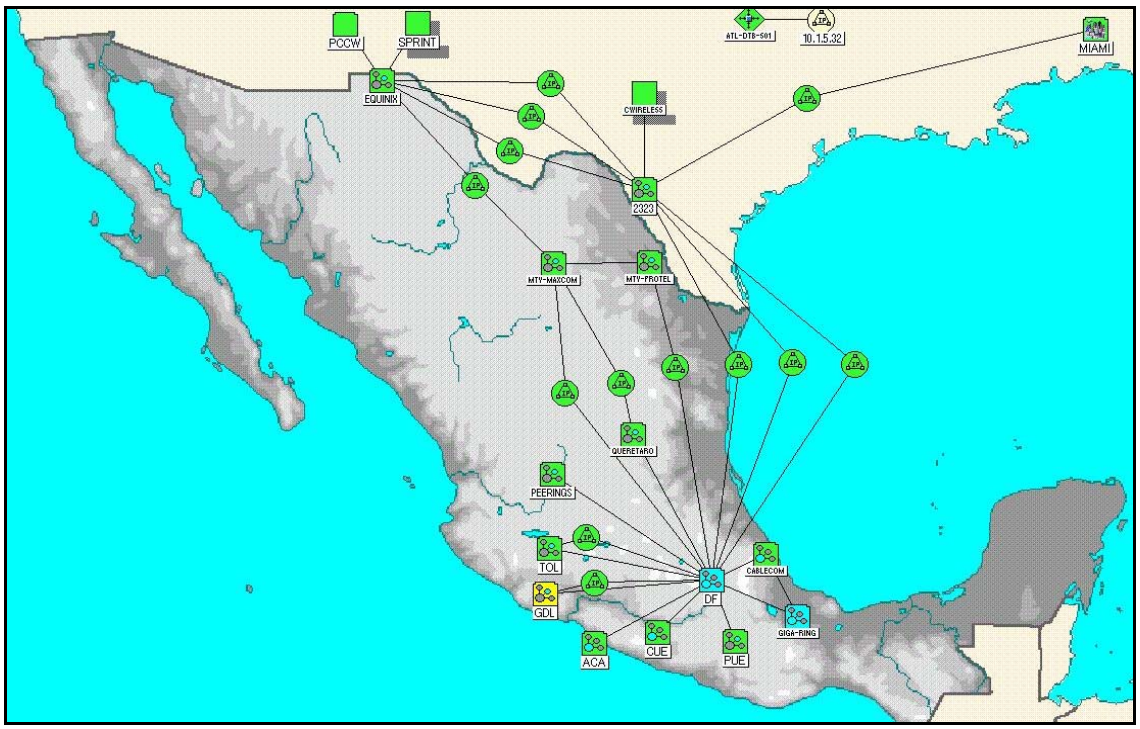


Figura 4.6 Flujos de los enlaces principales.

La figura 4.7 muestra los flujos que se dan entre los anillos de fibra. Cabe mencionar que el flujo de la información tiene el sentido de las manecillas del reloj, y que la redundancia se da al cambiar este sentido, cada vez que se tiene un corte físico. La comunicación es dúplex, lo que hace funcionar a cada equipo de distribución como fuente y destino a la vez.

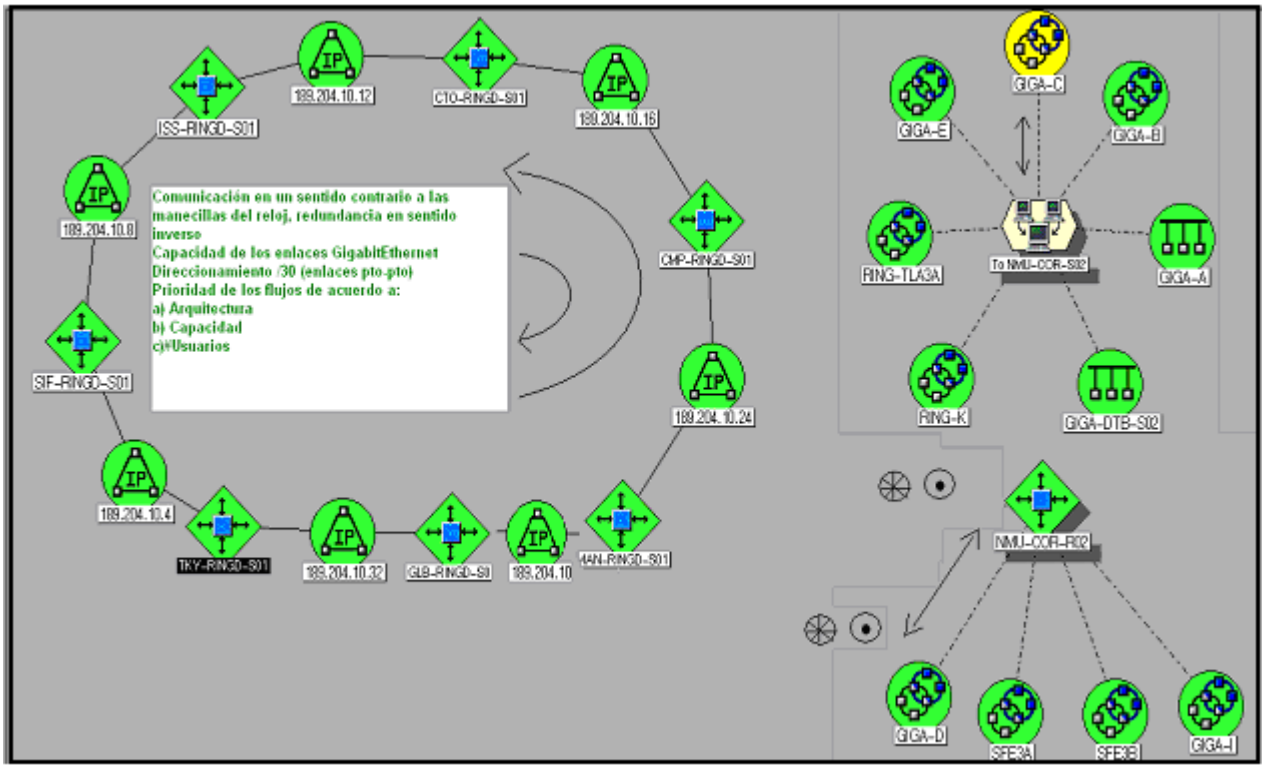


Figura 4.7 Anillos de fibra.

La figura 4.8 muestra en conjunto un mapa de los flujos de red y la derivación de los equipos de distribución de los equipos de core, de acuerdo a la arquitectura de red. Cabe mencionar que el tipo de direccionamiento es a treinta bits, por ser enlaces punto a punto.

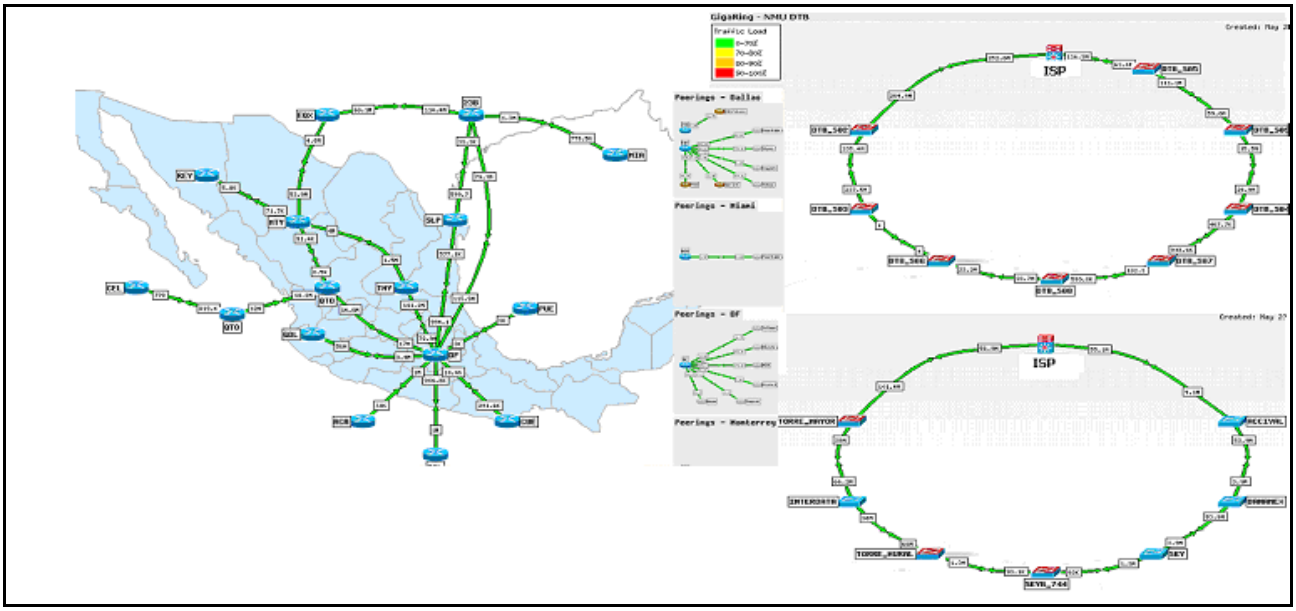


Figura 4.8 Derivación de anillos de los equipos de core.

A continuación, en la figura 4.9, se presenta un ejemplo a detalle de cómo está configurado un peer nacional. Aquí se observa el direccionamiento, que es a 30 bits, y el tipo de ruteo, principalmente.

