35
2ES

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

SEGURIDAD EN REDES

SEMINARIO DE INVESTIGACION INFORMATICA
QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

PRESENTA:

EDITH TAPIA RANGEL

ASESOR DEL SEMINARIO
L.I. Ma. CONCEPCION CAMARGO FAJARDO

MEXICO, D.F. 1995

A Dios
por su infinito amor

A mis padres
Judith y Adelaido
por su maravilloso ejemplo

A mis hermanos
Claudia, Alejandra y Edgardo
por su invaluable y eterna amistad

A Iván y David
mis consentidos

A mi familia
tanto la presente como la ausente
por su presencia en mi vida

A Pablo
por el cariño y amor
que me has brindado

A Conny
Por su ayuda y apoyo

A todos aquellos amigos que me apoyaron tanto física como moralmente, especialmente a Pablo, Jorge, Miguel, Jose Juan, Daniel, Lorena, Jose Luis y Marcos

Gracias.....

INDICE

INDICE DE FIGURAS

INTRODUCCION

El desarrollo de un proyecto de tesis no es solo una tarea más que realizar. Es un proceso que nos conduce a la culminación de un objetivo que por muchos años esta fijo en nuestra mente. Esta etapa tan significativa también representa un paso más para continuar el camino del desarrollo profesional.

El texto presentado a continuación representa la materialización de una meta. No pretende mostrar lo experto que se es o no se es en un tópico. Simplemente es una panorámica de un aspecto importante en las comunicaciones de hoy en día: la seguridad. Sin embargo, su valor más significativo radica en el conocimiento que proporciona en cuanto a redes, administración de red, seguridad en redes, etc, que han contribuido a menguar mi incultura informática.

Este documento es una recopilación de las características físicas, lógicas y humanas que en materia de seguridad pueden implementarse en una red. Esta estructurado para conducir al lector a través de un razonamiento lógico que lo lleve a comprender y aprovechar el esquema de seguridad de una red. No pretende ser el testimonio de un perito en la materia que indique cómo, cuando y donde debe implementarse una arquitectura de seguridad en una red, simplemente es una referencia de los procesos, instrumentos, técnicas y personal que se requiere para establecer un esquema de seguridad en nuestras redes.

En el primer Capítulo se exponen a manera de antecedentes los conceptos básicos relacionados con las redes. En él se definen los elementos presentes en las redes actuales tales como: tipos de red, topologías de red, técnicas y medios de transmisión, arquitectura de red del modelo OSI, arquitectura de una WAN y de LAN

y la forma de interconectar las redes. El propósito de este capítulo es proporcionar al interesado una vista general del ambiente que debe asegurar.

El Capítulo segundo establece el bosquejo general de la Administración de red, que se describe como la amalgama de instrumentos, procedimientos y recursos humanos que controla la actividad de la red. El capítulo también incluye una descripción de los modelos que conforman la Administración de red, los cuales son: el modelo de información, el modelo funcional, el modelo organizacional, el modelo arquitectural y el modelo de comunicación. Posteriormente, se describen brevemente las funciones y procedimientos de cada uno de los dominios funcionales (de configuración, de fallas, de desempeño, de contabilidad y de planeación de la capacidad de la red) que conforman el modelo funcional.

El capítulo tercero esta dedicado completamente al dominio de seguridad del modelo funcional de la administración de red. Comienza con una descripción de los procesos que lo constituyen, que son: el análisis de riesgos que se encarga de detectar las vulnerabilidades de los sistemas de cómputo/comunicación y las amenazas que pueden atacarlos; la evaluación de los servicios de seguridad que debe proporcionar la administración de red a nivel físico y lógico (protección del hardware, identificación y autentificación, control de accesos, etc); las técnicas del dominio de seguridad que apoyan la prestación de los servicios de seguridad y que abarcan desde el encriptamiento hasta las máquinas firewall; las acciones a tomar cuando se detecta y/o descubre un intruso; la protección de los sistemas de administración de red; el monitoreo de la seguridad mediante la auditoría informática aplicada a la seguridad de la red. Finalmente expone los intrumentos que existen en la actualidad para el monitoreo y protección de la red y una descrición del personal que soporta las funciones anteriores.

En el Capítulo IV se destaca la aplicación de los procedimientos, instrumentos y recursos humanos del dominio de seguridad en una LAN. Puesto que las LAN son el tipo de red más utilizado en las organizaciones, se aterrizaron algunos aspectos de la seguridad de una LAN. El capítulo finaliza con la esquematización de un ambiente seguro utilizando Netware Novell 4.x, uno de los sistemas operativos para red más utilizados en México.

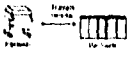
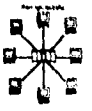
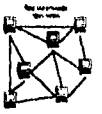
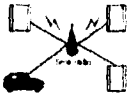
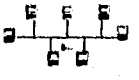
La parte final del escrito incluye las conclusiones obtenidas durante la elaboración de esta tesis, un glosario de términos de los conceptos que no pudieron profundizarse en su momento y las fuentes de información consultadas.

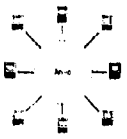
CAPITULO I. INTRODUCCION A LAS REDES

"Una red de computadoras es un sistema de comunicación que permite a las computadoras intercambiar información una con otra de forma significativa. El término computadora debe ser interpretado en su sentido más amplio como un sistema de procesamiento de información"[WAT91]. Las redes pueden enlazar computadoras del mismo tipo (redes homogéneas) o pueden enlazar computadoras de diversos tipos (redes heterogéneas) y cubrir áreas de diversos tamaños, extendiéndose ya sea a través de una habitación, un edificio, una ciudad, un país o todo el mundo. La información es transmitida en las redes por medio de paquetes, que son secuencias de *bits* que contienen información de control e información del usuario, cada paquete tiene un tamaño específico determinado por el tipo de red.

I.1 BREVE HISTORIA

La capacidad de comunicación de las redes de nuestros días es producto de un proceso de evolución originado por la necesidad compartir y aprovechar recursos. Podemos apreciar el origen y desarrollo de las comunicaciones a través del siguiente cuadro[WAT91]:

Protocolos		Conexiones cerradas y específicas	Principios 1960
Paquetes		Conexión vía telefónica	
Redes		Conexión equipo central-terminal	Mediados 1960
		Conmutación de paquetes	Baran, 1967
		Comunicación de paquetes por radio (ALOHA)	Abramson, 1970
		Estándar de Ethernet	Metcalfe y Boggs, 1976

	Anillo de Cambridge	Wilkes y Wheeler, 1979
	Redes de Area Metropolitana (Metropolitan Area Networks) Redes Digitales de Servicios Integrados (Integrated Services Digital Network ISDN)	Mediados y finales de los 80's
	Frame Relay Modo de Transferencia Asíncrono (Asynchronous Transfer Mode ATM)	Principios de los 90's

Podemos observar que la necesidad de comunicación se presentó a principios de los 60's, cuando la 2a. Generación de computadoras (1959-1963) tocaba fin. El primer objetivo en esta área consistió en transferir los datos colectados en las computadoras de los científicos a los *mainframes* para ser procesados. Se implementaron para ello primitivos formatos y procedimientos de transferencia que pueden considerarse como el origen de los protocolos.

Para mediados de 1960, hizo su aparición la 3a. Generación de computadoras y se incrementó la capacidad de comunicación. Se conectaron las minicomputadoras a los mainframes vía telefónica. Estas minicomputadoras se denominaron estaciones de ingreso de trabajos remotos y proporcionaban las funciones de Entrada/Salida al mainframe. También a mediados de los 60's se adaptaron las estaciones de trabajo remotas para incluir terminales, permitiendo a usuarios remotos accesar a las instalaciones del mainframe. De esta forma, no solamente era posible la transferencia de información, sino el intercambio de datos mediante un proceso interactivo de entrada/salida.

Conforme se incrementó la capacidad del equipo central, se necesito de una solución útil para compartir recursos valiosos tales como: paquetes de programación especializados, bases de datos y almacenamiento, y respaldo de archivos. Por las razones anteriores, nació la primera red, que tenía la forma de estrella y donde el mainframe actuaba como un conmutador que permitía se compartieran recursos

adicionales a los de entrada/salida, como el almacenamiento y el uso de memoria.

Posteriormente, se desarrolló el concepto de conmutación de paquetes, que representó un antecedente muy importante para la construcción de redes con topologías más complicadas. La conceptualización de esta idea fue escrita por Baran en 1964 pero no fue hasta 1967 cuando se implementó por primera vez en el Laboratorio Nacional de Física (National Physical Laboratory NPL). En Estados Unidos con la misma técnica se diseño *ARPANET* (Advanced Research Projects Agency NETwork). Más adelante, diversas compañías desarrollaron sus propia arquitectura, ejemplos de ello son SNA (Systems Network Architecture) de IBM (International Bussiness Machine) y DECNET (Digital Equipment Corporation Network) de DEC (Digital Equipment Corporation). La conmutación de paquetes incrementó el número de comunicaciones activas, redituando en más operaciones atendidas en un período específico de tiempo.

A principios de 1970, la Universidad de Hawai (Abramson) desarrolló un sistema de comunicación de paquetes con señales de radio. Como resultado de estas investigaciones nació ALOHA, un método para la transmisión de paquetes que utiliza el método de *broadcast* y que puede ser aplicable a los sistemas de radio y satelitáles. Variantes de este método permitieron que surgieran las primeras redes de área local.

Soportados por estos avances, los investigadores desarrollaron las LAN de diversas formas. Su objetivo primero fue que se compartieran dispositivos muy costosos entre máquinas austeras, así como proporcionar formas flexibles para permitir que diversas computadoras trabajen en el mismo problema.

La idea de un sistema digital común para todas las comunicaciones locales fue elaborado en los 70's en el Centro de Investigación Xerox de Palo Alto (Metcalfe y Boggs, 1976). Ahí fue desarrollado *Ethernet*, basado en transmisión broadcast sobre un *bus*. En la Universidad de Cambridge, se desarrolló e implementó el Anillo de Cambridge por Wilkes y Wheeler (1976 - 1979).

Los desarrollos de los últimos diez años, ha proporcionado más velocidad a las MAN y WAN. Estos avances permiten que hoy en día contemos con : *ISDN* (Integrated Services Digital Network - Red Digital de Servicios Integrados), *ATM*

(Asynchronous Transfer Mode - Modo de transferencia asíncrono), *Frame Relay* y *FDDI* (Fiber Distribuited Data Interface).

I.2 CLASIFICACION DE REDES

Una vez descrito brevemente el origen y evolución de las redes, es importante establecer la clasificación de la redes que se hace de acuerdo al área geográfica que abarcan. De esta forma, encontramos tres tipos principales de redes.

RED DE AREA LOCAL (LOCAL AREA NETWORK LAN)

La IEEE (Institute of Electrical and Electronics Engineers) define una red de área local (Local Area Network, LAN) como:

> " Un sistema de comunicación de datos que permite que un número de dispositivos independientes se comuniquen directamente unos con otros, dentro de un área geográfica de tamaño moderado sobre un canal físico de comunicaciones y con velocidades moderadas de datos" [MAR89].

Esto significa que las redes de área local soportan la comunicación *peer-to-peer* (de igual a igual), donde todos los dispositivos que están en comunicación tienen el mismo estado en el sistema; toma lugar en un área geográfica que no rebasa los 10 km; los dispositivos se comunican directamente mediante un cable dedicado o algún otro medio de comunicación; y finalmente por lo que respecta a la velocidad, hay que señalar que los adelantos en la tecnología ya que permiten velocidades de hasta 100 Mbps y por lo tanto ya no es vigente considerar el término de "velocidades moderadas de datos".

RED DE AREA METROPOLITANA (METROPOLITAN AREA NETWORK MAN)

Las redes de área metropolitana algunas veces enlazan los edificios de una organización dentro de una ciudad; o bien enlazan un grupo de fábricas y oficinas.

Las LAN y las WAN son redes de comunicación que transportan información entre las diferentes estaciones que se conectan a ellas. Las redes MAN surgen como complemento de las redes antes mencionadas. Cubren regiones que pueden ir más allá de los 100 km (aproximadamente el tamaño de una metrópoli), permiten la conexión de más de 500 estaciones, y transmiten información a más de 50 Mbps.

Algunas de las aplicaciones previstas inicialmente para las MAN son :

a) La interconexión de redes locales

b) la transferencia masiva de datos

c) la transmisión de voz digitalizada y de video comprimido

Las redes metropolitanas pueden ser públicas o privadas. Las primeras conectan sitios de una misma organización, por tanto, la necesidad de seguridad no es muy alta; las segundas conectan diversas organizaciones y por ello, son manejadas de forma central por un operador público, por esta razón requieren de algunos estándares y salvaguardas contra el maluso, sea éste deliberado o accidental [WAT91].

RED DE AREA AMPLIA (WIDE AREA NETWORK WAN)

Es una red de comunicación de datos diseñada para servir a un área de cientos de miles de km, así como a redes de conmutación de circuitos de tipo público o privado, y redes de telefonía nacional. Utilizan las facilidades de las telecomunicaciones públicas para proporcionar al usuario acceso a la capacidad de las instalaciones de almacenamiento masivo de datos asociado con los mainframes y para permitir un rápido intercambio de información con usuarios de diversas redes. Diversos dispositivos se incorporan diariamente a estas redes tales como: terminales inteligentes, minicomputadoras, computadoras personales, etc.

Las WAN pueden interconectar redes de uno o varios paises. Estas redes

normalmente utilizan para comunicarse la técnica de conmutación de paquetes. Son controladas por organizaciones telefónicas y telegráficas; organizaciones privadas para su uso exclusivo o para uso del público en general (*INTERNET*). Estas redes incluyen también segmentos conectados por señales de microondas y enlaces satelitáles.

DIFERENCIAS ENTRE LAN, MAN y WAN

Cuatro características básicas distinguen a cada uno de estos tres tipos de redes :

Primera, la delimitación y extensión de la red (la distancia que separa a los dispositivos) y las velocidades de transmisión de datos empleadas, este punto se encuentra íntimamente relacionado con el medio de transmisión;

Segunda, la probabilidad de errores durante la transmisión y por lo tanto, los mecanismos de detección y recuperación de errores que deben implementar los protocolos correspondientes;

Tercera, el carácter privado de la subred, esto es, la propiedad de la información que se contiene en los diversos dispositivos conectados a las subredes; y

Cuarta, los eventos que se consideran al momento de su planeación. Mientras que los diseñadores de una WAN se ven forzados (por razones legales, económicas ó políticas) a utilizar la telefonía pública existente, los diseñadores de las MAN y LAN tienen completa libertad de hacer uso de la tecnología de red que consideren conveniente.

I.3 TOPOLOGIAS DE RED

Con topología de una red nos referimos a la "..forma en la que se conectan físicamente los dispositivos a la red"[MAR89]. Por diversas razones, las redes LAN utilizan topologías sencillas, a diferencia de las redes MAN y WAN que utilizan

generalmente una topología de malla. Las topologías de red más conocidas son [BEA90]:

CONFIGURACION DE MALLA

Las redes que describen esta topología son redes totalmente conectadas (Figura 1.1). En una red de este tipo, enlaces bidireccionales separados son establecidos entre cada par de *nodos*. No existen nodos intermedios involucrados en la comunicación y cada dispositivo final se enlaza directamente por medio de la comunicación nodo a nodo con cualquier otro dispositivo final. Una red totalmente conectada tiene n nodos que requerirán n(n-1)/2 enlaces. Esta conexión ofrece mucha confiabilidad, pero presenta la desventaja de que un paquete puede pasar a través de diversas conmutaciones que no son necesarias para alcanzar su destino final. En contraparte, las rutas altenativas estarán generalmente disponibles aún si muchos enlaces están fallando. Esta topología se utiliza generalmente en una WAN.

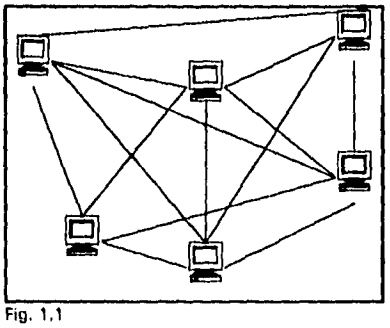


Fig. 1.1

CONFIGURACION DE TIPO ESTRELLA

La configuración de tipo estrella como la mostrada en la Figura 1.2, se caracteriza por contar con un controlador central al cual están conectados directamente todos los nodos. Todas las transmisiones de un nodo a otro pasan a través del controlador central, el cual es responsable de la administración y control de

las comunicaciones. Frecuentemente, el controlador central actúa como un dispositivo de conmutación. Cuando un nodo desea comunicarse con otro nodo, el controlador central establece un circuito, o ruta dedicada, entre los dos nodos que desean comunicarse. Una vez que el circuito se ha establecido, los datos pueden ser intercambiados entre los dos nodos como si se encontraran enlazados por una liga dedicada *point-to-point*. Esta topología ha sido empleada por muchos años en los sistemas de conmutación telefónica, donde conjuntos individuales de teléfonos son los nodos y un ***PBX*** (Private Branch Exchange - Conmutador) funciona como el controlador central.

La desventaja principal de la red de tipo estrella es su vulnerabilidad a fallas del controlador central, ya que de él depende la comunicación de todos los nodos.

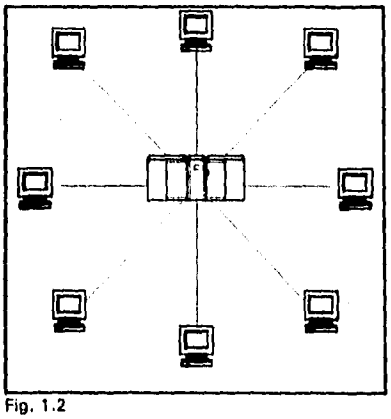


Fig. 1.2

CONFIGURACION DE TIPO BUS

En la topología de bus, mostrada en la Figura 1.3, cada nodo está unido directamente a un canal común de comunicación. Las señales que se transmiten sobre el canal toman la forma de mensajes. Como cada mensaje pasa a través del canal todos los nodos lo reciben. Cada nodo determina entonces, basado en la dirección contenida en el mensaje, aceptar y procesar el mensaje o simplemente ignorarlo.

Esto significa que la red es también el medio de transmisión y por lo tanto se deben efectuar arreglos especiales a los nodos de la red introduciendo los denominados *transcievers* que pueden ser intertados o a agregados a los nodos.

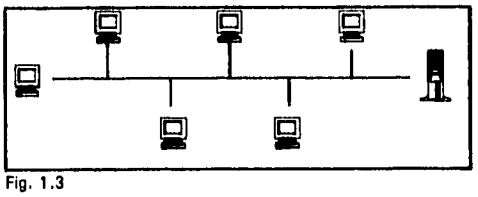


Fig. 1.3

CONFIGURACION DE TIPO ANILLO

La topología de anillo se encuentra representada en la Figura 1.4. y consiste de una serie de nodos conectados uno con otro en forma de un circuito cerrado. Los nodos son arreglados de forma que sólo acepten datos transmitidos a ellos de su nodo vecino inmediato, con el cual están conectados y puedan transmitir los datos bit por bit al siguiente nodo conectado. Esta función solo la pueden realizar en una dirección, de tal forma que los nodos, denominados también repetidores tienen una sencilla tarea que realizar. En una red de tipo anillo, los mensajes son transmitidos en paquetes, cada uno de los cuales contiene una dirección destino.

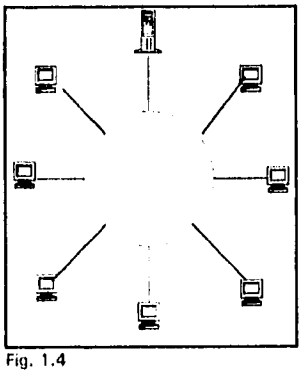


Fig. 1.4

I.4 TECNICAS Y MEDIOS DE TRANSMISION

TECNICAS DE TRANSMISION

Son dos las técnicas de transmisión de señales: la transmisión Baseband y la transmisión Broadband [MAR89]:

TÉCNICA DE TRANSMISIÓN BASEBAND

La transmisión Baseband utiliza señales digitales, esto es, las señales de datos son transportadas sobre el medio físico en la forma de pulsos discretos de electricidad o luz. En esta forma de transmisión, un dispositivo de envío manda pulsos directamente sobre el canal de comunicación, y el dispositivo de recepción los detecta. Con esta técnica se utiliza la capacidad completa del canal para transmitir una sola señal de datos. Los múltiples dispositivos unidos a la red que utilizan la transmisión Baseband comparten el canal de comunicación por medio de la multiplexión por división de tiempo (*time-division multiplexing TDM*). Con TDM, los dispositivos toman su turno de transmisión, y solo un dispositivo transmite a un tiempo. Los datos de diferentes dispositivos son entonces depositados en el canal de comunicación. Como una sola estación puede transmitir a un tiempo, debe haber maneras de determinar cual estación tiene permitido transmitir. Para ello se utilizan los métodos de control de acceso.

TÉCNICA DE TRASMISIÓN BROADBAND

La transmisión Broadband típicamente emplea transmisión analógica utilizando un rango más amplio de frecuencias que la Baseband. Con la transmisión analógica, las señales empleadas son contínuas y no discretas. Las señales fluyen a través del medio de transmisión en la forma de ondas electromagnéticas. Estas ondas electromagnéticas tienen tres características que son útiles en las telecomunicaciones: amplitud, frecuencia y fase. En el cable eléctrico, la amplitud de onda se asocia con el nivel de voltaje trasportado en el cable. La amplitud de onda se refiere a la intensidad de un rayo de luz. La frecuencia de una onda indica el número de ciclos u

oscilaciones que la onda realiza por segundo. La fase de una onda se refiere al punto en el cual la onda alcanza su ciclo completo. Con la transmisión analógica, una señal de datos se sobrepone en un señal de trasporte mediante la variación ó modulación de cualquiera de las tres características de la señal. El ancho de banda del canal de transmisión tiene relación directa con la velocidad a la que viajan los datos, ó el número de bits por segundo que pueden ser trasportados sobre él.

MEDIOS DE TRANSMISION

Los medios de transmisión física son los enlaces que se tienden entre los dispositivos para comunicarse. Es la facilidad física usada para interconectar juntas estaciones del usuario y dispositivos, para crear una red que transporte mensajes entre los mismos. Estos enlaces, se pueden clasificar en:

ENLACES FÍSICOS TERRESTRES:

CABLE COAXIAL

Consiste de un núcleo de cobre que funge como conductor central ya que está rodeado de material aislante. Este aislante se ve cubierto a su vez por otro segundo conductor, el cual consiste de una malla trenzada, a la cual finalmente se sobrepone una protección de material no conductor. Este cable ha sido empleado para las señales de televisión. Otras características que presenta son : transmite señales digitales y analógicas; se conecta al transciever; se utiliza en redes tipo bus y algunas veces en las tipo anillo; tiene un alcance de 1 a 10 kms; el ancho de banda llega hasta los 100 Mbps; es de costo medio y presenta poca inmunidad a lo ruidos.

PAR TRENZADO

Este medio consiste de dos hebras de cable de cobre aisladas que han sido trenzadas. Un número de estas hebras se agrupan dentro de una protección para formar un cable. Otra variedad de este cable protege cada par de hebras y que disminuye más la interferencia eléctrica. Este tipo de cable ha sido utilizado antes por

las líneas telefónicas. Otras características de este medio son: Transporta señales de tipo analógico y digital; se puede utilizar en redes de cualquier topología (estrella, anillo, etc); su alcance promedio es de 3 km; tiene un ancho de banda de 1Mbps y es de bajo costo.

FIBRA ÓPTICA

Consiste de un cilindro extremadamente delgado de vidrio llamado núcleo, rodeado por una capa concéntrica de vidrio conocida como "vestimenta" y cubierta por un protector. Varias de estas fibras en conjunto forman un cable. En este medio en especial, la luz que viaja por el núcleo se refleja nuevamente en él cuando choca con la vestimenta. Presenta otras características tales como : Transporte de señales digitales; no es afectada por interferencia eléctrica; tiene un ancho de banda de hasta 1 Gbps; su alcance es de 10 km; puede utilizarse en redes tipo anillo y estrella y actualmente su adquisición e implementación resultan costosas.

ENLACES AÉREOS:

MICROONDAS

En un sistema de microondas se usa el espacio aéreo como medio físico de transmisión. En este medio, la información es transmitida por medio de ondas de radio cuya característica es su longitud corta. Gran parte de los canales que envía llevan señales analógicas, sin embargo, los servicios digitales toman mayor importancia conforme crece la demanda de estos servicios. Estas señales pueden direccionar múltiples canales a múltiples estaciones con un solo enlace, y también pueden establecer enlaces point-to-point (un solo canal, una sola estación). Las estaciones emisoras/receptoras están conformadas por una antena con la forma de plato y por circuitos que interconectan esta antena con el nodo. La transmisión debe establecerse en línea recta, y por esta razón se ve afectada por accidentes geográficos, edificios, mal tiempo, etc. Los sistemas de microondas no solo

proporcionan servicios tan eficientes como los largos *backbones* de coaxial sino que proveen servicios internacionales a través del uso de múltiples repetidores. La longitud de un circuito indiviual tiene un rango de 30 a 6400 km con capacidad de rutear de 60 a 22,000 circuitos

Una ventaja importante de este medio es su capacidad de transportar miles de señales de datos a través de grandes distancias.

ENLACE SATELITAL[TAN89]

La comunicación vía satélite puede considerarse como un gran repetidor de microondas en el cielo. Este dispositivo contiene uno o más *transponder*, cada uno de los cuales escucha una porción del espectro electromagnético, amplifica la señal de origen, y después la retransmite en otra frecuencia, para evitar interferir la siguiente señal origen que está próxima a llegar.

Para prevenir el caos total en el cielo, se han establecido acuerdos internacionales acerca de cuantos y quienes utilizan cuales órbitas y frecuencias. Las bandas de 3.7 a 4.2 GHZ y de 5.925 a 6.425 GHZ han sido diseñadas como frecuencias de telecomunicaciones hacia y desde el satélite respectivamente. Estas bandas, normalmente referidas como 4/6 GHz ya están sobresaturadas.

Las siguientes bandas disponibles están de los 12 a los 14 GHz. Estas bandas aún no se encuentran congestionadas, y en estas frecuencias los satélites pueden estar espaciados a 1° en el plano ecuatorial. Sin embargo, existe otro problema: la lluvia. El agua es excelente absorbente de estas cortas señales de microondas.

Un satélite típico extiende su ancho de banda de 500 MHz sobre una docena de transponders, cada uno de los cuales con 36 MHz de ancho de banda. Cada transponder puede ser usado para codificar una cadena de 50 Mbps, canales de voz digitales u otras combinaciones.

Además, dos transponder pueden usar diferentes polarizaciones de la señal, y de esta forma utilizar el mismo rango de frecuencias sin interferirse mutuamente.

Los satélites de comunicación tienen muchas propiedades que son radicalmente diferentes a los enlaces point-to-point terrestres. Para comenzar, a pesar de que las

señales de y hacia el satélite viajan a la velocidad de la luz (300,000 Km/segundo), el viaje cuenta con un pequeño retardo y un enlace terrestre cuenta con un retardo menor. Otra diferencia radica en el costo de transmisión de un mensaje, que es independiente de la distancia a que se encuentren los satélites. Y finalmente, los anchos de banda que alcanzan los satélites no tienen comparación con los anchos de banda de los enlaces terrestres.

I.5 ARQUITECTURA DE LA RED

La arquitectura en el ámbito computacional, es el arte de determinar las necesidades del usuario para realizar despues los diseños necesarios para satisfacer dichas necesidades de la forma más efectiva dentro de limitantes económicas y tecnológicas. La arquitectura debe incluir consideraciones de ingenieria a fin de que el diseño sea económico y factible; esto es la arquitectura da más énfasis a las necesidades del usuario, mientras que la ingenieria da enfatiza las necesidades del fabricante[MAR89].

OBJETIVOS Y PROPIEDADES

Los objetivos que se pretenden alcanzar con una arquitectura de red son:

- Conectividad. Permitir que *hardware* y/o *software* de diversa índole pueda conectarse y formar un sistema de red unificado.

- Modularidad. Integrar pequeños conjuntos de bloques producidos en serie y de propósito general en una amplia gama de dispositivos de red.

- Facilidad de implementación. Dar una solución general a la comunicación de la red, para que sea fácilmente instalada en una variedad de configuraciones y de soluciones a todos los tipos de usuarios.

- Facilidad de uso. Dotar de facilidades de comunicación a los usuarios de la red, de forma que no se preocupen por la estructura o implementación de la red.

- Confiabilidad. Establecer los mecanismos apropiados para la detección de errores y su corrección, así como implementar las medidas necesarias para proporcionar seguridad al usuario.

- Facilidad de modificación. Permitir a la red evolucionar y establecer los parámetros adecuados para que sea modificada de acuerdo a las necesidades del usuario o a las nuevas tecnologías disponibles.

Por otra parte, una arquitectura de red debe considerar en su estructura las siguientes propiedades [PER92]:

- Ambito. La red debe ser diseñada para soportar un rango amplio de aplicaciones y tecnologías subyacentes

- Escalabilidad. El diseño ideal de la red debe trabajar bien con WANs y también debe ser eficiente con LANs

- Fuerte. Debe estar diseñada para operar de forma contínua, aún si fallan algunos nodos ó enlaces. Para subsanar las fallas no es suficiente la búsqueda de rutas alternas, deben estar presentes otras características, tales como:

a- Barreras. Si se secciona una red con barreras, una interrupción afectará solamente lo que limite dicha barrera.

b- Autoestabilización. Este concepto significa que después de cualquier corrupción en la Base de Datos, sea por malfuncionamiento de Hardware o errores de datos no detectados, la red debe regresar a su estado normal de operación sin intervención humana y dentro de un período razonable de tiempo.

c- Detección de fallas. Esto es, poseer la habilidad de diagnosticarse a sí misma, de forma que la pieza del equipo que está fallando pueda ser identificada.

d- Robustez Bizantina. La robustez bizantina significa que la red pueda trabajar cuando alguno de los nodos presente fallas bizantinas. Una falla Bizantina es aquella que considera que un nodo falla no solo cuando cesa de operar, sino cuando esta funcionando de forma impropia, sea este suceso originado por defectos, fallas de hardware o sabotaje.

- Autoconfiguración. Esto es, la capacidad de la red para agregar automáticamente a su dominio un nuevo nodo que sea conectado a ella y de esta forma reconfigurar su base de información.

- Migración. Es importante que puedan agregarse nuevas características a los nodos de la red sin interrumpir su operación.

PROTOCOLOS

La arquitectura de una red involucra un amplio rango de funciones de comunicación que deben ejecutarse. Estas funciones están organizadas en grupos, los cuales se alojan en las diversas capas funcionales. Esto significa que una arquitectura de red puede definirse en términos de los servicios proporcionados por cada capa y las interfases entre capas. Un aspecto fundamental en cualquier arquitectura de comunicaciones es que uno o más protocolos operen en cada capa de la arquitectura y que dos protocolos semejantes en la misma capa pero en diferentes entidades, cooperen para lograr la función de comunicación.

Existe un conjunto de funciones básicas que ejecutan los protocolos, estas son:

- Segmentación y ensamblado. Cuando una aplicación envía datos en forma de mensajes o de una cadena continua, los protocolos de niveles inferiores pueden necesitar fragmentar los datos en bloques de tamaño pequeño. Este proceso se denomina segmentación. Podemos referir como PDU (Protocol Data Unit - Unidad de datos de protocolo) a cada bloque de datos intercambiado entre dos entidades mediante un protocolo. La contraparte de la segmentación es el ensamblado. Eventualmente, los datos segmentados deben ser ensamblados en mensajes apropiados para las capas superiores.

- Encapsulamiento. A la adición de información de control sobre los datos se le conoce como encapsulamiento. La información de control puede contener cualquiera de estas características :

  - Dirección. La dirección de los nodos emisor y/o receptor.
  - Código de detección de errores. Pequeña clave que indica la validez de la información.

- Control del protocolo. Ayuda a implementar las funciones del protocolo.

• Mulplexión. Es una función que debe realizarse cuando más de una capa de la arquitectura emplea un protocolo connection-oriented. Puede ser utilizado en dos sentidos. Multiplexión hacia arriba, que ocurre cuando múltiples conexiones de capas superiores comparten una sola conexión en la capa inferior. Existe también la multiplexión hacia abajo cuando una sola conexión de capas superiores se construye sobre múltiples conexiones de capas inferiores. Esta técnica puede utilizarse para proporcionar confiabilidad, eficiencia y rendimiento.

Lo anterior nos muestra que los protocolos definen los servicios ofrecidos a través de la interfase de la capa y las reglas que son permitidas en el proceso de ejecución de cada servicio. Los formatos de los paquetes para intercambiar la información a través de las interfases son definidos también como parte de la arquitectura.

ARQUITECTURA EN CAPAS

Existen dos tipos de interfases entre las capas de una red. La primera es la que existe entre las capas de un mismo nodo, esto es, el flujo se da de manera vertical (Figura 1.5). Para ello, los protocolos y formatos de datos describen el proceso a ejecutarse en cada capa y se mandan ejecutar los servicios que prestan las capas, tanto de capas superiores a capas inferiores y viceversa.

La segunda agrupa el conjunto de interfases que existen entre capas semejantes de diferentes entidades, lo cual nos habla de una interfase horizontal. Para ello, los protocolos y formatos de datos se utilizan para coordinar el proceso que se ejecutará por las capas de los nodos emisor y receptor. De esta manera, las capas semejantes realizan un intercambio de mensajes.

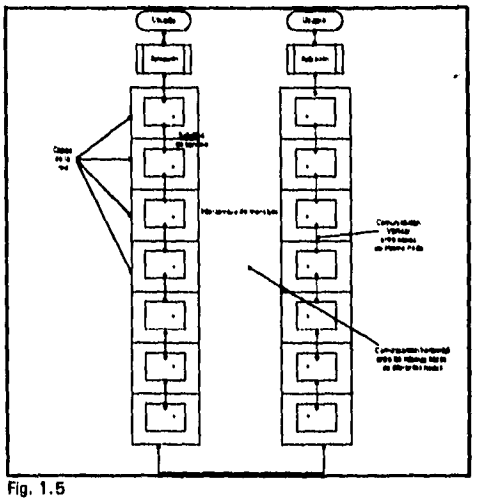


Fig. 1.5

Existe un conjunto de atributos afines a cada arquitectura de red. Estos elementos son [HEN90]:

- Una capa comprende un conjunto de funciones, las cuales proporcionan determinados servicios cuando son activadas por las solicitudes del usuario.
- Cada función tiene un mensaje de control asociado. Estos mensajes realizan un convenio entre un par de capas de dos estaciones diferentes a fin de que la función de transferencia pueda ser ejecutada por la cooperación entre capas sin ambigüedades.
- En la especificación del protocolo de la capa se encuentran definidas las funciones, formatos y parámetros de los mensajes de control, y las acciones a tomar cuando se recibe un mensaje de control o una solicitud de servicio de un usuario.
- La funcionalidad de una capa se presenta a las capas usuario como un conjunto de servicios
- La parte de un protocolo relacionada con la realización de un servicio en particular se denomina elemento de servicio.

- La especificación de los servicios disponibles y de las reglas de acceso a ellos constituyen la definición de los servicios de la capa.
- Esto es, cada capa está definida por un estándard el cual contiene una definición de servicios y una especificación del protocolo.
- Cada capa se relaciona con:
  = Servicio. El conjunto de servicios que ofrece a las capas usuarias.
  = Protocolo. Las funciones que ejecuta en conjunción con la entidad correspondiente en el sistema remoto.
  = Uso de servicios. Los servicios provistos por las capas subordinadas y usados para generar los servicios que presta.

OPERACION DE LA RED

Una red puede operar en dos formas básicas :

SERVICIOS CONNECTION-ORIENTED (ORIENTADOS A LA CONEXIÓN)

Funcionan estableciendo conexiones fijas e intercambiando datos en paquetes discretos. Una o más computadoras intermediarias especializadas conocidas como *switches* (conmutadores), pueden ser utilizadas para transportar cada paquete de datos de un sistema a otro. Su velocidad de operación es baja, típicamente sobre los 64 Kbps, sin embargo, pueden operar sobre cualquier distancia. La técnica de conexión que utilizan estas redes es la conmutación de circuitos (*circuit switching*) la cual da una velocidad de transmisión común a ambos usuarios. Otras características que posee son: establece la ruta antes de comenzar a enviar los datos; la información no puede salirse de una secuencia establecida; si más de un proceso esta utilizando el mismo enlace, los n procesos deberán hablar al mismo sistema remoto; utiliza todo el circuito mientras dura la transmisión y es bueno para la transmisión de un número de paquetes constante. El manejo de paquetes se hace por medio del circuito virtual (*virtual circuit*) el cual considera a toda una relación de paquetes como uno.

SERVICIOS CONECCTIONLESS (NO ORIENTADOS A LA CONEXIÓN)

Su capacidad de transmisión soporta altas velocidades, tipicamente sobre los 10 Mbps. Esto es posible por la naturaleza del medio físico, el cual puede ser instalado entre sistemas de mucha proximidad. Normalmente están disponibles dentro de áreas geográficas localizadas. Su técnica de conexión es la de conmutación de paquetes la cual presenta como características : acceso a una velocidad conveniente para el usuario; inicio inmediato de la transmisión; arribo de paquetes fuera de secuencia; comunicación de diversos procesos con diversos sistemas; se utiliza la red solo cuanto los paquetes se envían y es bueno para "ráfagas" de datos (se conoce a las ráfagas como tráfico repentino y abundante de paquetes, conocido también como *burst traffic*. El manejo de paquetes se realiza mediante los ***datagramas*** que consideran a cada paquete independiente de todos los otros.

Adicional a los elementos antes descritos, existen un conjunto de funciones comunes a los protocolos de WANs relacionadas con los modes de operación de la red. Estas funciones son [WAT91]:

= Direccionamiento

Cualquier paquete que viaja a través de la red debe contener la información suficiente para que ésta pueda enviarlo al destino correcto. También es normal incluir la dirección del nodo origen del paquete, de manera que pueda solicitarse una retransmisión si es necesario.

La naturaleza del esquema de direccionamiento puede tener un efecto considerable en los procesos eficientes de generación de paquetes y en la flexibilidad de la red.

Para el modo de operación connectionless, cada paquete (datagrama) debe contener la dirección completa de su destino. En cambio, el trabajo connection-oriented solo necesita especificar la dirección destino completa una sola vez que es cuando se inicializa la llamada, los paquetes subsecuentes utilizarán en lugar de la dirección destino, el número de canal lógico asignado a la llamada.

- Jerarquía de direcciones

Las direcciones pueden ser jerárquicas o simples. En el direccionamiento simple, a cada nodo existente en la red se le asigna un número único. En el direccionamiento jerárquico cada dirección consiste de un número determinado de campos. Conforme se inspecciona cada campo, el paquete se acerca más a su destino. Si un paquete pasa a través de muchas redes, cada una puede utilizar sus conocimientos para reconocer la dirección del paquete y dirigirlo a su destino. Los nodos de la red no necesitan conocer nada acerca de la estructura o codificación de los campos que conforman la dirección que no se relacionen con ellos. Dentro de cada campo, la ubicación de las direcciones de nodos individuales es responsabilidad del administrador de la red asociada.

- Asignación de nombres

Las direcciones de red, son normalmente cadenas de bits difíciles de recordar. Por ello, una práctica común es proporcionar una lista de n nombres que correspondan a otras n direcciones. Este servicio puede ser accesible en toda la red o de forma local. Esta facilidad de translación es llamada "servicio de búsqueda de nombres" o "servidor de nombres". Una de las ventajas que presenta es que si se mueve un nodo, su nombre podrá conservarse, aún si su dirección ha cambiado.

- Servicios de direccionamiento en el nodo

Las direcciones se utilizan para accesar el servicio de un nodo en particular, sin embargo el nodo puede proporcionar diversos servicios. Si un nodo puede aceptar muchos usuarios remotos, es muy desgastante iniciar muchos servicios de puerto por cada llamada, y por lo tanto el usuario no podría conocer que puertos están disponibles. Para solucionar este problema, la máquina que proporciona el servicio puede recibir llamadas en un puerto conocido por los nodos y después asignar recursos y un nuevo puerto al resto de la conversación cuando se efectúa una solicitud de conexión.

= Ruteo

Aún para una WAN con topología simple, es necesario que existan rutas alternativas, las cuales puedan tomarse para enrutar un paquete y llevarlo a su

destino. Por esta razón se requiere de un algoritmo de ruteo para decidir que ruta tomar. Las metas típicas de este tipo de algoritmos incluyen: evitar la congestión de la red, minimizar costos de funciones como el retraso de paquetes, asegurarse que los paquetes no viajen en círculos dentro de la red, y que los paquetes sean reconocidos y aceptados en sus destinos correctos.

Para el modo de operación connectionless, cada paquete de una estación es ruteado de forma independiente. En contraste, en las llamadas de circuito virtual, solo se inicializa una sola ruta, con la desventaja de que no pueden salirse de la secuencia establecida.

- Ruteo estático

El ruteo estático es sencillo de implementar y eficiente. En esta técnica cada nodo tiene una tabla que indica las mejores rutas a cada destino en un orden de prioridades. Para hacer uso de esta técnica la propuesta más simple es utilizar el enlace con la prioridad más alta, asumiendo que se encuentra disponible. Por otro lado, se obtiene una distribución del tráfico más balanceada si la ruta se asigna de acuerdo a bases estadísticas. El ruteo estático es directo de implementar, mientras la tabla no cambie frecuentemente y pueda administrarse fácilmente.

- Ruteo centralizado

Es similar al ruteo estático, excepto que las tablas son actualizadas periódicamente por un nodo central denominado centro de control de la red. Los nodos informan al centro del estado de sus conexiones locales, de esta manera el centro puede enviar las tablas de rutas las cuales proporcionan una mejor vista de la red como un todo. Una desventaja de este esquema es que es totalmente vulnerable a las fallas del centro de control de la red.

- Ruteo aislado

En este método, cada nodo rutea paquetes de acuerdo con el punto de vista que tenga de la red en ese momento. La propuesta más simple es pasar cada paquete en la ruta que tenga la cola más corta, sin importarle a donde llega ese enlace. A esta técnica se le conoce como el algoritmo de la "papa caliente". Otra posibilidad es utilizar el aprendizaje retrospectivo (backwards learning) donde cada

paquete de datos lleva información adicional acerca del nodo fuente y el número de saltos que efectúa durante el viaje. Lo más aceptable es combinar las técnicas anteriores con algún conocimiento de rutas preferidas, como el que proporciona el ruteo estático.

- Ruteo distribuido

En lugar de tratar de obtener una vista de las condiciones de la red en forma aislada, o de un nodo central, es posible que los nodos intercambien información de ruteo con sus vecinos inmediatos. La información apropiada puede ser un estimado del retraso implicado en alcanzar un nodo en particular. Esto puede obtenerse utilizando paquetes especiales de tipo *echo*, donde el receptor registre marcas de tiempo y lo envíe de regreso tan rápido como sea posible. El esquema de ruteo original de ARPANET fue similar a esto. Una desventaja importante es la vista limitada de algunos nodos, ya que algunos paquetes quedaban atrapados en ciclos formados en la red. En el presente esquema, cada nodo tiene una vista de toda la red incluyendo retrasos entre cada par de nodos. Esta consistencia reduce el número de paquetes ciclados.

- Inundación (Flooding)

En este método todos los paquetes que llegan a un nodo de conmutación son enviados a todos los enlaces que tenga. Esto resulta en un gran número de paquetes replicados con al menos dos problemas : ¿Como puede pararse el proceso? y ¿Como serán descartados los paquetes duplicados en el nodo destino?. Una solución a esto es limitar cada paquete a un número máximo de saltos, de forma que sea descartado cuando se agote su cuenta. Alternativamente, se pueden utilizar secuencias de números, las cuales, cuando se toman junto con la dirección del nodo origen indican duplicados. De cualquier forma, la inundación es práctica solamente donde hay mucha probabilidad de fallas en los nodos o enlaces, como en las aplicaciones militares.

= Control de congestión

En redes de conmutación de circuitos, la congestión resulta en bloqueos cuando se intenta iniciar una llamada. En contraste, la congestión puede manifestarse en una

red de conmutación de paquetes después que una llamada ha sido inicializada, como resultado de un repentino incremento en la carga de tráfico de ese instante. Debido a la naturaleza estadística de los orígenes del tráfico, es normalmente difícil anticipar dicha congestión al momento de iniciar una llamada.

Una de las metas importantes durante el diseño de la red es controlar que no haya congestión, y no poner la capacidad de la red bajo cargas pesadas, ni tampoco permitir que la red llegue a una situación de estancamiento o deadlock donde el tráfico no puede moverse. Dos nodos vecinos pueden entrar en una situación de estancamiento si cada uno de ellos tiene permiso de usar todo el espacio del buffer para encolar paquetes destinados al otro. Si las colas se llenan en ambos nodos, ningún nodo podrá aceptar paquete alguno y se presenta un estancamiento. Una situación similar de estancamiento puede causarse por la falta de espacio en el *buffer* de recepción de un número de nodos que forman un ciclo dentro de la red. Una tercera situación de estancamiento puede ocurrir en un nodo que reensambla subpaquetes. Si en un tiempo dado se requiere un número de subpaquetes para formar paquetes completos pero no hay espacio libre en el buffer de ensamblado, entonces ningún paquete será completado y tampoco se liberará el espacio del buffer.

- Técnicas de control de congestión

La elección de una técnica de control de la congestión es esencialmente un balance entre el monto de memoria del buffer en los nodos y la eficiencia con la cual se utilizan los enlaces de la red. Algunas de estas técnicas son:

- Preasignación de recursos. En el caso de operaciones connection-oriented, es posible asignar un buffer en cada nodo de un circuito virtual en particular cuando se inicia una llamada. Esto es, el origen puede indicar el número de subpaquetes esperado en un paquete, de forma que se reserve un buffer con el espacio suficiente en el receptor advertido.

- Descartar paquetes. Si el número de buffers disponibles en un nodo se saturan, lo más deseable es simplemente descartar los paquetes que lleguen y que están destinados a las largas colas de espera. Los paquetes destinados a colas menores no serían descartados y por lo tanto se asegura que la capacidad total del

nodo es maximizada.

- Restringir el número de paquetes en la subred. Si un nodo tiene permitido transmitir un paquete solamente cuando cuenta con un permiso especial de la red, entonces el número total de paquetes en la red a un tiempo puede restringirse, asegurándose que el número de permisos en existencia es limitado.

- Uso del control de flujo

El control de flujo puede utilizarse para asegurar que los nodos no están inundados de información de sus vecinos inmediatos. Sin embargo normalmente es insuficiente para controlar una congestión amplia de la red y por lo tanto es mejor combinarla con una de las técnicas antes descritas.

- Paquetes de corte

Otra forma de controlar la congestión requiere que cada nodo monitoree el estado de sus colas de recepción y envíe un "paquete de corte" de regreso al origen del tráfico si las colas se vuelven muy largas. Después de la recepción de este paquete, el nodo emisor debe reducir el rango de paquetes que envía al nodo destino.

= Control de flujo

El propósito fundamental del control de flujo es prevenir que un emisor inunde rápidamente con paquetes a un receptor lento. El control de flujo típicamente es implementado utilizando alguna forma de retroalimentación del receptor al emisor tal y como la confirmación positiva (acknowledgment) que indica que un paquete de datos ha sido recibido y que puede enviarse otro. En algunos casos una confirmación puede aplicarse a más de un paquete.

Una aplicación importante del control de flujo se realiza en los protocolos a nivel de la capa de enlace de datos. En dicho contexto, el control de flujo es normalmente combinado con control de errores, que se especifica cuando el receptor no confirma un paquete que ha sido corrompido en su camino. La falla de la confirmación puede causar eventualmente una interrupción, y el emisor enviará el paquete apropiado nuevamente. Alternativamente, el receptor puede enviar una confirmación negativa (unacknowledgment) cuando recibe un paquete corrupto, evitando el retraso asociado con la interrupción y de esta forma mantener la capacidad de la red. Se puede obtener

un incremento en la eficiencia de una conexión en dos sentidos si una confirmación es enviada en la forma piggy-backed, es decir sobre un paquete de datos que viaja en dirección opuesta (del receptor al emisor).

- Protocolos Alto y espera (Stop-and-wait)

La propuesta más simple para controlar el flujo es que el emisor transmita un solo paquete y después espere una confirmación de que fue recibido antes de enviar el siguiente. Este método funciona para nodos vecinos, pero para enlaces más largos no es tan conveniente ya que retarda la transmisión.

- Protocolos de ducto (pipeline) o ventanas deslizantes

Una forma de incrementar la capacidad del protocolo de control de flujo cuando opera sobre un enlace con un retraso largo, es que se envíen muchos paquetes antes que se espere la confirmación del primero. Esto es como llenar un ducto con información entre el emisor y el receptor. En el emisor, un rango de números de secuencia están contenidos en una ventana de transmisión y esto representa los paquetes para los cuales las confirmaciones no han sido recibidas. La ventana se desliza conforme los números de secuencia se confirmen, habilitándo que se envíen más paquetes. El tamaño de la ventana de transmisión está determinado por el número de paquetes que pueden estar en el ducto en un tiempo dado. El receptor también tiene una ventana la cual especifica los números de secuencia de paquetes que el receptor está preparado para aceptar y almacenar. Los protocolos "Regresa-a-N" (go-back-N) y de repetición selectiva (selective repeat) hacen uso de este principio denominado "ventana deslizante".

- Regresa-a-N

Este protocolo utiliza una ventana de recepción del tamaño de un paquete. Si un error es detectado en un paquete, todos los paquetes subsecuentes son descartados por el receptor, hasta que se reciba una nueva versión del paquete. Cuando el emisor se da cuenta que no recibe la confirmación del paquete corrupto, lo vuelve a mandar hasta que reciba la confirmación exitosa del paquete. Mientras esta propuesta tiene la ventaja de que sólo se necesita almacenar un paquete en el receptor al mismo tiempo, tiene la desventaja de que algunos paquetes son retransmitidos

innecesariamente, y por lo tanto se desperdicia el ancho de banda del enlace.

- Repetición selectiva

La característica que distingue al protocolo de repetición selectiva es que la ventana receptora es mas larga y contiene a más de un paquete y puede ser tan grande como la ventana de transmisión. Esto significa que un paquete que esta llegando y tiene cualquier número de secuencia dentro de la ventana de recepción es aceptado, aún si esta fuera de la secuencia. Si un paquete corrupto es recibido, se descarta, pero esto no tiene efecto alguno en la aceptación de paquetes subsecuentes. Cuando el emisor se ha asegurado que algo está mal, simplemente retransmite el paquete apropiado. Esta técnica hace eficiente el uso del ancho de banda del enlace, pero requiere más espacio de buffer en el receptor que el método anterior.

MODELO DE ARQUITECTURA DE RED OSI

Hasta este momento, sólo hemos hablado de los elementos de una arquitectura de red en general. A continuación se presentará el modelo de arquitectura de red adoptado por la CCITT (Consultive Committee on international Telegraphy and Telephony). Este modelo es denominado OSI (Open Systems Interconnection) y fue establecido por ISO (International Standards Organization). El modelo OSI adopta el modelo de capas. Su arquitectura se conforma de 7 capas las cuales son: la capa de aplicación, la capa de presentación, la capa de sesión, la capa de transporte, la capa de red, la capa de enlace de datos y la capa física.

A continuación se presentan descripciones generales de las capas. Cada descripción concluye con una tabla que presenta los servicios y funciones que cada una realiza, sin el propósito de profundizar en cada una de ellas.

