UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Estudios Superiores Aragón

Propuesta de infraestructura tecnológica para dar salida a Internet a una aplicación PeopleSoft.

TRABAJO DE TITULACIÓN EN LA MODALIDAD DE SEMINARIOS Y CURSOS DE ACTUALIZACIÓN Y CAPACITACIÓN PROFESIONAL

Para obtener el título de

INGENIERA MECÁNICA ELECTRICISTA
ÁREA ELÉCTRICA Y ELECTRÓNICA

P R E S E N T A:

BRENDA PAULINA VILLALOBOS GONZÁLEZ

ASESORA: Ing. Blanca Estela Cruz Luévano.

NEZAHUALCÓYOTL, ESTADO DE MÉXICO 2012

Índice

Introducción.

Desde hace algunos años la industria de las telecomunicaciones se encuentra en su mejor desarrollo, nuevos sistemas de comunicaciones aparecen, exponiendo alternativas para mejorar la funcionalidad de los sistemas y prestación de servicios. Los avances tecnológicos en las Telecomunicaciones y la Informática han revolucionado la forma en que la información es procesada y enviada, actualmente ya no existe diferencia entre enviar voz, datos y video porque la infraestructura y estándares de comunicación actuales, permiten manejar elevados anchos de banda para la transmisión de datos.

Los proveedores de servicio y producto de Telecomunicaciones se enfrentan a una reñida lucha en donde, para ser competitivos, los recursos humanos que comercializan sus productos requieren demostrar un sólido conocimiento en las tecnologías y soluciones que pueden ofrecer. Las empresas requieren de recursos humanos altamente capacitados en tecnologías relevantes de las Telecomunicaciones, además que tengan habilidades en la toma de decisiones que involucren planeación, diseño, mantenimiento y operación de redes de comunicación

En México las telecomunicaciones han tenido un gran auge en los últimos 14 años, además de un acelerado crecimiento lo que ha generado una gran demanda de conocimiento. La Universidad Nacional Autónoma de México a través de la Facultad de Estudios Superiores Aragón da respuesta a los requerimientos de la sociedad ofreciendo la Licenciatura de Ingeniería Mecánica Eléctrica Electrónica en el área eléctrica – electrónica en la cual prepara profesionistas capaces de desarrollar sistemas electrónicos, manejo, implantación y administración de sistemas de telecomunicaciones, los egresados tienen conocimientos fundamentales de la teoría de las telecomunicaciones, además conocen algunas tecnologías aplicadas en este campo que les permiten analizar, diseñar, planear, organizar, producir, instalar y desarrollar, además de mantener en operación y administrar redes y sistemas de telecomunicaciones

Como complemento a lo anterior la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM, ha creado el Diplomado Integral de Telecomunicaciones dirigido a Directores, gerentes, jefes de departamento o ingenieros que estén involucrados en la toma de decisiones, planeación, diseño, operación y mantenimiento de proyectos de Telecomunicaciones.

El diplomado está dividido en 17 módulos, Introducción a las Telecomunicaciones, Regulación, normatividad y mercados de Telecomunicaciones, Medios de transmisión alámbricos, medios de transmisión inalámbricos, Redes de comunicación, tecnología de transporte de información, Interconexión y administración de redes de datos, Redes inalámbricas, Sistemas de comunicaciones de microondas, Sistemas de comunicación satelital, Redes de telefonía

inteligentes, Redes telefónicas celulares, Seguridad en redes de comunicación, Administración de redes, Diseño de un proyecto de telecomunicaciones, Administración de un proyecto de Telecomunicaciones.

Durante los primeros módulos del diplomado se analizó la historia, desarrollo, evolución de las telecomunicaciones, conceptos básicos, el funcionamiento de un sistema de comunicaciones, los principales instrumentos y organismos nacionales e internacionales normativos que facilitan la prestación de servicios y el comercio en los principales mercados de telecomunicaciones en México y el mundo.

Durante los módulos de medios de transmisión alámbricos y medios de transmisión inalámbricos, se expusieron parámetros, tipos, técnicas de instalación, configuración y normas aplicables a los medios empleados en las telecomunicaciones.

Los elementos de interconexión, funcionamiento del modelo OSI aplicado a una red, se detallo en el módulo de Redes de comunicación, mientras que el análisis del transporte de la información y protocolos de enrutamiento para estructura de redes se trataron en el módulo 6 y 7.

A partir del módulo 8 hasta el 13, fueron temas especializados por ejemplo las microondas, telefonía, redes satelitales, telefonía inteligente, cada uno de ellos tenía como objetivo que el integrante comprendiera los elementos y conceptos que integraban las diferentes tecnologías.

Para el presente trabajo se utilizó el conocimiento de los primeros 8 módulos y de los módulos 14 al 18, los cuales hacen referencia a la administración de redes, seguridad a las redes, diseño y administración de proyectos de telecomunicaciones.

Uno de los temas que se tratan en el diplomado es el de seguridad en las telecomunicaciones por ejemplo las intrusiones y ataques cuestan dinero a los negocios en términos de información robada, perdidas de productividad por servicios comprometidos y costes de recuperación de usuarios comprometidos. A pesar del interés que se pone en la seguridad de la red, las intrusiones se están volviendo más frecuentes y sofisticadas. Solamente la detección automatizada de las intrusiones y las soluciones preventivas pueden mitigar los ataques complejos con la velocidad que se requiere o prevenir daño real o costes desbocados. Por lo anterior, el propósito de este trabajo es proponer una infraestructura tecnológica para dar salida a la red pública a una aplicación PeopleSoft. Para la propuesta se tomará como ejemplo la empresa Nacional Monte de Piedad con su aplicación PeopleSoft.

PeopleSoft es un ERP (Enterprise Resource Planning) para uso de grandes y medianas organizaciones en todo el mundo. Estas organizaciones incluyen a las empresas financieras,

instituciones educativas, etc. PeopleSoft es una aplicación para gestionar las áreas funcionales como los clientes, el capital humano, la gestión financiera, contable y la gestión de cadenas de suministro, cada uno con una serie de características especificas de la industria.

La arquitectura de PeopleSoft ha ido evolucionando a lo largo de los años, actualmente es una aplicación desarrollada para gestionarse por navegadores Web, PeopleSoft la llama "Pure Internet Architecture". PeopleSoft es una cadena de tecnologías relacionadas que se extienden entre el usuario y la base de datos. Está conformada por un Servidor Web, Servidor de Aplicaciones y Servidor de Base de datos.

El modelo que se propone debe ser una estructura segura, con alta disponibilidad, y redundancia.

El diseño de la red de alta disponibilidad previene la pérdida financiera, previene la pérdida de productividad, reduce los costos de apoyo reactivo y mejora la satisfacción y fidelidad del cliente.

La alta disponibilidad se refiere a la capacidad de la red de recuperarse de todo tipo de fallos y al deseo de tener la red disponible todo el tiempo o lo más cercano posible de todo el tiempo. Los siguientes puntos muestran cómo se debería diseñar en muchas capas.

- Capa 1: Vínculos redundantes y el hardware proporciona caminos físicos alternativos a través de la red.
- Capa 2 y 3: Protocolos de caminos alternativos y convergencia rápida.
- Disponibilidad de aplicación: Los procesos de las aplicaciones del servidor y el cliente deben soportar fallos para tener disponibilidad máxima.

El almacenamiento en caché de contenido dinámico entrega de manera instantánea la información solicitada con mayor frecuencia directamente desde el equipo de almacenamiento para mejorar aún más la experiencia del usuario. Existen equipos como NetScaler que responde en forma dinámica a los cambios en las cargas de trabajo. NetScaler proporciona detección y respuesta de sobrecarga para optimizar el uso de los recursos del servidor aún con tráfico impredecible. El Balanceo de carga global de servidores (GSLB) garantiza que las aplicaciones estén disponibles para los usuarios en todo el mundo y constituye un elemento clave para las estrategias de recuperación ante desastres

La red de una empresa es como cualquier otro activo, tiene valor y afecta al éxito y los ingresos de la misma. En los equipos de cómputo se almacena la información de la empresa y se debe de proteger. La seguridad de Internet es gran preocupación debido a la exposición de los datos que viajan a través de redes inseguras vulnerables a cualquiera que pueda leer, alterar o

falsificar la información que contiene. Usando herramientas de acceso como los protocolos de análisis, casi cualquier persona puede leer paquetes y acceder a información clasificada. Personas o grupos hostiles, pueden también intentar forzar los paquetes, impedir los envíos o evitar las comunicaciones en red. Existen muchas herramientas para poder proteger la información.

- Encriptación.
- Firewalls.
- Sistemas de Prevención de Intrusos.
- Políticas de seguridad.

Con la difusión del uso de Internet la posibilidad de conexión IP es accesible a los hogares y lugares públicos, como aeropuertos y cafeterías. Los proveedores de servicio ven más efectivo a nivel de costo ofrecer WAN basadas en IP antes que circuitos exclusivos. Las empresas tienen que ofrecer extensos servicios de Internet a sus empleados, clientes y proveedores para ser competitivas.

Las redes privadas virtuales (VPN) permiten a las empresas extender su red local. La VPN es un conjunto de soluciones y tecnologías diseñadas para hacer seguras (encriptadas) las conexiones sitio a sitio y de acceso remoto que usan redes públicas. Estas conexiones proporcionan alternativas de bajo coste a las redes WAN exclusivas y permiten a los teletrabajadores conectarse a la red corporativa a través del cable de televisión, DSL o sistemas de llamada. Las conexiones VPN pueden instalarse rápidamente usando infraestructuras existentes y proporcionan una alternativa excelente a redes privadas de uso exclusivo como Transferencia de Tramas o ATM.

Los beneficios de las VPN son:

- **Bajos costos**: Las VPN usan las redes públicas de tipo IP, que son bajas en costos, para conectar a los usuarios de oficinas lejanas con el sitio principal de la corporación, eliminando costos dedicados a los vínculos WAN.

- **Seguridad**: Las VPN proporcionan un alto nivel de seguridad usando encriptación avanzada y protocolos de verificación.

- **Posibilidad de crecimiento a escala**: Las VPN pueden instalarse fácilmente sobre las infraestructuras de red existentes, permitiendo a las corporaciones añadir capacidad a extenderse sin añadir infraestructura significativa.

- **Compatibilidad con las redes de banda ancha**: Las VPN permiten a los trabajadores en movimiento, teletrabajadores y las instalaciones temporales aprovecharse de la ventaja de

la conexión de alta velocidad por banda ancha, como DSL y cable de televisión para la conexión con la red.

- **Facilidad de acceso:** El acceso a la red se puede conseguir desde cualquier lugar del mundo con puntos de acceso a Internet (POP).

Las redes privadas virtuales (VPN) basadas en el estándar IPSec se están convirtiendo en una de las tecnologías líderes, sin embargo existen nuevas alternativas basadas en SSL las cuales son más sencillas a la hora de crear conexiones seguras por Internet. SSL está presente en la gran mayoría de navegadores Web, esto permite ahorrar tiempo a los usuarios en la configuración de software, porque no se requiere en la máquina remota.

La mayor ventaja de SSL VPN es que está basado en Web y no requiere que los administradores instalen previamente ningún cliente "pesado" en cada estación de trabajo remota. Esto aumenta significativamente la flexibilidad y ofrece un nivel de acceso mucho más amplio. Con un explorador Web estándar, los usuarios remotos pueden activar un portal Web personalizado para acceder a correos electrónicos, archivos aplicaciones y sitios Web internos (intranets). No obstante, existen aplicaciones donde un cliente pesado podría conllevar ventajas. La tecnología IPSec podría utilizarse especialmente en áreas donde el administrador de TI controla y gestiona muy de cerca solo una cantidad pequeña de estaciones de trabajo remotas. La ventaja del sistema VPN de cliente pesado es que los administradores pueden brindar un mayor nivel de acceso a los usuarios

Parte importante de la propuesta de infraestructura es la redundancia que se refleja de tal forma que si un equipo se vuelve no operativo, la red automáticamente se redireccionará a otro equipo redundante para no perder disponibilidad. Duplicar los equipos también permite compartir la carga cuando los dos están disponibles.

El monitoreo de los servidores y los dispositivos de la red permiten a los administradores de ésta descubrir rápidamente problemas o paros, lo que contribuye a minimizar el tiempo que la red está fuera de servicio. El objetivo es descubrir los problemas antes de que afecten a la capacidad de la red de pasar el tráfico. El software de gestión de red se usa normalmente para el monitoreo de la red.

