UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA

ACTUALIZACION DE LA PLATAFORMA TECNOLOGICA Y DEL ESQUEMA DE SEGURIDAD, E IMPLEMENTACIÓN Y DISEÑO DE UNA RED DE ALTA VELOCIDAD EN LA FUNDACIÓN CARACAS

Trabajo presentado por la

Ing. Janeth González

Ante la ilustre Universidad Central de Venezuela
para optar al Titulo de
Especialista en Comunicaciones y Redes de Comunicaciones de Datos

Caracas, Octubre de 2005

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA

ACTUALIZACION DE LA PLATAFORMA TECNOLOGICA Y DEL ESQUEMA DE SEGURIDAD, E IMPLEMENTACIÓN Y DISEÑO DE UNA RED DE ALTA VELOCIDAD EN LA FUNDACIÓN CARACAS

Trabajo presentado por la

Ing. Janeth González

Ante la ilustre Universidad Central de Venezuela
para optar al Titulo de
Especialista en Comunicaciones y Redes de Comunicaciones de Datos

Tutor: Prof Carlos Moreno

Caracas, Octubre de 2005

Hecho el Depósito de Ley
Depósito Legal ift487200562076

RESUMEN

La plataforma de redes de la Fundación Caracas poseía una serie de problemas que necesitaban ser atendidos y solucionados, para así mejorar la calidad y seguridad de los servicios y recursos que ella ofrece a las distintas parroquias y comunidades que se atienden en Fundacaracas.

El trabajo que aquí se presenta tiene como objetivo la solución de dichos problemas, proponiendo, diseñando e implantando un plan de actualización de la red local y del esquema de seguridad, que permitiera mejorar el desempeño de la red, garantizar su disponibilidad y satisfacer la creciente demanda de servicios y recursos, mejorando la seguridad de la información y los tiempos de respuesta de las aplicaciones que apoyan los procesos de toma de decisión de las distintas unidades, coordinaciones y gerencias de Fundacaracas.

Para la actualización de la plataforma de redes se plantearon varias soluciones, tales como la creación y administración de redes virtuales (VLAN); cambio de todos los equipos de la Fundación, cambio de los equipos de cada piso, instalación de un equipo de seguridad, creando 4 zonas (intranet, extranet, Internet y DMZ), implantación de un software que controla y regula la salida hacia Internet y por último la modificación de las normas y políticas de uso de los servicios. Además, se va a adiestrar a todo el personal de las unidades de redes y soporte técnico para que presten el apoyo necesario y diario que requiere la plataforma para mantener su calidad y disponibilidad.

Todas estas modificaciones permitieron mejorar considerablemente los tiempos de respuestas de las aplicaciones, la disponibilidad de recursos y servicios, así como la seguridad de la información. Como punto final, cabe destacar que es necesario considerar múltiples factores a la hora de elaborar un proyecto de actualización de una plataforma ya existente, dentro de los cuales se pueden mencionar los siguientes: los protocolos de comunicación utilizados, el tráfico de la red, capacidad de los equipos, etc. Estos son puntos que juegan un papel importante al momento de diseñar un proyecto y la consideración de los mismos contribuye en gran parte con su éxito.

DEDICATORIA

A Dios, por estar siempre a mi lado

A mi Madre, mi mayor fuente de Inspiración

A mi Padre, por brindarme su apoyo cuando lo necesito

A mi Esposo Andrés Eloy por el Amor tan grande que me dá, Te Amo,

A mis dos hijos Andrés Gerardo y Daniel Andrés, por ser luz en mi Vida

A mis hermanas, hermano y primos, que los quiero y los respeto

A mis Tías, por confiar en mí

A mis sobrinos, que los amo y nunca los olvido

A mis amigas, porque ese lazo que nos une

AGRADECIMIENTOS

A Dios Todopoderoso, mi mayor fuente de inspiración, mi guia, a quien todo se lo debo.

A Andrés Eloy, mi esposo, por todo el apoyo en la realización de este y todos los trabajos de mi formación profesional.

A mis hijos, Andrés y Daniel, por llenar mi vida de dulzura y ternura cada amanecer, Los Amo.

A mis padres, tias, hermanos y primos por creer una vez más en mi, en todos mis avances profesionales.

A mis eternas amigas Yosmar, Italia, Cecy, Yoraima y Catalina por ser como son.

A todos mis sobrinos, que aunque algunos están lejos, siempre están en mi memoria.

A mis vecinos, en especial a Francis, que de alguna manera contribuyeron a la finalización de esta meta.

A mis suegros y cuñados por darle siempre tanto amor a mis hijos.

Al profesor Carlos Moreno y Vicencio Mendillo por estar siempre dispuesto a atenderme y asesorarme en este trabajo.

INDICE GENERAL

Pág.

Pág.

INDICE DE FIGURAS

Pág.

INTRODUCCIÓN

La Fundación Caracas es un ente descentralizado enmarcado en una actividad pública de carácter social y local. Le corresponde ejecutar la política municipal de vivienda y hábitat en consonancia con la política nacional sectorial. Es por esto que actualmente para poder cumplir con las exigencias que sus funciones, la Fundación Caracas requiere la automatización de muchos de sus procesos.

Esta automatización de procesos trae como consecuencia que la plataforma de seguridad, de redes y de comunicaciones que posee actualmente Fundacaracas esté por debajo de lo requerido para que los sistemas funcionen y respondan de forma eficiente y efectiva. Otros aspectos a destacar, son el aumento exponencial en la cantidad de usuarios en red, así como el aumento en la cantidad de servicios que se ofrecen.

Todo esto llevo a la Coordinación de Informática de Fundacaracas a realizar un proyecto de actualización tecnológica en su plataforma de red y de seguridad, el cual se desarrolló en dos etapas y se estructuró de la siguiente forma:

- En el Capítulo I se plantea la problemática existente y se justifica la necesidad de actualización. Posteriormente se definen los objetivos del proyecto, exponiendo sus alcances y limitaciones.
- El Capítulo II se resumen las bases teóricas necesarias utilizadas en la elaboración del presente trabajo.
- En el Capítulo III se expone la metodología utilizada en el desarrollo del proyecto, la cual consiste en cinco etapas: formulación del problema de investigación, fase exploratoria, fase de análisis, diseño de la solución y la implantación y pruebas.

- En el Capítulo IV se presenta el diseño de la solución, el cual comtempla el modelo de red, modelo de seguridad, normas y politicas de red y las políticas a implantar en el Websense para la salida Internet. Igualmente se describe el proceso de adquisición de la solución.
- En el Capitulo V se explica la instalación de los equipos y software, así como las pruebas realizadas para comprobar su operatividad.

Finalmente se incluyen las conclusiones del trabajo, las recomendaciones, las referencias bibliográficas, el glosario de términos y los anexos.

CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1. EL PROBLEMA DE INVESTIGACIÓN

1.1. Formulación del problema

La plataforma de redes y seguridad de la Fundación Caracas posee una serie de problemas que deben ser atendidos y solucionados de forma eficiente, para mejorar la calidad y disponibilidad de los servicios y recursos que se ofrecen a las distintas Oficinas, Coordinaciones y Gerencias que conforman la Fundación Caracas.

Los problemas a considerar en la plataforma de redes son los siguientes:

a. Retrasos en los tiempos de respuesta de las aplicaciones que funcionan en red: servicio de correo, servicio de impresión, sistema de personal (KOMITIVA), sistema de gestión administrativa (KARAVANA), sistema de contabilidad, entre otros.
b. No posee un servicio de impresión centralizado, lo que genera un gasto excesivo en cartuchos para impresoras.
c. Descontento de los usuarios en cuanto al tiempo de acceso para los archivos (memos, informes, hojas de cálculo, etc.) almacenados en el servidor de documentos.
d. Aumento de la cantidad de computadores personales en la Fundación Caracas, distribuidos en todas sus Coordinaciones y Gerencias, lo cual ha incrementado el tráfico en la red.
e. Desactualización de los switches de la red de área local (LAN), ya que estos equipos poseen más de ocho años de uso.
f. No posee firmware que permita la creación de redes virtuales (VLAN) interconectadas entre sí.

g. Cableado horizontal con estaciones de trabajo funcionando a 10 Mbps y 100Mbps y un cableado vertical (backbone) operando a 100 Mbps, lo cual representa un cuello de botella.
h. Posee un solo Servidor funcionando a 100 Mbps, el cual no reúne las características mínimas para el número de usuarios en la red, ya que este es un computador Pentium IV.

En cuanto a los problemas de seguridad se tienen los siguientes:

a. No existe zona de seguridad, lo cual representa un riesgo para la red local.
b. No poseen equipos de seguridad principal (firewall), lo que genera una gran cantidad de problemas en la Red de Área Local.
c. El equipo que funciona como Servidor no posee redundancia, lo cual representa un riesgo si este equipo falla.
d. Falta de control y auditoria en el uso de los servicios de Internet.

1.2. Contexto del problema

La Fundación Caracas posee una plataforma de comunicaciones y redes con las siguientes características:

a. Cableado horizontal: existen 08 pisos más el sótano, no en todos los pisos se tienen switches, solo en el piso 1, 3, 4, 6 y 7 poseen un switches *Cisco 1900* algunos con 12 y otros con 24 puertos a 10 Mbps. El cableado es UTP categoría 5 con norma 568A y existen 20 puntos por piso. La topología es en estrella. (Ver figura I.1).

b. Cableado vertical: El cableado es UTP categoría 5 con norma 568A y existen 20 puntos por piso. La topología es en estrella. (Ver figura I.1).

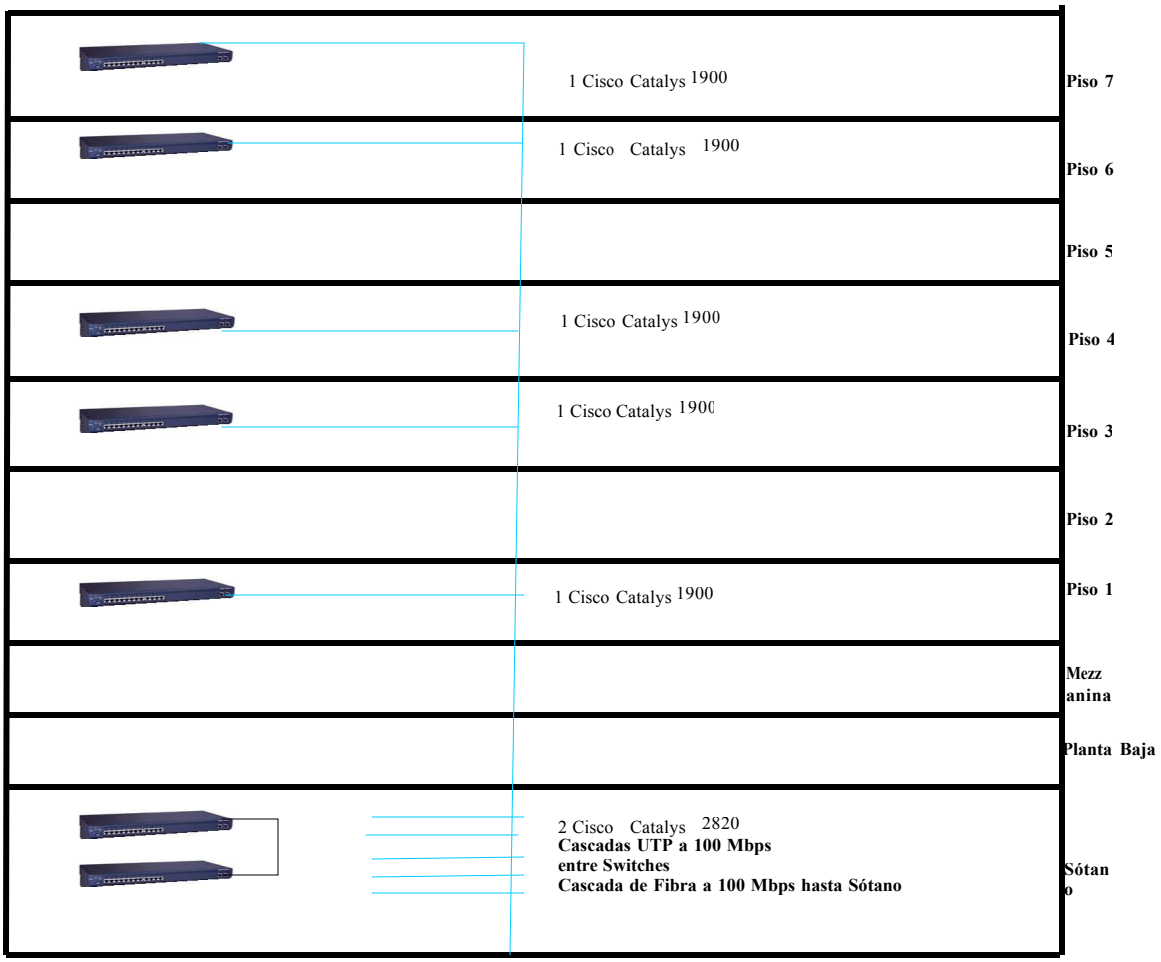


Figura I.1. Esquema de conexión de la Red de Área Local (LAN)

c. Equipos de comunicación remota: se tiene un enrutador *Cisco 5400* con 12 puertos seriales, de los cuales cinco están en uso, y cuatro puertos Ethernet de 10 Mbps. Este enrutador es utilizado para la conexión con el Despacho de la Alcaldía del Municipio Libertador, conexión con el Banco Banesco, con el Banco Mercantil, Gerencia del Cementerio General y CONAVI. Los puertos Ethernet son utilizados para el enrutamiento entre las redes locales del edificio. Para el servicio Internet se dispone de un enrutador *Cisco 2501*. (Ver figura I.2).

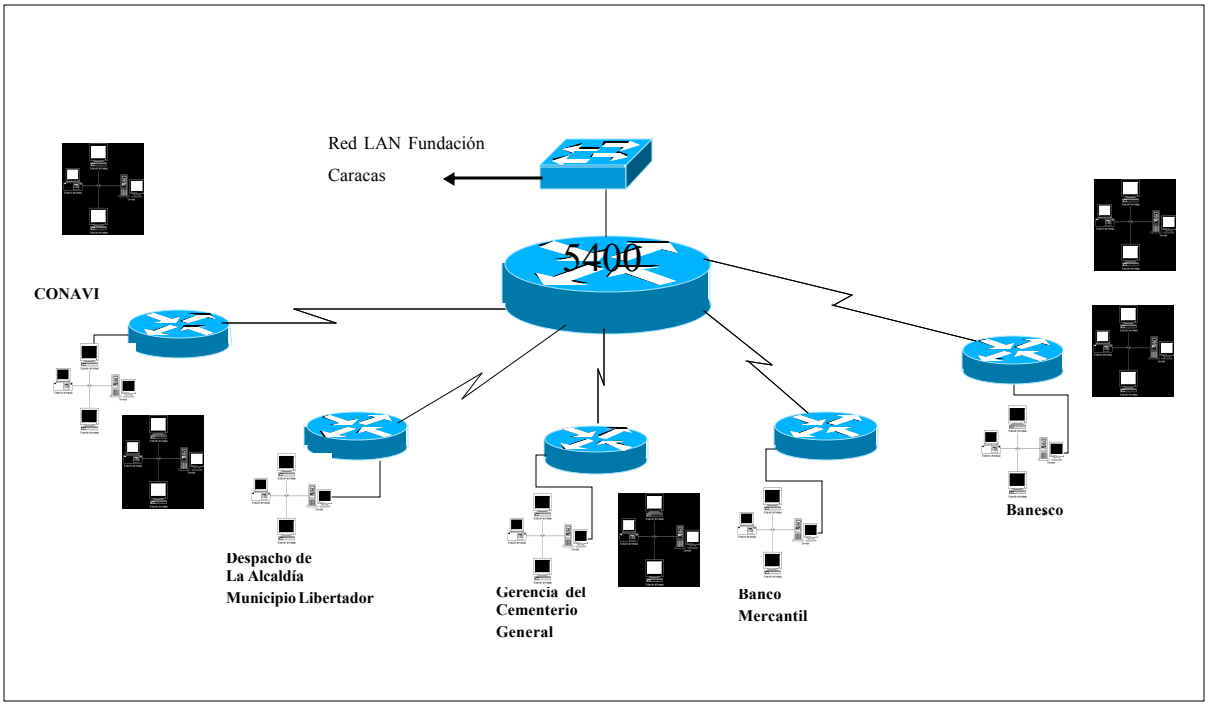


Figura I.2. Esquema de conexión de la Red de Área Amplia (WAN)

d. Esquema de seguridad: No se dispone de ningún *Firewall*, lo cual permite una gran vulnerabilidad en la zona externa (outside), formada por Internet y un DNS externo y de la zona interna (inside). (Ver figura I.3).

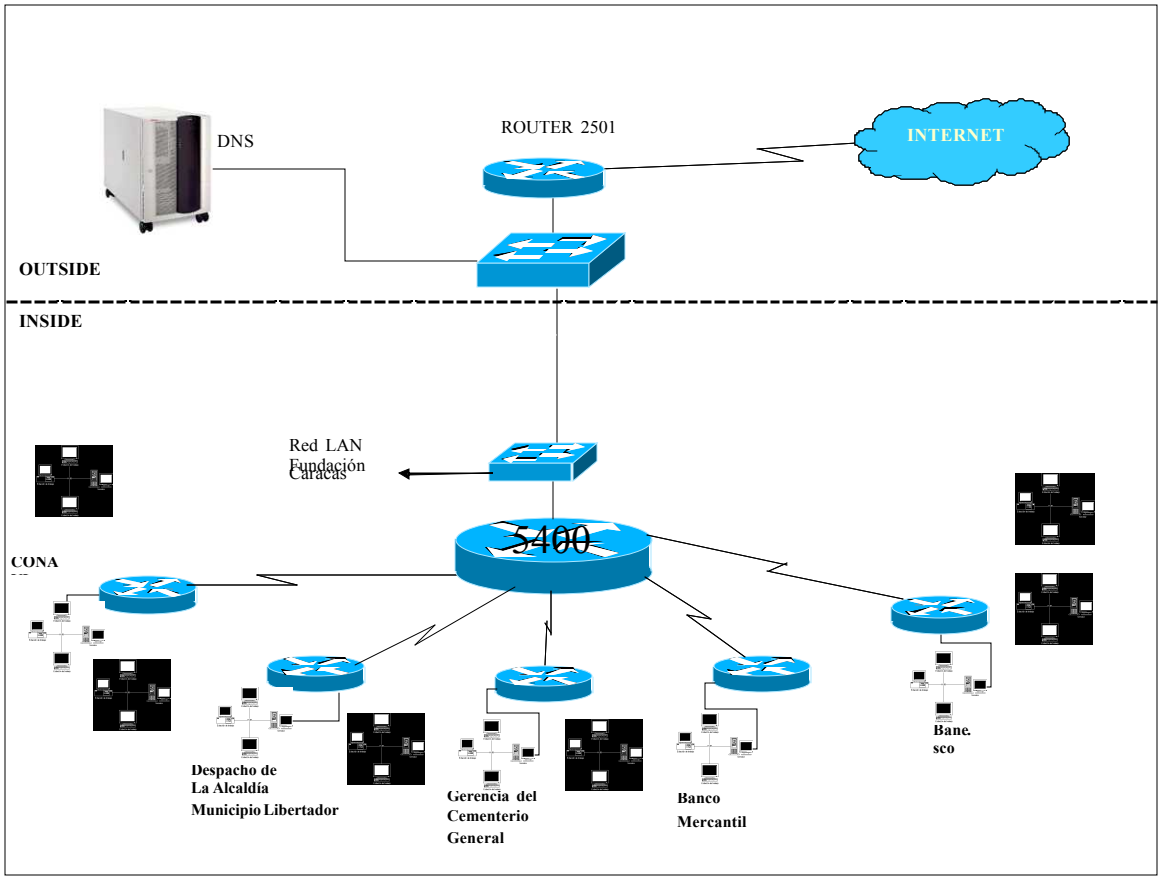


Figura I.3. Esquema de Seguridad

2. JUSTIFICACIÓN

Hoy en día la Fundación Caracas posee grandes necesidades de automatización para poder cumplir con las exigencias de las 22 parroquias Caraqueñas, en materia de economía. Existen algunos procesos muy importantes que están automatizados, entre los cuales se pueden mencionar al Sistema de Gestión Administrativa (KARAVANA) y Sistema de Personal (KOMITIVA). Dichos sistemas presentan graves problemas en sus tiempos de respuesta, ya que los mismos son muy lentos.

Se requiere, además, la automatización de otros procesos de la Fundación Caracas los cuales están a cargo de la Coordinación de Contabilidad, la Oficina de Gestión de Control y Planificación, la Coordinación de Bienes y Servicios. Esta automatización

generará gran carga en el tráfico de la red, lo cual no puede ser satisfecho con la plataforma de redes que se posee actualmente. Por otra parte, la información que maneja la Fundación Caracas es vital y de mucho valor para el municipio Libertador, por lo que la misma debe estar protegida bajo estrictos controles de seguridad.

Todo lo expuesto exige que en la Fundación Caracas se realice la actualización de la plataforma tecnológica y de seguridad de la red local, con el fin de poder soportar la automatización de los procesos de sus distintas Coordinaciones y Gerencias, dar continuidad al apoyo tecnológico de los procesos ya automatizados y proteger la información confidencial.

La actualización de la red permitirá la creación y administración de redes virtuales, ampliación de las zonas de seguridad de la red, mejora en los tiempos de respuestas de las aplicaciones, disponibilidad de recursos y servicios e implantación de un sistema de seguridad redundante.

3. OBJETIVOS

3.1. Objetivo General

Actualización de la Plataforma Tecnológica y de la red local de la Fundación Caracas, diseñando, adquiriendo e implantando un modelo de red y de seguridad, que permita mejorar la prestación de los servicios de red, garantizar su disponibilidad y satisfacer la creciente demanda de servicios y recursos, mejorando la seguridad de la información y los tiempos de respuesta de las aplicaciones que apoyan los procesos de las distintas Coordinaciones y Gerencias de la Fundación Caracas.

3.2. Objetivos Específicos

a. Estudio de la estructura de la red local de la Fundación Caracas, para definir los límites y alcance que tendrá la actualización propuesta. En este punto se definirán las sub-redes y super-redes, equipos de interconexión (conmutadores y enrutadores), servidores (Unix y Windows NT/2003), servicios y las zonas de seguridad.
b. Elaboración de un cronograma de actividades, definiendo inicio de la instalación, recursos humanos, alcance de las pruebas, entonación, culminación y entrega de documentación.
c. Definición de las necesidades de ampliación de ancho de banda local y protección de la información de las distintas Coordinaciones y Gerencias de la Fundación Caracas. En este punto se definirán las políticas de seguridad de la red a implementar en el dispositivo de seguridad.
d. Diseño del modelo de red y del esquema de seguridad.
e. Estudio de factibilidad para determinar disponibilidad presupuestaria, ambiente físico donde serán instalados los equipos, seguridad y condiciones ambientales.
f. Adquisición de los equipos a través de procesos licitatorios, ajustándose a los reglamentos de la misma.
g. Instalación física y conectorización de los equipos.
h. Instalación y configuración de Redes Virtuales (VLAN) interconectadas.
i. Prueba y entonación de todos los equipos LAN.
j. Instalación y configuración de:
    - Equipo de seguridad, según las políticas y las zonas definidas.
    - Cambio de direccionamiento.
    - Software para el control y monitoreo del acceso a Internet.
k. Prueba y entonación del esquema de seguridad.

l. Revisión y aprobación de las normas y políticas de uso de la red por parte de la dirección de recursos humanos, consultoría jurídica y despacho del ministro.

4. ALCANCE

Tanto el diseño como la adquisición e implantación de un nuevo modelo de red local y de seguridad abarca únicamente la sede principal de la Fundación Caracas ubicado en la ciudad de Caracas, avenida Universidad, edificio Tarqui, y no se contemplan la red local de la sede remota (Cementerio General del Sur).

5. LIMITACIONES

a. Por razones presupuestarias no se contrató con una empresa especializada un análisis de tráfico de red, antes y después de la actualización tecnológica, de forma tal de comprobar estadísticamente las mejoras en los tiempos de respuesta de las aplicaciones.

b. Por razones de tiempo, no se pudo contratar a una empresa especializada en seguridad para la realización de un análisis de vulnerabilidades y riesgos que permitiera definir un modelo de seguridad mucho más ajustados a las necesidades de la Fundación Caracas.

c. No se pudo abarcar la otra sede de la Fundación Caracas, por problemas presupuestarios.

d. La instalación y configuración de los equipos sólo puede llevarse a cabo en días feriados o fines de semana, ya que la actualización de la red local y del esquema de seguridad afecta la prestación de los servicios.

CAPÍTULO II. MARCO TEÓRICO

1. BASE TEÓRICA

1.1. Estándares Ethernet/ IEEE-802.3/IEEE-802.2

Ethernet es una tecnología bastante sencilla y económica. Es la que predomina en los diseños de redes locales.

Topología

Tradicionalmente ethernet funciona sobre un modelo de topología tipo bus o bus-estrella. Como se ilustra en la figura II.1, si se envía un paquete desde el PC C al PC B, esta trama será transmitida también a los PC A y D.

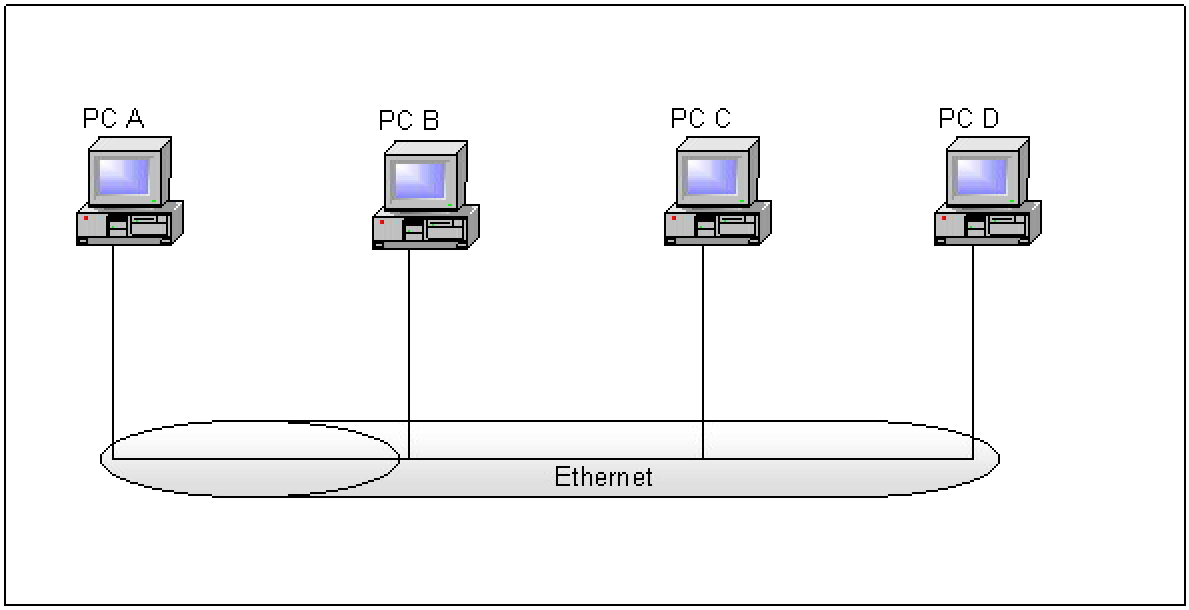


Figura II.1. Topología Bus

El primer problema en una red de tipo bus es que, aún cuando la trama no vaya destinada a los demás PC, por las propiedades de la arquitectura de bus debe viajar a través de todos los PC del bus. Ello se debe a que en una topología de bus física verdadera todos los PC comparten el mismo cable. Aunque haya múltiples segmentos físicos de cables, todos ellos se acoplan y comparten la misma señal eléctrica.

Otro problema que surge con la topología de tipo bus es que si se rompe un cable todos los PC resultan afectados. Por esta razón un bus físico debe tener un resistor, llamada terminador dispuesta en los dos extremos del bus.

La arquitectura de tipo bus-estrella que es hoy mucho más común que la de tipo bus estándar, opera de una forma ligeramente diferente. El bus-estrella es una estrella física y un bus lógico. La configuración física de estrella significa que todos los dispositivos conectados a la red tienen su propio segmento físico de cable. Estos segmentos confluyen por lo general en un punto central a través de un dispositivo conocido como concentrador (hub). Este dispositivo no tiene ningún componente inteligente y su único objetivo es amplificar y repetir las señales recibidas de cada puerto a todos los demás. Esta función constituye el bus lógico requerido por Ethernet.

La ventaja de la configuración física de estrella es que si se rompe un segmento de cable ningún otro dispositivo resulta afectado por el problema y simplemente el puerto correspondiente del concentrador queda fuera de servicio hasta que se repare o se sustituya el cable.

En lo que respecta al bus lógico de la configuración Ethernet de bus-estrella, el funcionamiento es el mismo que el de una arquitectura de bus físico. Si se envía una señal al PC B desde el PC C, deberá ser transmitida también a los PC A y D, tal como se ilustra en la figura II.2.

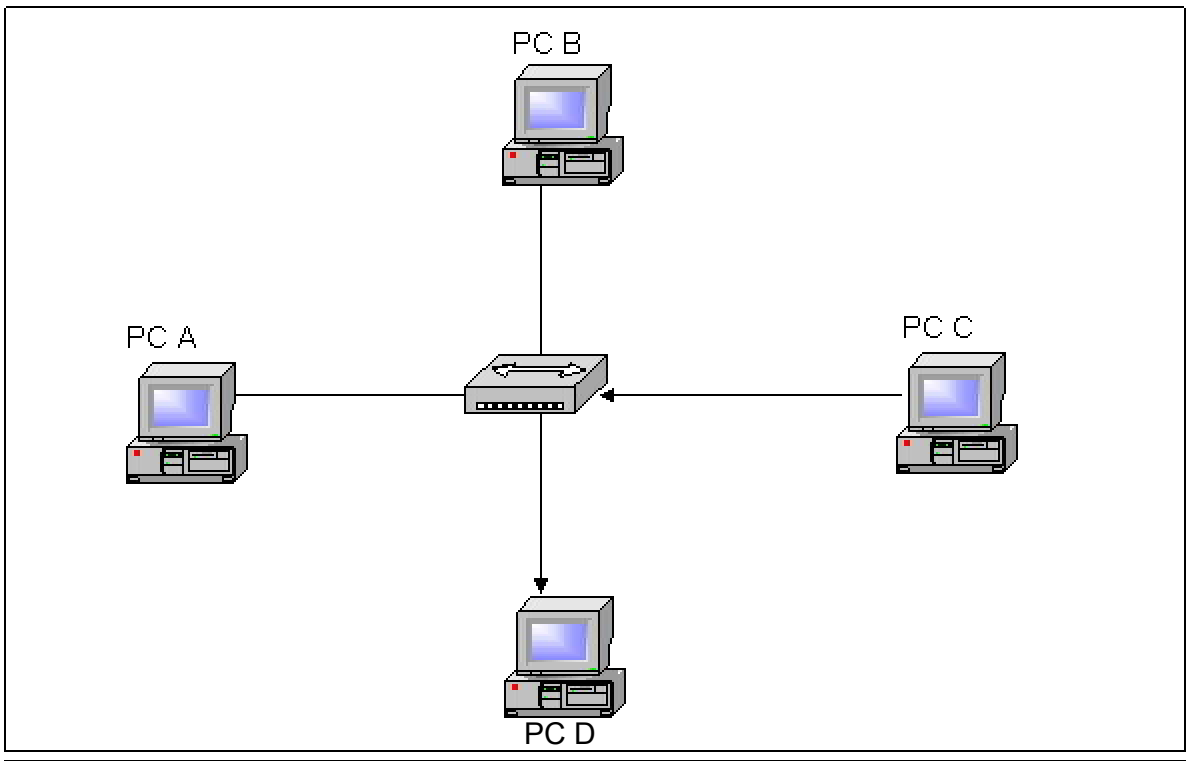


Figura II.2. Funcionamiento bus-estrella

Ancho de banda

Ethernet funciona a múltiples velocidades, desde 10 Mbps a 10 Gbps. La más común actualmente es 100 Mbps, aunque este valor debe tomarse con reserva. En primer lugar, hay que entender que en el estándar Ethernet se está usando un segmento de cable lógico (bus lógico) y se trabaja en modo half-duplex, donde sólo una máquina puede enviar información en un instante dado. Ello conduce a un problema de primera magnitud: el ancho de banda compartido. Por ejemplo, si se tienen 100 clientes conectados al Ethernet de 100 Mbps, cada cliente tendrá una velocidad media de transferencia máxima de 1 Mbps. Además, debe recordarse que aquí se está hablando de megabits por segundos, no de megabytes por segundo. Ello significa que se tiene una velocidad media de transferencia máxima de unos 125 Kbps.

Dúplex

Ethernet puede funcionar en modo dúplex o half-dúplex. En este último se puede enviar y recibir mensajes en cualquier instante, pero no las dos cosas a la vez. Ello significa que si en el mismo momento otro dispositivo está enviando datos en un momento dado (que el primer usuario estaría recibiendo), entonces dicho usuario tendría que esperar hasta que se complete esa transmisión antes de enviar su propia información por la red. También significa que las colisiones no sólo son posibles, sino bastantes probables. Una red Ethernet half-dúplex puede compararse con una carretera de un solo carril donde las tramas serían autobuses interurbanos que circulan por esa carretera. Si un autobús avanzara por ella en un sentido y viniera otro en sentido contrario, se produciría una colisión, de la que resultaría la pérdida de los 2 autobuses o tramas.

La configuración Ethernet en modo full-duplex o bidireccional soluciona este pequeño dilema, al abrir un segundo carril en esa carretera. Los dispositivos que pueden manejar tecnología full-duplex se denominan conmutadores (switches). Trabajando en full-duplex es posible enviar y recibir al mismo tiempo. Esta proeza se consigue utilizando cables físicos independientes para la emisión y la recepción. En modo full-duplex cada vez que llega algo al conmutador desde un par de emisión, el conmutador debe saber como enviar esa señal a todos los pares de recepción.

Atenuación

Aunque no es sólo un problema de Ethernet, la atenuación es una de las preocupaciones más relevantes de esta tecnología. Se llama atenuación a la degradación de una señal con el tiempo o la distancia. Esta degradación se debe a que el cable en si ofrece cierta resistencia al flujo de señal, lo que produce una reducción

en la señal eléctrica conforme se desplaza por dicho cable. La señal se envía a una cierta tensión y amperaje, pero con la distancia la resistencia del cable hace que la señal se vaya degradando. Si lo hace en demasía, la relación señal-ruido caerá por debajo de niveles mínimos aceptables, y el dispositivo final no será capaz de determinar cuál es la señal y cuál el ruido.

La atenuación se puede resolver por distintos métodos, dos de las soluciones son definir longitudes de cables máximas y repetir o amplificar la señal. Definir longitudes de cableado máximas ayuda a aliviar el problema al establecer límites máximos a la resistencia total según el tipo de cable. Si se repite la señal, el problema puede resolverse, amplificando la señal cuando se hace muy baja. Sin embargo, esta estrategia sólo funcionará un pequeño número de veces, ya que el repetidor no reconstruye la señal; simplemente amplifica lo que existe en el cable conductor. Por tanto, amplifica tanto la señal como el ruido. De este modo, la relación señal-ruido no mejora, y lo único que se hace es garantizar que el volumen de la señal mantiene un nivel aceptable.

Interferencia electromagnética

La interferencia electromagnética (IEM) es otro problema no específico únicamente de Ethernet. Las IEM se producen en una u otra medida en todos los cables de cobre. Si embargo, suelen ser más acusadas en Ethernet debido al uso predominante de cableado de pares trenzados sin apantallar (UTP, Unshielded Twisted Pair). Todos los equipos electrónicos generan interferencias electromagnéticas por el simple hecho de que cada vez que se envía un impulso eléctrico por un cable, se crea un campo magnético (es el mismo principio que hacen que funcionen los electroimanes, los motores eléctricos y el opuesto al efecto que sustenta el funcionamiento de los generadores, con un campo magnético móvil a través de un cable). Este efecto hace que se induzcan campos magnéticos en los dispositivos externos, que ejercen una acción sobre el cableado de cobre provocando impulsos eléctricos en ellos; estos

impulsos eléctricos de los cables de cobre crean de nuevo campos magnéticos que actúan a su vez sobre los equipos externos. De este modo los 2 problemas clásicos asociados a interferencias electromagnéticas son producto de que los cables pueden interferir con otros cables y de que los dispositivos electrónicos (como las lámparas de alta potencia) tienen posibilidades de interaccionar con los cables de comunicaciones.

Las interferencias electromagnéticas son también causantes de un problema bastante común en el cableado que se conoce como diafonía. La diafonía se produce cuando dos cables cercanos entre si generan impulsos eléctricos uno en el otro, corrompiendo la señal original. Este problema se reduce considerablemente en los cables de tipo UTP al trenzar los hilos entre si (de hecho el número de vueltas por metro es una de las mayores diferencias que existen entre los cables de categoría 3 y 5).

Direccionamiento Ethernet

Ethernet utiliza direcciones de Media Access Control (MAC, Control de Acceso al Medio) para su estructura de direccionamiento. Siempre que se envíe una trama Ethernet, los dos primeros campos son las dirección MAC de destino y la dirección MAC origen. Estos campos son obligatorios. Si la pila de protocolos no sabe todavía cuál es la dirección MAC del receptor pretendido (o el mensaje se envía a todos los servidores de la red), se usara una dirección MAC especial denominada dirección de difusión (broadcast). La dirección de difusión es todo F, es decir, FF-FF-FF-FF-FF-FF. Esta dirección es importante porque en Ethernet, aunque cada cliente suele recibir todas las tramas (por la topología de bus lógico), dicho cliente no procesará ninguna cuya dirección MAC destino no se corresponda con la suya.

Las tramas de multidifusión pueden también transferirse a capas superiores de la pila de protocolos, ya que las direcciones MAC de multidifusión pueden hacerse corresponder con direcciones IP de multidifusión.

Por ejemplo, si la dirección MAC de un PC es 01-02-03-AA-BB-CC y este PC recibe una dirección MAC de destino 55-55-55-EE-EE-EE, la tarjeta de interfaz de red (NIC: Network Interface Card) rechazará la trama en la capa de enlace de datos, y el resto de la pila de protocolos nunca la procesará. Sin embargo, hay dos excepciones a esta regla. La primera es una difusión general y la segunda el llamado modo promiscuo.

Las difusiones generales se manejan de forma diferente a las trama normales. Si el PC recibe una trama cuya dirección MAC de destino es todo F, enviará la trama a la pila de protocolos, ya que es un mensaje que hay que remitir a todos los PC. En general sólo uno de los PC necesita el mensaje, pero el PC de origen no tiene ni idea de cual es. Así que envía la trama a todos los PC, y la máquina que necesita la trama responde al mensaje. El resto desecha la trama cuando se dan cuenta que no son el dispositivo “buscado”. El aspecto negativo de las difusiones generales es que exigen su procesamiento en todas las máquinas del dominio de difusión (lo que desperdicia ciclos de procesador a gran escala); más aún, en una red conmutada desperdician el ancho de banda.

La otra excepción de la regla es el modo promiscuo. Cuando una tarjeta de red se configura en modo promiscuo, procesa todas las tramas, sea cual sea el destino pretendido para las mismas. Por lo general, una NIC se coloca en modo promiscuo de forma que puedan analizarse cada paquete individual, por medio de un dispositivo denominado analizador de red (coloquialmente conocido también como sniffer o rastreador). Un analizador de red es un software extraordinariamente útil. Si se conoce la estructura de una trama y la lógica y la configuración de las unidades de datos del protocolo (PDU: Protocol Data Unit), es posible detectar y resolver con toda rapidez, muchos problemas de las redes que a primera vista parecerían irresolubles. Sin embargo, estos analizadores tienen una reputación bastante mala, porque se

utilizan también para ver y analizar datos a los que supuestamente no se esta autorizado (como, por ejemplo, contraseñas encriptadas).

Estructura de tramas en Ethernet

Ethernet tiene la capacidad de agrupar los paquetes de múltiples formas. En la figura II.3, se ilustran los tipos estándar de estructuras de tramas de Ethernet.

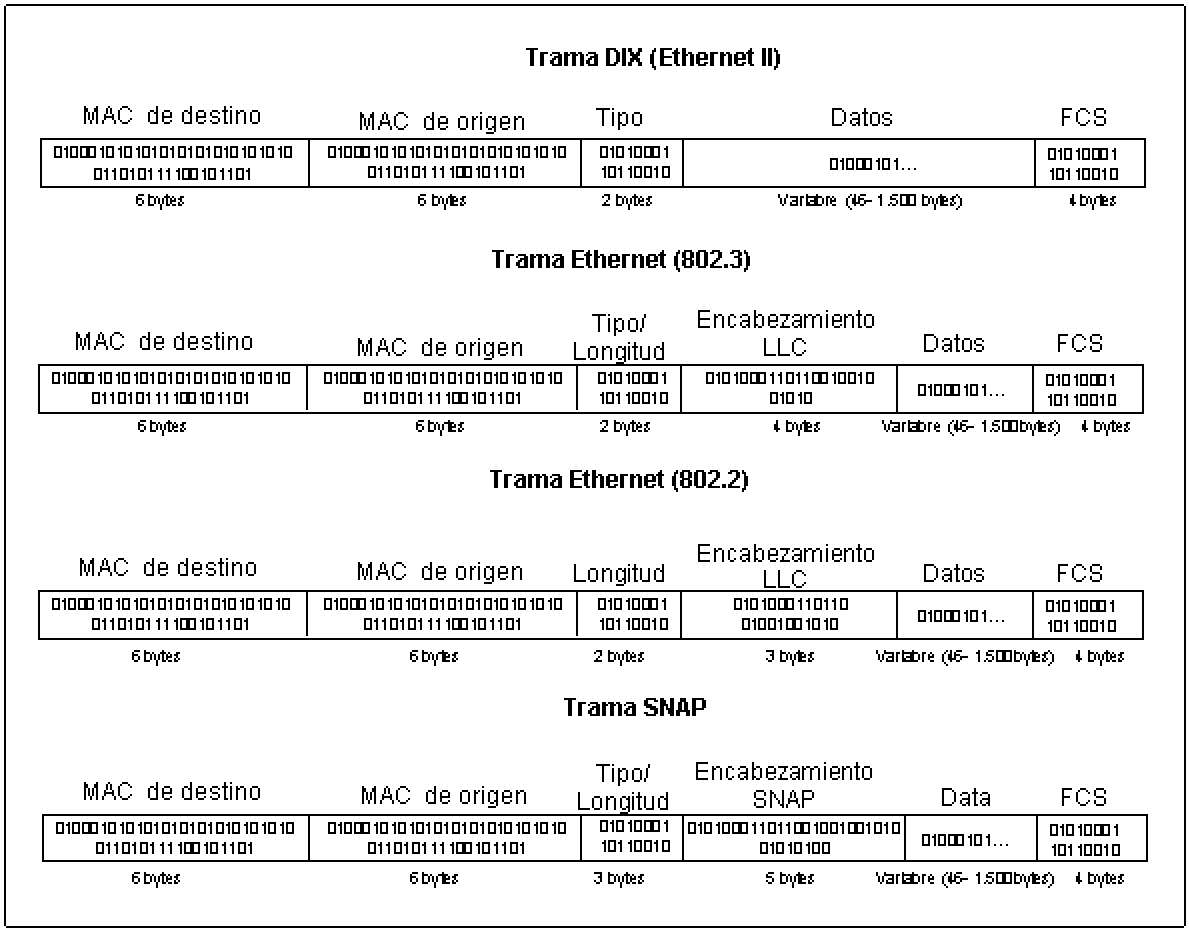


Figura II.3. Tipos de trama estándar de Ethernet

El primer tipo de trama mostrado en la figura se conoce como Ethernet II o DIX (Digital Intel Xerox, así llamado por las empresas que escribieron esta especificación). Este tipo de trama es el más comúnmente utilizado en los diseños

actuales y los restantes tipos no se utilizan en la mayoría de las redes, aunque los equipos de Cisco también los admiten.

