MODULO

REDES LOCALES AVANZADO- ELECTIVA

AUGUSTO ALBERTO DAVID MEZA
MARDELIA YOLIMA PADILLA SANTAMARIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍAS E INGENIERÍA
PROGRAMA DE INGENIERIA DE SISTEMAS
BOGOTA D.C., 2007

TABLA DE CONTENIDO

INTRODUCCION

El curso de Redes Locales Avanzado es fundamental para el desarrollo profesional del ingeniero de sistemas. Es un curso que le suministrara al ingeniero de sistemas los fundamentos teórico- prácticos en lo que se refiere a su desempeño como administrador de redes en cualquier empresa, abarcando aspectos que van desde el uso de tecnologías de interconexión hasta la administración y protección de los recurso de una red.

Este curso también pretende que el ingeniero de sistemas desarrolle capacidades para solucionar las diferentes problemáticas que se presentan en el momento de realizar el análisis, diseño y montaje de redes.

El curso de redes Locales avanzado tiene 3 créditos y esta compuesto por 3 unidades didácticas que se describen a continuación:

Unidad 1. El modelo OSI en la LAN: pretende que el estudiante enfoque el modelo de referencia OSI como un modelo aplicado en la practica, comenzando con la capa física donde el estudiante descubre como realizar instalaciones de medios de transmisión en la LAN basados en los estándares tanto del cableado estructurado, como de las redes inalámbricas. Analizar el comportamiento de las redes Lan basadas en cualquiera de las arquitecturas de la capa de enlace y profundizar en temáticas como la interconexión de redes por medio de protocolos de la capa de red y el servicio que brinda la capa de transporte para garantizar una verdadera calidad de servicio.

La Unidad 2. Administración de Redes: Inicialmente se hace una introducción a la administración de redes: donde se trata de explicarles las diferentes herramientas administrativas con que cuenta el estudiante y que le permiten organizar la red que estén administrando y solucionar los diferentes problemas que se le puedan presentar durante el desarrollo de sus funciones de administrador de red. Posteriormente se profundiza en teas como la administración y configuración de servidores: en esta parte el estudiante aprende a configurar los diferentes servidores de la red, posibilitando servicios de correo electrónico, transferencia de archivos, DHCP entre otros. Además se identifican los aspectos fundamentales a tener en cuenta para mantener el rendimiento de una red y la forma de solucionar problemas que se presenten en un punto determinado de la red.

Unidad 3. Seguridad en Redes. Se realiza una introducción en lo que refiere a aspectos de seguridad informática como son las amenazas de seguridad a las que esta expuesta una red y las diferentes políticas de seguridad que se deben implantar en la empresa comenzando con las bases de la criptografía y luego profundizando en los algoritmos y protocolos de encriptación de tal forma que se puedan garantizar aspectos como la integridad, disponibilidad y privacidad de la información. En esta última unidad también se profundiza en las temáticas

referentes la seguridad aplicada, indicándole al estudiante la forma efectiva de establecer estrategias de seguridad como son el Firewall, Las firmas y certificados digitales, además de otras técnicas como las biométricas y las esteganográficas, que garanticen la integridad, disponibilidad y privacidad de la información. En el momento de realizar cualquier transacción electrónica que involucre el uso de la red.

El curso de Redes Avanzado esta orientado a brindarle al estudiante las herramientas necesarias para el diseño y montaje de redes seguras de alto rendimiento y además suministrarle las habilidades necesarias que le permitan una correcta administración de los recursos que ofrecen las mismas.

PRIMERA UNIDAD: EL MODELO OSI EN LA LAN

INTRODUCCION

En esta unidad se pretende que el estudiante visualice el modelo de referencia OSI como un modelo aplicado en la práctica, cambiando el enfoque tradicional teórico que siempre se maneja cuando se habla del modelo OSI.

El primer capitulo se fundamenta en los principios de la capa física refiriéndose a los medios de transmisión guiados utilizados en la LAN, las diferentes aplicaciones de los mismos y su utilización en los sistemas modernos de cableado estructurado de los edificios. También se plantean temáticas sobre los dispositivos activos de red de la capa física y por supuesto los diferentes estándares que rigen las comunicaciones inalámbricas en la LAN.

En el segundo capitulo se analiza el comportamiento de las redes Lan basadas en las arquitecturas de la capa de enlace y se profundiza en temáticas referentes a las diferentes tecnologías de los dispositivos activos de red que trabajan en la capa de enlace.

El tercer capitulo profundiza en temáticas como la interconexión de redes por medio de protocolos de la capa de red, el uso del direccionamiento IP y la implementación de subredes.

El cuarto capitulo hace referencia al servicio que brinda la capa de transporte, lo diferentes protocolo que intervienen en este nivel y técnicas que debe aplicar el ingeniero de sistemas para garantizar el funcionamiento de redes que tengan un óptimo desempeño y ofrezcan una verdadera calidad de servicio.

OBJETIVOS

- Que el estudiante comprenda el modelo OSI como un modelo Práctico aplicado en las redes de área local.
- Que el estudiante conozca las características de los diferentes medios de transmisión y su adecuada utilización en redes LAN.
- Que el estudiante conozca y aplique los diferentes estándares actuales que se aplican en las redes de área local.
- Que el estudiante adquiera habilidad en el diseño de soluciones para montaje físico y lógico de redes de área local.

CAPITULO 1: LA CAPA FISICA

1.1 Los Medios de Transmisión

La capa física tiene la función de transmitir los bits puros por un canal de comunicación, además define las características eléctricas, mecánicas, funcionales y de procedimiento de la red. Dado lo anterior los medios guiados forman parte de la capa física pues su única función es transportar los bits puros de emisor a receptor.

En los medios transmisión guiados, la capacidad de transmisión, en términos de velocidad de transmisión, depende de los siguientes factores:

- El ancho de banda
- La distancia
- Numero de receptores

Para uso en la LAN se destacan los siguientes medios guiados:

- Par Trenzado
- Cable Coaxial
- Fibra Óptica

1.1.1 El Par Trenzado

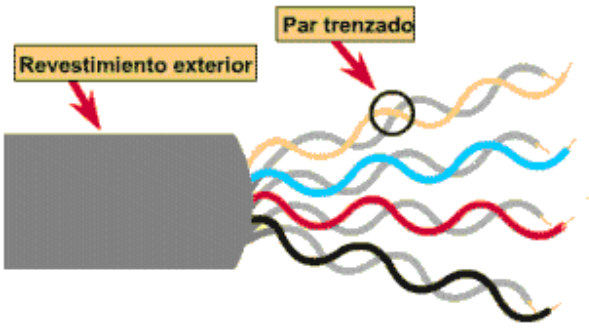


Figura 1.1. Cable Par trenzado.

El par trenzado (ver figura 1) consiste en dos cables de cobre embutidos en un aislante entrecruzados en forma de espiral. Cada cable constituye sólo un enlace

de comunicación. Típicamente, se utilizan haces en los que encapsulan varios pares mediante una envoltura protectora.

En aplicaciones de larga distancia, la envoltura puede contener cientos de pares. Mientras que en las redes de área local normalmente se utiliza el cable de 4 pares.

El uso del trenzado tiende a reducir las interferencias electromagnéticas (diafonía) entre los pares adyacentes dentro de una misma envoltura. Para este fin, los pares adyacentes dentro de una misma envoltura protectora se trenzan con pasos de torsión diferentes. Típicamente, los hilos se trenzan para reducir la interferencia y la longitud del trenzado varía dependiendo del tipo de par trenzado y se sabe que entre mas trenzas por unidad de longitud existan mayor es su inmunidad a la interferencia. Los conductores que forman el par tienen un grosor que varía típicamente entre 0,04 y 0,09 pulgadas.

Aplicaciones

Tanto para señales análogas como para señales digitales, el par trenzado es con diferencia el medio de transmisión más usado y sus aplicaciones son las siguientes:

- Es el medio más usado en las redes de telefonía
- Su uso es básico en el establecimiento de redes de comunicación dentro de edificios.
- En aplicaciones digitales, para las conexiones al conmutador digital o a la PBX digital, con velocidades de hasta 64 Kbps.
- El par trenzado es el medio de transmisión más utilizado en redes de área local. La velocidad típica en está configuración está en torno a los 100Mbps. No obstante, recientemente se ha desarrollado redes de área local con velocidades de 1000Mbps, aunque estas configuraciones están bastantes limitadas por el número de posibles dispositivos conectados y extensión Geográfica de la red.
- Es el medio recomendado por los estándares internacionales para conexiones en redes de área local en implementaciones de sistemas de cableado estructurado para edificios.
- Para aplicaciones de larga distancia el par tranzado se puede utilizar a velocidades de 4 Mbps o incluso mayores.

Características De Transmisión

Los cables de pares se pueden usar para transmitir los siguientes tipos de señales:

- **Análogas**: Normalmente para redes Telefónicas u otro tipo a larga distancia, donde puede ofrecer más de 250 KHz de ancho de banda.

- **Digitales:** Normalmente para redes LAN, ofrece velocidades de 10, 100 o 1000 Mbps.

Comparando con otros medios guiados (cable coaxial y fibra óptica), el par trenzado permite:

- Menores distancias

- Menor ancho de banda

- Menor velocidad de transmisión.

- Tiene una fuerte dependencia de la atenuación con la frecuencia.

- Este medio se caracteriza por su gran susceptibilidad a las interferencias y al ruido

Para reducir estos afectos negativos es posible tomar algunas medidas. Por ejemplo, el apantallamiento del cable con malla metálica reduce las interferencias externas. El trenzado en los cables reduce las interferencias de baja frecuencias, y el uso de distintos pasos de torsión entre pares adyacentes reduce la diafonía.

Ventajas Del Par Trenzado

Algunas de las más importantes ventajas del par trenzado son las siguientes:

- Diámetro externo reducido

- Fácil de instalar

- Ahorra espacio

- Reduce congestión

- Universalidad de Aplicaciones

- Liviano
- Fácil conexionado
- Baja atenuación
- Transmisión Balanceada
- Efectos de crosstalk controlados
- Reducción del crosstalk sin necesidad de blindaje
- Uso de adaptadores para balanceo y eliminación de radiación al ambiente.
- Buena relación señal ruido(SER)
- Amplio ancho de banda

TIPOS DE PAR TRENZADO

Existen muchas variantes de pares trenzados:

- Apantallados (STP, FTP, S-FTP)
- Sin apantallar (UTP)

En este modulo se analizaran solamente los más utilizados en la LAN. El UTP y el STP.

UTP (Unshielded Twisted Pair): El par trenzado no apantallado (ver figura 2) es el medio habitual en telefonía. Actualmente es práctica habitual en el cableado de redes de área. Esto es así ya que hoy por hoy, el par sin apantallar es el menos caro de todos los medios de transmisión que se usan en las redes de área local, además de ser fácil de instalar y manipular.

El par trenzado sin apantallar se puede ver afectado por interferencias electromagnéticas externas, incluyendo interferencias con pares cercanos y fuentes de ruido.

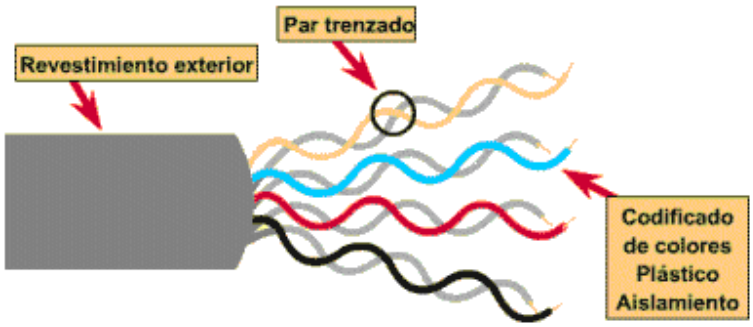


Figura 1.2. Par Trenzado No Apantallado

El cable UTP ha evolucionado y a través del tiempo han aparecido varias categorías:

Categoría 1: Solo soporta transmisión de voz este medio fue orientado para implementaciones telefónicas de la época.

Categoría 2: Soporta velocidades de 4 Mbps permitiendo transmisión de voz y datos como texto, archivos planos este cable no soporta características multimedia.

Categoría 3: Maneja frecuencias hasta 16 MHz y soporta velocidades de hasta 10 Mbps, tiene trenza cada 7 a 10 centímetro y es utilizado todavía en las redes Ethernet.

Categoría 4: Maneja Frecuencias hasta 20MHz y soporta velocidades de 16 Mbps. Este cable fue usado frecuentemente en arquitecturas Token Ring

Categoría 5: Maneja Frecuencias hasta 100MHz y Soporta velocidades de hasta 100 Mbps. El número de trenzas es del orden 1 a 2 por centímetro.

Categoría 5E: Es una mejora del 5, este cable también es denominado 100 Base T y es el Estándar actual recomendado para la LAN. Maneja frecuencias hasta 100 MHz y es utilizado en redes Fast Ethernet de 100 Mbps. También es compatible con redes Gigabits de 1000 Mbps

Categoría 6: Maneja frecuencias de hasta 250 MHz y soporta velocidades superiores a 1000 Mbps, este es un medio que es considerado revolucionario ya que los expertos nunca imaginaron que un cable de cobre alcanzaran estas velocidades, solo comparables con las alcanzadas por medios ópticos.

El cable UTP categoría 6 cada vez es mas utilizado en la LAN y ya los estándares lo recomiendan para las redes LAN.

Categoría 7: Alcanza velocidades superiores a los 10 Gbps, manejando frecuencias de hasta 600 MHz. Este estándar especifica 4 pares blindados individualmente dentro de otro blindaje.

STP (Shielded Twisted Pair) El par trenzado apantallado (ver figura 3) es una manera de mejorar las características de transmisión del UTP colocándolo dentro de una malla metálica, reduciéndose así las interferencias. Este cable proporciona mejores resultados a velocidades de transmisión bajas. Ahora bien, este último es más costoso y difícil de manipular que el anterior.

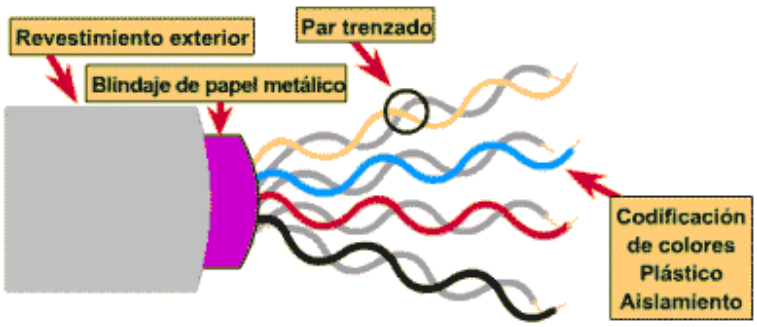


Figura 1.3. Par Trenzado Apantallado

STP Vs UTP

A continuación se comparan los cables STP y UTP:

- Un cable STP no provee por si solo inmunidad al ruido
- La pantalla del cable STP afecta la capacidad distribuida del cable limita la velocidad de transmisión
- El cable STP resulta más costoso
- El cable UTP es capaz de rechazar el ruido igual que un STP

Conectores Del Par Trenzado

El conector utilizado en las instalaciones del cable par trenzado en redes de área local es el Rj 45 (Ver figura 4). Se caracteriza por disponer de ocho pines, muy parecido al que se usa en aplicaciones telefónicas el Rj 11 que solo posee cuatro pines.

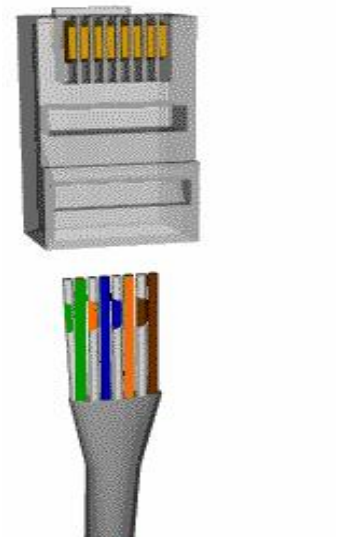


Figura 1.4. Conector Rj 45.

1.1.2 El cable Coaxial

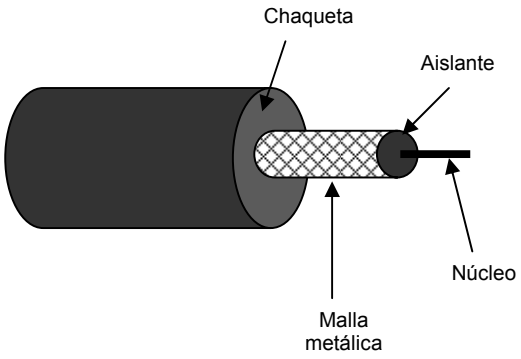


Figura 1.5. El Cable Coaxial

El cable coaxial (Ver figura 5), al igual que el par trenzado, tiene dos conductores pero está construido de forma diferente para que pueda operar sobre un rango mayor de frecuencias.

Sus componentes son los siguientes:

- ***Núcleo:*** Conductor central por donde se transmite la señal, puede ser macizo o trenzado. Normalmente el núcleo es de cobre, pero también existen presentaciones en aluminio.

- ***Aislante o dieléctrico:*** Es el material que recubre el núcleo su función es aislarlo de las interferencias, además de evitar un corto circuito del núcleo con la malla.

- ***Malla Metálica***: su función es la de llevar todas las señales redundantes a tierra, además de servir de referencia para la comunicación.

- ***Chaqueta***: Es el recubrimiento del cable, normalmente es elaborado de PVC lo que lo hace un poco flexible, sin embargo algunos coaxiales resistentes a altas temperaturas son fabricados con un material que los hace mas rígidos pero resistentes a los incendios.

El cable coaxial puede soportar mayores distancias que el cable par trenzado.

Aplicaciones

El cable coaxial es quizá el medio de transmisión más versátil, por lo que está siendo cada vez utilizado en una gran variedad de aplicaciones. Las más importantes son:

- Distribución de televisión
- Telefonía a larga distancia
- Conexión con periféricos a corta distancia
- Redes de área local

El coaxial tradicionalmente fue un cable utilizado en la LAN, sin embargo actualmente ya no es recomendado por los estándares Internacionales para implementaciones de sistemas de cableado estructurado.

Tipos

Para uso en la LAN tradicionalmente se recomendaron dos tipos de coaxial:

- ***Fino:*** llamado también 10Base2, esto quiere decir que trabaja a 10 Mbps en sistema banda base y tiene una distancia útil de aproximada de 200 metros. Es un cable de aproximadamente 6mm de diámetro.
- ***Grueso:*** Llamado también 10Base5, esto quiere decir que trabaja a 10 Mbps en sistema banda base y tiene una distancia útil de 500mts, es más rígido que el anterior con un diámetro aproximado de 12 mm. Su uso principal en la LAN estaba orientado a servir como columna vertebral.

Como norma general, cuanto más grueso es un cable, más difícil es trabajar con él. El cable fino es más flexible, fácil de instalar y relativamente barato. El cable grueso no se dobla fácilmente y, por lo tanto, es más difícil de instalar. Éste es un punto importante a considerar cuando la instalación requiere la introducción del cable en espacios reducidos, tales como canaletas, tubos u otro tipo de conducciones. El cable grueso es más costoso, pero tiene la ventaja de llevar las señales a mayores distancias.

Conectores Del Coaxial

Los conectores utilizados para el cable coaxial son los tipo BNC (ver figura 6.) los cuales pueden ser Cilíndricos simples, en T, Tipo empalme y terminadores.

Figura 1.6. Conectores BNC

1.1.3 La Fibra Óptica

La fibra óptica es un medio flexible y extremadamente fino (de 2 a 125um), capaz de conducir energía de naturaleza óptica. Para la fibra se puede usar diversos tipos de cristales y plásticos cada material ofrece sus propias características:

- Las perdidas menores se han conseguido con la utilización de silicio fundido ultra puro.

- Las fibras ultra puras son muy difíciles de fabricar.

- Las fibras de cristal multicomponente tienen mayor perdida y son más económicas, pero proporcionan unas prestaciones suficientes.

- La fibra de plástico tiene todavía un coste menor y se pueden utilizar para enlaces de distancias cortas, para lo que son aceptables perdidas moderadamente altas.

Un cable de fibra óptica (ver figura 7) tiene forma cilíndrica y está formado por tres secciones concéntricas:

El núcleo: Es la sección más interna, está constituido por una o varias hebras o fibras muy finas de cristal o plástico. Su indice de refracción es mayor que el del revestimiento.

Revestimiento: Cada fibra está rodeada por su propio revestimiento, que no es sino otro cristal que envuelve al núcleo.

La cubierta: está hecha de plástico y otros materiales dispuestos en capas para proporcionar protección contra la humedad, la abrasión, aplastamientos y otros peligros.

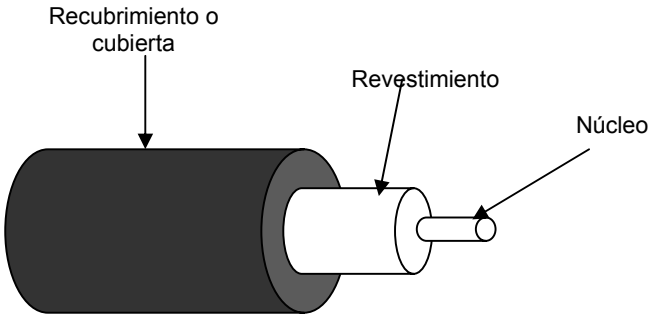


Figura 1.7. Estructura básica de la fibra óptica

Aplicaciones

El desarrollo de los sistemas de comunicación de fibra óptica ha sido uno de los avances tecnológicos más significativos en la transmisión de los datos.

La fibra óptica en los últimos años ha disfrutado de una gran aceptación en el montaje de muchas infraestructuras de comunicación entre las cuales se destacan:

- Las telecomunicaciones a larga distancia
- Redes de área metropolitana
- Acceso a áreas rurales.
- Servicios de última milla.
- Los entornos LAN.

En el entorno Lan la fibra óptica utilizada es la multimodo que se explicara con más detalle en las siguientes secciones, esta fibra se instala como cable central que soporta el gran trafico de información de una empresa evitando los indeseables cuellos de botella.

Diferencias con otros medios guiados

Las características diferenciales de la fibra óptica frente al cable coaxial y el par trenzado son:

- Mayor ancho de banda
- Menor tamaño y peso
- Atenuación menor
- Aislamiento electromagnético
- Mayor separación entre repetidores

Tipos de fibra óptica

Existen dos tipos de fibra óptica:

- **Multimodo (fibra índice gradual, fibra índice escalonado)**
- **Monomodo**

Fibra Multimodo

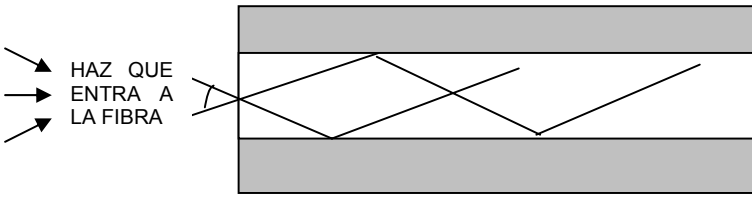


Figura 1.8. Fibra óptica Multimodo

Es la fibra óptica más utilizada en la LAN, su funcionamiento se basa en el transporte de varios haces de luz (modos) simultáneamente, donde los modos que parten con un ángulo de inclinación menor recorren mayores distancias debido a que experimentan un menor numero de rebotes con el revestimiento, este comportamiento es el que hace que la fibra multimodo no soportes grandes distancias debido a que cada vez que un haz de luz se refleja experimenta perdida de energía. La fibra multimodo normalmente tiene un diámetro de 62.5/125 micras esto es una relación núcleo revestimiento, sin embargo existen fibras multimodo con otros diámetros que no son tan comerciales.

En la fibra óptica multimodo ocurre la dispersión Modal la cual se produce debido a que cada modo recorre diferentes caminos, dando como resultado que los modos lleguen al otro extremo de la fibra en tiempos diferentes, ensanchando los pulsos y disminuyendo por lo tanto la máxima velocidad de transmisión de datos. Su uso en la LAN esta enmarcado en su flexibilidad, peso y bajo costo en comparación con la monomodo.

La fibra óptica multimodo puede ser de dos tipos:

- ***Índice Escalonado***: El índice de refracción es constante en todo el núcleo y varia únicamente en el revestimiento.
- **Índice Gradual**: el índice de refracción varía a medida que los modos recorren el núcleo.

Fibra Monomodo

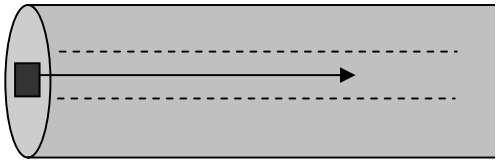


Figura 1.9. Fibra óptica Monomodo

El funcionamiento de la fibra monomodo o unimodo se basa en el transporte de un solo haz de luz (1 modo), generado por un emisor láser. La fibra óptica monomodo es mucho más delgada que la multimodo con un diámetro aproximado de 8 micras. Este funcionamiento hace que este tipo de fibra tenga una distancia útil mucho mayor que la fibra multimodo, además de una mayor capacidad, el rayo láser concentra gran cantidad de energía en un solo haz de luz y además al no rebotar la luz no existe perdida de energía constante como ocurre con la fibra multimodo.

La fibra monomodo no tiene mucho uso en la LAN, sin embargo es mas utilizada para grandes tróncales de comunicación en redes de área metropolitana o para interconectar ciudades. En los últimos años a tenido gran acogida en las implementaciones de cable submarino que incluso atraviesan grandes océanos.

Emisores y fotorreceptores de la fibra óptica

La fibra óptica utiliza dos clases de fuentes de luz para producir señales:

LED (Diodos Emisores de Luz): Utilizado principalmente en fibras ópticas multimodo. Presentan las siguientes características:

- Son muy económicos
- Se utilizan para enlaces de corta distancia
- Se fabrican para las tres ventanas de operación
- La luz generada por un LED cubre un ancho espectral amplio
- Tiempo de subida alto.

Láseres Semiconductores: Utilizados en las fibras monomodo. Presenta las siguientes características:

- Son más costosos
- Tienen un reducido ancho espectral
- Se utilizan para enlaces de larga distancia
- Alta potencia de salida
- Tiempo de subida bajo

La fibra óptica utiliza dos clases de fotodiodos receptores

PIN: Son fotorreceptores utilizados en la fibra multimodo, emiten un pulso eléctrico cuando son golpeados por un haz de luz producido por un LED.

APD: Son fotorreceptores utilizados en la fibra monomodo, emiten un pulso eléctrico cuando son golpeados por un haz de luz producido por un Láser.

Conectores de la Fibra Óptica

Existen muchos conectores para la fibra óptica y su instalación es cada vez más sencilla. La figura 1. 10 muestra los diferentes conectores para la fibra óptica.

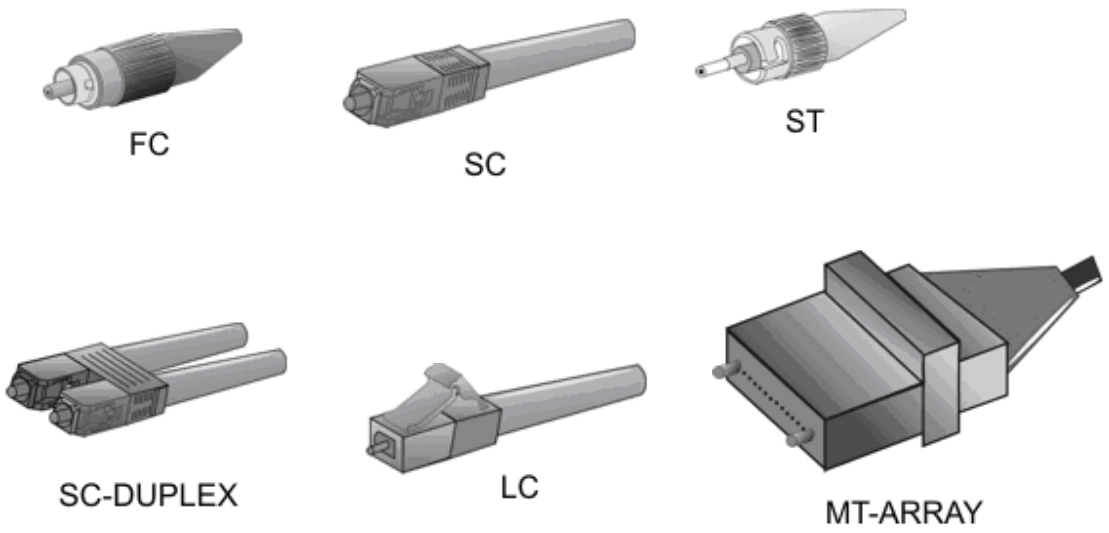


Figura 1.10. Conectores de la fibra óptica

Elección del cableado

Para determinar que tipo de cableado es el más adecuado para una determinada aplicación, se deben contestar las siguientes preguntas:

- ¿Qué cantidad de tráfico va a soportar la red?
- ¿Cuales son los requerimientos de seguridad de la red?
- ¿Que distancia va a tener la red?
- ¿Cuáles son las posibles opciones de cableado?
- ¿Cual de las opciones de cableado se ajusta a los estándares de cableado estructurado?
- ¿De que presupuesto para cableado se dispone?

Cuanto mejor proteja un cable contra la interferencia de otras señales eléctricas, mayor sea la distancia útil, velocidad de transmisión, calidad y seguridad mayor es su costo.

1.2 Sistema de cableado Estructurado

Definición

El cableado estructurado es un conjunto de dispositivos y cables que son propiamente instalados en un edificio o en un conjunto de ellos (campus), que pueden soportar a largo plazo todas las conexiones y servicios que requieran los usuarios.

Es una infraestructura confiable y con capacidad de habilitar en un edificio para todos los usuarios los servicios de telecomunicaciones en una única y sencilla estación de trabajo.

Garantiza la flexibilidad para su reconfiguración dinámica y para la implementación de tecnologías de punta en aplicaciones (paquetes) y equipos activos de acuerdo con los nuevos servicios y requerimientos de manejo de información.

El cableado estructurado esta orientado a la integración de servicios, para lo cual establece una serie de consideraciones propias de su infraestructura:

- Distancias predeterminadas
- Medios identificados
- Topología definida
- Arquitectura de sistemas abiertos
- Terminología utilizada por EIA/TIA
- De aplicación para voz, datos y videos
- Protección de la inversión
- Facilidad para administración

Antecedentes

Con la libertad que existía para la escogencia entre cables y conectores, se inicio una gran confusión y se creó un gran desorden en el cableado de redes.

Antes de la estandarización del sistema de cableado estructurado para edificios se presentaban las siguientes desventajas:

- Saturación de estructuras actuales para cableado

- Tiempo de instalación de nuevos servicios prolongado
- Inflexible a los cambios
- Adaptabilidad reducida y costosa
- Infraestructura de cables independientes
- Aumento de la demanda de servicios y de capacidad
- Imposible reutilización de la infraestructura actual
- Servicios aislados tanto técnica como administrativamente

Sin embargo las empresas empezaron a evolucionar lo que genero:

- Sofisticación creciente de usuarios finales
- Crecimiento de procesos de cómputo a nivel de escritorio
- La necesidad de los proyectos actuales de redes locales hacia:
    - Productividad
    - Manejabilidad
    - Protección a la inversión
    - Anticipación al futuro

Elementos del cableado estructurado

- Medios guíados
- Patch cord
- Conectores
- Tomas
- Paneles de recolección
- Gabinetes
- Rack
- Organizadores de cable
- Canaletas

Subsistemas del Cableado Estructurado

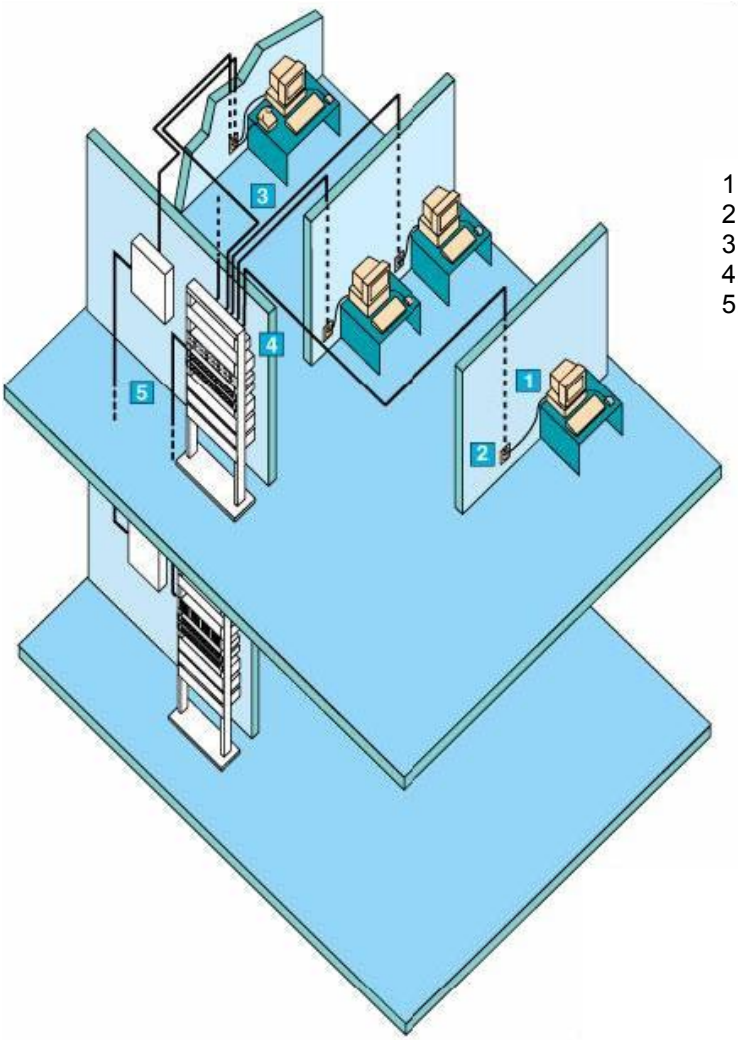


Figura 1.11. Subsistemas de cableado estructurado.

Los (ver figura 1.11) de un sistema de cableado Estructurado son:

- Entrada del Edificio
- Sala de equipo
- Cableado central
- Cuarto de telecomunicaciones

- Cableado horizontal
- Área de trabajo
- Campus

Entrada de construcción

La instalación de entrada del edificio da el punto en donde el cableado exterior entra en contacto con el cableado central interior del edificio. Los requerimientos físicos del contacto de red son definidos en el estándar EIA/TIA-569.

Sala de equipo

Los aspectos de diseño de la sala de equipo se especifican en el estándar EIA/TIA-569. Las salas de equipo, generalmente alojan componentes de mayor complejidad que los closets de telecomunicación. Cualquiera o todas las funciones de un cuarto de telecomunicaciones pueden estar disponibles en una sala de equipo.

Otros requerimientos de diseño

- Topología en estrella
- No más de dos niveles jerárquicos de interconexiones
- No se permiten derivaciones de puente
- Los puentes de interconexión principales e intermedias o cables de parcheo no deben exceder los 20 metros (66pies)
- Evitar su instalación en áreas donde puedan existir fuentes de altos niveles de EMI/RFI
- La conexión a tierra debe cumplir los requerimientos como se define en el EIA/TIA 607

Nota: se recomienda que el usuario consulte a los fabricantes del equipo, a las normas de aplicación y a los proveedores del sistema, por obtener información adicional cuando se planeen aplicaciones cubiertas compartidas en cables centrales UTP.

Cableado horizontal

(Topología Específica: en Estrella)

El sistema de cableado horizontal (ver figura 1.12) se extiende desde la toma de corriente de telecomunicaciones (información) del área de trabajo hasta el armario de telecomunicaciones y consiste en lo siguiente:

- Cableado horizontal
- Salida de Telecomunicaciones
- Terminaciones de cable
- Interconexiones

Se reconocen tres tipos de medios como opción para cableado horizontal, cada uno extendiéndose una distancia máxima de 90 metros:

1) cable 4- pareado 100 ohm UTP (conductores sólidos 24 AWG)
2) cables 2-pareado 150 ohm
3) cable de fibra óptica 2-fibra 62.5/125 um

Conforme la velocidad de transmisión ha aumentado el cableado de alto rendimiento se ha convertido en una necesidad. Además, debieron establecerse algunos medios para clasificar cables horizontales UTP y del equipo de conexión, por su capacidad de rendimiento. Estas capacidades han sido detalladas en una serie de categorías como sigue:

- Categoría 3
- Categoría 4
- Categoría 5
- Categoría 5e
- Categoría 6

Actualmente, el cable coaxial 50 ohm puede ser una opción como de tipo medio. Sin embargo, no es recomendado para instalaciones nuevas de cableado y se estima que su uso en la LAN se cambiará definitivamente.

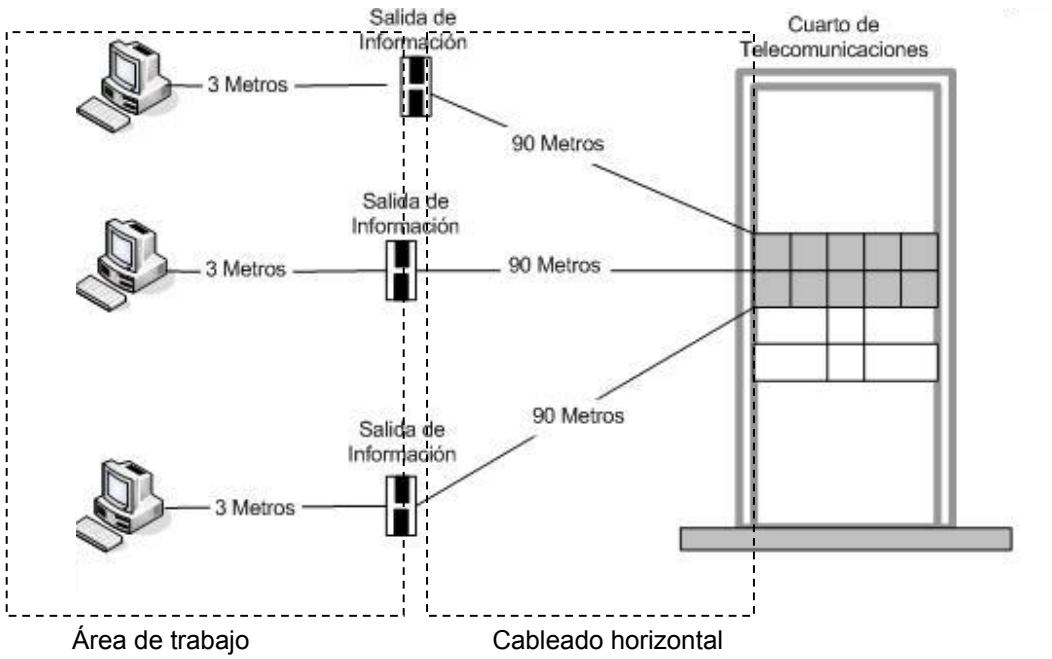


Figura 1.12.Subsistema de área de trabajo y Horizontal

Nota: Las distancias máximas especificadas arriba están basadas en transmisión de voz en UTP y transmisión de datos en STP y fibra. La distancia de 90 metros para STP corresponde a aplicaciones con una anchura de banda espectral de 20 Mhz a 300 Mhz. Una distancia de 90 metros también se aplica a UTP a anchuras de banda de 5Mhz-16Mhz para CAT 3, 10Mhz-20 Mhz para CAT 4 y 20 Mhz – 100MHz para CAT 5.

Sistemas de datos de menor velocidad como el sistema IBM36, 38, AS400 y asincrónicos (RS232, 422, 423, etc.) pueden obtener un UTP (o STP) para distancias considerablemente mayores –generalmente, desde varios cientos de pies hasta más de 1000 pies. Las distancias reales dependen del tipo de sistema, la velocidad de datos y las especificaciones del fabricante para el sistema electrónicos y los componentes asociados utilizados(es decir, balunes, adaptadores, conductores de cable, etc.). El estado actual de las instalaciones de distribución normalmente incluye una combinación de cables de cobre y fibra óptica en central.

Además de los 90 metros de cable horizontal, se permiten un total de 10 metros para área de trabajo y cuarto de telecomunicaciones provisionales y puentes.

Área de trabajo

Los componentes del área de trabajo se extienden desde la salida de información hasta el equipo de estación. El cableado del área de trabajo está diseñado de manera que sea sencillo el interconectarse, para que los cambios, aumentos y movimientos se puedan manejar fácilmente.

Los componentes de Área de Trabajo son:

- Cableado de parcheo- computadoras, terminales de datos, teléfonos, etc.
- Cableado provisionales- cables modulares, cables adaptadores de PC, puentes de fibra, etc.
- Adaptadores- balunes, etc. – deben estar fuera de las salidas de información.
- Cables par trenzado sin Blindar de 100 Ohms
- Sistema de cableado (UTP)

Tanto para el sistema de área de trabajo como para el horizontal se recomienda instalar el cableado aplicando las normas 568 A o 568 B (ver figura 1.13).

El uso de una de estas normas garantiza la interconexión de todos los puntos de la red ya que todos los fabricantes las implementas en sus productos.

Combinar normas no es recomendable, se aconseja utilizar una sola en toda la red, sin embarbo hay Switches inteligentes que pueden interconectar redes con diferentes normas.

Normas 568A Y 568B

N° PIN	568A	568B
1	BLANCO-VERDE	BLANCO-NARANJA
2	VERDE	NARANJA
3	BLANCO-NARANJA	BLANCO-VERDE
4	AZUL	AZUL
5	BLANCO-AZUL	BLANCO-AZUL
6	NARANJA	VERDE
7	BLANCO-CAFE	BLANCO-CAFE
8	CAFE	CAFE

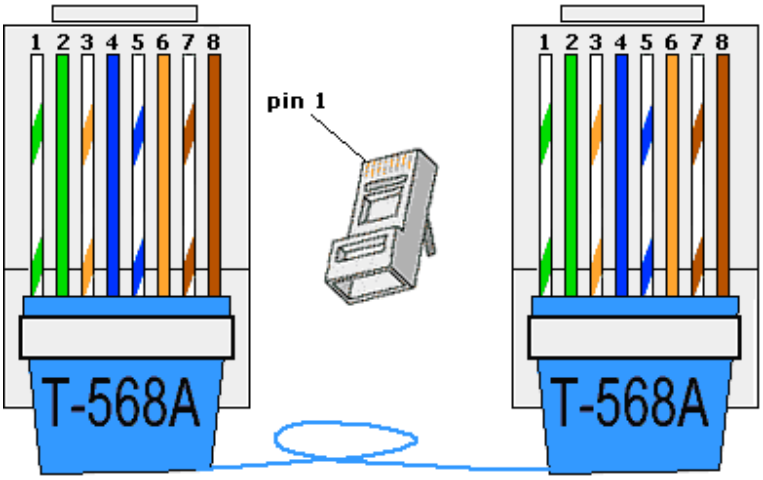


Figura 1. 13. normas 568A y 568B

Cableado vertical o central

El cableado central (ver figura 1.14) provee la interconexión entre los cuartos de telecomunicación, sala de equipo e instalaciones de entrada. Consiste en los cables centrales, interconexiones intermedias y principales, utilizado para interconexiones de central a central.

Esto incluye:

- Conexión vertical entre pisos (conductores verticales “riser”)
- Cables entre las sala de equipo y las instalaciones de entrada del cableado del edificio
- Cableado entre edificio

Los tipos de cableados reconocidos y máximas distancias centrales son:

100 ohm UTP(24 a 22 AWG)	800 metros (2625 ft) voz
150 ohm STP	90 metros (2955 ft) Datos
Fibra óptica 62.5/125 um multimodo	2,000 metros (6560 ft)
Fibra óptica 8.3/125 um uni-modo	3,000 metros (9840 ft)

Nota: La distancias centrales están sujetas a la aplicación.

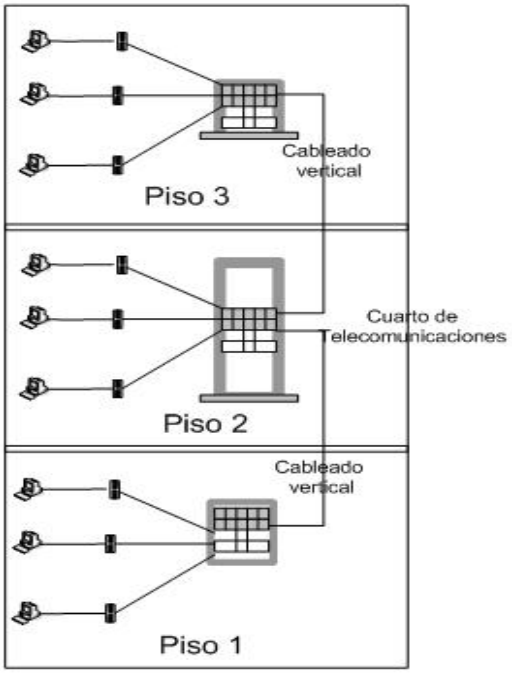


Figura 1.14 Cableado vertical

Cuarto de telecomunicaciones

Un armario de telecomunicaciones es el área de un edificio que aloja el equipo del sistema de cableado de telecomunicaciones. Esto incluye las terminaciones mecánicas y/o interconexiones para el sistema de cableado central y horizontal. Por favor, vea el estándar EIA/TIA-569 para las especificaciones del armario de telecomunicaciones.

Subsistema de Campus

El subsistema de campus abarca todo el cableado que interconecta diferentes edificaciones dentro de un campus como lo muestra la figura 1.15.

El cable recomendado para interconectar edificios dentro de un mismo campus es la fibra óptica, sin embargo dependiendo de los requerimientos se pueden utilizar cables de cobre de alta capacidad.

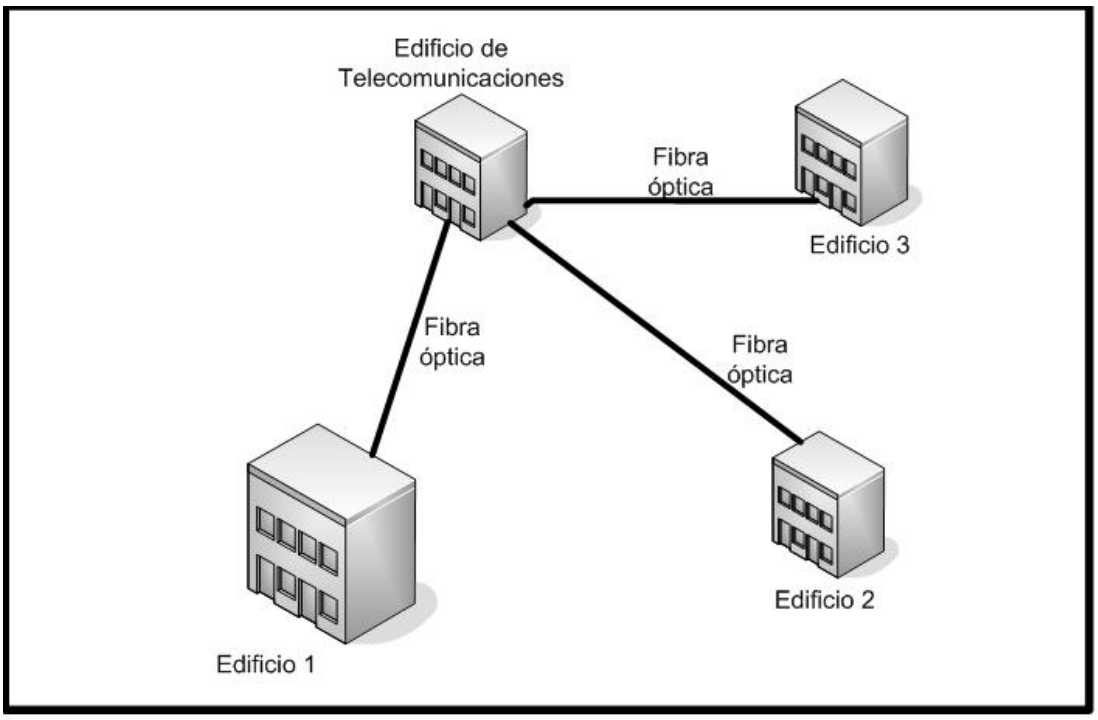


Figura 1.15. Subsistema de Campus

Consideraciones Eléctricas

En todo sistema de cableado estructurado deben tenerse consideraciones con respecto al sistema eléctrico. Se deben tener en cuanta las siguientes consideraciones:

- Instalar sistemas de puesta a tierra: esto permite proteger todos los equipos de cómputo y dispositivos activos de la red de descargas eléctricas producidas por rayos.

- Instalar sistemas de alimentación ininterrumpida (UPS): las UPS permiten que el sistema siga funcionando temporalmente a pesar de que se corte la alimentación eléctrica, esto garantiza que los usuarios terminen sus actividades y los equipos se apaguen correctamente.

- Instalar estaciones eléctricas para regular la corriente: todos los equipos y dispositivos de red deben estar conectados a fuentes eléctricas reguladas, es decir la corriente es controlada por fusibles que garantizan que a pesar de que ocurra un alto de energía nunca se afectaran los equipos de la red. Si se conectan los equipos directamente a tomas con corriente normal se exponen a que sufran daños por lo inconstante que es la corriente.

1.3 Dispositivos Activos

Concentrador

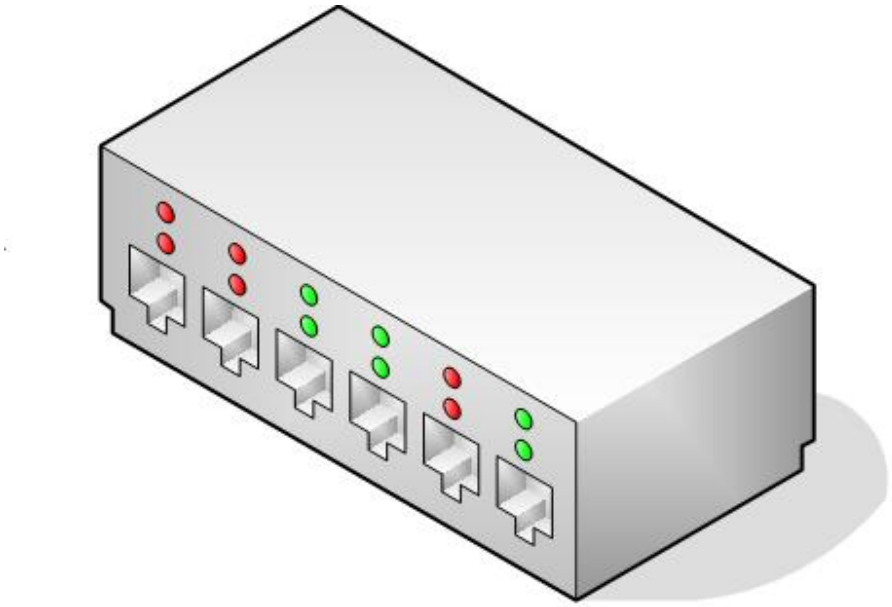


Figura 1.16 Concentrador o Hub

Un concentrador es un dispositivo que permite centralizar el cableado de una red. También conocido con el nombre de hub (ver figura 1.16).

Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases.

Pasivo: No necesita energía eléctrica.

Activo: Necesita alimentación.

Inteligente: También llamados smart hubs, son hubs activos que incluyen microprocesador.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Visto lo anterior se pueden sacar las siguientes conclusiones:

- El concentrador envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

- Este tráfico añadido genera más probabilidades de colisión.

- Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

- Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 Mbps le trasmitiera a otro de 10 Mbps, se perdería del mensaje.

- En el caso del ADSL los routers suelen funcionar a 10 Mbps, si lo conectamos a nuestra red casera, toda la red funcionará a 10 Mbps, aunque nuestras tarjetas sean 10/100 Mbps

Un concentrador es un dispositivo simple, esto influye en dos características:

1. El precio es barato.

2. Un concentrador casi no añade ningún retardo a los mensajes.

Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los Sniffer. La disponibilidad de Switches ethernet de bajo precio ha dejado obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

1.4 LAN Inalámbricas

El protocolo IEEE 802.11 o WI-FI (Wireles Fidelity) es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

Wireless significa 'sin hilos', por lo tanto, todo sistema inalámbrico de interconexión es denominado como wireless.

La figura 1.17 indica el modelo desarrollado por el grupo de trabajo 802.11.

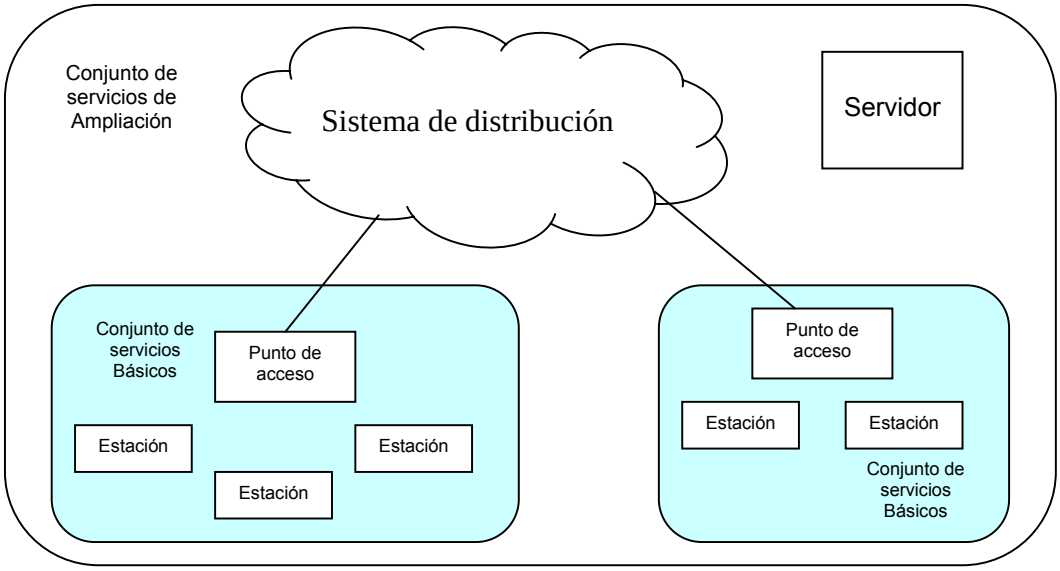


Figura 1.17. Arquitectura IEEE 802.11

A continuación se definen una serie de conceptos básicos que se incorporan en el estándar y que son fundamentales para la administración de cualquier LAN inalámbrica:

•***Estaciones:*** computadores o dispositivos con interfaz inalámbrica.

•**Medio:** se pueden definir dos la radiofrecuencia y los infrarrojos

•***Punto de acceso*** (AP): tiene las funciones de un puente (conecta dos redes con niveles de enlace parecidos o distintos), y realiza por tanto las conversiones de trama pertinente.