1. Justificación del problema.

Internet es un aspecto base de negocio para casi todas las compañías. Sin embargo, conforme mas equipos se conectan a redes públicas y los empleados de empresas se conectan a internet, se incrementa la probabilidad de ataques maliciosos. Los ataques a las redes se dan por una gran variedad de razones, extorsión, fraude, espionaje o curiosidad. El modo más seguro para no sufrir ataques es no conectarse a la red, sin embargo ésta no es la solución práctica y competitiva. El problema a resolver, consiste en tener una presencia externa y estar relativamente seguros frente a los ataques.

La respuesta podría ser colocar un sistema de firewall[1], los cuales mantienen a las redes privadas y corporativas seguras de los ataques revisando los paquetes de perfiles conocidos y actuando como un aislante entre el usuario y el mundo exterior. Un firewall o cortafuegos proporciona una barrera para el tráfico sin embargo algunas partes del tráfico podrían parecer legitimas (ser de hecho legitimas) pero al mismo tiempo pueden estar llevando virus peligrosos o programas que ataquen, por lo que es importante elegir otras medidas adicionales para detectar pautas de tráfico que un cortafuegos no puede detectar. Los sistemas de detección de intrusos proporcionan esta posibilidad.

Los IDS analizan datos en tiempo real para detectar, registrar e impedir errores y ataques. Existen IPS (Sistemas de Prevención de Intrusos), es similar a IDS, ambos requieren de una base de datos de señales de ataques conocidos para ser programados en el dispositivo de red de IDS o IPS,

Con el auge de Internet, además de la seguridad en las redes existen otros problemas como los siguientes:

- No ser capaz de acceder a un sitio Web, porque los servidores Web no están en condiciones de manejar una enorme cantidad de usuarios conectados simultáneamente.
- Una empresa internacional intentando tratar de localizar sus páginas Web para cada uno de los países.

[1] El término "firewall / fireblock" significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. El cortafuego está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Un firewall puede ser implementado en hardware o software.

- El almacenamiento en caché de una red proporciona ubicar contenido de la red más cerca de los solicitantes. El almacenamiento en caché de direcciones soluciona los problemas anteriores al acelerar la entrega de contenido y optimizar la utilización del enlace WAN. Es decir se mueve el contenido más cerca del usuario.

- Hoy en día las compañías tienen que ofrecer extensos servicios de Internet a sus empleados, socios y clientes para ser competitivos. Dada la confluencia del IP público y las redes corporativas, extender estás más allá del campo es más práctico y barato que antes. Las VPN permiten a los teletrabajadores, clientes, etc., a la red corporativa a través del cable de televisión, DSL o sistema de llamadas.

Ante éste escenario el Nacional Monte de Piedad desea incorporar las nuevas tecnologías en materia de telecomunicaciones con el fin de mejorar sus procesos y ofrecer a sus colaboradores un mecanismo más eficiente y seguro de comunicación con sus sistemas a través de Internet. Por ello se diseñará un mecanismo que permita satisfacer de manera óptima esta necesidad.

1.1 Objetivo.

Dar acceso remoto a las aplicaciones PeopleSoft de Nacional Monte de Piedad.

1.2 Objetivos Específicos.

A partir del objetivo General del proyecto, se han identificado los siguientes objetivos específicos a cumplir durante el proyecto:

- Diseñar la infraestructura tecnología para dar acceso remoto a las aplicaciones PeopleSoft.
- Permitir el acceso a las aplicaciones únicamente a los usuarios autorizados.
- Proporcionar alta disponibilidad al sistema.
- Proteger la información.

1.3 Planeación.

En esta etapa se determina las actividades para integrar una propuesta de solución a las necesidades expuestas por Nacional Monte de Piedad, de tal manera que se pueda tener una visión general de todos los elementos requeridos hasta su ejecución exitosa. A continuación se listan dichas actividades:

1. Entrevista con usuario clave para revisar requerimientos del proyecto.
2. Desarrollar criterios de aceptación para que el usuario clave los valide y de su autorización.
3. Elaborar una propuesta de solución que cubran sus requerimientos.

    3.1 Definir arquitectura.

    3.2 Determinar los equipos de comunicación requeridos.

    3.3 Obtener cotizaciones de los equipos y enlaces.

    3.4 Revisión y Evaluación del costo-beneficio.

    3.5 Selección de equipos a utilizar con base en la evaluación.

1.3.1 Alcance general.

Con esta propuesta el Nacional Monte de Piedad podrá ofrecer una herramienta que permita a sus usuarios (sucursales, proveedores, etc.) acceder de manera remota a servicios que les ofrece la aplicación PeopleSoft. Un ejemplo de esto es un fácil crecimiento del NMP al poder crear nuevas sucursales sin tener que implementar soluciones particulares en cada una de ellas.

El alcance del proyecto implica la integración de nuevos equipos de comunicación y agregar mecanismos de seguridad y redundancia que no afecten el funcionamiento actual de las aplicaciones PeopleSoft.

1.4 Objetivo y Actividad principal del NMP.

El Nacional Monte de Piedad es una Institución de Asistencia Privada con personalidad jurídica propia, sin fines de lucro, que tiene como tarea realizar labores de carácter asistencial y humanitario.

Dentro de sus objetivos están, por un lado, el brindar liquidez inmediata mediante el otorgamiento de préstamos prendarios con la tasa más baja de interés y el propósito de ayudar a todos aquellos que tengan necesidades económicas urgentes.

Por el otro lado, destinar el remanente de la operación prendaria a proyectos asistenciales mediante otras Instituciones de Asistencia Privada (IAP´s), que ofrecen sus servicios a niños, jóvenes, adultos mayores, enfermos carentes de recursos económicos en áreas de protección, salud, trabajo y educación, entre muchos otros.

El NMP es una Institución de Asistencia Privada que conserva la esencia altruista de su origen teniendo como objeto social:

- Celebrar contratos de préstamo prendario
- Realizar obras asistenciales
- Ayudar a los pequeños artesanos a vender sus artículos

1.5 Misión de NMP.

Maximizar el beneficio para la sociedad mexicana generado a través de la operación prendaria, de otros servicios financieros y acciones asistenciales de alto impacto.

1.6 Visión de NMP.

Ser la Institución privada y altruista líder de los sectores prendario y asistencial, con capacidad de transformar estos sectores y fomentar la viabilidad del sector asistencial, al ofrecer la mejor combinación de productos, calidad y servicio, con una gestión eficiente y rentable.

2. Marco teórico.

Para poder tener una mejor comprensión de la solución a implementar, es importante tener en cuenta los elementos teóricos que la fundamentan. Estos temas son la base con lo que fueron construidos muchos de los componentes que forman parte de la propuesta presentada y/o que permiten la integración entre sí.

2.1 Modelo y arquitectura OSI.

El modelo OSI está conformado por 7 capas que describen las funciones de las computadoras para comunicarse entre sí. La International Organization for Standardization (ISO) publicó este modelo en 1984 para describir una aproximación estratificada con el objetivo de proporcionar servicios de redes usando un sistema de protocolos llamados OSI. La base de la definición consiste en que cada una de las capas tiene una función particular que desarrollar, y cada una de las capas solo necesita comunicarse con las capas inmediatamente por encima y por debajo de ella. Una de las mayores ventajas de este sistema de capas que se comunican solo con las adyacentes permite sistemas de comunicaciones que se pueden adaptar y modificar fácilmente conforme las tecnologías avanzan. Por ejemplo, conforme las nuevas tecnologías se introducen en un nivel más bajo, como el nivel 1, los niveles superiores no se tienen que modificar. Al contrario, las adaptaciones en el nivel 2 permiten a los niveles por encima usar las tecnologías de forma transparente.

2.1.1 Sistemas Abiertos vs Sistemas con propietario.

A pesar de que el modelo de código abierto es bien conocido hoy, cuando el modelo OSI estaba siendo desarrollado, había una pelea en marcha para equilibrar la apertura técnica con la ventaja competitiva. En aquel tiempo cada vendedor veía como ventaja desarrollar tecnología que no se pudiera copiar y únicamente equipos de la misma compañía podían interactuar entre sí.

El sistema de propietarios puede complicar el trabajo de un administrador de redes, cerrándole en un solo vendedor, reduciendo la competitividad y permitiendo al vendedor cargar precios más altos. Si el vendedor se sale del mercado, ya nadie queda para dar soporte y mantenimiento a los equipos

La alternativa es un enfoque de sistemas abiertos en el cual los cuerpos de normas como el Institute of Electrical and Electronic Engineers (IEEE) o el ISO definen las tecnologías.

2.1.2 Siete capas.

La siguiente lista son las 7 capas del modelo OSI comenzando con la más baja:

- **Capa 1. Física:** La capa física es responsable de convertir una trama (la salida de la capa 2) en señales eléctricas que sean transmitidas por la red. La red física real puede ser un cableado de cobre, fibra óptica, señales de radio o cualquier otro medio que pueda transmitir señales. Esta capa proporciona un método para que el aparato de recepción valide que los datos no se han estropeado durante la transmisión.

- **Capa 2. Enlace de datos:** La capa de enlace de datos es responsable de establecer, mantener y controlar la sesión de comunicación entre dos equipos diferentes. Para redes de computadoras, la capa de enlace de datos añade un cabezal que identifica el protocolo concreto de la capa 3 que se usa y las direcciones de hardware fuente y destino (también conocidas como direcciones Media Access Control MAC). En este punto el paquete (la salida de la capa 3) se procesa con éxito en una trama de la capa 2 y está listo para entrar a la red. El encendido de Ethernet y punteando operan este nivel.

- **Capa 3. Red:** La capa de red es donde la mayoría de los protocolos de comunicación funcionan, en dependencia de las capas 2 y 1 para enviar y recibir mensajes de otras computadoras o dispositivos de redes. La capa de red añade otro cabezal delante del paquete, que identifica las direcciones de la IP de la fuente y destino del emisor y receptor del paquete. El proceso de envío de paquetes IP se da a este nivel. Proporciona conectividad y selección de ruta entre dos sistemas finales.

- **Capa 4. Transporte:** La capa de transporte es responsable de tomar el grupo de datos desde la aplicación y prepararlo para su navegación en la red. Preparar los datos para el transporte implica cortar todos en piezas más pequeñas y añadirles un cabezal que identifica la aplicación que se está enviando y recibiendo (en ocasiones son conocidos también como números de puerto). Detección y recuperación de fallas, controla el flujo de información.

  Por ejemplo en el Protocolo de Transferencia de Hipertextos (HTTP) el tráfico WEB usa el puerto 80, y el tráfico FTP usa el 21. Cada porción de datos y su cabezal asociado recibe el nombre de paquete.

- **Capa 5 Sesión:** La capa de sesión controla las conexiones entre usuarios. Si la aplicación de un anfitrión necesita hablar con la aplicación de otro, el nivel de sesión establece la conexión y asegura que los recursos están disponibles para permitir la conexión. La gente de la red suele referirse a las capas 5 a 7 como los niveles de aplicación.

- **Capa 6. Presentación:** La capa de presentación proporciona servicios de formateo para el nivel de aplicación. Garantiza que los datos sean legibles para el sistema receptor. Por

ejemplo, la compresión de archivos se produce a este nivel, y crea una conversión de formatos.

- **Capa 7. Aplicación:** La capa de aplicación proporciona servicios de redes a un usuario o aplicación. Por ejemplo, cuando se envía un e-mail, la capa de aplicación empieza el proceso de tomar los datos del programa del e-mail y lo prepara para ponerlo en la red, procesando desde la capa 1 a la 6.

  El modelo OSI se considera todavía la base de toda comunicación de redes.

  El modelo OSI es un marco conceptual que define las funciones y secuencias de las redes. El marco simplifica las interacciones complejas de redes convirtiéndolas en elementos modulares simples. Esta aproximación de marcos abiertos permite a muchos desarrolladores independientes trabajar en funciones separadas de red que pueden comunicarse en modo "plug-and-play".

El modelo OSI actúa como una línea guía para crear e implementar sistemas de normas de redes, diseños y escenarios de Internet. Las ventajas de usar el modelo OSI son las siguientes;

- Rompe aspectos interrelacionados de redes en aspectos menos complejos.
- Permite a las compañías e ingenieros individuales especializar diseños y esfuerzos de desarrollo en funciones modulares.
- Proporciona interfaces estándar para compatibilidad "plug-and-play" integrando distintos vendedores.
- Separa diferentes capas de la red para proporcionar una adopción más fácil de nuevas tecnologías dentro de cada capa.

