CAPÍTULO II

2. MARCO TEÓRICO

2.1. INTRODUCCIÓN

Los primeros sistemas de redes locales fueron desarrollados a mediados de los años 70 por diversos fabricantes. Xerox en el año de 1980, en cooperación con Digital Equipment Corporation e Intel, desarrolla y publica las especificaciones del primer sistema comercial de red denominado Ethernet. En 1986 IBM introdujo la red Token Ring. La mayor parte de empresas utiliza hoy día la tecnología Ethernet.

En el año de 1982 aparecen los ordenadores personales, siendo hoy una herramienta común de trabajo. Esta difusión del ordenador ha impuesto la necesidad de compartir información, compartir ficheros, impresoras, otros recursos, enviar mensajes electrónicos, ejecutar programas en otros ordenadores, etc.

2.2. REDES DE ÁREA LOCAL (LAN)

Una Red de Área Local (LAN) es un conjunto de computadoras o dispositivos de procesamiento conectadas entre sí en forma física y lógica con la finalidad de optimizar sus recursos y emular el proceso de un sistema de computo único. Una LAN está limitada en cobertura al entorno definido por el

usuario (generalmente su área de trabajo o edificio). Estas características dan a los usuarios de una LAN muchas ventajas a diferencia de lo que pudiera desarrollar un usuario aislado, entre las principales se puede mencionar: la posibilidad de conectar equipos de diferentes tecnologías, acceso a bases de datos comunes, correo electrónico, así como utilizar aplicaciones en red y procesamiento distribuido, etc.

Usualmente funcionan en base a un cableado propio por lo que se dispone de un gran ancho de banda. Así, en una red LAN el tráfico entre estaciones puede ser en banda base y estar regulado por algoritmos de acceso simples.

2.2.1. Definición de una Red LAN

Una red LAN consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio y regular el orden de acceso al mismo.

2.2.2. Elementos de una Red LAN

En una LAN existen elementos de hardware y software entre los cuales se pueden destacar: el servidor, estaciones de trabajo, sistema operativo, tarjetas de interfase de red, y el cableado estructurado.

El servidor es el elemento principal de procesamiento, contiene el sistema operativo de red y se encarga de administrar todos los procesos dentro de el, controla también el acceso a los recursos comunes como son las impresoras y las unidades de almacenamiento.

Las estaciones de trabajo, en ocasiones llamadas nodos, pueden ser computadoras personales o cualquier terminal conectada a la red. De esta manera trabaja con sus propios programas o aprovecha las aplicaciones existentes en el servidor.

El sistema operativo de red es el programa (software) que permite el control de la red y reside en el servidor. Ejemplos de sistemas operativos de red son: Netware, Lan Manager, entre otros.

La tarjeta o interfaz de red, proporciona la conectividad de la terminal o usuario de la red física, ya que maneja los protocolos de comunicación de cada topología específica.

El cableado estructurado está constituido por el cable utilizado para conectar entre sí el servidor y las estaciones de trabajo.

2.2.3. Protocolos de Área Local

Los protocolos de comunicación son las reglas y procedimientos utilizados en una red para establecer la transmisión de información entre los nodos que

tienen acceso a la red. Los protocolos de comunicación definen las reglas para la transmisión y recepción de la información entre los nodos de la red, de modo que para que dos nodos se puedan comunicar entre sí es necesario que ambos empleen la misma configuración de protocolos.

2.2.3.1. Protocolos de Bajo Nivel

El protocolo de bajo nivel es básicamente la forma en que las señales se transmiten por el cable, transportando tanto datos como información y los procedimientos de control de uso del medio por los diferentes nodos. Los protocolos de bajo nivel más utilizados son: Ethernet, Token Ring, Token Bus, FDDI, HDLC, Frame Relay y ATM.

2.2.3.2. Protocolos de Red

El protocolo de red determina el modo y organización de la información (tanto los datos como los controles) para su transmisión por el medio físico con el protocolo de bajo nivel. Los protocolos de red más comunes son: IPX/SPX, DECnet, X.25, TCP/IP, Apple Talk y NetBEUI.

2.2.4. Analizadores de protocolos LAN

Los analizadores de protocolos son dispositivos que colaboran en la tarea de monitorear el comportamiento de las redes o enlaces de datos, para que la

productividad de una entidad no se deteriore por fallas o anomalías de dichos sistemas.

El analizador de protocolo permite estudiar el comportamiento del tráfico y congestión que ocurren dentro de la red de datos de una organización.

2.3. SISTEMAS DE CABLEADO ESTRUCTURADO

El cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local, cumpliendo estándares internacionales; suele tratarse de cable de par trenzado de cobre o también de fibra óptica o cable coaxial.

El sistema de la red está constituido por el cable utilizado para conectar entre sí el servidor y las estaciones de trabajo. Hace un tiempo el cable estaba más estandarizado que ahora. ArcNet y Ethernet usaban cable coaxial y, Token Ring usaba par trenzado.