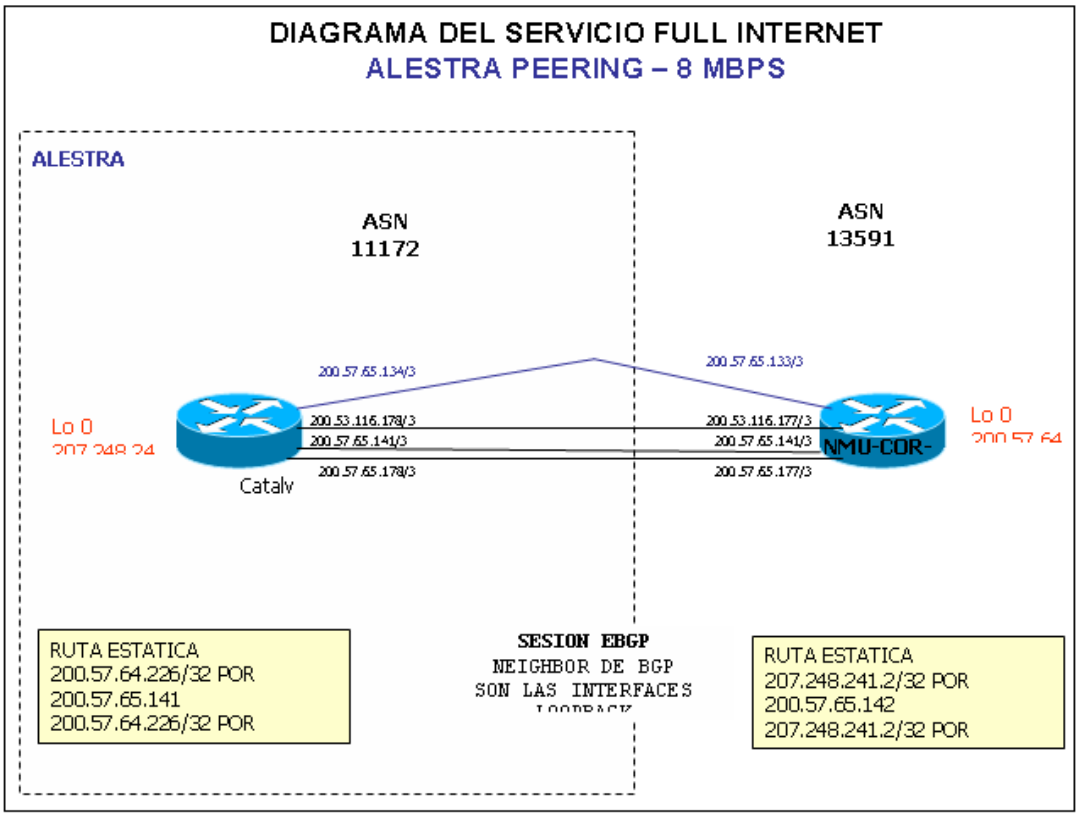


Figura 4.9 Ejemplo de peering.

La figura 4.10 ilustra el flujo de las fibras, de donde se pueden derivar más anillos en la zona Reforma, Polanco e Insurgentes.

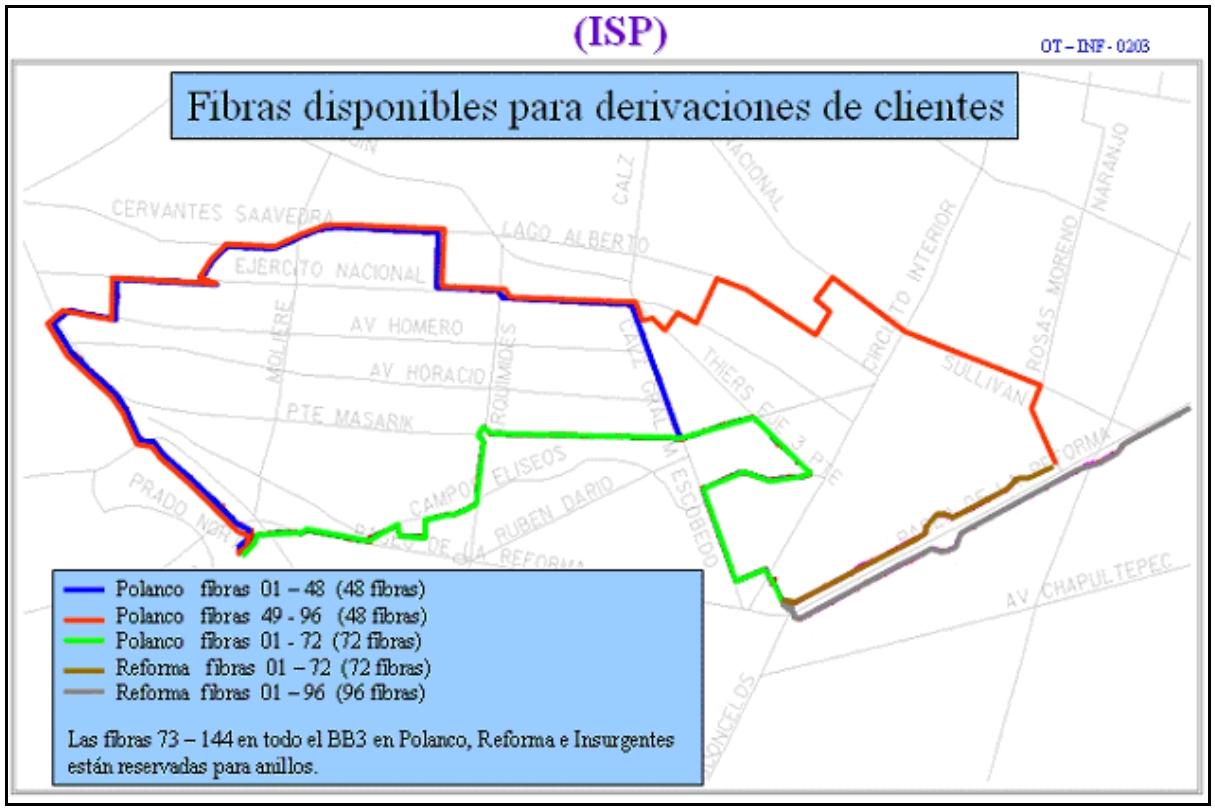


Figura 4.10 Distribución de fibras para derivaciones.

4.3 Análisis de seguridad

Estado actual de la seguridad de la red de estudio, en la tabla 4.5.

Tipo	Tecnología	Descripción (Problemas o amenazas que resuelve)	Operando
Física	Acceso físico a los equipos controlado	Permite el acceso físico a personal autorizado	NO
	Fuentes de poder y aire acondicionado certificados	Instalaciones certificadas permite tener mayor seguridad de no presentar accidentes	NO
	Resguardo físico de respaldos de información en más de una localidad	Permite recuperar de manera más rápida la información en caso de un desastre	NO
	Sistemas de alarmas de humo	Actuar con menor tiempo en caso de incendio	SI
	Sistema de circuito cerrado	Monitoreo de las actividades del personal y equipos	SI
Lógica	SNMP	Administración personalizada de desempeño de equipos	SI
	Autenticación vía TACACS	Control de acceso a equipos	SI
	Filtrado de redes	Filtrado de redes para evitar el paso de las no autorizadas	SI
	Limitación de ancho de banda	Limita al cliente sólo a usar el ancho de banda contratado	80%
	Herramientas de acceso con encriptación	No permitir el flujo de contraseñas en texto libre	SI
	Perímetro de seguridad (NAT, Firewalls)	Tratar de asegurar el equipo por medio de herramientas físicas o lógicas. Sólo se cuenta con Firewalls que protegen las consolas de gestión.	NO
	Seguridad de acceso remoto (Métodos AAAA, DMZ)	El acceso remoto ayuda eliminar tiempos y costos de desplazamientos	SI
	Control de direccionamiento	Mejor administración de direccionamiento IP	NO
	Políticas y procedimientos de Seguridad en la red establecidas de manera formal	Mejores prácticas de seguridad	NO
Puntos de mejora: Otorgar mayor importancia al tema de seguridad en la red, ya que sólo se cuenta con la seguridad para las consolas de gestión de los equipos, y no se cuenta con niveles de seguridad aplicados en cada nivel de la arquitectura. Tener un mejor resguardo físico de los equipos y planes de contingencia.			

Tabla 4.5 Elementos de seguridad básicos.

4.4 Arquitectura de la red

Los elementos de la arquitectura que se desarrollan a continuación son: el direccionamiento y la administración.

El tipo de arquitectura y direccionamiento se definieron en las condiciones iniciales, dentro de la evaluación técnica inicial.

A continuación se presentan los elementos que se monitorean y administran, las herramientas de administración, las MIBs con las que trabaja SNMP, la información de monitoreo recolectada, y su análisis.

4.4.1 Características que se monitorean y administran

En la tabla 4.6 se presentan los detalles del monitoreo que se realiza, los protocolos, tipo y frecuencia de monitoreo, herramientas y parámetros, que serán colectados entre las principales.

Tipo de Red:	Pruebas:		Real:	**X**		
Tipo de información monitoreada:	Traps SNMP				b) Sólo se procesa la recolectada por los Probes	
Tipo de respaldo de la información:	Parcial:		Total:	**X**	Periódico	**X**
Dispositivos para despliegue:	Monitor:		Pantallas:	**X**	Móviles:	**X**
Tipo de monitoreo:	Monitoreo por Eventos:	**X**	Análisis y planeación:		Configuración y troubleshooting de la red	**X**
Frecuencia de monitoreo	365 días las 24 h					
% BW del tráfico de monitoreo	Significante		No significante	**X**	Aproximado de:1Kb	
Herramienta de monitoreo:	Del tipo Framework: HpOpenView que trabaja con SNMPv2 para la configuración de eventos, con acceso a los equipos para configuración y troubleshooting					

Parámetros que son monitoreados:		
		Herramientas
Por enlace	Ancho de banda consumido	Herramienta personalizada (Cacti) basada en MGRT (The Multi Router Traffic Grapher)
	Disponibilidad de un enlace mensual del 99.95%	Routers Cisco llamados Probes
	Pérdida de paquetes con un umbral de 0.5%	Routers Cisco llamados Probes
	Delay de 20 ms nacional y 40 ms internacional	Routers Cisco llamados Probes trabajando con la MIB RTT
Por Dispositivo	CPU al 70% de utilización	Cisco Enviroment Monitor MIB (por el cacti)
	Memoria	Cisco Enviroment Monitor MIB (por el cacti)
	Temperatura	Cisco Enviroment Monitor MIB (por el Cacti)

Tabla 4.6 Características de monitoreo.

4.4.2 Herramientas de administración

A continuación, en la tabla 4.7 se muestran las características de las herramientas de monitoreo, con una descripción de qué son y para qué sirven, además de presentar el perfil del personal que administra la red, ya que constituyen una pieza clave para el soporte de esta red.