Las cuatro capas más bajas (las capas de flujo de datos) definen los protocolos de conexión y los métodos para intercambiar datos.

Las tres capas superiores (las capas de aplicación) definen el modo en que las aplicaciones se comunican entre sí y con los usuarios dentro de los dispositivos finales de estación.

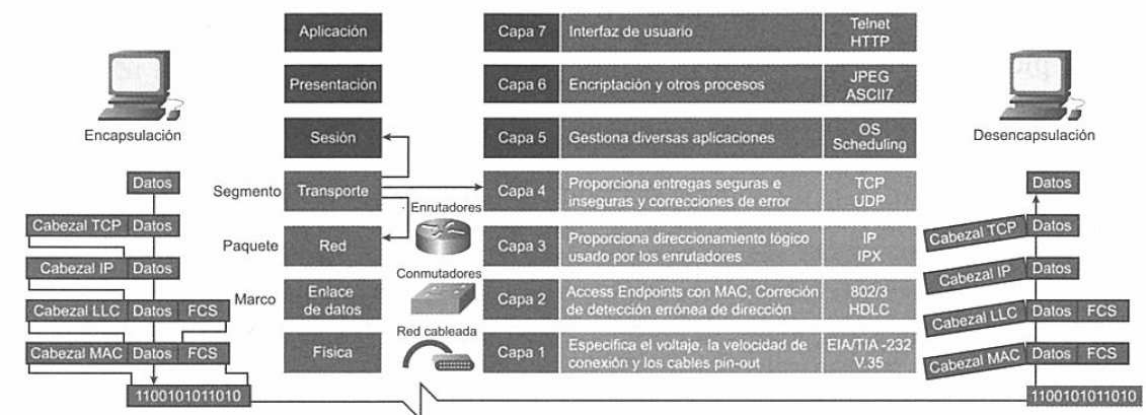


Figura 2.1 Relación entre capas.

2.1.3 Comunicación entre capas.

Cada capa del modelo OSI usa su propio protocolo para comunicarse con la capa paralela en el dispositivo destino. El modelo OSI especifica como cada capa se comunica con las capas superiores e inferiores, permitiendo a los desarrolladores enfocarse en las capas específicas que trabajarán con las capas adyacentes de cualquier otro desarrollador. La información es intercambiada entre capas usando PDU (Unidades de Protocolos de Datos). Las PDU incluyen información de control (en la forma de cabezales y registros) y datos de usuarios. Las PDU incluyen tipos diferentes de información conforme se sube o bajan las capas (conocidas como pila). Para aclarar donde está el PDU dentro de la pila, se le da nombre a cada una de las capas inferiores.

Un PDU es un segmento (capa 4) que incluye toda la información de la aplicación de la capa. Un paquete (capa 3) incluye información de control de la capa de red, además de los datos y la información de control contenida en la capa de transporte.

De forma similar, una trama (capa 2) es un PDU que incluye la información de control de la capa de enlace de datos, además de los datos e información de control de la capa superior. Finalmente los PDU de la capa física (capa 1) reciben el nombre de bits.

2.1.4 Encapsulación.

El proceso de transportar datos hacia abajo en la pila usando PDU se llama encapsulación. La encapsulación trabaja así: cuando una capa recibe un PDU de la capa superior, encapsula el PDU con un cabezal y un registro, y entonces pasa el PDU hacia abajo a la siguiente capa. La información de control que se añade al PDU se lee por la capa similar en el dispositivo remoto.

2.1.5 Desencapsulación.

La Desencapsulación es lo contrario a la encapsulación. Es el proceso de pasar la información hacia arriba en la pila. Cuando una capa recibe un PDU de la capa anterior hace lo siguiente:

1. Lee la información de control proporcionada por el dispositivo fuente paralelo.
2. La capa desmonta la información de control (cabezal) desde la trama.
3. Procesa los datos (normalmente pasándolos hacia arriba de la pila).

2.2 TCP/IP.

Los protocolos de Internet resumen los protocolos de redes de datos sin propietarios más populares en el mundo. Los protocolos de Internet son protocolos de comunicación usados por los dispositivos electrónicos para hablar entre sí. Inicialmente las computadoras eran los clientes primarios de los protocolos de internet pero hoy en día son muchos los dispositivos que se pueden conectar a través de las redes, por ejemplo impresoras, celulares, equipos mp3, hasta máquinas expendedoras, lavaplatos y automóviles.

Los dos protocolos más conocidos son el Protocolo de Control de Transmisiones (Transmission Control Protocol, TCP) y el Protocolo de Internet (IP).

Desde que IP se convirtió en el protocolo más importante de Internet, sirviendo como base para la World Wide Web (WWW) y de Internet en general. Los protocolos de Internet se discuten y adoptan en el dominio público. Los boletines técnicos llamados Documentos de Requerimientos y Comentarios (Requests For Comments, RFC), proponía protocolos y prácticas. Estos documentos se revisaban, editaban, publicaban y analizaban para ser aceptados por la comunidad de Internet (lo que llevaba años).

El protocolo base de Internet también resume los protocolos e aplicación incluyendo definiciones para lo siguiente:

- Correo electrónico
- Telnet
- Transferencia de archivos
- HTTP

IP se considera un protocolo de capa 3 de acuerdo al modelo OSI y el TCP es un protocolo de capa 4.

TCP es un protocolo fiable orientado a la conexión que divide los mensajes en segmentos y los reagrupa en la estación destino (además reenvía paquetes no recibidos en el destino. El TCP también proporciona circuitos virtuales entre aplicaciones-

Un protocolo orientado a conexión, la establece, la mantiene durante una transmisión. El protocolo debe establecer la conexión antes de enviar los datos. En cuanto la transferencia de datos se completa la sesión cambia de sentido.

UDP es un protocolo alternativo a TCP que también trabaja en capa 4. El UDP es un protocolo considerado como no fiable y no orientado a la conexión. No fiable indica en este contexto que el protocolo no garantiza que cada paquete llegue a su destino. UDP se usa para aplicaciones que proporcionan su propio proceso de recuperación de errores o cuando la retransmisión no tiene sentido. UDP es simple y eficiente creando una buena relación entre confianza y velocidad.

Detrás de cada sitio Web, Localizador Universal de Recursos (URL) y ordenador u otro dispositivo conectado a Internet, hay un número que solo identifica a ese dispositivo. Este identificador único se llama dirección.

2.2.1 Diagramas de datos TCP/IP.

La información TCP/IP se envía por diagramas de datos. Un mensaje simple se puede dividir en series de diagramas de datos que se deben reagrupar en su destino. Se asocian tres niveles con el protocolo de bloque TCP/IP:

- **Capa de agrupación**: Este nivel especifica los protocolos para correo electrónico, transferencia de archivos, inicio de sesión remoto y otras aplicaciones. La gestión de redes también está soportada.

- **Capa de transporte**: Este nivel permite aplicaciones múltiples de nivel superior para usar la misma corriente de datos. Los protocolos TCP y UDP proporcionan control de flujo y fiabilidad

- **Capa de red**: Varios protocolos funcionan en el nivel de red incluyendo IP, ICMP, ARP y RARP.

Los usuarios de TCP/IP usan el Protocolo de Control de Mensajes en Internet (ICMP) para llevar el mensaje de error y controlar mensajes con diagramas de datos IP.

El Protocolo de Definición de Direcciones (ARP) permite la comunicación de un medio con acceso múltiple como Ethernet convirtiendo las direcciones IP conocidas en direcciones MAC.

El Protocolo Reverso de Definición de Direcciones (RARP) se usa para convertir una dirección MAC conocida en una dirección IP.

2.2.2 Como se establecen las conexiones TCP.

La estación final intercambia bits que reciben el nombre SYN (por sincronizada) y los Números de Secuencia Inicial (ISN) para sincronizar durante el establecimiento de la conexión. El TCP/IP utiliza lo que se conoce como el "apretón de manos a tres bandas" para establecer las conexiones.

Para sincronizar la conexión a cada lado envía sus propios números de secuencia inicial y espera recibir una confirmación en acuse de recibo (ACK) del otro lado. La siguiente imagen muestra un ejemplo:

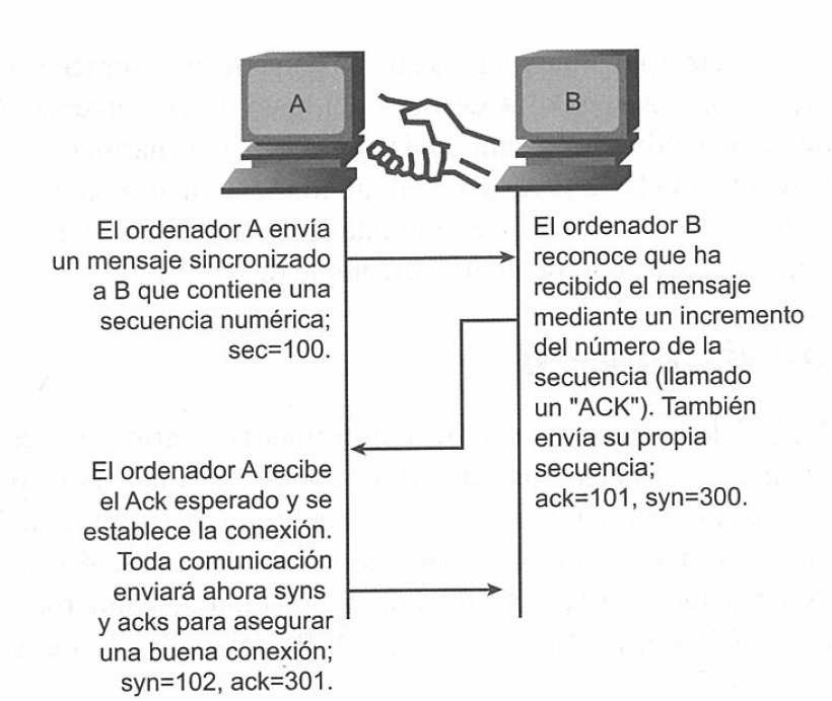


Figura 2.2 Ejemplificación de conexión TCP

Cada dispositivo de la red tiene 2 direcciones.

1. **Dirección MAC.** Es un número de identidad colocado por el fabricante (como un número de serie) que es permanente y único para cada dispositivo de red en la tierra. No existen dos dispositivos con el mismo número.

2. **Dirección IP.** Esta es la dirección que mas importa en las redes básicas. A diferencia de la dirección MAC, la dirección IP es de cualquier dispositivo es temporal y se puede cambiar. Solo se necesita ser única dentro de la red.

2.2.3 Historia de TCP/IP.

En la siguiente figura se muestra la historia de TCP/IP.

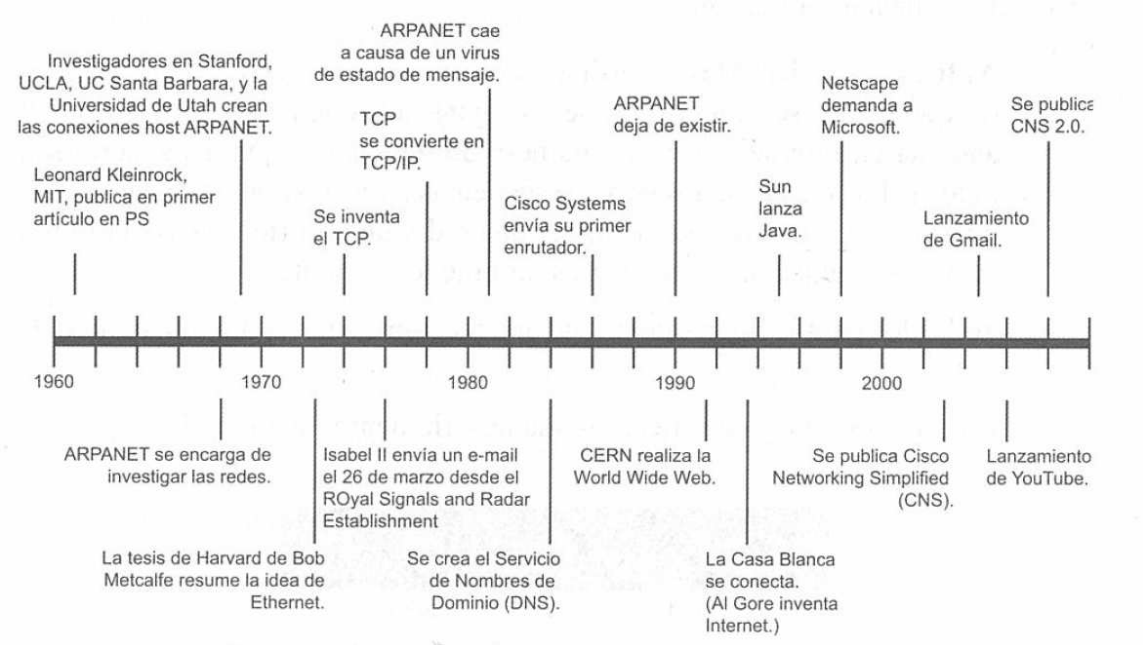


Figura 2.3 Historia de TCP/IP

2.3 Aplicaciones de Internet.

Internet es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP. Tuvo sus orígenes en 1969, cuando una agencia del Departamento de Defensa de los Estados Unidos comenzó a buscar alternativas ante una eventual guerra atómica que pudiera incomunicar a las personas. Tres años más tarde se realizó la primera demostración pública del sistema ideado, gracias a que

tres universidades de California y una de Utah lograron establecer una conexión conocida como ARPANET (Advanced Research Projects Agency Network).