El segundo y tercer tipo de trama, ilustrados también en la figura los utiliza principalmente Novell. Aunque ambos contienen técnicamente un campo "tipo", se usan únicamente para especificar la longitud total del paquete y no la clase de protocolo empleada, lo que hace que sean adecuados para IPX/SPX. El segundo tipo suele conocerse por 802.3. Novell le llama 802.3, mientras que Cisco lo conoce por Novell, lo que hace que su denominación genérica sea bastante confusa. El tipo de trama 802.3 se utiliza sobre todo en Netware 3.11 y versiones anteriores dentro IPX/SPX. El tercer tipo de trama se llama genéricamente 802.2 o LLC (Novell lo llama 802.2 y Cisco LLC). Este es el tipo de trama creado por la IEEE para especificar el protocolo de la subcapa LLC que corresponde en funciones a la capa de enlace. Este protocolo es compatible con todos los protocolos de nivel MAC de la serie 802. De esta forma todas las redes locales 802 presentan una interfaz común a la capa de red independientemente de cual sea el medio físico y el protocolo MAC que se esté utilizando. El protocolo LLC está basado en HDLC.

Por último, el tipo 802.3 SNAP (Sub-Network Access Protocol, Protocolo de Acceso a Subredes, llamado Ethernet-SNAP por Novell y simplemente SNAP por Cisco) se creó para aliviar el problema de una trama Ethernet capaz de admitir únicamente dos bytes de tipos de protocolos, lo cual se mostró rápidamente insuficiente, por lo que se ideó un mecanismo que permitiera 'extender' en longitud el campo protocolo. La solución fue reservar un valor en el DSAP y el SSAP (el hexadecimal 'AA') para indicar la existencia de un campo adicional denominado SNAP (Sub-Network Access Protocol), inmediatamente a continuación del campo LLC Control y antes de los datos, que permitiría especificar con holgura cualquier protocolo.

Normalmente en TCP/IP se usa el tipo de trama DIX o Ethernet II. Sin embargo, ello depende en cierta medida del sistema operativo, ya que algunos sistemas operativos (como AIX, la versión UNIX de IBM) son capaces de utilizar varios tipos de tramas.

Debe tenerse en cuenta que lo importante es recordar que para que dos servidores puedan comunicarse directamente han de entender los mismos tipos de tramas.

Ahora se verán de forma resumida los distintos campos contenidos en estos dos tipos de tramas.

a. Dirección de destino. Este campo indica la dirección MAC de destino.
b. Dirección de origen. Indica la dirección MAC fuente.
c. Tipo. Este campo se utiliza para indicar el tipo de protocolo de capa 3 de la parte de carga útil de la trama. Por ejemplo, una designación del tipo 0800 en hexadécimal indica que en el campo de carga útil sigue un encabezamiento IP. Este campo hace así posible que puedan funcionar varios protocolos de capa 3 en un mismo protocolo de capa 2.
d. Longitud. Se utiliza para indicar el tamaño de la trama, de forma que la máquina receptora pueda saber cuando se ha completado.
e. DSAP. Punto de acceso al servicio de destino (Destination Service Access Point), que se usa para indicar a la estación receptora cuál es el protocolo de capa superior a que se envía la trama (semejante al campo tipo). Es una parte del encabezamiento LLC.
f. SSAP. Punto de acceso al servicio origen (Source Service Access Point), que se emplea para indicar al protocolo de capa superior de dónde procede la trama. Forma parte del encabezamiento LLC.
g. Control. Este campo se utiliza para funciones administrativas en algunos protocolos de capas superiores. Forma parte del encabezamiento LLC.
h. OUI. Identificador único de organización (Organizationally Unique ID), empleado únicamente en tramas SNAP. Indica al otro lado de la comunicación qué fabricante creo el protocolo de capa superior utilizado.
i. Secuencia de verificación de tramas (FCS). Este campo es un algoritmo matemático complejo que se usa para determinar si la trama a sufrido algún daño durante el tránsito.

Arbitraje

El arbitraje es el método que controla cómo varios servidores pueden acceder al cable y, más en concreto, qué debe hacerse si varias de estas máquinas intentan enviar datos en un mismo momento. Ethernet utiliza como método de arbitraje el llamado acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD: Carrier Sense Multiple Access with Collision Detection). Para comprender mejor este concepto convine analizar mejor sus componentes.

Detección de portadora significa que, antes de enviar los datos, Ethernet "escuchará" el cable para determinar si existen ya otros datos en tránsito. Supóngase una instalación con varios aparatos telefónicos enganchados en la misma línea. Si se descuelga un teléfono y se oye que hay otra persona hablando, debería esperarse que esta terminara antes de llamar. Pero si no hay nadie mas usando la línea, podrá utilizarse. Eso es lo que hace Ethernet.

Acceso múltiple quiere decir que varias máquinas pueden usar la red al mismo tiempo, lo que produce colisiones y da origen a la necesidad del último componente del método.

Detección de colisiones significa que Ethernet es capas de detectar cuándo se ha producido una colisión para poder reenviar los datos. El modo en que actúa Ethernet para lograrlo carece de importancia, pero cuando se envía una trama, Ethernet escuchará sus primeros 64 bytes para asegurarse de que no se ha producido una colisión con alguna otra. No es necesario "escuchar" toda la transmisión porque en el momento en que se han transmitido los primeros 64 bytes todas las demás máquinas de la red se habrán enterado de al menos la existencia del primer bit de la trama y, por tanto, se abstendrán de efectuar envíos. El tiempo que tarde este proceso recibe el

nombre de “retardo de propagación”. En una red estándar de 10 Mbps, el retardo de propagación se estima en unos 51,2 microsegundos. En Ethernet de 100 Mbps, se reduce a 5,12 microsegundos, que es donde entra en juego la limitación de distancia propia de Ethernet debida a cuestiones de sincronización. Si la longitud total de cable de un segmento lógico de Ethernet (concepto llamado también dominio de colisión), es cercano o mayor que la longitud máxima recomendada, se tendrá un número elevado de colisiones tardías.

Las colisiones tardías se producen después del envío de la “franja” inicial, o tiempo de transmisión de 64 bytes en Ethernet, y por tanto son indetectables para las tarjetas de interfaz de red emisoras. Ello significa que estas NIC no retransmitirán los datos, y el cliente no los recibirá. En cualquier caso, suponiendo que se producen colisiones detectables por las tarjetas de red, estas esperarán un intervalo de tiempo aleatorio (de forma que no se vuelva a producir la colisión con otra estación) y luego reenviarán los datos. Repetirán esta operación hasta un máximo de 16 veces, momento en el cual renunciarán a la trama y la descartarán.

Aunque toda la especificación Ethernet utiliza CSMA/CD como método de arbitraje, en realidad sólo se necesita para modo de operación half-duplex. En entornos full-duplex no hay colisiones, por lo que la función se desactiva.

Conmutación Ethernet básica

La conmutación Ethernet de capa 2 (también llamada puente transparente) responde a un concepto bastante simple. En vez de un concentrador (hub), es un conmutador Ethernet el que procesa y mantiene un registro de las direcciones MAC utilizadas en la red y crea una tabla (Content-Addressable Table [CAM, tabla direccionable por contenidos]) que vincula esas direcciones MAC con puertos. Luego se envía una trama de entrada sólo desde el puerto asociado específicamente a la dirección MAC de destino de la trama. El conmutador Ethernet crea su tabla CAM atendiendo a todas

las transmisiones que se producen en el seno de la red y anotando a través de qué puerto entra cada dirección MAC de origen. Hasta que se establece la tabla CAM, envía la trama a todos los puertos excepto el de origen, ya que todavía no sabe a cuál de ellos se dirige la trama. Este concepto recibe el nombre de "inundación" (flooding).

La principal ventaja de la conmutación es que separa, o segmenta lógicamente, la red en dominios de colisión. Un *dominio de colisión* es un área en la que pueden producirse colisiones. Si un equipo se encuentra en cierto dominio de colisión, los únicos dispositivos con los que sus tramas pueden colisionar son dispositivos de ese mismo dominio de colisión (ver figura II.4).

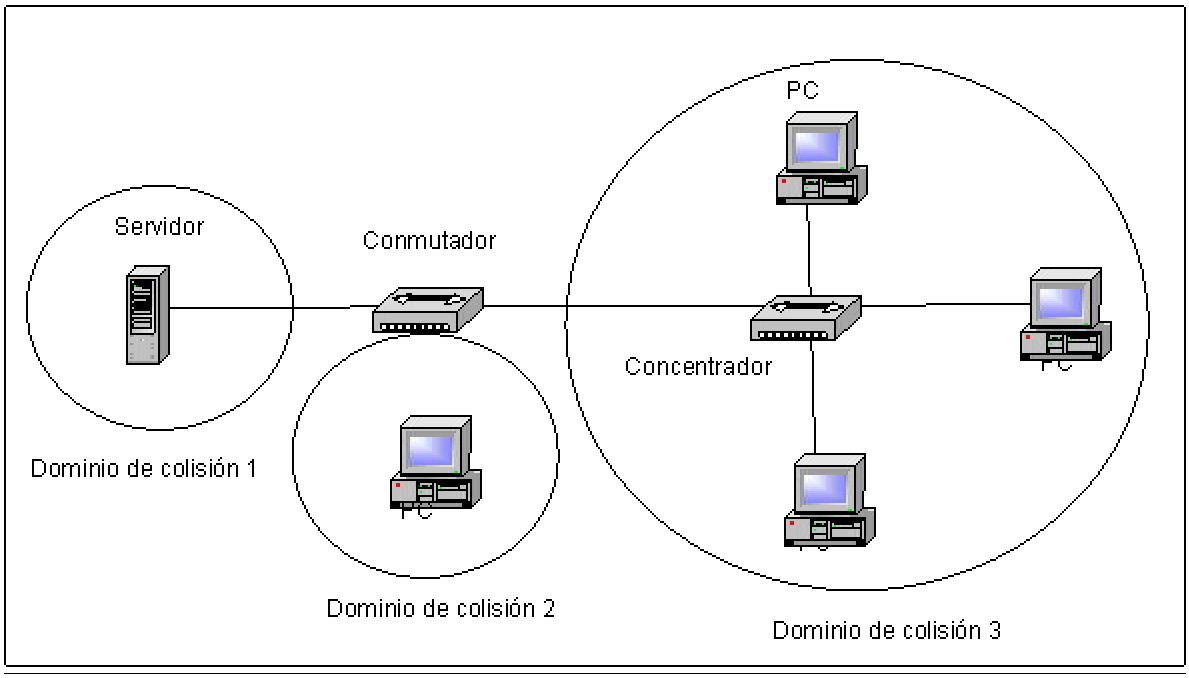


Figura II.4. Segmentación de una red Ethernet

Tecnologías Ethernet

En primer lugar, debe advertirse que todas las tecnologías comunes Ethernet utilizan el método de señalización de banda base, lo que significa que sólo es posible transmitir por el medio una frecuencia en cada momento. La señalización de banda base se diferencia así de la señalización de banda ancha, donde es posible transmitir múltiples frecuencias (normalmente llamadas canales) al mismo tiempo. Para ilustrar esta diferencia puede utilizarse el ejemplo de la televisión por cable que usa transmisiones de banda ancha, lo que hace posible cambiar de canal de manera instantánea. El receptor simplemente sintoniza el canal a la frecuencia que corresponda. Si la televisión por cable utilizara señalización de banda base, el receptor tendría que hacer una petición expresa para recibir un flujo de datos distintos cada vez que se quiera cambiar de canal, lo que conllevaría un retardo.

En segundo lugar cabe señalar que todas las especificaciones de Ethernet habituales se rigen por el siguiente esquema de denominación: velocidad/base/tipo de cable. La velocidad de expresa en Mbps. Base quiere decir "banda base" la tecnología de señalización; y el tipo de cable se representa mediante diversos términos, como T (que significa par trenzado) y 2 (que es coaxial delgado, un cable de 0,25 pulgadas). De este modo 10BaseT quiere decir señalización de banda base a 10Mbps, mediante el uso de cable de par trenzado.

En tercer lugar, las especificaciones Ethernet se adscriben a la llamada regla 5/4/3. Esta regla establece que pueden tenerse hasta cinco segmentos y cuatro repetidores con no más de tres segmentos ocupados por los usuarios. En las redes Ethernet de tipo bus-estrella, esta tecnología funciona de una manera un tanto diferente, pero la regla práctica indica que dos anfitriones no deben estar separados por más de cuatro repetidores o cinco veces la longitud de segmento máxima en metros de cable.

Seguidamente se indicará que la mayoría de los tipos de Ethernet en los equipos de Cisco admiten la "autonegociación", que hace posible que el conmutador configure automáticamente el enlace para que sea de 10 o 100 Mbps, full-duplex o half-duplex.

Sin embargo, ha de saberse también que la práctica sugerida es configurar el modo full-duplex de manera manual, ya que es sabido que la autonegociación (especialmente entre productos de marcas diferentes) falla.

Conmutadores de almacenamiento-reenvío (store-forward) y de atajo (cut-through)

Con la conmutación de almacenamiento-reenvío, toda la trama se recibe y almacena en un buffer de entrada antes de enviarse al puerto de destino. El aspecto atractivo de este enfoque es que se verifica la ausencia de errores en la trama antes de reenviarla. Las tramas con errores se desechan (aunque los errores son pocos comunes en una LAN bien acondicionada). Las operaciones de almacenamiento y reenvío introducen una latencia considerable en el proceso de conmutación (varios milisegundos en el caso de tramas grandes).

Con la conmutación de atajo la dirección de destino se compara con una tabla de puertos de reenvío mientras la trama se está recibiendo. Si el puerto de destino está disponible la trama, se pasa de inmediato al puerto de salida. Obviamente, las operaciones de atajo casi no introducen latencia en el proceso de conmutación. Este tipo de conmutación es muy común, y muchos conmutadores inician con atajo y revierten a almacenamiento-reenvío en caso de presentarse errores. En el caso de tramas pequeñas las diferencias en el desempeño entre la conmutación de almacenamiento-reenvío y atajo son insignificantes.

1.2. Redes de Area Local (LAN: Local Area Network)

Las redes de área local, generalmente llamadas LAN (Local Area Network), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajos en oficinas de compañías y fábricas con el objeto de compartir recursos, por ejemplo impresoras, correo, etc., e intercambiar

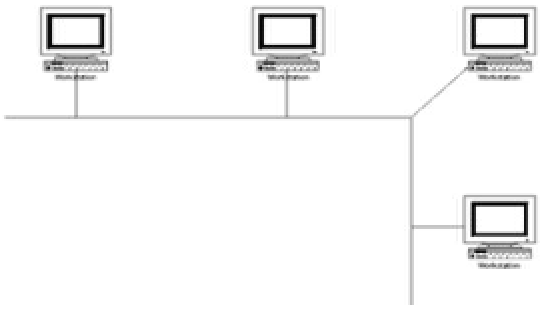
información. Las LAN se distinguen de otros tipos de redes por tres características: su tamaño, su tecnología de transmisión y su topología.
Las LAN están restringidas en tamaño, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano. Conocer este limite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos y también simplifica la administración de de la red.

Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas, como las líneas compartidas de la compañía telefónica que solían usarse en áreas rurales. Las LAN tradicionales operan a velocidades de 10, 100 y 1000 Mbps, tienen bajo retardo (décimas de microsegundos) y experimentan muy pocos errores.

Cuando hablamos de topología de una red, hablamos de su configuración. Esta configuración recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en cómo se trata la información dentro de la red, cómo se dirige de un sitio a otro o cómo la recibe cada estación. A continuación se explica de manera sencilla cada una de las posibles topologías:

Bus

En la topología tipo bus se tiene un enlace por cada nodo, y estos se conectan a un enlace que une todas las estaciones. Esta configuración es típica en Ethernet (figura



II.5).

Figura II.5. Red con topología de bus

Anillo

En esta topología cada nodo tiene dos enlaces, debido a que la información siempre la recibe un nodo por un enlace y la envía a otro nodo por otro enlace. Un ejemplo de esta configuración se encuentra en Token Ring (figura II.6).

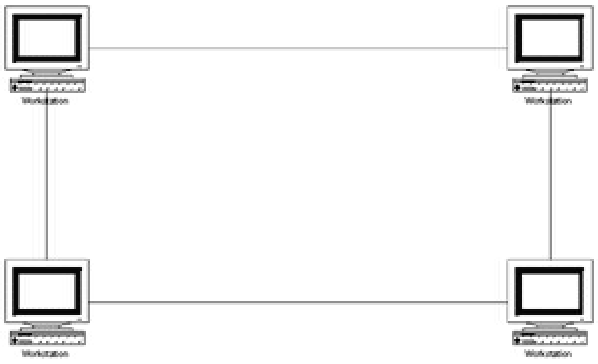


Figura II.6. Red con topología de anillo

Estrella

En esta topología el sistema se centra en una estación donde se conectan todas las demás estaciones. La estación central, para N estaciones, tiene N-1 enlaces, mientras

que las otras estaciones tan sólo tienen un enlace hacia la estación central. (figura II.7).

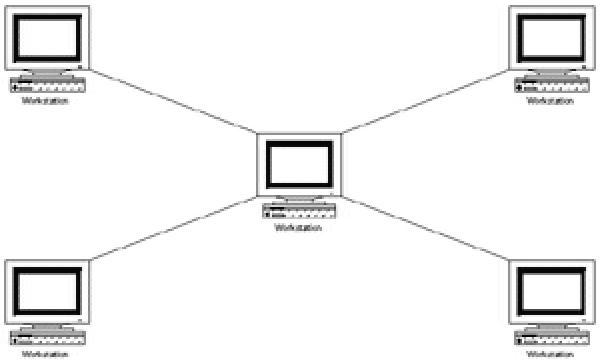


Figura II.7. Red en estrella

Árbol

Todas las estaciones dependen de un ordenador central y se conectan entre ellas a través de los hub que hayan instalados.

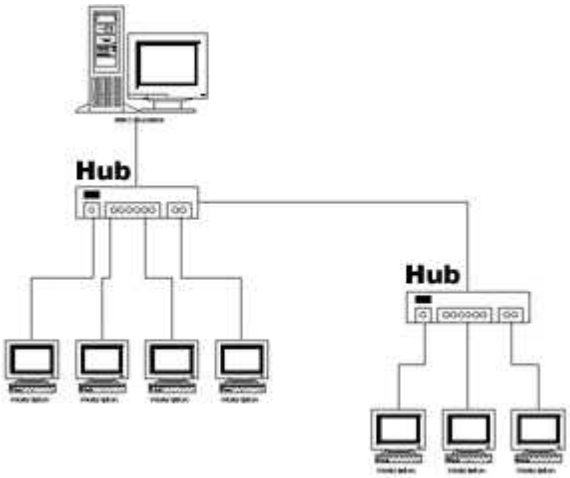


Figura II.8. Red en árbol

Tipos de LAN

En febrero de 1980 el Comité 802 de la IEEE, encargado de la estandarización de LAN, definió los niveles bajos para redes locales, creando la siguiente relación:

Estándares 802.x	Tipo de LAN
802.1	Relación de estándares, gestión de red, interconexión de redes.
802.2	LLC (Logical Link Control)
802.3	Bus con técnica de acceso CSMA/CD
802.4	Bus con paso de testigo
802.5	Anillo con paso de testigo
802.6	Redes de área metropolitana (MAN)
802.7	Recomendaciones banda ancha (broadband)
802.8	Recomendaciones fibra óptica
802.9	Integración voz y datos en LAN
802.10	Seguridad
802.11	Wireless LAN
802.12	LAN's de alta velocidad (Fast Ethernet variante de 802.3)

1.3. LAN de alta velocidad

El crecimiento de las LAN ha sido conducido a través de la introducción de la tecnología Ethernet, al igual que las PC disponibles en el mercado. Como resultado de lo anterior, muchas aplicaciones pueden correr ahora en una red LAN. Pero algunas aplicaciones de multimedia, groupware o imágenes, pueden provocar que las redes se vuelvan más lentas, cuando se trata de redes que utilizan 10 Mbps, como en Ethernet.

La velocidad de las redes y su disponibilidad son requerimientos críticos. Con más aplicaciones que requieren mayores velocidades en una LAN para tener un desempeño aceptable, los administradores de redes se enfrentan a una gran cantidad de opciones para implementar tecnologías de alta velocidad para una LAN.

Por poner algún ejemplo, en una aplicación para una preprensa electrónica, un documento de una sola página, puede producir más de 8 megabytes de datos.

Las PC y estaciones de trabajo (workstations) que cuentan con un alto desempeño, o las nuevas arquitecturas de redes pueden no satisfacerse por las arquitecturas de 10 Mbps. Sus aplicaciones requieren un gran ancho de banda para mover sus grandes cantidades de datos a través de una red de una manera rápida.

Para aquellas empresas con instalaciones Ethernet, es preferible el incrementar la velocidad de su red a 100 Mbps que el invertir en una nueva tecnología LAN. Esta preferencia provocó que se especificara una ethernet de mayor velocidad que operara a 100 Mbps.

En julio de 1993, un grupo de compañías de redes se juntaron para formar la alianza de Fast Ethernet. Este grupo incorporó un bosquejo de la especificación 802.3u 100BaseT de la IEEE, y aceleró la aceptación de dicha especificación en el mercado. El objetivo principal de la alianza es el de asegurar que se pueda pasar del Ethernet tradicional a Fast Ethernet, manteniendo el protocolo tradicional de transmisión de Ethernet.

Cisco realizó contribuciones importantes para el desarrollo de las características básicas y opcionales de la especificación Fast Ethernet. Por ejemplo, en la capa física 100BaseTX, contribuyó con el Multi-Level Transmit (MLT-3), tecnología de codificación en línea que le permite tranmisiones de 100 Mbps, tanto a Fast Ethernet como a FDDI, corriendo bajo la categoría 5 de UTP, también contribuyó para la especificación del MII (Media Independent Interface), el cual soporta transceivers externos en la capa física y que equivale a un AUI (Auxiliary Unit Interface) en

10baseT. Por último, colaboró para la especificación de la operación en full - duplex, primeramente para el estándar de Ethernet de 10 Mbps, para luego proponer el estándar para la especificación de Fast Ethernet.

Ventajes de Fast Ethernet

a. Opera con un throughput de 100 Mbps y soporta tanto a las aplicaciones de Ethernet como a las de token ring.
b. Cuenta con un diseño y una configuración muy sencillos.
c. Ofrece un fuerte soporte para multimedia.
d. Requiere de nuevas tarjetas adaptadoras, hubs y switches.
e. Un enrutador 100VG es utilizado para la comunicación entre segmentos Ethernet y token ring.
f. 100VG y 100BaseT son mejores alternativas que ATM, FDDI, y Fibre Channel.
g. Los adaptadores para ATM y FDDI son mucho más caros que los de 100VG y 100BaseT, pudiendo ir desde $1000 por cada tarjeta.

Comparaciones de las tecnologías LAN de alta velocidad

	100BaseT Fast Ethernet	**100VG-AnyLAN**	**CDDI/FDDI**	**ATM**	**LAN Conmutada (Switching)**
Tasa de datos	100 Mbps	100 Mbps	100 Mbps	25 to 622 Mbps	10 or 100 Mbps
Método de acceso	CSMA/CD	Demand priority	Token passing	Cell based	LAN-based Switching
Tamaño de la trama (frame)	64 to 1500 bytes	64 to 16 KB	64 to 4500 Bytes	53 bytes	64 to 8 KB
Servicios	Asynchronous	Asynchronous and synchronous	Asynchronous and synchronous	Isochronous, asynchronous y synchronous	Asynchronous
Gestión	SNMP y Ethernet MIBs	SNMP MIB	SMT, SNMP	Proprietary MIBs y SNMP	SNMP y Ethernet MIBs
Costo	Bajo	Bajo	En descenso	Muy alto	Bajo
Tolerancia a	Spanning tree		Dual homing	Multiple paths	Spanning tree

fallas			MAC ring		
Aplicaciones	Desktop, workgroup y backbone	Desktop, backbone y multimedia	Desktop, workgroup y backbone	Backbone, WAN, LAN, multimedia y desktop	Desktop, workgroup y backbone

1.4. Redes de Área Amplia (WAN: Wide Area Network)

Una red de área amplia o WAN (Wide Area Network), se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene una colección de máquinas, tradicionalmente llamados servidores (**hosts),** dedicadas a ejecutar programas de usuario (es decir, de aplicación)**.** El termino sistema terminal (end system) se utiliza también ocasionalmente en la literatura. Los servidores (hosts) están conectados por una subred de comunicación o simplemente subred. El trabajo de la subred es conducir mensajes de un servidor a otro, así como el sistema telefónico conduce palabras del emisor al receptor. La separación entre los aspectos exclusivamente de comunicación de la red (subred) y los aspectos de aplicación (los servidores), simplifica enormemente el diseño total de la red.

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

Los elementos de conmutación son computadores especializados que conectan dos o mas línea de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. Desafortunadamente no hay una terminología estándar para designar estos computadores; se les denomina “nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos”, entre otras cosas. Como termino genérico para los computadores de conmutación, se usará la palabra enrutador. En la

figura II.9, cada host generalmente está conectado a una LAN en la cual esta presente un enrutador, aunque en algunos casos un host puede estar conectado directamente al enrutador. La colección de líneas de comunicación y enrutadores (pero no los hosts), forman la subred.

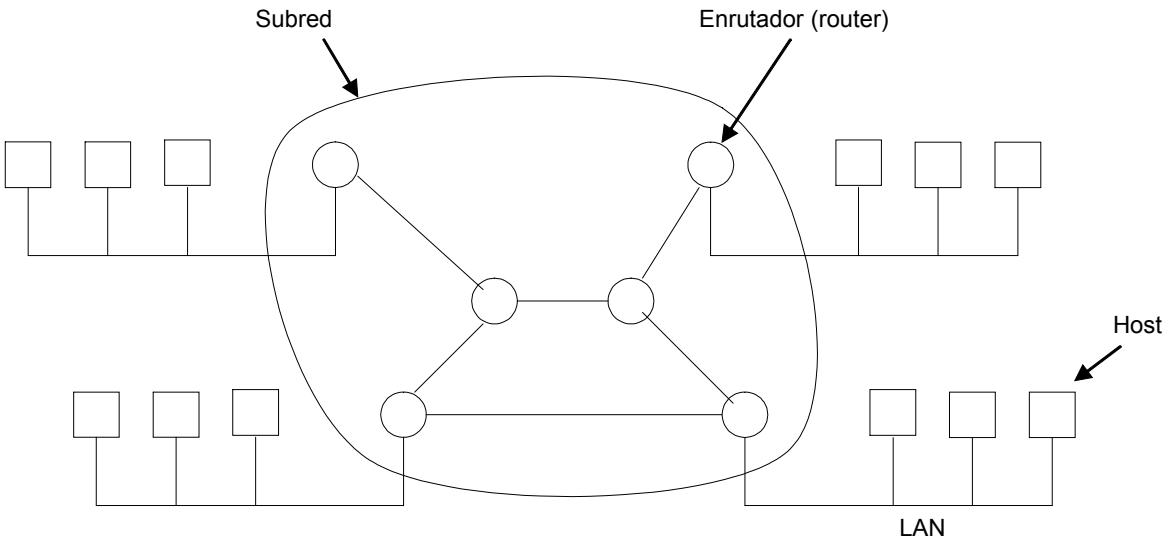


Figura II.9. Relación entre los servidores (hosts) y la subred

En casi todas las WAN, la red contiene numerosas conexiones o líneas dedicadas, cada una conectada a un par de enrutadores. Si dos enrutadores que no comparten una conexión desean comunicarse, deberán hacerlo indirectamente, por medio de otros enrutadores. Cuando se envía un paquete de un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe completo en cada enrutador intermedio, se almacena hasta que la línea de salida requerida esté libre y a continuación se reenvía. Una subred basada en este principio se llama de **punto a punto,** de

almacenar y reenviar o de **paquete conmutado.** Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse **celdas** (ejemplo ATM).

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión del enrutador. La figura II.10 muestra algunas posibles topologías. Las redes locales que fueron diseñadas como tales usualmente tienen una topología simétrica. En contraste, las redes de área amplia típicamente tienen topologías irregulares.

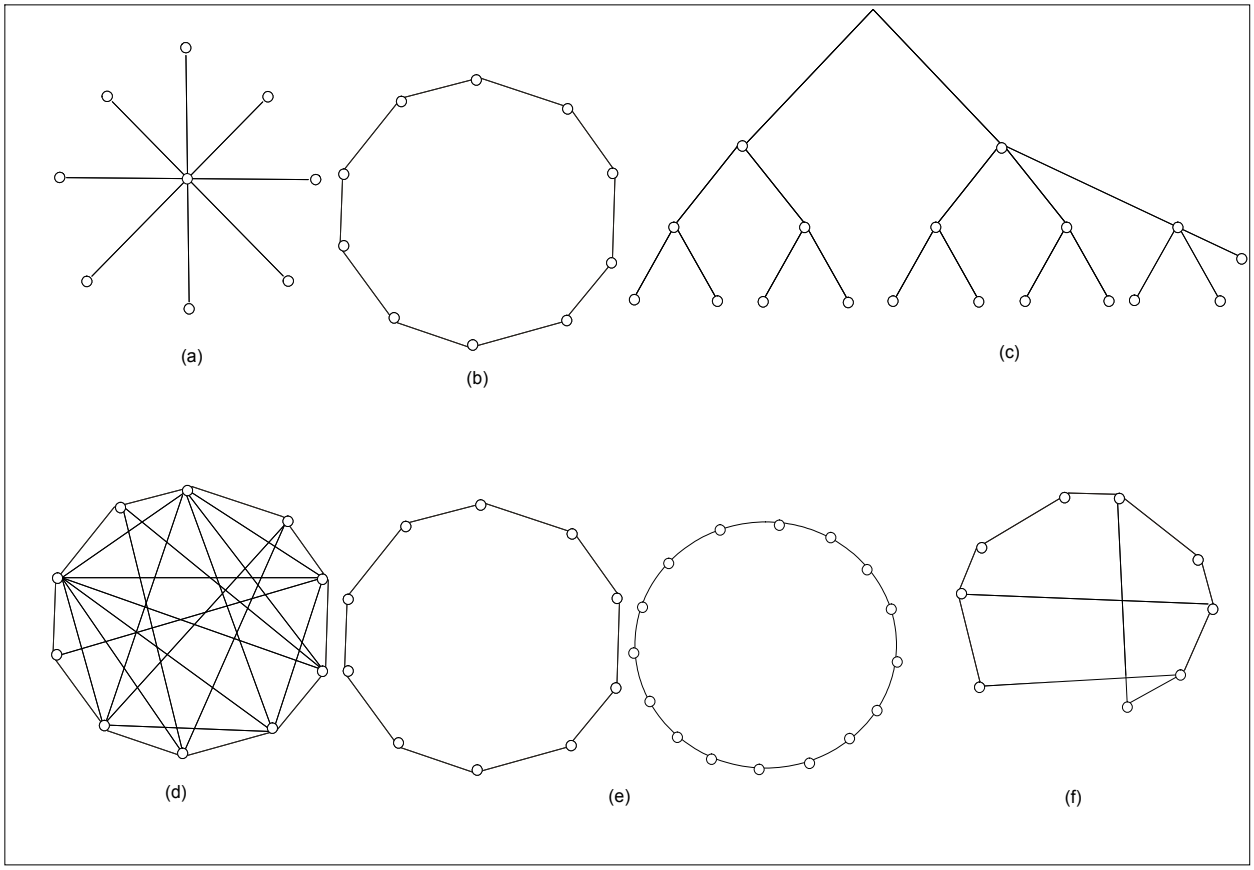


Figura II.10. Posibles topologías para una subred punto a punto. (a) Estrella. (b) Anillo. (c) Arbol. (d) Completa. (e) Intersección de anillos. (f) Irregular.

Una segunda posibilidad para una WAN es un sistema de satélite o de radio terrestre. Cada enrutador tiene una antena por medio de la cual puede enviar y recibir. Todos los enrutadores pueden oír las salidas enviadas desde el satélite y en algunos casos pueden también oír la transmisión ascendente de los otros enrutadores hacia el satélite. Algunas veces los enrutadores están conectados a una subred punto a punto de gran tamaño y únicamente algunos de ellos tienen una antena de satélite.

1.5. VLAN

En una red local (LAN: Local Area Network) típica, un segmento de LAN está definido por la conexión física del cable a un puerto. En este sentido, la configuración y el enrutamiento resultante están determinados por el hardware subyacente. En cambio, una LAN virtual (VLAN: Virtual LAN) define un segmento de LAN en software, como se muestra en la figura II.11. El enrutamiento corre por cuenta de las tablas de reenvío de tramas (*forwarding tables*), que agrupan las estaciones de trabajo en segmentos lógicos y de los puertos físicos asociados a dichas tablas.

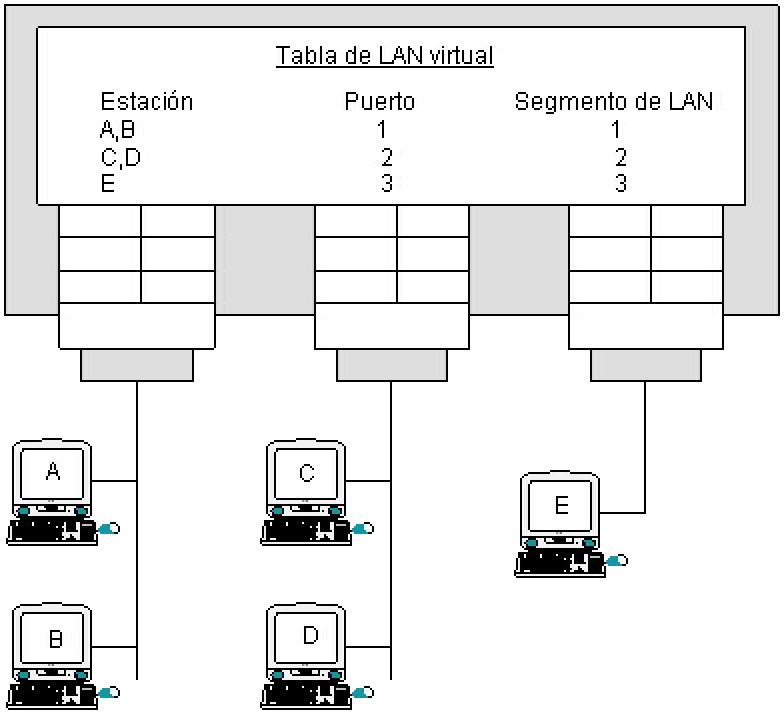


Figura II.11. La red virtual (VLAN)

Una ventaja de las LAN virtuales es su capacidad de mover las estaciones fácilmente. La estación de trabajo se puede cambiar a un puerto distinto y seguir siendo miembro del mismo segmento de LAN virtual. Esta capacidad hace que la organización y reconfiguración de grupos de trabajo sea una tarea relativamente sencilla.

Algunas implementaciones de las LAN virtuales permiten que un dispositivo sea miembro de más de una LAN virtual; por ejemplo, un servidor de nombres o un servidor de archivos podría pertenecer a más de una LAN virtual.
Con las VLAN el entorno se puede dividir en dominios independientes de difusión con un único conmutador y un único enrutador. Gracias a la versatilidad y a los ahorros que proporcionan las VLAN, se suelen considerar como una de las mejoras más útiles conseguidas en la conmutación de capa 2.

El principio básico de las VLAN es bastante sencillo. Se conectan los puertos individuales en un conmutador y se separan en diferentes dominios de difusión. Igual que se hará con múltiples conmutadores, para pasar de un dominio de difusión a otro hay que utilizar un enrutador. Sin embargo, cuando se va más allá de la superficie, aparecen varios elementos avanzados, los cuales se explicaran a continuación.

Definición de una VLAN

En el nivel más básico, la definición de una VLAN consiste en asignar un nombre y un número a la VLAN. Si no se utiliza el proceso llamado *trunking* (compartición), el número y el nombre pueden ser diferentes en cada conmutador de la empresa (aunque se desaconseja por completo esta práctica). Aunque realmente no es obligatorio asignar nombres, generalmente se suelen utilizar para que las VLAN tengan nombres sencillos de recordar; por ejemplo “personal” para el departamento de personal de la empresa.

Utilizar nombres ayuda cuando hay que reconfigurar las VLAN, en caso contrario, en los entornos grandes, habrá que utilizar planos u otra documentación para ayudar a recordar los elementos de la VLAN. En un conmutador Cisco pueden existir varias VLAN por defecto, dependiendo de los tipos de medio que soporta el conmutador. En cualquier caso, VLAN 1 es la VLAN Ethernet por omisión, y también por omisión, todos los puertos Ethernet del conmutador son miembros de esta VLAN.

Pertenencia a una VLAN

La pertenencia a una VLAN define si un dispositivo determinado es miembro de una VLAN. La pertenencia a una VLAN se puede definir de manera estática o dinámica. La forma más habitual es la estática. Cuando la pertenencia se define estáticamente se basa en el puerto de conmutador al que está conectado el dispositivo. Es el método más sencillo para configurar la pertenencia a una VLAN.

La pertenencia a una VLAN definida dinámicamente se basa en las direcciones MAC del dispositivo. Esta configuración es un poco más complicada, pero permite desplazar los servidores según se desee y que la pertenencia les siga, lo que puede resultar muy útil para empresas que pueden desplazar a sus empleados a menudo o que tienen muchos usuarios conectados a la red mediante portátiles.

Etiquetado de VLAN

El etiquetado de VLAN es un proceso por el que se identifica una trama miembro de una VLAN, de manera que otros conmutadores y enrutadores pueden decir en qué VLAN se originó la trama. Como resultado, se pueden enviar tramas desde muchas VLAN sobre el mismo puerto físico, este proceso es llamado compartición (trunking). Este proceso es una mejora extremadamente útil que permite ahorrar puertos en conmutadores y enrutadores, ya que por un sólo puerto de compartición (Trunk) pueden viajar múltiples VLAN.

Sin embargo, también existen un par de problemas con la compartición. Primero, sobre Ethernet se puede efectuar compartición (trunking) sólo con enlaces fast-ethernet o giga-ethernet. Segundo, el etiquetado de VLAN requiere la modificación de la trama Ethernet, lo que significa que todos los conmutadores que participan en el etiquetado de VLAN (al menos en el protocolo ISL: Inter.-Switch Link de Cisco) deben soportar el etiquetado de VLAN. Finalmente se puede efectuar el etiquetado de VLAN de una o dos maneras incompatibles, utilizando el protocolo ISL de Cisco o el IEEE 802.1q de múltiples fabricantes. Por supuesto los conmutadores también deben ser capaces de soportar el protocolo específico que se utilice.

Si se utiliza el protocolo 802.1q como método de etiquetado de tramas, existirá interoperatividad entre diferentes fabricantes, así como conservación del formato de trama estándar de Ethernet.

Protocolo de compartición para VLAN

El protocolo de compartición para VLAN (VTP, VLAN Trunking Protocol) es una característica adicional interesante que se emplea para gestionar las VLAN y que permite asignar definiciones VLAN a múltiples conmutadores de una red. VTP ayuda con las definiciones de las VLAN, permitiendo utilizar números y nombres en las VLAN, para configurar un conmutador independiente y propagarlo por toda la red de la empresa. Obsérvese que VTP no propaga los miembros de las VLAN a todos los conmutadores, sino sólo la definición (nombre, número y otra información básica).

Para llevar a cabo esta proeza, VTP anuncia la información de configuración de la VLAN a todos los puertos compartidos que se encuentren activados. Así, los conmutadores vecinos aprenden cuáles son las VLAN presentes en la red y su configuración. Entonces estos conmutadores propagan la información de VLAN a

otros conmutadores y así sucesivamente. Además, este proceso tiene varias facetas: modos VTP, dominios VTP, versiones VTP y recorte (pruning) VTP.

Modos VTP

VTP puede ejecutarse en un conmutador en tres modos:

a. Cliente. En este modo el conmutador escucha y propaga los mensajes de VTP sobre su dominio de gestión. Efectúa cambios a su configuración VLAN basados en estos mensajes.

b. Servidor. En este modo, el conmutador también escucha y propaga los mensajes VTP sobre su dominio de gestión, pero además genera nuevos mensajes. Este modo permite modificar directamente la información VLAN en el conmutador, incluyendo añadir y eliminar datos de las VLAN desde el dominio de gestión. Modificar la configuración VTP del dominio de gestión produce la actualización de la configuración del número de revisión, esta actualización hace que todos los conmutadores del dominio de gestión actualicen su configuración VTP con la nueva información. Apropiadamente, sólo deben existir uno o dos servidores VTP en cada dominio de gestión.

c. Transparente. En el modo transparente se envía la información VTP, pero se ignoran las configuraciones VLAN contenidas en estos mensajes. La configuración VLAN puede modificarse directamente en un conmutador que se encuentre en el modo transparente, pero esas modificaciones sólo se aplicarán al conmutador local.

Dominio de gestión VTP

La configuración VTP se controla mediante los dominios de gestión VTP. Un dominio de gestión es un nombre específico al que deben pertenecer todos los

conmutadores que participen en un dominio VTP. En otras palabras, si un conmutador no es miembro de un dominio VTP, no obtendrá la información de la VLAN enviada a ese dominio. Los conmutadores deben pertenecer a un único dominio VTP.

Versiones VTP

VTP tiene dos versiones la 1 y la 2. Estas versiones son, por supuesto, completamente incompatibles entre si, y el resultado de configurar ambas en una misma red pueden ser desastrosos. La versión 2 simplemente incluye algunas características adicionales a la de la versión 1, pero sólo dos de ellas tienen una importancia real en la mayoría de las redes, el soporte para las redes Token Ring y el soporte para el modo multidominio transparente VTP.

En un conmutador de la versión 1 los conmutadores en modo transparentes propagan la información VTP sólo si el dominio de gestión de los mensajes VTP se adapta por si mismo. En la versión 2 se propagan todos los mensajes sin tener en cuenta el dominio.

Recorte (pruning) VTP

Finalmente, VTP incluye una mejora excepcional conocida como recorte (pruning) VTP, que permite que VTP determine automáticamente qué redes VLAN tienen miembros en un conmutador determinado y elimina (o recorta) el trafico de difusión (broadcast) innecesario desde esos conmutadores. Esta ventaja puede conducir obviamente a una reducción significativa del tráfico de difusión en redes con poblaciones concentradas de usuarios.

1.6. Modelo OSI

El modelo OSI (Open Systems Interconnection o interconexión de sistemas abiertos), fue diseñado en su origen con el propósito de permitir que existieran protocolos independientes de los proveedores y de eliminar las pilas de protocolos monolíticas, pero este modelo apenas se usa hoy para tales fines. Sin embargo, aún conserva un uso importante, ya que es una de las mejores herramientas de que se dispone en la actualidad para describir y catalogar las complejas series de interacciones que tienen lugar en el diseño de redes. Dado que la mayoría de las pilas de protocolos utilizadas actualmente (como TCP/IP) fueron diseñadas a partir de modelos diferentes, muchos de los protocolos de estas pilas no se adaptan exactamente al modelo OSI. Lo fundamental es mirar el modelo como lo que verdaderamente es: "una herramienta para enseñar y describir cómo tienen lugar las operaciones de una red.

Antes de comenzar a describir el modelo OSI, es importante definir qué es un paquete. Los términos paquete, trama, mensaje y segmento tiene, en esencia, el mismo significado. Simplemente existe en distintas capas del modelo OSI. Podría pensarse en un paquete como un elemento de correo. Si se quiere enviar una carta por correo convencional, se necesitaría una serie de componentes, igualmente se necesita para el envío de un paquete.

a. Carga útil. Este componente es el conjunto de datos que se están enviando, como podría ser un correo electrónico.
b. Dirección de origen. Dirección de retorno del e-mail. Identifica al remitente.
c. Dirección de destino. Dirección de correo del destino, para que el correo pueda despacharse correctamente.
d. Sistema de verificación. En el contexto de un paquete, este componente consiste en un cierto tipo de sistema de control de errores. En este caso se usará la secuencia de verificación de trama (FCS: Frame Check Sequence). Este campo es

un algoritmo matemático complejo que se usa para determinar si la trama a sufrido algún daño durante el tránsito.