CAPA DE APLICACIÓN

La meta del modelo OSI fue realizar la capa de aplicación, ya que ésta presta el servicio de comunicación a los usuarios finales. Las capas inferiores del modelo

existen para soportar y hacer posible las actividades que toman lugar en la capa de aplicación.

En esta capa son ejecutadas todas las aplicaciones de alto nivel independientes del sistema operativo. Esta actividad es coordinada por un conjunto de operaciones incrustadas dentro del sistema operativo local, las cuales realizan la interfase entre el sistema independiente y el sistema de la computadora. Podemos denominar este conjunto de operaciones como agente de aplicación. Un agente de aplicación puede funcionar como un proveedor de servicios de los recursos del sistema local a los usuarios remotos que accesen a él. Esta capa engloba un amplio rango de funciones de aplicación independientes, algunas de las cuales están reconocidas y estandarizádas con ISO. Entre estas se incluyen:

- Transferencia de archivos y operaciones con archivos y directorios
- Servicios de manejo de mensajes (Correo electrónico)
- Transferencia de trabajos y administración de trabajos remotos.

Los servicios y funciones en general establecidos para esta capa se presentan en la siguiente tabla [STA90]:

Servicios
Transferencia de información
Identificación de sistemas (candidatos) que intentan comunicarse
Identificación de la disponibilidad de los candidatos que intentan comunicarse
Establecimiento de las autoridades para comunicarse
Acuerdo de los mecanismos de privacidad (seguridad)
Autentificación de los candidatos a comunicarse
Establecer la metodología para determinar el costo por enlace
Adecuación de recursos
Establecimiento de una calidad de servicio aceptable
Sincronización de las aplicaciones cooperativas

Selección de la disciplina del diálogo, incluyendo los procedimientos de inicialización y liberación
Acuerdo de la responsabilidad en la recuperación de errores
Acuerdo de los procedimientos para el control de la integridad de los datos
Identificación de las limitantes de la sintáxis de los datos
Funciones
Realiza todas aquellas funciones que implican la comunicación entre los sistemas abiertos y que no son realizados por las capas inferiores. Estas funciones se agrupan en 3 grupos: - Elementos del usuario : Es aquella parte de un proceso de aplicación que concierne especificamente a los servicios OSI. - Elementos de servicio de aplicación común : Proporcionan capacidades que son útiles generalmente a un gran número de aplicaciones. Estas capacidades son: Control de asociación y CCR (Comitment, currency and recovery). La primera tiene como propósito soportar el establecimiento, mantenimiento y término de asociaciones de aplicación. El CCR es un servicio que coordina las interacciones múltiparte en forma infalible, aún en el caso de caídas repetidas del sistema. Todas las aplicaciones que requieren alto grado de confiabilidad utilizan CCR. - Elementos específicos del servicio de aplicación : Aporta las capacidades requeridas pare satisfacer las necesidades particulares de aplicaciones específicas

De todo esto concluimos que la capa de aplicación se encarga de proporcionar servicios, cubriendo el rango de aplicaciones orientadas al usuario final. La actividad de la capa de aplicación involucra la transferencia de la información sobre OSI entre los diversos sistemas de computación cooperativos.

CAPA DE PRESENTACIÓN

Su función es establecer una representación común de la información de una aplicación mientras ésta se encuentre transitando entre dos sistemas de cómputo cooperativos. Entre las diferencias que tienen que salvar se encuentran : la traducción de códigos, conversión de datos, compresión y expansión de datos o representación de caracteres. Por ejemplo, para lograr la representación correcta de datos entre dos máquinas que utilizan diferentes códigos, la capa debe negociar entre los dos sistemas para establecer una forma de representación común de la información que utilicen

mientras dicha información está transitando entre ellos.

Existen dos aspectos fundamentales de representación relacionados con la capa de presentación [WAT91] :

- Los datos que serán transferidos entre las entidades de aplicación. Esto es, la información del usuario final
- La estructura de datos que las entidades de aplicación refieren en su comunicación. Esto es la estructura de la unidad de datos del servicio de aplicación (Application service data unit ASDU).

La siguiente tabla presenta de forma general los servicios y funciones con los que cumple la capa de presentación [STA90]:

Servicios
Transformación de sintáxis
Selección de sintáxis
Funciones
Solicitar que se establezca una sesión
Raalizar la transferencia de datos
Efectuar la negociación y renegociación de sintáxis
Transformar la sintáxis, incluyendo transformación de datos, formateo y transformaciones de propósito especial
Solicitar que finalice una sesión

El propósito de la capa de presentación es asegurarse que los sistemas finales puedan comunicarse exitosamente, aún si utilizan diferentes esquemas de representación. Esto se realiza proporcionando una representación común para utilizarla en la comunicación y convirtiendo la información de la representación local a esa representación común.

CAPA DE SESIÓN

La capa de sesión se ocupa del área que existe entre las capas superiores orientadas a la aplicación y el ambiente de comunicación de datos en tiempo real. Presta servicios de administración y control del flujo de datos entre dos sistemas.

El propósito de la capa de sesión es proporcionar las formas para la cooperación entre entidades a nivel de presentación para organizar y sincronizar su diálogo y para administrar el intercambio de datos. Para lograr esto, la capa de sesión establece una conexión de sesión e impone una estructura para la interacción ó diálogo entre dos sesiones de usuario.

La siguiente tabla nos muestra de manera general, los servicios y funciones de la capa de sesión [STA90]:

Servicios
Establecimiento de una conexión de sesión entre entidades de presentación
Liberar la conexión de sesión en forma ordenada y sin pérdida de datos
Efectuar el intercambio de las unidades de datos de servicio (Service Data Units SDU)
Intercambiar de forma expedita los datos
Efectuar una administración interactiva; simultánea en dos sentidos, alterna en dos sentidos ó una sola interacción
Sincronizar la conexión de sesión permitiendo a las entidades del nivel de presentación definir puntos de sincronización y resincronizar esos puntos
Realizar un reporte de excepciones que notifique a las entidades de presentación
Funciones
Efectuar un mapeo uno-a-uno de la conexión de las entidades de sesión a las correspondienres entidades de transporte
Controlar el flujo de la conexión de sesión
Transferir datos de forma expedita
Recuperar la conexión de sesión después de una falla
Liberar la conexión de sesión

Administrar las actividades relacionadas con la capa de sesión

Los servicios de administración de la capa de sesión permiten inicializar, interrumpir, abandonar o reiniciar una transmisión bajo la instrucción de la capa de aplicación. El uso de estos servicios permite a una aplicación ordenar y administrar su trabajo, esto es, una actividad puede ser interrumpida para permitir que otra actividad más urgente tome su lugar y al terminar ésta última, reiniciar nuevamente.

CAPA DE TRANSPORTE

La capa de transporte permite la transferencia transparente de los datos entre entidades que están en sesión. Libera a las entidades de los aspectos relacionados con la forma detallada con la cual se logra una transferencia confiable y efectiva de datos. Todos los protocolos en esta capa realizan la conexión *end-to-end* entre las entidades de transporte de los sistemas finales.

La tabla que contiene los servicios y funciones generales que esta capa proporciona se presenta a continuación [STA90]:

Servicios
Establecer la conexión de transporte (entre las capas de transporte)
Realizar la transferencia de datos
Liberar la conexión de transporte
Funciones
Rastrear las direcciones de transporte en las direcciones de red. Las direcciones de transporte son denominadas puntos de acceso a servicios de transporte (Transport service access points TSAPs) y las direcciones de red se conocen como puntos de acceso a servicios de red (Network service access points NSAPs)
Ramificar las conexiones de transporte en conexiones de red
Establecer y liberar las conexiones de transporte
Controlar la secuencia end-to-end de conexiones individuales

Efectuar la detección de errores end-to-end y cualquier monitoreo necesario para asegurar la calidad del servicio
Establecer los mecanismos para la recuperación de errores end-to-end
Realizar la segmentación, y concatenación end-to-end
Controlar el flujo end-to-end en conexiones individuales
Ejercer las funciones de supervisión
Transferir de forma expedita las unidades de datos para el servicio de transporte (Transport service data units TSDU)

El servicio de transporte proporciona la forma para establecer, mantener y liberar conexiones de transporte entre dos entidades de sesión. Dos entidades en sesión en diferentes sistemas finales pueden establecer más de una conexión de transporte entre ellas.

Para entender la función de la capa de transporte debemos hablar un poco de las capas inferiores que se relacionan más con la transmisión de datos sobre el medio físico. La comunicación entre medios, así como las técnicas de transmisión difieren en aspectos fundamentales. A la conjunción del medio físico con una técnica específica de comunicación se le denomina subred. Esto nos indica que a pesar de que cada subred define los mismos servicios, la calidad de estos difiere de una a otra. La calidad de servicio es un factor de capacidad importante de la subred, capacidad que se aprecia mejor al momento de la detección y corrección de errores de transmisión. Algunas subredes están diseñadas para ofrecer buenos servicios de detección y corrección de errores, otras, no son tan eficientes en esta actividad. Por esto, una función importante de la capa de transporte es realizar el manejo de errores de los datos transmitidos sobre las subredes que no fueron diseñadas para un intercambio confiable de datos. Aqui, la capa de transporte presta a la capa de sesión un servicio confiable de transmisión, sin tomar en cuenta la naturaleza de la subred existente[HEN90]. La independencia del tipo, calidad y número de subredes involucradas en la comunicación entre sistemas es parte de los servicios ofrecidos por la capa de transporte.

Un punto final acerca de la subred nos dice que "..de la forma en la cual las tres capas inferiores sean implementadas, dependerá el tipo de red y podrán diferir considerablemente, por ejemplo, entre una WAN y una LAN.."[WAT91].

CAPA DE RED

Esta capa define las funciones para establecer, mantener y terminar conexiones de red, y permite el intercambio de las unidades de datos del servicio de red (Network service data units NSDU) entre entidades de transporte. Independiza a las entidades de transporte de los detalles de la o las subredes, incluyendo aspectos de ruteo y funciones de transmisión requeridas para enviar unidades de datos a través de la subred.

Las funciones de la capa de red son necesarias para soportar los servicios ofrecidos por la capa de transporte.

Estas funciones y los servicios que ofrece la capa están comprendidas en el siguiente cuadro [STA90]:

Servicios
Direcciones de red que identifican de manera única las entidades de transporte
Conexiones de red entre entidades de transporte
Identificadores de puntos finales en la conexión de red
Transferencia de unidades de servicio (SDU, Service data unit) de red
Parámetros de calidad de servicio que son opcionalmente seleccionables
Notificación de errores no recuperables
Secuenciamiento y entrega ordenada de paquetes
Control de flujo de las unidades de servicio
Transferencia expedita de unidades de servicio de red, manejo expedido de las unidades de servicio
Reinicialización, esto es, descartar las SDU y la conexión lógica se reinicializa
Liberar (Release) la conexión de red y notificar a la entidad de transporte del otro sistema

Funciones
Ruteo y transmisión. Sistemas abiertos intermedios pueden proveer la transmisión; se determina entonces una ruta a través de estos
Conexiónes de red
Multiplexión de conexiones de red en una conexión de enlace de datos o de subred
Segmentación de las unidades de servicio de red en bloques para facilitar la transferencia
Detección de errores, notificación de los mismos y mecanismos adicionales
Recuperación de errores detectados
Secuenciamiento de paquetes
Control de flujo entre las entidades de red
Transferencia de datos expedita
Reinicialización
Selección de servicio, es decir, asegurarse que el servicio sea el mismo en cada punto final de la conexión a nivel capa de red entre redes distintas
Administración de las actividades relacionadas con la capa de red

CAPA DE ENLACE DE DATOS

La capa de enlace de datos debe coincidir con los requerimientos del medio de comunicación y los requerimientos del usuario [STA90]. Su propósito primario es establecer una forma confiable de transmitir los datos a través del enlace físico. Además proporcionalos mecanismos funcionales y los procedimientos para establecer, mantener y liberar un conexión de enlace de datos entre entidades de red.

Existe para esta capa una topología, que basicamente se refiere a el arreglo físico de las estaciones en el enlace. De esta forma existen los enlaces *point-to-point* cuando solo hay dos estaciones y *multipoint* cuando son más de dos estaciones.

Otra característica del enlace se refiere a la dirección y tiempo del flujo de señales. De este modo tenemos [STA90]:

- La transmisión simplex cuando el flujo corre en una dirección;
- Half-duplex cuando el enlace puede enviar y transmitir pero no a un tiempo;
- La transmisión full-duplex que permite enviar y transmitir al mismo tiempo.

Un compendio de las funciones y servicios proporcionados por esta capa se presenta en la siguiente tabla [STA90]:

Servicios
Conexión de las entidades de red
Intercambio de SDUs de enlace de datos
Identificadores de puntos finales de la conexión de enlace de datos
Secuenciamiento y entrega ordenada de unidades de servicios
Notificación de errores irrecuperables
Control de flujo
Parámetros de calidad de servicio
Funciones
Establecer y terminar la conexión de enlace de datos
Planear el enlace de datos de SDUs
Multiplexar la conexión de enlace de datos sobre diversas conexiones físicas
Delimitar y sincronización de los paquetes de bits
Controlar la secuencia de paquetes
Detectar errores de transmisión, de formato y de operación
Realizar la recuperación de errores mediante la retransmisión de PDUs
Controlar el flujo entre capas de enlace de datos de dos o más entidades
Identificar e intercambiar parámetros entre entidades
Controlar la interconexión entre un circuitos de datos proporcionado para el control de la capa de red
Administrar las actividades relacionadas con la capa de enlace de datos

CAPA FÍSICA

La capa física proporciona los medios mecánicos, eléctricos, funcionales y procedimentales para activar, mantener y terminar el enlace físico entre dos sistemas.

El término mécanico se refiere a las propiedades físicas de la interfase con un medio de transmisión (tamaño, configuración).

Eléctrico se refiere a la representación en bits (niveles de voltaje) en el medio y los rangos de transmisión de bits.

Funcionales nos indica las actividades ejecutadas por elementos individuales de la interfase física entre el sistema y el medio de transmisión.

Procedimentales nos especifica el protocolo por el cual las cadenas de bits son intercambiadas sobre el medio físico.

La tabla siguiente presenta los servicios y funciones que realiza la capa física [STA90]:

Servicios
Conexión física de los sistemas a través del medio de transmisión
SDU físico que consiste de un solo bit
Puntos finales de una conexión física que se utilizan para identificar un punto físico único y asignarlo al medio de transmisión
Identificación del circuito de datos o ruta física de comunicación para referencia de capas superiores
Secuenciamiento y entrega de bits en el orden que fueron presentados
Notificación en caso de error a las entidades de enlace de datos
Parámetro de calidad del servicio que caracteriza la calidad de la ruta de transmisión
Funciones
Activar y terminar la conexión física, con ello efectúa el control del enlace físico
Transmisión física síncrona o asíncrona de los bits o SDUs
Administración de las actividades relacionadas con la capa física

I.6 ARQUITECTURA DE REDES WAN

El modelo OSI no indica que protocolos deben utilizarse para proporcionar los servicios a la red. Actualmente, las redes públicas y algunas redes privadas de conmutación de paquetes hacen uso de la recomendación X.25 de la CCITT. Esta recomendación establece un servicio de red del tipo connection-oriented. X.25 cuenta con una descripción de las tres capas inferiores del modelo OSI (la capa de red, la capa de enlace de datos y la capa física), esto es, define la subred.

La descripción de X.25 tiene como fundamento el enlace de datos y las reglas para enviar y recibir datos entre dos o más ubicaciones localizadas en una red. Las partes básicas del enlace son [IBM95]:

- El DTE (Data Terminal Equipment - Equipo terminal de datos). La parte del enlace de datos que envía y recibe datos y realiza la función de control de la comunicación de datos de acuerdo a los protocolos
- El DCE (Data Circuit-terminating Equipment - Equipo de datos de fin del circuito). Es el equipo instalado por el usuario que proporciona todas las funciones necesarias para establecer, mantener y finalizar una conexión, y la conversión de señales y codificación entre el DTE (Data Terminal Equipment) y la línea
- La línea, que está conformada por el medio físico de transmisión

Todas las capas de X.25 especifican como realizar la conexión de DTEs mediante los DCE. A continuación se presenta la descripción que X.25 hace de las capas de red, enlace de datos y física.

NIVEL 3 CAPA DE RED [WAT91]

En X.25 nivel 3, la capa de red proporciona un servicio de red a la capa de transporte. Este servicio transfiere los datos de forma transparente ya que utiliza un enlace end-to-end entre los usuarios del servicio, haciéndolo parecer invisible al usuario. Ofrece direccionamiento no ambiguo y la capacidad de selección de la calidad del servicio. El servicio determina el grado de calidad que se acordará entre las

conexiones para que puedan ser inicializadas o desconectadas. Esto ofrece control de flujo y, opcionalmente, transferencia expedita (la cual permite a los datos alcanzar otros datos que aún se encuentran encolados) y confirmación del receptor. X.25 nivel 3 indica como deben ser intercambiados los paquetes entre un DTE y DCE. Cada paquete esta contenido dentro del campo de información de un *frame* de información X.25 nivel 2.

PROTOCOLO DTE-DCE X.25

Este protocolo especifica el servicio de circuito. El servicio de circuito de X.25 nos permite utilizar dos tipos de circuitos: los virtuales y los permanentes. Un circuito virtual es el que se establece dinámicamente utilizando llamadas a procedimientos para inicializarlo y limpiarlo. Un circuito permanente es el que se encuentra asignado permanentemente. En él la transferencia de datos ocurre como en el circuito virtual, pero no requiere de inicializarse y limpiarse.

La interfase DTE-DCE es asimétrica, esto es, sólo la información de los protocolos de capa tres es transferida en forma end-to-end entre los suscritos DTEs. Gran parte de la información operativa como control de flujo y confirmaciones sólo tienen significado local.

La forma en la cual los datos son encapsulados es interesante. El DTE emisor debe fraccionar sus datos en unidades de una longitud máxima. X.25 especifica que la red debe soportar un campo de datos de usuario de al menos 128 *octetos* de longitud. Por esta razón, la red puede elegir algún otro tamaño máximo de campo en el rango de 16 a 4096 octetos. El DTE construye paquetes de control y encapsula los datos en paquetes de datos. Ya formados, son transmitidos al DCE. De esta forma, el paquete es encapsulado en un frame de la capa 2. El DCE quita los códigos de control de la capa 2 y encapsula el frame de acuerdo al protocolo interno.

NIVEL 2 CAPA DE ENLACE DE DATOS [WAT91]

La función básica de la capa es dividir la información en frames para obtener las ventajas de la multiplexión en la conmutación de paquetes. Cada frame incluye un

número de secuencia y bits de verificación, de manera que puedan llevarse a cabo los procedimientos de control de flujo y detección y recuperación de errores.

La capa de enlace de datos de X.25 esta basada en el procedimiento de control de enlace de datos de ISO denominado HDLC (High Data Link Control - Control de enlace de datos de alto nivel). HDLC es un protocolo orientado a bit y esta fuertemente relacionado con SDLC (Synchronous data link control - Control de enlace de datos síncrono) de IBM. HDLC es una familia de protocolos que soportan diversos modos que incluyen el *multipoint polling*, el enlace point-to-point tipo maestro-esclavo, y el enlace entre semejantes tipo point-to-point. Las versiones están diferenciadas por el procedimiento de acceso al enlace (Link Access Procedure LAP). El nivel 2 de X.25 puede usar LAP o LAPB (link access procedure balanced. Procedimiento de acceso al enlace balanceado), pero LAPB es preferido. LABP permite utilizar de uno a múltiples enlaces físicos entre un DTE y un DCE.

CARACTERÍSTICAS BÁSICAS DE HDLC[STA90]

Para satisfacer las necesidades de independencia de código, alta eficiencia y confiabilidad, HDLC define: tres tipos de estaciones, dos configuraciones para enlaces y tres modos de operación para transferencia de datos.

Los tres tipos de estaciones son :

- Estación primaria : Tiene la responsabilidad de controlar la operación del enlace. Los frames que utiliza se denominan comandos.
- Estación secundaria : Opera bajo el control de la estación primaria. Los frames que utiliza se denominan respuestas. La estación primaria mantiene un enlace lógico separado con cada estación secundaria en la línea.
- Estación combinada : Combina las características de las dos primeras. Hace uso de comandos y respuestas

Los dos tipos de configuraciones para enlaces son :

- Configuración no balanceada. Utilizada para operar en modo point-to-point y multipoint. Esta configuración consiste de una estación primaria y una o más

secundarias y soporta las transmisiones full-duplex y half-duplex.

- Configuración balanceada. Utilizada solamente para operar en modo point-to-point. Consiste de dos estaciones combinadas y soporta las transmisiones full-duplex y half-duplex.

Finalmente, los tres modos de operación para transferencia de datos son:

- Modo de respuesta normal. Corresponde al de una configuración no balanceada. La estación primaria puede iniciar la transferencia de datos hacia una estación secundaria, pero una estación secundaria solamente puede transmitir datos en respuesta a un comando de la estación primaria
- Modo balanceado asíncrono (Asynchronous Balanced Mode ABM). Se relaciona con una configuración balanceada. Cada estación combinada puede iniciar la transmisión sin recibir el permiso de la otra estación combinada.
- Modo de respuesta asíncrona (Asynchronous Response Mode ARM). Se utiliza en configuraciones no balanceadas. En este modo, la estación secundaria puede iniciar la transmisión sin permiso explícito de la estación primaria, sin embargo, la estación primaria aún es responsable de la línea, incluyendo la inicialización, recuperación de errores y desconexión lógica.

NIVEL 1 CAPA FISICA

La capa física está relacionada con las características eléctricas y mecánicas del enlace. X.25 especifica dos protocolos diferentes para la capa física - uno para los circuitos digitales y otro para los circuitos analógicos. Estos se encuentran descritos en las recomendaciones X.21 y X.2bis de la CCITT respectivamente.

X.21 (CIRCUITOS DIGITALES)

El estándar X.21 define los nombres y funciones de ocho circuitos de intercambio (líneas de señalÇ en el enlace. Estos circuitos se denominan :

-T- Transmite información del usuario del DTE

-C- Transmite información de control del DTE

-R- Transmite información del usuario del DCE

-I- Transmite información de control del DCE

-S- Establece la coordinación de tiempo de los bits

-B- Establece la coordinación de tiempo de bytes

-Ga-Referencia a tierra

-G- Tierra de protección

X.21 permite la operación point-to-point y la conmutación de circuitos. Para lograr la operación point-to-point, el estado por omisión de la línea es el estado de transferencia de datos. Como los datos son transmitidos transparentemente, puede utilizarse cualquier control de enlace síncrono, de forma que el procedimiento de la capa física no restrinja a protocolos de capas superiores.

Para operar con conmutación de circuitos, debe ocurrir una secuencia de eventos para poder inicializar y limpiar una llamada en la línea. La llamada puede venir de cualquier punto de enlace e involucrar procedimientos sencillos. X.21 con conmutación de circuitos ofrece alta confiabilidad y establece las llamadas rápidamente.

X.21 BIS (CIRCUITOS ANALÓGICOS)

Esta especificación cuenta con las siguientes características :

- Especificación eléctrica. Define el envío de señales entre un DTE y un DCE.

- Especificación mecánica. Define los conectores físicos y sus especificaciones.

- Especificación funcional. Los circuitos de intercambio que define X.21 bis pueden agruparse en categorías de datos, control, coordinación de tiempo y tierra. Hay un circuito de datos en cada dirección para que sea posible la operación en modo full-duplex.

Existen definidos catorce circuitos de control

Los ocho primeros se relacionan con la transmisión de datos sobre el canal primario. De estos, seis son utilizados para transmitir asíncronamente y 2 más son utilizados para la transmisión síncrona.

Los siguientes tres circuitos controlan el uso del canal secundario.

El último grupo realiza una evaluación *loopback* que localiza y aisla fallas.

I.7 ARQUITECTURA DE REDES LAN

Los estándares definidos para redes de área local se ajustan al modelo OSI. En particular, existe un conjunto de estándares determinados por la IEEE conocidos como el PROYECTO 802. Estos se refieren únicamente a las capas contenidas en la subred. Las reglas generales que se siguieron para su diseño son [MAR89]:

- Convergente con el HDLC (High-Level Data Link Control). Esto es, que haya independencia del estándar con respecto a la operación de protocolos en capas superiores.
- Transparente a la topología
- Transparente a la velocidad de transmisión
- Transparente al medio

El formato del paquete y las convenciones en la dirección son comunes en todos los tipos y niveles de los protocoles del estándar IEEE 802. Los elementos comunes del paquete de comunicación del estándar 802 son:

- Un campo de información
- Un campo de control
- Marcas de inicio y fin
- Campos de dirección.

ENLACE DE DATOS

La capa de enlace de datos se subdividió en dos subcapas [MAR89]:

♦ SUBCAPA LLC 802.2 (LOGICAL LINK CONTROL- CONTROL DE ENLACE LÓGICO)

- El control de enlace lógico es responsable de las funciones de enlace de datos independiente del medio y permite que las capas superiores accesen los servicios de una red sin preguntar como está implementada la red. Acordes con la metodología OSI de protocolos entre capas múltiples, la estructura del paquete se torna más compleja conforme éste avanza hacia las capas capas inferiores como LLC, MAC (Medium Access Control) y la capa física.

La subcapa LLC es común a los diversos métodos de acceso al medio. Al llegar un mensaje a la LLC, ésta adiciona al paquete un encabezado que contiene un DSAP (Destination Service Access Point - Punto de acceso al servicio destino), un SSAP (Source Service Access Point - Punto de acceso al servicio origen) y un byte de control.

La característica clave que señala la diferencia entre los estándares LLC y HDLC, es que LLC está diseñado para operar sobre un enlace semejante multipunto. En este caso, existen múltiples dispositivos asignados al medio de transmisión, y todos ellos están capacitados para iniciar la transmisión. Aquí, no existen dispositivos primarios en el enlace. Para poder cumplir con esta característica, cada unidad de datos transmitida incluye las direcciones del emisor y del receptor, y no solamente la de este último.

La interfase de LLC presta dos tipos de servicio. El modo 1 ó servicio connectionless, que permite la transmisión entre estaciones sin la garantía de entregar los paquetes; y el modo 2 o servicio connection-oriented, que se basa en establecer una sesión entre dos estaciones y proporciona una comunicación confiable, con la confirmación respectiva de la recepción del mensaje.

Con estos servicios, LLC puede realizar estas tres combinaciones : servicio connectionless sin confirmación (Unacknowledged connectionless service); servicio connection-oriented (connection-oriented service) y servicio connectionless con confirmación (acknowledgment connectionless service).

♦ SUBCAPA MAC (MEDIUM ACCESS CONTROL - CONTROL DE ACCCESO AL MEDIO)

- Su función se relaciona con los métodos de control de acceso que determinan como controlar el uso del medio de transmisión físico. Las interfaces que se presentan en esta capa son :

a) La interface entre MAC y LLC. Incluye mecanismos para la transmisión y recepción de paquetes y para la operación del estado de la información para uso de los procedimientos de recuperación de errores de capas superiores.
b) La interfase entre MAC y la capa física. Incluye señales para la transmisión y solución de colisiones, procesos para pasar corrientes de bits separadas y una función de espera para coordinar.

A la MAC le concierne primordialmente la definición de reglas cuyo objetivo es dar capacidad a las estaciones para compartir el medio de transmisión. Existen cuatro funciones básicas para esta subcapa:

- Administración de acceso al medio. Las reglas o procedimientos utilizados por las estaciones de la red para controlar el acceso compartido al medio de transmisión.
- Generación de frames. La adición de encabezados y marcas con información necesaria para identificar el inicio y fin de un mensaje, para sincronizar al emisor y al receptor, rutear el mensaje y habilitar la detección de errores.
- Direccionamiento. La determinación de las direcciones de red apropiadas a fin de identificar dispositivos involucrados en el envío y recepción de mensajes.
- Detección de errores. La verificación se realiza para asegurar que un mensaje ha sido recibido y transmitido correctamente.

El proyecto 802 definió algunos estándares que integran la subcapa MAC y la capa física. Estos estándares son :

ESTANDAR 802.3 CSMA/CD (CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION)

CSMA/CD es un método de acceso aleatorio. Bajo CSMA/CD, la estación debe "escuchar" el medio de transmisión antes de iniciar la transmisión a fin de determinar si alguna estación está transmitiendo en ese momento un mensaje. Si el medio de transmisión esta "callado" (esto es, ninguna estación está transmitiendo) la estación manda su mensaje. Cuando un mensaje es transmitido, viaja por todas la estaciones de la red. Cuando el mensaje llega a una estación, ésta examina la dirección asociada con el mensaje. Si la dirección corresponde a dicha estación, entonces ésta recibirá y procesará el mensaje. Ocasionalmente sucede que dos estaciones mandan sus mensajes simultáneamente, resultando lo que se conoce como colisión. Para manejar estas situaciones, cada estación transmisora espera por un período de tiempo determinado aleatoriamente, y después intenta retransmitir de nuevo.

El estándar 802.3 define un modelo que comprende seis funciones. Tres de estas funciones están asociadas con la transmisión de datos y tres funciones paralelas se refieren a la recepción de datos.

Las funciones de encapsulación/decapsulación y administración de acceso al medio son ejecutadas por la subcapa MAC. Las funciones de codificación/decodificación de datos y asignación de la estación al medio físico son ejecutadas por la capa física, que opera debajo de MAC.

La función de Encapsulación de datos la aplica la estación emisora cuando adiciona información al principio y fin del mensaje a transmitir. Esta información se utiliza para:

- Sincronizar la estación receptora con la señal
- Delimitar el inicio y fin del mensaje
- Identificar las direcciones de las estaciones emisora y receptora.
- Detectar errores de transmisión

Cuando se recibe un frame, la función de decapsulamiento se realiza en la estación receptora que es responsable de reconocer la dirección destino, determinando si corresponde a su dirección, ejecutando la verificación de errores y despues

removiendo la información de control que fue adicionada por la función de encapsulamiento en la estación emisora, antes de pasar el frame hacia capas superiores.

Para la administración del acceso al medio, la estación emisora es responsable de determinar cuando está disponible el medio de transmisión, para usarlo e iniciar la transmisión cuando sea posible. También determina las acciones a tomar cuando se detecta una colisión y cuando se intenta retransmitir. En la estación receptora, la administración realiza pruebas de validación del frame antes de pasarlo por la función de decapsulación.

La codificación/decodificación de datos, se realiza en la capa física y es responsable de transladar los bits que están siendo transmitidos en señales eléctricas propias para enviarse a través del medio de transmisión. Para CSMA/CD, la decodificación se realiza con el método de Fase Manchester, el cual translada cadenas de bits en señales eléctricas. Cuando se recibe la señal, la decodificación de datos la translada nuevamente de señales eléctricas a las cadenas de bits que dichas señales representan. La decodificación de datos también es responsable de escuchar el medio de transmisión y de notificar a la administración cuando el medio se encuentre libre y/u ocupado y cuando detecta una colisión. Adicional a las funciones de codificación/decodificación, la capa física ejecuta funciones relacionadas con la asignación de una estación a un medio físico de transmisión en particular. Estas funciones son realizadas generalmente por el transciever.

ESTANDAR 802.4 TOKEN BUS

El estándard 802.4 establece un control de forma centralizada. Sus funciones primarias son:

= Interfase con LLC. La MAC debe recibir las unidades de datos de la subcapa LLC y prepararlas para la transmisión. En el lado receptor, la subcapa MAC debe recibir las unidades de datos que han sido transmitidas a través de la red y las pasa a LLC.

= Manejo del token. Incluye pasar el token de una estación a la siguiente, reconocer el token cuando se recibe y opcionalmente, dar prioridad a las unidades de datos. El token es una corta unidad de datos de control que controla el aceso al medio de transmisión. El token representa el derecho de transmitir, ya que cuando una estación posee el token, puede transmitir por un período de tiempo. Cuando ha finalizado la transmisión o se agoto el tiempo, la estación transmitirá el token a la siguiente estación. Si no hubiera mensaje que transmitir, el token pasará inmediatamente a la siguiente estación.

La arquitectura de token bus puede describirse como la combinación de un anillo lógico en un bus físico. Como la unidad de datos cuenta con la dirección de la estación, la estación acepta y procesa solamente los datos que tienen su dirección. Como una sola estación posee el token, no se puede presentar el fenómeno de colisión.

= Mantenimiento del Anillo. El anillo lógico que forman las estaciones, necesita ser inicializado cuando la red es inicializada y modificado cuando se adicionan o eliminan estaciones. El control de la operación del anillo está determinado por el conocimiento que cada estación tiene de las direcciones de su predecesor y sucesor.

= Detección y recuperación de fallas. El estándard 802.4 también define los métodos de detección y corrección de determinadas condiciones de error. Algunas de estas condiciones de error son:

- Presencia de múltiples tokens en el anillo
- Inactividad de una estación cuando posee el token
- Pérdida del token en el anillo

= Envío y recepción de frames. En una estación emisora, las unidades de datos deben pasar de la subcapa MAC a la capa física para transmitirse sobre la red; en una estación receptora, las unidades de datos deben recibirse por la capa física a MAC. Estas funciones incluyen la adición y substracción de la información de control necesaria para formar las unidades de datos en los formatos de token bus.

= Tipos de transmisión. El estándard token bus utiliza tres tipos de transmisión diferentes. Para cada tipo de transmisión, existe una especificación para la capa física

y una descripción del medio físico de transmisión. Las especificaciones de la capa física incluyen descripciones detalladas de sus características funcional, eléctrica y física, así como especificaciones de ambiente relacionadas con la seguridad, ambiente eléctrico y electromagnético, temperatura, humedad y elementos reguladores.

Las descripciones del medio de transmisión especifican también características funcionales, eléctricas y físicas y consideraciones ambientales, así como aspectos relacionados con el retardo en la ruta de transmisión y en algunos casos, consideraciones del tamaño de la red.

Los tres tipos de transmisión definidos son : codificación con cambio de frecuencia fase-contínua canal-simple (single-channel phase-continous FSK Frecuency-shift keying) que utiliza la transmisión baseband y modula la frecuencia con FSK; codificación con cambio de frecuencia fase-coherente canal-simple (single-channel phase-coherent FSK) que también utiliza la transmisión baseband; y finalmente la transmisión Broadband que utiliza la ténica de modulación denominada codificación con cambio de fase/amplitud modulada multinivel duobinario (multilevel duobinary AM/PSK Phase-shift keying).

ESTANDAR 802.5 TOKEN RING

Con el estándard token ring, una unidad de control denominada token se pasa de una estación a la siguiente a través de un anillo físico. Cuando una estación recibe el token, tiene el permiso de transmitir por un período de tiempo. Una estación que transmite unidades de datos es responsable de removerlos del anillo y después mandar el token libre a la siguiente estación. Las estaciones alrededor del anillo que reciben un token con datos tienen la capacidad de colocar bits en él, indicando donde fue reconocido el paquete, donde fue copiado o si se detecto algún error.

El estándar token ring adiciona a las funciones normales del token otras dos funciones de solución de fallas. Estas funciones dependen de dos condiciones de error que pueden afectar seriamente la operación del anillo : la pérdida del token o un token continuamente ocupado (sin desocupar). La forma adoptada para detectar y corregir estas condiciones es tener una de las estaciones funcionando como monitor activo.

Este monitor, debe vigilar continuamente la red. Si pasa un período predeterminado de tiempo sin que se detecte token alguno, el monitor asume que el token se ha perdido y genera un nuevo token. Para verificar si un token se encuentra continuamente ocupado, el monitor coloca un bit monitor en el token ocupado cuando pase con él. Si el token ocupado regresa a la estación monitor con el bit de monitor aún encendido, el monitor deduce que la estación origen está fallando en su función de remover los datos del token, por lo que el monitor cambia el token por un token libre y lo envía a la siguiente estación.

Todas las demás estaciones de la red actúan como monitores pasivos que supervisan la operación del monitor activo. Si por alguna razón el monitor activo falla, el monitor pasivo utiliza un procedimiento de resolución por concatenación para determinar que estación debe tomar el papel de monitor activo.

El control de acceso de token ring puede operar sobre bases prioritarias y no prioritarias. Cuando el esquema de prioridad no se implementa, una estación puede enviar mensajes cuando reciba un token libre. Cuando se implementa el esquema de prioridad, tres bits de cada unidad de datos se usan para representar su estado de prioridad. Cuando la estación recibe un token libre, compara el valor de la prioridad del token contra la prioridad de la unidad de datos a transmitir. Si la prioridad es mayor o igual se transmite. Si es menor, no se transmite.

El paquete de transmisión del token ring contiene un delimitador inicial, control de acceso, campos de dirección, verificador de secuencia y delimitador final. Este estándar codifica los datos con el método Manchester diferencial.

OTROS ESTANDARES FDDI (FIBER DISTRIBUITED DATA INTERFACE)[TAN89]

Es una LAN token ring de fibra óptica que permite velocidades de 100 Mbps sobre distancias arriba de los 200 km y que soporta más de 1000 estaciones conectadas.

Puede utilizarse en la misma forma que cualquier LAN 802, pero posee un ancho de banda más grande. Otro uso que tiene es el de un backbone que conecta LANs.

FDDI utiliza fibras multimodales porque el gasto adicional que generan las fibras de un solo modo no es necesario para redes que solo corren a 100 Mbps. FDDI utiliza *LEDs* en lugar de rayo laser, debido no solo a su bajo costo, sino también porque FDDI puede algunas veces utilizarse para conectar directamente las estaciones de trabajo del usuario.

El cableado de FDDI consiste de dos anillos de fibra óptica, uno transmite en el sentido de las manecillas del reloj y el otro contra el sentido de las manecillas del reloj. Si cualquiera de ellos se rompe, el otro puede utilizarse como respaldo. Si ambos se rompen en el mismo punto, ya sea por fuego u otro acidente en el ducto del cable, los dos anillos pueden unirse en un sólo anillo del doble de largo.

FDDI define dos tipos de estaciones A y B. Las estaciones de clase A se conectan a ambos anillos. Las estaciones B, son más baratas y solo se conectan a uno de los anillos. Dependiendo de que tan importante debe ser la tolerancia a las fallas, una instalación puede escoger estaciones clase A, clase B o una combinación de ambas.

La capa física de FDDI no utiliza la codificación Manchester, utiliza un esquema de codificación llamado 4 out of 5. En este esquema, cada grupo de cuatro símbolos de la subcapa MAC (ceros, unos y las marcas de inicio del frame) son codificados como un grupo de cinco bits en el medio. Dieciseis de las treinta y dos combinaciones son para los datos, tres para delimitadores, dos para control, tres para señales de hardware y ocho no se utilizan.

Los protocolos básicos de FDDI están diseñados de forma muy parecida a los del estándar 802.5. Para transmitir datos, un nodo debe capturar primero el token. Entonces éste transmite un frame y lo remueve cuando llega de nuevo con él. Una diferencia entre FDDI y 805.2 es que en 802.5, una estación no puede generar un nuevo token hasta que el frame haya dado la vuelta completa y regrese. En FDDI, con potencialmente 1000 estaciones y 200 km de fibra, el monto de tiempo gastado en la espera del frame que circunnavega por el anillo puede ser substancial. Por esta razón, se decidió permitir a una estación poner un nuevo token en el anillo y tan

pronto como esto se efectúe, transmitir sus frames. En un anillo largo, diversos frames pueden estar en el anillo al mismo tiempo.

FDDI permite frames de datos similares a los de 802.5, incluyendo los bits de confirmación y el byte de estado del frame.

El protocolo para la subcapa MAC requiere que cada estación tenga una marca de tiempo de rotación del token para conservar pistas de cuanto tiempo ha pasado desde que el último token fue visto. Un algoritmo prioritario similar al de 802.5 se utiliza para determinar las clases prioritarias que pueden transmitir en un token dado. Si el frame tiene una prioridad mayor o igual a la del token entonces se transmitirá, en caso contrario, deberá esperar a que baje el nivel de prioridad del token.

I.8 INTERCONEXION DE REDES

Las redes se interconectan para permitir a los usuarios accesar servicios o información localizados en otra red. De forma general, se interconectan redes múltiples para establecer comunicación a través de diversos puntos, y también para transportar información entre dos redes que están ubicadas entre distancias muy grandes.

Las LAN tienen limitaciones de tamaño, por lo que la interconexión con otras redes es esencial para contar con una cobertura geográfica más amplia. Las redes pequeñas ofrecen más confiabilidad y mejor desempeño que las redes grandes; interconectando un número de redes pequeñas donde la mayor parte de la comunicación toma lugar dentro de las redes en lo individual, nos muestra que estas ventajas pueden preservarse mientras se logra una interconexión más amplia.

ASPECTOS GENERALES

Los objetivos básicos que debe cumplir la interconexión de redes son :

- Proporcionar un enlace entre redes

- Realizar el ruteo y entrega de datos entre los procesos en las estaciones asignadas a las diferentes redes
- Implementar un servicio de *bitácora* que guarde toda huella del uso de las diversas redes y gateways y mantener el estado de dicha información.
- Habilitar los servicios de ajustes a:
    - Diferentes esquemas de direccionamiento: debido a que las redes usan diferentes nombres y direcciones.
    - Tamaños máximos de paquetes diferentes: Los paquetes de una red pueden dividirse en piezas pequeñas.
    - Diferentes mecanismos de acceso a la red. Los mecanismos de acceso a las estaciones de las diferentes redes
    - Diferentes límites de tiempo. Los procedimientos de tiempo en la interconexión deben permitir una transmisión exitósa que impida retransmisiones innecesarias
    - Recuperación de errores. El servicio de interconexión no debe depender y no debe ser interferido por la capacidad natural de la red para recuperar errores
- Técnicas de ruteo. Debe ser capaz de coordinar las técnicas de ruteo de datos entre sistemas de diferentes redes

Las redes interconectadas forman una internet. Al respecto se nos dice: "Si cada red constituyente retiene su identidad, y se necesitan mecanismos especiales para comunicarse a través de las múltiples redes, entonces, toda la configuración es referida como una internet, y cada red que la constituye como una subred" [WAT91].

Para poder referirse a la función de interconexión de redes, es importante describirla en su modo de operación. Estos, como ya conocimos son :

MODO DE OPERACIÓN CONNECTION-ORIENTED (ORIENTADO A LA CONEXIÓN)

Se asume que cada subred cuenta con una forma de servicio orientada a la

conexión. Esto significa que es posible establecer una conexión lógica de red entre dos DTEs asignados a la misma subred. Existen dos versiones de la operación de la interconexión en Connection-oriented:

- Interconexión de subredes soportando todos los elementos del servicio de red OSI: En este caso, un solo protocolo de la capa de red se utiliza entre los sistemas final e intermedios asignados a cada subred para proporcionar el servicio de red OSI. Los DCEs realizan las funciones de ruteo y envío, necesarias para soportar el servico de red end-to-end.
- Conversión. El servicio de cada subred que no soporta todos los elementos del servicio de la capa de red es transladado de tal forma que sea idéntico al servicio de red OSI. Esto requerirá la operación de uno o más protocolos antes de utilizar el protocolo típico de la subred.

Para lograr estas funciones, los DCE incluyen en su conformación dos funciones:

-Envío : Las unidades de datos que llegan a una subred a través del protocolo de la capa de red son remitidos a otra subred. El tráfico está sobre las conexiones lógicas que fueron unidas por los DCEs.

- Ruteo : Cuando una conexión lógica end-to-end es inicializada, cada DCE que participa en la secuencia debe realizar una decisión de ruta que determine el siguiente paso en la secuencia.

MODO DE OPERACIÓN CONNECTION-LESS (NO ORIENTADO A LA CONEXIÓN)

Aquí, cada unidad de datos del protocolo de red es tratada de forma independiente, y es ruteada del DTE origen al DTE destino a través de los DCEs y redes. Para cada unidad de datos transmitida por A, A toma la decisión de cual DCE debe recibir dicha unidad de datos. La unidad de datos viaja a través de la internet de un DCE a otro hasta alcanzar la subred destino. En cada DCE, se toma una decisión de ruta (de forma independiente para cada unidad de datos) relacionada con el

siguiente paso en la ruta. De esta forma diferentes unidades de datos viajan en diferentes rutas entre los DTE origen y destino.

DIRECCIONAMIENTO

A fin de transferir datos de un DTE a otro, debe haber una forma única de identificacion para el DTE destino. Esto es, para cada DTE, debemos asociar una dirección o identificador único. Esta dirección permitirá a DTEs y DCEs ejecutar la función de ruteo de la forma más apropiada.

En el ambiente OSI, esta dirección única es equivalente al Punto de acceso al servicio de red (Network Service Access Point NSAP). Un único NSAP identifica una DTE dentro de una internet. Una DTE puede tener más de un NSAP, pero cada uno es único con respecto a un sistema en particular. Podemos referir a ello y a la dirección como una dirección global de la internet. Frecuentemente, esta dirección se encuentra en la forma (red, *host*) donde el parámetro de red identifica una subred en particular; y el parámetro host identifica un DTE en particular asignado a dicha subred.

Cada subred debe mantener una dirección única para cada DTE asignado a ella. Esto permite a la subred rutear las unidades de datos a través de la subred y enviarlas al DTE elegido. Podemos referir como dirección del punto de asignación a la subred (Subnetwork attachment point address) a la dirección del host.

Puesto que las subredes utilizan diferentes formatos y tamaños de direcciones, debemos asumir que el parámetro de host tiene un significado global, y la dirección ó punto de asignación a la subred tiene un significado sólo dentro de una red en particular.

DISPOSITIVOS DE INTERCONEXION

Existen diversos DCEs que realizan la labor de interconectar redes, estos dispositivos son:

REPETIDORES

La forma más simple para interconectar redes es el repetidor. Los repetidores se utilizan para conectar segmentos individuales de redes a fin de formar una red extendida más larga. La función del repetidor es recibir un mensaje y despues retransmitirlo, regenerando la señal con su fuerza original. Para que pueda utilizarse un repetidor, ambos segmentos de la red deben ser del mismo tipo. Deben usar los mismos protocolos de red para todas las capas y el mismo método de control de acceso al medio, así como la misma técnica de transmisión física. Las estaciones de los diferentes segmentos que conecta un repetidor no pueden tener la misma dirección.

BRIDGE (PUENTE)

Un bridge es un dispositivo que puede presentarse en forma separada o en una estación que pertenece a dos o más redes simultáneamente. El bridge recibe todos los mensajes de cada subred de la que forma parte. Verifica la dirección destino y cuando reconoce que un mensaje corresponde a una estación en una subred diferente, transmite el mensaje a dicha subred. Este tipo de conexión se implementa mediante una función de almacenamiento-y-transmisión, ya que los mensajes son almacenados temporalmente en el bridge y después enviados a la otra subred. Un bridge opera a nivel de la capa de enlace de datos. La interconexión mediante bridge puede utilizarse para redes que usan diferentes protocolos a nivel de capa física, y hacen uso de protocolos comunes en la capa de enlace de datos. Para ello, nuevamente se requiere que todas las direcciones de estaciones de redes interconectadas sean únicas y utilicen formatos y tamaños de paquetes lo suficientemente similares para que las diferencias puedan ser manejadas por la capa de enlace de datos.

Para pasar los mensajes de forma apropiada, una estación que opera como bridge debe saber cuales estaciones pertenecen a las diferentes subredes que están interconectadas. Se pueden establecer diversas formas para lograr esto. El bridge puede ser provisto de esta información mediante una fuente externa; por ejemplo el

administrador de red, o también puede programarse para aprender esta información, por ejemplo, mandando un mensaje a cada una de las subredes y solicitando respuesta de todas las estaciones de dicha subred.

ROUTER (RUTEADOR)

El uso de un ruteador se basa en un concepto que normalmente no se aplica en una LAN - rutear un mensaje a través de nodos intermedios. En una LAN, cuando se transmite un mensaje, éste se envia a todos los nodos en la red. Un nodo receptor determina de acuerdo con la dirección destino contenida en el mensaje, si recibir y procesar o no el mensaje. Por eso, cuando la LAN se interconecta con otras redes, ya sean WAN's o LAN's, la función de ruteo se torna crítica.

Con otro tipo de redes, particularmente WANs, un mensaje es mandado de un nodo a otro en la red, y el mensaje puede pasar a través de una serie de nodos intermedios antes de alcanzar su destino. Hay quizás más de una secuencia de nodos que un mensaje puede tomar para alcanzar el nodo destino. Cuando un mensaje es enrutado a través de nodos intermedios, deben incluirsele dos direcciones. La primera dirección que contendrá es la del nodo destino y permanece constante mientras el mensaje atraviesa la red. La segunda es la dirección del siguiente nodo en la ruta y cambia conforme el mensaje se mueve de nodo en nodo a través de la ruta sobre la red.

Para que pueda utilizarse un ruteador, las redes que se desean interconectar deben tener los mismos protocolos en la capa de red y protocolos compatibles en capas superiores, lo cual significa que las redes pueden diferir en las capas física y de enlace de datos. Pueden utilizarse múltiples ruteadores y estos pueden interconectarse en múltiples formas que permitan diveras rutas entre dos subredes.

Una función clave del ruteador es determinar el siguiente nodo al cual será enviado el mensaje y existen diversos métodos que pueden lograr esto. La información de ruteo puede ser predefinida como parte de la función de diseño y administración de la red y almacenada en forma de tablas de ruteo. Los ruteadores pueden desarrollar

un mapa de la topología de la red intercambiando información de nodos y enlaces activos y despues seleccionar una ruta basados en el mapa actual de la red.

GATEWAY

El último y más complejo de los DCEs de interconexión de redes es el gateway. Un gateway se utiliza para interconectar redes que pueden tener arquitecturas completamente diferentes. Un gateway, po ejemplo, puede usarse para interconectar una red *SNA* con una red tipo X.25 de conmutación de paquetes. Como se usan diferentes arquitecturas, se pueden usar diferentes protocolos en una o todas las capas de la red. El gateway realiza cualquier conversión necesaria para traducir de un protocolo a otro, incluyendo:

- Conversión del formato del mensaje. Las redes pueden emplear diferentes formatos de mensaje, tamaños máximos de mensaje y códigos de caracteres. El gateway debe ser capaz de convertir mensajes en el formato, tamaño y código apropiado para la red a la que se envía el mensaje.

- Translación de direcciones. Las redes pueden hacer uso de diferentes estructuras de dirección. El gateway deberá transladar todas las direcciones asociadas con un mensaje a la estructura de dirección requerida por la red destino.

- Conversión de protocolos. Cuando un mensaje es preparado para transmitirse a través de una red, cada capa de la red adiciona información de control que se utilizará por la capa correspondiente (entidad) en el nodo receptor para determinar que protocolos se usarán y como serán procesados los mensajes. Un gateway debe ser capaz de reemplazar la información de control del mensaje insertada en la red origen con la información de control que se requiere para ejecutar las funciones de comparación en la otra red. Esta conversión requiere de los servicios de segmentación y ensamblado, control de flujo de datos, y detección y recuperación de errores.

CAPITULO II. ADMINISTRACION DE RED

La administración de red implica el monitoreo, análisis, control y planeación de las actividades y recursos de una red de comunicaciones, a fin de dotar a los usuarios de servicios de telecomunicación con determinado nivel de calidad [ZNA94].