El cable coaxial fue uno de los primeros que se usaron, pero el par trenzado fue ganando popularidad. El cable de fibra óptica se utiliza cuando es importante la velocidad, si bien los avances producidos en el diseño de las tarjetas de interfaz de red permiten velocidades de transmisión sobre cable coaxial o par trenzado por encima de lo normal. Actualmente el cable de fibra óptica sigue siendo la mejor elección cuando se necesita una alta velocidad de transferencia de datos.

2.4. REDES DE ÁREA EXTENDIDA (WAN)

Las redes de de área extendida se considera a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Típicamente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo a los situados en los contornos) no les concierne el contenido de los datos, al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

2.4.1. Definición de una Red WAN

Una Red de Área Extendida (WAN) es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí. Esta forma de comunicación aporta, como principal diferencia respecto a las Redes de Área Local (LAN) o las Redes de Área Metropolitana (MAN), ya que el ámbito geográfico que puede cubrir es considerablemente mayor.

La tecnología WAN ha evolucionado considerablemente en los últimos años, especialmente a medida que las administraciones públicas de

telecomunicaciones han reemplazado sus viejas redes de cobre con redes más rápidas y fiables de fibra óptica, dado que las redes públicas de datos son el soporte principal para construir una WAN.

Cuando una organización se plantea el uso de una Red de Área Extendida, persigue una serie de objetivos:

- Servicios integrados a la medida de sus necesidades (integración de voz, datos e imagen, servicios).
- Integración virtual de todos los entornos y dependencias, sin importar donde se encuentren geográficamente situados.
- Optimización de los costes de los servicios de telecomunicación.
- Flexibilidad en cuanto a disponibilidad de herramientas y métodos de explotación que le permitan ajustar la configuración de la red, así como variar el perfil y administración de sus servicios.
- Mínimo coste de la inversión en equipos, servicios y gestión de la red.
- Alta disponibilidad y calidad de la red soporte de los servicios.
- Garantía de evolución tecnológica.

2.4.2. Elementos de una Red WAN

A continuación se describen los elementos que componen una Red de Área Extendida:

2.4.2.1. Equipos de interconexión.

Los equipos de interconexión, proporcionan el establecimiento de comunicaciones entre redes geográficamente distantes, creando un entorno único de red. Las funciones básicas de dichos equipos son los siguientes:

- Extensión de la red
- Definición de segmentos dentro de una red
- Separación de una red de otra.

Los elementos mas comunes en una Red WAN son: repetidores, bridges, routers, gateways o switches.

2.4.2.2. Infraestructura de red

Es el elemento de soporte que hace posible que se pueda crear una WAN. La construcción de este tipo de redes se puede soportar mediante el uso de las redes públicas de datos o enlaces privados, ya sean alquilados o propios.

2.5. PROTOCOLOS DE ÁREA EXTENDIDA

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área extendida. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN tales como: compañías telefónicas, portadoras alternas, entre otras.

Los protocolos de enlace de datos WAN describen cómo los marcos se llevan entre los sistemas en un único enlace de datos. Incluyen los protocolos diseñados para operar sobre recursos punto a punto dedicados, recursos multipunto basados en recursos dedicados, y los servicios conmutados multiacceso tales como Frame Relay.

Los estándares WAN son definidos y manejados por un número de autoridades reconocidas incluyendo las siguientes agencias:

- International Telecommunication Union - Telecommunication Standardization Sector (ITU-T), antes el Comité Consultivo sobre Telegrafía y Telefonía Internacional (CCITT).
- Organización Internacional de Estándares (ISO).
- Intemet Engineering Task Force (IETF).
- Electronic Industries Association (ETA).

Los estándares WAN describen típicamente tanto los requisitos de la capa física como de la capa de enlace de datos.

2.5.1. Capa Física: WAN

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio, y el DTE es el dispositivo asociado. En este modelo, los

servicios ofrecidos al DTE se hacen disponibles a través de un módem o unidad de servicio del canal/unidad de servicios de datos (CSU / DSU).

Algunos estándares de la capa física que especifican esta interfaz son:

- EIA/TIA-232D: Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.
- EIA/TIA-449: Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.
- V.35: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha (analógico) que operara en el intervalo de 48 a 168 kbps.
- X.21: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.
- G.703: Recomendaciones del ITU-T, antiguamente CCITT, relativas a los aspectos generales de una interfaz.
- EIA-530: Presenta el mismo conjunto de señales que la EIA-232D.
- High-Speed Serial Interface (HSSI): Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

2.5.2. Capa de Enlace de Datos: Protocolos WAN

Las tramas más comunes en la capa de enlace de datos, asociadas con las líneas seriales sincrónicas se enumeran a continuación:

2.5.2.1. Synchronous Data Link Control (SDLC).

Es un protocolo orientado a dígitos desarrollado por IBM. SDLC define un ambiente WAN multipunto que permite que varias estaciones se conecten a un recurso dedicado.

SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.

2.5.2.2. High Level Data Link Control (HDLC).

Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores por la forma en que cada vendedor ha elegido cómo implementarla. HDLC soporta tanto configuraciones punto a punto como multipunto.

2.5.2.3. Link Access Procedure Balanced (LAPB).

Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de marcos así como también para intercambio, retransmitición, y reconocimiento de marcos.

2.5.2.4. X.25 y Frame Relay.

X.25 define la conexión entre una terminal y una red de conmutación de paquetes. Mientras que Frame Relay, utiliza los recursos digitales de alta calidad donde sea innecesario verificar los errores LAPB. Al utilizar un marco simplificado sin mecanismos de corrección de errores, Frame Relay puede enviar la información de la capa 2 muy rápidamente, comparado con otros protocolos WAN.

2.5.2.5. Point-to-Point Protocol (PPP).

Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.

2.6. TECNOLOGÍAS DE ÁREA EXTENDIDA

Las tecnologías de codificación y proceso digital de la información han progresado considerablemente durante los últimos años. En la actualidad, la combinación de tecnología digital con elementos de elevada escala de integración hace posible incrementar la capacidad, fiabilidad y calidad del tratamiento de información con una importante reducción de costes frente a las técnicas convencionales de proceso analógico.

Las tendencias de las distintas tecnologías en el área de la conectividad entre redes remotas son:

- ISDN
- Frame Relay
- ATM
- SONET/SDH

2.6.1. Integrated Services Digital Network (ISDN).

Un conjunto de servicios digitales que transmite voz y datos sobre las líneas de teléfono existentes.

2.6.2. Frame Relay

Es una nueva técnica de conmutación de paquetes que requiere menos proceso que X.25, lo que se traduce en velocidades de acceso mayores (2/1,5 Mbps frente a 64/56 kbps de X.25) y un coste de implementación menor.

Esta técnica se describe en las recomendaciones UIT-T.430/31 y Q.922, que añaden funciones de relay (repetición) y routing (encaminamiento) nivel de la capa de enlace del modelo de referencia OSI. El objetivo de diseño fue conseguir un servicio multiplexado que transporta tramas, minimizando los tiempos muertos y el overhead (sobrecarga) normalmente asociados a X.25,

para lo cual, funcionalidades del tipo control de errores, de flujo, etc., se eliminan.

Frame Relay nació en el seno de los comités encargados de la formulación RDSI con el objetivo de sacar el mayor provecho posible de los accesos primarios (2 Mbps) para servicios portadores de paquetes. Actualmente Frame Relay permite alcanzar hasta 45 Mbps.

Frame Relay a diferencia de su predecesor X.25, no incluye corrección de errores cada vez que un paquete es enviado de un nodo a otro, lo que agilita la transmisión de datos; en su lugar, el control de errores se realiza solamente entre el equipo del cliente y el nodo de conmutación. Con esta técnica, la detección de posibles errores descansa más en el protocolo de transmisión que utilizan las aplicaciones que se ejecutan en los equipos terminales.

Frame Relay opera sobre la dirección de las tramas sin analizar el contenido de los datos, delegando en la capa de red del modelo de referencia OSI las facilidades de conmutación. Opera sobre dos tipos de circuitos virtuales:

- **Circuitos virtuales permanentes (CVP)**

  Los CVPs son conexiones establecidas en forma permanente, que se utilizan en transferencia de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a

través de un CVP no requiere los estados de establecimiento de llamada y finalización que se utilizan con los CVCs.

Los CVPs siempre operan en alguno de los estados siguiente:

Transferencia de datos.- Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.

Ocioso.- Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los CVCs los CVPs no se darán por finalizados en ninguna circunstancia ya que se encuentran en estado ocioso.

Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

- **Circuitos virtuales conmutados (CVC)**

  Los CVCs son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una trasferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un CVC consta de cuatro estados:

  Establecimiento de la llamada.- Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.

Transferencia de datos.- Los datos se transmiten ente los dispositivos DTE a través del circuito virtual.

Ocioso.- La conexión entre los dispositivos DTE aún está activa, sin embargo no hay transferencia de datos. Si un CVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.

Terminación de la llamada.- Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual los dispositivos DTE deben establecer un nuevo CVC si hay más datos que intercambiar. Se espera que los CVC se establezcan, conserven y finalicen utilizando los mismos protocolos de finalización que se usan en ISDN. Sin embargo, pocos fabricantes de equipo DCE Frame Relay soportan CVCs. Por lo tanto, su utilización real es mínima en las redes Frame Relay actuales.

2.6.3. ATM

La tecnología ATM (Asynchronous Transfer Mode, Modo de Transferencia Asincrono) ha surgido como parte de un conjunto de investigaciones realizadas por los operadores públicos de telecomunicaciones para desarrollar la Red Digital de Servicios Integrados de banda ancha (RDSI-BA). En 1991, los trabajos de la UIT-T en el campo RDSI-BA dieron lugar a la definición de un estándar global de interfaces de usuario para redes ATM (recomendación UIT-

TI 121), con una capacidad de transferencia de información de 155,52 Mbps y 622,08 Mbps.

