Configuración y administración de una red multipunto con un firewall server

Autor: Gisela García Carrillo

Tesina presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

LICENCIATURA EN SISTEMAS COMPUTARIZADOS

" CONFIGURACIÓN Y ADMINISTRACIÓN DE UNA RED MULTIPUNTO CON UN FIREWALL SERVER "

T E S I N A

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA:

GISELA GARCÍA CARRILLO

ASESOR:

ING. Y M.A SERGIO FRANCISCO BARRAZA IBARRA

CLAVE 16PSU0014Q
ACUERDO 952006

MORELIA, MICH., DICIEMBRE 2000

DEDICATORIAS

A DIOS

Por brindarme la posibilidad de ser parte de este mundo y regalarme sus Bendiciones.....

A MIS PADRES

Con todo mi amor, por los innumerables esfuerzos que han hecho para mi formación, y cuyo ejemplo va marcando la senda de mi camino por la vida.

A MIS HERMANOS

Por su apoyo y entereza en cada minuto de mi vida

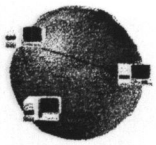
A MIS AMIGOS

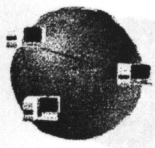
Por su apoyo y cariño incondicional.....

A MI ASESOR

Por su orientación y dedicación en el desarrollo del presente

INDICE





INTRODUCCIÓN

Las redes hoy en día han producido un impacto dentro de nuestra sociedad, siendo esta una herramienta revolucionaria ya que ha multiplicado la productividad y la eficiencia del trabajo tanto para las empresas como para los usuarios individuales. Teniendo una finalidad concreta que es la de transferir e intercambiar datos entre ordenadores.

El presente surge de la inquietud de documentar la manera de configurar y administrar una red multìpunto conectada a Internet por medio de un Firewall Server el cual es actualmente uno de los Hardware mas empleados en Redes.

Este trabajo contiene 10 apartados, en los cuales presento una recopilación de información referente a redes siendo indispensable para la comprensión clara del caso practico que desarrollo a continuación.

En el capitulo dos describo los Objetivos Generales que sirven como marco de referencia contextual, así como los Objetivos Específicos que he planteado al principio, orientados a facilitar a cualquier lector con conocimientos básicos para implementar el caso practico que fue abordado como ejemplo en este trabajo.

En el capitulo tres hago referencia a los Antecedentes de Redes e Internet tanto su historia como la evolución de las mismas ya que son fundamentales para la comprensión de estas plataformas de trabajo.

En el capitulo cuatro se cito los Beneficios de una Red y la Conectividad en el cual se puede ver la fiabilidad de tener una Red que permita compartir dispositivos, software, etc.

En el rubro cinco se describen los diferentes tipos de redes así como la tecnología de transmisión para comprender como se transmite la información por una Red.

En el capitulo seis se encuentran las Topologías en las que se puede configurar una red resaltado con diagramas para una mayor conceptualizaciòn de las mismas.

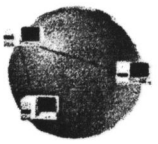
En el apartado siete describo los componentes de una Red tomando en cuenta el medio físico, Hardware, Protocolos y sistemas Operativos, con el fin de dar a conocer la tecnología que integra una red.

En el capitulo Ocho se hace referencia a las Tecnologías de acceso que son usadas para conectar los dispositivos de red al cable físico.

En el penúltimo capitulo contiene la Arquitectura de Redes basándose en las siete capas del OSI.

En el capitulo diez detallo la Instalación y configuración de un caso practico usando una red multìpunto con un firewall que permite la integración de todas los elementos vistos en cada uno de los apartados que integran el presente trabajo.

Por ultimo se encuentran las conclusiones sobre este trabajo de investigación así como la bibliografía empleada para la realización del mismo.



CAPITULO 2

OBJETIVOS DE LA INVESTIGACIÓN

2. - OBJETIVO GENERAL:

Diseñar, Configurar e implantar una red LAN para tener un mejor control y desempeño referente a la transferencia, compartición de software y seguridad de la información.

2.1 OBJETIVOS ESPECIFICOS

- Describir el proceso de Comunicación de datos en una red conectada a Internet.
- Mostrar las diferentes topologías de red existentes en el mercado.
- Detallar los diversos Protocolos más utilizados en redes locales e Internet.
- Mostrar la manera de configurar una red local Multipunto.
- Describir la manera de instalar y configurar Firewall Server.
- Citar los diferentes Sistemas Operativos de red.
- Detallar los beneficios de una red y la conectividad.
- Resaltar los componentes en los que esta formada una Red.

CAPITULO 3

ANTECEDENTES DE REDES E INTERNET

Los tres siglos pasados han sido dominados por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de la información. Entre otros desarrollos, hemos sido testigos de la instalación de redes telefónicas en todo el mundo, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedente de la industria de los ordenadores, así como la puesta en órbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años del siglo XX y comienzos del siglo XXI se ha dado una rápida convergencia de estas áreas; y también las diferencias entre la captura, transporte, almacenamiento y procesamiento de información están desapareciendo con rapidez. A medida que crece nuestra habilidad para recolectar, procesar y distribuir información la demanda de sofisticados procesamientos de información crece todavía con mayor rapidez.

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Para esto se utilizaron líneas telefónicas, ya que éstas permitían un traslado rápido y económico de los datos.

Se utilizaron procedimientos y protocolos ya existentes para establecer la comunicación y se incorporaron moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un módem.

Posteriormente, se introdujeron equipos de respuesta automática, que hicieron posible el uso de redes telefónicas públicas conmutadas para realizar las conexiones entre las terminales y la computadora.

Durante los años 60 las necesidades de teleproceso dieron un enfoque de redes privadas compuesto de líneas (leased lines) y concentradores locales o remotos que utilizan una topología de estrella.

A principios de los años 70 surgieron las primeras redes de transmisión de datos destinadas exclusivamente a este propósito como respuesta al aumento de la demanda del acceso a redes a través de terminales para poder satisfacer las necesidades de funcionalidad, flexibilidad y economía.

Se comenzaron a considerar las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, ya que dependiendo del grado de similitud entre computadoras es posible permitir que compartan recursos en mayor o menor grado.

La primera red comercial fue la *TransCanada Telephone System´s Dataroute*, a la que posteriormente siguió el *Digital Data System* de AT&T. Estas dos redes, para beneficio de sus usuarios, redujeron el costo y aumentaron la flexibilidad y funcionalidad.

El concepto de redes públicas de datos emergió simultáneamente. Algunas razones para favorecer el desarrollo de estas es que el enfoque de redes privadas es muchas veces insuficiente para satisfacer las necesidades de comunicación de un usuario dado.

La falta de interconectabilidad entre redes privadas y la demanda potencial de información entre ellas en un futuro cercano favorecen el desarrollo de las redes públicas.

La historia de INTERNET se remonta al año de 1969 cuando fue creada por una necesidad del Departamento de Defensa de los Estados Unidos de Norte América, cuyo proyecto fue realizado por la Agencia de Proyectos Avanzados de Investigación en Defensa (DARPANET). Su propósito principal era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para ligar redes de transmisión de paquetes de diferentes tipos capaces de resistir las condiciones de operación más difíciles y continuar funcionando aún con la pérdida de la parte de una red; por ejemplo en caso de guerra.

Estas investigaciones dieron como resultado el protocolo TCP/IP (Transmisión de control Protocol/Internet Protocol), un sistema de comunicaciones muy sólido y robusto bajo el cual se integran todas las redes que conforman lo que se conoce actualmente como INTERNET, por lo que a DARPANET se le conoce como la madre de Internet.

Durante el desarrollo del protocolo se incrementó notablemente el número de redes locales de agencias gubernamentales y posteriormente, cuando cuatro universidades de los Estados Unidos lograron enlazarse entre sí, dieron origen a la RED de REDES más grande del mundo.

A partir de la década de los 80's se forman dos nuevos bloques: ARPANET, ya conocido y MINET que es la red militar con información no clasificada; de esta manera las funciones militares se separaron, permitiendo así que todo aquel que lo requiriera sin importar el país que lo solicitara siempre y cuando fuera para fines académicos y de investigación, pudiera tener acceso a la red (claro está, pagando sus gastos de conexión) permitiendo de ésta manera una comunicación continua.

Asimismo otras redes experimentales que utilizaban paquetes de radio y satélites se conectaron a Arpanet utilizando la tecnología interconectada por Darpa. En un principio ésta interconexión de redes experimentales y producción se denominó INTERNET DARPA, posteriormente adoptó el nombre de INTERNET.

El grupo de mayor autoridad sobre el desarrollo de la red es la Internet Society, creada en 1992 y formada por miembros voluntarios, cuyo propósito principal es promover el intercambio de información global a través de la tecnología de INTERNET; es decir, éste grupo tiene la responsabilidad de la administración técnica y dirección de Internet, aunque no es el único.

Existen además otros tres grupos:

1. El Internet Architecture Board (que toma las decisiones de los estándares de comunicación entre las diferentes plataformas, para que puedan interactuar máquinas de distintos fabricantes sin problemas y a la vez siendo responsable de asignar las direcciones y otros recursos).

2. Network Information Center (NIC) administrado por el Departamento de Defensa de U.S.A., encargándose de autorizar estas asignaciones.

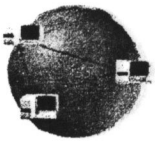
3. Internet Egineering Task Force (IETF) en el cual los usuarios de Internet expresan sus opiniones sobre cómo se deben implementar soluciones para problemas operacionales y cómo deben cooperar las redes para lograrlo.

INTERNET es la suma de interredes conectadas entre si sin importar el lugar geográfico en que se encuentren.

Es importante mencionar que una RED se forma cuando dos o más computadoras se conectan entre sí permitiendo el intercambio de información, en donde todas pueden utilizar simultáneamente los archivos y programas que tiene cada una por separado; ahora bien, en una de las computadoras de la RED, se concentran los principales archivos convirtiéndose ésta en una computadora central a la que se le denomina SERVIDOR, y al que se le enlazan las demás computadoras de la RED. Este SERVIDOR, a su vez se puede conectar a otro de cualquier otra RED formando así redes e interredes.

INTERNET, es el resultado de la gran disposición de los usuarios para compartir información de toda clase con las personas que la requieran, convirtiéndose en un medio de comunicación inmediato, accesible a los demás, sin condiciones ni permisos gubernamentales, utilizando sólo una computadora pudiendo ser del tipo (PC) con un mínimo en sus especificaciones con procesador486 , 133 mhz, 8 Mb en memoria RAM, monitor VGA o SVGA color, mouse, programa de Windows 3.1 cuando menos y fax módem.

O bien para poder funcionar óptimamente dentro de los requerimientos actuales; con una PC Pentium MMX, a 200 Mhz, 32 Mb en memoria RAM, Disco duro de 2 Ghz (como mínimo), Fax módem de 56 Kb. Windows 95 ó 98 (Con aplicaciones para Internet), Mouse, Tarjeta de Sonido y CD rom.



CAPITULO 4

BENEFICIOS DE UNA RED Y LA CONECTIVIDAD

4.1 VENTAJAS DE LA RED

Las redes de ordenadores presentan varias ventajas importantes de cara a los usuarios ya sea a empresas o a particulares.

1. Las organizaciones modernas suelen estar bastante dispersas y a veces incluyen empresas distribuidas en varios puntos de un país o extendidas por todo el mundo. Muchos de los ordenadores y terminales situados en los distintos lugares necesitan intercambiar datos e información, y con frecuencia ese intercambio ha de ser diario. Mediante una red puede conseguirse que todos esos ordenadores se intercambien información y que los programas y datos necesarios estén al alcance de todos los miembros de la organización.

2. La interconexión de ordenadores permite que varias máquinas compartan los mismos recursos. Así por ejemplo, si un ordenador se satura por estar sometido a una carga de trabajo excesiva, podemos utilizar la red para que otro ordenador se ocupe de ese trabajo, consiguiendo un mejor aprovechamiento de los recursos.

3. Las redes pueden resolver también un problema de especial importancia; la tolerancia a fallos. En caso que un ordenador falle, otro puede asumir sus funciones y su carga de trabajo, algo de particular importancia en los sistemas de control tráfico aéreo. Si un ordenador falla, los ordenadores de reserva entrarán en funcionamiento rápidamente y tomarán el mando de todas las operaciones de control, sin que en ningún momento llegue a existir peligro para los pasajeros.

4. El empleo de redes confiere una gran flexibilidad a los entornos laborales. Los empleados pueden trabajar desde su casa, usando terminales conectadas con el ordenador de la oficina. Hoy en día es frecuente ver personas que viajan con su ordenador portátil y los conectan a la red de su empresa a través de la línea telefónica.

La sociedad de nuestros días emplea la información para reducir los costos de producción de los bienes que consumimos y en general, para mejorar nuestra calidad de vida. Todo esto gracias a los sistemas de comunicaciones residentes en ordenadores esparcidos por todo el mundo.

4.2 BENEFICIOS DE CONECTIVIDAD

Los beneficios cotidianos que obtienen los usuarios de una red son:

Hardware Compartido

Los Usuarios de red pueden compartir muchos dispositivos de hardware, como impresoras, CDROM y espacio en disco entre otros. Esto implica el ahorro en la compra de periféricos costosos.

Aumento en la Productividad

Las redes hacen que la información crítica esté disponible de inmediato para muchos usuarios, lo cual significa que los individuos no necesitan ir de un lugar a otro para poder compartir los archivos ó copiarlos en discos flexibles para que varias PC tengan acceso.

Aumento en la Precisión

Puesto que la información compartida puede almacenarse en una sola ubicación, se requiere una menor introducción de datos. Por lo tanto existen menos probabilidades de error humano.

Soporte más fácil

En un entorno de red, es más fácil dar soporte a programas de aplicación y sistemas operativos comunes.

Comunicación Extendida.

La conectividad permite a los usuarios de computadoras comunicarse con otros, tanto dentro como fuera de la empresa. La compañía se beneficia porque pueden responder de manera más oportuna a las necesidades internas y externas.

Recursos de Investigación

Cuando están conectados a redes fuera de la empresa (Internet),los usuarios pueden tener acceso a mas información que nunca. Esto proporciona la oportunidad para tomar mejores decisiones con base en un cuerpo de información más amplio.

El resultado final de tener una conectividad óptima repercute en el retorno rápido de la inversión.

CAPITULO 5

REDES

5.1 DEFINICIÒN DE COMPUTADORA

Un Ordenador es un conjunto de circuitos electrónicos comprimidos en una pastilla de silicio (llamada Chip), siendo su función fundamental la de encausar las señales electromagnéticas de un dispositivo a otro.

El ordenador es en realidad el MICROPROCESADOR, o sea un conmutador, es el cerebro y razón de ser del ente denominado computadora. Todo lo demás que le rodea y se le es conectado no son más que dispositivos mediante los cuales el cerebro se alimenta de energía e interactua con el medio ambiente y por lo tanto con nosotros los usuarios.

5.2 ELEMENTOS DE LA COMUNICACIÒN

Es el proceso que permite el flujo de la información entre un emisor y uno o más receptores.

Todo sistema de comunicación consta Básicamente de los siguientes tres elementos:

- Emisor
- Medio
- Receptor

Tanto el emisor como el Receptor pueden ser cualquier dispositivo mecánico, eléctrico o electrónico, mientras que el medio requiere que la señal original se convierta, antes y después de ser trasmitida.

Por lo general, la señal original que contiene el mensaje no es apta para ser transmitida directamente por el medio de comunicación, así que el emisor se encarga de convertir dicha señal en una forma que sea adecuada y el receptor realiza la operación inversa al convertir esta señal modificada a la forma original. Idealmente, este proceso de conversión, transmisión, recepción y reconversión debe de producir una señal que es idéntica a la original pero siempre se genera algún cambio que en ocasiones puede llegar a modificar tanto la señal original que sea irreconocible.

5.3 DEFINICIÒN DE REDES

Las redes de computadoras, por el solo hecho de estar interconectadas a través de un medio físico no constituyen propiamente un sistema de comunicación completo. Para esto, es necesario contar con programas de aplicación y bases de datos para compartir entre ellas.

Es la conexión de varios ordenadores a través de un cableado especial para compartir datos. Las redes se pueden conectar mediante diferentes topologías, puede utilizar diferentes tipos de cables(incluso líneas telefónicas), mediante satélites, inalámbricas, con fibra óptica etc. Pueden compartir equipos periféricos, utilizar diferentes sistemas operativos y protocolos.

No existe una taxonomía generalmente aceptada dentro de la cuál quepan todas las redes de computadoras. En términos generales hay dos tipos de tecnología de transmisión.

. Redes de Difusión.
· Redes de punto.

5.3.1 Redes de difusión

Ésta tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los paquetes que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige.

Al recibir el paquete, la máquina verifica el campo de dirección, si el paquete esta dirigido a ella, lo procesa; si esta dirigido a otra máquina lo ignora.

Los sistemas de difusión generalmente ofrecen también la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama difusión (broadcasting). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo que se conoce como multidifusión.

5.3.2 Redes de punto a punto

Consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino un paquete en este tipo de red puede tener que visitar una o más máquinas intermedias.

A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo son muy importantes en estas redes.

5.4 REDES DE ÀREA LOCAL(LAN – Local Area Network)

Las redes de área local son redes de propiedad privada dentro de un solo edificio de hasta unos cuantos kilómetros de extensión. Es un sistema de comunicación entre computadoras, con la característica de que la distancia entre las computadoras debe ser pequeña. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir los recursos (impresoras, etc.) e intercambiar información. Las LAN se distinguen de otro tipo de redes por las siguientes tres características:

- Tamaño
- Tecnología de transmisión.
- Topología.

Las LAN están restringidas en tamaño, las computadoras se distribuyen dentro de la LAN para obtener mayor velocidad en las comunicaciones dentro de un edificio o un conjunto de edificios, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano.

Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos y también simplifica la administración de la red.

Las LAN a menudo utilizan una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas. Las LAN tradicionales operan a velocidades de 10 a 100 MBPS, tiene bajo retardo (décimas de microsegundos) y experimentan muy pocos errores. Las LAN nuevas pueden operar a velocidades cercanas a los cientos de megabits/seg.

Las LAN de transmisión pueden tener diversas topologías. La topología o la forma de conexión de la red, depende de algunos aspectos como la distancia entre las computadoras y el medio de comunicación entre ellas ya que éste determina la velocidad del sistema. Básicamente existen tres topologías de red:

- Estrella (Star)
- Canal (Bus)
- Anillo (Ring)

Los tres tipos de conexión mencionados son los principales para comunicar una serie de computadoras de la misma familia. En una red de bus (cable lineal), en cualquier instante una computadora es la máquina maestra y puede transmitir; se pide a otras máquinas que se abstengan de enviar mensajes. Es necesario un mecanismo de arbitraje para resolver conflictos cuando dos o más máquinas quieren transmitir mensajes simultáneamente, este mecanismo puede ser centralizado o distribuido.

La ETHERNET en una red de transmisión basada en bus con control de operación descentralizado a 10 o 100 Mbps.

Las computadoras de una Ethernet pueden transmitir cuando quieran; si dos o más paquetes chocan, cada computadora sólo espera un tiempo al azar para volver a mandar la información.

Otro tipo de difusión es el anillo, en éste cada bit se propaga por sí mismo sin esperar al resto del paquete. Típicamente cada bit recorre el anillo entero en el tiempo que toma transmitir unos pocos bits, a veces antes de que el paquete completo se haya transmitido.

Como en todos los sistemas de difusión, se necesitan reglas para arbitrar el acceso simultáneo al anillo.

Las redes de difusión se pueden dividir también en estáticas y dinámicas, dependiendo de cómo se asigne el canal. Una asignación estática típica divide el tiempo en intervalos discretos y ejecuta un algoritmo de asignación cíclica, permitiendo a cada máquina transmitir únicamente cuando le llega su turno. La asignación estática desperdicia la capacidad del canal cuando una máquina no tiene nada que decir durante su segmento asignado, por lo que muchos sistemas intentan asignar el canal dinámicamente (por demanda).

Los métodos de asignación dinámica para un canal común son centralizados o descentralizados. En un método de asignación de canal centralizado hay una sola entidad, la cuál determina quién será el siguiente. En el método de asignación de canal descentralizado no hay una entidad central; cada máquina debe decidir por sí misma si transmite o no.

Otro tipo importante de LAN se construye con líneas de punto a punto. Las líneas individuales conectan una máquina específica a otra.

5.5 REDES DE ÀREA METROPOLITANA(MAN - Metropolitan Area Network)

Una MAN es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar una serie de oficinas cercanas o en una ciudad, puede ser pública o privada.

Una MAN puede manejar datos y voz, e incluso podría estar relacionada con una red de televisión por cable local. Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Como no tiene que conmutar, el diseño se simplifica.

La principal razón para distinguir las MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este se llama DQDB (bus dual de cola distribuida). El DQDB consiste en dos buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras. Cada bus tiene una cabeza terminal (head-end), un dispositivo que inicia la actividad de transmisión.

El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior, él trafico hacia la izquierda usa el bus inferior.

Un aspecto clave de las MAN es que hay un medio de difusión al cuál se conectan todas las computadoras. Esto simplifica mucho el diseño comparado con otros tipos de redes.

5.6 RED DE ÀREA AMPLIA (WAM – Wide Area Network)

Una WAN se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas máquinas se llaman Hosts. Los Hosts están conectados por una subred de comunicación.

El trabajo de una subred es conducir mensajes de un Host a otro. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (Hosts), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos o canales) mueven los bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos(enrutadores).

CAPITULO 6

TOPOLOGÌAS

La configuración de una red suele conocerse como topología de la misma. La topología, es la forma(conectividad física) de la red. A la hora de establecer la topología de una red, el diseñador ha de plantearse tres objetivos principales:

1.- Proporcionar la máxima fiabilidad posible, para garantizar la recepción correcta de todo el tráfico.

2.- Encaminar él tráfico entre el transmisor y el receptor a través del camino más económico dentro de la red(aunque, si se considera, más importante otros factores, como la fiabilidad, este camino de costo mínimo puede no ser el mas conveniente).

3.- Proporcionar al usuario final un tiempo de respuesta óptimo y un caudal eficaz máximo.

El segundo objetivo a cumplir a la hora de establecer una topología para la red consiste en proporcionar a los procesos de aplicación que residen en el transmisor o emisor el camino más económico posible. Para ello es preciso:

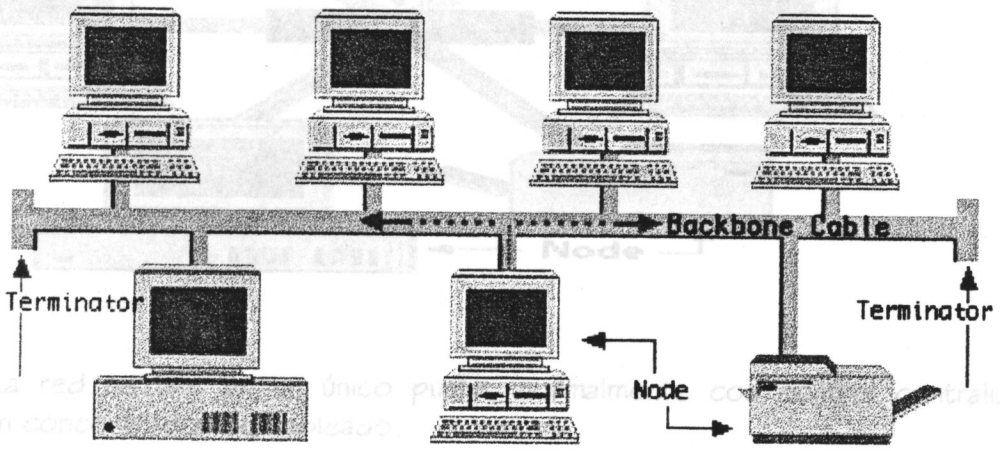
1.- Minimizar la longitud real del canal que une los componentes, lo cual suele implicar el encaminamiento del tráfico a través del menor número posible de componentes intermedios.

2.- Proporcionar el canal más económico para cada actividad concreta; por ejemplo, transmitir los datos de baja prioridad a través de un enlace de baja velocidad por línea telefónica normal, lo cual es mas barato que transmitir esos mismos datos a través de un canal vía satélite de alta velocidad.

El tercer objetivo es obtener un tiempo de respuesta mínimo y un caudal eficaz lo mas elevado posible. Para reducir al mínimo el tiempo de respuesta hay que acortar el retardo entre el transmisor y el receptor de los datos de un ETD (equipo terminal de datos) a otro.

6.1 TOPOLOGÌA DE BUS

Este tipo de topología es muy frecuente en redes de área local (LAN), su importancia radica en que permite que todas las estaciones de trabajo reciban todas las transmisiones, su desventaja esta en el hecho de que suele existir un solo canal de comunicaciones para todos los dispositivos de la red. En consecuencia, si falla, toda la red deja de funcionar.

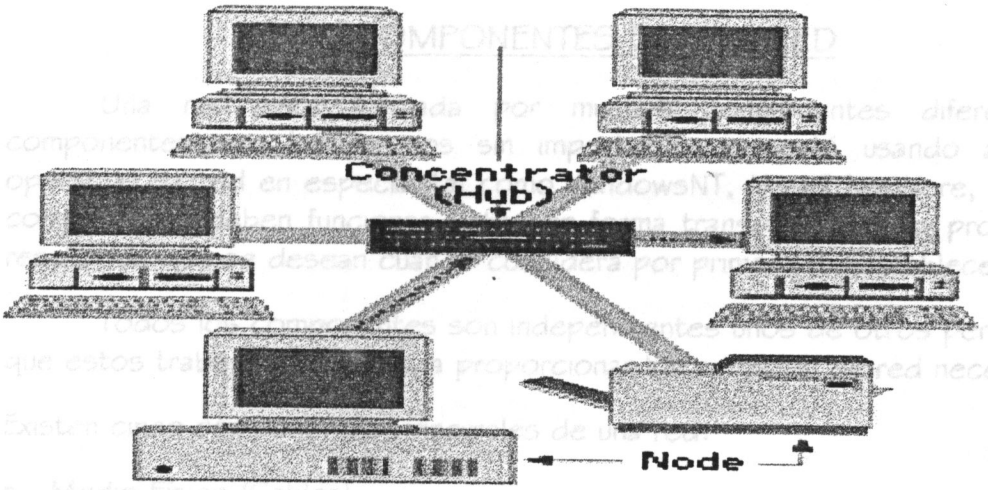


Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo.

6.2 TOPOLOGÀ DE ESTRELLA

Es una de las mas empleadas en los sistemas de comunicación de datos, fácil de controlar por software, el cual no es complicado y su flujo de tráfico es sencillo. Muy similar a la topología jerárquica, aunque su capacidad de procesamiento distribuido es limitado.

Es posible aislar las líneas para detectar algún problema en ellas.



La red se une en un único punto, normalmente con control centralizado, como un concentrador de cableado.

6.3 TOPOLOGÌA EN ANILLO

Se llama así por su forma de anillo y es bastante extendido en su caso, son raros los embotellamientos, su software es sencillo. Su desventaja es que todos los componentes del anillo están unidos por un mismo canal, si uno falla toda la red se interrumpe.

Es una de las tres principales topologías de red. Las estaciones están unidas una con otra formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Una variación del anillo que se utiliza principalmente en redes de fibra como FDDI es el doble anillo.

CAPITULO 7

COMPONENTES DE UNA RED

Una red esta formada por muchos componentes diferentes. Estos componentes son los mismos sin importar si se está usando algún sistema operativo de red en especial tal como WindowsNT, Novell NetWere, u O/S2.Estos componentes deben funcionar juntos en forma transparente para proporcionar los resultados que se desean cuando considera por primera vez establecer una red.

Todos los componentes son independientes unos de otros pero se requiere que estos trabajen juntos, para proporcionar los servicios de red necesarios.

Existen cinco componentes principales de una red:

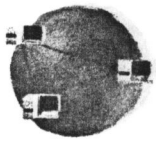
- Medio Físico (Cables)
- Hardware
- Protocolos
- Sistemas Operativos

7.1 MEDIO FÌSICO

El medio físico es el medio sobre el que se envían las señales eléctricas para realizar la transmisión de la información. Es el medio utilizado para conectar los equipos informáticos que constituyen la red. Los medios más comunes en la actualidad son:

7.1.1 Cables de cobre

Los cables de cobre utilizados para transmisión son conductores clásicos que en ocasiones no son de este metal, sino aleaciones que mejoran las características eléctricas del cable.



