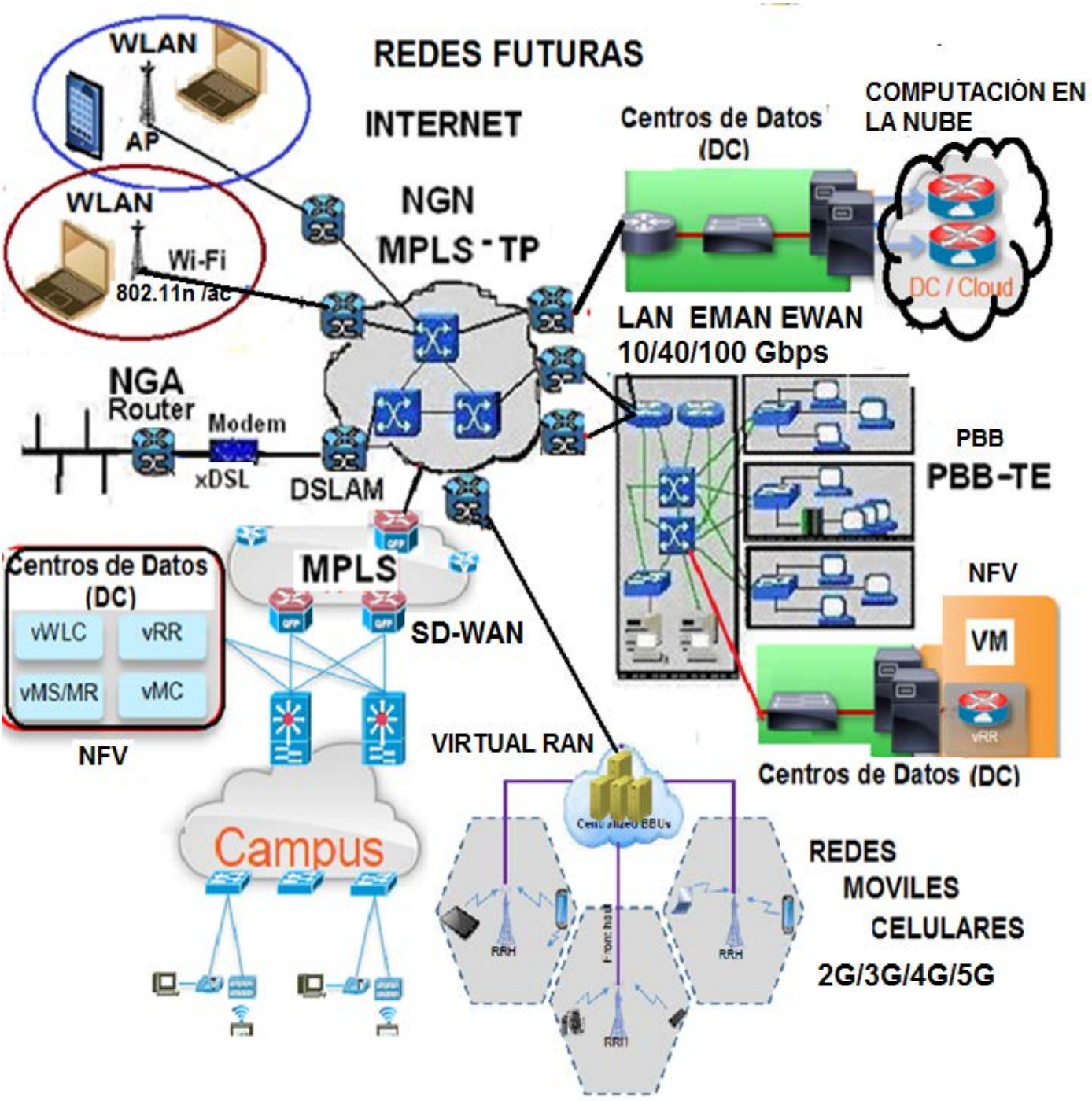
DISEÑO DE REDES EMPRESARIALES MODERNAS



Autor: Dr. Félix Alvarez Paliza
Dpto. Telecomunicaciones
UCLV

Introducción

El diseño de redes se refiere a la planificación de la implementación de la infraestructura de una red de comunicaciones y computadoras. El diseño de redes es ejecutado generalmente por ingenieros, diseñadores de redes, administradores de tecnologías de la información (TI) y otro personal del equipo de redes relacionado con la temática. Este proceso de diseño es realizado antes de la puesta en marcha de la infraestructura de una red.

El diseño de una red involucra evaluar, entender y abarcar la red antes de empezar su montaje y puesta en operación. El diseño completo o integral es a menudo representado por un diagrama de red que sirve como anteproyecto para implementar físicamente la red.

Cuando se mira el diseño de una red hay que considerar las tendencias de las redes y las necesidades futuras de una organización.

- La red tiene que estar lista para escalar apropiadamente en el transcurso del tiempo para encontrar las demandas que soporta la organización.
- Las demandas sobre los puntos de acceso inalámbricos (AP) con las últimas tecnologías (802.11ac de segunda generación y 802.11ax), requieren de una actualización del cableado de cobre existente para desplegar plataformas de red con capacidades multi-Gigabit.
- Hay que desplegar nuevos dispositivos con exigencias de alta potencia, tales como alumbrado, conmutadores de acceso remoto, puntos de acceso (AP), teléfonos IP, Sensores y otros dispositivos. Por lo que el diseño debe tener capacidad de soportar potencia sobre Ethernet (PoE con 60W por puerto).
- Internet de las cosas (IoT) impacta hoy en el diseño de redes y el diseño de una red debe soportar tecnologías de video vigilancia y otras tecnologías de virtualización y segmentación de la red que posibiliten escalar y expandir la red.
- El ancho de banda necesita ser potencialmente duplicado en múltiples plazos durante el tiempo de vida de la red de forma tal que la red desplegada hoy necesita estar preparada para añadirle nuevas capacidades de 10 Gbps, 40 Gbps y hasta 100 Gbps en el transcurso del tiempo.
- La plataforma de red desplegada hoy debe ofrecer la mejor longevidad hacia el futuro contra la selección del equipamiento que solo encuentra los límites de las necesidades actuales.
- Para diferentes tamaños y densidades de redes deben converger las plataformas de redes inalámbricas y alambradas a la hora en que la flexibilidad es la mejor forma para fijar las exigencias del despliegue.

Típicamente el diseño de red incluye los aspectos siguientes:

- Mapa lógico de la red a ser diseñada
- Cableado estructurado
- Cantidad, tipos y localizaciones de los dispositivos de red (enrutadores, conmutadores, servidores, etc.)
- Estructura de direcciones IP
- Arquitectura de seguridad de la red en conjunto con otros procesos de seguridad de la red

Análisis de una Red Empresarial típica

Por lo general las redes empresariales constan de varias redes LAN interconectadas por Enrutadores y Conmutadores de Capa 3, corriendo el protocolo IP en sus versiones IPv4 e IPv6 y donde el mayor volumen tráfico sobre esta red es basado en aplicaciones web, transferencia de ficheros, videoconferencias, teletrabajo, bases de datos, video vigilancia, Telefonía IP, Sensores, etc**.**

Las exigencias a una red empresarial actual se pueden sintetizar de la forma siguiente:

- Interconexión de redes LAN con estructura jerárquica
- Disponer de más de un protocolo de red
- Áreas configuradas con uno o dos protocolos de enrutamiento interno y externo**.**
- Facilidades de conexiones a la red para los empleados desde sus casas
- Interconexiones de la red a las oficinas ramales en otros lugares fuera del campus.
- Exigencias de nuevas conexiones a nuevas oficinas y de nuevos usuarios
- Servicios de Extranet a usuarios.
- Conexiones a Internet

La topología de las redes Empresariales muchos autores la dividen en bloques modulares o jerárquicos con la siguiente designación: Nivel de Acceso, Nivel de Distribución y Nivel Principal (Core), tal como se muestra de forma simplificada en la Figura 16.1 que se muestra a continuación.

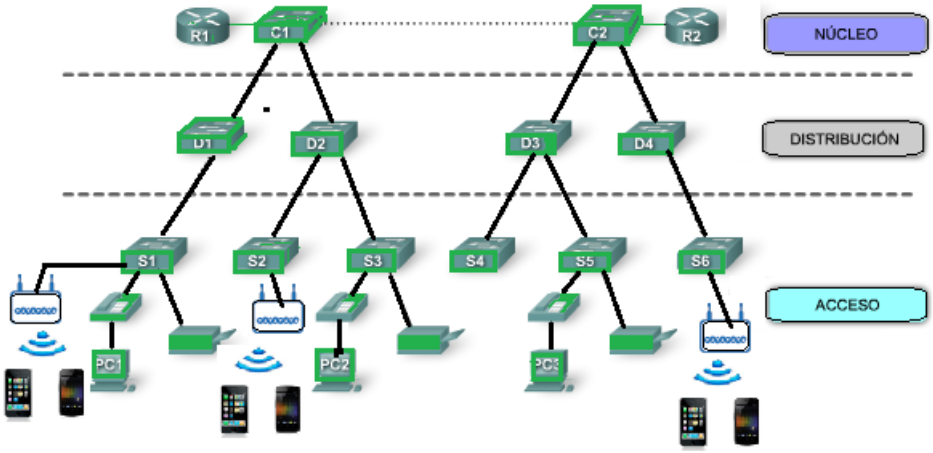


Fig.16.1 Esquema simplificado la jerarquía de red de tres niveles

Los niveles poseen las características siguientes:

Nivel de Acceso: Es el nivel donde los dispositivos controlados por los usuarios o accesibles a los usuarios y otros dispositivos finales son conectados a la red. Este nivel ofrece conectividad tanto alambrada como inalámbrica y comprenden rasgos y servicios que aseguran la seguridad y elasticidad de la red completa.

Nivel de Distribución: Este nivel apoya muchos servicios importantes. En una red donde la conectividad necesita atravesar la red LAN de extremo a extremo entre diferentes dispositivos o entre un dispositivo de nivel de acceso hasta una red WAN o hasta el borde de Internet, el nivel de distribución facilita esta conectividad. El nivel de distribución es el encargado de ofrecer la conectividad basada en las políticas, ofrecer seguridad, direccionamiento, delimitar el dominio de difusión y de grupos (multicast), encargarse del enrutamiento entre las VLAN y la traducción de medios entre tipos de redes.

Nivel de Núcleo (Core o Backbone): Este nivel es una parte crítica de una red escalable y aún es una de las partes más simple para el diseño. El mismo es diseñado con conmutadores de alta velocidad que trabajan como mínimo entre 1 a 10 GigabitEthernet. Caracterizándose por su alto nivel de disponibilidad y adaptación rápida a los cambios.

Entre las características que debe tener el Núcleo de la red están:

- Ofrecer un centro de conmutación de la red de alta velocidad
- Ofrecer alta confiabilidad
- Deber ser redundante para proporcionar alta fiabilidad
- Brindar alta recuperación ante fallos.
- Adaptarse a cambios rápidamente.
- Tener baja latencia y buen nivel de gestión.

Hay redes empresariales pequeñas o medianas donde solo se utilizan dos niveles, dado que se integran el nivel de distribución y el nivel principal o núcleo.

A continuación se muestra en la Figura 16.2 un esquema general (no es un plano de conexiones lógicas) a modo de ejemplo de una Red Empresarial (Intranet con acceso a Internet y servicios Extranet) en un edificio de oficinas de una empresa.

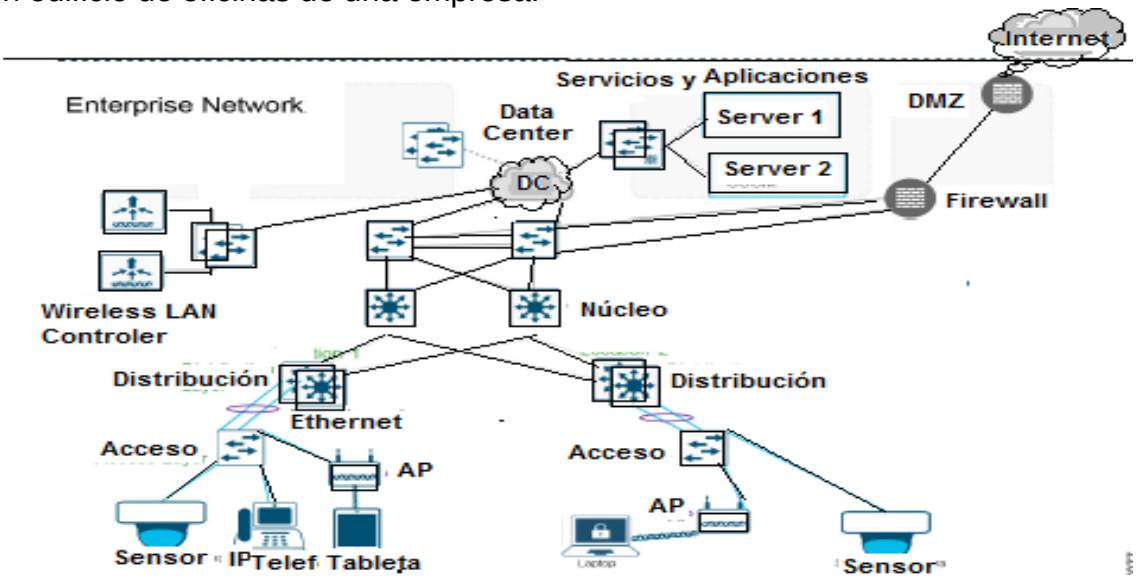


Fig.16.2 Esquema genérico de una Red Empresarial

Una red Empresarial utiliza diferentes tipos de medios de red, los diferentes segmentos de oficinas pueden ser redes Ethernet a 10/100/1000 Mbps y la red troncal que interconecta las diferentes redes y los servidores puede ser una red 1GigabitEthernet o de 10 Gigas, perfectamente.

Las conexiones a las redes externas, dígase Internet pueden ser de forma antigua sobre líneas arrendadas, mediante enlaces Frame Relay, o de forma más moderna mediante enlaces a 10, 40 0 100 Gigas Ethernet sobre WDM.

De forma análoga las conexiones a las oficinas ramales (en otros sitios de una ciudad o en ciudades distantes) pueden ser de la forma anterior o mediante túneles a través de las redes WAN, utilizando Redes Privadas Virtuales (VPN), VPLS, Carrier Ethernet o EVPN.

Luego hay que tener clara la situación de las conexiones de la red Corporativa a sus oficinas ramales e Internet y los tipos de Interfaces de los Enrutadores o Conmutadores que se van a utilizar en la misma.

O sea que una empresa moderna tiene que tener soluciones de comunicaciones empresariales inteligentes que le permitan tener una comunicación con el cliente y a su vez tener sus empleados la información requerida en el momento adecuado a fin de ofrecer un mejor servicio y satisfacción a los clientes.

Otro aspecto de alta importancia en las redes empresariales modernas son los Centros de Datos (Data Center).

Centro de Datos (Data Center)

Un centro de datos es una facilidad utilizada para hospedar sistema de cómputos y sus componentes asociadas, tales como sistemas de telecomunicaciones y sistemas de almacenamiento. El mismo incluye generalmente fuentes de potencia de respaldo redundantes, conexiones de comunicaciones redundantes, control ambiental (por ejemplo aires acondicionados, supresión de incendios, etc.) y dispositivos de seguridad. Los grandes centros de datos son operados a escala industrial, utilizando tanta electricidad como una pequeña ciudad.

El auge de los centros de dato vino durante la aparición de la burbuja de los negocios (.com) en Internet, cuando las compañías necesitaban de una forma rápida la conexión a Internet y operar sin parar. Inicialmente muchas compañías comenzaron construyendo facilidades muy grandes llamadas Centros de Datos de Internet (IDC).

Las nuevas tecnologías y aplicaciones prácticas fueron diseñadas para maniobrar la escala y las exigencias de tales operaciones en gran escala. Migrando hacia los centros de datos privados a diferentes escalas (pequeñas, medias y grandes).

Entre las mayores exigencias para un centro de datos moderno está la continuidad del negocio, por lo que sus sistemas de información y operación no pueden ser dañados ni detenidos de forma completa. Por lo que es necesario ofrecer una infraestructura confiable para las operaciones y una alta seguridad de la información. De ahí que un centro de datos tiene que por consiguiente mantener altos estándares que aseguren la integridad y funcionalidad del ambiente de cómputo hospedado en él. Por lo que esto es llevado a cabo mediante la redundancia de las conexiones de fibra óptica, redundancia de energía, sistemas de respaldo de emergencia, etc.

La asociación de industrias de Telecomunicaciones de USA tiene el estándar TÍA-942 para la infraestructura de los centros de datos, donde se especifican las exigencias mínimas para la infraestructura de telecomunicaciones y datos de un centro de datos. Tanto para un simple inquilino o múltiples inquilinos empresariales.

Hay una tendencia a la modernización de los centros de datos a fin de tomar ventajas en el incremento del desempeño de los mismos y el incremento del ahorro de energía con los nuevos equipos de tecnologías de la información y sus capacidades dado por la virtualización y la computación en la nube. Los proyectos de transformación de los centros de datos incluyen iniciativas de estandarización virtualización, automatización y seguridad.

Nuevos actores en las redes empresariales

Las tecnologías de la información y las comunicaciones (TIC), han estado transitando en este siglo XXI por un proceso de transformación muy importante, que impacta hoy con fuerza a todas las cosas que rodean al hombre.

A partir del 2011 la UIT-T creó grupos de trabajo para enfrentar nuevos retos en el campo de las redes de telecomunicaciones, denominándolas “Redes Futuras”, con vistas al quinquenio 2015-2020. Para esto se han emitido una serie de recomendaciones nuevas enmarcadas por la UIT-T como Redes Futuras en la Serie Y, de la Y.3000 a la Y.3499.

Entre las tecnologías y los objetivos de diseño de las redes futuras están:

- Virtualización de la red (Virtualización de los recursos)
- Redes de Dato/Orientadas a Contenidos (Acceso de Datos)
- Redes de ahorro de energía (Consumo de energía)
- Gestión distribuida de la red dentro del sistema (Gestión de la Red)
- Optimización de la Red (Optimización)
- Redes Móviles distribuidas (Movilidad)

La virtualización es una componente estratégica que acomoda diferentes objetos de la red en un entramado o encuadre simple. En otras palabras la virtualización es un facilitador de diversidad, contribuyendo al desarrollo de redes globales paralelas.
Con la creciente demanda de las tecnologías de Internet y la convergencia de los servicios de voz, datos, video y TV sobre una red de comunicaciones y computadoras, han convertido a las Redes de Área Local (LAN) en una componente crítica en el funcionamiento de cualquier empresa, organismo o institución.
Esta nueva generación de aplicaciones ha posicionado al protocolo IP como el protocolo dominante en el mercado de Redes de pequeño, mediano y gran tamaño, conociéndose como Redes de Nueva Generación o "todo IP".
Los móviles celulares hoy son los dispositivos clave en el acceso ubicuo a diferentes servicios multimedia y de datos en Internet, incluyendo a los servicios de computación en la nube.