Para que las redes puedan comunicarse entre ellas a través de internet se requiere de protocolos de comunicación, los cuales son reglas y normas que definen de qué forma se realizan las conexiones de tal manera que se puedan ofrecer servicios de consultas de páginas web, correo electrónico, transferencia de archivos, entre otros servicios los cuales pueden ser tan personalizados según las necesidades de los usuarios o las mismas empresas que lo requieran.

2.3.1 Internet y sus aplicaciones.

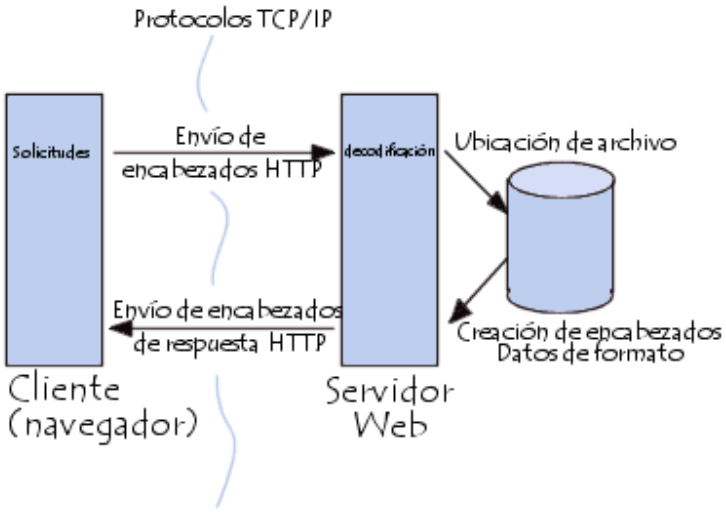
Lo que hacer a Internet útil e interesante para el usuario medio no es la red, sino más bien las aplicaciones que funcionan en ella. Las aplicaciones más comunes de Internet en nuestros días son el correo, los buscadores de Internet y las redes sociales.

2.3.2 HTTP y HTML sus usos y funciones.

Desde 1990, el protocolo HTTP (Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet, trabaja en la capa 7 en el modelo OSI y define las reglas para transferir archivos de información y multimedia.

El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML) entre un navegador (el cliente) y un servidor web (denominado, entre otros, httpd en equipos UNIX) localizado mediante una cadena de caracteres denominada dirección URL, es decir cuando un cliente se conecta con el servidor Web tecleando una dirección URL en el explorador o haciendo click en un hipervínculo, el sistema genera un mensaje de petición HTTP y lo transmite al servidor. Éste es un proceso de nivel de aplicación, pero para que esto pueda suceder, hay que establecer antes la comunicación a niveles más bajos.

- El navegador realiza una solicitud HTTP
- El servidor procesa la solicitud y después envía una respuesta HTTP.



HTML (Lenguaje de marcas de hipertexto) es el lenguaje de la Web, pero lo cierto es que tiene muy poco que ver con las funciones de los servidores Web. Los servidores Web son programas que entregan los archivos pedidos a los clientes. El hecho de que la mayoría de estos archivos contengan código HTML es indiferente, porque el servidor no los lee. Sólo afectan a las funciones del servidor cuando el cliente analiza el código HTML y pide archivos adicionales al servidor si son necesarios para que el explorador muestre la página Web, como archivos de imagen. Sin embargo, aun en este caso, el archivo de imagen pedido es sólo una petición adicional al servidor.

2.4 Dispositivos de interconexión.

Las LAN[2] se diseñaron originalmente para funcionar solamente con un número relativamente pequeño de computadoras –30 para redes Thin Ethernet y 100 para Thick Ethernet--, pero las necesidades de las empresas sobrepasaron rápidamente estas limitaciones. Para dar servicio a grandes instalaciones, los ingenieros desarrollaron productos que permitían a los administradores conectar dos o más LAN, formando lo que se conoce como una interconexión de redes, que es esencialmente una red de redes que posibilita a las computadoras de una red comunicarse con las de otra.

[2] Una LAN o un segmento de red es un grupo de computadoras que comparten un cable de red de modo que un mensaje de multidifusión emitido por un sistema llega a todos los demás, incluso si ese segmento está compuesto en realidad por muchos trozos de cable.

Se pueden conectar las LAN individuales entre sí usando diferentes tipos de dispositivos. Algunos de ellos simplemente extienden la LAN, mientras que otros crean una interconexión de redes. Estos dispositivos se explican en los siguientes subtemas.

2.4.1 NIC, Tarjetas de Red

Network Interface Card es el dispositivo que permite dar salida a la red a los dispositivos. Hay diversos tipos de adaptadores de red en función del tipo de cableado o arquitectura que se utilice en la red.

Las características de la tarjeta de red:

- Trabaja en la capa 2 de OSI
- Conecta al host con la red
- Tienen una dirección física única.

Figura 2.4 Tarjetas de Red.

2.4.2 Segmentos de Ethernet[3]

Un segmento es la forma más simple de red, en la cual todos los dispositivos están conectados directamente (figura 2.5). En este tipo de arreglo si uno de los dispositivos está conectado, o se añade otro, el segmento se deshabilita.

[3] Es el protocolo del nivel de enlace de datos utilizados por la mayor parte de las redes de área local que operan en la actualidad

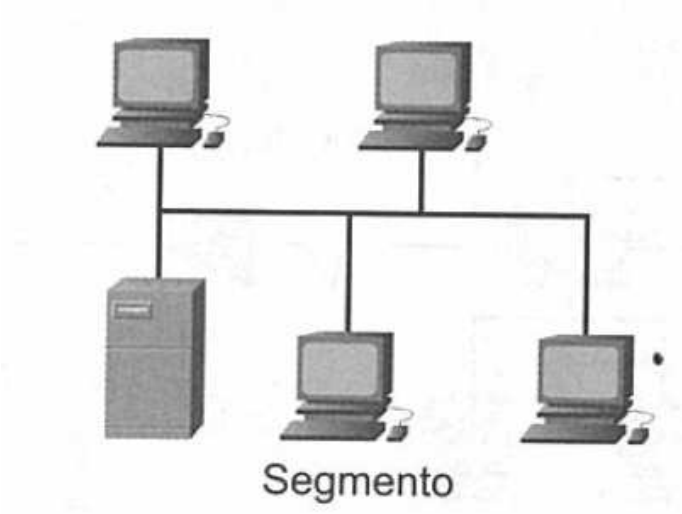


Figura 2.5 Segmento

2.4.3 Repetidores

Los repetidores simplemente extienden la distancia de transmisión de un segmento de Ethernet. (Figura 2.7)

- Se limita simplemente en regenerar la señal, para ampliar el rango de distancia de alcance.
- Se compone de 1 puerto de entrada y 1 de salida.
- Se define en la capa 1 de OSI
- No entiende de formatos, copia cualquier señal eléctrica (ruido e interferencias también)

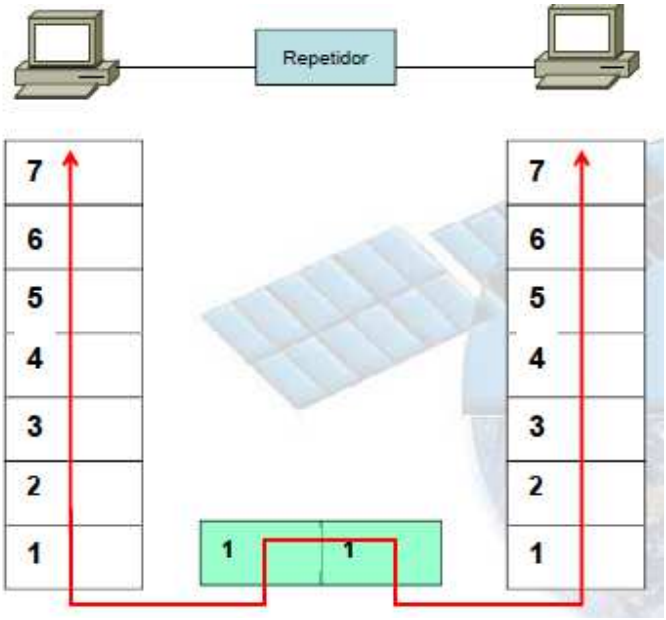


Figura 2.6 Conexión de un repetidor, capa en la que trabajan.

2.4.4 Concentradores

Los concentradores permiten añadir y quitar dispositivos sin desconectar la red, pero no crean dominios de colisión adicionales.

- Es un repetidor multipuerto.
- Crea un punto central de interconexión.
- Propaga la señal que recibe en un puerto a todos los demás.
- Extienden el dominio de colisión.
- Dispositivo que trabaja en la capa 1 de OSI.

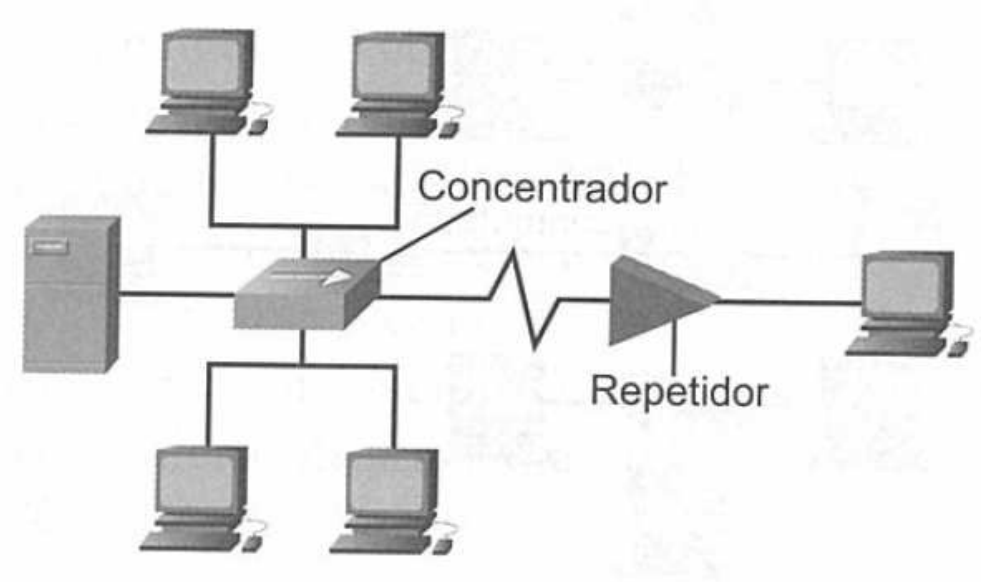


Figura 2.7 Conexión de concentrador y repetidor.