Para cumplir con este objetivo, la administración de red debe ser apropiada para coordinar redes internacionales (públicas o privadas) a las cuales están asignadas diversas organizaciones como si fuera una sola LAN. En este contexto, una organización puede: cubrir un ámbito nacional o multinacional, operar sobre una o varias ubicaciones comerciales y/o industriales, ser un gobierno o una comunidad académica o de investigación. En cada ubicación existen una o más LAN conectadas unas con otras. Este complejo escenario nos ayuda a exponer las características clave de la administración de red [STA90]:

- Muchos dominios administrativos, los cuales deben ser capaces de interactuar significativa y seguramente
- Diversas áreas, las cuales, aunque no cuentan con verdadera independencia, tienen un sistema de autonomía local
- Diferentes tecnologías de comunicación involucradas en la interconexión de LANs, MANs y WANs
- Largas WAN que forman parte estratégica de la institución
- La inevitable evolución de las redes con el tiempo

II.1 MODELOS DE ADMINISTRACION DE RED

La administración de red resalta cinco aspectos denominados: información, funcional, comunicación, arquitectural y organizacional. El modelo de información establece la representación de la red mediante datos. Proporciona un punto de vista unificado de los recursos de la red al darle estructura a la información que los representa. El modelo funcional define las funciones administrativas que deben implementarse para alcanzar los objetivos de la administración de red. El modelo arquitectural describe la estructura general de las entidades que realizan las tareas administrativas y las interfases entre ellas. El modelo de comunicación habilita los intercambios de información, controles, etc entre entidades administrativas. El modelo organizacional establece los roles de administradores y agentes, sus interrelaciones y su ubicación dentro de una configuración administrativa de red dada.

Estos modelos pueden ser aplicados a cualquier estructura de red, p.ej. la multi-red (interconexión de subredes heterogéneas), la subred, un sistema final, una capa del modelo OSI, etc.

ASPECTOS DE LA ADMINISTRACION DE REDES

Al inicio del capítulo establecimos una definición de administración de red, la cual nos invita a cuestionarnos lo siguiente: ¿ Qué vamos a monitorear ? ¿ Quién va a monitorear ? ¿ Cómo va a monitorear ? ¿ Qué conocimientos son necesarios para el análisis ? ¿ Cómo controlarlo ?. Para responder a todas estas preguntas se han definido cinco modelos o aspectos de la administración de red, los cuales clasifican los problemas similares en una misma categoría que se trata independientemente de las otras. Para responder al "Qué", necesitamos considerar un punto de vista informativo que proporcione una representación de la red con datos. El aspecto funcional es también de interés, ya que define las funciones que se aplicarán sobre ésta información para lograr propósitos específicos. Las entidades administrativas distribuidas sobre la red administrada contestan al "Quién" y ellas definen principalmente el aspecto organizacional. Finalmente, para responder al "Cómo" se

consideran tanto los modelos de comunicación como el arquitectural. El modelo de comunicación habilita los intercambios entre las entidades administrativas mientras que el modelo arquitectural describe la estructura general de las entidades administrativas y sus interfases[ZNA94-2].

QUE : MODELOS DE INFORMACION Y FUNCIONAL[ZNA94-2]

MODELO DE INFORMACION

En el campo de la administración de red, los objetos administrados son la abstracción de los recursos de procesamiento y comunicación de datos. Ellos representan la vista administrativa de los recursos de la red los cuales pueden ser físicos o conceptuales en su naturaleza. Basado en estos objetos debe describirse un modelo de información o representación de la red por datos. Esto permite proporcionar al coordinador de la red una vista unificada y exacta de los recursos de la red que serán administrados e identificar que es lo que se debe monitorear y controlar. Para alcanzar estos objetivos, es necesario dar una estructura al monto de información administrativa. ¿ Qué proporcionan los organismos de estandarización de la administración de red para definir el modelo de información ?.

El modelo de información ISO (International Organization for Standarization - Organización Internacional para la Estandarización) proporciona métodos para modelar los aspectos controlables de los recursos de comunicación tipo OSI y para estructurar el intercambio de esta información entre los sistemas. Este modelo de información está orientado a objetos. La especificación formal de la *sintáxis* para expresar las características de los objetos administrados está acompañada por el uso de un lenguaje denominado GDMO. Además proporciona conjuntos de objetos predefinidos (librerías) para desarrollar un modelo de información propio y específico.

En contraste, IETF (Internet Engineering Task Force - Fuerza de tareas de ingeniería en Internet) se enfoca en la administración de redes basadas en *TCP/IP*, ve los objetos administrados como simples variables residentes en un almacén virtual (Management Information Base MIB - Base de Información Administrativa).

La ITU (International Telecommunication Union - Unión Internacional de Telecomunicación), que está relacionada con la administración de redes de telecomunicación, aplica los lineamientos de OSI y define un modelo de información para administración de red genérico. Este modelo identifica los recursos genéricos que existen en una red y sus atributos, eventos, acciones y comportamiento asociados. Este modelo es recursivo ya que se aplica a diferentes niveles, denominados: nivel elemental de la red, nivel de red y nivel de servicio.

El Foro de Administración de red con su estándar OMNIPoint intenta conjuntar la administración de redes de telecomunicación y la administración tradicional de la comunicación de datos de una LAN/WAN. Por lo tanto, aplica una mezcla de los estándares de ISO y de IETF.

MODELO FUNCIONAL

Para realizar las actividades de la administración de red, deben definirse las operaciones y aplicarse al modelo de información. Las operaciones pueden definir dominios funcionales de administración específicos (Specific Management Functional Area SMFA) o establecer la funcionalidad para soportar requerimientos de SMFAs mediante funciones de administración de sistema (System Management Functions SMF).

En este modelo son identificadas seis áreas funcionales, cada una de las cuales se enfoca en un aspecto específico. Estas son: dominio de configuración, dominio de fallas, dominio de desempeño, dominio de contabilidad, dominio de seguridad y dominio de planeación de la capacidad de la red.

De acuerdo con los requerimientos de la administración de red en un contexto dado, un número de éstas áreas funcionales podrían implementarse dentro del sistema de administración de red. El resultado global es el modelo funcional.

Estas áreas funcionales y los aspectos que cubren son:

= Dominio de configuración: Identifica, administra y controla los objetos del sistema con el propósito de proporcionar una operación contínu de la red. El dominio

de configuración indica donse se encuentra ubicado todo en la red, como están interconectados los objetos y cuales son los parámetros de operación para cada uno de ellos.

= Dominio de fallas: Es el conjunto de servicios que establece la detección, aislamiento y corrección de operaciones anormales que ocurran en la red. Indica qué está haciendo la red y qué es lo que no está trabajando en la red dada una configuración.

= Dominio de desempeño: Está relacionado con la utilización de los recursos de la red y su habilidad para alcanzar los objetivos de nivel de servicio al usuario.

= Dominio de seguridad: Incluye acciones y mecanismos para proteger el acceso a los recursos de la redy del sistema de administración de red.

= Dominio de contabilidad: Aporta un conjunto de capacidades que determinan el uso del servicio de red y los costos para calcular tal uso.

= Dominio de Planeación de la Capacidad de la red : Es el proceso de determinación de una red óptima, teniendo como fundamento información del desempeño de la red, el flujo del tráfico, la utilización de los recursos, los requerimientos de conexión, los intercambios tecnológicos y el crecimiento estimado de las aplicaciones presentes y futuras.

Toda área administrativa debe utilizar diversas funciones (SMFs) a fin de manejar los propósitos de la administración, y algunas funciones pueden utilizarse por diferentes áreas. ISO define un conjunto de funciones de administración de sistemas, reutilizadas y complementadas por ITU. Por otro lado, NMForum definió funciones de administración suplementarias para lograr una interoperabilidad más práctica.

QUIEN : MODELO ORGANIZACIONAL[ZNA94-2]

La administración de sistemas interconectados es una aplicación del procesamiento de información. Como el ambiente a ser coordinado es distribuido, la administración de red es una aplicación distribuida que implica el intercambio de información administrativa entre procesos administrativos con el objetivo de monitorear y controlar los diversos recursos físicos y lógicos de interconexión. Por lo

tanto, se requiere un modelo organizacional para determinar el papel de los procesos administrativos, sus interrelaciones y su ubicación dentro de la red que se manejará.

En una interacción específica de tipo administrativo, los procesos tomarán uno de dos posibles papeles:

= El papel del coordinador, el cual inicia las directivas de operación y recibe las notificaciones.

= El papel de agente, el cual ejecuta operaciones sobre objetos controlados por el administrador y envía las respuestas y notificaciones de dichos objetos administrados si son requeridas.

COMO : MODELOS DE COMUNICACION Y ARQUITECTURAL

MODELO DE COMUNICACION

Las redes de hoy son multiplataforma (multivendedor) y están caracterizadas por la diversidad del tipo y número de los recursos que las conforman. Inclusive dentro de ambientes homogéneos la administración de red se ve incrementablemente distribuida entre diversas entidades por la introducción de nuevas tecnologías. Por ejemplo, éste es el caso de FDDI en subred. Cada estación FDDI tiene su propia entidad organizadora denominada SMT (Station Management - Administración de la Estación). Cada SMT FDDI coopera con otras SMTs para coordinar la subred FDDI como un todo de forma distribuida. Por lo tanto, se requieren mecanismos de comunicación para distribuir y coordinar tareas de administración entre los sistemas administrativos diferentes o dentro del mismo sistema de administración (nivel de administración en particular).

Este aspecto exhibe un cuarto modelo: el modelo de comunicación. Podemos establecer que la consideración fundamental del modelo de comunicación es la definición de una plataforma de comunicaciones uniforme para soportar los intercambios de información entre entidades administrativas.

Por ejemplo, podemos encontrar en este aspecto dos niveles: los sistemas de administración acorder con los protocolos de administración estándar, y las capas de

administración - como es el caso de FDDI - que coordinan las estaciones FDDI:

- A nivel de los sistemas de administración, dos protocolos de administración de red importantes han sido estandarizados, *CMIP* (Common Management Information Protocol), y *SNMP* (Simple Network Management Protocol) con su versión mejorada de SNMP2.

- En las capas de administración, por ejemplo las de FDDI, se han estandarizado ocho protocolos SMT. Estos son el Protocolo de Notificación al Vecino (Neighbor Notification Protocol NN), el *Polling* de información al vecino (Neighbor Information Polling NIP), el Polling del Estado de la Estación (Station Status Polling SSP), el Protocolo de Echo (Echo Protocol ECHO), el Protocolo de Asignación de Ancho de Banda Síncrono (Synchronous Bandwidth Allocation Protocol SBA) y el Protocolo de Servicio Extendido (Extended Servive Protocol ES). Estos protocolos de comunicación permiten la obtención de estadísticas de red; la detección, aislamiento y resolución de fallas en la red; y la afinación de la configuración y parámetros de operación de la red FDDI a fin de encontrar los requerimientos de conectividad y desempeño de las aplicaciones.

MODELO ARQUITECTURAL

Para describir la estructura general de las entidades que realizan las tareas de administración, sus interfases y formas de comunicación, debe proporcionarse un modelo arquitectural.

La recomendación ITU M.3010 "Principios para una Red de Administración de Telecomunicaciones" (Telecommunication Management Network TMN) juega un papel central en la arquitectura de cualquier sistema de administración de telecomunicaciones. TMN proporciona tres formas de arquitectura, la arquitectura de información (modelo de información y arquitectura de administración en capas), la arquitectura funcional (bloques de función y puntos de referencia entre ellos), y la arquitectura física (implementación de la arquitectura TMN consistente de elementos físicos).

El concepto básico detrás de TMN es proporcionar una estructura de red

organizada a fin de alcanzar la interconexión de varios tipos de sistemas de administración de red mediante el equipo de telecomunicaciones de la subyacente red administrada. Hay que notar que funcionalmente la TMN no es parte de la red de telecomunicaciones, sino que es una red separada que hace interfase con ella en un número determinado de puntos de referencia con el objeto de recibir información de y para controlar sus operaciones administrativas. Para nuestro modelo arquitectural consideraremos principalmente el aspecto funcional de la TMN y su arquitectura en capas.

Arquitectura Funcional

El aspecto funcional de una TMN consiste en describirla en términos de bloques de función y los puntos de referencia entre ellos. Están identificados cinco bloques de función:

- Función de Sistemas de Operaciones (Operations Systems Function OSF) la cual soporta las funciones de administración de telecomunicaciones.

- Función de Mediación (Mediation Function MF) que actúa entre la información que pasa entre un OSF y un NEF o un QAF. Algunos MFs mejorados proporcionan control de la comunicación, conversión de protocolos y manejo de datos, comunicación de funciones primitivas, procesos de decisión y almacenamiento de datos

- Función elemento de red (Network Element Function MEF). Bloque funcional el cual se comunica con la TMN con el propósito de ser administrado.

- Función de estación de trabajo (workstation Function WSF). Establece la forma para interpretar y presentar la información administrativa de TMN al usuario final.

- Función de Adaptación Q (Q Adaptation Function QAF). Conecta entidades diferentes a un TMN con una TMN transladándose entre un punto de referencia TMN y un punto en la entidad diferente de TMN (propietario).

Los puntos de referencia son puntos de información conceptuales intercambiados entre bloques de función que no se interponen. Los puntos de referencia definen las fronteras de servicio entre los bloques funcionales.

Arquitectura en capas

Para propósitos de operación, las grandes redes necesitan ser particionadas y sus funciones administrativas relacionadas necesitan ser agrupadas. Para alcanzar este objetivo, la recomendación M.3010 de ITU ha definido una arquitectura lógica en capas dentro de su arquitectura de información. Cada capa restrinje la actividad administrativa dentro de los límites de ella misma en un rango claramente definido que está relacionado con algún subconjunto de la actividad administrativa en su totalidad.

La arquitectura lógica en capas de una TMN se define como sigue:

- La capa de elemento de red es inherentemente dependiente de las tecnologías y arquitecturas utilizadas en los recursos y equipos de conmutación y transmisión específicos.

- La capa de elemento de administración coordina cada elemento de red en lo individual. Esta capa tiene un conjunto de elementos coordinadores cuyo papel es: controlar y administrar un subconjunto de elementos de red, proporcionar una función de gateway, y permitir a la capa de administración de red interactuar con elementos de red y mantener datos acerca de los elementos.

- La capa de administración de red es responsable de administrar todos los elementos de red individualmente y en conjunto, como si fueran presentados por la capa de elemento de administración. Esta capa está encargada de controlar y coordinar a todos los elementos de red dentro de su ámbito de dominio e interactuar con la capa de administración del servicio para lograr máximo desempeño, uso, disponibilidad, etc.

- La capa de administración del servicio está relacionada con los servicios que son proporcionados a los usuarios. Esta capa determina la interfase con el usuario e interactúa con la capa de administración de red y con la capa de administración del negocio mediante OSFs.

- La capa de administración del negocio tiene la responsabilidad de toda la plataforma y es aquella en la que se realizan los acuerdos entre operadores.

De acuerdo con el estándar de administración de red de ISO, el Marco de Administración de Sistemas OSI reconoce tres niveles de administración en la arquitectura OSI: administración de protocolos, administración de capas y administración de sistemas.

RELACIONES ENTRE LOS MODELOS DE LA ADMINISTRACION DE RED [ZNA94-2]

Después de haber descrito los cinco modelos de la administracion de red, debemos establecer las relaciones entre ellos (Figura 2.1). El elemento central del sistema de administración de red es el modelo de información, el cual proporciona una representación en datos exacta de la red. Este modelo es el fundamento de todos los otros modelos de administración de red. El modelo funcional está expresado como un conjunto de criterios que son aplicados a la información administrativa, el modelo arquitectural define una arquitectura lógica en capas donde el modelo de información es *instanciado* dentro de todas las capas administrativas, el modelo organizacional define las entidades que intercambian la información administrativa. El modelo de comunicación es también un soporte para los otros modelos. El modelo funcional utiliza el modelo de comunicación para adicionar datos a la información administrativa. Note que el modelo de información debe ser completo para poder soportar la implementación de cualquier área funcional administrativa. El modelo organizacional utiliza el modelo de comunicación para habilitar el intercambio de información administrativa entre las entidades coordinadoras. El modelo arquitectural que describe la estructura general de las entidades que realizan las tareas de administración, sus interfases y formas de comunicación involucra en este último punto al modelo de comunicación. Además, el modelo organizacional realiza funciones definidas dentro del modelo funcional y utiliza la arquitectura para interoperar con otras organizaciones o entidades administrativas.

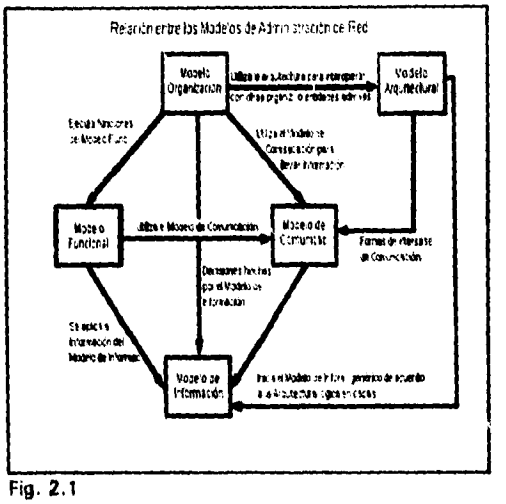


Fig. 2.1

Estas relaciones permaneces válidas siempre y cuando la capa administrativa sea una: capa multired, capa subred, capa sistema final, capa OSI, etc.

Finalmente, las relaciones posibles son:

Modelo Funcional = F1 (Modelo de Información, Modelo de Comunicación)

Modelo de Comunicación = F2 (Modelo de Información)

Modelo Organizacional = F3 (Modelo de Información, Modelo Funcional, Modelo de Comunicación)

Modelo Arquitectural = F4 (Modelo de Información, Modelo de Comunicación)

II.2 EL MODELO FUNCIONAL

FACTORES CRITICOS DEL MODELO FUNCIONAL

Los factores críticos son aquellos elementos clave de la actividad de una organización en los cuales son absolutamente necesarios los resultados favorables

para que una organización alcance sus metas. La meta de la administración de red es mantener niveles de servicio adecuados para el usuario final y asegurar que la red está operando efectiva y eficientemente en cualquier momento, a fin de no causar problema alguno en las operaciones a corto, mediano y largo plazo. Los factores críticos del modelo funcional de la administración de red son [TER92]:

= Procesos y procedimientos. Secuencia de pasos de una aplicación, incluyendo guías de cómo utilizar las herramientas para ejecutar las funciones de administración de red.

= Instrumentos. Hardware, software o ambos, para colectar, comprimir y guardar información en las Bases de Datos y predecir el desempeño futuro de los componentes de la red.

= Recursos Humanos. Individuos involucrados en las funciones de soporte a la administración de red.

PROCESOS Y PROCEDIMIENTOS

Como mencionamos anteriormente, las actividades principales de la administración de red se agrupan en dominios funcionales. Estos dominios son:

- El dominio de configuración, que se refiere al conjunto de actividades para controlar los inventarios físicos, eléctricos y lógicos, mantener los archivos de proveedores y las boletas de problema, dar seguimiento a las ordenes de proceso y provisión, administrar los cambios, y distribuir el software. Proporciona también el servicio de directorio y es una ayuda para generar diferentes redes.

- El dominio de fallas, o la colección de actividades que se requieren para mantener de forma dinámica el nivel de servicio de la red. Estas actividades aseguran alta disponibilidad de la red mediante el reconocimiento rápido de problemas y de degradaciones del desempeño, y el inicio de funciones de control cuando sea necesario. Estas últimas incluyen diagnóstico, reparación y evaluación del problema, recuperación del nivel de servicio y respaldo de la información. También realiza el

control de la bitácora y las técnicas de distribución de información.

- El dominio de desempeño realiza una evaluación en línea de la red a fin de verificar que se mantienen los niveles de servicio, identifica cuellos de botella actuales y potenciales, y establece y reporta tendencias de la red. La información de estos reportes se tomará como base para la planeación y toma de decisiones por parte de los responsables de la red. También se integran a este dominio las actividades para construir y mantener la Base de Datos de desempeño y automatizar algunos procedimientos para el control de las operaciones.

- El dominio de seguridad, cuyo objetivo es asegurar la protección de la red. Las actividades que realiza son: análisis de riesgos para lograr minimizarlos, implementación del Plan de seguridad de la red y monitoreo del mismo para verificar el éxito o fracaso de la estrategia de seguridad, evaluación de los indicadores de seguridad, administración de pasaportes, e implementación de avisos o de alarmas para el caso de que sucedan violaciones a las políticas establecidas en materia de uso de la red.

- El dominio de contabilidad que conjunta las actividades de recolectar, interpretar, procesar y reportar información de notificación de facturas y procedimientos de recargos por sobreusos de la red.

- El dominio de Planeación de la red, el cual involucra todas las actividades que conforman el proceso de determinación de una red óptima con base en los datos que emite el dominio de desempelo, en el flujo del tráfico, la utilización de recursos, los requerimientos de interconexión, los adelantos tecnológicos y el crecimiento estimado de las aplicaciones existentes y futuras.

Todos estos dominios interactuan y forman un todo. Ese todo constituye el modelo funcional para la administración de red.

INSTRUMENTOS

Los instrumentos que auxilian la labor de administración de la red pueden clasificarse en tres niveles:

CAPA BASE

Se forma de los elementos de la red o componentes que necesitan ser administrados como los PBX, LAN, servidores, computadoras, multiplexores, *modems*, conmutadores, bridges, routers, gateways, instalaciones, servicios, terminales, etc. En muchos casos, los elementos de la red contribuyen a administrar la red porque proporcionan información acerca de su estado y desempeño. Estos elementos pueden tener integrada la capacidad de generación de reportes de eventos, alertas o alarmas. Si no fuera así, deben adicionarse otros dispositivos de monitoreo externo a dichos elementos mediante una interfase de comunicación estándar.

El monitoreo externo puede realizarse mediante una amplia variedad de dispositivos, los cuales se agrupan en las siguientes categorías:

Monitores de línea o datascopios

El control técnico de los componentes de la red se encuentra cubierto en su gran mayoría por los monitores de línea, los cuales representan probablemente la forma más simple de evaluar equipo a fin de proporcionar información de la red en sitios remotos o centrales. Los datascopios monitorean y analizan los datos que pasan a través de la red de comunicación y despliegan la información en una pantalla, adicionalmente almacenan estos datos en un dispositivo de registro unido a la red para realizar análisis posteriores. Hoy en día, algunos de estos componentes (los más sofisticados) incorporan funciones de simulación y análisis de protocolos.

Estos monitores evaluan tanto las líneas digitales como las líneas analógicas. La evaluación analógica puede examinar las líneas de comunicación sobre la mayoría de los parámetros de transmisión especificados por tarifas comunes de los estándares cuando el equipo de comunicación está en condiciones de proporcionar de forma efectiva los datos para el cálculo de dichas tarifas. La categoría de evaluación digital se cubre ampliamente por los monitores de línea. Un monitor de línea de datos es un equipo de evaluación y/o diagnóstico utilizado para monitorear y analizar los datos que pasan a través de una red de comunicación de datos. Esto acelera el aislamiento y diagnóstico de problemas en la red, desplegando los datos e información de control

que fluye a través de la red. Esta unidad despliega toda la información de las líneas de comunicación de datos en ambas direcciones. Esto destaca la información de control en la línea, la cual normalmente no está disponible al usuario, así como también resalta señales cuando se detectan determinados eventos que afectan de forma crucial la transmisión y recepción de las señales de información.

Sistemas de control de red

La segunda categoría es denominada sistema de control técnico de la red (SCTR). Incluye sistemas de control técnico de tipo manual, automático o una combinación de ambos. El SCTR es alimentado por suministradores de información de *patching*, conmutación y modems. Estos sistemas ofrecen acceso a sitios remotos a través de líneas arrendadas o de líneas telefónicas mediante el uso de un canal secundario. Los SCTR ofrecen evaluación y control centralizado por medio de la integración de monitores de línea con suministradores de patching y del equipo de conmutación, montados en un *rack* en el centro de comunicaciones. Un sistema de control de red consta de tres elementos básicos:

- Canal de evaluación secundario: es un canal independiente de baja velocidad que utiliza frecuencias poco comunes del ancho de banda en las líneas telefónicas rentadas. La técnica de evaluación del canal secundario requiere que el usuario emplee dispositivos adicionales para soportar la transmisión de los datos administrativos en modem a través de la porción digital de sus redes.

- Módulo de evaluación de direccionamiento-remoto: es un módulo electrónico que se adiciona o integra en un modem. Un módulo de evaluación reconoce su propia dirección cuando acepta los comandos y ejecuta la función requerida. Esto permite un control de señales de modem externas e internas con el propósito de realizar diagnósticos, evaluaciones y funciones de control resolutorias.

- Control central: incorpora inteligencia en la ubicación central, controla de forma total la subred de evaluación del canal comunicándose con cada módulo de evaluación conectado sobre el canal de verificación. La consola de control de la red representa la interfase entre el operador del centro de comunicaciones y el sistema de

control de la red. Los sistemas de hoy en día están basados en microprocesadores altamente automatizados y la interfase del operador está diseñada para ser lo más amigable posible con el usuario.

Monitoreo y control con *CSU/DSU*

Es el principal componente en el monitoreo y control de redes point-to-point y backbones. Para facilitar el monitoreo, control y aislamiento de fallas en la red, el CSU cuenta con características que permiten la evaluación y monitoreo sofisticado del desempeño.

Los instrumentos de monitoreo CSU y DSU contribuyen con sistemas de administración de elementos propietarios mediante la generación de información de estado y en muchos casos también de alarmas. Los indicadores típicos con que cuenta señalan: pérdida del frame, pérdida de la señal, señal de alarma, alarmas preventivas y porcentajes excesivos de error. Los CSU y DSU inteligentes pueden trabajar en conjunción con herramientas de administración de software para proporcionar una vista comprensiva de todos los tipos de equipo como multiplexores, PBXs, bridges y routers. También proporciona conexiones con integradores que soportan la comunicación en dos sentidos.

SISTEMAS DE ADMINISTRACION DE ELEMENTOS DE RED

Se utilizan para dirigir los elementos de la red. Estos sistemas los podemos encontrar empotrados en el propio elemento de red o en un nodo de servicio. En muchos casos, estos sistemas soportan la comunicación en dos sentidos. Utilizan un subconjunto de datos comprimidos para supervisar la operación de la red en tiempo real. Estos datos son distribuidos a los operadores y tienen un ciclo de vida predefinido. También puede hacer uso de sistemas expertos para tomar decisiones heurísticas basadas en conocimiento preprogramado.

SISTEMAS INTEGRADOS DE ADMINISTRACION DE RED

Estos sistemas ofrecen conjuntar los sistemas de administración de elementos de red. Asimismo resaltan la información recolectada por los sistemas de administración de elementos de la red, presentándola al administrador de red mediante una interfase unificada y amigable para él. Para instrumentar estos sistemas se requiere de una base de datos confiable y de la planeación adecuada del sistema. Los datos contenidos en las bases de datos pueden utilizarse para generar reportes periódicos del desempeño de la red.

RECURSO HUMANOS

Lógicamente, se requiere un equipo de trabajo que soporte todas estas funciones y dominios administrativos. Las tareas a realizar son diversas y ninguna persona puede cumplir con todas ellas. La administración de red es exitosa solamente cuando la gente se siente parte vital de la organización y está bien asignada en el trabajo y para ello deben existir elementos como la estructura organizacional, la calificación de personal, etc.

La estructura organizacional más recomendable es la que asigna las funciones de acuerdo a los dominios administrativos establecidos (seguridad, planeación, contabilidad, etc). Por otro lado, algunas compañías progresivas han organizado la administración de la red en un solo recurso. Administrando este recurso para un grupo en común, se facilita un eficiente intercambio de ideas.

Una vez que se ha establecido el modelo funcional y sus factores críticos, procederemos a describir los dominios de configuración, fallas, contabilidad, seguridad, desempeño y planeación de la capacidad de la red. En las siguientes páginas se describirán los dominios anteriores excepto el de seguridad, que será tratado con más detalle en el siguiente capítulo.

II.3 DOMINIO DE CONFIGURACION

Su papel es mantener una adecuada conformación de la red, atendiendo las relaciones de la red tanto con los externos (proveedores) como con los usuarios (mediante los acuerdos de niveles de servicio).

La importancia de este dominio radica en la fuerte interrelación que presenta con los demás dominios funcionales, tal y como lo muestra la Figura 2.2

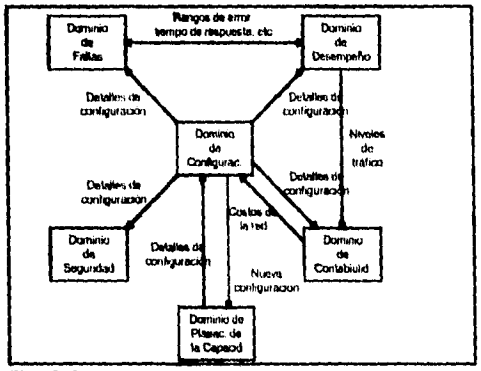


Fig. 2.2

Las funciones que conforman el dominio de configuración son:

CONTROL DEL INVENTARIO

El inventario es un padrón automático que proporciona una vista actualizada de la base de datos de componentes instalados y componentes de reserva. Los elementos que conforman el inventario incluyen equipo (modems, conmutadores, mainframens, *minicomputadoras* y *microcomputadoras*, etc), instalaciones (troncales y enlaces de línea), conexiones de cruz, circuitos (circuitos individuales y multipunto), redes, servicios ofrecidos, usuarios y proveedores, etc.

El segmento que corresponde al inventario en la base de datos general para la administración de red debe concordar con los atributos, la conectividad, y el estado real de los elementos y objetos administrados.

SERVICIO DE TOPOLOGIA DE LA RED

El servicio de topología de la red se proporciona mediante la base de datos que detenta las configuraciones actual e histórica de la red. La configuración desplegada de las capas física, lógica y eléctrica de la red y sus componentes está soportada de manera individual o de forma integrada. Esto es, los datos estáticos y dinámicos de la configuración son solicitados por los diversos dominios funcionales.

A fin de realizar ciertas funciones del dominio de configuración (como control de inventarios y administración del cambio) y del dominio de fallas (como solución de problemas y diagnósticos de problemas) la base de datos de la configuración de la red debe ofrecer la capacidad de un despliegue multicapas. Las capas que se recomienda presentar son:

- Red: Desplegando toda la red e indicando los problemas con cambios de color en las zonas en conflicto
- Región: Mostrando la configuración de una región en forma detallada
- Elementos: Presentando información más detallada del elemento que presenta problemas. Se puede incluir cualquier elemento contenido en la base de datos de elementos de la red.

Los servicios de topología de red son muy importantes para quienes prestan servicios con redes de valor agregado (*value-added networks*) y de conmutación de paquetes (*packet switching*). En combinación con las funciones del dominio de fallas, la vista de la configuración de la red ayuda a reconocer cuellos de botella funcionales y de desempeño en tiempo real. Los centros de control de red de estos proveedores (los de redes de valor agregado y de conmutación de paquetes) deben estar mejor equipados que aquellos que pertenecen a empresas privadas.

Se debe poner particular énfasis en los circuitos virtuales, y otros nodos clave que convierten protocolos nativos al formato del protocolo estándar o viceversa. También es importante desplegar las interconexiones con LANs, utilizando bridges, routers, y gateways como fuentes de información para proporcionar el servicio de topología.

ACUERDOS DE NIVELES DE SERVICIO

La función de niveles de servicio implica la aplicación de una metodología estándar que asegure los compromisos necesarios para que el nivel de servicio que se proporciona al usuario sea siempre consistente. El efecto de estos acuerdos es mejorar la planeación y reducir las crisis administrativas.

Un acuerdo de niveles de servicio, es un contrato escrito formal simple o elaborado que contiene :

= Identificación de las partes contratantes Los sujetos del contrato son el centro de redes y el departamento o entidad organizacional que solicita el servicio. El usuario y el centro de redes se hacen responsables de asegurarse que el sistema de producción se ejecute correctamente.

= Una descripción del trabajo que se procesará, incluyendo tipo de tarea, volumen de información,etc. El personal de sistemas debe especificar diferentes niveles de servicio para procesar los trabajos en períodos de mucha y/o poca carga de trabajo o para realizar trabajos de menor prioridad en determinadas circunstancias. Un aspecto crítico a considerar es el tamaño de los trabajos lo cual se simplificaría si los usuarios pudieran distinguir entre labores complejas, simples o aún triviales.

= Niveles de servicio que se proporcionarán, incluyendo tiempo de respuesta, tiempos muertos, precisión de resultados y disponibilidad de la red.

= Reporte de desempeño. Compara las características de las cargas de trabajo planeadas y actuales contra los niveles de servicio obtenidos durante el período en que se reporta, comparando las cargas de trabajo y el servicio. Mediante esta actividad es más fácil determinar si la falta de servicio se debió a exceso de trabajo o a un desempeño inadecuado por parte del centro de datos. Representan una oportunidad para identificar problemas y proponer soluciones.

= Castigos. Los castigos por sí solos pueden tener un impacto ligero. Sin embargo, dependen de la seriedad con la cual el usuario y el centro de redes tomen los compromisos descritos en el acuerdo. La pena máxima, para ambas partes es la cesantía del servicio.

= Provisión para modificaciones. Esta provisión permite al usuario o al centro de redes conocer las negociaciones para la aprobación de cambios en la prioridad del trabajo por parte de la administración. Generalmente, los cambios pueden hacerse solamente después de que el análisis ha demostrado que el problema no es una aberración.

= Fecha de expiración. El acuerdo se suscribe para que finalice después de cierto período de tiempo, como puede ser un año natural, el final del año de planeación o del año fiscal, etc.

DISEÑO, IMPLEMENTACIÓN Y PROCESAMIENTO DE LAS BOLETAS DE PROBLEMA.

La importancia de las boletas de problema radica en lo valiosa que es la información que contienen para el medir el desempeño de los proveedores, controlar el proceso de solución de problemas y alimentar la base de conocimientos. Pero más importante aún, sirven para supervisar los acuerdos de niveles de servicio ya que cuentan con la información para realizar los cálculos del dominio de desempeño.

Una boleta de problema incluye datos generales tales como: fecha, lugar, red, problema, técnico que atiende; información relacionada con el contacto con el proveedor como: persona con quién contactar, dirección y teléfono; definiciones de tiempos de: notificación, respuesta, reintentos y finalización de una sesión; descripción detallada del problema como: estado de los componentes, estado del problema, etc. Finalmente se incluyen los datos de tiempo total empleado en resolverlo y datos del mantenimiento preventivo.

Normalmente se implementan múltiples niveles de las boletas de problema. Los niveles pueden corresponder total o parcialmente a los niveles de determinación del problema. De acuerdo a esta jerarquía, los primeros datos son llenados por el área de soporte al usuario; y son obtenidos de las llamadas del usuario y de la información que proporcionan los dispositivos de monitoreo de la red y los medidores del software de comunicación. Dependiendo de la naturaleza del problema, el responsable del área de soporte puede enviar las boletas de problema de primer nivel a los grupos

responsables de la operación de la red (segundo nivel) o a los técnicos de mantenimiento (tercer nivel). Los resultados que se generan al resolver un problema, posteriormente pueden analizarse y almacenarse en una base de datos, relacionándola con archivos de inventarios y proveedores. Cuando haya madurado esta función, la administración de la red deberá generar procedimientos para el uso completo de boletas de problema de manera que se utilizen como fuente de información mediante un archivo de experiencias que será muy útil para el control de la operación de la red.

ORDENES DE PROCESO Y PROVISION

La orden de proceso avala entre otras cosas : la instalación de equipo y conexiones nuevas, la preparación y seguimiento de las ordenes de servicio, el acceso a los sistemas de ordenes a proveedores y la actualización de las bases de datos de inventario y configuración cuando se completa la instalación. La provisión contempla el movimiento físico y lógico de componentes de la red, actualiza el inventario y permite la ejecución de cambios programados y no programados, además, prepara y da seguimiento a las ordenes de servicio para mover, adicionar y/o cambiar elementos de la red.

Otro aspecto de la provisión se denomina servicio de provisionamiento el cual proporciona servicios de soporte a los usuarios de la red. El procesamiento también implica distribuir las ordenes de servicio a todas las áreas relevantes. Si una orden de intercambio o inter-intercambio involucra dos o más entidades de la organización entonces deben especificarse los requerimientos de desempeño para cada pieza que se intercambiará.

Cuando se recibe y verifica una orden de servicio, se elabora un diseño a nivel funcional para cumplir con el servicio solicitado. Este diseño podría constar de una identificación de las instalaciones de transmisión y de las funciones necesarias en las interfases de las instalaciones para proporcionar el servicio de manera óptima.

ADMINISTRACIÓN DEL CAMBIO

La administración de la red es la única área de la organización responsable de planear, aprobar, ejecutar y documentar los cambios en la red. Este proceso de planeación requiere de la siguiente información general: coordinador del cambio, número de cambio, fecha de la solicitud; en cuanto a datos del solicitante : nombre y afiliación; en cuanto al cambio: ubicación física, descripción del cambio, elementos de la red involucrados e identificados por el inventario, componentes de la red afectados por el cambio en menor, regular y mayor grado, fecha propuesta para efectuar el cambio, prioridad, razón del cambio, personal involucrado y procedimiento de recuperación; y una sección de evaluación de los resultados del cambio, retrasos en el cambio, fecha actual de implementación y cancelación o aplazamiento del mismo.

Después de evaluar esta información, el cambio es aprobado, a menos que haya objeciones. La aprobación contiene la agenda precisa de como se realizará y las responsabilidades delegadas a cada individuo involucrado en él. Las técnicas como *PERT y CPM* son útiles para supervisar las actividades del cambio. Es normal que cambios sencillos originen una cadena de solicitudes de cambios adicionales. Después de realizar el cambio, la documentación deberá completarse y habrá que actualizar los archivos de inventarios y proveedores.

SERVICIO DE DIRECTORIO

Esta función tiene como objetivo proporcionar una solución al problema de accesar y actualizar la información relacionada con el dominio de configuración que se encuentra almacenada en diversos sistemas, bases de datos y archivos. El servicio de directorio intenta mantener una vista lógica centralizada de los datos almacenados en los sistemas de administración que supervisan la red. Estos datos pueden residir en diferentes sistemas. Al proporcionarse este servicio las aplicaciones pueden escribirse sin referirse a una Base de datos en específico, de esta manera las llamadas a las Bases de datos se harán al directorio en un formato estándar y el directorio podrá atender la solicitud de datos dirigiéndola al sistema apropiado para su procesamiento.

Cada sistema remoto que participa en el directorio debe trasladar la solicitud de datos que recibe del directorio a la llamada a la base de datos correcta para su particular sistema de administración de base de datos.

El servicio de directorio también soporta el esquema de directorios múltiples en un ambiente de sistemas compartidos. En este caso, el servicio de directorio debe organizar las actualizaciones a los múltiples sistemas. Se debe contar con algún tipo de *bloqueo* que asegure la integridad de las bases de datos cuando se actualizan registros que pertenecen a múltiples sistemas. Estos bloqueos no deben liberarse hasta que retornen todas las confirmaciones positivas de actualización de cada sistema o hasta que se haya excedido algún límite de tiempo.

El servicio de directorio debe incorporar políticas de seguridad que permitan al usuario definir cuales terminales, identificadores y aplicaciones tienen acceso a los diferentes tipos de datos y más aún definir que tipos de operaciones (como leer, actualizar, adicionar o borrar) se pueden efectuar sobre los datos.

II.4 DOMINIO DE FALLAS

El dominio de fallas realiza todas aquellas actividades que dan seguimiento a una falla en la red, esto es, desde que se detecta un problema hasta que la red se encuentra totalmente recuperada. El proceso del dominio de fallas sigue el siguiente flujo [TER92]:

Como resultado de las llamadas de problema de los usuarios y del monitoreo de mensajes, eventos y alarmas pueden detectarse los problemas en los elementos e instalaciones de la red para posteriormente grabarse y etiquetarse. El proceso de las boletas de problema dinámicas, se encarga de dirigir los pasos para determinar el problema utilizando diferentes agentes para: la apertura de boletas, la revisión de estados de la red, la consolidación de la reparación y la conclusión de la boleta. Junto a las soluciones que se proporcionan en apoyo al área de soporte al usuario, se

ofrecen arreglos temporales en forma de revisiones e interrupciones de los elementos de la red. La determinación de problemas en segundo y tercer nivel involucra técnicas y herramientas más sofisticadas para identificar la naturaleza del problema y resolverlo, ya sea reparando y/o reemplazando elementos. Previo a restaurar la condición normal de la red, se recomienda efectuar evaluaciones en los puntos finales del enlace.

Las funciones que conforman el dominio de fallas son [TER92]:

SUPERVISION DEL ESTADO DE LA RED

Para llevar a cabo esta función es necesario realizar un despliegue de la configuración de la red en capas, mejor conocido como mapa de estado, el cual presenta una vista virtual del estado de los elementos críticos de la red y del estado del tráfico en un momento determinado lo cual permite adentrar al usuario en las partes en conflicto para verificar y aislar los problemas.

Esta actividad se encuentra fuertemente acoplada con el servicio que presta la función de servicio de la topología de la red del dominio de configuración. Las bases físicas de la supervisión del estado de la red la constituyen los dispositivos o sensores que residen empotrados o adjuntos a los elementos de la red. Algunos de estos instrumentos son : monitores de red, monitores de PBX, monitores de aplicaciones, monitores de multiplexores y conmutadores, e interfases a redes públicas y privadas de conmutación paquetes y de valor agregado.

La información obtenida del monitoreo se envía a los diversos sistemas de administración de elementos de la red, los cuales se encargan de procesar y distribuir los mensajes, eventos y alarmas.

En el nivel más bajo se esta actividad se generan los mensajes, los cuales reportan el estado de los elementos de la red. El estado significa la medida del comportamiento de un elemento en un momento específico. El estado se encuentra representado por un conjunto de *items* de información y los valores que tienen asignados en un momento específico.

La detección de eventos monitorea los reportes de cambios en el estado de los elementos administrados. Los elementos que conforman esta función son :

= Ubicación de la detección de eventos. La detección puede realizarse dentro o fuera del elemento administrado. La detección interna de eventos es una función del elemento en sí mismo y está integrada con las demás funciones que realiza. La detección externa utiliza los reportes de estado presentados por el elemento administrado y realiza una detección de eventos independiente.

= Detección de cambios en el estado. Cuando se detecta un cambio en el estado de un elemento deberá evaluarse a fin de conocer si se encuentra dentro de los criterios de generación de eventos. Este criterio se utiliza para determinar cuan significativo es un cambio de estado para el administrador de un elemento. Si se determina que el cambio es significativo, se generará un reporte del evento.

= Generación de reportes de eventos. Un reporte de evento se genera recolectando y empaquetando información de eventos significativos. Un reporte de eventos contiene información acerca del estado del elemento de la red, cambios en su estado, fecha y hora en que ocurren y cualquier otro dato significativo.

= Filtro global. Es el primer proceso que se realiza sobre el reporte de eventos. Separa los eventos antes de que se realize cualquier proceso, con el propósito de reducir el tráfico y la saturación en las demás funciones de detección de eventos.

= Filtro de distribución. Cada procesador de eventos toma la información para seleccionar los eventos que desea recibir. Solo aquellos eventos que son de interés para el procesador de eventos son escogidos y enviados por esta función, los que no son importantes, son descartados.

= Filtro del procesador de eventos. Cada procesador de eventos puede tener su propios filtros, los cuales deberán ser más específicos de acuerdo a la característica que van a medir.

= Distribuidor de eventos. Recibe los reportes de eventos filtrados y envía los reportes seleccionados a uno o más procesadores de eventos. La distribución de eventos se basa en el principio de subscriptor/proveedor. Cada procesador de

eventos debe suscribirse con el distribuidor de eventos a fin de recibir los reportes de evento del tipo que desea. La subscripción se realiza mediante una solicitud, la cual identificará el procesador de eventos inscrito y especificará el tipo de eventos que desea recibir. El distribuidor de eventos actualizará la lista de subscripción y la utilizará para determinar que reportes de eventos se enviarán al procesador de eventos.

= Procesadores de eventos. Examinan y procesan los reportes de eventos a través de funciones pasivas como el muestreo, y accesos y funciones de reactivación tales como corrección automática en caso de falla. La detección de eventos incluye un conjunto común de procesadores de eventos. De esta forma los reportes de eventos pueden enviarse a procesadores externos para posteriores procesos, específicos de otra área funcional del dominio de fallas. Los procesadores de eventos pueden ser:

- Procesadores de eventos comunes.

- De acceso. Recibe los reportes de eventos y sin un procesamiento posterior los almacena en la base de datos de eventos con el propósitos de archivarlos y analizarlos posteriormente. También cuenta con un conjunto de servicios compartidos para buscar y seleccionar reportes de eventos de la bitácora, de manera que la historia de los eventos pueda analizarse y/o desplegarse.

- De muestreo. Acoge los eventos que cumplan con un conjunto de criterios especificados y realiza copias de los eventos en la base de datos de eventos para análisis posteriores, ya sea del dominio de desempeño o con otros propósitos.

- De registro de estado. Se utiliza para aplicar los estados de cambio representados por los eventos a la representación de los objetos administrativos (elementos de la red) almacenados en las bases de datos. Esta función necesita contar con una representación actualizada de la base de datos, la cual es mantenida por otros procesos.

- Procesadores de eventos externos. Realizan el procesamiento de eventos que son específicos a un dominio funcional. Al igual que los procesadores de eventos comunes utilizan los mismos servicios y cuentan con una estructura similar.

Sin embargo desarrollan funciones específicas al área funcional en que residen.

= Marcas de tiempo. Registro de la hora en que fue generado el evento. Este dato lo pueden proporcionar los mecanismos de detección de eventos y es importante porque muchos procesadores de eventos necesitan que éstos se encuentren ordenados cronológicamente.

= Identificación del elemento o proceso que genera el reporte de evento

= Identificación del elemento administrado cuyo cambio de estado generó el evento. Mientras sea posible, debe ser un identificador único, para una rápida localización.

= Información adicional del elemento administrado, como la clase del elemento y sus atributos (proveedor, número de servicio, etc).

= Tipo de evento. Especifica la naturaleza del cambio de estado que precipito el evento. Una forma de determinar el tipo de evento es clasificarlo de acuerdo a su dominio funcional. Los cambios de estado para objetos genéricos pueden evaluarse dentro del contexto de cada dominio funcional y de ahí definir los eventos correspondientes. Este esquema permite identificar los siguientes tipos de eventos :

- Eventos del dominio de configuración. Reportan cambios en el estado generados por elementos de la red relacionados con aquellas funciones que son realizadas por dicho dominio y que forman parte de su operación básica dentro de un sistema abierto. Estos eventos manejan alarmas y se miden en base a un conjunto de estados de transición definidos por los elementos administrados.

- Eventos del dominio de fallas. Reportan cambios en el estado relacionados con una falla en un elemento. Estos eventos señalan el reconocimiento de la falla y el estado que cambio en los elementos, auxiliándose de las boletas de problema y de las actividades de evaluación.

- Eventos del dominio de desempeño. Muestran cambios relacionados con el desempeño de un elemento administrado. Esta información permite detectar en que momento las características de desempeño de un objeto se han salido de los niveles establecidos.

- Eventos del dominio de seguridad. Presentan cambios en el estado relacionados con el acceso y uso de los recursos del sistema. Enlista acciones tales como cambios en los perfiles de seguridad, violaciones de seguridad, etc.

- Eventos del dominio de contabilidad. Reportan cambios en el estado relacionados con los elementos del dominio de contabilidad.

= Efecto de un evento. Es el que resulta en el elemento administrado. Puede utilizarse para determinar la severidad del evento y la reacción del sistema ante él. Los efectos que se pueden presentar son:

- Permanentes (Permanecen hasta que una acción externa los resuelve)
- Temporales (Se corrigen automáticamente en un período corto de tiempo)
- Inminentes (Aún no ha ocurrido pero pronto lo hará)
- De deterioro (Proporciona el servicio, pero a niveles reducidos)
- De inhibición (No puede proveer el servicio)

= Reporte del estado original. El estado que existió antes del cambio, señalando el evento que ocurrió.

= Reporte del estado resultante. Incluye el resultado del evento y puede tener la forma de un reporte de estado incompleto, que contenga solamente aquellos elementos de información relacionados con el resultado del evento.

= Prioridad del evento. Esta puede ser asignada por el proceso que genera el evento o por la detección de eventos tomando en cuenta el contenido del reporte de evento y otra información disponible.

= Causa de cambio en el estado. La que originó el evento. Como los tipos de eventos, puede organizarse en base a los dominios funcionales.

= Información de acciones recomendadas. Descripción de la acción de operación que se recomienda en respuesta al evento. Esta acción puede diagnosticar, resolver o evitar el problema.

= Acción del sistema. Es la descripción de la acción que puede tomarse automáticamente como resultado de un evento. Estas acciones pueden desarrollarse

por el mismo elemento administrado o por el sistema de administración de la red.

El esquema general que sigue esta actividad se refleja en la Figura 2.3.

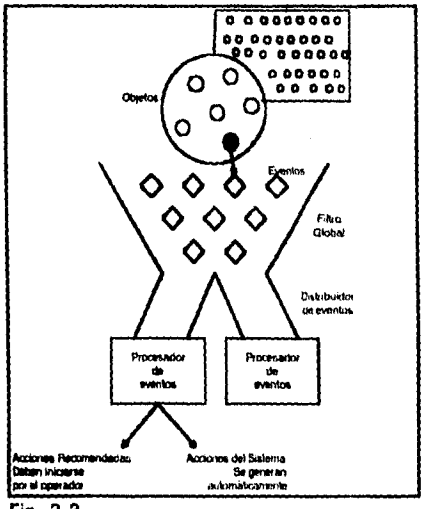


Fig. 2.3

SEGUIMIENTO DINAMICO DE PROBLEMAS

Esta actividad inicializa y relaciona las boletas de problema, despacha el problema al proveedor apropiado, verifica en línea el estado del progreso de la solución, cierra las boletas de problema y genera el registro histórico correspondiente.

Este proceso dirige la resolución de problemas manteniendo las conexiones de comunicación entre las diversas funciones dentro y fuera del dominio de fallas. Esta actividad se invoca cuando se presenta el evento de indisponibilidad de la red o de partes de ella, o de problemas de desempeño en cualquier lugar de la red. La palabra problema debe entenderse como un incidente o evento que causa una disfunción del sistema no esperada.

Los problemas encontrados en la red fluyen generalmente a través de un proceso de determinación de problemas que los analiza y resuelve. Dentro de este proceso, existen 6 niveles de complejidad de los problemas:

- Primer nivel: Problemas que puede resolver el área de soporte al usuario

- Segundo nivel: Problemas que pueden ser resueltos por los operadores de la red y/o operadores del sistema.

- Tercer nivel: Problemas tanto en hardware como en software que pueden solucionar los especialistas en comunicaciones de red.

- Tercer nivel bis: Si los síntomas muestran que la causa probable del evento son problemas relacionados con la aplicación, se despacha una boleta de problema al área de soporte de la aplicación.

- Cuarto nivel : Algunos problemas pueden manejarse solamente por los proveedores. Cuando el diagnóstico apunte en esta dirección, la boleta de problema se despacha al área de soporte técnico de los proveedores.

- Quinto nivel : Los problemas que afectan a servidores y estaciones en la LAN deben dirigirse al administrador de la misma.

Este seguimiento del problema, se encuentra representado graficamente por la Figura 2.4.