Fundamentos del modelo OSI

El modelo OSI ofrece un esquema por capas para el diseño de redes. Algunas de estas capas pueden no utilizarse de manera uniforme en la implementación de un protocolo dado, pero OSI se desglosa de tal forma que cualquier función de una red puede estar representada por una de sus siete capas o niveles. A continuación se describen cada una de las capas del modelo OSI:

Aplicación (capa 7). Esta capa es responsable de la comunicación directa con la aplicación usuario real. Permite escribir las aplicaciones con poco código de red. En vez de ello la aplicación informa al protocolo de la capa de aplicación de lo que necesita, y es responsabilidad de dicha capa traducir la petición a algo que la pila de protocolos sea capaz de entender.

Presentación (capa 6). Esta capa es responsable de todo lo relacionado con el formateo de un paquete: compresión, encriptación, decodificación y correspondencia de caracteres.

Sesión (capa 5). Esta capa es responsable de las conexiones, o sesiones, entre dos puntos extremos (normalmente aplicaciones). Asegura que la aplicación del otro extremo tengo configurados los parámetros correctos para establecer una aplicación bidireccional con la aplicación fuente. Es la responsable de establecer, mantener y terminar las sesiones.

Transporte (capa 4). Esta capa proporciona comunicación entre distintos programas de aplicación. Según el protocolo de que se trate, puede ser responsable de la

detección y recuperación de errores, del establecimiento y terminación de sesiones en la capa de transporte, del multiplexado, de la fragmentación y del control de flujo.

Red (capa 3). Esta capa es responsable principalmente del direccionamiento lógico y la determinación de rutas, o enrutamiento entre agrupaciones de direcciones lógicas. Mientras que los métodos empleados para el direccionamiento lógico varían según la pila de protocolos utilizados, los principios básicos siguen siendo los mismos. Las direcciones de la capa de red se utilizan principalmente para localizar geográficamente un cliente. Esta tarea suele realizarse dividiendo la dirección en dos partes: el campo red y el campo cliente.

Enlace de datos (capa 2). Esta capa es responsable del direccionamiento físico y del control de la tarjeta de interfaz de red (NIC, Network Interface Card). En el caso de Ethernet, puede realizar también el control de flujo. Esta capa añade además el FCS, que ofrece cierta capacidad de detección de errores. En general esta capa se ocupa del arbitraje, del direccionamiento físico, de la detección de errores y de la estructura de tramas.

Física (capa 1). Es la más simple de todas las capas y sencillamente gestiona las características físicas de la conexión de red: cableado, conectores y cualquier otro caso que sea puramente física. Esta capa es responsable así mismo de la conversión de bits y bytes (unos y ceros) a una representación física (impulsos eléctricos, ondas o señales ópticas), y de la conversión de estas representaciones en bits en el lado de la recepción.

Comunicación entre iguales

Se llama comunicación entre iguales al proceso de interconexión de redes en que cada capa se comunica con su capa correspondiente de la máquina de destino. Debe señalarse que las capas no se comunican directamente, pero el proceso es el mismo

que si lo hicieran. Un paquete se enviará de un anfitrión al siguiente con todos los encabezamientos adjuntos; pero, al pasar el paquete a través del modelo del otro lado, cada capa será responsable únicamente de la información de su propio encabezamiento. Todo lo demás lo ve como datos.

Unión de todos

Para terminar con el Modelo OSI se incluye un ejemplo de una comunicación de redes entre dos dispositivos desglosada por capas (figura II.12). Como puede verse, esta muestra no es exacta desde el punto de vista técnico y sólo tiene un fin ilustrativo, para mostrar que cada capa realiza una función determinada, aún cuando esa función no se lleve a cabo en la vida real exactamente de la misma manera que la indicada.

Aplicación (Programa correo electrónico)	Aplicación (Programa correo electrónico)
Capa de Aplicación Formato de datos: Enviado a (vía MAPI):Brian Hill <INICIO DE MENSAJE>	**Capa de Aplicación** Formato de datos: Recibido a (vía MAPI):Brian Hill <MENSAJE RECIBIDO>
Capa de Presentación Formato de datos: Enviado a <SMTP vía TCP/IP> bhill@techtrain.com <Versión mine: 1.0; Tipo de contenido: texto/plano; juego de caracteres=US-ASCII; Compresión: No>	**Capa de Presentación** Formato de datos: Recibido a <SMTP vía TCP/IP> bhill@techtrain.com <Begin Decoding; Versión mime: 1.0; Tipo de contenido: texto/plano; juego de caracteres=US-ASCII; Compresión: No>
Capa de Sesión Formato de datos: Enviado a: <TCP/IP vía DNS> bhill@209.130.62.55	**Capa de Sesión** Formato de datos: Recibido a: <TCP/IP vía DNS> bhill@209.130.62.55
Capa de Transporte Formato de datos: Enviado a: bhill@209.130.62.55 <Establecer sesión TCP: Tamaño de ventana: 32KB; Formato de segmento: 64KB; Total Segments: 4; Bytes totales: 256KB>	**Capa de Transporte** Formato de datos: Recibido a: bhill@209.130.62.55 <Establecer sesión TCP: Tamaño de ventana: 32KB; Formato de segmento: 64KB; Total Segments: 4; Bytes totales: 256KB>
Capa de red Formato de datos: Enviado a: <vía Dirección MAC> 2d6c9e446a32 <Dirección fuente: 165.200.2.23 = 6587da32bb5d6; Dirección de destino final: 209.130.62.55 = 2d6c9e446a32; Dirección de destino intermedia: 209.215.192.10 =4adc500ad23a; Tamaño de paquete: 64KB; Paquete totales: 4; Bytes totales: 256KB>	**Capa de red** Formato de datos: Recibido de: <vía Dirección MAC> 6587da32b5d6 <Dirección fuente: 165.200.2.23 = 6587da32bb5d6; Dirección de destino final: 209.130.62.55 = 2d6c9e446a32; Iniciar creación de paquetes; Tamaño de paquete: 64KB; Paquete totales: 4; Bytes totales: 256KB>
Capa de enlace de datos <Establecer enlace: Número de transceptor: 0; Tamaño de trama: 1500 bytes; Tramas totales: 175; Bytes totales: 256KB; Iniciar numeración de tramas; Iniciar transmisión>	**Capa de enlace de datos** <Enlace establecido: Número de transceptor: 0; Tamaño de trama: 1500 bytes; Tramas totales: 175; Bytes totales: 256KB; Iniciar verificación de secuencia; Iniciar recreación de trama>
Capa física Formato de datos: 0100010101111010001011101 01110101010000101110101011101011...	**Capa física** Formato de datos: 0100010101110100010111010 01110101010000101110101011101011...

Flujo de datos

1.7. Modelo TCP/IP

Implementado en los inicios de la década de los 70, TCP/IP ha experimentado un crecimiento tal que ha llegado ha convertirse en la pila de protocolos dominantes. Inicialmente diseñado por ARPANET, del Departamento de Defensa de los Estados Unidos, TCP/IP constituye una de las pocas pilas de protocolos actualmente utilizadas que es completamente independiente del fabricante.

El Protocolo de Control de Transmisiones/Protocolo de Internet (TCP/IP, Transmission Control Protocol/Internet Protocol), estuvo a punto de desaparecer en el año 1988, cuando el gobierno estadounidense decretó que todos los equipos de redes federales deberían adecuarse a la pila de protocolos OSI a partir de agosto de 1990. Por suerte nadie hizo caso de este anuncio y TCP/IP ha florecido desde entonces.

TCP/IP no es un estándar internacional como el modelo OSI. Se usa extensamente en ambientes de investigación, universidades, manufactura e ingeniería. Es un protocolo que fue concebido originalmente para diseminar información a una comunidad muy dispersa y del mismo estilo. Pero ahora, ya como un estándar de facto, se está usando ampliamente como protocolo principal o para *tunnelin*g en redes multiprotocolares. TCP/IP representa un conjunto relativamente estático de protocolos que suministran

sus funciones de una manera sencilla, práctica, mientras que el estándar OSI es más complejo, con protocolos más densos, pero tiene mayor funcionalidad, entre otras cosas porque los desarrollos en cada una de sus capas evolucionan continuamente. Algunos de los protocolos de la familia TCP/IP suministran los servicios de bajo nivel, correspondientes a las tres capas inferiores del modelo OSI; estos incluyen TCP, UDP, ICMP, IP. Los otros protocolos de la familia TCP/IP están orientados a las capas superiores, de aplicación y presentación, y están dirigidos a tareas o servicios específicos como correo electrónico, transferencia de archivos y acceso remoto.

La aproximación adoptada por los diseñadores del TCP/IP fue mucho más pragmática que la de los autores del modelo OSI. Mientras que en el caso de OSI se emplearon varios años en definir con sumo cuidado una arquitectura de capas donde la función y servicios de cada una estaban perfectamente definidas, y solo después se planteó desarrollar los protocolos para cada una de ellas, en el caso de TCP/IP la operación fue a la inversa; primero se especificaron los protocolos, y luego se definió el modelo como una simple descripción de los protocolos ya existentes. Por este motivo el modelo TCP/IP es mucho más simple que el OSI. También por este motivo el modelo OSI se utiliza a menudo para describir otras arquitecturas, como por ejemplo la TCP/IP, mientras que el modelo TCP/IP nunca suele emplearse para describir otras arquitecturas que no sean la suya propia. En el modelo TCP/IP se pueden distinguir cuatro capas:

Aplicación (capa 7, 6 y 5). Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La experiencia ha demostrado que las capas de sesión y presentación son de poca utilidad, debido a su escaso contenido, por lo que la aproximación adoptada por el modelo TCP/IP parece más acertada.

La capa de aplicación contiene todos los protocolos de alto nivel que se utilizan para ofrecer servicios a los usuarios. Entre estos podemos mencionar tanto los

'tradicionales', que existen desde que se creó el TCP/IP: terminal virtual (TelNet), transferencia de archivos (FTP), correo electrónico (SMTP) y servidor de nombres (DNS), como los más recientes, como el servicio de news (NNTP) y el Web (HTTP).

Transporte (capa 4). Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (host a host) en la red. Aquí se definen dos protocolos: el TCP (Transmission Control Protocol) ofrece un servicio confiable, con lo que los paquetes (aquí llamados mensajes) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar que por ejemplo un host rápido sature a un receptor más lento. Ejemplos de protocolos de aplicación que utilizan TCP son SMTP (Simple Mail Transfer Program, correo electrónico) y FTP (File Transfer Program).

El otro protocolo de transporte es UDP (User Datagram Protocol) que da un servicio no confiable. UDP no realiza control de errores ni de flujo. Una aplicación típica donde se utiliza UDP es la transmisión de voz y vídeo en tiempo real; aquí el retardo que introduciría el control de errores produciría mas daño que beneficio: es preferible perder algún paquete que retransmitirlo fuera de tiempo. Otro ejemplo de aplicación que utiliza UDP es el NFS (Network File System); aquí el control de errores y de flujo se realiza en la capa de aplicación.

La capa de transporte ejecuta dos funciones importantes:

a. Control de flujo con ventanas deslizantes (sliding windows).
b. Verificación proporcionada por números de secuencia y reconocimientos (acknowledgments).

La capa inter-red (internet/ capa 3). Esta capa es el 'corazón' de la red. Su papel equivale al desempeñado por la capa de red en el modelo OSI, es decir, se ocupa de enrutar los paquetes de la forma más conveniente para que lleguen a su destino y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa internet da únicamente un

servicio de conmutación de paquetes no orientado a conexión. Los paquetes pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados de forma adecuada.

A diferencia de lo que ocurre en el modelo OSI, donde los protocolos para nada intervienen en la descripción del modelo, la capa internet define aquí un formato de paquete y un protocolo, llamado IP (Internet Protocol), que se considera el protocolo "oficial" de la arquitectura.

Host-red (capa 2 y 1). Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP no dice gran cosa respecto a ella, salvo que debe ser capaz de conectar el host a la red por medio de algún protocolo que permita enviar paquetes IP. Podríamos decir que para el modelo TCP/IP esta capa se comporta como una "caja negra". Cuando surge una nueva tecnología de red (por ejemplo ATM) una de las primeras cosas que aparece es un estándar que especifica de que forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa internet ya puede utilizar esa tecnología de manera transparente.

Protocolos

Nivel de Aplicación. Existen protocolos para transferencia de archivos (TFTP, FTP, NFS), correo (SMTP), login remoto (telnet, rlogin), gestión de red (SNMP) y gestión de nombres (DNS).

Nivel de transporte. Se encuentran el Protocolo de Control de Transmisión (TCP) y el Protocolo de Datagrama de Usuario (UDP).

a. TCP es un protocolo orientado a conexión (confiable), en un ambiente orientado a conexión, una conexión es establecida entre puntos finales antes de transferir la

información. TCP provee un circuito virtual entre las aplicaciones de usuario final.

b. UDP es no orientado a conexión y no usa reconocimientos. UDP depende de protocolos de capas superiores para la verificación.

Nivel de Inter-red. Varios protocolos operan en esta capa:

a. Protocolo Internet (IP, Internet Protocol) el cual es no orientado a conexión, conocido como el protocolo del mejor esfuerzo.
b. ICMP (Protocolo de Mensajes de Control Internet), provee control y mensajes.
c. Protocolo de Resolución de Direcciones (ARP, Address Resoluction Protocol)

1.8. Modelo de 3 capas Cisco

Para simplificar el diseño, implantación y gestión de las redes, Cisco usa un modelo jerárquico para describir una red (ver figura II.13). Es importante entender este modelo para que realmente ayude a los diseñadores de redes a determinar qué tipo de equipos y qué características son requeridas para cada dispositivo en la red.

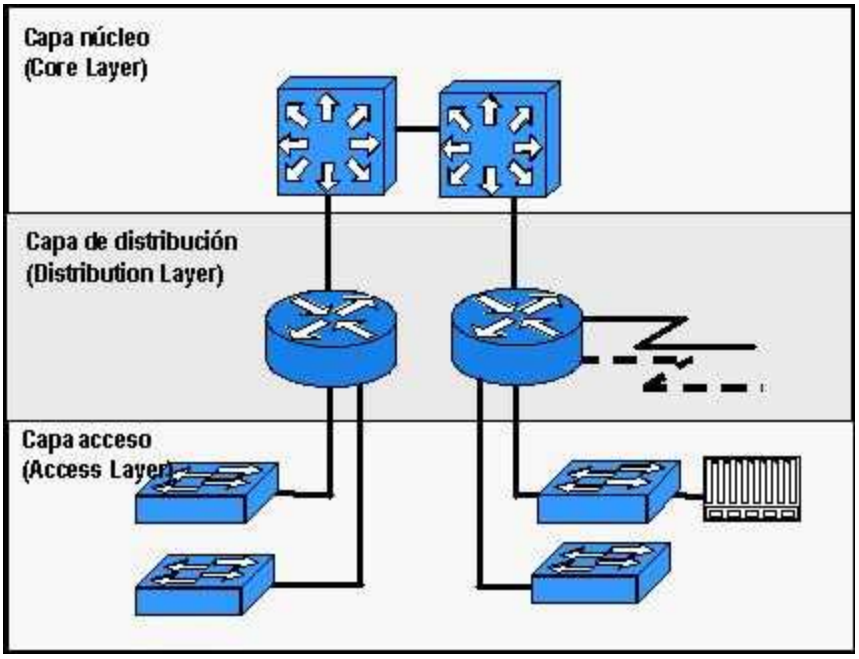


Figura II.13. Modelo de capas Cisco

La demanda de los usuarios y la complejidad de las aplicaciones obligan a los diseñadores e implementadores a usar los patrones de tráfico como un criterio para construir una red y su interconexión. Las redes no pueden dividirse en subredes basándose sólo en el número de usuarios. El crecimiento de servidores que ejecutan aplicaciones globales que afectan directamente la carga a través de la red resulta en la necesidad de técnicas de conmutación (switching) y enrutamiento (routing) más eficientes.

En el nuevo modelo de red, los patrones de tráfico definen el lugar donde son requeridos los servicios por el usuario final; así como la apropiada construcción de una red puede manejar el tráfico generado por dichos usuarios. El modelo jerárquico de tres capas de Cisco esta organizado de la siguiente forma:

- Capa de acceso
- Capa de distribución
- Capa núcleo (core)

1.8.1. Capa de acceso

La capa de acceso es el punto en el cual el usuario final se conecta a la red y por esta razón muchas veces es denominada la capa desktop. Los recursos que el usuario necesita acceder más frecuentemente están localmente disponibles en esta capa. El tráfico desde y hacia los recursos locales (por ejemplo impresoras) es confinado entre los equipos de esta capa (switches) y los usuarios finales. Múltiples grupos de usuarios y sus recursos existen en esta capa.

En muchas redes no es posible proveer a los usuarios de acceso local a todos los servicios, tales como impresoras, dispositivos de almacenamiento de archivos, o accesos al Web. En estos casos, el tráfico de usuario esta diseccionado a otra capa en la red llamada la capa de distribución.

1.8.2. Capa de distribución

La capa de distribución de la red, también referida como capa grupo de trabajo (workgroup), marca el punto entre la capa de acceso y el motor principal de la red, llamado el núcleo (core). La función principal de esta capa es ejecutar la manipulación de paquetes, tal como el enrutamiento, filtrado y acceso remoto (WAN: Wide Area Network). En un ambiente de red esta capa puede tener múltiples funciones, tales como:

- Direccionamiento o área de agregación para acceso a grupos y accesos remotos.
- Enrutamiento de tráfico, para proveer acceso departamental o por grupo de trabajo.
- Definición de dominios de broadcast o multicast.
- Traslación de medios físicos.
- Seguridad.

La capa de distribución puede verse como la capa que provee "políticas basadas en conectividad" porque esta determina si y cómo puede accederse al núcleo o backbone de la red. La capa de distribución determina el camino más rápido a seguir por un requerimiento de usuario y una vez que la capa de distribución determina el camino, envía el requerimiento a la capa núcleo.

1.8.3. Capa núcleo (core)

El único propósito de la capa núcleo (core) en la red es conmutar el tráfico tan rápido como sea posible. Tradicionalmente el tráfico es transportado hacia y desde los servicios que son comúnmente usados por los usuarios. Estos servicios son referidos como servicios empresariales, tales como, correo electrónico, acceso Internet, videoconferencia, etc.

1.9. Enrutamiento

La función real de la capa de red consiste en el enrutamiento de paquetes, desde la máquina origen hasta la máquina destino. En la mayoría de las subredes, los paquetes necesitarán realizar múltiples saltos para terminar el viaje. La única excepción notable es para el caso de las redes de difusión, pero aun aquí, el enrutamiento resulta ser un asunto interesante si el origen y destino no se encuentran en la misma red. Los algoritmos que seleccionan las rutas y las estructuras de datos que utilizan, representan una de las áreas principales del diseño de la capa de red.

El algoritmo de enrutamiento es aquella parte del software correspondiente a la capa de red, que es la responsable de decidir sobre qué línea de salida se deberá transmitir un paquete que llega. Si la subred utiliza datagramas internamente, esta decisión deberá tomarse de nuevo con cada paquete de datos que llega. Sin embargo, si la subred utiliza circuitos virtuales internamente, las decisiones de enrutamiento sólo se tomarán cuando se establezca un circuito virtual nuevo. Después, los paquetes de datos solo seguirán la ruta previamente establecida. A este último caso se le conoce a veces como enrutamiento de sesión, debido a que una ruta permanece durante una sesión entera de usuario (por ejemplo, el caso de una sesión en un terminal o una transferencia de archivo).

Algoritmos de enrutamiento

Los algoritmos de enrutamiento se pueden agrupar en dos clases principales: no adaptativos y adaptativos. Los algoritmos adaptativos no basan sus decisiones de

enrutamiento en mediciones o estimaciones del tráfico o topología actuales; más bien, la elección de la ruta utilizable para ir de la i a la j (para todo i y j), se determina anticipadamente, fuera de línea y se carga en los IMP cuando la red se arranca. A este procedimiento se le denomina a veces enrutamiento estático.

Los algoritmos adaptativos, por otra parte, intentan cambiar sus decisiones de enrutamiento para reflejar los cambios de topología y de tráfico actual. Existen tres familias distintas de algoritmos adaptativos, que se diferencian de acuerdo con la información que utilizan. Los algoritmos globales utilizan información recogida en toda la subred, para intentar tomar decisiones óptimas. A este planteamiento se le conoce como enrutamiento centralizado. Los algoritmos locales operan en forma separada sobre los IMP, y sólo utilizan la información que se encuentra disponible ahí, como la longitud de las colas de espera. A éstos se les conoce algoritmos aislados. Por último, la tercera clase de algoritmos utiliza una combinación de información del tipo global y local; y se les conoce como algoritmos distribuidos.

1.10. Seguridad en Redes

Qué es seguridad

Existen múltiples definiciones de "seguridad", no obstante en este trabajo se entenderá por seguridad en redes la protección frente a ataques e intrusiones a recursos corporativos por parte de entes que no esta permitido el acceso a dichos recursos. Por estos recursos entenderemos tanto el acceso a una carpeta compartida en un servidor, el acceso a los buzones de correo de los usuarios corporativos, o incluso el acceso a una sesión de Telnet de un servidor UNIX interno.

Existen dos enfoques básicos que se han dado al aspecto de la seguridad en redes. Estos dos enfoques han sido tradicionalmente la *defensa en profundidad*, que se caracteriza por proteger cada una de las máquinas susceptibles a ser accedidas por personas no autorizadas, y por otro lado *la defensa perimetral,* consistente en llevar

toda la carga correspondiente a la seguridad en la red corporativa al elemento de conexión de esta red corporativa con el exterior, o con las redes en las que potencialmente se encuentren las personas que puedan querer acceder a los recursos de forma no autorizada (ya que está demostrado que un tanto por ciento elevado de los fraudes informáticos proceden del interior de las propias organizaciones).

La seguridad en redes es esencial debido a que Internet ha hecho que los computadores en redes sean accesibles y vulnerables. Estos computadores se encuentran interconectados sin un límite. Debido a este hecho, las redes corporativas pueden llegar a ser accesibles y vulnerables desde cualquier computador en el mundo. Para las compañías que tienen negocios en Internet, nuevos riesgos se originan para los activos informáticos de las organizaciones.

Amenazas de la Seguridad en Redes

Existen 4 amenazas principales para la seguridad en redes:

- Amenazas no estructuradas
- Amenazas estructuradas
- Amenazas externas
- Amenazas internas

Las amenazas no estructuradas provienen la mayoría de individuos inexpertos que usan herramientas de hacking fácilmente disponibles en Internet. Algunas de estas personas en esta categoría están motivadas por el desafío (reto) intelectual y son comúnmente conocidos como script de niños. Ellos no son hackers talentosos o experimentados, pero tienen una motivación.

Las amenazas estructuradas: Provienen de hackers que están altamente motivados y son competentes. Ellos usualmente entienden los diseños del sistema de redes y sus vulnerabilidades, por lo cual pueden entender y crear script que permiten penetrar en dichos sistemas.

*Las amenazas externas: S*on individuos u organizaciones que trabajan fuera de la compañía quienes no tienen acceso autorizado para los sistemas o computadores. Ellos acceden principalmente desde Internet o mediante servidores de accesos dial-up.

Las amenazas internas: ocurre cuando alguien posee acceso a la red mediante una cuenta al servidor o mediante una conexión física al cable de red. Ellos pueden ser empleados descontentos o contratistas descontentos.

Principales ataques en redes

Existes básicamente tres tipos de ataques de red:

- *Ataques de reconocimiento*: Un intento del intruso para descubrir en una red sistemas, servicios y vulnerabilidades.
- *Ataques de acceso*: Un ataque que realiza el intruso a la red o a los sistemas para obtener información, ganar acceso o escalar sus privilegios de acceso.
- *Ataques de negación de servicio (DoS*): Un intruso ataca la red de manera que se daña o se corrompen los sistemas de las computadoras o niega el acceso a los usuarios de la red, de los sistemas o de los servicios.

Ataques de reconocimiento: Este es también conocido como recolección y en la mayoría de los casos después de esto se realiza un ataque de acceso o un ataque de negación de servicios (DoS: Denial of Service). Los intrusos maliciosos generalmente hacen ping de barridos a la red de destino para determinar qué direcciones IP están utilizadas. Después que esto es llevado a cabo, el intruso determina qué servicios o puertos están activos en los equipos con direcciones IP activos. Con esta información

el intruso consulta los puertos para determinar el tipo de aplicación y versión, también como el tipo y versión del sistema operativo que se está ejecutando en el host de destino.

El reconocimiento es algo análogo al ladrón de un vecindario que busca casas con cerraduras rotas, residencias desocupadas, puertas o ventanas fáciles de abrir. En muchos casos los intrusos van tan lejos que si ven la puerta abierta no entran inmediatamente, sino que buscan vulnerabilidades del servicio que pueda explotar posteriormente cuando hay menos vigilancia.

Ataques de acceso: El acceso se refiere a manipulación de datos no autorizados, acceso a sistemas y escalada de privilegios. La recuperación de datos no autorizados es simplemente leer, escribir, copiar o mover archivos que no pueden ser accesibles al intruso. Algunas veces es muy fácil encontrar carpetas compartidas en Windows 9X, Windows NT o directorios exportados por NFS en sistemas UNIX con acceso de lectura o lectura y escritura a todo el mundo. Los intrusos no tendrán ningún problema para obtener los archivos y frecuentemente acceder a información que es altamente confidencial y completamente desprotegidas a los ojos del espía, especialmente si el atacante es un usuario interno.

El acceso a los sistemas es la capacidad de un intruso para conseguir el acceso a una máquina, a la cual el intruso no tiene acceso permitido (por ejemplo, el intruso no tiene una cuenta o contraseña). Acceder al sistema en forma no autorizada generalmente envuelve ejecutar un script para espiar, o utilizar herramientas que exploten vulnerabilidades conocidas del sistema o de la aplicación que está siendo atacada.

Otra forma de ataque de acceso es la escalada de privilegios. Esto es realizado por usuarios legítimos con bajos niveles de privilegios de accesos, o intrusos que poseen los privilegios de accesos más bajos. El intruso intenta obtener información o ejecutar

procedimientos que no son autorizados en su nivel de acceso actual. En muchos casos esto implica ganar acceso como "root" en un sistema UNIX instalando un sniffer para grabar el tráfico de red, tales como nombre (username) y contraseña (password), los cuales pueden ser útiles para acceder a otra fuente. En algunos casos, los intrusos desean obtener acceso sin llegar a robar información, especialmente cuando el motivo es un reto intelectual, curiosidad o ignorancia.

Ataques de negación de servicios (DoS: Denial os Service): La negación de servicios es cuando un atacante deshabilita o corrompe redes, sistemas o servicios con el fin de negar los servicios a los usuarios que así lo requieran. Esto implica usualmente que los sistemas se caen o se vuelven tan lentos que son inutilizables. Pero un ataque de DoS también puede ser un simple borrado de información o insertar información corrupta en los servidores de la organización. El atacante no necesita primero acceder al destino debido a que todo el mundo puede acceder a estos sistemas. Por esta razón y debido al gran daño potencial, los ataques de DoS son los más temidos, especialmente por los operadores de sitios Web de comercio electrónico (e-commerce).

Seguridad de red vista como un proceso continuo

La seguridad de redes debe ser un proceso continuo construido alrededor de las políticas de seguridad. Una política de seguridad continua es más efectiva debido a que esto promueve las continuas pruebas y la actualización de las medidas de seguridad sobre una base continua. Este proceso de seguridad continua, es representado por el ciclo de seguridad.

Para comenzar este proceso continuo conocido como ciclo de seguridad, es necesario crear una política de seguridad que permita la aplicación de medidas de seguridad. Las políticas de seguridad necesitan llevar a cabo las siguientes tareas:

- Identificar los objetivos de seguridad de la Organización

- Identificar la infraestructura de red con un mapa actualizado de la infraestructura y un inventario.
- Documentar los recursos a ser protegidos

Para crear e implementar una política de seguridad efectiva, se necesita determinar qué es lo que se quiere proteger y de qué manera se va a proteger. Se debe conocer y entender cuáles son los puntos débiles y cómo ellos pueden ser explotados. También se debe entender cómo los sistemas funcionan normalmente y qué se debe saber acerca de cómo trabajan los dispositivos que son normalmente usados. Finalmente, se debe considerar la seguridad física de la red y cómo protegerla. El acceso físico a un computador, a un router, o a un firewall puede dar al usuario un control total sobre ese dispositivo.

Después que la política de seguridad es desarrollada, se aplica el ciclo de seguridad con los siguientes pasos:

Paso 1: Asegurar el sistema. Esto implica definir políticas de red y aplicarlas (implementarlas) en los dispositivos de seguridad (firewall, sistemas de autenticación, encriptamiento, etc.), con el fin de prevenir accesos no autorizados a los sistemas de red.

- Autenticación: Dar accesos únicamente a los usuarios autorizados (por ejemplo, usar un contraseña).
- Encriptamiento: Ocultar el contenido del tráfico para prevenir que se exponga a individuos maliciosos o no autorizados.
- Firewall: Filtrar tráfico de red de manera que sólo se permita tráfico y servicios válidos.
- Prevenir vulnerabilidades: Aplicar medidas que detengan la explotación de vulnerabilidades desconocidas. Esto incluye deshabilitar los servicios que no son necesarios en los sistemas, de tal manera que el hacker tenga menos posibilidades de vulnerar los sistemas.

Paso 2: Monitorear la red para detectar violaciones y ataques en contra de las políticas de seguridad corporativas. Las violaciones pueden ocurrir dentro de un perímetro seguro de la red proveniente de un empleado disgustado o desde la parte de afuera de la red por un hacker. Monitorear la red con un sistema de detección de intrusos en tiempo real, puede asegurar que los dispositivos de seguridad en el paso 1 han sido configurados apropiadamente.

Paso 3: Probar la seguridad. La validación es una obligación. Se puede tener los sistemas de seguridad de red más sofisticados, pero si no trabajan bien, la red puede verse comprometida. Por esta razón se deben probar los dispositivos que se implementaron en el paso 1 y 2 para asegurarse que funcionan adecuadamente.

Paso 4: Mejorar la seguridad. La fase de mejora de la seguridad involucra analizar los datos recolectados durante las fases de monitoreo y prueba, y desarrollar e implementar mecanismos que mejoren la definición de las políticas de seguridad.

Estos cuatro pasos, seguridad, monitoreo, prueba y mejora, deben ser repetidos en una forma continua y deben ser incorporados dentro de versiones actualizadas de la política de seguridad corporativa, ya que los riesgos y vulnerabilidades de redes surgen cada día.

Autenticación, Autorización y Contabilidad

El marco de trabajo para la seguridad basada en usuario se llama autenticación, autorización y contabilidad, del inglés, Authentication, Authorization and Accounting (AAA), pronunciado como triple A. El propósito de AAA es controlar quién tiene acceso a los dispositivos de red, qué servicios puede utilizar una vez que tiene acceso y controlar qué hace con los recursos. A continuación se describe brevemente en que consiste el modelo.

Autenticación (Authentication): Valida la identidad del usuario como auténtica antes de conceder el acceso, es decir, verifica quién es. Los diferentes requisitos de acceso a menudo exigen que se usen distintos métodos de autenticación en la misma red.

Autorización (Authorization): Concede al usuario el privilegio de acceder a las redes y comandos, verifica la integridad, qué tiene el usuario permitido acceder y hacer. La autorización es más complicada que la autenticación, ya que después de haber sido autenticado, se debe proporcionar la información específica referente a qué puede acceder y hacer el usuario.

Contabilidad (Accounting): Recopila datos para hacer seguimiento del uso de los servicios y recursos por parte de un usuario, servicio, equipo, en una hora determinada, día de la semana, etc. La contabilidad no permite ni niega nada, simplemente mantiene un registro de ejecución de lo que hace el usuario (una auditoria).

1.11. Cortafuegos (Firewall)

Un cortafuego (firewall) es un sistema o grupo de sistemas que administran los accesos entre dos redes. Los firewall pueden estar basados en tres tecnologías:

- Filtrado de paquetes: Limita la información dentro de la red basado en información estática de la cabecera del paquete. Un firewall puede usar filtrado de paquetes para limitar la información que se introduce en una red, o la información que se mueve de un segmento a otro. El filtrado de paquetes utiliza listas de control de acceso (ACL: Access Control List) lo cual permite que un firewall acepte o deniegue el acceso basado en tipos de paquetes y otras variables.

Este método es efectivo cuando una red protegida recibe un paquete desde una red no protegida. Cualquier paquete que es enviado a la red protegida y no cumple con el criterio definido por la ACL es desechado. Sin embargo, el filtrado de paquetes presenta los siguientes problemas:

a. Los paquetes arbitrariamente pueden ser diseñados para que cumplan con los criterios de la ACL y pasar a través del filtro.
b. Los paquetes pueden pasar a través del filtro siendo fragmentados.
c. ACL complejas son difíciles de implementar y mantener correctamente.
d. Algunos servicios no pueden ser filtrados.

- Servidor Proxy: Requiere de una conexión entre un cliente detrás del firewall e Internet. Un servidor Proxy es un dispositivo firewall que examina los paquetes en las capas más alta del modelo OSI. Este dispositivo oculta datos valiosos requeridos por el usuario para comunicarse con un sistema seguro por medio de un proxy. Los usuarios que acceden a la red pasan a través de un proceso donde se establece la sesión, se autentica el usuario y se autoriza el acceso. Esto significa que el usuario se conecta a servicios externos mediante un programa proxy que está en un dispositivo puente (gateway). Sin embargo, el servidor proxy presenta los siguientes problemas:

  a. Crea un punto simple de falla, lo cual significa que si la entrada a la red se compromete, entonces la red completa se compromete.
  b. Es difícil añadir nuevos servicios al firewall.
  c. Cuando hay mucho tráfico el rendimiento baja.

- Filtrado de paquetes stateful: Combina lo mejor del filtrado de paquetes y de la tecnología de servidor proxy. Limita la información dentro de una red no sólo basado en la dirección fuente y destino sino también en el contenido de los paquetes de datos. El filtrado de paquete stateful es el método usado por los

firewall Cisco. Esta tecnología mantiene completamente el estado de la sesión. Cada vez que una conexión TCP y UDP es establecida para conexiones de entrada (inbound) o de salida (outbound), la información es registrada en una tabla de flujo stateful.

La tabla de flujo de sesiones stateful contiene tanto la dirección fuente como la dirección destino, el número de puerto, la información de secuenciamiento TCP y flag adicionales para cada una de las conexiones TCP o UDP asociadas con una sesión particular. Esta información crea un objeto conexión y consecuentemente, todos los paquetes entrantes (inbound) y salientes (outbound), son comparados con la tabla de flujo de sesión stateful. Los datos pueden pasar a través del firewall solo si existe una conexión que valide su paso. Con esta metodología, los filtros stateful trabajan con las conexiones y no con los paquetes. Este método es efectivo debido a:

a. Este trabaja sobre conexiones.
b. Este registra datos en la tabla para cada transacción orientada a conexión o no orientada a conexión. Esta tabla sirve como punto de referencia para determinar si el paquete pertenece a una conexión existente o posee una fuente no autorizada.

Firewall del nivel de aplicación (capa 7)

Los firewall a nivel de aplicación son generalmente, hosts que corren bajo servidores proxy, que no permiten tráfico directo entre redes y que realizan logines elaborados y auditan el tráfico que pasa a través de ellas. Estos firewall se pueden usar como traductoras de direcciones de red, desde que el tráfico entra por un extremo hasta que sale por el otro. Los primeras firewall a nivel de aplicación eran poco transparentes a los usuarios finales, pero los modernos son bastante transparentes. Los firewall a nivel de aplicación, tienden a proporcionar mayor detalle en los informes auditados e

implementan modelos de conservación de la seguridad. Esto las hace diferenciarse de los firewall a nivel de red.

Firewall Cisco

El Private Internet Exchange (PIX) Firewall, es un elemento clave en todas las soluciones de seguridad Cisco extremo a extremo (end-to-end). El PIX Firewall es una solución de seguridad de hardware y software dedicada, que controla la seguridad sin impactar el rendimiento de la red. Este es un sistema híbrido debido a que usa lo mejor de ambas tecnologías: filtrado por paquete y servidor Proxy, sin llegar a implementar todas las funcionalidades de las mismas. El PIX Firewall presenta los siguientes beneficios:

- Es un sistema en tiempo real que a diferencia de los servidores proxy no hace uso intensivo de CPU, ya que no procesa paquetes de datos del nivel de aplicación. El PIX Firewall usa un sistema operativo propietario que es un sistema seguro y en tiempo real.
- Algoritmo Adaptable de Seguridad (ASA: Adaptive Security Algorithm). Implementa control de conexiones stateful a través del Pix Firewall.
- Proxy cut-through: Método de autenticación basado en usuario para ambos conexiones, entrantes (inbound) y salientes (outbound), proporciona mejoras en el rendimiento en comparación al servidor proxy.
- Filtrado de paquetes stateful: Método seguro para analizar paquetes de datos, que coloca información acerca de un paquete de datos dentro de la tabla. Para establecer una sesión, la información acerca de la conexión debe corresponder con la información en la tabla.
- Sistema operativo dedicado: El hecho de que el sistema operativo no sea UNIX, Windows NT o cualquier otro sistema operativo, elimina el riesgo asociado con los sistemas operativos de propósito general, permitiendo que el PIX Firewall tenga hasta 500.000 conexiones simultáneas, muchas más conexiones que las permitidas por un firewall basado en UNIX.

Operación Proxy cut-through

Esta operación es un método que verifica transparentemente la identidad de los usuarios en el firewall, y permite o deniega aplicaciones basadas en TCP o UDP. Esto es también conocido como autenticación basada en usuario de conexiones de entrada o salida. A diferencia de un servidor proxy que analiza cada paquete en la capa de aplicación del modelo OSI, el PIX Firewall primero autentica al usuario en la capa de aplicación. Después que el usuario es autenticado y la política es verificada, el PIX firewall cambia el flujo de la sesión a capas más bajas del modelo OSI para acelerar dramáticamente el rendimiento. Esto permite que las políticas de seguridad sean aplicadas en base a la identificación por usuario.
Las conexiones deben ser autenticadas con la identificación del usuario y contraseña antes que pueda ser establecida. La identificación del usuario y la contraseña (password) son introducidas vía una sesión inicial http, Telnet o ftp.

Redundancia (Failover)

La redundancia (failover) provee un mecanismos para que dos PIX firewall idénticos sirvan para la misma funcionalidad. El firewall activo presenta funciones de seguridad normal, mientras que el firewall que está en espera monitorea, y está listo para tomar el control en caso que el firewall activo falle.

El PIX Firewall usa un cable serial para distancia cortas entre los dos equipos (primario y failover), o un cable Ethernet para largas distancias. En ambos escenarios, el PIX Firewall puede ser configurado para **failover stateful**, de manera que las conexiones permanezcan activas cuando ocurre una falla.

Los dos firewall deben ejecutar la misma versión de software. La replicación de configuraciones ocurre bajo las siguientes circunstancias:

- Cuando un firewall secundario completa su **booteo** inicial, el firewall primario replica su configuración completa al firewall secundario.
- Al introducir el comando **write standby** en el firewall primario se pasa la configuración completa al firewall secundario.

Debido a que la replicación de configuración es automática desde el firewall primario al secundario (failover), la configuración debe ser modificada sólo en el firewall activo. Cuando una falla se genera, los mensajes syslog indican la causa de la falla. La detección de la falla y el levantamiento del failover ocurren dentro de 30 a 45 segundos.

Algoritmo de Seguridad Adaptativo (ASA)

El corazón del PIX Firewall es el ASA. El ASA mantiene la seguridad de los perímetros de red controlados por el firewall. ASA crea flujo de sesiones basadas en direcciones fuentes y destinos. Este emite aleatoriamente números de secuencias TCP, números de puertos y banderas (flag) adicionales TCP antes de completar la conexión. Esta función está siempre en operación, monitoreando los paquetes retornados para asegurar que ellos son válidos y permitir en una dirección entrante, saliente (inbound, outbound) conexiones sin una configuración explicita para cada sistema interno o aplicación. Los números de secuencias aleatorias buscan minimizar el riesgo de ataques por números de secuencia TCP. El conocimiento de ASA es fundamental para implementar la seguridad de acceso a Internet debido a que realiza las siguientes tareas:

- Obtiene la sesión identificando los parámetros, dirección IP y puertos para cada una de las conexiones TCP.
- Registra los datos en una tabla de flujo de control stateful y crea un objeto sesión.

- Compara los paquetes de entrada y salida con las conexiones de la tabla de flujo de sesión.
- Permite que los paquetes de datos fluyan a través del PIX Firewall sólo si una conexión existe para validar su paso.
- Temporalmente configura un objeto conexión hasta que la conexión sea terminada.
- Monitorea los paquetes de retorno para asegurar que son válidos.
- Emite números de secuencias aleatorios TCP para minimizar el riesgo de ataques.

ASA mantiene perímetros seguros entre las redes controladas por el PIX Firewall. Las conexiones orientadas a conexión stateful de ASA crean flujos de sesión basadas en direcciones fuentes y destinos. ASA aleatoriamente emite números de secuencias TCP, número de puertos, y banderas TCP antes de completar la conexión. Esta función siempre está ejecutándose y monitoreando los paquetes de retorno para asegurar la validez de los mismos.

Ejemplo de niveles de seguridad ASA

Los niveles de seguridad definen si una interfaz es confiable (y más protegida) o no confiable (y menos protegida) con respecto a otra interfaz. Un interfaz es considerada más confiable (más protegida) con respecto a otra interfaz si el nivel de seguridad es más alto que el nivel de seguridad de la otra interfaz y es considerada menos confiable (y menos protegida) en relación a otra interfaz si su nivel de seguridad es más bajo que el nivel de seguridad de la otra interfaz.

La principal regla para los niveles de seguridad es que una interfaz con más alto nivel de seguridad puede acceder una interfaz con un menor nivel de seguridad. Recíprocamente, una interfaz con un nivel de seguridad más bajo no puede acceder a una interfaz con un nivel de seguridad más alto sin un ***conduit*** o ***una lista de control***

de acceso (ACL). El rango de niveles de seguridad van de 0 a 100, y las siguientes son las reglas más específicas para estos niveles de seguridad:

- Nivel de seguridad 100. Este es el nivel de seguridad más alto para la interfaz interna (inside) del firewall. Es la configuración por defecto para el Pix Firewall y no puede ser cambiada. Debido a que 100 es el nivel de seguridad de la interfaz más confiable, la red corporativa debe instalarse detrás de ésta. Esto significa que nadie puede tener acceso a esta red al menos que se otorgue un permiso especifico. Igualmente cada dispositivo detrás de esta interfaz puede tener acceso al lado externo de la red corporativa.
- Nivel de seguridad 0. Este es el nivel de seguridad más bajo para la interfaz externa (outside) del Pix firewall. Esta es la configuración por defecto para el Pix Firewall y no puede ser cambiada. Debido a que 0 es el nivel de seguridad de la interfaz menos confiable, se debe configurar la red no confiable detrás de esta interfaz de manera que no se tenga acceso a otra interfaz a menos que se de un permiso explícitamente. Esta interfaz usualmente se usa para la conexión a Internet.
- Niveles de seguridad del 1 al 99. Estos son los niveles de seguridad que se pueden asignar a las interfaces que se encuentran en los perímetros del Pix Firewall. Se deben asignar los niveles de seguridad basados en el tipo de acceso que cada uno de los dispositivos tenga.

1.11.1. Comprender las DMZ

Una zona desmilitarizada (DMZ, Demilitarized Zone), también conocida como subred protegida o “apantallada”, constituye una medida de seguridad adicional para garantizar que la disponibilidad de recurso de acceso público no comprometa la seguridad de la red interna. Una DMZ separa los recursos de acceso públicos de los recursos completamente privados colocándolos en subredes distintas, autorizando el bloqueo de los recursos privados e incluso proporcionando seguridad a los recursos públicos. Las DMZ se pueden estructurar de diversas formas:

a. DMZ con cortafuegos individuales. Este tipo de DMZ consta de un cortafuego individual con tres o más interfaces y al menos una de las interfaces conectada a la red interna, una a la red externa y otra a la DMZ. Esta DMZ son más eficaces en términos de costo.
b. DMZ con cortafuegos dual. Esta clase de DMZ es una de las más comunes y consiste en un cortafuego externo, un cortafuego interno y una DMZ situada entre ambos. Los recursos internos quedan protegidos por el cortafuego interno, mientras que los recursos de la DMZ están protegidos por el cortafuego externo. Este tipo de estructura DMZ puede incrementar la seguridad sustancialmente. El cortafuego dual proporciona una protección suplementaria a los recursos internos. Sin embargo, el problema surge cuando se consideran que la DMZ con cortafuego dual tiende a ser mucho más cara que una con cortafuego individual, y al mismo tiempo, su manejo puede requerir conocimientos adicionales.
c. DMZ con cortafuegos triples. Se trata de una estructura que utiliza tres cortafuegos para proteger la red interna, y que al mismo tiempo utiliza DMZ interna y externa. Esta configuración de cortafuegos sólo se usa en instituciones en las que la seguridad es un elemento muy importante. Aunque resultan extremadamente seguros, estos cortafuegos son caros, tanto en lo que respecta a su implantación como a su mantenimiento.