Herramientas de administración y utilidades	Consolas del tipo Framework: HpOpenView con licencias ilimitadas de nodos a administrar, sobre ambiente UNIX, que permiten la gestión de los equipos vía SNMP. Para el caso de los Routers y Switches de la red de tipo Cisco, hay un template para graficar las condiciones de CPU, memoria y temperatura de los equipos, por medio de un "polling" a la MIB Enviroment. Burstable: Herramienta que colecta los bits de in/out de una interfaz y aplica la metodología 95 percentil para determinar el tráfico a facturar. Esta trabaja descartando el 5% de los picos más altos que el cliente tuviera en el mes Ejemplo de la Metodología del 95%: Durante todo el mes se toman muestras de tráfico cada 5 minutos En un mes de 30 días se tiene: (30 días * 24 hrs * 60 min) / 5 min = 8640 muestras Las 8640 muestras se ordenan de mayor a menor según su tráfico El 5% de las muestras mayores se descartan, es decir, las 432 muestras de mayor tráfico se ignoran y serán gratuitas para el cliente. Se factura la muestra siguiente disponible, es decir, la muestra 433, ya que partir de esta muestra no se considera que sean picos, sino tráfico sostenido. Routers Cisco, llamados Probes, que recolectan y envían la información de los enlaces a una aplicación personalizada, llamada IP SLA, cuya función es almacenar y procesar la información recolectada y presentar la disponibilidad, RTT y Packet Loss. SalesForce: Administración de clientes, y seguimiento a reportes de fallas y modificaciones de los servicios IP SLA: Herramienta personalizada que se encarga de obtener la disponibilidad de los enlaces, la pérdida de paquetes y el round trip					
Administración	Tipo de administración: Centralizada			Protocolo de administración: SNMP		
	Dispositivos Administrados	300		Dispositivos p/admón..	3 Consolas con S.O. HPOpenView	
	Aplicaciones Administradas	0		Aplicación p/admón..	3	
Configuración	CLI	**X**	In-band(I) o Out-Band(O)	**IN**	Telnet(T)/SSH	**X**
Descarga de archivos	TFTP	**X**	FTP	**X**	Copy/Paste	**X**
Respaldos S.O/Imagenes/Configuración	Locales	**X**	Externos			
Control de cambios	Sistema	**X**	Bitácora			

Personal de administración de la red				
	#	Nivel de estudios	Años de experiencia	Capacitación de la Empresa
Soporte 3 Nivel	1	M	15	No
Soporte 2 Nivel	1	L	8	No
Soporte 1 Nivel	7	L	2	No
Implementación	3	L	5	No
Ingeniería	5	L	4	No
Procedimientos de fallas	Si	X	No	Actualizados
Herramientas	Si	X	No	Actualizadas
Contraseñas	Si	X	No	NO actualizadas
Diagramas	Si	X	No	NO actualizados

Tabla 4.7 Herramientas de administración y utilidades.

4.4.3 MIBs de SNMP en las consolas de administración

A continuación, la tabla 4.8 muestra el detalle de las MIBs y traps, configurados en las consolas de gestión que trabajan con SNMPv2.

MIB´s SNMP en dispositivos	Traps Enviados	Vía Consola HPOV para IOS SupportSNMP versión 2
RFC 1902 SNMPV2 SMI	Acceso remoto	snmp-server enable traps tty
RFC 1903 SNMPv2 TC	CPU threshold	snmp-server enable traps cpu threshold
RFC 1906 SNMPv2 TM	Manipulación física de hardware	snmp-server enable traps flash insertion removal
RFC 1907 SNMPv2 TM	Cambios en la topología (elección de nuevo rootbridge)	snmp-server enable traps bridge newroot topologychange
	Inconsistencias de protocolos que puedan ocasionar loops (stp)	snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
RFC 1213-MIB-II	Response time reporter (para probes)	snmp-server enable traps rtr
RFC 2011-IP-MIB	Seguridad en puertos	snmp-server enable traps port-security
RFC 2012-TCP-MIB	Configuración de vtp	snmp-server enable traps vtp
RFC 2013-UDP-MIB	Creación de vlans	snmp-server enable traps vlancreate
	Miembros de Vlans	snmp-server enable traps vlan-membership
DMTF-DMI.MIB	Borrado de vlans	snmp-server enable traps vlandelete
ATMSVC.MIB	Notificación de direcciones mac	snmp-server enable traps mac-notification
	Estatus del ambiente (temperatura)	snmp-server enable traps envmon fan shutdown supply temperature status
CISCO-SMI.MY	Alerta de uso del comando copy-config	snmp-server enable traps copy-config
RFC2863-IF-MIB	Operación de routers and switches	snmp-server enable traps syslog
CISCO-PRODUCTS-MIB.MY	Tráfico mpls	snmp-server enable traps mpls traffic-eng
STRATA.MIB	Mpls LPD	snmp-server enable traps mpls ldp
SV+SERVICE.MIB	Ip Multicast	snmp-server enable traps ipmulticast
SV+NETWORK.MIB	OSPF	snmp-server enable traps ospf state-change
ERRORS.MIB		snmp-server enable traps ospf errors
RFC1315-FRAME		snmp-server enable traps ospf retransmit
RFC1406-DS1		snmp-server enable traps ospf lsa
OLD-CISCO-CHASSIS-MIB.MY		snmp-server enable traps ospf Cisco-specific state-change
CISCO-C3800-MIB.MY		snmp-server enable traps ospf Cisco-specific errors
CISCO-WAN-SVC-MIB.MY		snmp-server enable traps ospf Cisco-specific retransmit
CISCO-MODULE-MIB.MY		snmp-server enable traps ospf Cisco-specific lsa
CISCO-SYSTEM-MIB.MY	BGP	snmp-server enable traps bgp
CMMC.MIB		snmp-server enable traps mpls vpn
CISCO-SYSLOG-MIB-MY		snmp-server enable traps fru-ctrl
POWERNET361.MIB		snmp-server enable traps cluster
CISCO-VOICE-IF-MIB-VISMF.MY		snmp-server enable traps hsrp
OLD-CISCO-INTERFACES-MIB.MY		snmp-server enable traps rsvp
CMMCEFM.MIB		snmp-server enable traps l2tun session
STCS112.MIB		snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
SYNROL72.MIB		snmp-server enable traps msdp

Tabla 4.8 MIBs y Traps.

Se puede observar que los traps que son de interés, son los traps que nos indiquen cambios en la configuración (creación, eliminación, cambios), estados de los equipos (alertas de temperatura o cualquier manipulación física), así como los que indican cualquier anomalía en los protocolos OSPF y BGP.

El detalle de MIBs que se puede configurar en routers se muestra en el anexo A. Concentrado de MIBs para routers Cisco

Antes de exponer los resultados colectados por los Probes, se presentará la forma básica de cómo funcionan dentro de la administración de la red del ISP, para obtener las métricas de disponibilidad, pérdida de paquetes y round trip delay.

Probes

Los probes, en este caso, son routers Cisco que trabajan como agentes conocidos también como Service Assurance Agent (estos SAA son una característica del IOS que puede ser implementada como software), que recolectan estadísticas de los recursos de los routers de Backbone de este proveedor de servicios.

Formas en que trabajan los probes:

Pueden trabajar con MIBs específicas y sondear la red vía SNMP.

Por medio de SNMP se obtiene la información acerca del estado y las estadísticas de los dispositivos de la red, utilizando la instrucción "get" de SNMP para consultar a las variables (objetos) de interés de la MIB.

Pueden ser configurados con funciones tales como Ipicmp, Jitter, Tcpconnect, etc. De manera particular, los probes de esta red trabajan con las funciones Ipicmp y packet loss, de donde toman los tiempos de ida y regreso de los paquetes (round trip) entre POP y POP, así como la pérdida de paquetes dentro de un camino, ahorrando ancho de banda en los enlaces y permitiendo realizar una administración proactiva, pero limitada. La figura 4.11 muestra el funcionamiento de los probes.

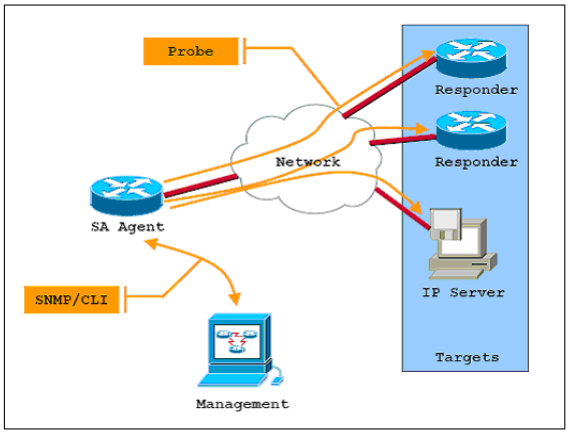


Figura 4.11 Funcionamiento de los probes.

De acuerdo a la figura 4.11, los probes pueden operar como Sender o Responder.

Las características del sender son:

El sender tiene como función enviar pruebas a los responders, los cuáles son otros routers y que son los objetivos (targets).

El target puede ser otra entidad (otro router).

Algunas peticiones requieren que el target cuente con el SAA responder

Las características de los responders son:

- Trabajan con el IOS Cisco
- Se debe configurar el 'rtr responder' o rttMonApplResponder.0=1 con SNMP
- El sender usa el protocolo SAA Control para comunicarse con el responder antes de enviar los paquetes prueba.
- El responder conoce el tipo de operación, el puerto usado y la duración
- La comunicación puede ser autenticada con MD5, no encriptada.

Las principales razones por las que se eligieron los probes son:

- Son dispositivos Cisco y es el tipo de tecnología usada en todo el backbone del ISP, y está disponible en casi todas las plataformas, interfaces y versiones de IOS
- Pueden proveer el desempeño de las métricas en tiempo real
- Pueden proveer notificaciones proactivas
- Al ser una característica del IOS de Cisco no requiere de equipo adicional para ser implementados, los propios equipos del backbone pueden ser configurados para funcionar como agentes SAA. En esta red se cuenta con routers sólo para esta función.
- Pueden ser implementados en los equipos de los clientes (CPE) en caso de que se requiera. En esta red los probes colectan la información de POP a POP, como se muestra en la figura 4.12.

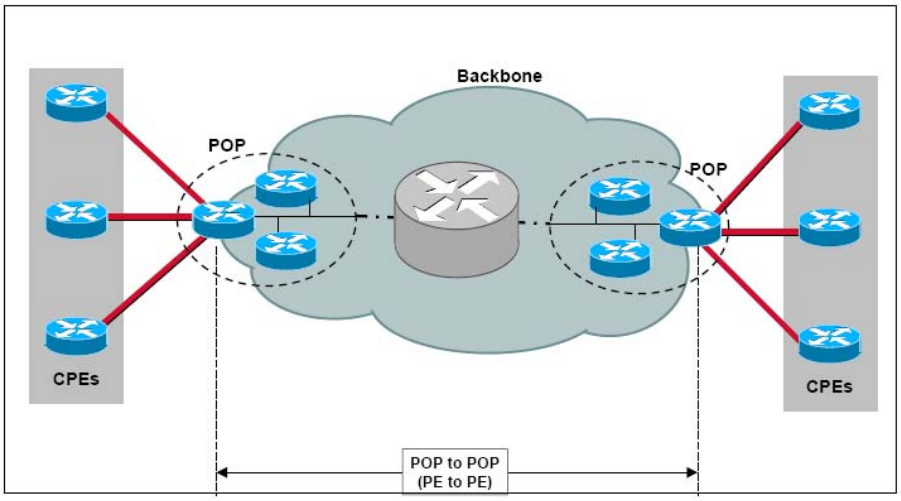


Figura 4.12 Puntos de demarcación de los probes.