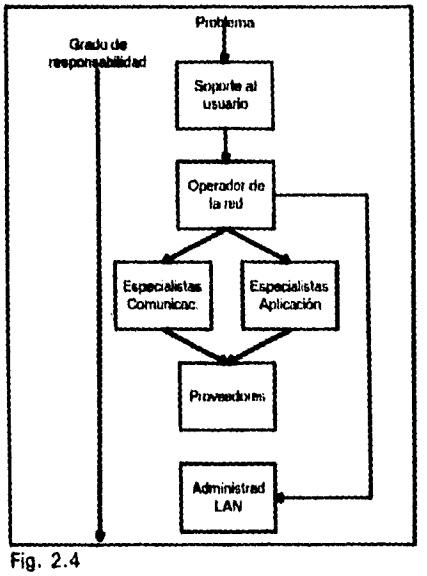


Fig. 2.4

Una actividad importante del seguimiento dinámico de problemas es la detección de los mismos. Para poder llevarla a cabo deben considerarse dos fuentes principales de información:

= La visualización del estado de la red con reportes extraordinarios de anomalías en sus funciones y/o servicios. La mayor parte del monitoreo de la red debe automatizarse estableciendo límites preestablecidos al software y hardware de monitoreo que deben ingresarse por los operadores de la red. Cuando se exceden los límites, se generan mensajes a la consola de red apropiada, los cuales alertan del problema a los operadores, dándoles además una identificación de su tipo y ubicación. Generalmente las alarmas disparan el proceso de determinación del problema.

= Mensajes del usuario, normalmente seleccionados por un sistema de administración de llamadas y/o por el área de soporte al usuario. También proviene información en menores cantidades de:

- Reportes en tiempo real del estado de la red
- Reportes del estado de la red del proveedor
- Pruebas resultado de rutinas de evaluación a la red automáticas o manuales

El seguimiento dinámico de problemas nos proporciona los siguientes beneficios:

- Inicio automático del seguimiento mediante eventos seleccionados; alarmas filtradas; llamadas de usuarios; selecciones por tiempo, proveedor y red basadas en fallas eléctricas severas; y límites de error preseleccionados.

- Presentación de estados y ayudas para el control de los progresos automáticos que aceleren y coordinen las actividades para la resolución de problemas.

- La actualización dinámica del estado de la falla y del nivel de severidad de la misma incluyendo algunos indicadores de las tendencias que se vislumbran.

- Mantenimiento de registros históricos que auxilien en el cálculo de los tiempos de reparación y tiempos entre fallas (tiempos muertos).

RESPALDO Y RECONFIGURACION

Esta función es una mezcla de procedimientos manuales, semiautomáticos y automáticos. La última decisión acerca de como implementarla depende de la infraestructura de la organización. Con infraestructura nos referimos a la variedad de los componentes de reserva, el ámbito de reconfiguración y la exactitud de la información de estado proporcionada por los dispositivos de monitoreo.

Se puede utilizar un sistema de respaldo y/o reconfiguración alrededor del problema utilizando alternativas preprogramadas. El respaldo y reconfiguración manual requiere de intervención humana para reconfigurar la red después de que se ha presentado un problema o para realizar un sistema de respaldo en tiempo real.

Los componentes de respaldo pueden ser físicos tales como: computadoras de reserva, capacidad de reserva en componentes existentes, etc. El respaldo también puede ser lógico utilizando equipo adicional y conexiones conmutadas o rutas físicas alternas. Los componentes de reserva frecuentemente se presentan en forma de:

- Redundancia de *front-end*s para que no operen a niveles de saturación
- Rutas o conexiones alternas que estén disponibles tanto física como lógicamente
- Nodos que al fallar puedan "librarse" rápidamente

Mientras se implementan las decisiones de reconfiguración de la red, es importante desplegar graficamente le evolución de la red resultante. Las nuevas rutas y los componentes impactados deberán indicarse mediante diferentes colores, parpadeo o una combinación de ambos. Un acercamiento lógico de esta vista puede ayudar al control de la operación de la red, mediante el análisis de los componentes antes y durante la reconfiguración.

DIAGNOSTICO Y REPARACION

Las funciones de diagnóstico y reparación incluyen herramientas para aislar y/o componer elementos y/o para proporcionar alternativas de respaldo a fin de mantener la integridad de la red. Esto permite determinar el origen específico de la falla, bloqueo

u otra interferencia.

El estado del problema debe monitorearse continuamente para determinar su posición. Para facilitar el diagnóstico, es necesario contar con relaciones robustas con el segmento de control del inventario de la Base de datos de la administración de red. Después de detectar y determinar el problema y sus componentes impactados, pueden desplegarse partes del archivo de control del inventario. También puede accesarse y utilizarse el conocimiento experto de la base de conocimientos en forma de estrategias de respaldo, problemas frecuentes y su solución y características técnicas de cada componente tales como nivel de saturación y nivel de utilización recomendados.

El diagnóstico de problemas puede facilitarse substancialmente con la combinación de vistas físicas y lógicas de la red las cuales generalmente separan mensajes, eventos y alarmas. La correlación de estas vistas con acciones manuales o automáticas puede ayudar a acelerar el proceso de resolución de un problema.

La recuperación de una red se torna cara si no se cuenta con procedimientos para lograr una restauración rápida de la red después de reparar los componentes fallidos y ponerlos en su lugar. Cuando se han completado todas las reparaciones requeridas, se deben ejecutar las evaluaciones correspondientes a fin de proporcionar un componente que funcione normalmente. Si las pruebas son satisfactorias, los componentes reparados y/o enlaces pueden inicializarse, a menos que la producción operativa se vea seriamente retrasada como resultado de dichas inicializaciones.

La evaluación es necesaria para la operación dinámica y correcta de la red y debe incluir componentes individuales como equipo (nodos) e instalaciones (enlaces de comunicación). Estas evaluaciones pueden ser:

- Evaluación end-to-end.

Permite valorar de acuerdo a bases programadas o demandas, presenta diagnósticos de los circuitos end-to-end, y ofrece pruebas de componentes y ciclos.

- Evaluaciones sin interrupción (No interfieren con el tráfico de datos del canal principal)

- Evaluaciones con interrupción (Causan interrupción del tráfico de datos del canal principal)

- Funciones remedio (Necesarias para restaurar y reconfigurar la red pasando por alto cualquier falla diagnosticada)

- Medidas analógicas (Proporcionan más información cuantitativa relacionada con la fuerza y degradación de la señal)

Las evaluaciones más comunes para examinar la integridad de las transferencias son :

- Pruebas de conectividad (Conexión entre dos equipos que están trabajando)

- Pruebas de integridad de los datos (El equipo puede intercambiar datos sin problemas, también debe medirse el tiempo en que establece la conexión)

- Pruebas de *loopback* (el mensaje puede intercambiarse entre los equipos sin problemas) :

= Loopback del canal local
= Loopback del canal compuesto local
= Loopback del canal remoto
= Loopback del canal compuesto remoto
= Evaluación pasa/falla del tipo end-to-end

Otras evaluaciones se concentran en:

- Evaluación de recursos internos. El equipo es examinado internamente. El resultado de la evaluación puede ser : aprobado, con fallas o pruebas inconclusas.

- Evaluación de la integridad del protocolo. Verifica la funcionalidad del protocolo.

- Evaluación de la capacidad. Busca encontrar los niveles de saturación de datos, saturación de conexiones y comportamiento del tiempo de respuesta. Sirve para evaluar el desempeño bajo condiciones de tensión.

II.5 DOMINIO DE DESEMPEÑO

Es el conjunto de actividades que miden continuamente los principales indicadores de desempeño de la operación de la red, para verificar como se mantienen los niveles de servicio, identificar cuellos de botella actuales y potenciales, y establecer y reportar tendencias del desempeño para la toma de decisiones y planeación de la red. También realiza el mantenimiento de la base de datos de desempeño, el desarrollo de los modelos de conexión y la preparación de procedimientos de medición automáticos.

Las funciones del dominio de desempeño son :

DEFINICION DE INDICADORES DE DESEMPEÑO

Establece la definición exacta de las métricas de desempeño para todas las formas de comunicación soportadas. Algunos de los indicadores que establece son: disponibilidad de la red, tiempo de respuesta, capacidad total, nivel de utilización, grado del servicio, volumenes de transmisión, cargas de trabajo ofrecidas, ocupación del canal y medidas de exactitud.

Las redes de comunicación no pueden administrarse cuando no es posible medir los indicadores significativos del desempeño de la red. Cualquier ambiente de red utiliza parámetros de desempeño. Dentro del grupo total de indicadores encontramos los indicadores orientados al servicio y los indicadores orientados a la eficiencia. Los primeros son los que tienen más prioridad ya que representan el grado de satisfacción del usuario.

INDICADORES ORIENTADOS AL SERVICIO

Pueden considerarse de interés exclusivo del usuario final, y desde su punto de vista, la disponibilidad de la red, el tiempo de respuesta y la precisión son los parámetros más importantes al controlar y planear sus procesos.

= Disponibilidad de la red. Mide la funcionalidad de la red de comunicaciones como un todo. Se mide mediante el porcentaje de tiempo que el usuario se toma para accesar los servicios de la red y contra el tiempo total en que dichos servicios están disponibles. La disponibilidad depende en gran medida de la confiabilidad técnica de los componentes de la red.

= Tiempo de respuesta. A nivel de usuario tiene un significado muy importante. Todas las partes deben ponerse de acuerdo para planear, medir e implementar dicho tiempo de respuesta. El tiempo de respuesta de la red incluye tiempo de envío, de recepción y de procesamiento. Puede incluirse o no el tiempo de transmisión a la pantalla. En la mayoría de los casos, el tiempo de respuesta del usuario es el tiempo que transcurre entre el momento en que oprime la tecla Intro y el instante en que se recibe el último carácter de la respuesta en la terminal. Para propósitos del reporte de desempeño se deben considerar al menos tres tiempos de respuesta : tiempo total de respuesta, retraso de la red (que incluye WANs, MANs y LANs) y retrasos por el procesamiento en los nodos.

= Exactitud. Se refiere a la entrega de respuestas exactas en la terminal del usuario. Debido a interrupciones en el camino entre los nodos fuente y destino, u otras acciones, la información entregada puede estar influenciada por:

- Caracteres erróneos recibidos
- Caracteres transmitidos pero no entregados
- Caracteres recibidos por un nodo al que no fueron enviados
- Caracteres entregados en forma duplicada

Estas anomalías deben preveerse y corregirse en la medida de lo posible.

INDICADORES ORIENTADOS A LA EFICIENCIA

Representan el interés de la organización por ofrecer servicios óptimos a la comunidad de usuarios. A fin de operar en el nivel más eficiente y cumplir con las expectativas de servicio de los usuarios, la relación entre la capacidad total de la red y su utilización debe medirse y actualizarse periódicamente.

= Capacidad total. Es una medida estática y global de la dimensión del servidor. Significa el límite técnico más alto (especificado por el proveedor) que puede alcanzarse bajo circunstancias ideales. Frecuentemente, cuando nos referimos a capacidad total, incluimos las interrelaciones entre los componentes de un sistema, lo cual reduce las características de capacidad de un componente en lo individual.

= Utilización. Es la medición dinámica de los recursos. Aporta información relacionada con los límites prácticos de la capacidad bajo determinadas circunstancias de operación. Utilizando estos indicadores pueden analizarse algunas situaciones que se presentan entre los componentes tales como: sobreposiciones, espera mutua de recursos y retrasos por la espera de ciertos recursos.

Los impactos a los indicadores pueden venir de: los parámetros establecidos, las mezclas de cargas de trabajo, el modo de acceso, la operación, los medios de transmisión, los rangos de capacidad del nodo y el enlace, los protocolos, la sobrecarga en la comunicación y el número de terminales de usuario conectadas a la red.

Se recomienda establecer los indicadores independientemente del sistema de comunicación, subdividiendo la interacción entre el usuario y los sistemas de comunicación de datos en tres fases fundamentales:

= Función de acceso (De ingreso al sistema)

= Función de transmisión (Durante el tiempo en que estén conectados los nodos)

= Función de desconexión (Momento en que finaliza la sesión)

MONITOREO DEL DESEMPEÑO

Establece las medidas para la evaluación de instalaciones y equipo, incluyendo monitoreo análogico, monitoreo del desempeño digital, evaluación de la transmisión análogica, supervisión del desempeño del nodo, vigilancia y evaluación de LANs y promedios de desempeño eficiente de las aplicaciones.

CONSIDERACIONES PARA LA DISPONIBILIDAD

Utilizando la configuración de la red del dominio de configuración, la disponibilidad de la red puede mostrarse mediante cambios en el estado de la misma. El estado se puede obtener a través de los comandos de control del anterior dominio. Estos comandos son disparados por mensajes que indican la activación y/o desactivación de recursos, recuperaciones exitosas de componentes y cualquier forma de errores y fallas eléctricas en los elementos de la red. Una tarea especial del dominio de configuración verifica los mensajes, estén estos incluidos o no en la tabla de disparadores (*triggers*), si se encuentran incluidos, se inician las evaluaciones. Los resultados son almacenados en una bitácora que mantiene el dominio de configuración. Otros reportes formales que indiquen la disponibilidad de la red pueden generarse sobre: disponibilidad de las ubicaciones de la red, período de las fallas eléctricas, promedio de tiempo entre fallas, número de fallas eléctricas por clase y otras excepciones donde los límites puedan establecerse por el usuario.

CONSIDERACIONES DEL TIEMPO DE RESPUESTA

Las mediciones del tiempo de respuesta en la interfase de comunicación son en muchos casos dependientes de los protocolos. El dispositivo de medición debe interpretar la forma en la que trabajan los protocolos, colocar marcas de tiempo a ciertos eventos y efectuar cálculos. Para el punto de vista del dispositivo de medición, existen cuatro elementos principales del tiempo de respuesta del usuario :

- Período inactivo del *polling* (incluyendo LANs)
- Tiempo de ingreso (incluyendo MANs y WANs). Es considerado como el intervalo de tiempo que transcurre entre el reconocimiento del primero al último frame de información
- Tiempo de retraso entre computadora y front-end. El período requerido para procesar una transacción y generar una respuesta.
- Tiempo de salida (incluyendo WANs, MANs y LANs). El que transcurre entre el envío del primer frame de respuesta y la confirmación del frame final que envía el dispositivo secundario.

El tiempo de respuesta puede interpretarse de diferentes maneras, indicando el tiempo que tardan los componentes más usuales más el retraso por transporte de la red. El tiempo de respuesta debe medirse, desplegarse y reportarse por cada forma de comunicación (datos, video, voz y *facsímil*) con que cuenta la organización.

CONSIDERACIONES DE EXACTITUD

La exactitud de las redes de comunicación puede impactarse en múltiples formas. Normalmente se implementan mecanismos con hardware y software para prevenir los problemas de exactitud, sin embargo, en muchos casos se espere que los analistas de desempeño proporcionen soluciones para el control operacional de dichos problemas. Estos mecanismos pueden incluir procedimientos automáticos de:

- Deshabilitación de terminales automática o manualmente
- Conmutación a modems de reserva de emergencia
- Línea de reserva en las instalaciones de línea privada.

CONSIDERACIONES DE CAPACIDAD Y UTILIZACIÓN

Simultáneamente con las mediciones orientadas al servicio, la información relacionada con la capacidad y la utilización debe extraerse de las fuentes correctas. Actualmente las mediciones son bien logradas en el campo de las computadoras, utilizando monitores de software. Por otro lado, la medición de procesadores y líneas de control de comunicación aún no es utilizada ampliamente, por lo que aún existe un área muy amplia que cubrir.

REPORTANDO LIMITES Y EXCEPCIONES

Consiste en realizar el análisis de la información de desempeño almacenada en la base de datos a fin de identificar cambios significativos en ella. Esta actividad permite a los administradores identificar, analizar y reconocer cambios en el desempeño de la red, estableciendo límites y generando reportes. Cuando se diseñan los sistemas de reportes del desempeño, deben considerarse los siguientes pasos:

= Determinación de las áreas de información e indicadores. Las áreas de información establecen la forma de agrupar los datos recolectados y almacenados. Los indicadores definen para cual de las áreas de información que están bajo la consideración del sistema de reportes se espera que se generen los reportes.

= Diseño de la matriz de distribución. El sistema de reportes tiene que servir a todas las unidades que participan en la administración de red. Dependiendo de las tareas, objetivos y responsabilidades de los receptores pueden ser completamente diferentes la forma, detalle, periodicidad y presentación de los reportes.

La estrategia de distribución de los reportes tiene que ser selectiva a fin de reducir el número de reportes impresos. La periodicidad con que se emiten debe corresponder con el nivel de detalle que requieren en términos de estructuras de datos de la base de datos y tipo de reportes. Es importante contar con fortaleza y disposición por parte del manejador de base de datos para poder presentar con prontitud y eficiencia la información solicitada.

ANALISIS Y AFINACION

Cualquier anomalía encontrada puede marcar el inicio de un proyecto de análisis. Frecuentemente, las solicitudes formales de análisis provienes de los dominios de seguridad, contabilidad y planeación de la capacidad. Un análisis de este tipo requiere de una metodología que lo lleve al logro de sus objetivos. A continuación se presenta un método propuesto [TER92]:

= El primer paso es decidir si el analista de desempeño debe apuntar hacia una tarea de afinación o hacia una actividad de soporte para el control de las operaciones.

= El segundo paso consiste en evaluar los objetivos y el período programado para desarrollar la solicitud de análisis que esta bajo consideración. Los datos necesarios para realizar esta actividad tienen que extraerse de las bases de

datos existentes. A fin de proporcionar información suficiente y con el detalle apropiado, debemos establecer la base de datos de desempeño. Es muy recomendable que el analista de desempeño se haga responsable del mantenimiento de dicho repositorio.

En cuanto al período de tiempo programado, es frecuente aquella verdad de "nunca es tarde para cancelar un proyecto". Este lapso de tiempo requerido depende en gran parte de las experiencias y resultados de medición disponibles. Si alguno de estos elementos está disponible, el plazo debe extenderse a través de un límite razonable. En suma deben determinarse los puntos de verificación para controlar los resultados.

= El tercer paso se refiere a la recolección de información o datos utilizando los dispositivos de monitoreo y la evaluación del desempeño de la red.

= Después que la información está disponible con el detalle y formato deseados, el analista inicia el cuarto paso con la formulación de la hipótesis. En la mayoría de los casos, al analista de desempeño estará interesado en la relación que existe entre los indicadores orientados a la utilización de servicios y los indicadores orientados a la utilización de recursos.

= En el quinto paso se evalúan la eficiencia y factibilidad técnica de la solución hipotética. Adicionalmente se examina cuantitativamente la factibilidad de cambios a la configuración y a los parámetros de corto alcance.

En esta fase, no existen consideraciones precisas relativas a cambios o mejoras a la configuración de la red. Muchas veces se espera que el analista de desempeño proponga una solución para mejorar el nivel de servicio en el corto plazo, o para extender las diferencias de tiempo hasta la siguiente liberación del cambio o actualización de la configuración de la red sin que esto provoque serios deteriores del nivel de servicio. En otras palabras, existe una búsqueda de formas para evitar el punto de saturación de la capacidad de la red antes de efectuar una actualización

programada. La mayoría de los analistas de desempeño están tentados por escoger alternativas tecnológicas sofisticadas y privilegiadas sin evaluar la economía de las alternativas. Su responsabilidad final debe ser excluir las alternativas hipotéticas que no son ni factibles ni económicas.

= En el sexto paso, se implementan los escenarios para la afinación de la red. La afinación es un proceso altamente iterativo. Frecuentemente deben implementarse un número diverso de alternativas y escenarios. Si fallan, los analistas deben considerar sus soluciones hipotéticas adicionales. Después que se han realizado un número establecido de experimentos con resultados fallidos el analista puede concluir que se ha agotado todas las posibilidades significativas de afinación y por lo tanto el dominio de planeación de la capacidad de la red debe tomar la responsabilidad de afinarla mediante una nueva planeación o la extensión de la capacidad de la red existente.

ESTABLECER ESTANDARES DE OPERACION

Esta función de soporte tiene la responsabilidad de desarrollar, instalar y mantener el software de comunicación de la red. El personal asignado a esta función consiste de programadores de sistemas de comunicación y expertos en comunicación.

En esta actividad se realiza la instalación de nuevas versiones del software de comunicación, así como las actualizaciones al software existente. Con software de comunicaciones nos referimos a la suma de todos los componentes de software que residen en los nodos de la red. Por otro lado, muchos productos o programas de comunicación requieren de modificaciones que los personalicen para que sean satisfechas las necesidades específicas del usuario y la encargada de definir las modificaciones de software requeridas por la red también es esta actividad.

II.6 DOMINIO DE CONTABILIDAD

Tiene como actividades el colectar, interpretar y reportar información relacionada con costos y recargos por el uso de recursos. Como parte de la contabilidad de los servicios de datos y voz en particular se incluye el registro de datos contables de procesamiento, verificación de facturas y procedimientos de recargos.

En general, las reglas de contabilidad de la organización definen la estrategia y los procedimientos financieros que lograrán de la mejor forma todos los objetivos corporativos. La recolección de información, el análisis de elementos de costo y el procesamiento y verificación de facturas de vendedores son absolutamente necesarios. Adicionalmente, debe existir una relación estrecha con la administración de toda la red para establecer las reglas de recargos, definir los procedimientos de recargos e integrar la contabilidad de la administración de la red a la contabilidad corporativa.

Las funciones del dominio de contabilidad son :

IDENTIFICACION DE LOS COMPONENTES DE COSTO

Estos componentes pueden categorizarse de la siguiente forma:

- Hardware: Computadoras, sistemas PBX, cables, microondas, satélites, repetidores, modems, etc.

- Software y sistemas: Incluye todo el software del centro de datos, de la red y de la ubicación del usuario final. Están inmersos en esta categoría los sistemas operativos, protocolos de comunicación, software de gateways, programas de aplicación, etc.

- Servicios: Incluye todos los servicios de red disponibles para los usuarios de la corporación. Contempla también los servicios públicos y privados como el correo electrónico, e inclusive ISDN.

- Personal: El personal corporativo involucrado directa o indirectamente en el suministro y/o soporte de hardware, software y servicios.

- Instalaciones generales: Incluye costos por edificios, instalaciones, mantenimiento, seguros, impuestos y otros servicios auxiliares.

En pocos casos el análisis de costos de la red es sencillo, lo más común es que sea un proceso complejo ya que en ésta cuantificación están involucrados factores tangibles e intangibles. Por otro lado, los costos pueden cambiar rápidamente y por lo tanto deben recalcularse frecuentemente.

ESTABLECIENDO POLITICAS DE RECARGOS

Un sistema de recargos tiene como objetivo la asignación de costos a los usuarios por el uso del recurso de comunicación. En algunas organizaciones, el dinero realmente cambia de unas manos a otras: se hacen ordenes de entrada, registros contables u otros instrumentos, pero no se da lugar a transferencias de dinero.

Para que un sistema de recargos tenga éxito debe ser:

- Entendible para el usuario
- Predecible, de forma que los administradores puedan planear efectivamente
- Un reflejo de la realidad económica de la empresa

La administración debe decidir cuales indicadores de uso de la red se utilizarán como base para el sistema de recargos. Dependiendo de esta decisión, la información de uso de la red debe colectarse y procesarse. Las políticas para lograr esto difieren entre ellas. De manera general se pueden distinguir tres alternativas:

= Cero recargo. Algunas organizaciones no recargan al usuario los costos de telecomunicación, los cuales simplemente se consideran como gastos generales de la institución, similares a los de la cafetería o los del del boletín informativo de la compañía.

= Recargo parcial. La mayoría de las empresas aplican recargos parciales a sus usuarios. En esta alternativa, parte de los costos de telecomunicaciones se absorben por la entidad, otra parte por algunos grupos (centro de datos) y los costos

restantes se cargan directamente al usuario de acuerdo a porcentajes específicos y factores de uso.

= Recargo total. Muy pocas empresas tratan de cobrar todos los costos por los servicios de telecomunicación prestados al usuario. Con frecuencia estos recargos se manejan a través de un costo del servicio y un precio negociado.

DEFINICION DE PROCEDIMIENTOS DE RECARGO

Asumiendo que se ha elaborado al sistema de recargos, deben definirse, desarrollarse e implementarse los correspondientes procedimientos para su ejecución. Los siguientes criterios son de interés principal en el diseño de metodologías de recargo:

= Simplicidad. La forma de costear los recursos y cobrarlos al usuario debe ser entendida fácilmente por todas las partes para resolver fácilmente los problemas entre los usuarios de la red y el centro de red.

= Exactitud. La contabilidad de la red debe arrojar resultados exactos.

= Responsabilidad. Los recargos deben ser proporcionales al servicio demandado por la comunidad de usuarios. Una de las problemáticas en este aspecto es la recolección de información sobre la utilización de recursos por cada usuario. Dependiendo de los requerimientos de exactitud en el cobro, deben emplearse varias técnicas y herramientas de recopilación de datos.

= Equidad. El usuario final espera un recargo justo por el servicio que demanda. Los cargos deben ser independientes de la computadora utilizada y de las rutas de transmisión seleccionadas. A fin de satisfacer al usuario se calculan valores promedios que se utilizan en los métodos de recargo.

= Visibilidad. La contabilidad de la red debe asistir a la tarea de determinar mejores pronósticos de recargos por uso de recursos para la información de presupuestos. Cuando la contabilidad es lo suficientemente avistable, la información podrá utilizarla también el dominio de planeación de recursos de la red en su actividad de definición de nuevos requerimientos de servicio con el propósito de

corregir defectos de diseño y de eliminar mal funcionamiento de componentes de hardware, software y comunicación en el ambiente de red.

Para la definición de recargos en la forma de costos unitarios existen tres métodos básicos: (1) Un sistema de costos proporcional que agrupa todos los costos en un todo y luego lo divide en partes iguales entre todos los usuarios del servicio. Existen desigualdades obvias en este sistema promediado, sin embargo tiene la virtud de ser simple y facil de implementar; (2) un método más sofisticado que consiste en establecer costos por tipo de equipo y dividirlos por clases de usuarios. Este método se conoce como costeo por responsabilidad, y básicamente aplica un factor ponderado de peso a los costos promedio proporcionales; y (3) un tercer método denominado de costos estándar, en el cual los gastos planeados por tipo de recurso dependen de dos factores: disponibilidad y utilización. La disponibilidad depende de la confiabilidad teórica de los recursos. El otro factor, la utilización, la controla el administrador de la red. Multiplicando el costo por unidad y el volumen de cargas de trabajo esperadas del usuario puede determinarse el costo por usuario asociado con la utilización de los recursos de información.

Una vez identificados, los costos estándar pueden utilizarse para establecer el sistema de recargos.

PROCESAMIENTO DE FACTURAS

El procesamiento correcto de las facturas es un aspecto importante que merece establecer procedimientos bien definidos los cuales serán realizados por el personal entrenado del Centro de Administración de la red. En esta área no existen problemas tan significativos como en los casos de la determinación de costos y recargos.

En este sentido, lo que es más importante, es el procedimiento para verificar la exactitud de las facturas del proveedor antes de pagarlas. Pueden encontrarse sobregiros significativos gracias al uso de procedimientos escritos precisos que analicen y verifiquen las facturas. Adicionalmente se requiere de procedimientos claramente definidos para dar seguimiento y registrar una factura a fin de prevenir cargos duplicados y multas y/o intereses moratorios.

INTEGRACION DE LA CONTABILIDAD DE LA RED A LAS REGLAS CONTABLES CORPORATIVAS

La contabilidad de la red es parte de la contabilidad corporativa y por lo tanto debe seguir las mismas reglas y procedimientos. Dos elementos comunes son especialmente importantes en esta área: el uso de las bases de datos y el uso de los programas de aplicación.

En la medida de lo posible las bases de datos de contabilidad de los centros de administración de redes deben integrarse a las bases de datos contables de la organización. Debe notarse, sin embargo, que las bases de datos de telecomunicación de los centros de administración de red utilizadas para el control y monitoreo no son parte de la estructura contable integrada.

Los programas de aplicación deben compartirse, ser útiles a todos los dominios y soportar reportes en línea hechos a la medida de todos los dominios. La presupuestación se puede considerar parte de esta actividad. La presupuestación es el proceso de la definición financiera del diseño de la red y de las decisiones de planeación de la capacidad de la red. Por lo tanto, esta función debe combinarse con la actividad de consideración de recursos demandados del dominio de planeación de la capacidad de la red.

II.7 DOMINIO DE PLANEACION DE LA CAPACIDAD DE LA RED

La planeación de la capacidad de la red es el proceso de determinación de una red óptima, teniendo como fundamento la base los datos de desempeño de la red, el flujo del tráfico, la utilización de los recursos, los requerimientos de conexión, los intercambios tecnológicos y el crecimiento estimado de las aplicaciones presentes y futuras. También se considera parte del proceso de planeación el establecimiento de reglas sobre el tamaño y número de interfases para el modelado de dispositivos.

La planeación de la capacidad de la red requiere de un amplio conocimiento de los cambiantes planes del negocio, su impacto en la red de comunicación y los avances en tecnología y arquitectura de comunicaciones. La meta final de la planeación de la capacidad de la red es llegar a establecer acuerdos de niveles de servicio utilizando la capacidad óptima de los recursos a un costo razonable. La optimización de la red puede verse como el proceso de balancear factores de diseño concernientes a la mejor configuración de la red dentro de las limitantes de factores como: disponibilidad, desempeño (tiempo de respuesta) y costo.

El proceso general de planeación de la capacidad de la red se refiere en cuatro fases.

Fase I : Determinando y cuantificando la carga de trabajo actual. En este paso se mide la carga de trabajo actual y después se utiliza una técnica para descomponerlo en elementos que representen segmentos discretos del negocio. Deben identificarse las herramientas y procedimientos de medición de dicha carga, y si es necesario, desarrollarlos y documentarlos. Comparando la utilización de recursos programada contra la medida resultan huecos en la planeación y se evitan malas interpretaciones en cuanto al consumo de los recursos e identificación de los componentes en general.

Fase II : Proyectando cargas de trabajo futuras. Esta fase requiere que el analista de planeación se comunique con la comunidad de usuarios finales, con los desarrolladores de aplicaciones y con los planificadores estratégicos del negocio a fin de obtener información acerca de aplicaciones futuras para determinar cargas de trabajo esperadas. Esta es la etapa más difícil y crítica en cualquier estudio de planeación de la capacidad.

Fase III : Desarrollando el Plan de capacidad de la red. Este proceso se basa principalmente en las guías técnicas de las características del hardware y/o software de los enlaces y nodos de la red. Después que se determinan los

puntos de actualización, debe planearse como se programará la implementación la cual toma en consideración períodos de tiempo para diseñar y proporcionar instalaciones y equipo.

Después que se completan estas tres fases, el Plan de capacidad se documenta y se presenta al administrador de los sistemas de información, a fin de que se estudie, en su caso se modifique y finalmente se implemente.

Fase IV : Implementación. Esta fase incluye solicitud de proposiciones, selección del proceso, preparación de operaciones y planes de conversión, elaboración de procedimientos de respaldo y recuperación, prototipos, evaluación de tensión y acuerdos finales con los usuarios.

DETERMINACION Y CUANTIFICACION DE LA CARGA DE TRABAJO ACTUAL

Las actividades que constituyen esta función son:

DETERMINACIÓN DEL NÚMERO DE ESTUDIOS A REALIZAR

Previo a desarrollar el estudio de planeación de la capacidad de la red, debe determinarse el número de estudios individuales requeridos por cada unidad de negocios. Este número depende de la naturaleza de las aplicaciones que soporta cada unidad de negocios.

CUANTIFICACIÓN DE LA CARGA DE TRABAJO ACTUAL QUE SE PRESENTA EN LAS INSTALACIONES DE LA RED

El primer paso en el desarrollo del estudio de capacidad de la red, consiste en colectar, analizar y clasificar los datos provenientes de diversas fuentes que reflejen su uso reciente. "Fuente" se utiliza como un término genérico que abarca las instalaciones y el equipo de la red. El segundo paso hace uso de técnicas grupales para categorizar la demanda de recursos. Por cada unidad de negocios deben describirse claramente las características que en materia de carga de trabajo presenta

cada aplicación sobre las instalaciones y equipo en lo individual utilizado para transportar los datos de transacciones de/hacia una aplicación. El tercer paso correlaciona elementos de la unidad de negocio con la demanda de recursos, esta correlación es conocida como una unidad de pronósticos natural. El resultado - el factor de las ecuaciones - se utiliza para proyectar las cargas de trabajo.

Cuantificación de la carga de trabajo actual del equipo de la red

Actualmente, es extremadamente difícil obtener datos cuantitativos de la utilización de equipos como procesadores front-end, multiplexores, modems, conmutadores y gateways que conectan LANs, MANs y WANs. Por ello se cuantifican en conjunto con las instalaciones.

Determinación del uso actual de los recursos

Primero debemos contar con la información recolectada por los dispositivos de monitoreo, para obtener después los siguientes elementos: número de transacciones por día y hora por cada aplicación y locación; número de transacciones en horas pico por aplicación y locación; número de transacciones durante un segundo promedio en horas pico por aplicación y locación; utilización de las instalaciones de comunicación y todos los demás precedentes a nivel del punto de vista global del centro de datos.

Comparación del uso actual contra la demanda de recursos proyectada

Utilizando las técnicas de recolección de datos pueden mostrarse las desviaciones entre el consumo de recursos actual y el proyectado. Si las desviaciones son significativas (+ del 15%), el analista debe identificar el origen de dichas desviaciones. Algunas razones posibles son: datos globales incluidos en la proyección, hipoestimación de cargas de trabajo en situaciones de contingencia, sobreestimación del impacto originado por la comprensión y compactación de datos, etc. En la mayoría de los casos, se puede pensar que el origen es una combinación de varias razones. Después de que se han analizado algunos ciclos de planeación se tornan más identificables las causas de desviación más frecuentes.

Después de completar esta fase estamos muy cerca de conocer la carga de trabajo actual y la demanda de recursos en las instalaciones de la red y parcialmente en todos los equipos de la red. Sin la exactitud suficiente en la cuantificación de la carga de trabajo actual no es posible lograr una buena proyección de demandas futuras de recursos por las cargas de trabajo actuales y futuras.

PROYECCION DE FUTURAS CARGAS DE TRABAJO

Esta fase identificará y cuantificará virtualmente todos los eventos futuros que afectarán los requerimientos por carga de trabajo. En adelante, las proyecciones deben realizarse sobre la carga total de trabajo futura.

La determinación de requerimientos futuros de carga de trabajo, es la tarea más difícil en el desarrollo del estudio de la capacidad de la red. Para lograr el objetivo exitosamente, el analista de planeación necesitará comunicarse con diversas áreas dentro de la compañía. También deberá revisar el plan estratégico de la compañía, el cual identifica todas las actividades necesarias para soportar las estrategias y los objetivos del negocio de la mejor forma. El objetivo de esta labor es identificar potenciales incrementos en el uso de las aplicaciones existentes; nuevas aplicaciones potenciales y tasas ad-hoc de futura actividad del usuario final. Los pasos para desarrollar esta función son:

- Identificar futuras cargas de trabajo en las instalaciones de comunicación
- Cuantificar futuras cargas de trabajo en los servicios
- Identificar futuras conexiones
- Evaluar nuevas tecnologías
- Consolidar estimados de futuras cargas de trabajo
- Identificar y cuantificar cargas de trabajo en posibles situaciones de contingencia
- Sumarizar el total de cargas de trabajo por ubicación

La información necesaria para realizar esta etapa proviene de las investigaciones que efectúe el analista con los usuarios y los desarrolladores de aplicaciones.

DESARROLLO DEL PLAN DE CAPACIDAD DE LA RED

Como resultado de las fases previas debe estar disponible la siguiente información antes de iniciar esta fase:

- Utilización actual de recursos, clasificada por promedio y horas pico
- Demanda de recursos de cada aplicación principal
- Proyecciones de cargas de trabajo, repartidas por promedio y máximos por usuario y por aplicaciones
- Estimados generales por recursos, carga de trabajo, sistemas operativos y programas de red
- Configuración existente

Los pasos de esta fase son :

DEFINICION DEL PROCEDIMIENTO GENERAL DE INSTALACIONES

Una instalación es una ruta de transmisión entre dos o más ubicaciones no incluyendo equipo terminal y de señalización. La adición de equipo terminal puede producir un canal, una línea o una troncal. La capacidad de las instalaciones es el nivel de utilización después del cual la instalación se encuentra no apta para realizar el trabajo dentro de los límites del nivel de servicio. La instalación ha alcanzado su capacidad máxima cuando su grado de uso ha llegado a un nivel en el cual el servicio solicitado no puede darse.

DEFINICION DEL PROCEDIMIENTO GENERAL DEL EQUIPO

El equipo es un término genérico que incluye todos los componentes de la red no definidos como instalaciones. La capacidad del equipo es el promedio de uso del mismo después de la cual no podrá trabajar correctamente. Un equipo ha alcanzado

su capacidad límite cuando se ha utilizado hasta alcanzar un punto en el que no pueden cumplirse los niveles de servicio.

EVALUACION DE CONFIGURACIONES ALTERNAS

Como resultado de la comparación entre la demanda de recursos y la capacidad disponible, se determinan las actualizaciones a determinados puntos de la capacidad de la red. Se identifican los espacios que deben cubrirse para lograr capacidad adicional o nueva capacidad. En ambos casos, las alternativas de reconfiguración deben evaluarse cuantitativamente. Para realizar esta evaluación podemos considerar cuatro alternativas:

- Uso de hojas de cálculo
- Uso de paquetes de modelado semisofisticados basados en PC
- Uso de paquetes de modelado avanzados
- Uso de simuladores

DEFINICION DEL PLAN DE ACTUALIZACION DE INSTALACIONES Y EQUIPO

La selección de la alternativa correcta de actualización debe satisfacer dos objetivos que en su naturaleza son contradictorios. El primero, debe minimizar el costo, lo que implica que debe mantenerse por debajo del nivel de capacidad deseada. El segundo, busca que las interrupciones a las operaciones se reduzcan al máximo mediante la instalación de recursos con capacidad suficiente (generalmente más costosos) de manera que la frecuencia con que se actualizan los equipos disminuya.

IMPLEMENTACION

La implementación consiste en la planeación de todas las actividades relacionadas con la actualización o instalación de componentes o conexiones. Estas actividades que son en parte administrativas y en parte técnicas se enumeran a continuación:

= Solicitud de propuestas. Es solicitar proposiciones para:

- Selección de instalaciones y equipo

- Selección de servicios de comunicación

- Selección de servicios con valor agregado

= Establecer criterios de selección y peso previo a la evaluación.

= Manuales de operación. Basados en las guías que se establecieron en el paso uno, y las decisiones de hardware y software del paso dos, deben prepararse los manuales de operación que describirán como debe utilizarse la red, sus componentes, instalaciones y servicios.

= Planes de conversión. Detallan los productos necesarios que deben instalarse y los períodos de tiempo necesarios para el desarrollo de estándares y procedimientos, aplicación del programa de capacitación y administración de la instalación.

= Plan de respaldo y recuperación. Cuando la red falla, el control operacional de la misma debe estar listo con un plan de acción preconcebido. Los planes de recuperación y contingencia se vuelven elementos clave en la operación de una red con servicio ininterrumpible. Debido a la importancia de una red, es esencial que haya planes predefinidos para restaurar el servicio en caso de que se presenten circunstancias inusuales. Se requieren 2 planes:

- Plan de Contingencia. Contiene las formas en las que la red puede ser temporalmente reconfigurada para sobrellevar la falla de uno de sus componentes y permitir la operación contínua de la misma durante el tiempo que tome resolver el problema.

- Plan de Recuperación. Define los métodos disponibles para restaurar a un solo elemento o a la red por completo a un estado de operación.

= Programación de cortes. De acuerdo al Plan de actualización, la implementación normalmente se lleva en varias etapas. La mejor forma de conducir la implementación es mediante fases cortas por ubicación o aplicación.

= Evaluación de tensión. Utilizando esta técnica, se pueden evaluar no solo la funcionalidad de la red sino también el nivel de servicio. Realizando un uso lo más intenso posible de las instalaciones, se vuelve más significativa la posibilidad de identificar posibles cuellos de botella. De esta forma; también el personal de operación

y de comunicaciones se entrena para hacer frente a todas las eventualidades posibles antes de la implementación.

= Procesos paralelos de volumen actual. Es recomendable que se evalúen los recursos instalados asignándoles tipos y volumenes de transacciones que emulen el sistema actual de la forma más parecida posible antes de que se de lugar a la transición. Si los resultados son satisfactorios, se encuentran los niveles de servicio adecuados y el personal esta entrenado adecuadamente, la implementación podrá realizarse completa y exitosamente.

CAPITULO III. DOMINIO DE SEGURIDAD

III.1 ASPECTOS GENERALES DE SEGURIDAD

A la seguridad de la red le concierne principalmente la protección de los componentes que la conforman contra: la divulgación de información, la modificación de datos, el uso no autorizado de recursos y la destrucción de sus componentes. La seguridad de los sistemas de procesamiento de datos y de las instalaciones de cómputo/comunicación ha sido objeto de interés y estudio por mucho tiempo. Con las redes de comunicación, estos intereses se combinaron e incrementaron, y por lo tanto, los problemas se agravaron.

La seguridad es necesaria en un ambiente donde los elementos que lo constituyen o la información que se maneja en él no deben estar disponibles para cualquier persona. En las redes de comunicación tiene interés primordial la seguridad de la información que pasa entre los sistemas interconectados.

Así como evolucionan las técnicas de comunicación, las oportunidades de interceptar la información mejoran y la necesidad de más y mejores mecanismos de protección crece. La llegada de técnicas de comunicación, y el arribo de las computadoras con vastas y mejoradas capacidades para procesar y almacenar información trajo consigo nuevas formas de comprometer la información.

La historia de la seguridad en cómputo inició hace 25 años cuando se introdujo un cambio en los sistemas operativos de mainframes. Al unísono IBM, DEC, y otras empresas anunciaron un esfuerzo mayor para implementar un esquema de seguridad activo dentro de sus sistemas operativos. Representaciones del gobierno estadounidense, del Departamento de Defensa de los E.U. (Department of Defense DOD) y de la comunidad académica propusieron las características necesarias para construir dichos sistemas operativos seguros para mainframes [NOV94].

A través de los años, la industria y el gobierno de los E.U. han gastado billones de dólares tratando de alcanzar la aludida condición de mantener un sitio seguro y controlado para procesar, intercambiar y almacenar información.

Hoy en día, las redes se han convertido en la columna vertebral de muchas compañías. Virtualmente todos los aspectos del trabajo diario dependen de las comunicaciones, tanto de voz como de datos, imagenes o cualquier otra combinación que exista ahora o en el futuro. Es por ello que debemos poner particular atención a tales recursos.

CLASIFICACION DE SEGURIDAD MILITAR/GUBERNAMENTAL DE LOS E.U.

En octubre de 1967, el gobierno de E.U. formó un grupo de trabajo en materia de Defensa a fin de establecer salvaguardas que proporcionarán seguridad a las computadoras y protegieran la información clasificada ubicada en sitios remotos y los recursos compartibles entre diversos sistemas de cómputo. Su reporte final denominado "Controles de seguridad para sistemas de cómputo" (Security Controls for Computer Systems) publicado en febrero de 1970 establece políticas y recomendaciones técnicas para reducir las amenazas a tales elementos.

Este documento representó el fundamento para la definición de una base de cómputo confiable y de los criterios de evaluación que podrían aplicarse a sistemas electrónicos de procesamiento de datos (Electronic data processing EDP) disponibles comercialmente.

Los criterios se aplicarían no solamente para la adquisición de sistemas EDP sino para su operación diaria. La clasificación de sistemas EDP fue formulada en dos conjuntos distintos de requerimientos: requerimientos específicos de características de seguridad y requerimientos de garantía. Estos requerimientos fueron codificados en un grupo de estándares titulados "Criterios de evaluación para Sistemas de cómputo confiables" (Trusted Computer System Evaluation Criteria) emitidos en diciembre de 1985 (conocido también como DOD85 o el Libro Naranja - Orange Book).

Estos estándares fueron trasladados a las redes de comunicación en un documento posterior, publicado el 31 de julio de 1987 y denominado "Interpretación

de red confiable de los Criterios de evaluación de cómputo confiable" (Trusted Network Interpretation of the Trusted Computer Evaluation Criteria) conocido también como el Libro Rojo - Red Book, y en otro documento que lo acompaña denominado "Líneamientos de ambientes para la interpretación de redes confiables" (Trusted Network interpretation Enviroments Guideline) publicado el 1o. de Agosto de 1990 [NOV94].

Estos documentos describen siete clases de seguridad, cada una progresivamente más restrictiva:

Clave	Descripción
D	Protección Mínima
C1	Protección de seguridad discrecional
C2	Protección de acceso controlado
B1	Protección de seguridad etiquetada
B2	Protección estructurada
B3	Dominios de seguridad
A1	Diseño verificado

Cada una de estas clases establece diversas medidas para alcanzar los siguientes requerimientos:

- Política de seguridad: Debe imponerse por parte del sistema una política de seguridad explícita y bien definida.

- Identificación: Todo sujeto debe ser identificado de forma única y deben verificarse todas las solicitudes de acceso.

- Etiquetado: Todo objeto debe estar asociado con una "etiqueta" que indique el nivel de seguridad del objeto

- Contabilización: El sistema debe mantener completos los registro de acciones que afectan la seguridad. Dichas acciones incluyen: alta de usuarios, asignación de derechos, cambio de nivel de seguridad e intentos de acceso denegados.

- Garantía: El sistema debe contar con mecanismos que impongan la seguridad, y de ser posible, medir la efectividad de estos mecanismos.

- Protección continua : Los mecanismos de hardware y software que implementan la seguridad deben protegerse contra cambios no autorizados

Estos requerimientos posteriormente son separados en criterios específicos los cuales son incorporados de diversas maneras en los rangos de D,C1,C2,B1,B2 y A. Esta fragmentación se muestra en la siguiente tabla :

Criterios	Clases						
	D	C1	C2	B1	B2	B3	A1
Políticas de seguridad							
Control de Acceso discrecional	X	R	R	-	-	R	-
Reuso de objetos	X	X	R	-	-	-	-
Etiquetas	X	X	X	R	R	-	-
Integridad de etiquetas	X	X	X	R	-	-	-
Exportac. de inform. etiquetada	X	X	X	R	-	-	-
Etiquetar salidas entendibles p/humano	X	X	X	R	-	-	-
Control de Acceso obligatorio	X	X	X	R	R	-	-
Etiquetas de sensibilidad del sujeto	X	X	X	X	R	-	-
Etiquetas de dispositivos	X	X	X	X	R	-	-
Cuentas de usuario							
Identificación y autentificación	X	R	R	R	-	-	-
Auditoría	X	X	R	R	R	R	-
Ruta confiable	X	X	X	X	R	R	-
Garantía							
Arquitectura del sistema	X	R	R	R	R	R	-
Integridad del sistema	X	R	-	-	-	-	-
Evaluación de la seguridad	X	R	R	R	R	R	R
Diseño de especificación/verificación	X	X	X	R	R	R	R
Análisis de cobertura de canales	X	X	X	X	R	R	R
Instalación administrativa confiable	X	X	X	X	R	R	-
Recuperación confiable	X	X	X	X	X	R	-
Distribución confiable	X	X	X	X	X	X	R
Documentación							
Guía de usuario de caract. de segur.	X	R	-	-	-	-	-
Manual de Instalaciones confiables	X	R	R	R	R	R	-

Documentación de evaluación	X	R	-	-	R	-	R
Diseño de documentación	X	R	-	R	R	R	R

X = No requerido
- = El mismo requerimiento que la clase inferior
R = Requerimiento adicional al de la clase inferior [NOV94]

Una vez que estos requerimientos se establecieron, se encomendó a las empresas de cómputo la incorporación de estos criterios en sus productos, a fin de producir sistemas que pudieran cubrir las diversas categorías de seguridad.

CLASIFICACION DE SEGURIDAD COMERCIAL

La clasificación anterior se condensó en un conjunto comercial más finito y orientado a la funcionalidad. Basado en las especificaciones del gobierno, la industria seleccionó los requerimientos más trascendentes para especificar su clasificación. Esta propuesta es más simple y homogénea que la estructura jerárquica de los militares y se presenta en la siguiente tabla:

Criterios	Clases			
	D	C	B	A
Seguridad				
Control de acceso discrecional	X	R	R	-
Reuso de objetos	X	R	-	-
Etiquetas	X	X	R	-
Integridad de etiquetas	X	X	R	-
Exportac. de inform. etiquetada	X	X	R	-
Etiquetar salidas entendibles p/humano	X	X	R	-
Control de Acceso obligatorio	X	X	R	-
Etiquetas de sensibilidad del sujeto	X	X	R	-
Etiquetas de dispositivos	X	X	R	-
Cuentas de usuario				
Identificación y autentificación	X	R	R	-
Auditoría	X	R	R	-
Ruta confiable	X	X	R	-
Garantía				

Arquitectura del sistema	X	R	R	-
Integridad del sistema	X	R	-	-
Evaluación de la seguridad	X	R	R	R
Diseño de especificación/verificación	X	X	R	R
Análisis de cobertura de canales	X	X	R	R
Instalación administrativa confiable	X	X	R	-
Recuperación confiable	X	X	R	-
Distribución confiable	X	X	X	R
Documentación				
Guía de usuario de caract. de segur.	X	R	-	-
Manual de instalaciones confiables	X	R	R	-
Documentación de evaluación	X	R	R	R
Diseño de documentación	X	R	R	R
X = No requerido - = El mismo requerimiento que la clase inferior R = Requerimiento adicional al de la clase inferior[NOV94]				

Las clases se definieron como sigue [NOV94]:

Clase D : Características de seguridad integradas en los sistemas operativos actuales y disponibles, las cuales normalmente no están habilitadas durante la instalación. Debido al bajo nivel de seguridad que proporciona esta clase, se recomienda evitar este tipo de esquema

Clase C : Es el conjunto de características de seguridad mínima recomendadas, que pueden ser examinadas e implementadas. Este nivel constituye una línea de base de seguridad sobre la cual se puede construir o fundar un sistema confiable

Clase B : Muchas compañías han asignado a sistemas no dedicados la función de manipular y transferir información sensitiva. Estos datos, clasificados como financieros, privados o propietarios son un bien salvaguardado y como tal debe protegerse por encima del nivel de seguridad normal.

Clase A : Esta clase generalmente no es una solución comecial viable. Su naturaleza restrictiva es difícil de implementar por su costo, y la sobrecarga de actividades que se genera puede limitar seriamente las capacidades de procesamiento y comunicación de los sistemas de aplicación que se ejecutan bajo esta clase.

III.2 EL DOMINIO DE SEGURIDAD

El dominio de seguridad como parte del modelo funcional de la administración de red, comprende el conjunto de funciones que aseguran la protección de la red y sus componentes en aspectos tales como: ingreso a la red, acceso a una aplicación, transferencia de información, protección de las herramientas de administración de red, minimización de riesgos, implementación del Plan de Seguridad de la red, y monitoreo de la estrategia de seguridad. Incluye también algunas funciones especiales como el examen de indicadores de seguridad, administración de pasaportes y generación de mensajes de advertencia o alarma en caso de violaciones.

Las empresas deben establecer políticas de seguridad para el uso de sus recursos de cómputo y telecomunicaciones así como para salvaguardar la información mientras sea almacenada o procesada por el sistema. Las políticas también deben reglamentar el mal uso o robo del equipo de cómputo y telecomunicaciones de la empresa, software, datos y documentación asociado a ellos. Las actividades del dominio de seguridad auxilian a [TER92]:

- Minimizar la posibilidad de ataques mediante el uso de un sistema de seguridad en capas que combine políticas y herramientas de hardware/software que construyan una trinchera uniforme contra los intrusos.

- Proporcionar una forma rápida y eficaz para detectar el uso no autorizado de recursos y determinar la cuenta de usuario donde se originó la violación. Esto aporta pistas de auditoría de la actividad del intruso.

- Facilitar al administrador de la red la reconstrucción manual de cualquier archivo o aplicación dañados y restaurar el sistema al estado previo al ataque. Esta característica de reconstrucción ayuda a disminuir los daños y permite recuperar el sistema

- Finalmente, monitorear a los intrusos y atraparlos por medio del grupo de operación de la red, finalizando con el castigo o prosecución consecuente.