•***Sistema de distribución***: importantes ya que proporcionan movilidad entre AP, para tramas entre distintos puntos de acceso o con los terminales, ayudan ya que es el mecánico que controla donde esta la estación para enviarle las tramas.
WIFI

•***Conjunto de servicio básico (BSS):*** Grupo de estaciones que se intercomunican entre ellas. Se define dos tipos:
Independientes: cuando las estaciones, se intercomunican directamente.
Infraestructura: Cuando se comunican todas a través de un punto de acceso.

•***Conjunto de servicio Extendido o de Ampliación (ESS):*** Es la unión de varios BSS.

•***Área de Servicio Básico (BSA):*** es la zona donde se comunican las estaciones de una misma BSS, se definen dependiendo del medio.

•***Movilidad:*** este es un concepto importante en las redes 802.11, ya que lo que indica es la capacidad de cambiar la ubicación de los terminales, variando la BSS. La transición será correcta si se realiza dentro del mismo ESS en otro caso no se podrá realizar.

•***Límites de la red:*** Los límites de las redes 802.11 son difusos ya que pueden solaparse diferentes BSS.

Arquitectura Del Protocolo Ieee 802.11

El grupo de trabajo 802.11 consideró dos tipos de proposiciones para un algoritmo MAC (Control de Acceso al Medio): protocolos de acceso distribuido, que como CSMA/CD, distribuyen la decisión de transmitir entre todos los nodos usando un mecanismo de detección de portadora, y protocolos de acceso centralizado, que implican la gestión centralizada de la transmisión, estos dos algoritmos se implementan en las topologías inalámbricas que se explican mas adelante en este modulo.

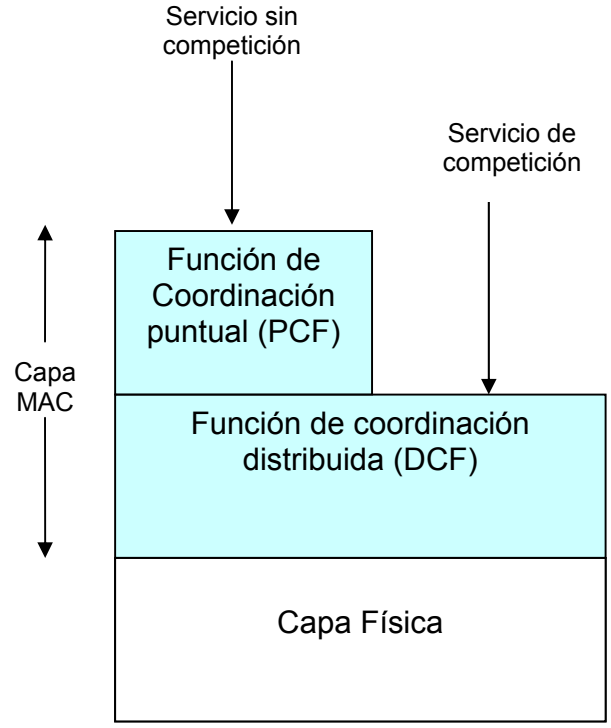


Figura 1.18. Pila de protocolos 802.11

El resultado final del 802.11 es un algoritmo MAC llamado MAC inalámbrico de principio distribuido (DFWMAC, "Distibuted Foundation Wireless MAC"), que proporciona un mecanismo de control de acceso distribuido con un control centralizado opcional implementado sobre él. La figura xxx ilustra la arquitectura. La subcapa inferior de la capa MAC es la función de coordinación distribuida (DCF). DCF emplea un algoritmo de competición para proporcionar acceso a todo el tráfico. El tráfico asíncrono ordinario usa DCF. La función de coordinación puntual (PCF) es un algoritmo MAC centralizado utilizado para proporcionar un servicio sin competición. PCF se constituye sobre DCF y aprovecha las características de DCF para asegurar el acceso a sus usuarios.

A continuación se explica las dos topologías para redes inalámbricas que implementan las dos propuestas del comité 802.11:

Topologías Inalámbricas

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no

administradas, alojadas y par a par, e infraestructura y "ad hoc". En este Modulo se utilizarán los términos "infraestructura" y "ad hoc". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

A continuación se explican las dos topologías Inalámbricas para la LAN:

- **INFRAESTRUCTURA**

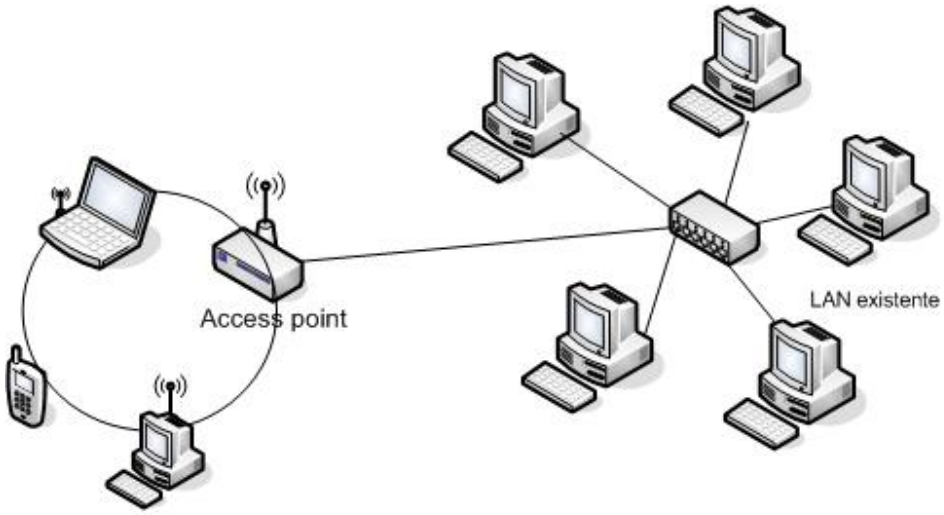


Figura 1.19. Topología de Infraestructura

Una topología de infraestructura (figura 1.19) es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

- **AD HOC**

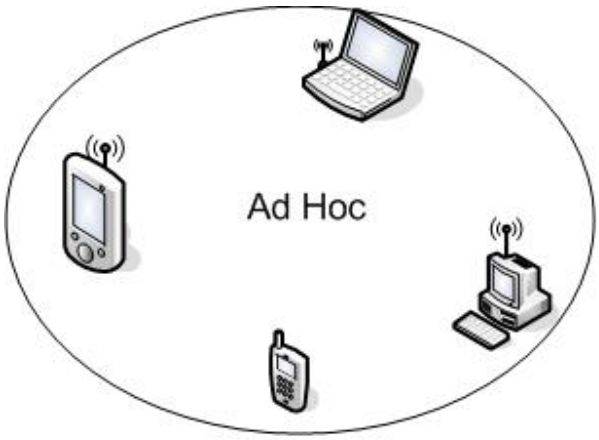


Figura 1.20. Topología Ad Hoc

En una topología ad hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas o Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los usuarios móviles colaborar, participar en juegos de equipo, transferir archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

Especificación Del Medio Físico

Existen varios estándares que se desarrollaron por la IEEE y que hoy permiten que las redes inalámbricas tengan una posición de privilegio en la LAN:

- La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 Mbps, que se transmiten por señales infrarrojas (IR) en la banda ISM (estas son bandas de uso no comercial) a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles. El estándar original también define el protocolo CSMA/CD (Múltiple acceso por detección de portadora evitando colisiones)

- La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CD, definido en el estándar original. El estándar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del

protocolo CSMA/CD, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbps sobre TCP y 7.1 Mbps sobre UDP.

- La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-división multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbps. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbps en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

- En el 2003, se ratificó un tercer estándar de modulación: Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbps, o cerca de 24.7 Mbps de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

- En el 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. la velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar. .

- Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF)

- Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz y 5 Ghz, alcanza una velocidad de transferencia de 108 Mbps.

Redes De Área Personal PAN

El comité IEEE 802.15 ha desarrollado un conjunto de normalizaciones para redes de área personal inalámbricas. Bluetooth es la norma que define este estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia.

Objetivos De Bluetooth

Los principales objetivos que se pretende conseguir con esta norma son:

•Facilitar las comunicaciones entre equipos móviles y fijos

•Eliminar cables y conectores entre éstos.

•Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales

Usos Y Aplicaciones

•Conexión sin cables entre los celulares y equipos de manos libres y kit para autos.

•Red inalámbrica en espacios reducidos donde no sea tan importante un gran ancho de banda.

•Comunicación sin cables entre la PC y dispositivos de entrada y salida. Mayormente impresora, teclado y mouse.

•Transferencia de ficheros entre dispositivos.

•Transferencia de fichas de contactos, citas y recordatorios entre dispositivos.

•Reemplazo de la tradicional comunicación por cable entre equipos GPS y equipamiento médico.

•Controles remotos (tradicionalmente dominado por el infrarrojo)

•Enviar pequeñas publicidades entre anunciantes y dispositivos con bluetooth. Un negocio podría enviar publicidad a celulares / teléfonos móviles con bluetooth activado al pasar cerca.

- Las consolas de juegos de video traen bluetooth para utilizar mandos inalámbricos.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 1

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 1 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue las normas vigentes de cableado estructurado y que entidad las desarrollo

4. Realice un laboratorio en grupo de curso donde aplique las diferentes normas de cableado estructurado.

5. Realice un laboratorio en grupo de curso refrente a instalación y configuración de redes Inalámbricas.

6. Elaborar un informe de cada laboratorio y entréguelo al Tutor.

CAPITULO 2: LA CAPA DE ENLACE DE DATOS

2.1 Arquitecturas LAN

Cuando se habla de arquitectura LAN, lo que se describe es una pila de protocolos basados en las dos primeras capas del modelo OSI, que incluye la capa física y las dos subcapas de la capa de Enlace de datos, la MAC (control de acceso al medio) y la LLC(control de enlace lógico)

Este modulo se limita al estudio de las arquitecturas utilizadas en las redes de área local LAN y se basa en los estándares OSI y 802 ver Figura 2.1.

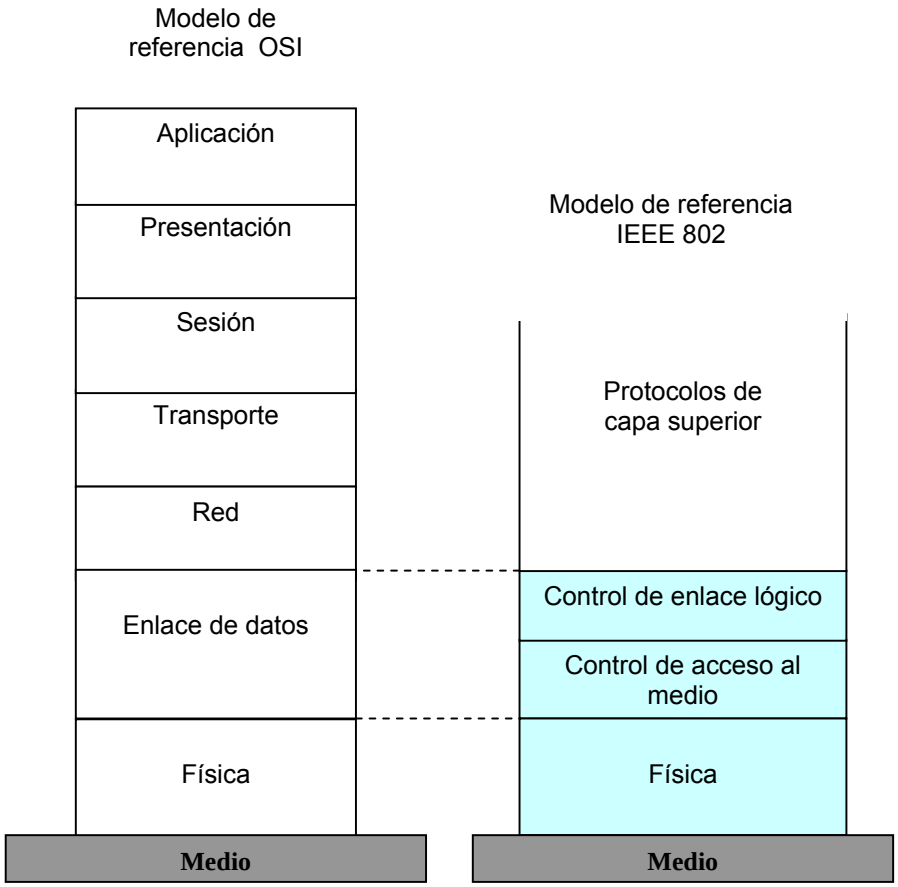


Figura 2.1. Arquitectura IEEE802 comparada con el modelo OSI.

En este capitulo se analizara las características de las arquitecturas LAN siguientes:

- Ethernet y Ethernet de alta velocidad

- Anillo con paso testigo y FDDI
- 100 VG-AnyLAN
- Redes LAN ATM

2.1.1 Ethernet y Ethernet de alta velocidad (CSMA/CD)

El estándar IEEE 802. 3 define la técnica de control de acceso al medio llamada acceso múltiple sensible a la portadora con deteccion de colisiones (CSMA/CD, “Carrier Sense Multipla Access With Colision Detection”). La cual es la más ampliamente usada para topologías en bus/árbol y en estrella

En las redes Ethernet se definen protocolos para la capa Física, como para la capa de control acceso al medio (ver figura 2.2).

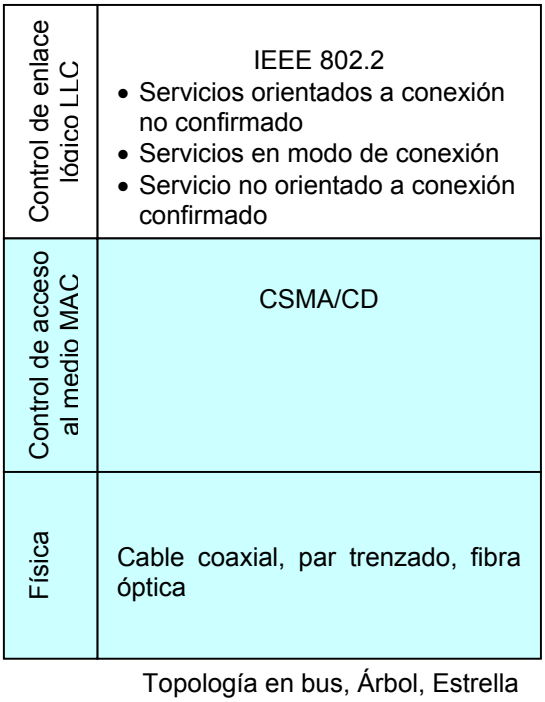


Figura 2.2 Arquitectura Ethernet.

Especificaciones capa física IEEE (802.3)

El comité 802.3 de la IEEE ha sido el más activo en la definición de configuraciones físicas para su arquitectura. Esto tiene ventajas y desventajas al mismo tiempo:

Ventajas

- La normalización responde a la evolución de la tecnología.

- El usuario tiene varias posibilidades disponibles que se ajusten a sus necesidades.

Desventajas

El consumidor, sin mencionar al potencial proveedor, se encuentra con una gran variedad de opciones y no saben cual es la más apropiada. Sin embargo el comité trabaja fundamentalmente en asegurar que todas las opciones puedan integrarse en una sola solución que satisfaga todas las necesidades.

El comité ha desarrollado una notación concisa con el fin de distinguir las distintas implementaciones que se encuentran disponibles:

- Razón de datos en Mbps

- Método de señalización

- Máxima longitud del segmento en centenas de metros

Las alternativas definidas son:

- 10 BASE 5
- 10 BASE 2
- 10 BASE T
- 10 ANCHA 36
- 10 BASE F
- 100 BASE T
- 100 BASE TX
- 100 BASE FX
- 100 BASE T4

Control de acceso al medio en IEEE 802.3

A través del tiempo se han implementado diferentes técnicas para acceder a un canal múltiple. A continuación se describe una muestra representativa de los más interesantes.

La técnica CSMA/CD y sus precursores pueden ser denominadas de acceso aleatorio o de competición. Son de acceso aleatorio en el sentido de que no existe un tiempo preestablecido o predecible para las transmisiones de las estaciones; ésta se realiza aleatoriamente. Son de competición en el sentido que las estaciones compiten para conseguir tiempo del medio.

ALOHA

Es la primera de estás técnicas, se desarrolló para redes de radio, siendo, a pesar de ello, aplicable a cualquier medio de transmisión compartido.

A continuación se estudian las dos versiones de ALOHA: ALOHA puro y Ranurado. Que difieren en si se divide o no el tiempo en ranuras discretas en las que deben caber todos los marcos.

ALOHA puro: como se llama a veces, es una técnica que no requiere sincronización de tiempo global. Supone una auténtica disputa entre las estaciones. Cuando una estación dispone de una trama a transmitir lo hace, pasando después a escuchar al medio durante un tiempo al máximo retardo de propagación posible de ida y vuelta a través de la red (dos veces al tiempo que tarda el envío de una trama entre las dos estaciones más separadas) más un pequeño incremento fijo de tiempo. Si durante este tiempo la estación oye una confirmación, de acuerdo; si no, retransmite la trama. Si la estación no recibe una confirmación después repetidas transmisiones, desde su intento. Una estación receptora determina si una trama recibida es correcta examinando un campo de secuencia de comprobación de trama, como en HDLC. Si la dirección de la trama es valida y la dirección de destino en la cabecera de la trama coincide con la de la receptora, la estación envía inmediatamente una confirmación. La trama puede ser incorrecta debido a la presencia de ruido en el canal o debido a que otra estación transmitió una trama casi al mismo tiempo. En el último caso, las dos tramas pueden interferir entre sí en el receptor de modo que no se acepta ninguna; esto se conoce como colisión. Si se decide que la trama recibida no es válida, la estación receptora simplemente ignora la trama.

ALOHA es tan sencilla como puede serlo, y por este motivo presenta puntos débiles. Dado que el número de colisiones crece rápidamente cuando aumenta la carga, la utilización máxima del canal es sólo de orden del 18%.

ALOHA Ranurado: Este protocolo se desarrollo con la finalidad de mejorar la eficiencia del ALOHA puro. En este esquema el tiempo del canal se organiza en ranuras uniformes del tamaño igual al tiempo de transmisión de tramas, siendo necesario el uso de un reloj central u otra técnica para sincronizar todas las estaciones. La transmisión sólo se permite al comienzo de una frontera de ranura. Así las tramas que se solapen lo harán completamente, lo que incrementa la utilización máxima del sistema has 37% aproximadamente.

En conclusión tanto ALOHA puro como ALOHA ranurado presentan una pobre utilización. Ninguna de las dos técnicas aprovecha una de las propiedades más importantes de la radio y las redes LAN, consistente en que el retardo de propagación entre las estaciones es generalmente muy pequeño en comparación con el tiempo de transmisión de tramas.

CSMA (acceso Múltiple sensible a la portadora)

Con CSMA, una estación que desea transmitir escucha primero el medio para determinar si existe otra transmisión en curso (sensible a la portadora). Si el medio se está usando, la estación debe esperar. En cambio si este se encuentra libre, la estación puede transmitir. Puede suceder que dos o más estaciones intenten transmitir aproximadamente al mismo tiempo, en cuyo caso se producirá colisión: los datos de ambas transmisiones interfieren y no se reciben con éxito. Para solucionar esto, una estación guarda una cantidad de tiempo razonable después de transmitir en espera de una confirmación, teniendo en consideración el retardo de propagación máximo del trayecto de ida y vuelta y el hecho de que la estación que confirma debe competir también por conseguir el medio para responder. Si no llega la confirmación, la estación supone que se ha producido una colisión y retransmite.

Se puede ver como esta estrategia resulta efectiva para redes que el tiempo de transmisión de tramas promedio es mucho mayor que el de propagación. Las colisiones solo se producen cuando más de un usuario comienza a transmitir con diferencias pequeñas de tiempo (periodo de retardo de propagación). Si una estación comienza a transmitir una trama y no existen colisiones durante el tiempo de propagación del inicio del paquete a la estación más lejana, no se producirá colisión para esta trama dado que todas las estaciones están enteradas de la transmisión.

CSMA/CD

El protocolo CMSA/CD, es mucho más eficiente que los protocolos ALOHA, ALOHA ranurado y CSMA. Se basa en una serie de reglas que permiten un mejor aprovechamiento del canal:

Regla1: La estación transmite si el medio está libre, si no se aplica la regla 2.

Regla 2: si el medio se encuentra ocupado, la estación continua escuchando hasta que encuentre libre el canal, en cuyo caso transmite inmediatamente.

Regla 3*:* si se detecta una colisión durante la transmisión, las estaciones transmiten una señal corta de interferencia para asegurarse de que todas las estaciones constatan la producción de colisión y dejan de transmitir.

Regla 4: Después de transmitir la señal de interferencia se espera una cantidad de tiempo aleatorio, e intenta transmitir de nuevo (paso 1)

Trama MAC 802.3

La trama del protocolo 802.3 (ver figura 2.3) consta de los siguientes campos:

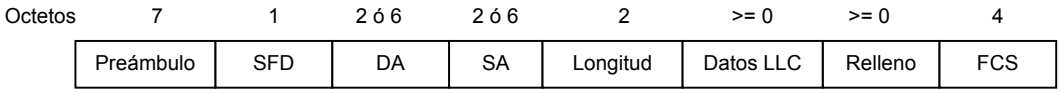


Figura 2.3 Formato de la trama Ethernet

Preámbulo: el receptor usa un octeto patrón de 7 bits cero y uno alternados para establecer la sincronización a nivel de bits.

Delimitador de comienzo de trama (SFD): consiste en la secuencia de bits 10101011, que indica el comienzo real de la trama y posibilita al receptor localizar el primer bit del resto de la trama.

Dirección de destino (DA): especifica la estación o estaciones a las que va dirigida la trama. Esta dirección puede ser de tres tipos:

- Una única dirección física
- Una dirección de grupo
- Una dirección global

Para su implementación se pueden elegir dos longitudes, 16 o 48 bits, y debe ser la misma en todas las estaciones de una LAN especifica.

Dirección de origen (SA): Especifica la estación que envió la trama.

Longitud: Longitud del campo de datos LLC

Datos LLC: Unidad de datos suministradas por LLC.

Relleno: Octetos añadidos para asegurar que la trama es suficientemente larga para un correcto funcionamiento de la técnica de detección de colisión.

Secuencia de comprobación de trama (FCS): comprobación de redundancia cíclica de 32 bits en base a todos los campos excepto los de preámbulo, SFD y FCS.

2.1.2 Anillo con paso testigo y FDDI

El protocolo MAC más usual en redes LAN con topología en anillo es el paso de testigo. A continuación se analizan dos normalizaciones que utilizan anillo con paso de testigo IEEE 802.5 y FDDI.

Anillo con paso de testigo IEEE 802.5

Para la arquitectura de anillo 802.5 (ver figura 2.4) se definen una serie de especificaciones para la capa física y para la capa de enlace.

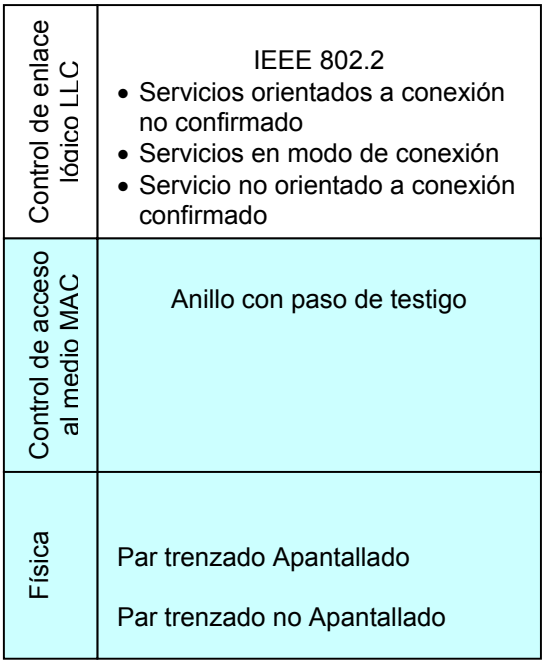


Figura 2.4. Arquitectura Token Ring

Especificaciones capa física de IEEE 802.5

La norma 802.5 especifica el empleo de par trenzado apantallado con capacidad de 4 ay 16 Mbps usando codificación Manchester Diferencial. Además del par trenzado no apantallado a 4 Mbps.

Control de acceso al medio en IEEE 802.5

La técnica de anillo con paso de testigo se basa en el uso de una trama pequeña, denominada testigo (“token”), que circula cuando todas las estaciones están libres.

Cuando una estación desea transmitir debe esperar a que le llegue un testigo. En este caso, toma el testigo cambiando uno de sus bits, lo que lo convierte en una secuencia de comienzo de trama para una trama de datos. A continuación, la estación añade y transmite el resto de campos requeridos en la construcción de una trama.

Cuando una estación toma un testigo y comienza a transmitir una trama de datos no existe testigo en el anillo, de manera que el resto de estaciones que desee transmitir deben esperar. La trama en anillo realiza una vuelta completa y se absorbe en la estación transmisora, quien insertará un nuevo testigo en anillo cuando se cumpla las dos condiciones siguientes:

- La estación ha completado la transmisión de su trama.
- Los bits iniciales de la trama transmitida han vuelto a la estación (después de un a vuelta completa al anillo).

Si la longitud del anillo es menor que la trama la primera condición implica la segunda. En caso contrario, una estación debería liberar un testigo después de que haya terminado de transmitir, pero antes de que comience a recibir su propia transmisión la segunda condición no es estrictamente necesaria, relajándose en determinadas circunstancias. La ventaja que implica la suposición de la segunda condición es que se asegura que, en un instante de tiempo dado, sólo puede haber una trama de datos en el medio y sólo puede estar transmitiendo una estación, simplificándose los procedimientos de recuperación de errores.

Una vez que se ha insertado un nuevo testigo en el anillo, la siguiente estación en la secuencia que disponga de datos a transmitir podrá tomar al testigo y llevar a cabo la transmisión.

Observe que en condiciones de baja carga, el anillo con paso de testigo presenta cierta ineficiencia debido a que una estación debe esperar a recibir el testigo antes de transmitir. Sin embargo, en condiciones de alta carga, que es la situación que

mas importante, el anillo funciona como la técnica de rotación circular (“round-robin”), que es eficiente además de equitativa.

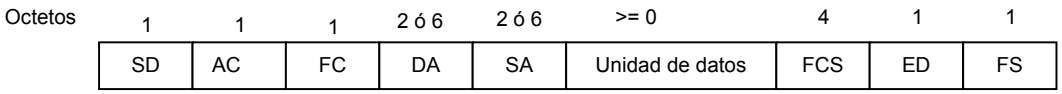
La configuración de anillo con paso testigo ofrece una serie de ventajas y desventajas:

La principal ventaja del anillo con paso de testigo es el flexible control de acceso que ofrece.

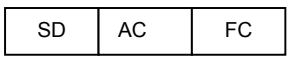
La principal desventaja del anillo con paso de testigo son los requisitos para el mantenimiento del anillo. La perdida de testigo impide posteriores utilizaciones del anillo. La duplicidad del testigo puede interrumpir también el funcionamiento del anillo. Se debe seleccionar una estación como monitora para asegurar que sólo hay un testigo en el anillo y para reinsertar un testigo libre en el caso necesario.

Trama MAC

El formato de tramas de protocolos 802.5 (ver figura 2.5) consta de los siguientes campos:



Formato general de trama



Formato de trama de testigo

Figura 2.5. Formato de la trama 802.5

- **Delimitador de comienzo (SD)**: indica el comienzo de la trama. SD consta de patrones de señalización distintos de los datos. Se codifican como sigue: JK0JK000, donde J y K símbolos de no datos.

- **Control de acceso (AC)**: Tiene el formato PPPTMRRR, donde PPP y RRR son variables de prioridad y reserva de 3 bits, y M es el bit monitor. T indica si es una

trama de testigo o de datos. En caso de una trama de testigo, el único campo posterior es el ED.

- **Control de trama (FC)**: indica si es una trama de datos LLC. Si no, los bits de este campo controlan el funcionamiento del protocolo MAC en el anillo con paso testigo.

Dirección de destino (DA): especifica la estación o estaciones a las que va dirigida la trama. Esta dirección puede ser de tres tipos:

- Una única dirección física
- Una dirección de grupo
- Una dirección global

Dirección de origen (SA): Especifica la estación que envió la trama.

- **Unidad de datos**: Contiene datos LLC

Secuencia de comprobación de tramas (FCS): comprobación de redundancia cíclica de 32 bits en base a todos los campos excepto los de preámbulo, SFD y FCS.

- **Delimitador de fin (ED)**: contiene el bit de detección de errores (E) que se activa si cualquier repetidor detecta un error, y el bit intermedio (I), usado para indicar que la trama no es la final en una transmisión de múltiples tramas.

- **Estado de Trama (FS)**: Contiene los bits de dirección reconocida (A) y de trama copiada (C). dado que estos bit no se encuentran cubiertos por el campo FCS, se encuentran duplicados con el fin de ofrecer una comprobación de redundancia para detectar valores erróneos.

FDDI

Es una arquitectura (Ver figura 2.6) que se basa en un esquema en anillo con paso de testigo igual que la IEEE 802.5 diseñada para aplicaciones LAN y MAN.

Para esta arquitectura se definen una serie de especificaciones para la capa física y para la capa de enlace.

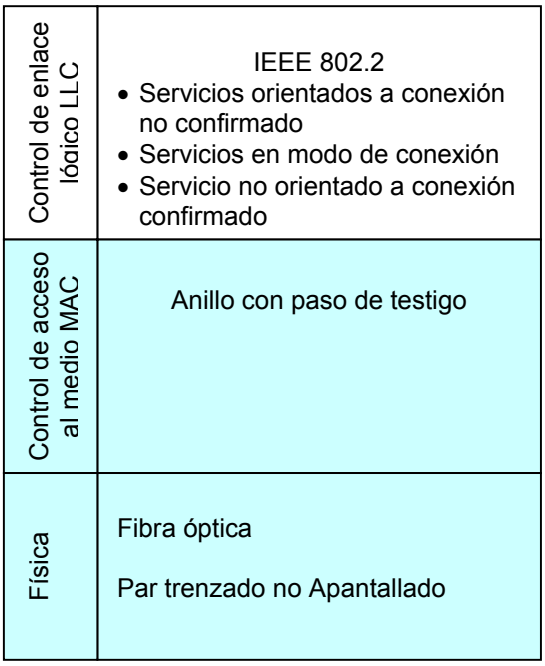


Figura 2.6. Arquitectura FDDI

Especificaciones de la capa física en FDDI

El estándar FDDI especifica una topología en anillo operando a 100 Mbps. Se incluyen dos medios de transmisión:

- Fibra óptica: que permite una distancia máxima de 2 Km.

- Par trenzado: que puede ser apantallado de 100 Ohmios o no apantallado de 150 Ohmios. En ambos casos permite una distancia máxima de 100 mts.

Control de acceso al medio en FDDI

El protocolo de acceso al medio en FDDI es fundamentalmente el mismo que IEEE 802.5, existiendo dos diferencias principales:

1. En FDDI, una estación que espera un testigo lo toma cancelando la transmisión del mismo en cuanto reconoce que se trata de una trama de testigo y no repitiendo como en 802.5.

2. En FDDI, una estación que ha transmitido trama de datos libera un nuevo testigo en cuanto completa la transmisión, incluso si no ha comenzado a recibir su propia transmisión. A diferencia de la 802.5 en este caso no se espera el retorno de su trama debido a que resultaría demasiado ineficiente debido a las altas velocidades que se manejan.

Trama MAC

La trama para el protocolo FDDI (ver figura 2.7) consta de las siguientes partes:

- **Preámbulo:** Sincroniza la trama con el reloj de cada estación. La estación que origina la trama usa un campo de

- **Delimitador de comienzo (SD**): indica el comienzo de la trama. Se codifica como JK, donde tanto J como K son símbolos de no datos.

- **Control de trama (FC):** tiene formato de bits CLFFZZZZ, donde C indica si la trama es sincronía o asíncrona; L indica el uso de direcciones de 16 ó 48 bits; FF indica si es una trama LLC, de control MAC o reservada. Para una trama de control, los 4 bits restantes indican el tipo de trama control.

- **Dirección de destino (DA):** Especifica la estación o estaciones a las que va dirigida la trama. Y puede ser una única dirección física, de grupo multidestino o una dirección de difusión. El anillo puede contener una mezcla de longitud de dirección de 48 bits.

- **Dirección origen (SA):** Especifica la estación que envió la trama.

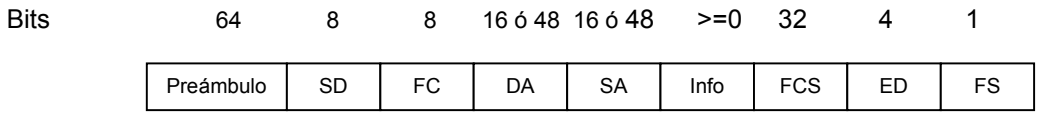
- **Información:** contiene datos LLC o información relacionada con una función de control.

- **Secuencia de comprobación de trama (FCS):** Comprobación de redundancia cíclica de 32 bits referente a los campos FC, DA, SA y de información.

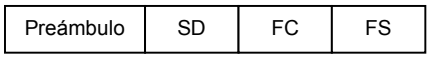
- **Delimitador de fin (ED):** contiene un símbolo de no datos (T) y marca el final de la trama sin contar el campo FS.

- **Estado de trama (FS):** contiene los indicadores de detección de error (E), dirección reconocida (A) y trama copiada (C). Cada indicador se representa

mediante un símbolo, que es R para “reinicio” o “falso”, y S para “activo” o ”verdadero”.



a. Formato de Trama general



b. Formato de Trama Testigo

Figura 2.7 Formato de trama FDDI

El formato de la trama Testigo (figura 2.7 a) es el siguiente:

- **Preámbulo:** como en la anterior.
- **Delimitador de comienzo**: como el anterior.
- Control de trama (FC): Presenta el formato de bits 10000000 ó 11000000 para indicar que se trata de un testigo.
- Delimitador de fin (ED): Contiene un par de de símbolos de no datos (T) como fin de la trama de testigo.

Comparando la trama de la arquitectura FDDI con la 802.5 se puede observar que son muy similares, la diferencia fundamental es el uso del preámbulo en FDDI para una mejor sincronización y velocidades mayores. Además de ser compatibles con direcciones tanto de 16 como de 48 bits lo que hace que sea mucho más flexible.

2.1.3 100 VG-AnyLAN

100VG-AnyLAN fue una arquitectura pensada para ser una ampliación a 100Mbps de la red Ethernet a 10Mbps y para administrar tipos de tramas IEEE 802.3.

También proporciona compatibilidad con la trama IEEE 802.5 de redes en anillo con paso de testigo. 100VG-AnyLAN usa un nuevo esquema MAC, conocido como prioridad de demanda, con el fin de determinar el orden en que los nodos comparten la red. Dado que esta especificación no utiliza CSMA/CD, ha sido normalizada en el grupo de trabajo, IEEE 802.12, en lugar de permanecer en el grupo 802.3.

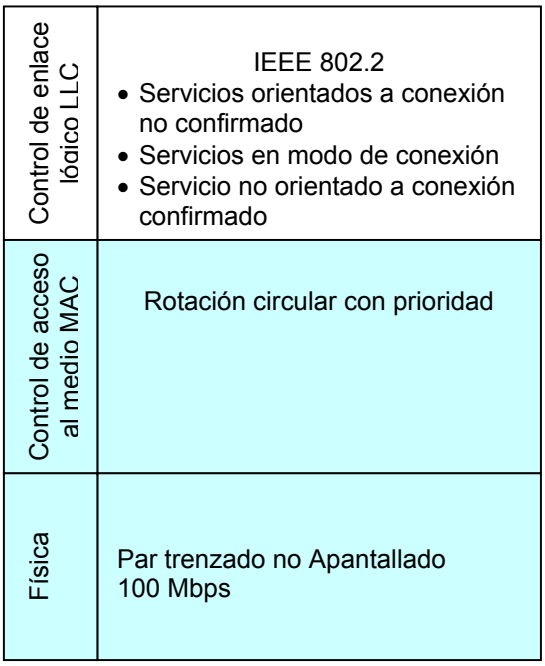


Figura 2.8. Arquitectura 100VG-AnyLAN.

Especificación de la capa física en 100VG-AnyLAN

Las versiones actuales de IEEE 802.12 requiere la utilización de cuatro pares trenzados no apantallados (UTP) empleando clase de 3, 4 ó 5. Futuras versiones admitirán también dos pares UTP de clase 5, par tranzado apantallado y cable de fibra óptica. La razón de datos es de 100 Mbps en todos los casos.

Codificación de señal

Un objetivo clave en 100VG-AnyLAN era la consecución de 100 Mbps para señales corta haciendo uso de cable tradicional de voz (clase 3). La ventaja de este hecho era que en mucho de los edificios existentes era abundante el cable de voz, y prácticamente inexistente otro tipo de cable. Así se minimizaban los costes de instalación y se puede utilizar el cable de clase 3.

Con la tecnología que existía en el momento de la aparición de esta arquitectura era prácticamente imposible conseguir una razón de datos de 100 Mbps a través de uno o dos pares de clase 3. Para alcanzar este objetivo 100VG-AnyLAN especifica un sistema de codificación nuevo, que hace uso de cuatro pares para transmitir datos en modo semiduplex, siendo necesaria, por tanto, sólo una razón de datos de 25 Mbps a través de cada canal para conseguir los 100 Mbps. Se utiliza el esquema de codificación conocido como 5B6B.

Los datos que provienen de la capa MAC se pueden ver como una secuencia de bits. Los bits de la secuencia se toman en grupos de cinco para construir una secuencia de quintetos, y se pasan a los cuatro canales de transmisión siguiendo la técnica de transmisión circular. Después, a cada quinteto se le aplica un sencillo algoritmo de mezcla para incrementar el número de transmisión entre 0 y 1 y mejorar el espectro de la señal. Llegados a este punto, es posible transmitir de forma sencilla los datos usando NRZ. Sin embargo, según el algoritmo de mezcla, se usa un paso adicional de codificación 5B6B para asegurar la sincronización y para mantener el equilibrio de tensión continua.

Ya que la trama MAC se ha dividido entre los cuatro canales, se debe transmitir el comienzo y el final de la trama en cada uno de los canales; éste es el objetivo de los generadores de delimitadores. Por ultimo, se emplea transmisión NRZ en cada canal.

Topología

La topología de una red 100VG-AnyLAN es una estrella jerárquica. La configuración más simple consta de un único centro (“hub”) y varios dispositivos conectados. Son posibles estructuras más complejas, en que existe un único centro raíz y uno o más centros de nivel 2; un centro de nivel 2 puede disponer de centros subordinados de nivel 3, y así sucesivamente hasta una profundidad arbitraria.

Control de acceso al medio

El algoritmo MAC en 802.12 sigue un esquema de rotación circular con dos niveles de prioridad. Describimos primero el algoritmo para una red con un único centro, pasando después a describir el caso general.

Red con único centro

Cuando una estación de trabajo desea transmitir una trama, primero envía una petición al centro principal y después espera permiso de éste para transmitir. Una estación debe asignar a cada petición una prioridad normal o alta.

El centro principal chequea continuamente todos sus puertos antes de la producción de una petición en forma circular. Así, un centro con n puertos mira primero la existencia de una petición en el puerto 1, después en el puerto 2, y así sucesivamente hasta llegar al puerto n. Tras finalizar en el puerto n, el proceso de comprobación comienza de nuevo en el puerto 1. El centro mantiene dos puertos: puntero de alta prioridad y otro de prioridad normal. Durante un ciclo completo, el centro concede cada petición de alta prioridad en el orden en que se produjo. Si en un momento dado no hay pendientes peticiones de alta prioridad, el centro atiende cualquier prioridad normal que detecte.

La secuencia de un evento es como sigue.

1. El centro activa ambos punteros del puerto 1 y comienza a comprobar. La primera prioridad detectada es del puntero 2. El centro concede esta petición y analiza el puntero de baja prioridad del puerto 3.

2. El puerto 2 transmite una trama de baja prioridad; el centro recibe esta trama y retransmite. Durante este periodo se generan dos peticiones de alta prioridad.

3. Una vez que se ha transmitido la trama del puerto 2, el centro comienza a conceder peticiones de alta prioridad siguiendo el esquema de rotación, comenzando por el puerto 1 y continuando con el puerto 5. El puntero de alta prioridad se pone a la prioridad del puerto 6.

4. Después que se complete una trama de alta prioridad del puerto 5 no existen peticiones de alta prioridad pendiente, por lo que el centro vuelve a las peticiones de prioridad normal. Se ha recibido cuatro peticiones desde que se transmitió trama de baja prioridad: de los puertos 2, 7, 3 y 6. Puesto que el puerto de prioridad normal se ha activado en el puerto 3, estas peticiones serán atendidas en el orden 3, 6, 7, 2 si no aparecen otras peticiones.

5. Se transmiten las tramas de los puertos 3, 6 y 7. Durante la transmisión de la trama 7, se recibe en una petición de alta prioridad por el puerto 1 y una de

prioridad normal por el puerto 8. El centro pone el puntero de prioridad normal igual que el puerto 8.

6. Puesto que las peticiones de alta de alta prioridad tienen preferencia, el puerto 1 será el siguiente en acceder.

7. Después que la trama del puerto 1 se ha transmitido, el centro tiene pendientes dos peticiones de prioridad normal. La del puerto 2 es la que más ha esperad; sin embargo, el siguiente en la rotación circular es el puerto 8, por lo que será atendida su petición, seguida de la del puerto 2.

Red jerárquica

En una red jerárquica, con el objeto de hacer uso de una red circular, todos los puertos de los sistemas finales de todos los centros se tratan como un único conjunto de puertos. Los centros se configuran para cooperar en el chequeo de los puertos en el orden adecuado. Dicho de otra forma, los centros se tratan lógicamente como un único centro.

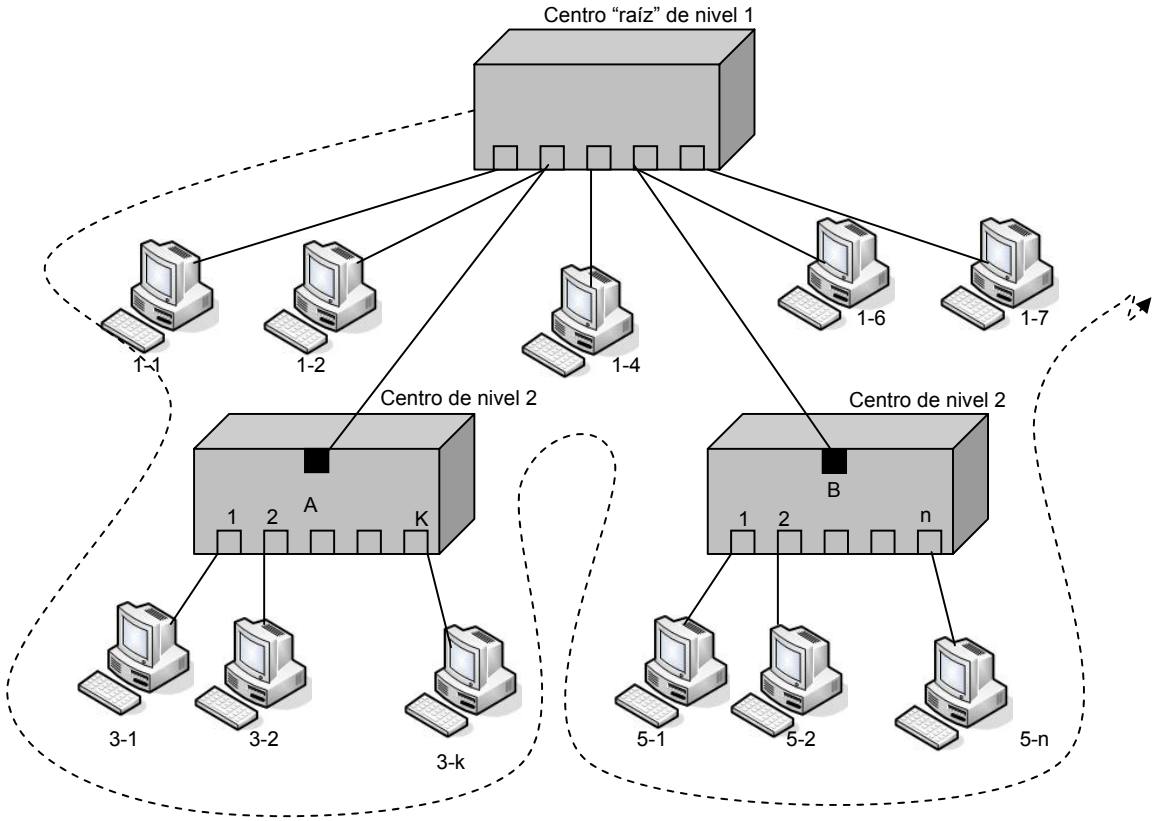


Figura 2.9. Ordenación de puertos de una red 100VG-AnyLAN de dos niveles.

El orden se genera siguiendo una representación en árbol de red (ver figura 2.9), en la que las ramas bajo cada nodo del árbol se establecen en orden creciente de izquierda a derecha. Con este convenio, el orden de los puertos se genera recorriendo el árbol en la forma denominada recorrido preordenado, que se define recursivamente como sigue:

1. visitamos el punto raíz.
2. recorremos los subárboles de izquierda a derecha.

Este método de recorridos se conoce también como búsqueda de profundidad 1 del árbol.

Consideremos ahora los mecanismos de acceso al medio y de transmisión de tramasen una red jerárquica. Es necesario considerar varias contingencias. En primer lugar consideremos el centro raíz. Este centro ejecuta los algoritmos de rotación circular de prioridad alta y baja de todos los dispositivos conectados directamente. Así, si hay pendientes una o más peticiones de alta prioridad, el centro atiende cualquier petición de baja prioridad siguiendo la técnica de rotación circular. Si no hay peticiones pendientes de alta prioridad, el centro atiende cualquier petición de baja prioridad siguiendo la misma técnica. Cuando el centro raíz concede una petición se un sistema final directamente conectado, este sistema puede transmitir inmediatamente una trama. Cuando el centro raíz concede una petición de un centro de nivel 2 directamente conectado, el control pasa al centro de nivel 2, pasando éste a llevar a cabo sus propios algoritmos de rotación circular.

Cualquier sistema final que se encuentre preparado para transmitir, envía una señal de petición al centro al que se encuentra conectado. Si el sistema está conectado directamente al centro raíz, la petición se transmite directamente a éste. Si el sistema esta conectado a un centro de nivel inferior, la petición se transmite directamente a este centro. Si este centro no posee actualmente control del algoritmo de rotación circular, pasa la petición al centro de nivel inmediatamente superior. Eventualmente, todas las peticiones no concedidas en un nivel inferior pasan al centro raíz.

El esquema descrito anteriormente no impone a las estaciones conectadas la disciplina de rotación circular, pero son necesarias dos mejoras. Primero, es necesario un mecanismo de preborrado. Esto se explica mejor con un ejemplo. Consideremos la siguiente secuencia de eventos.

1. Supongamos que el centro raíz (R) tiene el control y que no hay pendientes peticiones de alta prioridad en la red. Sin embargo las estaciones 5-1,5-2 y 5-3 han enviado peticiones de prioridad normal, provocando que el centro B envíe una petición de prioridad normal a R.
2. R concederá temporalmente esta petición, pasando el control a B.

3. B procede a tender sus peticiones pendientes de forma ordenada, una en cada instante de tiempo.
4. mientras que B atiende su primera petición de prioridad normal, la estación 1-6 envía una petición de alta prioridad.
5. en respuesta de petición 1-6, R envía una señal apropiada a B indicándole que seda el control cuando haya completado la transmisión en curso.
6. R atiende la petición de la estación 1-6 y continua con la petición de su algoritmo de rotación circular.

La segunda mejora consiste en un sistema de mecanismo para evitar que un centro distinto de la raíz tenga el control indefinidamente. Para ver este problema supongamos que B, tiene pendiente una petición de alta prioridad de 5-1. Tras recibir el control de R, B atiende la petición 5-1. Mientras tanto, otra estación subordinada a b envía una petición de alta prioridad. B podría continuar con la rotación circular para atender todas estas peticiones. Si llegan peticiones adicionales desde otros subordinados de B durante estas otras transmisiones, B continuará atendiendo peticiones indefinidamente, incluso aunque hubiese pendientes peticiones de alta prioridad en la red. Para evitar este tipo de parálisis, un centro subordinado sólo puede mantener el control durante un ciclo de rotación circular para todos sus puertos.

El algoritmo MAC IEEE 802.12 es bastante efectivo, cuando varias estaciones presentan alta carga, el protocolo se comporta de forma muy similar a un protocolo de anillo con paso de testigo, con rotación en el acceso a la red entre todos los demandantes de alta prioridad, seguidos por demandantes de baja prioridad cuando no hay peticiones pendientes de alta prioridad. El protocolo se comporta a baja carga de forma análoga a como lo hace CSMA/CD en las mismas condiciones: un único demandante consigue al acceso al medio casi inmediatamente.

2.1.4 Redes LAN ATM

El termino LAN ATM se ha completado por vendedores e investigadores para aplicarlo a una gran variedad de configuraciones. Como mínimo, una LAN ATM implica el uso del protocolo de transporte ATM en algún lugar dentro de las premisas locales. Entre los posibles tipos de redes LAN se encuentran:

- **Pasarela a ATM WAN:** un conmutador ATM funciona como un dispositivo de encaminamiento y un concentrador de tráfico para conectar una red preexistente con una WAN ATM.

- **Conmutador ATM central:** la interconexión de otras redes LAN se realiza a través de un único conmutador ATM o mediante una red local de conmutadores ATM.

- **ATM de grupo de trabajo:** las estaciones de trabajo multimedia de altas presentaciones y otros sistemas finales se conectan directamente con un conmutador ATM.

Éstas son todas las configuraciones “puras”. En la práctica, se usan dos o los tres tipos de redes para crear una LAN ATM.

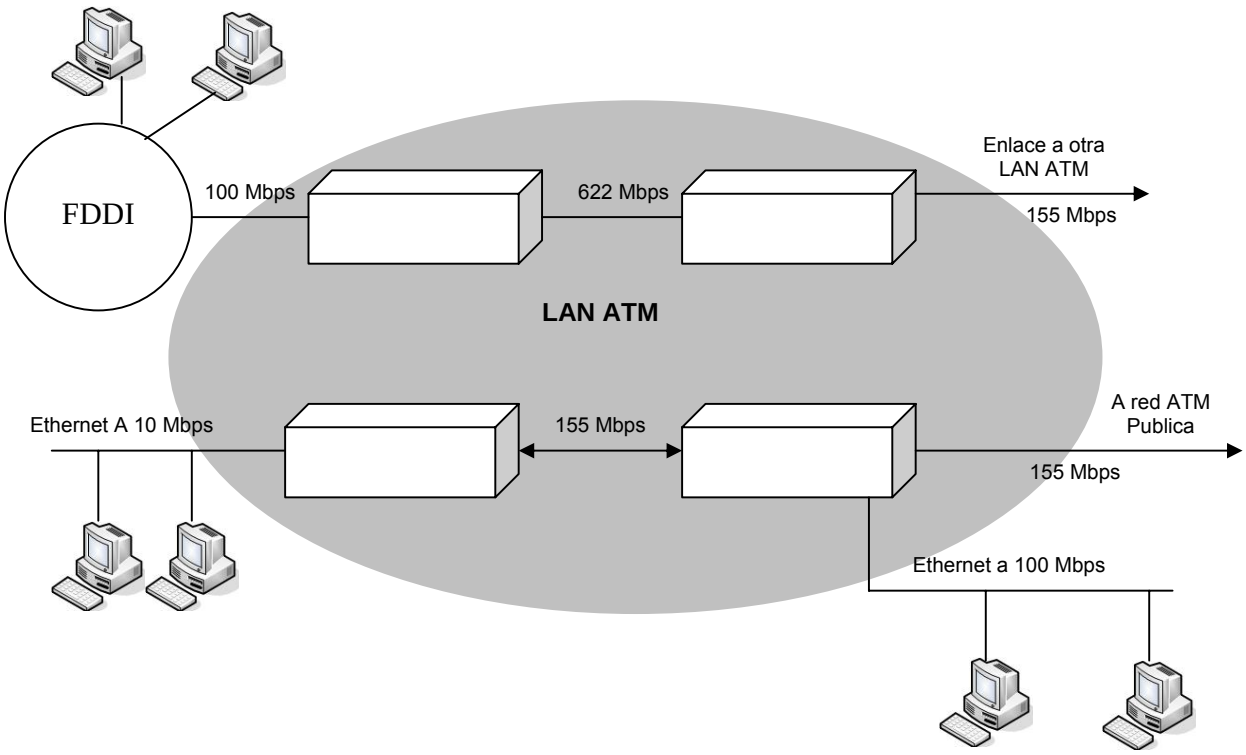


Figura 2.10 LAN ATM.

La figura 2.10 muestra un ejemplo de una LAN ATM núcleo que incluye enlaces hacia el mundo exterior. En este ejemplo, la red ATM local consta de cuatro conmutadores interconectados con enlaces punto a punto de alta velocidad operando a velocidades de transmisión de datos estándares de 155 y 622 Mbps. En la configuración preexistente hay otras tres redes LAN, cada una de ellas con una conexión directa a uno de los conmutadores ATM. La velocidad de transmisión de datos desde un conmutador ATM conectados a una LAN se ajusta a la velocidad de datos de esta LAN. Por ejemplo, la conexión con la red FDDI es de 100 Mbps. Así, el conmutador debe incluir cierta capacidad de almacenamiento temporal y de conversión de velocidad para transformar la velocidad de datos de la LAN conectada a una velocidad ATM. El conmutador ATM debe implementar también algún tipo de protocolo de conversión del protocolo MAC empleado en la LAN conectada a la secuencia de celdas ATM usada en una red ATM. Un enfoque sencillo consistente en que cada conmutador

ATM que se conecta con una LAN funcione con un puente o con un dispositivo de encaminamiento.

Una configuración LAN ATM como la mostrada en la figura 2.10 ofrece un método sencillo para insertar un núcleo de alta velocidad en entorno local. A medida que la demanda crece, se puede incrementar fácilmente la capacidad del núcleo mediante la incorporación de más conmutadores, aumentando el rendimiento de cada conmutador y aumentando la velocidad de transmisión de datos de enlace entre los conmutadores. Con esta estrategia se puede aumentar la carga de las LAN individuales dentro de las premisas, y puede crecer el número de redes LAN.

Sin embargo, esta sencilla LAN ATM núcleo no satisface todas las necesidades de comunicaciones locales. En particular, en la configuración del núcleo sencilla de los sistemas finales (estaciones de trabajo, servidores, etc.) permanecen conectados a redes LAN de medio compartido con las limitaciones impuestas por éste sobre la velocidad de transmisión de datos.