7.1.2 Coaxial

El término coaxial quiere decir eje común ya que un cable coaxial está formado por un conductor central rodeado de una capa de material aislante o dieléctrico, rodeada a su vez por una malla de hilos conductores cubierta por una funda de material aislante y protector, formado así cuatro capas concéntricas. Hay en el mercado gran variedad de cables coaxiales, envían una señal digital simple. Fueron creados para comunicación de datos y se acoplan a comunicación de voz, que se usan frecuentemente en topología bus - lineal y de árbol. Tiene el alcance de 1 a 10 Kms y cuenta con un ancho de banda de 10Mbps, llega a contener una red con este cable hasta 1000 dispositivos pero es muy propenso a los ruidos y solo puede usar el 40 % de su capacidad para permanecer estable.

Existen básicamente dos tipos de cable coaxial. El primero denominado de Banda Base, es el normalmente empleado en redes de computadoras, con una resistencia de 50 Ohm, por el que fluyen señales digitales, al contrario que su pariente más cercano, el cable coaxial de banda ancha.

El cable de banda ancha normalmente mueve señales analógicas posibilitando la transmisión de gran cantidad de información por varias frecuencias y su uso más común es la televisión por cable.

La instalación de una red empleando este cable es relativamente sencilla, quizás lo mas complicado sería el ajuste del conector BNC al cable coaxial pero se convierte en una tarea fácil luego de ser efectuada un par de veces. El nombre BNC proviene de las abreviaturas de "conector Nacional Británico" y existen diversos tipos de los mismos.

Cada una de las tarjetas de red de la computadora se conectan al conector BNV T. Este conector permite unir dos porciones o segmentos de red incorporando a una computadora a la misma red. El problema principal de esta red radica precisamente en la gran cantidad de conexiones o junturas que se realizan con estos conectores, lo que normalmente puede derivar en que una porción de la red quede inutilizada, hasta descubrir el conector aflojado.

Por una parte, cada porción de cable entre dos computadoras deben tener un conector BNC macho y uno hembra. Actualmente existen diversos tipos de conectores según la forma de conexión que tiene el cable coaxial, alguno de ellos son por presión, otros por inserción de púas, tornillos, etc.

Finalmente cabe destacar él ultimo elemento de una red por cable coaxial y son los terminadores. Estos dispositivos se conectan en cada uno de los extremos de la red, tal como si se tratase de una tubería de agua.

Su objetivo es el de proveer la resistencia necesaria en cada uno de los extremos, aspecto que es empleado por el protocolo de red para ciertas operaciones. Para mantener la compatibilidad hacia medios coaxiales, es importante contar con un hub provisto del respectivo conector BNC.

7.1.3 Par trenzado apantallado (STP, Shielded Twisted Pair)

Este tipo de cable está formado por grupos de dos conductores cada uno con su propio aislante trenzados entre sí y rodeados de una pantalla de material conductor, recubierta a su vez por un aislante. Cada grupo se trenza con los demás que forman el cable y, el conjunto total se rodea de una malla conductora y una capa de aislante protector.

Esta disposición reduce las interferencias externas, las interferencias entre pares y la emisión de señales producidas por las corrientes que circulan por el cable. Un uso común de este tipo de cables es la conexión de los tranceptores insertados en el coaxial de una red 10base5 con la tarjeta de red de una estación.

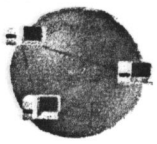
7.1.4 Par trenzado sin pantalla (UTP, Unshielded Twisted Pair)

El cable par trenzado, más conocido como UTP, es uno de los más comunes y difundidos debido a al alta expansión de las redes telefónicas en todo el mundo. Es uno de los medios más empleados para la transmisión de señales inteligentes de rango vocal en redes de conmutación de circuitos o las llamadas redes telefónicas.

Actualmente tiene una amplia difusión no solo en telefonía sino también dentro de las redes LAN de computadoras.

Esta adaptabilidad responde a que el mismo es fabricado en diversas categorías, cada una de las cuales tiene un objetivo especifico de aplicación.

Existen 5 categorías de cable UTP y una en proyecto, es decir la sexta. La primera categoría responde al cable UTP categoría 1, especialmente diseñado para redes telefónicas, el clásico cable utilizado en el teléfono y dentro de las



compañías telefónicas: el cable UTP categoría 2 es también empleado para transmisión de voz de datos hasta 4 Mbps; el cable UTP categoría 3 , es empleado en redes de computadoras con velocidad de hasta 16 Mbps; el cable UTP categoría 4 tiene la capacidad de soportar comunicaciones en redes de computadoras a velocidades de 20 Mbps. Finalmente cabe presentar el cable UTP categoría 5, un verdadero estandar actual dentro de las redes LAN particularmente, con la capacidad de sostener comunicaciones a 100Mbps.

Sintéticamente los cables UTP se pueden catalogar en una de dos clases básicas: los destinados a comunicación de voz y los dedicados a comunicación de datos en redes de computadoras.

En este tipo de cable, los conductores aislados se trenzan entre sí en pares y todos los pares del cable a su vez. Esto reduce las interferencias entre pares y la emisión de señales. Estos cables se utilizan, sobre todo, para los sistemas de cableado integral, combinando telefonía y redes de transmisión de datos, principalmente 10baseT.

Por lo general, la estructura de todos los cables UTP no difieren significativamente, aunque es cierto que cada fabricante introduce algunas tecnológías adicionales mientras los estándares de fabricación se lo permitan.

Así, la estructura de este cable está compuesto internamente por un conductor que es de alambre electrolìtico reconocido, de tipo circular, aislado por una capa de polietileno coloreado.

Debajo de la aislaciòn coloreada existe otra capa de aislaciòn también de polietileno, que contiene en su composición una sustancia antioxidante para evitar la corrosión del cable. El conducto solo tiene un diámetro de aproximadamente medio milímetro, y más la aislaciòn el diámetro puede superar el milímetro.

Sin embargo es importante aclarar que habitualmente este tipo de cable no se maneja por unidades, sino por pares y grupos de pares, paquete conocido como cable multipar. Todos los cables del multipar están trenzados entre sí con el objeto de mejorar la resistencia de todo el grupo hacia diferentes tipos de resistencia electromagnética externa.

Por esta razón surge la necesidad de poder definir colores para los mismos que permitan al final de cada grupo de cables conocer cual cable va con cual otro. Los colores de la aislaciòn están normalizados a fin de su manipulación por grandes cantidades.

Los cables, una vez fabricados unitariamente y aislados, se trenzan de a pares de acuerdo al color de cada uno de ellos; aun así, estos se vuelven a unir a otros formando estructuras mayores: los pares se agrupan en subgrupos, los subgrupos en grupos, los grupos en superunidades, y las superunidades se agrupan en el denominado cable.

De esta forma se van uniendo los cables hasta llegar a capacidades de 2200 pares; un cable normalmente esta compuesto por 22 superunidades; cada subunidad esta compuesta por 21 pares aproximadamente; este valor es el mismo para las unidades menores. Los cables telefónicos pueden ser armados de 6,10,18,20,30,50,80,100,150,200,300,400,600,900,1200,1500,1800 o 2200 pares.
Para el remplazo de eventuales pares defectuosos se colocan pares de reserva en cables que tengan 100 o más pares.

Se ubican en la parte más externa del cable y su numero no puede ser mayor al 1% de la cantidad total de pares del cable.

Todo el conjunto o cable se recubre con una cinta de material aislante, resistente a la humedad. Se aplica la cinta al cable de forma helicoidal o longitudinal. Adicionalmente, el cable es cubierto de polietileno laminado(compuesto por una parte de aluminio).

Presurizaciòn es un proceso por el cual se introduce al interior de los cables un gas seco, a efectos de eliminar la humedad del interior. Esto tan solo para los cables que poseen más de 50 pares.

Estandarización de colores

Nº PAR	COLOR CONDUCTOR Nº 1	COLOR CONDUCTOR Nº 2
1	Blanco	Azul
2	Blanco	Anaranjado
3	Blanco	Verde
4	Blanco	Marrón
5	Blanco	Gris Oscuro
6	Rojo	Azul

7.1.5 Fibra Óptica

Este es el medio de transmisión de datos inmune a las interferencias por excelencia, debido a que en su interior dejan de moverse impulsos eléctricos, al conducir luz por su interior, la fibra óptica no es propensa a ningún tipo de interferencia electromagnética o electroestática.

La fibra es un hilo fino de vidrio generalmente o plástico, cuyo grosor puede asemejarse al de un cabello humano, capaz de conducir la luz por su interior. Generalmente esta luz es de tipo infrarrojo y no es visible al ojo humano. La modulación de esta luz permite transmitir información tal y como lo hacen los medios eléctricos.

La estructura de la fibra óptica es relativamente sencilla, aunque la mayor complejidad radica en su fabricación.

La fibra óptica esta compuesta por dos capas, una denominada núcleo (Core) y la otra denominada Recubrimiento por núcleos. El extra delgado hilo de vidrio esta cubierto de una capa plástica que le brinda la protección necesaria, aunque normalmente un gran conjunto de fibras se une entre sí para obtener mayor seguridad.

La fibra óptica esta compuesta por dos capas de vidrio, cada una con distinto índice de refracción.

El índice de refracción del núcleo es mayor que el de revestimiento, razón por la cual y debido a las diferencias de índices, la luz introducida al interior de la fibra se mantiene y propaga a través del núcleo. Se produce por ende el efecto denominado Refracción total.

CONO DE ACEPTACIÒN.- Los rayos de luz pueden entrar a la fibra óptica si el rayo se halla contenido dentro de un cierto ángulo denominado CONO DE ACEPTACION. Un rayo de luz puede perfectamente no ser transportado por la fibra óptica si no cumple con el requisito del cono de aceptación. La fibra óptica presenta niveles de atenuación realmente bajos que permiten transmitir luz por varios kilómetros sin necesidad de reconstruir la señal (regenerar).

LONGITUD DE ONDA.- Todo rayo de luz se halla dentro de un espectro posible. El espectro incluye en la parte izquierda, los rayos de luz de menor longitud de onda, pero que poseen más energía, denominados ultravioletas.

En el otro extremo, se encuentran las luces de mayores longitudes de onda, pero que poseen energía, a las que denomina infrarrojas.

Un intervalo relativamente pequeño de todo este espectro, que se halla entre los colores violeta y rojo, es el que el ojo humano puede apreciar.

Son precisamente las luces que se hallan dentro del espectro correspondiente a los infrarrojos los que se emplean para transmitir información por el interior de las fibras ópticas.

Las fibras ópticas se clasifican de acuerdo al modo de propagación que dentro de ellas describen los rayos de luz emitidos. En esta clasificación existen tres tipos:

MONOMODO

En este tipo de fibra, los rayos de luz transmitidos por la fibra viajan linealmente.

Sus costos son elevados ya que el índice de refracción del núcleo varía del más alto, hacia él más bajo en el recubrimiento.

Este hecho produce un efecto espiral en todo rayo introducido en la fibra óptica, ya que todo rayo describe una forma helicoidal a medida que va avanzando por la fibra.

MULTIMODO-STEP INDEX.- Este tipo de fibra, se denomina de multimodo índice escalonado. No tiene una capacidad tan grande, pero la calidad final es alta.

El índice de refracción del núcleo es uniforme para todo el mismo. Las fibras se utilizan como guías de haces de luz láser sobre los cuales se modulan las señales que transmiten la información, permitiendo que la luz describa trayectorias curvadas, necesarias para poder instalar las redes en los edificios.

7.1.6 Radio

Las ondas de radio fueron el primer medio utilizado para transmitir información y, gracias a los avances tecnológicos como la telefonía celular y el auge de los equipos portátiles, se están convirtiendo en uno de los medios de transmisión más utilizados en la actualidad.

7.1.7 Inalámbrico

Usada para propósitos especiales de redes inalámbricas están ganando terreno, donde el cable físico es poco práctico e imposible de instalar.

7.2 HARDWARE

Es el conjunto de elementos físicos electrónicos que forman

7.2.1 Módem

Es el equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono. Cuando la señal llega a su destino, otro módem se encarga de reconstruir la señal digital primitiva, de cuyo proceso se encarga la computadora receptora. En caso de que ambos puedan estar transmitiendo datos simultáneamente, se dice que operan en modo *full-duplex;* si sólo puede transmitir uno de ellos, el modo de **operación se denomina *half-duplex.***

Para convertir una señal digital en otra analógica, el módem genera una onda portadora y la modula en función de la señal digital. El tipo de modulación depende de la aplicación y de la velocidad de transmisión del módem. Un módem de alta velocidad, por ejemplo, utiliza una combinación de modulación en amplitud y de modulación en fase, en la cual la fase de la portadora se varía para codificar la información digital.

El proceso de recepción de la señal analógica y su reconversión en digital se denomina demodulación. La palabra módem es una contracción de las dos funciones básicas: *mo*dulación y *demo*dulación.

Los primeros equipos eran muy aparatosos y sólo podían transmitir datos a unos 100 bits por segundo. Los más utilizados en la actualidad en los ordenadores personales transmiten la información a más de 33 bits por segundo.

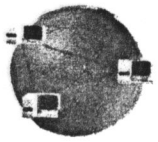
Pueden incluir funciones de fax y de contestador automático de voz.

7.2.2 Tarjetas de interfaz de Red

Las hay de varios fabricantes, para los sistemas de comunicación más populares como ARCnet, EtherNet y Token Ring casi cualquier PC equipada con una tarjeta cualquiera puede comunicarse con otra PC que tenga una tarjeta de un fabricante distinto. También hay tarjetas para comunicación tipo propietario, pero por el riesgo que implica no son muy usadas. Hay tarjetas para Bus MCA, EISA, ISA de 8, 16 ò 32 bits.

Existen tarjetas de tipo dominio de bus, las cuales tienen la capacidad de enviar y recibir datos de otras tarjetas directamente entre ellas sin que intervenga el procesador, con el cual se ahorra tiempo.

También existen las tarjetas inteligentes, las cuales tienen integrado un chip, que les permite manejar distintos niveles de comunicación. Y por ultimo hay tarjetas que incluso permiten el arranque remoto de un PC a partir de una copia remota del sistema operativo.



La configuración de tarjetas de red generalmente requiere el ajuste de varios conmutadores o puentes, entre los que destacan los siguientes:

Interrupción: Cuando la tarjeta necesita comunicarse con otra PC, tiene que indicar que requiere atención. Esto se logra por medio de una interrupción o IRQ, lo que ocasiona que el procesador detenga lo que esta haciendo y preste atención al instrumento que emite la interrupción. Es de vital importancia asegurarse que los diferentes instrumentos o periféricos no estén asignados al mismo IRQ.

Dirección de E/S(I/O): Los puertos E/S posibilitan la transmisión de datos de la memoria de la PC a la tarjeta o viceversa. Estos puertos están en un bloque de direcciones de memoria especiales. Los datos escritos en uno o más puertos E/S son interpretados por la tarjeta y enviados a donde quiera que vaya (ya sea a la tarjeta, para controlarlos a otra tarjeta), o los coloca conforme son recibidos.

DMA(Acceso Directo a Memoria):DMA es una técnica empleada para mover datos de un lugar en la memoria ya, sea a otro lugar en la memoria o puertos de E/S sin emplear el procesador. Es un método para reducir la carga de trabajo del procesador y mejorar su rendimiento.

Arranque Remoto: Este es opcional. Tiene que activarse ajustando un conmutador o puente y generalmente requiere la instalación de un chip en la tarjeta. Este chip que no es mas que de memoria ROM contiene el programa que ejecuta el arranque(o inicio) remoto. El arranque remoto se utiliza como técnica de seguridad en estaciones de trabajo sin disco o como una manera de centralizar los datos de configuración para que la red sea más manejable.

Tipo de Cable: En algunos sistemas de red, como EtherNet, el tipo de cable puede ajustarse a la tarjeta. Para EtherNet, esto significa que un tipo de tarjeta puede usarse con cables tanto gruesos como delgados.

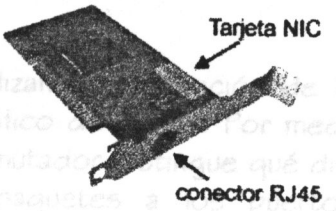
Dirección: En algunos de los sistemas de transporte antiguos, como ARCNet, es necesario para ajustar la dirección física de la tarjeta. Este sistema solo puede manejar 255 direcciones únicas. A la dirección física se le conoce generalmente como dirección MAC. En el caso de EterNet, la dirección de la tarjeta está fija y el fabricante garantiza que es única. En las redes, el término dirección se aplica a un número que es exclusivo de una tarjeta o red en particular.

Esto es muy parecido al número que tiene una casa en una calle, la direcciónde la tarjeta es equivalente al número de la casa, y la red a la que se conecta la tarjeta es equivalente a la calle.

Muchos fabricantes entregan sus NICs en alguna configuración estándar o por omisión(interrupción 3, dirección E/S base 300h,etc.)Si ésta configuración por omisión es la que se desea, hay que verificar que la tarjeta realmente este configurada así antes de instalarla.

En la mayoría de las tarjetas actuales, la configuración ya se lleva a cabo vía software.

Esto evita estar moviendo los pequeños interruptores o puentes, que vienen en las tarjetas, de cualquier forma, en algunos sistemas es necesario tener conocimiento de éstos para poder configurarlos.

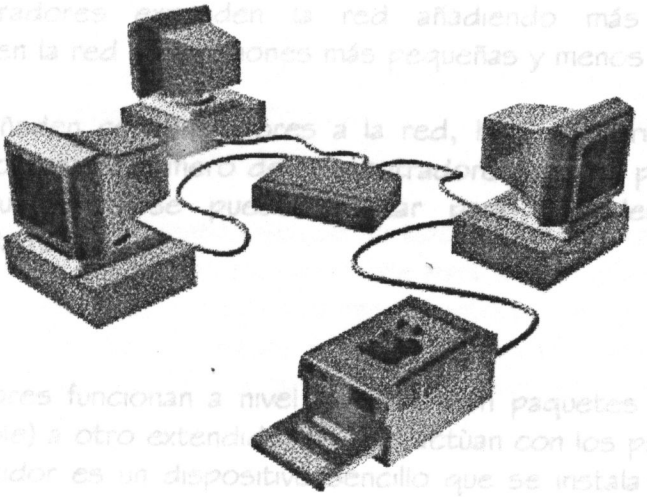


7.2.3 Concentradores y Conmutadores

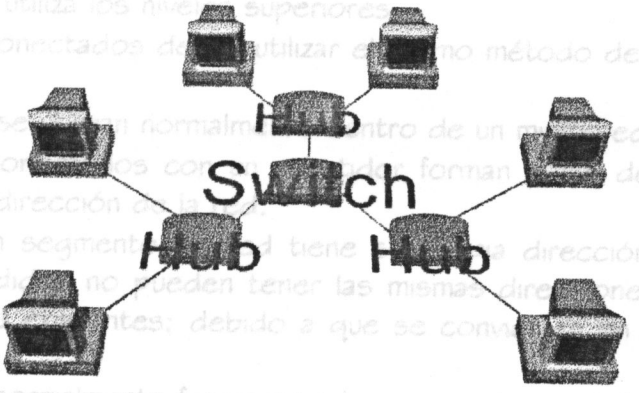
Los concentradores y conmutadores se utilizan para conectar PCs, impresoras y otros dispositivos. Los concentradores se diferencian de los conmutadores en el modo en que administran el tráfico de la red.

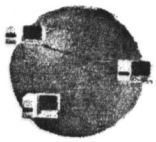
El término "concentrador" se utiliza a veces para referirse a una pieza de equipo de red que conecta PCs entre sí, aunque realmente hace las veces de repetidor. Se llama así porque pasa o repite toda la información que recibe a todos sus puertos. Los concentradores se pueden utilizar para ampliar una red.

No obstante, de esta acción puede resultar un exceso de tráfico innecesario porque se envía la misma información a todos los dispositivos de una red. Los concentradores están indicados para redes pequeñas, aunque es posible que las redes con alta carga de tráfico necesiten equipos de red adicionales, como puede ser un conmutador, que reduciría el tráfico innecesario.



Los conmutadores utilizan la información de la dirección de cada paquete para controlar el flujo del tráfico de la red. Por medio de la monitorización de los paquetes que recibe, un conmutador distingue qué dispositivos están conectados a sus puertos, y envía los paquetes a los puertos adecuados solamente. Un conmutador reduce la cantidad de tráfico innecesario porque la información recibida en un puerto se envía solamente al dispositivo que tiene la dirección de destino correcta, a diferencia de un concentrador, que la envía a todos los puertos.





Los conmutadores y los concentradores se utilizan a menudo en la misma red. Los concentradores expanden la red añadiendo más puertos, y los conmutadores dividen la red en secciones más pequeñas y menos congestionadas.

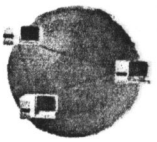
Cuando se añaden concentradores a la red, hay una serie de normas que deben conocerse acerca del número de concentradores que se pueden conectar a la vez. Los conmutadores se pueden utilizar para extender el número de concentradores en la red.

7.2.4 Repetidores

Los repetidores funcionan a nivel físico. Envían paquetes desde un sector de red primario (cable) a otro extendido, no interactùan con los protocolos de mas alto nivel. Un Repetidor es un dispositivo sencillo que se instala para amplificar la señal del cable, de forma que se puede extender la longitud de la red.

El Repetidor normalmente no modifica la señal, excepto que la amplifica para poder retransmitirla por el segmento de cable extendido. Algunos Repetidores también filtran el ruido. Un repetidor es básicamente un dispositivo "no inteligente" con las siguientes características:

- Un Repetidor regenera la señal de la red para que lleguen mas lejos.
- Se utilizan sobre todo en los sistemas de cableado lineales como Ethernet.
- Los Repetidores funcionan sobre el nivel más bajo de la jerarquía de protocolos; el nivel físico. No utiliza los niveles superiores.
- Los segmentos conectados deben utilizar el mismo método de acceso al medio de transmisión.
- Los Repetidores se utilizan normalmente dentro de un mismo edificio.
- Los segmentos conectados con un repetidor forman parte de la misma red y tendrán la misma dirección de la red.
- Cada nodo de un segmento de red tiene su propia dirección. Los nodos de segmentos extendidos no pueden tener las mismas direcciones que los nodos de los segmentos existentes; debido a que se convierten en parte del mismo segmento de red.
- Los Repetidores normalmente funcionan a la misma velocidad de transmisión que las redes que conectan.



7.2.5 Puentes

Los puentes interconectan dos o más redes, pasando los paquetes entre ellas. Soportan distintos tipos de redes. Éstos añaden un nivel de inteligencia a una conexión entre redes. Conecta dos segmentos de red iguales o distintos. Podemos ver un puente como un clasificador de correo que mira las direcciones de los puentes y los coloca en la red adecuada.

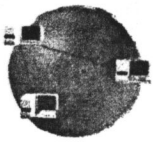
Cada segmento de red puede ser de un tipo distinto (Ethernet, Token Ring, fibra Optica, y demás). Se puede crear un puente para dividir una red amplia en dos o más redes más pequeñas. Esto mejora el rendimiento al reducir el trafico, ya que los paquetes para estaciones concretas no tienen que viajar por toda la red. Los puentes también se usan para conectar distintos tipos de redes. Los puentes trabajan a nivel enlace de datos.

Cualquier dispositivo que se adapte a las especificaciones del nivel de control de acceso al medio(MAC, Media Access Control)puede conectarse con otros dispositivos de nivel MAC. Recordemos que el nivel MAC es un subnivel de enlace de datos. El nivel MAC es modular; un controlador de placa de red enlaza sus rutinas de control de acceso al nivel.

El nivel superior de control de enlace lógico (LLC, Logical Link Control) hace de conmutador y enlace entre los módulos del nivel MAC. Los paquetes circulan entre las redes pasando por el nivel LLC. Este procesamiento extra incluye algún tiempo de latencia en el ancho de banda de la red, cundo se compara con la misma red sin puente o con repetidor.

Con un puente podemos conectar dispositivos que utilicen protocolos diferentes, pero el nivel de enlace de datos no sabe nada sobre el mejor camino hacia un cierto destino; no existe ninguna forma de enviar paquetes a un segmento de red de modo que alcancen su destino de la forma mas rápida o eficiente. Esa es la función de un Router.

No obstante los puentes ofrecen filtrado. El filtrado evita que los paquetes de un segmento de red local pasen por el puente y lleguen a segmentos de red donde no sirven para nada. Ésta ayuda a reducir el trafico entre redes e incrementa el rendimiento. Sin filtrado, los paquetes son enviados a todos los puntos de la red.



Un Puente se instala por las siguientes razones:

- Extender una red existente cuando se ha alcanzado su máxima extensión.
- Para eliminar los cuellos de botella que se generan cuando hay demaciadas estaciones de trabajo conectadas a un único segmento de red. De esta forma cada red trabaja con menos usuarios, mejorando el rendimiento.
- Para conectar entre sí distintos tipos de redes, como Token Ring y Ethernet.

7.2.6 Routers

Los Routers son similares a los puentes, si bien observan con mas detenimiento la dirección del paquete, y toman parte en la determinación del camino a seguir para llevarlo a su destino. Los Routers son críticos para las redes de gran alcance que utilizan enlaces de comunicación remotas.

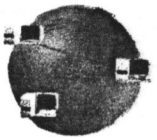
Mantiene el tráfico fluyendo eficientemente sobre caminos predefinidos en una interconexión de redes complejas, como la mostrada. Pueden inspeccionar la información en el nivel de red para determinar la información de la mejor ruta.

Razones para usar Routers:

- Los Routers ofrecen un filtrado de paquetes avanzado.
- Los Routers son necesarios cuando hay diversos protocolos en una interconexión de redes, los paquetes de ciertos protocolos tienen que confirmarse en una cierta área.
- Los routers ofrecen un encaminamiento inteligente, lo cual mejora el rendimiento. Un Router inteligente conoce la estructura de la red y puede encontrar con facilidad el mejor camino para un paquete.

Un Router examina la información de encaminamiento de los paquetes y los dirige al segmento de red adecuado. Si el Router esta en un servidor, envía los paquetes destinados para este servidor a los protocolos de niveles superiores. Un Router solo procesa los paquetes que van dirigidos ha él, lo que incluye a los paquetes enviados a otros routers con los que estén conectados.

Los Router envían los paquetes por la mejor ruta hacia su destino. Mantiene tablas de redes locales y routers adyacentes en la red. Cuando un Router recibe un paquete, consulta esta tabla para ver si puede enviar directamente el paquete destino. Si no es así, determina la posición de un Router que pueda enviar el paquete a su destino.



Los routers permiten dividir una red en redes lógicas. Estas redes lógicas son más sencillas de manejar.

Cada segmento de red tiene su propia dirección. Esta es la información contenida en el nivel de red al que accede los routers. La segmentación de las redes permite enviar las tormentas de difusión.

Estas ocurren cuando los nodos se conectan de forma adecuada, y la red se satura con la difusión de mensajes intentando localizar los destinos. Los métodos de filtrado y selección del mejor camino utilizados al segmentar, ayudan a reducir este efecto.

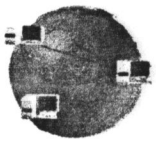
7.2.7 Backbone

Es un cable que conecta entre sí dos o mas segmentos de una red local y ofrece un enlace de datos de alta velocidad entre ellos. Mientras que un puente se establece instalando dos o más placas de red en un servidor, la interconexión de redes se realiza conectando varios servidores o segmentos de red local, generalmente con un enlace backbone.

Los enlaces backbone son generalmente medios de alta velocidad, como cables, y fibras ópticas. Los backbones se puede utilizar para agrupar los servidores en un punto por razones de gestión. Por ejemplo, los servidores de cada departamento de una organización se pueden agrupar juntos en un punto centralizado.

Estas son algunas de las ventajas de centralizar los servidores y la administración de la red:

- Los servidores se encuentran centralizados, mejorando la monitorizaciòn y el mantenimiento.
- Se mejora la seguridad ya que en la zona que están los servidores se puede tener cerrada y con una instalación antiincendios.
- Los servidores nose encuentran confinados en los departamentos individuales, en los que el personal de mantenimiento pueden tener problemas para acceder a ellos fuera de las horas de oficina.
- Cuando los servidores están centralizados en un punto, se puede monitorizar y mejorar el rendimiento con una mayor facilidad.



Un backbone puede ofrecer hasta diez veces la velocidad de transferencia de un segmento de red local; este ancho de banda es compartido por cada estación que usa el backbone .

Por ejemplo, si dos estaciones se comunican mediante un backbone de fibra óptica de 100 MB/Seg, existe la posibilidad de transferir datos a 100Mb/Seg.Si otras dos estaciones utilizan el enlace, el ancho de banda posible para cada estación se reduce a la mitad. Cada sesión usa una parte del ancho de banda, así que cuanto mayor sea el traficó en la red, más se degradara el rendimiento.