El protocolo IPv6
Cada día es mayor la cantidad de aplicaciones que necesitan direcciones IP únicas globales, válidas para conexiones de extremo a extremo y por lo tanto enrutables. Por todas estas razones muchas de las grandes compañías y empresas alrededor del mundo ven la necesidad de que sus redes transiten de forma rápida y efectiva a IPv6 con el objetivo primordial de lograr que cualquier dispositivo IP pueda comunicarse transparentemente con otros dispositivos, independientemente de su localización en la red global,
Todo ello unido a una gran variedad de nuevos servicios y automatización de procesos que tributan a la informatización de la empresa, aportándole mayor eficiencia, competitividad, flexibilidad, confiabilidad y buen desempeño.
Sin embargo, todos estos cambios repercuten directamente en las arquitecturas y diseño de redes, empleadas tradicionalmente por las empresas. La incorporación de los paradigmas antes mencionados incide en varios aspectos, entre los cuales se pueden mencionar los siguientes:

- Aumento significativo de los dispositivos conectados a la red debido a la gran variedad de equipos terminales, la movilidad y las conexiones máquina a máquina o de igual a igual (M2M o P2P), todo esto acelera la necesidad de migrar al protocolo IPv6 ante el agotamiento de direcciones del actual IPv4.
- Cambio en la relación de tráfico y controles de accesos, asociados a la centralización de recursos, la computación en la nube (empresarial o privada) y la necesidad de transmisión y procesamiento de datos a gran escala (Big Data), lo que evidencia el movimiento de los patrones de tráfico a relaciones de 20% del tráfico local y 80% en el troncal o backbone (20/80).
- Surgimiento de nuevas tecnologías más flexibles que se adaptan a la creciente velocidad de los cambios y las demandas de los servicios mediante la virtualización de equipos y servicios.
- Autoservicio bajo demanda a partir de dotar de una mayor independencia al usuario para obtener las capacidades necesarias sin necesidad de una interacción humana con el proveedor del servicio.
- Múltiples formas de acceso a la red, lo que permite que los recursos sean accesibles a través de la red y por medio de una amplia variedad de dispositivos finales.
- Utilización de forma común de los recursos, que facilitan acceso a los recursos de los proveedores; los que son compartidos por múltiples usuarios. Se van asignando capacidades de forma dinámica ignorando el origen de los recursos e incluso compartiendo sus propias capacidades.

Uno de los objetivos de este material es el de facilitar la introducción del protocolo IPv6 en los diferentes entornos de las redes empresariales, motivado por la preocupación de su lenta incorporación en la mayoría de los países en vías de desarrollo.

Diseño de Redes Empresariales

Luego el diseño de las Redes Empresariales ha cambiado y los diseñadores requieren balancear las expectativas de los usuarios con los costos, capacidades, habilidades y niveles de empleo. Por lo que se necesita de un diseño que emplee de forma eficiente los recursos y que efectivamente sirva a los directivos y usuarios.

Cuando se mira el diseño de una red empresarial hay que considerar las tendencias de las redes y las necesidades futuras de una organización.

- La red tiene que estar lista para escalar apropiadamente en el transcurso del tiempo para encontrar las demandas que soporta la organización.
- Las demandas sobre los puntos de acceso inalámbricos (AP) con las últimas tecnologías (802.11ac de segunda generación y 802.11ax), requieren de una actualización del cableado de cobre existente para desplegar plataformas de red con capacidades multi-Gigabit.
- Hay que desplegar nuevos dispositivos con exigencias de alta potencia, tales como alumbrado, conmutadores de acceso remoto, puntos de acceso (AP), teléfonos IP, Sensores y otros dispositivos. Por lo que el diseño debe tener capacidad de soportar potencia sobre Ethernet (PoE con 60W por puerto).
- Internet de las cosas (IoT) impacta hoy en el diseño de redes y el diseño de una red debe soportar tecnologías de video vigilancia y otras tecnologías de virtualización y segmentación de la red que posibiliten escalar y expandir la red.
- El ancho de banda necesita ser potencialmente duplicado en múltiples plazos durante el tiempo de vida de la red de forma tal que la red desplegada hoy necesita estar preparada para añadirle nuevas capacidades de 10 Gbps, 40 Gbps y hasta 100 Gbps en el transcurso del tiempo.
- La plataforma de red desplegada hoy debe ofrecer la mejor longevidad hacia el futuro contra la selección del equipamiento que solo encuentra los límites de las necesidades actuales.
- Para diferentes tamaños y densidades de redes deben converger las plataformas de redes inalámbricas y alambradas a la hora en que la flexibilidad es la mejor forma para fijar las exigencias del despliegue.

Para adherirse a las buenas prácticas de diseño hay que procurar que los principios del diseño de redes tengan las características siguientes:

Modularidad: Los diseños de las redes de campo modulares soportan crecimientos
y cambios mediante el empleo de bloques constructivos, también denominados módulos, lo que permite escalar la red de forma fácil en vez de rediseñar la misma.

Elasticidad: Los diseños de las redes de campo tienen que tener características de alta disponibilidad (HA) y su tiempo de funcionamiento tiene que ser de un 100%. Imaginen una red corporativa de un banco que podría perder millones de pesos por solo interrumpirse un segundo. De ahí que se hable de la capacidad de recuperación de una red en milisegundos.

Flexibilidad: Los cambios en los negocios es una garantía para cualquier empresa, de ahí que se requiera una rápida adaptabilidad y por ende los diseños de las redes corporativas tienen que procurar y facilitar esos cambios.

Todo ello sin olvidar los objetivos técnicos: Escalabilidad, Disponibilidad, Desempeño, Seguridad, Capacidad de gestión, Utilidad o funcionalidad, Adaptabilidad y la relación Costo-Efectividad.

En este material se abordará un enfoque integral donde se tomarán en consideración: las aplicaciones en la red, el tráfico en la red, la topología de la red, la fiabilidad de la red, la seguridad de la red, la gestión de la red y el transporte de datos; antes de la selección de los equipos y medios que operan en los niveles inferiores, siguiendo un proceso de arriba hacia abajo y de forma iterativa.

Las acciones anteriormente relacionadas para el diseño de una red y los pasos que ellas generan son mostradas en la Figura 16.3. El montaje y pruebas, así como la gestión de la red quedan fuera del alcance de este documento.

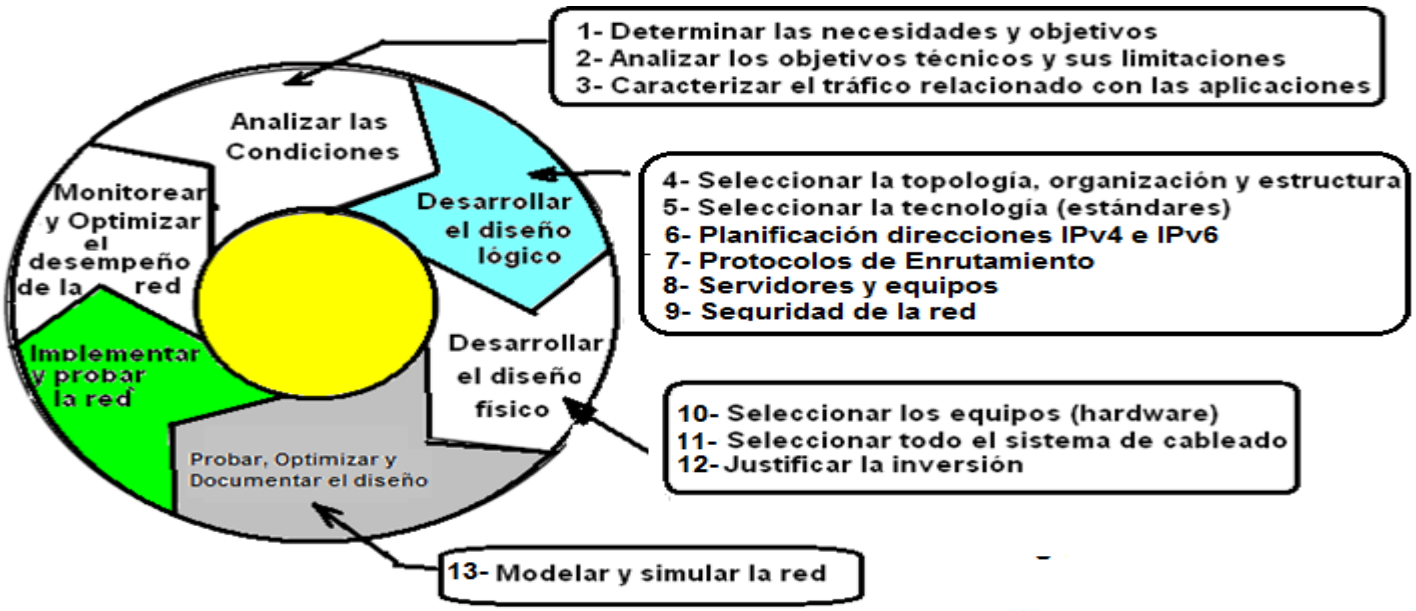


Fig. 16.3 Pasos para el diseño de una Red Empresarial

El diseño de una Red es un proceso profundo, el cual incluye de forma general las acciones que aparecen definidas en la figura anterior:

- **Análisis de las Condiciones**
  Primero hay que determinar bien las necesidades y los objetivos que desean los directivos y usuarios, para poder satisfacer sus expectativas***. Analizar los objetivos técnicos y sus limitaciones***, caracterizar la red o interconexión existente. En especial ***caracterizar el tráfico en la red*** desde un enfoque de las aplicaciones y el transporte de datos que desean, antes de ponerse a pensar en los equipos a emplear. Cantidad de usuarios actuales y futuros, aplicaciones actuales y futuras, etc.

- **Diseño lógico de la red**
  Para ello hay que partir del tipo de red, o sea si es una red para oficinas, edificio o para un campus. Si la misma tendrá una topología en estrella o de anillo, si su jerárquica será de dos o tres niveles, totalmente conmutada o enrutada, etc.
  Hay diferentes variantes dentro del estándar IEEE 802.3 y esto da opciones de ancho de banda (10 Mbps, 100Mbps, 1000 Mbps, 10 Gigas, 100 Gigas, etc.).
  Igualmente hay diferentes variantes dentro del estándar IEEE 802.11 y esto da opciones de anchos de diferentes anchos de banda actualmente del orden de Gigabit (802.11ac y 802.11ax).
  La configuración de redes VLAN para facilitar la gestión de grupos de usuarios es un aspecto de vital importancia en el diseño de redes Empresariales. También la integración de múltiples dominios de rutas, la selección de los protocolos de enrutamiento, la seguridad de la red mediante el filtrado de paquetes para filtrar el ingreso y el control de acceso y las estrategias de gestión entre otros.

- **Diseño Físico de la Red**
  Se requiere seleccionar los dispositivos y equipos de los niveles 1, 2 y 3 para la Red de Área Local (LAN), su acceso mediante las tecnología WLAN y su interconexión con la WAN. El sistema de cableado estructurado que se adoptará depende su actualización con las tecnologías WLAN.

Hay que hacer un análisis económico no solo del costo de los medios y equipos, sino también el costo de instalación y del costo de operación y mantenimiento de la red. En especial como recuperar la inversión.

- **Pruebas y Documentación del diseño**
  Hay varias formas de probar el diseño de una red, pero en el siglo XXI nadie monta una red si antes no la ha modelado y simulado previamente. Estas herramientas permiten analizar el comportamiento o desempeño de la red diseñada, a partir de los patrones de tráfico actuales y futuros, ante la cantidad prevista de usuarios y su futuro crecimiento, los servicios, nuevas aplicaciones. etc.
  La documentación debe ser tanto de todas las conexiones físicas, como de las conexiones lógicas, software instalado, políticas de seguridad (incluidas medidas de contingencia), etc.
  Este paso es muy importante, pues del mismo dependerán las acciones futuras de mantenimiento y operación.

El diseño de las Redes Empresariales permanece con fines específicos dados por los fabricantes y pobre comprensión, dado por la diversidad de escenarios y complejidades de las mismas. De ahí que en este material se hayan recopilado diferentes trabajos relacionados con esta temática, referidos en la bibliografía y en especial las estrategias de transición indicadas en las RFC (4057, 4554, 4582, 5375, 7381 y 8160).
Dándose prioridad a los escenarios de Redes Empresariales IPv4 con transición a IPv6 y escenarios con IPv6 (IPv6 Enterprise Network Scenarios) dada la necesidad de actualización de las redes empresariales y su pase definitivo a Redes IP V6 con todas sus aplicaciones y servicios.

A continuación se van a desglosar los pasos a seguir en el diseño de Redes Empresariales, los cuáles están muy relacionados con las redes LAN de campo, pero con aplicaciones y servicios de Intranet y Extranet.

Pasos para el diseño de una Red Empresarial

a)Condiciones generales

Esta primera acción es la que permite conocer cuáles son las condiciones, necesidades, objetivos y aplicaciones para enfrentar el diseño de la red. La misma consta de tres pasos:

Primer Paso: Análisis de las necesidades y objetivos

Es importante definir el alcance de la red LAN que se va a diseñar, pues no es lo mismo un segmento, que una red de un edificio, de un campo o una red empresarial (Enterprise network).

- **Segmento de red** – Si es una simple red LAN basada en protocolos de nivel 2.
- **Red LAN** - Formada por un conjunto de segmentos conmutados, basados en un protocolo de nivel 2, donde puede tener uno o m{as protocolos de nivel 3 asociados.
- **Red LAN de edificio** – Donde un conjunto de redes LAN están distribuidas dentro de un edificio e interconectadas por una red troncal de edificio.
- **Red LAN de Campo**- Múltiples redes de edificios distribuidos en un área geográfica interconectadas por una red troncal de campo.
- **Redes Empresariales – Una mezcla de redes LAN de campo, servicios de acceso remoto y servicios de Intranet e Internet.**

No es lo mismo una Red de Área Local (LAN) para las oficinas de una pequeña empresa comercial con pocas oficinas (SOHO), que para un hospital, un hotel, una universidad, un aeropuerto, o un salón de convenciones, etc. Cada instalación tiene sus necesidades propias, diferentes aplicaciones, diferencias en la exigencia en cuanto a calidad del servicio, diferencias en la cantidad de usuarios, etc.

Para ello hay que hacer un análisis de las necesidades de los directivos y usuarios, conocer qué objetivos persiguen desde el punto de vista de los negocios, tecnológicos y administrativos.
O sea que es importante determinar qué objetivos se persiguen:

- Mejorar las comunicaciones
- modernizar las tecnologías
- reducir costos de operación
- expandir los servicios
- mejorar la seguridad
- confiabilidad,
- ofrecer nuevos servicios

Hacer un examen de lo existente, permitirá obtener un "retrato" bastante preciso acerca de la estructura de la organización, las funciones de los departamentos, métodos empleados, etc.
Un análisis de lo instalado y de las necesidades, permitirá, a partir de las informaciones recogidas, encontrar la naturaleza y características de ellas.
Para ello hay que determinar que aplicaciones tienen implementadas, que sistemas operativos utilizan, la localización de los usuarios, los equipos de que disponen (hardware) , los software instalados y otros datos de interés.
Aplicaciones: Conocer si tienen o requieren de las más típicas, como son servicios de correo electrónico (e-mail), navegación en Internet, transferencia de ficheros (FTP), acceso a bases de datos (SQL), ficheros compartidos, trabajo en grupos de usuarios, etc. O si requieren de aplicaciones más modernas como: videoconferencias, Telefonía IP (VoIP), comercio electrónico, diseño electrónico, video vigilancia, Televisión, etc.
Sistemas: también es necesario conocer que aplicaciones tienen los diferentes sistemas, tales como autenticación de usuarios, nombres de las estaciones, si emplean configuración remota, servicios de directorio, sistemas de respaldo de la información (backup), herramientas de administración de la red, software distribuidos, etc.
Usuarios: cantidad, localización física (ubicación por áreas, Departamentos, pisos etc.), descripción del trabajo (ejemplo una facultad en laboratorios docentes, investigación etc.) ,requerimientos y crecimiento esperado (futuro).
Hardware: tipo de estaciones (PC) o laptop, capacidad de memoria si tienen o no facilidades de conexión en red (tipo de tarjetas de interfaz, NIC), número de ranuras de expansión disponibles, puertos USB, etc.
Software: Sistemas operativos, programas de aplicación y sobre las herramientas de software empleadas, en especial si son versiones para el trabajo en Red a fin de conocer los flujos del tráfico.
Otros datos: sistemas de cableado si existieran, Impresoras, Gráficadoras, Digitalizadores, Fax , Modems (o tarjetas de modems), otros periféricos , fuentes de suministro para respaldo, sistemas de almacenamiento, etc.
Las demandas de los usuarios: de tiempo, interacción, fiabilidad, calidad, adaptabilidad, seguridad, costos, cantidad, localización y crecimiento esperado están muy interrelacionadas con las demandas de buen desempeño del servicio dados por: retardos (tiempos de tránsito), fiabilidad y capacidad.

Algunos autores recomiendan que se utilice una lista de tareas para determinar si se ha dirigido bien a sus clientes en función de los objetivos que le competen.
Si Usted no puede acopiar todas las partes mencionadas en la lista, es necesario que refleje en algún documento lo que le falte en caso que se convierta en un aspecto crítico, pero no detenga el proyecto esperando a tener todos los detalles.
O sea que la metodología funciona si algún dato falta después de su análisis y para ello debe preguntarse:

1- Conoce ya bien a los clientes, las firmas y la competencia.
2- Entiende bien la estructura corporativa de los clientes.
3- Domina los objetivos de negocios de los clientes, iniciando con un objetivo general que explique el propósito primario del proyecto de diseño de la red.
4- Conoce si el cliente tiene identificadas las operaciones indispensables
5- Entiende los criterios de los clientes para los éxitos y consecuencias de los fallos.
6- Entiende el alcance del proyecto de diseño de la red
7- Tiene identificadas las aplicaciones de los usuarios de la red.
8- Conoce si el cliente tiene políticas claras con respecto a vendedores aprobados, protocolos y plataformas.
9- Conoce si el cliente tiene políticas claras con respecto a soluciones propietarias o abiertas.
10- Conoce si el cliente tiene cualquier política con respecto a distribuir la autoridad para el diseño de la red y su implementación.
11- Si el cliente conoce el costo del proyecto.
12- Si el cliente conoce el cronograma del proyecto, incluida la fecha final como hecho memorable.
13- Tener un buen entendimiento de la experiencia técnica de los clientes y cualquier aspecto interno o externo del cuerpo administrativo.
14- Tener discutido un plan de educación para el cuerpo administrativo del cliente.
15- Estar claro de cualquier política oficial que podría afectar el diseño de la red.

En esta etapa o paso, la tarea de mayor importancia estriba en entender al usuario, encontrar los medios que disponen o quieren tener. En especial que servicios y aplicaciones quieren implementar, tal como se muestra en la Figura 16.5.