Un enfoque más avanzado y más potente es el empleo de tecnología ATM en un núcleo central. Este enfoque sugiere las posibilidades que pueden ofrecer esta orientación cada centro ATM incluye puertos que funcionan a distintas velocidades de transmisión de datos y hacen uso de diferentes protocolos. Generalmente, estos centros constante varios módulos montados en un chasis, cada uno de ellos conteniendo puertos de razón de datos y protocolos determinados.

La diferencia básica entre los dos enfoques es la forma en que se gestionan los sistemas finales particulares. Observemos que el centro ATM, cada sistema final tiene un enlace punto a punto dedicado con el centro. Cada sistema incluye hardware y software necesarios para conectarse a un tipo específico de LAN, pero, en este caso, la red LAN sólo contiene dos dispositivos: el sistema final y el centro. Por ejemplo, cada dispositivo conectado a un puerto ethernet a 10 Mbps hace uso del protocolo CSMA/CD a 10 Mbps. Sin embargo, dado que cada sistema final tiene su propia línea dedicada, el efecto es que cada sistema final tiene en exclusiva su propia Ethernet a 10 Mbps. Por tanto, cada sistema final puede funcionar a una velocidad de transmisión cercana a 10 Mbps.

La desventaja consiste en que el uso de un entorno de mezclas de protocolos necesita la implementación de algún tipo de método de conversión de protocolo, un enfoque más sencillo, pero que requiere que los sistemas finales estén equipados con capacidades ATM es la implementación de una red LAN ATM “pura”.

Los sistemas finales conectados directamente a una LAN tradicionales implementan la capa MAC apropiada para este tipo de LAN. Los sistemas finales conectados directamente a una red ATM implementan los protocolos ATM y AAL. Como resultado, deben considerarse tres áreas de compatibilidad:

1. Interacción entre un sistema final en una red ATM y un sistema final en una LAN tradicional.

2. Interacción entre un sistema final en una red LAN tradicional y un sistema final en otra LAN tradicional del mismo tipo (por ejemplo, dos redes IEEE 802. 3).

3. Interacción entre un sistema final en una red LAN tradicional y un sistema final en otra LAN tradicional de distinto tipo (por ejemplo, dos redes IEEE 802. 3 y una red IEEE 802.5).

Un estudio sobre orientaciones que satisfagan estos requisitos implica lógicamente la consideración de puentes.

2.2 Dispositivos activos

2.2.1 Switches

Un Conmutador (ver figura 2.11) es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

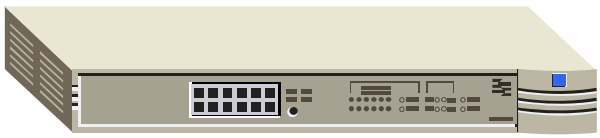
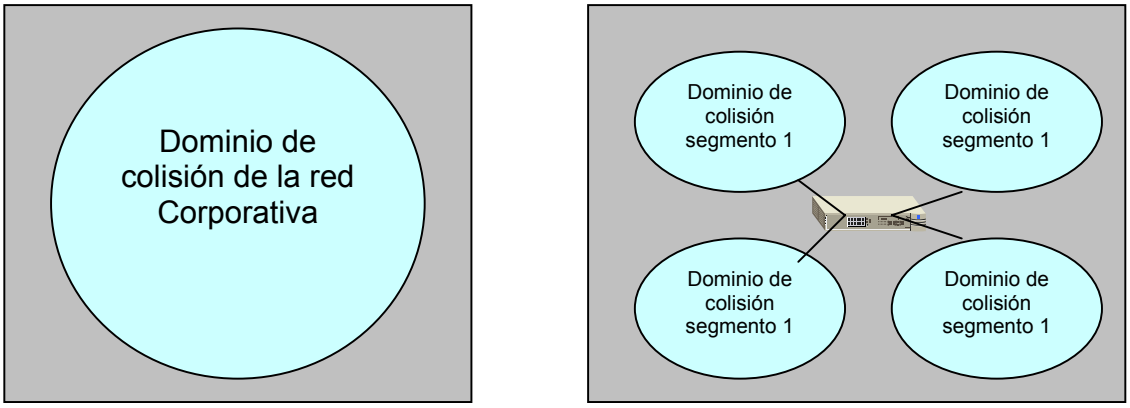


Figura 2.11. Switche o Conmutador.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Área Network- Red de Área Local).

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el dispositivo destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

Los conmutadores permiten segmentar la red en dominios de colisiones (Ver figura 2.12)



LAN sin Switche

LAN con Switche

Figura 2.12. Dominios de colisiones.

Bucles de red e inundaciones de tráfico

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten

alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Tipos de Switches

Los switches se pueden clasificar de manera muy general en dos tipos:

Switche tipo CORE: Estos Switches son utilizados en el centro de la red, donde los anchos de banda que se manejan no son tan elevados, su capacidad plena es limitada, así como su velocidad por puertos, normalmente este tipo de Switche es capa 2 y su costo es relativamente bajo.

Switche Tipo EDGE: Estos Switches son utilizados en las fronteras de la red donde los anchos de banda que se manejan son bastante elevados, debido a que en esta parte convergen todos los paquetes de los usuarios, la capacidad plena de este tipo de Switche es alta, así como su velocidad por puertos, normalmente este tipo de Switche es capa 3 o superior (hasta capa 7) y su costo es relativamente alto.

2.2.2 Puentes

Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete.

Así, varias redes físicas pueden combinarse para formar una sola red lógica, construyendo cada una un segmento de red (Ver figura 2.12). Teniendo en cuenta que ambas redes deben manejar el mismo protocolo de establecimiento de red.

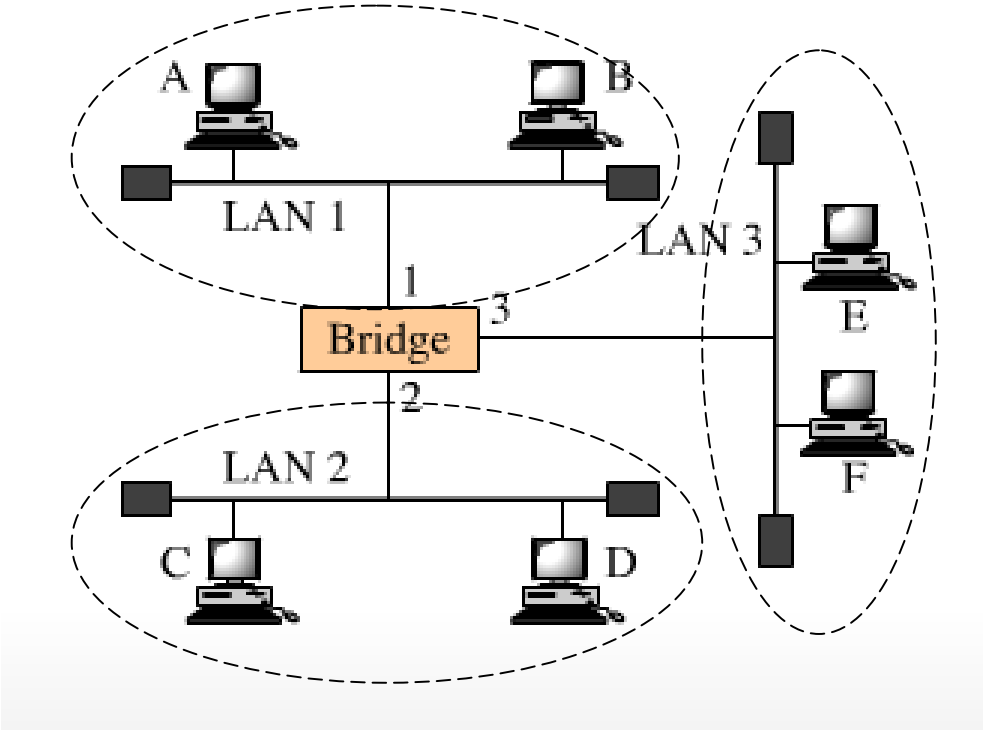


Figura 2.12. Implementación de Puentes.

La tabla de direcciones MAC, son detectadas en cada segmento a que está conectado el puente. Cuando ésta detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred o segmento.

Por ejemplo, se tienen dos PC, el equipo A y el Equipo B, cada uno en un segmento de red. Entonces, el equipo A manda un paquete al equipo B. El equipo B, recibe el paquete y sólo los de este segmento la pueden detectar y mirar. El resto del equipo A, no ve la trama que se envió. Sería lo mismo del Equipo B al A.

Lo que quiero decir es que no por ser un puente las redes no pueden chismosear lo que se está haciendo en la otra red. Por eso es que las segmenta cada una por su lado.

Los Puentes, los podemos clasificar en dos categorías:

- **Local**: Si proporciona una conexión directa entre múltiples segmentos de LAN situados en la misma área.

- **Remoto**: Si lo hace para las situadas en áreas distintas.

Interconexión de conmutadores y puentes

Los puentes (bridges) y conmutadores (switches) pueden ser conectados unos a los otros, pero existe una regla que dice que sólo puede existir un único camino entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, lo que tiene como resultado la transmisión infinita de datagramas de una red a otra.

Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 2

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 2 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. ¿Que dispositivos se utilizan para interconectar equipos en la LAN? Realice un cuadro comparativo que muestre las principales características y diferencias entre estos dispositivo?

4. Que factores deben tenerse en cuenta para calcular el ancho de banda? Explique porque son importantes.

5. Realice un cuadro comparativo de las arquitecturas de red utilizadas en la LAN, teniendo en cuenta criterios como: velocidad, protocolos, Topología, Longitud de trama, modo de transmisión.

6. Realice un laboratorio en grupo de curso y configure una red de área Local instalando y configurando dispositivos activos, tarjetas de red, servicios, protocolos.

7. Elaborar un informe del laboratorio y entréguelo al Tutor.

CAPITULO 3: LA CAPA DE RED

3.1 Principio de la Interconexión entre redes

Los requisitos globales del sistema de interconexión entre redes se pueden expresar en términos generales. Estos requisitos incluyen a:

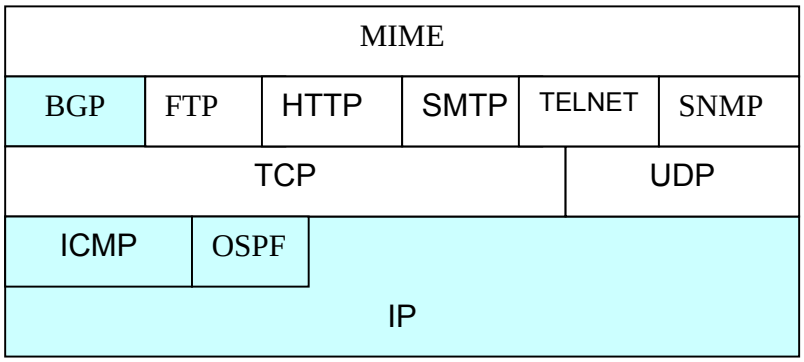


Figura 3.1 Protocolos de Interconexión entre redes en contexto

1. Proporcionar un enlace entre redes. Como mínimo, se necesita una conexión física y de control de enlace.

2. Proporcionar el encaminamiento y entrega de los datos entre procesos entre procesos en diferentes redes.

3. Proporcionar un servicio de contabilidad que realice un seguimiento de las diferentes redes y dispositivos de encaminamiento y mantenga información del estado.

4. Proporcionar los servicios mencionados de forma que no se requiera la modificación de la arquitectura de red de cualquiera de las redes interconectadas. Esto significa que el sistema de interconexión entre redes se debe acomodar a las varias diferencias existentes entre las distintas redes. Algunas de estas diferencias son:

   a. Diferentes esquemas de direccionamiento: Las redes pueden usar diferentes nombres y direcciones de los puntos finales y esquemas de mantenimiento del directorio.

   b. Diferentes tamaños máximos del paquete: Puede que se necesite romper un paquete en unidades más pequeñas al pasar a otra red. Este proceso se denomina segmentación o fragmentación.

c. Diferentes mecanismos del acceso de red: El mecanismo de acceso de la estación a la red podría ser diferente para estaciones de redes diferentes.

d. Diferentes valores de expiración de los temporizadores: Normalmente, un servicio de transporte orientado a conexión esperará la confirmación de una recepción correcta de datos hasta que un temporizadote expire, en cuyo caso retransmitirá su bloque de datos. En general, se requiere valores grandes del temporizador para realizar una entrega satisfactoria a través de redes múltiples. Los procedimientos que establecen los valores en la interconexión de redes deben permitir una transmisión satisfactoria que evite transmisiones innecesarias.

e. Recuperación de errores: Los procedimientos, dentro de una red, deben proporcionar un servicio que va desde no suministrar recuperación de errores hasta un servicio seguro extremo –a-extremo. El servicio de interconexión de redes no debería depender o no tendría que ser interferido por la naturaleza de la capacidad de recuperación de errores de redes individuales.

f. Informes de estado: Diferentes redes da informes de estado y de rendimiento de una forma distinta. Debe ser posible que el sistema de interconexión proporcione información de la actividad de interconexión a los procesos interesados y autorizados.

g. Técnicas de encaminamiento: El encaminamiento dentro de la red puede depender de la detección de fallos y de las técnicas de control de congestión particulares de cada red. El sistema de interconexión entre redes deben ser capaz de coordinar estas técnicas para encaminar los datos adaptativamente entre las estaciones de las diferentes redes.

h. Control de acceso del usuario: Cada red tendrá su propia técnica de control de acceso de los usuarios (autorización para usar la red). Estas técnicas se deben solicitar por el sistema de interconexión según se necesite. Además, se podría requerir una técnica diferente de control de acceso a la interconexión entre redes.

i. Conexión, sin conexión: Las redes individuales pueden proporcionar un servicio orientado a conexión (por ejemplo, circuitos virtuales) o no orientados a conexión (datagramas). Es deseable que el servicio entre redes no dependa de la naturaleza del servicio de conexión de las redes individuales.

3.2 Interconexión entre redes sin conexión

El protocolo Internet (IP, “Internet protocol”) fue desarrollado como una parte del proyecto de conexión de las redes de DARPA. Algún tiempo después, cuando la comunicación internacional de normalizaciones se dio cuenta de la necesidad de una operación sin conexión en la interconexión entre redes, se normalizó el protocolo ISO de red sin conexión (CLNP, “Connectionless Network Protocol”). Las funciones de IP y CLNP son muy similares; difieren en los formatos usados y en algunas características funcionales menores. A continuación se analizaran las funciones esenciales del protocolo de interconexión que se aplican tanto a CLNP como IP.
:

- Un sistema de interconexión sin conexión es flexible. Puede trabajar con una gran variedad de redes, algunas de las cuales serán también sin conexión. En esencia, IP requiere muy poco de redes sobre las que actúa.

- Un servicio de interconexión sin conexión hacer bastante robusto. Este es básicamente el mismo argumento que se da para un servicio de red datagrama frente a un servicio con circuitos virtuales. Para una discusión en profundidad.

- Un servicio de interconexión sin conexión es el mejor servicio para un protocolo de transporte sin conexión.

3.3 El protocolo IP

El protocolo Internet (IP) es parte del conjunto de protocolos TCP/P y actualmente es el protocolo de interconexión de redes más utilizado.

Este protocolo se caracteriza por ser no orientado a conexión y sin acuse de recibo. Además, define la unidad básica de transferencia de datos entre origen y el destino, atravesando toda la red. El software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes que son llamados datagramas y presentan las siguientes características:

- Es no orientado a conexión debido a que cada uno de los paquetes pueden seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.

- Es sin acuse de recibo porque los paquetes pueden perderse, dañarse o llegar retrasados.

- Cada datagrama es tratado en la red de manera independiente de los demás.

El protocolo entre entidades IP se describe mejor mediante la referencia al formato del datagrama IP, mostrado en la figura 3.2. Los campos son los siguientes:

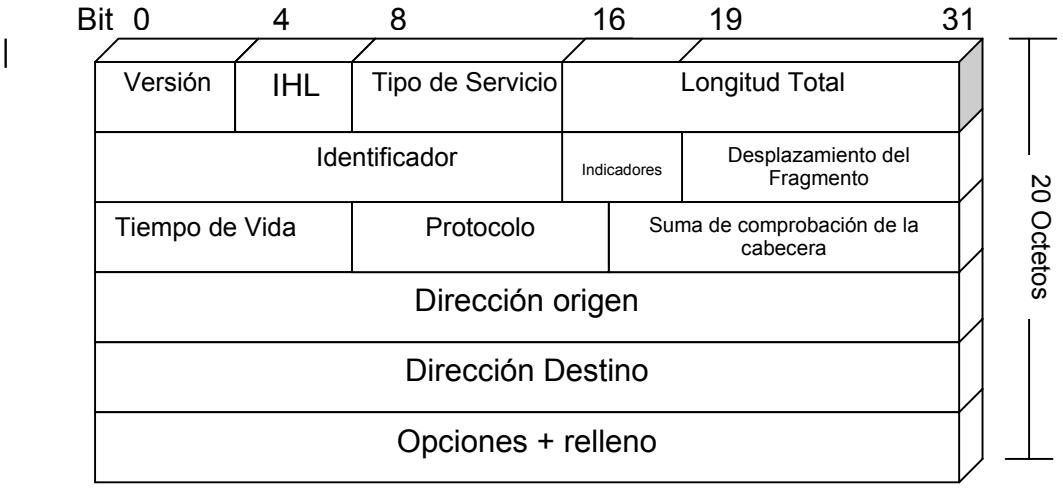


Figura 3.2 Cabecera TCP.

- **Versión (4 bits):** Indica el número de la versión del protocolo, para permitir la evolución del protocolo.

- **Longitud de la cabecera Internet (IHL, "Internet header length") (4bits):** Longitud de la cabecera expresada en palabras de 32 bits. El valor mínimo es de cinco, correspondiente a una longitud de la cabecera mínima de 20 octetos.

- **Tipo de servicio (8 bits):** Especifica los parámetros de seguridad, prioridad, retardo y rendimiento.

- **Longitud total (16 bits):** Longitud total de datagrama, en octetos

- Identificador: Un número de secuencia que, junto a la dirección origen y destino y el protocolo usuario se utilizan para identificar de forma única un datagrama. Por tanto, el identificador debe ser único para la dirección origen del datagrama, la dirección destino y el protocolo usuario durante el tiempo en el que el datagrama permanece en el conjunto de redes.

- **Indicadores (3 bits):** Solamente dos de estos tres bits están actualmente definidos. El bit "Más" se usa para segmentación y reensamblado, como se ha explicado previamente. El bit del "No fragmentación" prohíbe la fragmentación cuando es 1. este bit es útil para conocer si el destino tiene la capacidad de

reensamblar fragmentos. Sin embargo, si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo en una subred en la ruta. Por tanto, cuando el bit vale 1, es aconsejable usar encaminamiento por la fuente para evitar subredes con tamaños de paquetes máximos pequeños.

- **Desplazamiento de fragmento (13 bits):** Indica el lugar donde se sitúa el fragmento dentro del datagrama original, medido en unidades de 64 bits. Esto implica que todos los fragmentos excepto el último contienen un campo de datos con una longitud múltiplo de 64 bits.

- **Tiempo de vida (8 bits):** medido en saltos de dispositivos de encaminamiento.

- **Suma de comprobación de la cabecera (16 bits):** solamente se aplica a la cabecera un código de detección de errores. Ya que algunos campos de la cabecera pueden cambiar durante el viaje (por ejemplo, el tiempo de vida, campos relacionados con la segmentación), este valor se verifica y recalcula en cada dispositivo de encaminamiento. El campo suma de comprobación es la suma complemento a uno de todas las palabras de 16 bits en la cabecera. Por motivos de cálculo, este campo se inicializa a sí mismo a un valor de todo cero.

- **Dirección origen (32 bits):** codificada para permitir una aceptación variable de bits para especificar la red y el sistema final conectado a la red especificada.(7 y 24 bits, 14 y 16 bits, o 21 by 8 bits).

- **Dirección destino (32 bits): Igual** que el campo anterior.

- **Opciones (variable):** contiene las opciones solicitadas por el usuario que envía los datos.

- **Relleno (variable):** Se usa para asegurar que la cabecera del datagrama tengas una longitud múltiplo de 32 bits.

- **Datos (variable):** el campo de datos debe tener una longitud múltiplo de 8 bits. Máxima longitud de un datagrama (campos de datos más cabecera) es de 65535 octetos.

El protocolo IP maneja una serie de opciones de calidad de servicio:

Precedencia: una medida de la importancia relativa del datagrama. Se utilizan ocho niveles de presentación. IP tratará de proporcionar un tratamiento preferencial a los datagramas con precedencias superiores.

Seguridad: Se puede especificar uno de dos niveles: normal o alto. Un valor alto indica una petición para que se intente minimizar la probabilidad de que este datagrama se pierda o resulte dañado.

Retardo: Se puede especificar uno de dos niveles: normal o bajo. Un valor bajo indica una petición para minimizar el retardo que experimentará este datagrama.

Rendimiento: Se puede especificar uno de dos niveles: normal o alto. Un valor alto indica una petición para maximizar el rendimiento para este datagrama.

3.3.1 Direccionamiento IP

Los campos dirección origen y destino en la cabecera IP contienen cada uno una dirección Internet global de 32 bits, que generalmente consta de un identificador de computador. La dirección está codificada para permitir una asignación variable, de bits para especificar la red y el computador tal como se muestra en la figura 3.3. Este esquema de codificación proporciona flexibilidad al asignar las direcciones de los computadores y permitir una mezcla de tamaños de red en un conjunto de redes. En particular, existen tres clases de redes que se pueden asociar a las siguientes condiciones:

- Clase A: Pocas redes, cada una con muchos computadores

Tipo	Bit de orden alto	Dirección más baja	Dirección más alta
A	0	1.0.0.0	126.0.0.0

- Clase B: Un número medio de redes, cada una con un número medio de computadores.

Tipo	Bit de orden alto	Dirección más baja	Dirección más alta
B	10	128.0.0.0	191.255.0.0

- Clase C: Muchas redes, cada una con pocos computadores.

Tipo	Bit de orden alto	Dirección más baja	Dirección más alta
A	110	192.0.1.0	223.255.255.0

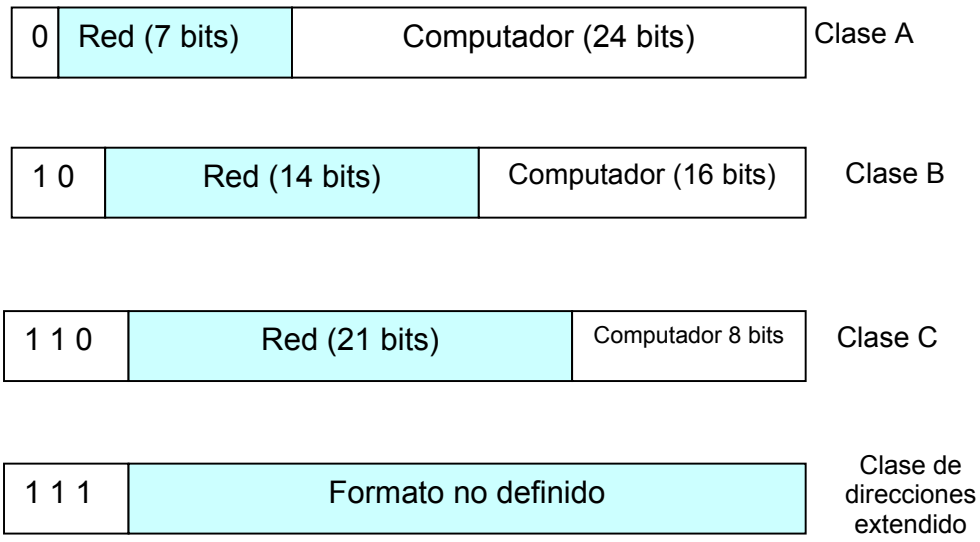


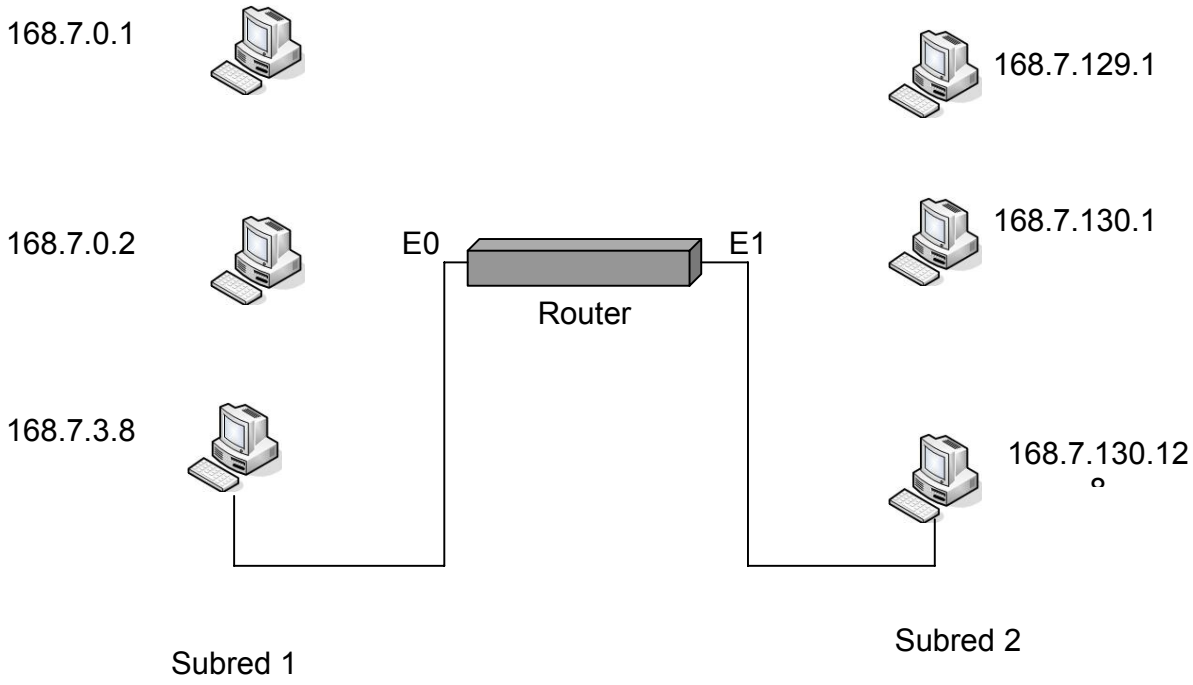
Figura 3.3. Formato de direcciones IP

En un entorno particular, podría ser mejor utilizar todas las direcciones de una clase. Por ejemplo, en un conjunto de redes de una entidad, constante en un gran número de redes de área local departamentales, se necesitaría usar direcciones Clase C exclusivamente. Sin embargo, el formato de las direcciones es tal que es posible mezclar las tres clases de direcciones en el mismo conjunto de redes; esto es lo que se hace en el caso de la misma Internet. En el caso de un conjunto de redes formado por pocas redes grandes, muchas redes pequeñas y algunas redes de tamaño mediano, es apropiado utilizar una mezcla de clases de direcciones.

3.3.2 Subredes

Con el incremento en el uso de la tecnología de información y de ahí el número de computadoras conectadas a una típica red corporativa, la estricta división en el esquema de direccionamiento IP en las clases A, B Y C es muy limitada, por ello se ha buscado una solución a través del uso de direccionamiento de subredes.

Las subredes aumentan el control del manejo de la red en el espacio de dirección y provee un mecanismo para usar routers cuando solamente uno o un número pequeño de redes esta disponible. El mecanismo para crear subredes es la mascara de subred, un número de 32 bits (4 octetos de de 8 bits cada uno) el cual está ligado con la dirección IP y la dirección de red. Las subredes dividen en un rango normal de identificaciones de host (16 millones para la clase A, 65,534 para la clase B y 254 para la clase C) en un número de subredes y un número reducido de host en cada subred. El producto de estos dos números no puede exceder el número original de host.



Tipo	Red	Mascara
B	168.7.0.0	255.255. 128.0

Figura 3.4 Ejemplo de Subred

A continuación se muestra un ejemplo de la segmentación en subredes de una red clase C:

Dada la dirección IP: 192.3.0.0 segmente la red en 8 partes y calcule la mascara.

Desarrollo

1. Determinar la clase de dirección IP que se esta trabajando, para definir el primer octeto de equipo.

1.

2. Se determina el número de bits significativos del primer octeto de equipos de la clase:

2.

$2^{n\ bits}$ = # de subredes

$2^{n\ bits}$ = 8 subredes

192	3	0	00000000

n = 3 bit significativos

Primer octeto de equipo de la clase

3. Se construye la tabla con base en la sustitución ordenada de los bits significativos:

Subredes	Bits	Dirección Inicial	Dirección Final
S1	000	192.3.0.0	192.3.0.31
S2	001	192.3.0.32	192.3.0.63
S3	010	192.3.0.64	192.3.0.95
S4	011	192.3.0.96	192.3.0.127
S5	100	192.3.0.128	192.3.0.159
S6	101	192.3.0.160	192.3.0.191
S7	110	192.3.0.192	192.3.0.223
S8	111	192.3.0.224	192.3.0.255

La mascara se calcula remplazando los 3 bits significativos llenos en el primer octeto de equipos de la clase:

Mascara de subred: 255.255. 255. 224

255	255	255	11100000

Primer octeto de equipo de la clase

Se debe tener en cuenta del ejercicio anterior que de las 32 direcciones de host de cada rango solo se toman 30, debido a que el numero host inicial es usualmente reservado para utilizarlo en la dirección como prueba dentro de la misma subred/red y el valor de host final del rango es utilizado para seleccionar todos los hosts (Broadcast).

3.4 Protocolos de encaminamiento

Dependiendo de la complejidad de la red se pueden utilizar dos tipos de encaminamiento:

- **Estático**: Se utiliza en redes sencillas.

- **Dinámico:** Se utiliza en redes complejas.

Al considerar las funciones de encadenamiento de los dispositivos de encadenamiento se deben distinguir dos conceptos importantes:

- **La información de encadenamiento**: Información sobre la topología y retardo del conjunto de redes.

- **Algoritmo de encaminamiento:** Algoritmo utilizado para la toma de decisiones de encaminamiento para un datagrama particular, basándose en la información de encaminamiento actual.

La función de encaminamiento se puede dividir en:

- Encaminamiento entre sistemas finales (ES, “end Systems”) y dispositivos de encaminamiento

- Encaminamiento entre dispositivos de encaminamiento

La división anterior se debe a que existen diferencias fundamentales entre lo que debe conocer un ES para encaminar los paquetes y lo que debe conocer un dispositivo de encadenamiento.

Existen dos tipos de protocolos de encaminamiento (ver figura 3.5):

- Protocolo de pasarela interior
- Protocolo de pasarela de frontera o exterior

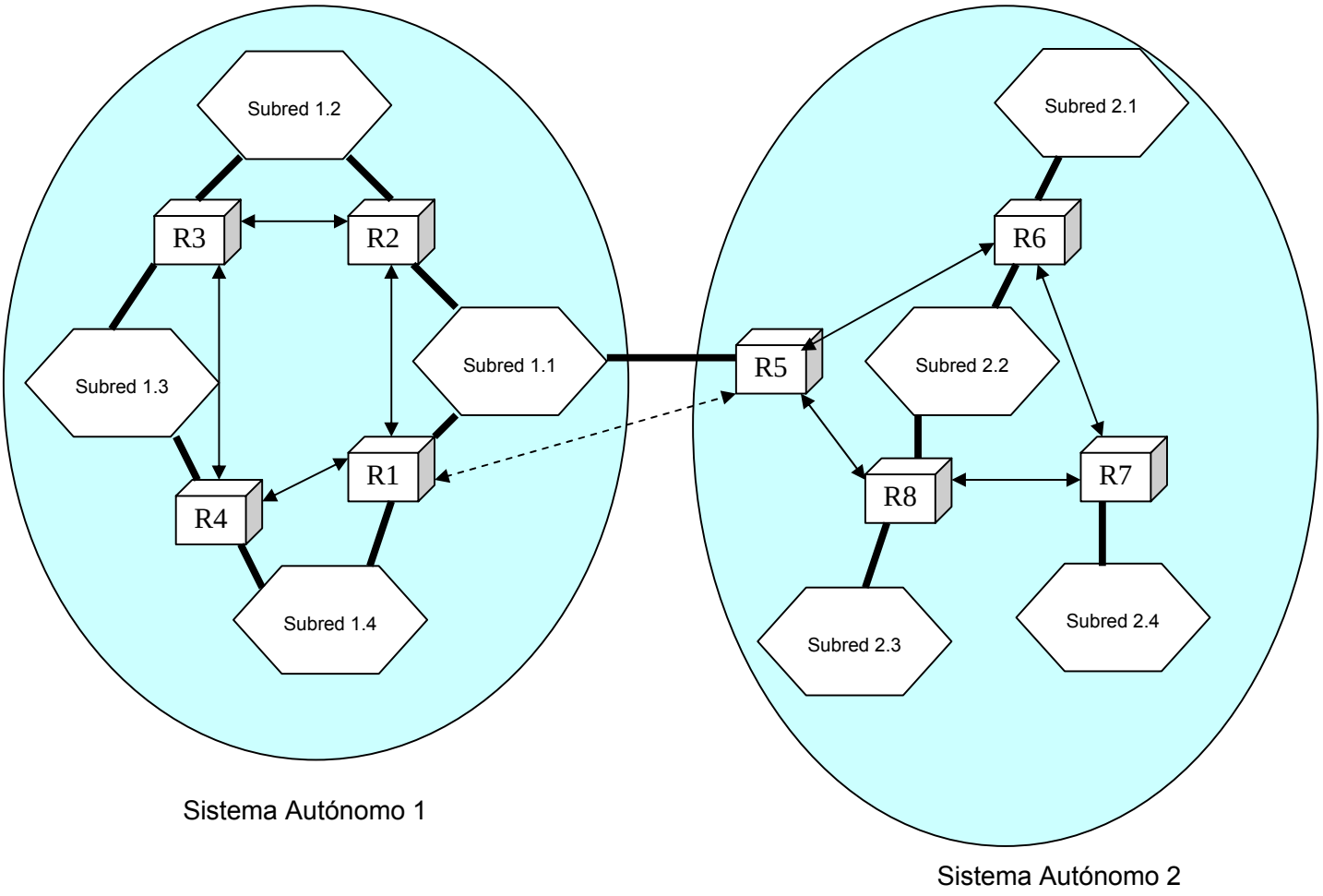


Figura 3.5. Aplicación de los protocolos de encaminamiento exterior e interior.

Protocolos de enrutamiento de pasarela interior

El protocolo de encaminamiento interior inicial en el conjunto de redes DARPA fue el protocolo de Información de Encaminamiento (RIP, "routing information protocol"), que era esencialmente el mismo protocolo que el protocolo ARPANET de la primera generación. Este protocolo requiere que cada dispositivo de encaminamiento transmita su tabla de encaminamiento completa. Aunque el algoritmo es sencillo y fácil de implementar, conforme se amplía el conjunto de

redes, la actualización de encaminamiento se hace más grande y consume significativamente más ancho de banda de la red. De acuerdo a esto, OSPF (protocolo abierto del primer camino mas corto) opera de una forma similar al algoritmo de encaminamiento ARPANET revisado. OSPF utiliza lo que se conoce como un algoritmo de encaminamiento de estado de enlace. Cada dispositivo de encaminamiento mantiene las descripciones del estado de sus enlaces locales a las subredes, y periódicamente transmite la información de estado actualizada a todos los dispositivos de encaminamiento de los que tiene conocimiento. Cada dispositivo de encaminamiento que recibe un paquete de actualización debe confirmarlo al emisor. Esta actualización produce un tráfico de encaminamiento mínimo ya que la descripciones de los son pequeños y es raro que se tenga que enviar.

El protocolo OSPF (RFC 1583) se usa muy frecuentemente como protocolo de dispositivo de encaminamiento interior en redes TCP/IP. OSPF calcula una ruta a través del conjunto de redes que suponga el menor coste para que exprese una función del retardo, la razón de datos, el coste en dólares, u otros factores. OSPF es capaz de igualar las cargas sobre múltiplex caminos de igual coste.

Cada dispositivo de encaminamiento mantiene una base de datos que refleja la topología conocida del sistema autónomo del cual forma parte. Esta topología se expresa como un grafo dirigido. El grafo consta de:

- Vértices, o nodos, de dos tipos:

  - Dispositivo de encaminamiento.

  - Red, que también puede ser de dos tipos:

    - De tránsito, si pueden transportar datos que no se han originado ni van dirigidos a un sistema final conectado a ella.
    - Terminal, si no es una red de tránsito.

- Arcos, de dos tipos:

  - Arcos de grafos que conectan dos vértices dispositivo de encaminamiento cuando los dispositivos de encaminamiento correspondientes están conectados el uno con el otro por un enlace punto-a-punto directo

  - Arcos del grafo que conectan un dispositivo de encaminamiento vértice a una red vértice cuando el dispositivo de encaminamiento está directamente conectado a la red.

Protocolos de enrutamiento de pasarela exterior

El Protocolo de pasarela frontera (GBP, “border Gateway protocol ”)se desarrollo para su uso en conjunción con conjuntos de redes que emplean la arquitectura de protocolos TCP/IP, aunque los conceptos son aplicables a cualquier conjunto de redes. BGP se ha convertido en el protocolo de dispositivo de encaminamiento exterior estándar en Internet.

Funciones

BGP se diseñó para permitir la corporación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento, llamados pasarela s en el estándar, en sistemas autónomos diferente. El protocolo opera en términos de mensajes, que se envían utilizando conexiones TCP.

BGP involucra tres procedimientos fundamentales que son:

- Adquisición de vecino
- Detección de vecino alcanzable
- Detección de red alcanzable

3.5 ICMP (INTERNET CONTROL MENSSAGES PROTOCOL)

Permite el intercambio de mensajes de control y de supervisión entre dos computadores. Toda anomalía detectada por el protocolo IP provoca el intercambio de mensajes ICMP entre los nodos de red. Este protocolo forma parte de la capa Internet y usa la facilidad de enviar paquetes IP para enviar mensajes.

ICMP es un protocolo de control que utiliza los dispositivos de encaminamiento para notificar las diferentes incidencias que puede haber en red IP. Está definido en el RFC 792. Proporciona información de realimentación sobre los problemas que ocurren y se utiliza, por ejemplo:

- El dispositivo de encaminamiento no tiene la capacidad de almacenar temporalmente el datagrama para poderlo reenviar.
- El dispositivo de encaminamiento indica a un computador que envíe el trafico por una ruta más corta (redireccionamiento de ruta). cada mensaje ICMP se encapsula en un paquete IP y luego es enviado de forma habitual. Como los mensajes ICMP se transmite en mensajes IP, no se puede garantizar que se puede garantizar que llegue a su destino.

Los mensajes ICMP incluyen lo siguiente:

- Destino inalcanzable.
- Tiempo excedido
- Problema de parámetro
- Ralentización del origen
- Redirección
- Eco
- Respuesta a eco
- Marca de tiempo
- Respuesta a la Marca de tiempo
- Petición de máscara de dirección
- Respuesta de máscara de dirección.

3.6 Dispositivos activos

3.6.1 Router

Figura 3.6 Router

Es un dispositivo o, en algunos casos, software en un computador, que determina el próximo punto (generalmente dirección lógica) en la red al cual debe ser enviado un paquete para llegar a su destino. El router trabaja en la capa de red, debe estar conectado al menos a dos redes para decir a cual de ellas enviar cada paquete que le llega, basándose en el conocimiento que tenga de las redes a las que está conectado y la defragmentación de cada trama recibida. Un router crea o mantiene una tabla de las rutas disponibles y sus condiciones, luego usa esta información de distancia y costo en un algoritmo de enrutamiento para determinar la mejor ruta por la cual evitar los paquetes que le llegan. Los routers poseen generalmente varios puertos los cuales son usados para configuración y para transmisión de datos. Normalmente un router posee al menos un puerto Ethernet (o cualquier otro estipulado por las normas IEEE, ej. Token Ring), un puerto serial y un puerto de Consola o Administración. Los puertos Ethernet en los routers son usados para conectar redes de área local, LAN, con el fin de que los hosts conectados a esta red puedan llegasr a otros puntos ubicados en diferentes redes a la de el, sea: pasando a otro puerto Ethernet, a algunos puertos seriales o a otro

puerto de datos del router. Al igual que los puertos LAN o Ethernet, los puertos seriales sirven para conectar el router con el exterior, sea una MAN o alguna WAN. Existen otros tipos de puertos, por ejemplo los puertos RAS (Remote Access Service) los cuales son usados para conexiones remotas por teléfono a alguna red del router.

Tipos de routers

Los tipos principales de routers son:

Estático: Los routers estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.

Dinámico: Los routers dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de instalación y configuración. Son más sofisticados que los routers estáticos, examinan la información de otros routers y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

Características de los tipos de Router

ESTATICOS	DINAMICOS
Instalación y configuración manual de todos los routers	Configuración manual del primer router. Detectan automáticamente redes y routers adicionales.
Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento	Pueden seleccionar una ruta en función de factores tales como coste y cantidad del tráfico de enlace.
Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.	Pueden decidir enviar paquetes sobre rutas alternativas.
Se consideran más seguros puesto que los administradores especifican cada ruta	Pueden mejorar la seguridad configurando manualmente el router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones

Otra clasificación de los Routers

Router central (Direccionador central): Nos permite conectar varias redes de área local

Router Periférico: El router periférico nos permite conectar redes de área local individuales.

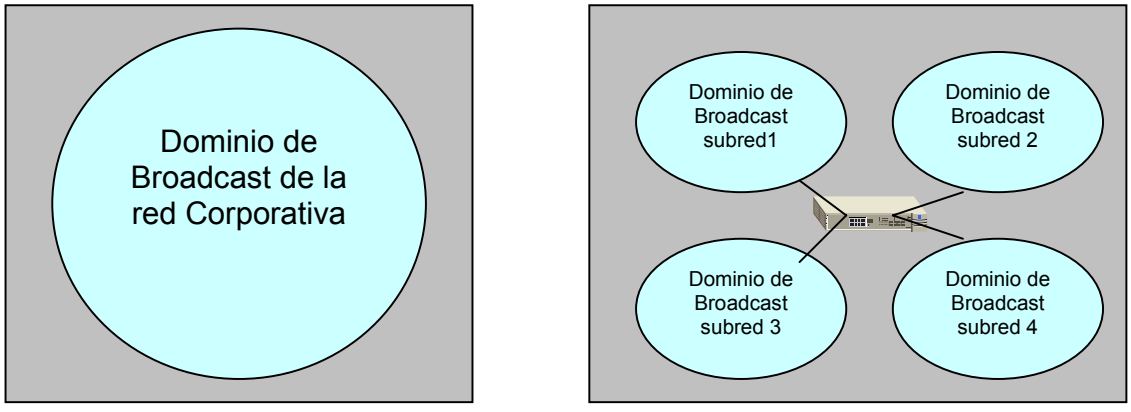
Router local: El router local viene limitado por la longitud del cable de red, ya que este funciona a su vez dentro de las limitaciones que pueda tener su controlador de dispositivos.

Router remoto: El router remoto se conecta a través de un MODEM o de una conexión remota y va más allá de las limitaciones que pueda tener su controlador de dispositivo.

Router interno: El router interno se integra dentro de un servidor de archivos de red.

Router externo: El router externo se localiza en la red, en una estación de trabajo.

Por trabajar en la capa de red los router permiten segmentar la red en dominios de Broadcast (Ver figura 3.7)



LAN sin Router

LAN con Router

Figura 3.7 Dominio de Broadcast

3.7 Multicasting por IP y por Hardware

Multicasting por IP

La comunicación IP es entre un trasmisor y un receptor. Sin embargo, en algunas aplicaciones es útil que un proceso pueda transmitir a una cantidad grande de receptores de manera simultánea. Como ejemplos están la actualización con réplica, las bases de datos distribuidas, la transmisión de cotizaciones de acciones a varias casas de bolsa y el manejo de conferencias telefónicas digitales (es decir multiparte).

El IP maneja la multitransmisión, usando direcciones clase D. cada dirección clase D identifica a un grupo de hosts. Hay 28 bits disponibles para la identificación de grupos, por lo que pueden existir 250 millones de grupos al mismo tiempo. Cuando un proceso envía un paquete a una dirección clase D, se hace un mejor esfuerzo para esfuerzo para entregarlo a todos los miembros del grupo dirigido, pero no se dan garantías. Algunos miembros podrían no recibir el paquete.

Se reconocen dos tipos de dirección de grupo: las direcciones permanentes y las temporales. Un grupo permanente siempre está ahí y no tiene que configurarse. Cada grupo permanente tiene una dirección permanente de grupo. Algunos ejemplos de direcciones permanentes de grupos son:

224.0.0.1 Todos los sistemas de una LAN
224.0.0.2 Todos los enrutadores de una LAN
224.0.0.5 Todos los enrutadores OSPF de una LAN
224.0.0.6 Todos los enrutadores OSPF designados de una LAN

Difusión por hardware

La Multidifusión por hardware tiene las siguientes características:

- La entrega por difusión significa que la red entrega una copia de un paquete para cada destino.

- El usuario especifica la entrega de difusión enviando el paquete hacia una dirección de destino especial y reservada, llamada dirección de difusión.

- La multidifusión permite que cada máquina elija si quiere participar en ella.

- El manejo de multidifusión en Ethernet se lleva a cabo de la siguiente manera:

Ethernet utiliza el bit de orden menor de octeto de orden mayor para distinguir la dirección de unidifusión convencional (con valor 0) de la dirección de multidifusión (con valor 1)

En hexadecimal el bit de multidifusión se toma como: $01.00.00.00.00.00_{16}$.

3.8 IPv6

La limitación impuesta por el campo de de dirección de 32 bits en IPv4, ha conducido a la adopción de una nueva versión, la cual nunca se quedaría sin direcciones, resolvería varios otros problemas y sería más flexible y eficiente también. Los desarrolladores plantearon inicialmente una serie de metas que debería cumplir el protocolo:

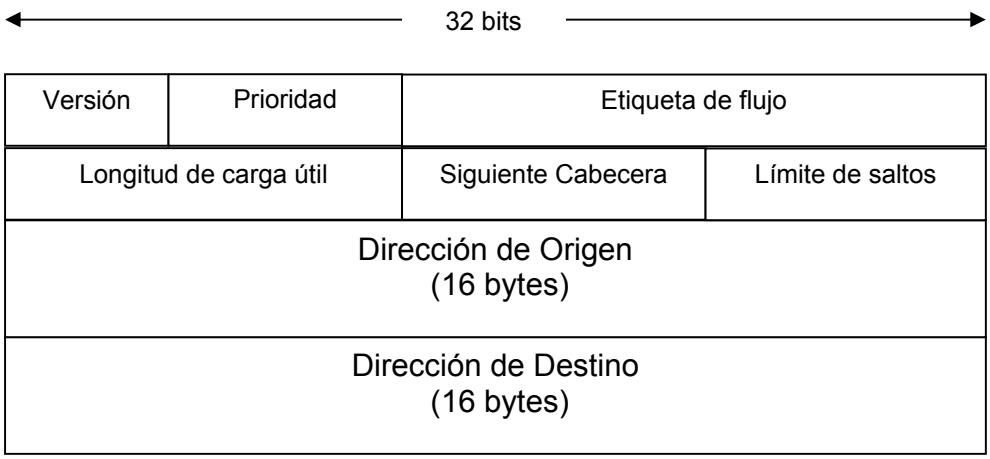


Figura 3.8. Cabecera del IPv6.

1. Manejar miles de millones de hosts, aún con asignación de espacio de direcciones ineficiente.

2. Reducir el tamaño de las tablas de enrutamiento.

3. Simplificar el protocolo, para permitir a los enrutadores el procesamiento más rápido de paquetes.

4. Proporcionar mayor seguridad (Verificación de autenticidad y confidencialidad) que el IP actual.

5. Prestar mayor atención al tipo de servicio, especialmente, con datos en tiempo real.

6. Ayudar a la multitransmisión permitiendo la especificación de alcances-

7. Posibilitar que un Host sea movil sin cambiar su dirección.

8. Permitir que el protocolo evolucione.

9. Permitir que el protocolo viejo y el nuevo coexistan por años.

El IPv6 actualmente cumple los objetivos bastante bien: mantiene las buenas características del IP, descarta y reduce las malas, y agrega nuevas donde se necesita. En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos Internet, incluidos UDP, TCP, ICMP, IGMP, OSPF, BGP y DNS.

3.8.1. IPv6 vs IPv4

A continuación se analizaran algunas mejoras IPv6 con respecto a IPv4:

- El IPv6 tiene direcciones más grandes que el IPv4; son de 16 Byte de longitud, lo que resuelve el problema que se buscaba resolver: proporcionar una cantidad prácticamente ilimitada de direcciones Internet.

Por ejemplo una dirección típica en IPV4 (32 bits) es:
128.10.2.1

Y una dirección típica en IPv6 (128 bits)

FF05:0:0:0:0:0:0:B3

- La segunda mejora es la simplificación de la cabecera, que contiene solo 7 campos (contra 13 de IPv4). Este cambio permite a los enrutadores procesar con mayor rapidez los paquetes y mejorar. Por tanto, el rendimiento.

- En IPv4 se verifica el tiempo y en IPv6 se verifica el número de nodos por el que esta pasando hasta su llegada al destino final

- Otra área importante en la que IPv6 presenta avance es la seguridad.

- Por último se tenia que prestar mayor atención al tipo de servicio que en el pasado. El IPv4 de hecho tiene un campo de 8 bits dedicado a este asunto, pero con el crecimiento esperado del tráfico multimedia, se requiere mucho más.

3.9 IP Móvil

Actualmente existen usuarios de Internet que tienen computadoras portátiles y quieren mantenerse conectados a la red a pesar de que se movilicen de un lugar a otro. Inicialmente esto fue un gran problema debido a la misma naturaleza del protocolo IP, el cual funciona estableciendo previamente unas direcciones de red, que son reconocidas por todos los router del mundo. Entonces cuando un router establece en su tabla de enrutamiento la ruta para llegar a un computador, si este cambia de ubicación, el sistema entero tendría que actualizarse y conocer la nueva dirección asignada al equipo, lo que se convirtió en un problema grande debido a que habría que informar a una gran cantidad de gente, programas y bases de datos sobre el cambio.

Un grupo de trabajo de la IETF formulo varias metas deseables para que el protocolo IP móvil solucionara la problemática anteriormente mencionada. Las principales metas fueron:

1. Todo host móvil debe ser capaz de usar su dirección IP base en cualquier lugar.

2. No se permiten cambios al software de host fijos.

3. No se permiten cambios al software del enrutador ni a sus tablas.

4. la mayoria de los paquetes para host móviles no deben desviarse de su camino.

5. No debe incurrirse en carga extrema cuando un host móvil esta en su base.

Entidades y Términos del IP Móvil

- **Nodo:** Es cualquier host o enrutador

- **Nodo Móvil:** Es un nodo que cambia su punto de conexión de una red o subred a otra.

- **Agente de casa (Home Agent):** Es un nodo que esta encargado de establecer un túnel cuando un nodo de su red se ha movido ha otra. Además posee la función de reenviar los paquetes hasta ese nodo en la red donde se encuentre.

- **Agente foráneo (Foreign Agent):** Es un nodo de la red visitante que presta servicios para la movilidad mientras se encuentran registrados con él.

Care of Address: Es el punto terminal del túnel para el nodo móvil, cuando se le reenvían mensajes en su ubicación.

Existen dos tipos:

- **Foreign agent Care-of Address**: Es una dirección de un Agente Foráneo al cual el nodo móvil se encuentra registrado.

- **Co-Located Care of Address**: Es una dirección de la red local obtenida en forma externa mediante la cual este nodo se encuentra asociado a la red (por ejemplo puede ser obtenida por DHCP)

- **Red Foránea (Foreign Network):** Cualquier red diferente a la red original del nodo móvil.

- **Dirección de casa (Home Address):** Es la dirección de red original del nodo movil.

- **Enlace de movilidad (Mobility Binding)**: Es la asociación de la dirección de casa con la Care-of Address.

- **Security Parameter Index (SPI)**: Es el índice de seguridad entre un par de nodos. Valores de SPI entre 0 y 255 son reservados y no se pueden utilizar.

Funcionamiento del Protocolo

El protocolo IP móvil funciona de la siguiente manera:

1. Por medio de un mensaje los Agentes de Movilidad (Home Agent y/o Foreign Agent) publican su presencia.

2. Un nodo móvil recibe el mensaje y determina si se encuentra en su red original o en una red foránea

3. cuando el nodo móvil detecta que está localizado en su red original este operará sin los servicios de movilidad.

4. cuando el nodo móvil detecta que se encuentra en una red foránea este obtiene una Care-of Address, puede ser a través de una Foreing Agent o por alguna asignación externa como por ejemplo DHCP.

5. El nodo móvil opera a través del Home Agent para cualquier mensaje para él.

6. Los paquetes enviados al nodo móvil son interceptados por Home Agent y este lo reenvía a través del túnel al nodo. El final del túnel pueden ser o el Foreing Agent o el mismo Nodo Móvil.

7. Los paquetes enviados por el Nodo Móvil utilizan los mecanismos de enrutamiento estándares de IP.

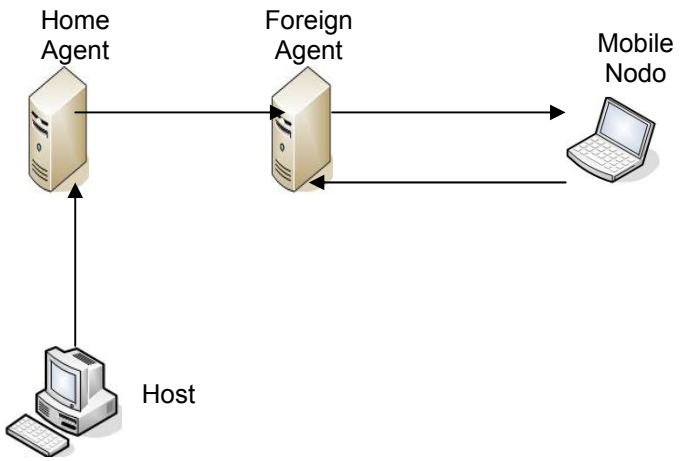


Figura 3.9. Funcionamiento del Protocolo

3.10 Voz sobre IP

Se trata de transformar la voz en "paquetes de información" manejables por una red IP (con protocolo Internet, materia que también incluye a las intranets y extranets). Gracias a algunos protocolos de comunicación es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de servicio en la comunicación.

Existen varios tipos de redes IP que se describen a continuación:

- **Internet:** El estado actual de la red no permite un uso profesional para el tráfico de voz.

- **Red IP pública:** Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.