7.3 PROTOCOLOS DE COMUNICACIÒN

Protocolos

- El término protocolo es usado para describir el intercambio de información entre procesos.
- Procesos: Programas que se ejecuten en un hardware.

Procesos en:

- Equipos de una red.
- Sistema multiprocesador, para controlar interacción de procesos paralelos.
- Aplicaciones en tiempo real para el control de dispositivos.
- En cualquier sistema donde no existe relación fija en el tiempo de ocurrencia de los eventos.

Definición mas formal:

- Especificación de la lógica y de los procedimientos de los mecanismos de comunicación entre procesos.
- La definición lógica constituye la sintaxis.
- La definición de los procedimientos constituye la semántica.

Funciones más importantes:

- Control de errores:
- Control de Flujo
- Control de Congestión
- Estrategias de encaminamiento

Control de Errores:

- Protege integridad de los datos del usuario y de los mensajes de control.

Control de Flujo y Congestión:

- Permite a la red compartir sus recursos entre un gran número de usuarios, entregando a cada uno un servicio satisfactorio sin que sus operaciones corran peligro.

Estrategias de Encaminamiento:

- Permite optimizar la utilización de los recursos de la red, aumentando la disponibilidad de los servicios de la red al proveer caminos alternativos entre nodos terminales.

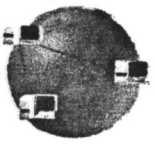
Procesos

- Los protocolos son implementados vía procesos.
  - Un proceso se ejecuta en un procesador virtual o lógico.
  - Un proceso es auto - contenido
  - No se de cuenta (y no le interesa), que un procesador real comparte sus recursos entre varios procesos activos.
- Entrada a los procesos ocurre por puertas lógicas de software, por donde el proceso recibe mensajes desde procesos residentes en el mismo o en otro procesador.
- Un conjunto de datos privados define el estado actual de un proceso y determinan la acción a tomar por el receptor de un mensaje.
- El resultado de la computación ejecutada por el proceso se envía por una puerta lógica de salida.

7.3.1 Funcionamiento de un protocolo

Los protocolos son un conjunto de reglas usadas para asegurar comunicaciones confiables. El protocolo de comunicación determina el formato de la información transmitida por la red. Dos dispositivos de hardware en la red deben entender los mismos protocolos para intercambiar información. Los protocolos de transporte son los "empacadores" reales que determinan como se transfiere la información a través de la red.

- Un proceso recibe un mensaje, lo procesa y envía una respuesta, sin que exista relación entre este evento y otro anterior o posterior.



- El proceso origen, conocerá la dirección del proceso destino y la incluirá en el mensaje.

- Esta dirección, identificará únicamente a un procesador, quien conocerá al proceso destino.
- El originador cuando atiende un mensaje, entra en un estado de espera de respuesta en una de sus puertas.

- El proceso destino ejecuta la función especificada en el mensaje, construye la respuesta (con resultados y dirección del origen) y envía el mensaje respuesta por una puerta de salida, (quedando libre para aceptar otro mensaje).

- La respuesta llega al originador, quien realiza un chequeo para asegurarse que viene del lugar correcto antes de aceptarla, luego, pasa al estado "no espera respuesta" en esa puerta de entrada.

Este es un protocolo muy simple, necesita de la sintaxis para definición de formatos de los mensajes y una semántica muy simple. Debe considerarse el hecho de que, la red introduce demoras causadas por congestión, encaminamiento, etc., e incluso puede ocurrir pérdida del mensaje.

Para esto, el proceso que realiza la consulta deberá tener un reloj (timer) el que será activado al enviar el mensaje. El reloj enviará una señal al expirar el tiempo indicado en la activación indicando que la respuesta no llegó en el tiempo esperado por, lo que el mensaje deberá ser retransmitido.

Los protocolos más comunes son:

- Apple Talk (Redes Macintosh)
- DLC (Redes IBM y HP)
- IPX/SPX(Redes Novell)
- NBF(Redes de Windows NT)
- Net BEUI(Redes Windows)
- TCP/IP(UNIX e Internet)

7.3.2 Algunos Protocolos

Diferentes empresas han dado diferentes soluciones a la conexión entre computadoras, implementando diferentes familias de protocolos, y dándole diferentes nombres (*TCP/IP*, *IPX/SPX*, NETBEUI, etc.).

TCP / IP.

Se conoce como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que se le llama *TCP/IP*, a la familia de protocolos que nos permite estar conectados a la red Internet. Este nombre viene dado por los dos protocolos estrella de esta familia:

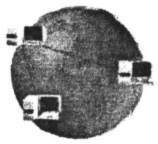
- El protocolo *TCP*, funciona en el nivel de transporte del modelo de referencia *OSI*, proporcionando un transporte fiable de datos.
- El protocolo *IP*, funciona en el nivel de red del modelo *OSI*, que nos permite encaminar nuestros datos hacia otras máquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre computadoras, además de los que proporciona los protocolos *TCP* e *IP*.

Se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada *TCP/IP*:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizará para realizar la comunicación (módem, tarjeta de red...)
- La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos máquinas.
- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial (distribución de las distintas computadoras).

De esta forma, podremos decir, que dos redes están interconectadas si hay una máquina común que pase información de una red a otra.



Además, también podremos decir que una red Internet virtual realizará conexiones entre redes, que ha cambio de pertenecer a la gran red, colaborarán en el tráfico de información

procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las máquinas que implementen estas funciones, y de los sistemas operativos que éstas utilicen.

El *TCP* (Transport Control Protocol) o protocolo de control de transporte se encarga de asegurar que la información se transporte correctamente entre dos computadoras que se conectan en la red empleando para ello diferentes técnicas de detección y corrección de pérdida de datos. Es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones.

Nivel de transporte

Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La máquina remota recibe exactamente lo mismo que le envió la máquina origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores, y se los pasa al nivel de red junto con la dirección de destino.

El protocolo *IP* (Internet Protocol) :se encarga de encontrar en la red mundial la computadora con el que se desea hacer una conexión y de manejar junto con el *TCP* todo lo relacionado a la comunicación entre las dos terminales. Las computadoras conectadas a Internet pueden clasificarse en tres tipos: los equipos *enrutadores*, las computadoras o equipos servidores y las computadoras o PC terminales.

Es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo. Cada *datagrama* se gestiona de forma independiente, por lo que dos *datagramas* pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados.

Es un protocolo no fiable, eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones *IP*, checksum).

Nivel de red

También recibe el nombre de Nivel Internet. Coloca la información que le pasa el nivel de transporte en *datagramas IP*, le añade cabeceras necesarias para su nivel y lo envía al nivel inferior.

NetBEUI

Es el protocolo utilizado por las antiguas redes basadas en Microsoft LAN Manager. Es muy rápido en pequeñas redes que no lleguen a la decena de equipos y que no muevan ficheros de gran tamaño, a partir de ahí es mejor que se descarte por otra opción y que sea desinstalado de los clientes y servidores, esto ultimo siempre que no utilices LAN Manager.

7.4 SISTEMAS OPERTIVOS

Un sistema operativo de red, permite ofrecer servicios a través de la red a otros usuarios. Existen diferentes tipos de sistemas operativos de red. Por ejemplo, Microsoft ha creado una serie de sistemas operativos entre los que se cuentan: Windows 95, Windows NT,Windows 98, y, más recientemente, el sistema operativo Windows 2000.

Estos sistemas operativos se comunican con otros dispositivos en su red utilizando un conjunto de normas. Estas normas se conocen como Protocolos.

Un sistema operativo puede soportar varios protocolos, pero solamente los dispositivos que utilizan el mismo protocolo pueden comunicarse entre sí. Cuando se conecta una computadora a la red (utilizando una tarjeta NIC, PCMCIA o módem), la computadora asocia automáticamente un protocolo con dicho dispositivo.

El protocolo asociado por defecto con el dispositivo dependerá del sistema operativo instalado en la computadora.

Por ejemplo, Windows 95 instala por defecto el protocolo NetBEUI y Windows 98 instala por defecto el protocolo TCP/IP.
Si unas computadoras utilizan NetBEUI y otras utilizan TCP/IP, se tendrán dos redes diferentes.

Las computadoras que utilizan NetBEUI (que son generalmente los que tienen el sistema operativo Windows 95) podrán reconocer y comunicar solamente con otras computadoras que utilicen NetBEUI.

Las computadoras que utilizan TCP/IP (que son generalmente los que tienen el sistema operativo Windows 98) podrán comunicar solamente con otras computadoras que utilicen TCP/IP.

Para solucionar este problema, debe asegurarse de que todas las computadoras de la red utilizan el mismo protocolo.

Se recomienda que las computadoras utilicen TCP/IP si:

- Se necesita tener acceso a Internet en la actualidad o en el futuro.
- Si se va a utilizar un software que necesite TCP/IP. Por ejemplo, muchos juegos de computadora de hoy en día requieren TCP/IP.
- La mayoría de las computadoras ya tienen Windows 98 instalado.

Más adelante se dará una explicación de como configurar TCP/IP.

Las características de los sistemas operativos de red ofrecen una amplia variedad de servicios:
Adaptadores y cables de red: Un sistema operativo de red debe admitir diversos tipos y marcas de interfaz de red.

Nomenclatura Global: Un sistema de nomenclatura global permite a los usuarios ver y acceder a los recursos; y a otros usuarios de cualquier punto de la red sin tener que saber exactamente donde se encuentran. Los usuarios simplemente deben buscar y elegir en una lista.

Algunos Sistemas Operativos de red son:

Windows 95 y 98, WindowsNT , Novell , Linux.

CAPITULO 8

TECNOLOGIA DE ACCESO

El hardware usado para conectar un dispositivo de red al cable físico, se llama hardware de acceso, este es responsable de dividir la información en fragmentos pequeños llamados tramas. Luego estas tramas se transmiten por el cable y se vuelve a ensamblar en el hardware receptor.

El proceso de dividir la información en tramas y transmitirlas por el cable lo controla el hardware diseñado, de acuerdo con especificaciones de tecnología de acceso estandarizadas. Los nombres comunes para las redes se derivan de los nombres de esas especificaciones. Ejemplo, Ethernet, Token Ring y ARCNet.

8.1 TECNOLOGÌA ETHERNET

Ethernet es el nombre de una de las redes de área local más populares hoy en día. La tecnología Ethernet consiste fundamentalmente en un cable coaxial llamado ether de aproximadamente una pulgada de diámetro y hasta 500 metros de longitud. Estos pueden ser extendidos por medio de dispositivos llamados repetidores que duplican señales eléctricas de un cable a otro. Sólo dos repetidores pueden ser usados entre dos computadoras, por lo que la longitud máxima de un ethernet es bastante moderada (1500 metros). Viene especificado por una nomenclatura especial, la cual, nos dice por sí sola qué velocidad de transmisión tiene, en qué medio realiza la transmisión (banda ancha, broad o banda base, base) y qué longitud de segmento podemos tener:

XX (Velocidad) –YYYY (BROAD/BASE)- ZZ (*100 metros)

Ethernet Características

10-BASE-5

Es la única especificada en el estándar original ANSI /IEEE de 1985. Ethernet gruesa (coaxial grueso), la velocidad de transmisión es de 10 Mbps usando la codificación Manchester en banda base. Los segmentos tienen como máximo una distancia de 500 metros, no pudiendo conectar más de

100 estaciones en un segmento. Los equipos se conectan a la red a través de un transceiver.

10-BASE-2
Ethernet fina (coaxial fino de 50 ohms), también llamada "Cheapernet" la velocidad de transmisión es de 10 Mbps y los segmentos tienen como máximo 185 metros, pudiendo conectar los equipos a la red directamente aunque solo permite 30 nodos por segmento.

10-BROAD-36
Usamos también cable coaxial (75 ohms), pero la transmisión se hace en banda ancha, usando un ancho de 14 Mhz. La velocidad es de 10 Mbps y la longitud de cada segmento es como máximo de 3600 metros.

1-BASE-5
Denominada StarLAN. Es una red de bajo costo para la conexión de ordenadores personales. La transmisión se realiza en banda base y usando la codificación Manchester, alcanzando una velocidad de 1 Mbps. La longitud máxima de las ramas (su topología es en forma de estrella, aunque lógicamente es en bus) es de 250 metros, siendo el medio de transmisión dos pares trenzados no apantallados.

10-BASE-T
Alcanza una velocidad de 10 Mbps sobre un par trenzado no apantallado, cuya longitud máxima es de 100 metros. Su topología es un bus con forma de estrella.

100-BASE-TX
Llamada Fast-Ethernet (Ethernet rápida), alcanza una velocidad máxima de 100 Mbps, puede ir con UTP (Par trenzado sin apantallar), STP (UTP apantallado) o con fibra óptica.

Este Método de acceso es él más común en una red LAN esto se debe a su bajo costo el hardware Ethernet y el alto rendimiento que se logra.

Usa una tecnología conocida como CSMA/CD (transportador Sensible de acceso múltiple / detención de colisión). La comunicación sigue estos pasos:

1. El Hardware da acceso que espera transmitir una trama debe escuchar el cable para ver si alguien mas ya esta transmitiendo.
2. Si nadie más esta transmitiendo, envía unas cuantas tramas y luego hace una pausa breve para que otros puedan transmitir, si es lo que desea.
3. Si ocurre una colisión entre dos piezas de hardware de acceso que transmiten a mismo tiempo, ambas piezas esperan un tiempo de duración aleatoria y luego, comienza de nuevo en el paso 1.
4. Estos pasos se repiten con tanta frecuencia como es necesario hasta que el mensaje completo termina de transmitirse.

8.2 TOKEN - RING

Bajo este método de acceso todos los miembros de la red se arreglan en anillo. Esto significa que no hay principio ni fin de la red. Token – Ring toma su nombre del hecho de que todas las máquinas están acomodadas en un anillo (ring) y la información se pasa de una máquina a otra por medio de una señal (token). La señal de un paquete de información, de hasta 4 KB de tamaño, que de manera continua esta circulando por el anillo.

Cuando la señal pasa por una máquina activa es inspeccionada para ver si contiene cualquier información destinada a esa máquina. Si es así, la máquina la toma, si no, pasa a la siguiente. Ahora, si una máquina necesita transferir un mensaje, examina la señal para ver si esta vacía.

Si lo esta, coloca una trama de datos en la señal y la envía para que siga su camino. Para cuando regrese debe estar vacía y así poder mandar la siguiente trama del mensaje.

8.3 FDDI y CDDI

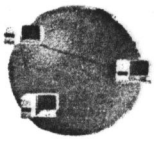
FDDI (Interfaz de Datos Distribuidos por Fibra) y CDDI(Interfaz de Datos Distribuidos por Cobre) Estos métodos de acceso son relativamente nuevos y por consiguiente, bastante costosos.

Las redes FDDI, permiten velocidades de transmisión de datos de 100 Mbps, en tanto que las CDDI, permiten velocidades de transmisión hasta de 600 Mbps. Mientras que Token – Ring se basa en una sola señal, FDDI y CDDI se basa en muchas señales que dan la vuelta. La ventaja sobre Etheernet es que este acceso no tiene colisiones.

8.4 ARCNet

La información en una red ARCNet se pasa en forma lineal, la señal no siempre avanza a la siguiente máquina a lo largo del cable. En lugar de ello la señal se pasa de una máquina a la máquina con la siguiente dirección superior en el adaptador de la red usado en la máquina.

Esto puede causar confusión si dos o mas máquinas tienen sus conmutadores DIP establecidos en la misma dirección. Este método de establecer direcciones simplemente significa otro elemento que debe rastrear el administrador del sistema.



CAPITULO 9

ARQUITECTURA DE REDES

Las redes de ordenadores modernas están diseñadas de una forma muy estructurada. La mayoría de las veses se organizan en una serie de capas o niveles, con objeto de reducir la complejidad de su diseño. Cada una de ellas se construye sobre su precedora.

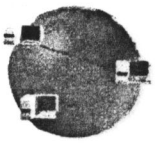
Él número de capas, el nombre, el contenido y función de cada una, varían de una red a otra. Sin embargo, en cualquier red, el propósito de cada capa es ofrecer servicios a las capas superiores, liberándolas del conocimiento detallado sobre como se realizan dichos servicios.

La capa *n* es un ordenador que conversa con la capa *n* de otro ordenador. Las reglas y conversiones utilizadas en esta conversación se conocen conjuntamente como " protocolos" de la capa *n* , para el caso de una red de siete capas. A las entidades que forman las capas correspondientes en ordenadores diferentes se les denominan procesos pares (igual a igual). En otras palabras, son los procesos pares los que se comunican mediante el uso del protocolo.

En realidad no existe una transferencia directa de datos desde la capa *n de un ordenador a la capa n* de otra; si no, mas bien, cada capa pasa la información de datos y control a la capa inmediatamente inferior, y así sucesivamente hasta que se alcanza la capa localizada en la parte más baja de la estructura.

Debajo de la capa 1 está el medio físico, a través del cual se realiza la comunicación real.

Entre cada par de capas adyacentes hay una interfaz, la cual define los servicios y operaciones primitivas que la capa inferior ofrece a la superior. Cuando los diseñadores de redes deciden él número de capas por incluir en una red, así como lo que cada una de ellas deberá hacer. Una de las consideraciones más importantes consiste en definir claramente las interfaces entre capas.



9.1 MODELO OSI

Nuestro modelo está basado en una propuesta desarrollada por la Organización Internacional de Normas(ISO) como un primer paso hacia la normalización internacional de varios protocolos. A este modelo se le conoce como Modelo de Referencia OSI(Interconexión de Sistemas Abiertos) de la ISO. Este modelo OSI consta de siete capas o niveles. Los principios que se aplicaron para llegar a este modelo son, de manera muy resumida, los siguientes:

El número de niveles debe de ser el justo, de manera que la tarea de describirlos e integrarlos no fuera más difícil de lo estrictamente necesario y para que no se tengan que realizar funciones distintas dentro del mismo nivel sin necesidad. Debe crearse un nivel siempre que se requiera un nivel de abstracción diferente en el manejo de los datos. Cada nivel debe realizar tareas bien definidas; funciones similares han de estar en el mismo nivel.

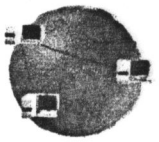
Las diferentes capas se deben elegir de manera que permitan la definición de normas de protocolos y con la suficiente flexibilidad como para que puedan ser rediseñados con el fin de aprovechar los posibles avances software y hardware.

El modelo OSI no es, por si mismo, una arquitectura de red, ya que no especifica exactamente los servicios y protocolos en cada una de las capas. Solo indica lo que se debe hacer en cada un de las capas. Pero, la ISO, ha generado normas para cada una de las capas, pero éstas no pertenecen al modelo. Cada una de ellas se han publicado como normas internacionales independientes.

9.1.1 Capa Física

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. A la hora de su diseño se ha de asegurar que sea capaz de controlar la seguridad de la comunicación, es decir, que lo que se envía sea lo mismo que lo que se recibe. Los problemas de diseño a considerar aquí son los aspectos mecánico, eléctrico, de procedimiento de interfaces y el medio de transmisión física, que se encuentran bajo la capa física.

Se podría decir que su diseño entra dentro del campo de la electricidad. *Los servicios que proporciona la capa física son los siguientes:*



- Conexiones físicas
- Unidades de datos de servicio físico(PSDU)
- Puntos extremos de conexión física
- Identificación del circuito de datos
- Secuenciamiento
- Notificación de condición de fallo
- Parámetros de calidad de servicio(QOS)

Las funciones básicas que realiza son:

- Activación y desactivación de la conexión física
- Transmisión de unidades de datos de servicio físico
- Gestión de nivel físico.

9.1.2 Capa de Enlace

La tarea primordial de la capa de enlace consiste en, un medio de transmisión común y corriente, transformando en una línea sin errores de transmisión para la capa de red. Esta tarea la realiza al hacer que el emisor trocee la entrada de datos en tramas de datos, y las transmita en forma secuencial y procese las tramas de asentimiento, devueltas por el receptor. Como la capa física básicamente acepta y transmite un flujo de bits sin tener en cuenta su significado o estructura, recae sobre la capa de enlace la creación o reconocimiento de los límites de la trama.

Esto puede llevarse a cabo mediante la inclusión de un patrón de bit especial al inicio y al término de la trama. Si estos patrones de bits pueden aparecer entre los datos, deberá tenerse un cuidado especial para evitar cualquier confusión al respecto.

La trama puede destruirse por completo debido a una ráfaga de ruido en la línea, en cuyo caso el software de la capa de enlace, perteneciente a la máquina emisora, deberá retransmitir la trama. Sin embargo, múltiples transmisiones de la misma trama introducen la posibilidad de duplicar la misma. Por ejemplo, el duplicado de una trama podría enviarse, si él cause de recibo que regresa al receptor se hubiera destruido.

Corresponde a esta capa resolver los problemas causados por daño, pérdida o duplicidad de tramas. Otros de los problemas que aparecen en la capa de enlace es referente a cómo evitar que un transmisor muy rápido sature con datos a un receptor lento. Este control se llevara a cabo mediante la utilización de mecanismos de regulación del trafico que permita que el emisor conozca el espacio de memoria que en ese momento tiene el receptor.

9.1.3 *Capa de Red*

La capa de red se ocupa del control de la operación de la subred. Un punto de suma importancia en su diseño, es la determinación sobre como encaminar los paquetes del origen al destino. Las rutas podrían basarse en tablas estáticas que se encuentran cableadas en la red y que difícilmente podrían cambiarse. También, podrían determinarse al inicio de cada conversación.

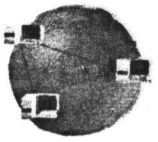
Por último, podrían ser de tipo dinámico, determinándose en forma diferente para cada paquete, reflejando la carga real de la red. Si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se obstruían mutuamente y darán lugar a un cuello de botella. El control de tal congestión dependerá también de la capa de red. Pueden surgir otros problemas cuando un paquete tenga que desplazarse de una red a otra para llegar a su destino.

El direccionamiento utilizado en la segunda red puede ser diferente al empleado en la primera. La segunda podría no aceptar el paquete en su totalidad por ser demasiado grande. Los protocolos podrían ser diferentes, etc. La responsabilidad, para resolver problemas de interconexión de redes heterogéneas recaerá, en todo caso, en la capa de red.

En redes de difusión el problema del encaminamiento es simple, por lo cual la capa de red es normalmente muy delgada o incluso no existe.

9.1.4 *Capa de Transporte*

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. Además, todo este trabajo se debe hacer de manera eficiente de tal forma que aísle la capa de sesión de los cambios inevitables a los que está sujeta la tecnología del hardware.



Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. Si la conexión de transporte necesita un gran caudal, ésta podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones de la red con objeto de mejorar dicho caudal. La capa de transporte determina qué tipo de servicio debe dar a la capa de sesión, y en último término a los usuarios de la red.

El tipo más popular de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregarán los mensajes en el mismo orden en el que fueron enviados.

Sin embargo, el transporte de mensajes aislados sin garantizar el orden de distribución y la difusión de mensajes a destinos múltiples es otra posibilidad de servicio de transporte.

El tipo de servicio se determina cuando se establece la conexión. Resumiendo, las funciones del nivel de transporte , son las siguientes:

- Direccionamiento
- Multiplexaciòn y partición de las conexiones de red
- Establecimiento y liberación de conexiones de transporte.
- Gestión de la capa de transporte
- Transferencia de datos por la conexión de transporte, incluyendo las funciones de secuenciamiento, bloqueo, segmentación, multiplexaciòn y partición, concatenación, control de flujo, detección y recuperación de errores, transferencia de datos expeditos e identificación de la conexión de transporte.

9.1.5 *Capa de Sesión*

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión, se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se utilizan en algunas aplicaciones.

Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo a distancia.

Algunos de los servicios principales relacionados con la capa de sesión y que en puntos posteriores explicaremos son la gestión del control del dialogo, la administración del testigo y la sincronización.

9.1.6 *Capa de Presentación*

La capa de presentación realiza ciertas funciones que se necesitan bastante a menudo como para buscar una solución general para ellas, mas que dejar que cada uno de los usuarios resuelva los problemas. En particular y , a diferencia de las capas inferiores, que únicamente están interesadas en el movimiento fiable de bits de un lugar a otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

En conjunto, la capa de presentación realiza las siguientes funciones:

- Funciones generales.
- Solicitud de establecimiento de sesión. *Negociación y renegociación de la sintaxis de presentación
- Formateado y transformación de los datos
- Transformaciones de propósito especial
- Solicitud de terminación de sesión
- Direccionamiento y multiplexaciòn
- Gestión del nivel de presentación

9.1.7 *Capa de Aplicación*

La capa de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay centenares de tipos terminales incompatibles en el mundo. Considérese la situación de un editor orientado a pantalla que desea trabajar en una red con diferentes tipos de terminales, cada uno de ellos con distintas formas de distribución de pantalla, de secuencias de escape para insertar y borrar texto, de movimientos de cursor, etc.

Una forma de resolver este problema consiste en definir una terminal virtual de red abstracto, con la que los editores y otros programas pueden ser escritos para trabajar con ella. Con objeto de transferir funciones de la terminal virtual de una red a una terminal real, se debe escribir un software que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueve el cursor del terminal virtual al extremo superior izquierdo de la pantalla, dicho software deberá emitir la

secuencia de comandos apropiados para que la terminal real ubique también su cursor en el sitio indicado. El software completo del terminal virtual se encuentra en la capa de aplicación. Otra función de la capa de aplicación es la transferencia de archivos.

Distintos sistemas de archivos tienen diferentes convenciones para denominar un archivo, así como diferentes formas para representar las líneas de texto, etc. La transferencia de archivos entre dos sistemas diferentes requiere de la éstas y de otras incompatibilidades.

Este trabajo, así como el correo electrónico, la entrada de trabajo a distancia, el servicio de directorio y otros servicios de propósito general y específico, también corresponden a la capa de aplicación.

CAPITULO 10

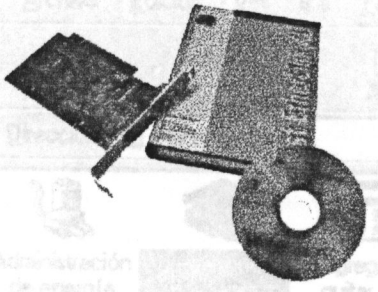
INSTALACIÒN CASO PRÀCTICO

10.1 INSTALACIÒN DE LA NIC

Para poder crear una red se debe tener en cada PC una tarjeta de interfaz de red (NIC, o "Network Interface Card"). Una tarjeta de red (conocida también como una tarjeta adaptadora) es un circuito integrado que se instala en la PC para que pueda establecer conexión con la red.

Para instalar la tarjeta de red, se deberá tener lo siguiente:

- El manual que se adjunta con la PC.
- La NIC y los CDs, discos y manuales adjuntos.
- Un desarmador adecuado para quitar la cubierta de la PC y asegurar la NIC en su lugar.
- El CD-ROM o disquetes de Windows 95 o Windows 98



Se debe asegurar que se conoce el nombre exacto de la NIC. Puede ser que encuentre varios nombres de controlador similares al configurar la NIC, por lo que es fundamental seleccionar el adecuado. Posteriormente se debe apagar la PC.

Consultar la información de seguridad y las instrucciones para quitar la cubierta de la misma. Hay que hacer las conexiones necesarias consultando el manual de la NIC. Se debe evitar el contacto con los componentes de la PC y la NIC ya que se pueden dañar con facilidad. Si hay más de una ranura del tipo necesario, se debe insertar la NIC en cualquiera de ellas.

Es fundamental que la NIC esté completamente insertada en la ranura adecuada. Puede ser necesario apretar un poco la tarjeta cuando se instala en la ranura. Se debe volver a poner la cubierta de la PC y conectar de nuevo el cable de red y los demás componentes que se hayan tenido que desconectar al quitar la cubierta. Al terminar se debe encender la PC y reiniciar Windows 95 o Windows 98. El proceso se apoya en un 'Asistente' que es parte de Windows 95 o Windows 98.

Un Asistente consiste en una serie de pantallas en las que el sistema solicita que se hagan selecciones o indica dónde encontrar otro software. De esta forma quedar instalado el software (o 'driver") adecuado para la NIC.