Al dominio de seguridad y sus actividades le aquejan en la actualidad algunos problemas. Estos son [TER92]:

= El área de seguridad es desconocida para la mayoría de la gente involucrada en las actividades de comunicación de voz y datos, quienes además no cuentan con indicadores que señalen cuando se presenta una violación, consideran complicadas las técnicas de protección de la red y sus responsabilidades no están claramente asignadas.

= No existen políticas claras sobre que es lo que debe protegerse en un ambiente de red complejo; si deben ser las aplicaciones, bases de datos, archivos, nodos, enlaces de comunicación, dispositivos del usuario final, o una combinación de todo esto. Sin un análisis profundo y adecuado, los presupuestos no pueden asignarse apropiadamente a ninguna de estas áreas.

= Existe poco de conocimiento de quién comete las violaciones de seguridad y porque. En este sentido no están disponibles reportes y registros para las organizaciones. Las razones son:

- Las violaciones no son detectadas por el grupo de operación de la red.
- Las violaciones son detectadas, pero no reportadas por la administración porque admite que una violación puede originar que los usuarios tengan conciencia de la compañía a la que pertenecen y de la red que operan
- Las violaciones son realizadas por usuarios legítimos de la red que han encontrado formas de accesar aplicaciones y datos a los que no están autorizados

= La mayoría de las violaciones a la seguridad de los sistemas las cometen los empleados de la compañía en un 75% más que los externos (25% restante).

= Existen instrumentos pobres para el monitoreo de las instalaciones, LANs y dispositivos de usuario final. La mayoría de las soluciones de monitoreo disponibles protegen al procesador y a sus aplicaciones.

= El dominio de seguridad es considerado un gasto, por lo que es tratado con poca prioridad, lo que resulta en un presupuesto insuficiente.

Este panorama nos muestra la poca aceptación que tiene esta función para los administradores de una red. La falta de conocimiento en su instrumentación, técnicas y procedimientos provoca gran parte de estos problemas. A pesar de ello, un estudio profundo de la organización puede desarrollar un esquema de seguridad ad-hoc a ella.

Antes de continuar con los elementos del dominio de seguridad, vamos a despejar el ambiente típico de seguridad de un sistema. En él se diferencian claramente tres segmentos principales (Figura 3.1):

= Segmento de los intrusos potenciales, los cuales violan las reglas de forma activa y pasiva

= Funciones de monitoreo e inspección que detectan la violación y realizan acciones activas o pasivas en contra de ella, generando respuestas inmediatas o retardadas en contra del atacante

= Segmento de los agentes de seguridad. Esto incluye la definición de indicadores de seguridad y sus límites, utilizando guías para la generación de reportes, análisis de bitácoras, análisis de reportes, y toma de decisiones que deben tomarse contra los atacantes.

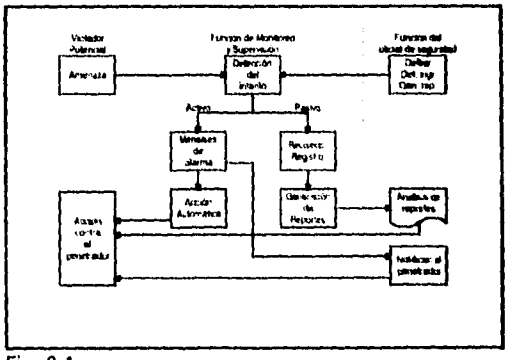


Fig. 3.1

Una vez establecido este esquema general del dominio de seguridad, procederemos a desarrollar todos los elementos que lo conforman a través de las funciones que realiza, los instrumentos que lo soportan y los recursos humanos que requiere.

III.3 ANALISIS DE RIESGOS

Cuando se está especificando el esquema de seguridad de un sistema (entendiendo como sistema un conjunto de elementos interrelacionados entre si), deben evaluarse cierto número de consideraciones, y para ello se debe cumplir con determinadas actividades. Parte del programa de seguridad debe definir la siguiente secuencia de pasos para llevar a cabo el análisis de la seguridad del sistema [WAT91]:

= Análisis de vulnerabilidad. Determina las partes vulnerables del sistema y evalúa las amenazas que pueden explotarlas. Algunas de las amenazas podrán tener poco riesgo asociado a ellas y por lo tanto pueden ser descartadas. Una herramienta útil para esta actividad es la matriz de amenazas, cuya estructura se muestra a continuación [TER92]:

Amenazas	Pasivas			Activas						Otros Probl	
Partes de la red	E.C.U	E.I.D	A.F.T	Rep.	Mod	Inser	I.F.	C.R	N.C.	R.F	F.O
Usuario-final	A	M	B	A	A	A	A	A	A	-	M
Estación de trabajo del usuario final	A	A	M	A	A	A	A	A	A	-	-
LAN											
Cable	M	M	M	M	M	M	M	M	M	M	M
Fibra	B	B	B	B	B	B	M	M	M	M	M
MAN											
Cable	B	B	M	B	B	M	M	M	M	B	-
Fibra	B	B	B	B	B	B	M	M	M	B	-
WAN											
Cable	A	A	A	A	A	A	M	A	M	-	-
Microondas	A	A	A	A	A	A	M	M	M	-	-
Fibra	B	B	B	B	B	B	M	B	M	-	-
Satélite	M	M	M	M	M	M	M	M	M	-	-
Componentes de procesamiento											
Sistemas operativos	B	B	B	M	M	B	M	M	B	B	M

Bases de datos	B	B	B	M	M	M	M	M	B	-	A
Aplicaciones	M	M	M	A	A	A	A	A	B	-	A
E.C.U = Escuchar conexión de usuario E.I.D = Escuchar intercambio de datos A.F.T = Analizar flujo de tráfico Rep. = Repetición Mod = Modificación						Inser = Inserción I.F. = Identidad falsa C.R = Congestión de la red N.C = Negar la comunicación R.F = Ruteo falso F.O = Falla en la operación					
Grado del Riesgo: A = Alto, M = Medio, B = Bajo											

= Análisis de resultados. Evalúa el beneficio potencial de un atacante al realizar cada amenaza, si la amenaza ofrece pocos beneficios normalmente se descarta.

= Análisis de costos. Evalúa el costo que debe cubrir el atacante por realizar cada amenaza. Cuando el costo es mayor que el beneficio, la amenaza puede descartarse

= Análisis de medidas de protección. Por cada amenaza restante se deben identificar los mecanismos de seguridad que pueden utilizarse contra ella.

= Justificación de mecanismos. Por cada amenaza hay que evaluar el costo e impacto en el desempeño de la red por introducir el mecanismo de seguridad que la contrarresta

= Evaluación de los requerimientos de seguridad. Debe determinarse el grado de seguridad requerido de acuerdo a la naturaleza de la aplicación que está utilizando la red. Cualquier aplicación que utiliza una red de computadoras debe asegurarse que las instalaciones proporcionadas por las computadoras involucradas y las interconexiones entre ellas son capaces de consolidar la suficiente seguridad para efectuar sus tareas.

Los elementos principales que se estudian en esta fase son las vulnerabilidades de los sistemas y de las redes de comunicación, las amenazas presentes en el ambiente de red y los métodos de ataque de los intrusos. A continuación abordaremos con más detalle cada uno de estos elementos.

VULNERABILIDADES

Como la ecuación riesgo/beneficio dicta, se requiere de un completo entendimiento de las amenazas antes de poder definir todo el ambiente de riesgo y las contramedidas requeridas. En 1970, el Dr. Willis Ware definió un conjunto de vulnerabilidades que se pueden encuentrar al utilizar un sistema de computación/comunicación [BAR85]. Los diferentes rangos de vulnerabilidades corresponden a los tradicionales problemas de usuarios/operadores/programadores y equipo de mantenimiento. Toda situación que implica computadoras y redes de comunicación incluye alguna mezcla de estas vulnerabilidades, las cuales son [BAR85]:

= Vulnerabilidad de la seguridad física. Las vulnerabilidades contenidas en esta clase incluyen todas aquellas actividades planeadas o circunstanciales que dañan físicamente los recursos de la red. Estas actividades incluyen fenómenos naturales como sismos, incendios, inundaciones y acciones humanas (ver seguridad física).

= Vulnerabilidad del personal. Una de las principales amenazas de las cuales hay que proteger la información crítica, es el personal en quien se ha confiado para realizar el manejo de la misma. Esta vulnerabilidad es tan real en un ambiente de computación/comunicación como cualquier otra, y frecuentemente se complica por el número de personas que deben adicionarse a la lista de personas de confianza.

= Vulnerabilidad de procedimientos. Se requiere tener un conjunto de procedimientos completo y razonable para la operación del sistema de comunicación, a fin de mantener protegida la información crítica. Los errores presentados en el cumplimiento de los procedimientos de verificación de la seguridad física y de las medidas de control de acceso pueden originar serios golpes a la integridad del sistema.

= Vulnerabilidad de las comunicaciones. Una vez que la información abandona el ambiente físico en el cual se generó o almacenó, es objeto de un análisis hóstil que es limitado solamente por el nivel de esfuerzo que el intruso hace por conocerla. Si la información es de valor limitado o perecedero, entonces serán suficientes las medidas que prestan poca protección. Sin embargo, si la información es de alto valor y/o retiene su valor por un largo período de tiempo, entonces pueden justificarse las

mejores medidas de protección disponibles.

= Vulnerabilidad del sistema de cómputo. Los grandes sistemas de cómputo que son repositorios de información crítica han operado por años protegiéndose solamente de las amenazas externas que provienen de usuarios no autorizados. Para muchas organizaciones, estas amenazas representan su mayor preocupación y están satisfechas proporcionando protección únicamente contra ellas. Sin embargo pueden ocurrir fallas en el hardware y/o software del sistema y también se deben establecer medidas de protección contra tales eventos, ya sean premeditados o accidentales.

AMENAZAS

Las vulnerabilidades se descubren a la vista cuando se presentan las amenazas. Las amenazas son las acciones que representan ataques potenciales a la red.

Una publicación del Departamento Nacional de Estándares del Reino Unido identifica algunos de los hechos que han contribuido para que crezca el interés por la seguridad en las organizaciones públicas y privadas [STA88]:

- Intentos planeados e intencionales para obtener información económica o de mercado de organizaciones competitivas en el sector privado.
- Intentos planeados e intencionales para obtener información económica de dependencias del gobierno
- Adquisición accidental de información económica o de mercado
- Adquisición accidental de información relacionada con individuos
- Fraude intencional mediante el acceso ilegal a los bancos de datos de un sistema, con el fin de adquirir datos de financiamiento, datos económicos, datos de aplicación de leyes y datos acerca de individuos
- Intrusión del gobierno en los derechos individuales
- Intrusión de las agencias de inteligencia en los derechos individuales

Los objetivos de las amenazas son:

- Interrumpir. El atacante trata de obtener información de un elemento de la red con el propósito de interrumpir el flujo de la misma.

- Violación de la integridad. El atacante trata de alterar la operación de un objeto o la interacción entre objetos con el fin de modificar la integridad del sistema

- Uso no autorizado de recursos. Se pueden realizar acciones en contra de los recursos que pueden poner en detrimento los intereses de la organización

- Uso no autorizado de recursos. Puede dar a los usuarios autorizados la oportunidad de ejecutar actividades que son perjudiciales para la organización. Estas actividades pueden ser intencionales o accidentales.

- Introducción de flujo de información no autorizada. El flujo de información debe ser controlado, no solo entre los usuarios finales, sino también entre los sistemas finales.

- Negativa de servicio. El atacante altera la operación de un elemento, la interacción entre objetos o la comunicación entre ellos para cancelar el servicio proporcionado por los mismos.

AMENAZA PASIVA

Es una explotación de la red donde no se efectúan alteraciones a los sistemas, su operación o mensajes (Figura 3.2).

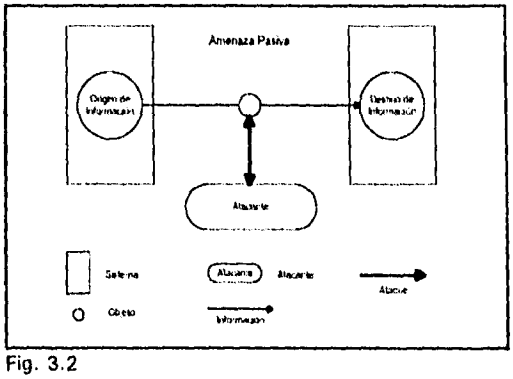


Fig. 3.2

Este tipo de amenaza generalmente se presenta en forma de observación no autorizada del comportamiento del sistema y de su información. Son difíciles de

detectar porque no alteran la información [STA88]. Este tipo de amenaza puede consistir en:

= Interceptar y escuchar el tráfico de comunicación con el propósito de identificar cada parte de la comunicación, obtener pasaportes para futuros usos no autorizados y para evaluar el intercambio de información. Esta acción da al intruso datos acerca de la naturaleza y contenido de los mensajes.

= Divulgar el contenido de las transmisiones. Una conversación telefónica, un mensaje del correo electrónico o un archivo transferido puede contener información crítica o confidencial. Podemos y debemos prevenir que el atacante aprenda o conozca el contenido de dichas transmisiones

= Analizar el flujo del tráfico. En esta actividad el atacante obtiene información acerca de volúmen de transacciones, dirección de transmisiones y períodos de tiempo, esto es, examina información vital. El análisis del flujo de tráfico funciona de la siguiente manera: supónga que el atacante tiene una forma de enmascarar el contenido de los mensajes u otra información de tráfico, de forma que si un mensaje ha sido capturado sea incapaz de extraer información de él. Si protegemos de esta forma al intruso solo le queda observar el patrón de los mensajes. Con ello, el atacante puede determinar la ubicación e identificación de las computadoras en comunicación y puede observar la frecuencia y longitud de los mensajes intercambiados. Esta información puede ser útil para adivinar la naturaleza de la comunicación que esta tomando lugar entre dichos sistemas.

AMENAZA ACTIVA

Es una explotación potencial donde pueden realizarse alteraciones a los sistemas, su operación o mensajes [STA88] (Figura 3.3).

Su objetivo principal es influir en el comportamiento del sistema. Las amenazas activas se presentan en forma de:

= Modificación de cadenas de caracteres en el mensaje. Significa que alguna porción de un mensaje legítimo se alteró porque se insertó o borró en partes o porque los mensajes son retrasados, reemplazados o reorganizados a fin causar

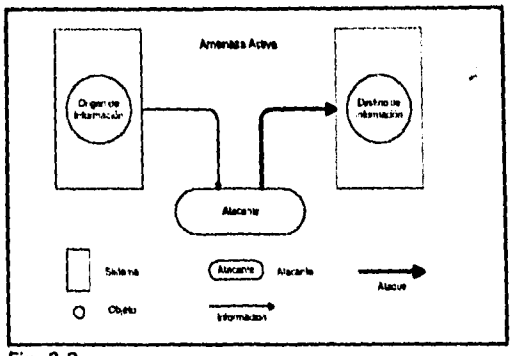


Fig. 3.3

confusión en el lado receptor, resultando una transmisión completamente falsa.

= Enmascaramiento. Toma lugar cuando una entidad pretende ser otra diferente, utilizando una identidad falsa, lo cual permite al intruso accesar a información que no tiene derecho a obtener.

= Repetición o retraso de la transferencia de información cuya finalidad es la de confundir a una de las partes en comunicación.

= Congestión del sistema de transmisión. Esto se logra insertando numerosos segmentos de información errónea, los cuales dificultarán la obtención de datos útiles de la transmisión. Este método es conocido también como inundación.

= Daños a las conexiones de comunicación en la parte receptora, lo cual causa confusión y serios daños al negocio.

METODOS DE ATAQUE

Un ataque es la realización o activación de una amenaza. Es la actividad que compromete la seguridad de la red y los sistemas que soporta. Los tipos de ataque que podemos encontrar son [WAT91]:

ATAQUES SOBRE OBJETOS EN INTERACCIÓN

El atacante intenta observar o modificar la operación de un elemento de red seleccionado.

Estos ataques se encuentran en la forma de:

= Un ataque de caballo de Troya. Es cuando un objeto es introducido en la red, presentándose ante ella para realizar un comportamiento autorizado y visible, pero con la consigna de comportarse de forma no autorizada.

= Un ataque interno. Sucede cuando una persona autorizada se comporta de manera no autorizada. Es similar al caballo de Troya salvo que el atacante es una persona, no a un objeto.

= Un ataque de trampa. Sucede cuando un objeto ha sido alterado para producir una acciónno autorizada cuando sea activado. Difiere del caballo de Troya en cuanto a que requiere reactivación. Con este mecanismo funcionan los virus.

ATAQUES EN OBJETOS AISLADOS

Un ataque en un objeto aislado requiere el establecimiento de un canal especial o de cobertura sobre el cual puede pasarse la información obtenida del objeto. El canal de cobertura necesita de un ataque del tipo del caballo de Troya o del de trampa para establecerse dentro del sistema que genera la información.

Se espera que el análisis de riesgos sea una función continua, con actualizaciones frecuentes. Su objetivo es mantener a la red a salvo de intrusos y violadores de seguridad. El análisis de riesgos debe incluir en su estudio todas las partes relevantes de la red de comunicación como son: Usuario final, estación de trabajo del usuario final, LANs, MANs, WANs y componentes de procesamiento (sistema operativo, base de datos, archivos y aplicaciones).

III.4 EVALUACION DE LOS SERVICIOS DE SEGURIDAD

A fin de evitar violaciones a la seguridad, deben estar disponibles algunos servicios, los cuales difieren en términos de:

- Sofisticación

- Costo
- Esfuerzo de implementación
- Esfuerzo de mantenimiento
- Demanda de recursos humanos

No existe un solo servicio que pueda prevenir todos los tipos de violaciones a la seguridad, pero una cuidadosa selección y combinación de estos servicios puede ayudar a adecuar soluciones y garantizar el funcionamiento del dominio de seguridad.

Dentro de los servicios más comunes tenemos [GAR91]:

SEGURIDAD FISICA

La seguridad física está relacionada con todo el medio ambiente que rodea los componentes de un sistema de cómputo/comunicación. Su ámbito comprende tanto la protección de los componentes de hardware como la protección de los elementos de software. A continuación se describirán algunos aspectos que se deben considerar para establecer la seguridad física de los componentes de la red.

PROTECCIÓN DEL HARDWARE

El ambiente

Los componentes de la red son dispositivos electrónicos complicados que solamente requieren el correcto balance de las condiciones físicas y ambientales que les permitan operar adecuadamente. Alterar este balance puede originar que fallen en forma inesperada e indeseable.

Fuego

Uno puede incrementar las oportunidades de que los equipos no sucumban entre las llamas asegurándose de que existe un buen equipo extintor cerca. En año recientes, los extintores de fuego de gas *Halón* se han vuelto muy populares en los centros de cómputo corporativos. Otra alternativa la constituyen los sistemas de aspersión. Muchas computadoras modernas no se dañan con los sistemas automáticos de aspersión, sin embargo hay que asegurarse que el equipo se encuentre

totalmente seco antes de volver a encenderlo. De cualquier forma, este último método no es muy recomendable para componentes electrónicos muy sensitivos.

Medidas:

- Verifique que cuenta con un extintor de fuego manual en la puerta de acceso al centro de cómputo/red y entrene a sus operadores en su uso cuando menos una vez al año.

- Si cuenta con un sistema de gas Halón o Bióxido de carbono, asegúrese que toda persona que ingrese al centro de cómputo sepa que hacer cuando suene la alarma y se activen dichos sistemas

- Si tiene un sistema de alarma en caso de incendio, hay que verificar que pueda anularse en caso de falsa alarma.

Humo

Es muy bueno para dañar el equipo de cómputo/red. El humo es un abrasivo potente que se acumula en las cabezas de los lectores de discos magnéticos, discos ópticos y unidades de cinta. Una sola partícula de humo puede causar daños severos a los medios de almacenamiento secundario.

Medidas:

- No permita que se fume en el centro de cómputo/red, o alrededor de la gente que utiliza los sistemas de cómputo/comunicación

- Instale detectores de humo en todas las habitaciones que contengan equipo de cómputo/comunicación

- Si tiene piso falso, coloque detectores de humo debajo del piso

Polvo

Como el humo, el polvo puede acumularse en las cabezas de discos magnéticos, unidades de cinta y unidades ópticas destruyendo lentamente la cabeza de grabación y el medio de almacenamiento. Por otro lado el polvo es conductor de electricidad y eventualmente causará que los circuitos sufran cortos y fallen.

Medidas:

- Conserve el centro de cómputo/red libre de polvo en la medida de lo posible

- Si su equipo cuenta con filtros de aire, limpielos regularmente

Temblores

Algunas partes del mundo son sujetas a frecuentes y severos temblores, otras los experimentan de forma ocasional. En un temblor algunos edificios sufren de verdaderos colapsos y otros permanecen de pie. Se debe poner cuidadosa atención a la ubicación de estantes y libreros en la oficina para poder incrementar las oportunidades de que los equipos sobrevivan en el peor de los desastres.

Medidas:

- Evite poner las computadoras en superficies elevadas
- No coloque objetos pesados en los estantes que estén cerca de los componentes de tal forma que podría caer sobre ellos durante un sismo
- Conserve los equipos lejos de las vantanas

Temperaturas extremas

Como la gente, los componentes electrónicos prefieren operar dentro de ciertos rangos de temperatura. La mayoría de los sistemas de cómputo se conservan entre los 50 y 90 grados Fahrenheit.

Medidas:

- Verifique la documentación de su equipo en cuanto a los rangos de temperatura puede tolerar
- Instale una alarma de temperatura en su centro de cómputo/red que se active cuando la temperatura es muy alta o muy baja

Ruido eléctrico

Una sumadora ordinaria enchufada dentro del mismo tomacorriente eléctrico que utiliza una estación de trabajo puede generar una descarga capaz de destruir la fuente de poder de la estación de trabajo.

Medidas:

- Verifique que no haya equipo que consuma mucha energía eléctrica en el circuito eléctrico que alimenta su sistema de cómputo/comunicación
- Si es posible, solicite un circuito eléctrico especial
- Instale un filtro de energía eléctrica en la fuente de poder de su equipo

- Si tiene problemas con la estática, puede aterrizar el área de cómputo/comunicación, o aplicar aerosol antiestático a la alfombra

- Los radio transmisores deben estar a una distancia mínima de 5 pies del equipo de cómputo, cables y periféricos

Agua

El agua puede destruir los componentes electrónicos. El daño principal es un corto eléctrico, el cual se presenta si el agua forma un "puente" entre una pista de un circuito impreso que lleva voltaje y una pista que lleva tierra. Un corto puede destruir componentes electrónicos al pasar corriente a través de ellos. El agua normalmente proviene de la lluvia o de las inundaciones. Algunas veces viene de un sistema de aspersión mal instalado.

Medidas:

- Aún si su centro de cómputo está localizado en el segundo piso, instale un sensor de agua en el piso

- Si cuenta con piso falso, coloque detectores de agua por debajo y por encima de él. Algunos detectores inclusive pueden cortar la energía eléctrica de los equipos automáticamente en caso de que se conecte la alarma

- No coloque los componentes de cómputo/comunicación en el sótano de su edificio si esta área es propensa a inundarse, o si su edificio cuenta con sistema de aspersión

Acceso físico

Piso y techo falso

En muchos edificios de oficina modernos, las paredes internas no se extienden sobre los pisos y techos falsos.

Medidas:

- Asegúrese que las paredes internas de su edificio se extiendan sobre el techo y/o piso falsos de las oficinas que deben tener acceso restringido

Salidas de ductos de aire

Si los ductos de aire que sirven el centro de cómputo/red son muy grandes, los intrusos pueden utilizarlos para ingresar sin autorización a un área segura.

Medidas:

- Las áreas que necesiten grandes volumenes de ventilación pueden ser servidas por muchos ductos pequeños, ninguno de los cuales debe ser lo suficientemente grande como para que una persona pueda introducirse. Como una alternativa, se pueden colocar rejillas en los ventiladores de aire.

Paredes de vidrio

Las paredes de vidrio son una mala elección desde el punto de vista de la seguridad. Son fáciles de romper y permiten observar a través de ellas, con lo que un intruso puede obtener conocimiento crítico (pasaportes) con la simple observación cuidadosa de la gente que está al otro lado de la ventana.

Medidas:

- Evite las paredes y los ventanales de cristal en áreas sensitivas de seguridad

Vandalismo

Los sistemas de cómputo son buenos objetivos para el vandalismo. El vandalismo en este ámbito es rápido, fácil y frecuentemente cuesta muy caro. Algunas razones para el vandalismo son:

- Interrupción intencional del servicio
- Venganza
- Motines, disturbios
- Violencia con ataques
- Diversión

En principio, cualquier parte de los componentes de la red - o del edificio que los alberga - puede ser objeto de vandalismo. En la práctica, algunos elementos son más vulnerables que otros.

Aberturas de ventilación

Los equipos que cuentan con estas aberturas las necesitan. No selle las aberturas para prevenir estos actos. Mejor observe políticas rígidas que no permitan introducir objetos como alimentos y bebidas en las áreas donde se localizan componentes electrónicos

Cables de red

Las LAN principalmente son muy vulnerables a este tipo de vandalismo. En muchos casos, cortando un solo cable con unas tijeras, un vándalo puede deshabilitar una subred de estaciones de trabajo. Comparado con Ethernet, los cables de dibra óptica son más vulnerables (porque pueden cortarse fácilmente) y son más difíciles de reparar (porque la fibra óptica no puede "reconectarse").

Medidas:

- Proteja físicamente sus cables de red. Coloque el cable dentro de un conductor eléctrico cuando sea instalado y podrá literalmente salvar mucho dinero en reparaciones y miles de horas de retraso

Conectores de red

Además de cortar un cable, un vándalo que tiene acceso a las terminales de la red - al conector de red - puede deshabilitar o dañar electronicamente la red. Las redes tipo Ethernet son especialmente vulnerables a problemas de tierra y con los *terminadores* de red. Simplemente, al remover un terminador al final del cable de la red o al aterrizar un conductor interno de Ethernet, toda la red puede volverse inoperable por completo

PROTECCIÓN DE LOS DATOS

Intercepción de la comunicación

La intercepción electrónica es quizá el tipo de pirateria de datos más siniestra. Aún utilizando un equipo modesto, es posible para un intruso hacer una transcripción completa de las acciones de la víctima - cada tecla oprimida, cada pieza de información vista en la pantalla o enviada a la impresora. La víctima mientras tanto,

no conoce de la presencia del intruso y despreocupadamente continúa sus labores, revelando no solamente información importante, sino pasaportes y procedimientos que pueden llevar al intruso a obtener información más importante.

En muchos casos es imposible saber si alguien monitorea la red. Algunas veces se conocerá la presencia de un intruso cuando trate de utilizar la información robada, lo cual significa que es muy tarde para prevenir el daño. Con cuidado y vigilancia, sin embargo, es posible decrementar significativamente el riesgo de ser monitoreado.

Intercepción de cables

Por su naturaleza, los cables eléctricos son candidatos idóneos para interceptar. Un intruso puede seguir una conversación entera con solo realizar un corte sencillo a un par de cables.

Medidas:

- Inspeccione periódicamente todos los cables de la red observando que no sufran de daño físico.

- Proteja sus cables del monitoreo de intrusos utilizando cable blindado.

- Si es muy importante la seguridad en su organización, coloque sus cables en conductos de acero. En aplicaciones que requieren de mucha seguridad, el conductor puede ser presurizado con gas. Los monitores de presión de gas pueden utilizarse para disparar un sistema de alarma en el caso de interferencia. Cabe mencionar que estas propuestas son caras de instalar y mantener.

Intercepción de Ethernet

Es recomendable inspeccionar periódicamente todos los números de estaciones que han sido conectados a la subred a fin de asegurarse que ninguna computadora no autorizada esta operando en la red local.

Intercepción por radio

Cualquier pieza de equipo eléctrico emite radiaciones en la forma de ondas de radio. Utilizando equipo especializado, es posible analizar la radiación emitida y generada por el equipo de cómputo/comunicación y determinar las operaciones que originaron la radiación. En los años 80's se desarrolló un sistema de certificación

denominado TEMPEST, el cual estima la susceptibilidad del equipo de cómputo a este tipo de monitoreo. El equipo que está certificado con TEMPEST es menos susceptible a la intercepción por radio que las computadoras que no lo son.

Respaldos

Los respaldos deben ser un prerequisito para la actividad de cualquier computadora/red. Mientras la información es almacenada en una computadora, los mecanismos de verificación y protección del sistema operativo previenen que gente no autorizada vea los datos. Una vez que la información es almacenada en una cinta de respaldo, cualquiera que tenga la posesión física de la cinta puede leer su contenido. Por está razón proteja sus respaldos, al menos como protege normalmente a sus componentes de cómputo/comunicación.

Medidas generales:

- No deje los respaldos olvidados y sin atender si su centro de cómputo/red es generalmente accesible a todo el personal
- No confíe sus respaldos a un mensajero que no es depositario de su confianza
- Sanee sus cintas de respaldo antes de reutilizarlas, utilicelas como cintas de emergencia o desechelas

Verifique sus respaldos

Revise los respaldos que tienen meses o años guardados, además de los que son del día o semana anterior. Algunas veces, los respaldos de archivos son borrados lentamente por las condiciones ambientales, la única forma de averiguar si ésto está sucediendo es verificando los respaldos periódicamente

Medidas:

- Al menos una vez al año verifique una de sus cintas de respaldo para asegurar que contiene datos válidos

Proteja sus respaldos

Para aumentar las oportunidades de que sobreviva su información en caso de un accidente o incidente inicuo, conserve los respaldos en diferente lugar al centro de cómputo/red.

Sanee sus medios de almacenamiento antes de desecharlos

Si tira sus cintas o cualquier otra pieza para grabar información, asegurese que los datos contenidos en las cintas han sido completamente borrados. Este proceso también es conocido como saneamiento. Un método de saneamiento común consiste en sobreescribir el disco o cinta por completo. Ahora que si uno es partidario de la alta seguridad y de la confidencialidad de la información en relación a los materiales podría sobreescribir en el disco o cinta muchas veces ya que los datos puede recobrarse de cintas que han sido sobreescritas una sola vez. Para lograr esto, comunmente las cintas son sobreescritas tres veces -una vez con bloques de ceros, la siguiente con bloques de unos y la final con ceros y unos esparcidos aleatoriamente.

Por otro lado es posible destruir físicamente las cintas de respaldo antes de tirarlas. Los incineradores pueden realizar bien este trabajo en las cintas y las trituradoras de papel en los diskettes, las técnicas de prensado son preferibles para las unidades de disco duro y los paquetes de discos.

Medidas:

- Sanee todos los medios de almacenamiento antes de desecharlos

Encriptamiento de respaldos

La seguridad de los respaldos puede ser substancialmente incrementada si encriptamos los datos almacenados en las cintas. Aunque el software de encriptamiento presenta hoy en día algunos problemas, es recomendable. Sin embargo hay que tomar en cuenta un detalle muy importante: si encripto el respaldo de un archivo del sistema y olvido la clave de encriptamiento, la información almacenada en el respaldo será inútil.

Almacenamiento local

Además de las computadoras y de los sistemas de almacenamiento en masa, muchas otras piezas de los equipos de procesamiento de datos electrónicos almacenan información. Naturalmente, cualquier pieza de memoria que es utilizada para conservar información crítica presenta un problema de seguridad - especialmente si dicha pieza de memoria no está protegida con un pasaporte, no está encriptada o no cuenta con

mecanismos similares. De cualquier forma, el almacenamiento local en muchos dispositivos representa un problema adicional de seguridad, ya que la información crítica es frecuentemente copiada en dicho medio sin el conocimiento del usuario.

Buffer de impresión

Las computadoras pueden transmitir información más rápido que la mayoría de las impresoras. Por ello, las impresoras son equipadas con un área de memoria para impresión - dispositivos con memoria semiconductora que reciben la información a la velocidad de la computadora y la transmiten a la impresora lentamente. Muchas áreas de impresión tienen la habilidad de hacer múltiples copias de un documento, algunas con solo apretar un botón que selecciona el número de copias. El riesgo en este caso es obvio: si cierta información crítica se encuentra aún en el buffer de la impresora, un intruso puede utilizar dicho botón para hacerse una copia. Por otro lado, hay que tener la precaución de limpiar las áreas de impresión de las impresoras laser despues de una impresión, ya que un intruso con habilidad suficiente puede obtener la información crítica en su totalidad o en partes.

Pantallas múltiples

Muchas terminales inteligentes están equipadas con múltiples pantallas de memoria, al presionar determinadas teclas, se puede ver la información que ya ha sido procesada en ellas. Cuando un usuario termina una sesión, la memoria utilizada para mantener la información presentada en la pantalla no se borra - aún cuando sea la pantalla principal.

Medidas:

- Asegúrese que al terminar su sesión todas las pantallas de memoria de su terminal se han borrado. Podría ser necesario enviar una secuencia de control o inclusive apagar la terminal para borrar su memoria.

Teclas de función

Muchas terminales inteligentes están equipadas con teclas de función que pueden ser programadas para enviar una secuencia arbitraria de caracteres a la computadora sin oprimir tecla alguna. Si alguna tecla de función es utilizada para almacenar un pasaporte, entonces cualquier persona que tenga acceso físico a la

terminal puede tomar el dato del pasaporte e ingresar al sistema.

Terminales no atendidas

Las terminales sin atender que los usuarios dejan conectadas al sistema, significan una atracción especial para un vándalo, que puede accesar los archivos de dicha persona con toda impunidad. Por otro lado, el vándalo puede utilizar la cuenta de la persona como punto de inicio para lanzar ataques contra el sistema de cómputo o la red entera: ya que cualquier seguimiento del ataque apuntará a la cuenta del usuario descuidado y no al vándalo.

Medidas:

- Nunca deje terminales sin atender por largos períodos de tiempo.

IDENTIFICACION Y AUTENTIFICACION

La autentificación es el proceso por el cual un usuario establece su identidad cuando accesa a un servicio o aplicación de la red. En la fase de identificación, el usuario introduce un identificador en el servidor, después de lo cual, el servidor pregunta por una autentificación o prueba de que el usuario és quién dice ser. La mayoría de los procesos de identificación utilizan una combinación de identificador y pasaporte como la clave para establecer un proceso de autentificación efectivo [NOV94].

VERIFICACION DE PASAPORTES

Antes de discutir algunos conceptos de I&A, debemos hablar brevemente acerca del significado de la verificación de pasaportes.

El pasaporte es un dispositivo utilizado para prevenir que una persona se "enmascare" como "otra" en la red. Su objetivo es evitar accesos no autorizados a recursos o datos de la red. Los usuarios proporcionan un pasaporte al servidor, el servidor comparará este dato con la copia que posee del pasaporte verdadero del usuario. Si son iguales, dará acceso al usuario.

Es importante que el mecanismo involucrado en la protección del pasaporte sea lo suficientemente robusto como para contrarrestar los ataques contra la seguridad de

la red a nivel de I&A.

Los mecanismos de protección de pasaportes pueden ser de naturaleza física y/o electrónica. La protección física de pasaportes puede cumplirse con no registrarlos, o con escoger aleatoriamente los pasaportes. La protección electrónica de pasaportes uitliza métodos matemáticos para "modificar" el pasaporte y con ello provocar que sea intelegible en otras manos excepto en las del servidor.

PROCESO BASICO DEL I&A

La identificación y autentificación implican más que solo teclear el identificador de ingreso y proporcionar un pasaporte para accesar. Técnicamente, el flujo básico de un proceso de I&A es como sigue :

= Conexión. La fase de conexión se refiere al proceso físico de accesar al medio de la red. Después se presenta la acción que decide cual servidor puede suministrar al cliente la información de red suficiente para permitir la comunicación temporal entre el cliente y el servidor en la red.

= Comunicación. En este punto, el contacto inicial con el medio de red ha sido establecido y el cliente y el servidor han creado una conexión de servicio lógica o ruta de comunicación no autentificada. Durante la fase de comunicación, es necesario que la estación de trabajo accese a objetos específicos de la red antes de que se apliquen las restricciones del proceso de autentificación.

= Identificación del usuario. Una vez establecido lo anterior, puede iniciar el proceso de identificación del usuario. En términos simplificados, la estación de trabajo solicita obtener información del directorio de la red al servidor de contacto inicial para buscar la identificación del usuario que corresponde al perfil suministrado.

= Autentificación del usuario. Si el servicio de directorio envía la respuesta que contiene los datos necesarios para completar el proceso de autentificación mutua entonces se ha completado esta fase.

= Control de accesos. Una vez verificada la identidad del usuario, el servidor debe proceder a asignarle los derechos que le corresponden mediante el control de accesos.

SEPARACION

La separación es un servicio de seguridad que se asegura que los elementos aislados puedan interactuar solamente por mecanismos de comunicación controlados y visibles [WAT91]. La separación puede aplicarse en diferentes niveles (Ver máquinas firewall) y es esencial para la operación segura de un sistema. La separación se basa en la creación de barreras entre elementos que necesitan protegerse unos de otros. La separación, por sí sola, no contrarresta todas las amenazas. Existe una necesidad de reglas la cuales deben especificar que elementos deben separarse de otros elementos o sujetos. Estás reglas son conocidas como reglas de seguridad, las cuales clasifican un objeto como elemento (el que necesita protección) o como sujeto (el objeto no confiable). La distinción entre objetos y sujetos variará dentro de una red de computadoras dependiendo del punto de vista del sistema bajo consideración.

Las reglas de seguridad para una red deben considerar las reglas individuales de seguridad de todas las aplicaciones que utilizan la red, así como especificar los requerimientos de seguridad de la red como un todo.

La separación se realiza en diferentes niveles y formas. Estos niveles son [WAT91]:

= Separación física. Los elementos están protegidos de atacantes potenciales colocándolos en diferentes ubicaciones. Para separar los elementos deben localizarse en máquinas físicamente separadas. El control de los elementos separados físicamente dependerá entonces del control de la comunicación entre ellos.

= Separación temporal. La separación temporal de elementos que utilizan un recurso común puede lograrse compartiendo dichos recursos por períodos de tiempo entre los elementos. Una computadora en particular de la red puede desempeñar pequeñas tareas de seguridad cuando se conecta a la red, pero se desconecta cuando desempeña tareas críticas. Cuando se presenta la conmutación entre elementos, es importante asegurarse que cualquier información relacionada con ellos sea removida del recurso común. Esto es para prevenir el uso de canales de cobertura.

= Separación Lógica. Los elementos son separados utilizando la separación física y la temporal a fin de obligar a que la interacción entre ellos ocurra a través de canales definidos y controlados.

= Separación por encriptamiento. En ella se separan los elementos mediante el uso de encriptamiento, lo cual garantiza que los atacantes no serán capaces de interpretar la información recibida. El encriptamiento crea canales lógicos separados a través de la red de comunicaciones.

CONTROL DE ACCESOS Y CAPACIDADES

El control de accesos a objetos (datos y programas) puede alcanzarse de diversas maneras. Para un control de accesos exitoso, debe existir un mecanismo que compare la identidad del usuario que intenta accesar a un objeto contra la lista de usuarios válidos especificados por el propietario del objeto [WAT91].

La correlación entre usuarios y derechos de acceso está descrita en una matriz de control de accesos (Figura 3.4). Los objetos que pueden ser accesados están representados por el eje horizontal y los usuarios/sujetos que desean accesar los objetos están representados por el eje vertical. La casilla donde convergen ambos ejes contiene los derechos de acceso de un sujeto a un objeto determinado.

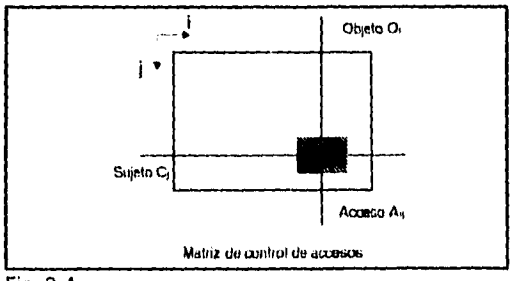


Fig. 3.4

Cuando un usuario completa la autentificación inicial requerida por el sistema, éste establece un proceso inicial para el usuario. El sistema pasa los derechos de acceso del usuario a los procesos de inicio. Estos derechos son controlados más

adelante por el sistema operativo, para limitar la extensión de operación del usuario y evitar un daño.

Los sujetos que requieren accesar pueden por tanto ser usuarios o procesos. Por otro lado, un grupo de usuarios puede compartir derechos de acceso idénticos, y por lo tanto formar un solo grupo. El objeto al cual se accesa es controlado variablemente de acuerdo al contexto. El punto de intersección de la matriz define elementos de acceso como: derechos de lectura, de escritura, de ejecución de programas, de insersión de datos en un archivo o de envío de datos a través de una ruta de comunicación.

Las matrices de control de accesos se utilizan para especificar derechos de acceso dentro de un sistema. Sin embargo, en la práctica, los sistemas requieren que esta información se represente en forma más compacta, lo cual se logra con las listas de control de accesos.

Listas de control de accesos

Intentan presentar los datos contenidos en una matriz de control de accesos de forma compacta. Cuando se comprime la columna de la matriz de acceso de un objeto determinado - de manera que no contenga elementos vacíos - describirá todos los grupos que tienen acceso a dicho objeto. Esta es la lista de control de accesos del objeto. Cada elemento de la lista debe contener un identificador único para el grupo apropiado.

Asegurar un identificador único para cada grupo es difícil de lograr en un sistema de red. Una propuesta a este respecto indica que cada sistema cuente con un subconjunto de grupos. Los usuarios que deseen unirse a un grupo accesarán primero su sistema huesped, y el identificador del grupo será entonces la concatenación del nombre local y el nombre del sistema que lo administra. El identificador es utilizado en forma encriptada y para seguridad adicional se le agrega una marca de tiempo y un tiempo de vida limitado.

CAPACIDADES

La matriz de acceso puede reducirse tomando un renglón correspondiente a un grupo y almacenando estos datos con el grupo, en lugar de todos los objetos. Cada elemento de esta nueva matriz unidimensional es llamado capacidad. Cuando el miembro de un grupo solicita accesar, presenta la capacidad como boleto de entrada para verificar que sus derechos de acceso existen.

COMBINANDO LISTAS DE CONTROL DE ACCESO CON CAPACIDADES

La lista de control de accesos permite un estricto control en la actividad de acceso y la posibilidad de cambiar esta actividad. Las capacidades proporcionan un mecanismo de verificación sencillo, sin embargo, no es fácil controlar los objetos que tienen un permiso de acceso. Las listas de control de acceso y las capacidades pueden combinarse permitiendo el acceso inicial a un objeto a través de la lista de control de acceso y creando una nueva capacidad para cualquier acceso subsecuente.

SEGURIDAD MULTINIVEL

El concepto de seguridad multinivel es un servicio aplicable en áreas donde la información puede organizarse en grandes categorías y donde los usuarios están autorizados con los permisos correspondientes para accesar ciertas categorías de datos [STA88]. Un sistema de seguridad multinivel debe imponer:

- No lecturas (No read up). Un sujeto puede leer solamente un objeto de menor o igual nivel de seguridad
- No escrituras (No write down). Un sujeto puede escribir en un objeto de mayor o igual nivel de seguridad.

Si estas reglas se establecen adecuadamente proporcionarán la seguridad multinivel. Para los sistema de procesamiento de datos, la propuesta que se ha tomado y ha sido objeto de investigación y desarrollo, está basada en el llamado monitor de referencia o núcleo de seguridad (Figura 3.5).

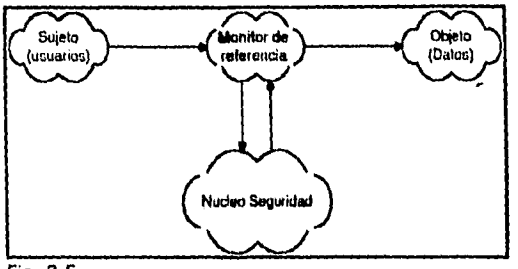


Fig. 3.5

El monitor de referencia controla el acceso de sujetos a objetos en base a los parámetros de seguridad del sujeto y dle objeto. El monitor de referencia impone las reglas de seguridad (no leer, no escribir) y tiene las siguientes propiedades:

= Medición completa. Las reglas de seguridad se aplican a todo acceso, y no solo cuando se efectúan ciertas operaciones (p.ej. abrir un archivo).

= Aislamiento. El monitor de referencia y la base de datos están protegidos contra modificaciones no autorizadas

= Verificable. Es probable la corrección/adecuación del monitor de referencia y también podemos demostrar de que el monitor de referencia si aplica las reglas de seguridad y proporciona intermediación y aislamiento completos.

ASEGURANDO LA INTEGRIDAD DE LOS DATOS

La integridad de un mensaje puede determinarse agregando campos adicionales dentro del mismo mensaje, como los campos *CRC* en la capa de enlace de datos. Si estos campos son correctos entonces cualquier modificación al mensaje por parte de un intruso implicará recalcular dichos campos. Si estos campos están incluidos dentro de la sección encriptada del mensaje, la modificación del mensaje sin alterar el método o clave de encriptamiento es más difícil de realizar. Alternativamente, el método de cálculo del campo de verificación puede ser un secreto común entre los dos sistemas en comunicación. Si los bits de verificación están correctos y el mensaje se desencripta correctamente entonces el mensaje debio provenir de un emisor confiable, y de esta forma el mensaje es autentificado por su

código y contenido. Adicionalmente se requiere que el mensaje contenga información que sólo el emisor puede crear. Esto es llamado signatura y es equivalente a la firma convencional de las personas.

Este mensaje signatado debe incluir una función de todo el mensaje de tal forma que ninguna parte del mensaje pueda modifiarse sin invalidar la signatura. La signatura depende de la informaión que sólo el emisor conoce, para evitar que un intruso pueda falsificarla El requerimiento final es que debe existir un mecanismo mediante el cual el receptor pueda validar la signatura.

EVITANDO EL ANALISIS DE FLUJO DEL TRAFICO

Este servicio en especial ayuda a prevenir que usuarios no autorizados obtengan conclusiones basados en el análisis de los patrones del tráfico de comunicación entre los diferentes tipos de usuarios. Esta protección debe considerar el encriptamiento entre puntos finales.

También se puede prevenir el análisis de flujo de tráfico utilizando mensajes de relleno para completar los espacios de tiempo entre transmisiones reales de datos.

CONFIRMACION DE EMISOR Y/O RECEPTOR

El emisor/receptor recibe una confirmación (acknowledgment) que indica que cierto monto de información ha sido enviado/recibido. Este servicio ayuda a evitar debates ocasionales sobre intercambios de información no protocolados propiamente entre emisor o receptor.

III.5 TECNICAS PARA EL DOMINIO DE SEGURIDAD

Los servicios de seguridad se auxilian de técnicas para poder funcionar adecuadamente. Algunas de las técnicas que auxilian al dominio de seguridad son:

CRIPTOGRAFIA

Como la bóveda de un banco, la seguridad de la información se ha basado en el concepto de una combinación secreta. El emisor asegura la información transmitida con una combinación secreta o clave, y el receptor es la única persona que conoce la clave y puede decodificar la información durante la recepción. Como en el caso de la bóveda, es teóricamente imposible acertar la combinación correcta por ensayo y error. Además, si la combinación tiene un número lo suficientemente largo de dígitos, el número de posibles combinaciones hace prácticamente imposible abrir la bóveda de esta forma [ROS82].

La criptografía se refiere al método y proceso de transformar texto intelegible a una forma no intelegible y reconvertir la forma no intelegible a la original a través de un proceso inverso de transformación. Este proceso se denomina encriptamiento y el proceso inverso se conoce como desencriptamiento [BAR85].

El proceso de encriptamiento toma lugar como una manipulación lógica/matemática del mensaje del emisor, con un proceso de manipulación inverso que toma lugar en el receptor final. En las comunicaciones binarias, el proceso matemático puede consistir simplemente en la adición binaria o la adición de una secuencia escogida aleatoriamente de longitud similar a la longitud del mensaje. Si la clave escogida al azar es al menos tan grande como el mensaje, y se utiliza una sola vez, entonces el mensaje es seguro y no puede violarse. Una llave de longitud finita puede ser lo suficientemente larga como para asegurar un nivel de seguridad convencional, lo que indica que tratar de determinar la clave apropiada por medio de una búsqueda es imposible en un sentido práctico. Se pueden utilizar las siguientes técnicas para lograr este proceso:

- Transposición. Realiza un desarreglo de la secuencia del mensaje, una mezcla aleatoria de letras que alteran el orden del mensaje.
- Substitución. Es el reemplazo de las letras del mensaje por símbolos, números y otras letras.

Algunos de los métodos de encriptamiento más comunes son:

ALGORITMO ESTÁNDAR DE ENCRIPTAMIENTO DE DATOS

(Algoritmo DES - Data Encription Standard). Fue la publicación número 46 del año de 1977 de los Estándares Federales de Procesamiento de Información (Federal Information Processing Standards FIPS) la que definió el estándar de encriptamiento de datos (Data Encription Standard DES) como una métrica federal para el Departamento Nacional de Estándares de E.U. Su objetivo fue que los organismos federales utilizarán DES para todas las comunicaciones de datos no clasificados pero importantes [STA88].

El algoritmo DES opera en bloques de texto plano de 64 bits (o texto cifrado), requiere una clave de 64 bits y produce bloques de texto encriptado de 64 bits (o texto plano). De la clave de 64 bits, solo se utilizan 56 bits en el proceso de encriptamiento, los ocho bits restantes conforman la paridad por cada byte de la clave. Por lo tanto, el número de claves diferentes disponibles es de 2^{56}. Desde el momento en que se conoce el algoritmo de DES, la seguridad del sistema es totalmente dependiente del secreto de la clave.

ENLACE ENCRIPTADO

Las técnicas de encriptamiento que se aplican a los sistemas de comunicación se encuentran comúnmente en forma de enlace encriptado, el cual implica que un par de dispositivos de encriptamiento se ubican en ambos puntos finales del enlace. Una vez que han sincronizado su operación, estos dispositivos convierten la información que fluye a través del enlace, de modo que las amenazas de intercepción activas y pasivas son frustradas. El ingrediente esencial en la sincronización de los dispositivos del enlace encriptado es que ambos posean la misma clave de encriptamiento. La clave es el punto de inicio para el proceso de encriptamiento, y tan pronto como ambos puntos finales cuenten con ella, serán capaces de comunicarse. La clave se convierte en el punto crucial del sistema al cual se proporciona protección. Si la clave se pierde o se compromete, entonces un intruso podrá utilizarla fácilmente para

desencriptar la comunicación que ha sido previamente interceptada sobre la línea. Por lo tanto se vuelve importante no solamente proteger la clave sino también establecer formas confiables para pasar nuevas claves a ambos puntos del enlace [BAR85] (Figura 3.6).

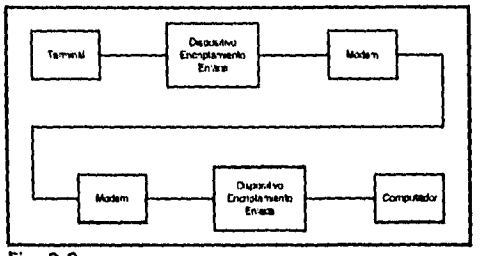


Fig. 3.6

ENCRIPTAMIENTO END-TO-END

Otra aplicación importante de encriptamiento en los sistemas de comunicación es denominado encriptamiento end-to-end. La diferencia entre este encriptamiento y el enlace encriptado es que la información que se enviará entre los dos puntos es encriptada antes de que ingrese a la red de comunicaciones y permanece así aún después de que ha dejado la red. Con esta propuesta, no hay necesidad de que los operadores de la red posean conocimiento del sistema de comunicación ya que ellos no tienen acceso directo a la información que fluye en la red. El enlace encriptado en conjunción con el encriptamiento end-to-end proporciona protección contra amenazas al flujo de información por intercepciones externas o radio intercepciones. Cuando se emplea el encriptamiento end-to-end, los operadores de la red de comunicación están impedidos para obtener acceso al contenido de los mensajes, aunque no hay forma de impedirles que obtengan información del flujo del tráfico [BAR85].