- **Intranet:** La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc..) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

Tipos de comunicación

Existen fundamentalmente tres tipos de comunicación VoIP:

- **Teléfono a Teléfono (Ver figura 3.10)**

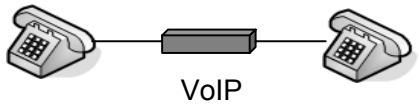


Figura 3.10. VoIP Teléfono a Teléfono

- **PC a Teléfono (Ver figura 3.11)**

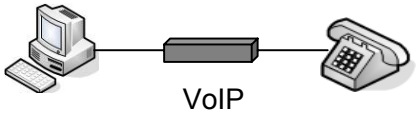


Figura 3.11. VoIP PC a Teléfono

- **PC a PC(Ver figura 3.12)**

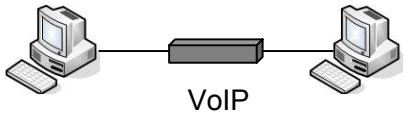


Figura 3.12. VoIP PC a PC

Elementos de una Red VoIP

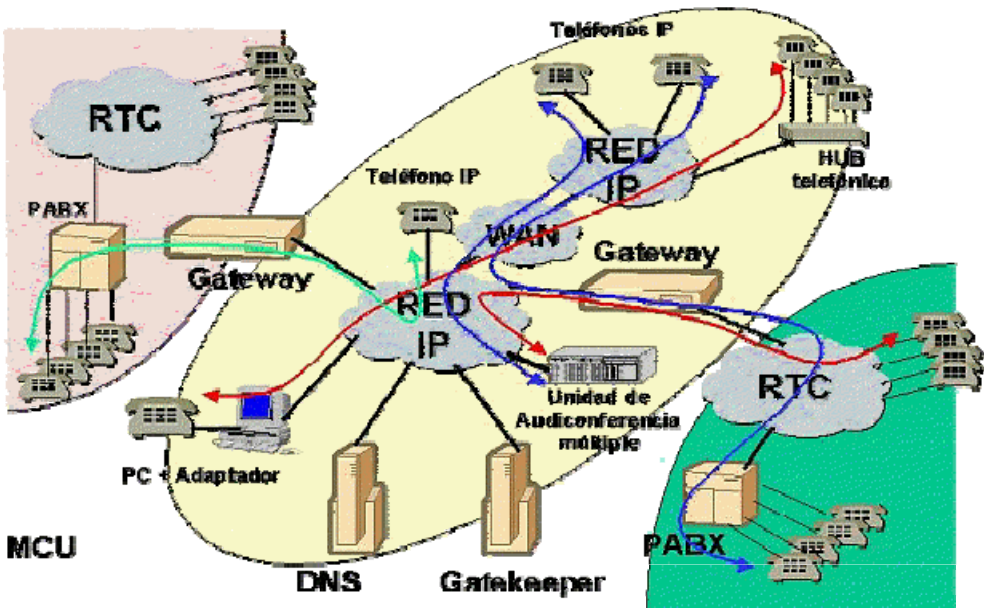


Figura 3.13. Elementos de una red VoIP

Teléfonos IP: Son los dispositivos terminales de voz de la red (en muchos casos Orígenes y destinos finales)

Adaptadores para PC: Permiten la conexión de dispositivos Telefónicos o de voz al PC

Hubs telefónicos: Permiten conectar a el varios teléfonos IP para acceder a la red IP.

GateWays (Pasarelas RTC/IP): Es un elemento esencial en la mayoría de las redes pues su misión es la de enlace zar la red VoIP con la red analógica o RDSI. Se puede considerar al Gateway Como una caja que por un lado tiene un interface LAN y por el otro cualquiera de las siguientes Interfaces:

- FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
- FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI (2B+D)
- PRI. Acceso primario RDSI (30B+D)
- G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps.

GateKeeper: Es un elemento opcional en la red, pero cuando esta presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es de gestión y control de los recursos de la red, de manera que no se produzca situaciones de saturación de la misma.

MCU (Unidades de Audio Conferencia Multiple): Permiten administrar los servicios de Audioconferencia simultaneos de la red asignando prioridad al servicio.

DNS: Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

Pila de Protocolos VoIP

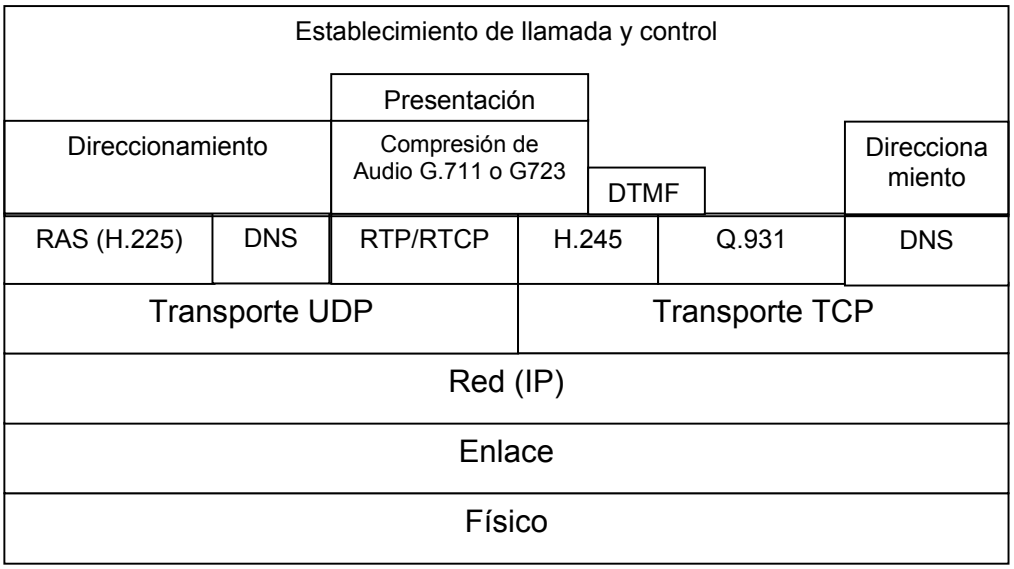


Figura 3.14 Pila de Protocolos VoIP

Todos los protocolos de la pila VoIP se orientan a 4 aspectos fundamentales de la comunicación:

- Direccionamiento
- Compresión de Voz
- Señalización
- Transmisión

Direccionamiento:

- RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.

- DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS

Compresión de voz:

- Requeridos: G.711 y G.723

- Opcionales: G.728, G.729 y G.722

Señalización:

- Q.931 Señalización inicial de llamada

- H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz

- H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz

Transmisión:

- UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

- RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción**.**

Ventajas de VoIP

- Integración sobre su Intranet de la voz como un servicio más de su red, tal como otros servicios informáticos.
- Las redes IP son la red estándar universal para la Internet, Intranets y extranets.
- Estándares efectivos (H.323)
- Interoperabilidad de diversos proveedores
- Uso de las redes de datos existentes
- Independencia de tecnologías de transporte (capa 2), asegurando la inversión.
- Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay)
- No paga SLM ni Larga Distancia en sus llamadas sobre IP.

Desventajas de VoIP

- No admite colisiones de paquetes
- El control de trafico es muy complejo
- No se puede garantizar su correcto funcionamiento (en Internet)
- La red IP
- Latencia

3.11 Redes LAN Virtuales

Una VLAN se encuentra conformada por un conjunto de dispositivos de red, los cuales funcionan de igual manera como lo hacen los de la LAN, pero con la diferencia de que las estaciones que constituyen la VLAN no necesariamente deben estar ubicadas en el mismo segmento físico.

La VLAN básicamente es una subred definida por software y es considerada como un dominio de broadcast (Ver figura 3.15).

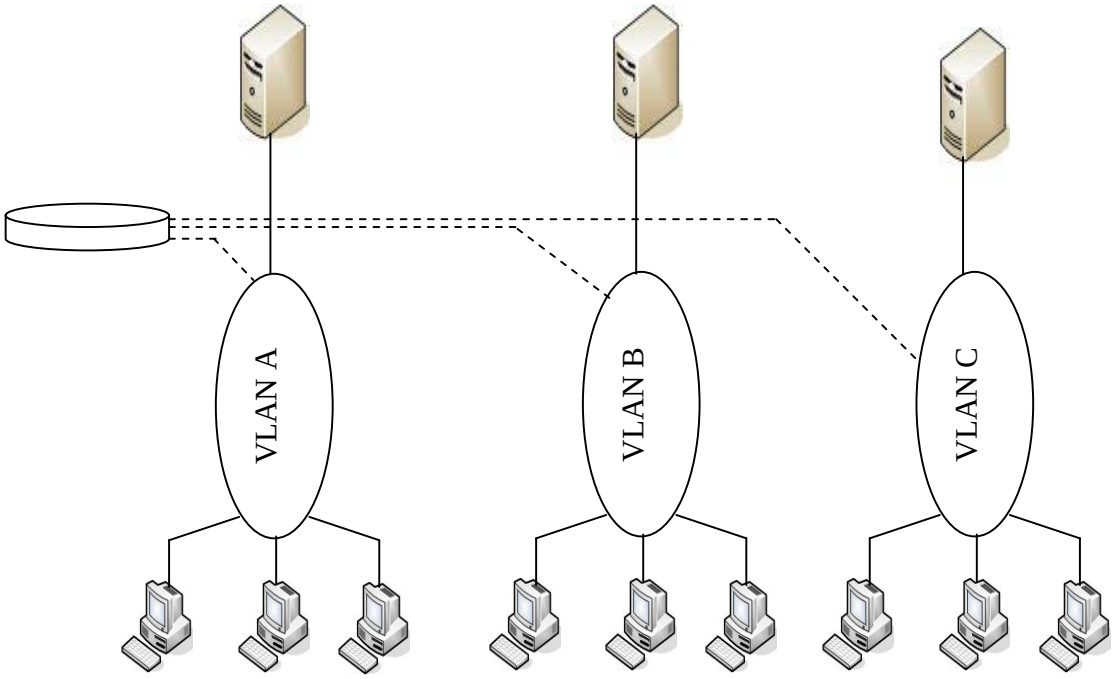


Figura 3.15. Perspectiva Lógica de una VLAN

Alguna de las características de las VLAN son las siguientes:

- Los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en distintos concentradores o hub de la misma.

- Al distribuir los usuarios de un mismo grupo lógico a través de diferentes segmentos se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios, la posibilidad de situar puentes y enrutadores entre ellos separando segmentos con diferentes tecnologías y protocolos.

Tipos de VLANs

Existen varias formas de organizar las VLAN en las redes de área local, a continuación se analizan las más utilizadas:

- **Basadas en agrupaciones por puertos**

En este caso se definen grupos de trabajo de acuerdo a agrupaciones de los puertos en los switches (ver Figura 3.16), es decir, puertos 1, 2, 3 pertenecen a la VLAN A y 4, 5 a la VLAN B. esto inicialmente se implemento en un solo Switche, luego la segunda generación se oriento a realizarlo en múltiples Switches.

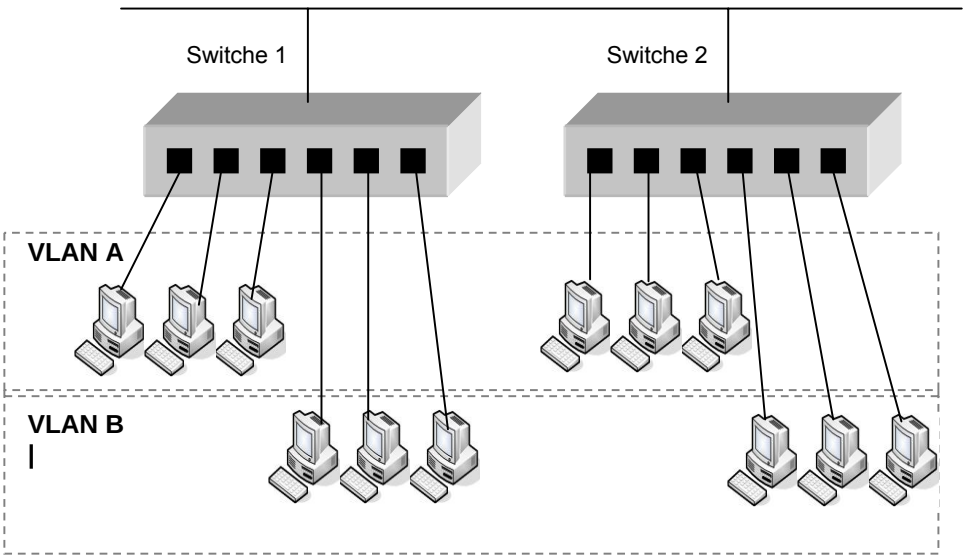


Figura 3.16. VLAN por Puertos

- **Basadas en direcciones MAC**

Como su mismo nombre lo indica, se basan en direcciones hardware presentes en cada tarjeta de red de cada equipo, esto es, al nivel de la capa 2 del modelo OSI, específicamente en la subcapa MAC. Es decir aprovechando que los switches operan con tablas de direcciones MAC, estas mismas tablas se pueden agrupar de tal manera que se puedan conformar grupos de trabajo y así crear una VLAN.

- **Basadas en capa de red**

En este caso existen dos posibilidades, primera basadas en direcciones IP, y segunda basadas en tipos de protocolos de la capa 3. de esta manera, desde el punto de vista del Switche, este inspecciona los números IP de las tramas que le lleguen o simplemente que le llegan o simplemente sirve de puente entre las VLANs definidas para diferentes protocolos. No se lleva a cabo ningún tipo de ruteo o algo similar. Debido a esto, algunos proveedores incorporan cierta inteligencia a sus Switches adaptándolos con cierta s capacidades a nivel de capa 3. Esto es, habilitándolos para tener funciones asociadas con el ruteo de paquetes.

- **Basadas en grupos Multicast**

En este caso lo que se tiene es un conjunto de direcciones IP, al cual le llegan paquetes vía multicast, estos paquetes son enviados a direcciones Proxy para que a partir de aquí se definan las direcciones IP que están autorizadas a recibir el paquete, esto se hace dinámicamente. Cada estación de trabajo, obtiene la oportunidad de escoger un tipo particular de grupo con direcciones IP Multicast, rtespondiendo afirmativamente a la notificación tipo Broadcast. Esto se presenta para que las VLAN trasciendan a conexiones al nivel de WANs.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 3

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual de capitulo 3 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. ¿Realice un cuadro comparativo entre Router y Switches?

4. Investigue los Algoritmos de enrutamiento y elabore un resumen con las principales características de cada uno.

5. Realice un Laboratorio en grupo de curso referente a direcciones IP, aplicación del concepto de subredes y configuración de Router.

6. Realice un laboratorio en grupo de curso y configure una red de Voz sobre IP sencilla en la LAN del CEAD.

7. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

CAPITULO 4: LA CAPA DE TRANSPORTE

4.1 El servicio de transporte

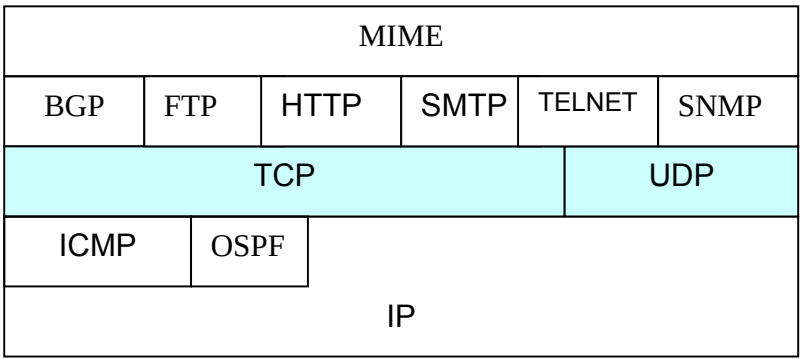


Figura 4.1. Protocolos del nivel de transporte en contexto

En este capitulo se comenzara analizando las clases de servicios que el protocolo de transporte puede o debería proporcionar a las capas superiores. La figura 4.2 sitúa el servicio de transporte (TS) en su contexto. En un sistema, existente una cantidad de transporte que proporciona servicios a los usuarios TS, que puede ser un proceso de aplicación o una entidad del protocolo de sesión. Esta entidad de transporte local se comunica con alguna entidad de transporte remota usando los servicios de alguna capa inferior, como la capa de red.

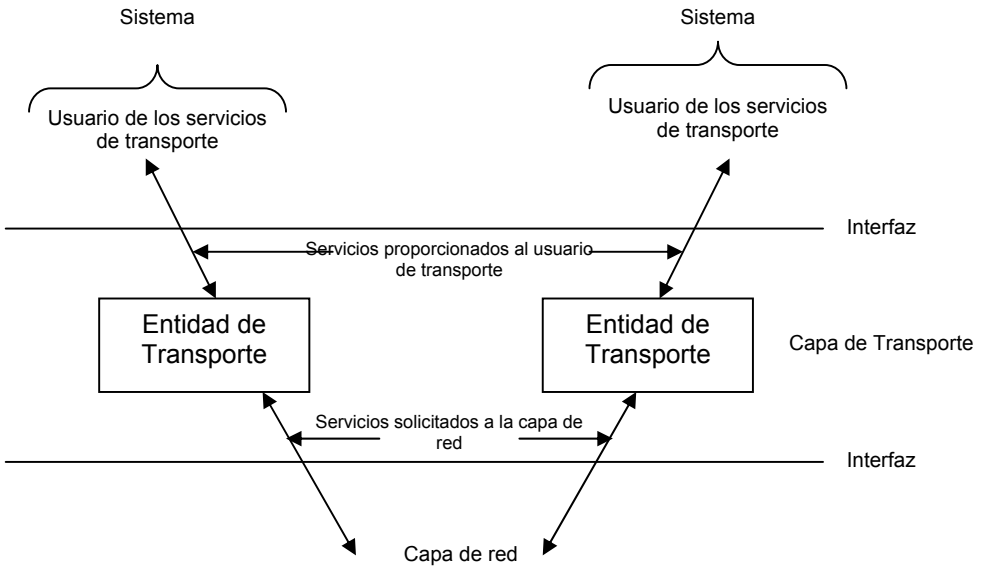


Figura 4.2 Contexto de una entidad de transporte

El servicio general proporcionado por un protocolo de transporte es el transporte extremo-a-extremo de datos de forma que se aísle al usuario del servicio de transporte (TS) de detalles de los sistemas de comunicación que sirve de base. Siendo más concreto, se debe considerar los servicios especificados que el protocolo de transporte pueda proporcionar.

4.1.1 Categorías y propiedades de la capa de transporte

Es útil considerar las siguientes categorías y propiedades de servicios para describir el servicio de transporte:

- Tipo de servicio
- Calidad de servicio
- Transferencia de datos
- Interfaz de usuario
- Supervisión de la conexión
- Transporte rápido
- Informe de estado
- Seguridad

Tipo de servicios

Son posibles dos tipos básicos de servicios orientados a conexión y no orientados a conexión o servicios data grama. Un servicio orientado a conexión proporciona el establecimiento manteniendo y cierre de una conexión lógica entre usuarios TS. Éste es el tipo de servicio de protocolo más común disponible hasta ahora y tiene una gran variedad de aplicaciones. El servicio orientado a conexión implica que el servicio generalmente es seguro.

La potencia de la opción “orientada a conexión” es clara. Proporciona unas características del tipo de conexión, tales como control de flujo, control de errores y transporte en secuencia.

Los servicios no orientados a conexión sin embargo, son más apropiados en algunos contextos. En capas inferiores (Internet, red), un servicio no orientado a conexión es más robusto. Además, representa un “denominador menos común” de los servicios que se espera ofrecer a las capas superiores. Pero, incluso en la capa de transporte y superiores existe una justificación para un servicio no orientado a conexión. Hay casos en los que la información suplementaria del inicio de la comunicación y el mantenimiento de la misma no está justificada e incluso resulta contraproducente.

En conclusión los servicios orientados a conexión son lentos pero fiables y seguros. Mientras los no orientados a conexión son rápidos pero no garantizan

confiabilidad ni seguridad, estos últimos son útiles en contextos de comunicación que requieran transmisión en tiempo real.

Calidad De Servicios QoS

La entidad de la capa de transporte debería permitir al usuario TS especificar la calidad del servicio de transmisión a ser suministrado. La entidad de transporte intentará optimizar al máximo de sus posibilidades el uso del enlace subyacente, la red, y los recursos de una colección de redes para proporcionar los servicios colectivos solicitados.

Algunos ejemplos de servicios que podrían ser solicitados son:

- Niveles de error y pérdida aceptable.
- Retardo medio y máximo aceptables
- Rendimiento medio y máximo deseado.
- Niveles de prioridad.

Por supuesto, la entidad de transporte esta limitada a las capacidades inherentes de los servicios sobre los que se apoya.

La capa de transporte también podría recurrir a otros mecanismos para intentar satisfacer los requisitos de los usuarios TS, tal como segmentar una conexión de transporte entre múltiples circuitos virtuales para aumentar el rendimiento de la red.

Transferencia de datos

El principal propósito, por supuesto, de un protocolo de transporte es transportar datos entre dos entidades de transporte. Ambos, datos de usuario y datos de control deben ser transferidos por el mismo canal o por canales separados. En esta capa se tiene que proporcionar un servicio duplex. Los modos semiduplex y simplex se podrían ofrecer para permitir peculiaridades de usuarios TS particulares.

Interfaz de usuario

No está claro que el mecanismo exacto de interfaz de usuario con protocolo de transporte debería ser normalizado. Más bien, debería estar optimizado para el entorno de la estación. Por ejemplo, los servicios de una entidad de transporte podría ser invocados por:

- Llamadas a procedimiento.

- Paso de los datos y parámetros a un proceso a través de buzón.
- Uso de acceso directo a memoria (DMA) entre un computador usuario y un procesador terminal que contiene la unidad transporte.

Supervisión de la conexión

Cuando se suministra un servicio orientado a conexión, la entidad de transporte es responsable de establecer y dar fin a la conexión. Se debería suministrar un procedimiento de establecimiento de la conexión simétrico, que permita a cualquiera de los dos usuarios TS iniciar el establecimiento de la conexión. También se podría suministrar un procedimiento simétrico para las conexiones simplex.

Dar fin a una conexión se puede realizar de forma abrupta u ordenada. De una forma abrupta, los datos que estén en tránsito se pueden perder. Hacerlo de una forma ordenada previene a cada lado de la conexión para que no se desconecte hasta que todos los datos hayan sido transferidos.

Transporte rápido

El transporte rápido de datos es un servicio similar al que proporcionan las clases de prioridad. Algunos datos enviados al servicio de transporte podrían reemplazar a datos que se han enviado previamente. La entidad de transporte se esforzará por transmitir los datos tan rápido como sea posible. En el extremo receptor, la entidad de transporte enviará una interrupción al usuario TS para notificarle la recepción de los datos urgentes. Así, el servicio de datos urgentes es, en esencia, un mecanismo de interrupción, y se utiliza para transferir datos urgentes ocasionales, tales como un carácter de cancelación (break) proveniente de un Terminal o una condición de alarma. En contraste, un servicio de prioridad podría dedicar recursos y ajustar parámetros de forma que, en promedio, los datos con prioridad más altas sean transportados más rápidamente.

Informe de estado

Un servicio de informe de estado permite al usuario TS obtener o conocer información relativa a la condición o a los atributos de la entidad de transporte o conexiones de transporte. Algunos ejemplos de información de estado son:

- Características de las prestaciones de una conexión (por ejemplo, rendimiento, retardo medio).
- Direcciones (de red, transporte).
- Tipo de protocolo en uso.
- Valores actuales de los temporizadores.

- Estado de la “máquina” de transporte que realiza la conexión.
- Degradación de la calidad del servicio requerido.

Seguridad

La entidad de transporte puede proporcionar una variedad de servicios de seguridad. El acceso de control puede ser proporcionado en la forma de verificaciones locales del envío o verificaciones remotas del receptor. El servicio de transporte puede también incluir encriptado/desencriptado de los datos en caso de ser requeridos. Finalmente, la entidad de transporte puede ser capaz de encaminar los datos a través de conexiones o nodos seguros si este servicio está disponible como recurso de la transmisión.

4.1.2 Servicios diferenciados (DiffServer)

La esencia de DiffeServ consiste en dividir el tráfico en múltiples clases y tratarlas de diferente forma:

DiffServ renombra al campo ToS (IP) como DS Field (Differented Services Field).

Por ejemplo una aplicación de los servicios diferenciados es de utilidad en un Proveedor de Sevicios de Internet (ISP), donde el cliente debe tener un SLA (Service Level Agreement) con su ISP. En este caso los servicios son:

- Expedited Forwaring Serveces (Premium): servicio con confiabilidad, baja demora y bajo Jitter (versión de la demora).

- Gold, silver y Bronze (Assured): Servicio con Confiabilidad y ciertos tiempo de transmisión.

- Best Effort: Servicio tradicional de Internet.

4.1.3 Servicios integrados (IntServ)

La capa de transporte permite ofrecer tres clases de servicios:

- Servicio Garantizado (GS)
- Carga Controlada (CL)
- Best Effort: Servicio tradicional de Internet

Otra caracteristica importante de es que la capa de transporte asocia la integración de servicios con la señalización RSVP.

IntServ es mapeado sobre algunas tecnologías de 2do nivel:

- Ethernet 802.1 IP
- ATM
- PPP

4.2 Elementos de los protocolos de transporte

En ciertos aspectos, los protocolos de transporte se parecen a los protocolos de enlace de datos. Las principales diferencias entre el nivel de transporte y el de enlace son las siguientes:

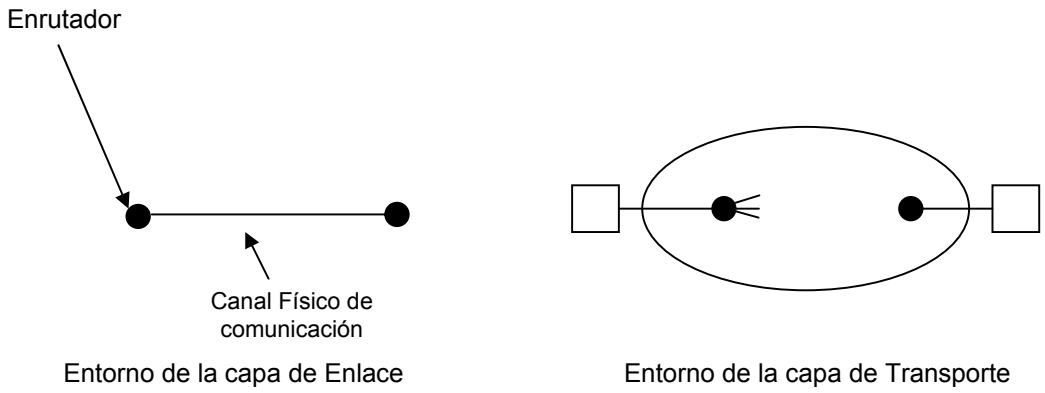


Figura 4.3. Entornos capa de Enlace de Datos y de Transporte

- El retardo que se observa en el nivel de transporte es mucho mayor que en el de enlace.

- En el nivel de enlace el medio físico entre las dos entidades tiene una capacidad de almacenamiento de información normalmente muy reducida y siempre la misma. En el de transporte los enrutadores intermedios pueden tener una capacidad considerable y ésta puede variar con el estado de la red.

- En el nivel de enlace se asegura que han salido del emisor (salvo que se pierdan, en cuyo caso no llegarán), en el nivel de transporte esto es cierto sólo cuando se utiliza un servicio no orientado a conexión el nivel de red. Si se utiliza un servicio no orientado a conexión el receptor podría recibir los datos en orden distinto al de emisor

- En el nivel de enlace las dos entidades se ven directamente (suponiendo una comunicación dúplex) lo que permite que el emisor sepa en todo momento si el receptor está operativo, y el operador sabe que los datos recibidos corresponden todos a una misma sesión del emisor. En el nivel de transporte la comunicación es directa, el emisor podría enviar datos, quedar fuera de servicio y más tarde entrar en funcionamiento otra vez. Si no se adoptan las medidas oportunas el receptor podría recibir todos esos datos sin siquiera percatarse de que corresponden a dos sesiones distintas del emisor o, incluso, podría pertenecer a dos usuarios distintos.

La capa de transporte debe de garantizar que sus protocolos cuenten con una serie de elementos fundamentales para el proceso de transporte de adatos entre emisor y receptor. Estos son:

- Direccionamiento
- Establecimiento de una conexión
- Liberación de una conexión
- Control de flujo y buffers
- Multiplexión
- Recuperación de caídas

4.3 El protocolo TCP

TCP está diseñado para proporcionar una comunicación segura entre procesos (usuarios TCP) paritarios a través de una gran variedad de redes seguras así como a través de un conjunto de redes interconectadas. Funcionalmente, es equivalente al protocolo de transporte ISO Capa 4. A diferencia del modelo OSI, TCP está intercambian un flujo de datos. Esto es, que TCP intercambian los datos. Los datos se sitúan en memorias temporales y son transmitidos por el protocolo TCP en segmentos. TCP proporciona seguridad y etiquetado de precedencia. Además, TCP suministra dos funciones útiles para etiquetar datos: cargar y urgente:

- **Cargar flujo de datos:** Normalmente, TCP decide cuando se ha acumulado suficientes datos para formar un segmento para se transmisión. El usuario TCP puede requerir que TCP transmita todos los datos pendientes a los que incluye una etiqueta con un indicador de carga. En el extremo receptor, TCP entregará los datos al usuario en la misma forma. Un usuario puede requerir esto si en los datos se detecta una interrupción lógica.

- **Indicación de datos urgentes:** Esta posibilidad proporciona un medio para informar al usuario TCP destino que en el flujo de datos entrantes existen datos

significativos o “urgentes ”. es responsabilidad de usuario destino realizar la acción apropiada.

Como en IP, los servicios suministrados por TCP se define en términos de primitivas y parámetros. Los servicios proporcionados por TCP son considerablemente más ricos que los proporcionados por IP y, por tanto, el conjunto de primitivas y parámetros es más complejo.
Las dos ordenes de establecimiento pasivo indican el deseo del usuario TCP de aceptar una petición de conexión. El establecimiento activo con datos permite al usuario comenzar transmitiendo datos con el establecimiento de la conexión.

Formato de la cabecera TCP

TCP utiliza un único tipo de unidad de datos de protocolo, llamado segmento TCP. Ya que la cabecera debe servir para implementar todos los mecanismos del protocolo, ésta es más bien grande, con un a longitud mínima de 20 octetos. Los campos son los siguientes:

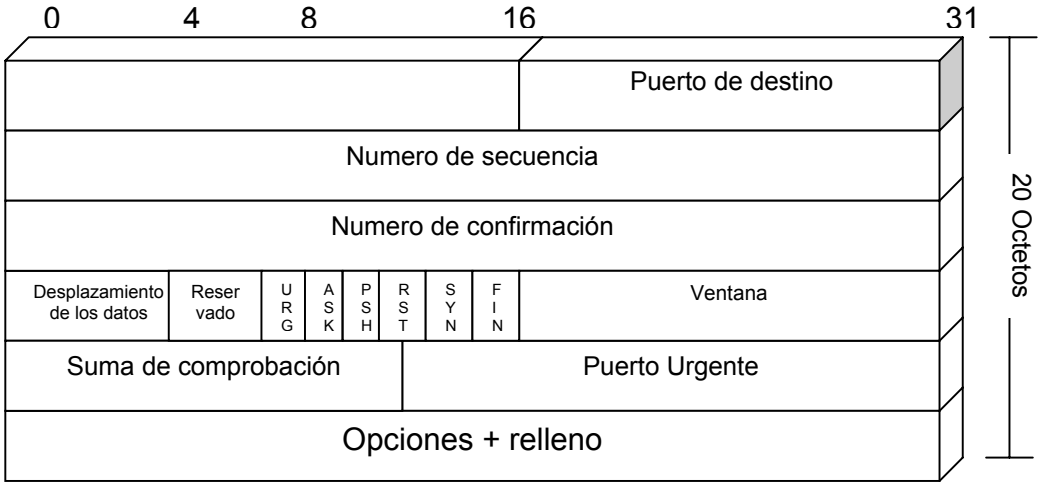


Figura 4.4. Cabecera TCP

- **Puerto origen (16 bit):** punto de acceso del servicio origen

- **Puerto destino (16 bit):** punto de acceso del servicio destino

- **Número de secuencias (32 bits):** número de secuencias del primer octeto en este segmento excepto si el indicador SYN esta presente. Si el indicador SYN está presente, es el número de secuencias iniciales (ISN, “inicial sequence number”) y en este caso el primer octeto de datos es el ISN+1.

- **Número de confirmación (32 bits):** una confirmación incorporada (“piggybacking”).

- **Longitud de la cabecera (4 bits):** número de palabras de 32 bits en la cabecera.

- **Reservados (6 bits):** bits reservados para un uso futuro.

- **Indicadores (6 bits):**

  URG: el campo puntero urgente es válido.
  ARK: el campo de confirmación es válido.
  PSH: función de carga.
  RST: puesta a cero de la conexión.
  SYN: sincronizar los números de secuencia.
  FIN: el emisor tiene más datos.

- **Ventana (16 bits):** asignación de créditos de control de flujo, en octetos. Contiene el número de octetos de datos comenzando con el que se indica en el campo de confirmación y que el que envía dispuesto a aceptar.

- **Suma de verificación (16 bits):** el complemento a uno de la suma módulo 2 -1 de todas las palabras de 16 bits en el segmento más una seudo-cabecera descrita más abajo.

- **Puntero urgente (16 bits):** señala el octeto que sigue a los datos urgentes. Esto permite al receptor conocer cuantos datos urgentes llegan.

- **Opciones (variable):** si está presente, solamente se define una opción, que especifica el tamaño máximo de los campos del segmento que será aceptado.

Algunos de los campos en la cabecera TCP requieren una descripción más detallada. El puerto origen y el puerto destino especifican el usuario origen y destino de TCP. Como con IP, existe un número de usuarios comunes de TCP a los que se les ha asignado números. Estos números están reservados para ese propósito en cualquier implementación. Otros números de puertos deben ser asignados de mutuo acuerdo entre las partes que se comunican.

El número de secuencia y el número de confirmación hace referencia a octetos en lugar de al segmento entero. Por ejemplo, si un segmento contiene el número de secuencia 1000 e incluye 600 octetos de datos, el número de secuencias se refiere al primer octeto en el campo de datos; el segmento siguiente en orden lógico tendrá el número de secuencia 1600. Es por eso que TCP está orientado a flujo lógicamente: acepta un flujo de datos del usuario, los agrupa en segmentos según él vea y numera cada octeto en el flujo.

El campo suma de verificación se aplica a todo el segmento entero más una seudo-cabecera Incorporada en el momento del cálculo (tanto en la transmisión como en la recepción). La seudo-cabecera incluye los siguientes cambios de la cabecera IP: dirección interna origen y destino, el protocolo y un campo longitud del segmento. Con la inclusión de la seudo-cabecera, TCP se protege a si mismo de una transmisión errónea de IP. Esto es, si IP lleva un segmento de un computador erróneo, aunque el segmento este libre de errores, la entidad TCP receptora detectará el error de transmisión. Si TCP se está usando a través de IPv6, la seudo-cabecera será diferente.

Se podría pensar que algunos campos están ausentes de la cabecera TCP, y es verdad en este caso. TCP está diseñado específicamente par atrabajar con IP. Por tanto, algunos parámetros de usuario se pasan a través de TCP a IP par su inclusión en la cabecera IP. Los más relevantes son:

- Prioridad: un campo de 3 bits.
- Retardo-normal/bajo-retardo
- Rendimiento-normal/ rendimiento-alto.
- Seguridad-normal7alta-seguridad.
- Protección: un campo de 11 bits.

Merece observar que esta unión TCP/IP significa que la información suplementaria mínima requerida para cada unidad de datos es en realidad para cada unidad de datos es en realidad de 40 octetos.

4.4 El protocolo UDP

UDP proporciona un servicio no orientado a conexión para los procedimientos de la capa de aplicación. Así, UDP es básicamente un servicio no seguro; la entrega y la protección contra duplicados no están garantizadas. En contrapartida se reduce la información suplementaria del protocolo lo que puede ser adecuado en muchos casos.

UDP se sitúa encima de IP. Ya que es no orientado a conexión, UDP tiene pocas funciones que hacer. Esencialmente, incorpora un direccionamiento a puerto a las capacidades de IP. Esto se ve mejor examinando la cabecera UDP. La cabecera incluye un puerto origen y un puerto destino. El campo de longitud contiene la longitud del segmento UDP entero, incluyendo la cabecera y los datos. La suma de verificación es el mismo algoritmo usado par TCP e IP. Para UDP, la suma de verificación se aplica al segmento UDP entero más una seudo-cabecera incorporada a la cabecera UDP cuando se calcula la suma y es la misma que la usada para TCP. Si se detecta un error, el segmento se descarta sin tomar ninguna medida adicional.

El campo de suma de verificación en UDP es opcional. Si no se utiliza, esté se pone todo a cero. Sin embargo, hay que indicar que la suma de verificación de IP se aplica sólo a la cabecera IP y no al campo de datos, que está compuesto, en este caso, de la cabecera UDP y los datos de usuario. Así, si UDP no implementa ningún cálculo de suma de verificación, los datos de usuarios no se comprueban.

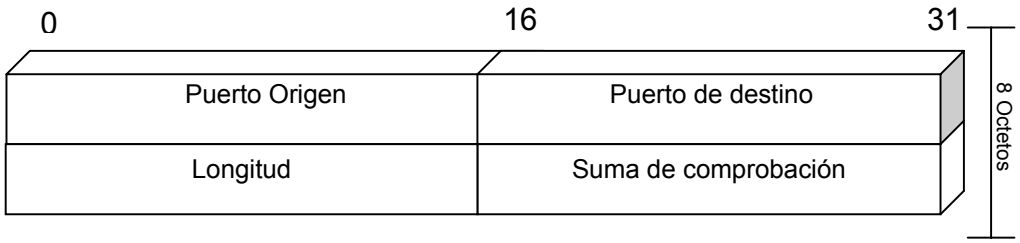


Figura 4.5. Cabecera UDP

4.5 TCP y UDP inalámbricos

En teoría, los protocolos de transporte deben ser Independientes de las tecnologías utilizadas en la capa de red. En particular, el TCP no deberá preocuparse si el IP está operando por fibra o por radio. En la práctica sí importa, puesto que la mayoría de las implementaciones de TCP han sido optimizadas cuidadosamente con base en supuestos que se cumplen en las redes alámbricas, pero no en las inalámbricas. Ignorar las propiedades de la transmisión inalámbrica puede conducir a implementaciones del TCP correctas desde el punto de vista lógico pero con un desempeño horrendo.

El problema principal es el algoritmo de control de congestionamiento. Hoy día, casi todas las implementaciones de TCP suponen que las terminaciones de temporización ocurren por congestionamiento, no por paquetes perdido. En consecuencia, al terminar un temporizador, el TCP disminuye su velocidad y envía con menor ímpetu. Lo que se pretende con este enfoque es reducir la carga de la red y aliviar así el congestionamiento.

Desafortunadamente, los enlaces de transmisión inalámbrica son muy poco confiables; pierden paquetes todo el tiempo. El enfoque adecuado para el manejo de paquetes perdidos es enviarlos nuevamente, tan pronto como sea posible. La reducción de la velocidad simplemente empeora las cosas. En efecto, al perderse un paquete en una red alambrada, el transmisor debe reducir la velocidad. Cuando se pierde uno en una red inalámbrica, el transmisor debe acelerar. Cuando el transmisor no sabe de qué clase de red se trata, es difícil tomar la decisión correcta.

Si bien el UDP no tiene los mismos problemas que el TCP, la comunicación inalámbrica también le produce dificultades. El problema principal es que los programas usan el UDP pensando que es altamente confiable; saben que no hay garantía, pero aun así esperan que sea casi perfecto. Un entorno inalámbrico estará muy lejos de serlo. En aquellos programas capaces de recuperarse de la pérdida de mensajes UDP, pasar repentinamente de un entorno en el que pueden perderse mensajes, pero rara vez ocurre, a uno en el que se pierden constantemente, puede dar pie a un desempeño desastroso.

La comunicación inalámbrica también afecta otras áreas, no sólo el desempeño. Por ejemplo, ¿cómo encuentra un host móvil una impresora local a la cual conectarse, en lugar de usar su impresora base?. Algo parecido a esto es cómo acceder a la página del WWW de la célula local., aun si no se conoce su nombre. También, los diseñadores de páginas WWW tienden a suponer que hay mucho ancho de banda disponible.

4.6 Desempeño de la Red

Los asuntos relacionados con el desempeño son muy importantes en las redes de cómputo. Cuando hay gran cantidad de computadoras conectadas entre sí, son comunes las interacciones complejas, con consecuencias imprevisibles. Frecuentemente esta complejidad conduce a un desempeño pobre, sin que nadie sepa por qué. A continuación examinaremos muchos temas relacionados con el desempeño de redes para ver los tipos de problemas que existen y lo que se puede hacer para resolverlos.

La capa de transporte no es el único lugar en el que surgen asuntos relacionados con el desempeño. Vimos algunos de ellos en la capa de red. No obstante, la capa de red tiende a ocuparse principalmente del enrutamiento y el control de congestionamiento. Los puntos más amplios, orientados al sistema, tienden a relacionarse con el transporte.

A continuación se analizaran cinco aspectos del desempeño de las redes:

1. Problemas de desempeño.
2. Medición del desempeño de una red.
3. Diseño de sistemas con mejor desempeño
4. Procesamiento TPDU rápido
5. Protocolos para redes futuras de alto desempeño.

Problemas de desempeño en las redes de cómputo

Algunos problemas de desempeño, como el congestionamiento, son causados por sobrecargas temporales de los recursos. Si repentinamente llegan más tráfico a un

enrutador del que puede manejar, se creará un congestionamiento y el desempeño bajará.

El desempeño también se degrada cuando hay un desequilibrio estructural de los recursos. Por ejemplo, si una línea de comunicación de gigabits está conectada a una PC de bajo rendimiento, la pobre CPU no será capaz de procesar los paquetes de entrada a la velocidad suficiente, y se perderá algunos. Estos paquetes se retransmitirán tarde o temprano, agregando un retardo, desperdiciando ancho de banda y reduciendo en general el desempeño.

Otro problema de desempeño que ocurre con las aplicaciones de tiempo critico como audio y vídeo es la fluctuación. Tener un medio de transmisión corto no es suficiente. También se requiere una desviación estándar pequeña. El logro de un tiempo medio de transmisión como corto con una desviación estándar requiere esfuerzos serio de ingeniería.

Medición del desempeño de las redes

Cuando una red tiene un desempeño pobre, sus usuarios frecuentemente se quejan con los operadores, exigiendo mejoras. Para mejorar el desempeño, los operadores deben primero determinar exactamente lo que ocurre. Para saberlo, los operadores deben efectuar mediciones. A continuación se analizara el ciclo básico usado para mejorar el desempeño de las redes que contiene los siguientes pasos:

1. Medir los parámetros pertinentes y el desempeño de la red.

2. Tratar de entender lo que ocurre.

3. Cambiar un parámetro.

Estos pasos se repiten hasta que el desempeño sea lo bastante bueno o que quede claro que se han hecho todas las mejoras posibles.

La medición del desempeño y los parámetros de una red tiene muchos escollos potenciales. A continuación se describen algunos de ellos:

- Asegúrese que el tamaño de la muestra es lo bastante grande

- Asegúrese que las muestras son representativas

- Tenga cuidado al usar relojes de intervalos grandes

- Asegúrese que no ocurra nada inesperado durante sus pruebas

- El caché puede arruinar las mediciones

- Entienda lo que está midiendo

- Tenga cuidado con la extrapolación de los resultados

Diseño de sistema para mejor desempeño

La medición y los ajustes pueden con frecuencia mejorar considerablemente el desempeño, pero no pueden sustituir un buen diseño original. Una red mal diseñada puede mejorar sólo hasta un límite. Más allá, tiene que rehacer desde el principio.

A continuación se mencionan algunas reglas empíricas basadas en la experiencia con muchas redes. Estas reglas se relacionan con el diseño del sistema, no sólo con el diseño de la red, ya que el software y el sistema operativo con frecuencia son más importantes que los enrutadores y las tarjetas de interfaz.

Regla #1: La velocidad de la CPU es más importante que la velocidad de la red.

Regla #2: Reducir el número de paquetes para reducir la carga extra de software.

Regla #3: Reducir al mínimo las conmutaciones de contexto.

Regla #4: Reducir al mínimo las copias.

Regla #5: Puede comprarse más ancho de banda, pero no un retardo menor.

Regla #6: Evitar el congestionamiento es mejor que recuperarse de él

Regla #7: Evitar terminaciones de temporización.

Procesamiento TPDU rápido

El desempeño de las redes generalmente es dominado por la carga extra de procesamiento de los protocolos y las TPDU, y esta situación empeora a mayores velocidades. Los protocolos deberían diseñarse para reducir al mínimo la cantidad de TPDU, de conmutaciones de contexto y de veces que se copie cada TPDU.

Protocolos para redes futuras de alto desempeño

El principio básico que deben aprender de memoria todos los diseñadores de redes de Gigabits son:

Diseñar pensando en la velocidad, no en la optimización del ancho de banda.

Los protocolos viejos con frecuencia se diseñan tratando de reducir al mínimo la cantidad de bits en el alambre, comúnmente usando campos pequeños y empacándolos en bytes y palabras. Hoy día hay más que suficiente ancho de banda. El procesamiento del protocolo es el problema, por lo que los protocolos deberían diseñarse para reducirlo al mínimo.

Una manera tentadora de acelerar el procedimiento es construir interfaces de red rápidas en hardware. Lo malo de esta estrategia es que, a menos que el protocolo sea excesivamente sencillo, “hardware” simplemente significa una tarjeta con una segunda CPU su propio programa. Para evitar que el procesador de la red sea tan caro como la CPU principal, con frecuencia se usa un chip más lento. La consecuencia de este diseño es que una buena parte del tiempo la CPU principal (rápida)está esta esperando que una segmenta CPU (lenta) haga el trabajo crítico. Es un mito pensar que la CPU principal tiene otras tareas que hacer mientras espera. Es más cuando dos CPU de propósito general se comunican, pueden ocurrir condiciones de competencia, por lo que se requieren protocolos complejos entre los dos procesadores para sincronizarlos correctamente. Generalmente el mejor enfoque es hacer que los protocolos sean sencillos y dejar que la CPU principal haga el trabajo.

Veamos ahora el asunto de la realimentación en los protocolos de alta velocidad. Debido al ciclo de retardo grande (relativamente), debe evitarse la realimentación: la señalización del receptor al transmisión tarda demasiado. Un ejemplo de realimentación es el control de la tasa de transmisión mediante un protocolo de ventana corrediza. Para evitar los retardos (grandes) inherentes en el envío de actualizaciones de ventana del receptor al transmisor, es mejor usar un protocolo basado en la tasa. En tal protocolo, el transmisor puede enviar todo lo que quiera, siempre y cuando no envíe a mayor velocidad que cierta tasa acordada de antemano entre el transmisor y el receptor.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 4

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 4 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. ¿Realice un cuadro comparativo entre los protocolos de la capa de transporte UDP y TCP?

4. Investigue otros protocolos de la capa de transporte y sus principales características.

5. Realice un Laboratorio en grupo de curso donde analice el rendimiento de su LAN y determine fortalezas y debilidades que influyen en el rendimiento de la red.

6. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

SEGUNDA UNIDAD: ADMINISTRACION DE REDES

INTRODUCCION

En esta unidad se pretende que el estudiante adquiera habilidad en el proceso de administración de redes. Se trata de explicar las diferentes herramientas administrativas con que cuenta el estudiante y que le permiten organizar la red que estén administrando y solucionar los diferentes problemas que se le puedan presentar durante el desarrollo de sus funciones de administrador de red.

El primer capitulo se refiere fundamentalmente a los conceptos básicos de la administración de redes como son: la administración de cuentas de usuario, administración de impresoras, administración de recursos de red, dominios y grupos de trabajo y las características que tienen los sistemas operativos de red.

En el segundo capitulo se profundiza un poco en los fundamentos de la administración de redes y específicamente en el tema de la auditoria de redes, que incluye el análisis de Riesgos, diseño de un plan de auditoria, implementación de un plan de auditoria, utilización de visores de sucesos, registro de seguridad, monitorización de recursos de red, y una serie de procedimientos recomendados que garantizan la correcta implementación de políticas de auditoria de redes.

El tercer capitulo se explica lo referente a la administración de copias de seguridad y restauración de datos donde se describen los requisitos para realizar una copia de seguridad, además de estudiar las diferentes estrategias para restauración de datos.

El cuarto capitulo trata todo sobre la administración de servidores de red. Como son los servidores FTP, Web, de correo electrónico y DHCP, entre otros Brindándole las herramientas necesarias al estudiante para realizar esta labor tan importante en la LAN o a nivel de cualquier Intranet.

Por ultimo en el quinto capitulo se centra en el análisis y optimización de redes que abarca temas tan importantes para el estudiante como determinar el rendimiento de la red, el tamaño y complejidad de la misma, conocimiento de los protocolos y herramientas de gestión de redes, solución de problemas comunes en redes LAN.

OBJETIVOS

- Describir las tareas necesarias para administrar una red de área local.

- Describir las tareas necesarias para administrar un sistema operativo de red.

- Que el estudiante diseñe estrategias para crear cuentas de usuarios.
- Que el estudiante conozca y aplique los procedimientos recomendaos para administrar recursos mediante permisos.
- Usar los procedimientos recomendados para configurar una impresora de red.
- Que el estudiante diseñe planes de auditoria y determine los sucesos que va a auditar.
- Describir los procedimientos recomendados para monitorizar los recursos de la red.
- Diseñar estrategias de copias de seguridad.
- Administrar servidores de Red utilizando los sistemas operativos de red.
- Monitorear redes LAN y determinar el comportamiento de la red en un punto o momento determinado.

CAPITULO 1. INTRODUCCIÓN A LA ADMINISTRACIÓN DE REDES

1.1 Administración de la red

Aún no se ha inventado una red que funcione por sí sola. Es necesario agregar nuevos usuarios y eliminar usuarios existentes, instalar y compartir nuevos recursos, y además otorgar los permisos de acceso adecuados. Los permisos de accesos son reglas asociadas a un recurso que, por lo general, consiste en un archivo de directorio o en una impresora. Los permisos regulan el acceso de los usuarios a los recursos.

Todo esto quiere decir que después de instalar una red es necesario administrarla. Todas las herramientas de administración de la red han sido consolidadas dentro del área de herramientas administrativas que se explican más adelante.

Cinco áreas de administración

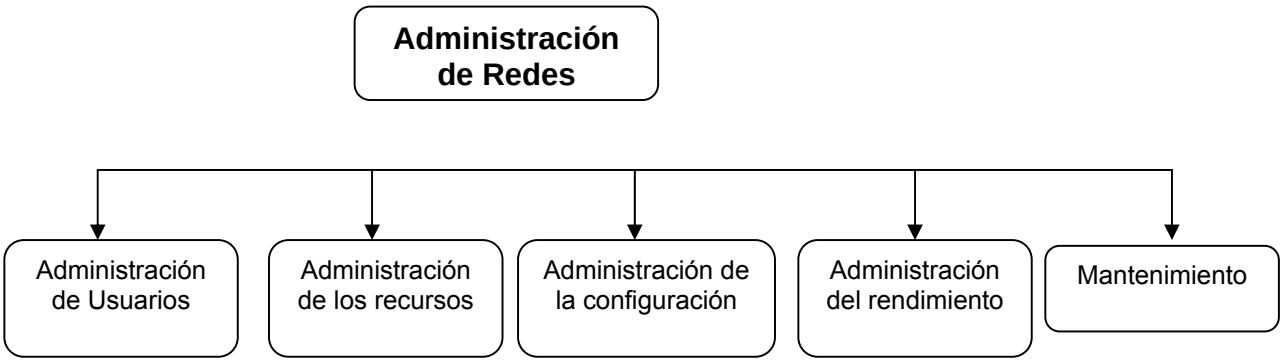


Figura 1.1 Áreas de la administración de redes

Existen cinco áreas principales destinadas a la administración de una red con las que el administrador debe estar familiarizado:

- **Administrador de usuarios:** La creación y el mantenimiento de cuentas de usuario y el acceso adecuado a los recursos.

- **Administrador de los recursos**: Implementación y soporte de los recursos de la red.

- **Administrador de la configuración**: Diseño y ampliación de la configuración original, así como el mantenimiento de la información y de la documentación de la configuración.

- **Administrador del rendimiento:** Supervisión y seguimiento de la actividad de la red para mantener y mejorar el rendimiento del sistema.

- **Mantenimiento:** prevención, detección y solución de problemas en la red.

1.2 Funciones del administrador de red

En las cinco áreas de administración es posible crear una lista de control de los deberes relacionados con la administración de la red, los cuales son responsabilidad del administrador. Esto incluye:

- Creación y administración de las cuentas de usuario.
- Seguridad.
- Entretenimiento y soporte a los usuarios según sea necesario
- Actualización del software existente e implementación del nuevo software
- Mantenimiento de los archivos
- Prevención de la pérdida de datos
- Supervisión y regulación del espacio de almacenamiento en el servidor
- Ajuste de la red para obtener el máximo rendimiento
- Copia de seguridad de los datos
- Protección de la red contra virus
- Solución de problemas
- Actualización y sustitución de componentes de la red cuando sea necesario
- Incorporación de nuevos equipos a la red

1.3 Los sistemas operativos de red

Hasta hace muy poco, el software de red de los equipos personales se agregaba a los sistemas operativos existentes. Un equipo que forma parte de una red ejecutaba dos sistemas operativos: uno automático y otro de red.

Ambos sistemas operativos tenían que estar instalados en el mismo equipo para poder realizar todas las funciones necesarias para la actividad en modo autónomo y en red. Por ejemplo, a Microsoft LAN Manager se le conocía como sistema operativo de red, pero realmente solo proporcionaba capacidades de red a sistemas operativos como MS-DOS, UNIX u OS/2.

Ahora, en la actualidad los sistemas operativos de red avanzados proporcionan toas las funciones necesarias para que un administrador de red pueda desempeñar sus funciones. Se pueden mencionar ejemplo de sistemas operativos de red reconocidos por los expertos como sistemas especializados en la labor administrativa de red:

- Linux versiones para redes.
- Windows NT Sever.
- Windows 2000 Server
- Windows 2003 Server
- Unix
- Novell Netware

En todos estos sistemas operativos, el sistema operativo autónomo y el de red se han combinado en un solo sistema operativo que ejecuta las funciones de equipo autónomo y de red. Este sistema operativo es la base para toda la actividad del hardware y del software del equipo.

Coordinación de hardware y software

El sistema operativo controla la asignación y el uso de los recursos de hardware. Como los siguientes:

- Memoria
- Utilización del CPU
- Administración y uso del disco duro
- Dispositivos periféricos (impresoras, módems, etc.)

El sistema operativo coordina la interacción entre el equipo y los programas de aplicación que se ejecutan. Es también la base con la que se construyen aplicaciones como procesadores de texto y hojas de cálculo. De hecho, los programas de aplicación se escriben pensando en que se van a usar en ciertos sistemas operativos. Los fabricantes pueden hacer notar que sus aplicaciones de

han diseñado para aprovechar las características más avanzadas de los sistemas operativos de red.