Ventajas y desventajas de tener estos puntos de demarcación:

- Se obtienen medidas del desempeño entre POPs
- Permite evaluar la calidad de un backbone compartido
- Puede predecir el desempeño de un nuevo POP, instalando una vrf en ese POP
- No permite medir el desempeño hasta el punto del cliente
- Desempeño de los probes:
- Depende del tipo, la frecuencia y número de pruebas configuradas
- El uso de la memoria es menos de 20KB por probe configurado
- El uso del CPU es -1% cuando se corre 60 pruebas por minuto; 9% con 360 pruebas por minuto en un router Cisco 2600.

En este caso las características técnicas de los probes son:

- Cisco Internetwork Operating System Software
- IOS (tm) C805 Software (C805-SY6-MW), Version 12.2(15)T14
- Número de pruebas configuradas 2: Round Trip y Packet Loss
- Frecuencia de las pruebas: 30 segundos
- Tiempo de almacenamiento: 1 hora
- Número de muestras por hora: 120
- Uso de CPU por probe -1%

A continuación las figuras 4.13 y 4.14 muestran como los probes funcionan para obtener el Round Trip y el Packet loss, respectivamente.

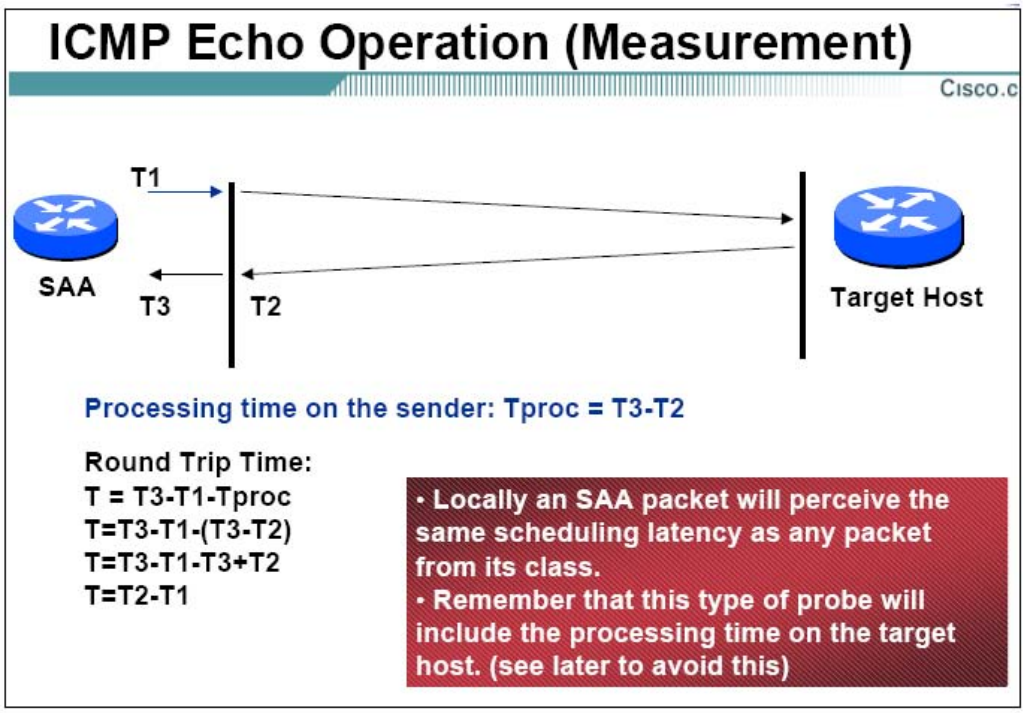


Figura 4.13 Round Trip.

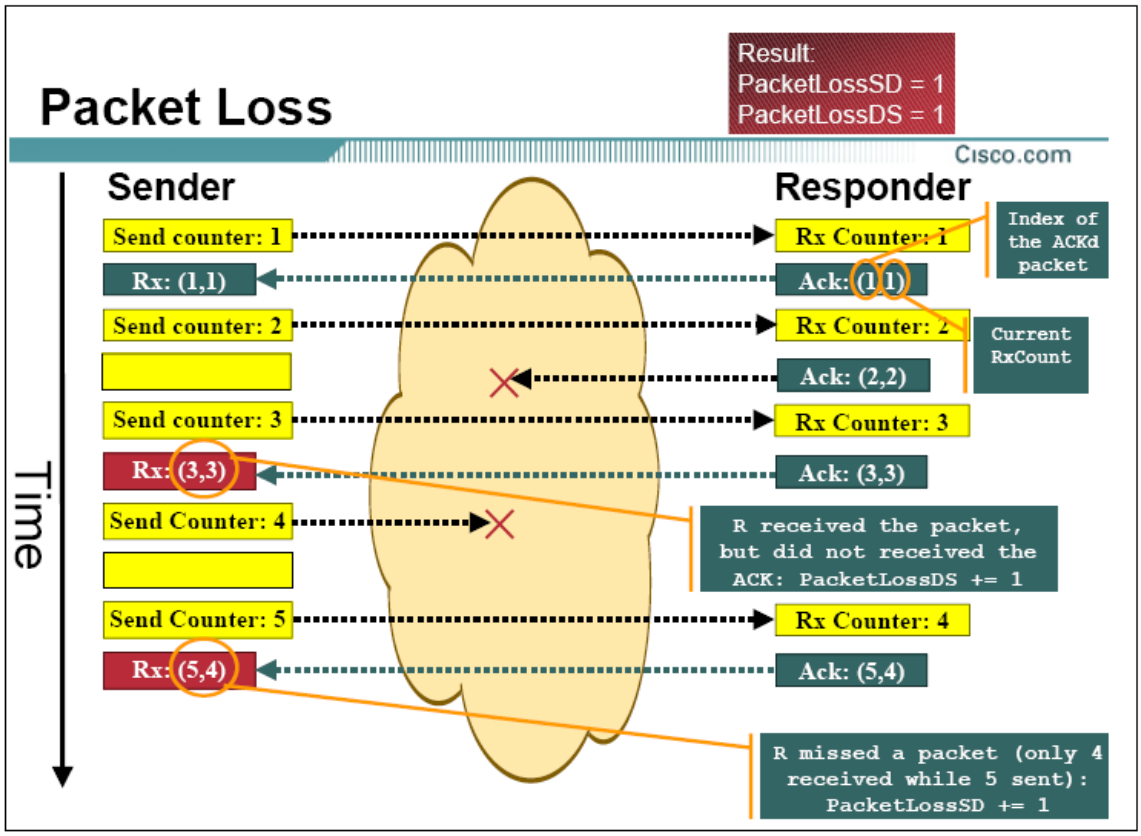


Figura 4.14 Packet Loss.

Por último, antes de mostrar los resultados colectados por los probes, es importante mencionar que el tipo de SLA para el caso del Round Trip Delay que se mide en esta red, es de tipo compuesto como se muestra en la figura 4.15.

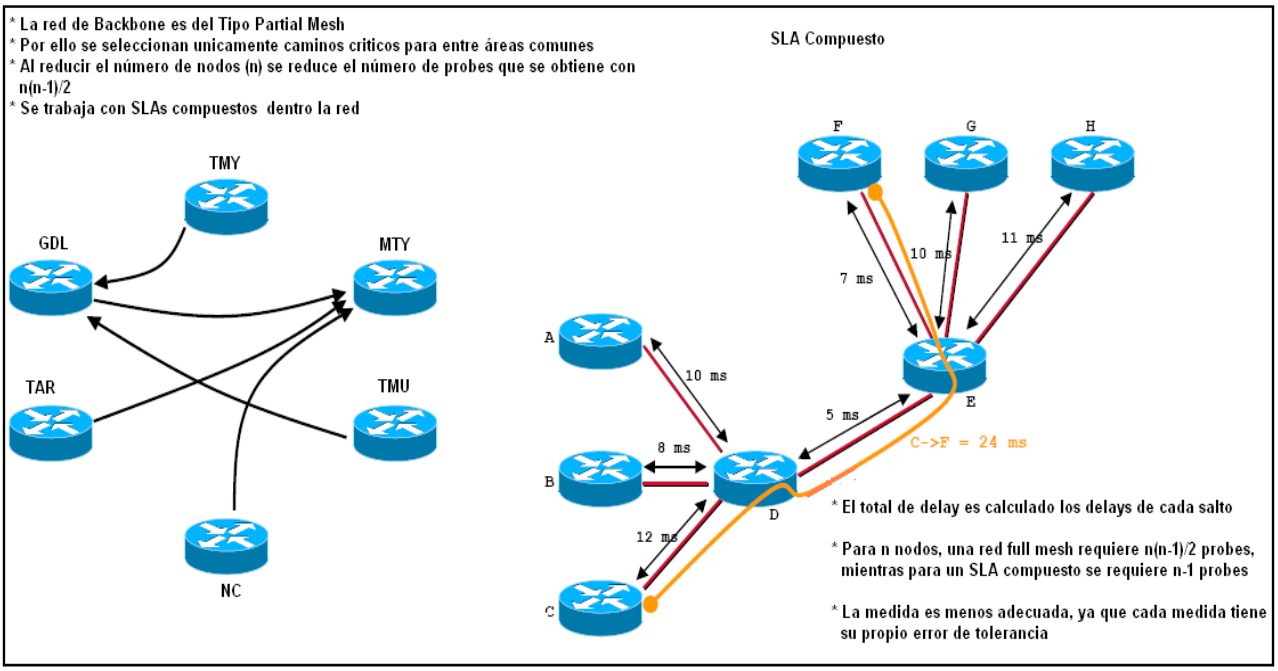


Figura 4.15 Round trip delay compuesto.