Un año después, la UIT-T había desarrollado más extensamente protocolos e interfaces estándares para redes ATM. A principios de 1992 se formó el ATM Fórum, que publicó su primera especificación en Junio de ese mismo año.

ATM fue diseñada para el transporte de datos sobre fibra óptica, de forma que el ancho de banda se reparte en bloques de tamaño idéntico denominados células (cells). Es una técnica del tipo Cell Relay orientada a la conmutación de células de tamaño constante a alta velocidad. El objetivo de ATM es realizar el routing y la multiplexación de las células. Es similar a Frame Relay diferenciándose, fundamentalmente, en que en esta última el tamaño de la célula (oframe) es variable.

Las redes ATM son transparentes a todos los tipos de información de usuario transportados mediante los servicios proporcionados por la red: voz, datos y vídeo. Soporta la transmisión de tráfico de diferente naturaleza de forma integrada.

La flexibilidad del ancho de banda es prácticamente ilimitada: es posible establecer cualquier ancho de banda hasta la capacidad máxima del enlace de transmisión utilizado.

Es una técnica eficiente para el tráfico de datos interactivo. Para aplicaciones del tipo de transferencia masiva de información o conexión entre redes de alta velocidad es la técnica idónea.

Una red ATM está formada por un conjunto de elementos de conmutación ATM interconectados entre sí por enlaces o interfaces punto a punto. Los conmutadores ATM soportan dos tipos de interfaces distintas: interfaz de red de usuario e interfaz de red de nodo. Las interfaces de red de usuario conectan dispositivos ATM finales (host, router, PBX, vídeo) a un conmutador ATM. Las interfaces de red de nodo conectan dos conmutadores ATM entre sí.

Las redes ATM están orientadas a conexión, es decir se requiere el establecimiento de un circuito virtual antes de la transferencia de información entre dos extremos. Los circuitos que establece ATM son de dos tipos: caminos virtuales y circuitos virtuales, que son la ampliación de un conjunto de caminos virtuales.

El funcionamiento básico de un conmutador ATM es el siguiente: una vez recibida una celda a través de un camino o circuito virtual asigna un puerto de salida y un número de camino o circuito a la celda en función del valor almacenado en una tabla dinámica interna. Posteriormente retransmite la celda por el enlace de salida y con el identificador de camino o circuito correspondiente.

Existen principalmente dos tipos de conexiones en ATM:

- **Conexiones virtuales permanentes**

  La conexión se efectúa por mecanismos externos, principalmente a través del gestor de red, por medio del cual se programan los elementos de conmutación entre fuente y destino.

- **Conexiones virtuales conmutadas**

  La conexión se efectúa por medio de un protocolo de señalización de manera automática. Este tipo de conexión es la utilizada habitualmente por los protocolos de nivel superior cuando operan con ATM.

  Dentro de estas conexiones se pueden establecer dos configuraciones distintas:

- **Conexión punto a punto**

  Se conectan dos sistemas finales ATM entre sí, con una comunicación uni o bidireccional.

- **Conexión punto multipunto**

  Conecta un dispositivo final como fuente con múltiples destinos finales, en una comunicación unidireccional.

Los conmutadores ATM intercambian cada cierto número de celdas de información otras denominadas RM (Resource Management). Estas viajan en un sentido y en el conmutador final son reescritas y devueltas al origen con la indicación de retransmitir más despacio o de que todo va bien y que se puede

continuar la transmisión del mismo modo. Este es un mecanismo de control de congestión.

Otra ventaja de la tecnología ATM es la utilización eficiente del ancho de banda: por el mismo "canal" circulan celdas que pueden llevar información de voz, datos o imagen y todas reciben el mismo tratamiento en los conmutadores.

Cuando una comunicación finaliza, el ancho de banda que ocupaba queda liberado para otra comunicación. Para establecer una comunicación, se negocia el ancho de banda y la calidad de servicio con el conmutador ATM, que puede aceptar la petición o limitar sus pretensiones de acuerdo con el ancho de banda disponible (este proceso de negociación forma parte de las especificaciones UNI, User Network Interface).

En la actualidad el servicio ATM ofrecido por los operadores dominantes está disponible en todo el territorio nacional ofreciendo servicios de transporte de datos, conmutación de voz, etc. interoperando con otras redes de comunicaciones como Frame Relay de mayor penetración en el mercado.

ATM pretende ser una solución multimedia totalmente integrada para la interconexión de edificios ofreciéndose por parte de los operadores de comunicaciones la posibilidad de alquiler o compra del equipamiento de acceso al servicio, e infraestructura de líneas en caso de establecimiento de redes privadas.