1.11.2. Listas de acceso

Las listas de acceso, también llamadas listas de control de acceso (ACL, Access Control Lists), constituyen los mecanismos principales de filtrado de paquetes en la mayor parte de los enrutadores Cisco. Así mismo las ACL se utilizan para otra serie de funciones, incluyendo el filtrado de ruta y la utilización de determinados comandos “show”. Por ello, resulta necesario tener un sólido conocimiento sobre las ACL para poder resolver cualquier clase de problema y configurar los equipos de Cisco en la mayoría de las redes. Las ACL permiten controlar qué clase de

coincidencia efectúa un enrutador en relación con una determinada función, como el envío de paquete.

Por ejemplo, si no existe una forma de especificar condicionalmente qué paquetes pueden enviarse de una red a otra (como es el caso de Internet), el usuario tendrá que autorizar el envío de todos los paquetes (lo cual hace que la red en cuestión sea un objetivo sencillo para los hackers), o bien rechazar todos los paquetes (lo que haría imposible la conectividad). El control general a través del filtrado de paquetes, constituye una función primaria de las ACL. Sin embargo, las ACL se pueden utilizar como comandos más complejos (como los mapas de rutas o las listas de distribución), lo que proporciona un grado de control muy preciso sobre la funcionalidad del enrutador. En resumidas cuentas, siempre que sea preciso utilizar alguna clase de coincidencia condicional, las ACL suelen ser la herramienta a elegir.

1.11.3. Uso de NAT y PAT

El NAT permite que se guarde la dirección de red interna detrás del firewall, de tal manera que sea desconocida para la red externa. El NAT lleva a cabo esto trasladando las direcciones de red interna (las cuales no son únicas globalmente) a direcciones IP aceptadas globalmente antes que el paquete sea enviado a la red externa.

Cuando un paquete IP de salida es enviado desde un dispositivo de la red interna, este alcanza el firewall el cual tiene configurado NAT (figura II.14). Así, la dirección fuente es extraída y comparada con la tabla que contiene direcciones internas con traslaciones existentes. Si la dirección del dispositivo está en la tabla, entonces esta es trasladada. Una nueva entrada es creada para ese dispositivo y es asignada una dirección IP desde un pool de direcciones IP globales. Después que esta traslación ocurre, la tabla es actualizada y el paquete IP trasladado es enviado. Después de un periodo de tiempo configurado por el usuario (o por defecto 2 minutos) durante el cual no ha sido traslado el paquete para esa dirección IP particular, la entrada es

removida de la tabla y la dirección global es liberada para ser usada por otro dispositivo interno. En la figura el host 10.0.0.11 inicia una conexión de salida. El firewall traslada la dirección fuente a la dirección 192.168.0.20, de manera tal que los paquetes que proviene del host 10.0.0.11 son vistos desde fuera como si tuvieran una dirección 192.168.0.20

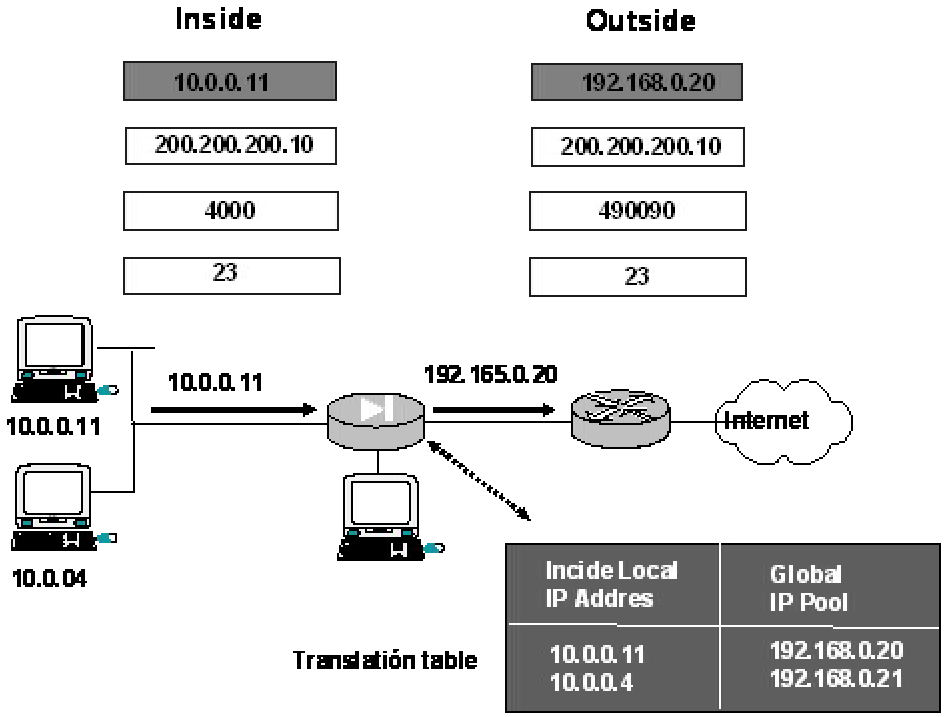


Figura II.14. Funcionamiento del NAT

La traslación de direcciones de red (NAT, Network Address Translation), puede simplificar la vida del programador evitando que tenga que concentrarse en los accesos no autorizados a clientes situados en la red privada. Por definición la NAT y la traslación de direcciones de puerto (PAT, Port Address Translation), generan tablas de traslación dinámicas (aunque también cabe la posibilidad de definir entradas estáticas) para autorizar clientes procedentes del mundo externo, de modo que entren en la red interna. Así mismo estas entradas dinámicas se crean sólo cuando un cliente interno necesita acceder al mundo externo. Si un cliente externo desea comunicarse con un cliente interno y el mecanismo NAT no dispone de una entrada en la tabla de traslación para el cliente de destino, el paquete se rechaza. Por consiguiente, como si se tratara de un subproducto NAT, los recursos internos ya tiene un nivel de seguridad similar al de una ACL reflexiva.

Si en la red interna existen clientes que deben resultar accesibles desde clientes situados en la red externa (como puede ser el caso de un servidor Web), basta con agregar una entrada estática en la NAT, similar a la entrada que habitualmente se colocaría en un filtro de paquete estándar, exceptuando el hecho de que hay que especificar la dirección externa y el puerto asociado con el servidor Web, así como la dirección interna y el puerto asociado con dicho servidor.

1.12. Websense Enterprise

El problema del uso indebido de Internet en los lugares de trabajo se ha incrementado a una velocidad exponencial. Para el 2003, se estimó que más de 260 millones de empleados en el mundo tengan acceso a Internet. Es claro que el acceso a una computadora de escritorio proporciona una inmediata oportunidad para la distracción. A pesar del riesgo potencial que Internet representa, estos necesitan acceso a dicha red.

En la Fundación Caracas se ha utilizado el Cisco PIX como un firewall capa 3. A pesar de que Cisco lo presenta como un firewall de capa 7 mediante su comando

"fixup", sus bondades a nivel de contenido son muy limitadas. De hecho, una de los productos que se integran con el PIX para el filtraje a nivel de aplicación es el Websense Enterprise.

Websense Enterprise es una solución que permite a las compañías monitorear y administrar transparentemente el uso de Internet por parte de los empleados. Websense incrementa la productividad, filtra sitios en Internet que pueden ser ofensivos y de alto riesgo para las organizaciones, permite implantar la política de uso de Internet en la organización y mejora el ancho de banda del enlace Internet, evitando el uso indebido de sus recursos.

Websense se basa en una tecnología de filtrado. El chequeo a través de filtrado requiere que todas las páginas del Web pasen a través de un control de Internet, como puede ser un firewall o un servidor proxy. Websense está integrado con estos componentes de control y verifica cada petición para determinar si debe ser permitida o denegada. En la gráfica II.15 se muestra la arquitectura de Websense. Cada una de las respuestas a las peticiones es registrada con propósitos de reporte.

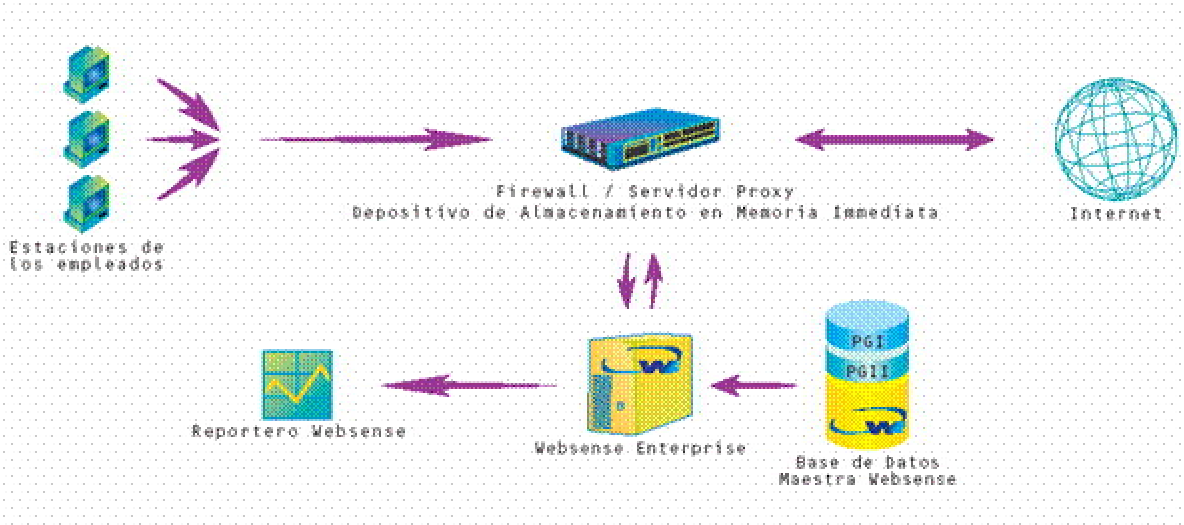


Figura II.15 Arquitectura de Websense Enterprise

Websense filtra el contenido de Internet junto con la **Websense Master Database** con más de 4 millones de sitios (que comprenden más de un billón de páginas Web). Esta base de datos está organizada en **más de 80 categorías**, entre ellas, MP3, apuestas, compras y contenido para adultos. Se puede optar por bloquear o permitir el acceso a categorías individuales por usuario, por grupo o por horario.

Websense perfecciona constantemente su base de datos de sitios, utilizando tecnología de inteligencia artificial y analistas profesionales de Internet. Diariamente se agregan sitios nuevos a la base de datos y Websense la actualiza automáticamente para garantizar que las organizaciones estén al día con la rápida evolución de Internet.

Administración de la Política Adaptable

El software de Websense se adapta para brindar apoyo a la política de acceso a Internet de una organización. Websense Enterprise puede acomodarse muy bien a cualquier política de acceso a Internet, ya que cuenta con ocho opciones de administración diferente y flexible. Además de poder bloquear y permitir acceso, otras características que se incluye son:

- Cuotas basadas en tiempo: Se puede permitir que los empleados tengan acceso a páginas no relacionadas con el trabajo por períodos de tiempo limitados, pero apropiados. Por ejemplo, permitir el acceso a sitios para operaciones bancarias o compras por hasta 20 minutos por día.
- Continuar y/o diferir: Permite que los usuarios escojan "continuar" navegando en las páginas bloqueadas que ellos consideren relacionadas con el trabajo o "diferir" la navegación personal a otro tiempo fuera del horario de trabajo. Las páginas diferidas están automáticamente marcadas para los empleados en la página AfterWork.com. Esta es una página gratuita, hospedada y mantenida por Websense.

- Horas del día: Todas las opciones de filtración pueden establecerse por horas específicas del día. Por ejemplo, se puede bloquear el acceso a compras durante las horas laborables y permitir el acceso en todas las demás horas.
- Políticas de acceso a Internet a la medida: Establecimiento del acceso a Internet por usuario, grupo, departamento, estación de trabajo o red. Por ejemplo, se puede clasificar el acceso por función, tal como Gerencia, Departamento de Compras o establecer el acceso para personas tales como el Administrador de servidores, Asesor en Finanzas, etc.
- Apoyo total a usuario y/o grupo: Permite acomodar las políticas de acceso basándose en los usuarios y grupos, como se define en Windows NT, Directorio Activo de Windows 2000 (modo mixto) y servicios de directorio accesibles LDAP (iPlanet). Los registros y reportes incluyen los nombres de los usuarios y grupos, lo que permite hacer fácilmente un análisis.
- Listas con "Sí": Cuando sea conveniente, emplee listas con "sí" para permitir el acceso únicamente a sitios específicos. Por ejemplo, para permitir que el Departamento de Consultoría Jurídica tenga acceso únicamente a las páginas de los tribunales.

Clasificación de Contenido Inteligente

Websense utiliza los métodos más avanzados para recolectar y clasificar el contenido de la Red (ver figura II.16 y el Anexo A).

- Filtro por nombre y tipo de archivo: Permite reglamentar las descargas de archivos por nombre o extensión de archivo, incluyendo audio, video e imágenes de anuncios.
- Categorías dinámicas de base de datos: permite la recepción automática de nuevas categorías de base de datos de Websense, conforme vayan surgiendo nuevos tópicos en Internet.

- Nombres de categorías en idioma local: Para el uso internacional, los nombres de categorías se encuentran disponibles en japonés, español, francés, alemán, chino y coreano.
- Filtración avanzada con grupos Premier: Permite una administración avanzada de Internet, ofreciendo filtrado por las categorías de los Grupos Premium:

  Grupo Premier I – Administración de Productividad: filtra banners, sitios de mensajería instantánea y otros.

  Grupo Premier II – Administración de Ancho de Banda: Permite administrar el ancho de banda mediante la filtración de medios publicitarios de anuncios, radio en línea y otros sitios con archivos extensos que utilizan gran ancho de banda.

  Grupo Premier III: Permite definir una capa de seguridad adicional a la red bloqueando los sitios infectados con código malicioso.

- Filtración opcional de palabras claves en URL: Permite la filtración mediante el bloqueo de sitios cuyos URL contengan palabras específicas, tales como "sexo" y "porno".

DATOS MAESTRA

Armas
Asuntos Ilegales y/o Cuestionables
Búsqueda de Empleos
Compras
- Subastas por Internet
- Bienes Raíces

Comunicaciones por Internet
- Charlas en la Red
- Correo Electrónico con Base en la Red

De Mal Gusto
Defensa del Aborto
- Páginas en Pro de la Decisión del Aborto
- Páginas Pro-vida

Deportes
- Clubes Deportivos de Cacería y Tiro al Blanco

Drogas (de acuerdo a como son caracterizadas por la ley en los Estados Unidos)
- Abuso de Drogas
- Complementos y Suplementos Alimenticios No Regulados
- Medicamentos con Prescripción Medica
- Mariguana

Educación
- Instituciones Culturales
- Instituciones Educativas
- Materiales Educativos

Entretenimiento
- MP3

Eventos Especiales
Gobierno
- Milicia
- Organizaciones Políticas

Grupos Activistas
Grupos de Apoyo
Juegos
Juegos de Azar con Apuestas
Mal Gusto
Material para Adultos
- Desnudos
- Educación Sexual
- Lencería y Trajes de Baño
- Páginas con Contenido para Adultos
- Sexo

Militancia y/o Extremistas
Negocios y Economía
- Información y Servicios Financieros

Noticias y Medios de Comunicación
- Publicaciones Alternativas

Racismo y Odio
Religión
- Religiones No Tradicionales
- Religiones Tradicionales

Salud
Estilos de Vida y Sociedad
- Alcohol y Tabaco
- Asuntos de Grupos Homosexuales, Gay y/o Lesbios
- Páginas Web Personales
- Pasatiempos
- Personales y Citas
- Restaurantes

Tecnología Informática
- Motores y Portales de Búsqueda
- Páginas de Hospedaje en la Red
- Páginas de Traducción de URLs
- Piratería Cibernética
- Sistemas para Evadir Proxys

Turismo
Violencia
Vehículos

Grupo Premier I (PGI) – Administración de Productividad

- Anuncios
- Corredurìa y Comercio en Línea
- Descarga de Programas Gratuitos y/o Software
- Mensajería Instantánea
- Páginas de Pago por Navegar
- Tableros para Mensajes y Clubes

Figura II.16 Categorías Websense

Registro y Reporte

Esta parte permite a la organización analizar el uso que se hace del servicio Internet a través de las funciones completas de registro y reporte del Reportero Websense.

- Reporte sobre la actividad en Internet: Se puede elegir entre más de 60 reportes, tablas y gráficas, incluyendo los sitios visitados más frecuentemente, así como los usuarios más activos.
- Reportes que se ajustan a las necesidades de la organización: Diseñe los reportes para enfocarse en la información que sea importante para su organización.
- Programación y entrega de reportes: Posibilidades de programar los reportes para que sean producidos diaria, semanal o mensualmente y puedan ser enviados automáticamente vía correo electrónico.
- Reportes de tiempo de navegación por Internet: Reportes que muestran la cantidad de tiempo utilizado navegando por Internet, por usuario, categoría y más.
- Reportes en idioma local: Crea reportes en japonés, francés, alemán, chino y coreano.

Administración Fácil

Websense es fácil de instalar y mantener, ya que dispone de facilidades, tales como:

- Identificación transparente del usuario: Permite identificar automáticamente a los usuarios por medio del nombre de usuario en Windows NT/2000. Debido a que no se requiere teclear el nombre y la contraseña del usuario para Websense, la identificación del usuario y/o grupo es completamente transparente y fácil de implementar. Ahora soporta nombres de usuarios en japonés, francés, alemán, español, chino y coreano.
- Páginas de bloqueo hechas a la medida: Permite confeccionar, a la medida de las necesidades, la página que los usuarios verán cuando hayan tenido acceso a un sitio bloqueado. Se puede crear una página con el logotipo y la política de acceso a Internet de la organización, editando el texto de la página original de Websense y modificándola.
- Páginas de bloqueo en idioma local: Las páginas de bloqueo por defecto ahora se encuentran disponibles en japonés, francés, alemán y español.
- Actualizaciones automáticas diarias: Las actualizaciones a la base de datos son bajadas automáticamente al servidor todos los días para garantizar que se este utilizando la base de datos más nueva y más confiable posible. Se bajan únicamente cambios y adiciones, para ahorrar ancho de banda y tiempo.
- Administración a distancia: Permite configurar Websense desde cualquier máquina Microsoft Windows 98, NT, 2000 o Sun Solaris en la red.
- Internacionalización: Para sistemas operativos que no estén en inglés, Websense trabaja con idiomas extendidos y de doble byte como japonés, coreano, chino y muchos otros.
- Alerta administrativa: Genera notificaciones por correo electrónico de eventos importantes del sistema Websense.
- Aviso de duración de la política de acceso: Cuando los usuarios solicitan sitios que han sido bloqueados, debe notificárseles si pueden ser consultados a otras horas o si siempre están bloqueados.

- Fácil Despliegue en su Red: Websense puede integrarse con una amplia variedad de firewall, servidores proxy y otras aplicaciones de Internet. Websense puede correr en los sistemas operativos Microsoft Windows NT, Windows 2000, Windows 2003, Sun Solaris o Red Hat Linux.

Websense Reporter

El Reportero Websense trabaja en combinación con Websense Enterprise como una herramienta de reportes completa y fácil de usar, que ayuda a evaluar el uso que los empleados de su compañía hacen de Internet. Identificando cualquier asunto posible relacionado con el acceso a Internet o el consumo de ancho de banda, por medio de la generación de reportes detallados, resúmenes o gráficas.

- Reporte sobre usuarios y grupos: Reporta cuáles sitios y categorías fueron visitados y cuáles usuarios o departamentos realizaron las visitas.
- Reportes completos y a la medida de sus necesidades: Ofrece más de 60 formatos diferentes de reporte, además de permitir diseñar y guardar informes a la medida de las necesidades de la organización.
- Programación y entrega de reportes: Permite exportar los reportes para que sean generados y distribuidos por correo electrónico automáticamente.
- Múltiples formatos de exportación: Exportación de los reportes en una gran variedad de formatos de archivo, incluyendo HTML, Microsoft Excel y Microsoft Word.
- Informes en idioma local: Permite crear informes en japonés, francés y alemán.

El Reportero Websense tiene tres componentes principales: La interfaz de usuario del Reportero, el Servidor de Registro y la Base de Datos de Registro.

Cuando Websense Enterprise procesa una solicitud, envía información sobre dicha solicitud al Servidor de Registro, el cual escribe las entradas en la Base de Datos de

Registro. La interfaz de usuario del Reportero se emplea para efectuar la búsqueda en la Base de Datos de Registro, establecer los criterios de reportes y generarlos.

El Reportero, el Servidor de Registro Websense y la Base de Datos de Registro pueden correr en la misma máquina o en diferentes máquinas que se comuniquen por medio de TCP/IP. Deberán ser instalados en una máquina aparte de la de Websense. El Reportero puede funcionar en varias configuraciones de red.

La base de datos Websense Master Database

La base de datos maestra de Websense trabaja en conexión con el software de Websense Enterprise para administrar de una manera efectiva el uso de Internet por parte del empleado. Es la base de datos de sitios en Internet más grande, más precisa y más actualizada en la categoría de filtrado.

Comprende los sitios visitados con mayor frecuencia en la Red y la base de datos incluye sitios en inglés, francés, alemán, portugués, español, japonés y muchos otros idiomas más.

La Base de Datos Maestra contiene más de 4 millones de anuncios de sitios, que representan más de un billón de páginas Web. Estos sitios están organizados en más de 80 categorías, lo que permite organizar (clasificar) las políticas de filtrado de Internet en la organización. Cada semana se anuncia un promedio de 25.000 sitios adicionales.

¿De qué manera se desarrolla y se mantiene la Base de Datos?

Los sitios primero se recolectan a través de técnicas de software propietarias y luego son clasificados en categorías. Los sitios que no son clasificados en categorías con el método anterior, son evaluados por medio de un análisis de Internet calificado, para

darles una categoría apropiada y son continuamente revisados con el fin de que dicha categoría sea precisa.

Websense Enterprise descarga automáticamente, todos los días, las actualizaciones a la Base de Datos Maestra, incluyendo altas, cambios y bajas, para que se tenga la seguridad de que en todo momento se está usando la base de datos más reciente.

¿Cuáles categorías están en la base de datos?

Websense mejora la flexibilidad de filtrado mediante una lista ampliada que incluye más de 80 categorías. Su flexibilidad integrada permite que los productos de Websense actualicen la lista de categorías según sea necesario.

Websense, Inc., no emite juicio de valor alguno respecto de las categorías o sitios dentro de Websense Master Database. Estas categorías se han seleccionado de acuerdo con la opinión de las comunidades de negocios y educativas sobre qué material puede considerarse inaceptable, inapropiado o indeseable en un entorno de negocios o escolar, puede influir negativamente sobre la productividad de los empleados, la seguridad de los estudiantes o bien, puede ser objeto de una acción legal.

1.13. Normas y políticas de red para el uso de los servicios y recursos

Qué son las políticas de seguridad

Las políticas de seguridad es un documento que está aprobado por la alta gerencia de la empresa y mediante el cual se especifican distintos aspectos referentes a la seguridad informática de la empresa. Estos aspectos pueden ser desde cuántas letras han de tener las contraseñas de los usuarios corporativos y cada cuanto tiempo han de cambiarlas, qué protocolos (telnet, http, smtp, ftp, etc.) van a permitir que hablen las

máquinas internas con las externas y quién va a poder iniciar la conexión, y hasta la política que se va a seguir para permitir el acceso restringido a recursos internos.

Es importante disponer de una correcta política de seguridad en la organización y de ella dependerá el grado de seguridad frente al uso indebido de los recursos corporativos. Esta política de seguridad debería implicar a todos los miembros de la empresa mediante la formación de sus empleados en cuanto a la importancia de que sus contraseñas de usuario sean seguras (no susceptibles a ataques de fuerza bruta o fácilmente adivinables), de que apaguen sus computadores cuando se ausenten de sus sitios o protejan sus escritorios, e incluso de que tengan cuidado con sus disquetes u hojas impresas con información sensible (no sería la primera vez que se reutiliza hojas con información de proyectos estratégicos de empresas). Todo esto depende del grado de seguridad (o de paranoia) que se quiera reflejar en la política de seguridad de las organizaciones, y variará mucho de una a otra.

Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas, instrucciones y procedimientos.
Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. De hecho, las declaraciones de políticas de seguridad pueden transformarse fácilmente en recomendaciones reemplazando la palabra "debe" con la palabra "debería".

Por otro lado las políticas son de jerarquía superior a las *normas*, *estándares* y *procedimientos* que también requieren ser acatados. Las políticas consisten de declaraciones genéricas, mientras las normas hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos en

detalle. Además las políticas deberían durar durante muchos años, mientras que las normas y procedimientos duran menos tiempo.

Las normas y procedimientos necesitan ser actualizadas más a menudo que las políticas porque hoy día cambian muy rápidamente las tecnologías informáticas, las estructuras organizativas, los procesos de negocios y los procedimientos.

Un documento sobre políticas de seguridad contiene, entre muchos aspectos: definición de seguridad para los activos de información, responsabilidades, planes de contingencia, gestión de contraseñas, sistema de control de acceso, respaldo de datos, manejo de virus e intrusos. También puede incluir la forma de comprobar el cumplimiento y las eventuales medidas disciplinarias.

Por qué son importantes las políticas

a. Por que aseguran la aplicación correcta de las medidas de seguridad.
b. Por que guían el proceso de selección e implantación de los productos de seguridad.
c. Por que demuestran el apoyo de la Presidencia y de la Junta Directiva.
d. Para evitar responsabilidades legales.
e. Para lograr una mejor seguridad.

Cómo deben elaborarse las políticas

a. Recopilar material de apoyo.
b. Definir un marco de referencia.
c. Redactar la documentación.

La longitud del documento sobre las políticas

Las políticas de seguridad deben diseñarse de acuerdo a las necesidades específicas de una organización. Algunas organizaciones tienen muchas políticas, mientras otros tienen sólo unas cuantas.

Aunque un documento conciso será leído y asimilado con más probabilidad, hay mucho a favor de un conjunto completo y extenso de políticas de seguridad. Un principio general es que se deben promulgar sólo aquellas políticas que sean absolutamente necesarias. Esto es debido a que las personas son inherentemente muy diferentes entre sí, como también son diferentes los grupos a que pertenecen. El imponer un único conjunto de reglas para todos puede llevar a resistencia y a pobres resultados. En cambio, al tener sólo aquellas políticas que son estrictamente necesarias, se favorece la iniciativa personal y la creatividad. Además tantas políticas de seguridad van a impedir que el trabajo se haga a tiempo.

La extensión y el grado de detalle de las políticas es una función de tipo de audiencia y puede haber distintos documentos según el caso. Por ejemplo, podría haber documentos para los usuarios, la gerencia y el personal de informática. Muchas de las políticas en cada uno de estos documentos serían iguales, aunque el grado de detalle, las palabras técnicas utilizadas, y el número de ejemplos puede variar de un documento a otro.

Para ayudar a aclarar qué son las políticas, se pueden incluir ejemplos específicos. Como ilustración, una política que prohíbe el uso de los recursos computacionales para fines personales podría incluir ejemplos sobre Internet Chat Relay (IRC) o juegos por computadora.

Si se opta por elaborar un conjunto muy completo de políticas de seguridad, se aconseja hacerlo en dos etapas. El primer paso involucra el obtener la aprobación de la Junta Directiva para un conjunto genérico de políticas, mientras que el segundo paso involucra la aprobación para un conjunto más específico de políticas. El conjunto genérico podría incluir de 10 a 20 políticas, y el juego específico podría incluir otras 50-100.

CAPÍTULO III. MARCO METODOLÓGICO

1. METODOLOGÍA DE LA INVESTIGACIÓN

Teniendo como objetivo general la actualización del esquema de seguridad y de la red local de la Fundación Caracas, diseñando, adquiriendo e implantando un modelo de red y de seguridad, se utilizó para el desarrollo de la investigación y su puesta en marcha una metodología que consta de cinco etapas:

1.1. Formulación del Problema de Investigación

La formulación del problema de investigación es la etapa donde se estructura formalmente la idea de investigación y es este el primer paso donde se define qué hacer. Una buena formulación del problema implica necesariamente la delimitación del campo de investigación, establecer claramente los límites dentro de los cuales se desarrollará el proyecto. Cuando esto ocurre las probabilidades de "no perderse" en la investigación tienden a maximizarse.

1.1.1. Elementos de la formulación del problema

a. Planteamiento del problema y el contexto en el cual se desarrolla.
b. Justificación**:** Se deben exponer las razones de la utilidad del estudio, en otras palabras se hace necesario argumentar a favor del estudio, qué utilidad y conveniencia tiene su realización. Entre los criterios para evaluar el valor potencial de la investigación se deben considerar la conveniencia, las implicaciones prácticas y el valor teórico.
c. Objetivos**:** Se hace necesario explicitar primeramente, qué se persigue o pretende con la investigación. Estos son los objetivos, son la guía del estudio.
d. Alcance del trabajo exponiendo su campo de acción.

e. Limitaciones: en este punto se exponen las restricciones que existen en el desarrollo y culminación del proyecto.

1.2. Fase Exploratoria

Está constituida por dos pasos esenciales: la revisión de la literatura y la construcción del marco teórico.

1.2.1. Revisión de la literatura

a. Búsqueda de la literatura: se pueden encontrar dos tipos básicos de fuentes de información. La fuente primaria proporciona datos de primera mano. Ej.: libros, tesis, publicaciones periódicas, Internet, etc. La fuente secundaria proporciona datos sobre cómo y donde encontrar fuentes primarias. Ej.: anuarios, catálogos, directorios, etc.
b. Obtención de la literatura: es la etapa donde se debe hacer posible el acceso a la bibliografía encontrada en el punto anterior.
c. Consulta de la literatura: aquí se toma la decisión de la utilidad de la literatura encontrada. Para esto se suele recurrir al índice o resumen.
d. Extracción y recopilación de la información: en esta etapa se realiza la recolección de información en medios digitales (con una idea, con cifras, con citas, con un resumen, etc.). Se hace necesario tomar todos los datos del texto revisado.

1.2.2. Construcción del marco teórico

El marco teórico se integra con las teorías, estudios y antecedentes en general que tengan relación con el problema a investigar. Para elaborarlo se hace imprescindible realizar el paso anterior (revisión de la literatura). Se debe tener en cuenta dos aspectos que facilitan este proceso de elaboración:

a. Realizar un índice (ayuda de guía para la redacción).

b. La redacción debe tener un esquema estructurado y bien definido.

1.3. Fase de Análisis

1.3.1. Estudio de la red actual y del esquema de seguridad

Esta tarea está orientada a revisar el diseño de la infraestructura actual, equipos, políticas y medios utilizados.

1.3.2. Definición de requerimientos

Permite identificar las expectativas en cuanto a los servicios prestados y el nivel de desempeño que experimentarán los usuarios con los nuevos equipos, esquemas y configuraciones.

1.4. Diseño de la Solución

1.4.1. Diseño

En esta actividad se procede a la elaboración del diseño del modelo de red, diseño del modelo de seguridad, diseño de las politicas del WebSense y la revisión y actualización de las normas y politicas de uso de los recursos de la red. Dichos diseños serán evaluados desde el punto de vista técnico, económico y operativo, con el fin de realizar los ajustes necesarios para garantizar la funcionalidad de los mismos en la implantación.

1.4.2. Adquisición de la solución

Aquí se define como se hará la adquisición de la solución. Por tratarse de una empresa de gobierno la adquisición del hardware, software, consultoría, instalación y

adiestramiento se realiza por la modalidad de licitación, en este caso una licitación selectiva y una licitación general.

1.5. Instalación y Pruebas

1.5.1. Instalación y configuración de hardware y software

La instalación se realiza de acuerdo al diseño de red, diseño de seguridad y diseño de políticas de WebSense, configurando toda la plataforma de comunicaciones y seguridad como lo indique el diseño.

1.5.2. Pruebas

Para comprobar el funcionamiento de los equipos y software, se deben definir una serie de pruebas pilotos para la red, seguridad y salida hacia Internet y en este último se utilizarán las politicas del WebSense.

1.5.3. Elaboración de informes

Esta actividad consiste en realizar la documentación referente a la instalación de los equipos, configuraciones realizadas en los equipos, politicas implantadas en el Firewall y en el WebSense, análisis de tráfico y manual de recomendaciones.

1.5.4. Adiestramiento del personal técnico

De acuerdo a un plan establecido se debe adiestrar al personal operativo de la Unidad de Comunicaciones y Redes para la administración, actualización y control de los equipos nuevos instalados.

CAPÍTULO IV. DISEÑO

1. DISEÑO DE LA SOLUCIÓN

La solución planteada, tanto en el modelo de red como en el modelo de seguridad, se basa en tecnología Cisco. La razón principal para la selección de esta marca en los equipos, es que todo el personal técnico y profesional de la unidad de redes y de la unidad de soporte están adiestrados y prontos a certificarse en esta plataforma, llevan más de 6 años trabajando con equipos Cisco (switches y routers). Todo este adiestramiento ha significado para la Fundación Caracas una inversión de miles de bolívares en sus empleados del área de tecnología de la información, por lo cual debe ser aprovechada al máximo.

1.1. Diseño del modelo de red

1.1.1. Modelo físico

La plataforma propuesta se divide en tres aspectos de la red según los niveles funcionales definidos por Cisco, para redes locales:

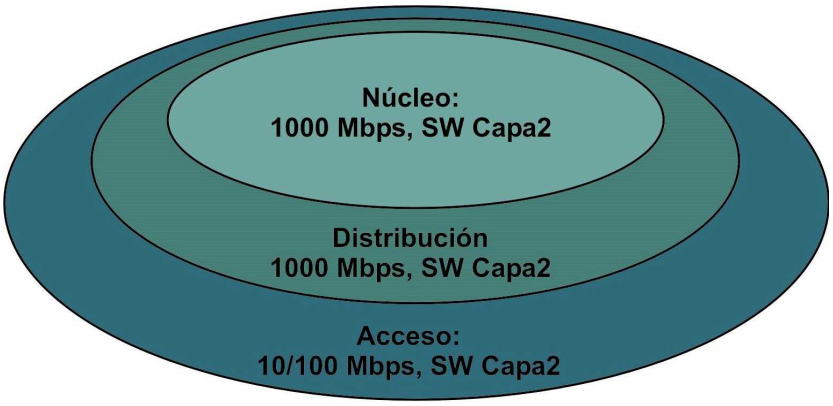


Figura IV.1. Niveles funcionales de la plataforma LAN, según Cisco

Capa de acceso

La capa de acceso es el punto en el cual los usuarios se conectan a la red. Esta capa es referida algunas veces como la capa "desktop". Aquí se maneja tráfico local entre usuarios y recursos que se encuentran conectados directamente en esta capa. Además, permite la conexión de los segmentos locales al troncal (backbone) de la red principal, permitiendo la conexión de puntos locales y distantes de la red en general.

En este nivel la red propuesta provee conexiones Ethernet conmutada de capa 2 (capa de enlace de datos) de 10/100 Mbps directo al usuario, para los apilamientos (stacking) entre equipos pertenecientes al mismo piso se tienen conexiones a velocidad de 2 Gbps entre equipos, utilizando la tecnología GigaStack GBIC.

Entre los dispositivos de acceso y el troncal (backbone) de la red, se permitirá una conexión a 1 Gbps hacia los servicios corporativos. Los equipos que llevarán a cabo esta función son los Cisco Catalyst serie 3500, modelo 3524 XL y 3548 XL Enterprise Edition y los Cisco Catalyst 3550, en sus modelos de 48 y 24 puertos (ver figura IV.2)

Figura IV.2. Cisco Catalyst serie 3500 y 3550

A continuación se muestran algunas especificaciones técnicas de los equipos de la serie 3500 y 3550:

Característica	Catalyst Serie 3524 y 3550-24	Catalyst Serie 3548 y 3550-48
Puertos fijos	24-puertos 10/100 autosensing 2-puertos 1000BASE-X (GBIC)	48-puertos 10/100 autosensing 2-puertos 1000BASE-X (GBIC)
Backplane (velocidad)	8.8 Gbps	13.6 Gbps
Apilable (stackable)	Si	Si
Full duplex	Todos los puertos	Todos los puertos
Máximo número VLAN	250-basadas en ISL ó 802.1Q	250- basadas en ISL ó 802.1Q
Capacidad de enlace entre switch	Si	Si
Capacidades de gestión	SNMP, Telnet, RMON, Cisco Visual Switch Manager, Web-based interface	SNMP, Telnet, RMON, CWSI, Cisco Visual Switch Manager, Web-based interface
Procesador	Diseño Cisco ASICs	Diseño Cisco ASICs
Memoria Flash	4 MB	4 MB
Memoria DRAM	Desde 8 MB hasta 64 MB	Desde 8 MB hasta 64 MB
RMON	Historial, eventos, alarmas y estadísticas	Historial, eventos, alarmas y estadísticas
Dimensiones (HxWxD)	1.75 x 17.5 x 14.4 pulgadas	1.75 x 17.5 x 16.3 pulgadas
Potencia	65W	110W

Capa de distribución

La capa de distribución de la red, también referida como la capa grupo de trabajo (workgroup), marca el punto entre la capa de acceso y la capa núcleo (core). La función primaria de esta capa es ejecutar la manipulación de paquetes para funciones de enrutamiento, filtrado y acceso a WAN. La capa de distribución puede verse como la capa que provee "políticas basadas en conectividad".

Para las funciones de enrutamiento y filtrado se seleccionó un equipo router 3620 (ver figura IV.3), el cual se encarga de comunicar las distintas subredes y VLAN definidas o por definir en la red.

Figura IV.3. Cisco Router 3620

A continuación se muestran algunas especificaciones técnicas de los equipos Router 3520.

Característica	Router 3620
Puertos fijos	Consola y AUX
Slot para módulos de red	2
Caudal	40 kbps
Memoria Flash	8 MB (por defecto) 32 MB máx.
Memoria DRAM	32 MB (por defecto) 64 MB máx.
Dimensiones (HxWxD)	1.75 x 17.5 x 13.5 in.
Potencia	70W

Capa núcleo

El nivel de núcleo (core) es el que se encarga de concentrar las conexiones provenientes de la capa de distribución para permitir la interacción con los servicios de la red, redundancia de conexión y acceso hacia otras rutas de la red.

Para este diseño la capa de núcleo contempla el equipo Catalyst serie 4000 (ver figura IV.3), que concentrará la conexión de todo el edificio, ya que este se encontrará en el nivel de sótano recibiendo las conexiones de fibra óptica de cada uno de los pisos. De la serie 4000, se seleccionó el modelo 4006, ya que ofrece la capacidad de un manejo robusto del ancho de banda de la red, teniendo en cuenta que soportará conexiones a 1Gbps. Tiene orientación modular, lo cual le permite un crecimiento moderado que se

ajusta al tamaño actual y futuro (según estimaciones y capacidad física del edificio) de la red de la Fundación Caracas. Además, brindará un óptimo tiempo de respuesta a las aplicaciones pesadas de la red, debido fundamentalmente a su fortaleza interna de conmutación (backplane).

A continuación se muestran algunas especificaciones técnicas de los equipos de la serie 4000.

Característica	Catalyst 4006
Puertos fijos	2 Gigabit
Máxima densidad de puertos	240 (10/100 Fast Ethernet) 240 (100-FX Fast Ethernet) 240 (10/100/1000BASE-T)
Módulos (slots)	6 (1 por supervisora)
Módulos disponibles	Surpervisor Engine II, Supervisor III
Backplane	64 Gbps
Apilable (stackable)	No
Fuentes de poder redundantes	3 (2 requeridas y 1 para redundancia)
RMON	Historial, eventos, alarmas y estadísticas.
Dimensiones (HxWxD)	17.5 x 17.25 x 12 pulgadas
Potencia	70W

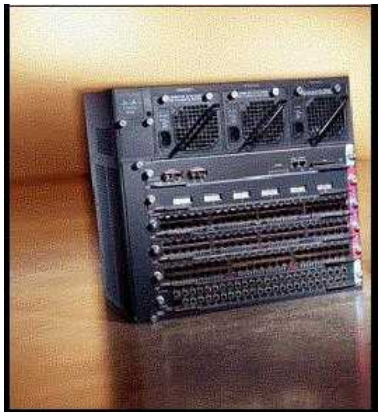


Figura IV.4. Catalyst serie 4000 modelo 4006

1.1.2. Modelo lógico

Configuración de VLAN

El primer paso para configurar una VLAN es definir la topología lógica que se necesita. Configurar una VLAN es un proceso bastante sencillo si se tiene un buen diseño con que trabajar y su implementación consta de los cinco pasos básicos siguientes:

Primero: Activar y configurar VTP.
Segundo: Definir las VLAN.
Tercero: Asignar los miembros a las VLAN.
Cuarto: Configurar la compartición (trunking).
Quinto: Interconectar las VLAN mediante un enrutador (router on a stick).

Es necesario activar y configurar VTP antes de definir las VLAN, ya que no pueden definirse a menos que el conmutador esté en dos de los modos VTP: servidor o transparente.

Para activar VTP hay que definir el nombre de dominio VTP y activar el modo VTP en el conmutador. En este punto, también se puede establecer una contraseña para el dominio. Si se establece una contraseña, habrá que configurar correctamente la contraseña en los conmutadores que vayan a formar parte de ese dominio. Luego de asignado el modo VTP es importante utilizar la revisión 2 de VTP si todos los conmutadores la admiten. Además, si se necesita, se puede activar el recorte VTP, lo cual no implica ninguna desventaja.

Tras configurar VTP hay que definir las VLAN, hay que asignar los números y los nombres a las VLAN y asignar los miembros estáticos de una VLAN.

Finalmente hay que configurar la compartición para el conmutador. Es importante conocer que existen dos variantes sobre la negociación de compartición: DISL (Dynamic ISL) y DTP (Dynamic Trunking Protocol), las cuales permiten que los puertos negocien si deben convertirse en puertos de compartición.

1.2. Diseño del modelo de seguridad

Para las funciones de seguridad (ver figura IV.5) se tienen dos equipos Cisco PIX Firewall 515UR (Unrestricted license), trabajando en modo redundante (failover). Estos equipos están diseñados para redes empresariales medianas o pequeñas, con proyección de crecimiento. Es un equipo montable en rack de tamaño 1U, diseñado para soportar seis interfaces FastEthernet (10/100Mbps) y capaz de integrar una gran cantidad de funciones de seguridad.

Figura IV.5 Cisco PIX Firewall

A continuación se presenta una tabla que resume algunas de las características y funcionalidades de los equipos Cisco PIX Firewall.

Característica	Beneficio
Seguridad	
Seguridad en hardware	• Usa una tecnología propietaria que elimina la dependencia de un sistema operativo foráneo.
Propiedades stateful	• Provee seguridad perimetral en la red para prevenir accesos no autorizados.