4.4.4 Consola de gestión en operación

A continuación, la figura 4.16 muestra la pantalla de la consola que trabaja con SNMP, por medio de la cual se gestiona la red. Aquí se puede observar, que los nodos cambian de color de verde a azul, cuando se genera un trap que es enviado con determinada categoría. En este caso se observa la categoría Major por ser un trap que indica que el enlace está abajo, y Normal cuando el servicio quedo reestablecido.

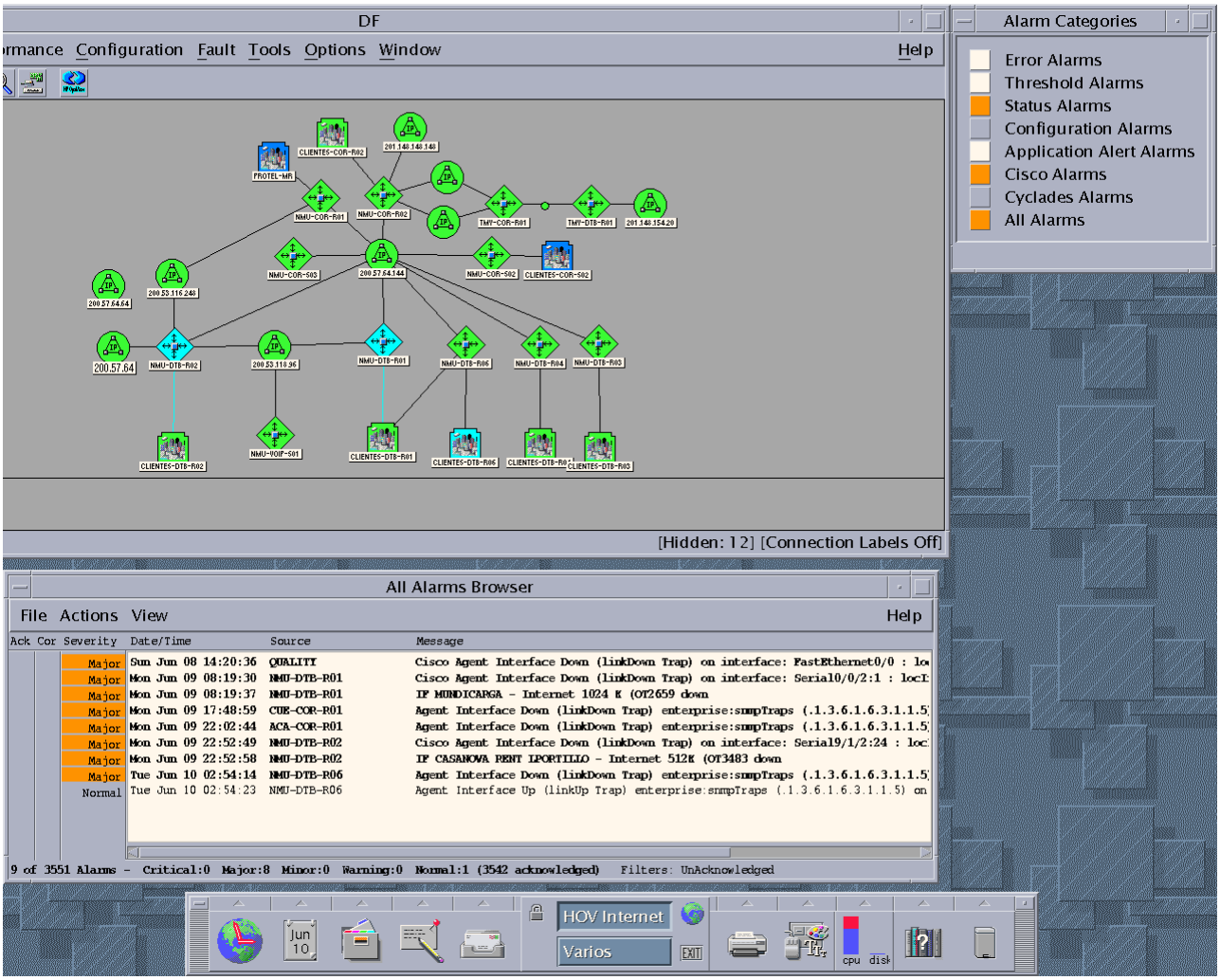


Figura 4.16 Consola de gestión con alarmas y mapa de red.

4.4.5 Información del monitoreo

A continuación, se muestran los resultados del monitoreo de las métricas como packet loss, round trip y disponibilidad, recolectadas por los probes y procesadas por la aplicación IP SLA con la que cuenta la empresa.

Sólo se muestran los resultados y a continuación su análisis.

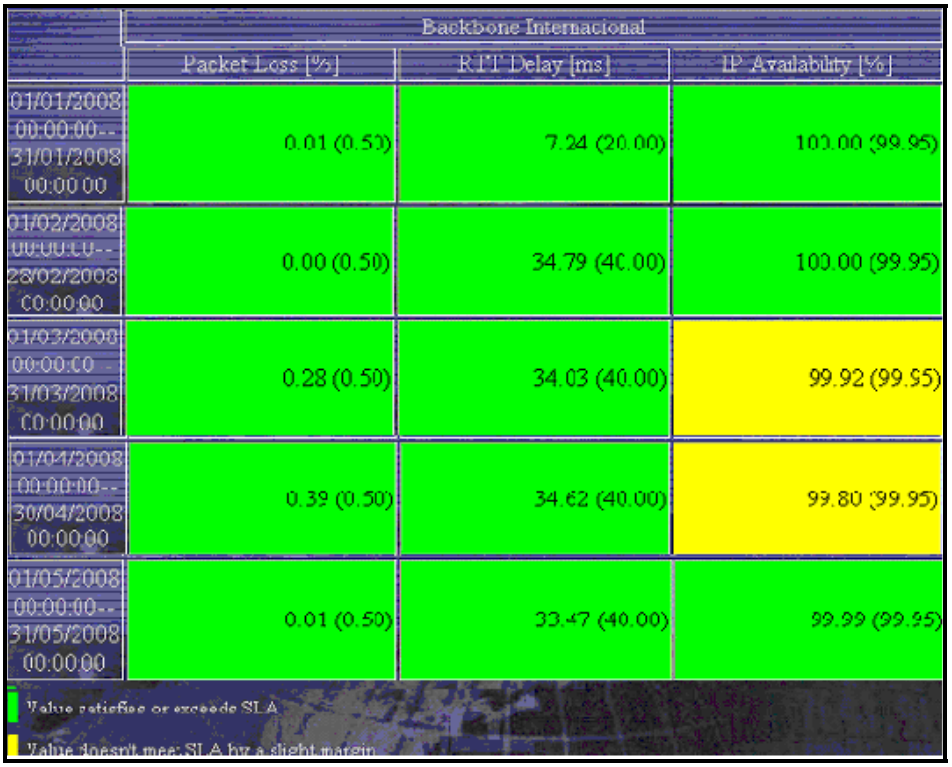
Información recolectada durante cinco meses correspondiente a los enlaces de backbone nacional:

	Backbone Nacional		
	Packet Loss [%]	RTT Delay [ms]	IP Availability [%]
01/01/2008 00:00:00 -- 31/01/2008 00:00:00	0.01 (0.50)	7.24 (20.00)	100.00 (99.95)
01/02/2008 00:00:00 -- 28/02/2008 00:00:00	0.03 (0.50)	7.21 (20.00)	99.97 (99.95)
01/03/2008 00:00:00 -- 31/03/2008 00:00:00	0.16 (0.50)	7.16 (20.00)	99.84 (99.95)
01/04/2008 00:00:00 -- 30/04/2008 00:00:00	0.03 (0.50)	7.25 (20.00)	99.98 (99.95)
01/05/2008 00:00:00 -- 31/05/2008 00:00:00	0.08 (0.50)	7.19 (20.00)	99.94 (99.95)

Value satisfies or exceeds SLA

Value doesn't meet SLA by a slight margin

Información recolectada durante cinco meses correspondiente a los enlaces de backbone internacional:



	Backbone Internacional		
	Packet Loss [%]	RTT Delay [ms]	IP Availability [%]
01/01/2008 00:00:00 -- 31/01/2008 00:00:00	0.01 (0.50)	7.24 (20.00)	100.00 (99.95)
01/02/2008 00:00:00 -- 28/02/2008 00:00:00	0.00 (0.50)	34.79 (40.00)	100.00 (99.95)
01/03/2008 00:00:00 -- 31/03/2008 00:00:00	0.28 (0.50)	34.03 (40.00)	99.92 (99.95)
01/04/2008 00:00:00 -- 30/04/2008 00:00:00	0.39 (0.50)	34.62 (40.00)	99.80 (99.95)
01/05/2008 00:00:00 -- 31/05/2008 00:00:00	0.01 (0.50)	33.47 (40.00)	99.99 (99.95)

Value satisfies or exceeds SLA

Value doesn't meet SLA by a slight margin

4.4.6 Análisis de la información de monitoreo

La aplicación de SLA cuenta con una base de datos, donde se almacena la información recolectada por los probes de packet loss y delay, para después ser presentada en conjunto con los eventos que son documentados en esta en caso de ventanas de mantenimiento o fallas masivas, como cortes de fibra en enlaces principales.

Aplicando la fórmula de la disponibilidad (antes expuesta) se obtuvieron los resultados de la disponibilidad en cada mes:

$$A = 100 \frac{MTBF}{MTBF + MTTR}$$

En donde:

A es la disponibilidad representada en minutos

MTBF es el tiempo que transcurre entre fallas

MTTR es el tiempo que se llevó en reparar las fallas

Tabla de resultados de backbone nacional

Mes	MTBF (min)	MTTR (min)	Cálculo de la disponibilidad	A (%)	Eventos
Ene	31díasx24hrsx60min= 44,640	0	A= [44,640 / (44,640 + 0)] x 100 = 100	100	Ninguno
Feb	16díasx24hrsx60min= 23,040min	7	A= [23,040 / (23,040 +7)] x 100 = 99.97	99.97	Ventana de mantenimiento programada el 16 de febrero
Mar	13d+2d=15 días 15díasx24hrsx60min= 21,600min	34	A= [21,600 /(21,600+34)] x 100 = 99.84	99.84	Falla inesperada por corte de fibra en POP Central el día 2 mazo
Abril	29d+26d= 55 días 55díasx24horasx60min= 79,200min	15	A=[79,200/(79,200 + 15)] x 100 = 99.98	99.98.	Ventana programada para el 26 de abril, que consistió en la implementación del enlace de México a San Luis, y cambio de posición de fibras del COR-R02 a TMY de enlaces México Guadalajara
May	4d+16d= 20 días 20x24x60= 28,800min	17	A=[28,800/(28,800 + 17)] x 100 = 99.94	99.94	Saturación del enlace México-Monterrey Por no tener la política que limitara el uso del ancho de banda contratada de un cliente.