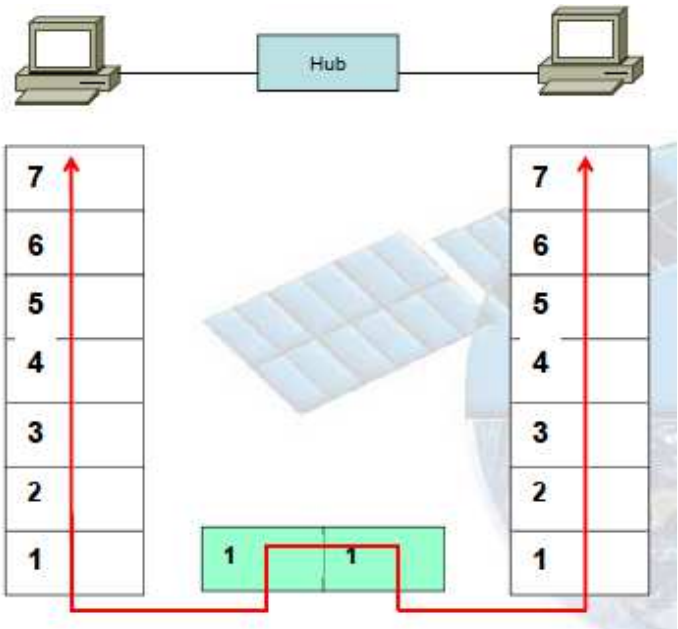


Figura 2.8 Conexión de un hub, capa en la que trabajan.

2.4.5 Puentes

Los puentes son dispositivos sencillos de capa 2 que crean nuevos segmentos, resultando menos colisiones (figura 2.9). Los puentes tienen que aprender las direcciones de los ordenadores de cada segmento para evitar dirigir el tráfico hacia el puerto erróneo. A diferencia de los concentradores, que son realmente utilizados por redes con un número pequeño de estaciones finales (de 4 a 8), los puentes pueden manejar redes mucho mayores con docenas de estaciones finales.

Características de los Puentes (bridges):

- Proporcionan las conexiones entre LAN.
- Dispositivo que trabaja en la capa 2 de OSI, generalmente en la subcapa MAC.
- Divide una red LAN en segmentos más pequeños.
- Verifican los datos para determinar si les corresponde o no cruzar el bridge, es decir, examina las direcciones origen y destino.
- Si las dos direcciones pertenecen a diferentes segmentos, se transfieren las tramas (forwarding, reenvío).
- Si las direcciones pertenecen al mismo segmento, se ignora y descarta el reenvío (filtering, filtrado).
- Si el bridge desconoce la dirección destino, envía la trama a todos los segmentos excepto aquel en el cual se recibió (flooding, inundación Un bridge puede mejorar el rendimiento de la red de manera notoria, si se ubica de forma estratégica.
- Para evitar bucles en redes complejas, en las topologías Ethernet (IEEE 802.3) utiliza el algoritmo: Transparent Spanning Tree.

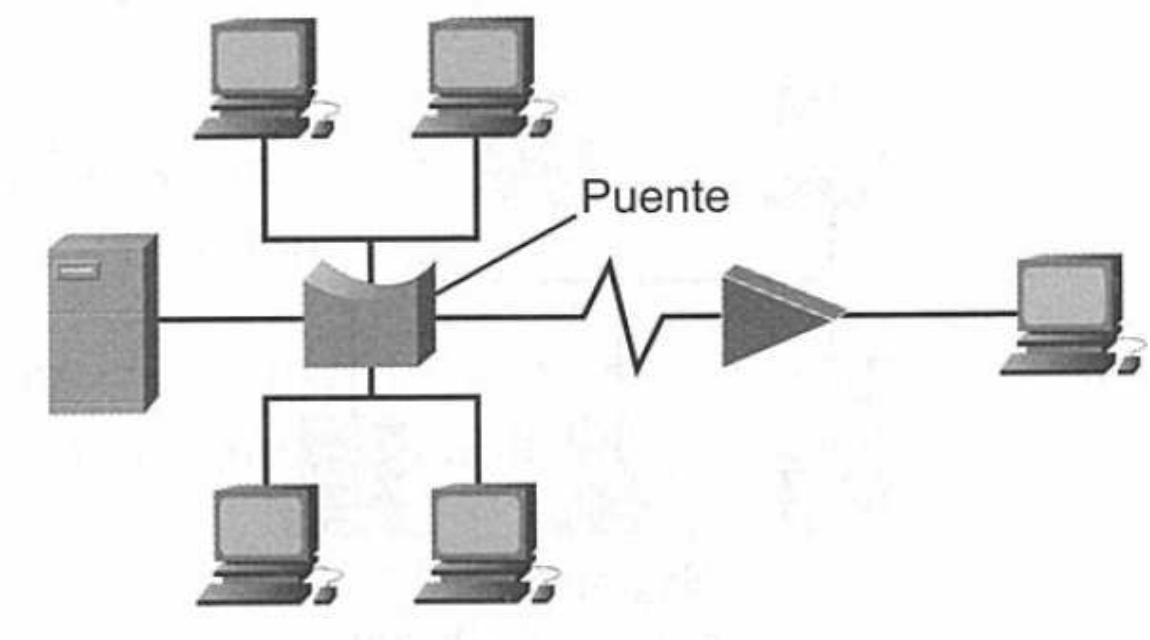


Figura 2.9 Conexión de puentes.

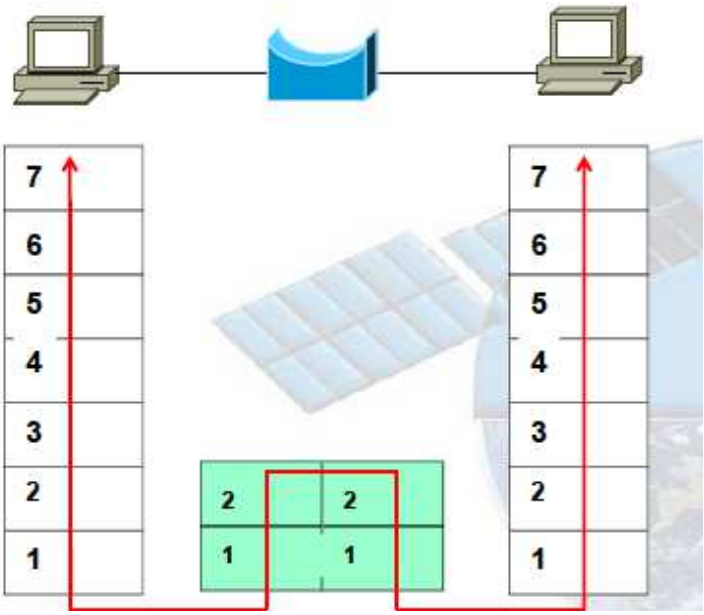


Figura 2.10 Conexión de puentes.

2.4.6 Colisión

- Se produce cuando más de un usuario trata de enviar datos al mismo tiempo que otro. Las colisiones degradan el rendimiento.

2.4.7 Dominio de colisión.

- Es el área dentro de la red donde los paquetes se originan y colisionan.
- Las interconexiones de capa 1 forman parte del mismo dominio de colisión.

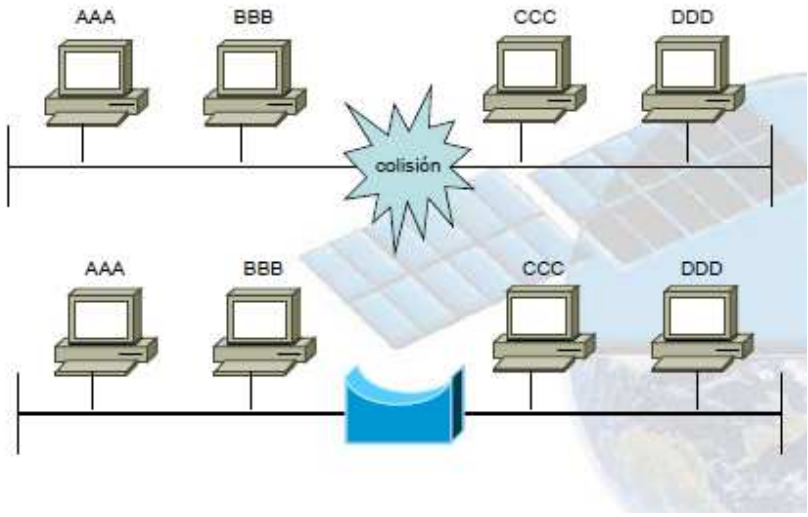


Figura 2.11 Dominios de colisión.

2.4.8 Switches.

- Dispositivos que realizan funciones en capa 2, aunque también hay los llamados switches multicapa que trabajan en el nivel 2/3.
- En cierta medida son Bridges multipuerto.
- Toma decisiones con base en direcciones físicas, "conmutando" datos sólo entre los puertos que requieren comunicarse.

Un conmutador de Ethernet se puede ver como un puente de múltiples puertos de gran velocidad con un cerebro (véase figura 2.13). Los conmutadores no sólo permiten a cada estación final tener un puerto exclusivo (lo que implica que no se producen colisiones), sino que también

permiten a las estaciones finales transmitir y recibir al mismo tiempo (usando dúplex completo), incrementando enormemente la eficiencia de la LAN.

A diferencia de los hubs, cada uno de los segmentos conectados a uno de sus puertos tiene un ancho de banda completo.

Su función es segmentar la red para repartir el tráfico, es decir, cada puerto representa un dominio de colisiones, al dividir el dominio de colisiones se obtiene un ancho de banda mayor por usuario.

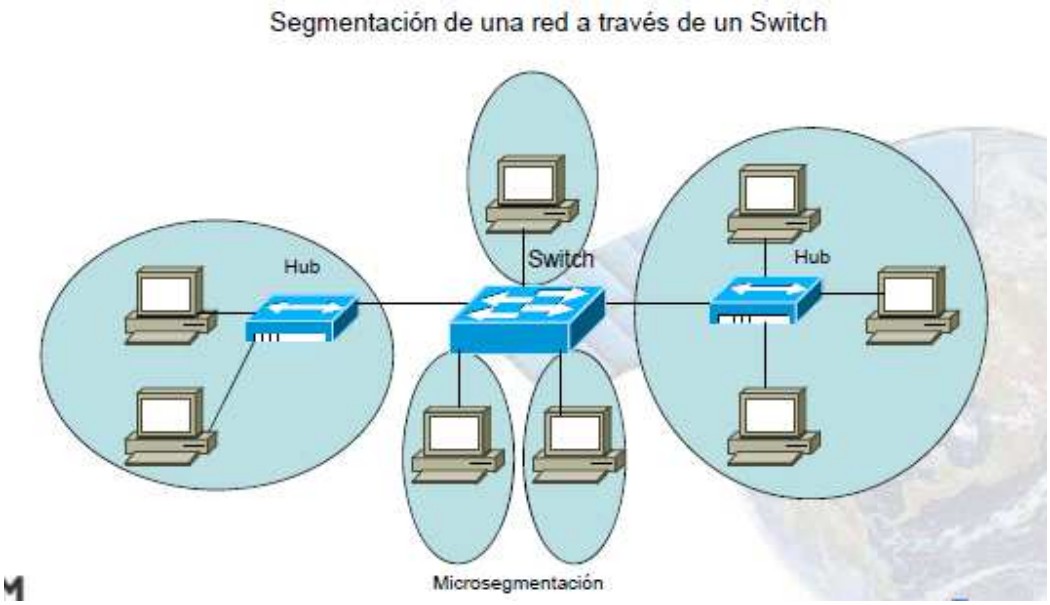


Figura 2.12 Segmentación de una red.

Operan a velocidades mucho más altas que los bridges y pueden admitir nuevas funcionalidades como por ejemplo LANs virtuales (VLAN).

La asignación de un puerto switch a un sólo hosts se le conoce como microsegmentación. Todo el ancho de banda es para un solo usuario.