PROGRAMA DE APOYO A LA SEGURIDAD DE LAS COMUNICACIONES COMERCIALES

Si bien el encriptamiento end-to-end aún tiene vida útil por un tiempo razonable, es muy cierto que algunas organizaciones no gubernamentales están comenzando a buscar reemplazos porque ven que se incrementa la vulnerabilidad de este algoritmo.

El reemplazo más probable es una familia de algoritmos desarrollados bajo el Programa de apoyo a la seguridad de las comunicaciones comerciales (Commertial Communications Security Endorsement Program CCSEP) de la Agencia de seguridad nacional (National Security Agency NSA) de los E.U. CCSEP es un esfuerzo conjunto de la NSA con la industria para producir una nueva generación de dispositivos de encriptamiento que son más seguros que el encriptamiento end-to-end, son de bajo costo y capaces de operar con grandes volúmenes de datos. Algunas características de los nuevos algoritmos CCSEP son:

= Los algoritmos CCSEP son desarrollados por la NSA y son clasificados. Así, los algoritmos por si mismos conservan el secreto y son sujetos a cambios en determinados períodos.

= Los participantes de la industria producirán la implementación en *chip* de los algoritmos, pero la NSA mantiene el control sobre el diseño, fabricación y distribución de los chips.

Dos tipos de algoritmos vienen bajo el encabezado del CCSEP. Los algoritmos del Tipo I están diseñados para proteger información clasificada. El equipo que utiliza el CCSEP del Tipo I estará disponible solamente para las agencias del gobierno y sus contratistas. Los algoritmos del Tipo II están diseñados para proteger información sensitiva y no clasificada. Las soluciones Tipo II intentan reemplazar el encriptamiento end-to-end [STA88].

Distribución de claves

Para que un escriptamiento convencional funcione, las dos partes del intercambio deben contar con la misma clave, y dicha clave debe mantenerse a salvo del conocimiento de otras personas. Más que eso, es deseable un cambiofrecuente de claves para limitar el monto de datos comprometidos en caso de que un intruso se aprenda la clave. Por esto, la fortaleza de cualquier sistema de encriptamiento reside en su técnica de distribución de claves, un término que especifica las formas de entregar una clave a dos partes que desean intercambiar datos, sin permitir a otros ver la clave. La distribución de claves puede alcanzarse en un número de formas diversas.

Para dos partes A y B:

- Una clave puede seleccionarse por A y entregarse físicamente a B
- Una parte tercera puede seleccionar la clave y entregarla físicamente a ambas partes
- Si A y B tienen una conexión encriptada a una tercera parte C, C puede entregar una clave en los enlaces encriptados de A y B.

Un esquema donde se implementa la técnica de distribución de claves es [STA88]:

= Clave de sesión: Cuando dos sistemas finales desean comunicarse, establecen una conexión lógica. Durante la duración de tales conexiones lógicas, se encriptan todos los datos del usuario con una clave de sesión que dura una vez por conexión. Al final de la conexión, la clave de sesión se destruye

= Clave permanente: Es utilizada entre ambas entidades con el propósito de distribuir claves de sesión. Esta configuración consiste de los siguientes elementos:

- Centro de control de accesos : determina cuales sistemas tienen permitido comunicarse uno con otro.
- Centro de distribución de claves : Cuando el permiso es autorizado por el centro de control de accesos para los dos sistemas que establecen una conexión, el centro de distribución de claves proporciona una clave de sesión que dura solamente el tiempo que permanezca la conexión.
- Unidad de interfase de la red : ejecuta un encriptamiento end-to-end y obtiene claves de sesión para la computadora o terminal.

Encriptamiento de clave pública

Como hemos visto, una de las dificultades principales con los esquemas de encriptamiento convencionales es la necesidad de distribuir la clave de una manera segura. Una forma ingeniosa de cumplir con este requerimiento nos la muestra un esquema de encriptamiento que sorpresivamente no requiere distribución de claves. Este esquema es conocido como encriptamiento de clave pública.

Para esquemas de encriptamiento convencionales, las claves utilizadas para encriptar y desencriptar son las mismas, sin embargo, esta no es una condición necesaria. En cambio, es posible desarrollar un algoritmo que utilice una clave para encriptar y una contraparte con claves diferentes para desencriptar, con lo que además, es posible desarrollar nuevos algoritmos. Sin embargo, la clave de encriptamiento no es suficiente para determinar la clave de desencriptamiento. De este modo, la técnica trabajará de la siguiente forma :

= Cada sistema final en una red genera un par de claves de encriptamiento y desencriptamiento

= Cada sistema publica su clave de encriptamiento y la coloca en un registro público o archivo. Esta es la clave pública. La clave compañero se conserva privada

= Si A desea enviar un mensaje a B, encripta el mensaje utilizando la clave pública de B

= Cuando B recibe el mensaje, lo desencripta utilizando su clave privada. Ningún otro receptor puede desencriptar el mensaje ya que solamente B conoce la clave privada.

El encriptamiento de clave pública resuelve el problema de distribución de claves porque no hay claves para distribuir. Todos los participantes tienen acceso a las claves públicas, y las claves privadas son generadas localmente por cada participante y por lo tanto nunca necesita ser distribuida.

MAQUINAS FIREWALL

Cuando se construyen departamentos o edificios de oficinas, normalmente son equipados con paredes a prueba de fuego (firewall) - que son paredes construidas especialmente para resistir el fuego. Si se inicia el fuego en el edificio, éste podrá arder sin control sólo en un área, porque la "pared" detendrá o disminuirá el progreso del fuego hasta que llegue la ayuda.

La misma filosofía puede aplicarse para la protección de redes contra ataques externos. En las redes, las máquinas firewall hacen difícil para los intrusos el "viajar"

de red en red. La instalación de máquinas firewall puede ayudar a detener o reducir daños e intrusiones [GAR91].

FIREWALL INTERNAS

La propuesta más sencilla en cuanto a esta técnica es conservar a las subredes independientes y de tamaño pequeño. Como ya hemos visto, una vez que el intruso compromete una máquina en una red, es más fácil que comprometa a otras. La tarea de penetrar las redes es más sencilla si se tiene todo el equipo conectado a la misma red física y lógica. En lugar de colocar todas las máquinas en una red local, se debe separar la instalación para formar conjuntos de LANs comunicándose a través de gateways o routers. Para lograr esto, siga los siguientes lineamientos [GAR91]:

- Cada LAN debe tener su propio servidor. Cada servidor y sus clientes deben tener su propio dominio de red.
- Ningún servidor o estación de trabajo en una red puede confiar sus computadoras a cualquier otra red
- Los usuarios que tengan cuentas en más de un red local deben contar con diferentes pasaportes para cada subred, y no permitir el acceso entre las redes sin el pasaporte respectivo
- Los gateways deben tener habilitado el nivel de acceso y el nivel de seguridad lo más restrictivo posible. Si es posible, no permita cuentas de usuario en los gateways
- No instale archivos de sistema de una red local a otra

Las firewalls internas ofrecen muchos beneficios:

- Ayudan a aislar fallas físicas de la red en un número pequeño de máquinas
- Limitan el número de máquinas que pasan información en cualquier segmento físico de la red, limitando por lo tanto el daño que puede hacerse al "interceptar" las conexiones.
- Limitan el número de máquinas que se pueden afectar por ataques del tipo de inundación

- Son una barrera contra instrusos internos y externos, que traten de atacar máquinas específicas en algunas de las redes.

FIREWALL EXTERNAS

Además de la partición de la red en pequeñas redes locales para disminuir o frenar a los intrusos, es importante instalar firewall externas, esto es, una máquina (o conjunto de máquinas) que formen una barrera entre la instalación local y el mundo exterior. Esta barrera puede configurarse para permitir que se ejecuten determinadas operaciones y para hacer difícil o imposible que un intruso externo la utilize para penetrar las redes que protege.

Hoy en día, muchas redes corporativas y académicas se conectan al mundo exterior con routers o bridges sencillos. Esto posibilita que cualquier estación de trabajo de la red alcance el exterior y viceversa - para una computadora del exterior es posible alcanzar y conectarse a cualquier estación de trabajo.

Algunas veces, los centros de red equipan sus servidores con dos interfases a la red y tienen al mismo equipo funcionando como servidor de archivos y como gateway.

COMPOSICIÓN DE UNA FIREWALL

Consiste de dos partes las cuales separan el exterior e interior de la red [GAR91] (Figura 3.7):

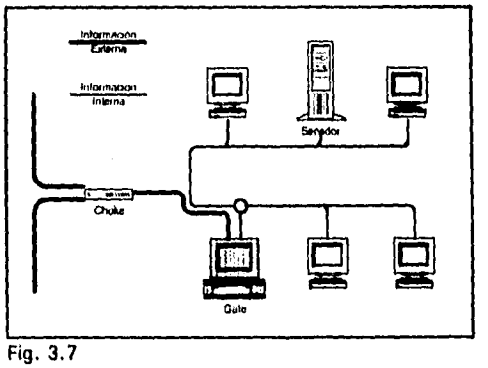


Fig. 3.7

Choke (Contenedor): Bloquea todos los paquetes del exterior de la red destinados al interior de la misma a menos que estén destinados al gate (puerto), y bloquea todos los paquetes del interior de la red destinados al exterior, a menos que provengan del gate. Es el puente entre el interior de la red y el exterior. No avanza los paquetes entre el exterior y la red a menos que los paquetes tengan la dirección del gate como dirección de origen/destino. Se puede configurar o instalar el choke para pasar solamente paquetes de algunos protocolos en particular.

Gate: Es la otra midad de la barrera. El choke obliga que toda la comunicación dentro y fuera de la red tome lugar a través del gate; el gate autentifica usuarios, sanea los datos (si es necesario) y retransmite. El gate debe tener una versión de sistema operativo básica (muy disminuida). No debe contar con compilador de "C" para prevenir que intrusos compilen los programas, ni tener cuentas normales de usuarios para limitar los lugares donde el atacante pueda ingresar.

El choke y el gate pueden ser la misma computadora, o pueden ser dos máquinas diferentes. Similarmente, el gate puede ser una computadora, o diferentes computadoras, una por cada protocolo.

PROTECCION DE MODEMS

Los modems son dispositivos que permiten a las computadoras transmitir información sobre líneas telefónicas ordinarias. La palabra por sí misma explica como trabaja el dispositivo: modem es un acrónimo formado de "**Modulador/Demodulador**". Los modems transladan una cadena de información en una serie de tonos (modulación), los transmite sobre la línea telefónica, y translada la serie de tonos nuevamente a la cadena de información en el otro extremo de la conexión (demodulación). Los modems son bidireccionales, esto es, cualquier modem contiene ambos elementos, el modulador y el demodulador, de forma que una transferencia de datos puede tomar lugar en ambas direcciones al mismo tiempo. Aún en esta era de las LAN y redes Ethernet, una de las maneras más comunes de accesar una computadora en forma remota es por teléfono, con los modems [GAR91].

MODEMS Y SEGURIDAD

Los modems originan un número de consideraciones en materia de seguridad porque crean enlaces entre una computadora y el mundo exterior. Los modems pueden utilizarse por individuos dentro de la organización para obtener información confidencial y también pueden utilizarse por gente ajena a la organización para ganar acceso no autorizado a nuestros equipos, y si el modem puede reprogramarse o de otra forma corromperse, puede utilizarse para engañar a los usuarios y descubrir sus pasaportes.

El primer paso para asegurar los modems es proteger los números telefónicos. Trate los números telefónicos justo como trata a los pasaportes: no los haga del conocimiento de nadie que no tenga necesidad de conocerlos ya que al darlos a conocer, se incrementan las oportunidades de que alguien trate de utilizarlos y viole los sistemas. Desafortunadamente, es imposible conservar los números telefónicos de los modems como secreto, ya que, después de todo, la gente necesita llamar a ellos. Y aún si fueramos extremadamente cuidadosos con los números, un intruso podría siempre descubrirlos "accidentalmente". Por esta razón, el secreto por sí solo no es la solución, los modems necesitan medidas más restrictivas.

Para adicionar seguridad a los modems se puede implementar el esquema de llamadas de verificación, que es aquél en el cual un externo llama a nuestra máquina, se conecta al sistema y proporciona alguna forma de identificación. El sistema entonces retiene la conexión y hace una llamada de verificación al externo a un número telefónico predeterminado. Esto fortalece la seguridad porque el sistema llamará solamente a números preautorizados, de forma que un intruso sin autorización no pueda ingresar al sistema.

Desafortunadamente, muchos sistemas telefónicos, especialmente algunos sistemas PBX, no desconectan la llamada del exterior hasta que ésta se desconecta de la línea. Por lo tanto, un intruso puede conservar la línea abierta despues de que el sistema lo desconecta la primera vez. El problema ocurre cuando el modem invierte el papel y trata de llamar fuera de la línea telefónica. El intruso necesita solamente "capturar" la línea en el momento en que el modem la abra, y entonces podrá engañar

al sistema haciéndole creer que se ha conectado con el número telefónico autorizado previamente. Los modems que detectan "tono de marcar" pueden ser engañados frecuentemente por un intruso si éste reproduce un "tono de marcar" grabado previamente sobre la línea abierta, de modo que cuando el modem se ponga a verificar, escuche el "tono de marcar" y autorice el ingreso.

La forma de evitar que un intruso trate de hacer este tipo de trucos es contando con dos conjuntos de modems - uno para recibir llamadas y otro para enviarlas. Para lograrlo, se debe pedir a la compañía de teléfonos que instale las líneas de manera que las líneas de ingreso no se puedan utilizar para llamar y las líneas de salida no tengan número telefónico para ingresar. Esto tiene un costo adicional al de una línea normal, pero adiciona una medida de seguridad extra para las conexiones telefónicas.

PROTECCIÓN FÍSICA DE LOS MODEMS

Aunque la protección física es pasada por alto frecuentemente, es importante proteger el acceso físico a la línea telefónica, así como se asegura la computadora a la cual están conectados el modem y la línea telefónica.

Este esquema puede seguir las siguientes guías [GAR91]:

= Proteja el acceso físico a la línea telefónica. Asegúrese que su línea telefónica está físicamente segura. Cierre todas las cajas de conexión y las rosetas. Dirija la línea telefónica en un conducto eléctrico insertado en las paredes o en áreas cerradas. Un intruso que obtiene acceso físico a la línea telefónica puede conectar su modem a la línea e interceptar las llamadas antes de que lleguen al cliente, engañando a los usuarios, y aprendiendo inclusive sus perfiles y pasaportes.

= Asegure que su línea telefónica no permita la transferencia de llamadas. Si su teléfono puede programarse para transferir las llamadas, un intruso puede transferir todas las llamadas que reciba el sistema al número que escoja. Si en el nuevo número hay una computadora que ha sido programado para actuar como el sistema original, sus usuarios pueden ser engañados, e introducirán sus perfiles y pasaportes.

= Línea privada (arrendada). Si todo el uso de nuestro modem es con una sola ubicación externa, considere obtener una línea privada. Una línea privada es un circuito dedicado entre dos puntos proporcionado por la compañía de teléfonos. Actúa como un cable dedicado y no puede utilizarse para hacer o recibir llamadas. Por lo tanto, nos permite conservar la conexión con el sitio remoto, pero no permite que alguien llame a nuestro modem e intente violarlo. Las líneas privadas son más caras que las líneas regulares, pero la seguridad que proporcionan supera el costo de las mismas.

SEGURIDAD ADICIONAL EN MODEMS

= Modems con pasaporte. Requieren que el usuario ingrese un pasaporte antes de que el modem lo conecte a la computadora. Normalmente, estos modems pueden almacenar una docena de pasaportes solamente. El pasaporte almacenado en el modem no debe ser el mismo que el pasaporte del usuario.

= Modems con encriptamiento. Debe utilizarse en terminales semejantes, las cuales encriptan toda la información transmitida y recibida de las líneas telefónicas. Estos modems ofrecen alto grado de seguridad no solamente contra intentos individuales de acceso en forma no autorizada, sino también contra la intercepción de cables

= Esquemas IAN. IAN es el acrónimo de Identificación automática de números (Automatic Number Identification). En este esquema, la compañía de teléfonos proporciona el número telefónico del usuario que llama al inicio de la conversación. El receptor podrá entonces verificar en su lista de números autorizados el número telefónico del usuario que intenta conectarse.

III.6 ALARMAS, ACCIONES Y REPORTES

El flujo general de los mensajes, eventos y alarmas es el mismo que se presenta en el dominio de fallas. Las acciones específicas que deben tomarse son, sin embargo, diferentes a aquellas del dominio de fallas. Las guías generales para tomar las acciones correctas son [TER92]:

- Minimizar el impacto en la operación de la red
- Maximizar las oportunidades de atrapar al intruso
- En caso de eventos sospechosos, ordenar una recuperación inmediata de los segmentos/aplicaciones de conexión impactados.
- Registrar toda acción extraña para análisis posteriores
- Si la recuperación no parece significativa, las conexiones de comunicación deben cerrarse.

Para facilitar las auditorías, las aplicaciones deben escribirse para registrar sus acciones en las bitácoras de seguridad, utilizando diversos conjuntos de criterios establecidos por el agente de seguridad. Para el diseño de reportes, son buenas guías las establecidas en el dominio de desempeño.

ACCIONES A REALIZAR CUANDO SE DETECTA UN INTRUSO

Existen dos reglas primordiales para manejar incidentes de seguridad [GAR91]:

REGLA # 1 ¡SIN PÁNICO!

Después que se ha presentado un incidente de seguridad, uno se enfrenta a alternativas muy diferentes. Debemos considerar que, no importa lo que haya pasado, solamente empeorarán las cosas si actuamos sin pensar. Antes de hacer cualquier cosa, es necesario contestarnos algunas preguntas y conservar las respuestas firmes en la mente:

= ¿ Tiene realmente un incidente de seguridad ? Algo que parece ser la acción de un intruso podría ser resultado de un error humano o fallas en el software.

= ¿ Existe daño realmente hecho ? Con muchos incidentes de seguridad el intruso accesa al sistema, pero no accesa a la información privilegiada, ni realiza cambios inicuos en el contenido de los archivos.

= ¿ Es importante obtener y proteger evidencia que pueda utilizarse en una investigación ?

= ¿ Es importante regresar el sistema a su modo de operación normal tan pronto como sea posible ?

= ¿ Esta usted en la disposición de cambiar aquellos archivos que han sido alterados o removidos ? Si no, ¿ Como puede asegurar que se han efectuado dichas modificaciones ?

= ¿ Es importante si cualquier persona dentro o fuera de la organización escucha noticias acerca del incidente ?

= ¿ Puede suceder esto nuevamente ?

Las respuestas a muchas de estas preguntas pueden ser contradictorias. Por ello, el responsable de la seguridad de la red debe decidir lo mejor para su organización.

REGLA # 2 DOCUMENTE

Inicie una bitácora inmediatamente. Anote todo lo que encuentre, siempre con fecha y hora. Examine archivos de texto, copias de impresión, señales y fechas de copias. Si tiene el espacio en disco suficiente, registre los detalles de cada sesión. Teniendo esta información en la mano y estudiándola después se puede ahorrar tiempo y problemas graves de forma considerable, especialmente si tiene que restaurar o cambiar archivos rápidamente para regresar el sistema a su estado normal.

DESCUBRIENDO INTRUSOS

Hay muchas maneras en que puede descubrir un intruso [GAR91]:

= Descubriendo al intruso "in flagranti". La forma más fácil de atrapar a un intruso, es examinando eventos como los siguientes:

- Un usuario que ha ingresado más de una vez

- Un usuario que no es programador y que ejecutó el compilador o el *debugger*
- Un usuario haciendo uso pesado de la red no característico de él
- Un usuario que no posee un modem, ingresó a la red mediante una línea conmutada
- Un usuario que esta ejecutando comandos exclusivos del supervisor
- Un usuario que ingreso en período de vacaciones u horarios anormales

= Deduciendo que un ataque se ha consumado al examinar cambios que se han hecho al sistema. Aún si no atrapa al intruso en el momento de la violación, todavía tiene una buena oportunidad de encontrar las huellas del mismo mediante una búsqueda constante en las bitácoras del sistema. Recuerde: busque cosas fuera de lo ordinario:

- Usuarios que ingresan a horas extrañas
- Ingresos fallidos por pasaportes inválidos
- Uso no autorizado o sospechoso de comandos
- Ingreso de usuarios en lugares no familiares de la red

Las bitácoras pérdidas o corrompidas significan que alguien en su sistema de administración fue cuidadoso y lo suficientemente habilidoso para borrar toda evidencia de su intrusión. Esto podría reflejarse inclusive en un programa automático colocado en el sistema que borre los archivos de bitácora en intervalos periódicos.

También puede descubrir que su sistema ha sido atacado por la notificación de cambios no autorizados en los programas del sistema o en archivos de usuario individuales.

= Recibiendo un mensaje del administrador de sistemas de otra red, indicando extraños cambios de actividad en la cuenta perteneciente a su adscripción.

III.7 PROTECCION DE LOS SISTEMAS DE ADMINISTRACION DE RED

Los sistemas de administración de red son poderosos elementos para administrar y operar las redes de comunicación. Estos sistemas contienen datos importantes como pasaportes, grupos de perfiles de usuario, procedimientos de cambio, procedimientos de recuperación y reinicialización, códigos de fin de sesión, algoritmos para rutas alternativas, etc. El dominio de seguridad de la red puede requerir particionarse para permitir a los diversos miembros del equipo de trabajo de este dominio administrar partes discretas de la red. Desafortunadamente, existen pocos instrumentos que ofrecen esta capacidad. La partición puede implementarse utilizando los siguientes criterios cualitativos:

- Funciones de administración de red agrupadas en configuración, fallas, desempeño, seguridad, contabilidad y planeación.
- Formas de comunicación
- Aplicáciones principales
- Diversas redes como LANs, MANs y WANs
- Particiones de la red en áreas de usuario final, transmisión y procesamiento.

La administración de los indicadores de seguridad y sus límites, pasaportes de usuarios, capacidades de grupos de usuarios, cambios de autorización a datos relacionados con la seguridad, etc, requieren de una cuidadosa atención. Es recomendable implementar diversas capas de seguridad que vigilen:

- Que el personal autorizado del área de administración de la red haga uso general de: funciones estadísticas, resultados de desempeño, acceso a reportes y modelos.
- Que el personal autorizado del área de administración de red haga uso restringido de: alarmas, algunas funciones de los dominios de configuración y fallas, bitácoras de violaciones a la seguridad y acceso a las bases de datos de desempeño y teleadministración.

- Que el personal autorizado del área de administración de red haga uso muy restringido de: alarmas de seguridad, cambio del sistema de medidas, control operacional, planes de negocio para el diseño y planeación de la red y perfiles y pasaportes de usuarios.

PROPUESTA DE MAHONY

Donald O'Mahony [MAH94] describe algunas consideraciones que pueden hacer segura la comunicación entre dos procesos administrativos que operan en diferentes dominios bajo el protocolo de administración CMIS. Su primera observación identifica dos grandes riesgos en este tipo de intercambios:

- La seguridad de la información intercambiada durante la asociación administrativa
- El control de accesos a la Base de información administrativa (MIB)

SEGURIDAD DE LA INFORMACION INTERCAMBIADA

Algunos de los mecanismos que propone para resolver el primer problema son:

= Autentificación de ambas entidades. Cuando se va a formar una asociación administrativa basada en CMIS, los sistemas que la inician utilizan una primitiva de inicialización. Asociada a esta primitiva existen algunos parámetros que incluyen las referencias al origen, destino y respuesta. Cada una de estas referencias puede citar un identificador único para la aplicación administrativa (entidad). Estas referencias contienen los denominados puntos de acceso al servicio de presentación (presentation service access point PSAP) que son direcciones que pueden utilizarse para verificar el origen de la asociación. Además se incluye también un parámetro de control de acceso que puede utilizarse para verificar que el estado de la identificación es válido. Haciendo uso de mecanismos basados en sistemas de encriptamiento con clave pública, los sistemas origen y destino pueden satisfacerse a si mismos con la autenticidad de la otra parte. También pueden utilizar los mismos mecanismos para ofrecer alguna prueba de la asociación que está tomando lugar en caso de que la parte autorizada niegue esto más adelante.

- Que el personal autorizado del área de administración de red haga uso muy restringido de: alarmas de seguridad, cambio del sistema de medidas, control operacional, planes de negocio para el diseño y planeación de la red y perfiles y pasaportes de usuarios.

PROPUESTA DE MAHONY

Donald O'Mahony [MAH94] describe algunas consideraciones que pueden hacer segura la comunicación entre dos procesos administrativos que operan en diferentes dominios bajo el protocolo de administración CMIS. Su primera observación identifica dos grandes riesgos en este tipo de intercambios:

- La seguridad de la información intercambiada durante la asociación administrativa
- El control de accesos a la Base de información administrativa (MIB)

SEGURIDAD DE LA INFORMACION INTERCAMBIADA

Algunos de los mecanismos que propone para resolver el primer problema son:

= Autentificación de ambas entidades. Cuando se va a formar una asociación administrativa basada en CMIS, los sistemas que la inician utilizan una primitiva de inicialización. Asociada a esta primitiva existen algunos parámetros que incluyen las referencias al origen, destino y respuesta. Cada una de estas referencias puede citar un identificador único para la aplicación administrativa (entidad). Estas referencias contienen los denominados puntos de acceso al servicio de presentación (presentation service access point PSAP) que son direcciones que pueden utilizarse para verificar el origen de la asociación. Además se incluye también un parámetro de control de acceso que puede utilizarse para verificar que el estado de la identificación es válido. Haciendo uso de mecanismos basados en sistemas de encriptamiento con clave pública, los sistemas origen y destino pueden satisfacerse a si mismos con la autenticidad de la otra parte. También pueden utilizar los mismos mecanismos para ofrecer alguna prueba de la asociación que está tomando lugar en caso de que la parte autorizada niegue esto más adelante.

= Autentificación del origen de los datos. Además de verificar la identidad de la entidad-aplicación origen, también debemos asegurar que las transacciones están siendo transmitidas del lugar correcto. Esta actividad protege contra un usuario ilegítimo accesando el servicio desde un sistema hóstil, o un usuario ilegítimo que de alguna manera obtuvo los parámetros de seguridad necesarios para accesar al sistema.

= Confidencialidad de los datos. Cada una de las solicitudes de servicio que forman parte del CMIS están relacionadas con las correspondientes unidades de datos de protocolo (Protocol data unit PDU) del Protocolo de información Administrativa Común (Common Management Information Protocol CMIP). Estas PDU en turno se direccionan a los denominados elementos de servicio de operaciones remotas (Remote operations service elements ROSE). Un intruso que intercepta un PDU tipo ROSE estará capacitado para obtener un conocimiento completo de la semántica de la primitiva CMIS original. Por esta razón, el contenido de estos PDUs debe encriptarse para su protección.

= Protección de la integridad de los datos. A fin de proteger la intercepción de PDUs individuales, o el reemplazo de secuencias de PDUs, las primitivas de inicialización y algunos parámetros de control de acceso que acompañan cada primitiva CMIS pueden utilizarse para asegurar que la integridad del contenido y la secuencia de la cadena de mensajes permanezca sin alteraciones.

Control de accesos a la MIB

Se recomienda un esquema de Control de autorizaciones para resolver el problema del control de accesos a la MIB.

Control de autorizaciones

Al hablar del control de autorización, debemos establecer que un sujeto (persona o programa de aplicación) está solicitando accesar a un objeto (archivo, impresora, etc) y que el sujeto ya ha sido autentificado. En este contexto, se deben tomar en cuenta tres cosas:

- Atributos del sujeto (Nombre y rol en el sistema)
- Atributos del objeto (Nombre y nivel crítico)
- Tipo de acceso solicitado (Se especifica por el tipo de operación a realizar)

Todos los esquemas de control de autorización están basados en los anteriores principios y todos ellos difieren en el lugar donde se almacenan los atributos relacionados con el sujeto y el objeto. La ubicación óptima de estos atributos dependerá del patrón de acceso y de la importancia relativa de los criterios de acceso.

Una forma de poder implementar el control de autorización es mediante un control de accesos similar al implementado en el servicio de directorio X.500, el cual se desarrolla de la siguiente manera:

Se definió una nueva clase de objetos denominada Quipuobject (de QUIPU, o nombre que se dio al control de autorización del servicio de directorio X.500), la cual contiene una clase denominada lista de control de acceso (Access Control List ACL). Cualquier objeto que sea instanciado de esta clase también contiene una ACL, lo cual permite que el acceso a él sea controlado. De esta manera, la nueva característica de control de acceso fue incorporada en el marco del directorio X.500 sin ningún cambio al protocolo de acceso. La ACL está basada en un conjunto de registros, cada uno de los cuales consiste del trio:

QUE: Especifica a que se refiere la lista de control de accesos- puede ser todo el registro, un atributo en específico o una rama del directorio

QUIEN: Describe las entidades a quienes se aplica este modo de acceso. Esto puede ser especificado como un grupo de nombres distintivos, un prefijo distintivo, el nombre distintivo al cual se refiere el objeto por sí mismo, etc.

CATEGORIA DE ACCESO. Especifica el tipo de acceso permitido, relacionado sobre todo con las operaciones que se pueden realizar

III.8 MONITOREANDO LA SEGURIDAD

La operación exitosa de un sistema seguro depende no solamente de las técnicas de seguridad utilizadas para construirlo, sino del monitoreo contínuo de estas técnicas para detectar cualquier vulnerabilidad. El monitoreo con éxito requiere de habilidad para vigilar la operación o comportamiento de los objetos dentro del sistema. Este seguimiento permite tomar acciones evasivas o correctivas en el caso de que este comprometida la seguridad del sistema.

Las razones por las que se deterioren las técnicas de seguridad establecidas recaen en las dinámicas de uso de la red y en la complejidad del ambiente. Factores típicos para ello son [NOV94]:

- Nuevos archivos creados por usuarios
- Nuevos usuarios autorizados a accesar el sistema
- Cambios en los propietarios de archivos, pero derechos reales no modificados
- Cambios realizados por el usuario que requieren modificaciones a derechos de usuarios y/o grupos
- Perfiles temporales autorizados, pero no renovados/eliminados en el tiempo establecido
- Nuevas aplicaciones o versiones instaladas

Auditar la seguridad implica dos actividades diferentes:

= Tareas de monitoreo de seguridad diarias: Los administradores de seguridad de tiempo completo deben realizar estas tareas diariamente, mientras los administradores de medio tiempo pueden realizar el monitoreo en base a períodos menos frecuentes.

= Auditorías de seguridad periódicas: Las revisiones y auditorías periódicas pueden realizarse por auditores internos o externos. Las revisiones periódicas se desarrollan anualmente o en períodos menos frecuentes, dependiendo del tamaño y necesidades de seguridad de la organización.

TIPOS DE AUDITORIA

Podemos clasificar las diferentes auditorías en tres categorías:

= Revisión de seguridad. Determina el estado de seguridad del área. Busca determinar el cumplimiento de las bases de seguridad y estándares de control que han sido especificados por las políticas corporativas y los mandatos legales/regulatorios. Es una vista o foto instantánea de las condiciones actuales. Los auditores pueden realizar una revisión de seguridad como parte de una auditoría regulatoria o de una auditoría externa.

El auditor evalúa los resultados de la revisión de seguridad independientemente de las funciones y aplicaciones del negocio. Los procedimientos incluyen básicamente el cuestionamiento y la observación. El ámbito que abarca incluye típicamente:

- Seguridad física y ambiente
- Respaldo, recuperación y planes de contingencia
- Acceso al sistema

= Auditoría del sistema. Es más profunda que una revisión de seguridad e incluye procedimientos de evaluación para resaltar preguntas y observaciones. Los estudios de perfeccionamiento de procesos o auditorías de cumplimiento normalmente incluyen el detalle y ámbito de una auditoría del sistema.

Normalmente una auditoría del sistema evalúa estas categorías:

- Políticas, procedimientos y estándares
- Seguridad física y ambiente
- Respaldo, recuperación y planeación de contingencias
- Operaciones del sistema, mantenimiento y resolución de problemas
- Acceso al sistema
- Utilización de recursos
- Desarrollo y adquisición de software

= Auditoría de aplicaciones. Es un tipo de auditoría altamente personalizada que destaca lo relacionado con control, seguridad y usos de una

aplicación. Estos puntos de control y seguridad pueden cambiar significativamente la estrategia básica de seguridad.

Los auditores realizan primero una auditoría de aplicación para evaluar la integridad, disponibilidad y confidencialidad de los controles y prácticas que soportan una aplicación específica.

Una vez que se ha decidido sobre que tipo de auditoría o revisión se va a basar, se puede uno enfocar a la situación ambiental y expandir los pasos de la auditoría en forma más apropiada.

PROPUESTA TIPICA DE AUDITORIA

DETERMINAR LOS OBJETIVOS Y CONDUCTA DE LA AUDITORÍA

La auditoría y las revisiones de seguridad necesitan ser ad-hoc a cada organización, sistema y/o aplicación. Algunos componentes de la red recibirán más o menos atención, dependiendo del tipo de revisión y de la complejidad de todo el ambiente.

Toda la red se encuentra formada por un conjunto de requerimientos funcionales basada en estos factores:

- Estándares corporativos, políticas y procedimientos (incluyendo requerimientos del gobierno federal, estatal y local)
- Las especificaciones de los componentes de proceso de la red
- Necesidades del usuario final

REALIZAR ANÁLISIS PRELIMINARES Y PLANEACIÓN DE LA AUDITORÍA

La planeación de la auditoría incluye una evaluación preliminar de riesgos y el establecimiento del ámbito de la auditoría. En este punto, el auditor reunirá información para entender el ambiente de red, incluyendo:

- Estándares corporativos y de la organización
- Hardware - servidores, routers, cableado, tarjetas de interfase de red y más

- Software - sistema operativo de las estaciones de trabajo, gateways, correo electrónico, aplicaciones y más
- Comunicaciones - de WAN, línea telefónicas y multiplataformas
- Gente - usuarios y comunidad de soporte

REUNIR INFORMACIÓN DETALLADA

La recolección de datos puede ser la tarea más difícil en el proceso de auditoría. La documentación y los registros de actividades normalmente no son parte del escenario de operación. Si existen, podrían no encontrarse mantenidos apropiadamente o estar dispersos a través de la organización, haciendolos dificiles de localizar. El auditor debe recolectar y revisar:

- La definición original de los requerimientos de la red, basados en el estudio de factibilidad, el diseño propuesto y alternativas, el estudio de intercambio y las decisiones finales
- Estándares de diseño, criterios, propuestas y documentación
- Planes de desarrollo e implementación
- Bitácoras de operación de la red, planes y procedimientos de mantenimiento
- Criterios de evaluación, planes, procedimientos y resultados
- Las configuraciones original y actual y los controles de cambio a la configuración
- Estándares de desempeño, reportes, historia, tendencias y las técnicas de medición aplicadas
- Identificación de componentes de la red críticos o vulnerables y controles para disminuir el riesgo
- Pistas de auditoría y herramientas de análisis para la red
- Planes de contingencia y recuperación de desastres
- Inventario de aplicaciones y usuarios de la red
- Análisis de los requerimientos de seguridad para las aplicaciones actuales y propuestas

- Inventario y análisis de circuitos actuales y propuestos
- Programa de entrenamiento de personal de la red

ANALIZAR Y EVALUAR EL AMBIENTE DE RED

Es invaluable para el auditor un total entendimiento del proceso de datos y del ambiente de red de la corporación. Esto incluye un entendimiento del ciclo de vida de los sistemas y cualquier cambio completo o planeado, integraciones, consolidaciones y expansiones del ambiente de red.

El hardware, software y configuración de la red deben ser precisos, actualizados y fácilmente disponibles para las operaciones autorizadas y para el personal de mantenimiento. No debe permitirse cambio alguno sin asegurar primero que no se afectarán la capacidad actual o la estructura y niveles de seguridad. Deben estar disponibles las provisiones para regresar a la configuración anterior en caso de que se necesite.

PREPARAR EL REPORTE DE AUDITORÍA O PLAN DE ACCIÓN

Como mínimo, el reporte de auditoría debe resaltar las debilidades significativas y proporcionar recomendaciones personalizadas a una situación en particular. El auditor puede jugar un papel importante en la evolución de los ambientes de usuario final, comunicando sus observaciones y transmitiendo soluciones que ha observado en otros departamentos. La información oportuna es de gran importancia ya que el ambiente de usuario evoluciona rápidamente. El auditor puede utilizar normalmente un plan de acción informal que es más rápido que un reporte de auditoría formal. Algunos elementos de este reporte son:

- Comparación de estándares
- Análisis de debilidades
- Respaldos
- Documentación de hallazgos anteriores

III.9 INSTRUMENTOS DEL DOMINIO DE SEGURIDAD.

Antes de introducirnos en este tema, es conveniente explicar las diferencias entre protección física y protección lógica de las redes de comunicación :

= La protección lógica representa los métodos para evitar que usuarios no autorizados accesen a las aplicaciones críticas y sus respectivas bases de datos y archivos. El esquema de protección incluye pasaportes, códigos de acceso, definiciones de grupos de usuarios y técnicas de encriptamiento. Estos esquemas son coordinados normalmente por los departamentos de procesamiento y comunicación de datos.

= Protección física. Se refiere a las unidades físicas que se utilizan para prevenir el acceso a la computadora, dispositivos de red, puertos a líneas públicas e instalaciones de transmisión. Esta responsabilidad es compartida por el área de la construcción de la seguridad, los administradores propietarios, los usuarios y las organizaciones de telecomunicaciones y comunicación de datos.

Una vez realizada esta aclaración, vamos a ver algunos de los instrumentos que auxilian en la actividad del dominio de seguridad.

DISPOSITIVOS DE MONITOREO

Los dispositivos de monitoreo pueden ser considerados una combinación de un dispositivo de control de acceso y un monitor tradicional con características de recolección de datos, alarmas y reporteador. Se colocan en elementos de la red tales como componentes de procesamiento, instalaciones y periféricos. Estos dispositivos especiales pueden categorizarse como sigue:

= Los que residen en los procesadores como parte del sistema operativo o servicio de administración de accesos, o como un producto para una sola máquina, con interfases con el usuario, el sistema operativo o demás recursos del sistema

= Los que se ubican en la red con una función activa de control y monitoreo del acceso

Como ejemplo de los primeros tenemos a RACF (Resource Access Control Facility - Servicio de control de acceso a los recursos) de IBM. RACF se caracteriza por ser una solución de seguridad horizontal. RACF tiene cinco funciones principales que son:

- Identificación del usuario y verificación del mismo mediante el pasaporte
- Verificación de la autorización para solicitudes de acceso
- Registro, bitácora, ingreso y reporte de violaciones de seguridad y acceso a los recursos del sistema
- Facilidades para delegar el control de recursos al nivel de organización apropiado
- Programas que reporten el estado de seguridad e integridad del equipo

Ejemplificando la segunda categoría tenemos al Net/Guard de Avant-Garde (Figura 3.8)

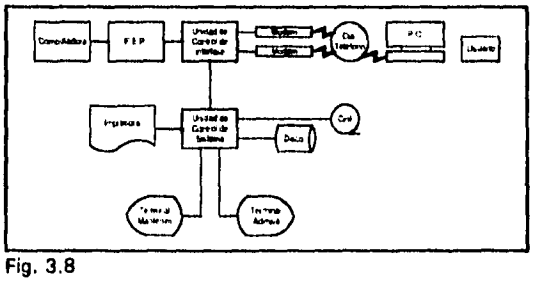


Fig. 3.8

Este sistema integra monitoro y control de acceso a terminales de las redes centrales, bases de datos y mainframes. Los problemas con servicios y las violaciones de seguridad son reconocidos dinámicamente. La arquitectura general de este guarda de la seguridad incluye las siguientes características:

- Despliega el estado de la red en tiempo real
- Es transparente para aplicaciones y clientes (usuarios)

- Cuenta con tres tipos de alertas:
    - Alertas de seguridad : cuando se intenta ingresar con un perfil invalido
    - Alertas de equipo : identifica fallas o mal funcionamiento en el hardware
    - Alertas de límites : cuando una conexión de usuario excede un límite de tiempo de conexión o límite de tiempo ocioso
- Una bitácora de ingresos y alertas
- Formas para atrapar intrusos :
    - Detecta retrasos artificiales en tiempos de respuesta
- Llamadas de verificación, utilizando números de teléfono específicos asignados a usuarios autorizados
- Pistas de auditoría comunes que incluyan:
    - Fecha y hora de todos los intentos de ingreso
    - Línea telefónica de donde provino la llamada
    - Línea telefónica por donde salió la llamada
    - Pasaporte utilizado
    - Razón de la desconexión
    - Usuario asociado con la llamada

DISPOSITIVOS DE ENCRIPTAMIENTO

La fortaleza de un algoritmo de encriptamiento, reside en la complejidad del mismo, y las computadoras han hecho de la complejidad un artículo barato. Sin embargo todo incremento en la fortaleza del proceso de encriptamiento implica que se requieran de ordenes de cómputo más poderosas para violarlo, por ello, la complejidad de un algoritmo es factor primordial en el costo de los dispositivos de encriptamiento. Una ventaja es que los sistemas que canalizan datos a través de un chip de encriptamiento pueden crecer a un chip más complejo a un costo mínimo. Sin embargo, es más fácil implementar el encriptamiento en el software.

LIMITANDO EL ACCESO A DISPOSITIVOS DE USUARIO FINAL

La prevención temprana de accesos no autorizados se puede establecer con la limitación de las oportunidades de acceso a los dispositivos de usuario final como: terminales, computadoras personales, estaciones de trabajo y más. Algunas técnicas como las *chipcard* y *chipkeys* están en el mercado para este fin. Esta técnica en conjunto es denominada también tarjeta inteligente, en referencia al control lógico inteligente nacido en estos circuitos electrónicos. Las tarjetas inteligentes se caracterizan por:

- Contar con un espacio amplio de almacenamiento (4kb o más)
- Ofrecer poca resistencia contra campos eléctricos
- Lectura fuertemente limitada
- Habilitar el procesamiento activo dentro de la tarjeta
- Limitar y deshabilitar los cambios del exterior
- Personalizar la tarjeta dependiendo de la clase de autorización del usuario

En el proceso de autentificación, la tarjeta inteligente proporciona toda la información necesaria para indicar si se autoriza un acceso o no. La adminitración de pasaportes puede ser substancialmente resaltada con largos pasaportes los cuales pueden inclusive generarse aleatoriamente. Los accesos denegados por errores de ingreso también pueden eliminarse.

El alto grado de seguridad que puede alcanzarse en una tarjeta inteligente depende de las capacidades de cálculo y procesamiento del microprocesador. La tarjeta inteligente facilita la descentralización de los dispositivos de seguridad hacia usuarios individuales a través de la aplicación de algoritmos de encriptamiento y proporciona niveles de seguridad por encima y debajo de ellos. El acceso individual ya sea de un dispositivo sencillo o una compleja red heterogénea puede controlarse por un proceso de identificación y autentificación individual.

DISPOSITIVOS BIOMETRICOS

Aprovechando la unicidad de algunas características humanas (como las huellas digitales) estos dispositivos representan un nuevo panorama en la identificación y autentificación de usuarios. Algunos de ellos son:

RASTREADORES DE MANO

La tecnología biométrica más vieja es utilizada hoy en día principalmente para el acceso físico. Este dispositivo observa ambas vistas de la mano de un persona (anvés y revés) utilizando una cámara empotrada y confrontando el patrón con una base de datos de los usuarios autorizados.

HUELLAS DIGITALES

La reputación de las huellas digitales como un identificador único hace a ésta técnica natural para los dispositivos biométricos. Las máquinas que identifican una huella digital en una base de datos de miles de usuarios son mucho más grandes y caras que los dispositivos utilizados solamente para verificar la gente que trata de identificarse. El utilizar los primeros dispositivos implica encontrar una huella digital en una amplia base de datos de huellas digitales; el otro implica asegurarse que la huella digital de la persona que coloca su dedo en el dispositivo es la misma que la que se encuentra registrada en la tarjeta.

PATRON DE OJOS

Las técnicas biométricas de patrón de ojos utiliza luz infrarroja de baja intensidad para inspeccionar la retina de un individuo, o la parte de atrás del ojo, la cual tiene una serie única de venas de sangre. Este esquema encuentra mucha resistencia por parte del usuario porque la tecnología requiere que un rayo de luz ilumine la pupila del usuario. Por esta razón, las compañías están trabajando en desarrollar un dispositivo que salve al usuario del rayo infrarrojo y examine solamente el iris, localizado en la superficie del ojo.

III.10 RECURSOS HUMANOS DEL DOMINIO DE SEGURIDAD

El tercer factor crítico para el éxito del dominio de seguridad es la gente. Las funciones antes discutidas deben adoptar primero una organización dentro del departamento de sistemas de información. Esta organización estará determinada por el tipo de gentes que se encargarán de las funciones de seguridad y que idealmente son:

- Supervisor de seguridad
- Oficial de seguridad
- Auditor de seguridad
- Analista de seguridad
- Coordinador de LAN

El siguiente cuadro nos muestra la distribución de las funciones del dominio de seguridad entre sus recursos humanos:

Funciones	Organización				
	Supervisor Seguridad	Oficial Seguridad	Auditor Seguridad	Analista Seguridad	Coordin LAN
- Análisis de riesgos	X	X	X	X	X
- Evaluación de los servicios de seguridad	X	X			
- Evaluación de las soluciones del dominio de seguridad	X	X			
- Alarmas, acciones y reportes			X	X	X
- Protección de los sistemas de administración de red	X			X	

SUPERVISOR DE SEGURIDAD

Funciones

- Evaluar los riesgos de seguridad
- Preparar los planes de seguridad
- Supervisar los procedimientos de evaluación de las bitácoras de seguridad
- Asistir en la definición de límites para determinar una violación de seguridad
- Asistir en la elaboración de planes de seguridad para el sistema de administración de red
- Establecer el programa educacional para su personal
- Supervisar los procesos de selección de productos

Contactos externos

- Otros supervisores de los dominios de la administración de red
- Vendedores y/o proveedores
- Administrador de la red

OFICIAL DE SEGURIDAD

Funciones

- Evaluar los riesgos de seguridad
- Supervisar la seguridad en tiempo real
- Dictar las acciones contra los intrusos
- Ayudar en la evaluación de las bitácoras de vigilancia
- Ayudar en la elaboración de los planes de seguridad
- Supervisar la seguridad del sistema de administración de red
- Administrar los pasaportes
- Ayudar en la selección de instrumentos

Contactos externos

- Auditor de seguridad
- Analista de seguridad

- Usuarios
- Proveedores de instrumentos relacionados con la seguridad

AUDITOR DE SEGURIDAD

Funciones

- Evaluar las bitácoras de vigilancia
- Ayudar en la estimación de riesgos de seguridad
- Ayudar en el establecimiento de limites para determinar una violación a la seguridad
- Categorizar los riesgos de seguridad
- Ayudar a encontrar la mezcla correcta de precauciones físicas y lógicas
- Auxiliar en la selección de instrumentos
- Escribir los reportes de avance de los planes de seguridad

Contactos externos

- Oficial de seguridad
- Analista de seguridad
- Usuarios
- Proveedores de instrumentos relacionados con la seguridad

ANALISTA DE SEGURIDAD

Funciones

- Definir las funciones de monitoreo y vigilancia
- Evaluar y seleccionar los servicios del dominio de seguridad
- Evaluar el impacto de las técnicas de seguridad en el desempeño de la red
- Construir la matriz de amenazas
- Recomendar instrumentos durante el proceso de selección de los mismos
- Supervisar la instalación de instrumentos
- Personalizar pasaportes y autorizaciones al control de acceso

- Programar los instrumentos
- Establecer procedimientos para asegurar el sistema de administración de red

Contactos externos

- Oficial de seguridad
- Proveedores
- Auditor de seguridad
- Otros usuarios

COORDINADOR DE LAN

Funciones

- Realizar el seguimiento del inventario y mantenimiento dal directorio de la LAN
- Controlar la configuración de la LAN
- Controlar las autorizaciones de acceso a las aplicaciones, servidores y gateways/routers y bridges de la LAN
- Revisar las bitácoras de vigilancia para estaciones y servidores de LAN/MAN
- Administrar los pasaportes locales
- Educar a los usuarios en las técnicas y productos del dominio de seguridad
- Asistir en la toma de acciones contra los intrusos

Contactos externos

- Usuarios
- Oficial de seguridad
- Analista de seguridad
- Auditor de seguridad

CAPITULO IV. SEGURIDAD EN LAN

IV.1 ¿ PORQUE LAS LAN DEBEN CONSIDERARSE APARTE ?

Las redes WAN, están planeadas por expertos, los cuales se basan en los extensos requerimientos de comunicación de una organización para poder implementarlas. Comunmente las WAN utilizan servicios de comunicación públicos, líneas rentadas u otros medios de valor agregado, los cuales obligan al diseñador a seguir las normas establecidas por tales medios. Generalmente cualquier requerimiento de seguridad para estas redes se satisface mediante la adición de hardware y software especial (sistemas de control de redes, modems inteligentes, dispositivos de encriptamiento, etc) al circuito de la red. Si bien los diseñadores y operadores de una WAN pueden instalar centros de control y administración de la red para proporcionar servicios de seguridad, la aplicación adecuada de las medidas de seguridad es responsabilidad del usuario de estos servicios. Los responsables de la WAN mantienen con esto, un nivel de servicio confiable sin aceptar totalmente la responsabilidad por la seguridad de la información que viaja en dicha red.

Con las LAN se presenta ante nosotros una situación diferente. Si bien la LAN puede conectarse a una o más redes WAN, o a otras LAN formando una internet, normalmente es planeada de forma menos estricta, es decir *ad-hoc* a las necesidades de la organización. Las LAN son redes de computadoras mucho más integradas y cerradas que una WAN, y los sistemas que las administran representan hoy en día una nueva forma de administrar redes para muchos responsables de ésta actividad. En una LAN, el control del flujo de la información de operación y la protección de la misma son responsabilidad compartida entre los responsables de la red y los usuarios de las estaciones de trabajo. Los responsables de las redes LAN prestan servicios

relacionados con la seguridad (como respaldos de archivos) y dependen de los usuarios para identificar las necesidades de seguridad de la LAN, estableciendo valores para los diversos elementos de información procesados en ella.

Las razones por las cuales se deben establecer e instrumentar diferentes medidas de seguridad en las LAN que en las WAN y/o MAN son las siguientes [SCH88]:

= Los usuarios de una LAN generalmente poseen más conocimientos de su red que los usuarios de una WAN; manejan algunos conceptos del sistema operativo y tienen un entendimiento más amplio de las estructuras de seguridad internas

= En un ambiente de LAN, existen muchos dispositivos que almacenan y mantienen los datos. Por lo tanto, la protección de la información se torna más difícil a medida que se incrementan dichos elementos

= En la actualidad, no disponemos de muchas utilerías para: proteger las copias, evitar la exposición del contenido de discos y realizar copias sofisticadas de archivos y/o discos

Normalmente, las LAN que son construidas con poca seguridad son baratas y pueden elegir entre una amplia variedad de hardware y software, sin embargo, las redes que requieren de mucha seguridad reducen sus opciones en forma considerable ya que requieren generalmente de hardware y software adicional más caro.