Multitarea

El soporte de la actividad de un sistema operativo de red y de la propia red es complejo. Una consideración que se debe tener en cuenta a la hora de elegir un sistema operativo para un entorno de red es la característica de ser multitarea real.

Los sistemas operativos multitarea proporcionan los medios para que un equipo procese más de una tarea a la vez. Un auténtico sistema operativo multitarea puede ejecutar tantas tareas como procesadores disponga. Cuando hay más tareas que procesadores, el equipo tiene que repartir el tiempo de manera que los procesadores disponibles dediquen cierta cantidad de tiempo a cada tarea, alternando entre las tareas hasta que todas terminen. Este sistema hace que el equipo parezca que está trabajando en varias tareas al mismo tiempo.

Hay dos tipos de tareas principales de multitarea:

Asignación prioritaria: En la multitarea de asignación prioritaria, el sistema operativo puede tomar el control del procesador sin la cooperación de la tarea.

Sin asignación prioritaria (cooperativa): En la multitarea sin asignación prioritaria, el procesador no es apartado de ninguna tarea. La propia tarea decide cuánto libera el procesador. Los programas escritos para sistemas multitareas sin asignación prioritaria tienen que proveer la liberación de control del procesador. Ningún otro programa puede ejecutarse hasta que el programa sin asignación prioritaria libere el control del procesador.

Debido a la constante interacción entre el sistema operativo autónomo y el sistema operativo de red, los sistemas multitarea de asignación prioritaria ofrecen ciertas ventajas. Por ejemplo, cuando la situación lo requiera, el sistema de asignación prioritaria puede desplazar la actividad del CPU de una tarea local a una tarea de red.

Componentes de software

Todos los sistemas de red solían ser programas de aplicación que se cargaban sobre un sistema operativo autónomo. Una diferencia significativa entre el sistema operativo de red y otros sistemas operativos es que las capacidades de red están incluidas dentro de él.

Un sistema operativo de red:

- Trata de forma conjunta todos los dispositivos y periféricos de la red.

- Coordina las funciones de todos los dispositivos y periféricos de las red
- Proporciona seguridad y acceso a los datos y los periféricos de la red.

Hay dos componentes principales en el software de red:

- El software de red instalado en los clientes.
- El software de red instalado en el servidor.

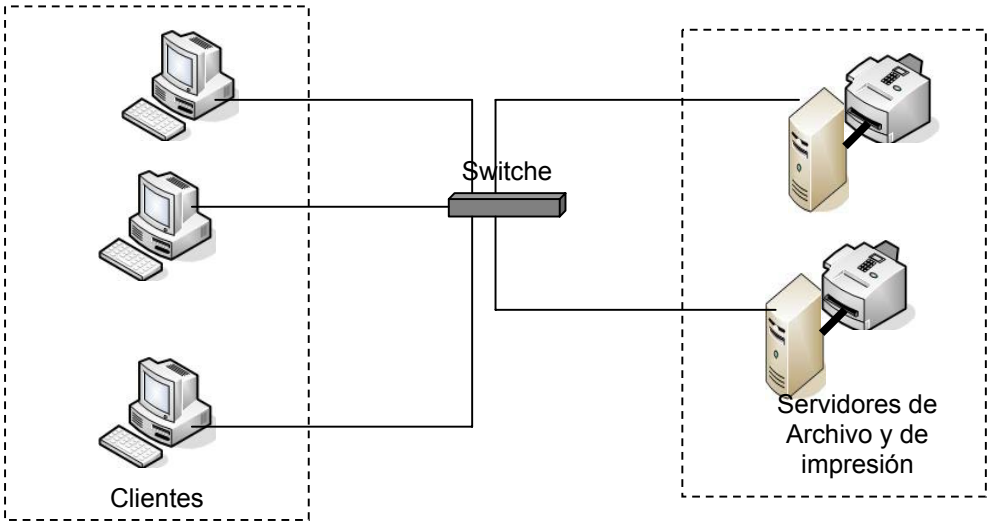


Figura 1.2. Solicitud de clientes a servidores

Por ejemplo, en la figura 1.2 los clientes son los equipos que solicitan el servicio de impresión en los dos servidores, los últimos tienen instalado un sistema operativo de red

Software cliente

Es un sistema autónomo, cuando el usuario escribe un comando que emite una petición para que el equipo realice alguna tarea, la petición ya por el bus local del equipo hasta su CPU. Por ejemplo, si quiere ver un listado del directorio de uno de los discos duros locales, el CPU interpreta la petición y después presenta un listado del directorio en la ventana.

Sin embargo, en un entorno de red, cuando un usuario inicia una petición para usar un recurso que se encuentra en un servidor en otra parte de la red, la petición tiene que reenviares o redirigirse fuera del bus local, hacia la red, hasta el servidor donde se encuentra el recurso solicitado.

El Redirector

El Redirector lleva a cabo el proceso de reenviar las peticiones. Dependiendo del software de red, a este Redirector también se le conoce como intérprete de comandos. El Redirector es una pequeña sección de código del sistema operativo de red que:

- Intercepta las peticiones en el equipo.
- Determina si se debe dejar que sigan su curso en el bus del equipo local o si se tienen que redirigir hacia la red hasta otro servidor.

La actividad del Redirector se origina en un equipo cliente cuando el usuario emite una petición sobre un recurso o servicio de red. Al equipo del usuario se le llama cliente porque hace peticiones a un servidor. El Redirector intercepta la petición y la reenvía hacia la red.

Unidades a recursos

El Redirector necesita hacer un seguimiento de las diferentes unidades asociadas con los recursos de red.

Si necesita tener a un directorio compartido y tiene los permisos necesarios para ello, tiene varias opciones dependiendo de su sistema operativo. Lo más comun son las unidades de red muy utilizadas en los sistemas operativos de Microsoft.

Periféricos

Los Redirectores pueden enviar peticiones a la PC o periféricos. Con el Redirector, LPT1 o COM1 pueden hacer referencia a impresoras de red en lugar de a impresoras locales. El redirector interceptará cualquier trabajo de impresión que vaya a LPT1 y lo reenviará desde la máquina local hasta la impresora de red específica.

El Redirector hace innecesario que los usuarios se preocupen de la ubicación real de la información o de los periféricos , o de lo complejo que puede ser establecer una conexión. Por ejemplo, para tener acceso a los datos de un equipo de la red, un usuario sólo necesita escribir la unidad asignada a la ubicación del recurso y el redirector se encarga de todo lo demás.

En la figura 1.3, la petición original se redirige desde el equipo que loa origina y se envía por la red hasta el equipo destino. En este caso, el destino es el servidor de archivos y de impresión en el que se encuentra la impresora solicitada, en la cual se imprime el archivo.

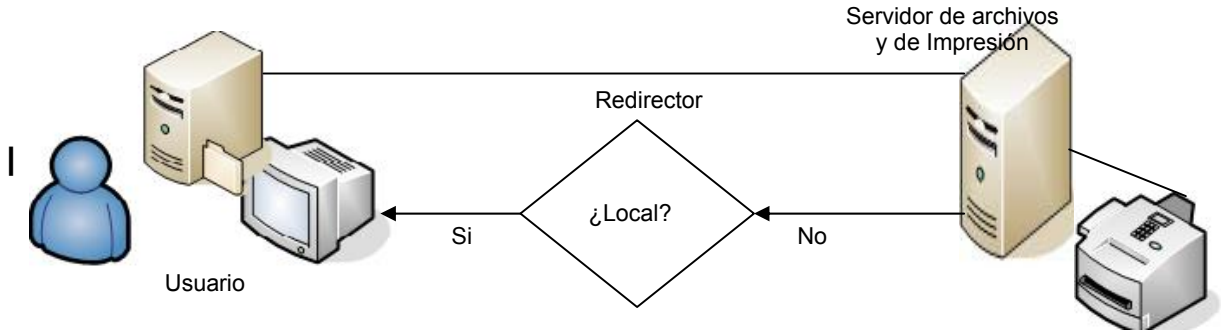


Figura 1.3. Petición del Redirector Hasta la impresora de red

Software Servidor

El software servidor hace posible que los usuarios de otras máquinas compartan los datos y periféricos del servidor, incluyendo impresoras, faxes, discos.

Normalmente, todos los equipos de un dominio o un grupo de trabajo contienen software cliente servidor. Si las estaciones de trabajo están actuando como clientes, tiene incluido el software para actuar como cliente y como servidores.

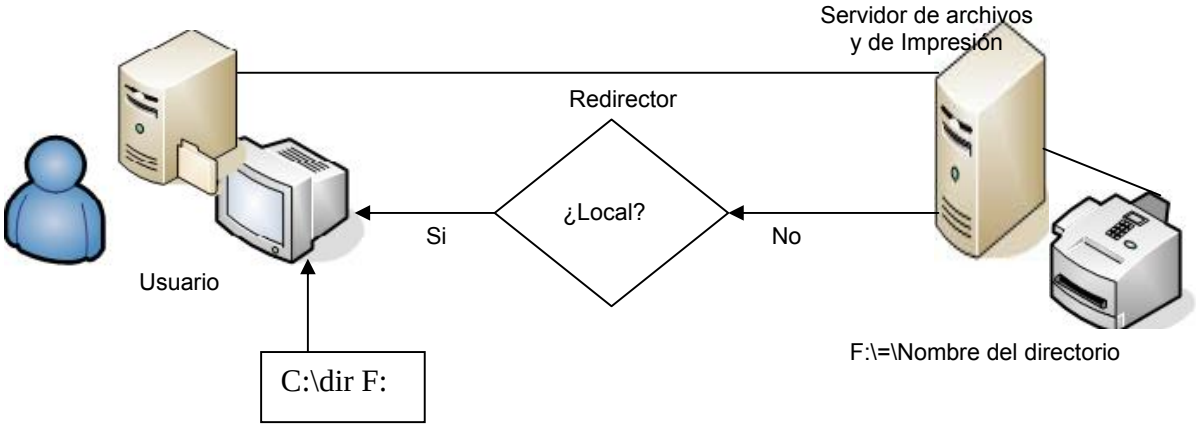


Figura 1.4. Petición de un listado del directorio de una unidad de red.

En la figura 1.4 un usuario está solicitado un listado del directorio de un disco duro compartido remoto. El director reenvía la petición hacia la red y la pasa al servidor de archivos y de impresión que contiene el directorio compartido. Se concede la petición y se suministra el listado del directorio.

Uso compartido de recursos

La mayoría de los sistemas operativos de red no sólo permite compartir, sino también determinar el grado de uso compartido. Este grado incluye:

- Permitir a diferentes usuarios distintos niveles de acceso a los recursos
- Coordinar el acceso a los recursos para asegurarse de que dos usuarios no utilizan el mismo recurso a la vez.

Por ejemplo, una gerente de una oficina quiere que todos los usuarios de la red conozcan cierto documento (archivo), así que comparte el documento. Sin embargo, ella controla el acceso al documento compartiéndolo de manera que:

- Algunos usuarios solo pueden leerlo.
- Otros usuarios pueden leerlo y modificarlo.

Administración de usuarios

Los sistemas operativos de red también permiten que los administradores de la red determinen que personas pueden hacer uso de la red. Los administradores usan el sistema operativo de red.

- Crear privilegios de usuario de los que el sistema operativo de red hace un seguimiento, el cual indica quien tiene acceso a la red
- Otorgar o quitar privilegios de los usuarios en la red
- Quitar usuarios de la lista de usuarios que mantiene el sistema operativo en red.

Administración de la red

Algunos sistemas operativos de red avanzados contienen herramientas de administración para ayudar a los administradores a hacer un seguimiento el comportamiento de la red.

Si en la red surge un problema las herramientas de administración pueden detectar los síntomas de los problemas y presentarlos en gráficos u otros formatos. Esto permite que el administrador de la red tome acciones correctivas antes de que el problema detenga el funcionamiento de la red.

1.4 Herramientas administrativas

Administrar una red incluye tareas posteriores a la instalación y diarias, necesarias para el correcto funcionamiento de la red. Estas tareas las realiza el apoyándose en una serie de aplicativos que se incorporan en los sistemas operativos de red. A continuación se detallan las herramientas administrativas más utilizadas en los sistemas operativos de red:

Asistentes de administración: Tiene como propósito servir de guía a través de las tareas administrativas, creación de Cuentas de usuario, la creación y modificación de cuentas de grupo, el establecimiento de permisos de archivos y carpetas, y la configuración de impresoras de red.

Administración de impresora: Configura las impresoras locales y de red y ayuda a solucionar los problemas más comunes. Esto asegura que los usuarios puedan conectarse y utilizar los recursos de impresora fácilmente.

Administrador de servidores: Muestra y administrar dominios y equipos.

Administrador de usuarios: Administra la seguridad para dominios, servidores miembros de un dominio y estaciones de trabajo.

Herramienta de Copia de seguridad: Hace copia de seguridad de los datos para proteger los de una pérdida accidental o del hardware o el medio magnético dañado.

Visor de sucesos: monitoriza los sucesos de un equipo. El visor de sucesos proporciona información acerca de errores, advertencias y la correcta o incorrecta ejecución tareas. Como el intento de inicio de sesión de los usuarios.

Diagnostico del sistema: muestra e imprime información sobre la configuración de sistemas, como la información acerca de la memoria, unidades de disco y servidores.

Ayuda: presenta información del sistema operativo y debe aclarar cualquier inquietud al usuario con respecto al uso del sistema operativo de red. La ayuda debe ser interactiva.

1.5 Dominios y Grupos de trabajo

Dominios

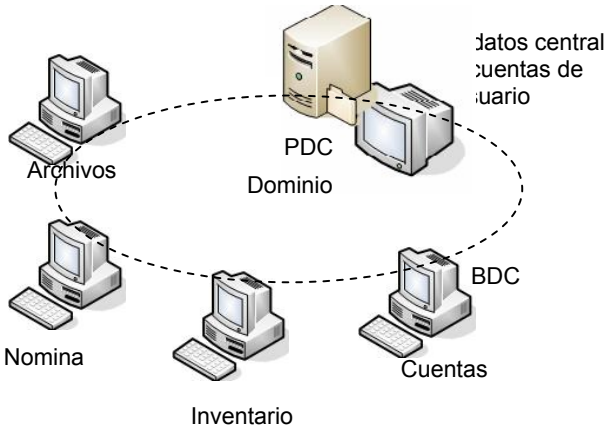


Figura 1.5. Modelo de Dominio

Un dominio es una agrupación lógica de equipos y usuarios. En un dominio, todos los equipos tienen acceso a una base de datos central de directorio que almacena la información de seguridad y de las cuentas de usuario del dominio. La base de datos del directorio es administrada por uno o varios controladores de dominio.

Como miembro de un dominio, un equipo puede compartir recursos, pero el dominio proporciona una solución centralizada a la administración y mantenimiento de las cuentas.

Equipos en un dominio

En un dominio, los equipos pueden operar como controladores de dominio o como servidores miembro. Cada dominio mantiene su propia base de datos de directorio. Un administrador necesita crear una cuenta de usuario sólo una vez en la base de datos de directorio del controlador principal del dominio (PDC, Primary Domain Controller). Cuando los usuarios inician una sesión en un dominio, un controlador del dominio valida el inicio de sesión. El controlador de dominio comprueba el nombre de usuario, la contraseña y las restricciones de inicio de sesión en la base de datos de directorio.

Todas las modificaciones de los datos de las cuentas tienen lugar en el PDC. El PDC copia su base de datos de directorio en otros equipos del dominio que estén configurando como controladores de reserva del dominio (BDC, Backup Domain Controller). Un BDC puede autenticar los inicios de sesión de los usuarios del dominio. Si falla el PDC, uno de los BDC del dominio pueden promoverse a PDC.

Cuando se comparte un recurso en un equipo de un dominio, se puede asignar permisos a las cuentas de usuarios que existan en la base de datos de directorio del dominio.

Servicios de directorio

Un dominio es la unidad administrativa de los servicios de directorio, en los que la administración y la seguridad están centralizadas. Hay una base de datos de directorio común para los datos de las cuentas y la información de seguridad. En un dominio, los equipos ejecutan las siguientes tareas:

- Obtener la validación de las cuentas de usuario desde la base de datos de directorio.
- Permitir el acceso a los recursos a los usuarios definidos en la base de datos de directorio.
- Funcionan como parte de un grupo administrado centralmente.

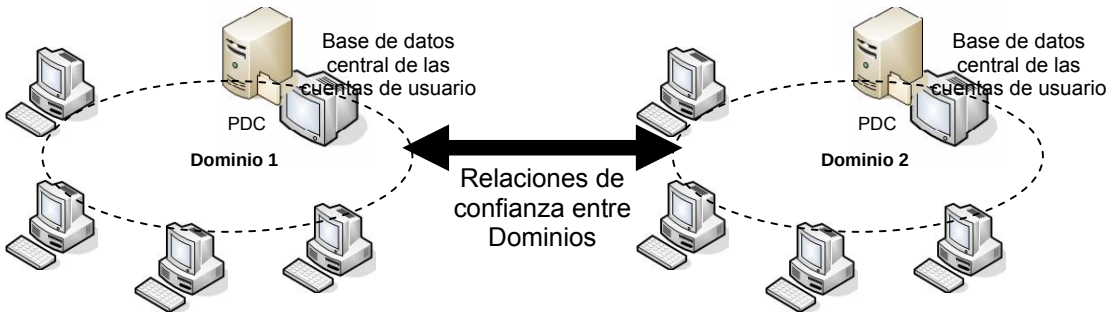


Figura 1.6. Seguridad entre Dominios

Los servicios de directorio de un sistema operativo de red administran una base de datos de directorio segura y distribuida, y proporcionan servicios a los usuarios finales y a los administradores de la red. Para los usuarios, el servicio de directorio proporciona servicios de autenticación que permiten que cada usuario tenga un identificador y una contraseña que puedan ser introducidos desde cualquier directorio de la red para tener acceso a servicios, aplicaciones y recursos ubicados en cualquier otra parte de la red. Para los administradores, el servicio de directorio proporciona una administración gráfica y servicios de seguridad que simplifican la creación y el mantenimiento de la identidades y los derechos para conjuntos de usuarios que van desde los grupos de trabajo hasta las grandes redes de varios dominios.

El Servicio de Directorio emplea una arquitectura flexible que integra en las organizaciones en las que cada usuario forma parte de varios grupos que indican una ubicación, un administrador, unas asignaciones de tareas u otras funciones necesarias.

Grupo de Trabajo

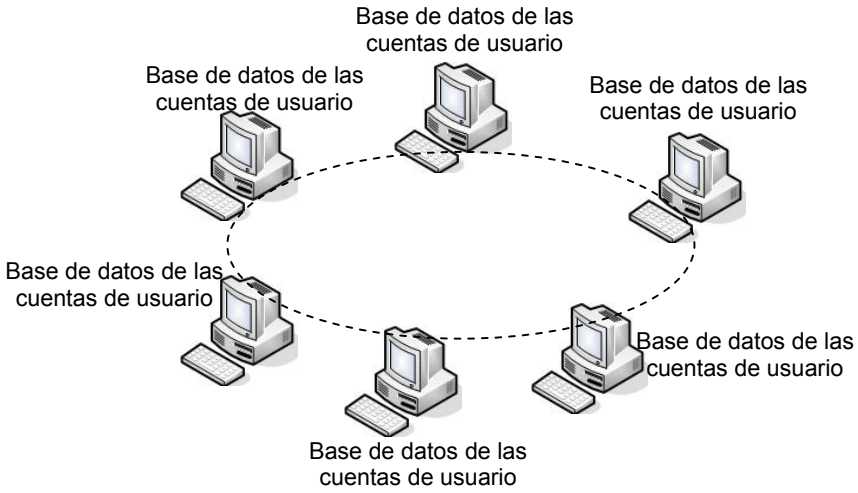


Figura 1.7. Modelo de grupo de trabajo

Un grupo de trabajo es una agrupación lógica de equipos y usuarios. Como parte de un grupo de trabajo, un equipo tiene su propia base de datos de directorio. Los recursos y las cuentas de usuario se administran individualmente en cada equipo. Los grupos de trabajo son adecuados para pequeños números de equipos que se utilicen para compartir recursos con los usuarios de otros equipos, en donde no sea necesaria una seguridad centralizada. El modelo de grupo de trabajo es una organización de red mediante la cual los recursos, la administración y la seguridad están distribuidos por toda la red. Cada equipo del grupo de trabajo tiene sus propias cuentas, su propia administración y sus propias directivas de seguridad.

1.6 Administración de cuentas de usuarios

Una cuenta de usuario constituye las credenciales únicas de un usuario y ofrece al usuario la posibilidad de iniciar la sesión en el dominio para tener acceso a los recursos de la red o de iniciar sesión en un equipo local para tener acceso a los recursos locales. Cada persona que utilice la red regularmente debe tener una cuenta. La cuenta de usuario se utiliza para controlar cómo un usuario tiene acceso al dominio o a un equipo. Por ejemplo, puede limitar el número de horas en las que un usuario puede iniciar una sesión en el dominio.

Todo aquel que trabaje en la red necesita una de usuario. Una cuenta está compuesta por el nombre de usuario y los parámetros de inicio de sesión establecidos para dicho usuario. El administrador introduce esta información y el sistema operativo la almacena en la red. La red utiliza ese nombre para comprobar la cuenta cuando el usuario intenta iniciar una sesión.

Todas las redes tienen una utilería que puede utilizar el administrador para introducir un nuevo nombre de cuenta en base de datos de seguridad de la red. Algunas veces, a este proceso se le conoce como creación de un usuario.

Cuando se crea una nueva cuenta esta contiene información que define a un usuario en el sistema de seguridad de la red. Esto incluye:

- Nombre y contraseña del usuario
- Derechos otorgados al usuario para acceder al sistema y utilizar sus recursos.
- Grupos administrativos a los que pertenece la cuenta y otros grupos a los que ha asignado.

Esta información es esencial para que el administrador cree la cuenta.

A continuación se explica algunos de los campos que normalmente se utilizan para crear un nuevo usuario.

Nombre de usuario: Identifica la cuenta del usuario. Un nombre de usuario no puede ser idéntico a otro nombre de usuario o de grupo dentro del dominio o del equipo administrado. Puede contener caracteres alfanuméricos y cualquier carácter en mayúsculas o minúsculas, excepto los signos " / \ : ; | = + * ¿ <>

Nombre completo: Nombre completo del usuario

Descripción: Texto que describe la cuenta de usuario.

Contraseña y confirmación de la contraseña: La contraseña puede tener hasta 14 caracteres de longitud. Distingue entre mayúsculas y minúsculas. Es necesario teclear la misma contraseña en ambos campos.

Configuración de los parámetros de usuario

La mayoría de las redes permitirán que los administradores de la red pueden establecer una serie de parámetros de usuario, incluyendo:

Horas de sesión: Destinadas a restringir los horarios en que los usuarios puedan tener una sesión dentro de la red.

Directorio particular: Proporcionan a los usuarios un área de almacenamiento para sus archivos privados.

Fecha de caducidad: Limita la vida de un usuario temporal en la red.

Creación de un plan de cuentas

El plan de cuentas determina cómo deben utilizar las contraseñas todas las cuentas de usuario. Este plan establece requisitos para lo siguiente:

- Duración máxima y mínima de contraseñas
- Longitud mínima de contraseñas
- Historial de contraseñas
- Opción de bloqueo de cuentas

De modo predeterminado, el único requisito de las contraseñas para las cuentas de usuario es que los usuarios cambien sus contraseñas la primera vez que inicien una sesión. Para utilizar un plan de cuentas y proporcionar así mayor seguridad para las cuentas de usuario, tenga en cuenta lo siguiente:

- No permita nunca contraseñas en blanco. Este tipo de contraseñas no proporciona ninguna seguridad. Nunca se deben utilizar en sistemas conectados a Internet o con capacidad de marcado.

- Exija una longitud mínima para todas las contraseñas. Cuanto más largas sea la contraseña, más difícil será adivinarla.

    - En redes de seguridad media, exija 6 a 8 caracteres.
    - En redes de alta seguridad, exija de 8 a 14 caracteres.

- Exija a los usuarios que cambien a menudo sus contraseñas. Esto permitirá evitar que los usuarios sin autorización puedan adivinarla.

    - En redes de seguridad media, cambie las contraseñas cada 45-90 días.
    - En redes de alta seguridad, cambie la contraseña cada14-45 días.

- Exija a los usuarios que utilicen una contraseña distinta cada vez que la cambien. Asegúrese de que una vez cambiada, no se puede volver a cambiar a la contraseña anterior.

    - En redes de seguridad media, exija 6 a 12 contraseñas distintas.
    - En redes de alta seguridad, exija de 12 a 24 contraseñas distintas.

1.7 Perfiles de Usuario

Es conveniente que el administrador sea capaz de estructurar un entorno de red para determinar usuarios. Esto puede ser necesario, por ejemplo, para mantener un determinado nivel de seguridad o si los usuarios no están lo suficientemente familiarizados con los equipos y los equipos y las redes como para ser capaces de utilizar por sí mismo la tecnología. El administrador puede utilizar perfiles para controlar el entorno de inicio de sesión del usuario.

Los perfiles se utilizan para configurar y mantener el entorno de inicio de sesión de un usuario, incluyendo las conexiones de la red y la apariencia del escritorio cuando el usuario inicia una sesión. Esto puede incluir:

- Conexiones a impresoras
- Configuración regional
- Configuración del sonido
- Configuración del Mouse
- Configuración de video
- Cualquier otra configuración definible por el usuario

Los parámetros del perfil también pueden incluir condiciones especiales de inicio de sesión e información acerca del lugar en el que el usuario puede almacenar sus archivos personales.

Cuentas de usuarios principales

Los sistemas operativos de red se suministran con determinados tipos de cuentas de usuario ya creadas, las cuales se activan automáticamente durante la instalación.

El administrador: la cuenta inicial

Cuando se instala un sistema operativo de red, el programa de instalación crea en forma automático una cuenta con toda la autoridad sobre la red; alguien debe poder:

- Iniciar la red
- Establecer los parámetros iniciales de seguridad.
- Crear cuentas de usuario.

En el entorno de red, la persona con cuenta de administrador, tiene el control total sobre todas las funciones de la red.

La cuenta invitado

Otra cuenta predeterminada que crea el programa de instalación de denomina Invitado o Guest. Se trata de una cuenta para adquirir personas que no tienen una cuenta de usuario válida, pero que necesitan tener acceso temporal a la red.

Contraseñas

Las contraseñas ayudan a garantizar la seguridad de un entorno de red. Lo primero que el administrador debe hacer cuando establece la cuenta inicial es introducir una contraseña. Ésta impide que usuarios no autorizados inicien una sesión como administrador y que puedan crear cuentas.

Los usuarios deben tener contraseñas únicas y almacenarlas en un lugar seguro. En situaciones particularmente delicadas, es conveniente hacer que los usuarios cambien sus contraseñas en forma periódica. Muchas redes proporcionan características de contraseña que requieren que el usuario haga esto en forma automática, en un intervalo establecido por el administrador.

En situaciones en las que la seguridad no es problema o cuando se necesita limitar el acceso (como en la cuenta Invitado) es posible modificar una cuenta para que no necesite contraseña.

El administrador debe estar atento ante situaciones como cuando un empleado ya no ésta contratado en la empresa. En este caso, el administrador debe desactivar la cuenta lo antes posible.

Existen ciertas sugerencias tradicionales que rigen el uso de las contraseñas, entre las que se incluyen:

- No se deben utilizar contraseñas obvias como la fecha de nacimiento, el número del seguro social, el nombre del conyugue, del hijo, de la mascota, etc.

- Memorizar la contraseña en lugar de escribirla y dejarla pegada en el monitor.

- Ser consciente de la fecha de caducidad de la contraseña (si es que existe) para poder cambiar antes de que caduque e impida el acceso al sistema.

Tras unas cuantas experiencias con usuarios que necesiten ayudar con sus contraseñas, el administrador puede determinar las normas sobre la misma.

1.8 Administración de discos

Para que sea posible dar formato a un disco con un sistema de archivo, primero es necesario crear particiones en él. Las particiones son divisiones lógicas de un disco duro en unidades más pequeñas a las que se pueden dar formato y usar de forma independiente. Las particiones se crean en el espacio libre del disco duro, que es la parte del mismo que no utiliza y que no está incluida en ninguna partición. El espacio libre puede dividirse en particiones primarias y extendidas.

Volúmenes

Un volumen es cualquier área de espacio en disco al que puede tener acceso el sistema de archivos como una entidad única y que tiene una única letra de unidad asignada al mismo. Un volumen puede ser una partición única o una colección de áreas no contiguas en discos distintos a los que se da formato para usarlos como un conjunto de volúmenes.

Es posible crear conjunto de volúmenes para optimizar el uso del espacio de disco. Un conjunto de volúmenes es un conjunto de áreas de espacio libre combinadas en una única unidad lógica. De este modo se aumenta el espacio de disco disponible en una misma unidad lógica, pero no se mejora el rendimiento.

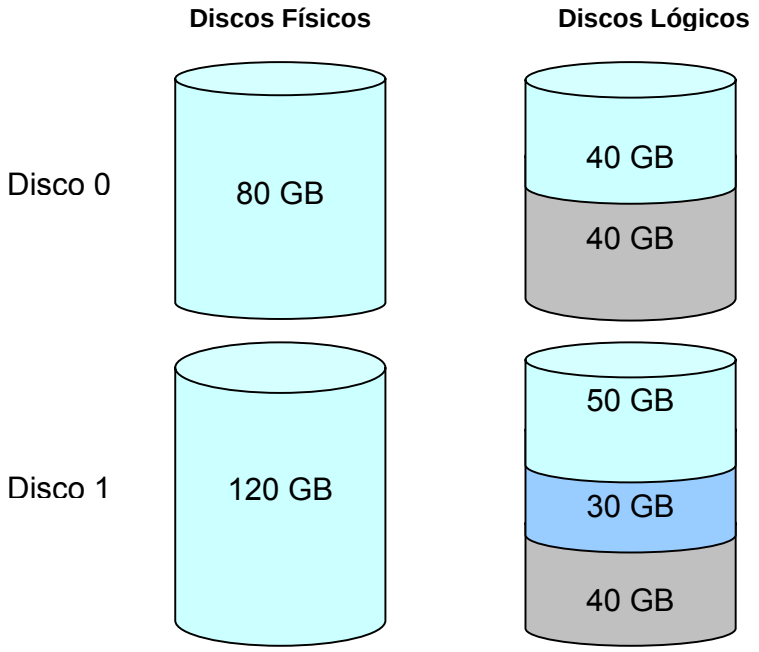


Figura 1.8 Conjunto de Volúmenes

Sistemas tolerantes a fallos

Los sistemas tolerantes a fallos protegen los discos duplicándolos o colocándolos en distintos lugares físicos, como en particiones o discos diferentes. La redundancia de los datos permite tener acceso a ellos aunque parte del sistema de datos falle. La redundancia es una característica importante común en la mayoría de los sistemas tolerantes a fallos.

Nunca debe utilizarse sistemas tolerantes a fallos como sustito de la copia de seguridad periódica de los servidores y de los discos duros locales. Una estrategia de copia de seguridad cuidadosa es el mejor seguro para recuperar los datos perdidos o dañados.

Los sistemas tolerantes a fallos ofrecen las siguientes alternativas frente a la redundancia de datos:

- Creación de conjuntos de bandas de disco o stripping
- Creación de conjunto de espejo
- Reserva de sectores
- Arreglos de unidades en espejo
- Agrupamiento

A continuación se analizan los dos sistemas de tolerancia a fallos mas utilizados:

- **Creación de conjunto de espejo**

La creación de espejo de disco duplica realmente una partición y mueve la duplicación hacia otro disco físico. Siempre hay dos copias de los datos, cada una en un disco distinto. Se pueden crear imágenes espejo de cualquier partición. Esta estrategia es la forma más sencilla de proteger un disco contra fallas. Se puede considerar la creación de conjuntos de espejo como una especie de copia de seguridad continua, ya que mantiene una copia totalmente redundante de una partición en otro disco.

Duplicación

La duplicación de disco es una pareja de discos en espejo con un controlador de disco adicional en la segunda unidad. Reduce el tráfico y puede mejorar el rendimiento. Se recomienda la duplicación para protegerse contra fallas de los controladores y de los medios.

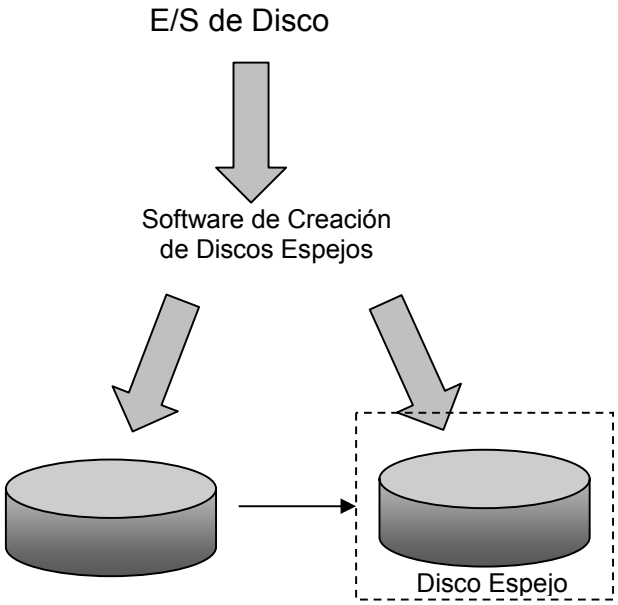


Figura 1.9 Creación de un conjunto de Espejos

Creación de conjuntos de bandas con paridad

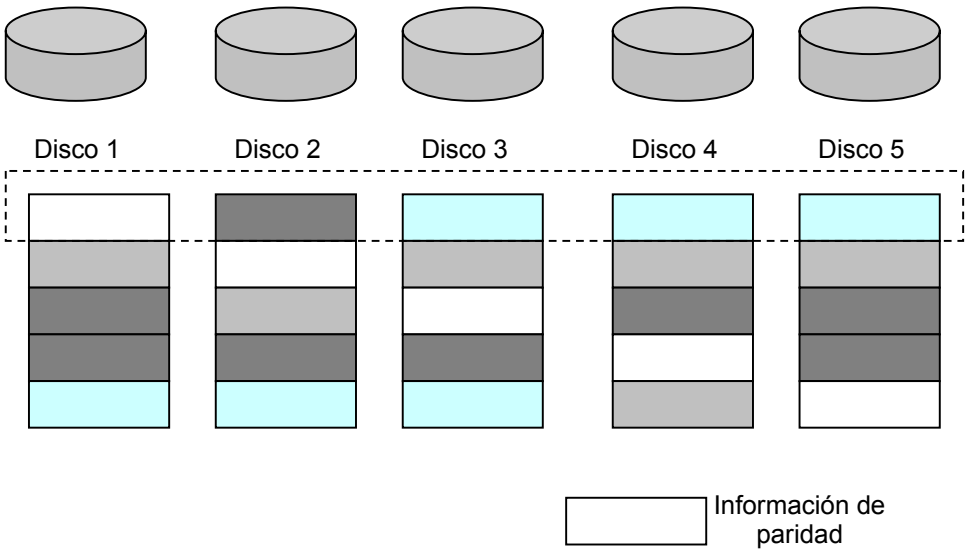


Figura 1.10 Creación de un conjunto de Bandas con paridad

Actualmente, la creación del Stripping con paridad es la solución más popular para el diseño de tolerancia a fallos. Acepta un mínimo de tres unidades y un máximo de 32, y escribe la información de paridad en todos los discos del arreglo (todo el conjunto de bandas). Los datos y la información de paridad se organizan de tal forma que siempre se ubican en discos distintos.

Existe un bloque de bandas con paridad con cada banda (fila) del disco. El bloque del stripping con paridad se utiliza para reconstruir los datos si se produce una falla física en el disco. Si falla una sola unidad, hay suficiente información diseminada en los discos restantes como para permitir la reconstrucción total de los datos.

El bloque de banda con paridad se utiliza para reconstruir los datos de un disco que ha tenido una falla física. Existe un bloque de bandas con paridad por cada banda (fila) del disco.

1.9 Administración de impresoras

Puede administrar las impresoras de red de forma local o remota a través de la red. Las tareas de administración incluyen:

- Administrar documentos, que conllevan las siguientes tareas:
  - Cambiar la prioridad de los documentos
  - Eliminar un documento
  - Establecer la hora de impresión de un documento
  - Establecer una notificación
- Administrar impresoras, que contengan las siguientes tareas:
  - Hacer una pausa y reanudar una impresora
  - Purgar una impresora
  - Redirigir documentos a otras impresoras
  - Tomar posición de una impresora
- Solucionar problemas de impresión.
- Para administrar las impresoras, es necesario tener el permiso de control total. Los que disfrutan de este permiso son los que poseen cuentas de administrador.

1.10 Protección de recursos de red

En la lista siguiente se enumeran los procedimientos recomendados para compartir carpetas:

- Organizar los recursos de los discos de modo que las carpetas con los mismos requisitos de seguridad se ubiquen dentro de una jerarquía de carpetas. Esto facilita las labores administrativas al simplificar la manera en que se asignan permisos.

- Almacenar datos y carpetas particulares en volúmenes diferentes del sistema operativo y de las aplicaciones. Esto separa los archivos de datos de los archivos del sistema y de aplicaciones y, por tanto, simplifica los procedimientos de copia de seguridad y restauración. Si el sistema operativo requiere una nueva instalación, el volumen que contiene los datos permanecerá intacto.

- Solo asignar permisos de acceso a los recursos, a usuarios autorizados para optimizar los recursos de impresión como tintas, papelería, etc.

- Asignar permisos a grupos en lugar de a usuarios particulares: esto simplifica las labores administrativas al permitir una rápida asignación de recursos a varios usuarios a la vez.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 1

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 1 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue las características de los principales sistemas operativos de red y las diferentes herramientas administrativas que ellos utilizan para que el administrador de red pueda realizar sus funciones.

4. Realice un laboratorio en grupo de curso implementando políticas de cuentas en sistemas operativos de red. Use de herramientas administrativas y protección de recursos de red mediante configuración de permisos.

5. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

CAPITULO 2: AUDITORIA DE RECURSOS Y SUCESOS

2.1 Introducción a la auditoria

La auditoria se utiliza para hacer un seguimiento de las actividades de los usuarios y los sucesos globales del sistema en una red. Mediante la auditoria puede especificar que una acción o suceso se escriba en un registro de seguridad. En la auditoria se registra lo siguiente:

- La acción realizada
- El usuario que realizó la acción
- La fecha y hora de la acción

2.2 Diseño de un plan de auditoria

El plan de auditoria se utiliza para seleccionar los tipos de sucesos de seguridad que se van a registrar en una red. Los sucesos aparecerán en le registro de seguridad de los servidores con la herramienta administrativa que audite los sucesos. El registro de seguridad se convierte en la herramienta para hacer un seguimiento de los sucesos especificados.

El plan de auditoria solo afecta al registro de seguridad de dicho equipo.

Puede establecerse un plan de auditoria en una red:

- Hacer un seguimiento del éxito o el fracaso de los sucesos, como cuando los usuarios inician sesiones, el intento de un usuario concreto de leer un archivo especifico, las modificaciones en los usuarios y los grupos, y las modificaciones del plan de seguridad.

- Eliminar o minimizar el riesgo del uso no autorizado de los recursos.

El visor de sucesos permite ver los sucesos auditados que se han registrado en el registro de seguridad.

- Puede archivar los archivos de registro para determinar tendencias a lo largo del tiempo. Esto es útil para determinar el uso de impresoras o archivos y para comprobar los intentos de uso no autorizado de los recursos.

Al diseñar un plan de auditoria, tenga en cuenta lo siguiente:

- Determine los sucesos que se va auditar, como:

    - El uso de recursos de archivos y directorios.

- Los inicios y finales de sesión de usuarios.

- Cuando se cierra y se vuelve a iniciar el sistema operativo.

- Las modificaciones en los usuarios y en los grupos.

- Las modificaciones de las directivas de seguridad tales como la asignación de privilegios o la capacidad de iniciar sesiones.

• Determine si auditará el resultado, correcto o incorrecto, de los sucesos.

- El seguimiento del resultado correcto de los sucesos puede indicar la frecuencia de uso de archivos o impresoras específicos. Pueden utilizar esta información a la hora de programar recursos.

- El seguimiento de resultado incorrecto de los sucesos le alertará de posibles defectos de seguridad.

• En redes de seguridad media y alta, debe hacer el seguimiento de lo siguiente:

- El resultado de los inicios de sesión de los usuarios

- El uso de los recursos.

• Determine si necesita hacer un seguimiento de las tendencias. En tal caso debe diseñar el archivo de los registros de sucesos.

2.3 Implementación de un plan de auditoria

Los planes de auditoria se establecen equipo por equipo. Por ejemplo, para auditar sucesos que ocurren en un servidor, como inicios de sesión de los usuarios y cambios realizados a las cuentas de usuario, deben establecer plan de auditoria en ese servidor. Para auditar sucesos de cualquier otro equipo de la red, como el acceder a un archivo de un equipo cualquiera, debe establecer un plan de auditoria en ese equipo.

Los sucesos se graban en el registro de seguridad del equipo local, pero puede verlos desde cualquier equipo todos aquellos usuarios que tengan privilegios administrativos en el equipo donde se produjeron los sucesos.

Requisitos para la auditoria

Los requisitos para configurar y administrar la auditoria son los siguiente:

- Sólo los administradores pueden configurar la auditoria en archivos, directorios e impresoras de controladores de dominio.
- Para configurar la auditoria en un equipo que no sea un controlador de dominio, debe ser miembro del grupo Administradores de dicho equipo.
- De forma predeterminada, el derecho de usuario Administrar los registros de auditoria y seguridad sólo está asignado al grupo Administradores.
- Los miembros tanto del grupo Administradores como el grupo Operadores del servidor pueden ver y archivar los registros de seguridad, así como realizar otras tareas administrativas una vez establecida la auditoria .
- Sólo puede auditar archivos y directorios de volúmenes NTFS.

Proceso de auditoria

La configuración de la auditoria es un proceso que consta de dos partes.

- Activar la auditoria en el dominio y seleccionar los sucesos que se van a auditar.
- Especificar los sucesos que se van a auditar para archivos, directorios e impresoras.

2.4 Visores de sucesos

El visor de sucesos es una herramienta que proporciona información acerca de errores, advertencias y el resultado correcto o incorrecto de una tarea. Esta información se almacena en tres tipos de registros:

- **Sistema**: contiene errores, advertencias o información generada por el sistema operativo. La selección de sucesos debe estar preconfigurada en el sistema operativo de red.

- **Seguridad:** contiene información acerca del éxito o el fracaso de los sucesos auditados. Estos sucesos son el resultado del plan de auditoria.

- **Aplicaciones:** contiene errores, advertencias o información generada por los programas de sucesos está preconfigurada por el programador del programa.

2.5 Registro de seguridad

Consiste en una base de datos donde se guardan todos los sucesos que se están auditando en el equipo local, pero puede verlos desde cualquier equipo todos aquellos usuarios que tengan privilegios administrativos.

En el registro de seguridad se almacenan tres tipos de información proveniente de los registros de:

- Sistema
- Seguridad
- Aplicaciones

2.6 Monitorización de recursos de red

Los recursos de la red se autorizan para evaluar y después administrar el uso de los recursos en servidores de red. Por ejemplo, puede ver si un usuario está conectado a un archivo al que otro usuario está intentando tener acceso. Puede enviar un mensaje al usuario que está conectado al archivo y hacerle saber que alguien más necesita acceso al archivo.

Durante la administración de servidores se pueden realizar las siguientes tareas:

- Ver lista de usuarios conectados
- Ver y administrar recursos compartidos
- Ver los recursos abiertos
- Enviar mensajes a los usuarios conectados
- Crear lista de usuarios que recibirán alertas.

2.7 Procedimientos recomendados

La siguiente lista proporcionan los mejores métodos para auditar recursos y sucesos:

- Definir un plan de auditoria útil pero manejable. Audite únicamente aquellos sucesos que proporcionen información útil acerca del entorno de red. Esto reducirá al mínimo el uso de los recursos del servidor y facilitará la búsqueda de información importante.

- En entornos con seguridad mínima y media, haga un seguimiento de los sucesos correctos si necesita determinar el uso de los recursos. En un entorno de alta seguridad, haga un seguimiento de todos los sucesos correctos.

- En entorno con seguridad mínima y media, haga un seguimiento de los sucesos erróneos para avisarle de posibles fallos en la seguridad. En un entorno de alta seguridad, haga un seguimiento de todos los sucesos erróneos.

- Audite el grupo Todos. Esto asegurará que se audita a cualquiera que pueda conectarse a la red.

- Configure un plan para ver los registros de auditoria. Conveniente en parte rutinaria de sus tareas de administración de la red.

- Archive periódicamente los registros de auditoria para hacer un seguimiento de las tendencias. Esto es útil para determinar el uso de los recursos de cara al diseño.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 2

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 2 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Elabore un ensayo referente a la auditoria de recursos y sucesos y envíelo al correo del Tutor

4. Realice un laboratorio en grupo de curso implementando un plan de auditoria que usted mismo debe diseñar, realice los respectivos seguimientos utilizando la correspondiente herramienta administrativa.

5. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

CAPITULO 3: COPIAS DE SEGURIDAD Y RESTAURACION DE DATOS

3.1 Diseño de una estrategia de Copia de seguridad

Un desastre en la instalación se define como cualquier cosa que provoca la pérdida de datos. Las causas de desastre en la red varían desde la naturaleza humana hasta las causas naturales, incluyendo:

- Incendios provocados
- Eliminación y corrupción de datos
- Robo o vandalismo
- Fuego
- Fallas en la fuente de alimentación y variación de voltaje.
- Fallas en los componentes
- Desastres naturales, tales como rayos, inundaciones, tornados y terremotos

En que se produzca un desastre en la instalación, el tiempo que se emplea en recuperar los datos de la copia de seguridad (si es que se tiene una)puede traducirse en una importante perdida de productividad. Sin copias de seguridad las consecuencias son más severas y probablemente dan como resultado graves pérdidas económicas. Algunas formas de prevenir la pérdida de datos son con:

- Copias de seguridad en cintas
- Fuente de alimentación ininterrumpida (UPS)
- Tolerancia a fallos

Se puede utilizar cualquiera de estos sistemas, o todos ellos, dependiendo de lo valioso que sean los datos de la organización y del presupuesto disponible.

Copias De Seguridad

Quizá la forma más sencilla y barata de evitar la desastrosa pérdida de datos sea implementar un plan de copias de seguridad periódicas almacenadas fuera de la instalación. Se trata de una de las formas más sencillas y económicas de asegurarse de que los datos permanecen seguros y utilizables.

Los ingenieros de redes experimentados saben que un sistema de copias de seguridad es la primera línea de defensa. Una estrategia segura de copias de seguridad minimiza el riesgo de pérdida de datos, ya que mantiene una copia de seguridad actual de forma que se pueda recuperar los archivos si les ocurre algo a los datos originales.

Las copias de seguridad de los datos implican:

- Equipo
- Un plan
- Una persona encargada de seguridad de que se cumpla el plan

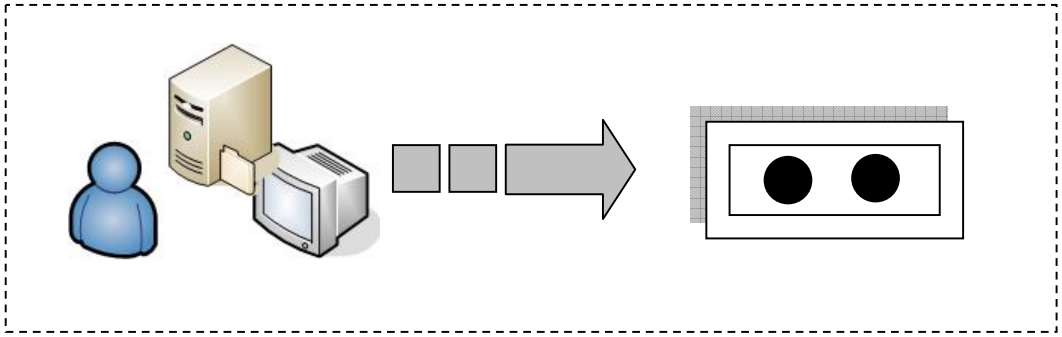


Figura 3.1 Copia de seguridad en medio magnético

El equipo normalmente consistirá en una o más unidades de cinta y cintas u otro sistema de almacenamiento masivo como CDROM o DVD. Todo gasto que se produzca en esta área se considera mínimo comparado con lo que se puede ahorrar.

3.2. Determinación de los archivos y carpetas que se van a copiar

La regla general es: si no puede vivir sin ello, haga una copia de seguridad. Hacer copias de seguridad de discos enteros, de directorios seleccionados o de algunos archivos, dependerá de lo rápido que quiera volver a funcionar tras una pérdida de datos importante. Las copias de seguridad completas facilitarán mucho la restauración de las configuraciones de los discos, pero requieren completas requieren varias cintas si existen grandes cantidades de datos. La copia de seguridad de archivos o de directorios individuales requerirá menos cintas, pero puede obligar al administrador a restaurar en forma manual la configuración de los discos.

La información crítica debería respaldar conforme a un plan diario, semanal o mensual, dependiendo de la importancia de los datos y de su frecuencia de actualización. Es mejor planear las operaciones de copia de seguridad durante los periodos de baja utilización del sistema. Se deberá notificar a los usuarios cuando se vaya a realizar la copia de seguridad para que no utilice los servicios durante la operación.

Puesto que la mayoría de las copias de seguridad se realizan con unidades de Almacenamiento masivo como cintas o CDROM, el primer paso es elegir una unidad donde almacenar los datos. El administrador debe tener en cuenta:

- La cantidad de datos
- La fiabilidad
- La capacidad
- La velocidad
- El costo de la unidad y los medios relacionados
- La compatibilidad del hardware con el sistema operativo

La unidad de almacenamiento ideal debería tener una capacidad más que suficiente para hacer una copia de seguridad del servicio del mayor tamaño en la red. También debería proporcionar un sistema de detección y corrección de errores durante las operaciones de copia de seguridad y de restauración.

3.3 Determinación del Tipo de copias de seguridad

Un plan eficiente para hacer copias de seguridad utilizará una combinación de los métodos que se enumeran:

Copia de seguridad completa: copia y marca los archivos seleccionados, aunque no hayan cambiado desde la última copia de seguridad.

Copia normal: copia los archivos seleccionados sin marcarlos como copiados

Copia de seguridad incremental: copia y marca los archivos seleccionados sólo si ha n cambiado desde la ultima copia de seguridad.

Copia diaria: copia sólo los archivos que han sido modificados ese día, sin marcarlos como copiados.

Copia de seguridad diferencial: copia los archivos seleccionados sólo si han cambiado desde la última vez que se copiaron, sin marcarlos como copiados.

3.4 Rotación de archivos y cintas

Los métodos de copias de seguridad normalmente utilizan unidades de cinta. Los administradores de redes experimentados han encontrado que es mejor utilizar varias cintas en un sistema cíclico para copiar grandes cantidades de datos.

Es posible copiar las cintas basándose en un sistema cíclico de varias semanas, dependiendo del número de cintas disponibles. Esta regla también es valida para los CDRW. No hay una regla rígida en cuanto a la duración del ciclo. El principio

es que en el primer día del ciclo el administrador lleva a cabo una copia de seguridad completa y continúa con copias incrementales los días sucesivos. Cuando termina el ciclo, el proceso comienza de nuevo. Algunos administradores han averiguado, gracias a la experiencia, que lo mejor es hacer varias copias de seguridad incrementales cada día en horarios determinados.

Comprobación y almacenamiento

Los administradores experimentados probarán el sistema de copia de seguridad antes de ponerlo en práctica. Harán una copia, eliminarán la información, restaurarán los datos e intentaran utilizarlos.

El administrador debe probar periódicamente los procedimientos de copia de seguridad para cerciorarse de que se haga una copia de seguridad de lo que realmente se desea. Además, debe probarse el procedimiento de restauración para asegurarse de que se pueden recuperar rápidamente los archivos importantes.

Lo ideal que el administrador haga dos copias. Una se guardará en la instalación y otra se almacenará en un lugar seguro fuera de las instalaciones. Recuerde que las copias de seguridad no arderán si se encuentran en un lugar a prueba de incendios, pero el calor puede estropear los datos que contienen.

3.5 Conjunto de copias, catálogos y registro de copias

Es vital mantener un registro de todas las copias de seguridad para su recuperación posterior. Debe guardarse una copia del registro junto con las cintas de la copia de seguridad dentro y fuera de la instalación. El registro debe contener la siguiente información:

- Fecha de copia de seguridad
- Número del conjunto de cintas
- Tipo de copia realizada
- Equipo del que se ha hecho copia
- Archivos copiados
- Quién realizó la copia
- Ubicación de las cintas

3.6 Programación de copias de seguridad

Es posible conectar las unidades de cinta a un servidor o a un equipo al iniciar las copias desde el equipo al que está conectado la unidad de cinta. Si se ejecutan copias de seguridad desde un servidor, las operaciones de copiado y restauración serán más rápidas ya que los datos no tendrán que viajar por la red.

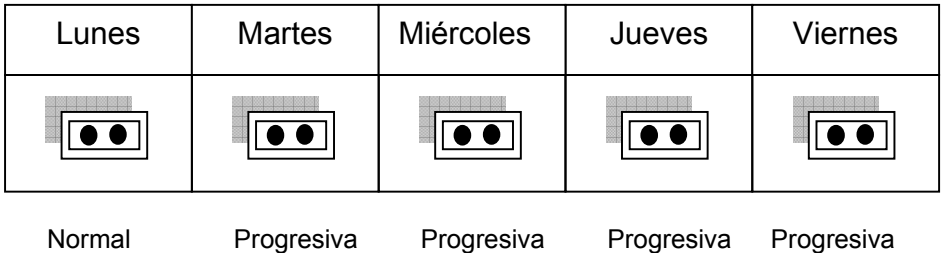


Figura 3.2 Programación de copias de seguridad.

Hacer la copia de seguridad desde la red es más efectivo que hacer copias de los diversos sistemas; sin embargo esto también crea un gran tráfico en la red y disminuye la velocidad de la misma. El tráfico de la red también puede ser la causa de la seguridad durante periodos de baja utilización del servicio.

Si varios servidores residen en un lugar, se puede reducir el tráfico de la copia de seguridad al colocar un equipo de copia de seguridad en un segmento aislado. El equipo de copia se conecta entonces a una tarjeta adaptadora de red distinta en cada servidor.

Si varios servidores residen en un lugar, se puede reducir el tráfico de la copia de seguridad al colocar un equipo de copia de seguridad en un segmento aislado. El equipo de copia se conecta entonces a una tarjeta adaptadora de red distinta en cada servidor.