	• Usa tecnología Cisco ASA para proveer un stateful robusto. • Provee capacidades de control de acceso para más de 100 aplicaciones predefinidas, servicios y protocolos. • Incluye ingeniería para inspeccionar aplicaciones avanzadas de red, tales como: H.323 Versión 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), etc. • Incluye filtrado de contenido Java y applets ActiveX.
Servicios VPN	• Provee acceso remoto a través de servicios VPN para una amplia variedad de software o hardware Cisco basado en clientes VPN. • Extiende el alcance de los servicios VPN usando Traslación de Direcciones de Red (NAT: Network Address Translation) o Traslación de Direcciones de Puerto (PAT: Port Address Translation), basado en los estándares de la Internet Engineering Task Force (IETF). • Soporte de los estándares VPN IKE e IPsec. • Garantiza privacidad/integridad de los datos y fuerte autenticación para redes y usuarios remotos sobre la Internet. • Soporte DES 56-bit, 3DES 168-bit, y AES 256-bit para encriptación de datos.
Protección contra intrusos	• Provee protección para más de 55 tipos de ataques de negación de servicios (DoS). • Integrado con censores de red Cisco para detección de intrusos (IDS: Intrusion Detection System) que le permiten bloquear o repeler nodos de red hostiles.
Soporte AAA	• Integrado con servicios TACACS+ y RADIUS para proveer autenticación, autorización y auditoria (AAA: authentication, authorization and accounting). • Provee fuerte integración con el Cisco Secure Access Control Server (ACS).
Certificados X.509	• Soporte de certificados bajo soluciones X.509 (Entrust, Microsoft y Verising.
Integración con soluciones de terceras partes	• Soporte para un amplio rango de soluciones de terceros que proveen filtrado de URL, filtrado de contenido, protección antivirus, gestión remota, etc.
Integración de servicios de red	
Virtual LAN (VLAN)	• Soporta la creación de interfaces logicas basadas en el estándar IEEE 802.1q (VLAN), y la creación de políticas de seguridad basadas en estas interfaces virtuales. • Soporte de múltiples interfaces virtuales en una simple interfaz física gracias a VLAN trunking.

Enrutamiento dinámico (OSPF: Open Shortest Path First)	• Provee servicios de enrutamiento dinámico, distribución de rutas estáticas y conectadas directamente. • Convergencia rápida y segura. • Soporte de balanceo de cargas a través de la asignación de costos iguales a los diferentes caminos.
Servidor DHCP	• Provee servicios de DHCP en una o más de sus interfaces para que los dispositivos obtengan una IP dinámicamente.
Soporte NAT/PAT	• Provee capacidades de NAT y PAT estático.
Capacidades de gestión	
CiscoWorks VPN/Security Management Solution (CiscoWorks VMS)	• Software de gestión para ambientes de red de gran escala. • Integra gestión de políticas, mantenimiento de software y monitoreo de seguridad.
PIX Device Manager (PDM)	• Interfaz simple basada en Web que permite una gestión remota segura. • Provee una amplia gama de información en tiempo real, reportes históricos que permiten conocer los eventos de seguridad, el rendimiento y los eventos críticos.
Cisco PIX CLI	• Permite el uso de una interfaz de comandos de línea muy conocida por administradores Cisco que permite una fácil instalación y gestión. • Interfaz accesible desde un puerto de consola, telnet y SSH.
SNMP y soporte syslog	• Provee capacidades de monitoreo y login, con integración de aplicaciones de gestión de terceras partes.
Capacidades de Expansión	
Opciones de expansión Fast Ethernet	• Soporte para una fácil instalación de interfaces adicionales vía 2 slot de expansión PCI. • Soporte para tarjetas de expansión que incluyen tarjetas de 1 interfaz hasta tarjetas de 4 interfaz.
Opciones de aceleración de VPN por hardware	• Provee servicios de VPN de alto rendimiento vía soporte VPN Accelerator Card (VAC) y VPN Accelerator Card+ (VAC+).

Para la definición de las políticas de seguridad que permiten la aplicación de medidas de seguridad, se llevaron a cabo las siguientes tareas:

a) Identificar los objetivos de seguridad de la Organización (se debe conocer y entender cuáles son los puntos débiles y cómo ellos pueden ser explotados). La Fundación Caracas posee en su estructura organizacional oficinas que manejan información con alto valor nacional y regional.
Adicionalmente desde el punto de vista de la Fundación Caracas como ente público, es muy importante proteger la información que se maneja en el despacho de Fundacaracas.

b) Documentar los recursos a ser protegidos (se necesita determinar qué es lo que se quiere proteger y de qué manera se va a proteger). La Fundación Caracas posee el Sistema de Seguimiento Evaluación y Control (SSEC), por el cual rinden todos los proyectos y acciones operacionales programados en un ejercicio fiscal. Además el Sistema de Cobranza (SIC) se encarga de verificar el estatus por concepto de cobranza de los cánones de arrendamientos, deudas, aportes y estados de cuentas. Es una aplicación desarrollada en Clipper y no esta integrada al sistema administrativo implementado actualmente. El Sistema Administrativo que se utiliza es Karavana y el Sistema KOMITIVA, con tres módulos fundamentales: Personal, Nómina y RAC. Igualmente se están conectando 3 puntos de red para la conexión al Sistema Administrativo. En la actualidad existe un Sistema instalado en la coordinación para llevar el registro y control y seguimiento de los créditos asignados. Este Sistema se denomina PIII y fue desarrollado en 2001 por una empresa externa utilizando Visual Foxpro y accediendo a una base de datos tipo DBF, la empresa entregó los archivos fuentes del programa a la Fundación. El sistema funciona en ambiente de red y es utilizado por todas las áreas que conforman la coordinación. A pesar de que el sistema está siendo utilizado sin mayores contratiempos, se hace necesaria la revisión de algunos módulos, entre ellos el módulo de registro y control de los pagos, dicho módulo no se encuentra en funcionamiento lo cual obliga al personal a realizar este control manualmente.

c) Identificar la infraestructura de red con un diagrama resultante de la actualización y un inventario (se debe considerar la seguridad física de la red y cómo proteger esta).

Para diseñar el esquema de seguridad que poseen estos recursos, enfocaremos dos aspectos, la seguridad física y la seguridad lógica. En la figura IV.6 se muestra la estructura de la red actualizada y un inventario de los equipos que posee la Fundación Caracas.

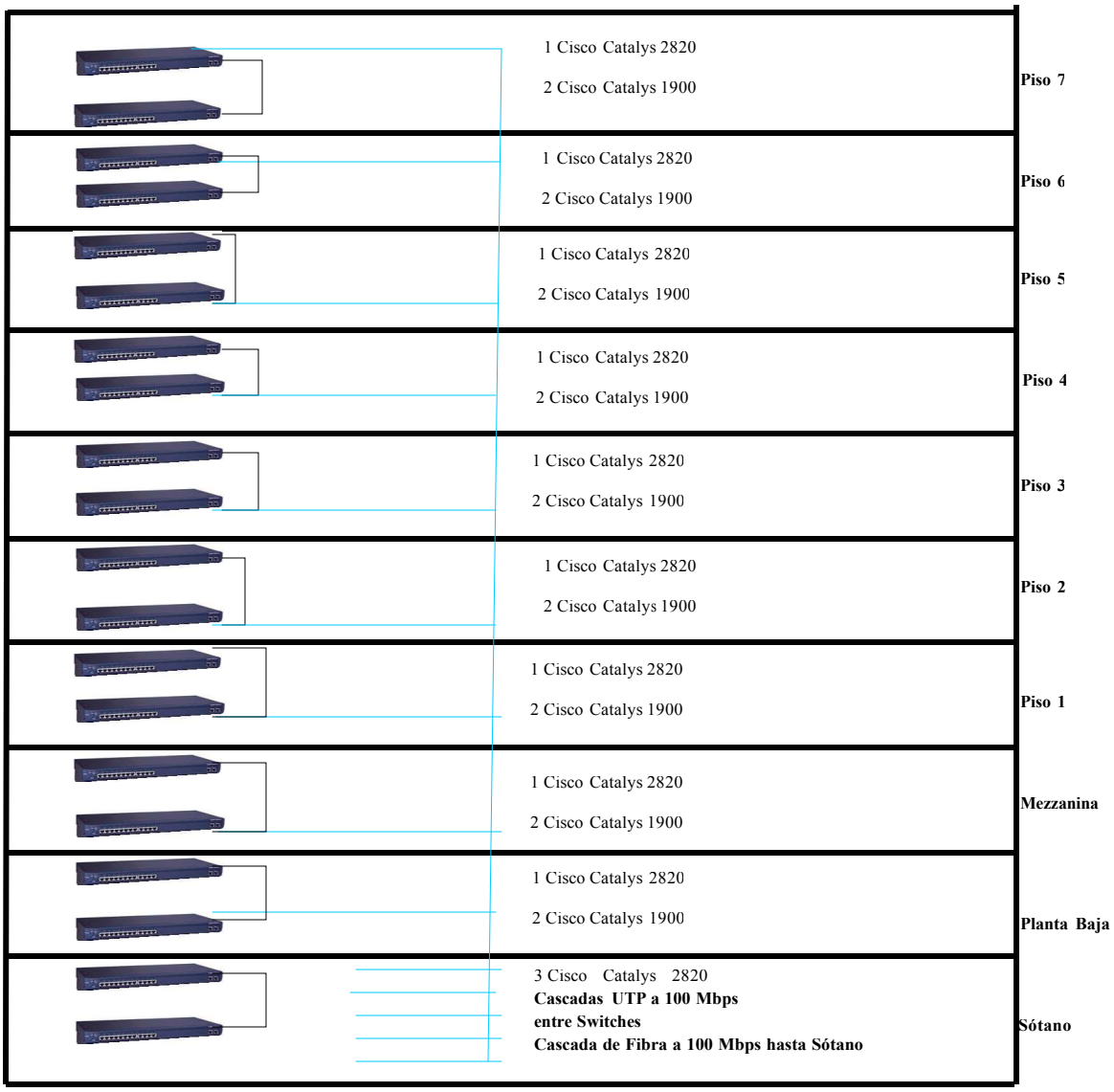


Figura IV.6. Estructura actualizada e inventario de la red de área local (LAN)

Seguridad Física

a. Se prevee el acondicionamiento del cuarto principal de comunicaciones de la Fundación Caracas y esto abarca revisión del aire acondicionado, mantenimiento de UPS, instalación de reguladores de pico, acondicionamiento eléctrico, revisión de los sistemas de detección y extinción de incendio.
b. La Fundación Caracas posee un sistema de control de acceso mediante carnet. Mensualmente o cuando exista algún egreso del personal que conforman el grupo de administradores de la red y servidores, se envía una comunicación a la Dirección General de Seguridad y Protección Integral, para que elimine los accesos de dicho personal a todas las áreas donde se encuentran los recursos y dispositivos de red y de esta forma se mantienen actualizados los accesos del personal autorizado por la Oficina de Informática.
c. Todos los servidores se encuentran en un área de acceso restringido y con condiciones ambientales óptimas. Cada servidor posee garantía en sitio por tres años y los equipos de comunicación más importantes (PIX Firewall, switch Cisco 4006, router Cisco7200, router Cisco 3620 inter-VLAN) poseen contrato SmartNet de Cisco.
d. Las cintas de respaldo mensual se guardan en las bóvedas del Despacho de la Fundación Caracas. Dichas bóvedas son contra incendio, inundaciones y terremotos.
e. Los sistemas operativos, service pack, antivirus, sistema de respaldo, licencias y todo software original que se usa en los servidores y equipos de comunicación, se encuentran en la bóveda de la Oficina de Informática, y sólo se trabaja con copias.

Seguridad Lógica

a. Se prevee la elaboración de kit de desastre por cada servidor donde se describen todos los procedimientos necesarios para la recuperación de un servidor. Además, se guardan los documentos que respaldan la garantía en sitio por tres años.

b. Sistema de respaldo: Se realizan respaldos de todos los servidores diario, semanal y mensual con un esquema rotativo de cinta. Las cintas mensuales se guardan en las bóvedas de la Oficina de despacho de la Fundación Caracas las cuales protegen contra incendio, inundaciones y terremotos.
c. Seguridad contra virus: todos los servidores y equipos clientes poseen sistemas antivirus actualizado (Norton y Trend Micro), así como un sistema para el control de navegación (Websense) y un equipo de la empresa Fortinet conocido como Fortiget para el análisis de trafico http proveniente de Internet y detección de virus en dicho tráfico.
d. Listas de control de acceso para que únicamente puedan ser accedidos por los administradores de la red y cambios de password periódicos de todos los dispositivos de comunicación y servidores.

Diseño lógico del sistema de seguridad

Se crearon cuatro zonas de seguridad, ya que se dispone actualmente de cuatro interfaces Fast-Ethernet y el modelo de PIX Firewall-515 soporta hasta seis interfaces Fast-Ethernet. Para cada zona se definió un nivel de seguridad y las relaciones entre zonas.

Niveles de seguridad por zonas

Nombre de la Zona	Nivel
Incide	100
DMZ	50
Extranet	10
Outside	0

La zona Inside comprende la red local (LAN) y todas las aplicaciones, servicios y recursos de uso interno, sólo accedidos por personal que se encuentra en las oficinas, gerencias y coordinaciones de la Fundación Caracas.

La zona DMZ que contendrá los servidores Web, de correo SMTP y cualquier otro recurso que tenga que ser accedido desde Internet.

La zona extranet que comprende las conexiones de los entes centralizados y descentralizados adscritos a la Alcaldía del Municipio Libertador.

La zona Outside formada por el acceso a Internet y el servidor DNS externo.

El nivel de seguridad usa el criterio del algoritmo ASA según el cual la zona con más valor para la organización y que requiere mayor nivel de seguridad posee el puntaje más alto. En el caso de la Fundación Caracas el Inside es donde está la red local y posee un valor de 100 y la zona con menos valor para la organización y que requiere menor nivel de seguridad (en este caso el Outside donde está Internet) posee el puntaje de 0.

En la figura IV.7 se muestra gráficamente la composición y división de las zonas de seguridad.

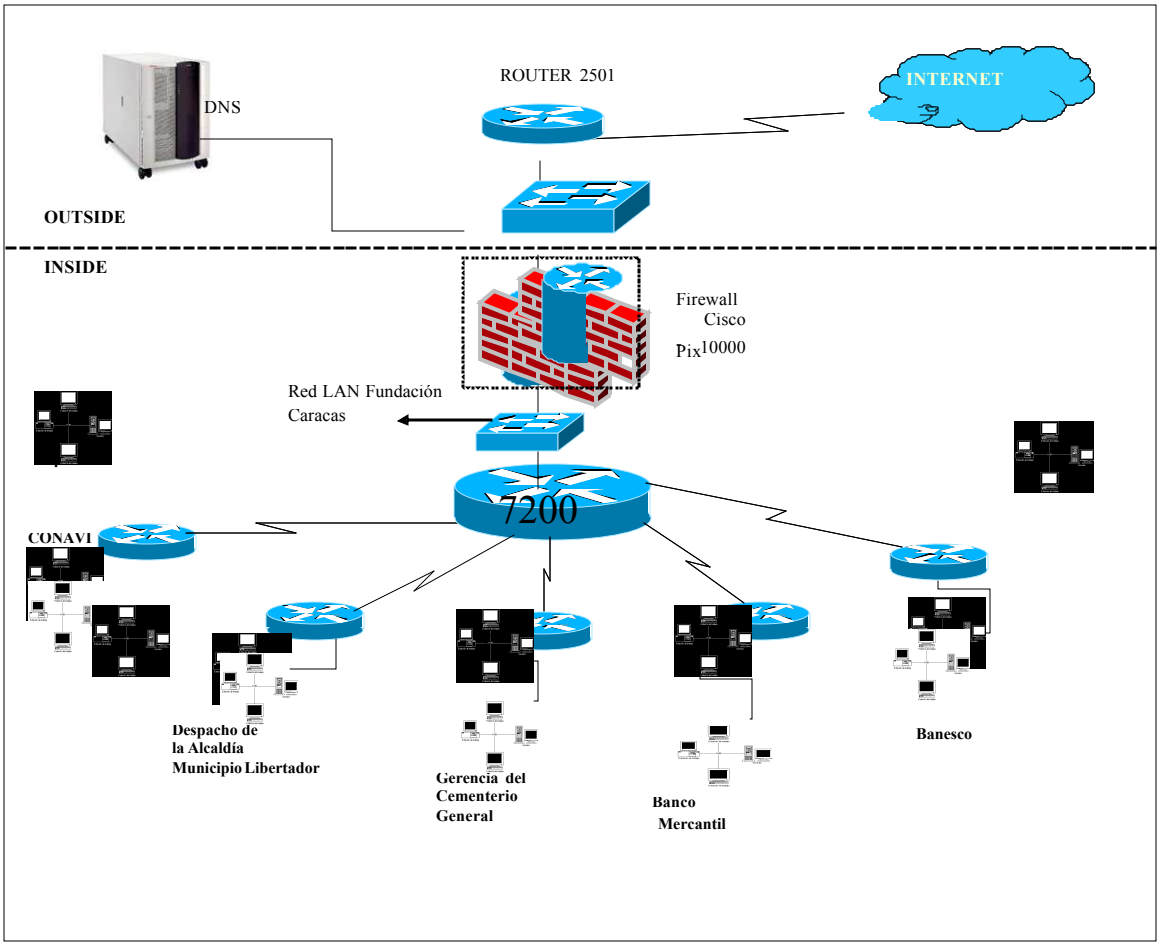


Figura IV.7. Esquema de seguridad para la red de la Fundación Caracas

Relaciones entre zonas de seguridad

En este cuadro se resumen las relaciones entre las cuatro zonas definidas: **X** significa desde y, **Y** significa hasta.

RELACIÓN	Inside	Extranet	DMZ	Outside
1	X	Y		
1	X		Y	
1	X			Y
2		X	Y	
2		Y	X	
3			X	Y
3			Y	X
4		X		Y

El resumen de las relaciones entre zonas da como resultado 4 conexiones unidireccional y 2 conexiones bidireccional:

Inside – Extranet (100 – 10) unidireccional
Inside – DMZ (100 – 50) unidireccional
Inside – outside (100 – 0) unidireccional
Extranet – DMZ (10 – 50) bidireccional
Outside - DMZ (0 – 50) bidireccional
Extranet – Outside (50 – 0) unidireccional

Definición de la composición de las zonas

Inside (Intranet): formada por la red local (LAN) del edificio sede, servidores de documentos, correo interno, base de datos, controlador de dominio, y todos los demás recursos de uso interno (equipos de comunicación, switch de piso, switch principal y routers).

Extranet: Formada por la conexión de todos los entes centralizados y descentralizados de la Alcaldía del Municipio Libertador hacia la Fundación Caracas

(red de área amplia: WAN). Estas conexiones llegan al router Cisco 7200, a través de enlaces punto a punto con CANTV. Existe una conexión con el Banco Banesco y el Banco Mercantil.

DMZ: Esta zona está conformada por equipos que son accedidos desde Internet. El servidor SMTP (servidor de correo Micrososft OWA: Outlook Web Access) y los servidores Web, serán colocados en esta zona.

Un equipo de acceso remoto vía dial-up el cual prestará servicios al Presidente de la Fundación y Directores Generales para la consulta, desde sus casas, de su correo y navegación Internet.

Internet: En esta se encuentra la salida Internet con direcciones certificadas y el servidor DNS externo con dirección IP certificada.

Accesos a definir en cada zona

Extranet

- La red formada por los entes centralizados y descentralizados de la Alcaldía de Caracas y demás entes externos, no tendrá por la red de la Fundación Caracas servicios de HTTP, FTP, Correo, Web, etc.

Inside (Intranet)

- Los usuarios de la red local (LAN) tendrán salida Internet restringida y acceso a la DMZ.

- El servidor de correo tendrá comunicación con el servidor SMTP de la zona DMZ.

- Los administradores y programadores del Sistema Administrativo Karavana tendrán acceso a todos los servidores de la extranet y a los servidores de los entes remotos.

- Sólo se permitirá que los administradores de servidores y equipos de comunicación puedan utilizar telnet hacia la extranet, DMZ o Internet. Dicho acceso deberá ser solicitado por correo con un justificativo.

Internet

- Desde esta zona sólo se podrá acceder al correo vía Web y servidores Web.

- Cualquier acceso al Inside (Intranet) desde esta zona será definido como una solicitud de servicio, debidamente justificado y aprobado.

DMZ

- Desde esta zona sólo se dará acceso al servidor SMTP para que a través de puertos específicos se conecte con el servidor de correo del Inside y no se dará acceso a ninguna otra zona o equipo, a menos que este debidamente justificado.

- Esta zona tendrá servidores que serán visto desde Internet, pero sólo a través de puertos específicos.

- Los equipos de esta zona tendrán salida hacia Internet.

1.3. Elaboración de las normas y políticas de uso de los servicios y recursos de la red

Los activos de información y los equipos informáticos son recursos importantes y vitales que apoyan los objetivos del negocio de la Fundación Caracas. Por esta razón la Oficina de Informática y las distintas Unidades de la Fundación Caracas tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Fundación Caracas debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PC, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las normas y políticas planteadas tienen entre sus objetivos dar a conocer a los usuarios de la Fundación Caracas las reglas para el uso de los equipos, servicios y recursos que ofrece la Red LAN/WAN de la misma, para así garantizar a los usuarios la prestación de los servicios y el acceso a la comunicación, en adecuadas condiciones de calidad, así como las sanciones establecidas por el incumplimiento de las mismas, con la finalidad de proporcionar un aprovechamiento justo de los mismos, resguardando la seguridad e integridad de la información, al facilitar y mejorar el trabajo compartido y en grupo. Para la definición de dichas normas y políticas se tomaron como base las normas y políticas de red actuales y las de otras instituciones similares.

Posterior a su elaboración, las normas y políticas se presentaron al actual Presidente de la Fundación Caracas para su consideración y aprobación, de forma tal de poder difundirlas y aplicarlas en todo la Fundación Caracas y sus distintas sedes. Esto permitirá que se garantice la integridad y seguridad de la información en dicha red.

Definición de responsabilidades

Oficina de Informática

La Oficina de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con las distintas Oficinas, Direcciones Generales y Coordinaciones de la Fundación Caracas. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

Oficinas, Direcciones Generales y Coordinaciones de la Fundación Caracas

Las distintas Oficinas, Direcciones Generales y Coordinaciones de la Fundación Caracas están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos dando cumplimiento a las políticas y normas de seguridad de la red de la Fundación Caracas. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberá notificar a la Oficina de Informática para que se tomen las acciones correctivas rápidamente para así reducir los riesgos.

Directores y Coordinadores de cada unidad funcional de la Fundación Caracas

Los directores y coordinadores de cada unidad funcional de la Fundación Caracas tendrán la responsabilidad de asegurar y garantizar el cumplimiento de las políticas y normas de seguridad de la red de la Fundación Caracas, para lo cual solicitarán el apoyo de la Oficina de Informática en la detección de irregularidades.

Usuarios

Los empleados, contratados y todo personal usuario que labore en la Fundación Caracas están en la obligación de cumplir las políticas y normas de seguridad establecidas en este documento sobre el uso de los equipos y servicios que ofrece la red. Su incumplimiento será sancionado de conformidad con lo establecido en la Ley sobre el Estatuto de la Función Pública, la ley del Trabajo y el reglamento de la Ley Orgánica del Trabajo.

El documento que reúne todas las políticas y normas de uso de los servicios y recursos de red elaboradas por la Oficina de Informática, forman el anexo B de este trabajo.

1.4. Diseño de las políticas a implantar en el Websense Enterprise

Para el control del acceso Internet se definieron políticas de seguridad en el Websense Enterprise, las cuales permiten diferentes opciones para el control de acceso (tales como bloquear o permitir el acceso a categorías individuales por usuario, grupo, estación de trabajo o red). A continuación se describen las políticas creadas y al final se muestra un cuadro resumen con las distintas políticas implantadas en la red.

Administradores: No poseen restricción de horario, pero tienen categorías restringidas. En este grupo se incluyen los administradores de red y servidores de la

Oficina de Informática de la Fundación Caracas. En la figura IV.8 se muestran las categorías restringidas.

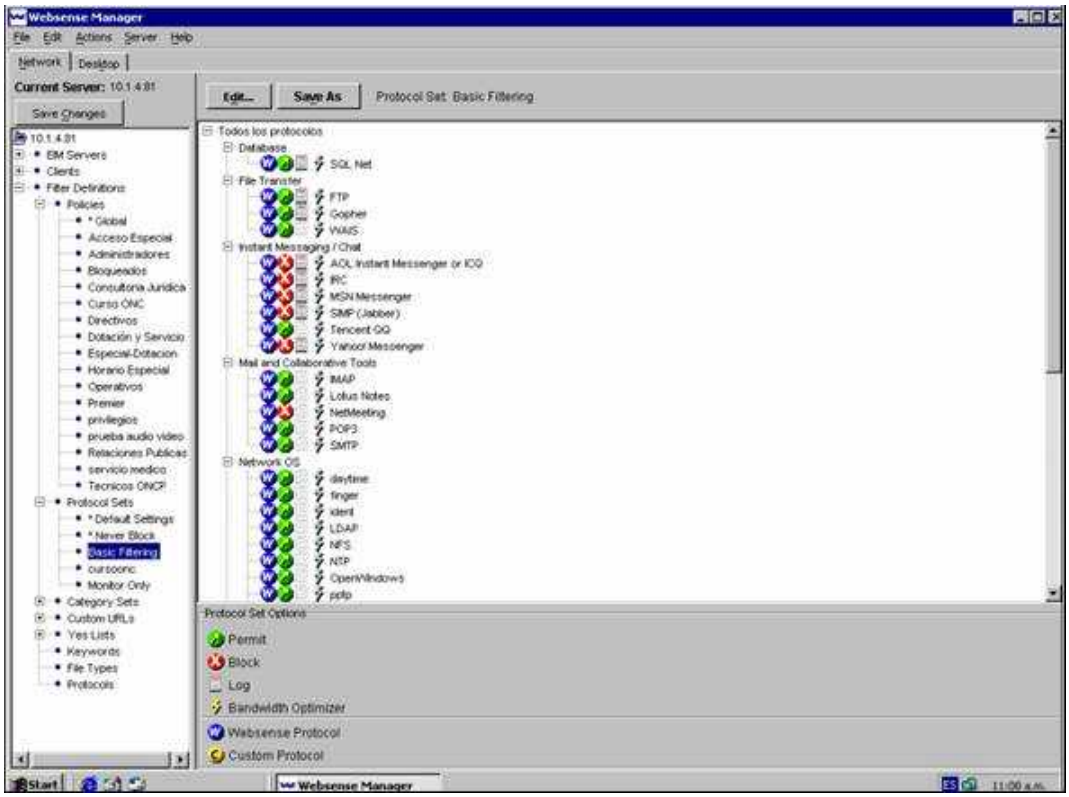


Figura IV.8 Categorías restringidas para los administradores

Globales: Todos los usuarios normales, sin requerimiento de acceso a Internet para sus labores diarias. Podrán navegar en todas las páginas permitidas. Poseen horario de navegación dividido en tres jornadas (de 6:00 am a 8:00 pm; de 11:30 a 1:00 pm y de 4:30 a 6:00 pm de lunes a viernes) con cuotas de 30 minutos cada una. En la figura IV.9 se detallan las categorías restringidas para estos usuarios.

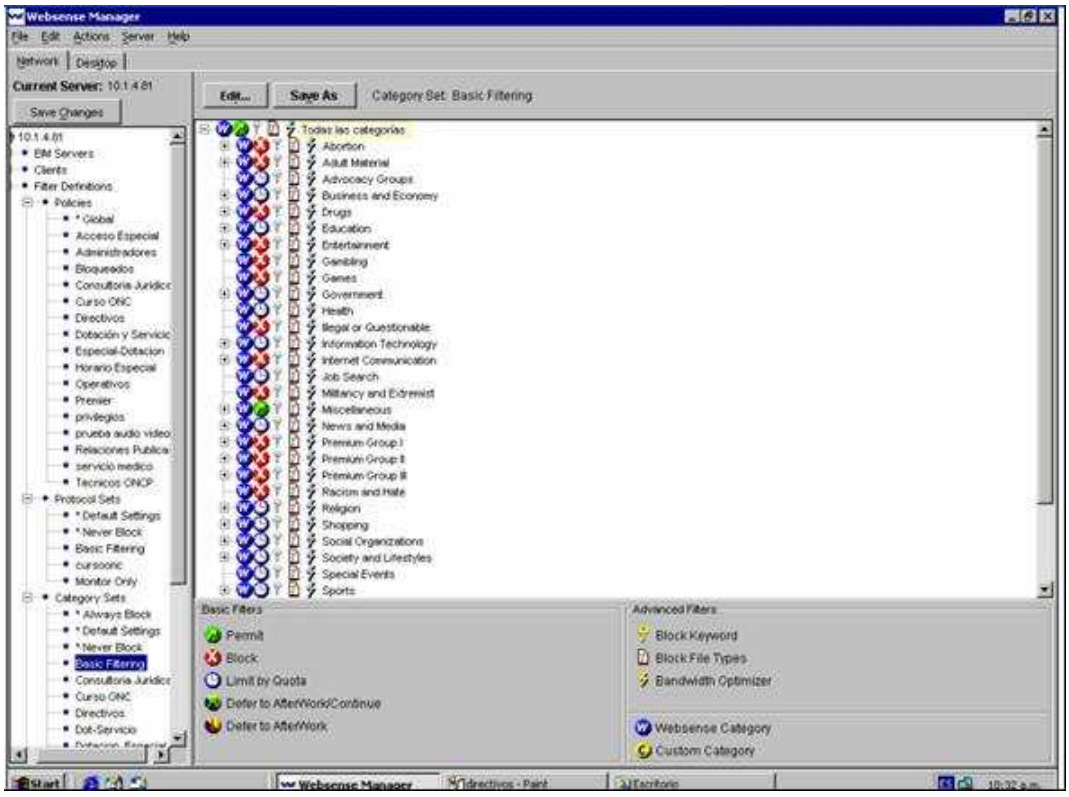


Figura IV.9 Categorías restringidas para los globales

Operativos: Aquellos usuarios que necesitan de Internet en el horario de la jornada laboral, como apoyo a las actividades que están desarrollando, poseen categorías restringidas. Como ejemplos en este grupo se encuentra personal del área de desarrollo de sistemas y de base de datos, personal técnico, asesores de Presidente de la Fundación Caracas, etc. Poseen un horario de navegación dentro de su jornada laboral (desde las 6:00 am a 8:00 pm) con cuotas de 90 minutos cada vez que accedan Internet, para un total de 240 minutos diarios. En la figura IV.10 se detallan las categorías restringidas para estos usuarios.

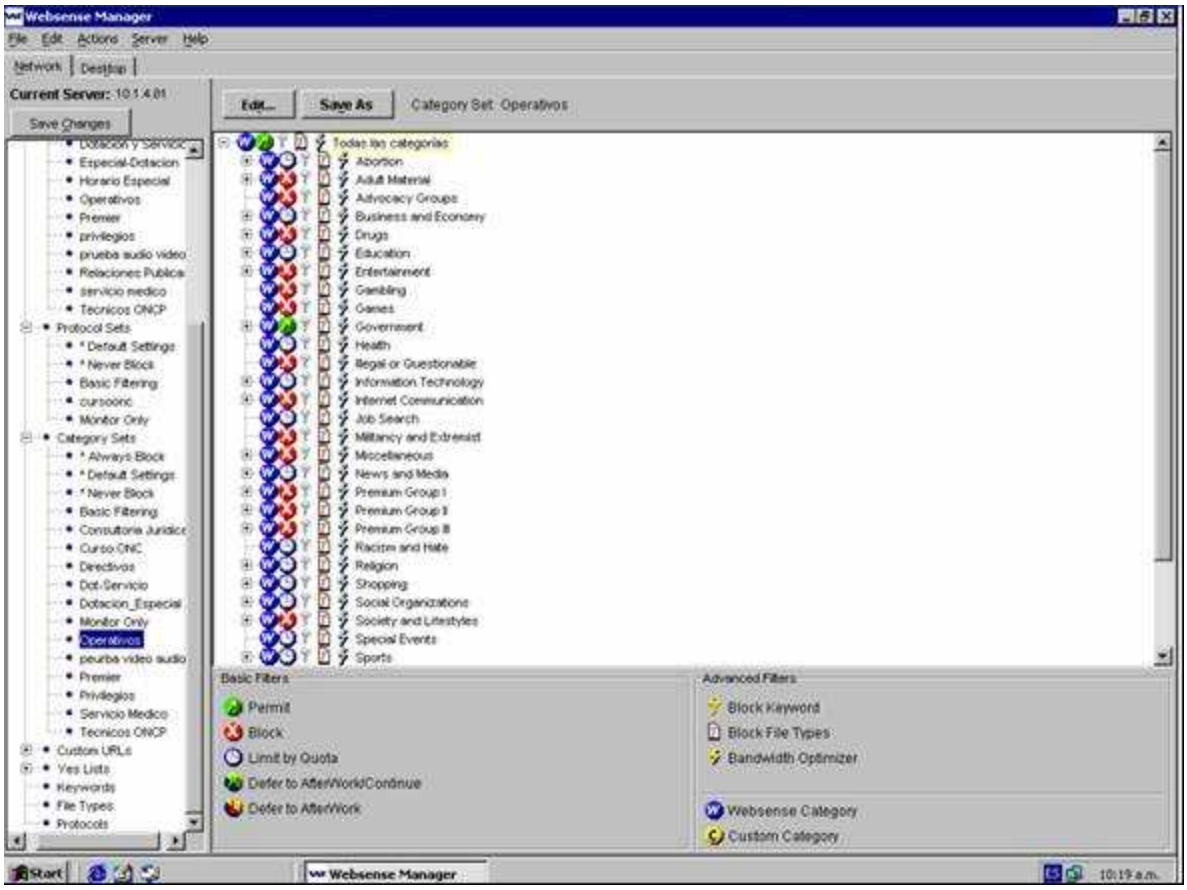


Figura IV.10 Categorías restringidas para los operativos

Directivos: No poseen restricción de horario pero tienen categoría restringidas. Estarán asociados los usuarios con grandes requerimiento de acceso a Internet, sin restricción de horario, con acceso total a páginas permitidas, no se permite correo vía Web. En la figura IV.11 se detallan las categorías restringidas para estos usuarios.

Premier (VIP): Este grupo está conformado por el Presidente de la Fundación Caracas solamente. El grupo no tiene restricciones de horario, no tiene asignada cuota de tiempo, tiene acceso total a las páginas permitidas, incluyendo correo Web. En la figura IV.12 se detallan las categorías restringidas para estos usuarios.

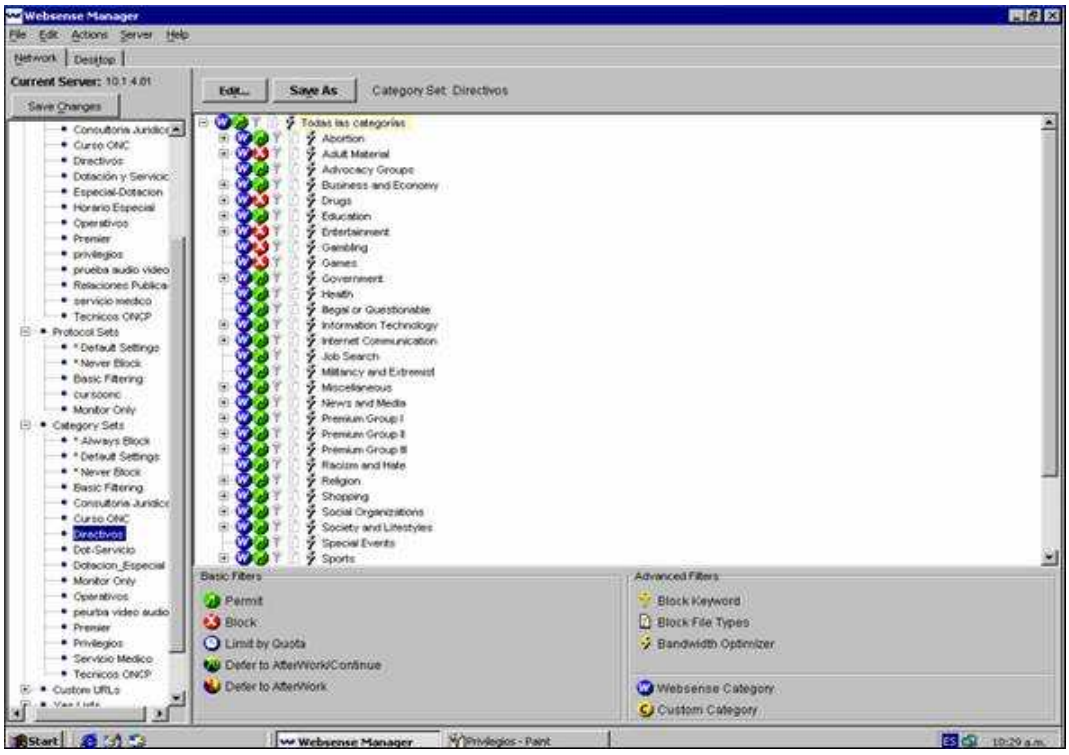


Figura IV.11 Categorías restringidas para los directivos

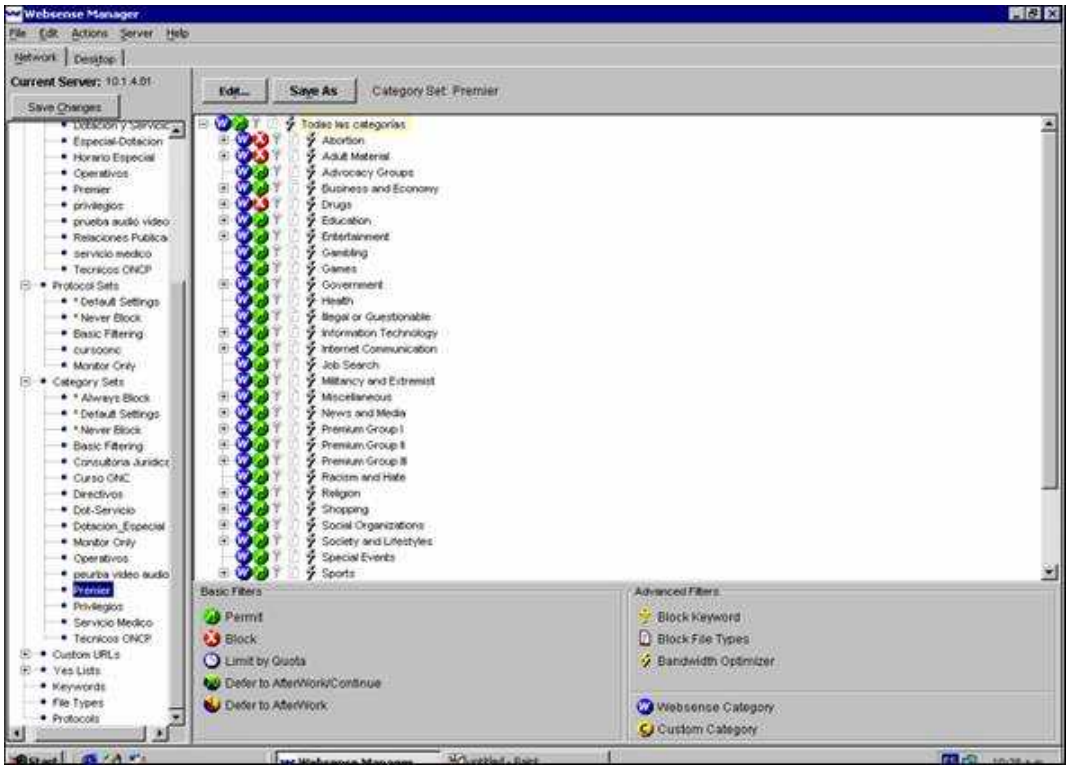


Figura IV.12 Categorías restringidas para los premier (VIP)

A continuación se tiene un cuadro que resume todas estas políticas.

Nombre de la Política	Miembros	Tipo de Acceso	Category Set	Horario Permitido	Horario Permitido Sábados y Domingos
Administradores	Administradores de red y servidores	Total	Never Block	Todo el día	Todo el día
Directivos	Directores, Jefes de División Asesores, etc.	Especial	Basic Filtering	Todo el Día	Todo el Día
Operativos	Usuarios Especiales	Limitado	Used-Defined	8:00 a.m. a 6:15 p.m.	8:00 a.m. a 6:15 p.m.
Global	Usuarios Finales	Limitado	Default Settings	6:30 a.m. a 8:30 a.m 11:45 a.m. a 1:30 p.m. 4:30 p.m. a 6:15 p.m.	8:00 a.m. a 6:15 p.m.
Premier (VIP)	Presidente de la Fundación Caracas	Especial	Premier	Todo el día	Todo el día

2. ADQUISICIÓN DE LA SOLUCIÓN

Para la selección de la solución se contactó a una empresa especializada en redes y seguridad la cual realizó una serie de pasos que permitieron seleccionar la solución que más se ajustará en costo/beneficio a las necesidades de la Fundación Caracas. Estos pasos fueron los siguientes:

a) Recolectar información de la red local, del esquema de seguridad, de las normas y políticas de uso y de las estadísticas de uso de Internet.
b) Identificar necesidades, problemas y deficiencias actuales que presentaba la red, los servicios y la seguridad.

c) Evaluar las características técnicas que ofrecen los equipos Cisco para redes locales y seguridad, así como la integración de Websense con estos equipos.
d) Evaluar el conocimiento técnico y especialización que posee el personal de redes y de soporte en la plataforma Cisco. Dicho personal se encuentra realizando los cursos de la especialización Cisco y tiene más de 6 años de experiencia en la configuración y administración de equipos Cisco.
e) Evaluar el costo/beneficio de quedarse con la misma marca de equipos.

De toda esta recolección de información y evaluación técnica/económica de beneficios, se obtuvieron los modelos de los equipos para cada piso, modelo del equipo para el centro (core) de la red, modelo de los equipos de seguridad y el número de licencias de Websense para el control del servicio Internet. Se elaboraron los pliegos licitatorios, con las especificaciones técnicas definidas, para la adquisición de la solución, la cual se dividió en dos etapas, es decir dos licitaciones, que permitieron actualizar toda la plataforma tecnológica.

La primera licitación fue selectiva por lo que sólo se invitaron a empresas asociadas (Partners) Cisco Systems, la segunda fue general y participaron todas las empresas que ofrecían equipos Cisco.

Para la evaluación de las ofertas presentadas por las empresas, se determinó:

1. Preseleccionar a las empresas que cumplieran con todos los requisitos mínimos exigidos por la Fundación Caracas, según los requerimientos del pliego de condiciones generales y técnicas de cada licitación. Este paso sólo aplica para la licitación general, ya que en la licitación selectiva la preselección se hace antes de publicar la licitación.

2. Las empresas que cumplieran con todos los requisitos mínimos exigidos por la Fundación Caracas se evalúan económicamente según la siguiente fórmula:

PropuestaEconómico = [Mínimo costo ofertado de todas las propuestas en Bs. / Costo en bolívares de la propuesta j-ésima] * 100

3. Para determinar cual de las propuestas presentadas es la mejor oferta técnico-económico, se toma en cuenta el aspecto técnico, el aspecto económico y la mejor relación costo/beneficio de los oferentes.

CAPÍTULO V. INSTALACIÓN Y PRUEBAS

1. ETAPA DE INSTALACIÓN

1.1. Personal Participante

a) *Grupo Gerencial:* Debido a que el proyecto contempla la instalación de nuevos equipos de comunicación LAN y de seguridad, así como la implantación de normas y políticas de uso de los servicios y recursos de la red, se ven afectadas todas las áreas funcionales de la Oficina de Informática, por lo tanto se definió un grupo gerencial conformado por: el director general de la Oficina de Informática, el coordinador de la Unidad de Redes y Comunicaciones (el cual es el líder del proyecto), el coordinador de la Unidad de Dotación y Servicios y el coordinador de la Unidad de Helpdesk.

b) *Grupo Técnico:* Conformado por personal experto en la instalación y configuración de equipos Cisco, expertos en el sistema operativo Windows 2003 y personal especializado en arreglo de cables y organización de rack de comunicaciones. La responsabilidad, en los dos primeros casos, se le asignó a la Unidad de Redes y Comunicaciones y para el trabajo de peinado y organización la responsabilidad fue de la Unidad de Dotación y Servicios.

c) *Grupo de Prueba*: Para la realización de las pruebas de todos los equipos, pruebas de interconexión, comunicación, pruebas de seguridad y pruebas de Websense, se formo un grupo integrado por personal de Redes y Comunicaciones, Dotación y Servicios (Soporte Técnico) y Help Desk.