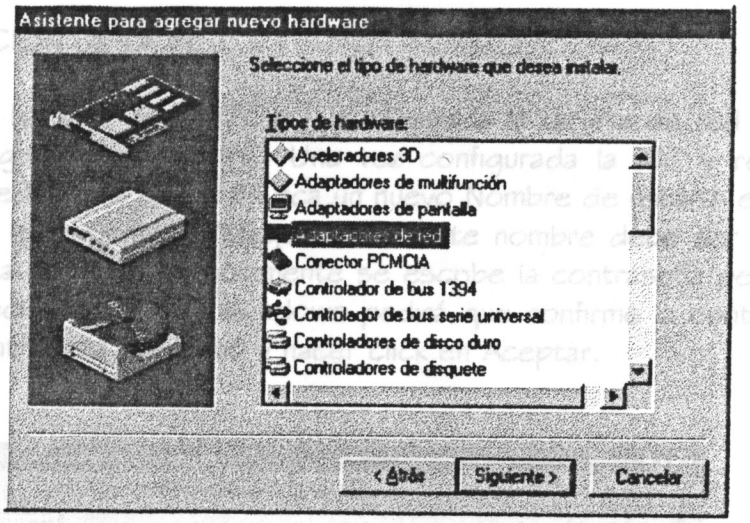
Nota: El aspecto de las pantallas del Asistente podría diferir dependiendo de la versión de Windows que esté ejecutando.

10.2 CONFIGURACIÒN LA NIC

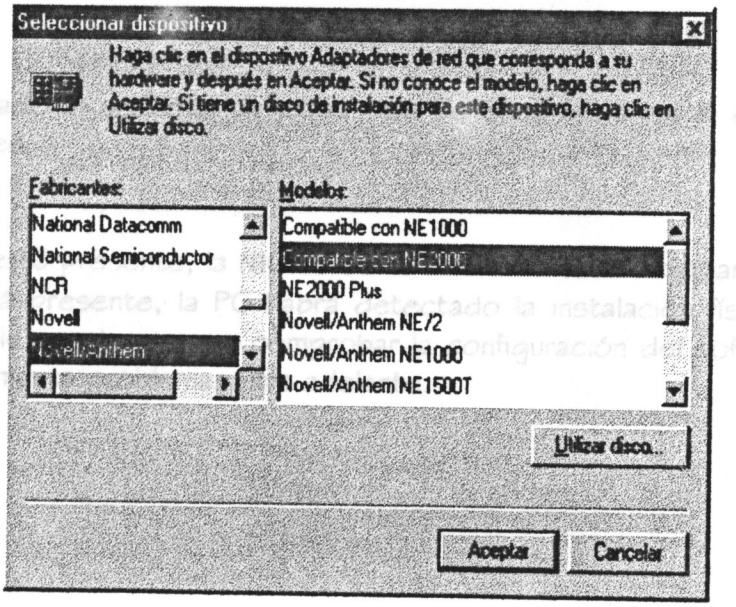
- En el menú Inicio, seleccione Configuración -> Panel de control.
- En la ventana del Panel de control, hacer doble click en Agregar nuevo hardware

- En el cuadro de diálogo de Asistente para agregar nuevo hardware, hacer click en Siguiente>.
- Si se está utilizando Windows 98, hacer click en Siguiente> de nuevo.

- Seleccionar No en la opción de búsqueda del nuevo hardware de Windows, y hacer click en Siguiente>.
- En el cuadro de lista, seleccionar Adaptadores de red y hacer click en Siguiente.



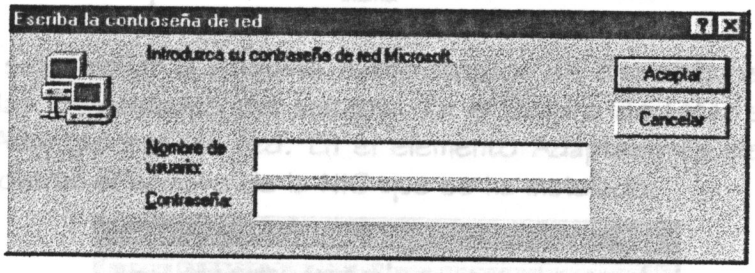
En los cuadros de lista, seleccionar el fabricante y el modelo de la NIC que sé este instalando. Si no se encuentra en la lista el modelo de la tarjeta, se debe hacer click en Utilizar Disco e introducir los discos que vienen junto con la NIC (consulte el manual de la NIC sí es necesario).



Windows pedirá que se inserte el CD de Windows 95 o Windows 98 o los discos de Windows 95. Una vez que terminada esta parte, se debe hacer click en Finalizar y reiniciar el equipo.

12.3 CONFIGURACIÒN DE LA Pc

Una vez que ha sido de instalada y configurada la tarjeta de red (NIC), toca el turno a la configuración de la PC. Una vez configurada la NIC y reiniciado el equipo, Windows pedirá que se introduzca un nuevo **Nombre de usuario** en el campo Nombre de usuario (por ejemplo: "MaquinaO1"). Este nombre debe ser único en la red. Para definir una **contraseña**, solamente se escribe la contraseña pertinente en el campo. Hacer click en Aceptar. Windows pedirá que confirme la contraseña. Se debe escribir la contraseña de nuevo y hacer click en Aceptar.

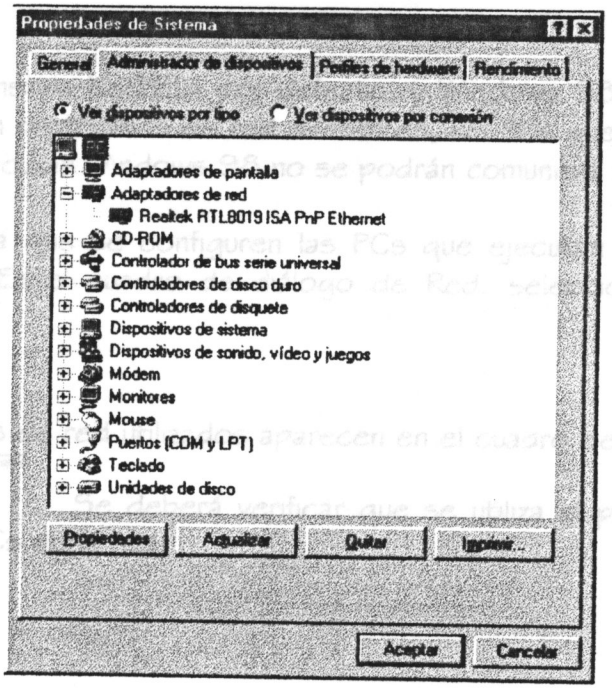


Una vez ingresado al sistema, un icono más se encontrara en el escritorio llamado Entorno de Red

- Si el icono no está presente, la NIC no se ha instalado satisfactoriamente.
- Si el icono está presente, la PC habrá detectado la instalación física de la NIC. Es probable que tenga que comprobar la configuración del software de la NIC si experimenta problemas más adelante.

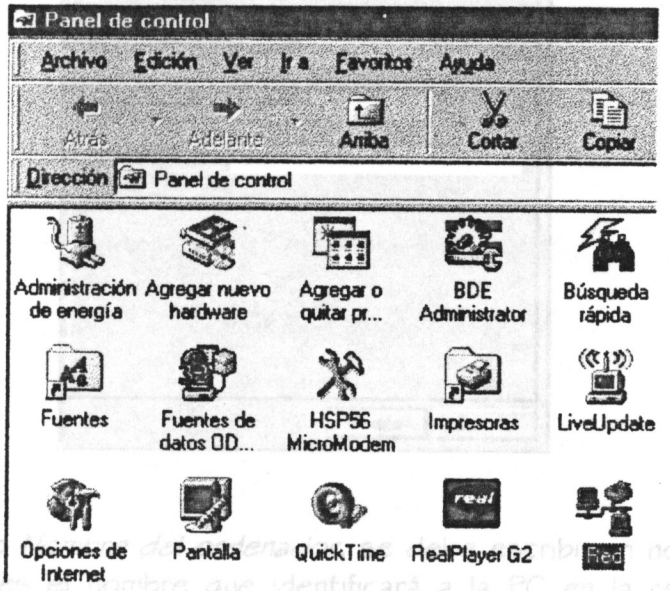
A continuación, se tendrá que configurar la PC para ser reconocida en la red. En el menú Inicio, seleccione Configuración y a continuación Panel de control. En la ventana del Panel de control, hacer doble click en Sistema.

Hay que seleccionar la etiqueta Administrador de dispositivos en el cuadro de diálogo de las Propiedades del sistema. En el cuadro de lista, se debe hacer doble click en Adaptadores de red. En el elemento Adaptadores de red se debe expandir para mostrar el nombre de la NIC que se ha instalado.



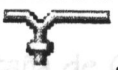
Si el sistema detecta la NIC y el icono de la misma no tiene un círculo amarillo y un símbolo de admiración ('!'), la NIC ha quedado correctamente configurada, de lo contrario la configuración de la NIC no ha sido la correcta.

Hacer doble click en icono de Red de la ventana Panel de control.

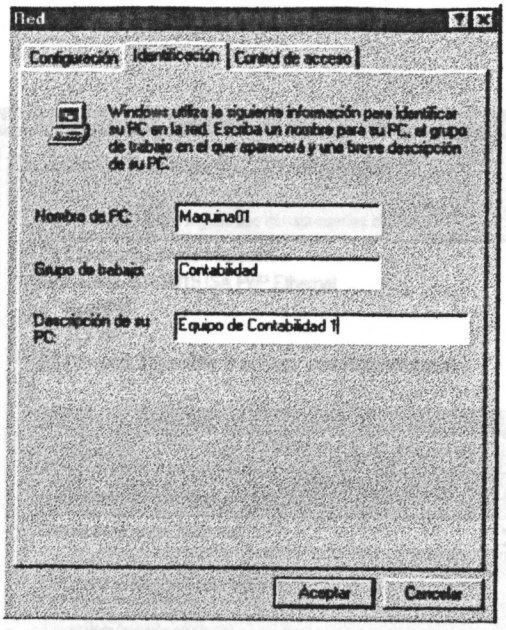


Windows 95 instala NetBEUI por defecto, y Windows 98 instala TCP/IP por defecto. Si se utilizan protocolos de red diferentes, las PCs que ejecutan Windows 95 y los PCs que ejecutan Windows 98 no se podrán comunicar entre sí.

Se recomienda que se configuren las PCs que ejecutan Windows 95 para que utilicen TCP/IP. En el cuadro de diálogo de Red, seleccione la pestaña de Configuración.

Los protocolos de red utilizados aparecen en el cuadro de lista identificados por el símbolo  . Se deberá verificar que se utiliza el protocolo correcto en cada una de las PCs de la red.

En el cuadro de diálogo de Red seleccione la pestaña Identificación.

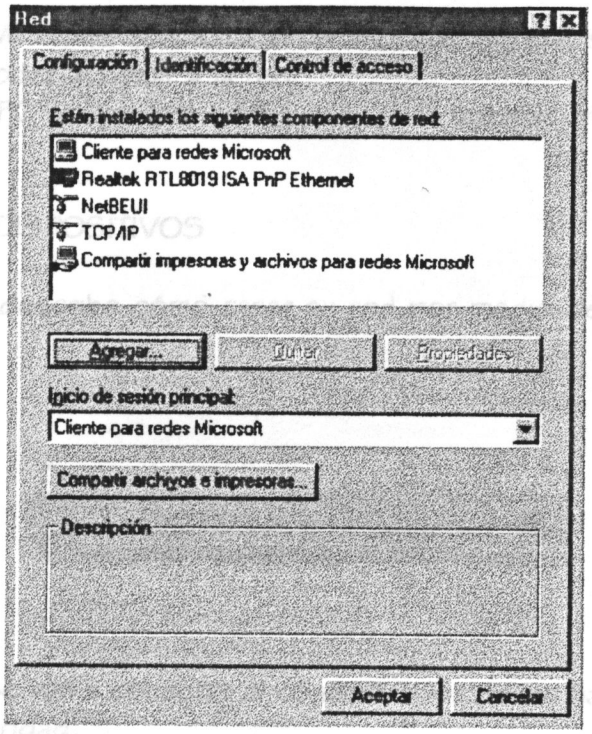


En el campo *Nombre del ordenador*, se debe escribir un nombre descriptivo para la PC. Este es el nombre que identificará a la PC en la red. Puede ser un nombre cualquiera (como por ejemplo: "Maquina01"), pero tiene que ser distinto de los nombres de las otras PCs de la red.

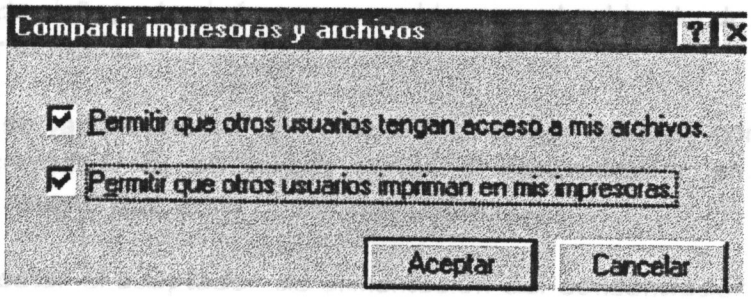
Se recomienda que se mantenga un registro de los nombres asignados a cada una de las computadoras conectadas a la red. Se debe escribir un nombre para la red en el campo del *Grupo de trabajo*. Este puede ser un nombre cualquiera, pero debe ser el mismo para todas las PCs de la red. Se recomienda apuntar y guardar el nombre del grupo de trabajo.

En la ventana del Panel de control, hacer doble click en el icono de Red.

En la pestaña de Configuración, hacer click en el botón Compartir impresoras y archivos.



En el cuadro de diálogo, Compartir impresoras y archivos, seleccionar ambas casillas.

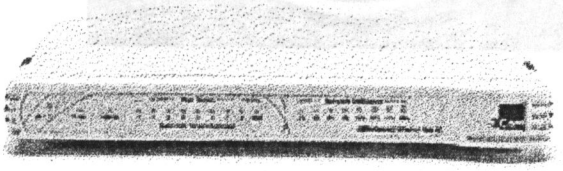


En el cuadro de diálogo de Red, asegrarse que en el cuadro de combinado de Inicio de sesión principal esté definido como *Cliente para Redes Microsoft.* Reiniciar la PC.

En el futuro, Windows solicitará al usuario que ingrese su nombre de usuario y contraseña para poder accesar a la red.
Con estos pasos la PC ha quedara configurada para trabajar en red.

12.4 INSTALANDO DISPOSITIVOS

Esta sección describe cómo crear su red por medio de la conexión de PCs al concentrador



Las PCs que se van a conectar al concentrador deben haberse configurado e instalado con anterioridad.

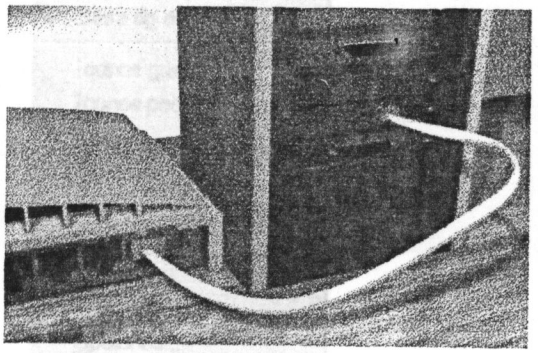
Se debe asegurar que sea un lugar adecuado en donde no pueda recibir golpes u otro tipo de daño, y también ser accesible para el cableado de las Pc que se vayan a conectar al mismo.

Las PCs que se van a conectar al concentrador deben haberse configurado e instalado con anterioridad. Si se quiere poner el concentrador en la pared, consulte la guía del usuario que viene con el dispositivo.

Hay que conectar el adaptador de alimentación del concentrador al enchufe de pared y al zócalo de alimentación del concentrador. Los LEDs del dispositivo deben iluminarse brevemente al encenderse.

10.4.1 Conectar el concentrador

Si el dispositivo está colocado y encendido correctamente, podrá conectar los PCs. Por cada PC, se debe tomar un cable de par trenzado de Categoría 5. Conectar uno de los extremos del cable al puerto RJ-45 de la tarjeta de red (NIC). Conecte el otro extremo del cable a un puerto RJ-45 en la parte trasera del concentrador.



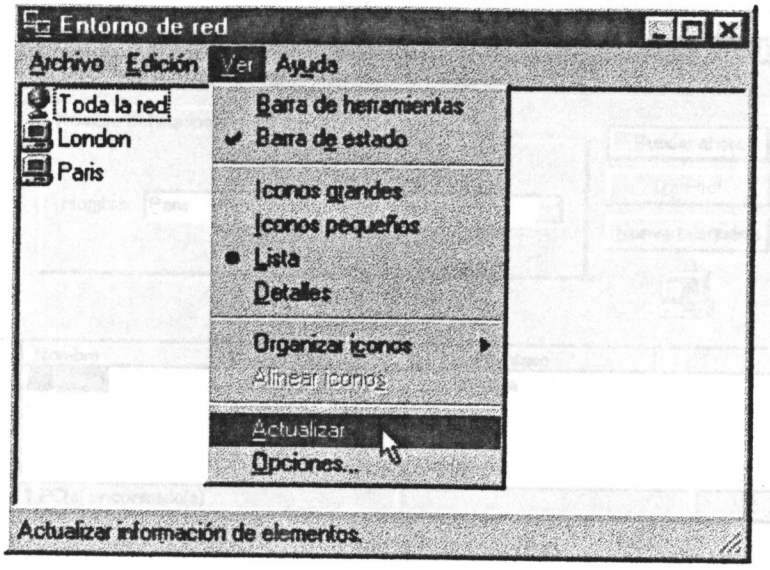
En la parte frontal del concentrador, compruebe que el LED de status esté encendido de acuerdo al número de puerto que se haya conectado.

10.4.2 Comprobar las nuevas conexiones

Las PCs deberían estar ahora conectadas a través del concentrador. Para comprobar las conexiones de red:

En una de las computadoras hacer doble click en el icono Entorno de red del escritorio de Windows. En la ventana del Entorno de red, seleccionar Actualizar en el menú Ver.

La ventana del Entorno de red deberá tener un icono por cada computadora incluida en la red.



- Si se muestran todas las PCs, estarán listas para utilizarse en la red.
- Si algunos de ellos no aparecen, esto indica que el Entorno de red no ha quedado actualizado.

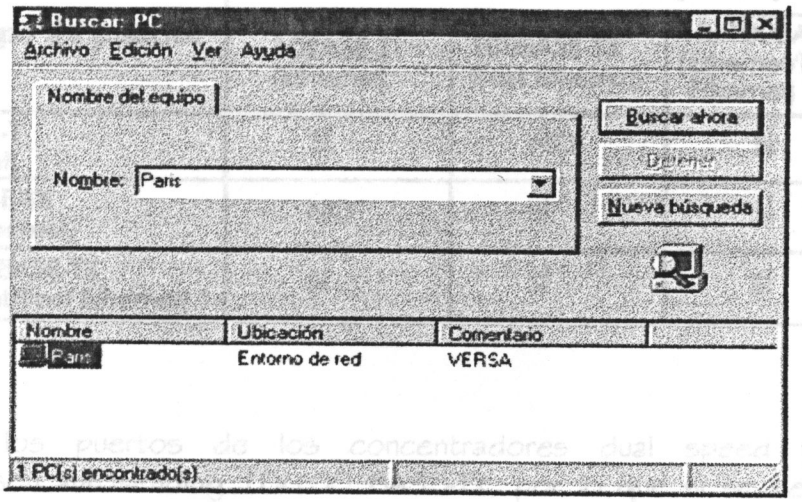
Se debe realizar la siguiente tarea para que los equipos estén conectados correctamente.

En el menú Inicio, seleccionar Buscar y a continuación PC.

En el cuadro de diálogo Buscar PC: especifique el nombre de una de las PCs que no aparecen y haga click sobre Buscar Ahora. Windows buscará la PC.

Si el sistema la encuentra, la incluirá en al cuadro de lista, dicha PC estará lista para utilizarse en la red.

Repita este proceso por cada PC que no se muestre en el Entorno de red.



Si Windows no pudiera encontrar alguna de las Pcses posible que exista un problema con la instalación de la red referente a dicha PC. Si las PCs que se encontraron en el cuadro de diálogo Buscar PC siguen sin verse en el Entorno de red, no hay ningún problema. El Entorno de red es a veces demasiado lento para mostrar los cambios realizados en la red.

10.4.3 Conectar varios Consentradores

En esta sección se describe cómo expandir la red por medio de la conexión de un concentrador a otro concentrador.

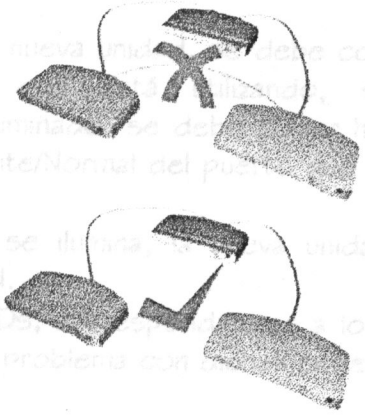
Al conectar otro concentrador a la red, se debe asegurar que el nuevo equipo es de una velocidad compatible, y que tiene puertos que pueden conectarse al concentrador existente.

La siguiente tabla muestra los tipos de puerto que se pueden conectar. Debe cumplir también con las normas de Ethernet o Fast Ethernet sobre la conexión de concentradores.

Este tipo de puerto:	Puede conectarse a este tipo de puerto:		
	10BASE-T (Ethernet)	100BASE-TX (Fast Ethernet)	10/100BASE-TX (Ethernet/Fast Ethernet) *
10BASE-T (Ethernet)	SÍ	NO	SÍ
100BASE-TX (Fast Ethernet)	NO	SÍ	SÍ
10/100BASE-TX (Ethernet/Fast Ethernet) *	SÍ	SÍ	SÍ

*Todos los puertos de los concentradores dual speed y de los conmutadores son autosending 10/100 BASE-TX, por lo que si se tiene uno de estos dispositivos, se podrá conectar cualquier componente del equipo 10BASE-T y 100BASE-TX sin preocuparse por cuestiones de compatibilidad.

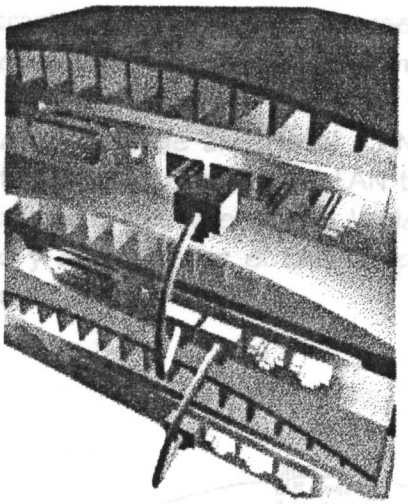
Un nuevo concentrador se puede conectar a otro concentrador existente en la red, permitiendo a todas las PCs comunicarse entre sí. Al conectar concentradores, cada unidad necesita solamente una conexión a la red. Si una unidad tiene más de una conexión, la configuración es incorrecta y se crea un bucle de red.



Para conectar la nueva unidad siga los siguientes pasos:

- Tome un cable con "empalme" de par trenzado de la Categoría 5.
- Conecte un extremo del cable a un puerto RJ-45 de la parte trasera de la unidad existente.
- Conecte el otro extremo del cable a cualquier puerto RJ-45 de la parte trasera de la nueva unidad.

Uno de los puertos debe de ser un puerto Enlace ascendente/Normal. Este puerto es habitualmente el que tiene la numeración más alta en el dispositivo.



En la parte frontal de la nueva unidad, se debe comprobar que el LED indicador del estado del puerto que está utilizando, este iluminado. Si el LED correspondiente no está iluminado, se debe pulsar hacia adentro y hacia afuera el interruptor Enlace ascendente/Normal del puerto que se haya utilizado, hasta que el LED se ilumine.

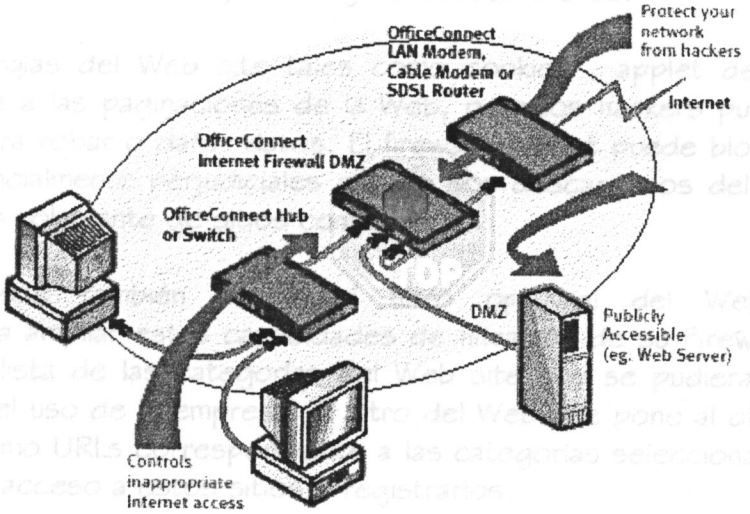
- Si el LED correcto se ilumina, la nueva unidad estará lista para utilizarse como parte de la red.
- Si algunos de los LEDs, correspondientes a los puertos utilizados, no están iluminados, existe un problema con dichas conexiones.

10.5 INTERNET FIREWAALL

El OfficeConnect Internet es una aplicación del Firewall que está instalada entre la LAN y el dispositivo de acceso a Internet , tal como un módem del LAN del ® de OfficeConnect. El Firewall Internet es un sistema completo de seguridad de red con toda la dotación física y software lógico instalados previamente. Èsto permite que actúe como Gateway, asegurando la transferencia de los datos que pasan entre el Internet y el LAN. El propósito del Firewall Internet es permitir que una red de área local privada (LAN) sea conectada con seguridad al Internet.

Usos del Firewall Internet:

- Prevenir el hurto, la destrucción, y la modificación de datos.
- Filtrar los datos entrantes para el contenido inseguro o desagradable.
- Registrar los acontecimientos que pueden ser importantes para la seguridad de su red.
- *Las fijar el acceso de la red,* de área local (LAN) a la red local a través de cubos y de interruptores. Los usuarios del LAN tienen acceso a los servicios Internet tales como E-mail, ftp, y el World Wide Web. Sin embargo, todos los sitios de trabajo y datos sobre el LAN se protegen contra los ataques del hacker que pudieran venir.



12.5.1 Características del Internet Firewall

Seguridad Del Firewall

El Firewall Internet de OfficeConnect se preconfigura para vigilar el tráfico de Internet, detecta y frustra *la negación de los ataques* del hacker al *servicio* (DoS) automáticamente.

Los ataques de DoS incluyen:

- Inundación De Syn
- Ataque De la Pista
- IP Spoofing
- Teardrop – (una herramienta del hacker de DoS que está extensamente disponible en el Internet.)

El Firewall Internet utiliza el stateful del paquete para determinar si un paquete de datos de Internet se acepta a través de la LAN privada. Los usuarios experimentados pueden ampliar las funciones de la seguridad del Firewall Internet agregando reglas del acceso a la red y privilegios del usuario.

Filtración Internet

Usted puede utilizar el Firewall Internet para vigilar y restringir a usuarios de la LAN de tener acceso a la información inadecuada sobre el Internet. Se puede crear una lista de todos los *URLs y* restringir el acceso a ellos.

Las tecnologías del Web site tales como cookies , applet de Java y de ActiveX dan realce a las paginaciones de la Web, pero los hackers pueden utilizar las tecnologías para robar o dañar datos. El firewall Internet puede bloquear estas aplicaciones potencialmente perjudiciales cuando son descargados del Internet, o permitir el acceso solamente de sitios confiados.

Usted puede también utilizar el filtro opcional del Web site de OfficeConnect para ampliar estas capacidades de filtración de su Firewall Internet. Proporciona una lista de las categorías del Web site que se pudiera considerar inadecuadas para el uso de la empresa. El filtro del Web site pone al día al Firewall Internet con el último URLs correspondiente a las categorías seleccionadas. Usted puede bloquear el acceso a estos sitios o registrarlos.

Registros y alarmas

El Firewall Internet mantiene un registro de todos los acontecimientos que se podrían considerar peligrosos para la seguridad del LAN. Puede también seguir a los acontecimientos dominantes tales como los 25 sitios alcanzados superiores del Web, se puede también instalar el firewall Internet para enviar un mensaje alerta con e-mail cuando hay peligro, tal como un ataque del hacker.

10.6 Preparar el Firewall de Internet

En esta sección se proporciona en una lista la información que usted necesita para configurar el Firewall de Internet.

Los Usuarios de Módem de cable

Si usted está usando el Firewall de Internet con un módem del cable telefónico, quizás necesite registrar la MAC address para lo cual, deberá contactar a su proveedor de servicio de teléfono antes de conectar el Firewall de Internet a su red. La MAC address del Firewall de Internet se encuentra en una etiqueta en la parte inferior de la unidad.