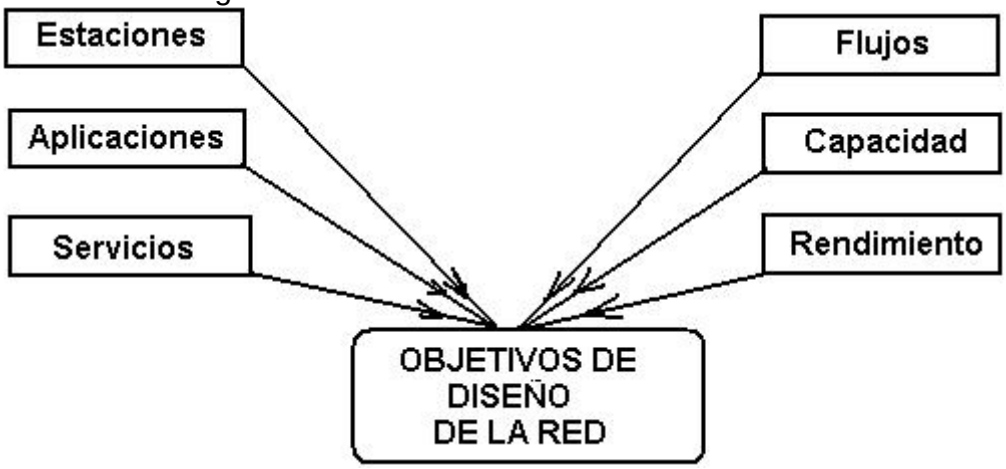


Fig. 16.5 Exigencias relacionadas con los objetivos de diseño.

Si el cliente ya dispone de una red y lo que desea es su actualización (up date), entonces es necesario analizar las aplicaciones existentes y la carga de la red.

<u>Segundo Paso</u>: Análisis de los objetivos técnicos
Es importante analizar los objetivos técnicos dado que los mismos permitirán determinar las tecnologías a emplear.
Entre los objetivos técnicos de una red están**:**
Escalabilidad, Disponibilidad (Availability), Desempeño (Performance), Seguridad, Capacidad de gestión, Utilidad o funcionalidad, Adaptabilidad y la Afordabilidad (Costo-Efectividad).
A continuación se profundizará en cada uno de ellos, dada su importancia.

Escalabilidad: La misma se refiere a cuanto es que crecerá la red y el diseño tiene que soportarlo. En el diseño de redes empresariales este es uno de los aspectos técnicos mas importantes. En especial conocer cuántos usuarios y aplicaciones se añadirán en los próximos años, dígase cuantas redes LAN se conectarán a la red de la empresa o dependencia. Si se resolverán los cuellos de botella de la conexión de la LAN con la WAN. También es necesario conocer si se incorporarán en el futuro nuevos servidores centrales, etc.
Por lo que es necesario conocer:

- ✓ ¿Cuántas posiciones serán añadidas en el próximo año o en los dos próximos años?
- ✓ ¿Cuán extensa será la red para llegar a esas posiciones?
- ✓ ¿Cuántos usuarios accederán a los servicios de la intranet en el próximo año?
- ✓ ¿Cuántos servidores serán añadidos a la red en el próximo año?.

Disponibilidad**:** Para asegurar la continuidad y evitar fallos catastróficos en la red, es importante identificar las áreas de fallos y disponer de planes de recuperación rápidos para minimizar los impactos en las aplicaciones durante las pausas o parada de la red. Generalmente hay tres tipos de métodos que ayudan a la supervivencia de la red:

- Resiliencia o elasticidad de los enlaces, ofreciendo redundancia ante fallas en los enlaces físicos. Por ejemplo corte de la fibra óptica, deficiencias en los transmisores o receptores, cableado incorrecto, etc.
- Resiliencia en los dispositivos
- Resiliencia operacional, de forma que ofrece una alta disponibilidad de la red como tal.

Este objetivo técnico se refiere a la cantidad de tiempo que la red está disponible para los usuarios y es a menudo un objetivo crítico en el diseño de la red.
La disponibilidad puede ser expresada en porciento de actividad por año, por mes, por semana o por horas comparado con el período total de tiempo. Por ejemplo si es una red que da servicios los 7 días de la semana , 24 horas y la misma solo está disponible 165 de las 168 horas de la semana, esto indica una disponibilidad de un 98.21%.
Por lo que es necesario exhortar a los usuarios que especifiquen las necesidades de disponibilidad con precisión.
Considere la diferencia entre un 99.70 % y 99.95% de actividad de una red, en el primero significa que la red estará fuera de servicio 30 minutos por semana, lo cuál puede ser inaceptables para muchos usuarios. Mientras que una actividad de 99.95% significa que solo la red estará fuera de servicio 5 minutos por semana.
En general el objetivo de disponibilidad significa mantener corriendo las aplicaciones de misión crítica y el tiempo fuera de actividad representa un costo. De ahí que se relacione la disponibilidad con un costo de pérdidas por estar fuera de actividad.

Además de expresar la disponibilidad en un porciento de actividad, la misma se puede expresar en forma de tiempo promedio entre fallos (MTBF) y en tiempo promedio para la reparación (MTTR).
Es necesario conocer el tiempo promedio entre fallos en la red (MTBF) que se quiere garantizar, y el tiempo promedio para la reparación de fallos (MTTR). Para tener una idea de una buena red, considere que el tiempo promedio entre fallos es de 4000 horas (166 días) y que en una hora se reparan los fallos, lo que da una disponibilidad de la red de un 99.98%.
Cuando se expresa la disponibilidad en función del tiempo promedio entre fallos (MTBF) y el tiempo promedio para la reparación de fallos (MTTR) se tiene la ecuación:

$$\text{Disponibilidad} = MTBF / (MTBF+MTTR)$$

Costo- Efectividad (Affordability)

Muchos usuarios toman en muchas ocasiones este objetivo por encima del desempeño y de la disponibilidad.
Para que un diseño de red sea costeable o asequible, el mismo debe transportar la mayor cantidad de tráfico para un determinado costo. Este costo financiero incluye el costo de los equipos y además los costos de instalación, operación y mantenimiento de la red.
En muchas ocasiones los usuarios quieren conmutadores (Switch) que tengan muchos puertos y que sea bajo el costo por puertos. Por otro lado buscan que el costo del cableado sea mínimo y que el proveedor de servicios los ofrezca baratos.
Por otro lado quieren que las tarjetas de interfaz (NIC) y los servidores sean baratos.
En dependencia de las aplicaciones que estén corriendo sobre los sistemas finales, el bajo costo es más importante para los usuarios que la disponibilidad y el desempeño en el diseño de una red de campo. Y esto tiene sus peligros, por lo que hay que tener mucho cuidado.
.
Desempeño**:** Muchos usuarios no pueden identificar como se desempeña su red, por lo que el ingeniero tiene que hacer sus consideraciones propias en cuanto a *parámetros que miden el desempeño tales como: capacidad o ancho de banda, utilización, razón de transferencia (throughput), carga, tráfico útil, eficiencia, retardos, variaciones del retardo y tiempo de respuesta.* Todos estos parámetros los analizará con la ayuda de herramientas de modelación y simulación, así como con mediciones.
El desempeño de una red permite conocer cuán bien ella está trabajando y es un asunto complejo con muchas variables e inconfundiblemente una tarea que no es trivial. Son varios los factores que impactan el buen desempeño o rendimiento de una red.
Luego la clave para el diseño de redes de alto desempeño está en la habilidad de modelar y estimar los parámetros o métricas que miden el desempeño. El ingeniero necesita ser capaz de determinar el volumen de tráfico futuro y sus características sobre la base del tráfico observado.

Tercer Paso: Caracterización del Tráfico relacionado con las aplicaciones
Hay que conocer el comportamiento de la aplicación en cuanto al tamaño de los datos, duración del tránsito por la red de los mismos y características de los flujos, aspectos estos que serán profundizados en la etapa siguiente.

En una red hay diferentes tipos de flujos de información dados por las aplicaciones y protocolos con atributos comunes tales como: origen y destino de los datos, tipo de información, tipo de encaminamiento etc. Tal como se muestra en la Figura 16.6

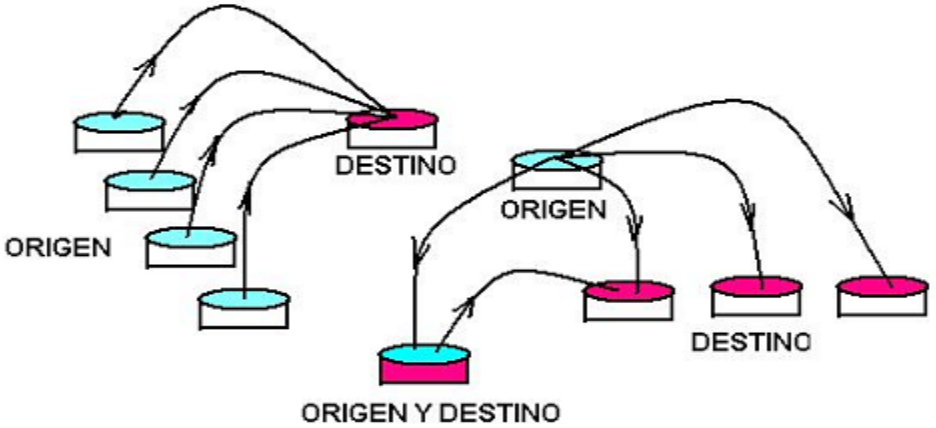


Fig. 16.6 Orígenes y destinos de los flujos de tráfico en la red

Hay diferentes tipos de modelos de flujos:

- De igual a igual (Peer to Peer)

- Cliente – Servidor
- Cooperativos
- Distribuidos.

El modelo de Flujo conocido como Cliente –Servidor se mantiene entre los más empleados por las aplicaciones aún hoy en día y el mismo se muestra en la Figura 16.7.

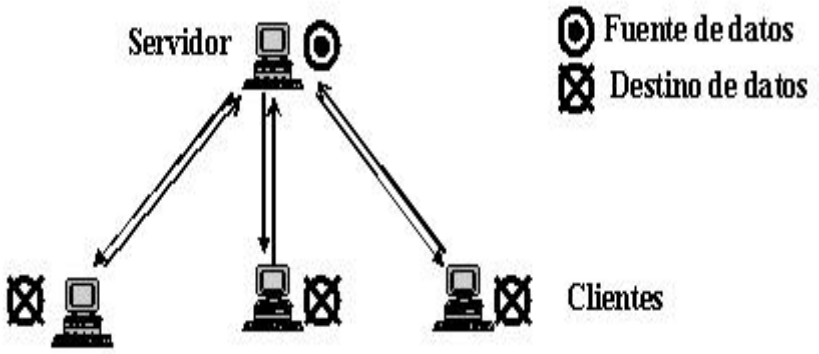


Fig. 16.7. Modelo de Flujo Cliente- Servidor.

Como característica principal del mismo está que es un flujo asimétrico, dado porque hay más tráfico hacia el cliente. Las peticiones de los clientes son pequeñas en tamaño, los clientes son destino de los datos, las respuestas del servidor son de gran tamaño hacia los clientes y el servidor normalmente es fuente de datos.

Entre las aplicaciones y servicios de redes más típicos están:

- Correo Eléctrónico (Email)
- Transferencia de ficheros, compartir ficheros y acceso a ficheros (File transfer, sharing, and access)
- Acceso a Bases de datos y actualización (Database access and updating)
- Navegación Web (Web browsing)
- Recreación en la red (Network game)
- Terminal Remoto (Remote terminal)
- Calendario (Calendar)
- Imágenes Médicas (Medical imaging)
- Videoconferencias (Videoconferencing)
- Video en demanda (Video on demand (VoD))
- Video de Multdifusión programado (Scheduled multicast video)
- Video Vigilancia y Seguridad (Surveillance and security camera video)
- Telefonía IP en la Intranet o por Internet (Internet or intranet voice (IP telephony))
- Facsímil por Internet o Intranet (Internet or intranet fax)
- Admisión de órdenes de ventas (Sales order entry)
- Reportes de gestión (Management reporting)
- Rastreo de ventas (Sales tracking)
- Diseño ayudado por la Computadora (Computer-aided design)
- Control de inventario y de embarques (nventory control and shipping)
- Telemetría (Telemetry)
- Respuesta de voz interactive (Interactive Voice Response (IVR))
- Ediciones Web (Web publishing)
- Pizarras electrónicas (Electronic whiteboard)
- Emulación de Terminal (Terminal emulation)
- Directorio telefónico en línea (Online directory (phone book))

La adopción de la tecnología IP ha conducido a cambios fundamentales en el diseño de redes, extendiendo nuevas aplicaciones y servicios de redes más novedosos y necesarios, tales como:

- Telefonía IP
- IP TV
- Video Vigilancia IP

También hay que tener en consideración las aplicaciones de los sistemas que incluyen los servicios de red:

- Autorización y Autentificación de usuarios (User authentication and authorization)
- Determinación de nombres de Dominio (Host naming and name resolution)
- Configuración dinámicas de estaciones (Dynamic host addressing)
- Carga Remota (Remote booting)
- Configuración Remota (Remote configuration download)
- Servicios de directorios (Directory services)
- Respaldo de red (Network backup)
- Gestión de Red (Network management)
- Distribución de Software (Software distribution)

Por lo que se recomienda hacer una tabla de aplicaciones con su nombre, tipo de aplicación, si es nueva en la red que se desea o ya existe, si la misma es considerada extremadamente crítica , un poco crítica o no crítica, así como las observaciones que se deseen realizar.

Luego hay que tipificar las aplicaciones y determinar si son:

- ✓ críticas del negocio (extremadamente, un poco, etc.)
- ✓ de capacidad específica
- ✓ o de tiempos de tránsito específicos.

Por lo que se hace necesario estimar los peores casos de tráfico durante los momentos más utilizados por los usuarios y durante los servicios de red organizados regularmente. También es importante conocer qué % de flujo es local y qué % es remoto (acceso a la intranet, acceso a Internet, etc.).

Subdivisiones administrativas

El uso de subredes está relacionado con la necesidad de contar con subdivisiones administrativas para abordar cuestiones de tamaño y control. Cuantos más estaciones (hosts) y servidores hay en una red, más compleja será la tarea de administración. Al crear divisiones administrativas y utilizar subredes, la gestión de una red compleja resulta más fácil.

La decisión de configurar subdivisiones administrativas para su red la determinan los factores siguientes:

- Tamaño de la red

Las subredes también son útiles incluso en una red relativamente pequeña cuyas subdivisiones están ubicadas a lo largo de una amplia área geográfica.

- Necesidades comunes compartidas por grupos de usuarios

Por ejemplo, posiblemente tenga una red que esté limitada a un único edificio y que admita un número relativamente pequeño de máquinas. Estos equipos se reparten en una serie de subredes. Cada subred admite grupos de usuarios con diferentes necesidades. En este ejemplo, puede utilizar una subdivisión administrativa para cada subred

Luego tomando en consideración los elementos anteriores es necesario pensar acerca de los usuarios como grupos colectivos basados en el papel de cada usuario en la organización (directivos, empleados, técnicos, clientes, etc.) a fin de conocer que recursos ellos deben compartir dentro de la empresa.

Hoy la forma más común de agrupar a los usuarios es mediante redes LAN Virtuales (VLAN), pues ellas permiten tomar un grupo de usuarios que estén localizados físicamente en lugares diferentes y conectados a diferentes conmutadores y agruparlos en una simple subred lógica.
Por ejemplo el caso típico de permitir el acceso a Internet solo del personal directivo y técnico en una empresa. Esto facilita que tanto las políticas de enrutamiento como de filtrado de paquetes sea aplicada a una misma subred lógica.
Cada red VLAN constituye un dominio de difusión separado, de ahí que es importante lograr en el análisis de tráfico que cada enlace sea configurado para permitir solo el tráfico apropiado para las VLAN.
Otro aspecto es el de la ubicación de los Enrutadores que van a funcionar como Puente raíz del árbol de expansión de la VLAN, pues hay que delimitar el número de enlaces que ven el tráfico de difusión (broadcast) de las VLAN. Por lo que es importante colocar el Puente Raíz (Root Bridge) para reducir el tráfico de difusión en la red y reducir las ineficiencias en la comunicación.
Por lo que a partir de lo anteriormente expresado hay que decidir sobre el número de redes VLAN, la mejor ubicación de los Enrutadores en el Puente Raíz del árbol de expansión y las políticas de filtrado.

Diseño lógico de la Red
En esta acción están varios pasos que definirán la futura red, de ahí su importancia.

Cuarto Paso: Seleccionar la topología, organización y estructura de la red
Para ello se deben hacer comparaciones a fin de evaluar el tipo de LAN a seleccionar en cuanto a los objetivos técnicos antes mencionados: escalabilidad, disponibilidad, desempeño, seguridad, etc. Y como es lógico irá valorando los costos.
El modelo jerárquico de tres niveles ha sido el método típico empleado para conseguir buen desempeño, alta disponibilidad y escalabilidad en el diseño de redes LAN. Este modelo de diseño emplea cuatro principios claves de diseño: jerarquía, modularidad, facilidad de recuperación ante fallos (resiliency) y flexibilidad. En la Figura 16.8 se muestra la distribución del mismo en los niveles de Acceso, Distribución y Núcleo (Core).

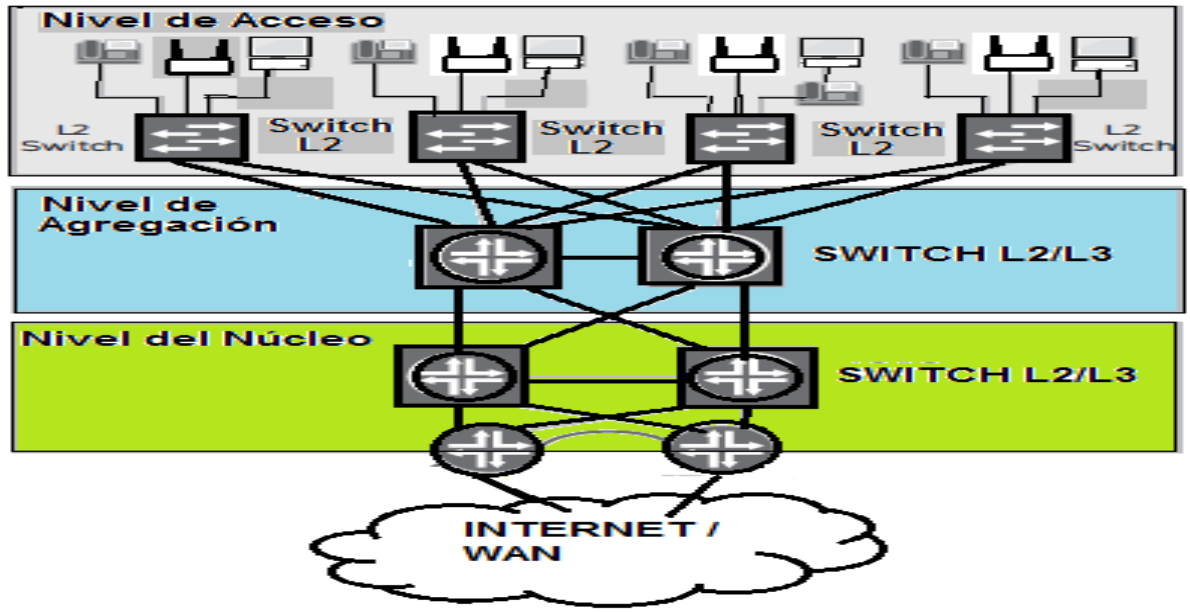


Fig. 16.8 Modelo Jerárquico de tres niveles de red LAN
Cada nivel en este modelo jerárquico tiene un papel único a desempeñar:

- Nivel de Acceso – Su función primaria es la de ofrecer acceso alambrado e inalámbrico a los usuarios finales de la red. Por lo general este nivel se ejecutan funciones de capa 2 del modelo OSI, interconectando mediante puentes o conmutadores de capa 2 a grupos de usuarios, aplicaciones y otros puntos finales. Este nivel de acceso se interconecta con el nivel de distribución.
- Nivel de Distribución – En un sistema de múltiples propósitos sirve de interconexión entre el nivel de Acceso y el nivel de Núcleo. Entre sus funciones están: Sumar y terminar los dominios de difusión (broadcast) de capa 2, ofrecer conmutación, enrutamiento y políticas de acceso a la red en función del acceso del resto de la red. También en este nivel hay redundancia en la distribución mediante Conmutadores que ofrecen alta disponibilidad a los usuarios finales con costo igual de trayectorias al núcleo. También este nivel puede suministrar servicios diferenciados de varias Clases de Servicio (CoS) a las aplicaciones a nivel de red.
- Nivel de Núcleo o Troncal – Este nivel permite alta velocidad, escalabilidad, confiabilidad y conectividad de baja latencia. Este nivel permite añadir varios conmutadores de distribución que pueden estar en diferentes edificios. Los Enrutadores de núcleo troncales son un punto de concentración que ofrece el tránsito para acceder la red interna y externa.