1.2. Instalación física de los equipos

En la implantación de la red de área local (LAN: Local Area Network), los equipos se distribuyeron e instalaron de la siguiente forma: los equipos switches Catalyst 3500 y 3550 se instalaron en los cuartos de comunicaciones de piso (se instalaron 2 switches en cascada, mediante una conexión GBIC, que proporciona una velocidad de conexión de 2 Gbps entre equipos) y estos sustituyeron a los switches 1900 y 2820 que existían en las instalaciones. El Catalyst 4006 se implantó en un rack que se encuentra en el centro de la red, ubicado en el sótano de la Fundación Caracas y que sustituyó a varios equipos Cisco 2820 que existían, los cuales formaban el núcleo (core) de la red. Se destaca que la seguridad física de los equipos está garantizada, ya que para tener acceso físico a cualquiera de los cuartos de comunicaciones (capa de acceso) se necesita la llave y acceso por carnet. En el sótano la seguridad física es mayor porque se necesita la combinación de una llave, carnet y una clave secreta que consta de 6 dígitos.

En cuanto al dispositivo de seguridad PIX Firewall, este se instaló en el sótano, en un rack anexo al de los dispositivos de conmutación. En la figura V.1 se muestra la ubicación física del PIX Firewall (primario y secundario) y del switch principal.

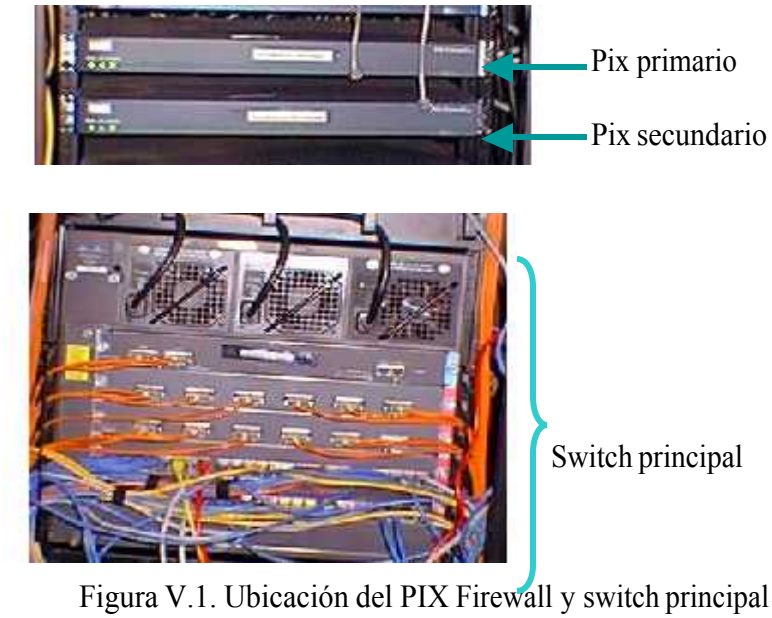


Figura V.1. Ubicación del PIX Firewall y switch principal

1.3. Configuración

Configuración del switch principal Cisco 4006

A continuación se describen los pasos para la configuración completa del conmutador.

a. Se configuró el nombre del switch: SwitchPpal.
b. Se definieron los password de consola, de telnet y de enable para el acceso.
c. Se describieron los puertos por punto físico de la red.
d. Se colocó un número IP para administración remota.
e. Se definió el dominio VTP y el modo VTP en Servidor.
f. Se definieron 2 VLAN: VLAN 1, viene por defecto, aquí se ubican los equipos de comunicación y se colocó una parte de los usuarios de la red de la Fundación Caracas, VLAN 3 la cual se conectan al Banco Banesco.

La configuración total del switch principal quedó como sigue:

```
Time: Fri Sep 19 2004, 09:00:34
#version 6.2(2)
#system web interface version(s)
#test
#system
set system name  SwitchPpal
set system location Sotano
set system contact  Dept Informatica
#frame distribution method
set port channel all distribution mac both
#vtp
set vtp domain Funda
set vtp passwd
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 3 name RedBan type ethernet mtu 1500 said 100003 state active
#ip
set interface sc0 1 10.1.8.3/255.255.0.0 10.1.255.255
set interface sl0 down
set interface me1 down
```

```
set ip route 0.0.0.0/0.0.0.0         10.1.8.1
#spantree
#vlan 1
set spantree priority 8192   1
#vlan 3
set spantree priority 8192   3
#syslog
set logging console disable
set logging level cops 2 default
#set boot command
set boot config-register 0x2
set boot system flash bootflash:cat4000.6-2-2.bin
#mls
set mls nde disable
#module 1 : 2-port 1000BaseX Supervisor
set port name       1/1  Planta Baja
set port name       1/2  Mezzanina
set trunk 1/1  on dot1q 1-1005
set trunk 1/2  on dot1q 1-1005
#module 2 : 6-port 1000BaseX Ethernet
set port name       2/1  Piso 1
set port name       2/2  Piso 2
set port name       2/6  Piso 6
set trunk 2/1  on dot1q 1-1005
!
#module 3 : 6-port 1000BaseX Ethernet
set port name       3/1  Piso 7
set port name       3/2  Piso 8
!
#module 4 : 24-port 10/100/1000 Ethernet
set vlan 3    4/9,4/16-17,4/20-22
set port disable    4/17-18
set port speed      4/16-18  10
set port speed      4/5-6,4/20,4/22  100
set port speed      4/1 1000
set port duplex     4/5-6,4/16-18  full
set port name       4/1  MFDOC01
set port name       4/2  MAIL
set port name       4/3  MFPPL01
set port name       5/5  ONC-WEBSITE
clear trunk 5/14 2,5-1005
set trunk 5/14 on dot1q 1,3-4
set trunk 5/15 off dot1q 1-1005
!
#module 6 empty
end
```

Configuración de los switches de piso

A continuación se muestra parte de la configuración de los switches de piso. Los pasos a seguir fueron los siguientes:

a. Se definió una nomenclatura para identificar los switches dependiendo del lugar donde se encuentran. Así el switch con "hostname 3524_P3_1", es un 3524 que se encuentra en el piso 3 y es el número 1 en cluster.
b. Se definieron los password de consola, de telnet y de enable para el acceso de los mismos.
c. Se describieron los puertos por punto físico de la red.
d. Se colocó un número IP para administración remota.
e. Se definió la VLAN a la que pertenece con su dominio VTP.

```
VTP Version                     : 2
Configuration Revision          : 10
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
VTP Operating Mode              : Client
VTP Domain Name                 : Funda
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      :
```

f. Se definió el puerto trunk "switchport trunk encapsulation dot1q".

La configuración completa de un switch de piso quedó como sigue:

```
service password-encryption
hostname 3524_P3_1!
ip subnet-zero!
cluster enable Piso03 0
cluster member 1 mac-address 0008.a34b.6040
spanning-tree extend system-id
interface FastEthernet0/1
```

```
 description P03-D201
 no ip address
interface FastEthernet0/2
 description P03-D202
 no ip address
interface FastEthernet0/24
  description P03-D224
 no ip address
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 interface Vlan1
 ip address 10.1.8.224 255.255.0.0
ip default-gateway 10.1.8.1
ip classless
ip http server
ip access-list extended CMP-NAT-ACL
 dynamic Cluster-HSRP deny   ip any any
 dynamic Cluster-NAT permit ip any any
!
!
line con 0
!
!
line vty 0 4
!
¡
line vty 5 15
```

Configuración del enrutador de VLAN (on-a-stick)

El enrutador on-a stick es aquel que permite interconectar las VLAN. Esto es debido a que el switch 4006 no posee la tarjeta supervisora que permite conmutación capa 3. A continuación se muestra parte de la configuración de dicho router. Se destaca en esta configuración que las subinterfaces FastEthernet1/0.1 y FastEthernet1/0.3 se configuraron con el protocolo dot1Q para conexión entre las distintas VLAN.

```
hostname 3600_Fundacaracas
!
!
interface Serial0/0
 description CSB
 ip address 10.0.0.77 255.255.255.252
 no fair-queue

interface Serial0/1
 description Conexion BAN
 ip address 172.17.1.146 255.255.255.252
 no cdp enable

interface FastEthernet1/0.1
 description Vlan de Usuarios
 encapsulation dot1Q 1 native
  ip address 10.1.8.1 255.255.0.0
!
interface FastEthernet1/0.3
 description Vlan 3 - Banco
 encapsulation dot1Q 3
 ip address 10.78.10.1 255.255.255.0 secondary
 ip address 10.78.2.1 255.255.255.0 secondary
 ip address 10.79.10.1 255.255.255.0 secondary
 ip address 10.79.2.1 255.255.255.0 secondary
 ip address 10.78.1.1 255.255.255.0 secondary
 ip address 10.79.1.1 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.8.2
```

Configuración del PIX Firewall

A continuación se muestran los pasos a seguir para la configuración del PIX Firewall:

a. Se estableció el nivel de seguridad para cada interfaz: 0 outside, 100 inside, 50 extranet y 10 DMZ.
b. Se definieron los password de consola, de telnet y de enable para el acceso de los mismos.
c. Se configuró el nombre del PIX y el dominio.
d. Se definieron cuatro listas de accesos (ACL):

Uno) ACL 101:Para el tráfico proveniente de la zona outside (Internet).

Dos) ACL 102: Para el tráfico proveniente de la zona inside (red local).

Tres) ACL 103: Para el tráfico proveniente de la zona DMZ.

Cuatro) ACL 104: Para el tráfico proveniente de la zona extranet (conexión con otros Entes).

e. Se aplicaron las listas mediante el comando ip access-group.
f. Se colocaron los números IP a las interfaces inside, outside, DMZ y extranet.
g. Se colocaron los números IP a las interfaces failover, inside, outside, DMZ y extranet.
h. Se configuró el PAT mediante los comandos globales y nat (inside, extranet y DMZ).
i. Se definieron los servidores que tendrán NAT fijos mediante el comando static.
j. Se configuraron las rutas para la comunicación entre zonas.
k. Se configuró la integración con el servidor Websense.
l. Se habilitó el PDM (PIX Device Manager).

La configuración completa del PIX Firewall quedó como sigue:

```
Building configuration...
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 extranet security50
nameif ethernet3 dmz security10
enable password
passwd
hostname funda01
domain-name mf.gov.ve
names
name 10.1.4.9 webprueba
name 10.78.1.9 promafusigma
```

```
.
.
.
object-group service AUT_ADS tcp
  description Grupo de puertos que se necesitan para autenticarse en ADS
  port-object eq domain
  port-object eq ldap
  port-object eq 135
  port-object eq 88
  port-object eq 445
  port-object eq 3268
  port-object range 1024 1054
object-group service AUT_ADS_UDP udp
  description Listas de puertos UDP para autenticar DC
  port-object eq domain
  port-object eq 88
access-list 101 permit tcp any host 200.11.187.6 eq smtp
access-list 101 permit tcp any host 200.11.187.6 eq www
access-list 101 permit tcp any host 200.11.187.6 eq pop3
access-list 101 permit tcp any host 200.11.187.6 eq https
access-list 101 permit tcp any host 200.11.187.7 eq www
access-list 101 permit udp any host 200.11.187.12 eq 2082
access-list 101 permit tcp any host 200.11.187.26 eq www
access-list 101 permit tcp any host 200.11.187.23 eq 3389
access-list 102 deny tcp host 10.1.9.154 any eq www
access-list 102 permit tcp host mfdpnappengine01 host 10.3.4.4 eq smtp
access-list 102 permit tcp host mfdpnappengine02 host 10.3.4.4 eq smtp
access-list 102 permit ip host gatekeeper any
access-list 102 permit ip host 10.1.4.2 any
access-list 102 permit ip host 10.1.4.3 any
access-list 102 permit ip host 10.2.2.6 any
access-list 102 permit ip host 10.2.2.112 any
access-list 102 permit ip fjhernandezp 255.255.255.248 any
access-list 102 permit ip 10.1.0.0 255.255.0.0 10.3.0.0 255.255.0.0
access-list 102 permit ip 10.78.1.0 255.255.255.0 10.3.0.0 255.255.0.0
access-list 102 permit ip 10.79.1.0 255.255.255.0 10.3.0.0 255.255.0.0
access-list 102 permit ip 10.1.0.0 255.255.0.0 host 10.4.4.1
access-list 102 permit tcp host 10.80.208.78 host 10.4.4.1 eq 1610
access-list 102 permit tcp host 10.80.208.78 host 10.4.4.1 eq sqlnet
access-list 102 permit tcp host 10.80.208.78 host 10.4.4.1 eq telnet
access-list 102 permit icmp host 10.80.208.78 host 10.4.4.1
access-list 102 permit tcp host 10.80.208.78 host 10.4.4.1 eq ftp
access-list 102 permit icmp host 10.80.208.5 host 10.4.4.1
access-list 103 permit tcp host 10.3.4.4 host 10.3.9.40 eq smtp
access-list 103 permit tcp host 10.3.4.4 host 10.3.9.41 eq smtp
access-list 103 permit ip host websunacic host 10.3.9.2
access-list 103 permit icmp host websunacic host 10.3.79.69 echo-reply
access-list 103 permit ip host websunacic host 10.3.79.13
access-list 103 permit ip host websunacic host 10.3.79.14
```

```
access-list 103 permit icmp host mfweb host 10.3.4.27 echo-reply
access-list 103 permit tcp host mfweb host 10.3.9.6 eq 1433
access-list 103 deny ip any 10.3.0.0 255.255.0.0
access-list 103 permit ip any any
access-list 104 remark Regla necesaria para el acceso a DC por TCP
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu extranet 1500
mtu dmz 1500
ip address outside 200.11.187.57 255.255.255.0
ip address inside 10.1.8.2 255.255.0.0
ip address extranet 10.4.8.2 255.255.0.0
ip address dmz 10.3.8.2 255.255.0.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 200.11.187.11
failover ip address inside 10.1.8.107
failover ip address extranet 10.4.8.11
failover ip address dmz 10.3.8.11
pdm history enable
arp timeout 14400
global (outside) 2 200.11.187.4-200.11.187.10
global (outside) 2 200.11.187.12-200.11.187.15
global (outside) 2 200.11.187.17-200.11.187.19
global (outside) 2 200.11.187.22-200.11.187.30
global (outside) 1 200.11.187.50
global (extranet) 1 10.4.30.50
global (dmz) 1 10.3.30.50
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 1 0.0.0.0 0.0.0.0 dns 0 0
nat (extranet) 1 0.0.0.0 0.0.0.0 0 0
nat (dmz) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 200.11.187.23 promafusigma netmask 255.255.255.255 0 0
static (inside,outside) 200.11.187.27 webpromafe netmask 255.255.255.255 0 0
static (inside,outside) 200.11.187.5 webprueba netmask 255.255.255.255 0 0
static (inside,outside) 200.11.187.29 gatekeeper netmask 255.255.255.255 0 0
static (dmz,outside) 200.11.187.7 fcweb netmask 255.255.255.255 0 0
static (dmz,outside) 200.11.187.26 websunacic netmask 255.255.255.255 0 0
static (inside,dmz) 10.3.9.40 fcpnappengine01 netmask 255.255.255.255 0 0
static (inside,dmz) 10.3.9.41 fcdpnappengine02 netmask 255.255.255.255 0
access-group 101 in interface outside
access-group 102 in interface inside
access-group 104 in interface extranet
access-group 103 in interface dmz
```

```
route outside 0.0.0.0 0.0.0.0 200.11.187.1 1
route inside 10.2.0.0 255.255.0.0 10.1.8.1 1
route inside 10.78.0.0 255.255.0.0 10.1.8.1 1
route inside 10.79.0.0 255.255.0.0 10.1.8.1 1
route inside 10.80.0.0 255.255.0.0 10.1.8.5 1
route inside 172.22.48.0 255.255.255.192 10.1.8.2 1
route inside 192.20.0.0 255.255.0.0 10.1.8.1 1
timeout xlate 24:00:00
timeout conn 12:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
url-server (inside) vendor websense host mfweb01 timeout 5 protocol TCP version 4
url-cache dst 128KB
filter url except 10.79.0.0 255.255.0.0 10.4.0.0 255.255.0.0
filter url except 10.78.1.0 255.255.255.0 10.4.0.0 255.255.0.0
filter url except 10.2.0.0 255.255.0.0 10.4.0.0 255.255.0.0
filter url except 10.1.0.0 255.255.0.0 10.4.0.0 255.255.0.0
filter url except 10.2.0.0 255.255.0.0 10.3.0.0 255.255.0.0
filter url except 10.1.0.0 255.255.0.0 10.3.0.0 255.255.0.0
filter url except 10.78.1.0 255.255.255.0 10.3.0.0 255.255.0.0
filter url except 10.79.0.0 255.255.0.0 10.3.0.0 255.255.0.0
filter url http 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
http server enable
http 10.1.4.2 255.255.255.255 inside
http fcdoc01 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
no floodguard enable
crypto ipsec transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set TRANS_ESP_3DES_MD5 mode transport
isakmp enable outside
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:
: end
```

Administración mediante el PIX Device Manager (PDM)

Se instaló el PIX Device Manger 3.0 (1). Esta herramienta gráfica proporciona facilidades para la gestión del PIX Firewall, mediante una interfaz de usuario muy sencilla. Se puede acceder a esta herramienta mediante una conexión HTTPS.

El PDM simplifica la configuración, operación y monitoreo del PIX Firewall. Provee acceso a todas las funciones del PIX, incluyendo soporte para las nuevas características disponibles en la versión 6.3 del PIX OS. A continuación se muestra el sumario de características que ofrece el PIX. Al iniciar una sesión https://IP del host se muestra el certificado.

Una vez que el usuario acepta el certificado, se inicia la consola principal la cual se muestra en la figura V.2. Esta interfaz contiene información general del PIX (Versión OS, tipo de dispositivo, licencias, total memoria, versión del PDM, tipo de licencias 3DES, failover e IKE), del estado y tráfico de cada una de las interfaces y del estado de los recursos del sistema.

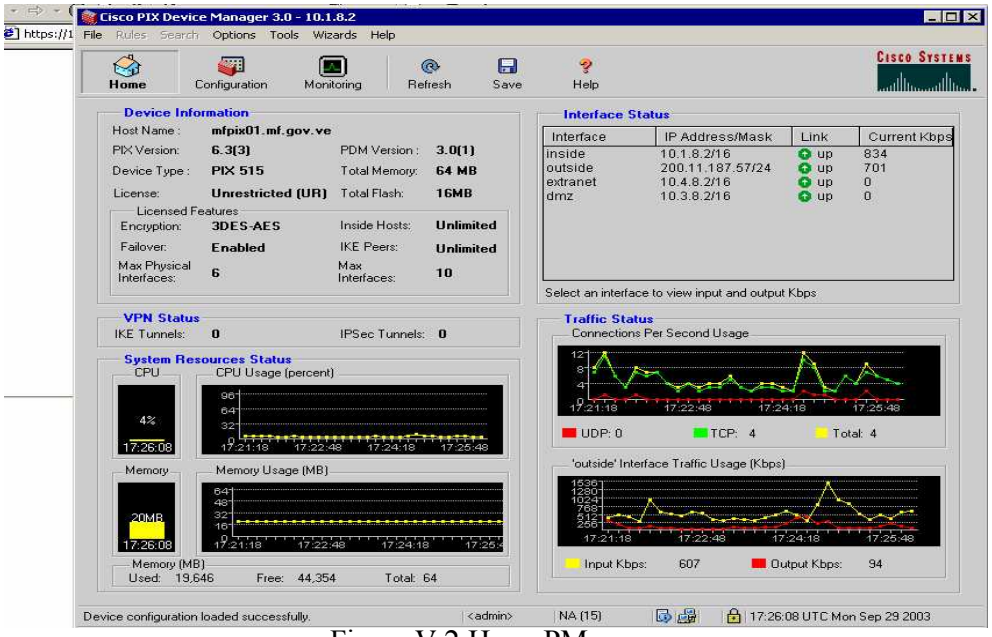


Figura V.2 HomePM

La consola de la figura V.2 permite acceder a la interfaz de configuración y monitoreo, en la cual se pueden realizar tareas como añadir, borra y modificar listas de accesos (llamadas reglas de accesos en esta interfaz); configurar rutas estáticas (llamadas reglas de traslación); configurar VPN; definir nombres de host y de redes, lo cual hace más fácil la administración del PIX y sólo tiene significado local (ver figura V.4).

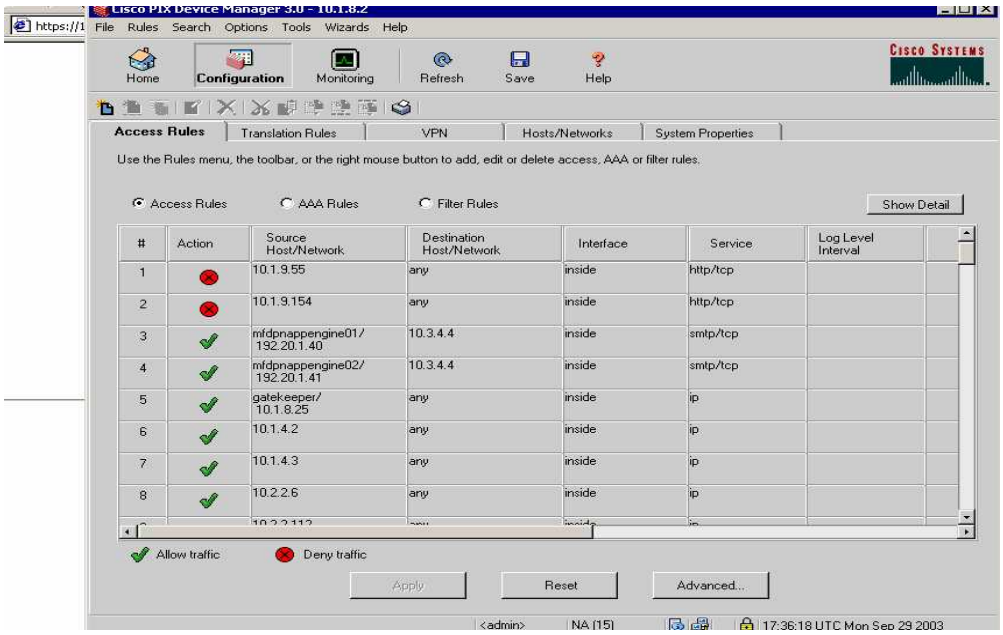


Figura V.3 Configuración PDM

En la figura V.4 se observa un ejemplo con traslación de direcciones estáticas entre dispositivo que se encuentran en la interfaz interna (inside) con la red de Internet (outside) y la DMZ.

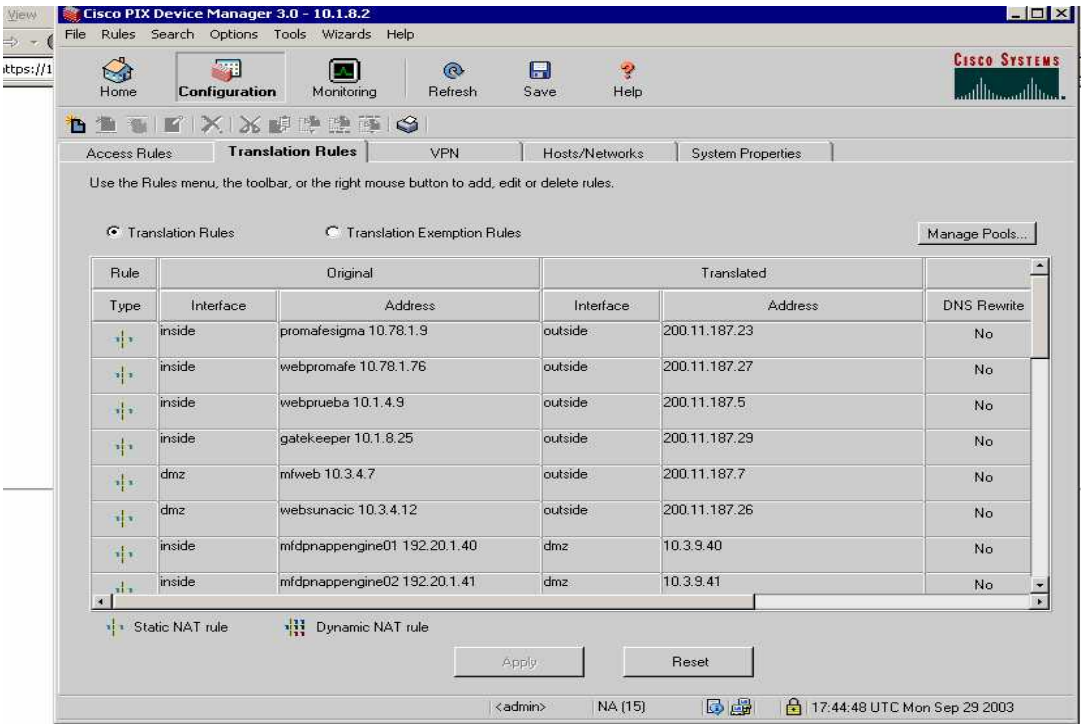


Figura V.4 NAT estático PDM

En la figura V.5 se observa todos los parámetros de configuración necesarios para implantar una VPN en cuatro formas: a) entre dos PIX firewall realizando funciones de servidor VPN, entre un enrutador cisco y un firewall realizando funciones de servidor VPN, entre un host cliente VPN comunicándose por Internet a un firewall realizando funciones de servidor VPN, o entre un dispositivo no Cisco y un firewall Cisco. La comunicación de un cliente con un servidor se puede hacer mediante el cliente de Windows o mediante el vpnclient de Cisco. Adicionalmente el PDM trae un wizard que permite implementar una VPN entre dos dispositivos en forma muy rápida. En las figuras V.6 y V.7. se muestra parte de este wizard.

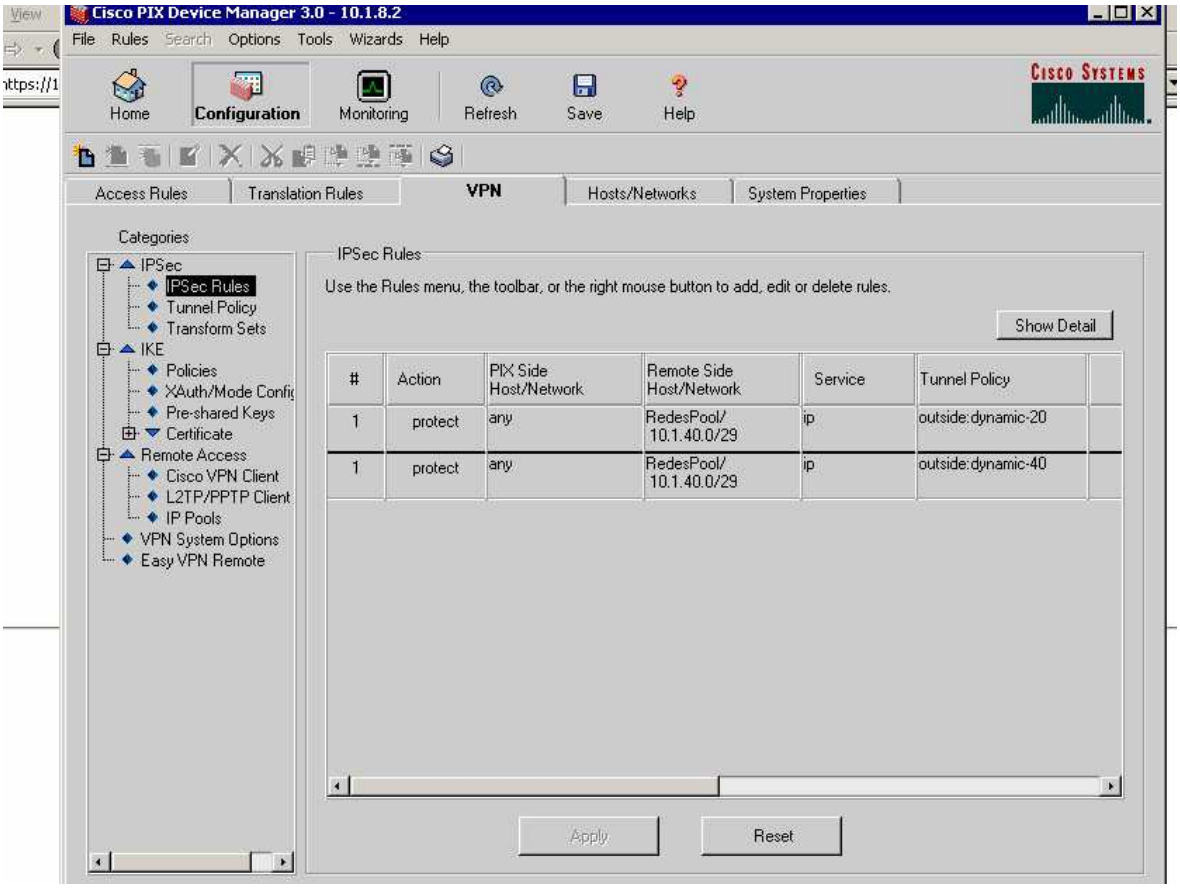


Figura V.5 Configuración VPN

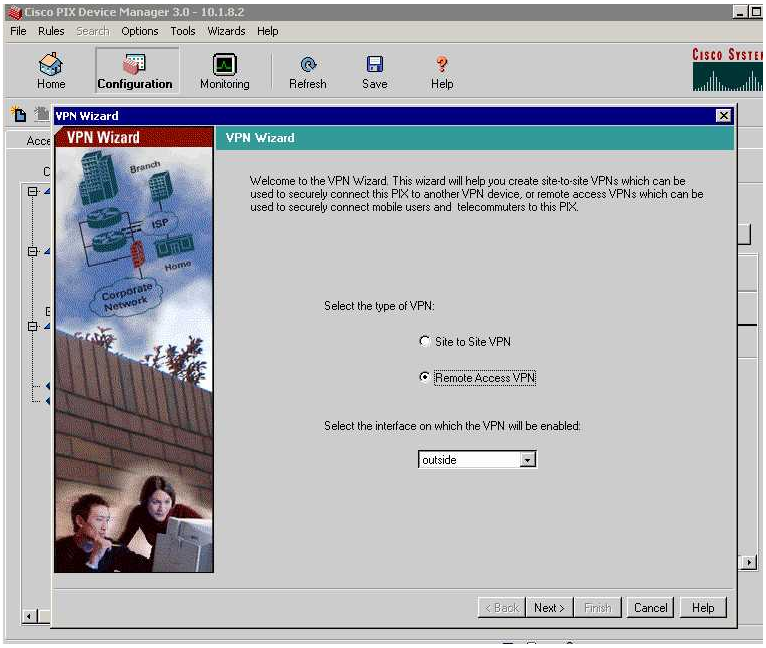


Figura V.6 Configuración VPN

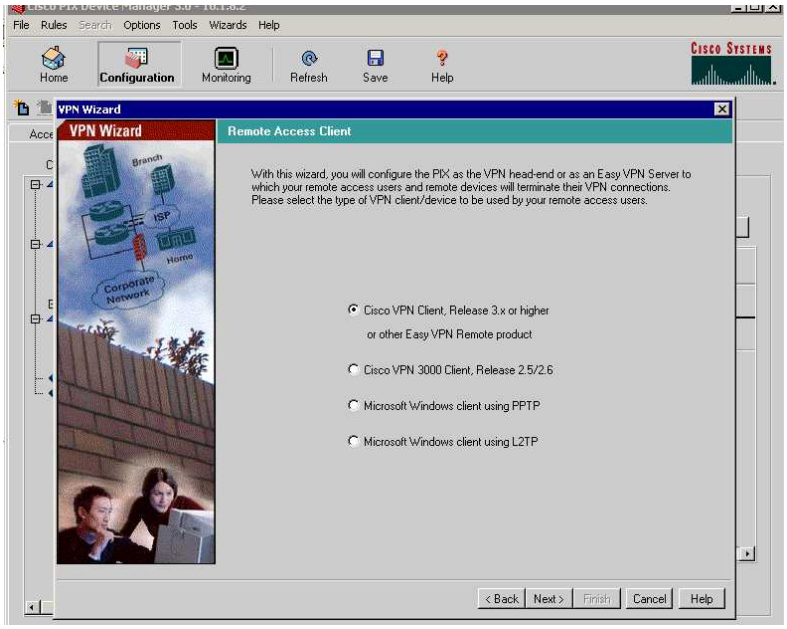


Figura V.7 Configuración VPN

En la figura V.8 se muestra la interfaz que permite configurar propiedades del sistema, tales como rutas, redundancia, usuarios administrativos, actualización automática, servicios DHCP, filtros de URL para integración con otros productos tales como Websense, etc.

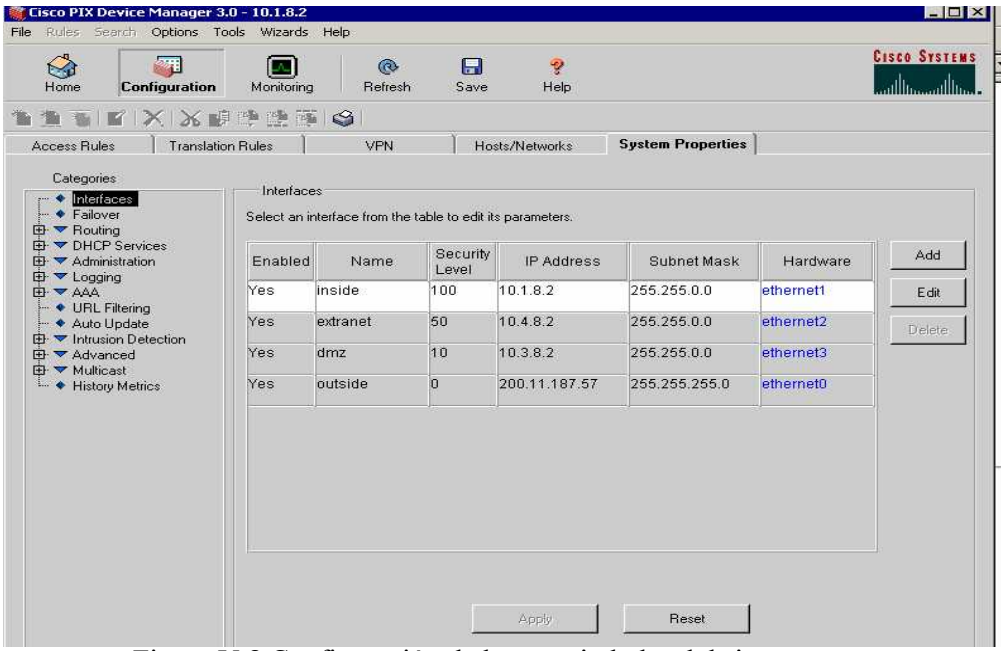


Figura V.8 Configuración de las propiedades del sistema

La interfaz de monitoreo que se muestra en la figura V.9 permite graficar y monitorear diversos parámetros del PIX en forma sencilla.

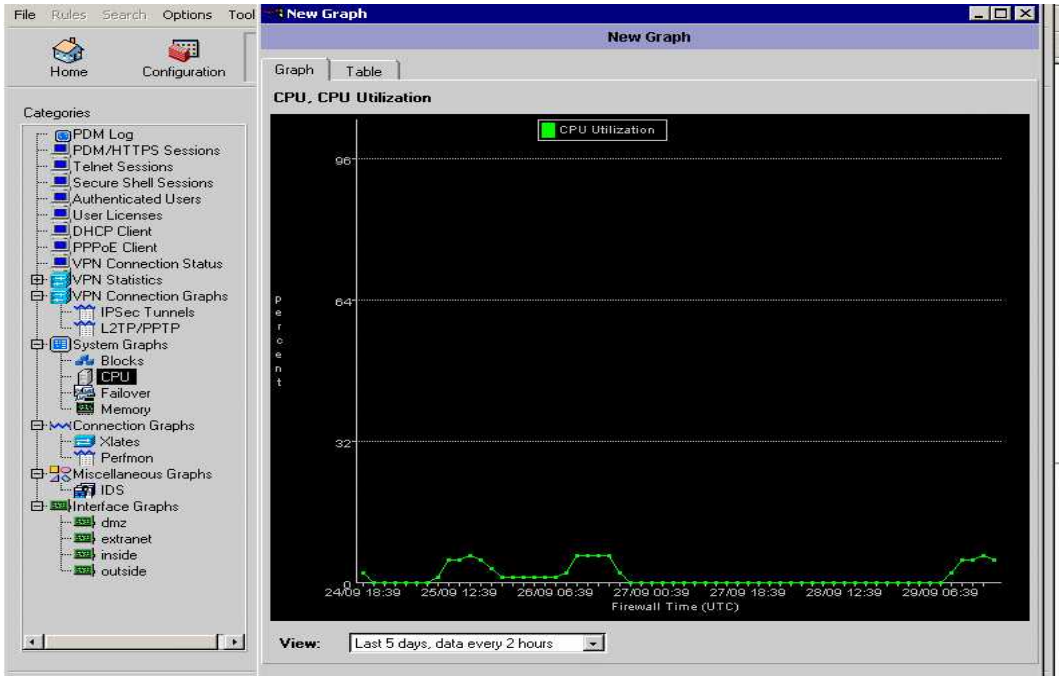


Figura V.9 Gráfico de utilización del CPU durante los últimos 5 días.

Finalmente, mediante PDM se puede salvar la configuración y acceder a la interfaz de comandos en línea mediante la opción Tools.

2. ETAPA DE PRUEBA

Las pruebas realizadas a todos los equipos de comunicación se basaron en los siguientes comandos, cada uno de los cuales permite probar la operatividad de los equipos y la comunicación entre ellos.

Switch principal

- Revisión de conexión física, la cual se prueba por el encendido de los LEDs de cada tarjeta del switch principal. Cuando el switch se enciende se ejecuta el POST, el cual consta de 8 self-tests que se ejecutan automáticamente para garantizar que el switch funciona correctamente. Cuando el switch comienza el POST, los LEDs de los puertos se encienden en color ámbar por 2 segundos, luego se colocan en verde y por último se apagan. Si todo sale bien el LEDs de "status" de cada tarjeta se coloca en verde, en caso contrario este LEDs se coloca en color ámbar.
- Comando "show cdp neighbors detail" (capa de enlace). A continuación se muestran los resultados de dicho comando y se puede constatar que desde el switch principal se pueden ver todos los switches de piso.

show cdp neighbors detail
Port (Our Port): 1/1
Device-ID: 3524_PB_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 145 sec
Capabilities: SWITCH IGMP
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
  Copyright (c) 1986-2003 by cisco Systems, Inc.
  Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-24
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 1/2
Device-ID: 3524_MZ_1
Device Addresses:
  IP Address:
  IP Address:

Holdtime: 123 sec
Capabilities: SWITCH IGMP
Version:
 Cisco Internetwork Operating System Software
 IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
 Copyright (c) 1986-2003 by cisco Systems, Inc.
 Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-24
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 2/1
Device-ID: 3550_24_P1_1
Device Addresses:
 IP Address:
 IP Address:
Holdtime: 133 sec
Capabilities: SWITCH IGMP
Version:
 Cisco Internetwork Operating System Software
 IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
 Copyright (c) 1986-2003 by cisco Systems, Inc.
 Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-24
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 2/2
Device-ID: 3550_48_P2_1
Device Addresses:
 IP Address:
 IP Address:
Holdtime: 163 sec
Capabilities: SWITCH IGMP
Version:
 Cisco Internetwork Operating System Software
 IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
 Copyright (c) 1986-2003 by cisco Systems, Inc.
 Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-48
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda

Native VLAN: 1
Duplex: full

Port (Our Port): 2/3
Device-ID: 3524_P3_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 133 sec
Capabilities: SWITCH IGMP
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
  Copyright (c) 1986-2003 by cisco Systems, Inc.
  Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-24
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 2/4
Device-ID: 3548_P4_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 180 sec
Capabilities: TRANSPARENT_BRIDGE SWITCH
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
  Copyright (c) 1986-2003 by cisco Systems, Inc.
  Compiled Mon 30-Apr-03 07:51 by devgoyal
Platform: cisco WS-C3548-XL
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 2/5
Device-ID: 3550_48_P5_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 136 sec
Capabilities: SWITCH IGMP
Version:

Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-48
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 2/6
Device-ID: 3550-24_P6_1
Device Addresses:
IP Address:
IP Address:
Holdtime: 143 sec
Capabilities: SWITCH IGMP
Version:
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-24
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 3/1
Device-ID: 3550_48_P7_2
Device Addresses:
IP Address:
IP Address:
Holdtime: 125 sec
Capabilities: SWITCH IGMP
Version:
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-48
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 3/2
Device-ID: 3550_48_P8_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 140 sec
Capabilities: SWITCH IGMP
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
  Copyright (c) 1986-2003 by cisco Systems, Inc.
  Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-48
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda

Native VLAN: 1
Duplex: full
Port (Our Port): 3/3
Device-ID: 3548_P9_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 124 sec
Capabilities: TRANSPARENT_BRIDGE SWITCH
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
  Copyright (c) 1986-2002 by cisco Systems, Inc.
  Compiled Mon 30-Apr-02 07:51 by devgoyal
Platform: cisco WS-C3548-XL
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 3/4
Device-ID: 3550_48_P10_1
Device Addresses:
  IP Address:
  IP Address:
Holdtime: 147 sec
Capabilities: SWITCH IGMP
Version:
  Cisco Internetwork Operating System Software
  IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-48
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 3/5
Device-ID: 3550_24_P11_2
Device Addresses:
IP Address:
IP Address:
Holdtime: 178 sec
Capabilities: SWITCH IGMP
Version:
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(11)EA1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 28-Aug-03 09:33 by antonino
Platform: cisco WS-C3550-24
Port-ID (Port on Neighbors's Device): GigabitEthernet0/1
VTP Management Domain: Funda
Native VLAN: 1
Duplex: full

Port (Our Port): 4/6
Device-ID: MFRAS
Device Addresses:
IP Address:
Holdtime: 151 sec
Capabilities: ROUTER
Version:
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-IK9O3S-M), Version 12.2(12a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Tue 24-Sep-03 00:55 by pwade
Platform: cisco 3620
Port-ID (Port on Neighbors's Device): FastEthernet0/0
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: full

Port (Our Port): 4/20
Device-ID: SWITCHPRO
Device Addresses:
IP Address:

Holdtime: 137 sec
Capabilities: SWITCH IGMP
Version:
 Cisco Internetwork Operating System Software
 IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1, RELEASE SOFTWARE (fc1)
 Copyright (c) 1986-2003 by cisco Systems, Inc.
 Compiled Wed 24-Apr-03 06:57 by antonino
Platform: cisco WS-C2950-12
Port-ID (Port on Neighbors's Device): FastEthernet0/1
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: half

Port (Our Port): 5/13
Device-ID: 7200_Fundacaracas
Device Addresses:
 IP Address:
Holdtime: 145 sec
Capabilities: ROUTER
Version:
 Cisco Internetwork Operating System Software
 IOS (tm) 7200 Software (C7200-IS-M), Version 12.2(7a), RELEASE SOFTWARE (fc2)
 Copyright (c) 1986-2003 by cisco Systems, Inc.
 Compiled Thu 21-Feb-03 09:18 by pwade
Platform: cisco 7206
Port-ID (Port on Neighbors's Device): Ethernet1/0
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: full

Port (Our Port): 5/14
Device-ID: 3600_Fundacaracas
Device Addresses:
 IP Address:
Holdtime: 148 sec
Capabilities: ROUTER
Version:
 Cisco Internetwork Operating System Software
 IOS (tm) 3600 Software (C3620-IK9S-M), Version 12.2(12a), RELEASE SOFTWARE (fc1)
 Copyright (c) 1986-2002 by cisco Systems, Inc.
 Compiled Tue 24-Sep-02 01:19 by pwade
Platform: cisco 3620
Port-ID (Port on Neighbors's Device): FastEthernet1/0.1
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: full

Port (Our Port): 5/24
Device-ID: Switch
Device Addresses:
IP Address:
Holdtime: 135 sec
Capabilities: TRANSPARENT_BRIDGE SWITCH
Version:
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1),
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:51 by devgoyal
Platform: cisco WS-C3548-XL
Port-ID (Port on Neighbors's Device): FastEthernet0/47
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: unknown

- Comando ping (capa de red). A continuación se muestran los resultados.

SwitchPpal> (enable)ping 10.1.8.1
!!!!!
----10.1.8.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) fun/avg/max = 6/8/11

SwitchPpal> (enable) ping 10.1.8.5
!!!!!
----10.1.8.5 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) fun/avg/max = 6/21/76

- Para probar la conectividad de los servidores y otros equipos que están directamente conectados al switch principal se tiene el comando “show port”.