3.7 Implementación de una estrategia de restauración

Una buena estrategia de restauración depende de lo siguiente:

- Una buena estrategia de copia de seguridad. Por ejemplo, si siempre realiza una copia de seguridad completa de un volumen, en el caso improbable se que se produzca un fallo de disco, podrá resultar el volumen en una única operación. La rotación de las cintas en un periodo de una semana asegura que puede restaurar una versión anterior de un archivo.

- Conserve documentación de cada copia de seguridad. Si crea e imprime un registro de cada copia de seguridad, podría encontrar rápidamente los archivos que hay que restaurar sin necesidad de cargar los catálogos de todos los conjuntos de copias actuales.

Dependiendo del registro que cree, éste puede incluir información acerca del tipo de copia de seguridad, los archivos y carpetas que se han copiado y en qué cinta se encuentran.

- Realice periódicamente una restauración de prueba par asegurarse de que los archivos se copiaron correctamente. Una restauración de prueba puede desvelar problemas del hardware que no aparecen con las comprobaciones por software.

  Restaure la cinta en una unidad distinta de la original y compare los datos restaurados con los datos de la unidad original.

- Mantenga un registro de múltiples copias de seguridad en forma de calendario en el que se muestre los días en que se realizaron las copias de seguridad. para cada copia, anote el tipo de copia y el identificador de cinta (un número, por ejemplo). Si hay algún problema, con un rápido vistazo localizará copias de seguridad de varias semanas y qué cinta se utilizó para cada una de ellas.

3.8 El sistema de alimentación ininterrumpida (UPS)

El UPS es un sistema automático de energía externa que evita que el servidor u otros dispositivos que estén funcionando sufran los efectos de una falla de corriente. UPS se beneficia de los sistemas de alimentación ininterrumpida que se pueden conectar a un sistema operativo de red. El UPS estándar le proporciona a la red dos componentes esenciales:

- Una fuente de alimentación para utilizar el servidor durante un tiempo breve.
- Un servicio seguro de administración para apagar el equipo.

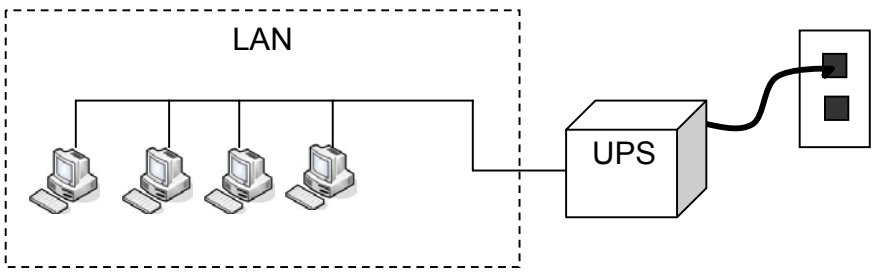


Figura 3.3. Sistema de alimentación Ininterrumpida

El sistema de alimentación generalmente consta de una batería, pero también puede tener un generador de corriente con un volante o un motor de gasolina que haga funcionar un sistema de alimentación de corriente alterna.

Si la corriente falla, el UPS avisa a los usuarios de la falla para que terminen sus tareas. El UPS espera un tiempo predeterminado y lleva a cabo un cierre ordenado del equipo.

Un buen sistema UPS:

- Impide que otros equipos tengan acceso al sistema
- Envía un mensaje de alerta al administrador de la red a través del servidor.

El UPS casi siempre se coloca entre el servidor y la toma de corriente.

Si vuelve la corriente mientras el UPS está activo, éste avisará a los usuarios que la corriente ha regresado.

Tipos de sistemas UPS

Los mejores sistemas UPS funcionan en línea. Cuando falla la corriente normal, las baterías de UPS automáticamente se ponen en marcha. El proceso es invisible para los usuarios.

También existen sistemas UPS independientes que se inician cuando falla la corriente. Son menos caros que los sistemas en línea, pero no son tan confiables.

Implementación de un UPS

Las siguientes preguntas ayudarán a que el administrador de la red determine cómo implementar un sistema UPS.

- ¿El UPS será capaz de resolver las necesidades básicas de energía de la red? ¿Cuántos componentes acepta?

- ¿El UPS se comunica con el servidor para avisarle que ha ocurrido un fallo de energía y el servidor esta funcionando con baterías?

- ¿El UPS cuenta con una característica de protección contra variaciones de voltaje?

- ¿Cuál es el tiempo de vida de la batería del UPS ?¿Cuánto tiempo puede estar inactiva antes de empezar a degradarse?

- ¿El UPS avisará al administrador y a los usuarios que está funcionando sin corriente?

3.9 Procedimientos recomendados

En la lista siguiente se proporcionan los procedimientos recomendados para realizar copias de seguridad y restaurar datos:

- En redes con seguridad mínima y media, conceda a un usuario derechos de copia de seguridad y otro usuario diferente derecho de restauración.

  - Sólo debe conceder derechos de copia de seguridad a usuarios que conozcan esta labor.

  - Sólo debe conceder derechos de restauración mediante la creación de un grupo local llamado Operadores de restauración y la posterior asignación al grupo del derecho de usuarios Restaurar directorio y archivos. Después, cree un grupo global llamado sólo restaurar y agrégalo al grupo local.

- Realice copia de seguridad de volúmenes enteros en el caso improbable de que se produzca un fallo de disco. Resulta más eficaz restaurar todo el volumen en una única operación.

- Haga siempre copia de seguridad del registro en un controlador de dominio para evitar la pérdida de información sobre cuentas de usuario y seguridad.

- Cree siempre e imprima un registro de copia de seguridad para cada copia de seguridad. mantenga un libro de registros para facilitar la localización de determinados archivos.

- Mantenga tres copias de los datos. Mantenga al menos una copia externa en un entorno debidamente controlado.

- Realice periódicamente una restauración de prueba para asegurarse de que los archivos se copiaron correctamente. Una restauración de prueba puede desvelar problemas de hardware que no se detectan con las comprobaciones por software.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 3

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 3 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue que entidades externas se encargan de guardar las copias de seguridad de las empresas y como es este procedimiento.

4. Explique en no mas de dos hojas porque las copias de seguridad son más importantes que cualquier otro sistema de protección de información.

5. Realice un Laboratorio en grupo de curso donde aplique los procedimientos recomendados para realizar copias de seguridad y restaurar datos.

6. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

CAPITULO 4: CONFIGURACION DE SERVIDORES

4.1 Servidores de ficheros e impresoras

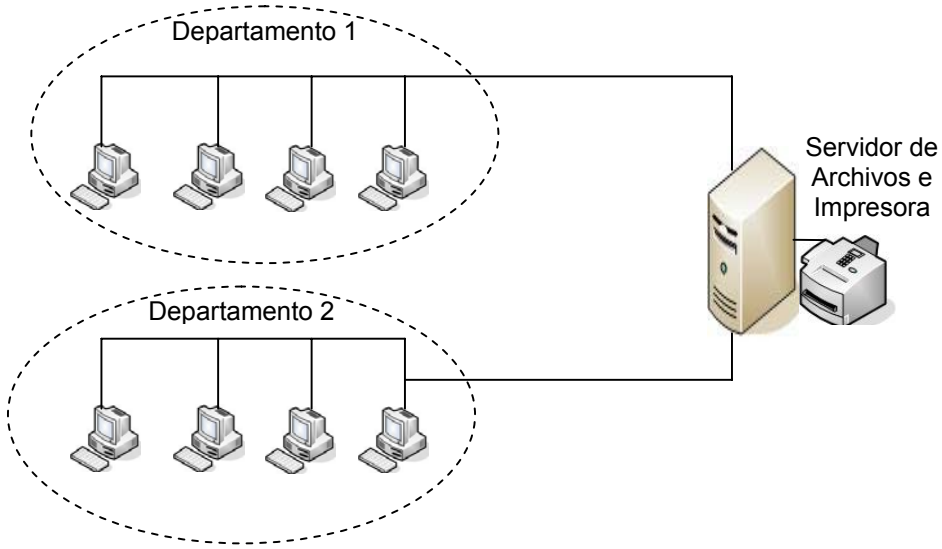


Figura 4.1 servidor de Archivos e Impresoras

Un servidor de archivos es un programa que se ejecuta en un equipo principal y que permite que el resto de Computadores de red tengan acceso controlado a los archivos. Este acceso suele hacerse desde Windows a través de unidades de red compartidas y desde Linux mediante puntos de montaje.

Supongamos que todos los miembros de un departamento determinado deben poder acceder al área de documentos corporativos; no es práctico mantener copias de todos estos archivos en cada ordenador ni mediante CDs o DVDs (son muy peligrosos por la facilidad de pérdida o robo). Estos dos métodos no son viables si existe la posibilidad que se incorporen nuevos archivos a la dependencia o se modifiquen los existentes.

El sistema más efectivo es emplear un ordenador central (servidor) cuya única función sea servir los archivos en unidades compartidas donde el resto de ordenadores se conectarán.

Limitaciones:

Si, por la naturaleza de los datos, es frecuente que varias personas accedan simultáneamente al mismo archivo y lo modifiquen (con los serios problemas que

esto puede implicar), significará que las necesidades reales escapan de lo que puede ofrecer un servidor de archivos. Probablemente deberá estudiarse el contenido de ese archivo y desarrollarse una solución a medida; normalmente esta solución es bastante sencilla y consiste en crear una base de datos central y unas pocas pantallas de acceso.

4.1.1Configuración

Las carpetas compartidas se utilizan para ofrecer accesos a los usuarios a aplicaciones de red, datos y carpetas particulares. A continuación se dan algunas importantes observaciones y recomendaciones para tener en cuenta en el momento de configurar el uso compartido:

- Las carpetas de aplicaciones de red centralizan la administración al designar una ubicación para configurar y actualizar el software. De esta manera se evita el mantenimiento de aplicaciones en los clientes.

- Las carpetas de datos proporcionan una ubicación centralizada para que los usuarios puedan almacenar y tener acceso a archivos comunes.

- Las carpetas particulares de los usuarios proporcionan una ubicación centralizada para realizar una copia de seguridad de los datos del usuario.

- Se deben asignar permisos a las carpetas y recursos compartidos, para garantizar que los usuarios pertinentes sean los que utilicen correctamente el recurso.

- Cuando una carpeta o recurso de la red tiene el atributo de compartida. Los usuarios con los permisos apropiados tienen acceso a la manipulación total de esos recursos.

Los permisos que con más frecuencia se utilizan en los diferentes sistemas operativos de red son los siguientes:

- Lectura
- Escritura
- Lectura/Escritura
- Ejecución
- Cambio
- Control total
- Sin acceso

4.2 Servidor de correo

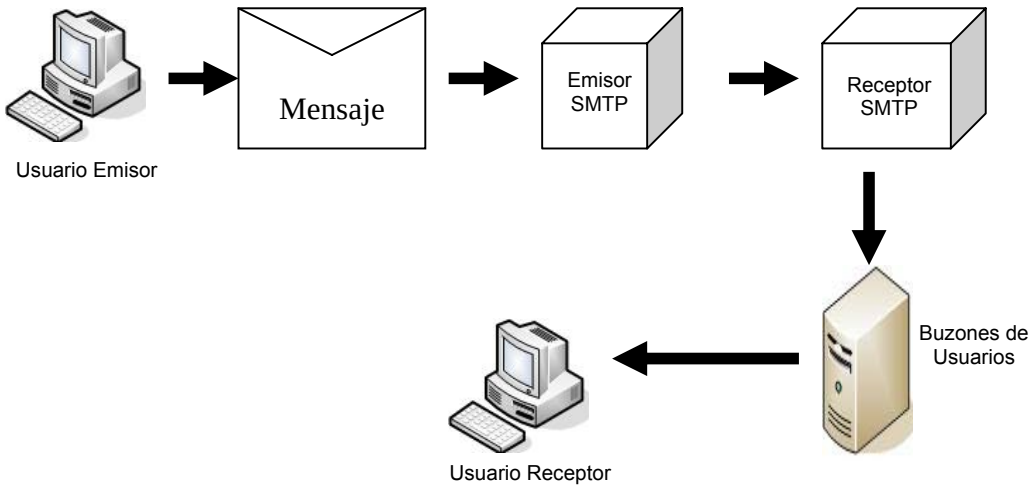


Figura 4.2 Servidor de Correo

Un servidor de correo es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

Para lograrlo se definen una serie de protocolos, cada uno con una finalidad concreta:

- **SMTP (Simple Mail Transfer Protocol):** Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes.

POP (Post Office Protocol): Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes.

Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes, y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

4.2.1 Configuración

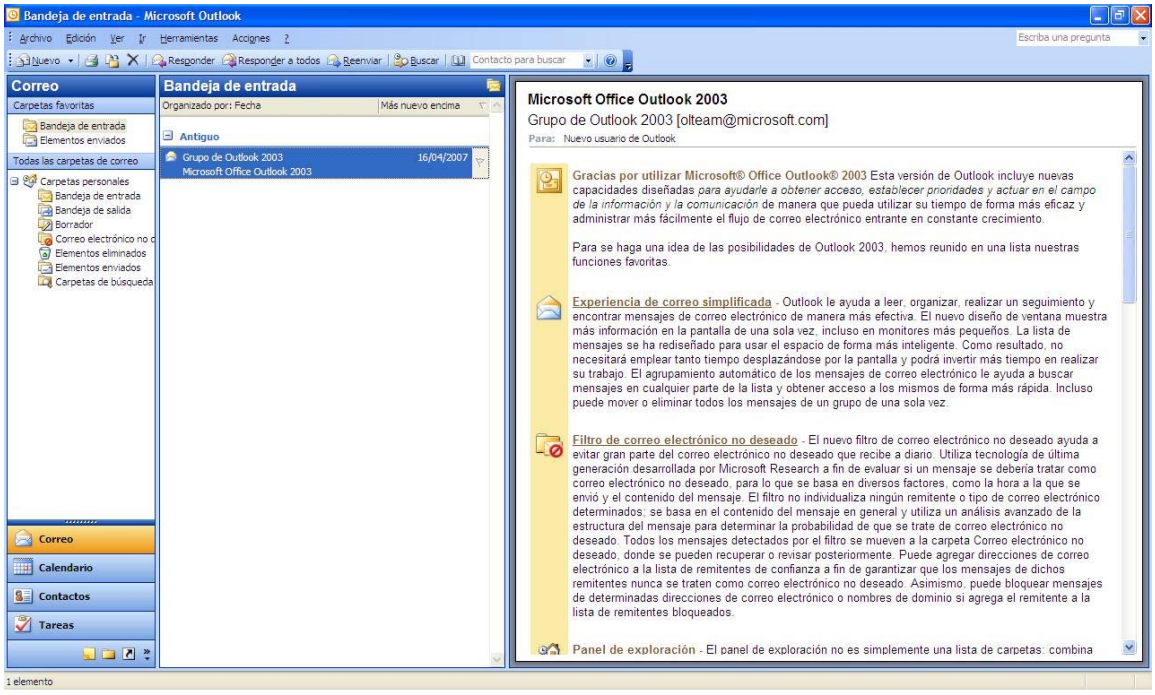


Figura 4.3 Aplicativo para el servicio de correo en clientes

Para obtener los mensajes del servidor, los usuarios se sirven de clientes, es decir, programas que implementan un protocolo POP/IMAP. En algunas ocasiones el cliente se ejecuta en la máquina del usuario (como el caso de Mozilla Thunderbird, Evolution, Microsoft Outlook). Sin embargo existe otra posibilidad: que el cliente de correo no se ejecute en la máquina del usuario; es el caso de los clientes vía Web, como Gmail, Hotmail, OpenWebmail, SquirrelMail o Terra. En ellos la arquitectura del servicio es más compleja:

En una máquina (A) tenemos el servidor SMTP y el servidor POP/IMAP. En otra (B) tenemos un servidor Web con una aplicación cliente POP/IMAP. El usuario conecta vía WEB con (B) y entonces el cliente POP/IMAP establece una conexión POP/IMAP con el servidor de la máquina A; éste servidor le devuelve a B los mensajes del usuario, y una vez recibidos, el cliente genera una página Web con los mensajes recibidos. La página Web se pasa al servidor Web que será el que la envíe al explorador Web del usuario.

En cualquier caso, los protocolos SMTP/POP/IMAP son inseguros en cuanto a que los mensajes viajan en claro por la red, es decir, es fácil obtener nuestros mensajes y contraseñas. Para ello se suele añadir una capa SSL, es decir, un método de cifrado que puedan implementar tanto el servidor como el cliente. En el caso del correo vía Web se pueden utilizar dos capas SSL: una entre A y B y otra entre el servidor Web de B y el navegador Web del usuario.

4.3 Servidores Web y FTP

4.3.1 Servidores Web

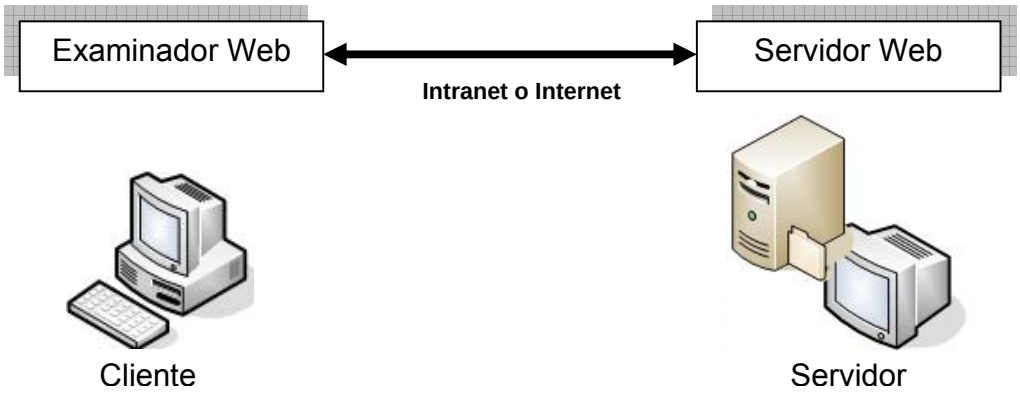


Figura 4.4 Servidor Web

Un servidor Web es un programa que implementa el protocolo HTTP (Hypertext Transfer Protocol). Este protocolo está diseñado para lo que llamamos hipertextos, páginas Web o páginas HTML (Hypertext Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

Un servidor Web se encarga de mantenerse a la espera de peticiones HTTP llevada a cabo por un cliente HTTP que solemos conocer como navegador. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al teclear cualquier dirección Web en un navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla. Como vemos con este ejemplo, el cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Sobre el servicio Web clásico podemos disponer de aplicaciones Web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- **Aplicaciones en el lado del cliente:** El cliente Web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Normalmente, los navegadores permiten ejecutar aplicaciones

escritas en lenguaje javascript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins.

- **Aplicaciones en el lado del servidor:** El servidor Web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones Web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional, como sí ocurre en el caso de querer ejecutar aplicaciones javascript o java. Así pues, cualquier cliente dotado de un navegador Web básico puede utilizar este tipo de aplicaciones. Algunos servidores Web importantes son:

- Apache
- IIS (Internet Information Server)
- Cherokee

4.3.2 Servidores FTP

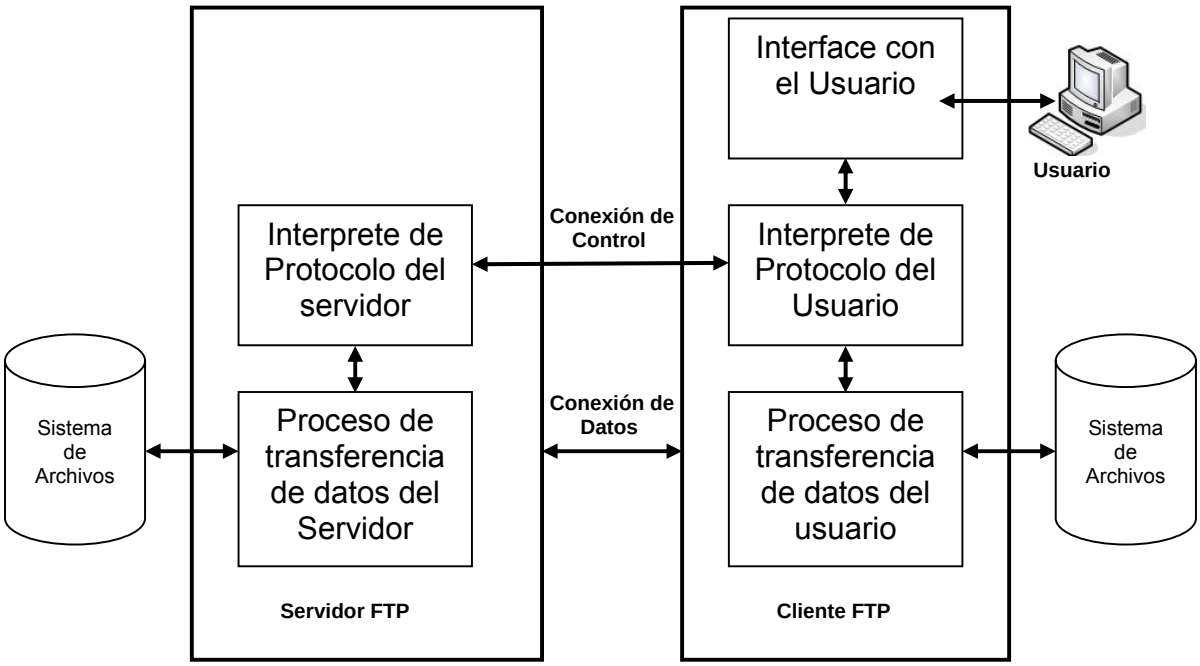


Figura 4.5. Servicio FTP

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

Por lo general, los programas servidores FTP no suelen encontrarse en los ordenadores personales, por lo que un usuario normalmente utilizará el FTP para conectarse remotamente a uno y así intercambiar información con él.

Las aplicaciones más comunes de los servidores FTP suelen ser el alojamiento Web, en el que sus clientes utilizan el servicio para subir sus páginas Web y sus archivos correspondientes; o como servidor de backup (copia de seguridad) de los archivos importantes que pueda tener una LAN. Para ello, existen protocolos de comunicación FTP para que los datos se transmitan cifrados, como el SFTP (Secure File Transfer Protocol).

Cliente FTP

Cuando un navegador no está equipado con la función FTP, o si se quiere cargar archivos en un ordenador remoto, se necesitará utilizar un programa cliente FTP.

Un cliente FTP es un programa que se instala en el ordenador del usuario, y que emplea el protocolo FTP para conectarse a un servidor FTP y transferir archivos, ya sea para descargarlos o para subirlos.

Para utilizar un cliente FTP, se necesita conocer el nombre del archivo, el ordenador en que reside (servidor, en el caso de descarga de archivos), el ordenador al que se quiere transferir el archivo (en caso de querer subirlo nosotros al servidor), y la carpeta en la que se encuentra.

Algunos clientes de FTP básicos en modo consola vienen integrados en los sistemas operativos, incluyendo Windows, DOS, Linux y Unix. Sin embargo, hay disponibles clientes con opciones añadidas e interfaz gráfica. Aunque muchos navegadores tienen ya integrado FTP, es más confiable a la hora de conectarse con servidores FTP no anónimos utilizar un programa cliente.

Acceso anónimo

Los servidores FTP anónimos ofrecen sus servicios libremente a todos los usuarios, permiten acceder a sus archivos sin necesidad de tener una cuenta de usuario. Es la manera más cómoda fuera del servicio Web de permitir que todo el mundo tenga acceso a cierta información sin que para ello el administrador de un sistema tenga que crear una cuenta para cada usuario.

Si un servidor posee servicio 'FTP anonymous' solamente con teclear la palabra "anonymous", cuando pregunte por tu usuario tendrás acceso a ese sistema. No

se necesita ninguna contraseña preestablecida, aunque tendrás que introducir una sólo para ese momento, normalmente se suele utilizar la dirección de correo electrónico propia.

Solamente con eso se consigue acceso a los archivos del FTP, aunque con menos privilegios que un usuario normal. Normalmente solo podrás leer y copiar los archivos existentes, pero no modificarlos ni crear otros nuevos.

Normalmente, se utiliza un servidor FTP anónimo para depositar grandes archivos que no tienen utilidad si no son transferidos a la máquina del usuario, como por ejemplo programas, y se reservan los servidores de páginas web (HTTP) para almacenar información textual destinada a la lectura en línea.

Acceso de usuario

Si se desean tener privilegios de acceso a cualquier parte del sistema de archivos del servidor FTP, de modificación de archivos existentes, y de posibilidad de subir sus propios archivos, generalmente se suele realizar mediante una cuenta de usuario. En el servidor se guarda la información de las distintas cuentas de usuario que pueden acceder a él, de manera que para iniciar una sesión FTP debemos introducir un login y un password que nos identifica unívocamente.

Acceso de invitado

El acceso sin restricciones al servidor que proporcionan las cuentas de usuario implica problemas de seguridad, lo que ha dado lugar a un tercer tipo de acceso FTP denominado invitado (guest), que se puede contemplar como una mezcla de los dos anteriores.

Tipos de transferencia de archivos en FTP

Es importante conocer cómo debemos transportar un archivo a lo largo de la red. Si no se utilizan las opciones adecuadas se puede destruir la información del archivo. Por eso, al ejecutar la aplicación FTP, se debe de utilizar uno de estos comandos (o poner la correspondiente opción en un programa con interfaz gráfica):

Type ASCII

Adecuado para transferir archivos que sólo contengan caracteres imprimibles (archivos ASCII, no archivos resultantes de un procesador de texto), por ejémplo páginas HTML, pero no las imágenes que puedan contener.

Type binary

Este tipo es usado cuando se trata de archivos comprimidos, ejecutables para PC, imágenes, archivos de audio...

4.4 Servidores DHCP

4.4.1 Introducción a DHCP

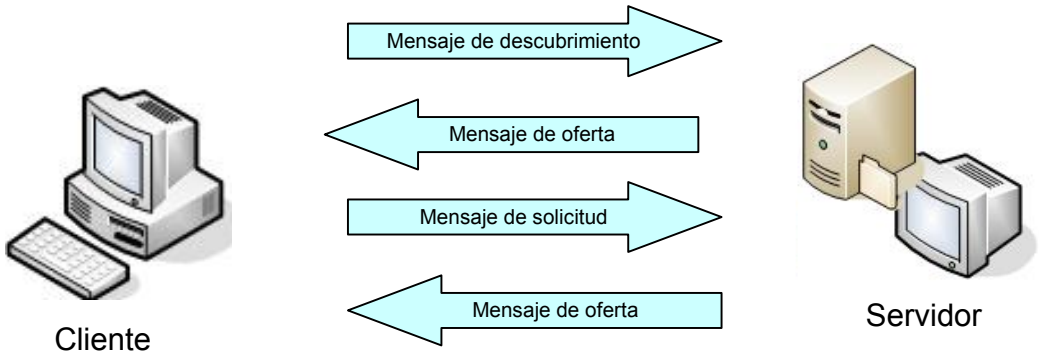


Figura 4.6 Servidor DHCP

El servicio Servidor DHCP (Dynamic Host Configuration Protocolo) centraliza y administra la asignación de los datos de configuración de TCP/IP al asignar automáticamente direcciones IP a los equipos que están configurados para utilizar DHCP. Al implantar DHCP se eliminan algunos de los problemas de configuración asociados con la configuración manual de TCP/IP.

Utilice DHCP para definir los parámetros TCP/IP globales y de subred de una red. Los parámetros de configuración de TCP/IP que un servidor DHCP puede asignar dinámicamente incluye:

- Dirección IP para cada una de las tarjetas adaptadoras de red de un equipo.
- Máscaras de subred que identifiquen la parte de la dirección IP que es el identificador del segmento físico (subred).
- La puerta de enlace o gateway predeterminada (enrutador) que conecta la subred con otros segmentos de la red.
- Parámetros de configuración a los clientes DHCP, como un nombre de dominio.

Cada vez que se inicie un cliente DHCP, solicita esta información de configuración TCP/IP al servidor DHCP: cuando un servidor DHCP recibe una petición, seleccionada una dirección definidas en sus bases de datos y, a continuación, la ofrece al cliente DHCP. Si el cliente acepta la oferta, la dirección IP se concede al cliente durante un período especificado de tiempo.

Para entender por qué es beneficioso DHCP en la configuración de direcciones IP en clientes, es útil contrastar el método manual de configuración de TCP/IP con el método automático mediante DHCP.

Configuración manual de direcciones IP

La asignación y configuración manual de las direcciones IP tienen los siguientes efectos sobre la administración y presenta los siguientes problemas:

- El administrador de un cliente puede escribir una dirección IP aleatoria en el lugar de una dirección IP válida asignada por el administrador de la red. El establecimiento de una dirección no válida o de una dirección que ya esté en uso puede provocar problemas de red cuya causa es difícil de encontrar.

- La configuración incorrecta de la máscara de subred o de la puerta de enlace o gateway predeterminada puede causar problemas de comunicación. Por ejemplo, si la puerta de enlace predeterminada no está configurada correctamente, podría ser imposible establecer comunicaciones fuera de la red local.

- Existe una carga de trabajo de tipo administrativo si los equipos pasan frecuentemente de una subred a otra. Por ejemplo, para permitir que un equipo se comunique desde una nueva ubicación, es necesario cambiar la dirección IP y la dirección IP de puerta de enlace o gateway predeterminada.

Uso de DHCP para configurar direcciones IP

El uso de DHCP para configurar automáticamente las direcciones IP proporciona las siguientes ventajas:

- El cliente recibe una dirección IP válida

- La información de configuración es correcta, lo que elimina muchos problemas de red de difícil seguimiento.

4.2 Configuración de Ámbitos

Antes de que los clientes DHCP puedan obtener direcciones IP de un servidor DHCP, es necesario crear al menos un ámbito. Un ámbito es un rango de direcciones IP con una serie de opciones de configuración que se aplican a los clientes que utilizan las direcciones del ámbito. Todos los ámbitos tienen las siguientes propiedades:

- Un nombre de ámbito.
- Una máscara de subred.
- Una dirección de la concesión.

Cualquier herramienta de administrador DHCP permite configurar los aspectos relacionados con DHCP.

Antes de crear un ámbito, se deben determinar los siguientes datos:

- La dirección IP inicial del rango asignado al ámbito.
- La dirección IP final.
- La máscara de subred utilizada.
- Cualquier dirección del rango que desee excluir y no ofrecer a los clientes.
- La duración de la concesión.

4.3 Administrar varios servidores DHCP

Una red admite cualquier número de servidores DHCP, varios servidores reducen la carga de trabajo de un solo servidor y posibilitan la asignación de direcciones DHCP en caso de uno de ellos.

Desgraciadamente no es posible contar con servidores DHCP redundantes para el mismo ámbito. DHCP no dispone de un mecanismo que permita a los servidores intercambiar la información de sus concesiones. Si una dirección IP aparece en las definiciones de ámbito de dos servidores, puede producirse la asignación de direcciones IP duplicadas. Esta ausencia de tolerancia a fallos es un grave defecto de la arquitectura DHCP.

Es posible dotar al sistema de cierta tolerancia a fallos mediante la configuración de dos servidores DHCP para cada subred. A continuación se divide el rango de direcciones de subred entre los ámbitos de los dos servidores. Esta solución no es perfecta, ya que cuando uno de los servidores está fuera de servicio no es posible utilizar la mitad de las direcciones IP. Sin embargo, los clientes pueden obtener concesiones de uno de los servicio en caso de fallo del otro.

Otro método que aporta una supuesta tolerancia a fallos consiste en configurar dos servidores DHCP con ámbitos exactos. En este caso, uno de los servidores permanece apagado mientras el otro proporciona las concesiones. En caso de fallo del servidor activo, debe iniciarse el servidor de respaldo.

El problema de este sistema radica en que el servidor DHCP recién activado no dispone de una copia de la base de datos del servidor que ha fallado. Por tanto, no es capaz de determinar las direcciones que entren en conflicto con las activas. Asimismo, puede denegar la renovación de concesiones a los clientes que estén trabajando en la red y hayan obtenido sus direcciones del antiguo servidor. La situación puede llegar a ser muy complicada. La única posibilidad consiste en copiar la base de datos del servidor inactivo. En cualquier caso, el éxito de esta opción depende de la posibilidad de acceder a los archivos del amigo servidor DHCP..

El uso de dos servidores que comparten un mismo espacio de direcciones de subred no mejora la situación. Hay que realizar un seguimiento exhaustivo de los fallos del servidor DHCP y estar preparado en todo momento para recuperar la información a la mayor brevedad posible.

4.5 Conexión a Internet y RAS

El tipo de conexión entre las computadoras de la LAN e Internet depende en gran medida de lo que se espera conseguir de la conexión. La siguiente lista presenta algunas posibilidades:

- Algunos usuarios necesitan algún acceso esporádico a los servicios de Internet.
- Desea que todos los usuarios de la LAN puedan conectarse a Internet.
- Desea instalar un servidor FTP para que los usuarios de texto puedan utilizar Internet para enviar y recibir archivos. Los usuarios internos deben acceder a los archivos del servidor FTP pero no necesitan conexión a Internet.
- Desea configurar un servidor Web para anunciar su empresa en Internet
- Todos los usuarios necesitan acceder a Interne. Además, desea que los usuarios externos de Internet puedan acceder a los servicios de su red e intercambiar datos con los usuarios internos a través de correo electrónico y transferencia de archivos.

Una vez definidos los requisitos de organización, puede comenzar a plantearse las siguientes preguntas:

- ¿Necesita un acceso permanente a Internet o es suficiente un acceso conmutado (telefónico)?

- ¿Necesita computadoras dedicadas para ofrecer servicios como FTP o World Wide Web, o puede proporcionar los servicios desde un sistema no dedicado?

- ¿Cuáles son los riesgos del tipo de conexión deseado y qué precauciones deben tomarse?

Es posible conectar las computadoras a Internet utilizando dos métodos: una conexión conmutada (telefónica) o un canal de comunicación dedicado. Las conexiones conmutadas y dedicadas dan respuesta a distintos tipos de necesidades.

4.5.1 Conexiones a Internet conmutadas

El servidor de Acceso remoto (RAS) admite varios tipos de conexión a Internet:

- Modems analógicos. Conexiones telefónicas que utilizan los protocolos SLIP y PPP a la velocidad de los módems analógicos.

- RDSI. Conexiones telefónicas de alto rendimiento utilizando el protocolo PPP

- Conmutación de paquetes hasta 56 Kbps.

Las conexiones conmutadas, por ejemplo con un modem analógico o a través de RDSI, se adaptan mejor a los usuarios que solo requieren un acceso esporádico a Internet. Es posible configurar una computadora con un modem analógico a modem de encaminador TCP/IP entre una red e Internet. Sin embargo, cualquier usuario que haya utilizado un modem para conectarse a Internet ha podido comprobar la lentitud de las conexiones analógicas. No es imaginable que varios usuarios puedan compartir un modem de 56 Kbps para establecer una conexión cómoda.

Una idea equivocada pero extendida con respecto a los modems analógicos consiste en que la compresión de datos es un método fiable para conseguir altas velocidades de transmisión. Aunque la mayoría de los modems actuales admiten comprensión de datos, varios factores limitan su utilidad:

- La escasa calidad de las conexiones impide que los modems utilicen su velocidad máxima. Los modems negocian la velocidad de transmisión cuando se conectan por primera vez. Para bello, se basan en la velocidad máxima que permite una transmisión fiable considerando la calidad de la conexión. Normalmente, la velocidad es inferior a su potencial teórico.

- La escasa calidad de las conexiones pueden impedir que los modems utilicen la comprensión de datos.

- Los datos comprimidos no pueden comprimirse nuevamente. Muchas tareas que conllevan el transporte de grandes cantidades de datos, la carga y descarga de archivos, por ejemplo, suelen implementar su propia comprensión. Como ejemplo, la mayoría de los gráficos de la página Web se guardan en formato comprimido. Los modems no son capaces de conseguir una mayor comprensión de estos datos y por tanto, la velocidad queda limitada a la tasa máxima de transmisión sin comprensión de datos.

Por consiguiente, los modems deberían considerarse como herramientas de conectividad personal.

RDSI es otro método de comunicación conmutada. El servicio RDSI proporciona dos canales “B” de 64 Kbps que pueden utilizarse conjuntamente para conseguir una velocidad total de 128 Kbps. RDSI puede dar servicio a varios usuarios, pero sigue siendo un método de conectividad conmutado. Es necesario establecer una conexión cada vez que se accede a Internet. Las tarifas del servicio RDSI se basan en el tiempo de conexión, y el coste puede dispararse si los usuarios se conectan durante largos periodos de tiempo.

RAS admite una opción no conmutada: X.25. Aunque es posible conseguir una conexión X.25 dedicada, el límite de la velocidad de transmisión es de 64 Kbps. Este valor es adecuado para unos cuantos usuarios de Internet pero resulta inaceptable si docenas de usuarios envía archivos o acceden a la Web.

Las conexiones conmutadas requieren una llamada previa. Si desea que su presencia en Internet sea permanente para ofrecer Web, FTP u otro servidor, debe recurrir a una conexión dedicada y permanente.

4.5.2 Conexiones permanentes a Internet

Una conexión permanente a Internet implica el alquiler de una línea digital dedicada entre su sitio y el sitio que proporciona la conexión Internet. Existen líneas dedicadas para una gran variedad de tasas de datos: desde 56 Kbps hasta mega bits por segundo. Su coste es elevado aunque inevitable si desea una presencia permanente en Internet.

Normalmente, cuando configure una conexión permanente a Internet, trabajará con un ISP o un proveedor de servicios de telecomunicaciones que se encargaría de diseñar e instalar el circuito y los equipos terminales necesarios. La red local deberá conectarse a la interfaz de un enrutador situado en su extremo de la conexión. El proveedor de servicios se encargará de todos los aspectos relacionados con la conexión de la interfaz WAN a Interne, pero en ningún caso de

la red local. Por tanto, debe asegurarse de comprender la interfaz y las tareas de confirmación y administración que deberá llevar a cabo en el lado de la red local. Si es necesario, recurra al proveedor de servicios para obtener la formación y el soporte técnico que le permitirán administrar su parte del enlace de comunicaciones.

Las conexiones a Internet permanentes implican un riesgo. La seguridad no fue una consideración principal durante el diseño de los protocolos TCP/IP, y muchos usuarios de Internet disponen de conocimientos suficientes para entrar en su red.

Aislar el servidor

Si su organización sólo desea ofrecer un servicio a la comunidad Internet sin permitir que los usuarios internos utilicen la misma conexión, resulta sencillo controlar riesgos de seguridad, aislando por completo a los usuarios locales con respecto a Internet. Si alguien consigue entrar en su servidor de Internet, no podrá penetrar en la red local.

Considere la siguiente situación. Su organización es una editorial de revistas. Desea que los autores puedan enviar sus artículos a través de ftp y desea que lo editores puedan conseguirlo si la red local está aislada del servidor Internet. En la figura, la red local está aislada físicamente de Internet, lo que hace segura pero impide la comunicación entre los entornos local y remoto.

4.5.3 Conexiones a través de un servidor Proxy

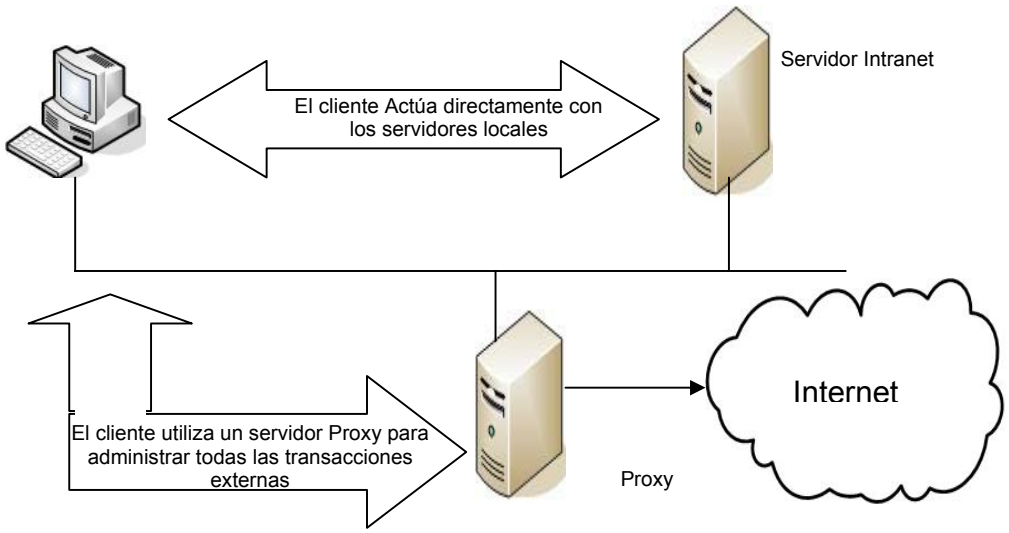


Figura 4.7. Conexión a través de un Proxy.

Un servidor Proxy ofrece otra alternativa para controlar el tráfico entre la red local e Internet. Un servidor Proxy utiliza el siguiente procedimiento para surtir a los hosts locales que interactúan con una red externa.

1. un cliente que necesita acceder a un host examina una tabla para determinar si la dirección IP de host pertenece a la red local o remota.
2. si la dirección IP es remota, el cliente envía la solicitud al servidor Proxy.
3. El servidor Proxy utiliza su dirección para reemplazar la dirección IP del host. A continuación, encamina la solicitud al host remoto.
4. El host remoto responde a la solicitud devolviendo el resultado al servidor Proxy.
5. El servidor Proxy sustituye la dirección IP con la del host que ha originado la solicitud y la envía la respuesta.

4.5.4 Uso de RAS para conectarse a Internet

Una conexión telefónica a través de RAS puede ser método de conexión a Internet aceptable para los particulares y las LAN de tamaño reducido. Las cuentas TCP/IP de acceso telefónico utilizan dos protocolos. SLIP es un antiguo protocolo que ofrece un alto rendimiento carente de comodidades como la detección de errores. PPP es un protocolo mejorado y más fiable que SLIP que ofrece cierta ventaja administrativas a cambio de un menor rendimiento. La mayoría de cuentas de acceso telefónico a Internet utilizan el protocolo PPP.

Necesita los siguientes elementos para conectarse a Internet:

- Una cuesta SLIP o PPP con un proveedor de acceso a Internet. Debe disponer de la siguiente información:
  - Número telefónico de acceso
  - Nombre de usuario.
  - Nombre de host
  - Contraseña
- Si las direcciones IP no se asignan dinámicamente al establecer la conexión, necesita la siguiente información:

- Dirección IP
- Máscara de subred
- Dirección de la Gateway predeterminada
- Dirección IP de los servidores DNS primario y de respaldo.

4.6 Servidores DNS

La resolución de los nombres DNS se realiza por medio de servidores de nombres: programas que ejecutan en los hosts de la red. Dada la amplitud de Internet, DNS se diseño para que varios servidores de nombres pudieran repartirse las tareas de resolución. Para ello, el espacio de nombres se divide en zonas. Cada zona puede ser atendida por sus propios servidores.

Organización de los servidores de nombres DNS

Un servidor de nombres que administra los datos de una zona disponible de autoridad sobre la zona. Todo servidor de nombres tiene autoridad sobre, al menos, una zona, pero un solo servidor puede tener autoridad sobre varias zonas. Observe que no es necesario que la zonas se ajusten a la estructura de domino. Aunque un dominio debe consistir en un subárbol del espacio de nombres general, no es preciso que las zonas consistan en nodo solo servidor de nombres preste servicios de resolución a varios dominios.,

El servidor de nombre principal de una zona se denomina servidor maestro primario y contiene los datos de la zona en sus archivos de configuración. Los servidores maestro secundarios contienen copias redundantes de los servidores primarios y obtienen la información mediante transferencias de zonas procedentes del servidor maestro primario de la zona. La configuración de varios servidores de nombres en una misma zona aporta tolerancia a fallos y mejora el rendimiento gracias a la distribución de los procesos de resolución de nombres entre varios hosts.

La asignación de los servidores primarios y secundarios es sumamente flexible. Un servidor puede tener autoridad sobre una o varias zonas y puede funcionar como primario para una zona y secundario para otra.

Dado que los intentos de resolución de nombres comienzan por la raíz del dominio, el dominio raíz de Internet dispone de nuevos servidores de nombres, incluidos los NSFNET, MILNET, SPAN (NASA) y Europa. Todos ellos tienen autoridad sobre todos los dominios de máximo nivel de Internet. La autoridad sobre los dominios secundarios e inferiores se reparte entre numerosos servicios administrados por las organizaciones que están presentes en Internet.

Cuando una organización obtiene un nombre de dominio. En muchos casos, designar un servidor de nombre que tenga autoridad sobre su dominio. En muchos casos, los servidores de nombre residen en un host administrado por el propietario del dominio. Sin embargo, no es necesario que cada organización se responsabilice de su propio servidor. Muchas de las conexiones a Internet se obtiene mediante proveedores comerciales de acceso. Muchos de ellos mantienen las zonas de los clientes en sus servidores de nombres. Es recomendable recurrir a un proveedor de acceso a Internet que administre el espacio de nombre del

dominio si la organización es de pequeño tamaño o si no se justifica el coste de mantenimiento de DNS: el personal experto y el hardware necesario par los servidores primario y secundario.

El mantenimiento del conjunto del espacio de nombres de dominio de Internet recae sobre varios servidores de nombre que, en cierta medida, se reconocen entre sí. La red distribuida de servidores de nombre coopera para prestar servicios de resolución a toda la comunidad de Internet.

Resolución de nombres DNS

El componente cliente del servidor de nombre se basa en subprogramas de resolución. Que forman parte de los procesos y aplicaciones TCP/IP y que utilizan los nombres de host DNS. Los subprogramas de resolución están incluidos en los software de cada aplicación, por ejemplo FTP o Telnet, y permiten establecer contacto con un servidor de nombres para iniciar consultas de resolución de nombres. El subprograma de resolución de una aplicación puede generar una consulta DNS, pero la resolución se lleva a cabo en los servidores de nombres de la red.

La configuración de una host TCP/IP incluyen la dirección IP de, al menos, un servidor DNS. Cuando una aplicación solicita un servicio de resolución de nombre, genera una consulta y la envía al servidor conocido, identificado en la figura como <servidor de nombres local>. Si éste no es capaz de resolver el nombre consultado, inicia un proceso de búsqueda que comienza por uno de los servidores de nombre raíz. El servidor de nombres raíz proporciona la dirección de un servidor que tenga autoridad sobre primer nivel del dominio al que hace referencia la consulta. La búsqueda prosigue pasando al servidor nombres de dominio del segundo nivel, y desciende hasta llegar a un servidor que pueda proporcionar una respuesta.

El proceso de búsqueda de nombres depende del estado de la jerarquía de servidores de nombres. Las resoluciones fallan si, en algún nivel, no existe un servidor disponible. Esta particularidad demuestra la importancia de utilizar servidores primarios y secundarios y explica la existencia de nueve servidores en el dominio raíz de Internet. Aunque los servidores de nivel inferior reducen el tráfico mediante el uso de un caché de nombres resueltos recientemente, si todos los servidores de nombres del dominio raíz fallaran, podría paralizarse el servicio de resolución de nombres.
Existen dos mecanismos distintos de consulta, denominados iterativo y recursivo, sobre los que encontramos, con frecuencia, referencias a ambos tipos de consulta, por tanto, es importante conocer sus características.

Consultas iterativas

El servidor local tiene la mayor responsabilidad en el proceso de resolución. Debe consultar repetidamente a los servidores remotos para obtener las partes de información que componen la respuesta final. Los servidores de nombres remotos realizan una de las dos acciones: devuelven los datos solicitados o devuelven una referencia a otro servidor de nombres que pueda llevar a cabo el siguiente paso de consulta.

Este tipo de consultas, realizadas por el servidor local, se de nomina resolución iterativa (o resolución no recursiva). El término iteración se utiliza en informática como sinónimo de <repetición>. Un solo proceso se repite, utilizando normalmente el resultado de la última repetición, hasta que se obtiene la respuesta deseada o se produce un error. En una situación óptima, el resultado de cada iteración se aproxima más al objetivo de búsqueda.

Dado que gran parte del trabajo de resolución de un nombre se lleva en el servidor local, el proceso puede llevarse a cabo a través de un único subprograma de resolución situado en el lado de la aplicación. Además , aunque las consultas iterativas generan un número mayor de diálogo entre servidores, son relativamente fáciles de implementar. Por tanto, éste es el método empleado en la mayoría de los casos.

Consultas recursivas

Otra variante de la resolución de nombres es la resolución o resolución recursiva. Cuando un servidor de nombres recibe una consulta recursiva, sólo puede devolver los datos buscados o un error. Si el servidor carece de autoridad sobre el dominio al que hace referencia la consulta, debe encargarse de consultar a otro servidor para obtener los datos.

El servidor de nombres locales recibe una consulta recursiva del cliente. El servidor local puede responder a ella haciendo referencia a otro servidor, debe proporcionar el nombre que se busca o notificar que se ha producido un error.

El servidor local satisface la consulta del cliente realizando consultas iterativas a otros servidores de nombres que proporcionan referencias sucesivas que permiten a acceder a un servidor con autoridad.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 4

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 4 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue las características de los diferentes Aplicativos FTP del mercado utilizados para transferencia de archivos.

4. Que sistemas operativos ofrecen Administración DHCP o herramientas que lo permitan. Explique brevemente sus características.

5. Investigue nombres y características de algunos servidores Web y que empresas los desarrollan.

6. Realice un Laboratorio en grupo de curso donde configure los diferentes servicios de la red y realice las diferentes pruebas para verificar la correcta prestación de los servicios FTP, Web, RAS, Proxy, DNS entre otros.

7. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

CAPITULO 5. ANALISIS Y OPTIMIZACION DE REDES

5.1 Salud y rendimiento de la red

Los administradores de red supervisan el rendimiento de la red por varias razones:

- Para mejorar el rendimiento basándose en la configuración existente.
- Para ofrecer capacidades de diseño y previsión
- Para obtener información esencial con el fin de detectar los cuellos de botella

Cuellos de botella

La mayoría de las actividades de la red implica la actividad coordinada de varios dispositivos. A cada dispositivo le lleva una cierta cantidad de tiempo realizar su parte de la transacción. Un rendimiento deficiente se presenta cuando uno de los dispositivos utiliza ostensiblemente más tiempo que los demás. Por lo general, a este dispositivo problemático se le conoce como cuello de botella. La mayor parte de la supervisión del rendimiento consiste en identificar y eliminar los cuellos de botella.

Los siguientes dispositivos tienden a producir cuellos de botella:

- CPU de los Servidores
- Memoria
- Tarjetas de red
- Controladores de disco
- Medios de transmisión de la red
- Hub o Switches de baja capacidad

Un dispositivo se convierte en cuello de botella debido a algunas de las siguientes razones:

- No se utiliza con la eficiencia adecuada.
- Emplean más recursos o tiempo del CPU de lo que debería.
- Es demasiado lento.
- No tiene la capacidad de manejar la tarea asignada.
- Honesta ubicado en el punto adecuado de la red.

Una supervisión adecuada reconocerá estas situaciones y proporcionará información que será útil para identificar el o los componentes problemáticos.

5.2 Tamaño y complejidad de la red

Las redes y los sistemas de procesamiento distribuidos son de una importancia crítica y creciente en las empresas, gobierno y otras instituciones. Dentro de una institución, la tendencia es hacia redes más grandes, más complejas y dando soporte a más aplicaciones y más usuarios. A medida que estas redes crecen en escala, existen dos hechos que se hacen penosamente evidentes:

- La red y sus recursos asociados y las aplicaciones distribuidas llegan a ser indispensables.

- Hay más cosas que pueden ir mal, pudiendo inutilizar la red o una parte de ella o degradar las prestaciones a un nivel inaceptable.

Una red grande no se puede instalar y gestionar solo con el esfuerzo humano. La complejidad de un sistema tal impone el uso de herramientas automáticas de gestión de la red. La urgencia de la necesidad de esas herramientas se incrementa y también la dificultad de suministrarlas es mayor, si la red incluye equipos de múltiples distribuidores. En respuesta, se ha desarrollado normalizaciones para tratar la gestión de red, y que cubren los servicios, los protocolos y la base de información de gestión.

5.3 Protocolo para la gestión de redes

SNMP (Protocolo Simple de Gestión de Redes)

Es una herramienta sencilla para gestión de red. Define una base de información de gestión (MIB) limitada y fácil de implementar constituida por variables escalares y tablas de dos dimensiones, y define un protocolo para permitir a un gestor obtener y establecer variables MIB y para permitir a un agente emitir notificaciones no solicitadas, llamadas intercepciones (“traps”). Esta similitud es la potencia de SNMP. SNMP se implementa de una forma fácil y consume un tiempo modesto del procesador y pocos recursos de red. También, la estructura del protocolo y de la MIB son suficientes directos de forma que no es difícil alcanzar la interconexión entre estaciones de gestión y software de agente de varios distribuidores.

La esencia de SNMP es un protocolo que se utiliza para intercambiar información de gestión. Cada “Ente” en un sistema de gestión de red mantiene una base de datos locales de información relevante de gestión de red, conocida como base de información de gestión (MIB). El estándar SNMP define la estructura de esta información y los tipos de datos permitidos; esta definición se conoce como estructura de información de gestión (SMI. “Struture of Management Information”). Se puede pensar que esto constituye el lenguaje para definir la información de gestión. El estándar también proporciona varias MIB que son generalmente útiles

para la gestión de red. Además los vendedores y los grupos de usuarios pueden definir nuevas MIB.