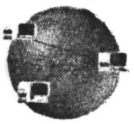
Configuración inicial que usa al Internet Firewall Wizard

El CD proporcionado con el Firewall de Internet contiene una utilidad llamada Internet Firewall Setup Wizard. El Wizard ejecuta" el Setup.exe" del CD.

El wizard asume que usted tiene una conexión de Internet activa y que el Firewall de Internet está en su estado de valor por defecto de fábrica.

Lo lleva a través de los pasos siguientes:

1 . Determine su setup de la red.
2 . Determine los settings para el Firewall de Internet.
3 . Conecte el Firewall de Internet a su red.
4 . Envíe las settings determinados en el paso 2 al Firewall de Internet.
5 . Pruebe que el Firewall de Internet se instale correctamente.



La Información requerida

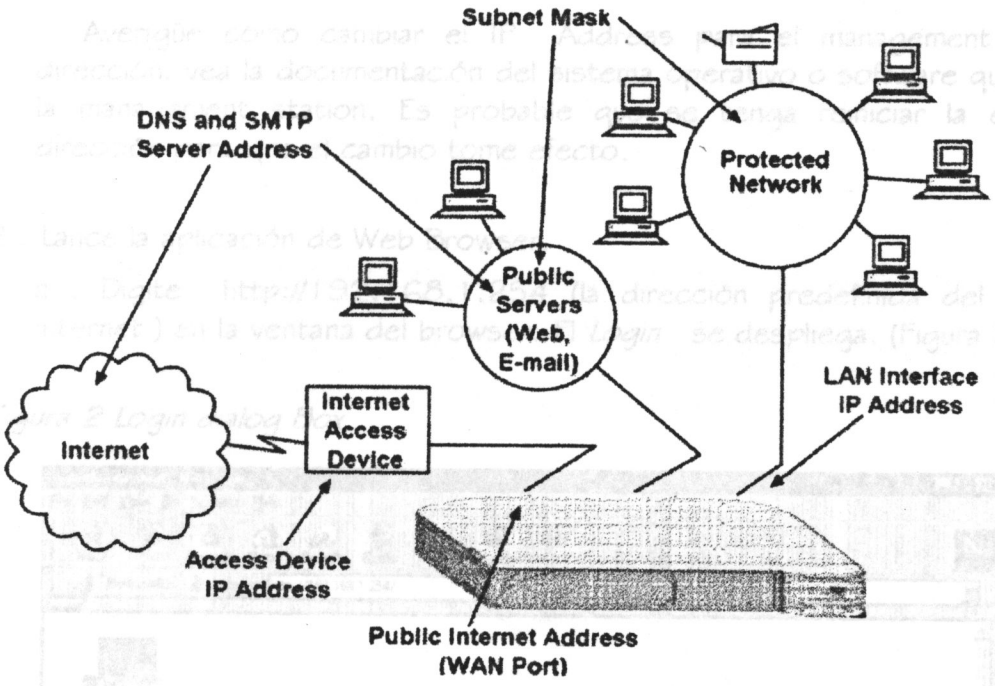
Al configurar el Firewall de Internet, usted necesita la información sobre IP de la Network. Usted puede obtener esta información del Internet Servicio Proveedor (ISP). Lo siguiente ilustra donde es utilizada esta información.

- Internet Firewall LAN Interface IP Address.
  Este es el IP Address que se usa para manejar el Firewall de Internet. La dirección se asigna al puerto de LAN. Escoja que un único IP se dirija al rango del LAN Network .
- Subnet Mask
  Este valor es para protección de la LAN y describe el rango de Direcciones de IP que pertenecen al LAN.
- IP Address de Internet para el acceso al dispositivo
  Ésta es la dirección de Internet para el acceso al dispositivo que conecta el LAN al Internet.
- La Dirección DNS para el Servidor
  Ésta es la dirección de un Nombre de Dominio Sistema servidor, y/ o puede ser para un servidor en el LAN o Internet. Ésta se requiere para transmitir actualizaciones del OfficeConnect Web Site Filter, así como para el Nombre de Lookup tool. La dirección se proporciona por el ISP.

- La SMTP Server Address (Optativo)
  Ésta es la dirección de un servidor de e - mail que se usa para enviar los mensajes, y /o puede ser para un servidor en el LAN o Internet. Es recomendable que utilice el mismo servidor que esta usando en la LAN para e - mail. Una vez que el Firewall de Internet se ha configurado, use el Nombre Lookup tool para encontrar el IP y diríjase al nombre SMTP Server.

- Public Internet Address
  Si se quiere usar Network Address Traslation (NAT), se necesita la dirección de Internet Pública. Esta dirección IP es la que se utiliza en la red entera para acceder al Internet. Esta dirección se proporciona por el ISP.

Figure 1 Donde es usada la Dirección de Información



Setting up de Internet Firewall

En esta sección se describe el setup del Firewall de Internet que usa el Web Browser.

1 . Preparando una estación de dirección.

Se puede manejar el Firewall de Internet para su Web Browser aplicando el uso del Web Management interface. Usted puede manejar el Firewall de Internet en cualquier computadora que esté conectada a la misma red como el Firewall de Internet. Cualquier computadora usada para la dirección es llamada Management Station (*estación de dirección*).

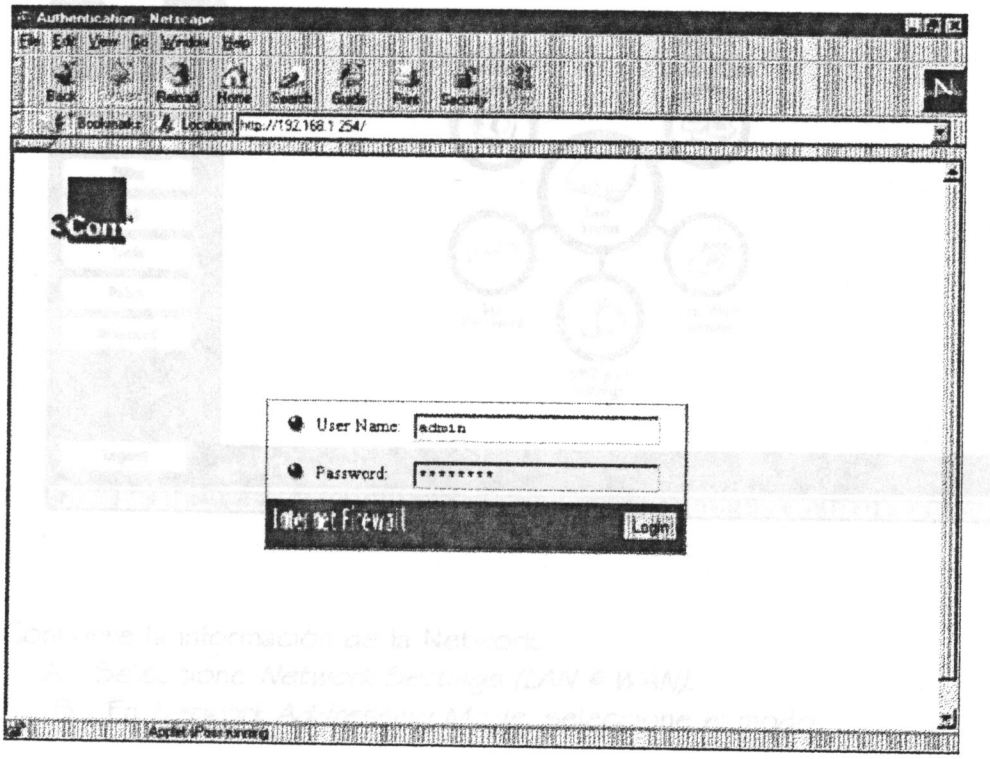
El Firewall de Internet tiene un IP Address predefinido, 192.168.1.254. Durante este setup inicial, usted debe cambiar temporalmente los IP Address de la management station a uno en el mismo subnet como el Firewall de Internet. Por ejemplo, ponga los IP Address de la estación a 192.168.1.200.

Averigüe cómo cambiar el IP Address para el management station de dirección, vea la documentación del sistema operativo o software que se usa en la management station. Es probable que se tenga reiniciar la estación de dirección para que el cambio tome efecto.

2 . Lance la aplicación de Web Browser.

a . Digite **http://192.168.1.254** (la dirección predefinida del Firewall de Internet) en la ventana del browser. El *Login* se despliega. (Figura 2)

Figura 2 Login dialog Box



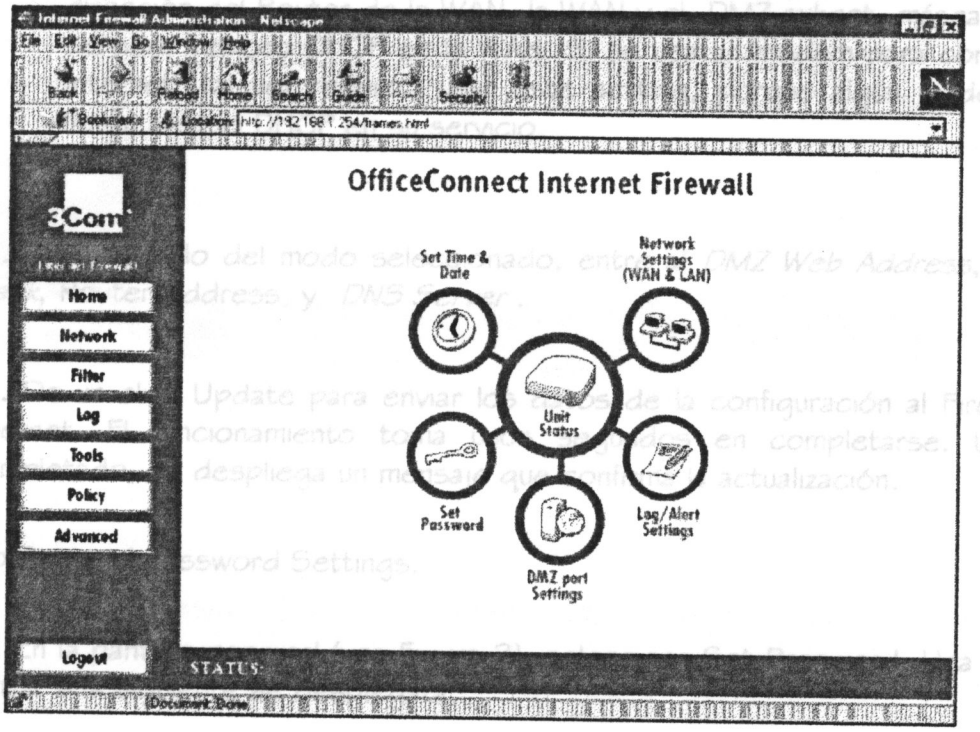
B . En el User Name, teclee el nombre del usuario predefinido: el admin

C . En el Password, teclee el password predefinido: password

D . De un Click en *Login*.

La pantalla principal del management interface se desplegará.

Figura 3 Internet Firewall Home Screen
(Ventana principal del Firewall Internet)



3 . Configure la información de la Network.

A . Seleccione *Network Settings (LAN & WAN).*

B . En *Network Addressing Mode*, seleccione el modo.

- Escoja Standard si su red no usa un IP Address privado o si usted tiene las direcciones de IP para cada máquina que requiere el acceso al Internet.

- Seleccione *NAT Enabled* si usted quiere usar un solo IP Address para acceder al Internet, si se quiere usar una direccion IP privada en la red o si no se tiene una dirección de IP para cada máquina que requiera el acceso al Internet.

- Seleccione NAT con cliente DHCP: si desea el NAT público IP Address, la dirección del Router de la WAN, la WAN y el DMZ subnet máscara de un servidor remoto DHCP en la WAN. Si se usa un módem para conectar al Internet, tal vez requiera usar este setting, porque algún módem ISPs llevan a cabo DHCP en su servicio.

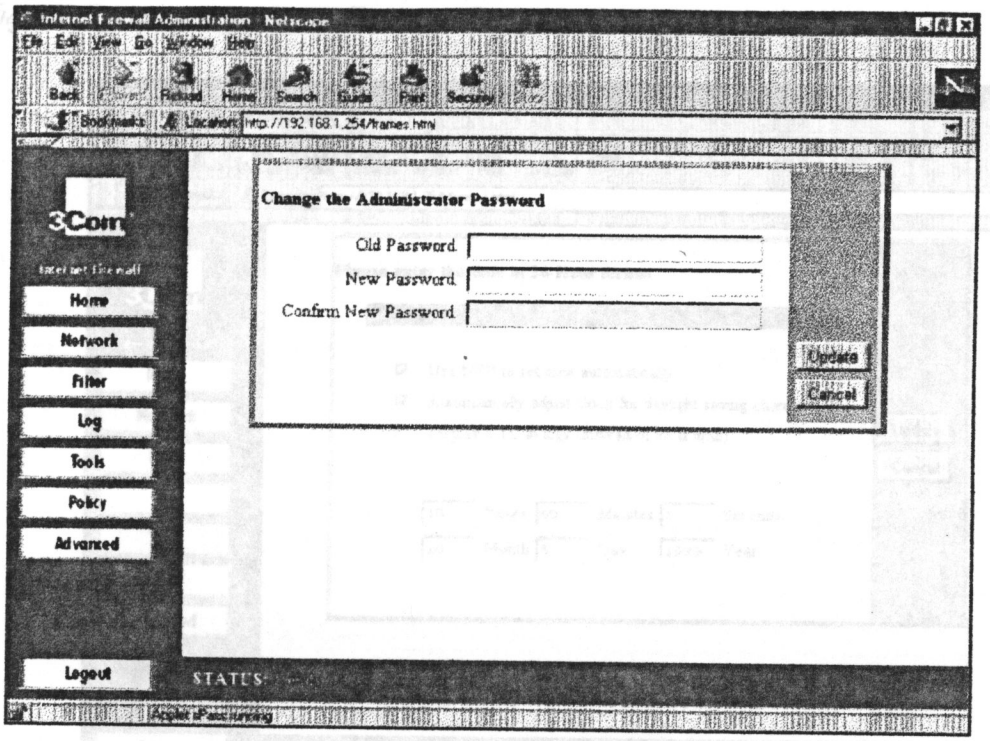
C . Dependiendo del modo seleccionado, entre al *DMZ Web Address*, *Subnet Mask*, Router Address, y *DNS Server* .

D . De un click Update para enviar los datos de la configuración al Firewall de Internet. El funcionamiento toma unos segundos en completarse. Una vez completado, se despliega un mensaje que confirma la actualización.

4 . Configure el Password Settings.

A . En la pantalla principal (vea Figura 3), seleccione Set Password. Una ventana similar a la siguiente se desplegará.

Figura 4 Cambie el Password del Administrador



B . En el Old Password, teclee el Password anterior.

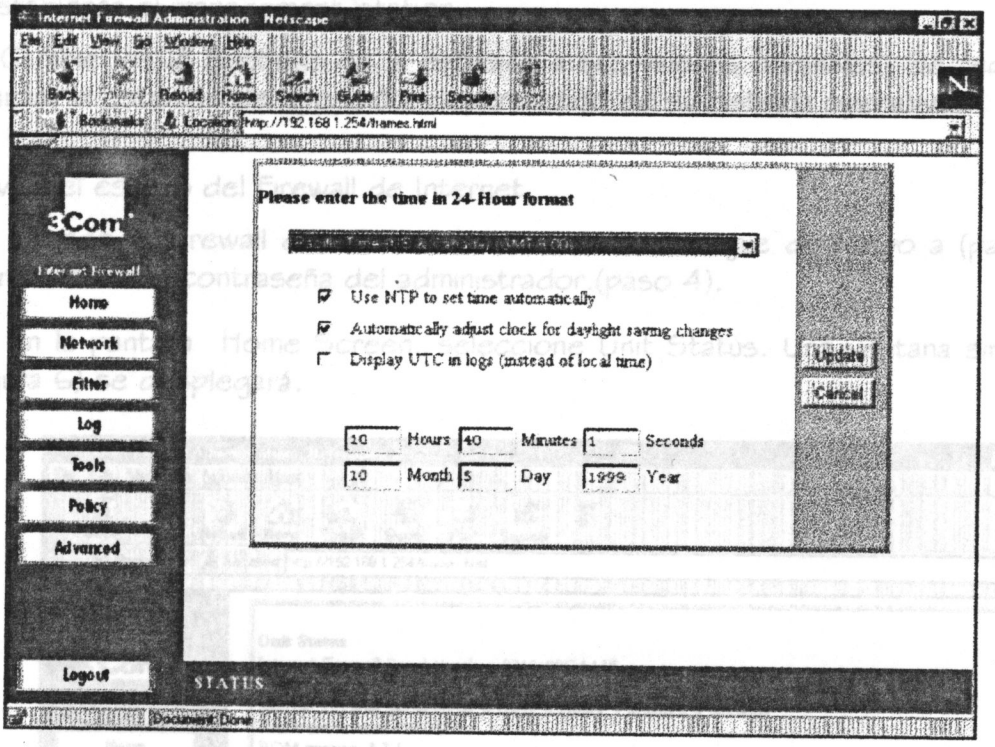
C . En el New Password y *Confirm New Password*, teclee el nuevo Password.

D . De un click en Update para enviar los datos de la configuración al Firewall de Internet.

5 . Ponga la Fecha y Tiempo.

A . En la pantalla principal (vea Figura 3), seleccione Set Date & *Time*. Una ventana similar a la siguiente se desplegará.

Figura 5 Ventana para la Fecha y Tiempo



B . Teclee el tiempo en formato de 24 - horas.

C . De click en Update para enviar los datos de la configuración al Firewall de Internet.

6 . Reinicie el Firewall de Internet.

A . De un click en Tools en el lado izquierdo de la ventana del Browser.

B . Seleccione *Restart* .

C . De un click en *Restart Firewall de Internet.*

D . De un click en yes para confirmar el Restart.

El Firewall de Internet toma aproximadamente 90 segundos para reiniciar durante este tiempo se activa el LEND. El Firewall de Internet está funcionando

Ahora y está protegiendo el LAN de Internet – de los ataques. Los Filtros de Internet no se habilita todavía.

7 . Restablezca el management Station.

Cambie los IP Settings de la estación a sus valores originales. Sé requerirá reiniciar la estación de dirección, dependiendo de su sistema operativo.

8 . Revise el estado del Firewall de Internet.

A . Cuando el Firewall de Internet ha reiniciado, navegue de nuevo a (paso 2) usando la nueva contraseña del administrador.(paso 4).

B . En la pantalla Home Screen, seleccione Unit Status. Una ventana similar a (Figura 6) se desplegará.

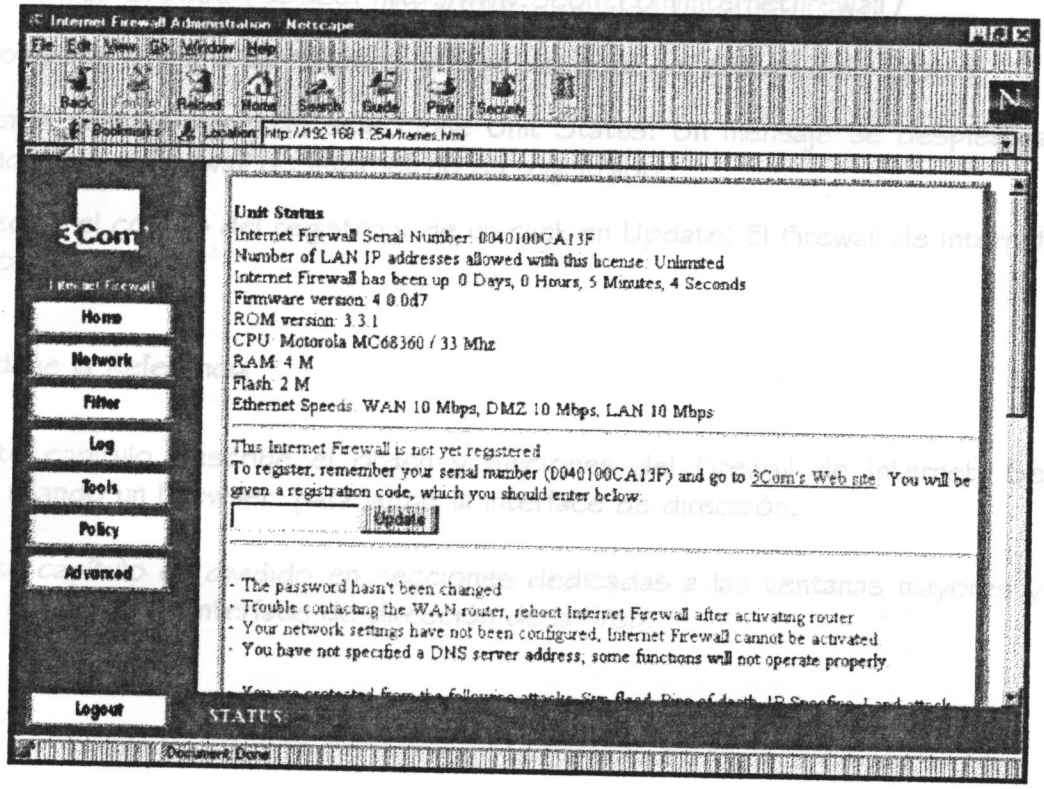


Figura 6 Ventana de Status

Esta ventana desplegara el estado actual del Firewall de Internet. Cualquier problema se enlista en texto rojo. Por ejemplo, si el Internet de acceso al dispositivo es erróneo, o la contraseña predefinida no fue cambiada, éstas se enlistan de rojo y requieren la acción inmediata, de corregirlas.

Los mensajes del estado de funcionamiento general, como protección de ataques de hackers, que se enlistan en Web Site Filter status, se encuentran en los listados back.tex.

En la ventana de *Unit Status* también muestra si el Firewall de Internet está registrado.

9 . Registrar el Firewall de Internet:

A . En el Web Browser, teclee: **http://www.3com.com/internetfirewall /**

B . Complete la forma de registro, y haga una nota del código del registro.

C . En la pantalla principal, seleccione Unit Status. Un mensaje se desplegara avisando que el Firewall de Internet no es registrado.

D . Teclee el código del registro y de un click en Update. El Firewall de Internet es ahora registrado.

12.6 Ordene la Referencia

Este capítulo describe el orden y funciones del Firewall de Internet. Se accede a usando un Browser para lanzar la interface de dirección.

Este capítulo es dividido en secciones dedicadas a las ventanas mayores y funciones dentro de la interface de dirección de la Web.

La Network Settings

En la barra opciones, de un click en Network para seleccionar el menú de Network Settings. Alternativamente usted puede usar el icono de Network Settings de Home Screen graphic.

Los Settings básicos

Pulse el botón de Label Settings *se mostrara* la ventana de Network Settings. Una ventana similar (Figura 7) se desplegará.

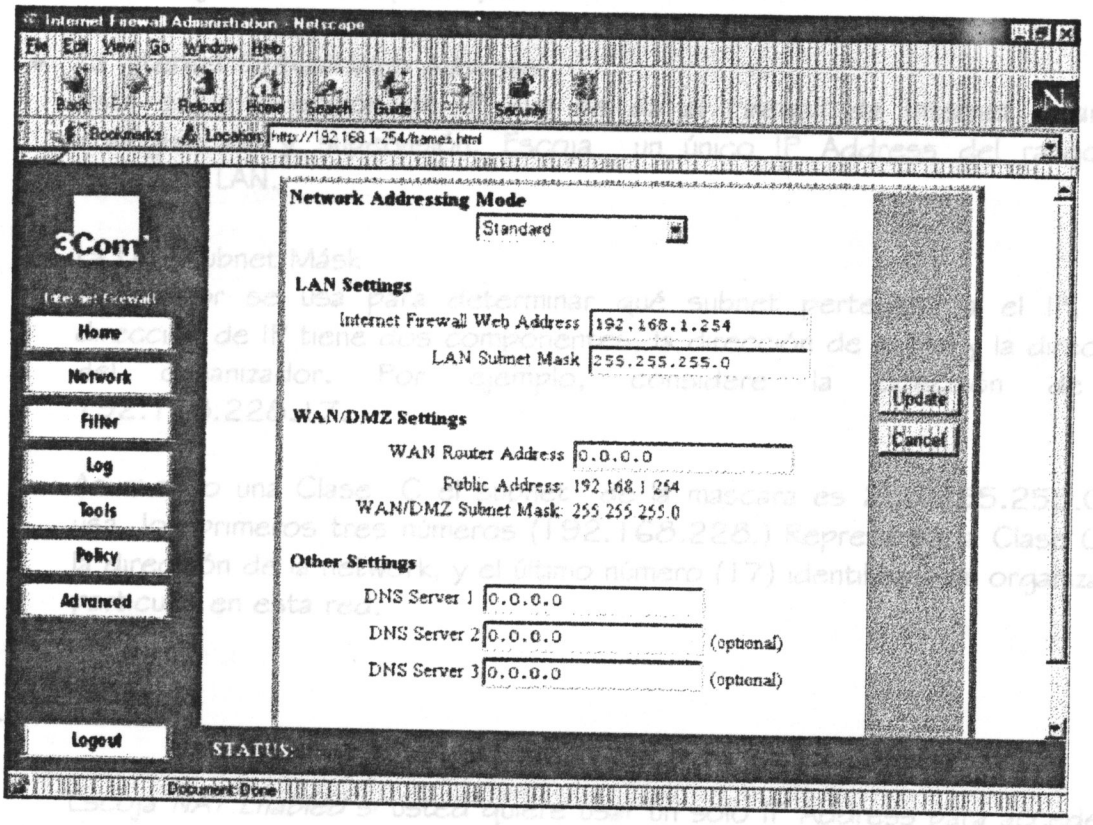


Figura 7 La Ventana de Settings de red

Settings

En Network Addressing *Mode* contiene tres modos:

1.- Standard

Ésta se emplea cuando se tiene las direcciones de IP asignadas por un ISP para cada máquina que requiere el acceso al Internet. Cuando se ha seleccionado *Standard*, *Network Address Translation* (NAT),todos los nodos en el LAN deben usar las direcciones de IP públicas válidas. La información siguiente es requerida.

Para los Settings de LAN, especifique:

- La Internet Firewall Web Address.
  Esta es la dirección de IP que se da al Firewall de Internet para la configuración y supervisión. Escoja un único IP Address del rango de dirección LAN.

- La LAN Subnet Másk
  Este valor se usa para determinar qué subnet pertenece a el IP. Una dirección de IP tiene dos componentes, la dirección de la red y la dirección del organizador. Por ejemplo, considere la dirección de IP 192.168.228.17.

  Asumiendo una Clase C el subnet de la mascara es 255.255.255.0 se usa, los primeros tres números (192.168.228.) Represente la Clase C de la dirección de la network, y el último número (17) identifica a un organizador particular en esta red.

2.- NAT Enabled

Escoja *NAT Enabled* si usted quiere usar un solo IP Address para acceder al Internet, o si usted no tiene una dirección de IP asignada por su ISP para cada máquina que requiera el acceso al Internet.

Network Address Translation (NAT), proporciona la anonimidad a las máquinas en el LAN conectanda la red entera al Internet que usa una sola dirección de IP.

Èsto es útil para dos propósitos:

- La seguridad adicional se proporciona porque todas las direcciones en el LAN son invisibles al mundo externo.
- En casos donde una red use IP inválido o direcciones para suministros cortos, NAT puede ser configurado para conectar el LAN al Internet sin cambiar las direcciones de IP de computadoras y otros dispositivos en el LAN.

El acceso autenticado remoto no es posible con NAT.

Al usar las direcciones de IP en un LAN que no se ha sido asignado por un Proveedor de servicio de Internet, es una idea buena para usar las direcciones de un rango de dirección especial para este propósito.

La siguiente dirección IP puede ser usada para IP privados en la Networks.

10.0.0.0-10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0 - 192.168.255.255

Seleccione *NAT Enabled* de Network Addressing Mode, use la dirección IP privada. Una ventana similar a (Figura 8)se desplegará.