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
1/1	Planta Baja	connected	trunk	normal	full	1000	1000BaseSX
1/2	Mezzanina	connected	trunk	normal	full	1000	1000BaseSX
2/1	Piso 1	connected	trunk	normal	full	1000	1000BaseSX
2/2	Piso 2	connected	trunk	normal	full	1000	1000BaseSX

```
2/3  Piso 3          connected  trunk     normal   full  1000 1000BaseSX
2/4  Piso 4          connected  trunk     normal   full  1000 1000BaseSX
2/5  Piso 5          connected  trunk     normal   full  1000 1000BaseSX
2/6  Piso 6          connected  trunk     normal   full  1000 1000BaseSX
3/1  Piso 7          connected  trunk     normal   full  1000 1000BaseSX
3/2  Piso 8          connected  trunk     normal   full  1000 1000BaseSX
3/6                  notconnect 1           normal   full  1000 No Connector
4/1  MFDOC01         connected  1           normal   full  1000 10/100/1000
4/2  MAIL            connected  1           normal a-full a-1Gb 10/100/1000
4/3  MFPPL01         connected  1           normal a-full a-1Gb 10/100/1000
4/4  MFBD01          notconnect 1           normal   auto  auto 10/100/1000
4/5  Mantenimiento   connected  1    normal   full   100 10/100/1000
4/6                  connected  1           normal   full   100 10/100/1000
4/7  mfbddev01       connected  1           normal a-full a-100 10/100/1000
4/8                  connected  1           normal a-full a-1Gb 10/100/1000
4/9                  notconnect 3           normal   auto  auto 10/100/1000
4/10                 connected  1           normal a-full a-100 10/100/1000
4/11                 notconnect 1           normal   auto  auto 10/100/1000
4/12 mfapldev02      connected  1           normal a-full a-100 10/100/1000
4/13                 connected  1           normal a-full a-1Gb 10/100/1000
4/14 Ss-Karavana     connected  1           normal a-full a-100 10/100/1000
4/15                 notconnect 1           normal   auto  auto 10/100/1000
4/16 AS-400          connected  3           normal   full    10 10/100/1000
4/17                 disabled   3           normal   full    10 10/100/1000
4/18                 disabled   4           normal   full    10 10/100/1000
4/19 fcwebdev02      connected  1           normal a-full a-100 10/100/1000
4/20                 connected  3           normal   half   100 10/100/1000
4/21                 connected  3           normal a-half a-100 10/100/1000
4/22                 connected  3           normal   half   100 10/100/1000
4/23 FCSMS01         connected  1           normal a-full a-1Gb 10/100/1000
4/24                 notconnect 1           normal   auto  auto 10/100/1000
5/1                  connected  3           normal   full   100 10/100/1000
5/2                  connected  3           normal   half   100 10/100/1000
5/3                  notconnect 1           normal   auto  auto 10/100/1000
5/4                  notconnect 3           normal   auto  auto 10/100/1000
5/5  FC-WEBSITE      notconnect 3           normal   auto  auto 10/100/1000
5/6                  notconnect 1           normal   auto  auto 10/100/1000
5/7                  notconnect 1           normal   auto  auto 10/100/1000
5/8                  notconnect 1           normal   auto  auto 10/100/1000
5/9                  notconnect 1           normal   auto  auto 10/100/1000
5/10                 notconnect 1           normal   auto  auto 10/100/1000
5/11                    connected  3           normal a-full a-100 10/100/1000
5/12                    notconnect 1           normal   auto  auto 10/100/1000
5/13 Router7200      connected  1           normal   full    10 10/100/1000
5/14 RTR_Funda Fast1/0 connected  trunk     normal   full   100 10/100/1000
5/15 RTR_Funda Fast1/1 notconnect 3         normal   full   100 10/100/1000
5/16 Pix             connected  1           normal a-full a-100 10/100/1000
5/17 pix Faillover   connected  1           normal a-full a-100 10/100/1000
5/18 Websense        connected  1           normal a-full a-100 10/100/1000
```

```
5/19                    connected  1       normal a-full a-100 10/100/1000
5/20 FCWEB          connected  1       normal a-full a-100 10/100/1000
5/21 FCALARMA01 notconnect 3       normal   auto  auto 10/100/1000
5/22 SMTP             notconnect 3       normal   auto  auto 10/100/1000
5/23                    notconnect 4       normal   auto  auto 10/100/1000
5/24 REUTERS       connected  1       normal a-full a-100 10/100/1000
```

Switches de piso

- Revisión de conexión física, la cual se prueba por el encendido de LEDs en el switch. Cuando un switch se enciende se ejecuta el POST, el cual consta de 8 tests que se ejecutan automáticamente para garantizar que el switch funciona correctamente. Cuando el switch comienza el POST, los LEDs de los puertos se encienden en color ámbar por 2 segundos, luego se colocan en verde y por último se apagan. Si todo sale bien el LEDs de "status" se coloca en verde, en caso contrario este LEDs se coloca en color ámbar.
- Comando "show cdp neighbors detail" (capa de enlace). A continuación se muestran los resultados de dicho comando donde se puede verificar la conexión de cada switch de piso al switch principal, así como se muestra la configuración con el comando "show configuration", donde se puede observar la conexión en cluster con el switch compañero de piso.

```
-------------------------
Device ID: JAB054804WE(SwitchPpal)
Entry address(es):
  IP address:
Platform: WS-C4006,  Capabilities: Trans-Bridge Switch
Interface: GigabitEthernet0/1,  Port ID (outgoing port): 2/1
Holdtime : 125 sec

Version :
WS-C4006 Software, Version McpSW: 6.2(2.0) NmpSW: 6.2(2)
Copyright (c) 1995-2002 by Cisco Systems, Inc.

advertisement version: 2
VTP Management Domain: 'Funda'
Native VLAN: 1
Duplex: full
```

```
-------------------------
Device ID: 3524_P1_3
Entry address(es):
  IP address:
Platform: cisco WS-C3524-PWR-XL,  Capabilities: Trans-Bridge Switch
 Interface: FastEthernet0/13,  Port ID (outgoing port): FastEthernet0/24
Holdtime : 171 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.2)XU,
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 17-Jul-01 18:29 by ayounes

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010121FF0000000000000000628200000FF0001
VTP Management Domain: 'Funda'
Native VLAN: 1
Duplex: full

-------------------------
Device ID: 3548_P1_2
Entry address(es):
  IP address: 0.0.0.0
  IP address:
Platform: cisco WS-C3548-XL,  Capabilities: Trans-Bridge Switch
 Interface: GigabitEthernet0/2, Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 162 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.3)WC(1),
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Mon 30-Apr-02 07:51 by devgoyal

advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=0A4B5E400000000101012BFF000B5FB011800008A34B5E40010001
VTP Management Domain: 'Funda'
Native VLAN: 1
Duplex: full
```

Resultado del comando “show configuration”

```
Using 4449 out of 32768 bytes
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname 3548_P1_2
!
ip subnet-zero
!
cluster commander-address 000b.5fb0.1180 member 1 name P1
!
!
interface FastEthernet0/1
 description P01-D101
 switchport access vlan 3
!
.

interface FastEthernet0/48
 description P01-D148
 switchport access vlan 3
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface VLAN1
 no ip address
 no ip directed-broadcast
 no ip route-cache
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
line vty 5 15
```

!
end

- Comando ping (capa de red). A continuación se muestran los resultados de los ping que se hicieron a varios equipos de comunicación.

3550_24_P1_1#ping 10.1.8.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.8.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip fun/avg/max = 8/208/1008 ms

3550_24_P1_1#ping 10.1.8.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.8.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip fun/avg/max = 1/201/1004 ms

3550_24_P1_1#ping 10.1.8.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.8.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip fun/avg/max = 1/2/4 ms

PIX Firewall

- Revisión de conexión física, la cual se prueba por el encendido de LEDs en los PIX Firewall. Cuando se enciende se ejecuta el POST, el cual consta de 8 tests que se ejecutan automáticamente para garantizar que el equipo funciona correctamente. Cuando el firewall comienza el POST, los LEDs se encienden en color ámbar por 2 segundos, luego se colocan en verde y por último se apagan. Si todo sale bien el LEDs de "status" se coloca en verde, en caso contrario este LEDs se coloca en color ámbar.
- Para la verificación del funcionamiento del PIX Firewall se procedió a la activación del Syslog, el cual muestra los mensajes generado por el firewall según los eventos que registre, tales como alertas, reducción drástica de recursos, etc.

Los mensajes Syslog pueden ser usados para crear correos de alerta y archivos "log" (ver figura V.10).

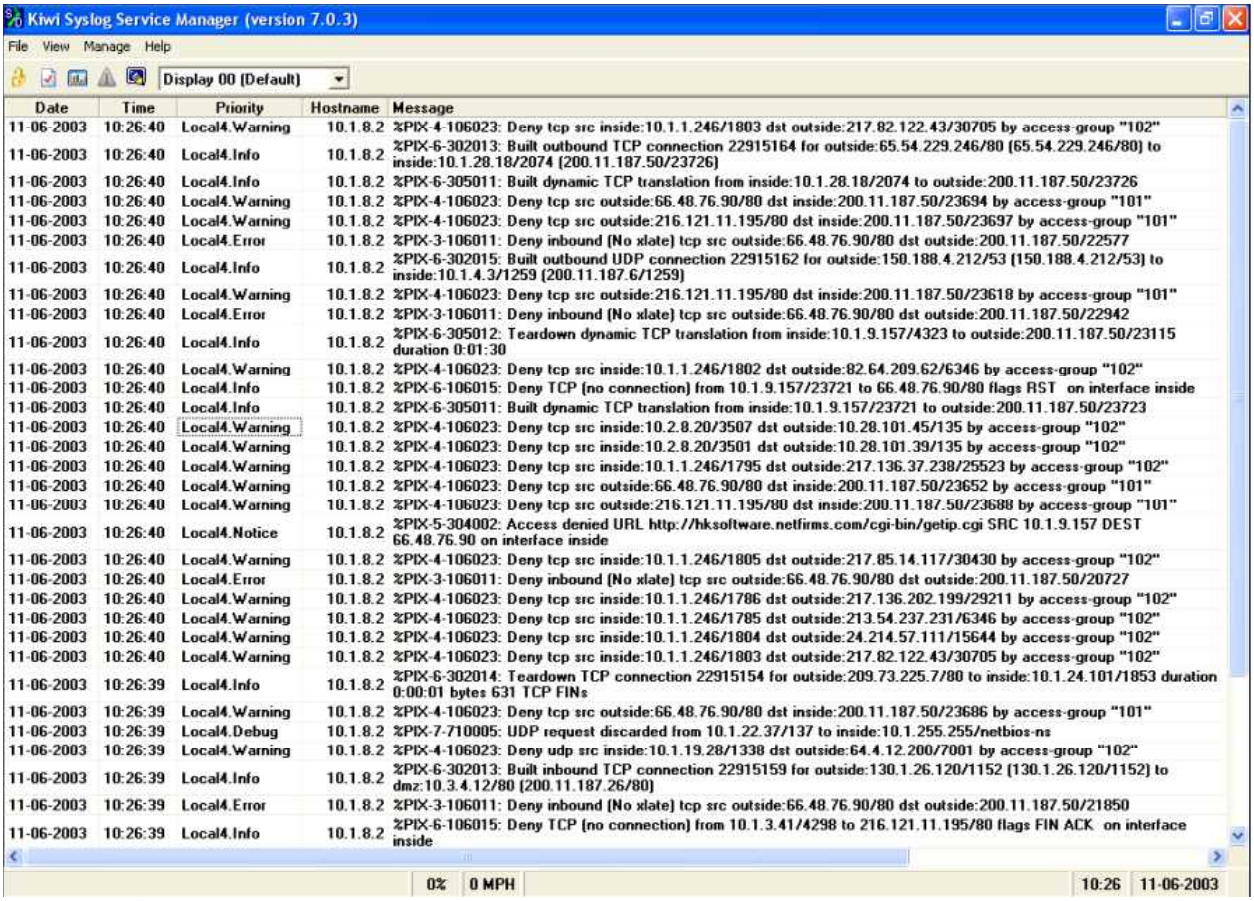


Figura V.10. Servicio Syslog del PIX Firewall

- Otra forma de verificación fue la ejecución de los comando "show xlate" y "show conn". El primer comando muestra los IP origen que están conectados a Internet y el segundo comando muestra la cantidad total de licencias utilizadas, el IP origen y destino el cual varía dependiendo de la zona.

show xlate
576 in use, 7701 most used
PAT Global 200.11.187.50(52992) Local 10.1.28.34(1226)
PAT Global 200.11.187.50(52736) Local 10.1.9.157(2620)
PAT Global 200.11.187.50(52993) Local 10.1.3.16(3471)

PAT Global 200.11.187.50(20738) Local 10.1.24.100(1556)
PAT Global 200.11.187.50(52994) Local 10.79.1.79(3351)
PAT Global 200.11.187.50(52995) Local 10.1.24.39(1370)
PAT Global 200.11.187.50(52739) Local 10.1.9.157(2622)
PAT Global 200.11.187.50(52996) Local 10.1.24.39(52995)
PAT Global 200.11.187.50(52997) Local 10.1.19.18(2699)
PAT Global 200.11.187.50(52485) Local 10.1.23.30(3797)
PAT Global 200.11.187.50(52229) Local 10.1.2.64(3221)
PAT Global 200.11.187.50(52859) Local 10.1.9.157(2658)
PAT Global 200.11.187.50(50555) Local 10.1.28.53(1119)
PAT Global 200.11.187.50(53116) Local 10.1.9.157(2765)
PAT Global 200.11.187.50(52860) Local 10.1.29.17(4784)
PAT Global 200.11.187.50(53117) Local 10.1.9.157(53116)
PAT Global 200.11.187.50(52861) Local 10.1.23.30(3830)
PAT Global 200.11.187.50(53118) Local 10.1.9.157(2767)
PAT Global 200.11.187.50(52862) Local 10.1.29.17(4785)
PAT Global 200.11.187.50(52940) Local 10.1.9.157(52936)
PAT Global 200.11.187.50(53197) Local 10.1.9.157(2793)
PAT Global 200.11.187.50(52941) Local 10.1.24.39(52939)
PAT Global 200.11.187.50(52685) Local 10.1.9.157(2598)
PAT Global 200.11.187.50(12494) Local 10.1.6.90(3355)
PAT Global 200.11.187.50(53198) Local 10.1.24.45(1491)
PAT Global 200.11.187.50(52942) Local 10.1.9.157(52938)
PAT Global 200.11.187.50(53199) Local 10.1.24.45(1492)
PAT Global 200.11.187.50(52943) Local 10.1.9.157(2709)
PAT Global 200.11.187.50(52687) Local 10.1.9.157(2600)
Global 200.11.187.5 Local webprueba
PAT Global 200.11.187.50(53200) Local 10.1.9.157(53197)
PAT Global 200.11.187.50(52944) Local 10.1.9.157(52943)
PAT Global 200.11.187.50(53201) Local 10.1.9.157(2795)
PAT Global 200.11.187.50(52945) Local 10.1.9.157(2711)
PAT Global 200.11.187.50(52689) Local 10.1.24.39(1312)
PAT Global 200.11.187.50(53202) Local 10.1.24.45(1493)
PAT Global 200.11.187.50(52946) Local 10.1.19.18(2697)
PAT Global 200.11.187.50(52434) Local 10.1.6.77(1739)
PAT Global 200.11.187.50(1491) Local 10.1.23.4(1492)
PAT Global 200.11.187.50(53203) Local 10.1.3.16(3518)
PAT Global 200.11.187.50(52947) Local 10.1.9.157(52945)
PAT Global 200.11.187.50(52691) Local 10.1.9.157(2602)
PAT Global 200.11.187.50(52948) Local 10.1.25.35(2020)
PAT Global 200.11.187.50(52949) Local 10.1.9.157(2713)
PAT Global 200.11.187.50(52693) Local 10.1.19.18(2680)
PAT Global 200.11.187.50(52950) Local 10.1.3.16(3461)
PAT Global 200.11.187.50(52694) Local 10.1.19.18(2681)
PAT Global 200.11.187.50(52951) Local 10.79.1.30(1313)
PAT Global 200.11.187.50(48087) Local 10.78.1.47(1089)
PAT Global 200.11.187.50(52952) Local 10.79.1.79(3348)
PAT Global 200.11.187.50(4825) Local 10.1.6.74(2008)
PAT Global 200.11.187.50(52953) Local 10.1.9.157(52949)

PAT Global 200.11.187.50(52697) Local 10.1.9.157(2604)
PAT Global 200.11.187.50(52185) Local 10.1.19.18(2646)
PAT Global 200.11.187.50(52954) Local 10.1.9.157(2715)
PAT Global 200.11.187.50(52955) Local 10.79.1.79(3349)
PAT Global 200.11.187.50(52187) Local 10.1.19.18(2647)
PAT Global 200.11.187.50(33499) Local 10.1.23.19(2499)
PAT Global 200.11.187.50(52956) Local 10.1.9.157(52954)
PAT Global 200.11.187.50(46044) Local 10.1.24.20(2601)
PAT Global 200.11.187.50(52957) Local 10.1.9.157(2717)
PAT Global 200.11.187.50(52701) Local 10.1.9.157(2606)
PAT Global 200.11.187.50(52958) Local 10.1.28.38(1289)
PAT Global 200.11.187.50(39902) Local 10.1.29.7(1057)
PAT Global 200.11.187.50(52959) Local 10.1.28.38(1290)
PAT Global 200.11.187.50(45023) Local 10.79.1.79(3128)
PAT Global 200.11.187.50(52960) Local 10.1.25.35(2021)
PAT Global 200.11.187.50(52961) Local 10.1.28.30(3047)
PAT Global 200.11.187.50(15586) Local jbellomo(1374)
PAT Global 200.11.187.50(52962) Local 10.1.19.18(2698)
PAT Global 200.11.187.50(58606) Local 10.78.1.60(2319)
PAT Global 200.11.187.50(52975) Local 10.1.28.30(52968)
PAT Global 200.11.187.50(52719) Local 10.1.23.30(3822)
PAT Global 200.11.187.50(52986) Local 10.1.28.34(1222)
PAT Global 200.11.187.50(52987) Local 10.1.28.34(1223)
PAT Global 200.11.187.50(17916) Local 10.1.10.16(1093)
PAT Global 200.11.187.50(52988) Local 10.1.7.134(1777)
PAT Global 200.11.187.50(52732) Local 10.1.9.157(2618)
PAT Global 200.11.187.50(52989) Local 10.1.3.16(3469)
Global 10.3.79.14 Local openviw14
PAT Global 10.3.30.50(17327) Local 10.1.10.66(4944)
PAT Global 10.3.30.50(17328) Local 10.1.10.66(4945)
Global 10.3.79.13 Local openview
Global 10.3.9.6 Local 10.1.4.6
Global 10.3.9.2 Local mail
Global 200.11.187.23 Local promafusigma
Global 10.4.9.2 Local fcppl01
Global 200.11.187.7 Local fcweb
Global 200.11.187.27 Local webpromafe

show conn
329 in use, 7019 most used
TCP out 200.31.4.194:14745 in mfweb:80 idle 0:00:00 Bytes 28039 flags UIOB
TCP out 207.46.110.4:80 in 10.78.1.21:2987 idle 0:00:11 Bytes 409455 flags UIO
TCP out 62.43.120.108:4662 in 10.1.24.100:1556 idle 9:19:55 Bytes 33534 flags UIO
TCP out 150.185.65.9:25 in mail:18946 idle 0:11:31 Bytes 120591 flags UIO
TCP out 200.35.64.34:80 in mlopez:4727 idle 2:06:43 Bytes 1226 flags UIO
TCP out 207.46.110.12:80 in 10.1.19.18:2248 idle 0:00:07 Bytes 195732 flags UIO
TCP out 200.84.170.148:80 in 10.1.2.64:3295 idle 0:01:17 Bytes 0 flags saA
TCP out 207.46.110.17:80 in jbellomo:4458 idle 0:00:06 Bytes 34163 flags UIO

TCP out 207.46.110.31:80 in 10.1.25.38:4877 idle 0:00:06 Bytes 203349 flags UIO
TCP out 192.165.220.1:443 in 10.1.23.4:1492 idle 0:01:43 Bytes 151538 flags UIO
TCP out 208.63.148.111:443 in 10.1.19.15:3828 idle 0:00:19 Bytes 15529 flags UIO
TCP out 208.63.148.111:443 in 10.1.19.15:3827 idle 0:00:19 Bytes 21499 flags UIO
TCP out 208.63.148.111:443 in 10.1.19.15:3816 idle 0:00:19 Bytes 46678 flags UIO
TCP out 208.63.148.111:443 in 10.1.19.15:3815 idle 0:00:19 Bytes 66489 flags UIO
TCP out 200.35.64.51:80 in 10.1.24.18:1738 idle 0:00:06 Bytes 56212 flags UIO
TCP out 200.35.64.51:80 in 10.1.24.18:1739 idle 0:00:06 Bytes 15711 flags UIO
TCP out 207.46.106.187:1863 in lmalvarez:4485 idle 0:03:31 Bytes 8473 flags UIO
TCP out 207.68.178.238:80 in jbellomo:4470 idle 0:03:48 Bytes 808 flags UIO
TCP out 207.46.110.3:80 in 10.1.6.77:1403 idle 0:00:08 Bytes 51229 flags UIO
TCP out 63.246.128.180:80 in 10.1.19.18:2287 idle 0:13:26 Bytes 8948 flags UO
TCP out 207.46.110.46:80 in 10.1.24.40:1102 idle 0:00:06 Bytes 915894 flags UIO
TCP out 207.46.110.25:80 in 10.79.1.67:2842 idle 3:27:02 Bytes 19397 flags UIO
TCP out 207.46.110.6:80 in 10.1.28.33:4534 idle 0:00:34 Bytes 19768 flags UIO
TCP out 192.165.220.1:443 in 10.1.10.10:1150 idle 0:01:35 Bytes 1781643 flags UIO
TCP out 192.165.220.1:443 in 10.1.28.24:1126 idle 0:02:23 Bytes 100204 flags UIO
TCP out 161.58.165.95:80 in 10.1.28.34:1277 idle 0:00:12 Bytes 127417 flags UIO
TCP out 161.58.165.95:80 in 10.1.28.34:1278 idle 0:00:12 Bytes 53119 flags UIO
TCP out 207.46.110.13:80 in 10.1.3.140:1217 idle 0:00:17 Bytes 21965 flags UIO
TCP out 207.46.110.19:80 in 10.78.1.84:1105 idle 0:00:01 Bytes 413675 flags UIO
UDP out 161.196.216.22:53 in mail:1259 idle 0:00:12 flags -
UDP out 161.196.216.22:53 in mail:1259 idle 0:00:12 flags -
UDP out 161.196.216.22:53 in mail:1259 idle 0:00:12 flags -
UDP out 161.196.216.22:53 in mail:1259 idle 0:00:12 flags -
TCP out 192.165.220.1:443 in 10.1.29.24:1119 idle 0:02:17 Bytes 772442 flags UIO
TCP out 150.185.65.13:25 in mail:21348 idle 0:03:03 Bytes 547 flags UfFRIO
TCP out 200.9.3.98:80 in 10.79.1.50:4664 idle 0:00:38 Bytes 61761 flags UIO
TCP out 192.165.220.1:443 in 10.1.10.11:1126 idle 0:02:01 Bytes 604651 flags UIO
TCP out 192.165.220.1:443 in 10.1.10.3:1130 idle 0:01:25 Bytes 409383 flags UIO
TCP out 24.46.124.35:80 in 10.1.3.16:3716 idle 0:00:51 Bytes 0 flags saA
TCP out 207.68.178.238:80 in 10.79.1.30:1391 idle 0:00:10 Bytes 1733 flags UIO
TCP out 200.31.4.194:31422 in mfweb:80 idle 0:00:31 Bytes 0 flags UB
TCP out 150.185.65.9:25 in mail:22662 idle 0:00:23 Bytes 0 flags U
TCP out 172.168.112.131:80 in 10.1.3.16:3990 idle 5:43:27 Bytes 88385 flags UIO
TCP out 63.246.128.180:80 in 10.1.19.18:2794 idle 0:00:44 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2795 idle 0:00:44 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2792 idle 0:00:47 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2793 idle 0:00:47 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2798 idle 0:00:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2799 idle 0:00:37 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2796 idle 0:00:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2797 idle 0:00:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2786 idle 0:01:06 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2787 idle 0:01:02 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2784 idle 0:01:06 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2785 idle 0:01:06 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2790 idle 0:00:47 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2791 idle 0:00:47 Bytes 0 flags saA

TCP out 63.246.128.180:80 in 10.1.19.18:2788 idle 0:01:01 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2778 idle 0:01:13 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2779 idle 0:01:13 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2776 idle 0:01:13 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2777 idle 0:01:13 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2783 idle 0:01:09 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2780 idle 0:01:13 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2781 idle 0:01:13 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2770 idle 0:01:20 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2768 idle 0:01:27 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2769 idle 0:01:21 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2775 idle 0:01:14 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2762 idle 0:01:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2763 idle 0:01:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2760 idle 0:01:43 Bytes 0 flags saA
TCP out sqldmz:445 in 10.1.4.6:4004 idle 0:00:55 Bytes 9519112 flags UIO
TCP out 63.246.128.180:80 in 10.1.19.18:2761 idle 0:01:43 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2766 idle 0:01:36 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2767 idle 0:01:33 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2764 idle 0:01:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2765 idle 0:01:40 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2754 idle 0:01:47 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2755 idle 0:01:47 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2753 idle 0:02:00 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2758 idle 0:01:45 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2759 idle 0:01:43 Bytes 0 flags saA
TCP out 136.166.36.152:80 in 10.1.3.16:3751 idle 0:00:25 Bytes 0 flags saA
TCP out 63.246.128.180:80 in 10.1.19.18:2757 idle 0:01:45 Bytes 0 flags saA
TCP out 64.124.83.174:80 in lmalvarez:2182 idle 0:00:51 Bytes 784204 flags UIO
TCP out 207.46.110.18:80 in 10.78.1.87:1227 idle 0:00:15 Bytes 27136 flags UIO
UDP out 150.188.8.196:123 in ofsalazar:123 idle 0:00:02 flags -
TCP out 207.46.110.4:80 in 10.1.6.42:4441 idle 0:00:09 Bytes 205811 flags UIO
TCP out 136.166.36.152:80 in 10.1.3.16:3634 idle 0:01:33 Bytes 0 flags saA
TCP out 136.166.36.152:80 in 10.1.3.16:3689 idle 0:01:00 Bytes 0 flags saA
TCP out 200.31.4.194:64084 in mfweb:80 idle 0:00:00 Bytes 20960 flags UIOB

Websense

Para probar esta herramienta se estableció un grupo piloto en el cual cada técnico pertenecía a un grupo determinado y de esa forma se verificaba si se cumplían las reglas de bloqueo. A continuación se muestran algunas pantallas de los resultados obtenidos según el grupo al que pertenece el usuario. Figuras V.11, V.12 y V.13.

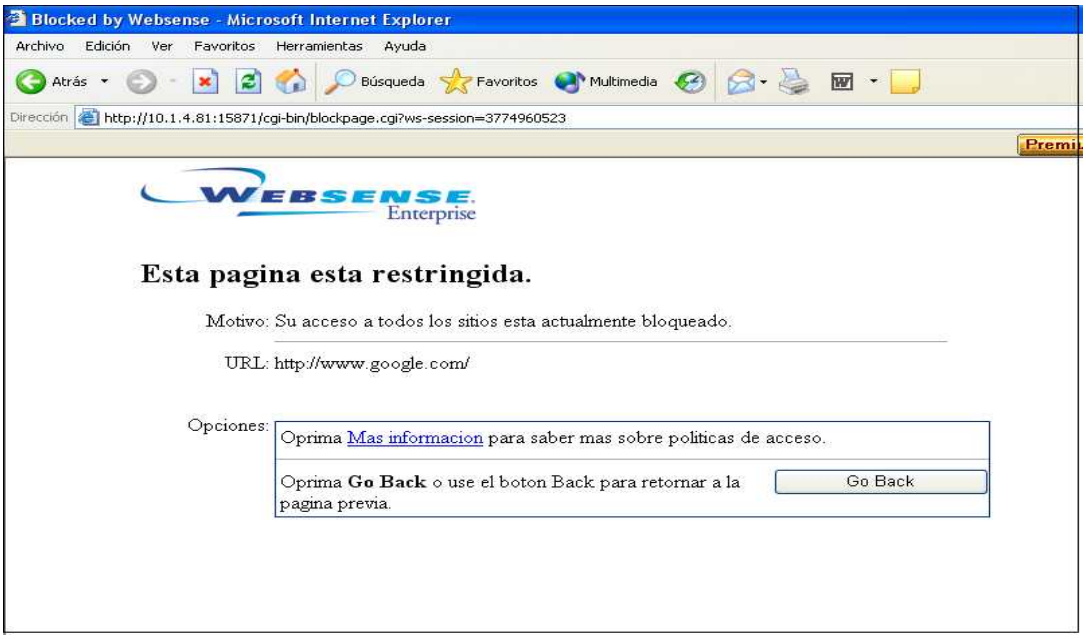


Figura V.11. Usuario bloqueado

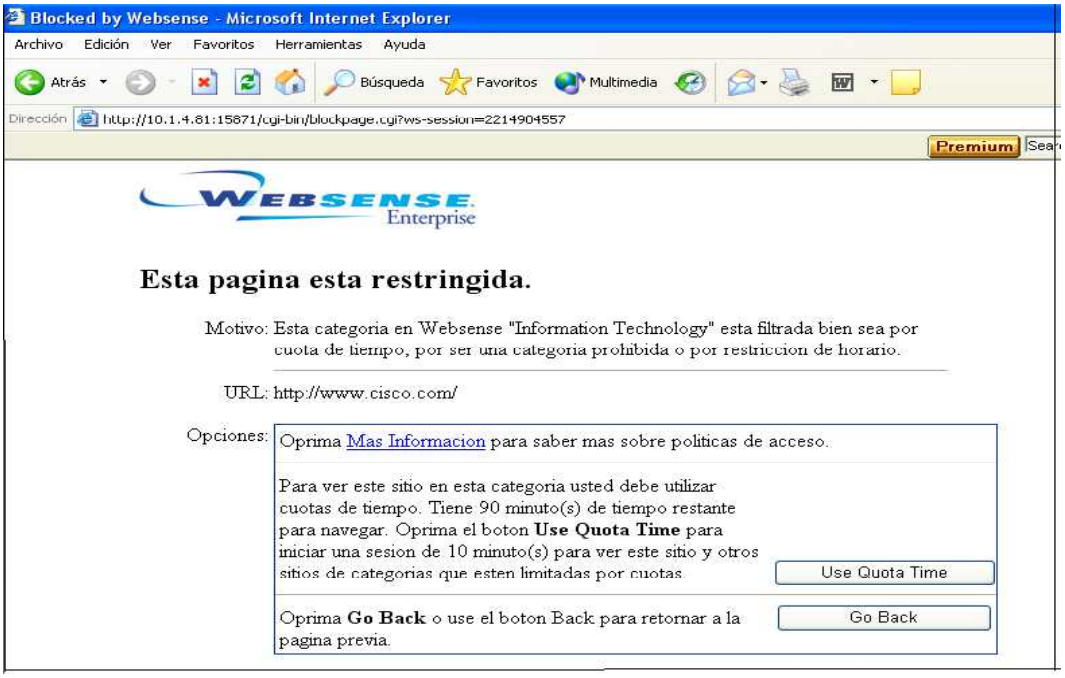


Figura V.12. Usuarios Operativos, que tienen cuota de tiempo

Figura V.13. Usuario Administrador, los cuales tiene accesos especiales.

CONCLUSIONES

Las actuales demandas de información, comunicación, servicios y automatización de procesos están obligando a las empresas, organismos públicos, universidades, etc., a evaluar sus plataformas tecnologicas y los procedimientos operacionales para determinar si pueden satisfacer todas estas necesidades de forma efectiva.

Es así como surge la necesidad de evaluar la plataforma de red local, esquema de seguridad y acceso a Internet de la red corporativa de la Fundación Caracas, con el objetivo de hacer accesible la información, servicios y recursos en el momento requerido; racionalizar el recurso técnico y humano; mejorar la productividad, desempeño y calidad de servicio, así como reducir los costos.

Toda esta actualización tecnológica trajo muchos beneficios a la plataforma de la red local corporativa, las cuales se pueden resumir en:

1. Mejora de los tiempos de respuesta, lo cual satisface el creciente uso de las aplicaciones cliente/servidor, aplicaciones Web, acceso Internet, envío y recepción de correo, compartición de archivos, etc.
2. La utilización de conmutadores (switches), permite que muchos usuarios se comuniquen en paralelo a través del uso de circuitos virtuales y segmentos de red dedicados en un entorno libre de colisiones.
3. El actualizar el entorno LAN a un ambiente conmutado no causó problemas en cuanto al cableado, ya que se pudo reutilizar el existente.
4. El software que poseen los equipos nuevos (switches y firewall) proporciona a los administradores una gran flexibilidad a la hora de gestionar la red.
5. La creación de VLAN permiten una actividad de difusión (broadcast) controlada, además de proporcionar seguridad de grupos de trabajo.

6. La implantación de un esquema de seguridad por zonas, permite gestionar y controlar cada área por separado, lo cual facilita la detección de posibles ataques o accesos no autorizados. Esto a su vez facilita la corrección de una vulnerabilidad o hueco de seguridad.
7. Las mejoras en el entorno de red local, tales como eliminación de la congestión y latencia, aumento del ancho de banda y de la velocidad de transmisión, permiten continuar con la automatización de los procesos que realiza la Fundación Caracas.
8. El establecimiento de políticas de acceso Internet, mediante categorías, grupos y horarios, permite un mayor control y monitoreo del servicio, lo cual se traduce en un mejor uso del acceso Internet y mayor productividad.

Todo avance tecnológico debe ir acompañado de sus respectivas políticas y normas de uso, que establece la alta gerencia de una organización, ya que esto permitirá especificar los aspectos referentes a la seguridad informática de la misma. Por lo tanto, la implantación de las políticas y normas de uso de los servicios y recursos de red en la Fundación Caracas representan el mayor avance de toda esta actualización, permitiendo el uso productivo de los recursos y la aplicación de sanciones en caso de irregularidades o alteraciones.

RECOMENDACIONES

Con base en la experiencia obtenida en la realización de esta actualización tecnologíca y para fortalecer la solución implantada, se recomienda:

1. Realizar todos los trámites necesarios para colocar redundancia en el centro (core) de la red, es decir adquirir otro equipo equivalente al Cisco 4006, para tener un respaldo y si es necesario balanceo de carga.
2. Es muy importante que los administradores de red se mantengan actualizados tecnológicamente, esto con el fin de aprovechar al máximo la plataforma instalada, así como realizar un mantenimiento de gran calidad.
3. Contratar una empresa especializada el análisis de tráfico y de seguridad, por lo menos 4 veces al año, para así determinar cualquier problema que pueda estar generando una aplicación, tarjeta de red, equipo activo, servidor o estación de trabajo. Así como detectar y corregir cualquier hueco de seguridad.
4. Realizar un estudio de factibilidad, con su respectivo análisis costo-beneficio para la actualización del cableado estructurado a categoría 6, así como utilizar el mismo cable para voz y datos, eliminando el cableado telefónico categoría 3 que actualmente existe.
5. Colocar otro firewall en la zona Internet, bien sea Cisco o de otra marca, para crear lo que se conoce como DMZ con cortafuegos (firewall) dual. Esto permitirá proteger al PIX Firewall que controla todas las zonas de seguridad de la red. Además, permite que no exista un sólo punto de falla ante un ataque desde Internet.
6. Colocar en otra VLAN los usuarios que comparten con los equipos de comunicación la VLAN 1, ya que es recomendado por los estándares de seguridad, el separar los equipos de comunicación y de seguridad de los usuarios, utilizando VLAN distintas.

BIBLIOGRAFIA

Mendillo Vincenzo, "**Material de apoyo de la asignatura: Redes de Alta Velocidad**". UCV, Abril 2004.

Mendillo Vincenzo, "**Material de apoyo de la asignatura: Seguridad en Informática y Comunicaciones**". UCV, Octubre 2004.

Brian Hill, "**Manual de Referencia Cisco**", Mac Graw Hill, 2003.

Steve McQuerry, CCIE, "**Interconnecting Cisco Network Devices**", Cisco Press, Abril 2002.

Black Uyless, "**Tecnologías emergentes para redes de computadoras**". Prentice-Hall Hispanoamericana, S.A. Mexico 1.999.

Shaughnessy Tom, "**Manual de Cisco**". Osborne Mc Graw-Hill. España 2001.

H. Kim Lew, Spank McCoy, "**Interconectividad. Manual para resolución de problemas**", Prentice-Hall, 2000.

John Wait, Carl Lindholm, "**Guía del Segundo año**", Academia de networking de Cisco Systems, Cisco Press, 2002.

Tanenbaum, A., "**Redes de Computadoras**". Prentice-Hall Hispanoamericana, S.A. Mexico 1997.

Douglas E. Commer, "**Redes Globales de Información con Internet y TCP/IP**", Prentice Hall, 1996.

Manel Capell i Botey, "**Topología y tipos de LAN**", Canal TI, Octubre 1997.

REFERENCIAS BIBLIOGRAFICAS EN INTERNET

http://www.cisco.com/en/US/products/index.html

http://www.it.uniovi.es/material/arss7-redeslocales-a.pdf

http://www.syntax.es/comStd.asp?pagename=comLAN.asp

http://www.redes.upv.es/gyurl/teoria_0203/tema5_2p_CAS.pdf

http://www.elistas.net/grupos/Informatica/Seguridad

http://www.arturosoria.com/eprofecias/art/wireless_seguridad.asp

http://www.geocities.com/CapeCanaveral/2566/seguri/segurint.htm

http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_179.html

http://www.websense.com/products/about/Enterprise/

http://www.asl-websense.co.uk/websense/enterprise/

http://www.firewallguide.com/

http://www.vnunet.es/Actualidad/An%C3%A1lisis/Seguridad/Sistemas_de_protecci%C3%B3n/20030924050

Anexo B

DESCRIPCIÓN DE LAS CATEGORÍAS Y GRUPOS PREMIUM EXISTENTES EN WEBSENSE ENTERPRISE

- **Aborto**
  Sitios Web con una posición neutral o balanceada respecto a este tema.
  - **Pro-Aborto** – Sitios que proveen información acerca del aborto o son patrocinantes de organizaciones que apoyan el aborto legalmente.
  - **Pro-Vida** – Sitios que proveen información y se oponen legalmente al aborto, buscando incrementar las restricciones de aborto.
- **Material adulto**
  Categoría formada por: Contenido adulto, ropa íntima y trajes de baño, nudismo, sexo, educación sexual.
  - **Contenido adulto** – Sitios que muestran desnudos parciales o totales, pero no actividad sexual; erotismo; parafernalia sexual; sexo orientado al negocio, tales como clubes nocturnos, servicios de dama de compañía; y sitios que ofrecen la compra en línea de servicios sexuales.
  - **Ropa íntima y trajes de baño** – Sitios que ofrecen imagines de modelos con poses y formas sugestivas pero no satírico con semidesnudos. Esto incluye calendarios, fotografías, retratos. Además, Sitios Web donde ofrecen ropa íntima y trajes de baño para su compra.
  - **Nudismos** – Sitios que ofrecen descripciones de nudismo o seminudismo de formas humanas, solas o en grupo, no presentan claramente actos sexuales.
  - **Sexo** – Sitios que describen gráficamente actividad sexual, incluyendo exhibiciones.
  - **Educación Sexual** – Sitios que ofrecen información acerca del sexo y la sexualidad de forma no pornográfica.
- **Grupos de defensa**
  Sitios que prometen cambiar o reformar la política, la opinión pública, las prácticas sociales, las actividades económicas y las relaciones.
- **Negocios y economía**
  Sitios patrocinados por o dedicados a las firmas de negocios, asociaciones de negocios, grupos industriales o negocios en general.
  - **Servicios y datos financieros** – Sitios que ofrecen noticias y cotizaciones de valores, bonos, inversiones en vehículos, anuncios, etc., pero no comercio en línea. Incluye bancos, tarjetas de crédito y seguros.
- **Drogas**
  Categoría formada por: Abuso de drogas, prescripción de medicamentos, marihuana, suplementos y componentes no regulados.
  - **Abuso de drogas** – Sitios que proveen información acerca del uso de drogas prohibidas, excepto la marihuana, parafernalia asociada con el uso y abuso de las drogas.

  - **Marihuana** – Sitios que proveen información acerca del cultivo, preparación y uso de la marihuana. Prescripción de medicamentos – Sitios que proveen información acerca de drogas aprobadas y sus uso médico.
  - **Suplementos y componentes no regulados** – Sitio que provee información acerca de la venta o uso de productos químicos no regulados, tales como los de componentes naturales.
- **Educación**
  Categoría formada por: Instituciones culturales, institutos educacionales y material educativo.
  - **Instituciones culturales** – Museos, galerías, teatros (pero no películas), librerías e instituciones similares.
  - **Instituciones educativas** – Escuelas y otras facilidades educacionales, instituciones de investigación no académicas, eventos y actividades relacionadas con la educación.
  - **Material educativo** – Sitios que proveen o venden información de materias o ofrecen instrucción directa, revistas de aprendizaje y otras publicaciones similares.
  - **Material referencial** – Sitios que ofrecen material de referencia tales como atlas, diccionarios, enciclopedias, formularios, páginas blancas y amarillas y publicación de datos estadísticos.
- **Entretenimiento**
  Sitios que proveen información de radio, televisión, pinturas en movimiento, libros, humor y revistas.
  - **MP3** – Sitios que permiten descargar MP3, archivos de música o escuchar directamente de un servidor.
- **Apuestas**
  Sitios que proveen información de juegos en línea que implican el riesgo de perdida de dinero.
- **Juegos**
  Sitios que ofrecen juegos electrónicos, juegos de video, juegos de computadora, representación de juegos o juegos en línea.
- **Gobierno**
  Sitios relacionados con los niveles de gobierno.
  - **Militar** – Sucursales o agencies de servicios armadas.
  - **Organización política** – Sitios que ofrecen información acerca de partidos políticos y grupos enfocados en elecciones o legislación.
- **Salud**
  Sitios que ofrecen información sobre la salud personal, procedimientos o servicios, pero no drogas. Incluye grupos de auto ayuda.
- **Ilegal o controversial**
  Sitios que proveen información de crímenes no violentos, comportamientos poco éticos o deshonestos o evasiones legales.
- **Información tecnológica**
  Sitios de información sobre computadoras, software, Internet, proveedores, venta de hardware, software, periféricos y servicios.

- **Seguridad de computadoras** – Ofrecen descarga gratuitas de herramientas para la seguridad de las computadoras.
- **Hacking** – Sitios desde los cuales se puede acceder ilegalmente a computadores, equipos de comunicación, software o bases de datos.
- **Evasión de Proxy** – Ofrecen información de cómo evadir un servidor proxy de una organización y obtener acceso no restringido a Internet.
- **Motor de búsqueda y portales** – Ofrecen soporte para búsquedas en el Web, grupos de noticias o índices de direcciones.
- **Sitios que trasladan URL** – Ofrecen traslación en línea de URLs, esto permite evadir un servidor proxy y obtener accesos no autorizados.
- **Hospedaje Web** – Ofrecen organizaciones que proveen servicios de hospedaje, páginas de dominios de alto nivel de comunidades Web.

- **Comunicación Internet**
  Contiene las categorías: Correo y chat vía Web.
  - **Web Chat** – sitios que proveen servicios de chat en el Web (chat vía HTTP o IRC).
  - **Correo basado en Web** – sitios que ofrecen correo basado en Web.
- **Buscadores de empleo**
  Sitios que ofrecen empleos o empleados.
- **Militancia y extremismo**
  Información acerca de grupos extremistas contra gobierno.
- **Noticias y medios de comunicación**
  Ofrecen noticias actuales y de opinión, prensa escrita, revistas u otro medio de información.
- **Racismo y odio**
  Identificación de grupos raciales, denigración de grupos o superioridad de grupos.
- **Religión**
  Conforma las categorías: religiones tradicionales y no tradicionales.
  - **Religiones no tradicionales, ocultas o folkloricas** – Proveen información de religiones no especificas, cultos y creencias o prácticas folklóricas.
  - **Religiones tradicionales** – Información acerca del budismo, bahaísmo, catolicismo, cristianismo, hinduismo, islamismo, judaísmo, mormonismo, etc., así como el ateísmo.
- **Compras**
  Sitios que ofrecen compras en línea de artículos de consumo y servicios.
- **Organizaciones sociales**
  Contiene las categorías: organizaciones de profesionales y obreros, organizaciones de servicios y filantropía, organizaciones sociales.
- **Sociedad y estilos de vida**
  Sitios que proveen información relacionada con la vida diaria, excluyendo el entretenimiento, salud, empleos, sexo y deporte.
  - **Alcohol y tabaco** – ofrece información de ventas de bebidas alcohólicas o tabaco, así como todo lo relaciona con estos.