El nivel de acceso ofrece el tránsito hacia las otras redes, tiene funciones inteligentes de Potencia sobre Ethernet (PoE), se conforman las redes VLAN, selección de los Puentes de Proveedores (PB, IEEE 802.1AD), Movilidad, Auto QoS, etc. Además tiene que tomar decisiones de conducción de Capa 2 y Capa 3, unido a servicios de seguridad de puertos bajo el estándar IEEE 802.1X, filtrado de paquetes mediante Listas de control de Acceso (ACL), etc. Así como calidad de servicio mediante clasificación, marcado y colas.

Mientras que el nivel de distribución ofrece el tránsito entre la red interna y externa, ofrece optimización de Rutas, virtualización del sistema y de la red y además la interconexión a Nivel o Capa 2. Además tiene que tomar decisiones de conducción de Capa 2 y Capa 3, unido a servicios de seguridad de puertos, inspección de ARP dinámica, seguridad contra espionaje DHCP, ACL o Filtrado de Rutas, etc. Así como calidad de servicio mediante clasificación, marcado y colas.

En el núcleo (core) se repiten las funciones enumeradas para el nivel de Distribución, con solo añadir que las decisiones de conducción se realizan a nivel de Capa 3.

A continuación se muestra en la Figura 16.9 un ejemplo del diagrama de conexiones lógico de una red empresarial con una estructura jerárquica conformada por la red de Acceso, red de Distribución y red del Núcleo o troncal. En ella se aprecian otros elementos importantes como son: la zona segura (DMZ), el Borde o Frontera con la red externa (Internet), El Centro de Datos (Data Center) y el Centro de Gestión de la Red (CGR).

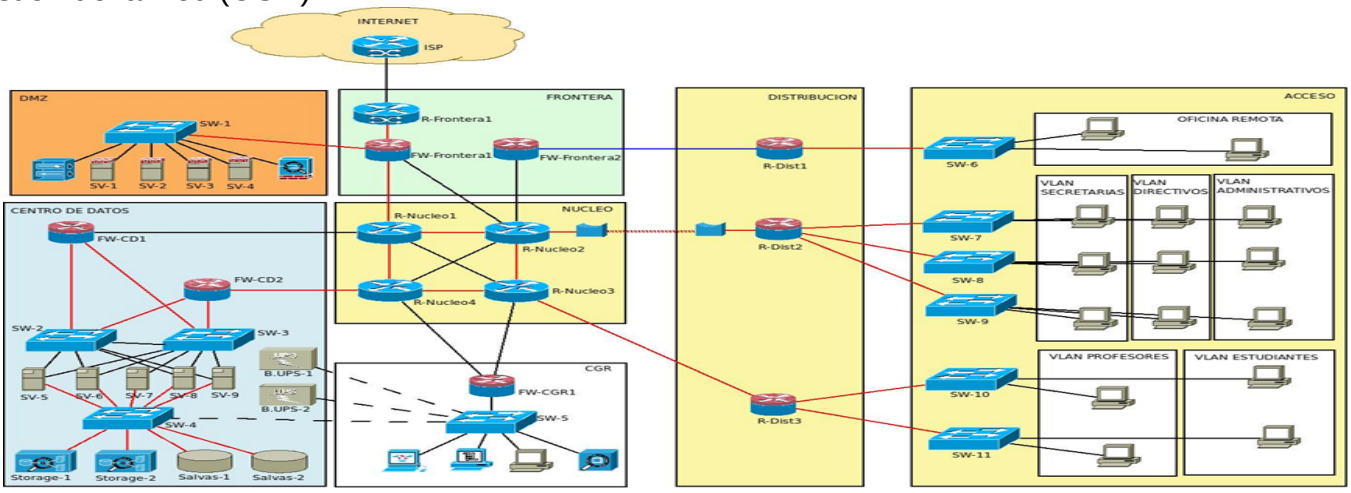


Fig. 16.9 Estructura jerárquica de una red empresarial de campus.

En la Figura 16.9 también se puede apreciar en la parte de acceso las redes VLAN, mientras que en la red troncal se puede apreciar la Redundancia de los enlaces entre los Enrutadores que conforman el núcleo.
Hay que destacar que en muchos casos de pequeñas empresas se utiliza el modelo jerárquico de dos niveles, donde la jerarquía de Núcleo y Distribución son unidas en una sola y se le denomina Diseño de Red Troncal Desplomado (Collapsed Core Network Design). Esto tiene el objetivo primario de reducir costos, pues mantiene la mayoría de los beneficios del modelo de tres niveles.
En estas redes troncales las funciones del nivel de núcleo y de distribución pueden ser implementadas en un simple dispositivo, pero esto no es recomendado. Aunque sea más complejo es mejor utilizar dos dispositivos con enlaces redundantes a fin de alcanzar alta fiabilidad y desempeño. En la Figura 16.10 se muestra el modelo jerárquico de una red troncal desplomada con redundancia.

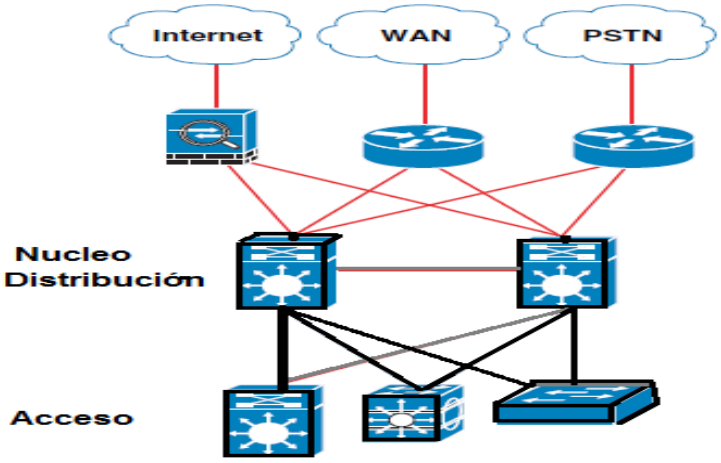


Fig. 16.10 Modelo Jerárquico de dos niveles

A continuación, se presentan algunas de las decisiones de planificación que debe tomar relacionadas con el hardware:

- ✓ La topología de red, el diseño y las conexiones del hardware de red
- ✓ El tipo y número de sistemas host que admite la red, incluidos los servidores que pueden ser necesarios
- ✓ Los dispositivos de red que se instalarán en estos sistemas
- ✓ El tipo de medios de red que se utilizarán, como Ethernet, etc.
- ✓ Si necesita conmutadores de capa 3 o enrutadores que extiendan este medio o conecten la red local a redes externas
- ✓ Grupos de usuarios con diferentes necesidades lo que determina la cantidad de subredes

Una vez definidos los aspectos anteriores se debe pasar a dibujar el esquema lógico de la Red LAN. También se debe elaborar una lista preliminar del equipamiento y dispositivos (hardware) necesarios para la red: tipos de cables, tarjetas de interfaz a la red (NIC), tipos de Conectores, armarios o racks, repetidores, transceptores (transceivers), conmutadores de capa 2 o capa 3,

<u>Quinto Paso:</u> Seleccionar la tecnología
Hay diferentes variantes dentro del estándar IEEE 802.3 y esto da opciones de ancho de banda (10 Mbps, 100Mbps, 1000 Mbps, 10 Gigas, 100 Gigas, etc.).
La redes LAN que se han impuesto en el mercado por su buena relación costo-desempeño son las conocidas como Ethernet o estándar IEEE 802.3 (Ethernet, FastEthernet, GigabiEthernet, 10 Gigas, etc.)

Luego realice una selección del tipo de Red Ethernet / IEEE 802.3 que usted recomienda para la LAN de la dependencia y justifique su selección, comparándola con otras en cuanto a topología, costo-desempeño, ancho de banda, etc.
Igualmente realice la selección del tipo de red WLAN/IEEE 802.11 que se recomienda y justifique su selección, comparándola con otras en cuanto a infraestructura (Controladores y Puntos de Acceso).
O sea que la red o estructura de interconexión debe satisfacer la carga de tráfico previamente calculada para la cantidad de usuarios y aplicaciones.
Elabore una propuesta de ancho de banda (Mbps) requerido para la Red tomando en consideración la carga de tráfico de la red en dependencia de las aplicaciones, servidores, cantidad de usuarios, interacción típica y frecuencia de interacciones por usuario.

Sexto Paso: Planificación de las direcciones IPv4 e IPv6 de la red Empresarial
Al planificar el esquema de direcciones de la red, debe tener en cuenta los siguientes factores:

- ✓ El tipo de dirección IP que desea utilizar: IPv4 o IPv6
- ✓ El número de sistemas potenciales de la red
- ✓ El número de sistemas que son enrutadores o sistemas de host múltiple, que requieren varias tarjetas de interfaz de red (NIC) con sus propias direcciones IP individuales
- ✓ Si se utilizarán direcciones privadas en la red
- ✓ Si habrá un servidor DHCP que administre las agrupaciones de direcciones IPv4

Brevemente, los tipos de direcciones IP incluyen los siguientes:
Direcciones IPv4, diseñar un esquema de direcciones IPv4 CIDR
Direcciones DHCP: Los servidores DHCP cuentan con agrupaciones de direcciones IP desde las que se asignan direcciones a los clientes DHCP. Un sitio que utilice DHCP puede utilizar una agrupación de direcciones IP menor que la que se necesitaría si todos los clientes tuvieran asignada una dirección IP permanente. Puede configurar el servicio DHCP para administrar las direcciones IP del sitio, o parte de ellas.
Direcciones IPv6: Al igual que con las direcciones IPv4 en formato CIDR, las direcciones IPv6 no tienen clase y utilizan prefijos para designar la parte de la dirección que define la red del sitio.
Direcciones privadas y prefijos de documentación: La IANA ha reservado un bloque de direcciones IPv4 y un prefijo de sitio IPv6 para utilizar en redes privadas. Las direcciones privadas se utilizan para tráfico de red dentro de una red privada. Estas direcciones también se utilizan en la documentación.

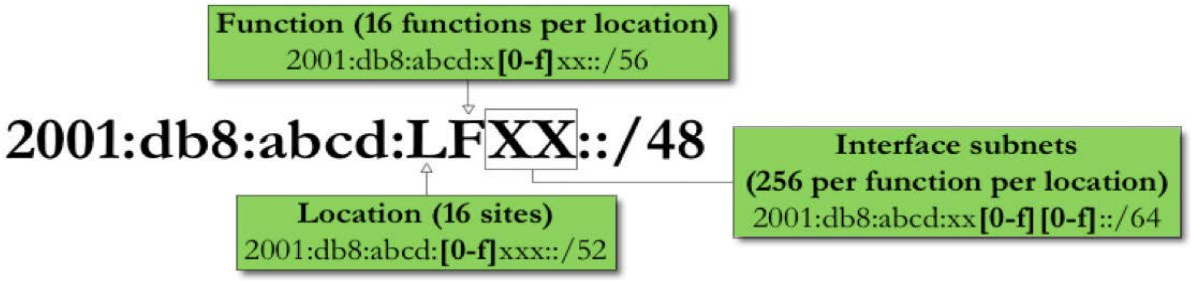
O sea que hay que asignar las direcciones IP a la red Corporativa, en este caso para el escenario que se ha designado de forma hipotética. Para ello hay que seleccionar direcciones IPv4 de redes Privadas, donde se tome en consideración el crecimiento futuro de la red (nuevas subredes y nuevos usuarios). Hay que evitar el desperdicio de direcciones IPv4 y para ello se deben utilizar máscaras de subredes de longitud variable (VLSM). En esto hay que tener en consideración los protocolos de Enrutamiento que permiten trabajar con este tipo de máscaras de subredes de longitud variable.
En cuanto a las direcciones IPv6 hay que tomar en cuenta lo expresado en la RFC4057 y en la más actual RFC 7381 (Enterprise IPv6 Deployment Guidelines).
Hay diferentes métodos para la asignación o planificación de las direcciones IPv6:

- Método de asignación Mejor-Adecuado (Best-Fit Method)
- Método de asignación esparcido (Sparse Allocation Method)
- Método de asignación aleatoria (Random Allocation)

Sin embargo otros autores los clasifican de otra forma como:

- Método basado en las direcciones IPv4 existentes y traducirlas a IPv6 (IPv4 mapped IPv6)
- Método basado en la topología de la red
- Método basado en la organización
- Método basado en servicios

El método basado en la topología de la red asigna un bloque de direcciones para todas las localizaciones dentro de los límites de la red. Por ejemplo una empresa que le ha sido asignada el prefijo 2001:db8:abcd::/48 por su proveedor y tiene diferentes sitios a través de un país, tal que la topología es dividida en 8 regiones. Por lo que se podría seleccionar los primeros 4 Bits de los 16 disponibles para subredes para identificar las regiones. Con este esquema la red podría tener 16 regiones y cada región podría tener a su vez 4096 subredes (2 EXP 12).
El método basado en la organización es raramente utilizado, dado que el mimo no promueve un esquema de agregación eficiente.
El método basado en servicios o funciones permite asignar prefijos en base al tipo de servicio que es ofrecido. Por ejemplo servicios de Voz sobre IP (VoIP), servicios de redes inalámbricas (WLAN), etc.
En muchas ocasiones se mezclan los métodos de asignación de direcciones IPv6, tal como se muestra a continuación:



En IPv6 también hay que tener en consideración la asignación de direcciones de las subredes IPv6 relacionadas con los números de las VLAN
Esto es principalmente en redes donde hay muchas subredes VLAN y ello facilita la simplificación de la administración.
Los números de las VLAN emplean 12 Bit (o – 4096), mientras que los números de las subredes emplean 16 Bits (considerando un prefijo de /48 para la organización).

Por lo que se pudieran utilizar los acercamientos siguientes a modo de ejemplo:

2001:db8:1234: V V V V V V V V V V V V B B B B ::/ 64
2001:db8:1234: B B B B V V V V V V V V V V V V ::/ 64

Sin embargo las direcciones IPv6 son escritas en notación hexadecimal, pero los números de las VLAN son escritas en decimal. Tal que la aproximación anterior requiere de una conversión entre hexadecimal y decimal, lo que oscurece la relación y niega la ventaja de simplificación.

Por lo que una aproximación preferible es tomar el número decimal de la VLAN y utilizar este en el lugar del número hexadecimal de la subred.
Por ejemplo la VLAN 2783 simplemente se convierte en la subred 2001:db8:1234:2783::/64
A continuación se muestra una tabla con diferentes opciones:

VLAN ID	IPv6 decimal	IPv6 hexadecimal (high)	IPv6 hexadecimal (low)
1	2001:db8:1234:0001::/64	2001:db8:1234:0010::/64	2001:db8:1234:0001::/64
12	2001:db8:1234:0012::/64	2001:db8:1234:00c0::/64	2001:db8:1234:000c::/64
2783	2001:db8:1234:2783::/64	2001:db8:1234:adf0::/64	2001:db8:1234:0adf::/64
4094	2001:db8:1234:4094::/64	2001:db8:1234:ffe0::/64	2001:db8:1234:0ffe::/64

En la aproximación anterior el tipo de uso (F) y la localización (L) no aparecen en la dirección IPv6, por lo que no será posible optimizar las políticas de seguridad y las tablas de rutas
Sin embargo es posible combinar la codificación de la localización y el tipo de uso con el número de la VLAN.
Observe a continuación un ejemplo donde primero se codifica la localización y el tipo y después el número de la VLAN.

	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	
2001:db8:1234:	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	::/ 64
	L	L	L	L	T	T	T	T	B	B	B	B					

A continuación se muestra otro ejemplo de codificación del tipo de uso y posteriormente la localización en el número de la VLAN, en los bits de la subred de las direcciones IPv6.

	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	
2001:db8:1234:	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	::/ 64
	T	T	T	T	L	L	L	L	B	B	B	B					

Por la importancia del tema se resumen varias recomendaciones importantes cuando se construye el plan de asignación de subredes IPv6:

- Utilice solo prefijos /64 para los segmentos que tengan sistemas finales (host attached), dado que en el direccionamiento IPv6 un /64 es el tamaño estándar de subred para direccionar interfaces.
- La excepción para el estándar /64 son las subredes utilizadas para los enlaces punto a punto. En la RFC 6164 se establece que estos enlaces deben utilizar un /127, aunque el uso de un /126 también se admite. Un /127 es posible debido a que IPv6 no tiene direcciones de difusión (broadcast). Sin embargo la dirección con todos ceros en cada subred es la dirección anycast de todos los enrutadores (Routers).
- Para consistencia con el plan de direcciones todo enlace punto a punto puede serle asignado un /64 pero configurado con un simple /127 desde esta asignación.
- Un /126 permite que las direcciones de todos ceros (all-zeroes) sean saltadas, pero sin embargo las direcciones 128 en cualquier subred son reservadas para direcciones anycast (RFC 2526). Pero en la práctica esto no es problema.
- Un /120, permite evitar todas las direcciones anycast reservadas.
- Sin embargo un /112, permite evitar las direcciones anycast reservadas y tiene la ventaja de que un valor hexadecimal de cuatro dígitos después de los dos puntos en la dirección IPv6 identifican sistemas dentro de la subred.
- Tome ventaja de la topología de la red y de los puntos de agregación naturales para resumir la información de los prefijos.
- Deje espacios en el plan de asignación de direcciones para futuros crecimientos
- Agrupe la asignación de subredes en múltiplos de 4 bits (/48, /52, /56, /60), pues aunque este método reduce la granularidad disponible en el plan de direcciones, pero mejora la legibilidad de los prefijos de red.

Después de planificar la red, las direcciones son asignadas, de forma manual o mediante servidores DHCP en los rangos o gama descrita en la tabla para todas las PC en la red troncal y en los segmentos o subredes.
Uno de los aspectos más útiles de IPv6 es su capacidad para auto configurarse automáticamente, aun sin el uso de un protocolo de configuración de direcciones tal como DHCPv6. Una Estación (host) IPv6 puede automáticamente configurar una dirección de enlace local para cada interface.