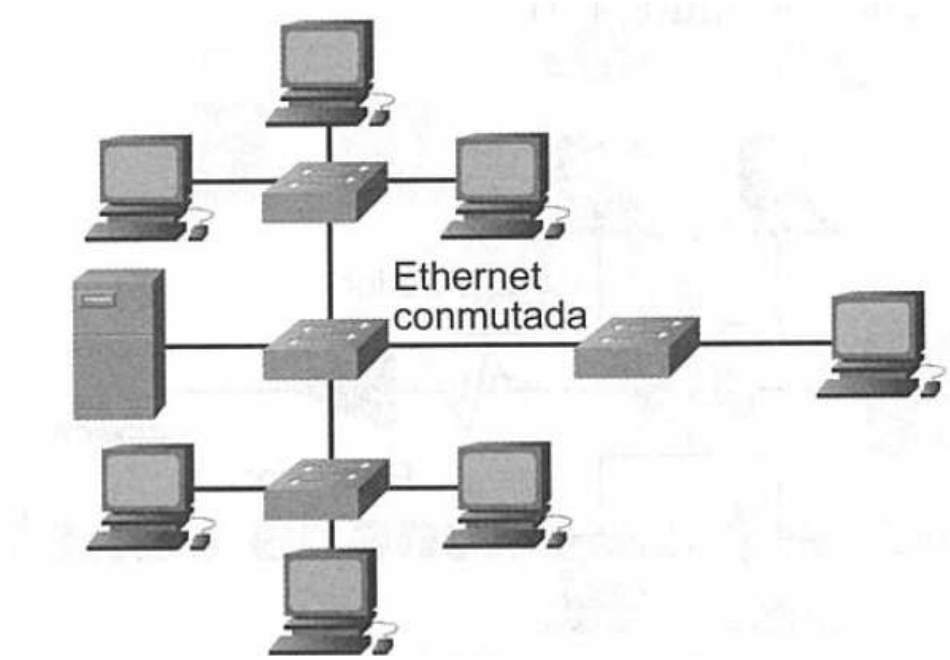
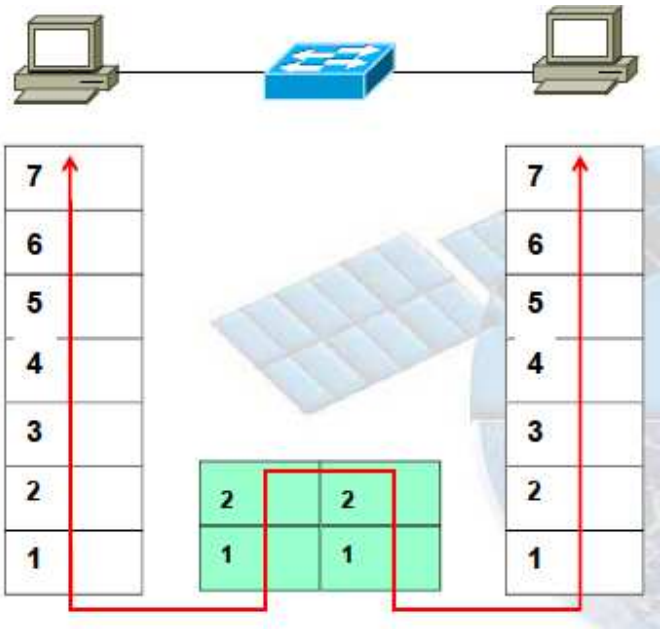


Figura 2.13 Ethernet conmutada.



2.14 Switch.

2.4.9 Enrutadores LAN

Los enrutadores de base LAN aumentan de forma importante la velocidad, distancia e inteligencia de las redes LAN. Los enrutadores también permiten que el tráfico sea enviado a lo largo de caminos múltiples (figura 2.15). Los enrutadores, sin embargo requieren un protocolo común entre el enrutador y la estación final.

Los routeadores realizan funciones de capa 3 del modelo OSI, toma decisiones con base en direcciones de red, forma la parte dorsal de Internet. Encamina los paquetes de router a router. Cada paso de un paquete de un routeador a otro se denomina salto (hop).

Junto con los protocolos de enrutamiento se busca que los paquetes sigan una trayectoria con el menor número de saltos posibles y por la mejor ruta posible.

Cada puerto es un dominio de broadcast, además puede conectarse diferentes tecnologías de LAN.

Un routeador examina los paquetes de entrada y lo dirige hacia un puerto de salida.

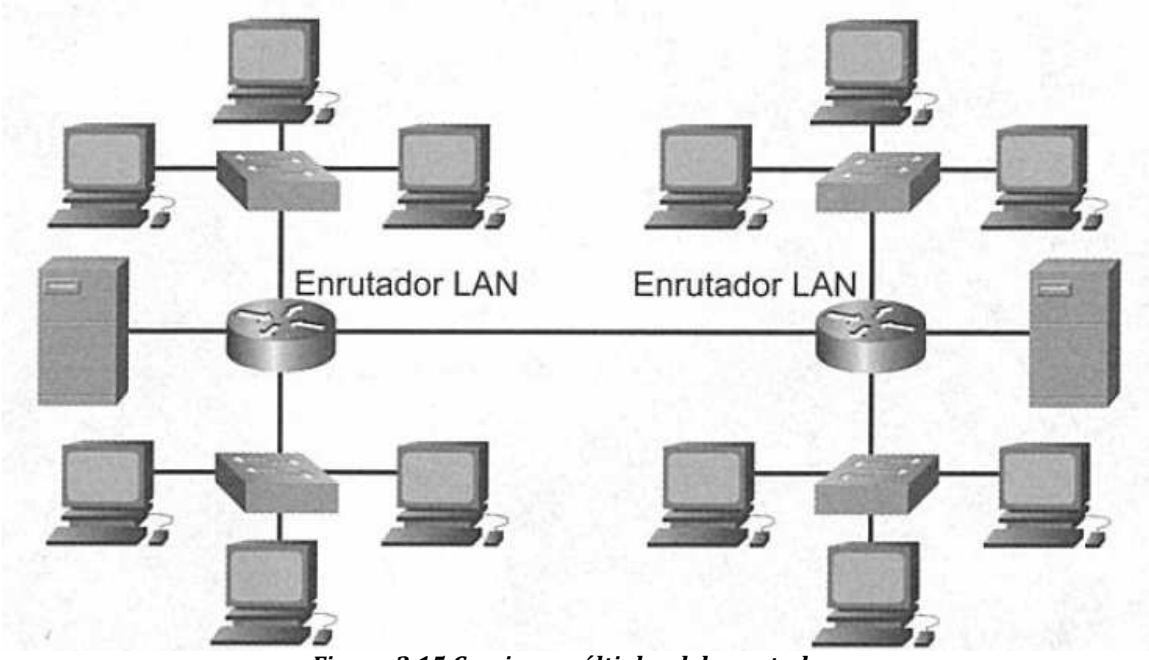


Figura 2.15 Caminos múltiples del enrutador.

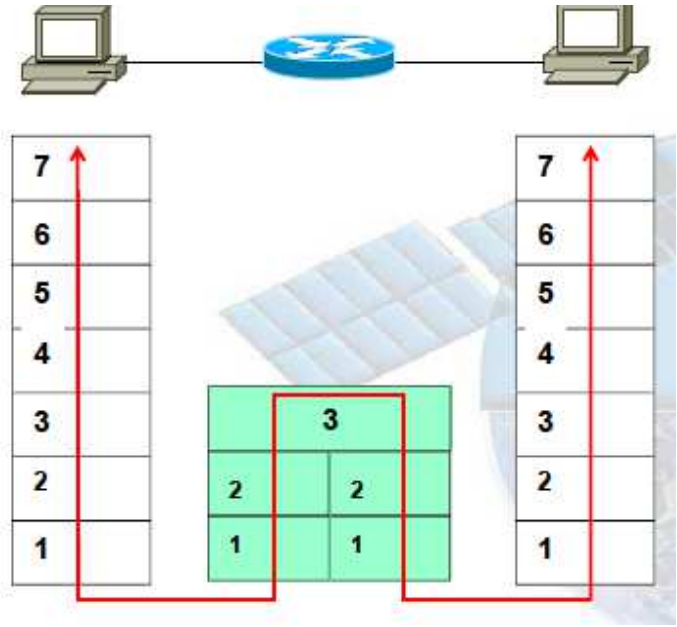


Figura 2.16 Router.

2.4.10 Gateway

Realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones, normalmente es un router.

2.5 Conmutación LAN

La conmutación consiste en el establecimiento de un sistema de comunicación entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de equipos o nodos de transmisión, es decir que con el proceso de conmutación podemos hacer entrega de una señal desde un puerto origen hacia un puerto destino.

La conmutación es un proceso que funciona en la capa 2 del modelo OSI (Enlace de datos).

Existen dos tipos de conmutación en la arquitectura de la redes de comunicación:

- Conmutación de circuitos: El camino o circuito entre los extremos del proceso de comunicación. Se mantiene en forma permanente durante el tiempo que dure la comunicación, esto se hace para mantener el flujo de información entre los dos extremos.

- Conmutación de paquetes: En la conmutación de paquete no existe circuito permanente entre los extremos, en este proceso simplemente la red se dedica a

encaminar paquete a paquete la información para los usuarios que establecen la comunicación.

Difusión y dominios de colisión.

De tiempo en tiempo, un dispositivo de la red querrá comunicarse con otros dispositivos "locales" al mismo tiempo. Normalmente esto ocurre cuando un dispositivo solicita en red una dirección IP, cuando un dispositivo se añade por primera vez a la red o cuando se produce un cambio en la red. (figura 2.16).

Un grupo de dispositivos que reciben todos los mensajes de difusión miembro de ese grupo se llama un dominio de difusión. Los dominios de difusión de red se segmentan normalmente por dispositivos de nivel 3. Pensar en un dominio de difusión es como estar en un jardín y dar un alarido tan fuerte como uno pueda, los vecinos que escuchan el alarido son el dominio de difusión de la persona.

Remitiendo y filtrando

Desde un punto de vista de una red eficiente es fácil de ver que es mucho mejor para la red cuando el intercambiador conoce todas las direcciones de cada puerto. Sin embargo no es siempre práctico introducir toda esa información manualmente. Conforme crece la red y se van haciendo cambios, se vuelve casi imposible mantenerse al día. Un intercambiador siempre hace algo cuando recibe el tráfico. Lo normal es enviar el tráfico a un puerto especifico (lo que recibe el nombre de filtrado), pero esto solo funciona cuando se conoce la localización del destino previsto. Cuando no se conoce la localización del destino previsto el intercambiador envía el tráfico a todos los puertos excepto al que ha enviado el dicho tráfico. Este proceso se llama inundación

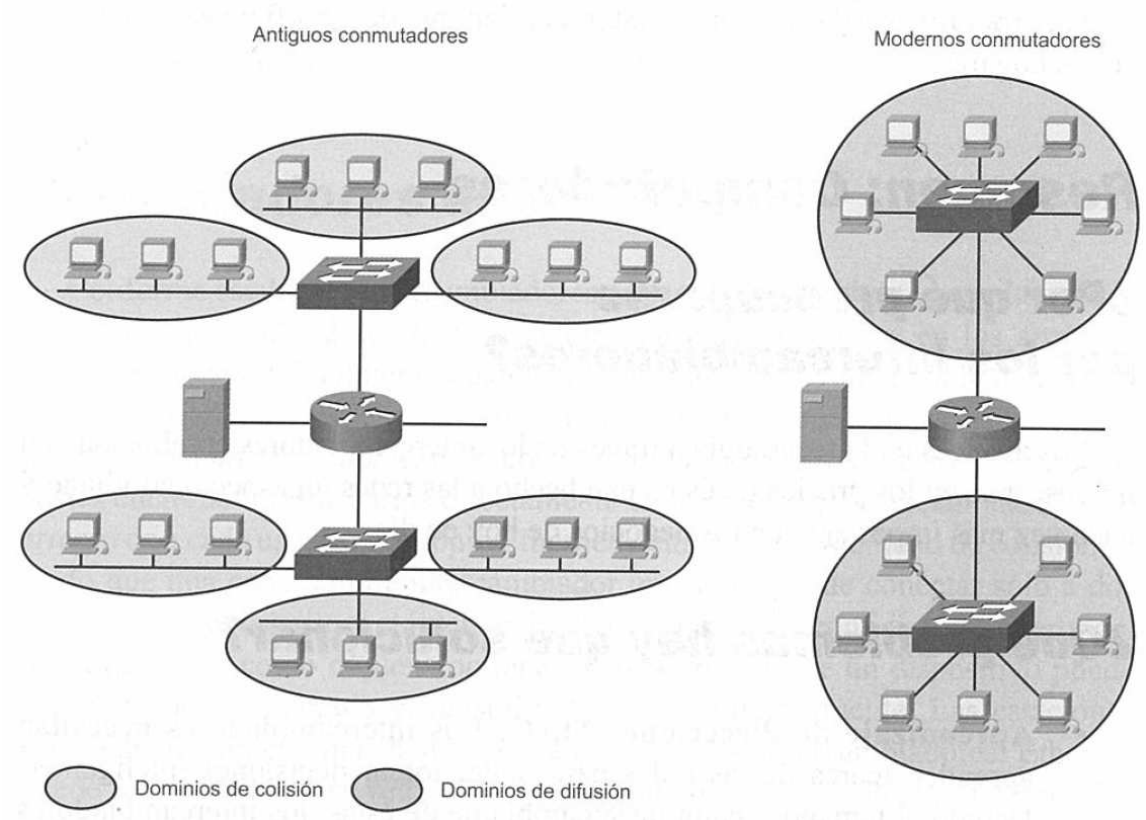


Figura 2.16 Conmutación LAN

2.6 Seguridad de red

La seguridad es un elemento esencial de cualquier red, y muchas de las tareas cotidianas de mantenimiento que los administradores de red llevan a cabo están relacionadas con la seguridad. Todos los mecanismos de seguridad proporcionados por los diversos componentes de la red están diseñados para proteger el hardware y el software y los datos del sistema de daños accidentales o del acceso no autorizado. El objetivo del proceso de administración de seguridad es proporcionar a los usuarios acceso a todos los recursos que necesitan, mientras se les aísla de aquellos que no necesitan. El uso adecuado de las herramientas de administración de seguridad proporcionadas por los componentes de la red es esencial para mantener una red segura y productiva.