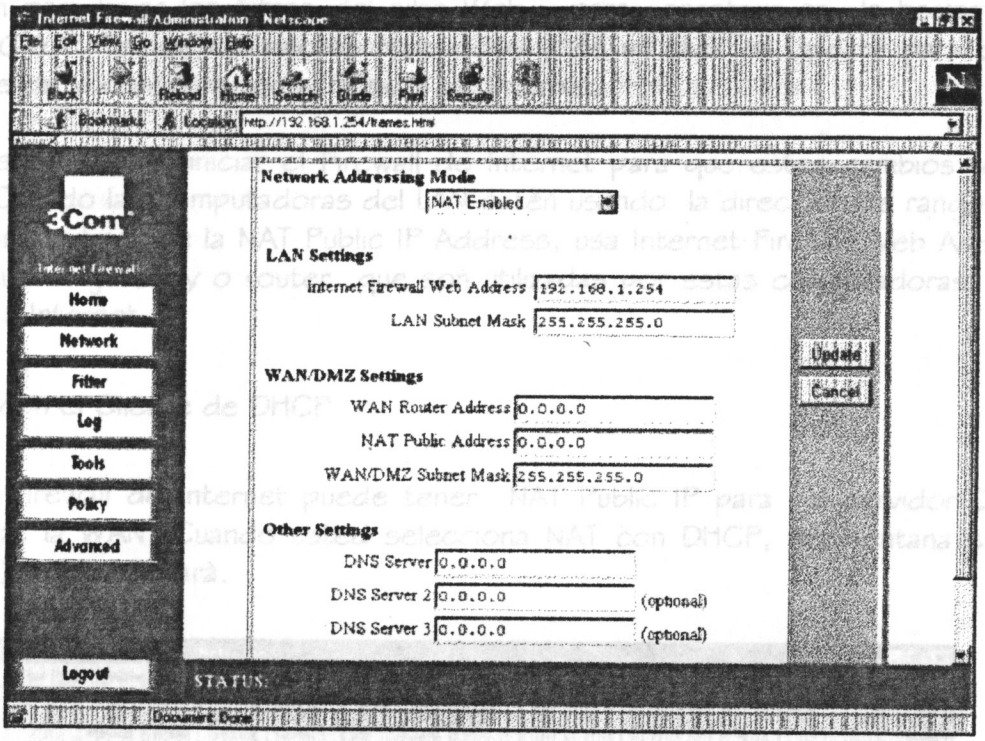


Figura 8 La Ventana de Settings Network, NAT Enabled,

Para los settings de LAN, especifique:

- La dirección de Internet Firewall

  Ésta es la dirección de IP que da a la interfaz del Firewall de Internet LAN y es usado para acceder y configurar el monitoreo. Elija una única dirección de IP para el rango del LAN.

- La LAN Subnet Másk

  Este valor se usa para determinar qué subnet e IP es al que pertenece. Una dirección de IP tiene dos componentes, la dirección de la red y la dirección del organizador.

Para Other Settings, especifique el *DNS Servers*. Estos servidores son empleados por el Firewall de Internet para mostrar las direcciones de las máquinas

que usan para bajar los filtros del sitio Web y para construir en la herramienta *DNS LOOKUP*. Teclee los valores requeridos y dé un click en Update para enviar los datos de la configuración al Firewall de Internet.

Usted debe reiniciar el Firewall de Internet para que estos cambios tomen efecto. Cuando las computadoras del LAN estén usando la dirección de rangos ,no es la misma subnet de la NAT Public IP Address, usa Internet Firewall Web Address por default el gateway o router que son utilizadas por estas computadoras para acceder a Internet.

3.- NAT con el Cliente de DHCP

El Firewall de Internet puede tener NAT Public IP para el servidor DHCP remoto de la WAN. Cuando usted selecciona NAT con DHCP, una ventana similar (Figura 9) se desplegarà.

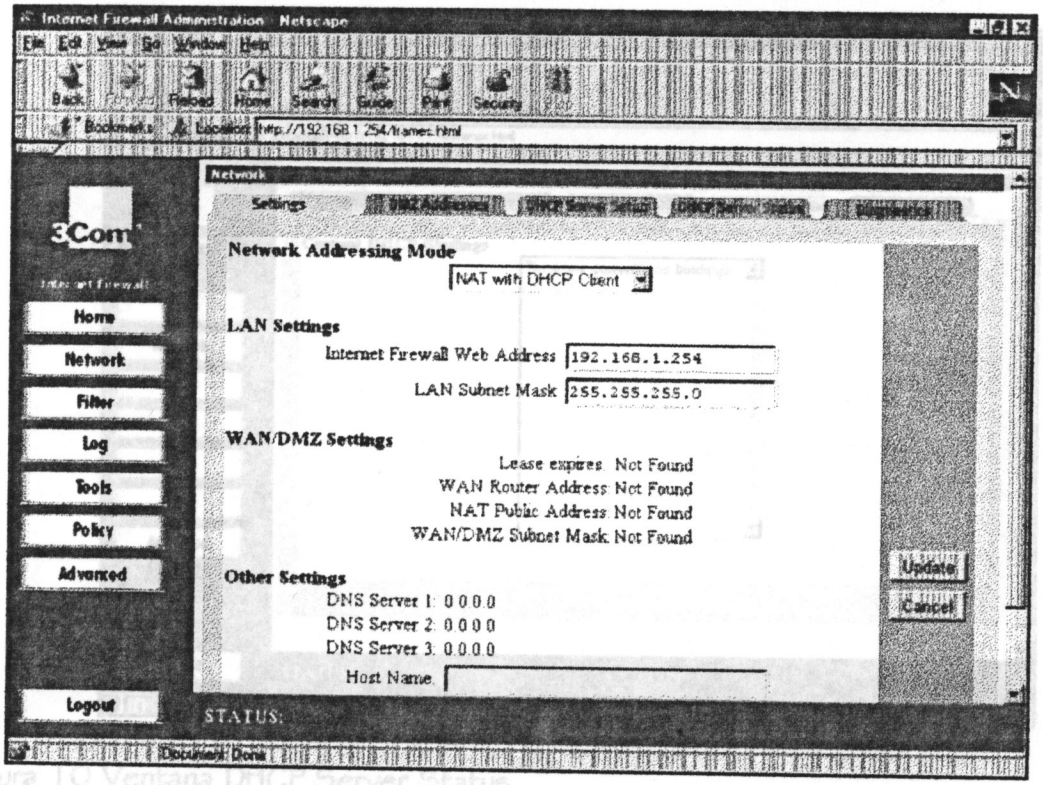


Figura 9 La Ventana de Settings de la Network, NAT con el Cliente de DHCP,

Teclee los valores requeridos y de un click Update para enviar los datos de la configuración al Firewall de Internet. Usted debe reiniciar el Firewall de Internet para que estos cambios tomen efecto. Cuando las computadoras en el LAN estén usando una dirección que no va en el mismo subnet como el NAT la dirección de IP Pública, use la Internet Firewall Web Address como la entrada predefinida al gateway o router address .

El DHCP Servidor de Estado

De click en Network y seleccione el *DHCP Server Status*. Una ventana similar(figura 10) se desplegará.

La ventana del desplazamiento muestra los detalles actuales:

- IP y MAC address
- El tipo de ligar (Dynamic, Dynamic BootP, o Static BootP).

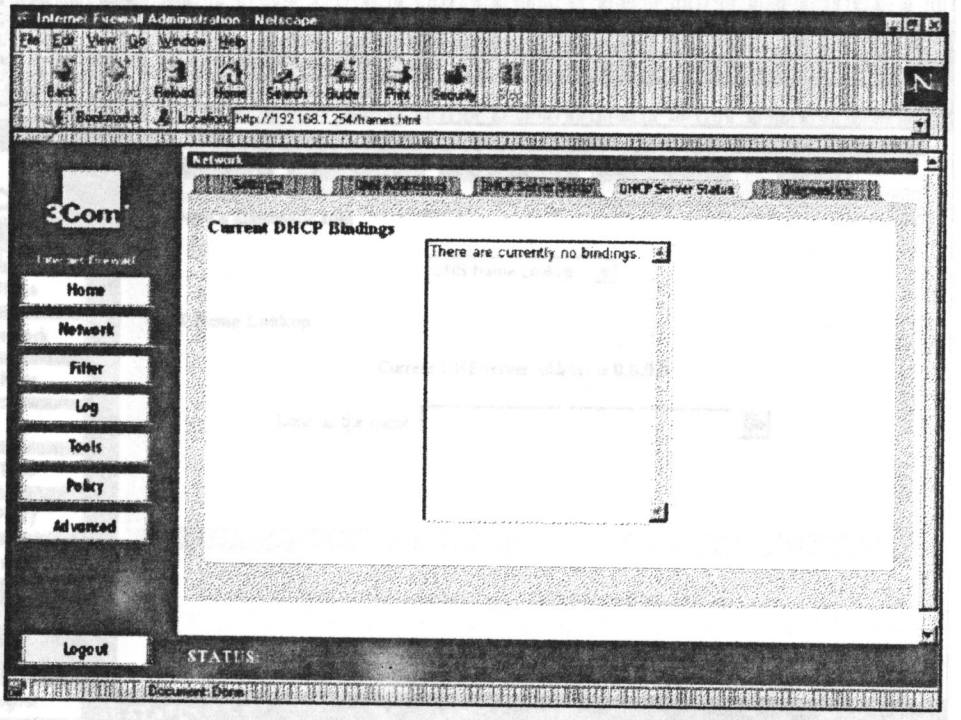


Figura 10 Ventana DHCP Server Status

Herramientas de Diagnóstico

El Firewall de Internet tiene varias herramientas construidas que son útiles para resolver los problemas de la red. Dé un click en Network y seleccione Diagnostics.

DNS Name Lookup

El Internet tiene un servicio llamado *Servicio de Nombre de dominio* (DNS) que permite a los usuarios entrar en un nombre del organizador fácilmente recordado, como **www.3Com.com**, en lugar de las direcciones de IP numéricas para acceder los recursos de Internet. El Firewall de Internet tiene un *DNS LOOKUP* (herramienta que devuelve la IP dirección numérica de un nombre de host).

Seleccione *DNS Name Lookup* del Choose a *Diagnostic tools del* menú. Una ventana similar a (Figura 11) se desplegará.

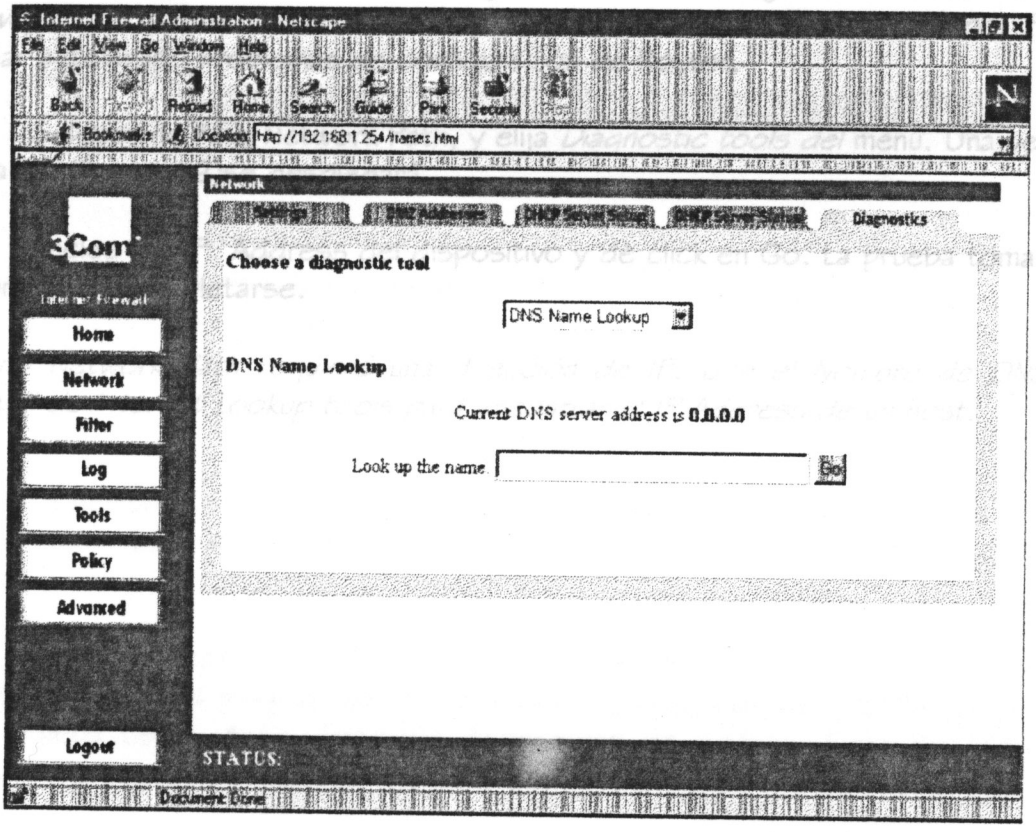


Figure 11 Ventana DNS Lookup

Teclee el nombre del Host al lookup y dè click en *Go*. El Firewall de Internet entonces requerirá del servidor DNS y desplegará el resultado al fondo de la pantalla.

La dirección IP del servidor DNS debe estar presente en la etiqueta Network Settings para que funcione correctamente.

Find Network Path

Utilice la herramienta Find Network Paht para mostrar el puerto, LAN, WAN o DMZ, y el IP del Host. Siendo útil para determinar si el Firewall de Internet se configura propiamente.

El Find Network Path también muestra si el nodo designado está detrás de una router, y si los Ethernet se dirigen del nodo designado o router. *El Find Network Path* también muestra el router del nodo que se está usando. Puede ayudar a aislar los problemas de configuración de Router.

Seleccione Find Network Path, y elija *Diagnostic tools del* menú. Una ventana similar a (Figura 12)se desplegará.

Teclee los IP Address del dispositivo y dè click en Go. La prueba toma unos segundos en completarse.

El Find Network Path requiere una dirección de IP. Use el Nombre de DNS del Firewall de Internet Lookup tools para encontrar el IP Address de un host.

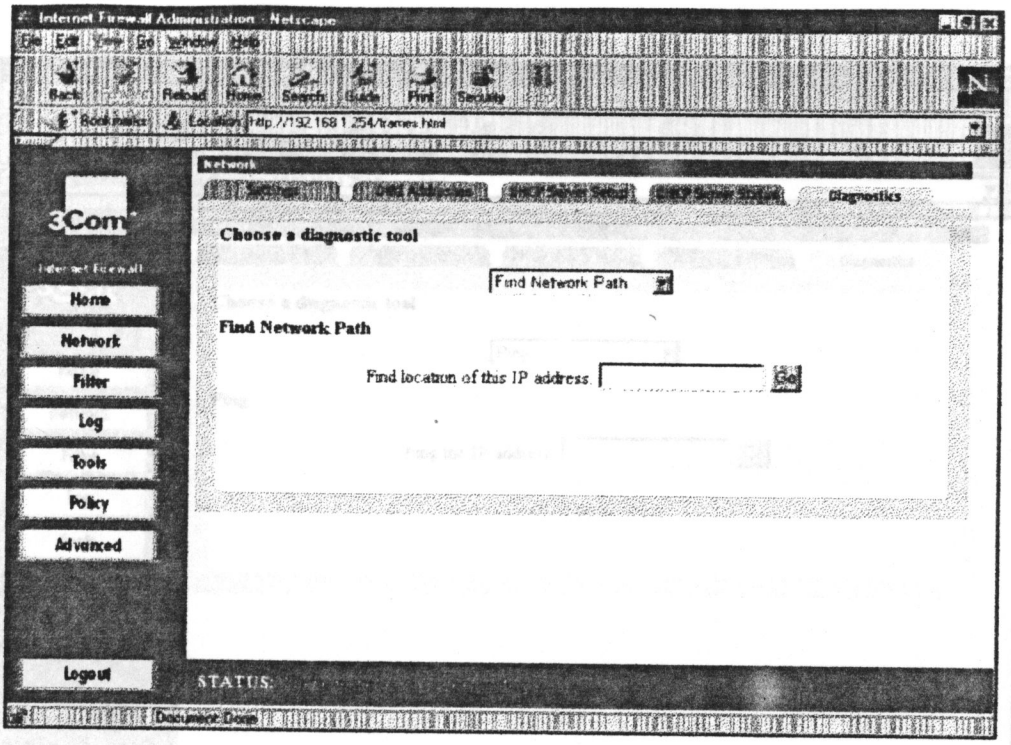


Figure 12 Ventana Find Network Path

El Ping

La herramienta Ping rechaza un paquete fuera de una máquina en el Internet al remitente. Esta prueba muestra si el Firewall de Internet puede avisar al host remoto.

Si los usuarios en el LAN tienen problemas para acceder a los servicios de Internet, pruebe el pinging del DNS server , u otra máquina ISP`s location. Si esta prueba tiene éxito, trate los dispositivos de pinging fuera del ISP. Esto muestra si el problema queda con la conexión del ISP`s.

Seleccione *El Ping* y elija *Diagnostic tool* del menú. Una ventana similar a(Figura 13) se desplegará.

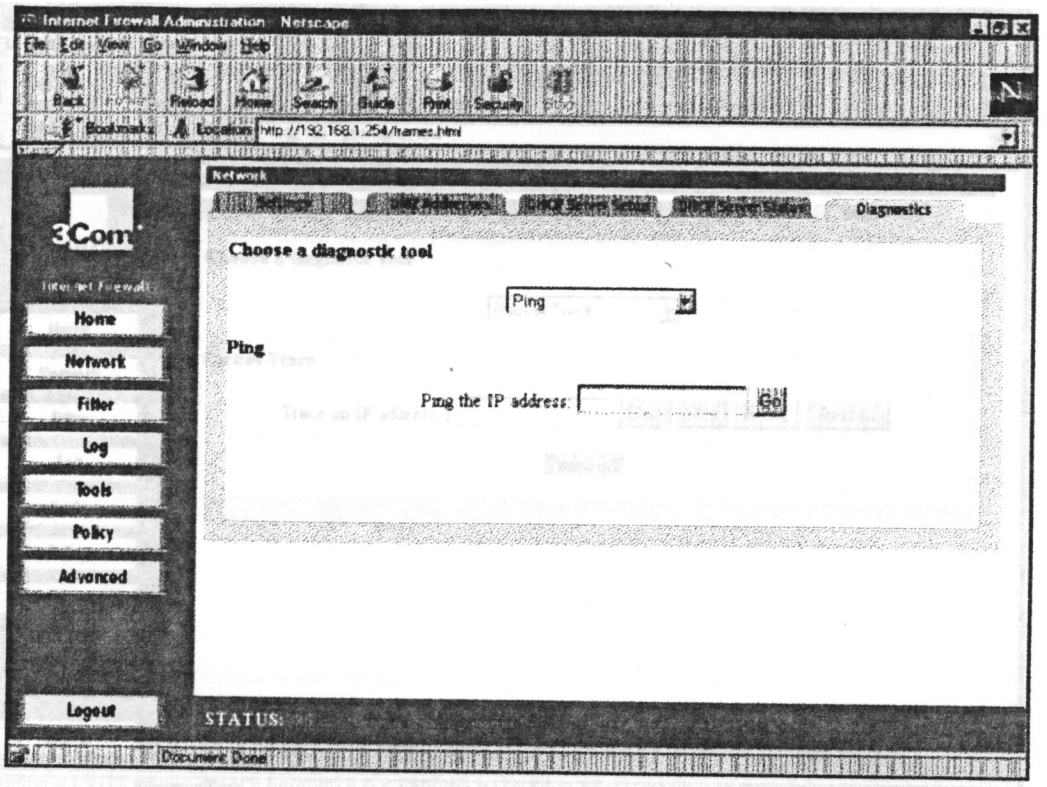


Figure 13 Ventana de Ping

Teclee los IP Address del dispositivo que es ping y dé un click en Go. La prueba toma unos segundos en completarse.

El Ping requiere una dirección de IP. Use el Nombre de DNS del Firewall de Internet Lookup tools para encontrar el IP Address de un host.

Packet Trace

Ésta es una herramienta útil para determinar si un paquete o el arroyo de comunicaciones está deteniéndose en el Firewall de Internet, o está perdido en el Internet.

Seleccione Packet Trace y *escoja Diagnostic tool.* Una ventana similar a (Figura 14)se desplegará.

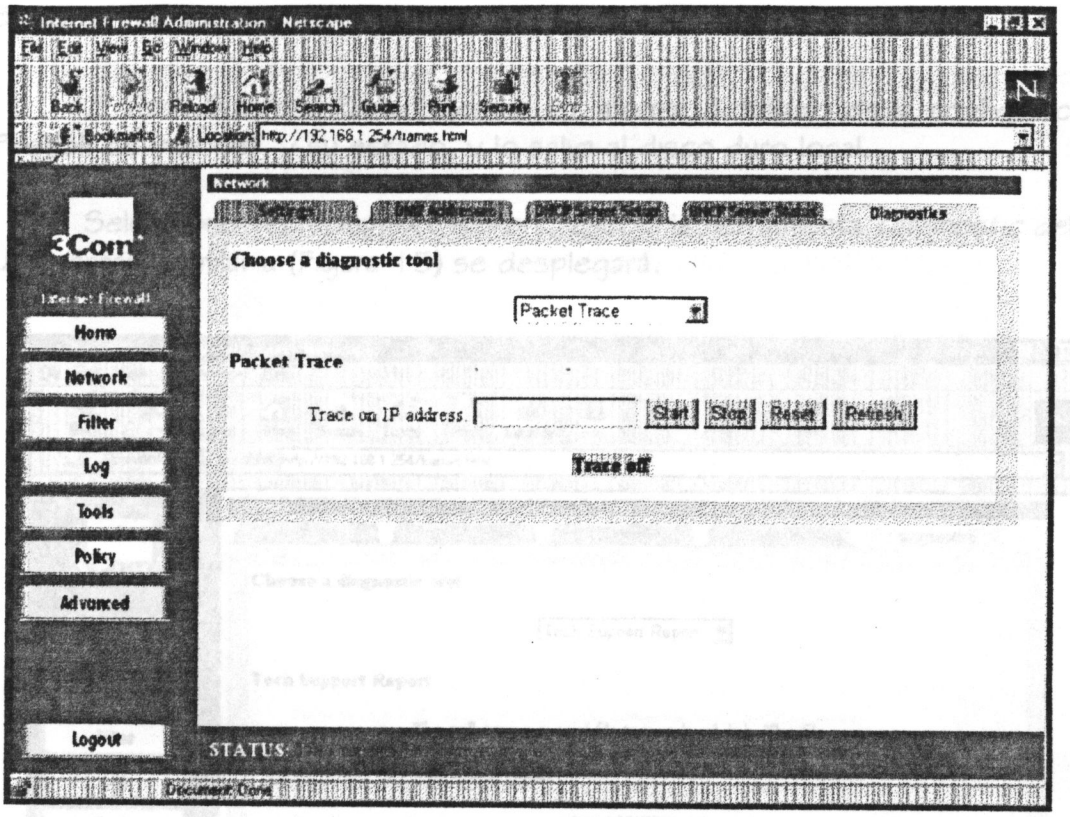


Figure 14 Ventana Packet Trace

El Packet Trace requiere una dirección de IP. Use el Nombre de DNS del Firewall Internet Lookup tool para encontrar el IP Address del hots.

1 . Introduzca los IP Address al host remoto en el Trance IP address, y dé un click Star.

2 . Comience una sesión de IP con el host remoto, usar IP de un cliente, como Web, FTP, o Telnet.

Use los IP Address en el Trance en *IP Address*, no un nombre de host, como **www.3Com.com.**

3 . Dé un click en *Refresh* para desplegar la información de rastro de paquete.

4 . Dé un click en Stop para terminar el rastro del paquete, y *Reset* para limpiar los resultados.

Soporte Técnico de Reportes

El Tech Support Report genera un informe detallado de la configuración del Firewall de Internet y su estado, y lo salva al disco duro local.

Seleccione Tech Support Report, *Escoja* la herramienta *Diagnostic* del menú. Una ventana similar a (Figura 15) se desplegará.

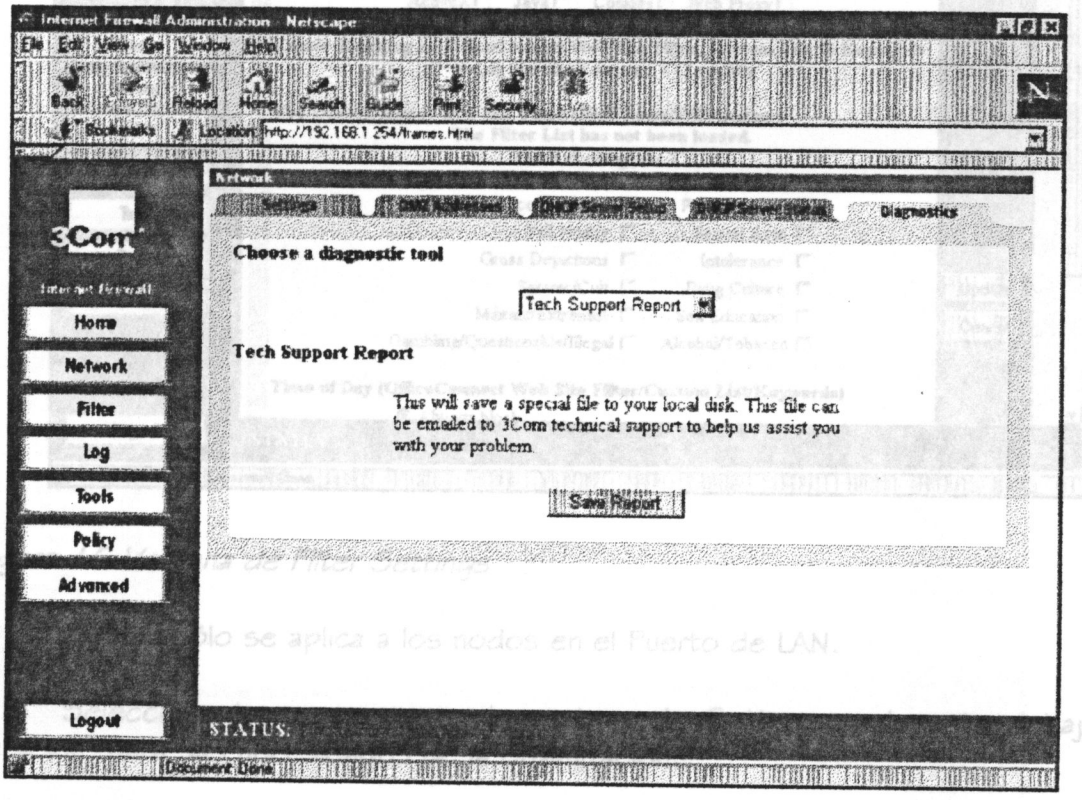


Figure 15 Ventana de Soporte técnico de Reportes.

Dé un click en Save Report para guardar el informe como un archivo del texto al disco local.

Filter Settings

Dé un click en Filter, y seleccione Settings. Una ventana similar a (Figura 16) se desplegará.

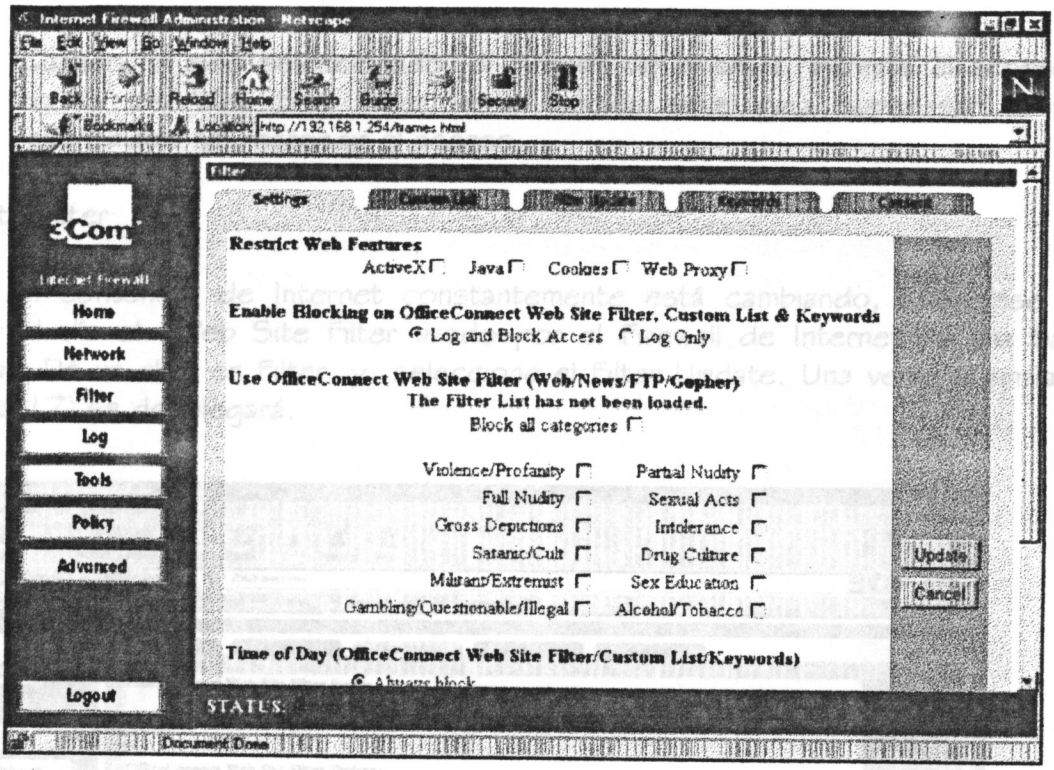


Figure 16 Ventana de Filter Settings

El filtro sólo se aplica a los nodos en el Puerto de LAN.