ATM es la apuesta de las empresas de equipos de comunicaciones condicionada por la demanda de servicios multimedia y la liberalización del mercado de las comunicaciones, ya que es una tecnología que permite a los nuevos operadores de comunicaciones ser rápidamente competitivos. Un ejemplo de esta tendencia la presentan los operadores de cable que ofrecen multiservicios por una única infraestructura (televisión de alta definición, transporte de datos de gran ancho de banda, telefonía, etc.)

2.6.4. SONET / SDH

SONET (Synchronous Optical Network, Red Óptica Síncrona) y SDH (Synchronous Digital Hierarchy, Jerarquía Digital Síncrona) en terminología UIT-T, es un estándar internacional, desarrollado por el Working Group TI XI de ANSI para líneas de telecomunicación de alta velocidad sobre fibra óptica (desde 51,84 Mbps a 2,488 Gbps). SONET es su nombre en EE.UU. y SDH es su nombre europeo. Son normas que definen señales ópticas estandarizadas, una estructura de trama síncrona para el tráfico digital multiplexado, y los procedimientos de operación para permitir la interconexión de terminales mediante fibras ópticas, especificando para ello el tipo monomodo.

Para entender el funcionamiento de SDH es conveniente hacer una introducción previa a PDH (Plesiochronous Digital Hierachy).

2.6.4.1. PDH

PDH surgió como una tecnología basada en el transporte de canales digitales sobre un mismo enlace. Los canales a multiplexar denominados módulos de transporte o contenedores virtuales se unen formando tramas o módulos de nivel superior a velocidades estandarizadas 2 Mbps, 8 Mbps, 34 Mbps, 140 Mbps y 565 Mbps.

Es una jerarquía de concepción sencilla, sin embargo contiene algunas complicaciones, que han llevado al desarrollo de otras jerarquías más flexibles a partir del nivel jerárquico más bajo de PDH (2 Mbps) equivalente a una trama MIC de RDSI (30B+D).

La principal problemática de la jerarquía PDH es la falta de sincronismo entre equipos. Cuando se quiere pasar a un nivel superior jerárquico se combinan señales provenientes de distintos equipos. Cada equipo puede tener alguna pequeña diferencia en la tasa de bit. Es por ello necesario ajustar los canales entrantes a una misma tasa de bit, para lo que se añaden bits de relleno. Sólo cuando las tasas de bit son iguales puede procederse a una multiplexación bit a bit como se define en PDH. El demultiplexor debe posteriormente reconocer los bits de relleno y eliminarlos de la señal. Este modo de operación recibe el nombre de plesiócrono, que en griego significa cuasi síncrono.

Los problemas de sincronización ocurren a todos los niveles de la jerarquía, por lo que este proceso ha de ser repetido en cada etapa de multiplexación.

Este hecho genera un gran problema de falta de flexibilidad en una red con diversos niveles jerárquicos. Si a un punto de la red se le quieren añadir canales de 64 Kbps, y el enlace existente es de 8 Mbps o superior, debe pasarse por todas las etapas de demultiplexación hasta acceder a un canal de 2 Mbps y luego volver a multiplexar todas las señales de nuevo.

La falta de flexibilidad dificulta la provisión de nuevos servicios en cualquier punto de la red. Adicionalmente se requiere siempre el equipamiento correspondiente a todas las jerarquías comprendidas entre el canal de acceso y la velocidad del enlace, lo que encarece en extremo los equipos.

Otro problema adicional de los sistemas basados en PDH es la insuficiente capacidad de gestión de red a nivel de tramas. La multiplexación bit a bit para pasar a un nivel de jerarquía superior y con bits de relleno se convierte en tarea muy compleja seguir un canal de tráfico a través de la red.

2.6.5. Jerarquía Digital Síncrona (SDH)

Una red síncrona es capaz de incrementar sensiblemente el ancho de banda disponible y reducir el número de equipos de red sobre el mismo soporte físico que otro tipo de tecnologías. Además la posibilidad de gestión de red dota a ésta de mayor flexibilidad.

El desarrollo de equipos de transmisión síncronos se ha visto reforzada por su capacidad de interoperar con los sistemas plesiócronos (PDH)

existentes destinados principalmente al transporte de telefonía vocal. SDH define una estructura que permite combinar señales plesiócronas y encapsularlas en una señal SDH estándar.

Las facilidades de gestión avanzada que incorpora una red basada en SDH permiten un control de las redes de transmisión. La restauración de la red y las facilidades de reconfíguración mejoran la incorporación y prestación de nuevos servicios.

Este estándar de transmisión síncrona se recoge en las recomendaciones G.707, G.708, y G.709 del ITU (Unión Internacional de Telecomunicaciones) bajo el epígrafe SDH (Synchronous Digital Hierachy).

Las recomendaciones del ITU definen un número de velocidades de transmisión básicas en SDH:

- 155 Mbps, STM - 1 ('Synchronous Transport Module')
- 622 Mbps, STM – 4
- 2,4Gbps,STM-16
- 10 Gbps, STM - 64 (en desarrollo)

Estas recomendaciones definen también una estructura de multiplexación, donde una señal STM-1 puede portar señales de menor tráfico, permitiendo el transporte de señales PDH entre 1,5 Mbps y 140 Mbps.