Es por estas razones que en éste capítulo abordaremos con más énfasis el aspecto de seguridad en las LAN, finalizando con las características de seguridad que se pueden implementar con Netware Novell 4.x.

IV.2 CARACTERISTICAS DE SEGURIDAD PARA UNA LAN

Existen una serie de factores que son comunes al establecer servicios de seguridad en una LAN. Estas características son:

ADMINISTRATIVAS

Un aspecto importante en la seguridad de las LAN, pero frecuentemente descuidado es el papel del administrador de la LAN. Este individuo es el responsable del control de los accesos físicos y/o lógicos a la red, y de los procedimientos para efectuar la recuperación de errores, los respaldos y el monitoreo de las infracciones potenciales a la seguridad de la red.

La primera actividad de los responsables de la LAN será definir el conjunto de elementos de seguridad de una LAN (Figura 4.1), para lo cual es necesario contestar las siguientes preguntas [SCH88]:

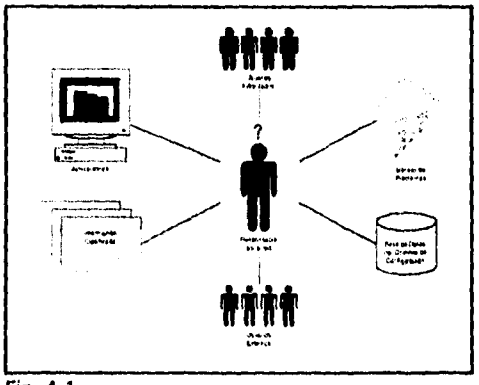


Fig. 4.1

1.- ¿ CUALES SON LAS APLICACIONES A LAS QUE DEBE SERVIRSE Y CUALES SON SUS REQUERIMIENTOS DE SEGURIDAD Y CONTROL CUANDO CIRCULAN EN LA LAN ?

Cuando hablamos de aplicaciones nos referimos a los sistemas de administración de clientes, administración de personal, etc. Los archivos estratégicos

del negocio y su material para trabajar - lo cual es natural se incluya en una LAN -, son las piezas que deben protegerse cuidadosamente y controlarse estrictamente en su distribución.

En muchos casos, una estratégia más estricta para la protección de la información consiste en aplicar el encriptamiento en los niveles normales de control de acceso a los archivos.

2.- ¿ SON SUFICIENTES LOS CONTROLES DEL NEGOCIO EXISTENTES ?

Una función de la organización que involucra la recuperación de información de archivos importantes puede ser una candidata atractiva para desarrollar una aplicación que funcione en la LAN. Sin embargo, hay que estar concientes de que no todos los controles manuales pueden adecuarse en una red. A menos que la red proporcione controles flexibles y conserve registros de todas las actividades, no podrá ser capaz de asegurar que solo se están efectuando las transacciones adecuadas.

3.- ¿ CÓMO SE MANEJARÁ LA INFORMACIÓN CLASIFICADA DE LA COMPAÑÍA ?

Asumiendo que las decisiones de valorización de la información están hechas, debe determinarse como controlar y proteger dicha información en la red. Si por ejemplo, en el procedimiento manual se utilizan etiquetas para indicar la clasificación de alguna información, se podrían adecuar estas etiquetas en una aplicación, que despliegue la información solamente si el usuario está autorizado.

4.- ¿ QUIENES DEBEN SER LOS USUARIOS AUTORIZADOS DE LA RED ?

Es muy importante durante el proceso de planeación tomar la decisión de quienes estarán autorizados a ingresar a la red, porque de lo contrario, los individuos compartirán sus identificaciones, el control de perderá y será imposible encontrar a los auténticos responsables de acciones no autorizadas (ataques). Aunque muchas LAN cuentan con un proceso efectivo de identificación y autentificación de usuarios, el uso apropiado de pasaportes y otros métodos para autentificar recaen en el

comportamiento del usuario, por ello, es importante la concientización del mismo mediante capacitación, seminarios, etc.

5.- ¿ QUE PRIVILEGIOS DE RED ESTARÁN AUTORIZADOS A LOS EXTERNOS ?

Los coordinadores de la red deben determinar si la LAN será cerrada (disponible sólo para empleados) o abierta (disponible para empleados y externos). Aunque los responsables decidan inicialmente hacerla cerrada, con el tiempo se impondrán las aplicaciones que se conectan con externos. Cuando ingresen externos se debe definir claramente cómo utilizarán la red dichos usuarios y cómo se controlarán sus actividades para que la LAN este preparada con mejores sistemas de control e ingreso. La coordinación de la LAN debe establecer privilegios precisos en términos de accesos y acciones así como determinar quién esta activo en la red y que sucede con dicho usuario en un momento determinado, especialmente en ubicaciones críticas de la red, como las que se localizan en las oficinas centrales de la organización.

6.- ¿ CÓMO SE PROTEGERÁ LA INFORMACIÓN DE ALTO VALOR ?

Para manejar la información de alto valor de forma segura, la LAN podría :

- Etiquetar todos los documentos, archivos y mensajes de alto valor con un bit o marca de seguridad para asegurar que la protección que la LAN proporciona es consistente dondequiera que se encuentren dichos elementos de datos.

- Encriptar todos los datos de alto valor cuando deban viajar sobre la LAN u otras líneas comunes de comunicación en áreas fuera del control de la compañía.

- Establecer un control de autentificación extra para accesar a archivos que contienen datos valiosos. Esto es con el fin de no dar acceso a dicha información al personal técnico u operativo de la red, quienes normalmente lo tendrían por su grado de autoridad.

- Establecer un mecanismo para registrar todos los accesos a los archivos importantes, incluyendo marcas de tiempo, fecha e identidad del usuario.

7.- ¿ QUE CONTROLES DE ADMINISTRACIÓN GENERAL SE UTILIZARÁN PARA MONITOREAR Y CONTROLAR LA ACTIVIDAD DE LA RED ?

Deben establecerse de acuerdo a los lineamientos de cada organización. Algunos recomendados son:

= Administrar de acuerdo a los estándares de la compañía en cuanto a la operación de la red

= Controlar el ambiente de la LAN (cambios en infraestructura, servicios, topología, etc)

= Definir y monitorear los servicios de operación y soporte de la red

= Definir los niveles de servicio esperados (incluyendo los servicios de seguridad), de manera que la red preste un servicio consistente en todas las estaciones de trabajo

= Resolver los problemas de la red, incluyendo un proceso de intensificación en la resolución de problemas técnicos y un proceso que genere reportes eventuales al proveedor del equipo o software de la LAN

= Establecer formalmente el dominio de configuración de la red, incluyendo los métodos para adicionar nodos o servicios de forma controlada dentro de la capacidad de la red dado un nivel de servicio acordado

= Crear un procedimiento formal para implementar las actualizaciones de equipo o la instalación de nuevas versiones de software

8.- ¿ COMO SE MANEJARÁN LOS PROBLEMAS, INCLUYENDO LOS DE SEGURIDAD ?

Es necesario establecer un sistema de generación de reportes de incidentes y problemas que informe a los niveles superiores de la organización, a fin de asegurar la corrección e investigación del problema. Muchos incidentes de seguridad requieren un doble reporte de actividad, esto es, el reporte debe enviarse a través de los canales administrativos de la red y a los canales de seguridad de la organización. Este reporte informará sobre la integridad dañada de la red y demás información involucrada.

ACCESO FISICO

FACTOR MULTIPLE[COB92]

Este término se expresa en base a los problemas de seguridad asociados con una computadora *stand-alone* multiplicado por un el número de computadoras conectadas en la LAN.

La seguridad de las computadoras que están conectadas en una LAN inicia con la seguridad de cada computadora en lo individual. No es posible contar con una red segura si las computadoras que conforman su fundamento no lo son. Cada computadora conectada debe estar:

- Protegida en los aspectos de: lugar, sistema y control de acceso a los archivos
- Soportada por fuentes de energía ininterrumpible compatibles y por equipo de respaldo de datos
- Observada por un operador/administrador que la vigile

El factor múltiple anuncia que proteger dos computadoras es al menos doblemente más difícil que proteger una.

Al conectar n computadoras en una red, sobresalen algunos aspectos de seguridad positivos. Si todos los archivos importantes utilizados por X usuarios son almacenados en una máquina, entonces es más efectivo hacer uso de un sistema de respaldo de archivos rápido y automatizado, el cual además deberá ser más confiable y realizarse con más frecuencia que si fuera delegado a cada uno de los X usuarios con instalaciones de respaldo menos sofisticadas. Una fuente de energía ininterrumpible es también más fácil de asignar a una máquina que sirve a muchos usuarios que a cada estación de trabajo en lo individual. Por otro lado, desde una perspectiva de software, el sistema operativo de red adiciona generalmente características de seguridad no encontradas en sistemas operativos para stand-alone.

El aspecto negativo de la LAN se contempla cuando se presenta un ataque a la seguridad de una computadora de la red, ya que posibilita al intruso para ingresar a muchas otras computadoras y a los datos valiosos que éstas contengan. Este

aspecto convierte a la computadora conectada en un objetivo mucho más atractivo, y consecuentemente la pone en riesgos más grandes que a una computadora stand-alone.

CONTROLANDO EL ACCESO A LOS RECURSOS DE LA RED[COB92]

La seguridad en cualquier ambiente de procesamiento de datos también implica el control de acceso al equipo. Aunque el riesgo se encuentre intrínsicamente distribuido en toda la topología de la LAN, la protección de sus recursos principales requiere que los servidores de archivo y las impresoras se ubiquen en habitaciones de acceso controlado y seguro. También es importante considerar el acceso al sistema de cables de la LAN por la relativa facilidad para interceptar la red, insertar nuevos nodos u observar el tráfico de datos. Si la información que se maneja es importante, no debemos descartarla protección de la propia estación de trabajo. Algunas recomendaciones para establecer el control de accesos se encuentran en el Capítulo III.

SUMINISTRO ININTERRUMPIBLE DE ENERGÍA ELÉCTRICA[COB92]

Ciertamente, el servidor de archivos de la LAN requiere un UPS (uninterruptible power supply). Muchos de los UPS tienen integrada la capacidad de enviar señales al servidor de archivos mediante un cable de conexión para indicar que la energía ha fallado y que hay un suministro limitado de energía en las baterías del UPS.

Si todas las estaciones de trabajo cuentan con un sistema UPS, cuando suceda un corte de energía eléctrica, se podría evitar al administrador de la red la labor de comunicar dicho evento a todos los usuarios a través del correo electrónico. Si el corte se prolonga, el administrador puede organizar que las estaciones de la red salgan ordenadamente. Algunos sistemas pueden *dar de baja* automáticamente la LAN, finalizando las sesiones de los clientes de forma ordenada y haciendo respaldos esenciales mientras haya energía eléctrica disponible.

ESTACIONES DE TRABAJD SIN DISCO DURO[COB92]

Claramente hay una necesidad de prevenir la copia de programas y datos contenidos en la red en discos flexibles, así como de eliminar la posibilidad de que los virus u otros programas mal intencionados sean copiados de discos flexibles a la red. Una solución es proporcionar a los usuarios vulnerables las denominadas estaciones de trabajo sin disco duro. Estas unidades cuentan esencialmente con la misma arquitectura que una IBM PC, pero con la diferencia importante de no poseer unidades de disco flexible ni disco duro. De esta forma, el usuario está obligado a almacenar sus datos y programas en el disco duro del servidor de la red.

PROTEGIENDO EL SERVIDOR[COB92]

La parte más importante de una LAN es el servidor. La concentración de datos y programas en el servidor, hace que sea esencial protegerlo de todas las eventualidades, mediante elementos como:

- Control de acceso al servidor. Significa estableces mecanismos que impidan el ingreso de presonal ajeno al centro de red.

- Respaldo del servidor. Dada la importancia del servidor y el monto de datos que éste maneja, están justificadas las opciones de respaldo más exóticas (Figura 4.2). Una de ellas señala que múltiples unidades de respaldo pueden arreglarse en sistemas automáticos que proporcionen varios gigabytes de almacenamiento mediante mecanismos que coloquen los discos magnéticos en dichas unidades.

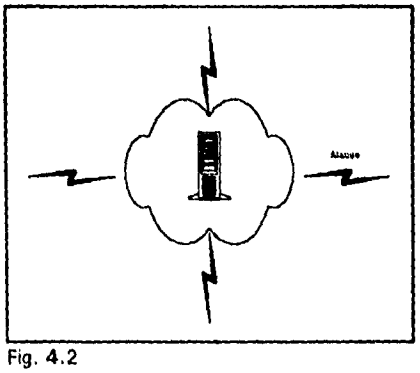


Fig. 4.2

Cabe recordar que los respaldos de los servidores de archivo son un recurso valioso, y deben conservarse en un lugar protegido. En este sentido, podemos aplicar las medidas establecidas en el capítulo anterior.

EQUIPO ESPEJO (DUPLEXING AND MIRRORRING)[COB92]

Los primeros sistemas de tolerancia de fallas consistían de una unidad de disco secundaria que se mantenía como un "espejo" de la unidad principal. Cualquier dato que era escrito en la primera unidad tenía también que escribirse inmediatamente en la segunda (Figura 4.3). Si la unidad primaria fallaba por cualquier razón, la unidad de disco secundaria tomaba su lugar, permitiendo que el disco primario fuera reemplazado sin interrumpir las operaciones del servidor de archivos.

Aún dentro del sistema de disco espejo existen diferentes niveles de redundancia y tolerancia de fallas. Mientras algunas soluciones duplican los datos de un disco a otro, otras duplican solamente los datos críticos.

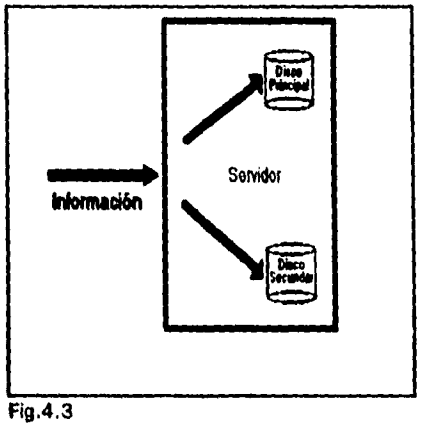


Fig.4.3

ACCESO LOGICO

Las técnicas de acceso físico están diseñadas para conservar a usuarios no autorizados fuera de la red. Las técnicas de acceso lógico están diseñadas para limitar

el acceso de usuarios autorizados a archivos no autorizados. El control de acceso a la información es responsabilidad del sistema operativo de la red y de sus utilerías. El acceso al servidor mediante un pasaporte y los derechos/permisos sobre directorios o archivos representan los puntos de seguridad básicos proporcionados por un sistema operativo en red.

En una típica LAN de PCs, el software de red permite que una computadora con disco duro pueda compartir su espacio de alamcenamiento con otros usuarios, los cuales podrán accesar archivos en dicha computadora, almacenar ahí sus archivos y ejecutar programas de la misma. Un servidor de archivos - la computadora que dispone su disco duro a otros - representa claramente un riesgo de seguridad. Se debe controlar quién puede realizar tal compartición de recursos y quién tiene permitido ser usuario de un área compartida, así como los límites del área compartida, asegurando que los clientes no puedan accesar el resto de los archivos contenidos en el servidor.

La seguridad lógica de la red se debe establecer a través de los niveles lógicos del sistema operativo, como lo muestra la Figura 4.4:

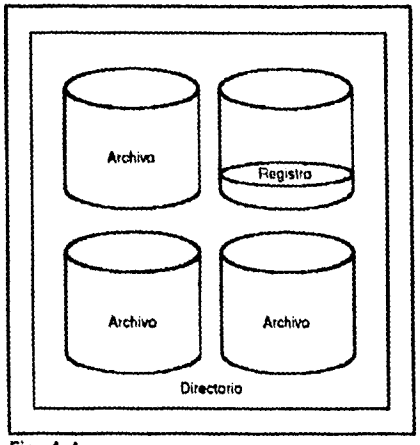


Fig. 4.4

SEGURIDAD EN DIRECTORIOS[STA88]

Este punto es el más problemático en la temática de la seguridad en las LAN. El control de acceso a directorios significa que el sistema de seguridad debe autentificar a los usuarios para poder determinar cuales elementos de información pueden utilizar. Este proceso presupone que el propietario de la información ha asignado un valor a la información y ha especificado quién puede ver u operar dicha información.

El acceso a directorios normalmente es controlado mediante el perfil de usuario, el cual describe a un usuario de acuerdo a los privilegios que posee sobre la información relacionada con su trabajo. Esta descripción se encuentra descrita en la tabla de derechos contenida en el objeto Usuario. Otro método de establecer el control de directorios es mediante la asignación de un pasaporte a cada usuario para el acceso a algún directoio. Esta última propuesta tiene diversas deficiencias y sólo es utilizado fuera en el área local, es decir, se localiza en las computadoras personales donde los individuos pueden establecer pasaportes para proteger sus directorios privados.

El control de acceso a directorios se implementa mediante la autorización de determinadas acciones de los usuarios sobre los directorios, tales como :

- Leer archivos
- Escribir archivos
- Abrir archivos
- Crear archivos y directorios
- Borrar archivos y directorios
- Derechos de padre en un directorio, manejando libremente los subdirectorios
- Buscar en directorios
- Modificar las banderas de estado de archivos/directorios y renombrar archivos

SEGURIDAD A NIVEL DE ARCHIVOS[STA88]

Este control está basado en los derechos sobre archivos para leer, mover, modificar, etc y es asignado por el identificador personal del usuario. Para contar con un control de archivos efectivo, debemos asegurarnos que el propietario de cada archivo ha establecido derechos para la actividad de cada usuario o clase de la red. También hay que asegurarse que los privilegios autorizados para realizar determinadas actividades sean acordes con las necesidades de operación del negocio.

El control de acceso a archivos se implementa a través de una serie de banderas que controlan sus características de acceso. Se puede controlar entre otras cosas:

- Si el archivo es de solo lectura
- Si el archivo es oculto
- Si el archivo es archivo de sistema
- Si el archivo es de ejecución
- Si el archivo es compartido

CONTROLANDO LA ACTIVIDAD A NIVEL REGISTRO[STA88]

La autorización de acceso a un archivo no cubre totalmente las necesidades de seguridad, sobre todo de sistemas críticos. Es común que se requiera la autorización expresa de lectura a un archivo, sin embargo, si deseo cerrar más la restricción, se puede determinar sobre cuales campos tiene autorización leerlos. Esta utilidad es muy apreciada en documentos legales o información clasificada

SEGURIDAD ENTRE REDES

En una internet se debe garantizar que la distribución de servicios será segura y confiable. Los servicios de seguridad en cada subred serán manejados por el servidor local de la red que está prestando los servicios solicitados. De esta forma, los recursos de la internet con niveles de seguridad mayores a los solicitados por el cliente sea cual sea la ubicación de éste, serán invisibles para él (no podrá verlos), y por lo tanto no podrá leerlos, escribir en ellos o destruirlos.

ANALIZADOR DE PROTOCOLOS

Un analizador de protocolos en las manos de la persona equivocada puede ser una amenaza a la seguridad. Si un infiltrador puede obtener acceso a un conector de la LAN o es capaz de interceptar el cable, el analizador puede revelar información útil para el intruso. Un analizador puede capturar todo el diálogo que toma lugar sobre la LAN o inclusive desplegar pasaportes en forma desencriptada. La apropiación de pasaportes es fácil mediante el uso de los analizadores, pero los pasaportes no siempre pueden ser útiles, sobre todo si la LAN fue bien diseñada. Esto es, podemos restringir las estaciones a las que un usuario pueda ingresar. Así, aunque el infiltrador posea el pasaporte de la cuenta del supervisor, no podrá ingresar como él si no utiliza la terminal de éste. Adicionalmente, las utilerías para generar pistas de auditoría pueden reportar ingresos y salidas de la red, poniendo atención especial al perfil del supervisor.

Mientras que los analizadores de protocolos pueden representar un problema para la seguridad de la LAN, por otro lado pueden utilizarse para monitorear infracciones que ocurran en la red. Una técnica sencilla consiste en buscar las estaciones de trabajo que no deben estar conectadas a la red. El administrador puede utilizar una aplicación que despliegue la red para señalar las estaciones desconocidas. Facilitamos esta actividad si asignamos un identificador fácil de leer a cada estación en la LAN. Con algunos modelos de analizadores, el administrador de la red puede escribir pequeños programas en C que realicen funciones especializadas, por ejemplo, un programa que busque a través de los datos para localizar las estaciones que ingresaron en el servidor de archivos y que no muestran actividad por largos períodos de tiempo. Esta aplicación podría indicarnos si en una estación el usuario ha dejado la misma conectada a la red y no la está utilizando, lo cual es una violación a las reglas de seguridad en muchas instituciones.

IV.3 LOS MODELOS DE SEGURIDAD DE NETWARE NOVELL 4.X

Podemos ubicar la interpretación de seguridad de Netware Novell 4.x en la clasificación de seguridad comercial en la clase D, ya que sus características de seguridad no son activadas automáticamente durante su instalación. Esto significa que si uno instala Netware Novell 4.x sin activar sus características de seguridad, contará con un sistema de seguridad de clase D. Es importante tomar un amplio espacio de tiempo para habilitar y tomar ventaja de las características de seguridad de Netware Novell 4.x.

Los modelos de seguridad que establece Netware Novell 4.x son progresivos en cuanto a su naturaleza restrictiva, ya que cada uno se enfoca en un nivel superior de protección. Estos modelos se presentan como un "esqueleto" sobre el cual se puede construir una implementación propia de seguridad. Adicionalmente, se puede ver cada uno de estos modelos como un punto de reflexión, dependiendo del monto de riesgo que se está dispuesto a asumir para nuestro propio sistema.

Cualquier intento de presentar un modelo de seguridad completo implica diversas dificultades. Si los requerimientos de una organización son diferentes a los modelos, entonces el nivel de importancia que pone en su seguridad puede ser desproporcional al beneficio actual que espera. Esta es una dificultad de trabajar con modelos generalizados, sin embargo, los modelos que a continuación se expondrán van a servirnos para señalar los intentos de la industria para proporcionar redes seguras.

Los cinco modelos de seguridad que propone Netware Novell 4.x son [NOV94]:

- Simple
- Básico
- Protegido
- Auditado
- Asegurado

Como ya mencionamos, cada modelo se construye sobre el que le precede (Figura 4.5) y cubre los siguientes eventos en el orden establecido:

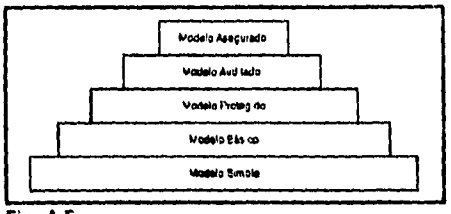


Fig. 4.5

- Implementando la seguridad física
- Estableciendo señales de alarma pasivas
- Implementando medidas de seguridad pasivas - incluyendo aislamiento físico de componentes de cómputo y utilizando software de respaldo y almacenamiento de datos en otra ubicación
- Modificando las opciones predeterminadas de Netware Novell 4.x
- Utilizando de forma activa los pasaportes y el mecanismo de detección de intrusos de Netware Novell 4.x
- Haciendo uso en forma activa del software de detección de virus
- Educando a los usuarios finales en aspectos de seguridad
- Protegiendo los archivos del sistema y los directorios

MODELO SIMPLE

El modelo de seguridad simple se aplica cuando los responsables de la red cuentan con pocos conocimientos de seguridad. Puede implementarse por un usuario final, el cual puede iniciar esta labor en cualquier momento sin necesidad de conocimientos previos. Proporciona un nivel de seguridad mínimo y algunas directrices las cuales previenen daños accidentales a Netware Novell 4.x o al servidor y equipo (componentes) de la LAN. Este modelo establece un nivel de seguridad equivalente al nivel medio de la clase D de la clasificación de seguridad comercial.

Uno de los métodos de seguridad más sencillos consiste en colocar una señal de advertencia que cifre "No intervenir". Desafortunadamente, en algunos ambientes, una señal de advertencia no es suficiente para prevenir una pérdida o daño. En estos ambientes puede ser ventajosa la simple seguridad física proporcionada al asegurar servidores y equipo esencial en lugares donde no pueden accesarse físicamente. Las razones para implementar la seguridad física son relativamente directas. Uno tiene una inversión - tanto en hardware como en software - y quisiera tener uso ininterrumpido de su inversión. El software de respaldo cumple parte de esta necesidad. El uso apropiado de software de respaldo en coordinación con la custodia de las copias de respaldo en otra ubicación, proporciona cierta garantía para contar con el uso contínuo de la información en el caso de pérdida. Esto permite recuperar archivos de datos en caso de desastres o accidentes no esperados.

Los usuarios finales son responsables de más catástrofes en hardware y software que los criminales o empleados disgustados. Mas importante aún, los usuarios finales tienen acceso garantizado al servidor de la red a través de sus estaciones de trabajo locales - especialmente en ambientes donde no tienen que utilizar pasaporte para accesar a los recursos de cómputo. Los pasaportes solamenten aseguran que los usuarios tengan acceso - no hacen nada para prevenir accidentes (borrado de archivos), o ingreso de virus de cómputo por discos contaminados. Por todo ello, los respaldos son esenciales.

Aún con métodos activos - seguridad física, pasaportes, rastreo de virus- no existe substituto para la educación del usuario. Una de las medidas de seguridad más importantes es una educación apropiada.

MODELO BASICO

Este modelo se desarrolla sobre las bases del modelo simple descrito anteriormente y muestra un énfasis incrementado en las restricciones impuestas al usuario sobre el sistema de archivos y NDS. Entre las acciones que propone están: segregar aplicaciones y archivos de datos buscando reducir el riesgo de ingresos accidentales o de corrupción, y dirigir al administrador de red en el desarrollo de las

políticas de seguridad. Este modelo proporciona un nivel de seguridad equivalente al nivel superior de la clase D de la clasificación de seguridad comercial.

En adición al modelo simple presentado en la sección anterior, el modelo básico busca garantizar una función de administración apropiada, habilitando funciones de seguridad y contando con alguien que revise lo que sucede en la red.

La meta del modelo básico es habilitar los servicios de NDS para la administración del sistema y del usuario final. Propone directivas al sistema de archivos para el acceso a archivos y expone la cuestión de la integridad de los archivos en las estaciones de trabajo como un objetivo realista. Este modelo pone atención a la estación de trabajo para ver si usuarios no autorizados han accesado y que se puede hacer para prevenir esto, y a los componentes de las estaciones de trabajo (como teclados y unidades de disco).

Una sugerencia para prevenir accesos no autorizados es registrar e implementar las políticas de seguridad y cualificar cuales amenazas son reales.

MODELO PROTEGIDO

Este modelo es actualmente un modelo auditado, pero sin los auditores profesionales requeridos en el modelo auditado. Pone en marcha las funciones de auditoría de Netware Novell 4.x para obtener información acerca del sistema. Proporciona seguridad equivalente al nivel bajo de la clase C de la clasificación de seguridad comercial. El modelo protegido se auxilia mucho en la educación. Esta educación debe ser más formal que simples cursos, es decir, se requiere de un entrenamiento contínuo en cuanto a la protección de pasaportes, procedimientos antivirus y políticas de seguridad para la PC en cuanto a su organización. La educación se extiende más alla de las políticas de seguridad de los sistemas operativos de la estación de trabajo y de Netware Novell 4.x ya que los administradores necesitan conocer y dominar la administración de NDS y del sistema de archivos. La organización de las políticas de seguridad se vuelve parte importante de la operación de la red, y éstas deben referenciarse y actualizarse frecuentemente. En el modelo protegido, debe detallarse el significado de una pérdida para poder delinear claramente

las políticas de seguridad. Las unidades de disco de la estación de trabajo incrementan su importancia a nivel de seguridad. En el modelo protegido, el acceso a las unidades de disco debe monitorearse, asegurándolas con dispositivos de control de acceso o removiéndolas físicamente. Adicionalmente, la estación de trabajo por sí sola puede asegurarse en una habitación segura, y de esta forma, solo ser accesible a usuarios confiables.

MODELO AUDITADO

Este modelo es controlado por auditores profesionales. Las actividades, instalaciones y políticas de la red son evaluadas regularmente por auditores de red profesionales. El modelo auditado también requiere de los servicios de administradores de seguridad, y de una interacción constante entre los administradores de seguridad y los usuarios finales, así como entre los departamentos y los auditores. La auditoría profesional (ajena a la seguridad) se vuelve un ciclo de retroalimentación para hacer confiable la red de cómputo. Proporciona la seguridad equivalente al nivel medio de la clase C de la clasficación de seguridad comercial.

La diferencia más grande entre los modelos auditado y protegido radica en como son afectadas las políticas de seguridad por la retroalimentación de las auditorías. Los administradores son responsables de implementar las políticas de seguridad, y la actividad que rodea la red es revisada y monitoreada.

Un programa de monitoreo de las estaciones de trabajo es necesario en este tipo de modelo. Este programa puede incluir etiquetado y vigilancia de los gabinetes de las estaciones de trabajo y conexiones de red y deshabilitación de los teclados y unidades de disco flexible (o removidas y cerradas en el gabinete) cuando no sean utilizadas. Las políticas de seguridad son plasmadas en un documento formal. Este documento debe contener una tabla de contenido, páginas numeradas y estar bajo revisión constante para asegurar que todas las páginas y actualizaciones son presentadas. Los auditores pueden inspeccionar las políticas de seguridad, y las bitácoras de operación de aquellos responsables de conocer e implementar los estándares de seguridad dentro de la organización. Los auditores también pueden

hacer sugerencias para innovar o actualizar algunas políticas de seguridad. La implementación de políticas de seguridad puede ser cara y requerir de personal adicional, pero también pueden ser realizadas por los administradores de departamentos y los usuarios finales. De cualquier forma, si una política de seguridad no es efectiva o no es implementada, existe la posibilidad de que los componentes electrónicos de datos del negocio se vean adversariamente afectados, resultando en pérdidas financieras.

MODELO ASEGURADO

El modelo asegurado es muy diferente a los modelos previos. Se basa en la premisa de que alguien está tratando activamente de penetrar la red. Su implementación es muy diferente, tanto en hardware como en personas, y no puede ser establecido en lo individual, requiere de un administrador profesional con experiencia para la evaluación de la seguridad. Este modelo no es la solución completa en seguridad, necesita de una evaluación y monitoreo constante de la red para proporcionar seguridad a la información y proteger la red. El modelo asegurado proporciona seguridad equivalente al nivel alto de la clase C de la clasificación de seguridad comercial.

Este modelo se basa en una adherencia estricta a las políticas de seguridad definidas e implementadas de forma precisa. Es necesario que exista un conjunto de políticas de seguridad completas y que sean distribuidan dentro de la compañía. Es también esencial que todos entiendan su papel en los procedimientos de seguridad. En un ambiente con este nivel de seguridad, se requiere de el mantenimiento y evaluación en línea de las contramedidas implementadas. Las contramedidas se originan en la implementación de todos los elementos de los modelos previos, y en la investigación en línea para determinar si nuevas amenazas a la seguridad de la red han alcanzado un estado de credibilidad. Las contramedidas también se basan en la evaluación contínua de las estaciones de trabajo, instalaciones de comunicación, servidores de red, y el aislamiento de usuarios confiables de componentes poco confiables dentro de la red.

El modelo asegurado puede tener cualquier número de usuarios, pero está limitado por la conjunción de éstos en grupos de trabajo. Este modelo restringe la comunicación externa mediante bridges y routers (Máquinas firewall). El acceso a los componentes físicos de la red esta asegurado, indescifrablemente marcado y mantenido en una capa secreta translúcida. Todas las reparaciones son hechas con un evaluador de seguridad presente.

Este modelo se alcanza a través de la combinación de las características de protección de Netware Novell 4.x y las medidas de protección del tipo end-to-end que buscan mantener la integridad de la red y haceria infinitamente difícil de atacar. En este modelo, el monitoreo de las estaciones de trabajo es solo una parte de las políticas de seguridad. Tanto las estaciones de trabajo como los servidores son asegurados con todo el hardware y software que haya disponible. Los routers, bridges y equipos de telecomunicación seguros son la norma, no la excepción. El monitoreo y administración de la red es en línea.

IV.4 ELEMENTOS DEL ESQUEMA DE SEGURIDAD DE NETWARE NOVELL 4.X

Netware 4.x tiene dos niveles de seguridad distintos: la seguridad del sistema de archivos y la seguridad de los Servicios de Directorio Netware (Netware Directory Services NDS). Todos estos elementos los podemos observar en la Figura 4.6.

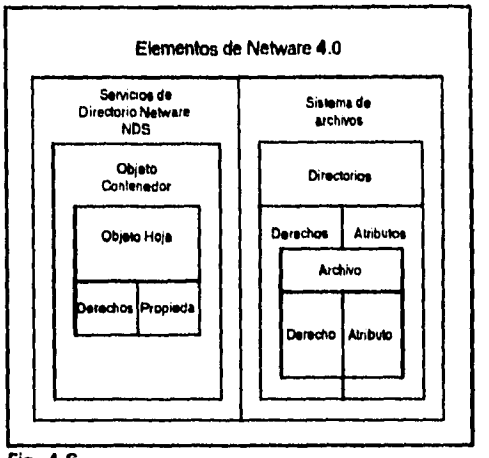


Fig. 4.6

La seguridad del sistema de archivos controla el acceso a archivos y directorios localizados en los diversos volumenes de la red. También asegura los programas de aplicación y sus archivos de datos. Cuenta con características que le permiten efectuar procesos de compresión y migración de datos, pero su objetivo primordial es establecer control y permitir el acceso a los usuarios del sistema de archivos de directorios y archivos.

La seguridad de NDS contempla la administración de la base de datos de NDS, sus objetos y propiedades. Las funciones de seguridad de NDS son similares a las antiguas funciones del supervisor (versiones anteriores) que no están relacionadas con el sistema de archivos, como son: crear usuarios, editar *programas de inicio (login script)*, crear servidores de impresión, asignar derechos a usuarios y crear un coordinador de grupos de trabajo o un operador de consola.

Generalmente la seguridad del sistema de archivos y de NDS no se afectan entre sí y son independientes una de otra. De hecho, una de las características de Netware Novell 4.x es la habilidad de separar la administración del sistema de archivos

y la administración propia de la red (NDS). El usuario que controla el árbol NDS y sus objetos puede ser diferente al responsable del sistema de archivos. También puede haber diferentes coordinadores para: ramas del árbol NDS, volúmenes, directorios o archivos.

CONCEPTOS Y CARACTERÍSTICAS DE NDS[NOV94]

OBJETOS NDS

Los objetos NDS pueden ser de dos tipos: contenedores y "hojas" (refiriéndonos a todo el sistema NDS como un árbol). Los cuatro tipos de objeto contenedor son: [Raíz], País, Organización y Unidad Organizacional, y se denominan así porque, como su nombre lo indica pueden contener otros objetos. Los objetos contenedores conforman la estructura jerárquica de la base de datos NDS, la cual es similar a la estructura de los directorios en el sistema de archivos. Un árbol NDS está compuesto de un objeto [Raíz], algunos niveles de objetos contenedores y muchos objetos hojas. NDS cuenta con 16 tipos de objetos hoja estándares entre los cuales tenemos: Usuario, Grupo, Alias, Estación de trabajo, Correspondencia de directorio, Servidor Netware, Perfil, Impresora, etc.

Cada objeto NDS tiene un conjunto específico de propiedades asociadas a él. Más de 120 propiedades separadas son definidas dentro del esquema de NDS. El subconjunto en particular de estas propiedades asociadas con una clase de objeto define como puede operar dicho objeto en la red de Netware Novell 4.x. Por ejemplo, algunas propiedades del objeto Usuario son: Bloquear cuenta, Perfil por omisión, Servidor por omisión, Descripción, Registro de fecha/hora de último ingreso, programa inicial, Equivalencias de seguridad, etc.

OBJETOS NDS, DERECHOS Y PROPIEDAOES

La base de datos NDS permite tantos niveles de acceso como se quieran crear o coordinar. Estos niveles de acceso son controlados a través de cada objeto mediante sus derechos y propiedades. Los derechos de un objeto NDS se utilizan para controlar

quién puede realizar funciones administrativas sobre los objetos como crearlos, borrarlos o renombrarlos. Las propiedades de un objeto en NDS se utilizan para controlar quién puede examinar, utilizar o cambiar los valores de las diversas cualidades de un objeto. Los derechos que se pueden otorgar sobre un objeto son:

Derecho		Descripción
S	Supervisor	Tiene todos los privilegios
B	Browse	Ver el objeto
C	Create	Crea nuevos objetos (válido en contenedores)
D	Delete	Borrar un objeto
R	Rename	Cambiar el nombre de un objeto

Por otro lado, las propiedades de un objeto pueden ser:

Propiedad		Descripción
S	Supervisor	Todos los derechos sobre las propiedades
C	Compare	Permite comparar valores de propiedades
R	Read	Permite leer el valor de una propiedad
W	Write	Permite adicionar, cambiar o remover cualquier valor de la propiedad
A	Add/Remove Self	*Elemento autorizador (Trustee)* que permite adicionar o removerse a si mismo como valor de su propiedad

LISTA DE CONTROL DE ACCESO

Así como los derechos asignados a un usuario o grupo en el sistema de archivos son almacenados en las Tablas de entradas del Directorio (Directory Entry Tables), los derechos asignados a NDS son almacenados en un atributo común a todos los objetos conocida como la propiedad de Lista de Control de Acceso (Access Control List ACL). La ACL indica a cuales objetos se han asignado derechos por medio de un elemento autorizador explicito y cuales derechos han sido autorizados a ellos. La ACL indica quién tiene acceso a un objeto en particular o a sus propiedades, y no que derechos podría tener el objeto.

OBJETO COMO ELEMENTO AUTORIZADOR

Cualquier objeto puede ser un elemento autorizador de sí mismo o de cualquier otro objeto en el árbol NDS. Los típicos objetos que son elementos autorizadores son los cuatro contenedores ([Raíz], País, Organización y Unidad Organizacional) y algunos objetos del tipo hoja (Usuario, Grupo y Función Organizacional).

CONTENEDOR COMO ELEMENTO AUTORIZADOR

Un nuevo concepto de seguridad en Netware Novell 4.x es la habilidad de asignar los derechos del sistema de archivos y del NDS a los contenedores. Cuando los derechos son asignados a un contenedor en específico, todos los subcontenedores y objetos dentro del contenedor reciben estos derechos y por lo tanto la seguridad equivalente a la del contenedor.

DETERMINANDO LOS DERECHOS EFECTIVOS PARA NDS

Para cada objeto NDS, los derechos efectivos de un usuario a un objeto están determinados por:

- Asignaciones de derechos explícitas hechas al objeto para un usuario, más
- Cualquier asignación de derechos explícita hecha a cualquiera de las equivalencias de seguridad de los objetos: Grupo, Función Organizacional, [Público], y contenedores a los que pertenece incluyendo el [Raíz].

ADMINISTRACIÓN SUBARBOL

Porque la Base de datos de NDS es global (contiene información de toda la red), puede tener contenedores que representen geográficamente diversas organizaciones. Normalmente es más conveniente utilizar diferentes coordinadores del árbol NDS y de los sistemas de archivos locales, que tener solamente una autoridad administrativa central. En general, existen tres formas de dividir la administración para cada subárbol: un administrador por ramificación, múltiples administradores por rama y administradores por grupo de trabajo. La forma que se elija dependerá de las necesidades de la organización.

Administrador por ramificación simple: Dependiendo de las necesidades de seguridad de la organización, puede ser que solamente se requiera un usuario que posea todos los derechos de coordinación sobre una ramificación en particular. Si éste es el caso, sería necesario eliminar algunos derechos heredados del *usuario ADMIN* original, tales como:

- Asigne al responsable del subárbol como un elemento autorizador explícito del contenedor a ser controlado, asignándole todos los derechos sobre los objetos y sus propiedades.

- Revoque derechos heredados para que el ADMIN original no transmita estos derechos al contenedor

- Remueva cualesquiera derechos heredados al contenedor del usuario ADMIN original

- Asegúrese que el coordinador del subárbol tiene derechos del tipo supservisor y después remueva cualquier asignación de derechos del usuario ADMIN original, para que éste no pueda restringir los derechos del responsable del subárbol.

Administradores múltiples: Si las necesidades de la organización requieren de un adminitrador por ramificación, entonces debemos autorizar a cada responsable con los derechos apropiados sobre contenedor. Esto es:

- Asigne cada administrador de subárbol como un elemento autotizador explícito del contenedor a ser controlado, asignándole todos los derechos sobre los objetos y sus propiedades

- Si el usuario ADMIN original no va a coordinar la ramificación, remuevale derechos hereditarios, para que no transmita dichos derechos al contenedor

- Si el usuario ADMIN original no va a controlar la ramificación, remueva cualesquiera asignaciones de derechos del usuario ADMIN original al contenedor

- Si los administradores de cada subárbol necesitan ser independientes uno de otro, entonces asegúrese que cada administrador subárbol tiene derechos de objeto tipo supervisor para sí mismos, y entonces elimine cualquier otra asignación de derechos de usuario para cada administrador subárbol y elimine derechos heredados,

estableciendo el *IRF* de cada administrador de árbol independiente de los derechos de objeto del tipo Browse y propiedades del tipo Read.

Administrador de grupo de trabajo: Su organización puede tener necesidades de seguridad que requieran de una administración central que además permita la coordinación de grupos de trabajo o departamentos. Por esto, es imperativo establecer la seguridad de forma que si el responsable de una rama abandona la compañía bajo circunstancias no favorables, los recursos en dicha rama puedan ser aún administrados. Para ello:

- Asigne al administrador del grupo de trabajo como un elemento autorizador explícito del contenedor a ser administrado
- Asegúrese que el usuario ADMIN cuenta con la asignación de derechos explícita al contenedor asignando los derechos y las propiedades sobre el objeto
- Asigne al usuario ADMIN derechos explícitos sobre el objeto usuario que será responsable del grupo de trabajo
- Revoque todos los derechos heredados (excepto el Browse) al coordinador del grupo de trabajo de forma que no herede los derechos necesarios para administrarse

ASIGNANDO LOS PROGRAMAS INICIALES DE LOS PERFILES

Los programas iniciales de los perfiles se utilizan cuando diversos grupos de usuarios necesitan ambientes de trabajo comunes. Para poder ejecutar el programa inicial, los usuarios deben tener consignada la capacidad para leerlo. Para ello, el objeto Perfil (que es el objeto que lo contiene) debe contar con los derechos necesarios sobre el sistema de archivos.

OBJETOS DE CORRESPONDENCIA A DIRECTORIOS

Estos objetos son utilizados para corresponder al apuntador de un directorio más que al directorio en sí mismo. Cuando se utilizan estos objetos, los usuarios son

capaces de leer las propiedades asignadas al directorio correspondido. Este objeto puede tener también derechos del sistema de archivo asignados a él, sin embargo, estos derechos no se transmiten automáticamente al usuario. De cualquier forma, si los usuarios tienen asignado un nivel de seguridad equivalente al del objeto de Correspondencia de Directorio, el administrador del sistema podrá fácilmente redireccionar una aplicación así como reasignar lo derechos del sistema de archivo de dichos usuarios con la simple acción de cambiar los valores del objeto de Correspondencia de Directorio.

ALIAS DE INGRESO

En Netware Novell 4.x un usuario puede tener un objeto Alias creado para él. Cuando un usuario ingresa con el objeto Alias, el usuario ejecuta el programa de inicio del contenedor e inmediatamente ingresa el Alias. Si se crea un objeto Alias en un contenedor diferente al del objeto original, necesitará asignar los derechos del objeto Alias para ejecutar el nuevo programa inicial del contenedor.

CONCEPTOS Y CARACTERISTICAS DEL SISTEMA DE ARCHIVOS[NOV94]

Los derechos que el sistema de archivos otorga a directorios y archivos se presentan a continuación en las siguientes tablas:

Derechos sobre directorios del Sistema de Archivos		
Derecho		Descripción
S	Supervisor	Autoriza todos los derechos sobre el directorio, sus archivos y sus subdirectorios. Este derecho prevalece sobre cualquier restricción esignede a subdirectorios o archivos a través de un IRF.
R	Read	Permite que el directorio pueda abrirse y leerse
W	Write	Permite a los usuarios abrir y escribir archivos. No es posible desplegar los archivos existentes sin la autorización Read
C	Create	Permite a los usuarios crear directorios y archivos. Esta autorizeción se requiere para escribir datos a cualquier archivo creado.
E	Erase	Permite al usuario borrar directorios, sus archivos y subdirectorios

Derechos sobre directorios del Sistema de Archivos		
M	Modify	Permite a los usuarios cambiar los atributos de archivos y subdirectorio y renombrar el directorio, sus archivos y subdirectorios. No permite modificar el contenido de los archivos
F	File Scan	Permite a los usuarios ver los archivos
A	Access Control	Permite a los usuarios cambiar las asignaciones de derechos del directorio y los IRFs para los directorios. Esto permite a los usuarios modificar las asignaciones de derechos sobre archivos. Los usuarios pueden autorizar cualquier derecho (excepto el de supervisor) a cualquier otro usuario

Derechos sobre archivos del Sistema de archivo		
Derecho		Descripción
S	Supervisor	Autoriza todos los derechos sobre el archivo. Los usuarios con este derecho pueden autorizar cualquier derecho de archivo a otro usuario y pueden modificar todos los derechos en el IRF del archivo
R	Read	Abrir y leer el archivo
W	Write	Abrir y escribir archivos.
C	Create	Recuperar el archivo despues que se ha borrado.
E	Erase	Borrar el archivo.
M	Modify	Modificar los atributos del archivo y renombrarlo. No permite modificar el contenido del mismo.
F	File Scan	Ver el archivo cuando se esta desplegando el contenido del directorio.
A	Access Control	Modificar las asignaciones de derechos de archivos y su IRF. Los usuarios pueden autorizar cualquier derecho (excepto el de supervisor) a cualquier otro usuario.

En cuanto a los atributos que puede otorgar el sistema de archivos sobre directorios y archivos son:

Atributos de directorios del Sistema de archivo		
Atributo		Descripción
Dc	*Don't Compress	Adicionado a un directorio, este atributo evita que todos los archivos dentro del directorio sean comprimidos.

Atributos de directorios del Sistema de archivo		
Di	Delete Inhibit	Previene que los usuarios borren directorios, aún cuando tengan autorizado el derecho de Erase.
Dm	*Don't Migrate	Adicionado a un directorio, este atributo no permite que los archivos dentro del directorio migren a un dispositivo de almacenamiento secundario
H	Hidden	Esconde los directorios cuando se ejecuta el comando DIR de DOS. El programa NDIR de Netware Novell 4.x los desplegará si el usuario cuenta con los derechos de File Scan apropiados
Ic	*Inmediate Compress	Adicionado a un directorio, este atributo alerta al sistema de archivos para comprimir un archivo tan pronto como el sistema operativo pueda manejar dicha acción
N	Normal	Marca un directorio como Read/Write y No compartido. Remueve cualquier otro indicador.
P	Purge	Cuando este atributo es asignado a un directorio, automáticamente Netware Novell 4.x removerá por completo todos los archivos qua hayan sido borrados en el directorio. Esta acción impedirá recuperarlos después.
Ri	Rename Inhibit	No permite que los usuarios renombren los directorios, aún cuando cuenten con el derecho de Modify.
Sy	System	Esconde los directorios cuando se ejecuta el comando DIR de DOS y no permite que sean borrados o copiados. El programa NDIR de Netware Novell 4.x puede ver estos direcotrios si el usuario cuenta con los derechos de File Scan.

Atributos de archivos del Sistema de archivos		
Atributo		Descripción
A	Archive Needed	Identifica los archivos modificados después del último respaldo. Netware Novell 4.x asigna este bit automaticamente.
Ci	Copy Inhibit	Restringe los derechos de copiado y los otorga solamente a los usuarios que ingresaron desde estaciones de trabajo Macintosh. Aún si los usuarios cuentan con los derechos de Read y File Scan a nivel del archivo o del directorio no podrán copiar el archivo.

Atributos de archivos del Sistema de archivos		
Dc	*Don't Compress	No permite que los datos sean comprimidos. Este atributo es superior a los atributos de compresión automática de archivos no accesados dentro de un número de días específico.
Di	Delete Inhibit	Restringe los derechos de borrado de aquellos usuarios que ingresaron a la red a través de una estación de trabajo Macintosh.
Dm	*Don't Migrate	Previene la migración de archivos del disco duro del servidor a otro medio de almacenamiento.
H	Hidden	Oculta los archivos de manera que no puedan verse con el comando DIR de DOS. Pueden ser vistos con el comando NDIR.
I	Index	Esto indica a Netware que los elementos en la *FAT* del archivo deben de ser indexados en la memoria del servidor para accesar más rápido el archivo.
Ic	*Inmediate Compress	Comprime los datos de un archivo tan pronto como éste se cierre.
N	Normal	Mientras no tengan el atributo N en los atributos del archivo, si habilita este atributo el archivo será de Read/Write.
P	Purge	Cuando se asigna este atributo a un archivo, Netware removera este archivo despues que se haya borrado.
Ri	Rename Inhibit	Evita que el archivo sea renombrado
Ro	Read Only	Evita que el archivo sea modificado. Este atributo automáticamente habilita los atributos Delete Inhibit y Rename Inhibit.
Rw	Read Write	Permite escribir en un archivo. Todos los archivos son creados con este atributo.
S	Shareable	Permite a diversos usuarios accesar un archivo simultáneamente. Este atributo es utilizado normalmente con el atributo Read Only, para que un archivo que es utilizado por múltiples usuarios no pueda modificarse.
Sy	System File	Oculta estos archivos del comando DIR de DOS y evita que se copien o borren.
T	Transactional	Permite que el archivo sea registrado y protegido por el Sistema de registro de Transacciones.
X	Execute Only	Evita que un archivo sea copiado, modificado o respaldado. Este atributo no puede ser removido a menos que el archivo sea borrado. Utilicelo solamente en archivos .EXE o .COM.

Banderas de estado de atributo de archivos nuevos		
Bandera		Descripción
Co	Compress	Bandera de estado que indica si el archivo esta comprimido.
Cc	Can't Compress	Bandera de estado que indica que el archivo no puede comprimirse.
M	Migrated	Bandera de estado que indica que el archivo ha aido migrado.

DETERMINANDO LOS DERECHOS EFECTIVOS PARA EL SISTEMA DE ARCHIVOS

Los derechos efectivos que un usuario puede posee sobre un directorio o archivo son determinados por:

- El derecho Supervisory sobre un directorio, el cual autoriza todos los derechos al directorio y subsecuentes subdirectorios y archivos que pertenezcan a él. El derecho de Supervisory no puede reasignarse ni revocarse por un IRF.

- Cualquier asignación de derechos explícita a usuarios sobre un directorio

- Cualquier asignación de derechos explícita a usuarios hechas mediante un Grupo ó Función Organizacional donde el usuario es: miembro de, equivalente en seguridad de o contenedor de un miembro de.

Los derechos sobre el sistema de archivos pueden ser asignados a nivel de directorio y archivo. Los derechos asignados a los directorios son asignados automáticamente a todos los archivos en él contenidos. Los derechos asignados a archivos en específico prevalecen sobre cualquier derecho heredado del directorio que lo contiene.

ASIGNANDO DERECHOS ADICIONALES AL SISTEMA DE ARCHIVOS

El administrador del sistema tendrá que asignar derechos adicionales al sistema de archivos para:

= Aplicaciones y archivos de datos que los usuarios necesitan accesar. Cuando se instalan nuevas aplicaciones en un servidor, los derechos del sistema de archivos deben ser asignados de forma que los usuarios puedan accesarlos. En suma, los usuarios necesitan un área separada para almacenar archivos de datos, a los cuales

necesitan accesar de la mejor forma. Esto se hace normalmente asignando un directorio a cada usuario.