Seleccione las opciones en la ventana de Settings , descrita debajo la filtración para las necesidades de la organización.

Blocking Options

Puede escoger los accesos a ActiveX,Java. Cookies,Web Proxy . Así como bloquear:

- *Log and Block Acces*
  Cuando ha sido seleccionado, el Firewall de Internet Bloquea todos los sitios en Web Site Filter.

- *Log Only*
  Cuando ha sido seleccionado, el Firewall de Internet, permite el acceso a todos los Web Site Filter, esta función sirve para supervisar el uso inapropiado sin restringir el acceso.

Update Filter

El contenido de Internet constantemente está cambiando, asegúrese de poner al día el Web Site Filter usado por el Firewall de Internet en una base regular. Dé un click en Filter, y seleccione el Filter Update. Una ventana similar a (Figura 17) se desplegará.

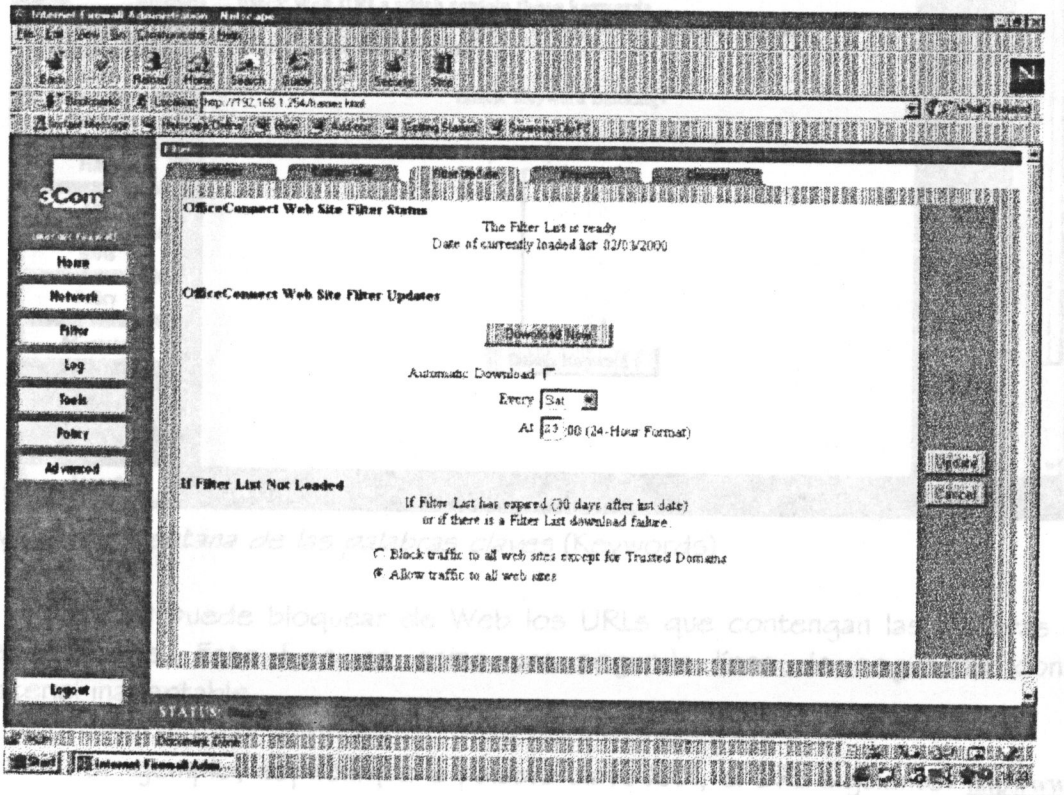


Figure 17 Ventana de Actualización de filtro

Cuando usted subscribe al Web Site Filter, usted puede especificar que se ponga al día todas las semanas automáticamente durante un año.

Keywords

Dé un click *en Filter* y seleccione Keywords. Una ventana similar a (Figura 18)se desplegará.

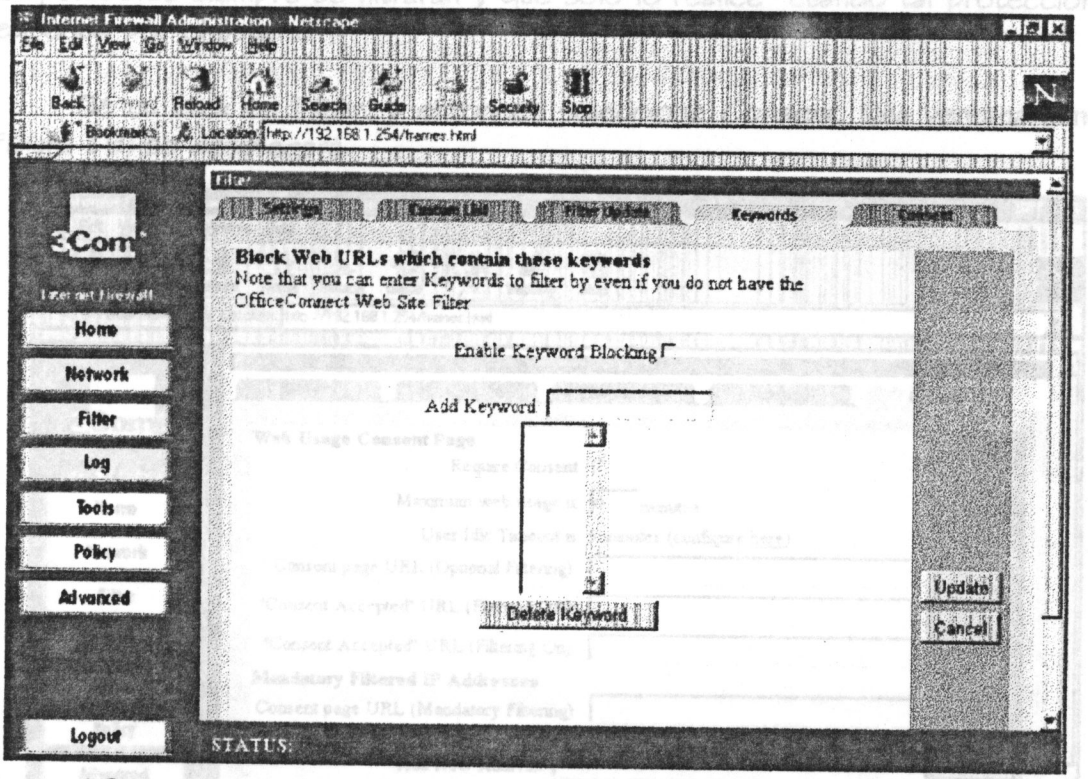


Figure 18 Ventana de las palabras claves (Keywords)

Usted puede bloquear de Web los URLs que contengan las palabras claves especificadas. Esto funciona como una segunda línea de seguridad contra el material inaceptable.

Por ejemplo, especifique la palabra clave XXX, el URL siguiente: http://www.new-site.com/xxx.html, se bloqueará, aun cuando no es incluido en el Web Site Filter. Para habilitar esté dé un click en Enable Keyword Blocking y click en Update.

Para agregar una Keyword, en el Add Keyword Blocking, y teclee la Keyword y pulsar el botón Update. Para quitar una Keyword, selecciónelo de la lista y dé un clic Delete Keyword

Consentimiento

Esta página debe residir en el Web Server y deben ser accesible como un URL para los usuarios de la LAN. Use el Consent para especificar qué computadoras siempre se filtrarán y que sólo lo realice cuando tal protección sea requerida por el usuario.

Dé un click en Filter, y entonces seleccione *Consent*. Una ventana similar a (Figura 19) se desplegará.

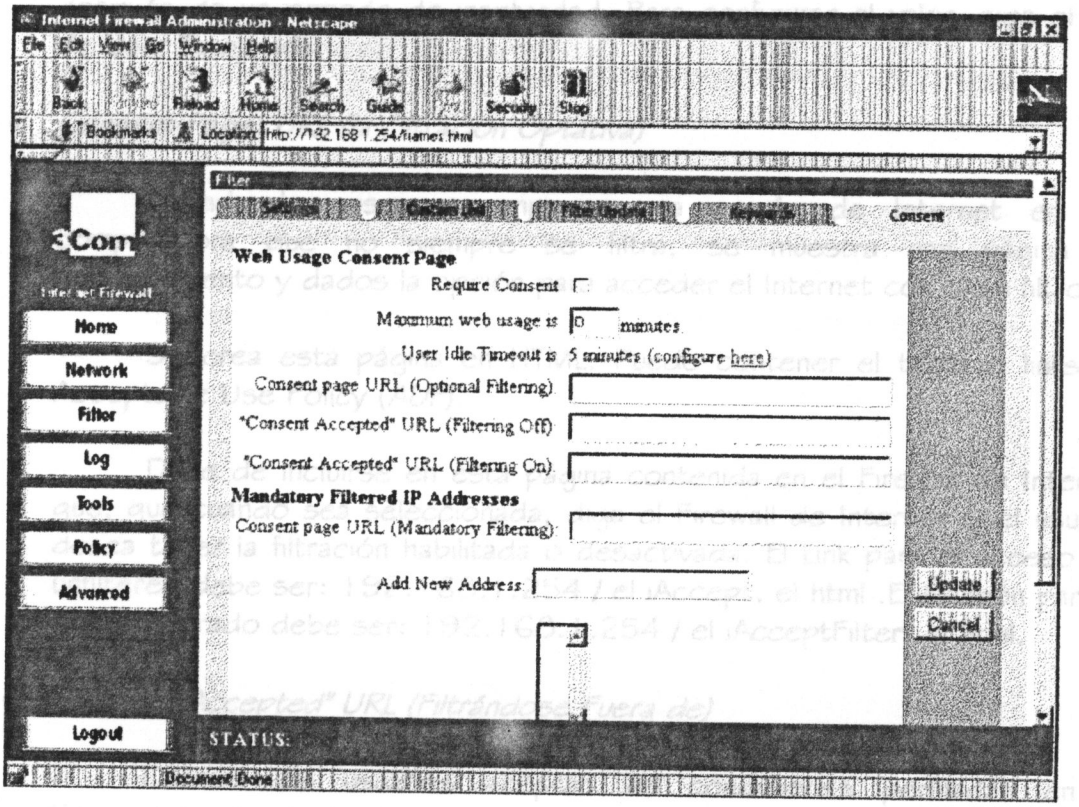


Figure 19 La Ventana de consentimiento

- *Require Consent*

  Se utiliza para habilitar el Consentimiento.

- *Maximun Web Usage*

  Se aplica en un ambiente en dónde hay más usuarios que las computadoras, como una aula o biblioteca, imponiendo los límites de tiempo.

- *User idle Timeout*

  El Firewall de Internet le exige al usuario que acepte las condiciones después de un periodo de inactividad. Para configurar el valor, siga el Link de User Privileges.

- *Consent Page URL (la Filtración Optativa)*

  Cuando los usuarios empiezan una sesión de Internet en una computadora que no siempre se filtra, se muestra una página de consentimiento y dados la opción para acceder el Internet con o sin filtro.

  Se crea esta página en HTML. Puede contener el texto o links de Acceptable Use Policy (*AUP*).

  Debe de incluirse en esta página contenida en el Firewall de Internet que, que cuando sea seleccionada, diga el Firewall de Internet si el usuario desea tener la filtración habilitada o desactivada. El Link para el acceso del unfiltered debe ser: 192.168.1.254 / el iAccept. el html .El eslabón para el acceso filtrado debe ser: 192.168.1.254 / el iAcceptFilter. el html.

- *"Consent Accepted" URL (Filtrándose Fuera de)*

  Cuando los usuarios aceptan las condiciones perfiladas en el Consentimiento de la página y escoge acceder el Internet sin la protección del filtro.

- *"El consent Acepted" URL (Filtrándose Adelante)*

Cuando los usuarios aceptan las condiciones perfiladas en la página de Consentimiento y escogen acceder el Internet con la protección del filtro.

- *El consented page URL (la Filtración Obligatoria)*

Cuando los usuarios empiezan una sesión de Internet en una computadora donde filtrarse es obligatorio, se muestran una página de consentimiento. Usted crea esta página, y puede agregar el texto de la Política del Uso Policy, y notificación de las violaciones del AUP.

Teclee el URL de esta página en el URL de la pagina de Consent *(la Filtración Obligatoria)* y dè un click en Update para enviar los datos de la configuración al Firewall de Internet.

- *Add New Address*

Usted puede configurar el Firewall de Internet para que siempre proporcione con seguridad la filtración a las computadoras en el LAN.

El Tipo las direcciones de IP de estas computadoras en el Add New Address y dè un click en *Sobmit.*

Logs Alerts

El Firewall de Internet mantiene eventos Logs que pueden ser las preocupaciones de seguridad. Usted puede ver este log con un Browser que usa el Firewall Internet. Si se quiere ser alertado de la información de prioridad, como un ataque en un servidor, usted puede especificar que esta información sea inmediatamente mandada al correo principal usado por el log, o a una dirección diferente, como un servicio de la paginación.

Dé un click en Log y seleccione View Log. Una ventana similar a (Figura 20)se desplegará.

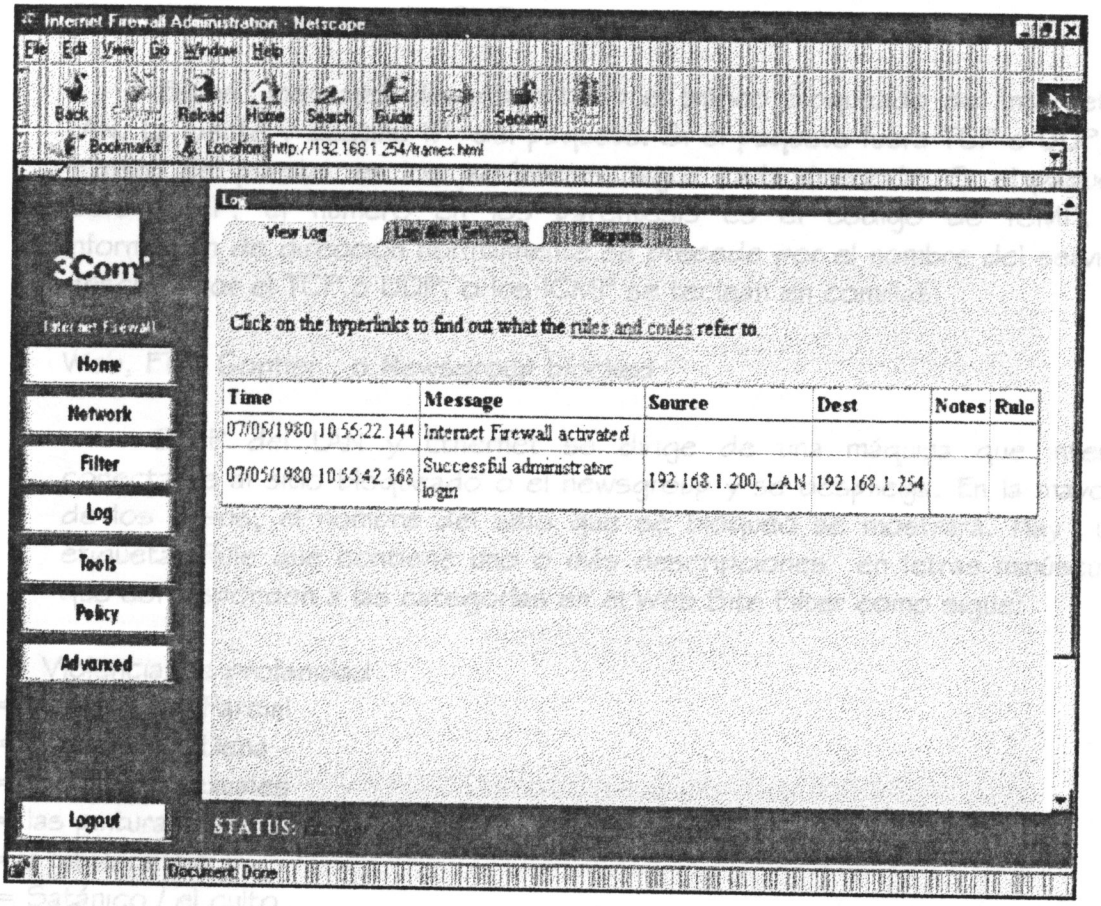


Figura 20 Ventana Log

El log despliega una lista en una tabla, pero puede aparecer diferente dependiendo del Browser. Es probable que tenga que ajustar el tamaño del conjunto de caracteres del Browser y otras características para desplegar los datos del log con mayor eficacia. Dependiendo del Browser, usted puede copiar las entradas del log y puede pegarlos en los documentos. Alternativamente, use la funcion e-mail *Log* y revise el log e_mail cliente con un Web Browser.

Cada entrada del log contiene la fecha y tiempo del evento, y un mensaje breve que describe el evento. Algunas entradas contienen la información adicional. Mucha de esta información se refiere al tráfico de Internet que atraviesa el Firewall de Internet.

- TCP, UDP, o paquetes de ICMP

  Estos mensajes describen todo el tráfico bloqueado del Internet al LAN. La fuente y destino IP del paquete. Si el paquete fuera TCP o UDP, el número del puerto, en los paréntesis, sigue cada dirección. Si el paquete fuera ICMP, el número en los paréntesis es el código de ICMP. La información de dirección normalmente se precede por el nombre del servicio descrito por el TCP o UDP, o los ICMP se teclean en comillas.

- Web, FTP, Gopher , o Newsgroup blocked

  El IP del LAN y Ethernet se dirige de una máquina que intenta conectarse al sitio bloqueado o el newsgroup y se despliega. En la mayoría de los casos, el nombre del sitio que se bloqueó se mostrará. Hay una etiqueta, Rule que contiene uno o más descripciones en letras minúsculas que corresponden a las categorías en el Web Site Filter como sigue:

un = Violencia / la profanidad
b = la desnudez Parcial
c = la desnudez Llena
d = los actos Sexuales
e = las pinturas Gruesas
f = la Intolerancia
g = Satánico / el culto
h = la cultura de Droga
i = Militante / extremista
j = la educación del Sexo

- ActiveX, Java, o Code Archive Blocked: La dirección IP de la fuente (máquina) y el servidor del destino se muestran.
- Bloqueó de las Cookie: El IP de la máquina local y el servidor remoto es mostrado.
- El Ping of Death, IP Spoof, y SYN Flood Attacks: Los IP se dirigen de la máquina del destino que puede estar bajo el ataque, así como la dirección de la fuente que aparece en el paquete. En estos ataques, la dirección de la fuente mostrada está normalmente limitada y no puede usarse para determinar la fuente del ataque.

Reiniciar el Firewall de Internet

Para reiniciar el Firewall de Internet:

1 . Dé un click en Tools y selecciona el Restart. Una ventana similar a (Figura 21) se desplegará.

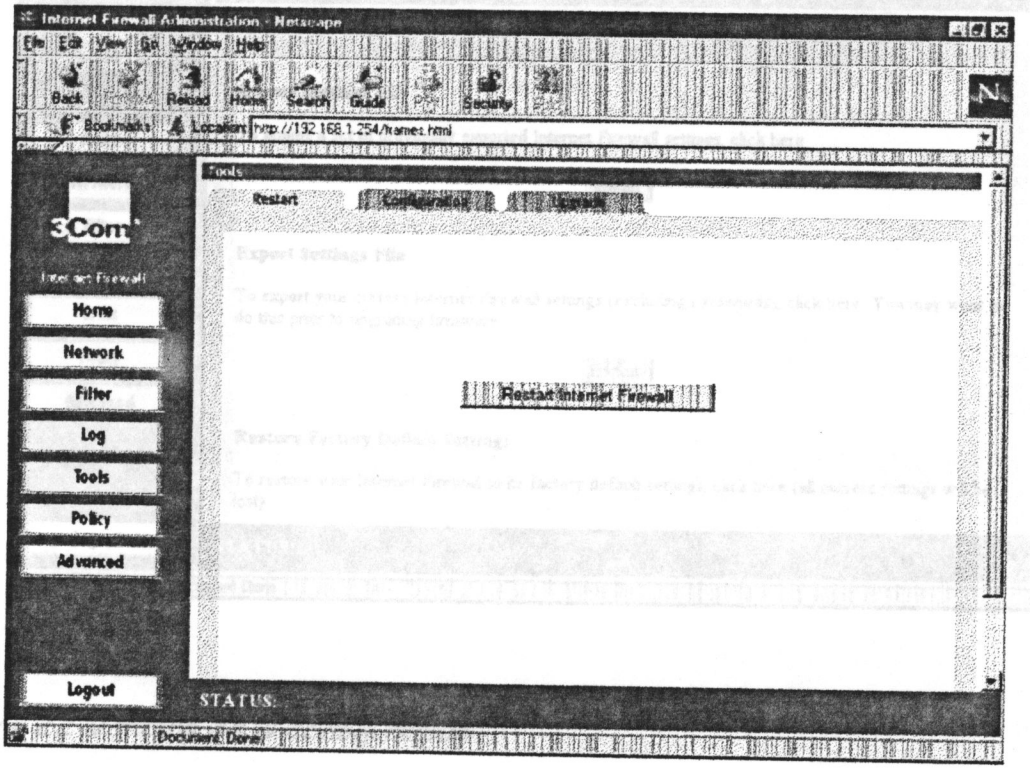


Figura 21 Ventana de Reiniciar

2 . Dé un Click en *Restart Firewall de Internet.*

3 . Dè un click en Yes para confirmar el Restart y envíe el Restart al Firewall de Internet. El restart toma aproximadamente 90 segundos, durante ese tiempo el Firewall de Internet no puede usar el Web Browser y todo el trafico de la red se detiene. Cuando el LED deje de flashear debe de dar refresh a su Browser.

Salvando y Restaurando la Configuracion de los Settings

Dé un clic en tools y seleccione Configuration. Una ventana similar a (Figura22)se desplegará.

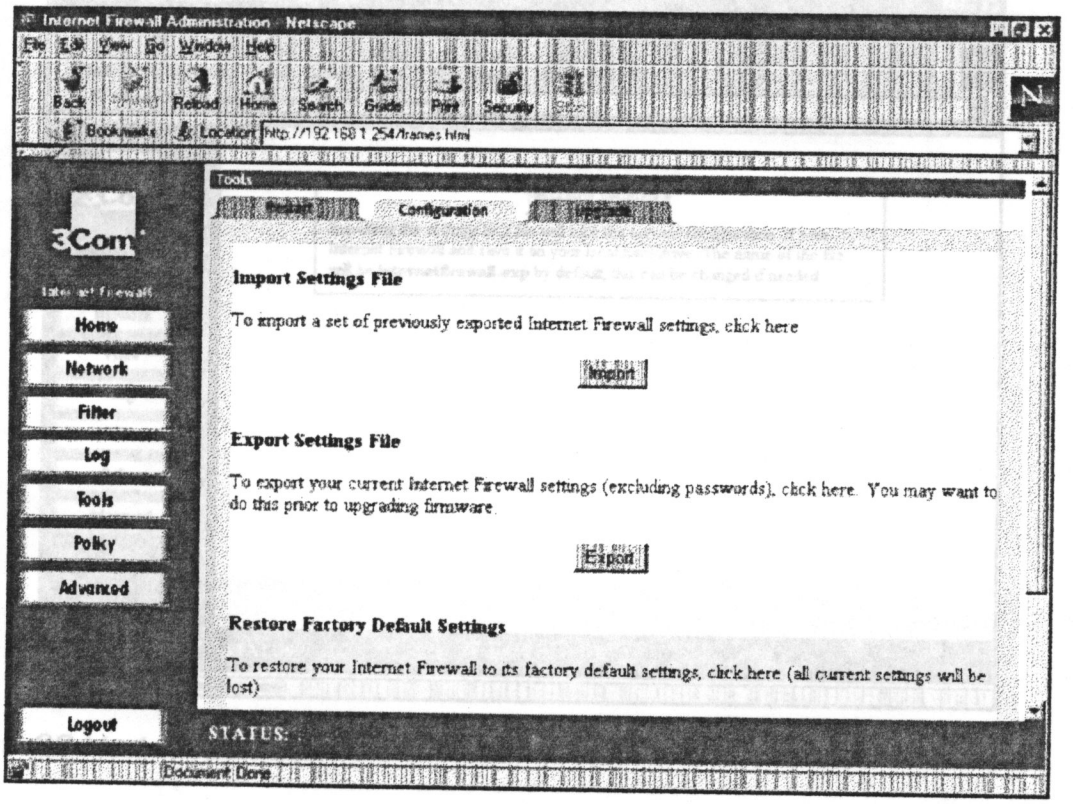


Figura 22 Ventana de la configuración

Use el Configuration para especificar en donde se salvarán y recuperarán los respaldos de los settings para el Firewall de Internet. Usted también puede restaurar los settings predefinidos del Configuration.

Especificación del Archivo de Exportación

Se puede salvar el Internet Firewall en configuración settings en un archivo de sistema local y puede recargar esos settings.

Dé un click en Export. Una ventana similar a (Figura 23) se desplegará.

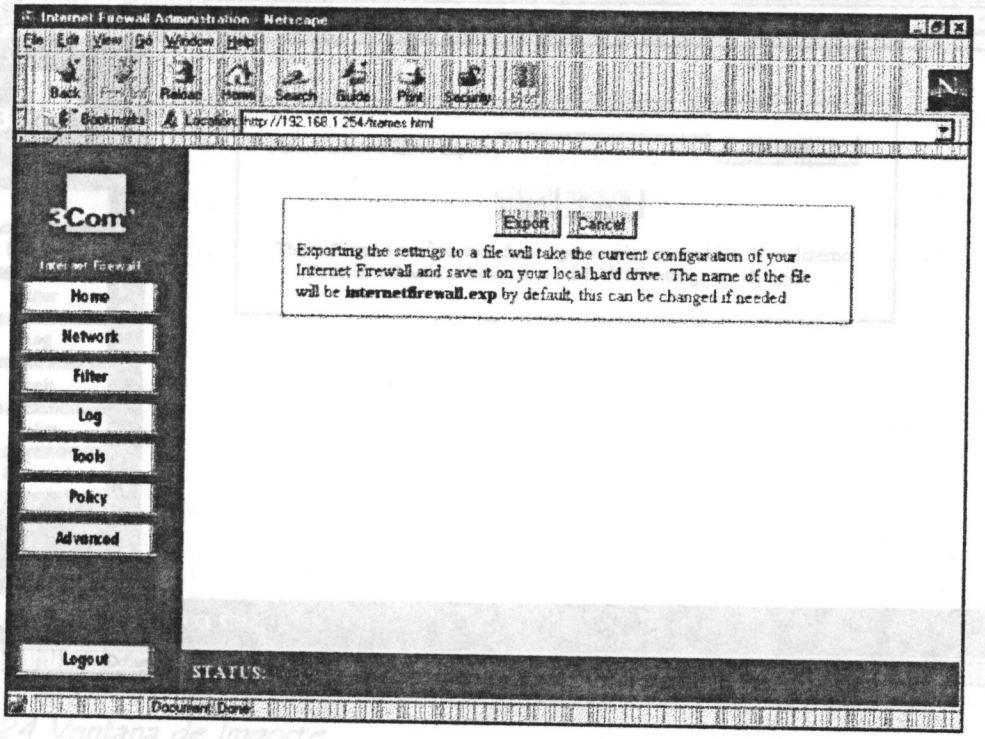


Figura 23 Ventana de Export

Escoja la locación de salvar los settings. Esto debe salvarse como < Filename >.exp. Esto es por default a internetfirewall.exp. El proceso en subirlos toma un minuto.

Recargando los Settings

Después de exportar un archivo de settings, usted puede importarlo al Firewall de Internet.

Dé un click en Import. Una ventana similar a (Figura 24) se desplegará.