SDH define un número de contenedores, cada uno de ellos correspondiente a una velocidad de transmisión PDH. La información de la señal PDH se introduce en su contenedor correspondiente y se añade una cabecera al contenedor, que permite monitorizar estas señales. Cabecera y contenedor forman un denominado contenedor virtual.

En una red síncrona todo el equipamiento se sincroniza con un mismo reloj de red. Variaciones de retardo asociadas a un enlace de transmisión inciden en una posición variable de los contenedores virtuales, lo que se resuelve asociándoles un puntero en la trama STM-1.

Ventajas de una red SDH:

- **Simplificación de red**

  Uno de los mayores beneficios de la jerarquía SDH es la simplificación de red frente a redes basadas exclusivamente en PDH. Un multiplexor SDH puede incorporar tráficos básicos (2 Mbps en SDH) en cualquier nivel de la jerarquía, sin necesidad de utilizar una cascada de multiplexores, reduciendo las necesidades de equipamiento.

- **Fiabilidad**

  En una red SDH los elementos de red se monitorizan extremo a extremo y se gestiona el mantenimiento de la integridad de la misma. La gestión de red permite la inmediata identificación de fallo en un enlace o nodo de la red. Utilizando topologías con caminos redundantes la red se

reconfígura automáticamente y reencamina el tráfico instantáneamente hasta la reparación del equipo defectuoso.

Es por esto que los fallos en la red de transporte son transparentes desde el punto de vista de una comunicación extremo a extremo, garantizando la continuidad de los servicios.

- **Software de control**

  La inclusión de canales de control dentro de una trama SDH posibilita un control software total de la red. Los sistemas de gestión de red no sólo incorporan funcionalidades típicas como gestión de alarmas, sino otras más avanzadas como monitorización del rendimiento, gestión de la configuración, gestión de recursos, seguridad de red, gestión del inventario, planificación y diseño de red.

  La posibilidad de control remoto y mantenimiento centralizado permite disminuir el tiempo de respuesta ante fallos y el ahorro de tiempo de desplazamiento a emplazamientos remotos.

- **Estandarización**

  Los estándares SDH permiten la interconexión de equipos de distintos fabricantes en el mismo enlace. La definición de nivel físico fija los parámetros del interfaz, como la velocidad de línea óptica, longitud de onda, niveles de potencia, y formas y codificación de pulsos. Asimismo se definen la estructura de trama, cabeceras y contenedores.

Esta estandarización permite a los usuarios libertad de elección de suministradores, evitando los problemas asociados a estar cautivo de una solución propietaria de un único fabricante.

Las redes de transmisión de telecomunicaciones que se desarrollan e implantan en la actualidad se basan principalmente en soluciones técnicas de jerarquía digital síncrona (SDH). Tanto las operadoras o PTPs en sus redes públicas, como empresas y organismos oficiales en sus redes privadas, están implantando SDH, que permite una integración de todos los servicios de voz, datos y vídeo a nivel de transmisión, lo que facilita la gestión de las redes y las beneficia de los niveles de protección y seguridad intrínsecos a SDH. Otra ventaja adicional de esta tecnología es que sobre ella se pueden desarrollar otras soluciones del tipo Frame Relay o ATM.

La tecnología PDH juega un papel todavía importante en la transmisión, al permitir segregar el tráfico en canales de comunicación de baja velocidad (menores de 64 Kbps). Es por ello que los equipos PDH se integran en el denominado acceso de usuario a las redes de transmisión en su jerarquía más baja (PDH a 2 Mbps). No obstante el resto de niveles de jerarquía superior en PDH (8, 34, 140 Mbps) están siendo desplazados por equipos de tecnología SDH, compatibles con PDH, pero más versátiles y económicos.

2.7. CALIDAD DE SERVICIO – QoS

En la UIT (Unión Internacional de Telecomunicaciones) aparece una primera definición de QoS (Quality of Service), en la recomendación E.800, en la que se define calidad de servicio como el efecto colectivo de prestaciones de servicio que determinan el grado de satisfacción del usuario en lo que respecta al servicio.

"La calidad del servicio (QoS) se refiere a la capacidad de una red para proporcionar un mejor servicio al tráfico de red seleccionado sobre varias tecnologías, incluyendo Frame Relay, Modo de transferencia asíncrona (ATM), redes Ethernet y 802.1, SONET y redes IP que pueden utilizar algunas o todas estas tecnologías subyacentes" [1]

La calidad de servicio consiste en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de proporcionar un determinado servicio. Debemos tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte (como puede ser Frame Relay, X.25, SDH, ATM, etc.) de manera que la gestión de QoS implica la interacción de estas tecnologías con los equipos de conmutación, que son los que finalmente determinarán el nivel de QoS alcanzado.