Tabla de resultados de backbone internacional

Mes	MTBF (min)	MTTR (min)	Cálculo de la disponibilidad	A (%)	Eventos
Ene	31x24x60= 44,640	0	A= [44,640 / (44,640 + 0)] x 100 = 100	100	Ninguno
Feb	29x24x60= 41,760	0	A= [41,760 / (41,760 +0)] x 100 = 100	100	Ninguno
Mar	29x24x60= 41,760	33	A= [41,760 / (41,760 +33)] x 100 = 100	99.92	Falla inesperada por corte de fibra en una salida internacional el día 29 marzo
Abril	2d+19d= 21 días 21x24x60= 30,240	60	A=[30240/(30240 + 60)] x 100 = 99.80	99.80	Falla inesperada por corte de fibra en dos salidas internacionales el día 19 abril
Mayo	11d+3d=14días	2	A=[20,160/(20,160 +2)] x 100 = 99.99	99.99	Ventana programada para la conexión de nuevo enlace San Luis a Dallas el día 3 mayo

Conclusiones y propuestas

- Se logró aplicar una metodología para analizar el desempeño de una red, aplicando la metodología de sistemas, que nos permitió ver a la red, aplicaciones, dispositivos y usuarios, como parte de un sistema que tiene dependencias e interacciones, las cuales son importantes para un mejor desempeño individual y en conjunto de estos elementos.
- Se logró realizar un análisis modular de los servicios de la red, encontrando los siguientes puntos de mejora en cada etapa del análisis:

Dentro del análisis de condiciones iniciales y requerimientos:

1. Falta de análisis costo-beneficio, para corroborar si se tiene mayor beneficio al implementar redundancia en enlaces principales y en equipos de core, ya que la falta de redundancia lleva a fallas que impliquen mayores penalizaciones y costos a largo plazo.
2. Falta de trabajo en equipo entre las áreas de la empresa por falta de integración.
3. Mayor control en la implementación de servicios.
4. Explicación al cliente por parte del área de ventas, acerca del servicio, de manera que el cliente conozca si cumple con sus expectativas, para evitar falsos reportes de los servicios.
5. Actualización periódica de los equipos.
6. Documentación completa y actualizada de la red.
7. Conocimiento completo del backbone por parte del personal de soporte.
8. Dentro del análisis de flujos:
9. Crecimiento oportuno de los enlaces en base a las necesidades de la empresa.
10. Capacidad GigabitEthernet en los enlaces principales.
11. Enlaces contratados con diferentes proveedores.
12. Para todos los servicios, implementación de políticas en el ancho de banda, para evitar saturación de los mismos por un uso indebido por parte del cliente.

Dentro del análisis de seguridad:

De acuerdo a los objetivos que se tiene en este trabajo no fue desarrollada esta etapa. Sólo se recolectó el estado actual de la seguridad en la red, y de este se observó que hace falta otorgar mayor importancia al tema de seguridad en la red.

Dentro de la administración:

1. Control total del direccionamiento asignado a los clientes para evitar duplicidad.
2. La administración de la red puede ser del tipo out-boud, aunque esto implicaría mayores costos, pero se tendría el beneficio de no perder gestión de los equipos, al momento de tener fallas en los enlaces.
3. Uso de la información de monitoreo para la planeación de mejoras en la red.
4. Falta de red de pruebas para capacitación y mejores implementaciones de servicios.
5. Falta de capacitación y estímulos por parte de la empresa y autoaprendizaje del personal.
6. Mejor cableado estructurado entre equipos de red para tener mejor acceso a estos.

Contribuciones

Este trabajo contribuye a ilustrar la importancia que tiene el análisis para contar con redes mejor diseñadas, ya que aunque parezca sencillo implementar una red, las decisiones iniciales siempre tienen impacto dentro de la operación de la red, y desafortunadamente este impacto es negativo cuando no se realiza un análisis.

Los resultados del análisis permitieron a los administradores de la red ver los puntos de mejora no considerados, por estar inmersos dentro de la operación diaria de la misma.

Por último, también contribuye a cambiar el enfoque que todavía se tiene de las redes, el cual aún considera a las redes como un elemento separado de los usuarios, las aplicaciones y dispositivos, sin considerar que sus características interactúan y dependen entre sí para un mejor desempeño.

Trabajo futuro

El análisis del desempeño de esta red, fue sólo a nivel IP o de capa de red. Cabe mencionar que por la dimensión y características de esta red, algunos puntos que se dejan pendientes por desarrollar en un trabajo futuro son:

A nivel de transmisión, un análisis de las tecnologías de fibra óptica utilizada para el transporte de datos.

Análisis de la parte inalámbrica (enlaces de microondas) con la que cuenta esta empresa.

Desarrollar el análisis de la tecnología de cómo son implementados los servicios que ofrece esta empresa, como son servicios de voz sobre IP, enlaces ruteados, enlaces virtuales (VPNs implementadas con mpls) y housing.

Realizar el análisis de seguridad, que por su extensión no se realizó.

Por último, lo que resta es diseñar redes en base a un análisis, antes de comprar tecnología y elegir topologías. Hay que analizar lo que se tiene y lo que se quiere, tanto a mediano como a largo plazo.

Glosario

API (Application Programming Interface - Interfaz de Programación de Aplicaciones), es el conjunto de funciones y procedimientos (o métodos si se refiere a programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

ARP (Address Resolution Protocol - Protocolo de Resolución de Direcciones), es un protocolo responsable de encontrar la dirección hardware que corresponde a una determinada dirección IP.

ASIC (Circuito Integrado para Aplicaciones Específicas), es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general.

BGP (Border Gateway Protocol), es un protocolo mediante el cual se intercambia información de encaminamiento entre Sistemas Autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos. Actualmente entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo. Estos routers deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un EGP (external gateway protocol

CRM (Customer Relationship Management). Es software para la administración de la relación con los clientes (venta y marketing).

DHCP (Dynamic Host Configuration Protocol - Protocolo Dinámico de Configuración de Anfitrión), es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Disponibilidad (Availability), también conocida como disponibilidad operacional, es la medida de la relación entre la frecuencia de fallas de misión crítica y el tiempo para restaurar el servicio. Es expresada en términos de Mean-Time-Between-Failures (MTBF) dividido entre la suma del MTTR y el MTBF.

DNS (Domain Name System), es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

EGP (Exterior Gateway Protocol), protocolo de ruteo usado para comunicar sistemas autónomos. Un sistema autónomo es una colección de redes bajo una administración común y que comparten una estrategia común de ruteo. Un ejemplo de un protocolo EGP es BGP

EIGRP (Enhanced Interior Gateway Routing), es un protocolo de encaminamiento híbrido, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia y del estado de enlace. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace.

Fiabilidad (Reliability), es la media estática de la frecuencia de fallo de una red y sus componentes y representa caídas imprevistas del servicio. Las medidas de fiabilidad son: MTBFs (Mean Time Between Failures) y MTBCF (Mean Time Between Mission Critical Failures), usualmente expresadas en horas.

FLSM (Fixed-Length Subset Masks), es cuando todas las subnet masks en la mayoría de las redes deben ser de tamaño fijo.

Frame Relay (Frame-mode Bearer Service), es una técnica de comunicación mediante retransmisión de tramas, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("frames") para datos, perfecto para la transmisión de grandes cantidades de datos.

FTP (File Transfer Protocol), es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

IANA (The Internet Assigned Numbers Authority) asigna números de sistemas autónomos para diversas jurisdicciones. El uso de un número de sistema autónomo de la IANA es requerido si la organización planea usar un EGP, tal como BGP. Sin embargo es una buena práctica conocer las características ambos esquemas de numeración de sistemas autónomos, el privado y el público.

IETF (Internet Engineering Task Force - Grupo de Trabajo en Ingeniería de Internet), es una organización internacional abierta de normalización, que tiene como objetivo el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

IGP (Interior Gateway Protocol), protocolo usado para intercambiar la información de ruteo dentro de un sistema autónomo. Los protocolos RIPv1 y RIPv2, EIGRP y OSPF son ejemplos de IGPs.

ITU-T (Unión Internacional de Telecomunicaciones), es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional, entre las distintas administraciones y empresas operadoras.

LAN (Local Area Network - Red de Área Local) Conexión física y lógica de dispositivos que tiene como fin compartir recursos dentro de un área local

MAC (Medium Access Control Address - Dirección de Control de Acceso al Medio), es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI.

Mantenimiento (Maintainability), es la medida estática de tiempo para restaurar el sistema a un estado de total operación después de que este experimenta un fallo. Este es generalmente expresado como Mean-Time-ToRepair (MTTR).

OSI (Open System Interconnection - Modelo de Referencia de Interconexión de Sistemas Abiertos), es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

OSPF (Open Shortest Path First), es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

PPP (Point-to-point Protocol - Protocolo Punto a Punto), es un protocolo del nivel de enlace, estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet. Más conocido por su acrónimo: PPP.

QoS (Quality of Service – Calidad de Servicio), es la medida de la calidad de transmisión y la disponibilidad del servicio de la red.

Red Stub (leaf node), es una red a la que se tiene acceso por una sola ruta y a ella no se interconectan más redes

RIP (Routing Information Protocol - Protocolo de encaminamiento de información), es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RMA (Reliability, Maintainability, Availability). Siglas en inglés de Fiabilidad, Mantenimiento y Disponibilidad

RTP (Real-Time Transport Protocol), es un protocolo diseñado para ser usado para el tráfico de tiempo real como voz. RTP usa los puertos UDP 16384 a 32767 (para evitar encabezado adicional y delay de TCP). RTP adiciona otro encabezado que incluye información de secuencia e información de marcado de tiempo para asegurar que los datos recibidos son procesados en orden correcto y que la variación del delay esta dentro de los limites aceptables.

SMTP (Simple Mail Transfer Protocol - Protocolo Simple de Transferencia de Correo). Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

VLAN (acrónimo de Virtual LAN, 'red de área local virtual'), es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3).

VLSM: Variable-Length Subset Masks, es cuando las subnet masks en la mayoría de las redes están conformadas por diferentes cantidad de bits.