Una estación puede determinar las direcciones de sus enrutadores vecinos, direcciones adicionales de configuración sin estado (stateless), prefijos de enlace, y otros parámetros de configuración mediante los mensajes de Solicitud y Anuncios de Enrutadores.
En los mensajes de aviso de los enrutadores se incluyen banderas que indican cuando un protocolo de configuración de direcciones (tal como DHCPv6) debe ser usado para configuración adicional.
Es necesario recordar que en IPv6 hay tres tipos de autoconfiguración y por lo tanto en el diseño de una red empresarial hay que determinar cuáles utilizar, donde emplear SLAAC con Enrutadores y donde utilizar servidores DHCPv6.

Entidades de denominación en la red
Desde el punto de vista del protocolo TCP/IP, una red es un conjunto de entidades con nombre. Un host es una entidad con un nombre. Un enrutador es una entidad con un nombre. La red es una entidad con un nombre. Del mismo modo, se puede asignar un nombre a un grupo o departamento en el que esté instalada la red, así como a una división, región o compañía. En teoría, la jerarquía de nombres que se pueden utilizar para identificar una red prácticamente no tiene límites. El nombre de dominio identifica un dominio.
Planifique un esquema de nomenclatura para los sistemas que compondrán la red. Para los sistemas que funcionan como servidores y que tienen varias NIC, se debe proporcionar al menos un nombre de host asociado con la dirección IP de su interfaz de red principal.
No puede haber dos máquinas en la red que tengan el mismo nombre de host. Por lo tanto, cada nombre de host debe ser exclusivo para cada sistema. Sin embargo, un host o un sistema con un nombre exclusivo asignado pueden tener varias direcciones IP. Cuando planifique su red, realice una lista de las direcciones IP y sus nombres de estaciones (Host) asociados para poder acceder a ellos fácilmente durante el proceso de configuración. Dicha lista le ayudará a verificar que todos los nombres de host sean exclusivos.

<u>Séptimo Paso</u>: Protocolos de Enrutamiento para la red Empresarial
Este es el paso donde hay que decidir cuales protocolos de enrutamiento Internos y externos se van a utilizar en la red: RIP, OSPF o EIGRP (internos) y BGP (externo).
Típicamente en las redes Empresariales o Corporativas se emplea el protocolo OSPF debido a su eficiencia en grandes redes, aunque en el caso de Redes con equipos Cisco se emplea mucho el protocolo EIGRP.
Igualmente hay que tener presente que se va a trabajar con IPv4 e IPv6.
Este es el paso donde hay que decidir que protocolos de enrutamiento Internos se van a utilizar en la red Corporativa: RIP, OSPF y EIGRP. Así como también los protocolos externos a utilizar: BGP o IS-IS.
Típicamente en las redes Corporativas se emplea el protocolo OSPFv3 debido a su eficiencia en grandes redes, aunque en el caso de Redes con equipos Cisco se emplea mucho el protocolo EIGRP. Otros prefieren el protocolo RIPng. Siempre teniendo presente las versiones actualizadas de estos protocolos que permiten trabajar con IPv4 e IPv6.
Luego la etapa de seleccionar y configurar los Enrutadores o Conmutadores de Capa 3 es clave y para ello de forma general se deben seguir los pasos siguientes:

a) Verificar la compatibilidad de todo el hardware instalado
b) Revisar toda la documentación del fabricante de los Enrutadores o Switch-L3
c) Instalar y configurar los protocolos de enrutamiento dinámico
d) Diseñar y desplegar el enrutamiento IP estático
e) Determinar los servicios de configuración automática (DHCP), mediante Enrutadores o Servidores DHCP.
f) Añadir y configurar agentes de retransmisión de DHCP, si hiciera falta.

g) Configurar los Enrutadores para soportar multidifusión (multicast)
h) Diseñar y desplegar la traducción de direcciones (NAT) en donde se necesite.
i) Configurar los filtros de paquetes IP (a nivel de TCP)
j) Configurar las listas de control de acceso (ACL)
k) Revisar las medidas de seguridad para Enrutadores y Switch-L3

Octavo Paso: Servidores y equipos

Para la selección de los equipos de interconexión (Router / Switch capa 3) hay que analizar varias opciones (no menos de tres) a fin de hacer comparaciones y fundamentar la selección.
Igualmente para los servidores hay que hacer lo mismo, pues debe recordarse que es un exigencia técnica y administrativa de evitar favoritismos e ilegalidades con determinados vendedores.
Realice la selección del hardware necesario para la red tales como: transceptores (transceivers), Conmutadores (Switch), Enrutadores (Routers), interfaces , Cortafuegos o Firewalls, Servidores, estaciones de trabajo adicionales, fuentes de respaldo (UPS) , etc.
Es importante la correcta selección de los Servidores acorde a los servicios (sitios web, correo, de transferencia de ficheros, de base de datos, DHCP, DNS etc.)
Sistemas Operativos a emplear, pues los mismos tienen capacidades de red incorporadas a ellos (Microsoft Windows, Linux, Ubuntu, Red Hat, Apple Mac, etc.).

A la hora de seleccionar los productos debe tener en consideración:

- Identificar los productos específicos en el mercado para conocer sus cualidades técnicas y presupuesto (recordar siempre que lo barato sale caro).
- Determinar la necesidad y efectividad de la documentación de cada producto en perspectiva (si está completa, clara, etc.).
- Considerar la reputación del fabricante y distribuidor.
- Hacer una selección comparando el presupuesto de lo que necesita el usuario y analizar la calidad de los productos y costos.
- Valorar el costo de los paquetes de software, su licencia de explotación, costo de actualizaciones, etc.
- Considerar las implicaciones de seguridad para: Acceso remoto, Acceso local, Acceso a ficheros, Acceso a hardware, Acceso a grabación etc.

Servicios de Infraestructura en una red empresarial

Hay algunos protocolos que son esenciales para la corrida de las aplicaciones en Internet y en las Intranet de una red empresarial, pero que no se ajustan de forma nítida al modelo de niveles.
Entre ellos están:

- Protocolo de Configuración de Estaciones Dinámico (DHCP)
- Protocolo del Sistema de Nombres de Dominio (DNS)

Estos protocolos no son aplicaciones que los usuarios o clientes invoquen explícitamente, pero sin embargo son servicios que todas las otras aplicaciones dependen de ellos.
DHCP es un protocolo que permite a las computadoras obtener información acerca de la red desde la propia red. Permitiendo a los servidores DHCP arrendar direcciones a los clientes por un período de tiempo.
Cuando los agentes DHCP son utilizados las computadoras de los clientes adquieren la configuración de forma automática a partir de los servidores. Requiriendo también de agentes retransmisores (Relay Agent DHCP), lo cuales tienen que ser configurados sobre los servidores ejecutando Enrutamiento y Acceso Remoto a través de los Enrutadores que están en posiciones claves.
De lo contrario, si se implementa un servidor DHCP en cada subred no haría falta instalar agentes retransmisores DHCP**.**

El resumen anterior del funcionamiento del protocolo DHCP es básicamente el mismo para DHCP en redes IPv4 que para DHCPv6.

Sin embargo DHCPv6 es muy diferente de DHCP en IPv4, de ahí que se tenga que tener en cuenta sus particularidades en el diseño de una red empresarial.

Es necesario recordar que en IPv6 hay tres tipos de autoconfiguración:

- ✓ Autoconfiguración sin estado (IPv6 Stateless Address Autoconfiguration, SLAAC), donde en la RFC 4862 se especifican los pasos que una estación toma en decidir cómo auto configurar sus interfaces en IPv6. Algunos autores lo denominan sin servidor ("serverless").
  En la RFC 6106 se especificaron nuevas extensiones que permitan a SLAAC incluir información de DNS en los mensajes de Aviso de Enrutadores (RA). Pero sin embargo la misma no es implementada en la mayoría de los casos.
- ✓ **Autoconfiguración con estado (DHCPv6**), según se establece en la RFC 3315 se define el protocolo de Configuración de Estaciones Dinámico DHCPv6 para establecer parámetros de configuración de direcciones stateful para las estaciones (host) IPv6. Esta configuración está basada en el uso de un protocolo de configuración de direcciones tal como DHCPv6, para obtener las direcciones IPv6 y otros parámetros de configuración.
  Una Estación emplea la autoconfiguración DHCPv6 cuando recibe un mensaje de advertencia del enrutador (Routers Advertisement message) sin opciones de Información de Prefijo (Prefix Information options) y además las banderas de ¨Managed Address Configuration¨ y ¨Other Stateful Configuration¨ fijadas a 1. Una Estación puede también utilizar autoconfiguración DHCPv6 cuando no existe enrutador presente en el enlace local y tener un servidor.

- ✓ **Mezcla de SLAAC y DHCPv6**. Esta variante está especificada en la RFC 3736. Cuando se está utilizando SLAAC un dispositivo utilizará la misma para asignar una o más direcciones IPv6 a una interfaz. Mientras que utiliza DHCPv6 para recibir parámetros adicionales. Entre los parámetros adicionales podrían estar información sobre las direcciones de los servidores de DNS o de NTP. La configuración se basa en la recepción de mensajes de advertencia de los enrutadores (Routers Advertisement messages) que incluyen opciones de Información de Prefijo (Prefix Information options), cada uno con su bandera Autónoma (Autonomous flag) fijada a 1, y tienen las banderas de ¨Managed Address Configuration¨ y ¨Other Stateful Configuration¨ fijadas a 1.

Es importante señalar que una implementación de IPv6 podrá encontrarse con múltiples direcciones fuente y destino en sus inicios, por lo que requiere de algún algoritmo por defecto para seleccionar la dirección fuente y destino cuando se inicia la comunicación.

Esto se complica en nodos configurados con doble pila (dual stack) con direcciones fuentes IPv4 e IPv6.

Por lo que en la RFC 6724 (Default Address Selection for Internet Protocol Version 6), se especifican dos algoritmos para seleccionar la mejor dirección fuente y la dirección de destino en el inicio de la comunicación.

Puesto que al utilizar DHCP, los agentes retransmisores (Relay Agent DHCP) tienen que ser configurados sobre los servidores ejecutando Enrutamiento y Acceso Remoto a través de los Enrutadores que están en posiciones claves. Cuando los agentes DHCP son utilizados las computadoras de los clientes adquieren las direcciones de los servidores.

De lo contrario, si se implementa un servidor DHCP en cada red no haría falta instalar agentes DHCP.

También es importante la configuración de los servicios de nombres de Dominio (DNS), así como determinar los servidores a colocar.

Sistema de Nombres de Dominio (DNS) en Redes IPv4 – IPv6

Las estaciones y servidores en Internet se identificaban anteriormente solo mediante una **dirección IPv4, sin embargo hoy en día se identifican también mediante una dirección IPv6**. Sin embargo los seres humanos prefieren utilizar **nombres (como www.yahoo.com),** porque son más fáciles de recordar, y porque ofrecen la flexibilidad de poder cambiar el dispositivo o estación en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él.
Para realizar esta conversión entre nombres y direcciones IP se utilizan los servidores de DNS. Los servidores DNS almacenan información acerca del espacio de nombres del dominio, y son conocidos como **servidores de nombres**. Los servidores de nombres suelen ser responsables de una o más zonas (entendiendo como zona un archivo físico que almacena registros de la base de datos de una parte del espacio de nombres DNS). El servidor de nombres se dice que tiene **autoridad** sobre esas zonas.
Un servidor de nombres principal es un servidor de nombres que obtiene los datos de sus zonas de archivos locales. Los cambios en una zona, como la adición de dominios, se realizan en el servidor de nombres principal.
Un servidor de nombres secundario obtiene los datos de sus zonas de otro servidor de nombres de la Red que tiene autoridad para esa zona (normalmente de un servidor de nombres principal). El proceso de obtención de información de estas zonas (es decir, el archivo de base de datos) por red se conoce como una transferencia de zona.
Es importante no olvidar que para acceder a los recursos de la red empresarial (Intranet) y a Internet, hay instalar los servidores de nombre de Dominio (DNS) primario y secundario de la red Corporativa tanto para IPv4 como para IPv6.
Para soportar el almacenamiento de las direcciones IPv6 en el DNS, la RFC 3596 define las siguientes extensiones:

- Un tipo de registro de recurso (RR) tipo AAAA es definido para correlacionar un nombre de dominio a una dirección IPv6 (forward mapping).
- Mientras que un registro de recurso (RR) tipo PTR es definido para correlacionar una dirección IPv6 con un nombre de dominio (reverse mapping).
- Un dominio es definido para soportar búsquedas basadas en una dirección IPv6.
- Las consultas existentes que llevan a cabo procesamiento de secciones adicionales para localizar direcciones IPv4 son redefinidas para realizar procesamiento de secciones adicionales tanto en direcciones IP v4 como en IPv6.
- Las extensiones están hechas para ser compatibles con aplicaciones existentes y con las propias implementaciones del DNS.
- La versión del protocolo IP usada para preguntar por registros de recursos es independiente de la versión del protocolo. Ejemplo: el transporte de IPv4 puede ser usado para consultar registros de IPv6 y viceversa.

O sea que un servidor de DNS puede incluir RR tanto de IPv4 como de IPv6 en un fichero de zona, tal como se muestra a continuación:

```
; zone fragment for example.com
$TTL 2d ; zone default = 2 days or 172800 seconds
$ORIGIN example.com.
....
www     IN      A       192.168.0.3
mail    IN      A       192.168.0.32
www     IN      AAAA    2001:db8::3
mail    IN      AAAA     2001:db8::32
```

Otros servicios a incluir en la red Corporativa
Entre los otros servicios a incluir en la red corporativa están:

- Telefonía IP

- Video Conferencias
- Video (Streamming)
- Respaldo de información
- Correo por Web (Web mail)
- Bases de datos
- Todos los servicios anteriores deben tener enlaces mediante la página web de la Intranet.

Hay que tener bien claro a cuales empleados (técnicos, administrativos, directivos, clientes, etc).se les permitirá el acceso y a cuáles no se les permitirá. Igualmente en una instalación hospitalaria (personal médico, paramédico, administrativo y pacientes), en una universidad (profesores, estudiantes y administrativos).

Noveno Paso: Seguridad de la red

Este es un aspecto de alta prioridad, lo que requiere definir las políticas y herramientas de seguridad informática a implementar en la red Corporativa.

Las técnicas de seguridad adoptadas en el nuevo protocolo IPv6 fueron diseñadas para ser fácilmente insertadas en IPv4. Sin embargo el protocolo IPv4 posee otros problemas y es poco deseado que la pila de protocolos de red actual sea modificada solo para implementar las nuevas técnicas de seguridad. Por el contrario estas técnicas se han convertido en un estándar que debe ser aplicado a todas las implementaciones de IPv6.

Luego en este material se van a tocar algunos aspectos de cómo garantizar un mínimo de medidas prácticas de seguridad en una red con los protocolos de Interconexión IPv4 e IPv6**.**

Cortafuegos o Muro de Seguridad (Firewall)

Es un sistema diseñado para prevenir el acceso ilegal hacia o desde una red privada conectada a Internet.

Un Cortafuegos es una combinación de hardware y software que separa una red interna de una organización de una red grande como Internet, permitiendo que algunos paquetes pasen y bloque los otros. Por lo que un Cortafuegos permite a un administrador controlar el acceso entre el mundo exterior y los recursos dentro de la red privada, mediante la gestión del flujo de tráfico desde y hacia esos recursos, tal como se muestra en la figura 16.11.

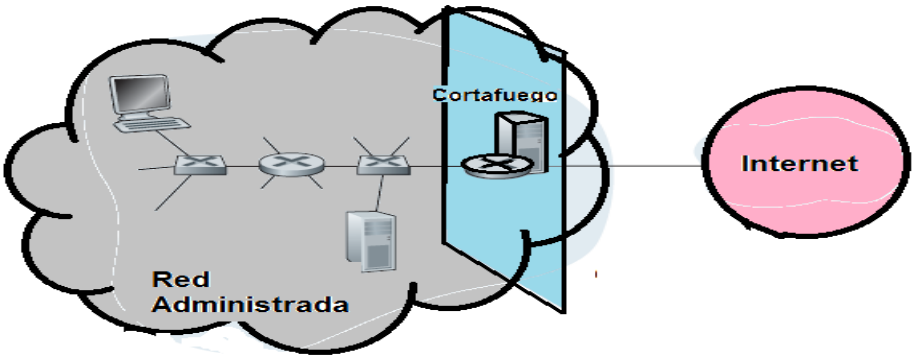


Fig. 16.11 Ubicación del cortafuego entre la red administrada y el mundo exterior

Un cortafuego tiene tres objetivos:

- Todo el tráfico desde el exterior hacia el interior y viceversa pasa a través del mismo. En la figura siguiente se muestra un cortafuego asentado en la frontera entre la red administrada y el resto de Internet. Mientras que las grandes organizaciones puede utilizar múltiples niveles de cortafuegos o estar distribuidos. Localizar el cortafuego en un simple punto de acceso a la red facilita la gestión e impone una política de seguridad de acceso.

- Solo el tráfico autorizado, como se definió en la política de seguridad local, será permitido a pasar. Con todo el tráfico entrando y saliendo de la red institucional pasando a través del cortafuego, el mismo puede restringir el acceso a solo el tráfico autorizado.
- El cortafuego por sí mismo es inmune a la penetración. El cortafuego es un dispositivo conectado a la red. Si no está diseñado o instalado propiamente este puede ser comprometido y en ese caso puede ofrecer solo un falso sentido de seguridad (lo que es peor que no tener un cortafuego).

Hay dos políticas básicas en la configuración de un Cortafuegos que cambian radicalmente la filosofía fundamental de la seguridad en la organización:
Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El Cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.
La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.
Es muy común conectar al cortafuego a una tercera red neutral, llamada Zona desmilitarizada (DMZ), en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.
Un Cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.
Los Cortafuegos empresariales son colocados en el perímetro de la red para reforzar la política de seguridad, mediante el permiso o denegación de cierto tráfico en la red.
De forma general hay tres tipos de Cortafuegos Empresariales, los cuáles vamos a ordenar por su complejidad:

1) Filtrado de paquetes
2) Filtrado de paquetes con Servidor
3) Aplicaciones Delegadas (Proxies)

Esta es la forma más sencilla de Cortafuegos y generalmente en una empresa se tiene un Enrutador que conecta la red interna al Suministrador de Servicios de Internet (ISP). Todo el tráfico que abandona o entra a la red interna pasa por este Enrutador y el filtrado de paquetes es realizado en el mismo.
El filtrado de paquetes examina cada paquete de forma individual, determinando cuando es permitido que pase o si debe ser descartado basado en la reglas especificadas por el administrador.
Las decisiones de filtrado son típicamente basadas en:

- Direcciones IP fuente y destino
- Tipos de protocolos en paquetes IP: TCP, UDP, ICMP, OSPF, etc.
- Banderas TCP: SYN, ACK, etc.
- Tipos de mensajes ICMP
- Otras reglas para mensajes que abandonen o entren a la red
- Diferentes reglas para las diferentes interfaces del enrutador.

Un administrador de una red configura el cortafuego basado en las políticas de la organización. Donde la política puede apropiarse de la productividad y del ancho de banda tomados en consideración así como todo lo concerniente a la seguridad de una empresa.

En la tabla siguiente se listan posibles políticas que una organización puede tener y como ellas son dirigidas con un filtro de paquetes.