La Calidad de Servicio se define mediante:

- Clasificación: especifica qué campos de paquetes coinciden con valores específicos, todos los paquetes que concuerden con las especificaciones definidas por el usuario, se clasifican juntos.

[1] Internetworking Technologies Handbook. Quality of Service Networking

- Acción: define la gestión del tráfico, en la que se reenvían los paquetes de acuerdo a su información y los valores de su campo, por ejemplo, prioridad de VLAN (VPT) y DSCP (Punto de Código de Servicio Diferenciados).

La calidad de servicio se puede definir desde dos puntos de vista:

- Como un servicio que un usuario final solicita, ya sea directa o indirectamente de acuerdo a sus requerimientos; este servicio es cuantificado en la máquina de dicho usuario. En este caso es posible para el usuario determinar si el objetivo de la QoS se cumple.
- Como los servicios que el administrador de la red puede ofrecer, se hace referencia al rendimiento de red, es decir la capacidad de la red para proporcionar las funciones deseadas. En este caso hay objetivos administrativos para los diferentes tipos de tráfico que podrían no ser aparentemente cuantificables para un usuario final, pero si para el administrador de la red.

2.8. SEGURIDAD EN REDES

2.8.1. Introducción

La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos, recursos del sistema de información de una organización, de daños accidentales o daños intencionales.

Se puede entender como seguridad un estado de cualquier sistema que nos indique que está libre de peligros, daños o riesgos. Para que un sistema se pueda definir como seguro tiene que cumplir las siguientes características:

- Integridad: La información no puede ser modificada por quién no está autorizado.
- Confidencialidad: La información solo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesite.
- Antirrechazo: Que no se puede negar la autoria.

2.8.2. Riesgos de Seguridad

2.8.2.1. Intrusión

Alguien entra ilegalmente a un sistema y es capaz de utilizarlo y modificarlo como si fuera un usuario legítimo.

2.8.2.2. Rechazo de Servicios

Alguien logra que no puedan prestarse los servicios a los usuarios legítimos, puede ser dañando al sistema o sobrecargando el sistema o la red.

2.8.2.3. Robo de Información

Alguien tiene acceso a información confidencial, secreta, reservada o restringida. Es común en espionaje industrial, piratería, etc.

2.8.3. Técnicas de ataque

2.8.3.1. Ingeniería Social

El objetivo es convencer a algún usuario para que revele información acerca del acceso (Login, passwords, claves, etc.). Para esto se hacen pasar como administradores o usuarios.

2.8.3.2. Bugs del Sistema

Se aprovechan diversos errores de los sistemas para poder accesarlos o dañarlos. Algunos errores se conocen y explotan por largo tiempo, hasta que se corrigen.

2.8.3.3. Back Door

Intencionalmente se programaban entradas alternativas al sistema para usarlas en caso de emergencia o para poder acceder sistemas que sean manejados por otras personas.

Una variante es que cuando un intruso llegue a entrar a un sistema, lo modifique para crear su propia back door. Después de que se detecta una intrusión es recomendable reinstalar el sistema.

2.8.3.4. Caballos de Troya

Programas que aparentan ser una cosa, pero en realidad crean problemas de seguridad. Es una forma común de introducir virus.

2.8.3.5. Señuelos

Programas diseñados para hacer caer en una trampa a los usuarios. Un usuario puede sustituir el login por un programa que si intenta entrar el root le notifique el password.

2.8.3.6. Método del Adivino

Probar todas las posibles combinaciones para el password hasta encontrarlo. Las combinaciones son muchas, dependiendo del número de caracteres del password y el número de caracteres diferentes permitidos.

2.8.3.7. Revisión de Basura

Se revisa la basura en busca de información útil.

2.8.4. Puntos para mejorar la seguridad

2.8.4.1. Identificación y Autentificación

Los usuarios deben identificarse y después comprobar que son quien dicen ser. Lo más común es usar login y password

2.8.4.2. Integridad

Los sistemas se deben poder chequear en cuanto a su integridad, esto con el fin de detectar modificaciones que puedan afectar la seguridad.

Si el sistema se corrompe o es modificado, sería deseable detectar el origen del problema y restituir la integridad.

2.8.4.3. Confidencialidad

Usualmente se manejan permisos de acceso individuales o grupales y encriptamiento para transmisión en la red y para almacenamiento de información crítica.

2.8.5. Estrategias de Seguridad

2.8.5.1. Mínimos privilegios

El objetivo es minimizar los daños en caso deque la cuenta de un usuario sea invadida. En caso de que un usuario quiera realizar actividades diferentes tiene que solicitar que se le asignen los privilegios correspondientes.

2.8.5.2. Check Point

Se hace pasar todo el tráfico de la red por un solo punto y se enfocan los esfuerzos de seguridad en ese punto.