VPN (Virtual Private Network - Red Privada Virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Anexo A. Concentrado de MIBs para routers Cisco

All the Cisco MIBs are at http://www.Cisco.com/public/mibs/
http://www.Cisco.com/public/mibs/trapsInteresting MIBs for Routers

Description	MIB - textual OID	MIB - numeric OID
Cisco Local Free Mem	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.freeMem	1.3.6.1.4.1.9.2.1.8
	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferElFree(9)	1.3.6.1.4.1.9.2.1.9
	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferElMax(10)	1.3.6.1.4.1.9.2.1.10
Cisco Local Buffer Hit	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferElHit(11)	1.3.6.1.4.1.9.2.1.11
Cisco Local Buffer Miss	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferElMiss(12)	1.3.6.1.4.1.9.2.1.12
	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferElCreate(13)	1.3.6.1.4.1.9.2.1.13
Cisco Local Buffer Fail	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferFail(46)	1.3.6.1.4.1.9.2.1.46
Cisco Local Buffer NoMem	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.bufferNoMem(47)	1.3.6.1.4.1.9.2.1.47
Cisco Local CPU avgBusy1	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.avgBusy1(57)	1.3.6.1.4.1.9.2.1.57
Cisco Local CPU avgBusy5	iso.org.dod.internet.private.enterprises.Cisco.local.lsystem.avgBusy5(58)	1.3.6.1.4.1.9.2.1.58
Cisco MemoryPoolUsed		1.3.6.1.4.1.9.9.48.1.1.1.5
Cisco MemoryPoolFree		1.3.6.1.4.1.9.9.48.1.1.1.6
CIP CPU Util		1.3.6.1.4.1.9.9.20.1.1.1.5
CIP Free Memory		1.3.6.1.4.1.9.9.20.1.1.1.4
LocIfSlowInPkts		
LocIfSlowOutPkts		
LocIfFastInPkts		
LocIfFastOutPkts		
LocIfotherInPkts		
LocIfotherOutPkts		
LocIfipInPkts		
LocIfipOutPkts		
IpInReceives	iso.org.dod.internet.mgmt.mib-2.ip.ipInReceives(3)	1.3.6.1.2.1.4.3
IpInHdrErrors	iso.org.dod.internet.mgmt.mib-2.ip..ipInHdrErrors(4)	1.3.6.1.2.1.4.4
IpInAddrErrors	iso.org.dod.internet.mgmt.mib-2.ip.ipInAddrErrors(5)	1.3.6.1.2.1.4.5
IpForwDatagrams	iso.org.dod.internet.mgmt.mib-2.ip.ipForwDatagrams(6)	1.3.6.1.2.1.4.6
IpInDiscards	iso.org.dod.internet.mgmt.mib-2.ip.ipInDiscards(8)	1.3.6.1.2.1.4.8
IpInDelivers	iso.org.dod.internet.mgmt.mib-2.ip.ipInDelivers(9)	1.3.6.1.2.1.4.9

Anexo B. El modelo OSI y TCP/IP

El Modelo OSI.

La Organización internacional para la estandarización por sus siglas en inglés ISO (Internacional Organization for Standardization), creo una lista de las funciones requeridas para el envío de datos, dividida en siete categorías. Estas categorías en conjunto son conocidas como el Modelo OSI el cual fue creado en 1984. El modelo y algunos protocolos que corresponden a cada capa son mostrados en la figura B-1

> Para consultar a detalle cada una de las capas se puede consultar la referencia bibliografica **[9]**

7	Aplicación	ej. HTTP, DNS, SMTP, SNMP, FTP, Telnet, SSH y SCP, NFS, RTSP, Feed, Webcal , POP3
6	Presentación	ej. XDR, ASN.1, SMB, AFP
5	Sesión	ej. TLS, SSH, ISO 8327 / CCITT X.225, RPC, NetBIOS
4	Transporte	ej. TCP, UDP, RTP, SCTP, SPX
3	Red	ej. IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IGRP, EIGRP, IPX, DDP
2	Enlace de datos	ej. Ethernet, Token Ring, PPP, HDLC, Frame Relay, RDSI, ATM, IEEE 802.11, FDDI
1	Físico	ej. cable, radio, fibra óptica

Figura B-1. Modelo OSI

El modelo OSI provee un marco de referencia para la comunicación de protocolos usados entre computadoras. Muchas suites de protocolos definen varios protocolos que corresponden a las funciones definidas en las siente capas del modelo OSI, incluyendo protocolos de ruteo, aplicaciones, etc. Las suites de protocolos son conocidas como *pilas de protocolos.*

TCP/IP es la pila de protocolos mas usada en redes, sobre todo en Internet.

Las capas del modelo OSI.

La capa 1, física, define las especificaciones, tales como las condiciones eléctricas y mecánicas que son necesarias para activar, mantener y cambiar los enlaces físicos entre dispositivos. Estas especificaciones incluyen niveles de voltaje, tipo de cableado y conectores. La capa física maneja la transmisión a nivel de ***bits.***

La capa 2, enlace de datos, define el formato de los datos para ser transmitidos a través de la red física e indica cómo el medio físico es accedido, incluyendo direccionamiento físico, control de errores y control de flujo. La capa de enlace de datos envía ***frames*** de datos; diferentes medios tienen diferentes tipos de frames.

Un frame es definido como el conjunto de datos que incluye control de información y direccionamiento, y es transmitido entre dispositivos de red.

Para Lans, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) dividió esta capa en dos subcapas: control lógico del enlace (LLC, Logical Link Control) y control de acceso al medio (MAC, Media Access Control)

La capa 3, de red, es responsable del ruteo, el cual permite el envió lógico de datos a través de redes. Los protocolos de esta capa incluyen protocolos de ruteo y ruteables. Los protocolos de ruteo determinan el mejor camino que debe ser usado para enviar datos a través de las redes hasta su destino.

La capa de red envía ***datagramas (o paquetes);*** diferentes protocolos de ruteo tienen diferentes tipos de datagramas

Un datagrama es un conjunto de datos que incluye dirección e información de control, y es ruteado entre la fuente y el destino. Si un datagrama necesita ser enviado a través de la red que únicamente controla cierta cantidad de datos a la vez, el datagrama puede ser dividido en múltiples paquetes y entonces es reensamblado en su destino. El formato de un datagrama IP se muestra en la figura B-2.

Los Datagramas IP están formados por al menos 20 Bytes:

Versión	Hlength	TOS (Tipo de Servicio)	Longitud Total	
Identificación			Flags	Fragment offset
TTL		Protocolo	Header checksum	
Dirección IP de la Fuente				
Dirección IP del Destino				
Opciones IP (Opcional)				Padding
DATOS				

B-2. Formato del Datagrama IP

Versión (4 bits). Versión de IP. La actual versión IP es la 4.

Hlength (4 bits). Tamaño de la cabecera en palabras.

TOS Tipo de servicio (8 bits). Específica cómo el datagrama debe ser controlado dentro de la red. Estos bits marcan el tráfico para una específica calidad de servicio (QoS). Su estructura es:

Prioridad	D	T	R	Sin Uso

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes. Los tipos D, T y R solicitan un tipo de transporte dado: D = Procesamiento con retardos cortos, T = Alto Desempeño y R = Alta confiabilidad.

Longitud total (16 bits). Número total de octetos de los encabezados y campos de datos

Identificación (16 bits), flags (3 bits), y fragment offset (13 bits). Controlan casos en donde un datagrama grande debe ser fragmentado -- dividido en múltiples paquetes – para ir a través de una red que no puede controlar datagramas de ese tamaño.

TTL (8 bits). Asegura que los datagramas no formen loops en la red, este campo debe ser decrementado en uno por cada router por el que pasa el datagrama.

Protocolo (8 bits). Indica el protocolo de la capa cuatro (transporte de datos) que el datagrama esta portando. El número 6 indica que esta portando un segmento TCP, mientras que el 17 indica que el datagrama porta un segmento UDP.

Header checksum (16 bits). Asegura que el encabezado es recibido correctamente.

Dirección IP Fuente y Destino (32 bits cada una). Dirección IP asignada para la fuente y destino del datagrama.

Opciones IP y Padding (de ancho variable, 0 o multiplos de 32 bits). Usados para pruebas de red.

La capa 4, de transporte, se encarga de las conexiones de extremo a extremo entre la fuente y el destino. Esta capa provee servicios para capas superiores, incluyendo transporte de tipo connection-oriented y connectionless, multiplexación, chequeo de errores y recuperación de datos

Transporte de tipo connection-oriented, establece una conexión lógica y usa números de secuencia para asegurar que todos los datos son recibidos en el destino, por ello también se dice que es de tipo fiable.

Transporte de tipo connectionless, envía los datos sin establecer ningún tipo de conexión y confía en mecanismos de detección de las capas superiores para reportar y corregir problemas

Multiplexación permite a varias aplicaciones usar la misma conexión física.

La capa de transporte envía ***segmentos.***

Un segmento es un conjunto de datos que incluyen información de control y es enviado entre las capas de transporte de la fuente y el destino de los datos.

La capa 5, de sesión, es la responsable de establecer, mantener, y terminar las sesiones de comunicación entre las aplicaciones corriendo en diferentes dispositivos.

La capa 6, de presentación, específica el formato, la estructura de los datos, codificación, compresión y otras maneras de representar los datos para asegurar que la información enviada por la fuente puede ser leída por el destino.

La capa 7, de aplicación, es la más cercana al usuario final; ésta interactúa con el software de la aplicación que necesita comunicarse sobre la red.

TCP/IP

Es la pila de protocolos más usada en redes y sobre todo en Internet es TCP/IP.

Su nombre hace referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia.

Normalmente, los tres niveles superiores del modelo OSI (Aplicación, Presentación y Sesión) son considerados simplemente como el nivel de aplicación en el conjunto TCP/IP. Como TCP/IP no tiene un nivel de sesión unificado sobre el que los niveles superiores se sostengan, estas funciones son típicamente desempeñadas (o ignoradas) por las aplicaciones de usuario. La diferencia más notable entre TCP/IP y OSI es el nivel de Aplicación, en TCP/IP se integran algunos niveles del modelo OSI en su nivel de Aplicación. Una interpretación simplificada de la pila TCP/IP se muestra:

4	Aplicación	ej.HTTP,FTP,DNS (protocolos de enrutamiento como BGP y RIP, que por varias razones funcionen sobre TCP y UDP respectivamente, son considerados parte del nivel de internet)
3	Transporte	ej.TCP,UDP,RTP,SCTP (protocolos de enrutamiento como OSPF, que funcionen sobre IP, son considerados parte del nivel de Internet)
2	Internet	Para TCP/IP este es el Protocolo de Internet (IP) (protocolos requeridos como ICMP e IGMP funcionan sobre IP, pero todavía se pueden considerar parte del nivel de red; ARP no funciona sobre IP)
1	Interface de Red	ej. Ethernet, Token Ring, PPP, HDLC, Frame Relay, RDSI, ATM, IEEE 802.11, FDDI

El nivel de Interface de red

Comprende las funciones de la capa física y enlace de datos

El nivel de Internet

Se encarga del enrutamiento de paquetes a través de una red de redes, conocida como Internet.