  - **Intereses homosexuales, lesbianos o bisexuales** – sitios de información que responde a estilos de vida homosexuales, lesbianismo o bisexualidad, incluyendo compras en línea, pero excluyendo caracteres sexuales.
  - **Pasatiempos** – ofrece información de pasatiempos para sedentarios, pero no juegos electrónicos.
  - **Sitios Web personales** – sitios donde las personas publican y mantienen ellas mismas su información individual con intereses personales y para expresarse.
  - **Citas personales** – Sitios que ayuda a los individuos a establecer relaciones personales, sin intenciones de sexo y excluyendo intereses homosexuales, lesbianos o bisexuales.
  - **Restaurantes y comidas** – ofrece listas, reseñas, avisos de comidas, cenas u otros servicios en esta categoría.
- **Eventos especiales**
  Ofrece información de eventos que requieren una categoría especifica.
- **Deportes**
  Ofrece información sobre deportes, juegos activos y recreación.
  - **Caza y club de tiro** – Ofrece información de clubes de tiro o similares, incluyendo juegos de guerra.
- **De mal gusto**
  Sitios con contenido ofensivo o chocante, pero no violento o atemorizante.
  Incluye sitios dedicados a la escatología o tópicos similares, lenguaje impropio, humor o comportamiento.
- **Viajes**
  Sitios que proveen información sobre servicios de viajes y destinos.
- **Definidas por el usuario**
  Categorías definidas por el usuario.
- **Vehículos**
  Información sobre vehículos, incluyendo soporte en línea para la compra de vehículos o partes.
- **Violencia**
  Sitios que ofrecen violencia o daños corporales, incluyendo despliegue de imagines de muerte, sangre o heridas, presentación de imagines o descripciones grotesca o atemorizantes.
- **Armas**
  Información sobre ventas de armas y todo lo relaciona con estas.
  Grupos Premium (disponibles con un costo adicional)
- **Grupo Premium I.** Categoría formada por: publicidad, descarga de software sin costo, mensajería instantánea, club de noticias electrónicas, comercio y corretaje en línea, pagar para navegar.

  - **Publicidad** – Ofrece avisos gráficos o de texto.
  - **Descarga de software sin costo** – Ofrece descarga de software sin costo.
  - **Mensajería instantánea** – Ofrecen mensajería instantánea.
  - **Clubes de noticias electrónicas** – ofrece clubes de negocio, grupos de discusión, noticias electrónicas.

  - **Comercio y corretaje en línea** – Sitios que soportan actividades comerciales e inversiones seguras y bien gestionadas.
  - **Pagar para navegar** – Sitios donde los usuarios pagan para poder navegar un sitio, para usar correo o publicidad.
- **Grupo Premium II.** Categoría formada por: Radio y TV Internet, telefonía Internet, compartición de archivos, transferencia de archivos, almacenamiento de archivos personales en servidores de Internet para respaldo o intercambio y películas de cine.
- **Grupo Premium III.** Categoría formada por: Sitios Web maliciosos.
  - **Sitios Web maliciosos** – Ofrecen código que puede intencionalmente modificar los sistemas de usuario sin permiso y causando daños.

Fundación Caracas
Oficina de Informática

Informe Técnico No. 044

Caracas, 20 de Noviembre de 2003

ASUNTO

Actualización de las Políticas y Normas de Seguridad de la Red de la Fundación Caracas para los administradores de red y usuarios finales, así como su aprobación por parte del Presidente de la Fundación Caracas para su puesta en marcha a partir del 01 de enero de 2004.

OBJETIVO

Presentar para su consideración y aprobación una serie de políticas y normas sobre el uso de los servicios informáticos que ofrece la red de la Fundación Caracas, de forma tal que se garantice la integridad y seguridad de la información en dicha red.

En la realización de estas normas se tomaron en cuenta las Normas y Políticas de la Red, aprobadas por el Ciudadano Ministro Dr. José Rojas en Punto de Cuenta Nº OI-06 de fecha 30 de abril de 2001 y distribuidas a todas las Direcciones en fecha 02 de mayo de 2001, modificándose algunas de ellas y agregándose otras nuevas.

JUSTIFICACION

Los activos de información y los equipos informáticos son recursos importantes y vitales que apoyan los objetivos del negocio de la Fundación Caracas. Por esta razón la Oficina de Informática y las distintas Unidades de Fundacaracas tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Fundación Caracas debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa

(PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las siguientes normas y políticas tienen como objeto dar a conocer, a los usuarios de la Fundación Caracas las reglas para el uso de los equipos, servicios y recursos que ofrece la Red LAN/WAN de la Fundación Caracas, para garantizar a los usuarios la prestación de los servicios y el acceso a la comunicación, en adecuadas condiciones de calidad; así como, las sanciones establecidas por el incumplimiento de las mismas, con la finalidad de proporcionar un aprovechamiento justo de los mismos, resguardando la seguridad e integridad de la información, al facilitar y mejorar el trabajo compartido y en grupo..

RESPONSABILIDADES

Oficina de Informática

La Oficina de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con las distintas Oficinas, Direcciones Generales y Coordinaciones. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

Oficinas, Direcciones Generales y Coordinación de la Fundación Caracas

Las distintas Oficinas, Direcciones Generales y Coordinaciones de la Fundación Caracas están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos dando cumplimiento a las Políticas y Normas de Seguridad de la Red de la Fundación Caracas. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberá notificar a la Oficina de Informática para que se tomen las acciones correctivas rápidamente para así reducir los riesgos.

Directores, Supervisores y Coordinadores de cada unidad funcional de la Fundación Caracas

Los Supervisores, Coordinadores ó Directores de cada unidad funcional de la Fundación Caracas tendrán la responsabilidad de asegurar y garantizar el cumplimiento de las Políticas y Normas de Seguridad de la Red de la Fundación Caracas, para lo cual solicitarán el apoyo de la Oficina de Informática en la detección de irregularidades.

Usuarios

Los usuarios son responsables de cumplir con todas las Políticas y Normas de Seguridad de la Red de la Fundación Caracas. Los empleados, contratados y todo personal usuario que labore en la Fundación Caracas están en la obligación de cumplir las Políticas y Normas establecidas en este documento, sobre el Uso de los Equipos y Servicios que ofrece la Red; su incumplimiento, será sancionado de conformidad con lo establecido en la Ley sobre el Estatuto de la Función Público, la ley del Trabajo y el reglamento de la Ley Orgánica del Trabajo

POLÍTICAS

Generales

1. La Oficina de Informática tiene entre sus funciones el monitoreo de los servicios que ofrece la red (correo, salida Internet, impresión, compartición de archivos, etc.), controlar el uso y acceso a dichos servicios y detectar, reportar y corregir cualquier abuso, acceso no autorizado o violación a las normas establecidas por Fundacaracas. Este monitoreo consistirá en la aplicación de auditorias periódicas, y que podrán contemplar grupos aleatorios de estaciones de trabajo o a toda la red LAN / WAN de la Fundación Caracas.

2. La mudanza o traslado de las partes ó piezas de los teléfonos y Equipos de Computación, tales como CPU, monitores, teclados, ratón (mouse), impresoras y otros accesorios, corresponden a la Dirección General de Servicios, Dependencia a quien debe ser solicitada. A su vez, la Oficina de Informática supervisará y asesorará la ejecución de los traslados de las áreas involucradas, a fin de garantizar las condiciones mínimas de seguridad para los equipos. Cuando el activo informático sea trasladado fuera de la sede de la Fundación Caracas debe ser aprobada su salida mediante autorización escrita por la Oficina de Informática, la Oficina de Seguridad y la Dirección General de Servicios de Fundacaracas.

3. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

4. Con el fin de mejorar la productividad y dar cumplimiento al Gobierno Electrónico, la Fundación Caracas promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Fundación Caracas y no propiedad de los usuarios de los servicios de comunicación.

5. Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

6. Se prohíbe el uso de software analizadores de red, de vulnerabilidades, sniffer o relativos al estudio de características de la red sin la autorización por escrito del Director General de la Oficina de Informática de la Fundación Caracas.

7. El personal profesional, técnico y administrativo de la Oficina de Informática deberá vigilar el cumplimiento de las Normas en todas las dependencias y direcciones de la Fundación Caracas, reportando cualquier irregularidad que detecte.

8. La información interna es propiedad de la Fundación Caracas y no puede ser copiada, modificada, anulada o usada para otros propósitos.

9. El incumplimiento de alguna de las Normas sobre el uso de los recursos y servicios de red, será sancionado de conformidad con la Ley Orgánica del Trabajo y su Reglamento General.

NORMAS

Uso de los equipos

1. Corresponderá a la Oficina de Informática, la instalación de los equipos en lugares con condiciones ambientales adecuadas, es decir, temperaturas bajas, buena iluminación, libre de humedad (sin goteras o filtraciones, etc.), al mismo tiempo el usuario velará por mantener dichas condiciones. En caso de surgir algún problema que impida tener las condiciones exigidas, la Oficina de Informática hará las recomendaciones necesarias al usuario, de forma tal que este las comunique a la Dirección General de Servicios para su adecuación.

2. La Dirección General de Servicios debe garantizar que las mesas o estantes a ser utilizadas para la colocación de los equipos (computadores personales, impresoras, fotocopiadoras, etc.), se encuentren en buenas condiciones. En caso de no poseer dichos muebles estos deben ser solicitados a la Dirección General de Servicios, previa especificación técnica de la Oficina de Informática, sobre los requerimientos necesarios para dicha instalación.

3. La Oficina de Informática es la única autorizada para instalar el software adecuado, de acuerdo al perfil y área de trabajo de los usuarios. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Fundación Caracas está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

4. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la Oficina de Informática.

5. La Oficina de Informática debe velar porque el equipo se encuentre conectado a un regulador de voltaje, con el fin de protegerlo de fluctuaciones de corriente. En caso de no poseer regulador, éste debe ser solicitado por el usuario a la Dirección General de Servicios.

6. El personal que utiliza un computador portátil de la Fundación Caracas y que contenga información confidencial del mismo, no debe dejarlo en un lugar público y de fácil acceso, sobre todo cuando esté de viaje.

7. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

8. Los equipos de computación de la Fundación Caracas sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

9. Debe respetarse y no modificar la configuración de hardware y software establecida por la Oficina de Informática

10. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

11. Es responsabilidad del usuario hacer respaldo periódico de los datos guardados en el computador personal asignado para su uso.

12. Cuando se repare un computador personal fuera de la Fundación Caracas se debe eliminar toda la información confidencial de dicho equipo (almacenada en sus unidades de disco duro local) antes de salir de las instalaciones.

13. Los Usuarios no deben:

    a) Llevar al sitio de trabajo computadores portátiles (laptop) y PDA, ya que mediante estos equipos puede ser extraída información relevante de la Fundación Caracas. En caso de ser necesario se requiere solicitar la autorización de la Oficina de Informática.
    b) Copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la Fundación Caracas, sin la aprobación previa del Director General (o grado equivalente) de la Unidad a la cual pertenece la información.
    c) Usar módems en los computadores personales que están conectados a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la Fundación Caracas. Esto con el fin de prevenir la intrusión de hackers a través de puertas traseras.
    d) Pegar a los equipos (Monitor, CPU, teclado y ratón) e impresoras cualquier tipo de calcomanía o etiqueta que no sea la de identificación del bien.
    e) Colocar contraseñas de sistema (setup) al equipo. Estos requerimientos deben ser solicitados a la Oficina de Informática.
    f) Cambiar los parámetros de configuración del equipo (impresoras conectadas, resolución de vídeo, conexión a los servidores, configuración de red, etc.). Estos cambios deben ser solicitados a la Oficina de Informática.
    g) Instalar juegos, ni ningún software en los computadores personales que no este autorizado por la Oficina de Informática.
    h) Intercambiar componentes tales como, teclado, ratón (mouse), CPU, monitor, con otros equipos, sin la previa autorización de su supervisor o del personal técnico de la Oficina de Informática.
    i) Consumir alimentos, bebidas y fumar en el área donde están instalados los equipos de computación o los teléfonos.

Uso del correo electrónico

1. El uso del correo electrónico es un servicio que presta la Fundación Caracas a su personal, para mejorar el desempeño y productividad en las labores inherentes a su cargo.

2. Las cuentas de correo son intransferibles, quedando terminantemente prohibido facilitar su utilización a otras personas. Cada usuario es el dueño y responsable de todos los actos que se registren con su cuenta.

3. Se entiende por mal uso de correo electrónico, entre otras cosas, lo siguiente:

   a) Uso del correo electrónico violando normas éticas, incluyendo agresión a la reputación de las personas, amenazas, uso de lenguaje abusivo, violación de la propiedad intelectual, etc.
   b) Uso del correo electrónico para acciones comerciales ajenas a la actividad de la Fundación Caracas.
   c) Uso del correo electrónico referido a cualquier tipo de información religiosa o política sin la debida autorización.
   d) Uso del correo electrónico referido a aspectos sociales, recreacionales, culturales, educacionales o caritativos sin la debida aprobación.
   e) Uso del correo electrónico referido a cualquier información pornográfica o de carácter sexista.
   f) Uso del correo electrónico referido a cualquier tipo de información discriminatoria por razones de sexo, raza, filiación política o religiosa, minusvalía física o condición social.
   g) Uso del correo electrónico para difundir "**correos en cadena**". Los referentes a virus electrónicos, deben ser transmitidos al Administrador del Sistema, quien se encargará de difundir las advertencias necesarias.

Uso de Directorios y Almacenamiento de Archivos

1. Los usuarios deben almacenar la información que se relacione con el objeto de la Fundación Caracas y toda aquella información a compartir en el Servidor de Archivos de la red. Para ello se debe hacer la solicitud a la Oficina de Informática, siguiendo los pasos de una solicitud de servicios contemplados dentro de este manual de normas y políticas.

2. Los Jefes, Directores o Coordinadores de área deberán especificar el tipo de acceso que tendrá su personal a la data compartida en los servidores de la

Fundación Caracas.

3. La Oficina de Informática realizará entre sus funciones de mantenimiento preventivo de los computadores personales de la red, la eliminación de archivos temporales generados por Internet, Word, Excel, etc., y archivos de música (.mp3).

Uso de los Servicios de Internet

1. El uso de los servicios Internet es exclusivo para labores de investigación en áreas afines al ámbito de trabajo en que se desempeña el usuario. Debe evitarse la consulta de páginas pornográficas, juegos, horóscopo, chat, farándula y club de amistades.

2. Los usuarios no deben bajar (copiar), almacenar o instalar en sus equipos software de Internet y en general software que provenga de una fuente no confiable que no estén relacionado con su área de trabajo o que no represente material de apoyo a las labores que desempeña en la Fundación Caracas. En caso de ser necesario su uso este software debe ser comprobado en forma rigurosa y debe estar aprobado su uso por la Oficina de Informática.

3. No debe utilizarse software bajado de Internet.

4. La oficina de Informática monitorea la salida a Internet de cada usuario detectando cualquier uso indebido.

5. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Fundación Caracas y en tal sentido deben usarse las horas no laborables establecidas por la oficina de Informática y controladas mediante el software Websense. Los usuarios deben moderar su conexión a Internet, es decir, restringir y controlar el tiempo de conexión, ya que este servicio es utilizado por todos los empleados de la Fundación Caracas y se cuenta con una salida limitada.
6. Los servicios de Internet están registrados a nombre del usuario que utiliza el servicio, esta cuenta es intransferible y las auditorias realizadas a la conexión serán presentadas a su nombre. Cualquier irregularidad detectada será única y exclusivamente responsabilidad del usuario registrado.

Uso de las Cuentas de Usuario (Login)

1. Los usuarios no deben utilizar contraseñas fáciles de adivinar, tales como su fecha de nacimiento, edad, placa del carro, su nombre o el de sus hijos, etc., en el inicio de la sesión de red, sino aquellas que brinden seguridad en la información, ya que estas son intransferibles.

2. Los usuarios deben utilizar su cuenta de red (login), sólo desde su computador personal ya que todas las tareas y accesos que se registren en su cuenta, independientemente del equipo donde se realicen son de su responsabilidad. Es importante que el usuario recuerde que las cuentas de usuario son intransferibles, quedando terminantemente prohibido facilitar su utilización a otras personas.

3. Los usuarios no deben utilizar su cuenta de red para realizar actos de sabotaje en los servidores de la red u otros equipos que no sean de su competencia. La violación de esta norma será sancionada de conformidad con lo previsto en la Ley Orgánica de Trabajo y su Reglamento General.

4. El password de acceso a la red caducará cada treinta (30) días.

5. Corresponde a la Oficina de Recursos Humanos notificar oportunamente a la Oficina de Informática:

   a) Los empleados que ya no laboren en la Fundación Caracas o que estén en Comisión de Servicio, con la finalidad de proceder a la eliminación de la cuenta de red y de correo.

   b) El ingreso de nuevo personal a la Fundación Caracas, a objeto de determinar la disponibilidad de equipos, revisar los puntos de red y telefonía, para crear las cuentas de correo y de red solicitadas.

Uso de las impresoras

1. Utilizar las impresoras sólo para la impresión de trabajos relacionados con su área.

2. Verificar, antes de imprimir, que el equipo cuenta con la suficiente cantidad de papel, para evitar molestias a otros usuarios. Deben colocar en las bandejas el papel de tamaño adecuado, de acuerdo a la configuración de las mismas, ya

que al introducir una hoja de tamaño incorrecto se produce un " atasco de papel ", hecho que podría generar daños a la impresora, además de detener el servicio de impresión a los usuarios compartidos.

3. Hacer uso racional de los recursos de impresión, por ser un servicio en red compartido por muchos usuarios.

4. Ver la presentación preliminar del documento a fin de efectuar las correcciones que sean necesarias y verificar el formato del mismo (márgenes, tamaño y orientación del papel), antes de dar la orden de impresión. Igualmente, se recomienda verificar la impresora a la cual se está enviando la impresión, a fin de evitar errores en la selección.

5. Evitar manipular el Panel de Control de la impresora, pues esto puede desconfigurar el servicio de impresión en red, si se utiliza en forma inadecuada.

6. Evitar manipular las cubiertas que conducen a las partes interiores de la impresora, sólo debe manipular las bandejas donde se introduce el papel.

7. No utilizar la impresora para reproducir los dibujos de Internet relacionados con caricaturas, tarjetas, juegos, poemas, tarjetas de cumpleaños, imágenes indebidas y todo aquello que no este relacionado con el trabajo del empleado.

8. Evitar el uso de papel de reciclaje, ya que el papel usado puede atascarse y causar daño en la impresora.

9. No introducir objetos de metal (grapas, clips, etc.) o colocarlos sobre las tapas o bases de la impresora.

10. Los usuarios solo pueden interrumpir los servicios de impresión propios, no puede apagar la impresora, reiniciarla o borrar los trabajos de la cola de impresión de otras personas.

11. Cuando existan problemas relacionados con la calidad de impresión, atasco de papel, desconexión a la impresora, etc., los usuarios deben comunicarse (vía correo o telefónicamente) con el personal de Escritorio de Ayuda (Help Desk) para recibir el soporte técnico necesario.

Uso de los teléfonos

1. Los usuarios tendrán asignada una clave de acceso telefónico con salida externa, la cual representa un seguro para la realización de llamadas.

2. La clave telefónica es intransferible y una vez utilizada por su propietario queda registrada en el sistema.

3. El sistema telefónico posee un perfil de categorías, las cuales son asignadas a los empleados dependiendo de sus funciones y necesidades. Para la asignación de éstas categorías, se requiere la autorización de los funcionarios que a continuación se listan:

CATEGORIA	NIVEL DE ACCESO	PERSONA QUE AUTORIZA
1	Internacional	Presidente – Director General
2	Nacional - Celular	Director General
3	Nacional (sin Celular)	Director General
4	Local - Celular	Director de Línea
5	Local	Director de Línea
6	Interno	Categoría por defecto

4. Todo usuario que pierda su clave de acceso telefónico deberá notificarlo a su Jefe Inmediato, quien solicitará a la Oficina de Informática mediante memorando, una nueva clave.

5. El número telefónico de cada empleado esta asociado a un punto de red de voz, no al teléfono. Por lo tanto, si el empleado es mudado a un nuevo cubículo el número de su extensión cambia.

6. La Oficina de Informática conjuntamente con los Jefes Inmediatos y los usuarios, deben cuidar que los teléfonos sean colocados en lugares seguros para evitar daños físicos.

7. La Oficina de Informática de la Fundación Caracas procesará datos estadísticos sobre el uso de los teléfonos mediante los reportes de la central telefónica (PABX) los cuales contienen detalles sobre el número llamado, la duración de la llamada, el costo y la hora en que se efectuó la llamada.

Solicitudes de Servicio

1. Los usuarios deben realizar las solicitudes de servicio, sin excepción, a través del centro de Escritorio de Ayuda (Help Desk) de la Oficina de Informática por las extensiones 1472 y 1494, por correo electrónico (***soporte@fundacaracas.gov.ve***) o por cualquier otro mecanismo que defina la Oficina de Informática. Entre los servicios que pueden ser solicitados por este medio se encuentran:

   a) Creación y conexión de usuarios nuevos en la red.
   b) Problemas de conexión a la red.
   c) Cambios de categoría telefónica.
   d) Asignación de claves telefónicas.
   e) Problemas con el correo, impresoras, teléfonos.
   f) Virus.
   g) Problemas con los componentes físicos del equipo.

2. Para la solicitud de conexión Internet, la Oficina de Informática suministrará el formulario denominado “SOLICITUD DE SALIDA INTERNET”, el mismo debe ser llenado con los datos del empleado al cual se le dará el servicio. Dicho formulario debe venir firmado y sellado por el Director del Área a la cual pertenezca el empleado.

3. La hoja de servicios denominada FORMULARIO DE CONTROL DE SERVICIOS, representa una constancia de los servicios prestados por el personal de la Oficina de Informática a los usuarios. Por lo tanto, al ser firmada por el usuario se considera conforme lo expuesto en dicho formulario.

   - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
   - No divulgar información confidencial de la Fundación Caracas a personas no autorizadas.
   - No permitir y no facilitar el uso de los sistemas informáticos de la Fundación Caracas o a personas no autorizadas.
   - No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo de la Fundación Caracas.
   - Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

NORMAS PARA LOS ADMINSITRADORES DE RED

1. Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

2. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

3. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
4. La Oficina de Informática debe respaldar la información almacenada en los servidores del la Fundación caracas y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones.

Elaborado por:

María Hernández
Coordinadora de Informática

Janeth Gonzalez
Especialista en Informática

Revisado por:

Jesús Cubillan
Analista de
Procesamiento de Datos

Jesús Ramos
Analista de
Procesamiento de Datos I

Douglas Rodríguez
Asesor Técnico

Aprobado por:

Ligia Isabel Terrazas
Directora General de la
Oficina de Informática

Nota: Este informe no es válido, sin las firmas correspondientes a los que elaboraron, revisaron y aprobaron lo aquí expuesto.

GLOSARIO

ACL (lista de control de acceso)**:**

Lista mantenida por un router de Cisco para controlar el acceso desde o hacia un router para varios servicios (por ejemplo, para evitar que los paquetes con una dirección IP determinada salgan de una interfaz en particular del router). Ver también ACL extendida y ACL estándar.

ACL estándar (lista de control de acceso estándar):

ACL que filtra basándose en la máscara y dirección origen. Las listas de acceso estándares autorizan o deniegan todo el conjunto de protocolos TCP/IP. Ver también ACL, ACL extendida.

ACL extendida (lista de control de acceso extendida)**:**

ACL que verifica las direcciones origen y destino. Comparar con ACL estándar. Ver también ACL.

Actualización del enrutamiento:

Mensaje que se envía desde el router para indicar si la red es accesible y la información de costo asociada. Normalmente, las actualizaciones del enrutamiento se envían a intervalos regulares y luego de que se produce un cambio en la topología de la red. Comparar con actualización relámpago.

Administración de red:

Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallas de una red.

Administrador de red:

Persona a cargo de la operación, mantenimiento y administración de una red.

Almacenamiento y envío:

Técnica de conmutación de paquetes en la que las tramas se procesan completamente antes de enviarse al puerto apropiado. Este procesamiento incluye calcular el CRC y verificar la dirección destino. Además, las tramas se deben almacenar temporalmente hasta que los recursos de la red (como un enlace no utilizado) estén disponibles para enviar el mensaje.

Analizador de red:

Dispositivo de hardware o software que le brinda diversas funciones de diagnóstico de fallas de la red, incluyendo decodificadores de paquete específicos del protocolo, pruebas de diagnóstico de fallas específicas preprogramadas, filtrado de paquetes y transmisión de paquetes.

Ancho de banda:

Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

Aprendizaje de la dirección MAC:

Servicio que caracteriza a un switch de aprendizaje en el que se guarda la dirección MAC origen de cada paquete recibido, de modo que los paquetes que se envían en el futuro a esa dirección se pueden enviar solamente a la interfaz de switch en la que está ubicada esa dirección. Los paquetes cuyo destino son direcciones de broadcast o multicast no reconocidas se envían desde cada interfaz de switch salvo la de origen. Este esquema ayuda a reducir el tráfico en las LAN conectadas. El aprendizaje de las direcciones MAC se define en el estándar IEEE 802.1.

ARP *(Protocolo de Resolución de Direcciones)***:**

Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826. Comparar con RARP.

ARP proxy *(protocolo proxy de resolución de direcciones)***:**

Variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un router) envía una respuesta ARP en nombre de un nodo final al host solicitante. ARP proxy puede reducir el uso del ancho de banda en enlaces WAN de baja velocidad.

AS *(sistema autónomo)***:**

Conjunto de redes bajo una administración común que comparte una estrategia de enrutamiento en común. También denominado dominio de enrutamiento. La Agencia de Asignación de Números Internet le asigna al AS un número de 16 bits.

Asignación de direcciones:

Técnica que permite que diferentes protocolos interoperen convirtiendo direcciones de un formato a otro. Por ejemplo, al enrutar IP en X.25, las direcciones IP deben

asignarse a las direcciones X.25 para que la red X.25 pueda transmitir los paquetes IP

Atenuación:
Pérdida de energía de la señal de comunicación

AUI (*interfaz de unidad de conexión*)**:**

Interfaz IEEE 802.3 entre una MAU y una tarjeta de interfaz de red. El término AUI también puede hacer referencia al puerto del panel posterior al que se puede conectar un cable AUI, como los que pueden encontrarse en la tarjeta de acceso Ethernet del LightStream de Cisco. También denominado cable transceptor.

Autenticación:
Con respecto a la seguridad, la verificación de la identidad de una persona o proceso.

Backbone:
Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Bit:
Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno. Ver también byte.

BOOTP (*Protocolo Bootstrap*)**:**

Protocolo usado por un nodo de red para determinar la dirección IP de sus interfaces Ethernet para afectar al inicio de la red.

Bootstrap:

Operación simple predeterminada para cargar instrucciones que a su vez hacen que se carguen otras instrucciones en la memoria o que hacen entrar a otros modos de configuración.

BPDU (*unidad de datos de protocolo de puente*)**:**

Paquete Hello del protocolo Spanning-Tree (árbol de extensión) que se envía a intervalos configurables para intercambiar información entre los puentes de la red.

Broadcast:

Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

Byte:

Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits).

Cable de fibra óptica:

Medio físico que puede conducir una transmisión de luz modulada. En comparación con otros medios de transmisión, el cable de fibra óptica es más caro, pero por otra parte no es susceptible a la interferencia electromagnética, y permite obtener velocidades de datos más elevadas. A veces se denomina fibra óptica.

Cableado de categoría 3:

Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps. Ver también UTP.

Cableado de categoría 4:

Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Ver también UTP.

Cableado de categoría 5:

Uno de los cinco grados del cableado UTP descrito en el estándar EIA/TIA 568B. El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps. Ver también UTP.

CHAP (*Protocolo de autenticación de intercambio de señales*)**:**

Función de seguridad utilizada en líneas que usan el encapsulamiento PPP para evitar el acceso no autorizado. CHAP no impide por sí mismo el acceso no autorizado, pero sí identifica el extremo remoto; el router o servidor de acceso determina entonces si se permite el acceso a ese usuario.

Cifrado, codificado (*encryption*)**:**

Método para proteger los datos de un acceso no autorizado a los mismos. Se utiliza normalmente en Internet para sustraer el correo electrónico.

CIR (*velocidad de información suscrita*)**:**

Velocidad en bits por segundo, a la que el switch Frame Relay acepta transferir datos.

Circuito:

Ruta de comunicaciones entre dos o más puntos.

Circuito asíncrono:

Señal que se transmite sin sincronización precisa. Estas señales normalmente tienen diferentes frecuencias y relaciones de fases. Las transmisiones asíncronas habitualmente encapsulan caracteres individuales en bits de control (denominados bits de inicio y detención) que designan el principio y el final de cada carácter. Ver también circuito síncrono.

Circuito síncrono:

Señal transmitida con sincronización precisa. Estas señales tienen la misma frecuencia, y los caracteres individuales están encapsulados en bits de control (denominados bits de arranque y bits de parada) que designan el comienzo y el fin de cada carácter.

Circuito virtual:

Circuito creado para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par VPI/VCI y puede ser permanente (PVC) o conmutado (SVC). Los circuitos virtuales se usan en Frame Relay y X.25. En ATM, un circuito virtual se denomina canal virtual. A veces se abrevia VC.

Cliente:

Nodo o programa de software (dispositivo front-end) que requiere servicios de un servidor. Ver también servidor.

Colisión:

En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Confiabilidad:

Proporción entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación es alta, la línea es confiable. Utilizado como métrica de enrutamiento.

Congestión:

Tráfico que supera la capacidad de la red.

Conmutación:

Proceso de tomar una trama entrante de una interfaz y enviarla a través de otra interfaz.

Conmutación de circuito:

Sistema de conmutación en el que un circuito físico dedicado debe existir entre el emisor y el receptor durante la "llamada". Se usa ampliamente en la red de la compañía telefónica. La conmutación de circuito se puede comparar con la contención y la transmisión de tokens como método de acceso de canal y con la conmutación de mensajes y la conmutación de paquetes como técnica de conmutación.

Conmutación de paquetes:

Método de networking en el cual los nodos comparten el ancho de banda entre sí enviando paquetes.

Conmutación rápida:

Conmutación que ofrece el nivel más bajo de latencia, enviando inmediatamente un paquete después de recibir la dirección destino.

Consola:

Equipo terminal de datos a través del cual se introducen los comandos en un host.

Control de flujo:

Técnica para garantizar que una entidad transmisora no supere la capacidad de recepción de datos de una entidad receptora. Cuando los búferes del dispositivo receptor están llenos, se envía un mensaje al dispositivo transmisor para que suspenda la transmisión hasta que se hayan procesado los datos en los búferes. En las redes IBM, esta técnica se llama pacing.

Convergencia:

Velocidad y capacidad de un grupo de dispositivos de interconexión que ejecutan un protocolo de enrutamiento específico para concordar sobre la topología de una interconexión de redes luego de un cambio en esa topología.

Costo:

Valor arbitrario, basado normalmente en el número de saltos, ancho de banda del medio, u otras medidas, que es asignado por un administrador de red y utilizado para comparar diversas rutas a través de un entorno de internetwork de redes. Los valores de costo utilizados por los protocolos de enrutamiento determinan la ruta más favorable hacia un destino en particular: cuanto menor el costo, mejor es la ruta

CSMA/CD (*Acceso múltiple con detección de portadora y detección de colisiones*)**:**

Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una

colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

CSU/DSU (*unidad de servicio de canal/unidad de servicio de datos*)**:**

Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

DCE (*equipo de transmisión de datos*)**:**

Dispositivo usado para convertir los datos del usuario del DTE en una forma aceptable para la instalación de servicios de WAN. Comparar con DTE

Dirección broadcast:

Dirección especial reservada para enviar un mensaje para todas las estaciones. Por lo general, una dirección broadcast es una dirección destino MAC compuesta exclusivamente por números uno. Comparar con dirección multicast y dirección unicast. Ver también broadcast.

Dirección de red:

Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo

Dirección de subred:

Parte de una dirección IP especificada como la subred por la máscara de subred.

Dirección destino:

Dirección de un dispositivo de red que recibe datos. Ver también dirección origen

Dirección MAC (*Control de Acceso al Medio*)**:**

Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

Dirección multicast:

Dirección única que se refiere a múltiples dispositivos de red. Sinónimo de dirección de grupo. Comparar con dirección broadcast y dirección unicast. Ver también multicast.

Dirección origen:

Dirección de un dispositivo de red que envía datos.

DLCI (*identificador de conexión de enlace de datos*)**:**

Valor que especifica un PVC o un SVC en una red Frame Relay. En la especificación Frame Relay básica, los DLCI son significativos localmente (es decir, dispositivos conectados que usan diferentes valores para especificar la misma conexión). En la especificación extendida LMI, los DLCI son significativos globalmente (es decir, los DLCI especifican dispositivos de extremos individuales).

DNS (*Sistema de denominación de dominio*)**:**

Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

Dominio de colisión:

En Ethernet, el área de la red en la que las tramas que colisionan se propagan. Los repetidores y los hubs propagan las colisiones, mientras que los switches de LAN, puentes y routers no lo hacen..

DTE (*equipo terminal de datos*)**:**

Dispositivo en el extremo del usuario de una interfaz usuario a red que sirve como origen de datos, destino, o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza normalmente señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como computadores, traductores de protocolo y multiplexores. Comparar con DCE

EEPROM (*memoria programable de solo lectura borrable eléctricamente*)**:** EPROM que se puede borrar utilizando señales eléctricas aplicadas a contactos (pins) específicos.

EIA/TIA568:

Estándar que describe las características y aplicaciones para diversos grados de cableado UTP.

Encapsulamiento:

Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la

trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red.

EPROM (*memoria programable de sólo lectura borrable*)**:**

Chips de memoria no volátil programados después de su fabricación y que, de ser necesario, pueden ser borrados por ciertos medios y reprogramados. Comparar con EEPROM y PROM

Estándar:

Conjunto de reglas o procedimientos de uso generalizado o de carácter oficial.

Ethernet:

El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

Fast Ethernet:

Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3. Ver también Ethernet.

Fibra multimodo:

Fibra óptica que soporta la propagación de múltiples frecuencias de luz.

Fibra óptica:

Fibra basada en el vidrio, que sustituye a los clásicos cables de cobre y permite transmitir un gran volumen de información a alta velocidad y a gran distancia. La información no se transmite mediante impulsos eléctricos, sino que se modula en una onda electromagnética generada por un láser.

Filtro:

En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

Firewall:

Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Flooding:

Técnica de transmisión de tráfico utilizada por switches y puentes, en la cual el tráfico recibido por una interfaz se envía a todas las interfaces de ese dispositivo, salvo a la interfaz desde la cual se recibió originalmente la información.

Gb (*gigabit*)**:**

Aproximadamente 1.000.000.000 de bits.

Gbps (*gigabytes por segundo*)**:**

Medida de velocidad de transferencia

Host:

Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers. Ver también nodo.

Interfaz:

Conexión entre dos sistemas o dispositivos. 2. En terminología de enrutamiento, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI.

Internet:

La interconexión de redes más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad Internet. Internet evolucionó en parte de ARPANET.

IP (*Protocolo Internet*)**:**

Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo. Ver también IPv6.

IPv6 (*IP versión 6*)**:**

Reemplazo de la versión actual de IP (versión 4). IPv6 brinda soporte para identificación de flujo en el encabezado del paquete, que se puede usar para

identificar flujos. Anteriormente denominado IPng (IP de próxima generación).

ISL (Inter.-Switch Link):

Es un protocolo propietario de Cisco para interconectar multiples switches y mantener información VLAN, tales como tráfico entre switches. ISL proporciona capacidades VLAN en puertos FastEthernet en modo full o half duplex. Se ejecuta en puertos Trunk y es altamente recomendado. ISL funciona en la capa 2 del modelo OSI, encapsulando la trama con una cabecera y un CRC. Además es independiente del protocolo que se utilice en la capa superior.

ISO (*Organización Internacional para la Normalización*)**:**

Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking.

kb (*kilobit*)**:**

Aproximadamente 1.000 bits.

kB (*kilobyte*)**:**

Aproximadamente 1.000 bytes.

kbps (*kilobits por segundo*)**:**

Medida de velocidad de transferencia.

kBps (*kilobytes por segundo*)**:**

Medida de velocidad de transferencia.

LAN (*red de área local*)**:**

Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas. Comparar con MAN y WAN. Ver también VLAN.

Latencia:

Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

MAC (*Control de Acceso al Medio*)**:**

Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir. Ver también capa de enlace de datos y LLC.

Máscara de subred:

Máscara utilizada para extraer información de red y subred de la dirección IP.

Máscara wildcard:

Cantidad de 32 bits que se utiliza junto con una dirección IP para determinar qué bits en una dirección IP deben ser ignorados cuando se compara dicha dirección con otra dirección IP. Una máscara wildcard se especifica al configurar una ACL.

Mb (megabit):

Aproximadamente 1.000.000 de bits.

Memoria flash:

Almacenamiento no volátil que se puede borrar eléctricamente y reprogramar, de manera que las imágenes de software se pueden almacenar, iniciar y reescribir según sea necesario. La memoria flash fue desarrollada por Intel y se otorga bajo licencia a otras empresas de semiconductores.

MTU (*unidad máxima de transmisión*)**:**

Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

Multicast:

Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

NAT (*traducción de direcciones de red*)**:**

Mecanismo que reduce la necesidad de tener direcciones IP exclusivas globales. NAT permite que las organizaciones cuyas direcciones no son globalmente exclusivas se conecten a la Internet transformando esas direcciones en espacio de direccionamiento enrutable global. También denominado traductor de dirección de red.

NIC (*tarjeta de interfaz de red*)**:**

Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

NVRAM (*RAM no volátil*)**:**

Memoria RAM que conserva su contenido cuando se apaga una unidad.

PAP (*Protocolo de Autenticación de Contraseña*)**:**

Protocolo de autenticación que permite que los PPP iguales se autentiquen entre sí. El router remoto que intenta conectarse al router local debe enviar una petición de autenticación A diferencia de CHAP, PAP pasa la contraseña y el nombre de host o nombre de usuario sin cifrar. PAP no evita el acceso no autorizado, sino que identifica el extremo remoto, el router o el servidor de acceso y determina si a ese usuario se le permite el acceso. PAP es compatible sólo con las líneas PPP. Comparar con CHAP.

ping (*búsqueda de direcciones de internet*)**:**

Mensaje de eco ICMP y su respuesta. A menudo se usa en redes IP para probar el alcance de un dispositivo de red.

POST (*pruebas al inicio*)**:**

Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando se enciende.

PROM (*memoria programable de sólo lectura*)**:**

ROM que puede programarse utilizando equipo especial. Las PROM pueden ser programadas solamente una vez. Comparar con EPROM.

Puerto:

Interfaz en un dispositivo de internetwork (por ejemplo, un router). 2. Enchufe hembra en un panel de conmutación que acepta un enchufe macho del mismo

tamaño, como un jack RJ-45. En estos puertos se usan los cables de conmutación para interconectar computadores conectados al panel de conmutación. Esta interconexión permite que la LAN funcione. 3. En la terminología IP, un proceso de capa superior que recibe información de las capas inferiores. Los puertos tienen un número, y muchos de ellos están asociados a un proceso específico. Por ejemplo, SMTP está asociado con el puerto 25. Un número de puerto de este tipo se denomina dirección conocida. 4. Volver a escribir el software o el microcódigo para que se ejecute en una plataforma de hardware o en un entorno de software distintos de aquellos para los que fueron diseñados originalmente.

RARP (*Protocolo de Resolución Inversa de Dirección*)**:**

Protocolo en la pila TCP/ IP que brinda un método para encontrar direcciones IP con base en las direcciones MAC. Comparar con ARP.

Red:

Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Redundancia:

En interconexión (internetwork), duplicación de dispositivos, servicios o conexiones, de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla. 2. En telefonía, la porción de la información total contenida en un mensaje que se puede eliminar sin sufrir pérdidas de información o significado esencial.

Rendimiento:

Velocidad de la información que llega a, y posiblemente pase a través de, un punto determinado del sistema de red.

Resolución de direcciones:

En general, un método para resolver diferencias entre esquemas de direccionamiento del computador. La resolución de direcciones habitualmente especifica un método para asignar las direcciones de capa de red (Capa 3) a las direcciones de capa de enlace de datos (Capa 2).

Router:

Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

Segmento:

Sección de una red que está rodeada de puentes, routers o switches 2. En una LAN que usa topología de bus, un circuito eléctrico continúo que a menudo está conectado a otros segmentos similares a través de repetidores. 3. En la especificación TCP, una unidad única de información de capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Software Cisco IOS (*Sistema Operativo de Internetwork*)**:**

Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura CiscoFusion. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetwork, garantizando al mismo tiempo la compatibilidad con una amplia variedad de protocolos, medios, servicios y plataformas.

Spanning tree:

Subconjunto sin bucles de una topología de red de Capa 2 (conmutada).

Split horizon:

Función de IGRP destinada a evitar que los routers tomen rutas erróneas. El horizonte dividido evita que se produzcan bucles entre routers adyacentes y mantiene reducido el tamaño de los mensajes de actualización.

spoofing:

La acción de un paquete que ilegalmente dice provenir de una dirección desde la cual en realidad no se lo ha enviado. El spoofing está diseñado para contrarrestar los mecanismos de seguridad de la red, tales como los filtros y las listas de acceso.

Subinterfaz:

Una de una serie de interfaces virtuales en una sola interfaz física

Switch:

Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de

espera.

Los switches son más "inteligentes" que los "Hubs" y ofrecen un ancho de banda más dedicado para los usuarios o grupos de usuarios. Un switch envía los paquetes de datos solamente a la computadora correspondiente, con base en la información que cada paquete contiene. Para aislar la transmisión de una computadora a otra, los switches establecen una conexión temporal entre la fuente y el destino, y la conexión termina una vez que la conversación se termina.

TCP (*Protocolo de Control de Transmisión*)**:**

Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP (*Protocolo de Control de Transmisión /Protocolo Internet*)**:**

Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años '70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Telnet:

Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos y utilicen los recursos como si estuvieran conectados a un sistema local. Telnet se define en RFC 854.

Trama:

Agrupamiento lógico de información enviada como unidad de capa de enlace de datos a través de un medio de transmisión. A menudo se refiere al encabezado y a la información final, utilizadas para la sincronización y control de errores, que rodean

los datos del usuario contenidos en la unidad. Los términos datagrama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

UDP (*Protocolo de Datagrama de Usuario*)**:**

Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos. UDP se define en la RFC 768.

URL (*localizador de recursos uniforme*)**:**

Esquema de direccionamiento estandarizado para acceder a documentos de hipertexto y otros servicios utilizando un explorador de Web.

UTP (*par trenzado no blindado*)**:**

Medio de cable de cuatro pares que se emplea en varias redes. UTP no requiere el espacio fijo entre conexiones que es necesario para las conexiones de tipo coaxial. Existen 7 tipos de cableado UTP de uso común: cableado de Categoría 1, 2, 3, 4, 5, 5e y 6.

VLAN (*LAN virtual*)**:**

Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos. Debido a que las LAN virtuales están basadas en conexiones lógicas en lugar de físicas, son extremadamente flexibles.

VPN (*Red Privada Virtual*)**:**

Una Red Privada Virtual, o Virtual Private Network, VPN, permite establacer una conexión segura a través de una red pública, o Internet. Una VPN permite que el tráfico IP viaje suguro a través de una red pública TCP/IP al encriptar el tráfico desde una red hasta la otra. Una VPN usa tunneling para encriptar toda la información en el nivel IP.