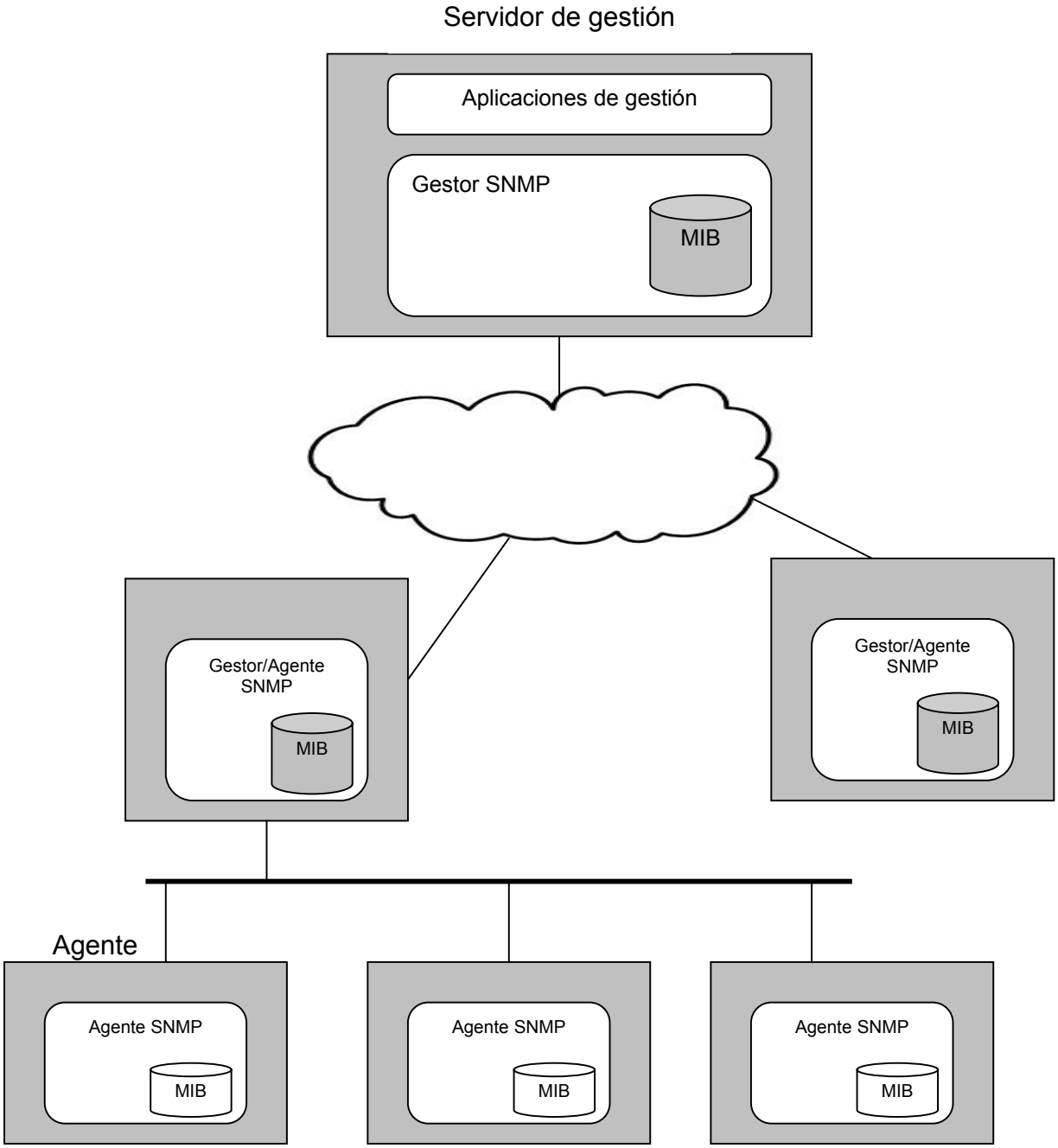


Figura 5.1. Configuración gestionada por SNMP.

Al menos un sistema de la confirmación debe ser responsable de la gestión de red. Es aquí donde se debe instalar cualquier aplicación de red. Debe haber más

de una de estas estaciones de gestión, para proporcionar redundancia o simplemente dividir las obligaciones en una red grande. La mayoría del resto de los sistemas actúan con un papel de agente. Un agente recoge información localmente y la almacena para acceso posteriores de un gestor. La información incluye datos sobre el mismo sistema y también pueden incluir información sobre el tráfico de red o redes a las que está conectado el agente.

SNMP dará apoyo a una estrategia de gestión de red altamente centralizada o distribuida. En este último caso, algunos sistemas operan con ambos papeles, el de gestor y el agente. En su papel órdenes están relacionadas con la MIB local en el agente. Otras órdenes requieren que el agente actúe como delegado para dispositivos remotos. En este caso, el agente delegado asume el papel de gestor para acceder a la información en un agente remoto, y después asume el papel de agente para pasar esa información a un gestor superior.
Todos estos intercambios se realiza utilizando el protocolo SNMP, que es un protocolo sencillo del tipo petición /respuesta. Normalmente, se implementa encima del protocolo se datagrama de usuario (UDP), que es parte del conjunto de protocolos TCP/IP. También se puede implementar por encima del protocolo de transporte de ISO.

Analizadores de red

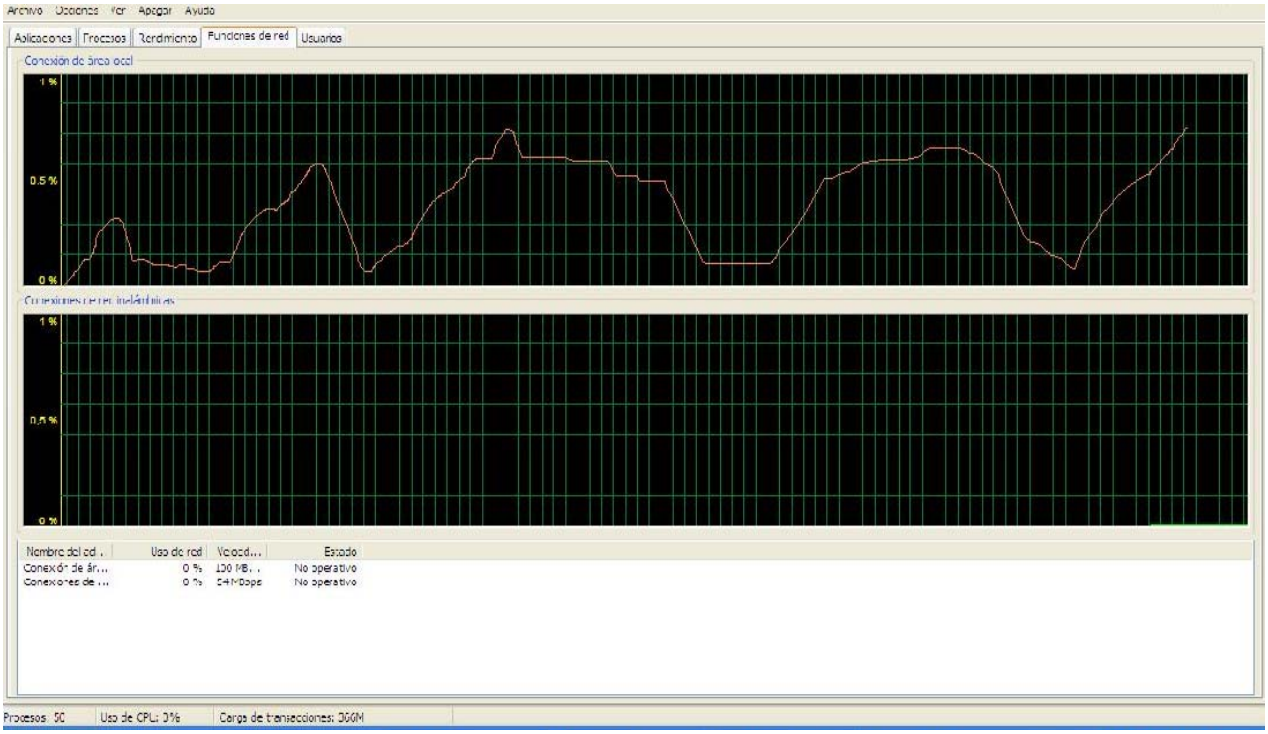


Figura 5.2 . Monitorización de la red con Sniffer

Son herramientas de administración de red que constan de un conjunto integrado de funciones para:

- Capturar tráfico de red para un análisis detallado.
- Diagnosticar problemas usando un analizador experto
- Monitorear la actividad de la red en tiempo real.
- Recolectar estadísticas detalladas de error y utilización para estaciones individuales o cualquier porción de la red.
- Guardar información histórica de utilización y errores para análisis
- Generar alarmas visibles y audibles en tiempo real y notificar a los administradores de red cuando los problemas son detectados.
- Probar la red con herramientas activas para simular tráfico, medir tiempos de respuesta, conteo de saltos y verificar problemas.

Cuando se utiliza una herramienta como el analizador de red, lo primero que se debe hacer es establecer una línea de referencia para el rendimiento de la red. Al mantener un registro del rendimiento de la red en condiciones normales, usted podrá comprender los valores de un rendimiento razonable. Con este registro, se obtiene una línea de referencia para comparar el momento en que las cosas cambian o cuando sea necesario actualizar o sustituir algo. Sin esta línea de referencia, resultará difícil determinar y mantener los niveles aceptables para el rendimiento.

Una vez establecida la línea de referencia, es posible supervisar el rendimiento de la red y comparar los resultados con la línea de referencia. Los resultados de este análisis ayudarán a determinar la necesidad de mejorar un área específica del rendimiento de la red.

Con el tiempo, la supervisión de la red también le permitirá estudiar las tendencias. Mediante el estudio de las tendencias será capaz de detectar problemas antes de que lleguen a un punto crítico. Esto hará que la planeación para el futuro y el mantenimiento de un nivel aceptable del rendimiento sean tareas más sencillas. Por ejemplo, si la red disminuye su velocidad, usted podrá determinar dónde se está produciendo el cuello de botella y tomar la acción correspondiente.

Los sistemas operativos también influyen en el rendimiento general de la red. Por tanto es indispensable realizar un seguimiento de su comportamiento en puntos claves de la red.

Supervisión del rendimiento del sistema operativo

La mayoría de los sistemas operativos de red actuales incluyen una utilería de supervisión que ayudará a que el administrador de la red haga un seguimiento sobre diversos aspectos del rendimiento del servidor de la red.

El Monitor de sistema puede:

- Grabar la información sobre el rendimiento.
- Enviar una señal de alerta al administrador de la red
- Iniciar otro programa que puede regresar el sistema a sus valores aceptables.

5.5 Analizadores de protocolos

Los analizadores de protocolos, llamados también analizadores de red, efectúan una serie de funciones en el análisis del tráfico de la red en el tiempo real, además de captura, decodificación y transmisión de paquetes. Muchos administradores e ingenieros de soporte técnico de redes experimentados que tienen bajo su responsabilidad grandes redes, confían en el analizador de protocolos. Es la herramienta que utilizan más a menudo para monitorear la red interactivamente.

Los analizadores de protocolos buscan en los paquetes para identificar la causa de un problema. También genera estadísticas basadas en el tráfico de la red para ayudar a crear una imagen de la red:

- Cableado
- Software
- Servidor de archivos
- Estaciones de trabajo
- Tarjetas de interfaz

El analizador puede proporcionar datos sobre el comportamiento de las redes entre los que se incluyen:

- Componentes de la red defectuosos
- Errores de configuración o conexión
- Cuellos de botella LAN
- Fluctuaciones del tráfico
- Problema de protocolo
- Aplicaciones que pueden entrar en conflicto
- Tráfico inusual en el servidor

Ya que los analizadotes de protocolos pueden identificar tantos aspectos del comportamiento de la red, se pueden utilizar para:

- Identificar los equipos más activos y los que están enviando paquetes con errores. Si un equipo está enviando tanto tráfico que hace disminuir la velocidad de la red para otros usuarios, el administrador o el ingeniero de soporte pueden considerar trasladar ese equipo a otro segmento de la red. Los equipos que generan paquetes erróneos se pueden reparar o quitar

- Identificar, ver y firmar determinados tipos de paquetes. Esto es importante en lo que concierne al enrutamiento y al tráfico entre redes. Como el analizador puede distinguir protocolos, puede determinar qué tipo de tráfico está circulando por un determinado segmento o componente de la red.

- Hacer un seguimiento del funcionamiento de la red durante un periodo para identificar tendencias. Reconocer tendencias puede ayudar al administrador a diseñar y configurar mejor la red, basándose en la utilización real para acomodar periodos pico y aplicaciones exigentes.

- Comprobar diversos componentes, conexiones y cableado generando paquetes de pruebas haciendo un seguimiento de los resultados.

- Identificar condiciones en que surgen problemas estableciendo los parámetros del analizador para generar alertas si el tráfico de la red cae fuera de los parámetros

5.6 Rendimiento en redes LAN

La aproximación del diseño tradicional de redes de computadores sigue un análisis de sistemas estructurados y el proceso de diseño como tal, es muy similar al que se utiliza para construir sistemas de aplicaciones. podemos decir que sigue los siguientes pasos:

- El analista de la red se reúne con los usuarios para determinar las necesidades y las aplicaciones que se van a utilizar.
- El analista de la red estima el tráfico de datos sobre la cada parte de la red.
- El analista de la red diseña los circuitos necesarios para soportar este tráfico y obtener costos estimados
- Finalmente, 1 ó 2 años después, la red es implementada.

Existen 3 fuerzas que están haciendo que la aproximación del diseño tradicional sea menos apropiada para la mayoría de las redes de computadores hay en día:

- La tecnología subyacente de computadores, dispositivos de red y los circuitos que están siendo rápidamente reemplazados.
- El crecimiento del tráfico de la red va a paso agigantados.
- El balance de los costos ha cambiado dramáticamente durante los últimos 10 años

El proceso de diseñar una red, envuelve fundamentalmente 3 pasos que son:

1. Análisis de necesidades (fase de Análisis)
2. Diseño de tecnologías (Fase de Diseño)
3. Costos de valuación (Fase de análisis de costos)

La meta del análisis de necesidades es entender por qué vamos a construir una red, cuáles serán sus usuarios y qué aplicaciones serán utilizadas. Mucho del trabajo se pudo haber hecho ya, supervisando loso sistemas existentes, que pueden proporcionar un baseline contra los requisitos futuros del diseño. Pero. ¿Qué es baseline? Un baseline es un valor o un perfil de una métrica de rendimiento pueden ser empleados de manera útil. Por ejemplo, si usted conoce la utilización promedio de un URL en particular en esta semana, este promedio puede ser usado como una baseline la cual puede comparar futuros cambios en la utilización de ese URL.

5.7 Certificadores de cables

Analizadores Avanzados

Funcionan más allá del nivel físico de OSI, en los niveles 2,3 e incluso 4. Pueden mostrar información acerca de estado del cable físico, así como:

- Recuentos de tramas de mensajes
- Colisiones por exceso
- Colisiones por demora
- Recuentos de tramas erróneas
- Errores de congestión
- Balizamiento

Estos analizadores pueden monitorear el tráfico general de la red, determinados tipos de situaciones de error o tráfico desde y aun equipo determinado. Indican si un cable particular o una tarjeta adaptadora de red determinada está causando problemas.

Reflectómetros en el domino del tiempo

Los TDR envía al cable al cable impulsos similares a un sonar para buscar cualquier tipo de fisura, cortocircuito o imperfección que pueda afectar el

rendimiento. Si un impulso encuentra un problema, el TDR lo analiza y muestra el resultado. Un buen TDR puede ubicar una fisura en un cable con un margen de centímetros de las separación real del cable. Esta herramienta se utiliza mucho durante la instalación de una red nueva, pero también es muy valiosa en la solución de problemas y en el mantenimiento de las redes existentes.

Osciloscopios

Los osciloscopios son instrumentos electrónicos que miden la cantidad de voltaje de señal por unidad de tiempo y muestra los resultados en un monitor. Cuando se utilizan con un TDR, pueden mostrar:

- Cortocircuito
- Arrugas o dobleces en el cable
- Figuras en el cable
- Datos de voltaje que pueden indicar atenuación (perdida de potencia de señal)

5.8 Problemas comunes en redes LAN

Los usuarios pueden ser de gran ayuda para recopilar la información, si se les hacen las preguntas apropiadas. El ingeniero debe preguntar: ¿Qué hace la red y qué le hace pensar al usuario que no funciona correctamente. Otras observaciones de los usuarios que pueden dar pistas son:

- “La red va realmente despacio”
- “No me puedo conectar con el servidor”
- “Estaba conectado con el servidor, pero perdí la conexión”
- “Una de las aplicaciones no funciona”
- “No puedo imprimir.”

El administrador o el ingeniero de soporte técnico experimentado tiene en cuenta los comentarios iniciales del usuario y elabora una serie de preguntas disyuntivas o de respuesta afirmativa o negativa que le ayudan a aislar el problema. Por ejemplo:

- ¿El problema afecta a muchos usuarios o a uno solo, o a varios usuarios aleatoriamente?
- ¿Ha caído toda la red o sólo un equipo?
- ¿Ya estaba ahí el problema antes de la actualización?
- ¿se produce el problema constantemente o es intermitente?
- ¿Aparece el problema con todas las aplicaciones o sólo con una?
- ¿El problema es similar a uno anterior?
- ¿Hay nuevos usuarios en la red?
- ¿Hay nuevos equipo en la red?

- ¿se instaló una aplicación nueva antes de producirse el problema?
- ¿Se trasladó parte del equipo últimamente?
- ¿De qué fabricante eran los productos implicados?
- ¿Existe un patrón entre determinados fabricantes y componentes como tarjetas, concentradores, unidades de disco, software operativo de redes?
- ¿Alguien ha intentado solucionar el problema?

Otras áreas que el administrador de redes o el ingeniero de soporte técnico deberían considerar son:

- Versiones de aplicaciones, sistemas operativos y otro software.

- Cambio de configuración de los componentes de la red o del sistema operativo de redes.

Como administradores de redes o ingeniero de soporte técnico, usted llegará a familiarizarse con los componentes y las aplicaciones de su propia de red, y será dónde debe buscar primero para hallar las cuentas posibles.

5.9 Solución a problemas

A continuación se dan una serie de recomendaciones para tener en cuanta en el momento de solucionar un problema de red.

- Asegúrese de entender el problema y poder replicarlo
- Determine si el problema está asociado a algún cambio
- No asuma nada
- Trate cada situación de tal forma como si nunca hubiera ocurrido

Determine si el problema está afectado:

- Toda la red
- Un segmento
- Una VLAN
- Un nodo
- La meta aquí es aislar el problema a un nodo, grupo o a un usuario.
- Si el problema se presenta en un segmento de la red, solo deja nodos de ese segmento
- Realice pruebas con los dos nodos si operan de forma correcta adicione uno a uno el resto de nodos. Si hay comunicación, primero revise la capa física
- Si el problema está aislado a una sola estación, intente con una tarjeta de red diferente, reinstale la tarjeta, conecte la red y compare con otras estaciones.
- Utilice partes, cables y dispositivos probados y de buena calidad
- Si un solo usuario es el que presenta el problema revise:

- Políticas de seguridad en la red
- Permisos del usuario
- Compare la situación del usuario en problemas con otros usuarios que si pueden acceder al servicio
- Una vez asimilado y localizado el problema, identificar la falla debe ser simple
- Si el problema es con el hardware, reemplace las partes que generan el problema
- Si el problema es de software: reinstale y configure
- Realice las pruebas que confirma que el problema sido solucionado
- Realice contra pruebas
- Tenga en cuenta que solución a un problema puede generar nuevos problemas.

5.10 Asignación optimas de capacidades

La solución del problema del reparto del canal consiste en buscar la forma de repartir un solo canal de difusión entre usuarios competidores. Existen dos esquemas generales que son el estático y el dinámico. A continuación vamos a ver cada uno de ellos:

Reparto estático

La manera tradicional de repartir un canal es la multiplexación por división en frecuencia (FDM). Si sólo hay N usuarios, el ancho de banda se divide en N partes iguales, una para cada usuario por lo que no hay interferencias. Cuando hay un poco y fija cantidad de usuarios, FDM es eficiente; si el número de transmisores es grande y varía continuamente, si el espectro se divide en N regiones y hay menos parte de N usuarios interesados en comunicarse, se desperdiciará una parte del espacio. Si más de N usuarios quiere comunicarse, a algunos se les negará el permiso por falta de ancho de banda.

El retardo medio de un canal de C bps de capacidad con una tasa de recepción de marcos/seg es:

$$T = 1 /(\mu C - \lambda) = NT$$

Si dividimos el canal en N el retardo medio al usar FDM es N veces peor:

$$T_{FDM} = N/(\mu C - \lambda) = NT$$

Reparto dinámico de canales en las LAN

Como primera medida, se debe formular el problema de reparto basado en los siguientes 5 supuestos:

- **Modelo de estación**: Consiste en N estaciones independientes, cada una con programa o usuario que genera, marcos para transmisión. Una vez se ha generado un marco, la estación se bloquea hasta que el macro sea transmitido con éxito.

- **Modelo de canal único**: hay un solo canal disponible para todas las comunicaciones, transmisión y recepción; en hardware todas las estaciones son iguales y con el software se asignan propiedades.

- **Supuesto de colisión**: Si dos marcos se transmiten simultáneamente se traslapan en el tiempo y la función resultante se altera, a esto se le llama colisión. Todas las estaciones las pueden detectar, no hay otros errores, sólo los causados por colisiones.

- **Tiempo continuo**: la transmisión de un marco puede comenzar en cualquier momento. No hay reloj que divida el tiempo en intervalos discretos.

- **Tiempo rasurado**: el tiempo se divide en intervalos discretos (ranuras); la transmisión de los marcos siempre comienza al inicio de una ranura.

- **Detección de portadora**: las estaciones pueden saber si el canal está en uso antes de intentar usarlo

- **Sin detección de portadora**: las estaciones no pueden detectar si el canal esta en uso antes de usarlo. Simplemente transmiten.

5.11 Los pasos claves

Aunque se efectúe el mejor diseño, monitoreo y mantenimiento, se seguirán produciendo problemas en las redes. Cuando surge un problema, al administrador de la red o el ingeniero de soporte técnico normalmente será capaz de determinar y resolver el problema con más eficiencia utilizando un procedimiento estructurado que probando soluciones aleatoriamente.

El procedimiento estructuras implican cinco pasos que llevarán a la solución del problema:

Paso 1: Recolección de información

Paso 2: Localización el problema

Paso3: Aislamiento el problema

Paso4: Corrección el problema

Paso 5: Verificación de la solución

5.9 Caso de estudio

A continuación e analiza un caso donde el problema es que no hay servicio en un punto de red:

No hay servicio en un punto de red.

Síntomas

- El usuario conecta un equipo en el punto de red y no obtiene los servicios de esta.
- Punto de vista del usuario: “la red no sirve”

Antes de actuar

- En realidad no hay servicios
- Comando ping

Elementos a considerar

- El PC del usuario.
- NIC (físico o lógico)
- Configuración

Cableado estructurado:

- Path Cord
- Toma de datos
- Toma de path panel
- Cableado horizontal

Switch

- Puerto (físico o lógico)
- Up Link

Casos típicos

- Parth cord sueltos o dañados
- Desconfiguración de la tarjeta
- Punto de red no habilitado
- Es usarlo cambio el PC de punto de red
- Problema de clave (password)
- Problema de permisos (perfil de usuario)

Conclusiones

- Cuando un usuario reporta un problema créale
- No crea todo lo que dicen los usuarios
- Guié al usuario con preguntas claves

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 5

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 5 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue las Plataformas para la gestión de redes más utilizadas en el mercado y sus principales características.

4. Cuales son las tecnologías de cables que ofrecen mayor capacidad para instalaciones de redes LAN y cuales son sus características.

5. Investigue que dispositivos de red ofrecen mejor rendimiento en las redes LAN y sus características.

6. Realice un Laboratorio en grupo de curso donde se utilizan todas las opciones de un analizador de red y analice los resultados para la toma de decisiones.

7. Elaborar los respectivos informes de los laboratorios y entréguelos al Tutor.

TERCERA UNIDAD: SEGURIDAD EN REDES

INTRODUCCION

La seguridad informática es un tema que ha tomado importancia en los últimos años, gracias que día a día se están globalizando cada vez más los sistemas de comunicación. En principio, la seguridad se enfoco hacia el control del acceso físico ya que para poder tener acceso a cualquier computador, se requería la presencia física de la persona frente al sistema. Más tarde, aparecen los sistemas multiusuarios, los cuales traen consigo nuevos riesgos tales como la utilización del sistema por personal no autorizado y la suplantación de usuarios. A raíz de estos problemas, aparece un esquema de seguridad basado en códigos de usuarios y contraseñas, los cuales ayudarían a restringir el acceso al sistema, y esto traería un mayor control de acceso a los recursos.

En esta unidad se comienza con una visión general de los requisitos de seguridad en red y luego se profundiza en temas específicos relacionados con los sistemas de encriptado convencional, Firewall, entre otros sistemas de protección.

El primer capitulo se fundamenta en los requisitos y amenazas de seguridad LAN. En esta parte se analizan los fundamentos de seguridad informática, exigencias como la confidencialidad, la integridad y disponibilidad de la información. También los diferentes tipos de amenazas a los que esta sometida una red que se conecta a Internet.

En el segundo capitulo se analiza los diferentes sistemas de encriptación de datos, los sistemas simétricos, asimétricos y las ventajas y desventajas que implica la utilización de cada sistema. Además se estudian los diferentes algoritmos de encriptación de datos y su implementación en los diferentes protocolos de seguridad.

El tercer capitulo profundiza en temáticas de seguridad en redes, como son las firmas y los certificados digitales, la manera como estos sistemas garantizan a los usuarios seguridad en sus transacciones electrónicas en redes que están expuestas a terceras personas.

El cuarto capitulo hace referencia a los Firewall o dispositivo que funciona como cortafuego entre redes, permitiendo o denegando las transmisiones de una red a la otra. También se describen las diferentes políticas de antivirus que se deben implementar en una red y que en combinación con los sistemas de firewall el administrador de red logra garantizar la seguridad de la misma.

En el ultimo capitulo de esta unidad se complementa con tematicas relacionadas con las diferentes tecnicas esteganograficas y biométricas de mucha utilidad para

los sistemas de red y que de una u otra forma tienden a evolucionar con el avance de las tecnologías de comunicaciones y otras áreas de las ciencias.

OBJETIVOS

- Que el estudiante comprenda limportancia de conocer las técnicas de seguridad utilizadas en las redes para proteger la información de los usuarios de la LAN.

- Que el estudiante conozca las características de los Sistemas Cortafuegos y de Antivirus como métodos para proteger la red de Amenazas

- Reconocer la importancia que tienen las politicas de seguridad al interior de las organizaciones.

- Que el estudiante adquiera habilidad en el diseño de soluciones de seguridad en las redes de área local.

- Conocer y aplicar en la LAN los estándares internacionales de seguridad.

CAPITULO 1: REQUISITOS Y AMENAZAS DE SEGURIDAD

1.1 Fundamentos de seguridad informática

Los requisitos en seguridad de la información dentro de una organización han sufrido una serie de cambios en las últimas décadas. Antes de que se extendiera la utilización de los equipos de procesamiento de datos, la seguridad de la información, que era de valor para una institución se conseguía fundamentalmente por medios físicos y administrativos. Como ejemplo del primer medio está el uso de cajas fuertes con combinación de apertura para almacenar documentos confidenciales. Un ejemplo del segundo tipo es el empleo de procedimientos de investigación de personas durante la fase de contratación.

Con la introducción de los computadores, fue evidente la necesidad de herramientas automáticas para proteger los ficheros y otras informaciones almacenadas en su memoria. Éste es especialmente el caso de los sistemas multiusuarios, tal como son los sistemas a los que se pueden acceder desde los teléfonos públicos o redes de datos. El nombre genérico del campo que trata las herramientas diseñadas para proteger los datos y frustrar a los piratas informáticos es seguridad en computadores. Aunque este es un tópico muy importante, está fuera del ámbito de este libro y será tratado muy brevemente.

Otro cambio relevante, que ha afectado la seguridad, es la inducción de los sistemas distribuidos y la utilización de redes y facilidades de comunicación para transportar datos entre terminales de usuario y computadores y de computador a computador. Las medidas de seguridad en redes son necesarias para proteger los datos su transmisión y garantizar que los datos transmitidos son auténticos.

Virtualmente la tecnología esencial subyacente en todas las redes automáticas y en las aplicaciones de seguridad en computadores es el encriptado. Existen dos técnicas fundamentales en uso: encriptado convencional, también conocido como encriptado simétrico, y el encriptado con clave pública, también conocido como encriptado asimétrico, estos tipos de encriptación se analizaran en el capitulo 2 de esta unidad.

1.2 Confidencialidad, Integridad y disponibilidad de la información

La seguridad en computadores y en redes implica tres exigencias:

- **Secreto:** Requiere que la información computador sea accesible para lectura sólo a los entes autorizados. Este tipo de acceso incluye imprimir, mostrar en pantalla y otras formas de revelación que incluye cualquier método de dar a conocer la existencia de un objeto.

- **Integridad:** Requiere que los recursos de un computador sean modificados solamente por entes autorizados. La modificación incluye escribir, cambiar de estado, suprimir y crear.

- **Disponibilidad**: Requiere que los recursos de un computador estén disponibles a los entes autorizados.

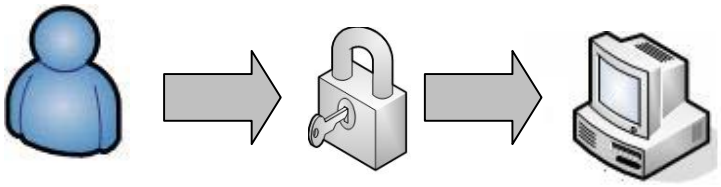


Figura 1.1. Seguridad en Redes de computadores

1.3 Amenazas de Seguridad

La mayoría de las empresas tienen sus LAN conectadas a redes Externas como el Internet, esto implica que la red este permanentemente sometida a una serie de agresiones. A continuación se analizan las categorías de agresiones más comunes:

- **Interrupciones:** Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente. Por ejemplo, destruir un disco duro, cortar una línea de comunicación o deshabilitar un sistema de consulta.

- **Intercepción**: Este es un ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podría ser una persona, un programa o una computadora. Ejemplos de este tipo de ataques son interceptar una línea para obtener información y copiar ilegalmente archivos o programas que circulen por la red, o bien la lectura de las cabeceras de mensajes para descubrir la identidad de uno o más de los usuarios involucrados en una comunicación que es interpretada ilegalmente.

- **Modificación**: Este es un ataque de una entidad no autorizada que consigue acceder a un recurso y es capaz de modificarlo. Ejemplo de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- **Fabricación:** Este es un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema. Ejemplo de este ataque son insertar mensajes no deseados en una red o añadir registro a un archivo.

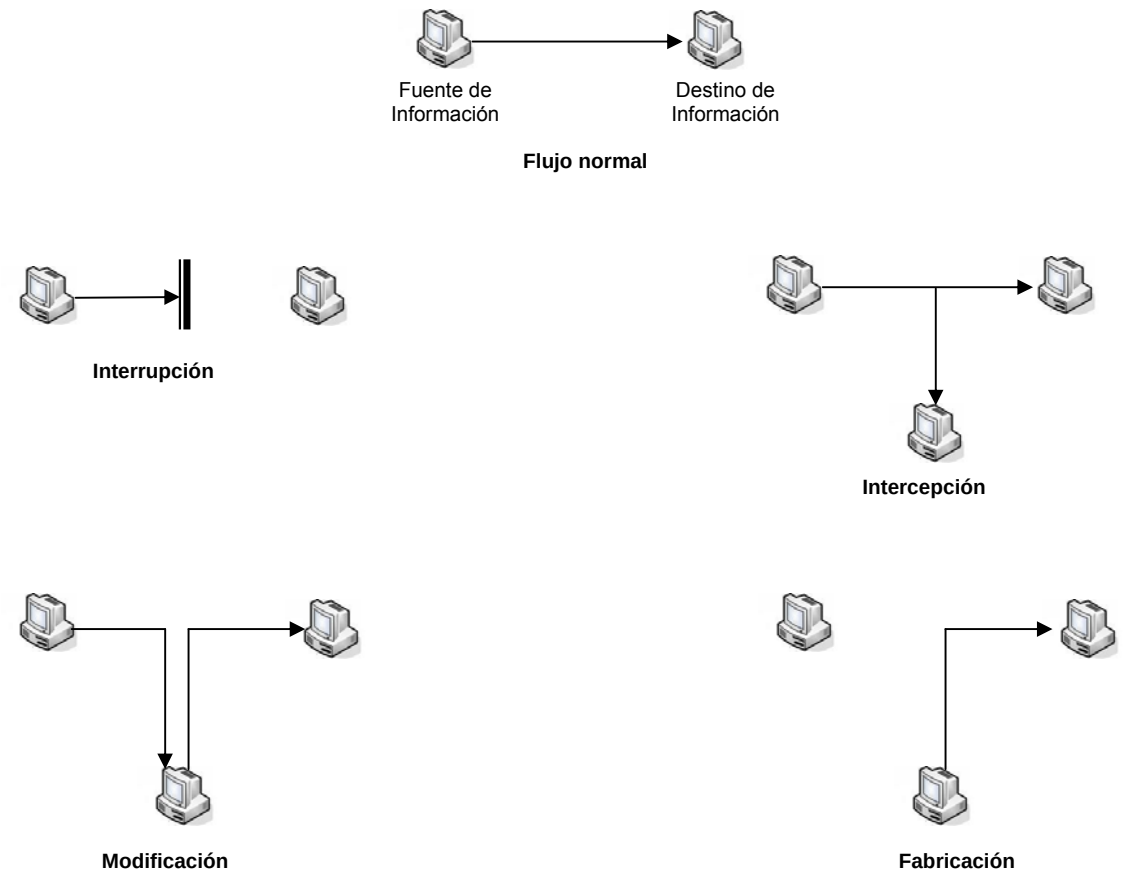


Figura 1.2. Agresión a la Seguridad

Las amenazas pueden clasificarse como pasivas y activas

- Amenazas pasivas
- Amenazas activas

1.4 Ataques pasivos

En este tipo de amenazas el ataque no altera la comunicación, sino que únicamente la observa, con el fin de obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención de origen y destinatario de la comunicación, leyendo las cabeceras de los mensajes interceptados.

- Control del volumen de tráfico intercambiado entre las entidades interceptadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información de los períodos de actividad.

Estas amenazas son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos, sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos de seguridad de la información.

1.5 Ataques activos

Estas amenazas implican algún tipo de modificación en el proceso de transmisión de información a través de la red o la creación de un falso proceso de transmisión, pudiendo subdividirse en cuatro categorías.

- **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación puede4n ser captadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Reactuación**: uno o varios mensajes legítimos son captados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- **Modificación de mensajes:** una porción del mensaje legítimo es alterado, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa diez mil dólares en la cuenta A” podría ser modificado por “Ingresa diez mil dólares en la cuenta B”.

- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso

podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes no deseados. Entre estos ataques se encuentra los de denegación de servicios, consisten en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Internet fue diseñado para ser sencillo, pero no para ser seguro. El hecho de que no existan fronteras en Internet representa ciertos riesgos, como son:

- La apropiación indebida de datos.
- La presencia de algunos virus u otras cosas que impiden el buen funcionamiento del computador.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 1

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 1 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue las diferentes amenazas de Internet, los daños que pueden ocasionar y las técnicas para contrarrestarlas.

4. Estudie los fundamentos de la seguridad informática y elabore un ensayo referente a estas temáticas.

CAPITULO 2: ENCRIPTACION DE DATOS

2.1 Introducción a la teoría de la información

Figura 2.1 Sistema de comunicación

Teoría de la información es una rama de la teoría matemática de la probabilidad y la estadística que estudia la información y todo lo relacionado con ella: canales, compresión de datos, criptografía y temas relacionados.

Fue iniciada por Claude E. Shannon a través de un artículo publicado en el Bell System Technical Journal en 1948, titulado Una teoría matemática de la comunicación (texto completo en inglés).

La información es tratada como magnitud física y para caracterizar la información de una secuencia de símbolos se utiliza la Entropía. Se parte de la idea de que los canales no son ideales, aunque muchas veces se idealicen las no linealidades, para estudiar diversos métodos para enviar información o la cantidad de información útil que se puede enviar a través de un canal.

Compresión de datos

La compresión de datos consiste en la reducción del volumen de información tratable (procesar, transmitir o grabar). En principio, con la compresión se pretende transportar la misma información, pero empleando la menor cantidad de espacio.

El espacio que ocupa una información codificada (datos, señal digital, etc.) sin compresión es el cociente entre la frecuencia de muestreo y la resolución. Por tanto, cuantos más bits se empleen mayor será el tamaño del archivo. No

obstante, la resolución viene impuesta por el sistema digital con que se trabaja y no se puede alterar el número de bits a voluntad; por ello, se utiliza la compresión, para transmitir la misma cantidad de información que ocuparía una gran resolución en un número inferior de bits.

La compresión de datos se basa fundamentalmente en buscar repeticiones en series de datos para después almacenar solo el dato junto al número de veces que se repite. Así, por ejemplo, si en un fichero aparece una secuencia como "AAAAAA", ocupando 6 bytes se podría almacenar simplemente "6A" que ocupa solo 2 bytes, en algoritmo RLE.

En realidad, el proceso es mucho más complejo, ya que raramente se consigue encontrar patrones de repetición tan exactos (salvo en algunas imágenes). Se utilizan algoritmos de compresión:

- Por un lado, algunos buscan series largas que luego codifican en formas más breves.

- Por otro lado, algunos algoritmos, como el algoritmo de Huffman, examinan los caracteres más repetidos para luego codificar de forma más corta los que más se repiten.

- Otros, como el LZW, construyen un diccionario con los patrones encontrados, a los cuales se hace referencia de manera posterior.

A la hora de hablar de compresión hay que tener presentes dos conceptos:

- **Redundancia**: Datos que son repetitivos o previsibles

- **Entropía**: La información nueva o esencial que se define como la diferencia entre la cantidad total de datos de un mensaje y su redundancia.

La información que transmiten los datos puede ser de tres tipos:

Redundante: información repetitiva o predecible.

Irrelevante: información que no podemos apreciar y cuya eliminación por tanto no afecta al contenido del mensaje. Por ejemplo, si las frecuencias que es capaz de captar el oído humano están entre 16/20 Hz y 16.000/20.000 Hz s, serían irrelevantes aquellas frecuencias que estuvieran por debajo o por encima de estos valores.

Básica: la relevante. La que no es ni redundante ni irrelevante. La que debe ser transmitida para que se pueda reconstruir la señal.

Teniendo en cuenta estos tres tipos de información, se establecen tres tipologías de compresión de la información:

1. **Sin pérdidas reales**: es decir, transmitiendo toda la entropía del mensaje (toda la información básica e irrelevante, pero eliminando la redundante).

2. **Subjetivamente sin pérdidas**: es decir, además de eliminar la información redundante se elimina también la irrelevante.

3. **Subjetivamente con pérdidas:** se elimina cierta cantidad de información básica, por lo que el mensaje se reconstruirá con errores perceptibles pero tolerables (por ejemplo: la videoconferencia).

Diferencias entre compresión con y sin pérdida

El objetivo de la codificación es siempre reducir el tamaño de la información, intentando que esta reducción de tamaño no afecte al contenido. No obstante, la reducción de datos puede afectar o no a la calidad de la información:

• Compresión sin pérdida: los datos antes y después de comprimirlos son exactos en la compresión sin pérdida. En el caso de la compresión sin pérdida una mayor compresión solo implica más tiempo de proceso. Se utiliza principalmente en la compresión de texto.

• Un algoritmo de compresión con pérdida puede eliminar datos para reducir aún más el tamaño, con lo que se suele reducir la calidad. En la compresión con pérdida tasa de bits puede ser constante o variable. Hay que tener en cuenta que una vez realizada la compresión, no se puede obtener la señal original, aunque sí una aproximación cuya semejanza con la original dependerá del tipo de compresión. Se utiliza principalmente en la compresión de imágenes, videos y sonidos.

2.2 Introducción a la teoría de los números

La teoría de números es la rama de matemáticas puras que estudia las propiedades de los números en general y de los enteros en particular, así como diversos problemas derivados de su estudio. Contiene una cantidad considerable de problemas que podrían ser comprendidos por "no matemáticos". De forma más general, este campo estudia los problemas que surgen con el estudio de los enteros.

La teoría de números ocupa entre las disciplinas matemáticas una posición idealizada análoga a aquella que ocupan las matemáticas mismas entre las otras ciencias.

Según los métodos empleados y las preguntas que se intentan contestar, la teoría de números se subdivide en diversas ramas.

Teoría elemental de números

En la teoría elemental de números, se estudian los números enteros sin emplear técnicas procedentes de otros campos de las matemáticas. Pertenecen a la teoría elemental de números las cuestiones de divisibilidad, el algoritmo de Euclides para calcular el máximo común divisor, la factorización de los enteros como producto de números primos, la búsqueda de los números perfectos y las congruencias. Son enunciados típicos el pequeño teorema de Fermat y el teorema de Euler que lo extiende, el teorema chino del resto y la ley de reciprocidad cuadrática. En esta rama se investigan las propiedades de las funciones multiplicativas como la función de Möbius y la función φ de Euler; así como las sucesiones de números enteros como los factoriales y los números de Fibonacci.

Diversos cuestionamientos dentro de la teoría elemental de números parecen simples, pero requieren consideraciones muy profundas y nuevas aproximaciones, incluyendo las siguientes:

• Conjetura de Goldbach sobre si todos los números pares (a partir de 4) son la suma de dos números primos.

• Conjetura de los números primos gemelos sobre la infinitud de los llamados números primos gemelos

• Último teorema de Fermat (demostrado en 1995)

• Hipótesis de Riemann sobre la distribución de los ceros de la función zeta de Riemann, íntimamente conectada con el problema de la distribución de los números primos.

Teoría analítica de números

La teoría analítica de números emplea como herramientas el cálculo y el análisis complejo para abordar preguntas acerca de los números enteros. Algunos ejemplos de esta son el teorema de los números primos y la hipótesis de Riemann. El problema de Waring, la conjetura de los números primos gemelos y la conjetura de Goldbach también están siendo atacados a través de métodos analíticos.

Teoría algebráica de números

La teoría algebráica de números es una rama de la teoría de los números en la cual el concepto de número se expande a los números algebraicos, los cuales son las raíces de los polinomios con coeficientes racionales.

Teoría geométrica de números

La teoría geométrica de números (tradicionalmente llamada geometría de números) incorpora todas las formas de geometría. Comienza con el teorema de Minkowski acerca de los puntos comunes en conjuntos convexos e investigaciones sobre superficies esféricas.

Teoría combinatoria de números

La teoría combinatoria de números trata los problemas de la teoría de números involucrando ideas combinatorias y sus formulaciones o soluciones. Paul Erdős es el creador de esta rama de la teoría de números. Los temas típicos incluyen sistemas cubiertos, problemas de suma cero, diversos conjuntos restringidos y progresiones aritméticas en un conjunto de enteros. Los métodos algebráicos o analíticos son bastante poderosos en este campo.

Teoría computacional de números

La teoría computacional de números estudia los algoritmos relevantes de la teoría de números. Los algoritmos rápidos para evaluar números primos y factorización de enteros tienen importantes aplicaciones en criptografía.

2.3 Introducción a los criptosistemas clásicos y Modernos

La palabra criptografía proviene del griego Kryptos que significa esconder y gráphein que significa escribir, es decir, significa escritura escondida.

El tradicional y más simple significado al que nos refiere la palabra criptografía, es el de mantener en secreto alguna información. La criptografía es una llave en sistemas de seguridad.

La Criptografía es el estudio de las técnicas matemáticas relacionadas con aspectos de seguridad de la información, tales como confidencialidad, integridad de datos, autentificación y no rechazo. Actualmente tiene el significado de ciencia de la comunicación segura, y su objetivo es que dos partes puedan intercambiar información sin que una tercera parte no autorizada, a pesar de que capte los datos, sea capaz de descifrar la información.

La criptografía se divide en dos tipos de sistemas que son los criptosistemas clásicos y los criptosistemas modernos.

- **Los criptosistemas clásicos:** son aquellos que existieron desde siempre y son métodos desarrollados para cifrar mensajes escritos a mano o en máquinas de impresión. Los criptosistemas clásicos se basan en la sustitución de letras por otras y en la transposición, que juegan con la alteración del orden lógico de los caracteres del mensaje. Así, a los criptosistemas clásicos le han salido dos formas de cifrado, que son: Por Sustitución y Por Transposición.

- **Los criptosistemas modernos**: son más complejos de elaborar y un buen ejemplo de ello además de los ordenadores son las tarjetas de acceso electrónicas, capaces de trabajar con estas encriptaciones por la elevada velocidad de computación que presentan. Al estar basados en complejas transformaciones matemáticas de una secuencia, es indispensable disponer de memoria volátil y capacidad de procesamiento. Estos sistemas de cifrado modernos son capaces de cifrar palabras de más de 128 bits y normalmente se cifran en bloques.

La principal diferencia de los sistemas criptográficos modernos respecto a los clásicos está en que su seguridad no se basa en el secreto del sistema, sino en la robustez de sus operadores (algoritmos empleados) y sus protocolos (forma de usar los operadores), siendo el único secreto la clave (los operadores y protocolos son públicos). Los criptosistemas modernos más importantes se dividen en tres grupos:

- Sistemas de clave secreta (simétricos.)

- Sistemas de clave publica (asimétricos).

- Sistemas de cifrado de logaritmos.

2.3.1 Criptosistemas de Clave Secreta

Método criptográfico que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y este lo descifra con la misma. Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo.

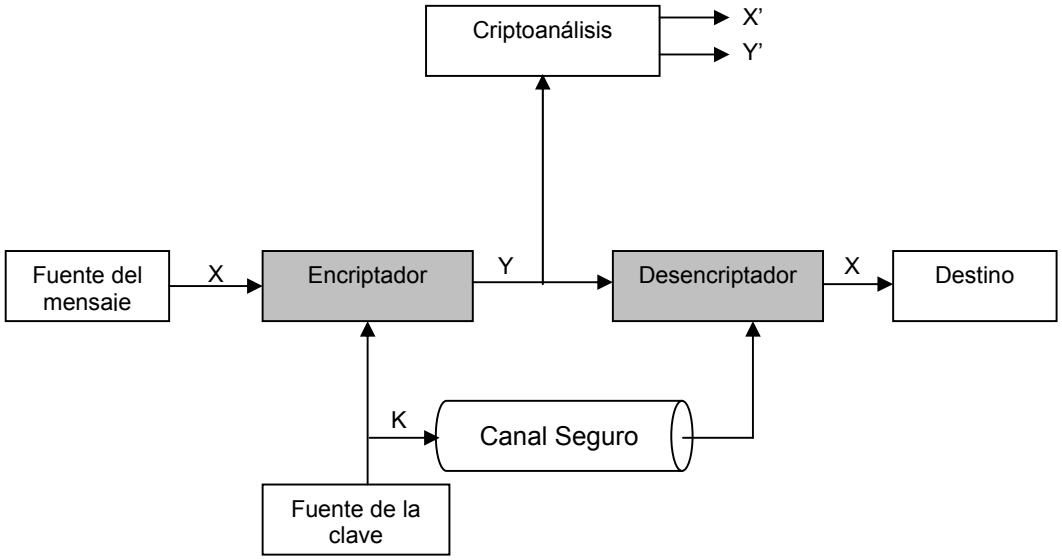


Figura 2.2. Criptosistema clave secreta.

Dado que toda la seguridad esta en la clave es importante que sea muy difícil de adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea el espacio de posibilidades de claves, debe ser amplio.

Hoy por hoy los ordenadores pueden adivinar claves con extrema rapidez, y esta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevados a 56 claves posibles. 2 elevados a 56 son 72.057.594.037.927.936 claves. Esto representa un numero muy alto de claves, pero una maquina computadora de uso general puede comprobar todo el espacio posible de claves en cuestión de días. Una maquina especializada lo puede hacer en horas. Por otra parte, algoritmos de cifrado de diseño mas reciente como: DES, 3DES, Blowfish, IDEA, RC2, RC4,Skipjack. Todos estos usan claves de 128 bits, lo que significa que existen dos elevados a 128 claves posibles. Esto representa muchas, muchísimas mas claves y aun en el caso de que todas las maquinas del planeta estuvieran cooperando, todavía tardarían mas tiempo que la misma edad del universo en encontrar la clave.

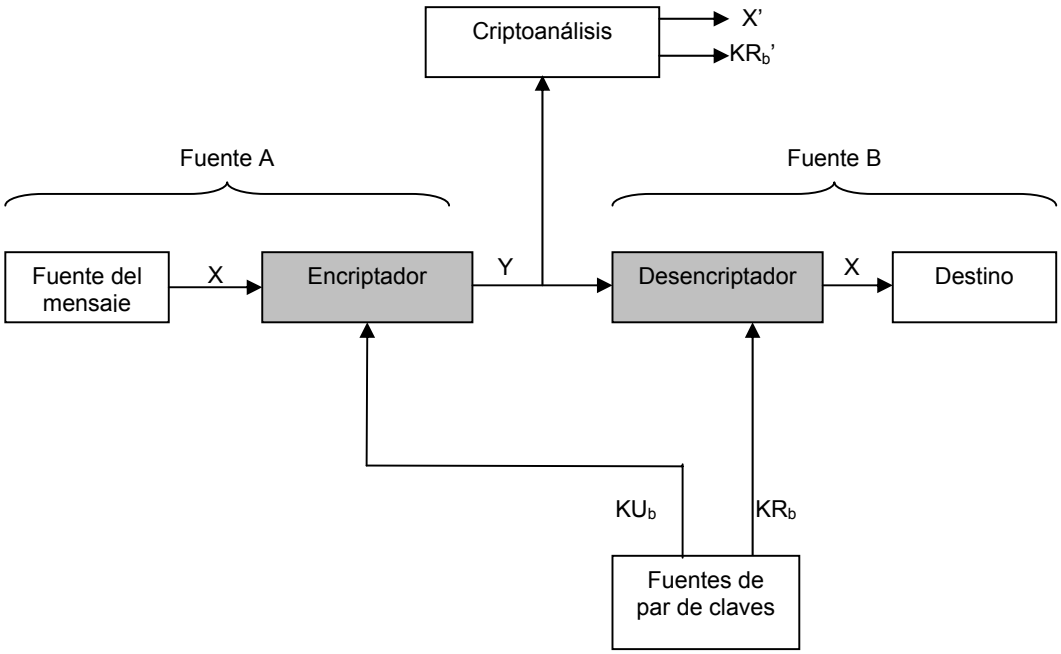
Inconvenientes

El principal problema con los sistemas de cifrado simétrico no esta ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarla para comunicarse con seguridad.

Ventajas de las claves simétricas

Son sencillas. Los ordenadores las manejan fácil y rápidamente. Hay claves simétricas muy sofisticadas y seguras.

2.3.2 Criptosistemas de Clave Pública



.

Figura 2.3 Criptosistema de clave Pública

La criptografía asimétrica utiliza dos claves complementarias llamada clave privada y clave publica. Lo que esta codificado con una clave privad necesita su correspondiente clave publica para ser descodificado y viceversa, lo codificado con una clave publica solo puede ser descodificado con su clave privada.

Las claves privadas deben ser conocidas únicamente por su propietario, mientras que la correspondiente clave pública puede ser dada a conocer abiertamente. Si ana quiere enviar a benito un mensaje de forma que solo el pueda entenderlo, lo codificara con la clave publica de benito. Benito utilizara su clave privada, que solo el tiene, para poder leerlo. Pero otra posible utilidad del sistema es garantizar la identidad del remitente. Si A envía a B un mensaje codificado con la clave privada de A, B necesitara la clave pública de A para descifrarlo.

La criptografía asimétrica esta basada en la utilización de números primos muy grandes. Si multiplicamos entre si dos números primos muy grandes, el resultado obtenido no puede descomponerse eficazmente, es decir, utilizando los métodos aritméticos mas avanzados en los ordenadores mas avanzados, seria necesario utilizar durante miles de millones de años tantos ordenadores como átomos que existen en le universo. El proceso será mas seguro cuanto mayor sea el tamaño de los números primos utilizados. Los protocolos modernos de encriptación tales como SET y PGP utilizan claves generadas con números primos de un tamaño tal que los hace completamente inexpugnables.

El problema de las claves asimétricas es que cuando el texto a tratar es largo el proceso de codificación es muy lento. Los protocolos modernos codifican el texto base con una clave simétrica tipo DES o IDEA y utilizan las claves asimétricas para la comunicación de la simétrica usada. Cuando un texto se codifica con la clave simétrica y se envía esta clave codificada con la publica del recepto, el resultado se llama “sobre digital”

Seguridad de la criptografía asimétrica

Como con los sistemas de cifrado simétricos buenos, con un buen sistema cifrado de clave publica toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de seguridad del sistema, pero no se puede comparar el tamaño de cifrado simétrico con el de cifrado de la clave publica para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe prob0r hasta 2^{81}-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con una clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales).

Desventajas respecto a las cifras simétricas

- La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de procesos.

- Las claves deben ser de mayor tamaño que la simétrica.

- El mensaje cifrado ocupa mas espacio que el original.

2.3.3 Funciones de Autenticación e Integridad

La función **hash** es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente, funciona en una sola dirección, es decir, no es posible a partir del valor resumen calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades para el usuario, para ello se usan software que automatizan tanto la función de calcular el valor hash como su verificación posterior.

2.4 Algoritmos de encriptación

DES

Es un algoritmo desarrollado originalmente por IBM a requerimiento del NBS (nacional Buread Of. Standard, en la actualidad denominado NET, nacional Instituta Of. Standard ana tecnología) de EE.UU. y posteriormente modificado y adoptado por el gobierno de EE.UU en 1977 como estándar descifrado de todas las informaciones sensibles no calificadas. Es el más estudiado y utilizado de los algoritmos de clave simétrica o de cualquier otro tipo. Posteriormente, en 1980, el NIST estandarizo los diferentes modos de operación del algoritmo.

Tras las modificaciones introducidas por el NBS, consistentes básicamente en la reducción de la longitud de claves y bloques, DES cifra bloques de 64 bits cada vez, produciendo así 64 bits cifrados.

Los modos de operación de DES

Existen 4 modos de operación definidos para DES (los cuales han sido generalizados para cualquier cifrado de bloques). Estos modos fueron estandarizados en 1980 por NIST. Se trata de los siguientes:

ECB (Electrónica Codebook): Cifra cada bloque de 64 bits del mensaje en claro uno tras otro con la misma clave de 56 bits. Un par de bloques idénticos de mensajes en claro producen bloques idénticos de mensajes cifrados.

CBS (Cipher Block Chainning**):** Sobre cada bloque de 64 bits del mensaje en claro se ejecuta un OR exclusivo con el bloque previo del mensaje cifrado antes de proceder al cifrado con la clave DES. De este modo el cifrado de cada bloque depende del anterior y bloques idénticos de mensajes en claro producen diferentes mensajes cifrados.

CFB (Cipher Fedback): El cifrado de un bloque de mensajes en claro procede de ejecutar un OR exclusivo del bloque de mensaje en claro con el bloque previo cifrado. CFB puede modificarse para trabajar con bloques de longitud inferior a 64 bits.

OFB (Output Feedback): Similar al modo CFB excepto en que los datos sobre los que se ejecutan el OR exclusivo junto con los bloques de mensajes en claro es generada independientemente del mensaje en claro y del mensaje cifrado.

Seguridad de DES

DES puede ser atacado mediante la fuerza bruta, probando toda las claves posible 2^{56}, siendo este algoritmo de una complejidad O (2^{55}). A pesar de los rumores que aseguraban que el NBS modifico el algoritmo para hacerlo mas débil, a un no ha sido roto públicamente mas que por la fuerza bruta. Aunque ha habido diferentes análisis que han demostrado que pueden disminuirse la complejidad del problema hasta 2^{43}, han resultado de implementación poco practica.

TRIPLE-DES (3DES)

Una mejora del algoritmo DES, que siempre había sido muy criticado debido a la pequeña longitud de la clave, es triple DES. Con este procedimiento, el mensaje es cifrado 3 veces. Existen varis implementaciones:

DES-EEE3. Se cifra cada tres veces con una clave diferente cada vez.