La red de una empresa es como cualquier otro activo, tiene valor y afecta al éxito y a los ingresos de la misma. La información y equipos de cómputo se encuentran en la red entonces es muy necesario protegerla.

Las amenazas a la seguridad se presentan de muchas formas distintas:

- Un hacker informático entrando en la red para robar información confidencial o destruir datos de la compañía.
- Un desastre natural, como fuego, un tornado o terremoto que destruye los ordenadores y el equipo de red.
- Un trabajador descontento o que intencionadamente intenta modificar, robar o destruir información y dispositivos de la empresa.
- Un virus o gusano de ordenador.
- Un acto de guerra o terrorismo.

Las amenazas más frecuentes a la seguridad introducidas por la gente incluyen las siguientes:

- Paquetes de red creados para fisgonear.
- Contaminación de direcciones IP.
- Ataques a las contraseñas.
- Distribución de información confidencial interna a fuentes externas.
- Ataques no intencionados.

La seguridad de Internet también es una gran preocupación debido a la exposición de los recursos de datos de las empresas a la parte de Internet públicamente accesible. Tradicionalmente se podía conseguir seguridad separando físicamente las de redes de las empresas de las redes públicas. Sin embargo, con servidores Web y bases de datos de empresa éstas tienen que ser especialmente diligentes en la protección de sus redes. Otra área de reciente preocupación de seguridad son las redes inalámbricas. Las redes tradicionales se establecían a través de circuitos físicos de cables. Sin embargo la mayoría de las empresas tienen redes inalámbricas instaladas en sus edificios, de forma que los empleados puedan vincularse a la red de la empresa desde las salas de conferencias y otros espacios compartidos desde sus computadoras portátiles. De forma adicional los proveedores de servicio ofrecen servicios públicos inalámbricos de Internet. Las siguientes secciones describen las diferentes categorías de seguridad en la red.

2.6.1 Identidad

La identidad es la identificación de los usuarios, aplicaciones, servicios y recursos de la red. Determinar quien está en la red es la primera parte de cualquier diseño de seguridad. Ejemplos de estas tecnologías son los certificados digitales, tarjetas inteligentes, sistemas biométricos y servicios de directorio.

La identidad puede incluir los siguientes aspectos:

- Identidad del usuario basada en clave, tarjeta inteligente, firma digital u otra.
- Dispositivo para la identidad (como un teléfono IP) basado en direcciones IP o MAC.
- Aplicación de identidad basada en dirección IP o en número de puerto TCP/UDP.

La identidad está fuertemente vinculada a la autorización. Tan pronto se establece la identidad, se puede aplicar, controlar y reforzar la directiva adecuada para ese usuario, dispositivo o aplicación.

2.6.2 Seguridad de perímetro.

La seguridad del perímetro controla el acceso a aplicaciones, datos y servicios claves de la red, de forma que solo los usuarios y la información de la red autorizados puedan pasar a través de la red. Algunos ejemplos son los cortafuegos que son dispositivos que permiten pasar solo a tráfico autorizado, rastreadores de virus, filtros de contenido, lista de acceso de los enrutadores. El perímetro de seguridad es particularmente importante cuando una red de negocios se conecta a una red compartida, como Internet.

2.6.3 Privacidad de datos.

Parte importante de la información que pasa a través de una red es confidencial. Tanto si trata de información de negocios, como si es de tipo personal, la información ha de ser protegida de ser vista por gente no autorizada. Las tecnologías y protocolos de encriptación como el Protocolo de Seguridad de Internet (IPsec), la Capa de Conexión Segura (SSL) y el Protocolo de Seguridad en Tiempo Real (SRTP) se usan normalmente para proteger los datos, especialmente, cuando se transportan a través de una red compartida o no confiable, como un proveedor de servicio WAN o de Internet público. Las tecnologías como la “marca de agua” y la Gestión de Derechos Digitales de los datos, están ganando seguridad.

2.6.4 Controlar la seguridad.

Independientemente de cuánta seguridad se desarrolla todavía es necesario revisar las redes y sus componentes para asegurarse de que la red sigue siendo segura, los administradores de red deben de checar y comprobar periódicamente la situación de las soluciones de seguridad. Las herramientas de revisión de la seguridad de la red y sistemas de detección de intrusos proporcionan visibilidad al estado de seguridad de la red. Los sistemas de control de

vulnerabilidades y sistemas de detección de intrusos se deben de utilizar en forma combinada para que el administrador pueda responder en tiempo real los ataques.

Además de la tecnología de control, una de las mejores herramientas de seguridad continúa siendo el que los empleados pongan atención, un poco de entrenamiento lleva muy lejos.

Las 14 vulnerabilidades de seguridad más frecuentes

Las siguientes son las 14 vulnerabilidades de seguridad más frecuentes:

1. Inadecuado control de acceso de ruta.
2. Puntos de acceso lejano que proporcionan entradas fáciles a la red corporativa, inseguros y no controlados.
3. Escapes de información (a través de señales inalámbricas o incluso intentos de ingeniería social) pueden proporcionar al atacante información sobre el sistema operativo y aplicaciones.
4. Usuarios que manejan servicios innecesarios.
5. Claves fáciles, que se prestan con frecuencia o que se usan demasiado.
6. Cuentas de usuario o de prueba con demasiados privilegios.
7. Servidores de Internet mal configurados, especialmente FTP anónimos.
8. Cortafuegos mal configurados.
9. Software caducado, vulnerable o que se mantiene en configuraciones por defecto.
10. Falta de directivas de seguridad, procedimientos y normativas base aceptadas plenamente o bien comunicadas.
11. Relaciones de confianza excesivas, como Windows Active Directory y los .rhosts y los ficheros .equiv para usuarios de UNIX pueden dar a los hackers acceso no autorizado a sistemas sensibles
12. Vulnerabilidades inherentes a los programas populares de compartir archivos par-a-par.
13. Posibilidades de establecimiento de claves, control y detección inadecuados.
14. “Promiscuidad” de los dispositivos móviles como las lap-tops y smart phones, PDA que son

utilizados en entornos Wi-Fi públicos, redes de invitados, redes domesticas, etc., y luego son reintroducidos a la red corporativa.

Tabla 1. Vulnerabilidades en las redes.

2.6.5 Políticas de seguridad

Las herramientas y tecnologías no sirven de nada sin políticas de seguridad bien definidas. A pesar de la existencia de herramientas sofisticadas, las compañías tienen que emplear una política escrita con líneas claras para su cumplimiento. Ejemplo de estas políticas son los mecanismos que exigen al usuario cambiar su contraseña una vez al mes, o que el usuario tenga prohibida la instalación de software dentro de la computadora asignada en el trabajo o que se tenga prohibido el uso de Internet dentro de ciertas áreas de la empresa.

2.6.6 Hackers

El hackeo informático se reduce en las siguientes actividades:

1. **Introducirse.** Entrar en una red privada es normalmente la primera parte de una secuencia de hackeo. La mayoría de los ataques de introducción requieren una clave (que es adivinada o robada), pero hay otros modos de introducirse.

2. **Destruir información.** Tan pronto se introducen a la red muchos hackers(los anarquistas en particular) tratan de romper o deshabilitar toda la red o alguna parte de la misma, como los servidores.

3. **Robar información.** Los planos, esquemas, fuentes de código, propiedad intelectual pueden ser vendidos por gente sin escrúpulos a empresas, agencias de gobierno, etc.

4. **Dejar una tarjeta de visita.** Muchos hackers quieren asegurarse de que reciben el crédito de haber hecho su trabajo, de forma que encuentran un modo de firmar su trabajo o probar que estuvieron en la red.

2.6.7 Hacker y ataques.

En terminología de redes se refiere a cualquier intento de introducirse a un equipo, red o paquete, además de a cualquier intento de lanzar un programa malicioso o autorrepetido. Hay muchas clasificaciones de ataques, algunas son las siguientes:

Los ataques activos incluyen la inserción de archivos maliciosos, alteración de datos.

Los ataques pasivos como la observación de información no alteran la red, pero puede usarse para obtener información que puede utilizarse en un ataque activo. Los ataques por personas interpuestas se producen cuando un hacker se pone a sí mismo entre dos usuarios autorizados y se introduce para ver sus contraseñas. Los ataques pasivos son difíciles de detectar. Los ataques lejanos son dirigidos por personas que están fuera de la red, mientras que los ataques locales usan una cuenta existente para hacer estallar el sistema.

Los ataques de "darse a la fuga" colapsan rápidamente los sistemas, mientras que los ataques persistentes afectan a las víctimas solo cuando cesa el ataque.

Los más típicos son los siguientes:

1. **Dentro del trabajo:** El interior del trabajo incluye cosas como robo de contraseñas, espionaje industrial, empleados descontentos que intentan perjudicar al jefe o simples errores.

   Muchas de estas brechas pueden cerrarse con el cumplimiento de las políticas de seguridad y observación de cómo los empleados controlan sus equipos y contraseñas.

2. **Puertas traseras:** Los atajos administrativos, errores de configuración, contraseñas fácilmente descifrables y el acceso lejano inseguro puede ser utilizados por los hackers para entrar a la red. Con la ayuda de **bots** si una red tiene una debilidad, probablemente será controlada.

3. **Denegación de servicio:** El ataque DoS proporciona medios de derribar una red sin necesidad de entrar en ella. Los ataques DoS funcionan inundando un dispositivo de red o servidor de aplicación con tráfico falso.

   El DoS distribuido (DDoS) consiste en coordinar ataques DoS desde muchas fuentes. El ataque DoS es más difícil de bloquear porque usa muchas fuentes IP cambiantes que son difíciles de rastrear.

4. **Anarquistas, piratas y bromistas:** Los anarquistas simplemente quieren destruir información. Normalmente aprovechan cualquier oportunidad y objetivo.

   Los piratas son aficionados o profesionales que descubren contraseñas y desarrollan troyanos u otro software. Usan tanto ellos el software o lo venden.

   Los bromistas de pantalla son piratas frustrados. No tienen realmente la capacidad para ser piratas, así que compran o descargan warez, que a su vez lanzan.

5. **Virus y gusanos:** Los virus y los gusanos son programas que se autorrepiten o fragmentos de código que se atacan a sí mismos o a otros programas (virus) o máquinas (gusanos)

   Los virus normalmente permanecen asociados al usuario local y los gusanos tienden a repetirse y proliferar a través de la red.

6. **Troyanos:** Los troyanos son la causa principal de la mayoría de las rupturas de la red. Van asociados con otros programas, de forma que cuando el programa se descarga, el software del pirata instala un virus, un buscador de contraseñas o un software para el control remoto.

7. **Botnets:** Tan pronto como un equipo ha sido atacado por un troyano, puede ser controlado a distancia, el pirata puede utilizar este equipo para lanzar ataques DoS.

   Los grupos de equipos bajo el control de un pirata se llaman botnets.

   La palabra viene de robots, con el significado de equipos que siguen ciegamente a sus amos.