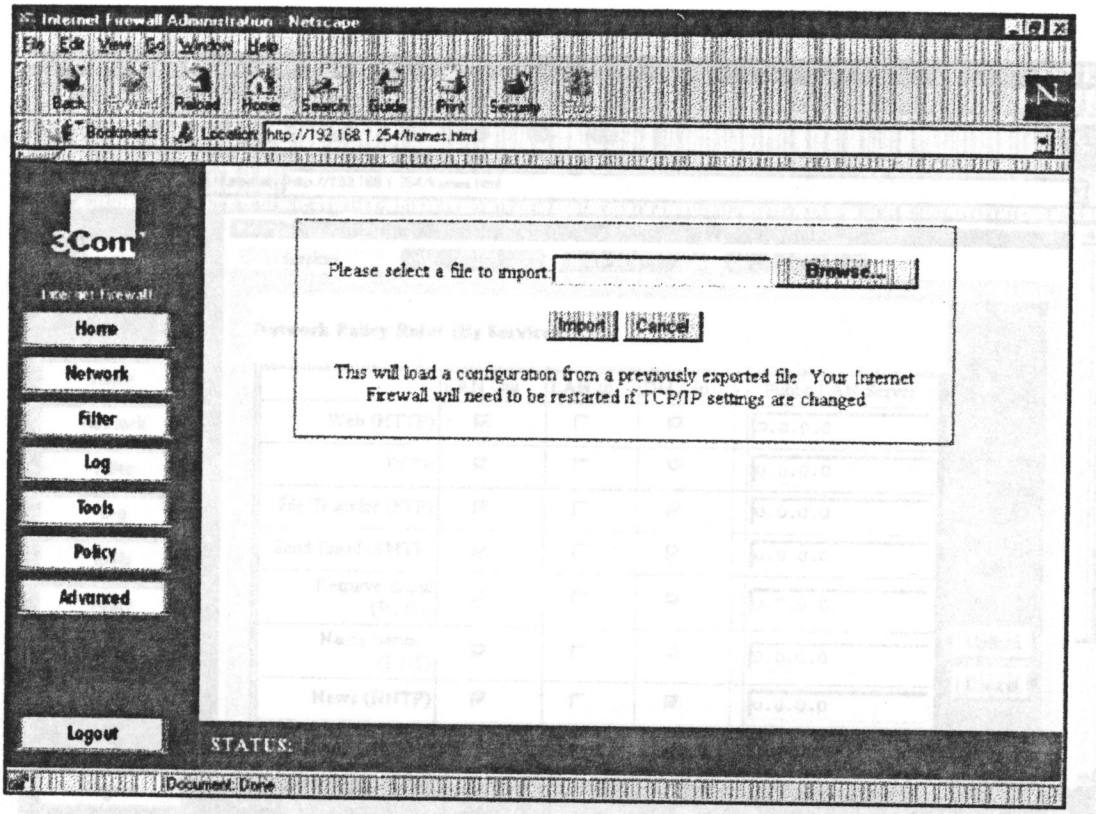


Figura 24 Ventana de Importe

Dé un click en Browser para encontrar el archivo que fue salvo usando previamente Export Una vez que se ha seleccionado el archivo, dé click en, Export y reinicie el Firewall de Internet para que los settings tomen efecto .

Policy

Esta sección cubre los servicios de red y restricciones del Firewall que permiten el acceso a través de un pasword.

Servicios

Haga click en Policy, y después seleccione Services.

Una ventana similar a (Figura 25) se desplegará.

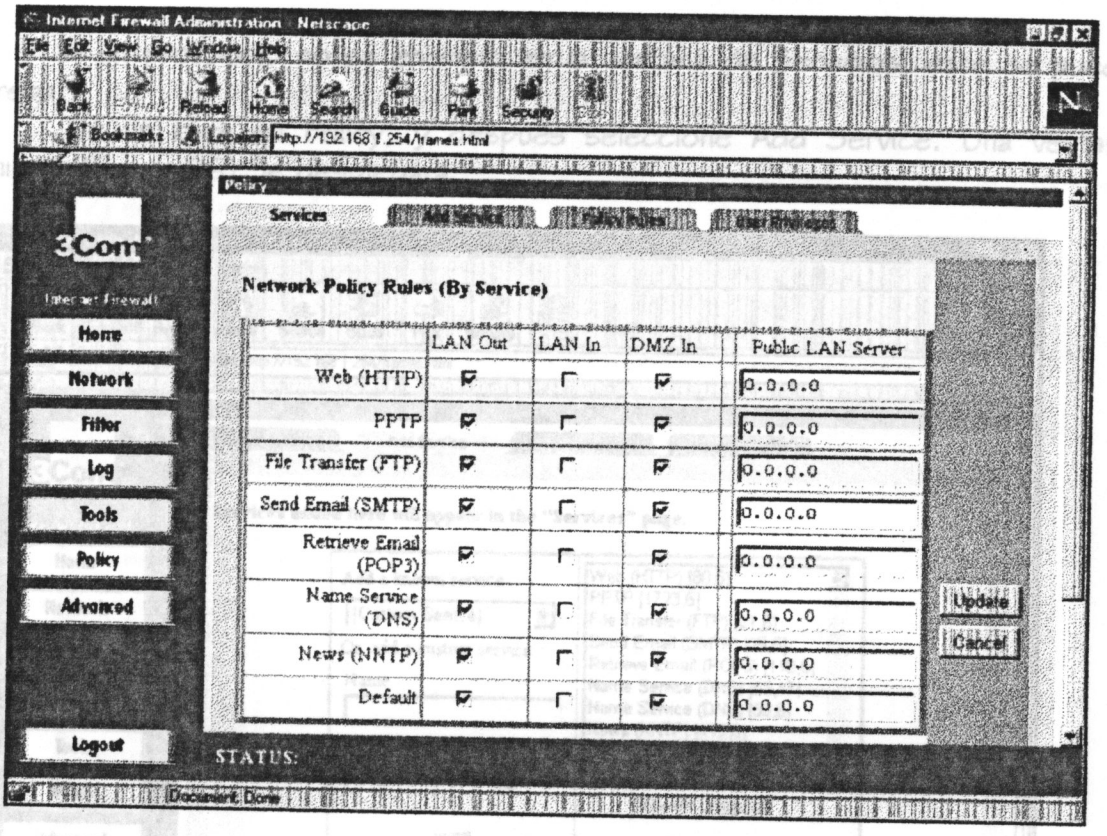


Figura 25 Ventana de Servicios

La ventana de Servicios contiene un vector que muestra las reglas de acceso de la Network. Las reglas se clasifican del más específico, al más general.

En el fondo del vector está la regla del valor por defecto. La regla del valor por defecto son todos los servicios del IP.

Usted puede crear reglas para reemplazar el comportamiento de la regla del valor por defecto. Por ejemplo, la regla del valor por defecto permite que los utilizadores en el LAN tengan acceso a todos los servicios Internet, incluyendo noticias del NNTP. Sin embargo, el acceso del LAN al NNTP puede ser bloqueado borrando el LAN fuera del rectángulo que corresponde al servicio de noticias del NNTP.

Agregar un Servicio

Si un protocolo no se enumera en la ventana de Servicios, este se puede agregar.

Dé un click en Policy, y después seleccione Add Service. Una ventana similar a (Figura 26) Se desplegará.

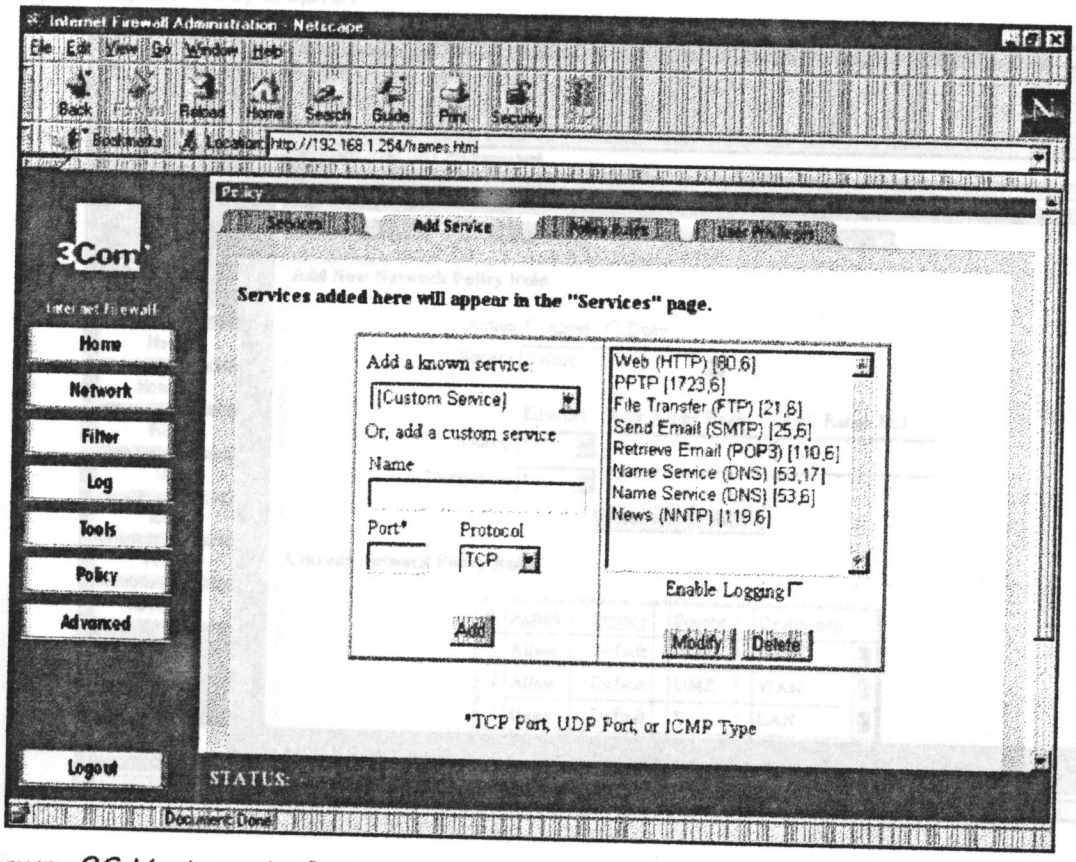


Figura 26 Ventana de Servicios

La lista a la derecha de la pantalla visualiza todos los protocolos del IP que se definen actualmente y que aparecen en la ventana de Servicios. Al lado el nombre del protocolo, dos números apareceran en corchetes. El primer número indica el número de acceso del IP que define el servicio (acceso del TCP, del UDP, o el tipo del ICMP). El segundo número indica el tipo del protocolo del IP (6 para el TCP, 17 para el UDP, o 1 para el ICMP).

Policy Rules

Network Access Rulers evalúa el tipo del protocolo del IP Address en el tráfico de la red, el destino del IP , y el protocolo del IP para decidir así el tráfico del IP que pasará ha través del Firewall.

Las Rulerss de encargo toman precedencia, y pueden pasar la inspección del paquete por default en el Internet Firewall.

Haga clicK en Policy, y después seleccione Policy Rules. Una ventana similar a (Figura27) se despleqará.

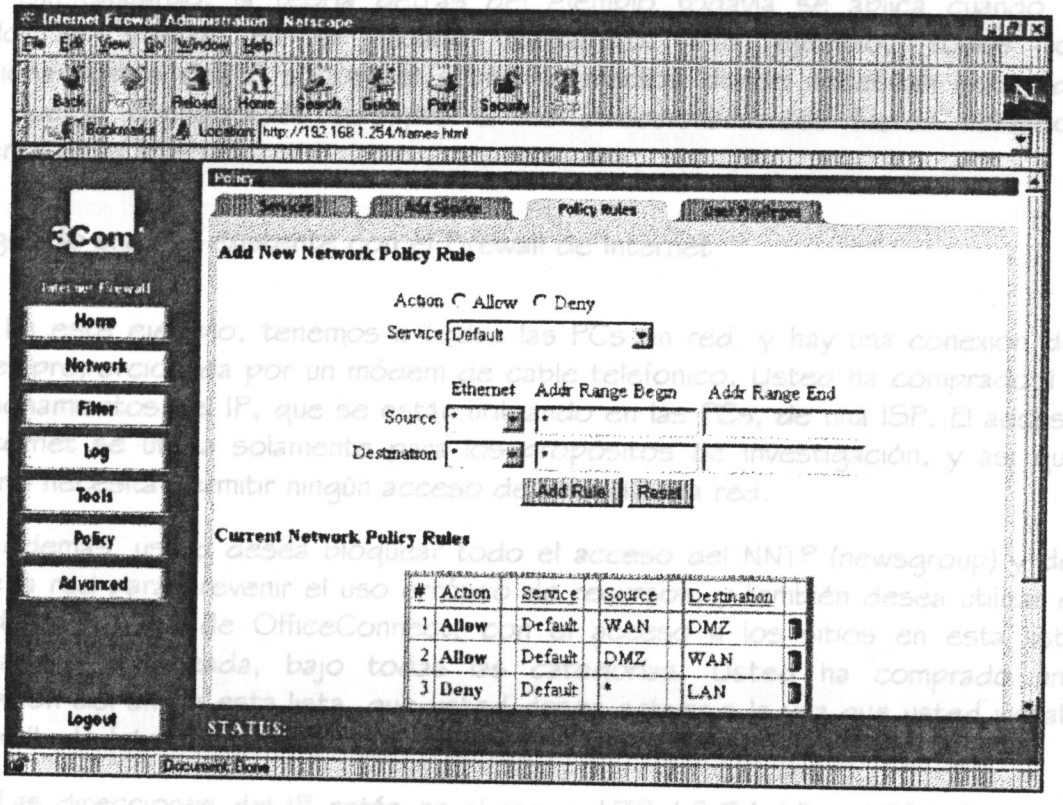


Figura 27 Ventana de Reglas y Políticas

Es importante considerar completamente la lógica que hay detrás de la nueva regla, antes de que usted la agregue. Utilice la lista en " lista de la lógica de la regla del acceso de red " para ayudarle a crear reglas lógicas.

10.8 EJEMPLO DE CONFIGURACIÒN DE UNA RED CON UN FIREWALL

El ejemplo proporciona una ilustración de cómo ciertas características del Firewall de Internet de OfficeConnect se deben utilizar realmente (sostener la información en el resto de este manual), y también cómo algunas de las características más avanzadas se pueden instalar, y sea beneficiosos.

El ejemplo es hipotéticos, y así que no debe intentar usar cualesquiera de los direccionamientos del IP (excepto los direccionamientos del IP del valor por defecto del Firewall de Internet y del módem del LAN), o los números de teléfono dados abajo, pues no trabajarán.

Sin embargo, la teoría detrás del ejemplo todavía se aplica cuando el ejemplo se utilizan en el mundo verdadero. Por ejemplo, todos los direccionamientos del IP son en el subnet correctos donde necesitan estar, de modo que la configuración trabajará si los direccionamientos fueron utilizados realmente en el Internet.

Protegiendo una red existente con el Firewall de Internet

En este ejemplo, tenemos a todas las PCs en red, y hay una conexión del Internet proporcionada por un módem de cable telefonico. Usted ha comprado 16 direccionamientos del IP, que se están utilizando en las PCs, de una ISP. El acceso del Internet se utiliza solamente para los propósitos de investigación, y así que usted no necesita permitir ningún acceso de entrada a la red.

Además, usted desea bloquear todo el acceso del NNTP (newsgroup) y del IRC de la red para prevenir el uso erróneo de recursos, y también desea utilizar el filtro del Web site de OfficeConnect, con el acceso a los sitios en esta lista registrada y bloqueada, bajo todas las categorías. Usted ha comprado una suscripción del año a esta lista, que usted desea activar a la vez que usted instala el Firewall de Internet.

Las direcciones del IP están en el rango 172,16,54,10 a 172,16,54,25 y estos direccionamientos son asignados estáticamente, y no proporcionados por

DHCP. El direccionamiento del Router para la ISP es 172,16,54,1 y el subnet mask es 255,255,255,0.

Además, el ISP tiene un mail server del SMTP en mail.3com.com y un servidor DNS en 172,16,54,253. Se desea que el Firewall de Internet mande los registros y las alarmas a automáticamente.

El Firewall de Internet debe tener su propio IP ADDRESS de modo que pueda trabajar correctamente y se pueda manejar. Si los 16 direccionamientos del IP están en uso, la ISP no utilizará la adición de este IP ADDRESS adicional.

Incluso si se ha configurado el Firewall de Internet para utilizar un direccionamiento en el subnet correcto, hay un riesgo que el ISP sea dada la dirección a otro usuario. En este caso, hay tres líneas de conducta que usted puede tomar:

- Quite el acceso del Internet a partir de la primera PC.
- Compre un IP ADDRESS adicional.
- Uso Nacional: Es posible que solamente alguna de las PCs requerirá su propio IP ADDRESS y sea presentado al Internet. El ejemplo " Expansión de numero IP Address de uso disponible NAT " describe cómo hacer un uso mejor de las múltiples direcciones del IP provistos por una ISP, mientras que todavía permite el acceso del Internet para todas las PCs que lo requieran.

En este ejemplo, se asume que la dirección es 172,16,54,16 puede ser liberada.

1. Apague el módem y conecte los accesos del Firewall de Internet.
    a. Conecte el acceso WAN del Firewall de Internet con el acceso de Ethernet en el módem.

    b. Conecte el puerto LAN al hub o switch, todas las PCs está conectadas directamente a una PC de la cual se intentará manejar el Firewall (The Management station).

2. Asumiendo que se está manejando el Firewall de Internet de la PC con la dirección 172,16,54,15 (por la conexión directa, o con un hub/switch), encienda el Firewall de Internet y checar el LED.

a. Espere la potencia del LED y se detenga el Flash (aproximadamente 90 segundos).

b. Cerciórese también de la alarma anaranjada LED cuando deje de parpadear.

3. Cambie el IP ADDRESS de management station de modo que esté en el mismo subnet de su Firewall de Internet.

a. El IP ADDRESS por defecto del Firewall del Internet es 192,168,1,254. Así, seleccione un IP ADDRESS en el mismo subnet para su management station - aquí la cambiaremos a 192,168,1,200.

b. Refiera a la guía del usuario para su sistema operativo en cambiar el IP ADDRESS de su management station.

Asegure especificar una dirección estática según lo dado arriba, con una subnet mask de 255,255,255,0. Ningunas otras configuraciones necesitarán ser modificadas.

c. Reanude la Management station, si es requerido.

4. De la PC management station, lance su web browser (Netscape 4 o Internet Explorer 4 o arriba) y la conexión como el administrador.

a. Incorpore http://192.168.1.254 para cargar la autenticidad de el password en la pantalla del Firewall de Internet.

b. En *el nombre del usuario,* Escriba admin

c. En el password, escriba la palabra por defecto password

d. Dé Click en Login.

5. Cuando usted ha entrado con éxito, la pantalla principal de la interfaz de la management para el Firewall de Internet se visualiza. De aquí, configure la unidad.

a. Haga click en Set *Password*.

c. En el viejo password, escriba password y después escriba el nuevo password dos veces. Los password son caso sensible, y usted no puede recuperarlos del Firewall Internet.

d. Dé Click en *Update*. La pantalla Home se visualiza otra vez. Si la barra de status en el fondo de la pantalla no muestra, que el password fue cambiado con éxito, repita este paso.

6. Fije la fecha y la hora.

El Firewall de Internet confíe en este para logs y las actualizaciones del filtro contenidos en la lista.

a. Dé click en Set Date Time en la ventana Home

b. Seleccione el tiempo de su zona

c. Aquí, usted desea utilizar el NTP para fijar el tiempo del Firewall de modo que la fecha y la hora sean fijadas por un reloj atómico, y es por lo tanto altamente exacto. Controle el " NTP para fijar la hora automáticamente ".

d. Pulse adentro, la fecha actual y la hora, en formato de 24 horas, y haga click en Update. Esto es necesario porque el Firewall del Internet no puede obtener su fecha y hora del Internet hasta que se configure éste, y la unidad pueda tener acceso al Internet.

7. Especificar el LAN y las configuraciones WAN, de la pantalla principal, hacer click en *configuraciones de la red (LAN y WAN)*

   a. Cuando se cargué la pantalla, de la lista drop-down, seleccione Standard.

   b. En la dirección *del Firewall de Internet en el* campo, pulsar 172,16,54,16. Ésta fue la dirección que se puso para que el Firewall utilice. Incorpore *un subnet mask del LAN* de 255,255,255,0.

   c. En *el direccionamiento del Router de la WAN*, escriba 172,16,54,1 (según lo provisto por la ISP).

   d. En *el servidor 1 del DNS*, escriba 172,16,54,253 y teclee *Update*. Las configuraciones son actualizadas y se visualiza la pantalla principal.

8. Invalide el acceso a los protocolos del NNTP (newsgroup) y del IRC (Internet Relay Chat).

El Firewall de Internet tiene un valor por defecto fijado en las reglas del acceso que permiten la mayoría de los accesos básicos del Internet (Web, ftp, HTTP, y así sucesivamente). Los usuarios pueden tener acceso solamente a esos servicios básicos y a cualquier otros que se permitan específicamente.

   a. Dé click en Policy para visualizar una lista de los servicios de red permitidos. Usted notará que el NNTP está en la lista, así que el acceso del newsgroup se permite actualmente. El IRC no está en esta lista, pero usted debe observar que también está permitido. Además de los servicios enumerados en esta paginación, el Firewall del Internet también tiene una lista de servicios sabidos, y éstos se permiten bajo título " valor por defecto ".
   La regla del valor por defecto cubre todos los servicios no cubiertos más específicamente a otra parte (por ejemplo, específicamente la prohibición del IRC reemplazará el hecho de que está permitida bajo título " valor por defecto").

   b. Para bloquear el acceso del NNTP, limpie *el LAN Out* y cheque el siguiente NNTP en la lista, y dé click en Update.

c. Para bloquear el acceso del IRC, primero hacer click en Add Service. Despues, en Add a Known Service, y seleccione IRC. Click en Add, y el IRC se agregará a la lista en el lado derecho.

c. Ahora cambie de nuevo *a los servicios*. Usted notará que el IRC ahora está en la lista de servicios en esta pagina. Para invalidarlo, en LAN Out y Update.

9. Encienda el módem, cerciórese de que este en línea y reinicie el Firewall de Internet.

a. Haga click en Tools.

b. Haga click en Restart Firewall *Internet*. Cuando pregunte la confirmación de esta acción, seleccione Yes. El Firewall de Internet se reinicia.

b. Restablezca el IP ADDRESS y el subnet mask de su estación managament a 172,16,58,15 subnet mask 255,255,255,0.

10. Cuando el Firewall de Internet ha reiniciado, cerciórese de que usted pueda tener acceso al Internet. Incorpore http: //www.3Com.com/internetfirewall para ver si usted puede tener acceso al sitio del registro para el Firewall del Internet.

11. Obtenga el código del registro del Firewall de Internet y permita la suscripción del filtro del Web site.

a. Pulse sus detalles en la forma de registro, y anote el código de registro cuando usted ha acabado.

b. Para permitir su suscripción del filtro del Web site, haga click en Upgrades en la paginación del registro de los 3Com. Seleccione *El OfficeConnect Web Site Filter*, y entonces pulsen el número de serie del Firewall de Internet. También pulse adentro el código de la activación para su suscripción (esto se puede encontrar en la parte posterior del manual que vino con la suscripción). Esto permite su suscripción del filtro del Web site.

12. Introduzca el código del registro.

    a. Cargue la interfaz de management otra vez y abra una sesión según lo descrito en el paso 4, a menos que use de nuevo la dirección del Web asignado al Firewall del Internet http: //172.16.54.16 y el nuevo password que usted fijó.

    b. En la pantalla Home, seleccione Unit Status. La pantalla del status visualizara un mensaje que indica que el Firewall de Internet no está registrado.

    c. Incorpore el código del registro en este rectángulo de texto, y de click en *Update*. El Firewall de Internet ahora se registra.

13. Obtenga el IP Address del mail server.

    a. Dé Click en Network y seleccione Diagnostics.

    b. Seleccione *DNS Name*.

    c. Cuando la paginación ha recargado, pulse el direccionamiento del mailserver, (en este ejemplo, mail.3com.com y teclee Go.

    d. Cuando el IP Address del mail server sé visualize, anòtelo.

14. Instale las características del registro.

    a. Haga click en Log y seleccione *las configuraciones de Log/Alert* Settings.

    b. Pulse el IP ADDRESS que usted ha observado en *el mail server*.

    c. Pulse la dirección de E-mail en la que usted quisiera que los registros fueran enviados en Send Log, y *las Send Alert*. Usted puede utilizar las mismas direcciones del E-mail. Utilice el direccionamiento completo del E-mail; por ejemplo: system_administrator@3com.com.

c. Dé Click en Update cuando termine. El regreso de la dirección, log@InternetFirewall simplemente identifica los mensajes que el Firewall del Internet envió. Esto no es un direccionamiento válido del E-mail, y así que ningunos E-mail pueden regresarse. Sin embargo, usted puede cambiar este direccionamiento del E-mail si usted lo desea.

15. Cargue la lista del filtro del Web site.

a. *Dé click en Filter* y seleccione Filter Update.

b. *Dé Click en Download Now* y espere para que la lista del filtro se descargue. El progreso se muestra en la barra de status en el fondo de la pantalla.

c. Si usted quisiera que el Firewall del Internet realice automáticamente las actualizaciones cada semana, hacer click *en Automatic Download*, selecciona un día de la semana, y pulse adentro el tiempo.

d. Dè click en *Update*.

e. Seleccione Settings, y cerciórese de que *el registro y el bloque tengan acceso*, y el bloqueo de *todas las categorías*. Y dè Click en *Update*.

CONCLUSIONES

Al finalizar este trabajo de investigación me pude percatar del gran desarrollo tecnológico en el campo de los sistemas utilizados en las organizaciones en los últimos años, y la importancia que tienen los equipos de cómputo como herramientas para compartir la información.

En su inicio, el equipo de cómputo y los sistemas de información basados en computadora soportaban sólo el control de funciones operacionales básicas, tales como inventarios, nómina, administración y contabilidad, sin embargo, su uso se ha extendido en la actualidad al desarrollo de sistemas basados en la infraestructura de las Redes.

Actualmente se cuenta con equipos de cómputo en las diferentes áreas administrativas, académicas y de investigación. En cada una de estas áreas la infraestructura computacional varía desde PC´s trabajando en un ambiente de sistema operativos y en red, este crecimiento no termina allí, y por lo que a la Dirección de Servicios de Cómputo se refiere, sus actividades e infraestructura computacional han crecido de tal forma que actualmente se cuenta ya con una conexión a la red INTERNET.

Para lograr este crecimiento ha sido necesaria la adquisición de equipo cada vez de mayor costo y que requiere una mayor protección.

Por tal motivo a lo largo de la investigación me fui percatando que el Firewall es altamente recomendable para las empresas que quieran enlazar su red a Internet de una manera más confiable ya que el Firewall vigila el tráfico de Internet, detecta y frustra posibles ataques de Hackers siendo ésta una medida de seguridad para proteger y garantizar el funcionamiento continuo de la red de área local (LAN).

Gracias al Firewall, pude observar la eficacia con que se cuenta para tener el control sobre el acceso a sitios en Internet que no es conveniente que algunos usuarios tengan acceso a ellos y manteniendo un registro de los acontecimientos que puedan ser importantes para la seguridad de la red, en síntesis esta investigación me aportó grandes conocimientos acerca de las redes y el manejo del Firewall de Hardware analizado.

BIBLIOGRAFIA

INTERNET

http://orbita.starmedia.com/~alex-torres/index.htm

URL: http://visviri.electa.uta.cl/eurofast/redes/topolog2.html

URL: http://visviri.electa.uta.cl/eurofast/redes/topolog5.html

http://www.geocities.com/Athens/9105/redes/red_ses_7.html

http:/www.geocities.com/Athens/9105/redes/red_ses_7.html

http:/www.bolnet.bo/eldiario/sucre57.html

http://support.3com.com

http://www.monografias.com/Computacion/Redes/

http://www.redes.ccm.itesm.mx/internet/index.html

LIBROS

COMPUTER NETWORKS AND THEIR PROTOCOLS

Communication Protocols and Interfaces

John Wiley & Sons

Segunda Edición

1979

IPV4 ADDRESS BEHAVIOUR TODAY

RFC 2101

Organización: IAB.

Febrero 1997

REDES DE COMPUTADORAS

Uyless Black

Editorial Macrobit

1990

REDES DE ORDENADORES

Andrew S. Tanenbaum

Editorial: Prentice Hill Hispanoamericana

Segunda Edición

1991

ELEMENTOS DE COMPUTACION

Guillermo Levine

Editorial Mc Graw Hill

1993

TELEINFORMATICA

Coediciòn: Colegio Nacional de educación profesional técnica y Alfaomega.

Editorial: Alfaomega

1995

ENCICLOPEDIA DE LA MICRO COMPUTACION

Adriana Marcela Rivas

Editorial: Printer Latinoamericana

1995

ENCICLOPEDIAS ELECTRONICAS

ENCICLOPEDIA MICROSOFT® ENCARTA® 2000. ©
1993-1999 Microsoft Corporation.
Reservados todos los derechos.