DES-EDE3. Primero se cifra, luego se descifra y por ultimo se vuelve a cifrar, cada vez con una clave diferente,

DES-EEE2 Y DES-EDE2. Similares a los anteriores con la salvedad de que la clave usada en el primer y en el último caso coinciden.

Se estima que las dos primeras implementaciones con claves diferentes, son las más seguras. Si se quiere romper el algoritmo utilizando la fuerza bruta, la complejidad asciende a O (2^{112}).

IDEA (Internacional data encryption algorithm)

IDEA opera con bloques de 64 bits usando una clave de 128 bits y consiste en 8 transformaciones idénticas y una transformación de salida (media ronda).El proceso para encriptar y descencriptar es similar.

IDEA utiliza tres operaciones en su proceso con las cuales logra la confusión, se realizan con grupos de 16 bits y son:

Suma modulo 2^{16} cuadrado con un mas.
Multiplicación modulo 2^{16} +1 (circulo con punto)
Operación O exclusiva (XOR) (circulo con un +).

Seguridad

Los diseñadores analizaron IDEA para medir sus fortalezas frente al criptoanálisis diferencial y concluyeron que lo es bajo ciertos supuestos. No se han reportado debilidades frente al criptoanálisis lineal o algebraico. Se han encontrado algunas claves débiles las cuales en la práctica son poco usadas siendo necesaria evitarlas explícitamente.

AES (**Advanced Encription Standard**)

(Estándar de cifrado Avanzado). También conocido como Rijndael.

Al contrario que las convocatorias DES, dos décadas a tras, AES ha sido un concurso abierto a cualquier participante mundial que cumpliese con una serie de requisitos, como velocidad tanto en Software como en Hardware, reducidas ocupación de memoria, implementación eficiente tanto en procesadores modernos como en CPU de 8 bits (utilizadas, por ejemplo en tarjetas inteligentes), etc.,. El ganador debe por otra parte, liberar cualquier tipo de patente en el algoritmo, para potenciar así el desarrollo de soluciones tecnológicas de buena calidad.

Descripción.

A diferencia del DES, el AES es una red de sustitución y permutación, y no una red tipo Feister. AES es rápido en Hardware y Software, es relativamente fácil de implementar, y requiere de poca memoria. Al ser un estándar se esta desplegando a gran escala.

Estrictamente hablando AES no es precisamente RIJNDAEL, este último soporta un gran rango de tamaño para claves y bloques, mientras AES tiene un tamaño fijo de 128 bits y una clave de tamaño 128, 192 o 256 bits. Mientras que RIJNDAEL, puede ser especificado en bloque y claves de tamaños múltiplos de 32 bits, con un mínimo de 128 y un máximo de 256 bits.

RSA

El sistema criptográfico con clave pública RSA es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma

autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes.

Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado.

Emplea expresiones exponenciales en aritmética modular.

La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

La computación cuántica podría proveer una solución a este problema de factorización.

Cifrado ElGamal

El algoritmo ElGamal es un algoritmo para criptografía asimétrica el cual está basado en Diffie-Hellman. Fue descrito por Taher Elgamal en 1984.

La seguridad del algoritmo depende en la dificultad de calcular logaritmos discretos.

ElGamal consta de tres componentes : el generador de claves, el algoritmo de cifrado, y el algoritmo de descifrado.

El algoritmo ElGamal fue ideado en un principio para producir firmas digitales, aunque después se extendió su uso para utilizarlo en el cifrado de mensajes.

Para generar un par de llaves, se escoge un número primo n y dos números aleatorios p y x menores que n.

Se calcula entonces:

$$y = p^x mod n$$

La llave publica es (p, y, n), mientras que la llave privada es x. Escogiendo n primo, garantizamos que sea cual sea el valor de p, el conjunto {p, p2, p3 . . .} es una permutación del conjunto {1, 2,..., n − 1}.

> Nótese que esto no es necesario para que el algoritmo funcione, por lo que podemos emplear realmente un n no primo, siempre que el conjunto generado por las potencias de p sea lo suficientemente grande.

2.5 Protocolos de seguridad

Se discuten SSH, SSL, TSL y HTTPS, los protocolos utilizados en la actualidad para intercambiar información de manera de hacer difícil que esta sea interceptada por terceros. Contar con protocolos seguros es importante tanto por las preocupaciones relacionadas con la privacidad como para permitir el comercio electrónico.

Seguridad en la Web

Dado el gran auge que hoy en día tiene Internet, su uso se ha masificado enormemente. Desde páginas meramente informativas hasta sitios interactivos usando tecnologías nuevas.

Empresas de diversa índole ya usan la Internet para comunicarse y el problema principal que surgió es la confiabilidad en que lo que se esta comunicando no sea visto por personas que puedan hacer mal uso de dicha información.

Por ejemplo, las tiendas comerciales ya están dando la posibilidad de realizar compras por la Web, pero el principal talón de Aquiles lo constituye la inseguridad que causa dar un número de tarjeta de crédito para pagar la compra.

O cosas tan simples como cuando uno envía un mail y no querer que nadie lo lea sino el destinatario.

A raíz de todo esto surgieron tecnologías que persiguen mejorar la seguridad de todas estas comunicaciones.

Seguridad en la transmisión

La seguridad de este tipo se basa en el hecho de poder encriptar los mensajes que se envían por a red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos.

Para llevar a cabo esta seguridad se crearon diversos protocolos basados en esta idea:

- **SSH:** Usado exclusivamente en reemplazo de telnet
- **SSL:** Usado principalmente en comunicaciones de hipertexto pero con posibilidad de uso en otros protocolos
- **TSL:** Es del mismo estilo del anterior.
- **HTTPS**: Usado exclusivamente para comunicaciones de hipertexto

SSH (Secure Shell)

Este protocolo fue diseñado para dar seguridad al acceso a computadores en forma remota.

Cumple la misma función que telnet o rlogin pero además, usando criptografía, logra seguridad con los datos.

A diferencia de telnet u otro servicio similar, SSH utiliza el puerto 22 para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el sshd.

El cliente debe ser un software tipo TeraTerm o Putty que permita la hacer pedidos a este puerto 22 de forma cifrada.

La forma en que se entabla una comunicación es en base la misma para todos los protocolos seguros:

- El cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido y le envía la llave publica al cliente para que pueda descifrar los mensajes.
- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

Se recomienda que si se esta en un computador propio, la clave sea guardada, en otro caso, destruirla.

SSL (Secure Socket Layer) y TLS(Transport Layer Secure)

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL es una capa por debajo de HTTP y tal como lo indica su nombre esta a nivel de socket por lo que permite ser usado no tan solo para proteger documentos de hipertexto sino también servicios como FTP, SMTP, TELNET entre otros.

La idea que persigue SSL es encriptar la comunicación entre servidor y cliente mediante el uso de llaves y algoritmos de encriptación.

El protocolo TLS esta basado en SSL y son similares en el modo de operar.

Es importante señalar que ambos protocolos se ejecutan sobre una capa de transporte definida, pero no determinada. Esto indica que pueden ser utiizados para cualquier tipo de comunicaciones. La capa de transporte más usada es TCP cobre la cual pueden implementar seguridad en HTTP.

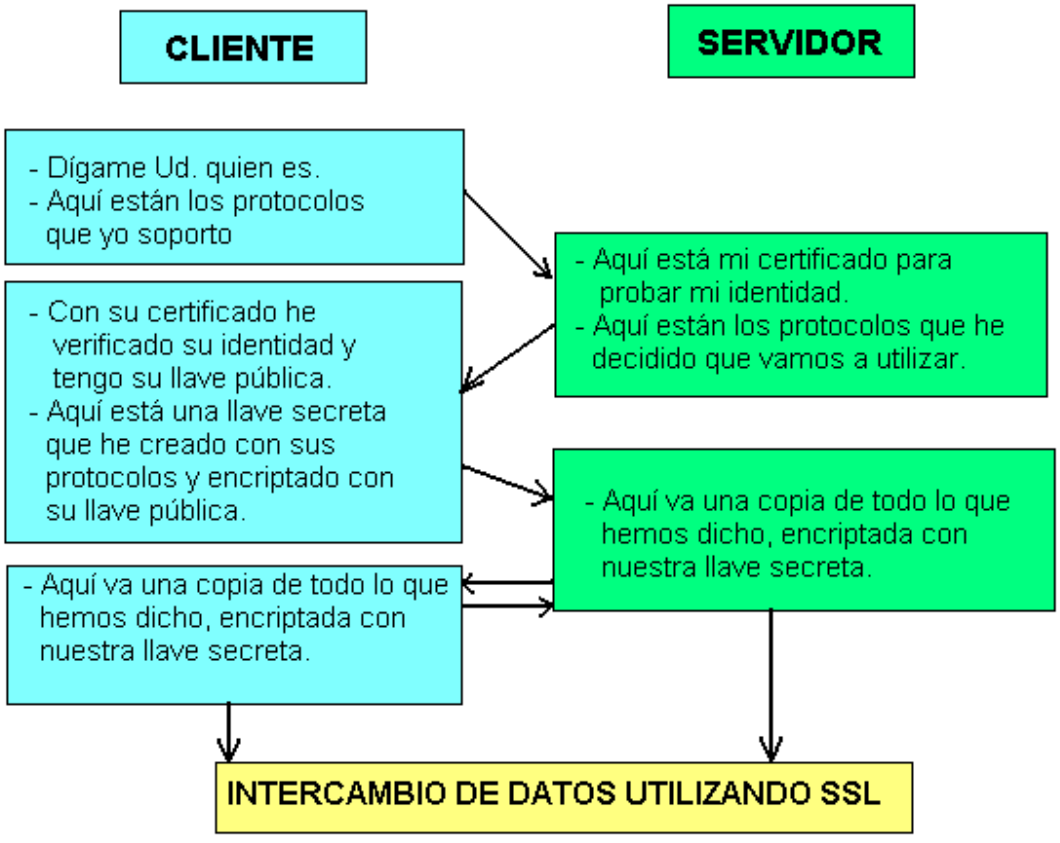


Figura 2.4 Intercambio de datos utilizando SSL

Como punto de diferencia se puede mencionar que existen protocolos implementados sobre la capa de red, por ejemplo sobre IP. Tal es el caso de IPSec.

¿De que están compuestos?

Estos protocolos se componen de dos capas: el Record Protocol y el Handshake Protocol.

El Record Protocol es la capa inmediatamente superior a TCP y proporciona una comunicación segura. Principalmente esta capa toma los mensajes y los codifica con algoritmos de encriptación de llave simétrica como DES, RC4 aplicándole una MAC (Message Authentication Code) para verificar la integridad, logrando así encapsular la seguridad para niveles superiores.

El Handshake protocol es la capa superior a la anterior y es usada para gestionar la conexión inicial.

PGP

Pretty Good Privacy o PGP (privacidad base buena) es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información protegida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

Seguridad en PGP

Utilizando correctamente, PGP puede proporcionar un gran nivel de seguridad. es más, observadores informados creen que ni siquiera las agencias del gobierno estadounidense como la NSA son capaces de descifrar directamente mensajes generados adecuadamente con PGP.

PGP es más fácil de utilizar que muchos otros criptosistemas, pero como ocurre casi siempre en el campo de la criptografía, su implementación y su utilización influyen muchísimo en la seguridad lograda. Existe la posibilidad de que haya errores en la implementación, y si se utiliza descuidadamente es posible desproteger fácilmente un archivo de texto protegido. Cualquier criptosisitema puede ser inseguro, independientemente de lo bueno que sea su diseño.

A diferencia de los protocolos de seguridad como SSL, que solo protege los datos en tránsito (es decir, mientras se transmiten a través de la red), PGP también puede utilizarse para proteger datos almacenados discos, copias de seguridad, etc.

SET

El SET (transacción electrónica segura) es un protocolo estándar para proporcionar seguridad a una transacción con tarjeta de crédito en redes de computadoras inseguras, en especial Internet.

SET surge de la solicitud de estándar por VISA y MasterCard en febrero de 1996 y la especificación inicial involucró a un amplio rango de compañías, tales como GTE,IBM, Microsoft, Netscape, RSA y VeriSing

SET utiliza técnicas criptográficas tales como certificados digitales y criptografía de clave pública para permitir a las entidades llevar a cabo una autenticación entre sí y demás intercambiar información de manera segura.

SET fue muy publicado en la década de 1990 como el estándar de facto para el uso de tarjetas de crédito. Sin embargo, no logró el éxito anunciado, debido a la necesidad de instalar software cliente (por ejemplo, una ewallet), y el costo y la complejidad de los vendedores para ofrecer soporte. Por otro lado las alternativas que utilizan SSL presentan un bajo costo y simplicidad en su implementación.

Está basado en la criptografía más segura, la criptografía de llaves públicas y privadas RSA, SET agrupa a las siguientes entidades en un solo sistema de pago:

Para poder hacer transacción SET cada uno de los participantes debe estar registrado por una entidad certificadora, que como su nombre lo indica emite un certificado electrónico en el que hace constar la identidad de una entidad.

SET pretende masificar el uso de Internet como “el mayor centro comercial del mundo”, pero para hacerlo SET fue diseñado para lograr:

- Confiabilidad de la información
- Integridad de los datos
- Autenticación de la cuenta del tarjeta habiente
- Autenticación del comerciante
- Interoperabilidad

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 2

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 2 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue Cual es el protocolo mas utilizado por las empresas que Comercializan artículos en Internet y porque.

4. Elabore un ensayo referente al uso de los algoritmos y protocolos de seguridad en las transacciones electrónicas.

CAPITULO 3: FIRMAS Y CERTIFICADOS DIGITALES

3.1 Firma Digital

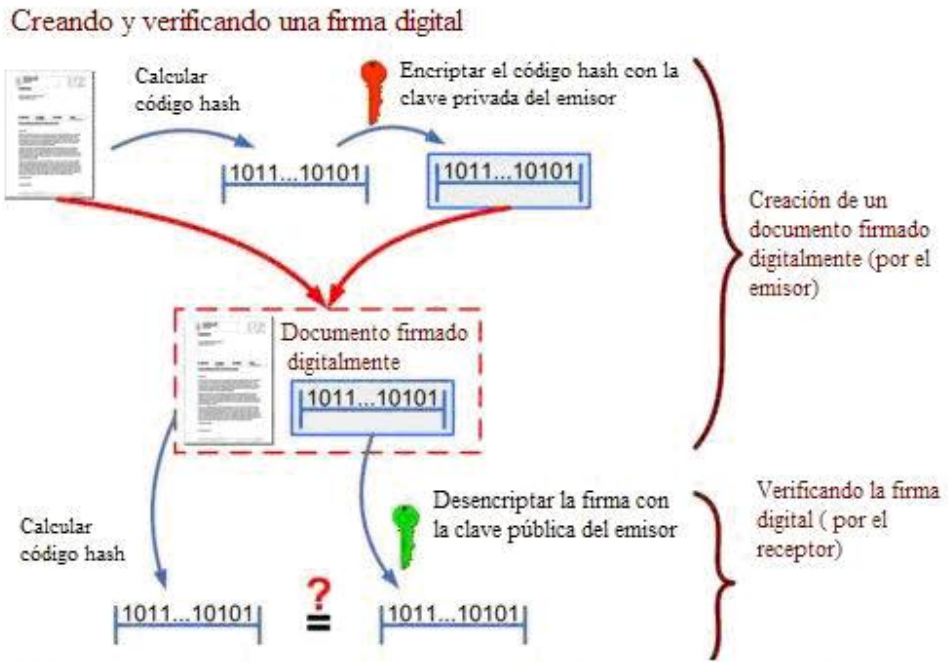


Figura 3.1 Firma Digital

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

Una firma digital utiliza el mismo funcionamiento del "public key" o algoritmo asimétrico mencionado anteriormente.

Como se mencionó, existe una "llave pública" y una "llave secreta", en el caso de firmas digitales la llave pública que es ampliamente conocida es capaz de identificar si la información proviene de una fuente fidedigna.En otras palabras, la llave pública será capaz de reconocer si la información realmente proviene de la "llave secreta" en cuestión.

3.1.1 Tipos de firmas digitales

El método más usado actualmente para firmas digitales es el conocido como RSA, este método es conveniente usarlo para poder ser compatible. Para que seas seguro la longitud de sus claves (una pública y otra privada) debe ser de 1024 bits, es decir un número de poco más de 300 dígitos.

Otro método reconocido para firma digital es el DSA, que es oficialmente aceptado para las transacciones oficiales en el gobierno de USA. Este método usa también claves del mismo tamaño que RSA, pero esta basado en otra técnica. Aún así, es casi equivalente en seguridad a RSA.

Una tercera opción es el método que usa curva elíptica, este método tiene la ventaja a los dos anteriores a reducir hasta 164 bits, es decir como 45 dígitos las claves, manteniendo la misma seguridad. Por lo que es más propio para ser usado onde existen recursos reducidos como en Smart Cards, PDAs, etc.

Entre los posibles ataques a los anteriores métodos esta la posible remota construcción de una computadora cuántica, esta podría efectuar una cantidad tan grande de cálculos al mismo tiempo que podría romper los esquemas anteriores, incluso ya existen estos algoritmos que romperían los sistemas. Sin embargo, ya existe otro método de forma que aún con la computación cuántica no existe aún algoritmo que pueda romperlos. Este sistema es que esta basado en lattices (retículas), se conoce como NTRU (number Theory Research Unit) y entre otras cualidades es más eficiente que RSA.

Existe aún más métodos para firmar, incluso algunos métodos derivados de las anteriores técnicas, sin embargo no han podido tener el impacto de las anteriores, de hecho puede crearse un método de firma para un caso particular.

3.2 certificado Digital

Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509. El certificado contiene usualmente el nombre de la entidad certificada, un número serial, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital), y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

3.2.1 Autoridades de Certificación

Cualquier individuo o institución puede generar un certificado digital pero si éste emisor no es reconocido por quienes interactuaran con el propietario del certificado, es casi igual a que si no hubiese sido firmado. Por ello los emisores deben acreditarse para así ser reconocidos por otras personas, comunidades, empresas o países y que su firma tenga validez.

La gran mayoría de los emisores tiene fines comerciales, y otros, gracias al sistema de Anillo de confianza pueden otorgar gratuitamente certificados en todo el mundo, como:

CAcert.org, emisor administrado por la comunidad con base legal en Australia.
Thawte, sólo para certificados personales. Emisor propiedad de Verisign.
Pero para que un certificado digital tenga validez legal, el prestador de Servicios de Certificación debe acreditarse en cada país de acuerdo a la normativa que cada uno defina.

La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad. Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la Autoridad de Certificación utilizando su clave privada. La Autoridad de Certificación es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública.

La confianza de los usuarios en la CA es importante para el funcionamiento del servicio y justifica la filosofía de su empleo, pero no existe un procedimiento normalizado para demostrar que una CA merece dicha confianza.

3.2.2 Clases de Certificados

Certificados de Servidor.

El Certificado de Servidor aporta a un WEB SITE la característica de seguridad y confianza necesaria para poder entablar cualquier tipo de relación con los potenciales usuarios. Es el elemento necesario para poder aprovechar la gran vía de negocio que supone el comercio a través de Internet con la máxima rentabilidad y seguridad.

Los Certificados de Servidor permiten incorporar el protocolo SSL (Secure Socket Layer) en un servidor Web. Gracias a este protocolo toda comunicación entre el cliente y el servidor permanece segura, cifrando la información que se envía a ambos puntos protegiendo los datos personales, datos de tarjetas de crédito,

números de cuenta, passwords, etc. Cobra especial importancia dentro del área del comercio electrónico, donde la seguridad de los datos es la principal barrera para el desarrollo de este sistema

Certificados para WAP

Los Certificados WAP permiten a las WEB comerciales existentes y de nueva creación la realización de transacciones seguras con los consumidores móviles. Los nuevos portales basados en transacciones móviles seguras expandirán el comercio electrónico entre los usuarios móviles y los WEB SITES dedicados al comercio.

Los servidores WAP necesitan proporcionar seguridad y confianza a los usuarios potenciales.

Esta es la base para que se establezca una contraprestación que satisfaga a ambas partes.

Los Certificados WAP permiten mantener conexiones seguras basadas en encriptación y autenticación con dispositivos de telefonía móvil.

Certificados Personales

Otorgan seguridad a los correos electrónicos basados en un standard S/MIME. Podrá Firmar o cifrar los mensajes de correo para asegurarse de que sólo el receptor designado sea el lector del respectivo mensaje.

Corporativas.

Es la solución óptima para las empresas que quieran disponer de un sistema de generación de cualquier tipo de Certificado para sus usuarios usuarios (trabajadores, proveedores, clientes, etc.) y servidores.

Una CA Corporativa puede generar cualquier tipo de certificado, ya sean Certificados Personales, de Servidor, para WAP, para firmar Código e incluso para IPSec-VPN.

En función del tipo de funcionalidad que se le quiera dar a la CA se deberá escogerse un diferente tipo de CA Corporativa.

Certificados para firmar Código

El Certificado para la Firma de Código, permitirá a un Administrador, Desarrollador o Empresa de Software firmar su Software (ActiveX, Applets Java, Plug-ins, etc.) y Macros, y distribuirlo de una forma segura entre sus clientes.

Certificados para IPSec-VPN

Los Certificados para VPN son los elementos necesarios para que la empresa aproveche las cualidades y ventajas de la utilización de las VPNs de un modo plenamente seguro.

Las VPNs surgen como consecuencia de la creciente demanda de Seguridad en las comunicaciones ya sea entre Router-Router o Cliente-Servidor. La apertura de las redes corporativas a empleados remotos (con gran importancia en el caso del Teletrabajo), sucursales, business partners o clientes

3.2.3 Certificados X.509

Este es el estándar de certificado que actualmente se maneja internacionalmente. Tiene unos componentes básicos:

public Key
Suject identity
Certification authority's signatura.

Son muy utilizados en contextos como: S/MIME, IPSec,SSL/TLS, SET, etc. Y se recomienda el uso de RSA.

Cuando el certificado es para un e-mail contiene además el e-mail del sujeto.

En el ambiente financiero: se necesita extender el certificado para codificar información acerca del credt card holder, como ser su número de tarjeta de crédito y límite de crédito.
La Internacional Telecomunicación union-telecomunication Standarization Sector (ITUT) y ISO/Internacional Electrochical Comisión (IEC), a dispuesto varios tipos de certificado:

- V1 - 1998 X.500 recomendations para servicios de directorio (BDde usuario).
- V2 – 1993 campos para soportar directory access control.
- V3 -1996 extentions fields

Un certificado X.509 contiene un conjunto de campos predefinidos y cero o más campos de extensión.A continuación se explica cada campo:

Versión: contiene la versión del certificado. Los valores legales son 1,2 y 3.

Certificante serial number: es un entero asignado por la CA. Cada certificado emitido por la CA debe ser único número de serie.

Signatura algorithm identifier: identifica el algoritmo (RSA o DSA) usado por el CA para crear la firma digital del certificado.

Issuer name: identifica al CA que firmó y emitió el certificado (en forma X.500)

Valid period: es el tiempo de validez del certificado, y el CA está obligado a mantener información acerca del estatus del sujeto. Consiste en una fecha de inicio, fecha cuando el certificado se vuelve válido, y fecha en que deja de ser válido.

Suject name: identifica la identidad del dueño del la clave pública que está en el public key information key.

Subject public key information: Contiene la clave pública y el identificador del algoritmo con el cual la clave es usada.

Otros campos opcionales y firma digitales (MAC) son:

Delegación de autoridad: Cada CA puede certificar y/o confirmar en otros CA, generando un árbol de confianza (trust).

Certification Revolcation List (CRL): Cada CA puede revocar certificados comprometidos, manteniendo una lista pública.

La versión 3 define 3 tipos de extensiones opcionales:

- key and Policy information
- certificate Suject and issuer Atributes
- certification Path Constraints

3.4 Aplicaciones Seguras

A la hora de considerar la seguridad, debe proteger los equipos de desarrollo de ataques de código malicioso y del daño a los datos, así como los servidores. En el entorno de desarrollo existen varios mecanismos que puede aprovechar para ayudar a proteger sus servidores de desarrollo:

Las observaciones sobre seguridad se deberían incluir en todos los aspectos de la creación de aplicaciones, desde el diseño hasta la implementación. En las secciones siguientes se proporcionan recursos en los que obtener más información sobre prácticas de codificación seguras.

Para garantizar que una aplicación funciona de manera segura, es preciso establecer directivas de seguridad como las siguientes:

- Longitud y período de validez de las contraseñas
- Auditorias y directivas de inicio de sesión
- Procesos de prevención contra intrusos
- Propiedad/responsabilidad de las cuentas de usuario
- Métodos para el cifrado de claves

Conviene diseñar directivas de seguridad para la propia aplicación de modo que se alcancen objetivos realistas a cambio de un coste razonable. Si bien las aplicaciones difieren entre sí, también comparten algunos objetivos fundamentales relacionados con el rigor en materia de seguridad, con el coste y con los métodos utilizados para obtener una aplicación segura.
Proteger los datos

Opte por tecnologías que utilicen el cifrado para proteger la privacidad de los usuarios y la integridad de los datos en toda la red. Establezca un estándar de protocolo para el sitio; ha de utilizar un estándar admitido por la comunidad de Internet, como:

- SSL (Secure Sockets Layer)
- TLS (Transport Layer Security)
- IPSec (Internet Protocol Security)

Si debe crear su propia criptografía y sus propios protocolos, procure que un experto en criptografía compruebe todo el código.

Utilizar mecanismos de control de acceso

Estos mecanismos limitan el acceso a los recursos en función de la identidad de los usuarios y de su pertenencia a varios grupos predefinidos. Se utilizan mecanismos de control de acceso para controlar el acceso de los usuarios a recursos de red como servidores, directorios y archivos.

Utilizar un enfoque de acceso mínimo

Un enfoque de acceso mínimo denota que deben bloquearse, desactivarse o quitarse los activos en línea que no requieran acceso en línea. Además, el acceso a los recursos ha de limitarse a aquellos usuarios que realmente lo necesiten.

Este enfoque tiende a reducir en gran medida situaciones como la pérdida de datos y la denegación de servicio debidas a las acciones involuntarias de usuarios que entran en áreas a las que no pertenecen. También reduce al mínimo el número de posibles puntos de entrada de fácil acceso para usuarios no autorizados. Por ejemplo, podría abrir únicamente los puertos 80 (HTTP) y 443 (HTTPS) del Protocolo de control de transmisión (TCP) para obtener acceso a los servicios Web y desactivar los demás. Entre otros ejemplos se incluyen la

deshabilitación de las cuentas de usuario invitado así como la restricción de acceso de sólo lectura a usuarios anónimos en áreas bien definidas del sitio.

Gran parte del esfuerzo debería orientarse a proteger los activos que pueden estar expuestos a alguna amenaza y a los que necesitan tener acceso los usuarios o el departamento de tecnologías de la información. Para ello, es preciso determinar la prioridad de las amenazas asignando una demanda mayor de seguridad a aquellos activos cuya pérdida pueda causar mayores daños a la organización.

Habilitar una autenticación rigurosa

Utilice esquemas de autenticación que estén integrados en los sistemas operativos de red y que utilicen protocolos estándar de Internet.

La autenticación de certificados de cliente de clave pública permite a los usuarios comunicarse con un sitio a través de Internet sin exponer contraseñas ni datos susceptibles de ser interceptados con facilidad. Si bien los certificados no proporcionan cifrado por sí solos, son fundamentales para establecer un canal de comunicación seguro.

Puede ser necesaria la compatibilidad con algunas características especiales, como la autenticación de tarjetas inteligentes o certificados de servidor con claves públicas que permiten a los usuarios autenticar los servidores como fuentes de confianza.

Fomentar el uso de contraseñas rigurosas

Si desarrolla un mecanismo de contraseñas propio, procure que los usuarios no utilicen contraseñas poco rigurosas. Las características que definen una contraseña rigurosa son que contiene al menos siete caracteres, distingue mayúsculas de minúsculas, incluye números y signos de puntuación, y no figura en ningún diccionario. Es recomendable que se admitan contraseñas largas.

Utilizar una autorización integrada en el sistema

Para controlar el acceso a los recursos, utilice estándares de autorización (control de acceso) integrados en el sistema. No confíe en el acceso a los recursos desde las aplicaciones. Este tipo de autorización facilita a los empleados y clientes autenticados el uso de los recursos que necesitan además de controlar eficazmente el acceso a recursos de valor.

Evitar desbordamientos de búfer

Las saturaciones del búfer representan una gran amenaza para la seguridad. Las aplicaciones que escuchan en un socket o puerto de E/S constituyen un blanco para los ataques. Es muy importante que los programadores, cuando tengan que

escribir datos en los búferes, no sobrepasen la capacidad permitida del búfer. Si la cantidad de datos que se escriben supera el espacio del búfer asignado a tal efecto, se produce un desbordamiento del búfer. Si esto ocurre, los datos se escriben en partes de la memoria que pueden estar asignadas a otros fines. En el peor de los casos, el desbordamiento de búfer contiene código malintencionado que entonces se ejecuta. Los desbordamientos de búfer representan un gran porcentaje de los puntos vulnerables de la seguridad.

Exigir privilegios mínimos

Las aplicaciones que están diseñadas para ejecutarse en el espacio de usuario no deben exigir privilegios de administrador para ejecutarse. Un desbordamiento del búfer en una aplicación que se ejecuta con privilegios de administrador permite que un atacante cause estragos en todo el sistema.

Dividir la aplicación en capas

El hecho de dividir una aplicación en capas independientes mejora la seguridad de la aplicación. En el núcleo de la aplicación debe encontrarse la parte que más se desee proteger; normalmente, el almacén de datos de la aplicación. La comunicación entre una capa y la capa siguiente debe producirse sólo a través de canales específicos. Cada capa agrega un obstáculo adicional a la entrada de un atacante.

Validar los datos proporcionados por el usuario

Es conveniente desconfiar siempre de los datos proporcionados por el usuario hasta que sean validados. Cualquier dato introducido por un usuario puede causar daños a un sistema. Hay que examinar y comprobar siempre que los datos sean correctos y que estén correctamente formados antes de actuar sobre ellos. Es conveniente recordar que, cuando se validan los datos, a veces resulta más fácil identificar información incorrecta (por ejemplo, buscar caracteres no válidos) que verificar que la información sea correcta.

Desarrollar planes de emergencia (diseño en caso de errores)

A la hora de defenderse ante los ataques, es recomendable elaborar un plan de emergencia al que se puede recurrir si no funciona dicha defensa. Los pasos que hay que dar en caso de que un usuario no válido consiga batir la defensa de una aplicación, deben esquematizarse claramente de cara al personal encargado de las operaciones. Estos planes deben tener como objetivo reducir los daños al mínimo y determinar en qué medida se ha visto afectada la aplicación.

Realizar copias de seguridad programadas

Los ataques que dan lugar a la denegación de servicio a los usuarios, como el bloqueo de un sistema de servidores, son difíciles de evitar e incluso de pronosticar. Es conveniente desarrollar directivas de seguridad que impongan la organización por clústeres y la realización de copias de seguridad sólidas para proporcionar a los usuarios la mayor disponibilidad posible al menor coste posible. La realización de copias de seguridad rutinarias es uno de los mecanismos más importantes de un plan de recuperación.

Supervisar errores no encontrados

El objeto de rendimiento del servicio Web incluye un contador que muestra los errores no encontrados. Los errores no encontrados se refieren a solicitudes de cliente a las que no se ha podido responder de forma satisfactoria porque incluyen una referencia a una página Web o a un archivo que no existe.

3.4.1Generación de claves con openSSL

Gracias a OpenSSL podemos tener comunicación encriptadas entre diferentes máquinas utilizando criptología asimétrica, es decir, claves públicas y privadas. Además, es posible montar entidades certificadoras que se encarguen de asegurar que una llave pertenece a quien dice pertenecer, de esta forma conseguimos encriptación y autentificación.

Las entidades certificadoras actuales cobran por el servicio de firma de llaves y no suele ser precisamente asequible. Por otro lado, montar una entidad certificadora oficial también resulta muy costoso ya que se demandan unas ciertas garantías que detrás del negocio hay una cierta seguridad. Por tanto, es habitual que los administradores de pequeñas redes se creen sus propios certificados para firmar sus claves. De esta forma podremos disponer de comunicaciones encriptadas sin necesidad de entidades certificadoras.

Estas entidades oficiales pagan para que aparezcan por defecto sus certificados en navegadores como Mozilla Firefox o Internet Explorer. De esta forma el propio navegador puede comprobar automáticamente que cuando se conecta a un sitio seguro, el certificado que recibe ha sido realmente firmado por una entidad oficial. Eso implica que nuestros certificados no serán reconocidos automáticamente por los navegadores a no ser que los añadamos manualmente, el único inconveniente que aporta esto es que el navegador mostrará un aviso extra al usuario (dependiendo de la configuración) advirtiendo que no reconoce la entidad certificadora.

3.4.2 Correo seguro con PGP

Mientras no existan clientes de correo que integren completamente las facilidades PGP, la utilización del mismo resulta bastante costosa y por tanto debe quedar reservada a casos concretos en los que la seguridad esta por encima de cualquier otro aspecto.

Ya se comento que PGP es una aplicación independiente y como tal habrá que instalarla en el ordenador utilizado habitualmente para el manejo del correo.

La aplicación PGP incluye tres módulos fundamentales:

1. Manejo de una base de datos de claves publicas donde se irán almacenando la claves de aquellas personas que envíen a la red mensajes cifrados o firmados. También almacenará el par de claves (publica y privada)

2. Facilidades para el firmado de documentos con nuestra clave y para el cifrado de ficheros destinados a un usuario del cual se tiene su clave publica.

3. Facilidades para el descifrado de mensajes y para la verificación de las firmas digitales.

Todo esto esta al margen del correo electrónico, y por tanto será un paso previo al envío del documento firmado y/o cifrado como un mensaje.

Existen, no obstante, algunas utilidades dependientes del sistema operativo y del cliente de correo utilizado que facilitan estas tareas, pero no existe por el momento ningún agente de usuario que integre de forma completa las facilidades PGP.

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 3

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 3 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Investigue el nombre de las más importantes Entidades Certificadoras a nivel de América y a que países pertenecen.

4. Elabore una lista de situaciones donde es conveniente utilizar firmas digitales.

5. Explique 5 razones por las cuales es necesario que las empresas adopten políticas serias en lo que se refiere al uso de firmas digitales.

CAPITULO 4: SISTEMAS DE FIREWALL Y ANTIVIRUS

4.1 Definición de Firewall

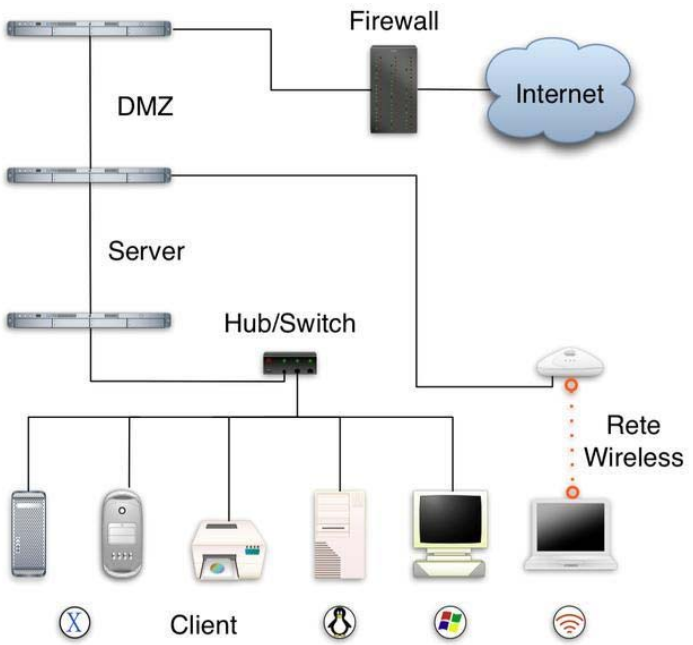


Figura 4.1 Protección de la red con Firewall

Un Firewall es un sistema ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una red externa que no lo es (por ejemplo Internet).

Un firewall es un dispositivo que funciona como cortafuego entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitiré o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

4.2 Funciones de los Firewall

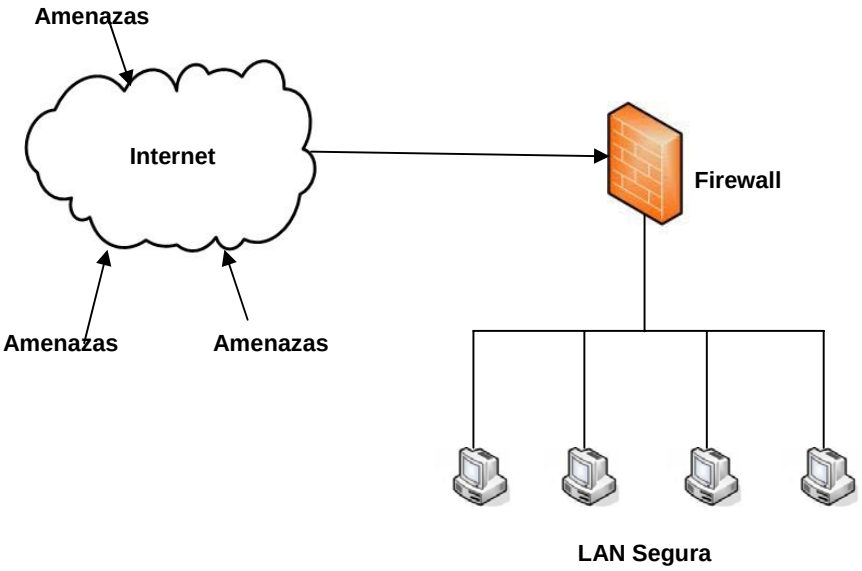


Figura 4.2. Funciones de los Firewall

Existen varios tipos de Firewall, algunos con más funcionalidades que otros, en términos generales los Firewall tienen las siguientes funciones:

- Control de usuarios
- Control de direcciones
- Control de servicios
- Control de comportamiento
- Control filtro de paquetes en un punto único
- Filtro de URLs.
- Antivirus
- Protección de Spam

4.3 Firewall Software

Estos programas son los más comunes en los hogares, ya que, a parte de resultar mucho más económicos que el hardware, su instalación y actualización es más sencilla. Eso sí, presentan algunos problemas inherentes a su condición, relacionado principalmente con el hecho de que consumen recursos de la PC, algunas veces no se ejecutan correctamente o pueden ocasionar errores de compatibilidad con otro software instalado.

Actualmente, los sistemas operativos más modernos como Windows XP y Linux integran soluciones básicas de firewall, en algunos casos, como en el software libre, son muy potentes y flexibles, pero requieren un gran conocimiento en redes y puertos necesarios para las aplicaciones. Para no tener problemas, existen una serie de herramientas externas que facilitan este trabajo de protección.

4.4 Firewall Hardware

Los firewall de hardware se utilizan más en empresas y grandes corporaciones. Normalmente son dispositivos que se colocan entre el router y la conexión telefónica. Como ventajas, podemos destacar que al ser independientes de la PC, no es necesario configurarlos cada vez que reinstalamos el sistema operativo y no consumen recursos del sistema.

Su mayor inconveniente es el mantenimiento, ya que son difíciles de actualizar y de configurar correctamente.

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Los Firewall tradicionales son de hardware, es decir, un dispositivo específico instalado en una red para levantar una defensa y proteger a la red del exterior. Son utilizados en entornos profesionales: el administrador de red define una serie de reglas para permitir el acceso y detiene los intentos de conexión no permitidos.

Los Firewall personales son programas que filtran el tráfico que entra y sale de una computadora. Una vez instalados, el usuario debe definir el nivel de

seguridad: permite o deniega el acceso de determinados programas a Internet (de forma temporal o definitiva) y autoriza o no los accesos desde el exterior.

4.5 Configuración de políticas de firewall

Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Dado lo anterior es fundamental que el administrador de la red establezca políticas que garanticen la eficiencia del Firewall.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).

- ¿De quién protegerse? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.

- Se pueden definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

- ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

Paradigmas de seguridad Se permite cualquier servicio excepto aquellos expresamente prohibidos.

Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.

Estrategias de seguridad

Paranoica: se controla todo, no se permite nada.

Prudente: se controla y se conoce todo lo que sucede.

- **Permisiva:** se controla pero se permite demasiado.

Promiscua: no se controla (o se hace poco) y se permite todo.

- ¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuanto es conveniente invertir.

4.6 Tipos de Firewall

- **Firewall de inspección de Paquetes**

Este tipo de Firewall se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

- **Firewall Personal**

Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.

- **Firewall de capa de red.**

Funciona al nivel de la red de la pila de protocolos (TCP/IP) como filtro de paquetes IP, no permitiendo que estos pasen el Firewall a menos que se atengan a las reglas definidas por el administrador del firewall o aplicadas por defecto como en algunos sistemas inflexibles de firewall.

Una disposición más permisiva podría dejar que cualquier paquete pase el filtro mientras que no cumpla con ninguna regla negativa de rechazo.

El cometido de los filtros (Packet Filtres) consiste en filtrar paquetes dejando pasar por el tamiz únicamente cierto tipo de tráfico. Estos filtros pueden implementarse a partir de routers.

- **Firewall de capa de aplicación.**

Trabaja en el nivel de aplicación, todo el tráfico de HTTP, (u otro protocolo), puede interceptar todos los paquetes que llegan o salen de una aplicación. Se bloquean otros paquetes (generalmente sin avisar al remitente). En principio, los firewall de aplicación pueden evitar que todo el tráfico externo indeseado alcance las máquinas protegidas.

Las pasarelas a nivel de aplicación (Application Gateway) se ocupan de comprobar que los protocolos a nivel de aplicación (ftp,http,etc...) se están utilizando de forma correcta sin tratar de explotar algunos problemas que pudiese tener el software de red.

Las políticas de accesos en un Firewall se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

4.7 Antivirus

Los virus dañinos son raros, pero existen y deben tenerse en cuenta cuando desarrollan los procedimientos de seguridad para las redes. Lamentablemente, ningún programa antivirus puede impedir el ataque de un virus; sólo puede efectuar lo siguiente:

- Evitar que el virus se active
- Eliminar el virus
- Reparar los daños en la medida de lo posible
- Mantener bajo control el virus una vez que se ha activado.

4.8 Políticas de Antivirus

La mejor manera de evitar el ataque de virus es impedir el acceso no autorizado. Debido a que la clave reside en la prevención, el administrador de la red necesita asegurarse de que se han tomado todas las medidas estándar, entre las que se incluyen:

- Contraseñas para reducir las posibilidades de acceso no autorizados

- Asignaciones de acceso y privilegios bien pensados para todos los usuarios

- Perfiles para estructurar el entorno de red de los usuarios con el fin de configurar y mantener un entorno de inicio de sesión de usuario, incluyendo las conexiones de red y los elementos de programa que ase mostrarán cuando el usuario inicie la sesión

- Normas que determinen el software que se puede cargar.

- Normas para implementar protección antivirus en las estaciones de trabajo clientes y en los servidores de la red.

- Actualizar permanentemente la protección de antivirus.

- Utilice sistemas de antivirus originales, donde el fabricante garantiza su efectividad

4.9 Combinación de Firewall y Antivirus

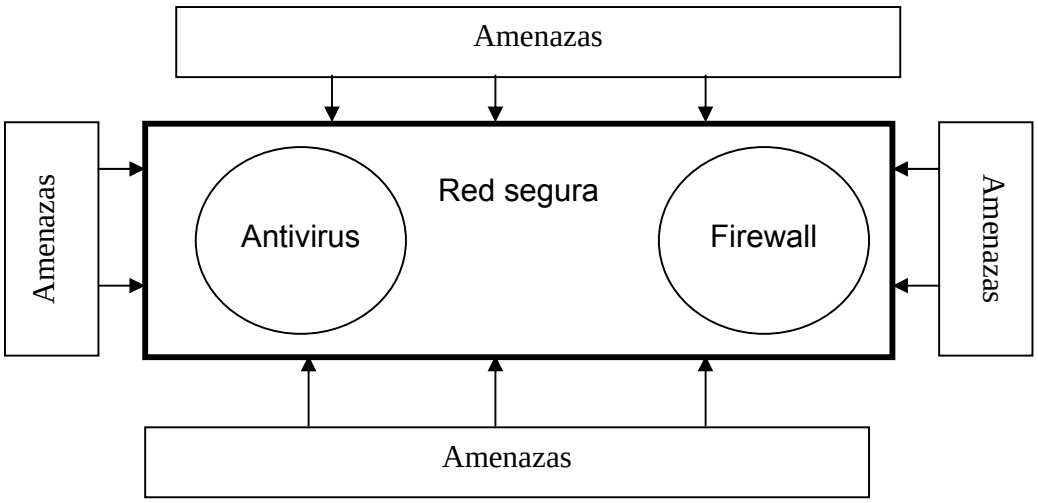


Figura 4.3. Los sistemas de Firewall y antivirus son complementarios

Los sistemas de Firewall solo protegen la red en su punto de interconexión con la red externa, cualquier otro punto de interacción con la red es vulnerable a posibles daños por infecciones de virus, es aquí donde es necesario implementar políticas de antivirus que ayuden a evitar la propagación de virus dentro de la empresa por acción de intercambio de información entre usuarios con medios extraíbles u otro medio de propagación.

Sin embargo es necesario aclarar que a pesar de que se cuente con un buen sistema de cortafuegos y una buena política de antivirus esto no es suficiente para evitar la perdida de los datos y las copias de seguridad se convirte en el mecanismo más eficiente para su restauración.

4.10 Diseño de Redes Seguras

Las siguientes preguntas le ayudaran a determinar lo amplia que debería ser la seguridad de su red. Recuerde que la clave es siempre la protección de los datos:

1. ¿Su empresa trabaja con algunos datos que no deberían ser accesibles para nadie en la red?

2. ¿Desea colocar la mayoría de los recursos compartidos en servidores dedicados, pero dejar que algunos se compartan en modo de punto apunto?

3. ¿Desea otorgar permisos a los recursos por pertenencia a grupo?(muchos administradores prefieren conceder derechos individuales a los usuarios hacia su almacenamiento personal en la red y utilizar grupos para conceder permisos al resto de los recursos compartidos de la red)

4. ¿Los empleados de sus empresas dejarán tranquilo el servidor si éste está en un lugar accesible, o algunos usuarios estarán tentados a manipularlo si hay algún problema en la red o si piensa que necesita algún ajuste?

5. ¿Hay empleados y visitantes que no deberían tener acceso a los recursos de la red?
6. ¿El entorno de su empresa permite que las contraseñas se presten o se roben?

7. ¿Algunos usuarios trabajan con datos confidenciales?

8. ¿Existen posibilidad que alguno de los usuarios de su instalación intente utilizar el equipo de otro sin permiso, o iniciar una sesión en la red con el nombre de otro sin autorización?

9. ¿Existe la posibilidad de que algún usuario de su instalación no comprenda correctamente la implementación de contraseñas o no entienda la importancia de la utilización de una contraseña?

10. ¿Su empresa requiere empleados temporales?

11. ¿Hay alguna necesidad de supervisar o restringir el acceso a determinados recursos o periféricos confidenciales de la red, o deben identificar a los usuarios que han tenido acceso a determinados recursos en periodos determinados?

12. ¿Hay alguna sospecha de que los empleados temporales o permanentes copien datos en forma intencional y se los lleven o hagan mal uso de ellos?

13. ¿Algunos de sus empleados son tan confidenciales que los podrían utilizar en contra de su empresa si cayeran en manos equivocadas?

14. ¿En la actualidad su red está protegida contra virus?

15. ¿Su empresa implementa políticas de cortafuegos para protección de redes externas

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 4

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 4 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

4. Investigue que Firewall se encuentran disponibles en el mercado y que características de protección brindan.

5. Realice un laboratorio en grupo de curso donde implemente políticas antivirus y de Firewall que usted mismo diseño.

6. Elabore un informe de laboratorio y entréguelo al Tutor.

CAPITULO 5: ESTEGANOGRAFIA Y BIOMETRIA

5.1 Esteganografía

La esteganografía es la rama de la criptología que trata sobre la ocultación de mensajes, para evitar que se perciba la existencia del mismo.

Es el arte y ciencia de escribir mensajes secretos de tal forma que nadie fuera de quien lo envía y quien lo recibe sabe de su existencia; en contraste con la criptografía, en donde la existencia del mensaje es clara, pero el contenido del mensaje está oculto. Por lo general un mensaje de este tipo parece ser otra cosa, como una lista de compras, un artículo, una foto, etc.

Los mensajes en la esteganografía muchas veces son cifrados primero por medio tradicionales, para posteriormente ser ocultados, por ejemplo en un texto que pueda contener dicho mensaje cifrado, resultando el mensaje esteganográfo. Un texto puede ser manipulado en el tamaño, letra, espaciado, tipo y otras características para ocultar un mensaje, sólo el que lo recibe, quien sabe la técnica usada, puede extraer el mensaje y luego descifrarlo.

5.2 Historia de la Esteganografía

Algunos ejemplos de técnicas de esteganografía que han sido usados en la historia son:

- Mensajes ocultos en tarjetas de ceda en la antigua Grecia, la gente escribía mensajes en tablas de madera y después la cubría con cera para que pareciera que no había sido usada.

- Mensajes secretos en papel, escritos con tintas invisibles entre líneas o en las partes en blanco de los mensajes.

- Durante la segunda guerra mundial, agentes de espionaje usaban miro-puntos para mandar información, los puntos eran extremamente pequeños, comparados con los de una treta de maquina de escribir por lo que en un punto se podía incluir todo un mensaje.

- Mensajes escritos en un cinturón enrollado en un bastón, de forma que sólo el diámetro adecuado revela el mensaje.

- Mensajes escritos en el cuero cabelludo, que tras crecer el pelo de nuevo, oculta el mensaje.

5.3 Técnicas Esteganograficas

Existen diferentes métodos que permiten ocultar información en imágenes digitales. Los cuales pueden ser clasificados en:

- Método en dominio espacial
- Método en dominio frecuencia

Método en dominio espacial

Dentro de este dominio, el método LSB (Least Significant Bit) es el más simple y sencillo de utilizar.

Técnica en el dominio espacial (LSB): Consiste en guardar información en los bits menos significativos de manera que los cambios no sean percibidos por el ojo humano.

Método en el dominio frecuencia: Son más robustos que los anteriores para ocultar información. En estos se utilizan transformaciones como la DFT (Discrete Fourier Transform), la DCT (Discrete Ccosine Ttransform) o la transformada Wavelet como medio para ocultar el mensaje secreto en áreas significativas de imagen.

Transformada discreta solo fase (TFSE): Esta técnica consiste en utilizar la transformada de Fourier y su antitransformada normalizada. Esta transformación descarta la información de la amplitud y preserva solo la fase, este proceso acompañado de la antitransformada normalizada actúa como un filtro que realza las frecuencias espaciales altas de modo que cuando es aplicado a imágenes que contienen bordes poco diferenciados produce un realce de los mismos.

Aplicación recorrido de grafos (método estego-graf): La utilización de la teoría de grafos en la estenografía viene dada para obtención de ciertas posiciones de imagen tal que a simple vista no se pueda observar que imagen ha sido modificada.

5.4 Aplicaciones

Con el desarrollo de la computación se ampliaron las técnicas esteganográficas., las cuales se empezaron a utilizar ara ocultar mensajes en contenidos multimedia o cualquier archivo que requieran demostrar propiedad de autor. Para utilizarla, se escoge un fichero, un documento Word, un documento PDF, una imagen BMP, un archivo de sonido. WAV o MP3 que nos sirva como contendor, y luego se crea el mensaje o el fichero que se desea oculta. El programa que realiza la ocultación,

modificará la portadora de varias formas posibles, alterando los valores de algunos de los puntos de la imagen, sumándoles o restándoles 1(+1 para indicar el bit 1 y -1 para indicar el bit 0), de forma que sea imperceptible, pero que alguien que sepa que esa imagen hay un mensaje, pueda recuperarlo. Otra forma de codificarlo es usar partes “no usadas” del fichero, por ejemplo, dentro de la cabecera del fichero hay a veces unos cuantos bytes que se dejan para usar las versiones posteriores, o después de la manera de fin de fichero, se puede añadir más información, sin que ningún de los programas habituales lo detecten. Existen métodos más robustos que usan tramas para el fondo de las imágenes, o alguna modulación determinada para el sonido, y conservan el mensaje aunque se cambie de tamaño o se pase a analógico.

Esta técnica se suele usar bastante para realizar “marcas de agua”, es decir, para que cuando uno vea una imagen, sepa que procede de un sitio determinado.

Existen muchos programas populares y sencillos para realizar esteganografía básica y se encuentran disponibles en el mercado y se encuentran de carácter libre como también licenciados.

5.5 Biometría

La biométrica es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La "Biométrica Informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

5.6 Historia de la Biometría.

La biométrica no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

En Occidente, la identificación confiaba simplemente en la "memoria fotográfica" hasta que Alphonse Bertillon, jefe del departamento fotográfico de la Policía de París, desarrolló el sistema antropométrico (también conocido más tarde como Bertillonage) en 1883. Éste era el primer sistema preciso, ampliamente utilizado científicamente para identificar a criminales y convirtió a la biométrica en un campo de estudio. Funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices. El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema, principalmente problemas con métodos distintos de medidas y cambios de medida. Después de esto, las fuerzas policiales occidentales comenzaron a usar la huella dactilar esencialmente el mismo sistema visto en China cientos de años antes.

En estos últimos años la biométrica ha crecido desde usar simplemente la huella dactilar, a emplear muchos métodos distintos teniendo en cuenta varias medidas físicas y de comportamiento. Las aplicaciones de la biometría también han mentado desde sólo identificación hasta sistemas de seguridad complejos.

5.4 Técnicas Biométricas

Los sistemas biométricos fundamentan sus técnicas en dos características fundamentales:

- **Características Físicas**

  - Huellas digitales
  - Geometría de las manos
  - Retina
  - Iris
  - Simetría de la cara

- **Características de comportamiento:**

  - Reconocimiento de voz
  - Reconocimiento de firma

- Reconocimiento de marcha
- Pulsaciones del teclado

En un sistema biométrico típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

A continuación se muestra un cuadro comparativo de las técnicas biométricas más comunes:

	Ojo (Iris)	**Ojo (Retina)**	**Huellas dactilares**	**Geometría de la mano**	**Escritura y firma**	**Voz**	**Cara**
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

ACTIVIDADES COMPLEMENTARIAS DEL CAPITULO 5

1. Elabore un resumen de cada una de las temáticas del capitulo y consulte las dudas con el Tutor.

2. Elabore un mapa conceptual del capitulo 5 donde se visualicen todos los conceptos del capitulo. Socialícelo con el Tutor y sus compañeros de curso.

3. Elabore un ensayo referente a la biometría y la esteganografia y su importancia en las redes de computadores