= Usuarios que no están instalados en el mismo contexto que el servidor y por lo tanto no adquieren derechos del sistema de archivos sobre SYS:PUBLIC. Por omisión, los derechos de Read y File Scan son asignados por SYS:PUBLIC al contenedor que está instalado en el servidor. Si se crean cuentas de usuario fuera de este contenedor, no heredarán estos derechos. Por lo tanto, los derechos del sistema de archivos deben ser asignados siempre a fin de que los usuarios puedan ejecutar la correspondencia con la unidad lógica donde se encuentra el programa inicial por omisión.

DONDE ASIGNAR LOS DERECHOS DEL SISTEMA DE ARCHIVOS

Con Netware Novell 4.x se tienen más opciones para asignar derechos. Se pueden asignar derechos a los contenedores Grupos, Función Organizacional, Usuarios, etc. El dónde serán asignados estos derechos dependerá de las necesidades de la organización.

- [Raíz]. Es un ambiente de red pequeño donde todos los usuarios necesitan accesar a todos los servidores, los derechos del sistema de archivos a SYS:PUBLIC pueden asignarse al objeto [Raíz], es decir, los derechos sobre aplicaciones comunes (procesadores de palabra, etc) pueden asignarse al objeto [Raíz]. En este caso, todos los usuarios adquirirán estos derechos.

- Organización. Asignar derechos a un objeto Organización es similar que asignarlos a nivel del [Raíz]. En lugar de asignar derechos de red WAN (Cuando la red esta en todo el mundo), las sentencias de derechos pueden segregarse por divisiones o ubicaciones designadas por el objeto Organización.

- Unidad Organizacional. El uso de objetos del tipo Unidad Organizacional proporciona flexibilidad adicional en la asignación de derechos. Los derechos del sistema de archivos asignados a nivel de este objeto son comunes en servidores que comparten una base de datos departamental. Los derechos a más aplicaciones y

archivos de datos se asignarán a los objetos de este tipo más cercanos a los objetos Usuario.

- Grupo o Función Organizacional. Cuando es imposible asignar derechos a nivel contenedor dada la sensibilidad de los datos, es posible crear objetos del tipo Grupo o Función Organizacional para poder establcer los derechos y propiedades. Los derechos del sistema de archivos sobre estos objetos son también prácticos en servidores especializados, como los servidores de aplicaciones o de base de datos, donde solamente un subconjunto de todos los usuarios necesitan accesar al sistema de archivo.

IV.5 IMPLEMENTANDO UN ESQUEMA DE SEGURIDAD CON NETWARE NOVELL 4.X

Con sus características en materia de seguridad, Netware Novell 4.x proporciona un sistema seguro y auditable que puede ser administrado por una base empresarial amplia. De cualquier forma, los diseñadores de red, responsables y usuarios deben activar y utilizar estas funciones para construir un ambiente de computación en red confiable tanto a nivel global como a nivel local.

Netware Novell 4.x ofrece seguridad multinivel flexible que controla el acceso a la red y a sus recursos. Estas características pueden categorizarse a través de NDS y el sistema de administración de recursos los cuales controlan la seguridad en: la red, el acceso, el ingreso, los derechos, los atributos y los servidores de archivos y de información.

Estas características permiten al coordinador del sistema controlar la seguridad de la red la cual puede implementarse en los servicios de directorio, red, servidor y niveles del sistema de archivos para determinar:

- Quién puede accesar la red,
- Que recursos pueden accesar los usuarios,

- Como pueden los usuarios utilizar los recursos,
- Quién puede efectuar tareas en la consola del servidor.

Para completar el esquema, Netware Novell 4.x presenta otras características como:

- Identificación del usuario en los niveles individual, grupo y administrativo
- Autentificación del usuario
- Administración de pasaportes y encriptamiento de los mismo
- Control de acceso a los recursos de la red mediante la asignación de derechos y atributos
- Seguridad en la consola para garantizar que solamente aquellos usuarios con las equivalencias de seguridad apropiadas tengan acceso a la consola del servidor.

MEDIDAS ESPECIFICAS DE SEGURIDAD PARA NETWARE 4.X[NOV94]

ASEGURANDO AL SERVIDOR

La seguridad del servidor esta fundamentada en dos aspectos primordiales: su seguridad física y su seguridad lógica. La primera puede proporcionarse implementando las medidas comentadas en el capítulo anterior. Una vez que el servidor ha sido asegurado físicamente, pueden ejecutarse acciones de seguridad adicionales en la consola como:

- Teclear REMOVE DOS para prevenir que se ejecuten *NLM*s localizadas en las unidades de disco flexible
- Teclear SECURE CONSOLE para restringir la ejecución de NLMs de otros lados que no sea el directorio SYS:\SYSTEM y para deshabilitar el ingreso al *debugger* desde un comando en el teclado
- Asegurar la consola del servidor de archivos dentro con el NLM llamado MONITOR
- Deshabilitar todas las capacidades de consolas remotas, o asignar a RCONSOLE un pasaporte único. RCONSOLE utiliza telnet y podría fácilmente

comprometer el pasaporte de la consola ya que el tráfico telnet viaja como un texto claro sobre el cable. Asegúrese que el pasaporte de la consola sea diferente al pasaporte del usuario ADMIN y nunca almacene dicho pasaporte en el AUTOEXEC.NCF en el servidor

ATAQUE MEDIANTE NLMS

Existen diversos ataques NLM en la actualidad que permiten cambiar el pasaporte del usuario ADMIN sin necesidad de conocer el viejo pasaporte. Estos NLM llaman una función denominada SetBinderyObjectPassword la cual se encuentra claramente documentada en las APIs del servidor de Netware Novell 4.x. Como los NLMs son extensiones del sistema operativo, tienen permitido hacer llamadas directar al sistema. Es tarea del administrador de la red conocer que NLMs pueden ejecutarse y que resultados producen.

SEGURIDAD EN EL PROCESO DE INGRESO

Existen muchos elementos que pueden originar problemas de seguridad o rupturas durante el proceso de ingreso. Este aspecto es considerado frecuentemente el punto débil en un sistema de seguridad en cómputo. Algunas medidas que se pueden tomar con Netware Novell 4.x son:

- Habilitar la detección de intrusos para que notifique al administrador del sistema cuando una cuenta ha sido bloqueada por haber agotado su capacidad de ingresos fallidos, ya sea porque ingreso con pasaporte inválido, o conociendo su perfil y el pasaporte no. Dos o tres intentos de ingreso erróneos deben ser el máximo permitido. Configure el servidor para que registre los intentos de ingreso erróneos de la última hora y para que bloquee la cuenta de dicho usuario por dos horas o más. Incremente estos límites de tiempo cuando sea necesario darse más tiempo para investigar.

- Establecer una política robusta de administración de pasaportes que de seguridad a todo el sistema. Como el proceso de ingreso involucra al elemento humano, la seguridad depende en gran medida de como son controlados los

pasaportes. Los pasaportes deben ser obligatorios para todas las cuentas de usuario. Una buena política es que los pasaportes se cambien de forma obligatoria cada 30 o 40 días y que sean únicos. Los *ingresos de gracia* pueden limitarse a 2 o 3 por cada usuario. Estos lineamientos pueden ser ajustados para conformar la política de seguridad de una organización.

ADMINISTRANDO CUENTAS ADMINISTRATIVAS

Las cuentas de administración deben estar limitadas a un máximo de 2 ó 3 por red, una por cada resposable. Debe haber más de un administrador en caso de una emergencia, y los perfiles de estos coordinadores de preferencia no deben ser semejantes a los de los usuarios ADMIN, Supervisor, [Raíz], etc.

ADMINISTRANDO CUENTAS DE USUARIO

La administración apropiada de las cuentas de usuario es un elemento importante de la seguridad de la red. Para empezar, los usuarios podrían tener solamente derechos autorizados a las áreas de la red que requieren accesar por sus requerimientos de trabajo. Los aspectos a vigilar son:

- Pasaportes de las cuentas de usuarios: Los usuarios de la red deben ser bien educados en la importancia de los pasaportes y su uso. Es virtualmente imposible para un administrador de red analizar todos los pasaportes de los usuarios a fin de asegurar que son una forma de detener a usuarios no autorizados. En las políticas de seguridad y el entrenamiento propuesto, establezca lineamientos específicos en cuanto a pasaportes y entrene a sus usuarios en su propósito e implementación apropiada.

- Valores iniciales en las cuentas de usuario y pasaportes. Cuando se crea una nueva cuenta de usuario el atributo de pasaporte no se encuentra activado. Hay que asignarlo de manera individual a cada usuario tomando en cuenta las características de: Longitud mínima (5 caracteres), periodo de vida útil (90 días), unicidad (No), Modificable por el usuario (Si), número de ingresos de gracia, y número de intentos erróneos permitidos. Es recomendable modificar estos parámetros de acuerdo a los requerimientos específicos de seguridad de la red.

EQUIVALENCIAS DE SEGURIDAD

El sistema operativo utiliza las equivalencias de seguridad propias de los contenedores para asignar automáticamente diversos derechos a objetos del tipo hoja. Cuando un usuario es adicionado a la lista de miembros del objeto Grupo o del objeto Función Organizacional, los derechos del Grupo o Función Organizacional están listados en la equivalencia de seguridad del usuario.

ENCRIPTAMIENTO DE PASAPORTES

Netware Novell 4.x posee una característica que controla el uso de pasaportes encriptados. El comando ALLOW UNENCRYPTED PASSWORDS se utiliza para encriptar pasaportes y resaltar su integridad, asegurándo que los pasaportes no sean interceptados ni utilizados por personas no autorizadas. El valor por omisión de este parámetro es de OFF y significa que todos los pasaportes se encriptarán. Cuando este parámetro está en ON, los pasaportes se pueden encriptar, pero no de manera obligatoria.

CONSOLA DE SEGURIDAD

Esta utilería permite a operadores autorizados hacer uso de la consola, al tiempo que evita:

- Ejecutar NLMs de directorios diferentes al SYS:SYSTEM. Con esto evitamos ejecutar dichos módulos desde discos flexibles.
- Ejecutar comandos desde el teclado dirigidos al debugger del sistema operativo. Esto restringe la capacidad de accesar directamente datos en el servidor.

DETECCIÓN DE INTRUSOS

Netware Novell 4.x proporciona varias opciones que (cuando están activadas) auxilian en la detección de intentos de ingreso erróneos y bloquea el objeto Usuario que intentó ingresar. Esta característica de detección/bloqueo de intrusos se puede establecer para reconocer a un usuario no autorizado que está tratando de ganar

acceso. Esta característica es administrada a nivel de los objetos Organización y Unidad Organizacional.

DESCONECTANDO ESTACIONES SIN ATENDER

Otra medida de seguridad fácil de implementar es entrenar a los usuarios para que terminen la conexión con la red cuando dejen sus computadoras. Si prefiere una alternativa para asegurar que los usuarios siempre se desconecten, dótelos de una utilería de seguridad que bloquee automáticamente la computadora cuando detecte un período de inactividad definido.

OTRAS SUGERENCIAS EN SEGURIDAD

- Limite las conexiones a una por usuario
- Establezca restricciones en cuanto a horarios y estaciones de trabajo autorizadas para ingresar a la red
- No permita pasaportes fáciles en el proceso de ingreso
- Deshabilite o elimine inmediatamente las cuentas de usuario de empleados dados de baja y de otros usuarios inactivos
- Ejecute programas de búsqueda de virus y realice los respaldos de forma frecuente.
- Utilize la utilería de SECURITY periódicamente a fin de descubrir problemas potenciales y tomar las acciones apropiadas

La administración remota de servidores (mediante una estación de trabajo en la red o de una computadora personal utilizando un modem) puede proporcionar más seguridad al servidor. Por otro lado, el teclado y el monitor del servidor pueden removerse y colocar el servidor en una ubicación segura. Además, pueden realizarse las siguientes actividades:

- Rastree los directorios y edite los archivos de texto en las particiones de DOS y de Netware Novell 4.x en el servidor
- Transfiera archivos al servidor

- Apague y reinicialice el servidor
- Instale o actualice Netware Novell en el servidor remoto

Finalmente, los modelos de seguridad de Netware Novell 4.x deben implementarse de la siguiente manera [NOV94]:

MODELO SIMPLE

= Compre un paquete antivirus para red (De preferencia que pueda cargarse en memoria RAM desde el AUTOEXEC.NCF)

= Asigne un pasaporte a cada usuario

= Instale siempre el software de aplicación en la red de acuerdo a las especificaciones de instalación

= Escoja un pasaporte para la clave ADMIN que sea difícil de adivinar. Invite a sus usuarios a hacer lo mismo con los propios

= Coloque el servidor y los dispositivos de respaldo en un lugar seguro. También conserve dispositivos y software de respaldo en otra ubicación.

= Realice los respaldos en forma regular

= Al finalizar la operación de respaldo, restaure el primer volumen del respaldo en otro directorio (a fin de evaluarlo)

= Asegure la consola del servidor de archivos con el módulo MONITOR.NLM

= No registre el pasaporte de la consola del servidor de archivos en el archivo AUTOEXEC.NCF

= Establezca alguna forma de educación entre sus usuarios relacionada con la seguridad en cómputo.

MODELO BASICO

= Implemente el modelo simple

= Eduque a los usuarios en materia de pasaportes y virus de cómputo

= Solicite a los usuarios que finalizen sus sesiones o las bloqueen cuando no utilicen la estación de trabajo

= Evalue su proceso de respaldo realizando el siguiente procedimiento:

- Cree un directorio
- Grabe en él archivos de datos no esenciales
- Respalde dichos archivos
- Borre los archivos del directorio
- Restaure los archivos del respaldo previamente realizado

= Mantenga una copia de todos los archivos de datos y de las aplicaciones fuera del edificio donde residen para poder realizar una recuperación en caso de desastre total

= Aprenda y entienda el sistema de archivo para directorios y archivos, le puede ayudar a establecer de mejor forma los derechos y atributos que cada usuario requiere de acuerdo a su trabajo

= Instale software en su propio directorio

= Remueva el sistema operativo DOS del servidor tecleando REMOVE DOS en la consola

= Asegúrese que el pasaporte de la consola es diferente al pasaporte del usuario ADMIN

MODELO PROTEGIDO

= Implemente el modelo básico

= Establezca un plan de educación en materia de seguridad

= Realice un programa cuya premisa sea la distribución de claves

= Establezca los pasaportes para los servidores de impresión

= Asegúrese que todos los usuarios terminen correctamente el programa inicial del sistema o asigneles sus propios programas iniciales

= Limite el número de conexiones concurrentes

= Asigne a su administrador de sistema las capacidades y equivalencias de seguridad del usuario ADMIN y luego borre éste último

= Verifique la lista de control de acceso y los derechos que ésta detenta en NDS para todos los usuarios diferentes al ADMIN.

= Las cuentas de usuario de empleados despedidos o cualesquiera otras no utilizadas deben cancelarse o definitivamente eliminarse

= Conserve una lista de cuentas borradas, usuarios y demás para utilizarla cuando restaure sus respaldos en caso necesario

= Habilite la detección de intrusos

= Ejecute el comando SECURE CONSOLE en el servidor para restringir que se ejecuten NLMs

= Deshabilite todas las capacidades de consola remota o asigne a RCONSOLE un pasaporte único

= Establezca restricciones de tiempo a los usuarios de la red

= Remueva los derechos Write y Create en el directorio MAIL del elemento autorizador [Público]

= Utilize un analizador de red para generar una lista de pasaportes inválidos

= Entrene a sus usuarios para que salgan de la red cuando dejen su computadora, o provéalos de alguna utilería que bloquee automáticamente la computadora.

= Establezca cambios regulares de pasaportes para todas las cuentas

= No permita el reuso de pasaportes

= Verifique el tamaño de sus ejecutables instalados con los tamaños especificados por el fabricante. Realice esta actividad periódicamente a fin de asegurarse que no han cambiado de tamaño

MODELO AUDITADO

= Establezca el modelo protegido

= Realice regularmente una auditoría a la Administración de red contratando auditores expertos

= Vigile el acceso a las habitaciones donde se localizan el servidor, los cables y las estaciones de trabajo

= Controle los archivos ejecutables

= Proporcione entrenamiento especializado en seguridad a sus usuarios y administradores con actualizaciones anuales del tópico

MODELO ASEGURADO

= Implemente el modelo auditado

= Remueva las unidades de disco de las estaciones de trabajo que no las utilicen

= Restrinja las direcciones físicas de las estaciones

= Asegúrese que solo usuarios confiables tienen acceso a las estaciones de trabajo

= Elimine cuentas de usuarios no confiables para mantener su red confiable

= Asegure todas las estaciones de trabajo

CONCLUSIONES

El desarrollo de este documento y el proceso natural de maduración de ideas, me permiten establecer en esta etapa final algunos aspectos que considero importante señalar. Estas observaciones son:

Actualmente, las redes son los elementos más importantes de las organizaciones necionales y multinacionales porque permiten interconectar todos los objetos que conforman el ambiente organizacional, estableciendo un mejor control y administración de los recursos y actividades de las instituciones a fin de mejorar la toma de decisiones y lograr con éxito los objetivos del negocio.

Les redes son un recurso tecnológico que involucra elementos físicos y lógicos, los cuales evolucionan rápidamente. Ante esta circunstancia, debemos estar preparados para realizar el cambio de tecnología gradualmente, y para ello, es necesario establecer un conjunto de lineamientos y políticas en materia de administración de red que organicen dichos procesos de renovación/sustitución y nos permitan anticipar las situaciones problemáticas a fin de proponer las respectivas soluciones y afectar lo menos posible la operación de las aplicaciones del negocio que utilizan la red. Un retraso en el proceso de dichas aplicaciones podría afectar de manera muy importante el rumbo del negocio.

Para establecer un esquema de Administración de red es necesario contar con la participación de los usuarios, los proveedores y los responsables de la red. Estos últimos deben estudiar y analizar los requerimientos de la red para: establecer y mantener su configuración, definir y aplicar los procedimientos en caso de fallas, medir el desempeño de los componentes de la red en lo individual y de ésta como un

todo, establecer indicadores que midan su actividad, implementar una arquitectura de seguridad y planear la capacidad de la red. Todos estos elementos en conjunto permiten que los coordinadores de la red cumplan con sus responsabilidades y sobre todo, sostengan lo comprometido con el usuario en los acuerdos de niveles de servicio. Uno de los modelos de la administración de red más importantes es el modelo funcional. Este modelo describe todos los procesos que el elemento humano debe realizar para alcanzar el objetivo de administrar la red.

Uno de los puntos que había permanecido olvidado dentro del ambiente de red es la seguridad. Las primeras políticas y procedimientos de seguridad eran muy estrictos y poco aplicables a la realidad. Con la llegada de las computadoras personales, este aspecto fue relegado por la poca relevancia que tiene proteger una computadora stand-alone cuyos recursos utiliza solamente una persona. Sin embargo, con el desarrollo que han tenido las comunicaciones, las redes de computadoras han proliferado en forma por demás extraordinaria. Esta interconexión de computadoras diversas ha sacado a relucir los viejos aspectos de seguridad de los sistemas de cómputo/comunicación que han permanecido guardados en el cajón de los recuerdos. Una arquitectura de seguridad de una red protege la información que viaja a través de la misma, auxiliándose de soluciones físicas y lógicas. Sin embargo, este esquema debe ajustarse siempre a las necesidades de la organización donde desee implementarse. Por eso es muy importante realizar primero los estudios y análisis que determinen el grado y nivel de seguridad que requiere la red.

Al momento de elegir la arquitectura de seguridad de la red adecuada a nuestras necesidades no debemos olvidas tres aspectos importantes:

- Totalidad. Es decir que el esquema de seguridad de la red cubra completamente con los requisitos de seguridad especificos de nuestra red

- Simplicidad. Este aspecto debe aplicarse tanto en el diseño como en el entendimiento y uso del esquema de seguridad. Si se complica demasiado la arquitectura, no habrá el suficiente personal ni tiempo para mantenerla y por lo tanto tiende a fracasar
- Integración. Se refiere al acoplamiento de todos los componentes de seguridad tanto físicos como lógicos pertenecientes a diferentes proveedores. Es muy importante buscar siempre la compatibilidad de los mismos para no "casarse" con un proveedor y poder contar con un sistema realmente abierto a las diversas soluciones que existan o que esten por venir. Este punto también incluye la interrelación robusta entre los procesos y procedimientos, instrumentos físicos y lógicos y recursos humanos del esquema de seguridad de una red.

Un aspecto muy importante que hay que considerar durante la implementación de un esquema de seguridad es el de los instrumentos con que contamos hoy en día para establecerlo. Estos dispositivos son escasos, es por eso que concluimos que se necesitan de nuevos desarrollos, tanto a nivel de hardware como a nivel de software, que soporten una arquitectura de seguridad que sea restrictiva con los intrusos potenciales y amigable con los usuarios autorizados, sin perder de vista la actividad de éstos últimos, pues esta confirmado que muchas veces, sus acciones afectan seriamente la integridad de la red.

Debemos considerar un estudio profundo para la adquisición de componentes de hardware y software que auxilien la labor de protección de la red. Esto es, no debemos dejarnos llevar por las palabras convincentes de un proveedor y comprar lo primero que nos presente sin reconocer primero su grado de aplicación en nuestro esquema. Hay que estar concientes de la importancia de la información que genera nuestra organización para poder determinar hasta que niveles es factible protegerla. Una protección muy restrictiva puede empeorar la situación en lugar de resolverla.

Esta observación nos lleva a otra también trascendente. Necesitamos conocer al personal que labora en nuestra institución y que utiliza el recurso de la red. Si perdemos de vista este aspecto, estaremos dejando a medias la labor de seguridad. El elemento humano es el más impredecible de todos, y el más difícil de controlar, sin embargo, una buena política de seguridad, aunada a un conjunto de normas y sanciones y a la paciencia, comprensión y decisión del administrador de red, facilitará esta labor tan problemática.

Dentro del recurso humano existe un aspecto poco valorado que es la educación del usuario. Hasta el día de hoy, las organizaciones no han comprendido que el entrenamiento del usuario en el uso y aprovechamiento de los recursos de computación/comunicación con las que cuenta la institución permite que el usuario apoye de forma más acertada la labor de resolución de problemas y detección y reparación de fallas, ya que sus solicitudes de servicio no serán vagas, como lo son actualmente en muchas entidades que cuentan con sistemas de cómputo/comunicación en México.

A pesar de las medidas de protección que tomemos, siempre existe la posibilidad de que un intruso ingrese en la red, y debemos estar siempre preparados para cuando llegue el momento en que se cruce en nuestro camino. Algunas de las acciones que a realizar son: identificar el ataque, capturar al culpable (en el mejor de los casos), y registrar los eventos de violación de la red en una bitácora para sentar precedente y establecer las medidas adecuadas para que no vuelva a suceder. Considero que esta es una lección importante que contiene este documento. No importa cuantos métodos intente el agresor para violar la red, lo importante es estar preparados.

Para terminar con el tópico de la seguridad en redes, no debemos olvidar que el tiempo se encarga de cambiar todas las situaciones, y que un sistema que dejamos seguro el día de hoy, no garantiza conservarse así al día siguiente. Una política contínua de auditoría es imprescindible para mantener los niveles de seguridad que tanto trabajo costo establecer. Esta labor ayudará en gran medida a los administradores de la red a detectar errores en el esquema de seguridad y sobre todo, permitirá corregirlos.

Finalmente, debo agregar que el conocimiento y experiencia que la elaboración de esta tesis ha dejado en mi, me permite participar de manera más activa en una rama de la Informática muy interesante : las comunicaciones. El Plan de estudios que curse de 1989 a 1993, no contempla un estudio muy detallade es este ámbito, sin embargo, si me permitió conocerlo y en mi caso muy particular preferirlo por encima de los demás. Vaya pues este espacio para agradecer a la Facultad de Contaduría y Administración por la oportunidad que me brindó al recibirme como alumna y facilitarme el aprendizaje de tantas cosas que han trascendido en mi persona y me hacen crecer como un profesionista. Gracias.

GLOSARIO DE TERMINOS

Ad-hoc. Apropiado a su fin.

ARPANET. (Advanced Research Projects Agency NETwork). Red Avanzada de Agencias para Proyectos de Investigación. Red de Investigación fundada por DARPA (originalmente ARPA) y construida por BBN, Inc., en 1969. Fue pionera en la tecnología de conmutación de paquetes y la piedra angular y base de la ahora gigantesca INTERNET. En 1983, la parte militar de comunicaciones se dividió como MILNET.

ATM. (Asynchronous Transfer Mode). Modo de transferencia asíncrona. Red estándar para transmitir información a alta velocidad por medio de fibras ópticas. Utiliza un paquete de 53 bytes de longitud fija para datos.

Backbone. En comunicaciones, la parte de una red que soporta el mayor tráfico. Puede interconectar diferentes localidades, y se pueden conectar a ella redes más pequeñas.

Baudio. Velocidad de señalización de una línea. Es la velocidad de conmutación, o el número de transiciones (cambios de voltaje o de frecuencia) que se realizan por segundo. Solo a baja velocidad, los baudios son iguales a los bits por segundo (bps); por ejemplo, 300 baudios es igual a 300pbs.

Bit.(BInary digiT). Dígito Binario. Un dígito simple de un número binario (1 ó 0). En la computadora, un bit es físicamente una celda de memoria (constituida por transistores), un punto magnético en un disco o una cinta, o un pulso de alto o bajo voltaje a través de un circuito.

Bitácora. Operación de registro, diario. Un registro de actividad de la computadora, que se usa con propósitos de estadística, y también de seguridad y recuperación.

Bloqueo. Se refiere al conjunto de técnicas para el manejo de las bases de datos en un entorno multiusuario. El bloque de un archivo impide a los usuarios accesar a un dato, texto o archivo de imagen mientras el usuario que lo "protegio" se encuentra utilizándolo. El bloqueo de un registro prohibe el acceso a un único registro dentro de un archivo o tabla de la Base de datos.

Broadcast. Difundir. Diseminar información a varios receptores simultáneamente. Transmisión simultánea de datos a mas de un destino.

Burst traffic. Tráfico de ráfaga. Un método alternativo para transmisión a alta velocidad en un canal de comunicaciones o computadoras. Implica que dadas ciertas condiciones, el sistema puede enviar una "ráfaga" de datos a mayor velocidad por cierto período de tiempo.

Bus. Canal o ruta común entre dispositivos de hardware, ya sea internamente entre componentes de la computadora o externamente entre estaciones de una red de comunicaciones. Cuando la arquitectura de bus es utilizada en una red, todas las terminales y computadoras están conectadas a una canal común constituido por par trenzado, cable coaxial o fibra óptica. Es una configuración de red que proporciona una instalación de transmisión bidireccional a la cual se "cuelgan" todos los nodos. Un nodo emisor transmite en ambas direcciones a los puntos finales del bus. Todos los nodos en la ruta copian el mensaje y lo dejan pasar.

Chip. Circuito integrado. Los chips tienen aproximadamente de 2 a 12mm de lado y aproximadamente 1mm de espesor. Contienen desde unas pocas decenas hasta varios millones de componentes electrónicos.

Bitácora. Operación de registro, diario. Un registro de actividad de la computadora, que se usa con propósitos de estadística, y también de seguridad y recuperación.

Bloqueo. Se refiere al conjunto de técnicas para el manejo de las bases de datos en un entorno multiusuario. El bloque de un archivo impide a los usuarios accesar a un dato, texto o archivo de imagen mientras el usuario que lo "protegio" se encuentra utilizándolo. El bloqueo de un registro prohibe el acceso a un único registro dentro de un archivo o tabla de la Base de datos.

Broadcast. Difundir. Diseminar información a varios receptores simultáneamente. Transmisión simultánea de datos a mas de un destino.

Burst traffic. Tráfico de ráfaga. Un método alternativo para transmisión a alta velocidad en un canal de comunicaciones o computadoras. Implica que dadas ciertas condiciones, el sistema puede enviar una "ráfaga" de datos a mayor velocidad por cierto período de tiempo.

Bus. Canal o ruta común entre dispositivos de hardware, ya sea internamente entre componentes de la computadora o externamente entre estaciones de una red de comunicaciones. Cuando la arquitectura de bus es utilizada en una red, todas las terminales y computadoras están conectadas a una canal común constituido por par trenzado, cable coaxial o fibra óptica. Es una configuración de red que proporciona una instalación de transmisión bidireccional a la cual se "cuelgan" todos los nodos. Un nodo emisor transmite en ambas direcciones a los puntos finales del bus. Todos los nodos en la ruta copian el mensaje y lo dejan pasar.

Chip. Circuito integrado. Los chips tienen aproximadamente de 2 a 12mm de lado y aproximadamente 1mm de espesor. Contienen desde unas pocas decenas hasta varios millones de componentes electrónicos.

Chipcard y Chipkeys. Tarjetas inteligentes. Son tarjetas plásticas con microprocesador y memoria integrados. La incorporación del microprocesador les permite realizar acciones más elaboradas que si contenido sólo fuera información.

Circuit switching. Conmutación de circuitos. La conexión temporal de dos o más canales de comunicaciones. Los usuarios disponen del pleno uso del circuito hasta que se termina la conexión.

CMIP. Common Management Information Protocol. Protocolo de información para la administración común. Un estándar aprobado por OSI que define las funciones de supervisión y control de una red.

CRC. Cyclic redundancy checksum. Verificador de redundancia ciclico. Campo que se adiciona al frame de datos para determinar la integridad de los mismos. El CRC es verificado por el receptos. Si su propio cálculo de CRC no concuerda con el valor del CRC del frame, el receptor envia una confirmación negativa al emisor.

Dar de baja. Desconectar a un nodo, terminal, o servidor de la red. En el caso de servidor incluye algunas acciones para que finalice su sesión (down en el caso de Netware Novell).

DSU/CSU. (Data Service Unit/Channel Service Unit). Unidad de servicio de datos/unidad de servicio de canal. Es un dispositivo de comunicaciones que conecta una línea interna a un circuito digital externo (Tí,DDS...).El DSU convierte los datos al formato requerido, mientras que el CSU es la terminación de la línea, que proporciona la regeneración de la señal y las pruebas remotas.

Datagrama. datagram. Unidad de mensaje TCP/IP que contiene las direcciones origen y de destino de la internet y los datos.

Debugger. Depurador. Una aplicación que asiste en la depuración de un programa. Proporciona formas de detener un programa o capturar diversos datos del sistema operativo en momentos prescritos.

Echo. Eco. En comunicaciones echo de verificación para determinar el estado correcto de la transmisión de los datos en los cuales los datos recibidos son regresados a el origen para compararse con los datos originalmente transmitidos.

Elemento autorizedor (trustee). Dícese del usuario o grupo al que han sido asignados derechos para accesar en un directorio o archivo. Puede heredar estos derechos si es asignado a otro objeto.

End-to-end session. Conexión lógica en la cual se ha establecido una relación de ruteo por afinidad entre el los nodos origen y destino, cada uno de los cuales puede ser una unidad lógica o un programa de aplicación. Las sesiones end-to-end necesitan ruteo por clave.

Ethernet. Estándar de LAN 802.3 *IEEE* originalmente desarrollado por Xerox, DEC e Intel que utiliza el método de acceso *CSMA/CD* transmite a 10Mbps y puede conectar en total hasta 1024 nodos.

Facsímil. Fax. Los fax exploran un formulario de papel y convierten su imagen en un código para la transmisión por el sistema telefónico. La máquina receptora reconvierte los códigos e imprime un facsímil del original. Un fax está compuesto por un explorador, una impresora y un modem para fax.

FAT. File Allocation Table. Tabla de asignación de archivos. Es un índice de una o más bloques de asignación a disco en los cuales un archivo es localizado. Los elementos de la FAT corresponden a los bloques que conforman un archivo. El primer elemento corresponde al primer bloque del archivo, el segundo al segundo bloque, etc.

FDDI. (Fiber optic Data Distribution Interface). Interfase de distribución de datos mediante fibra óptica. Conjunto de normas de ANSI (American National Standards Institute) para redes de área local con fibra óptica. Se aplica a las dos capas inferiores del modelo OSI y transmite a 100 Mgbps.

Frame Relay. Protocolo de comunicación de paquetes de alta velocidad que proporcionan una transmisión más rápida que X.25. Es más adecuada para la transferencia de datos e imágenes que para transmisión de voz.

Frame. En comunicaciones, un grupo de bits que conforman un bloque elemental de datos para su transmisión por ciertos protocolos.

Front-end. Punto frontal. Computadora que organiza el procesamiento de las comunicaciones en un entorno de computadoras de gran tamaño. Por un lado se conecta a los canales de comunicación y por el otro al mainframe. Transmite y recibe mensajes, ensamble y desemsambla paquetes y también detecta y corrige errores. Algunas veces es sinónimo de controlador de comunicaciones, aunque esto último generalmente no es tan flexible.

Gateway. Supercarretera. Una computadora que conecta dos tipos diferentes de redes de comunicaciones. Realiza la conversión de protocolos de una red a otra.

Halón. El Halón es un químico que asfixia la reacción química del fuego.

Hardware. Se refiere al equipo físico de los equipos de cómputo, periféricos y comunicación. Cuanto más memoria y almacenamiento en disco tiene un sistema informático, más trabajo puede hacer. Cuando más rápidos sean la memoria y los discos, para transmitir datos e instrucciones entre ellos y la CPU, más rápido se hará el trabajo. Un problema de usuario puede ser traducido a un requerimiento de hardware basado en el tamaño de los archivos y las bases de datos que serán

creadas, y el número de usuarios simultáneos en las terminales. El software, por otro lado, es más difícil de especificar. Los programas deben procesar adecuadamente las transacciones de negocios de la organización, e incluso la más pequeña compañía puede tener transacciones complicadas.

Host. Anfitrión. La computadora central o la computadora controladora en en entorno de procesamiento distribuido.

Ingreso de gracia. Se denomina al número de ingresos que un usuario puede realizar con su perfil y pasaporte anterior en caso de que no recordara el actual.

Instanciado. En Programación orientada a objetos, el miembro de una clase. Instanciar es la acción de crear elementos nuevos derivados de una clase, heredando sus atributos y métodos.

INTERNET. Red internacional orientada a la investigación que engloba más de tres redes gubernamentales y académicas en 40 países.

ISDN. (Integrated Services Digital Network) Red Digital de Servicios Integrados. Estándard internacional de telecomunicaciones para la transmisión de voz, video y datos a través de una línea de comunicaciones digitales. Los servicios ISDN se presentan en dos formas : 1. BRI (Basic Rate Interface) Interfase de régimen básico. Proporciona un servicio de 144kbits por segundo, que incluye dos canales "B" de 64kbps para voz, datos y video, y un canal "D" de 16 kbps para información de control 2. PRI (Primary Rate Interface) Interfase de régimen primario. Provee un servicio de 1.54 Mbits por segundo, que incluye 23 canales "B" de 64 Kbps y un canal "D" de 64 Kbps.

IRF. Inhereted Rigths Filter. Filtro de derechos heredados. Máscara que controla cuales derechos pueden heredar los usuarios mediante la revocació de algunos de ellos. Un

IRF revoca los derechos permitidos y afecta a todos los usuarios. Sirve para prevenir la herencia - o flujo - de derechos hacia los directorios del sistema de archivos o contenedores del árbol NDS.

Item. elemento. Una unidad o miembro de un grupo. Data item. elemento de dato, item de dato. Una unidad de datos que se almacena en un campo.

LED. (Light Emitting Diode). Diodo emisor de luz. Una tecnología de exhibición ("display") que utiliza una variedad particular de diodo semiconductor que emite luz cuando está cargado con electricidad. Los LEDs generalmente emiten un resplandor rojo, aunque también pueden generarse otros colores. Los LEDs eran los visores de dígitos en los primeros relojes digitales.

Loopback. Un procedimiento de diagnóstico en el cual un mensaje o señal transmitida se devuelve desde su estación de destino para comparar con los datos originales. Esto puede ser implementado por un circuito especial que causa que la transmisión desde el lado emisor vaya directamente al lado receptor de la misma unidad, sin ir por la línea a otro dispositivo.

Mainframe. Macrocomputadora. Una computadora de gran capacidad. A mediados de los años 60, todas las computadoras eran mainframes (que literalmente significa "bastidor principal"), ya que era el término que se refería al gabinete que contenía la *CPU*. Hay macrocomputadoras de escala pequeña, mediana y grande, manejando desde un grupo a varios miles de terminales en línea. Las macrocomputadoras de gran escala pueden tener centenares de Mbytes de memoria principal y centenares de Gigabytes de almacenamiento en disco. Las macrocomputadoras de mediana y gran escala usan computadoras más pequeñas como procesadores frontales que se conectan directamente a las redes de comunicaciones.

Microcomputadora. Una computadora que usa un microprocesador para su CPU. Es sinónimo de computadora personal.

Minicomputadora. Una computadora de pequeña a mediana escala que funciona como una sola estación de trabajo, o como un sistema multiusuario con hasta varios cientos de terminales. Dado que las microcomputadoras más sofisticadas y las macrocomputadoras menos sofisticadas ofrecen precios y rendimientos en el nivel tradicional de las minicomputadoras, el término está comenzando a tener menos significación. Algunas compañías están reemplazando este término con las designaciones de pequeña, mediana y gran escala.

Modem. MOdulador-DEModulador. Un dispositivo que adapta una terminal o computadora a la línea telefónica. Convierte los pulsos digitales de la computadora a frecuencias dentro del rango de audio del teléfono y los vuelve a convertir en pulsos en el lado receptor.

Multipoint. Relacionado con la comunicación entre más de dos estaciones sobre una linea sencilla de comunicación.

Multipoint line. Línea multipunto. En comunicaciones, una sola línea que interconecta tres o más dispositivos.

Multipoint line. Una línea de telecomunicación o circuito que conecta dos o más estaciones. Contrasta con la línea point-to-point.

Multipoint polling. Se refiere a utilizan la ténica de polling entre más de dos estaciones.

NLM. Netware Loadable Module. Módulo ejecutable de Netware. Son programas considerados como una extensión del sistema operativo Netware Novell que realizan funciones especializadas.

Nodo. En comunicaciones, un punto de conexión en una red (una terminal o una computadora)

Octeto. Un byte compuesto de ocho dígitos binarios.

Packet switching. Conmutación de paquetes. Una técnica para manejar altos volúmenes de tráfico en una red descomponiendo los mensajes en paquetes de longitud fija que son transmitidos a su destino a través de la ruta más oportuna. Todos los paquetes en un solo mensaje pueden no viajar por la misma ruta (ruta dinámica). La computadora de destino recompone los paquetes en su secuencia adecuada. Las redes de conmutación por paquetes además proveen servicios de valor agregado, como conversión de protocolo y correo electrónico.

Patching. Dicese de la acción de conectar dos ubicaciones localizadas en un patch a través de un puente físico.

PBX. (Private Branch eXchange). Sistema de conmutación telefónica que interconecta una línea con una red telefónica pública. Un PBX puede realizar varias funciones de administración telefónica, tal como direccionamiento de menor costo para llamadas externas, redireccionamiento de llamadas, llamadas de conferencia y contabilidad de llamadas. Los PBX modernos utilizan métodos digitales de conmutación y a menudo pueden manejar terminaels y teléfonos digitales, así como las líneas analógicas.

Peer-to-peer communications. Comunicaciones par a par. Comunicaciones en las que ambos extremos tienen la misma responsabilidad para iniciar la sesión.

PERT y CPM . Las dos principales técnicas de análisis de proyectos. PERT o Program Evaluation and Review Technique : técnica de evaluación y revisión de programas; y CPM o Critical Path Method : método de ruta crítica. Ambos sistemas fueron desarrollados de manera independiente hacia 1957- 1958. El primero fue creado por la Oficina de proyectos especiales de la armada estadounidense para coordinar a más de 3000 contratiscas y organismos que trabajaron en el programa Polaris (un submarino provisto de misiles nucleares). El sistema CPM fue creado por la empresa Du Pont a fin de facilitar el control de sus complejos proyectos industriales. Ambos sistemas se parecen en lo esencial, pero pueden dar resultados excelentes si se aplican en situaciones un poco distintas. El método de la ruta crítica se presta más a procesos repetitivos en los cuales las tareas tienen una duración fija y se conoce la fecha de terminación; en cambio, la técnica de evaluación y revisión de programas maneja de manera óptima procesos no repetitivos en los cuales apenas si pueden estimarse aproximadamente la duración y la fecha de terminación de las tareas.

Hay cuatro requisitos para traducir un proyecto en una red de PERT o CPM :

1. La actividad ha de ser dividida en tareas individuales. Estas se introducirán entonces en la red en forma de acontecimientos y actividades. Los acontecimientos (eventos) generalmente se indican dentro de círculos en la gráfica; representa las partes de las tareas que deben efectuarse en momentos específicos. Las actividades representan el tiempo o recursos requeridos para pasar de un evento a otro. Por lo regular se denotan con flechas en la gráfica.

2. Los eventos y actividades se ponene en la gráfica de una manera secuencial, lógica e integrada. Así, cada actividad está precedida y acompañada de los eventos apropiados; ninguna actividad comenzará antes que haya sido concluido el evento o eventos que la preceden.

3. La duración requerida en cada actividad se estima y se anota en la red. En el método de ruta crítica (CPM), se establece una sola estimación del tiempo para cada actividad. En la técnica de evaluación y revisión de programas (PERT), a cada actividad se le pueden asignar cuatro estimaciones de tiempo: una estimación "optimista" del tiempo que tardará la actividad en condiciones ideales; una estimación

"muy probable" del tiempo normal que tardaría dicha actividad; una estimación "pesimista" que tiene en cuenta la posibilidad de que todo salga mal; y una estimación del tiempo "esperado" que se basa en un análisis probabilistico de las otras tres estimaciones.

4. Determinar la ruta crítica de la red, o el camino más largo a través de la red en términos de tiempo. La importancia de la ruta crítica estriba en que determina la duración total del tiempo, o fecha de terminación del proyecto entero.

Point-to-point line. Una línea de telecomunicación conmutada o no conmutada que conecta una estación remota a una computadora. Contrasta con las líneas multipunto.

Polling. Encuesta, sondeo, interrogación, escrutinio para una línea multipunto. Una técnica de comunicaciones que determina cuándo una terminal está lista para enviar datos. La computadora continuamente interroga a todas sus terminales conectadas, en una secuencia cíclica. Si una terminal tiene datos para enviar, ésta devuelve un reconocimiento y la transmisión comienza.

Programas de inicio (login scripts). Pequeños archivos que contienen comandos que inicializan las variables de ambiente, correlacionan las unidades de red y controlan la ejecución de los programas de los usuarios.

Rack. bastidor. Armazón o gabinete dentro del cual se montan los componentes.

Stand-alone. Dícese de la computadora que no está conectada a ninguna red o a otra computadora, es decir, que se encuentra sola.

Sintáxis. Reglas que gobiernan la estructura de una sentencia en un lenguaje. Especifica la forma en que las palabras y símbolos se unen para formar una frase.

SNA. (Systems Network Architecture). Arquitectura de redes de sistemas. Principal estrategia de IBM para el uso de redes, introducida en 1974. La SNA está compuesta por una variedad de productos de hardware y software que interactúan todos entre sí.

SNMP. Simple Network management Protocol. Protocolo simple de administración de red. Protocolo utilizado para reunir la información acerca de la actividad en una red TCP/IP para propósitos de supervisión y estadísticos.

Software. Instrucciones que conforman los programas. Una serie de instrucciones que realizan una tarea en particular se llama programa o programa de software. Las dos categorías principales son software de sistemas de aplicaciones.

Switch. Conmutador. Dispositivo mecánico o electrónico que comanda el flujo de señales eléctricas u ópticas.

TCP/IP. (Transmission Control Protocol/Internet Protocol). Protocolo de control de transmisiones/protocolo. Internet. Conjunto de protocolos de comunicaciones desarrollado por la Defense Advanced Research Projects Agency (DARPA - Agencia de proyectos de investigación avanzada de defensa) para intercomunicar sistemas diferentes. Se ejecuta en un gran número de computadoras VAX y basadas en UNIX, y es utilizado por muchos fabricantes de hardware, desde los de computadoras personales hasta los de macrocomputadoras. Es empleado por numerosas corporaciones y por casi todas las universidades y organizaciones federales de los Estados Unidos.

Terminador. Componente de hardware que se conecta al último dispositivo periférico de una serie o al último nodo de una red.

Time Division Multiplexing (TDM). Multiplexado por división de tiempo. Técnica que combina varias señales de baja velocidad, formando una transmisión de alta velocidad. División de una transmisión en dos o más canales, para distribuir el canal común en diferentes canales de información.

Transciever. emisor-receptor. Transmisor y receptor de señales analógicas o digitales que vienen en diversos formatos. Cualquier terminal que puede transmitir y recibir tráfico.

Transponder. Receptor y transmisor de un satélite de comunicaciones. El transponder recibe una señal de microondas transmitida desde la tierra ("uplink" - enlace ascendente), la amplifica y la retransmite de regreso a la tierra en una frecuencia diferente ("down link" - enlace descendente). Hay varios transponders en un satélite de comunicaciones.

Trigger. Elemento activo de una base de datos que se "dispara" cuando se presenta alguna condición especificada previamente por el diseñador de la base de datos.

Usuario ADMIN. Es el primer usuario creado cuando se instala Netware Novell 4.x en el servidor. Es la cuenta que por omisión recibe inicialmente todos los derechos sobre NDs y sobre el sistema de archivos.

Value-added network.red con valor agregado. Una red de comunicaciones que proporciona servicios más allá de una transmisión normal, tales como la detección y corrección automática de errores, la conversión de protocolos y el almacenamiento y despacho de mensajes.

Virtual circuit. Circuito virtual. El trayecto resultante que se crea ente dos dispositivos comunicados entre sí en un sistema de conmutación por paquetes. Un mensaje de NY a LA (New York a Los Angeles) puede realmente comenzar en New York ir a través de Atlante, St. Louis, Denver y Phoenix antes de concluir en Los Angeles.

BIBLIOGRAFIA

[BAR85] Bartee Thomas C.
Data Communications, Networks and Systems
"Computer and Communications Security" by Stephen T. Walker
Howard W. Sams & Co.
U.S.A. 1985

[BEA90] Beauchamp K.G.
Computer Communications. Aspects of Information Technology
Segunda Edición
Chapman and Hall
Gran Bretaña 1990

[COB92] Cobb Stephen
The Stephen Cobb complete book of PC and LAN Security
Windcrest Books. McGraw-Hill Books
U.S.A. 1992

[GAR91] Garfinkel Simson, Spafford Gene
Practical Unix Security
Computer Security
O'Reilly & Associates, Inc.
U.S.A. 1992

[HEN90] Henshall John, Shaw Sandy
OSI Explained. End-to-end computer communication standards
Segunda Edición
Ellis Horwood Limited
Gran Bretaña 1990

[MAR89] Martin James, Kavangugh Kathleen
Local Area Networks. Architectures and Implementations
Prentice Hall, Englewood Cliffs
U.S.A. 1989

[PER92] Perlman Radia
Interconnections. Bridges and Routers
Addison-Wesley. Addison Wesley Professional Computing Series
U.S.A. 1992

[ROS82] Rosner Roy D.
Distribuited Telecommunications Networks. Via Satellites and Packet Switching.
"Security, Privacy, and Protection in Distribuited Communications Systems"
Lifetime Learning Publications
U.S.A. 1982

[SCH88] Schweitzer James A.
Protecting Information on Local Area Networks
Butterworth Publishers
U.S.A. 1988

[STA88] Stallings William
Local Networks
Tercera Edición
Macmillan Publishing
U.S.A. 1988

[STA90] Stallings William
Handbook of Computer Communications Standards
Volume I. The Open Systems (OSI) Model and OSI-Related Standards
Segunda Edición
Macmillan Computer Publishing
U.S.A. 1990

[TAN89] Tanenbaum Andrew
Computer Networks
Segunda Edición
Prentice Hall International
U.S.A. 1989

[TER92] Terplan Kornel
Communication networks management
Segunda Edición
Prentice Hall. Prentice Hall Computer Communication Series
U.S.A. 1992

[WAT91] Waters Gill
Computer Communication Networks. Essex Series in Telecommunication and Information Systems
McGraw-Hill
Gran Bretaña 1991

Davies D. Watts, Price W.L.
Security for computer networks. An Introduction to Data Security in Teleprocessing and Electronic Funds transfer
John Wiley & Sons
Gran Bretaña 1984

HEMEROGRAFIA

[MAH94] Mahony, Donald O'
Securiy considerations in a Network Management Enviroment
IEEE Network, The Magazine of computer communications
Mayo-Junio 1994. Volúmen 8. No. 3
ISSN 0890-8044
New York U.S.A.

Mukherjee Biswanath, Herbelein L. Todd, otros
Network Intrusion Detection
IEEE Network, The Magazine of computer communications
Mayo-Junio 1994. Volúmen 8. No. 3
ISSN 0890-8044
New York U.S.A.

Mirhakkak M.
A Distribuited System Security Arquitecture : Applying the Transport Layes Security Protocol
Computer Communication Review. ACM Sicomm.
Association for Computing Moderny. ACM Press
Octubre 1993. Volumen 23, No. 5
ISSN 0146-4833
New York U.S.A.

Katsavos P., Varadharajan V.
Security Protocol for Frame Relay
Computer Communication Review. ACM Sicomm.
Association for Computing Moderny. ACM Press
Octubre 1993. Volumen 23, No. 5
ISSN 0146-4833
New York U.S.A.

Kumar B., Crowcroft J.
Integrating Security in Inter-Domain Routing Protocols
Computer Communication Review. ACM Sicomm.
Association for Computing Moderny. ACM Press
Octubre 1993. Volumen 23, No. 5
ISSN 0146-4833
New York U.S.A.

[ZNA94] Znaty S., Sclavos J.
Annotated Bibliografy on Network Management
Computer Communication Review. ACM Sicomm.
Association for Computing Moderny. ACM Press
Enero 1994. Volumen 24, No. 1
ISSN 0146-4833
New York U.S.A.

Hadj Sadok D.F., Kelner J.
Privacy Enhaced Mail Design and Implementation
Computer Communication Review. ACM Sicomm.
Association for Computing Moderny. ACM Press
Julio 1994. Volumen 24, No. 3
ISSN 0146-4833
New York U.S.A.

[ZNA94-2]Znaty S., Sclavos J.
Network Management Viewpoints: A New way of encompassing the Network Management complexity
Computer Communication Review. ACM Sicomm.
Association for Computing Moderny. ACM Press
Julio 1994. Volumen 24, No. 3
ISSN 0146-4833
New York U.S.A.

Muftic S.
Security arquitecture for ODP Systems. Final results of the CECCOST-11 Ter "Security " Project
Computer Networks and ISDN Systems. The Internal Journal of Computer and Telecommunications Networking.
Agosto 1994. volumen 26 No. 11
ISDN 0169-7552
Holanda

Katsavos P., Varadharajan V.
A secure Frame Relay Service
Computer Networks and ISDN Systems. The Internal Journal of Computer and Telecommunications Networking.
Septiembre 1994. volumen 26 No. 12
ISDN 0169-7552
Holanda

[NOV94] Jarocki Stanley, Kelch Michael, otros
Building and Auditing a Trusted Network Environment with Netware 4
Network Support Encyclopedia
Application Note
Novell Inc.
Abril 1994

Lee Rich, Israel Jay, otros
Understanding the Role of Identification and Authentication in Netware 4
Network Support Encyclopedia
Application Note
Novell Inc.
Octubre 1994

[IBM95]IBM Inc.
Ayuda en línea del sistema IBM AS400
Modelo 320.
BANCOMEXT, México 1995