Política	Configuración del Cortafuego
No permitir acceso web al exterior	Descartar todos los paquetes que salen hacia cualquier dirección IP
No permitir conexiones TCP, excepto la pública del servidor web de la empresa	Descartar todos los paquetes de tipo TCP SYN a cualquier dirección IP, excepto a la dirección IP 200.45.6.7 por el puerto 80.
Evitar todos los radio-Web que se comen el ancho de banda	Descartar todos los paquetes UDP entrantes, excepto los paquetes con DNS.
Evitar que su red sea utilizada por un programa que ataca generando una denegación de servicio (DoS)	Descartar todos los paquetes ICMP de tipo ping que vaya dirigidos a una dirección de difusión (por ejemplo 222.33.255.255.
Evitar en la red un trazado de rutas	Descartar todos los paquetes de salida ICMP con expiración del TTL

Por lo que hay que considerar de forma cuidadosa que servicios de red serán permitidos pasar a través del Enrutador (en entrada y en salida) y hacia el Enrutador.
De ahí que se recomiende utilizar la regla siguiente: **Aquellos servicios que no son explícitamente permitidos son prohibidos.**
El filtrado de paquetes también debe ser utilizado para proteger a la red contra el uso de direcciones IP para suplantación de identidad (spoofing). De ahí la importancia de configurar las listas de Control de Acceso (ACL) y su ubicación en los Enrutadores.
Algunas empresas mantienen un listado de puertos y protocolos estándares que deben ser permitidos y soportados sobre sus redes. Debiendo rechazarse todos los otros
Una política de seguridad tiene que definir los objetivos específicos, emplear una zona de red desmilitarizada (DMZ) y en especial preparar un Cortafuegos (Firewall) con sus reglas de configuración básicas, tal como se muestra en la Figura 16.12.

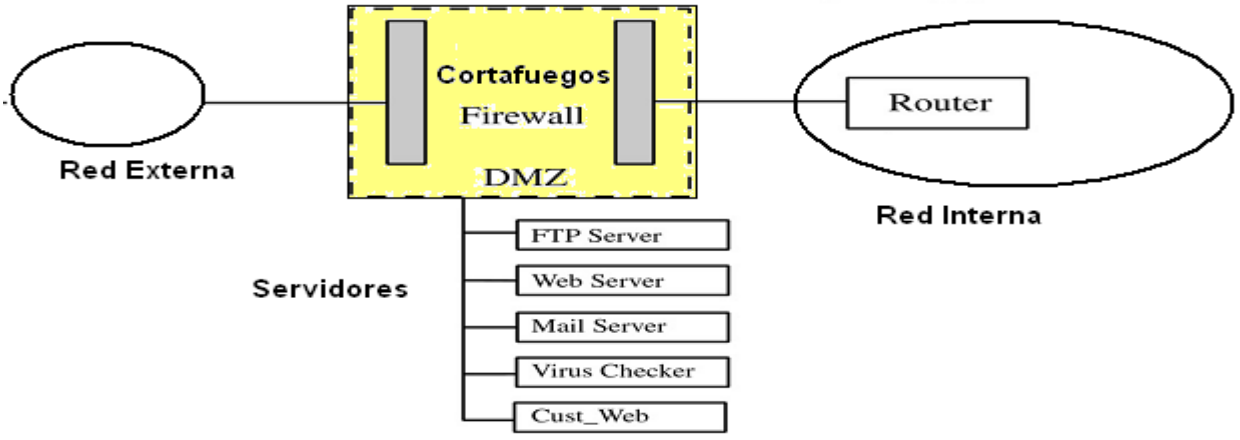


Fig.16.12 Relación entre la DMZ y el papel del Cortafuegos

Una red DMZ es una red añadida entre una red protegida y una red externa para ofrecer un nivel de seguridad adicional. A veces a la DMZ también se le denomina red perimetral y la misma es un ejemplo del principio de defensa en profundidad. La misma establece que la única forma de un sistema ser razonablemente segura es considerando todos los aspectos y seguridad de todos.
Una DMZ es un paso hacia la defensa en profundidad, dado que adiciona un nivel extra de seguridad por detrás de un simple perímetro.

La DMZ utiliza un cortafuego para restringir el acceso desde Internet a la DMZ para proteger los servidores y desde la DMZ a la Intranet para protegerse contra los compromisos.
Por Ejemplo: a) permitir conexiones desde Internet para el servidor de correo por el Puerto 25 (SMTP) y permitir conexiones desde la Intranet al servidor de correo sobre el puerto 993 (IMAP seguro).
Dos de las más básicas arquitecturas de diseño de la DMZ son:

a) Con un simple Cortafuegos
b) Con dos Cortafuegos

En la Figura 16.13 se muestran dos DMZ conectadas a los Cortafuegos, aunque también la DMZ pudiera estar entre los dos cortafuegos.
Es importante señalas que para crear una DMZ se necesita crear alguna VLAN sobre su infraestructura de conmutadores, además se necesita una interfaz IP sobre el Cortafuegos con una dirección IP de subred que se haya asignado y las reglas que permitan / nieguen tráfico hacia o desde la DMZ.

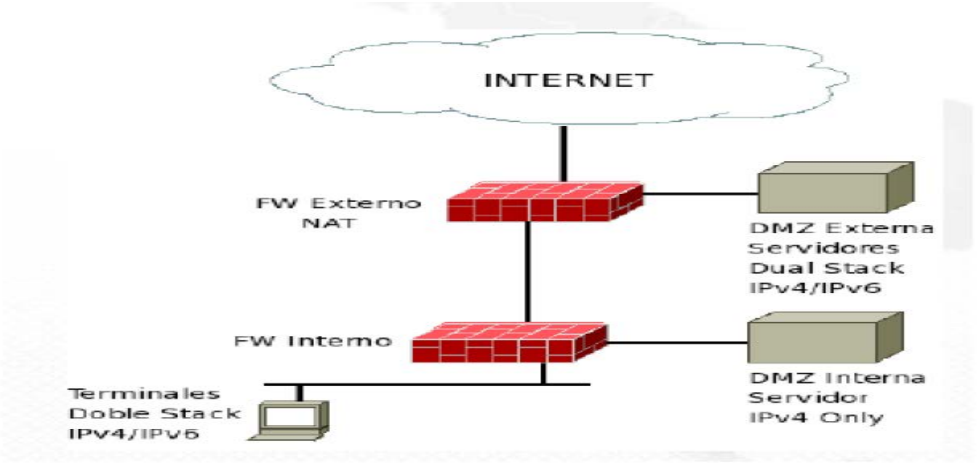


Fig.16.13 Empleo de dos Cortafuegos y dos DMZ

De forma simple se puede pensar que un servidor Proxy (Delegado) como un cortafuegos del nivel de aplicación. Pero en el caso de los servidores Delegados (proxies) web estos pueden servir para dirigir, redirigir o limitar el acceso a servidores y URL específicas.
Aunque el proxy puede ser colocado en paralelo con el cortafuego, preferentemente el mismo debe ser colocado detrás del cortafuego. En caso de mucho carga de tráfico se pueden utilizar varios cortafuegos en paralelo.
En casos extremos tiene que estar seguro que se han utilizado reglas consistentes para todos los cortafuegos.
Hay que valorar la utilización o no en una red Corporativa el empleo de Proxy directos e inversos.
La política de seguridad tiene que estar en un documento vivo, que forme parte de la práctica de la red de forma regular y que se revise y actualice ante diferentes eventos que ocurren tales como:

- Nuevas conexiones realizadas entre la red local y las redes externas
- Cambios de prácticas administrativas, procedimientos, de personal, etc.
- Cambios en la política general
- Despliegue de nuevas capacidades o nuevas componentes de red.
- Detección de ataques o compromisos serios.

En la Figura 16.14 se muestra un esquema general de una red empresarial segura con varias DMZ

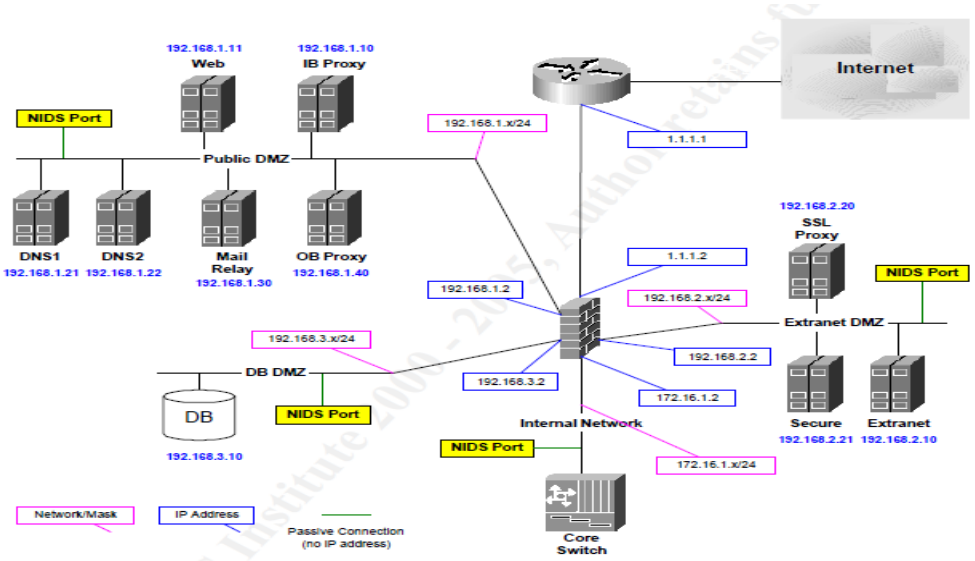


Fig.16.14 Arquitectura de red detallada de alta seguridad

En la Figura 16.15 se muestra el esquema de conexiones general de una red de una empresa, con sus servidores, dos cortafuegos, su zona segura (DMZ) y su conexión a Internet.

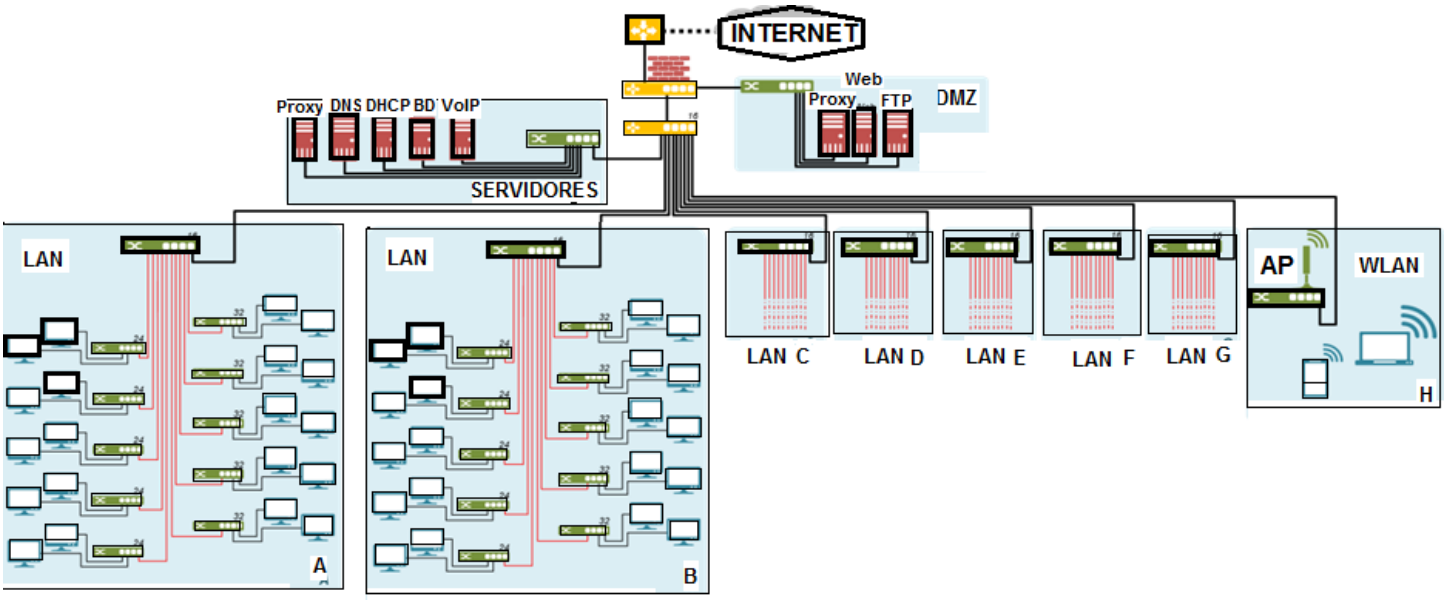


Fig.16.15 Esquemas de conexiones de una red empresarial con dos cortafuegos

A continuación se hace un resumen de los principales aspectos tomar en cuenta para la Política de Seguridad de un Enrutador:

Seguridad a nivel físico:

a) Designar quien está autorizado para instalar, desinstalar y mover el Enrutador.

b) Designar quién está autorizado para el mantenimiento del hardware y para cambiar la configuración física del Enrutador.

c) Designar quién está autorizado para ejecutar conexiones físicas al Enrutador

d) Definir controles sobre la colocación y uso de la consola y otros puertos de acceso directo.

e) Definir procedimientos de recuperación para casos de daños físicos al Enrutador o evidencia de sabotaje con el Enrutador.

Seguridad de la configuración estática:

a) Designar quién está autorizado a registrarse directamente en el Enrutador mediante la consola u otros puertos de acceso directo.
b) Designar quién está autorizado asumir privilegios administrativos sobre el Enrutador.
c) Definir procedimientos y prácticas para hacer cambios en la configuración estática del Enrutador (por ejemplo en el libro de registros, cambiar registros, revisar procedimientos, etc.)
d) Definir la política de palabras claves (passwords) para los usuarios y para administrativos o privilegiados.
e) Designar quién está autorizado para registrarse en el Enrutador remotamente (por TELNET, pero nunca por Web).
f) Designar los protocolos, procedimientos y redes permitidas para registrarse remotamente en el Enrutador.
g) Definir los procedimientos de recuperación, o identificar los responsables individuales para la recuperación, para el caso de configuración estática del Enrutador.
h) Definir la política de registro y auditoría para el Enrutador, incluyendo la práctica de administración de registros remota y los procedimientos.
i) Designar procedimientos y límites en el uso de administración remota automatizada y las facilidades de monitoreo (por ejemplo usando SNMP).
j) Definir líneas directivas para detectar ataques contra el Enrutador.
k) Definir las políticas de administración para claves criptográficas a largo plazo.

Seguridad de la configuración dinámica:

a) Identificar los servicios de configuración dinámica permitidos sobre el Enrutador y las redes permitidas acceder a estos servicios.
b) Identificar los protocolos de enrutamiento a ser utilizados y los rasgos de seguridad a ser empleados en cada caso.
c) Designar mecanismos y políticas para fijar el mantenimiento automático del sincronismo de reloj del Enrutador (por ejemplo, Manual, NTP,etc.)

Seguridad del Servicio de Red:

a) Enumerar los protocolos, puertos y servicios que serán permitidos o filtrados por el Enrutador.
b) Identificar los procedimientos y autoridades para autorizar los protocolos, puertos y servicios.
c) Definir procedimientos de respuesta, autoridades y objetivos en el caso de detección de ataques contra la red.

Es importante conocer las normas ISO/IEC 27000 relacionadas con la seguridad de Redes, en especial la ISO/IEC 27033-1:2009 la que ofrece una visión de la seguridad de redes y las definiciones relacionadas con ella.

A continuación se relacionan estas:

ISO 27033-2 Network security - Part 2: Guidelines for the design and implementation of network security
ISO 27033-3 Network security - Part 3: Reference networking scenarios -- Risks, design techniques and control issues
ISO 27033-4 Network security - Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues
ISO 27033-5 Network security - Part 5: Securing virtual private networks - Risks, design techniques and control issues
ISO 27033-6 Network security - Part 6: IP convergence
ISO 27033-7 Network security - Part 7: Wireless

Diseño Físico

Con esta acción se concretan los equipos y medios que tendrá la red futura y por tanto el costo de la red.

Décimo Paso: Selección del Hardware y Software relacionado con la red

Las soluciones de hardware están principalmente basadas en el estándar IEEE 802.3 con sus variantes Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigas, 40 Gigas y 100 Gigas, producto de sus altos rendimientos, grandes anchos de Banda y costos aceptables.

Mientras que las soluciones de redes inalámbricas están basadas en el estándar IEEE 802.11 con sus variantes: 802.11 n, 802.11 ac wave 2 y 802.11 ax presentes en las empresas modernas.

Realice la selección del hardware necesario para la red tales como: Tarjetas de Interfaz (NIC), Repetidores(Hub), transceptores (transceivers), Conmutadores (Switch), Enrutadores (Routers), Modems, fuentes de respaldo (UPS) , Cortafuegos o Firewalls, Servidores (sitios web, de correo , de ficheros, de bases de datos, etc) , estaciones de trabajo adicionales, Modems, fuentes de respaldo (UPS) , etc.

- ✓ Es importante la correcta selección de los Servidores acorde a los servicios (sitios web, correo, de ficheros, de base de datos, DHCP, DNS etc.)
- ✓ Sistemas Operativos a emplear, pues los mismos tienen capacidades de red incorporadas a ellos (Microsoft Windows, Linux, Ubuntu, Apple Mac, etc.).
- ✓ Por lo que las estaciones de trabajo tienen que estar actualizadas con respecto a los sistemas operativos seleccionados.
- ✓ Las herramientas de software para el monitoreo y gestión de la red.
- ✓ Requerimientos de seguridad y acceso remoto (RAS).

A la hora de seleccionar los productos debe tener en consideración:

- ✓ Identificar los productos específicos en el mercado para conocer sus cualidades técnicas y presupuesto (recordar siempre que lo barato sale caro).
- ✓ -Determinar la necesidad y efectividad de la documentación de cada producto en perspectiva (si está completa, clara, etc).
- ✓ Considerar la reputación del fabricante y distribuidor.
- ✓ Hacer una selección comparando el presupuesto de lo que necesita el usuario y analizar la calidad de los productos y costos.
- ✓ Valorar el costo de los paquetes de software, su licencia de explotación, costo de actualizaciones, etc.
- ✓ Considerar las implicaciones de seguridad para: Acceso remoto, Acceso local, Acceso a ficheros, Acceso a hardware, Acceso a grabación etc.

Luego la etapa de instalar y configurar los Enrutadores o Conmutadores de Capa 3 es clave y para ello de forma general se deben seguir los pasos siguientes:

- Verificar la compatibilidad de todo el hardware instalado
- Revisar toda las documentación del fabricante de los Enrutadores o Switch-L3
- Instalar y configurar los protocolos de enrutamiento dinámico
- Diseñar y desplegar el enrutamiento IP estático
- Determinar los servicios de configuración automática (DHCP), mediante Routers o Servidores DHCP.
- Añadir y configurar agentes de retransmisión de DHCP, si hiciera falta.
- Configurar los Enrutadores para soportar multidifusión (multicast)
- Diseñar y desplegar la traducción de direcciones (NAT)
- Configurar los filtros de paquetes IP (a nivel de TCP)

- Configurar las listas de control de acceso (ACL)
- Revisar las medidas de seguridad para Enrutadores y Switch-L3

<u>Décimo primer Paso</u>: Selección del sistema de cableado

El sistema de cableado puede ser centralizado o distribuido y en el mismo deben tomarse diferentes consideraciones tales como: si se requiere redundancia en diferentes lugares, si se requiere de múltiples fibras o pares de cobre en un mismo cable, múltiples cables en un mismo conductos, múltiples conductos por un mismo camino etc.