En la familia de protocolos de Internet, IP realiza las tareas básicas para **conseguir transportar datos desde un origen a un destino**. IP puede pasar los datos a una serie de protocolos superiores; cada uno de esos protocolos es identificado con un único "Número de protocolo IP". ICMP y IGMP son los protocolos 1 y 2, respectivamente.

El nivel de Transporte

Los protocolos del nivel de transporte pueden solucionar problemas como la fiabilidad y la seguridad de que los datos llegan en el orden correcto. En el conjunto de protocolos TCP/IP, los protocolos de transporte también determinan a qué aplicación van destinados los datos, los principales son TCP y UDP.

TCP (protocolo IP número 6) es un mecanismo de transporte fiable y orientado a conexión, que proporciona un flujo fiable de bytes, que asegura que los datos llegan completos, sin daños y en orden. TCP realiza continuamente medidas sobre el estado de la red para evitar sobrecargarla con demasiado tráfico. Además, TCP trata de enviar todos los datos correctamente en la secuencia especificada. Esta es una de las principales diferencias con UDP, y puede convertirse en una desventaja en flujos en tiempo real (muy sensibles a la variación del retardo) o aplicaciones de enrutamiento con porcentajes altos de pérdida en el nivel de Internet.

UDP (protocolo IP número 17) es un protocolo de datagramas sin conexión. Es un protocolo no fiable (*best effort* al igual que IP) - no porque sea particularmente malo, sino porque no verifica que los paquetes lleguen a su destino, y no da garantías de que lleguen en orden. Si una aplicación requiere estas características, debe llevarlas a cabo por sí misma o usar TCP.

UDP es usado normalmente para aplicaciones de streaming (audio, video, etc) donde la llegada a tiempo de los paquetes es más importante que la fiabilidad, o para aplicaciones simples de tipo petición/respuesta como el servicio DNS, donde la sobrecarga de las cabeceras que aportan la fiabilidad es desproporcionada para el tamaño de los paquetes.

DCCP está actualmente bajo desarrollo por el IETF. Proporciona semántica de control para flujos TCP, mientras de cara al usuario se da un servicio de datagramas UDP.

TCP y UDP: son usados para dar servicio a una serie de aplicaciones de alto nivel. Las aplicaciones con una dirección de red dada son distinguibles entre sí por su número de puerto TCP o UDP. Por convención, los puertos bien conocidos (*well-known ports*) son asociados con aplicaciones específicas.

RTP es un protocolo de datagramas que ha sido diseñado para datos en tiempo real como el streaming de audio y video que se monta sobre UDP.

Los campos de los segmentos de UDP y TCP se muestran en la figura B-3:

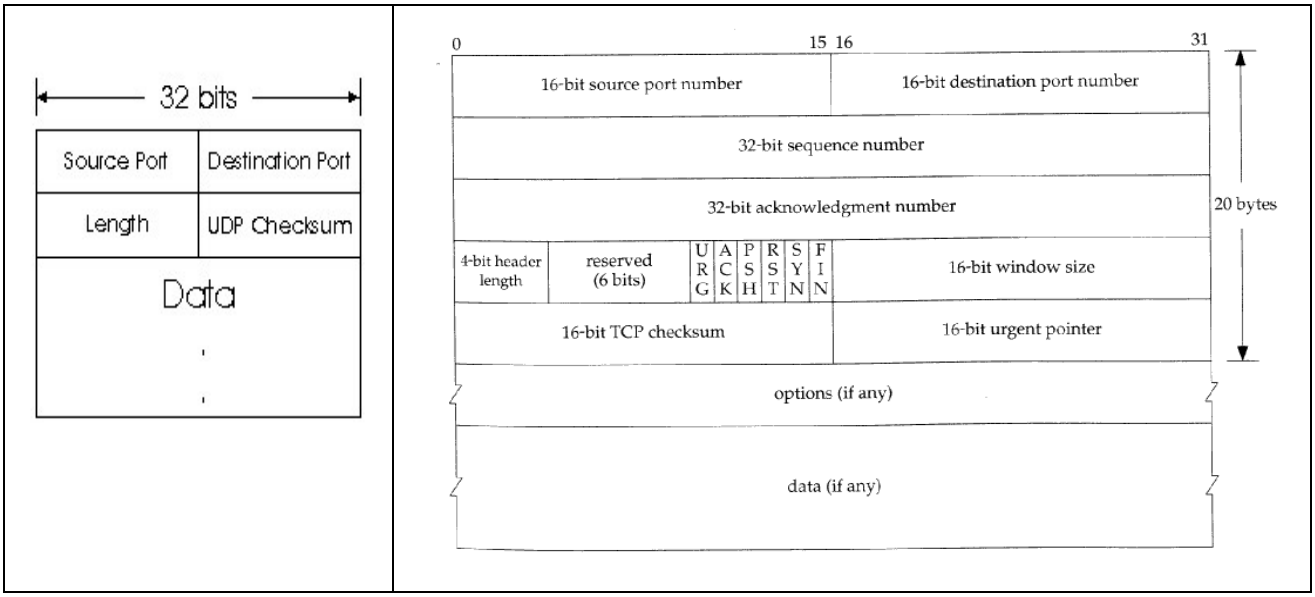


Figura B-3. Segmentos UDP y TCP.

Un segmento UDP al menos cuenta con 8 bytes, sus campos son:

Source/Destination Port (16 bits cada uno): Identifica el Puerto de las aplicaciones de la fuente y destino.

Length (16 bits). Número total de octetos de los encabezados y campos de datos

UDP checksum (16 bits). Asegura que el segmento es recibido correctamente.

Data (variable). Datos de las aplicaciones

Un segmento TCP debe contener al menos 20 bytes sus campos son:

Source/Destination Port (16 bits cada uno). Identifica el Puerto de las aplicaciones de la fuente y destino.

Sequence and acknowledgment numbers (32 bits cada uno). Asegura el orden correcto de los datos recibidos en cada destino.

Header lenght (4 bits). Indica el tamaño del encabezado.

Reserved (6 bits). Para uso futuro.

Code bits (6 bits). Indica diferentes tipos de segmentos. Por ejemplo la SYN (sincronizar), ACK (confirmación de recepción), FIN (termino de la sesión)

Window size (16 bits). El número de octetos que el dispositivo receptor esta aceptando antes de enviar un ACK

El nivel de Aplicación

El nivel de aplicación es el nivel que los programas más comunes utilizan para comunicarse a través de una red con otros programas. Los procesos que acontecen en este nivel son aplicaciones específicas que pasan los datos al nivel de aplicación en el formato que internamente use el programa y es codificado de acuerdo con un protocolo estándar.

Algunos programas específicos se considera que se ejecutan en este nivel. Proporcionan servicios que directamente trabajan con las aplicaciones de usuario. Estos programas y sus correspondientes protocolos incluyen a HTTP (*HyperText Transfer Protocol*), FTP (Transferencia de archivos), SMTP (correo electrónico), SSH (login remoto seguro), DNS (Resolución de nombres de dominio) y a muchos otros.

Una vez que los datos de la aplicación han sido codificados en un protocolo estándar del nivel de aplicación son pasados *hacia abajo* al siguiente nivel de la pila de protocolos TCP/IP.

En el nivel de transporte, las aplicaciones normalmente hacen uso de TCP y UDP, y son habitualmente asociados a un número de puerto bien conocido (*well-known port*). Los puertos fueron asignados originalmente por la IANA.

Bibliografía

[1] McCabe James D. Network Analysis, Architecture and Design, Second Edition,The Morgan Kaufmann Series in Networking

[2] Teare Diane, Paquet Catherine, Capítulos 1,2,3,4,6. Campus Network Design Fundamentals, Series Cisco Press, San José, California, 2006

[3] Curtis Nancy, Taylor Pamela, Lesson 4, Network+ CompTIA Certification Volumen 1,2, New York, Cuarta Edición, 2006

[4]Lesson1 Introducing Basic Layer 2 Switching and bridging functions, ICND v2.3 2006 Interconnecting Cisco Network Devices, Cisco Training and Certifications CCNA

[5] Amir Ranjbar, Capítulo 1,2. CCNP ONT Oficial Exam Certification Guide, Cisco Systems, 2007.

[6] Oram Andy, Peer-to-peer/Harnessing the Power of Disruptive Technologies, O´Reilly, P. 191.

[7] stewart Bret D, Capítulo 1 "Network design". CCNP ONT Oficial Exam Certification Guide, Cisco Systems, 2008

[8] Norris Mark, Held Gilbert Capítulo 8. Managing Total Area Ethernetworks, Enhacing Lan performance, Wiley, Tercera Edición, 2000

[9] Tanenbaum S. Andrew, Redes de computadoras, Prentice Hall, Cuarta Edición 2003

Cisco Systems, Inc. *Cisco MIB Reference* [en línea], San José, CA 95134-1706 USA: 1998, <http://www.sinclair.org.au/keith/Cisco/Cisco-mibs.html> [Consulta: Febrero 20, 2007]

Cisco Systems, Inc. *Empowered Branch Services* [en línea], San José, CA 95134-1706 USA, <http://www.Cisco.com/go/managedservices> [Consulta: Enero 11, 2007]

Cisco Systems, Inc. *Enterprise QoS Solution Reference Network Design Guide*, Version 3.3 [en línea], San José, CA 95134-1706 USA: Noviembre 2005, <http://www.Cisco.com/univercd/cc/td/doc/solution/esm/qossrnd.pdf> [Consulta: Septiembre 9, 2007]

Cisco Systems, Inc. *Virtual LANs/VLAN Trunking Protocol (VLANs/VTP* [en línea], San José, CA 95134-1706 USA, <http://www.Cisco.com/en/US/tech/tk389/tk689/tsd_technology_support_protocol_home.html> [Consulta: Agosto 20, 2007]

Wikipedia.org. < http://es.wikipedia.org > [en línea] [Consulta: 28 Octubre 2008]