2.8.6. Firewalls

Un firewall es un dispositivo que funciona como cortafuegos 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 permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el correo, etc. 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.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web. Dependiendo del firewall también se puede permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo de software o hardware, es decir, un aparato que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet; incluso podemos encontrar ordenadores muy potentes y con software específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

Un firewall se considera una primera línea de defensa en la protección de la Información.

2.8.7. Virus

Los Virus son programas de ordenadores que se reproduce a sí mismo e interfieren con el hardware de una computadora o con su sistema operativo. Los virus están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: es decir, el ordenador debe cargar el virus desde la memoria del ordenador y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus. La carga activa puede modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo.

Existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos.

Un caballo de Troya aparenta ser algo interesante, por ejemplo un juego, pero cuando se ejecuta puede tener efectos dañinos.

Una bomba lógica libera su carga activa cuando se cumple una condición determinada, como cuando se alcanza una fecha u hora determinada o cuando se teclea una combinación de letras.

Un gusano se limita a reproducirse, pero puede ocupar memoria de la computadora y hacer que sus procesos vayan más lentos.

Los virus informáticos se difunden cuando las instrucciones (código ejecutable) que hacen funcionar los programas pasan de un ordenador a otro. Una vez que un virus está activado, puede reproducirse copiándose en discos

flexibles, en el disco duro, en programas informáticos legítimos o a través de redes informáticas. Estas infecciones son mucho más frecuentes en los PC que en sistemas profesionales de grandes computadoras, porque los programas de los PC se intercambian fundamentalmente a través de discos flexibles o de redes informáticas no reguladas.

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un ordenador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente. Normalmente, un usuario no ejecuta conscientemente un código informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de la computadora o al usuario informático para que ejecute el programa viral. Algunos virus tienen la capacidad de adherirse a programas legítimos.

Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo. Cuando se ejecuta dicho programa, ocurre lo mismo con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el ordenador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

2.8.7.1 Tipos de Virus

Existen seis categorías de virus: parásitos, del sector de arranque inicial, multipartitos, acompañantes, de vínculo y de fichero de datos. Los virus parásitos infectan ficheros ejecutables o programas de la computadora. No modifican el contenido del programa huésped, pero se adhieren al huésped de tal forma que el código del virus se ejecuta en primer lugar. Estos virus pueden ser de acción directa o residentes. Un virus de acción directa selecciona uno o más programas para infectar cada vez que se ejecuta. Un virus residente se oculta en la memoria del ordenador e infecta un programa determinado cuando se ejecuta dicho programa. Los virus del sector de arranque inicial residen en la primera parte del disco duro o flexible, conocida como sector de arranque inicial, y sustituyen los programas que almacenan información sobre el contenido del disco o los programas que arrancan el ordenador. Estos virus suelen difundirse mediante el intercambio físico de discos flexibles. Los virus multipartitos combinan las capacidades de los virus parásitos y de sector de arranque inicial, y pueden infectar tanto ficheros como sectores de arranque inicial.

Los virus acompañantes no modifican los ficheros, sino que crean un nuevo programa con el mismo nombre que un programa legítimo y engañan al sistema operativo para que lo ejecute. Los virus de vínculo modifican la forma en que el sistema operativo encuentra los programas, y lo engañan para que ejecute primero el virus y luego el programa deseado. Un virus de vínculo puede infectar todo un directorio (sección) de una computadora, y cualquier programa ejecutable al que se acceda en dicho directorio desencadena el virus.

Otros virus infectan programas que contienen lenguajes de macros potentes (lenguajes de programación que permiten al usuario crear nuevas características y herramientas) que pueden abrir, manipular y cerrar ficheros de datos. Estos virus, llamados virus de ficheros de datos, están escritos en lenguajes de macros y se ejecutan automáticamente cuando se abre el programa legítimo. Son independientes de la máquina y del sistema operativo.

Los usuarios pueden prepararse frente a un virus creando regularmente copias de seguridad del software original legítimo y de los ficheros de datos, para poder recuperar el sistema informático en caso necesario. Puede copiarse en un disco flexible el software del sistema operativo y proteger el disco contra escritura, para que ningún virus pueda sobreescribir el disco.

Para detectar la presencia de un virus se pueden emplear varios tipos de programas antivirus. Los programas de rastreo pueden reconocer las características del código informático de un virus y buscar estas características en los ficheros del ordenador. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de rastreo deben ser actualizados periódicamente para resultar eficaces.

Los programas antivirus detectan actividades potencialmente nocivas, como la sobreescritura de ficheros informáticos o el formateo del disco duro de la computadora.

2.8.7.2. Sniffing

El sniffing comprende la captura de todos los paquetes que pasan por una red. Los mismos que son utilizados comúnmente entre los atacantes potenciales cuyo objetivo es obtener la mayor información posible de una organización.

2.8.7.3. Spoofing

Spoofing es la técnica de suplantación de identidad, mediante la creación de tramas TCP/IP utilizando una dirección IP falsa; donde el objetivo es desde un equipo se simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basado en el nombre o la dirección IP del host suplantado.