Hay que elaborar el plano físico de la red LAN con todos los detalles, con las medidas exactas en metros, tomando en cuenta:

- Tamaño de los locales, pisos, edificio, distancia entre edificios, etc.
- Ubicación de los usuarios y equipos
- Posición de las canaletas y distribuidores (techos, pisos, etc.)
- Precisar la posición de los armarios, gabinetes, etc.
- Closets de alambrado (racks, paneles, bandejas, etc.)
- Cuartos de conexión

El plano físico también debe ser preciso en el cuarto de control de la red, teniendo en consideración los elementos anteriores.

A modo de ejemplo se muestra en la Figura 16.16 el caso de un edificio donde hay que tomar en cuenta todos los elementos anteriormente enumerados.

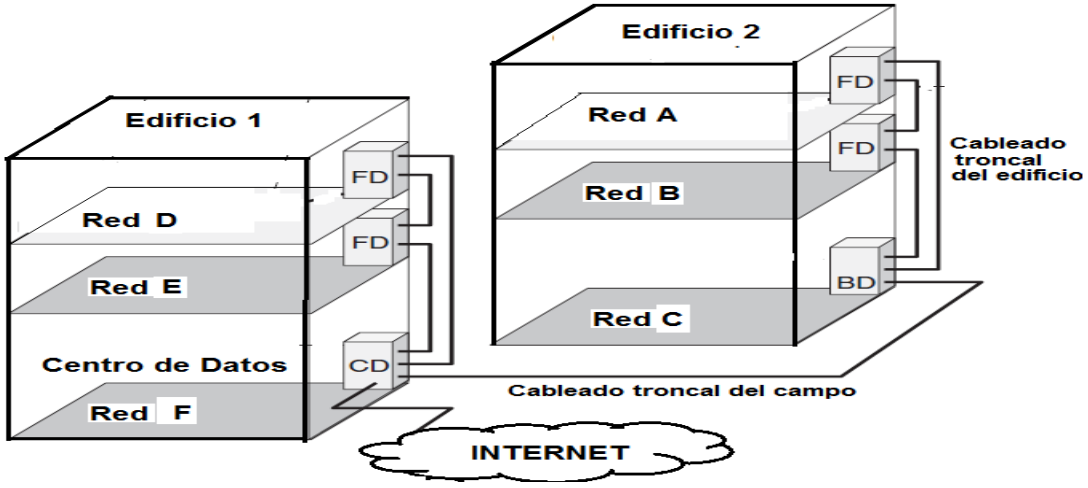


Fig.16.16 Ejemplo de la distribución del cableado troncal de edificio y campo

A partir del plano físico se calculará la cantidad de cables, tomas de pared, armarios, cantidad de canaleta, etc. A modo de ejemplo se muestra en la Figura 16.16 un plano físico de una planta donde se proyecta distribuir el sistema de cableado, con sus armarios y cuarto de Telecomunicaciones.

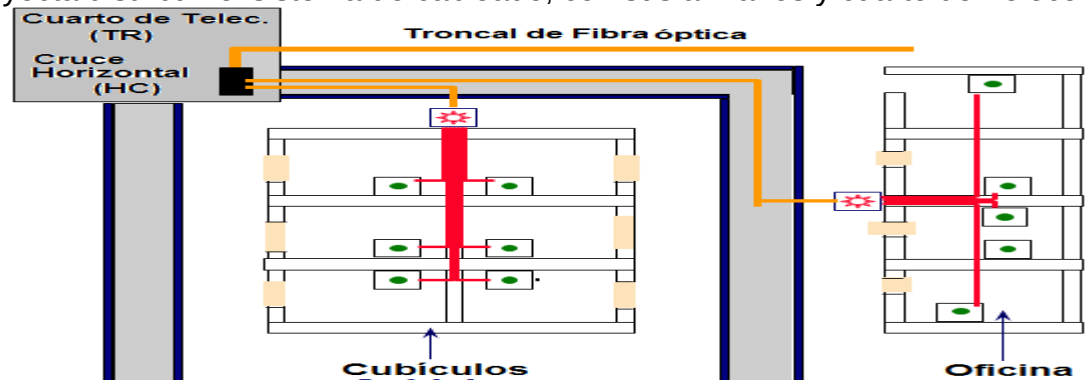


Fig. 16.17 Ejemplo de plano físico de una planta

No se puede incumplir con las exigencia en cuanto a la calidad del cable requerido, tanto para interiores (ignífugos) como para cables exteriores (sometidos a la luz del sol, humedad etc.)
Para justificar la propuesta de cableado de la Red, es necesario seleccionar la peor trayectoria, o sea la más distante entre dos elementos de la red y determinar los retrasos que se introducen en ella tomando en consideración: tipo y longitud de los cables, conectores, repetidores etc. que están en esa trayectoria.
Todo ello como es lógico dentro de las normas de cableado vigentes: EIA/TIA 558-D o ISO /IEC 11801 en su edición actual.
Por lo que debe definir bien claro las necesidades en cuanto a: canaletas, cables, conectores, distribuidores, cabinas, paneles, cables de conexión (patch cord), bandejas o paneles de conexión (path panels), etc.
Para ello se auxiliara de Manuales comerciales de firmas especializadas (ejemplo Legrand).
Por lo general todas las redes requieren de un Centro de Gestión (CGR) o de Control de la Red (CCR) a nivel de campo y muchas veces a nivel de cada edificio, por lo que se hace necesario definir la estructura del mismo, aclarando que el mismo no tiene que estar en el mismo lugar en que estén los equipos, servidores o nodos de la red troncal (core).
Otros elementos a tomar en consideración en el diseño de una red son:

- ✓ Medidas de seguridad informática, comenzando por la protección física de los equipos**.**
- ✓ La protección de tierra requerida para cada local para los equipos de red.
- ✓ La protección de sobre-voltajes y de descargas eléctricas.
- ✓ Necesidades de respaldo energético para el equipamiento (UPS, baterías etc.) a fin de cumplir con las misiones críticas y tener una disponibilidad de 99.99 %.

Las políticas y herramientas de seguridad informática y las herramientas de administración de la red no serán desarrolladas en este material pues no es objetivo del mismo.

<u>Décimo segundo Paso</u>: Justificación de la Inversión y modelos de costo
Costo Total de Propiedad (TCO)
Es muy común encontrar en la propaganda de los fabricantes de equipos para redes de comunicaciones comparaciones de costo, utilizando un indicador denominado Costo Total de Propiedad (TCO). Este indicador está relacionado con la compra de una infraestructura de red, pero no toma en consideración el costo de instalación, pues en muchas ocasiones la instalación la asumen las propias empresas o terceros que no involucran a los fabricantes.
Sin embargo el análisis de TCO es un método que permite evaluar de forma cuantitativa los productos.
Generalmente en estas comparaciones se toma en consideración aspectos interesantes, tales como:

- El número de puertos totales requeridos (por ejemplo 1000 GE para una red LAN de campus).
- El tipo de hardware utilizado para mantener las configuraciones (si es de bajo, medio o alto rango).
- Los precios del hardware y de las configuraciones en dependencia de los niveles de servicio.
- La cantidad de armarios de conexión.
- Los precios minoristas de cada componente de hardware y de software
- La eficiencia energética, el soporte al medioambiente y la gestión de energía de los dispositivos son factores también que se deben considerar.

Los costos de instalación no son incluidos en el los cálculos del TCO, pues un cliente puede utilizar sus propias fuerzas o un tercero experto que le permita reducir los costos.

Tampoco en el TCO son incluidos los costos del cableado, por lo que hay que utilizar otro modelo de análisis de costo.

Costo para Redes Empresariales con Fibra Óptica (FOLS)

Este modelo de costo se ha ido generalizando en los últimos años para Redes LAN y es conocido por sus siglas FOLS (Fiber Optics LAN Section). El mismo ha sido desarrollado por la Asociación de Industria de Telecomunicaciones (TIA). El mismo sirve para estimar los costos de infraestructura de una red LAN, teniendo un amplio alcance y enfocado al apoyo de las redes convergentes.

Este modelo de costo es interactivo y se encuentra en el sitio web www.fols.org, donde se ofrece una hoja de cálculo de Microsoft Excel muy completa para calcular el costo total de una red LAN. Además en el sitio ofrece un documento con instrucciones que explica varios escenarios. Ambos documentos pueden ser bajados sin costo alguno.

Este modelo compara los costos de una arquitectura de estrella horizontal (con UTP y fibra en el troncal) con otras tres arquitecturas de todo fibra.

El modelo FOLS sirve como un recurso educacional que facilita información a los usuarios acerca de los beneficios de usar fibra óptica en las redes.

A modo de ejemplo se muestra en la Figura 16.18 una hoja de cálculo que ofrece el modelo FOLS, donde no solo sirve para calcular el cableado, sino también el costo del hardware y de otros elementos.

LOCATION	UTP PLUS FIBER NETWORK	cost, $	per node	per node	man-hrs	
desktop	UTP NIC		42.00			3Com managed 10/100 NIC
	UTP jumper to wall plate		9.00			
	wall plate		2.29			
	jack		5.00	9.60	0.16	
	horizontal UTP cable		45.00			Data Warehouse
telecom	patch panel in closet		5.00	0.20	0.16	
room	jack in patch panel		5.00	9.60	0.16	
	UTP jumper to switch		5.59	5.00	0.08	
	switch; Cisco 3550	2995	89.14			
	conversion to fiber in hub; 1000Base SX	288	6.00	0.00		Data Warehouse
	rack	100	2.08	0.63	0.50	
A	cost/port		216.10	25.03		
	fiber jumper from switch to patch panel		6.40	0.00		FIS 2003 catalog
	fiber patch panel + enclosure		6.67	9.60	0.16	
	jack		0.00			
	2 fiber connectors + barrels in patch panel		10.70	10.00	0.17	FIS 2003 catalog
	vertical riser fiber cable		14.13			FIS 2003 catalog 24f/riser
	sub total		37.89	19.60		
B	cost/port		0.79	0.41		

Fig. 16.18 Ejemplo de una hoja de cálculo de FOLS

En este documento no se abarca el costo de Centro de Datos (Data Center), el cual lleva otros elementos en consideración.

Recuperación de la Inversión (ROI)

Para diseñar una nueva red o una actualización (Upgrade) de la red existente, es importante la justificación de la inversión. En especial justificar como el nuevo sistema puede reducir los costos.

Por lo que hay que el costo total aproximado, incluyendo los costos de los componentes, cableado, instalación, mantenimiento, operación y el de entrenamiento del personal; con vistas a tener claro estos elementos para buscar el financiamiento.

La justificación del negocio generalmente considera tres cuestiones:

- ¿Qué le ahorra a la empresa la inversión o actualización?
- ¿Le ayudara esta actualización a ganar más?
- ¿Le permitirá ser competitiva?

El elemento de medida para la consideración final de una actualización o inversión en una red es el denominado Índice de Recuperación de la Inversión (ROI), el cual es una medida de la ganancia de capital que ocurre como resultado de la actualización o inversión. Esto no es siempre posible medirlo de forma exacta, pero el mismo de forma general considera los costos principales contra los principales ahorros.

La fórmula básica está dada por la expresión siguiente:

ROI = (ahorros relacionados en el costo operacional + ingresos (earnings) por mejora de los servicios) – (costo inicial de la actualización + carga financiera + carga operacional para el periodo).

A modo de ejemplo considere que una empresa X actualiza su red, el éxito estriba en que mejora la productividad por usuario en un 5%, para un total de 800 trabajadores. La actualización o inversión costo $ 500 000. Después de 6 meses en la empresa X todo el mundo está feliz, pero cuál es el ROI. Si se considera que los 800 trabajadores recibirán un salario promedio por año de $ 3 5000, con un mejoramiento de la productividad de un 5 %, eso significa que el ROI creció en $ 1 400 000.

Similarmente el periodo de amortización para ROI puede ser hallado mediante la división del costo total de actualización por el costo estimado de pérdidas por caída de la productividad para un año laborable.

Por ejemplo si se considera que una red tiene unas pérdidas de un 2% de pérdidas de productividad y se tiene un grupo de trabajo que percibe unos $ 340.00 diarios, para un año de trabajo de 220 días laborables, se tendrá una pérdida de $ 225 000 .

Luego si el costo total de la inversión fue de 365 550, el periodo de amortización del ROI será de cerca de 20 meses (365 550 / 225 000 = 1.64 año) .

Pruebas, optimización y documentación de la Red

En esta acción se realizan las pruebas preliminares que permitirán hacer correcciones a los pasos anteriores y una vez satisfechas se procederá a la documentación de proyectos para enfrentar el montaje y puesta punto**.**

<u>Décimo tercer Paso:</u> Modelación y Simulación de la Red.

Un especialista en redes hoy en día tiene que dominar diferentes herramientas de software, tales como:

- **Packet Tracer** es una herramienta de entrenamiento y verificación del buen funcionamiento de una red desarrollada por Cisco. La misma se puede instalar en cualquier PC con sistemas operativos Windows (XP, 2003, 2007,2008, etc.), Linux, Ubuntu, RedHat, etc. El Packet Tracer se ha ido perfeccionando con el tiempo y las nuevas versiones han incorporado nuevos equipos, nuevos estándares de redes y nuevos protocolos actualizados (IPv6, RIPv3, OSPFv3, etc.).
- **Wireshark**, es un analizador de Protocolos que tiene amplia variedad de aplicaciones y apoyo a otras herramientas de modelación y simulación. La herramienta de software Wireshark (WS) ha sido desarrollada por la firma de su mismo nombre, construida utilizando Microsoft Visual C++ y es de Fuente Abierta (Open Source Software released under the GNU General Public License). Para ello puede consultar cualquier información en el sitio http://www.wireshark.org.
- **OPNET Modeler, Network Simulator (NS), OMNET ++ , COMMNET**, etc. Todas estas herramientas de modelación y simulación de redes compilan sobre C++. El OPNET es un

software propietario de Riverbed corporation, pero tiene licencias académicas y se utiliza en cientos de universidades de prestigio del mundo.

Con estas herramientas se pueden probar variadas topologías de redes con diferentes tecnologías, y aplicaciones. Permitiendo analizar bajo diferentes flujos de tráfico y situaciones, el desempeño de dichas redes.

Luego para probar la red diseñada, utilizará la Herramienta Packet Tracert (versión 6.0) lo que le permitirá realizar pruebas de conectividad de los equipos y otras pruebas para responder a las interrogantes siguientes:

¿Están siendo los paquetes IPv4 e IPv6 encaminados correctamente?
¿Está trabajando bien el NAT interno y externo?
¿Está trabajando correctamente los protocolos RIP y OSPF?
¿Están todas las redes incluidas en las tablas de rutas?
¿Funcionan bien los servidores (web, mail, ftp, VoIP, video, etc.)?
¿Funcionan bien las políticas de seguridad, en especial las ACL ?
¿Funcionan bien las redes LAN virtuales (VLAN)?
¿Están trabajando correctamente los túneles y dobles pilas IPv4 – IPv6?
¿Está funcionando adecuadamente el Cortafuegos (Firewall)?
¿Están funcionando bien los servidores Proxies?

Para poder evaluar el proyecto de diseño con cualquier herramienta de las enumeradas con anterioridad, va a tener que dibujar de forma simplificada la red a evaluar. Para ello partirá de la topología de conexiones lógicas de la red, diseñada en el Cuarto Paso, bajo diferentes escenarios o situaciones.

A modo de ejemplo se muestra en la Figura 16.19, el diagrama simplificado, utilizado en la Herramienta OPNET de las conexiones lógicas de una red empresarial.

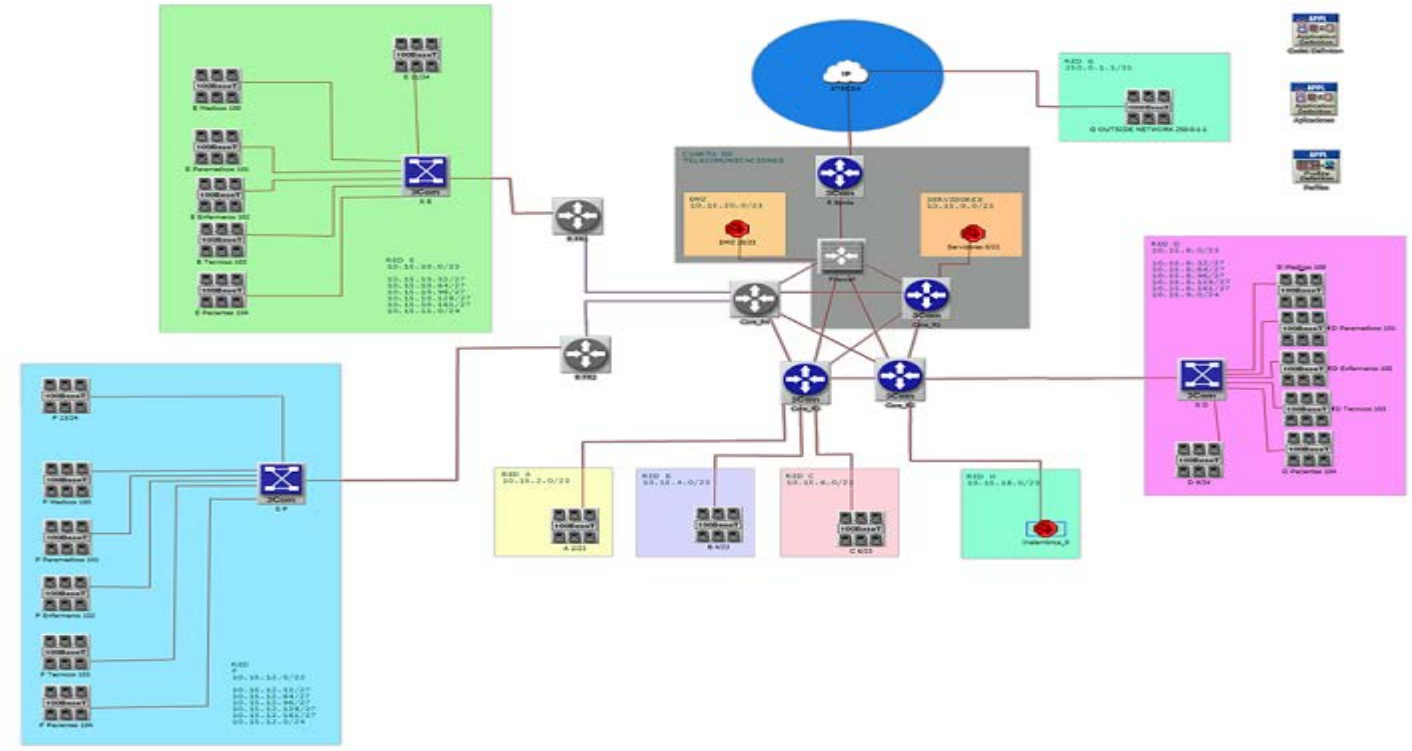


Fig. 16.19 Topología simplificada de una red Empresarial con OPNET Modeler.

Como resultado de las corridas de la simulación debe determinar el comportamiento de: la Razón de Transferencia (Throughput), Latencia o Retardo, Utilización de la Red, Utilización de los servidores y de los nodos de comunicación (routers, switch etc.), Tiempo de Respuesta de las aplicaciones, etc.
La simulación de redes ofrece las posibilidades siguientes:

- Un medio de probar cambios propuestos antes de ejecutarlos.
- Un medio de realizar un análisis de la confiabilidad de los elementos principales en una red.
- Un medio de valorar la situación ante pérdidas de elementos componentes.
- Un medio de planear el futuro crecimiento de la red.
- Un medio de diseño inicial de una red propuesta.

No debe olvidar que u*n modelo de simulación es una representación simplificada de un sistema, posibilitando estudiar el comportamiento y las propiedades del sistema*

Documentación

Esta tarea a veces es menospreciada o dejada para después, pero sin embargo es de vital importancia para poder posteriormente realizar las tareas de mantenimiento, reparación o modernización de cualquier red. Además de que es muy frecuente de que se cambie el personal de administración de una red y el nuevo personal no encuentre ninguna documentación.
Con el desarrollo de la computación hoy se disponen de diversas herramientas de software para el dibujo de planos lógicos y planos físicos.
La documentación consta de:

a) Plano físico de cada una de las instalaciones que abarca la red LAN (planta, edificios, campo, etc.)
b) Planos de conexiones lógicas de cada subred y la Red completa
   Los planos lógicos de la red que dan una visión de toda la Red, sirviendo además en caso de detección de problemas como para la implementación de futuras expansiones.
c) Plano de la Interconexión de los puertos de los Conmutadores y Enrutadores en los armarios y cuartos de control
d) Tablas de direccionamiento IPv4 e IPv6 empleado a cada nivel.
e) Tablas de Rutas
f) Tablas NAT
g) Tablas con las Redes VLAN.
h) Programas de configuración de cada Conmutador y cada Enrutador
i) Tablas y Gráficos de los principales parámetros que miden el desempeño de la red. Los resultados de las corridas ejecutadas con los principales resultados alcanzados en los diferentes escenarios. Recuerde que no basta con una corrida para considerar resultados fiables.

Es importante resaltar que una Red con una buena documentación reduce drásticamente los problemas al enfrentar el montaje y operación posterior.
Con este paso finaliza todo el proceso de diseño de una Red LAN, sin embargo producto de influencia en el montaje y pruebas, se van a resaltar algunos aspectos.

Montaje de una Red

El documento proyecto es la base para el montaje y ejecución de una red, y por lo tanto debe ser fácilmente inteligible por cualquier técnico.. Sin embargo es necesario tener en cuenta que las distintas partes del proyecto pueden ser utilizadas por personas diferentes y de muy diversa formación.
Así la parte descriptiva de la memoria no debe entrar en consideraciones de índole técnica que pueda escapar al alcance de quien solo desee adquirir una idea general de lo proyectado, mientras que en la parte justificativa se desarrollan los diseños y soluciones adoptadas. Por otra parte existen dos

documentos con carácter vinculante: los planos y el pliego de condiciones que deben ser cuidados al detalle.

El objetivo de la Memoria es dar una idea general del proyecto y generalmente se divide en tres partes: memoria justificativa, memoria descriptiva y cálculos. Sin embargo es una práctica común no separar las memorias descriptiva y justificativa y realizar una descripción del diseño a la vez que se justifica la solución adoptada, por lo que los cálculos aparecen en anejos de memoria.
La memoria llevará tantos documentos anexos como el proyectista considere oportuno, siendo los más usados el anejo de cálculos o el estudio de la distribución en planta, entre otros que se comentarán más adelante.

Para el montaje de una red hay que tomar en consideración diferentes normas internacionales y nacionales, tales como:

- Normativa sobre compatibilidad electromagnética (R.D 444/94)
- EN 55022/CISPR-22 clase A y B , sobre emisiones radioeléctricas.
- EN 50082-1 la misma es un estándar sobre la inmunidad electromagnética en las instalaciones.
- IEEE 802.3 que define diferentes tipos de red (denominados genéricamente redes Ethernet) que tienen en común la utilización del mismo protocolo de acceso al medio MAC (CSMA/CD). Dentro de esta normativa se encuentra la 10/100 Base T.
- IEEE 802.1D, 802.1Q, 802.1X, para las redes LAN conmutadas

De forma especial todas las normas relacionada con el cableado estructurado:

- ISO/IEC 11801 Cableado estructurado de propósito general. Certifican la correcta instalación del cableado junto con las normas, ISO11803, EN50173 o la especificación TSB 67

Según la reestructuración realizada para los estándares ISO/IEC desde su segunda edición, los mismos han sido agrupados en una simple familia constituida por:

- ISO/IEC 11801ISO/11801--1 Condiciones Generales (estructura, dimensiones, canal, etc.)
- ISO/IEC 11801ISO/11801--2 Ambiente de Oficinas Comerciales
- ISO/IEC 11801ISO/11801--3 Ambiente Industrial
- ISO/IEC 11801ISO/11801--4 Ambiente Residencial
- ISO/IEC 11801ISO/11801--5 Centros de Datos (Data Center)
- ISO/IEC 11801-6 para empleo futuro.

Este ejercicio de reestructuración está completo y no incluye cambios técnicos y es utilizado como base para el desarrollo de la Tercera Edición de la ISO/IEC 11801 (3.0).

- **ANSI/TIA-568 Cableado de telecomunicaciones en edificios comerciales**

En 1991 la TIA publicó su primer estándar de Cableado de Telecomunicaciones para un edificio comercial conocido como ANSI/TIA-568. Este fue el primer estándar que definió un sistema de telecomunicaciones genérico que podía apoyar ambientes de múltiples productos y de múltiples vendedores. Lo que permitió que los sistemas de cableado pudieran ser planificados e instalados sin un plan para equipos de telecomunicaciones específicos.
Igual que con el estándar ISO/IEC 11801, su contraparte de la ANSI/EIA/TIA ha evolucionado y a grandes rasgos podemos enumerar su transición hasta la actualidad:

La serie 568-A fue el estándar inicial en el año 1991
La serie 568-B reemplazó a la 568-A en el año 2001
La serie 568-C reemplazó a la 568-B en el año 2009
La serie 568-D reemplazó a la 568-C en el año 2015

ANSI/TIA – 568 D (2015)
La norma o estándar 568-D toma en cuenta nuevos aspectos en el desarrollo de la redes de comunicaciones y computadoras, así como en las tecnologías de cables. Pero la misma se mantiene muy relacionada con su precedente 568-C como se podrá apreciar a continuación:

ANSI/TIA-568.0-D Cableado de Telecomunicaciones Genérico para Instalaciones de Clientes. Se confirma en septiembre de 2015. Se incorporaron los contenidos de TIA-568-C.0-1 (referencias actualizadas) y TIA-568-C.0-2 (actualizaciones generales). Los requisitos para el cableado de oficinas abiertas (es decir, puntos de consolidación, conjuntos de tomas de telecomunicaciones multiusuario) se han trasladado a esta Norma. Se requiere cableado de categoría 5e o superior para todos los despliegues de cableado de par trenzado genérico equilibrado.

ANSI / TIA-568.1-D Cableado de Telecomunicaciones en Edificios Comerciales, publicado en septiembre de 2015. Los cambios significativos de la edición anterior incluyen: Una nota que indica que el cableado horizontal de categoría 6A puede ser necesario para soportar una gama más amplia de aplicaciones se ha añadido. Los requisitos para el cableado de oficina abierta (es decir, puntos de consolidación, conjuntos de tomas de telecomunicaciones para varios usuarios) se han trasladado a TIA-568.0-D. Se incorporaron los contenidos de TIA-568-C.1-1 (vías y espacios) y TIA-568-C.1-2 (actualizaciones generales).
ANSI / TIA-568.2-D Cables de pares trenzados balanceados.
ANSI / TIA-568.3-D Cables de fibra óptica

Otras especificaciones de vital importancia a tener en consideración para el montaje son:

- ***ANSI/EIA/TIA-569-B*** *"Commercial Building Standard for Telecommunications Pathways and Spaces".* Esta se refiere a los llamados espacios de telecomunicaciones, donde se incluyen las áreas de trabajo, los closets de Telecomunicaciones, las habitaciones para equipos, las facilidades de entrada y salida, consideraciones ambientales, medidas, aterramiento de los conductores, etc. La misma está vigente desde octubre del 2004.
- ***ANSI/EIA/TIA -606-B***"Administration Standard for the Telecommunications Infrastructure of Commercial Building". Son recomendaciones sobre la documentación y registros de la información del sistema.
- ***ANSI/EIA/TIA -607-B***"Grounding and Bonding Requirements for Telecommunications in Commercial Building". Recomendaciones de tierra y en las uniones.
- ***ANSI/EIA/TIA- 758-B "***Customer-Owned Outside Plant Telecommunications Infrastructure Standard". Para Infraestructura de telecomunicaciones de planta exterior.
- **ANSI/TIA-862**: "Building Automation Systems Cabling Standard for Commercial Buildings",

Pruebas a la red
Evaluar el propósito de la inversión o actualización en términos de:

- Velocidad: La necesidad de una mayor velocidad es probablemente una de las principales razones para la actualización de una red. Esto significa actualizar el hardware, tales como routers o los enlaces.
- Retardo de transferencia (Latency) Otro aspecto que afecta la eficiencia de una red es la latencia (retardos de transferencias) dentro de la red. Ello puede ser de hardware o enlaces lentos, protocolos ineficientes, servicios de aplicación lentos (por ejemplo mensajes lentos a través de un servidor SMTP). En otros casos los problemas de latencia pueden ser causados por la necesidad

de conversión de protocolos, controles de acceso y seguridad, retrasos como función de la distancia etc.

También están otros elementos tales como:

a) Número de usuarios
b) Tolerancia de fallos
c) Expansión futura.

Se debe considerar también el propósito de la LAN en términos de:

- Facilidad de expansión.
- Aplicaciones futuras.
- Interconexiones futuras redes LAN.

La recolección, comparación y análisis del desempeño y operación de una red es esencial para hacer una justificación práctica de la actualización de una red. Muchas herramientas en el mercado soportan el monitoreo de la red y la recolección de datos.

Que elementos de medida se deben tomar en consideración:

a) tráfico entre conmutadores (switch-to-switch)
b) carga del enlace
c) utilización por puerto y por canal en los Conmutadores y Enrutadores . Algunos establecen que cuando esta excede el 50% debe actualizarse. Mientras que otros establecen que para un Hub es del 35%.
d) carga total de la red y flujo lógico de datos(desde cual grupo hacia donde)
e) razón de errores de transmisión
f) utilización de los servidores
g) malfuncionamiento de los servidores etc.

Muchos de esos parámetros pueden ser evaluados mediante la modelación y simulación de la red.

La simulación de redes ofrece las posibilidades siguientes:

- Un medio de probar cambios propuestos antes de ejecutarlos.
- Un medio de realizar un análisis de la confiabilidad de los elementos principales en una red.
- Un medio de valorar la situación ante pérdidas de elementos componentes.
- Un medio de planear el futuro crecimiento de la red.
- Un medio de diseño inicial de una red propuesta.

No debe olvidar que u*n modelo de simulación es una representación simplificada de un sistema, posibilitando estudiar el comportamiento y las propiedades del sistema*.

Las estadísticas o **p**arámetros que demuestran el buen funcionamiento de la red actual y futura (incluyendo escenarios con mayores cantidades de usuarios y aplicaciones).

Gestión o administración de la Red Corporativa

Para monitorear una red y colectar mediciones en tiempo real se necesitan ejecutar las acciones siguientes:

- Determinar qué tipo de información se necesita y como se quiere representar (por ejemplo si se quiere tomar mensajes de alerta SNMP provenientes de Enrutadores o Conmutadores.
- Determinar que herramienta utilizar (por ejemplo RMTG, NAGIOS, Netflow, etc.)
- Determinar que se va a monitorear y como (por ejemplo si es importante obtener de forma detallada una visión en forma real de un conmutador).
- Establecer una comparación entre lo medido y una referencia.
- Observar las tendencias y planificar acerca de lo que necesita actualizar.

Simulación de la Red

Luego para probar la red diseñada, utilizará la Herramienta Packet Tracert (versión para estudiantes) lo que le permitirá realizar pruebas de conectividad de los equipos y otras pruebas para responder a las interrogantes siguientes:

¿Están siendo los paquetes IP v4 e IP v6 encaminados correctamente?
¿Está trabajando bien el NAT interno y externo?
¿Está trabajando correctamente los protocolos RIP y OSPF?
¿Están todas las redes incluidas en las tablas de rutas?
¿Funcionan bien los servidores (web, mail, ftp, VoIP, video, etc.)?
¿Funcionan bien las políticas de seguridad, en especial las ACL ?
¿Funcionan bien las redes LAN virtuales (VLAN)?
¿Están trabajando correctamente los túneles y dobles pilas IP V4 – IP V6?
¿Está funcionando adecuadamente el Cortafuegos (Firewall)?
¿Están funcionando bien los servidores Proxies?

No debe olvidar que u*n modelo de simulación es una representación simplificada de un sistema, posibilitando estudiar el comportamiento y las propiedades del sistema*.

Para demostrar el buen desempeño de la red Corporativa diseñada utilizará la Herramienta OPNET Modeler, con ello responderá:

¿Cuál es el desempeño de la red (retardo y razón de transferencia)?
¿Cuál es el tiempo de respuesta de las aplicaciones?
¿Cuál es la utilización de los servidores?

Para justificar lo anterior hay que documentarlo en un informe donde se muestren las pruebas realizadas y los resultados obtenidos (tablas, gráficos, etc.)

Informe

Se recuerda que el informe se realizará acorde a lo indicado y en especial en el desarrollo seguirá paso a paso lo anteriormente explicado que se vuelve a plasmar:

- ✓ Planos físicos y lógicos de la Red con sus equipos e interconexiones.
  En especial se levantará el plano físico y de conexiones lógicas del cuarto de telecomunicaciones de la red corporativa.
- ✓ Tablas de asignación de las direcciones IPv4 e IPv6 de la red Corporativa
- ✓ Identificación de las VLAN con su puertos y direcciones IP
- ✓ Tablas de Ruta de los Protocolos de Enrutamiento para la red Corporativa
- ✓ Servicios de DHCP y DNS seleccionados para la red Corporativa.
- ✓ Aplicaciones típicas y nuevas seleccionadas para la red Corporativa.
- ✓ Servidores y equipos seleccionados (hojas de datos en anexos).
- ✓ Configuración de cada uno de los equipos y servicios para la Red Corporativa (programas en CLI de cada equipo)
- ✓ Análisis de tráfico de las aplicaciones más importantes en la red (escenarios diseñados y simulados)
- ✓ Resultados de las corridas que demuestren el mejoramiento del desempeño (gráficos y curvas con el análisis de los parámetros)
- ✓ Medidas de Seguridad de la red adoptadas
- ✓ Herramientas de Gestión o Administración de la red
- ✓ Demostración práctica de las pruebas realizadas a la red Corporativa

Bibliografía :

1. Alvarez Paliza Félix, Notas del profesor, Tema “Interconexión de Redes”, disponible en \\10.12.1.68\FIE\Carreras\Telecom y Electrónica\Redes II.
2. ARUBA, ARUBA CAMPUS FOR LARGE NETWORKS Design & Deployment Guide, Noviembre de 2019.
3. Cisco validated design, Campus LAN and Wireless LAN Design Guide, January 2018
4. Cisco, Cisco Collaboration System 12.x SRND, Network Infrastructure Chap.3, March 1, 2018, pp 3-1 a 3-78**.**
5. Ruckus,Enterprise Campus Network Design Guide, Febrero 2019
6. Silvia Hagen, IPv6 Essentials, Third Edition, O`Really, 2014
7. Michael Doodley and Timothy Rooney, IPv6 Deployment and Management, John Wiley & Sons, Inc. 2013
8. **Cisco,** IPv6 Addressing White Paper, 2012
9. **SURFnet**, Preparing an IPv6 Address Plan Manual, Version 2, 18 September 2013.
10. **Metzler Jim**, Top 3 Factors Driving Campus LAN Redesign, Ashton, Metzler & Associates, 2012.
11. **Joseph Davies**, Understanding IPv6, 3era Edición, O´Really Media, 2012.
12. **Larry Peterson and Bruce S. Davie,** Computer Networks a System Approach, Morgan Kauffman , 2012
13. **ORACLE,** System Administration Guide: Planning and IPv6 addressing Scheme, Chapter 3, 2011, disponible en http://docs.oracle.com/cd/E19082-01/819-3000/ipv6-planning-1/index.html
14. Yu-Wei Eric Sung, et.al, Towards Systematic Design of Enterprise Networks, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 19, NO. 3, JUNE 2011.
15. Bound J., IPv6 Enterprise Network Scenarios, RFC 4057, June 2005.
16. Chown T.,Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, RFC 4554, Junio 2006.
17. **Gagliano Roque,** Planificando IPv6, disponible en sitio web de LACNIC, 2009.
18. **Shannon McF.,** Muninder S, Nikhil S., Sanjay H.,” IPv6 for Enterprise Networks (Networking Technology)”, Cisco Press, Abril 2011.

SITIOS WEB ÚTILES

AREAS DE INTERÉS	ORGANIZACIÓN	SITIOS
Internet standards and RFCs	Internet Society /IETF/ RFC editor	www.rfc-editor.org
	Internet Archives	www.faqs.org/rfcs/
	Network Coordination Centre)	www.ripe.ne
	LACNIC	**www.lacnic.net**
International telecommunications standards	International Telecommunications Union	www.itu.int
	ITU-T recommendations publications/index.html	www.itu.int/ITUT/
	Institution of Electrical and Electronics Engineers (IEEE)	www.ieee.org
	International Organization for Standardization (ISO)	www.iso.org

	International Electrotechnical Commission	www.iec.ch
Protocols	General protocols	www.protocols.com www.networksorcery.com
	Committee	http://grouper.ieee.org/groups/802/
IPv6	**IPv6 forum**	**www.ipv6forum.com**
	Portal IPv6Cuba	**http://www.cu.ipv6tf.org**
		✓ - **http://portalipv6.lacnic.net/**
		✓ - **http://www.ipv6tf.org/**
		✓ - **http://www.ipv6forum.org/**
		✓ - **http://www.ipv6ready.org/**
		✓ - **http://getipv6.info/**
		✓ - **http://www.cisco.com/IPv6/**
		✓ - **http://www.microsoft.com/ipv6**
Router and Network		
	Cisco Systems	www.cisco.com
	Extreme Networks	www.extremenetworks.com
	Foundry Networks	www.foundrynet.com
	Juniper Networks	www.juniper.net
	Lucent Technologies	www.lucent.com
	Northern Telecom (Nortel)	www.nortelnetworks.com
	3 Com	www.3com.com
	Huawei	www.huawei.com
LAN Design	**Cisco Small Enterprise Design Profile (SEDP)—Network Foundation Design**	**http://www.cisco.com/en/US/docs/solutions/Enterprise/**
	Brocade	**www.brocade.com/campusnetwork**.
	Allied Telesys	**alliedtelesys.com**
IP Address Tools		
	NetDot	**www.netdot.uoregon.edu**
	HaCi	**www.sourceforge.net/projects/haci**
	IPAT	**www.nethead.de/index.php/ipat**
	ipv6gen	**www.techie.devnull.cz/ipv6/ipv6gen/**
	sipcalc	**www.routemeister.net/projects/sipcalc/**
	freeipdb	**www.home.globalcrossing.net/~freeipdb/**