8. **Husmear y contaminar:** Husmear hace referencia al acto de interceptar paquetes TCP. Esto puede ser solo para observar información ajena o para algo más malicioso. Contaminar es el acto de enviar un paquete ilegitimo con un ACK esperado, que puede ser adivinado, predicho u obtenido fisgoneando

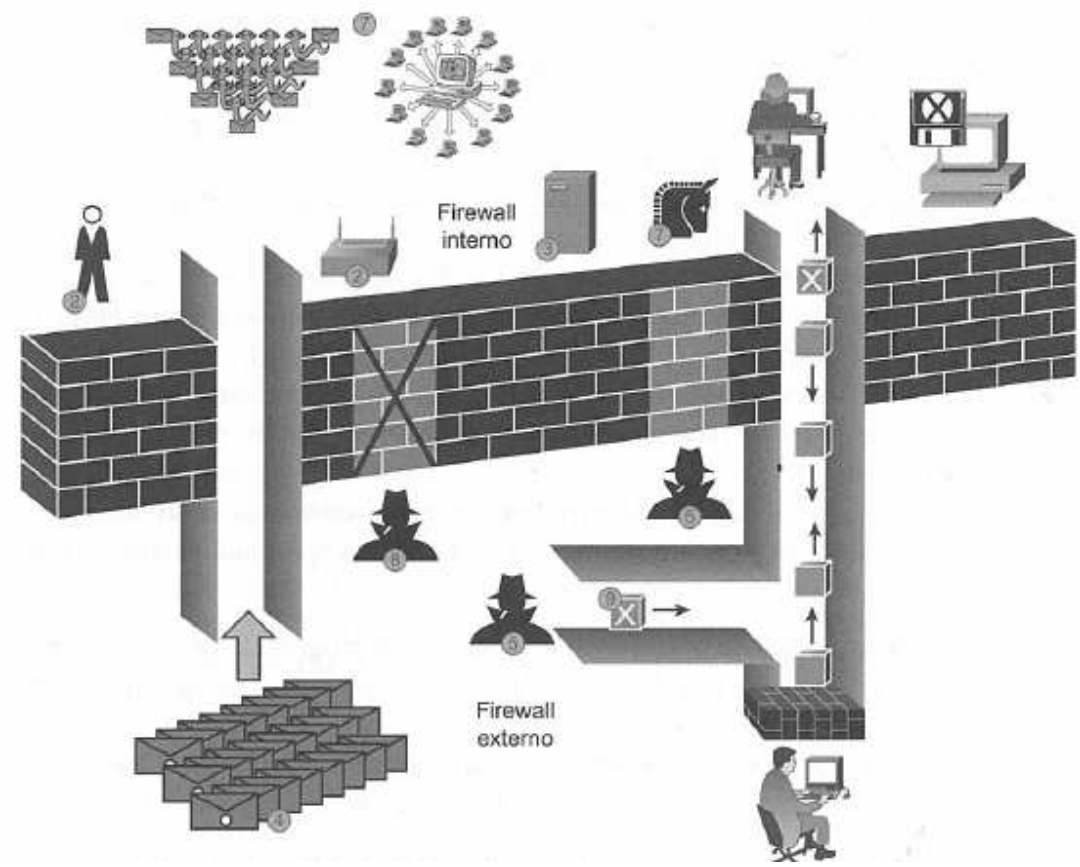


Figura 2.17 Ataques más comunes.

2.7 Firewalls (Cortafuegos).

Conforme mas computadoras se conectan a redes públicas y los empleados de las empresas se conectan para trabajar a través de Internet, se incrementan las oportunidades para los ataques maliciosos de hackers. Lo mismo es aplicable a las redes internas corporativas en las que las empresas deben proteger sus centros de datos y sus recursos de computadoras frente a ataques internos y externos.

El modo más seguro de evitar ataques es no conectarse a la red. La seguridad física sigue siendo un debate, pero irse de la red es el mejor modo de reducir la exposición a riesgos de seguridad.

Sin embargo esto no es una opción práctica. En su lugar está el concepto de perímetro de seguridad. El perímetro de seguridad lo proporciona normalmente el cortafuego (firewall). Estos se sitúan entre el sitio WAN inseguro (sucio) y un sitio seguro (limpio) LAN. Algunas veces los

dispositivos como los servidores Web o los productos de vigilancia de intrusión se sitúan entre los sitios WAN y LAN. Esta ubicación en el "limbo" entre las redes sucias y limpias se llama usualmente la zona desmilitarizada (DMZ).

Por ejemplo, un usuario doméstico podría poner un cortafuego entre su computadora y la conexión de internet. El lado del muro se conecta a Internet es el lado sucio (en el sentido de que el tráfico en éste no es confiable) y el lado del cortafuegos que se conecta a la red doméstica es el sitio limpio (en el que él es confiable). El cortafuegos revisa los paquetes que van en cada dirección y determina si se puede permitir pasar cada uno de ellos o si es mejor desecharlo. El cortafuego se ha convertido en el punto central para desarrollar actividades relacionadas con el perímetro.

2.7.1 Protección con cortafuegos.

Los cortafuegos se diseñan para combatir amenazas relacionadas con la seguridad de la red como las siguientes:

Observación pasiva: Los atacantes pueden ser programas de captura de paquetes para observar información importante o robar combinaciones de usuario clave.

Contaminación con direcciones IP: Un atacante simula ser una computadora confiable usando una dirección IP que está dentro del rango aceptado de direcciones IP internas. Esto es similar a simular una identidad.

Revisión del puerto: Los servidores "escuchan" tráfico en los diferentes puertos. Por ejemplo el puerto 80 es el lugar donde los servidores escuchan el tráfico http en la Web. Los atacantes encuentran modos de infiltrar servidores a través de servidores de puertos individuales.

Ataque DoS: El atacante intenta bloquear a los usuarios validos la posibilidad de acceder a los servicios creando paquetes TCP SYN que agotan la capacidad del servidor y no le permiten manejar otras peticiones válidas. Estos tipos de ataques se llaman también inundaciones ping

Ataque en la capa de aplicación: Estos ataques aprovechan la debilidad de ciertas aplicaciones para obtener acceso al servidor del usuario.

Los cortafuegos permiten bloquear éstos y otros ataques revisando el tráfico manteniendo registro de las sesiones válidas y filtrando el tráfico sospechoso para que no pueda pasar.

Los cortafuegos y los sistemas de detección de intrusos (IDS) proporcionan defensa de perímetro para las redes corporativas y personales. Conforme los hackers se vuelven más sofisticados y agresivos en sus ataques la tecnología que protege a las redes ha tenido que

evolucionar en el mismo sentido, ya que los cortafuegos e IDS se crearon en respuesta directa de los hackers, este tema tiene especial importancia para las aplicaciones Web.

2.7.2 ¿Qué hace un firewall?

Mantienen a las redes personales y corporativas seguras de los ataques revisando los paquetes a través de perfiles de paquetes conocidos y actuando como un aislante entre el usuario y el mundo exterior. Los perfiles (que son como firmas de virus o pautas del contenido del paquete) son normalmente descubiertos por compañías de servicios que venden el perfil del paquete a cambio de una tarifa.

La función de proxy funciona usando una tercera dirección (distinta de la dirección real del usuario y de la del servidor) cuando el usuario se comunica con el mundo exterior. De este modo nadie sabe la dirección real.

En término de sistemas de cortafuegos, los paquetes entran en dos categorías:

Los paquetes buenos con salida de la red son enviados por usuarios internos a localizaciones externas aprobadas como un sitio Web. Los paquetes buenos de entrada en la red se originan fuera del cortafuego externo. Puede corresponder a una sesión TCP originada por un usuario interno o están accediendo a servicios públicamente accesibles como en tráfico de la Web.

Los paquetes malos son todo lo demás, estos paquetes son eliminados para mayor seguridad.

2.7.3 Red limpia.

La red limpia es la red corporativa interior. Los únicos paquetes “externos” permitidos en la red limpia son los que han sido revisados y tienen el visto bueno de un paquete TCP generado por un equipo interno.

2.7.4 Filtro interior.

El filtro interior desarrolla las funciones de cortafuego y de sistema de detección de intrusos. Además para bloquear ataques como el DoS, revisa cada paquete, asegurándose de que ninguna sesión TCP iniciada externamente alcanza la red limpia, dado que los piratas pueden tener acceso contaminando una sesión. Cualquier paquete de origen dudoso se elimina. El filtro interno

también revisa paquetes de salida de la red para asegurarse del cumplimiento de las directivas de la empresa.

2.7.5 Aislamiento de la red.

El aislamiento de la red LAN o DMZ funciona como una memoria intermedia entre las aplicaciones de la cara externa (Web) y la red LAN limpia. Los servidores ubicados en la DMZ se llaman defensas del usuario. La gente de fuera los usa para acceder a páginas Web públicas o servidores FTP. Estos servidores están protegidos pero siguen siendo vulnerables a los piratas. Las defensas del usuario tienen que tener tan pocos servicios como sea posible y deberían tener reglas de acceso muy simples para evitar puertas traseras de acceso a la red limpia LAN.

2.7.6 Filtro externo

El filtro externo es un cortafuego que revisa en las respuestas TCP y los paquetes UDP con números de puertos asociados con las defensas de usuarios presentes. Este cortafuego debería tener solo rutas estáticas y reglas muy claras, dado que los procesos complicados son propensos a errores.

2.7.7 Los procedimientos de los hackers

Los hackers utilizan muchos trucos y herramientas para hacer estallar las redes, por ejemplo ataques DoS, contaminación de dirección IP, virus, gusanos, troyanos. (Figura 2.18)

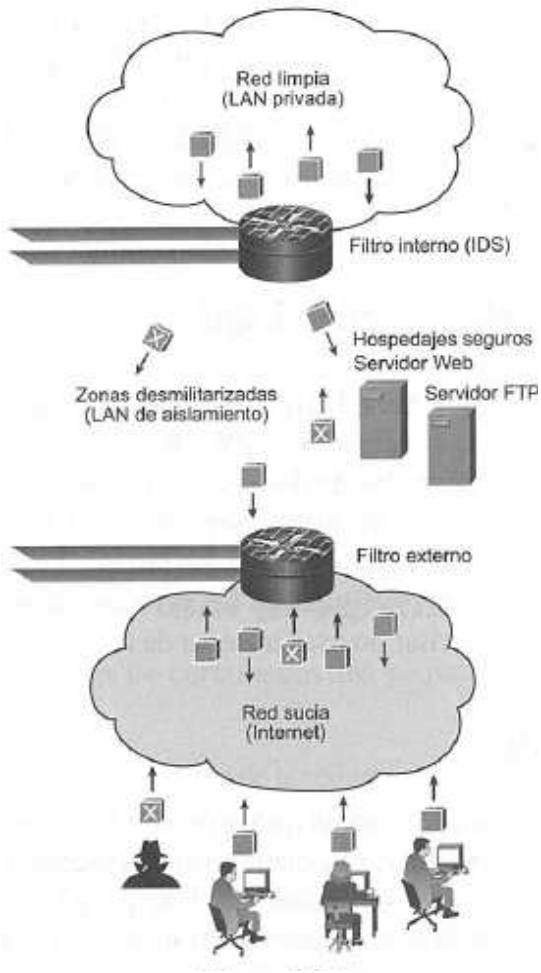


Figura 2.18 Hacker estallando redes.

2.8 Sistemas de prevención de intrusos

Los Sistemas de Detección de Intrusiones (IDS) analizan los datos en tiempo real para detectar, registrar e impedir errores y ataques. Los sistemas IDS basados en el usuario revisan las operaciones del servidor buscando cualquier hecho inesperado. Los sistemas IDS basados en la red revisan el tráfico de red en una parte concreta de la misma.

Los IDS basados en la red revisan el tráfico en tiempo real, mirando un conjunto de paquetes que llevan la firma de ataques conocidos. Cuando detecta un flujo de datos sospechoso concreto, el IDS impide la entrada. En ese momento puede decirle al enrutador que recibe el trafico que deniegue el tránsito y cualquier tráfico futuro de esa fuente.

Para ser efectivas las soluciones de detección de intrusos deben estar activas en todos los puntos de entrada de la red incluyendo los siguientes:

- Desde Internet.
- Desde sucursales y oficinas pequeñas u oficinas en hogares.
- Desde dentro de las empresas.

El sistema también tiene que dar protección a los activos de la red y a los servicios proporcionados por la red como los servidores. Un aspecto importante de la detección de intrusiones es la posibilidad de funcionar como un sistema pasivo de detección, registrando sucesos potenciales de intrusión o como un sistema de prevención activo, tomando acciones que mitiguen el daño en tiempo real. La detección de intrusos también tiene que ser capaz de establecer correlaciones entre varios hechos en un periodo de tiempo para detectar ataques complejos.

Control Pasivo.

Un IDS controla de forma pasiva la red y los sucesos registrados: En la figura 2.19 se pueden ver los pasos que se siguen.

1. El tráfico de la red se copia y se dirige al sensor IDS para sus análisis.
2. Si el tráfico es compatible con una señal de intrusión la señal “arde!.
3. El sensor IDS envía una alarma a la consola de gestión.

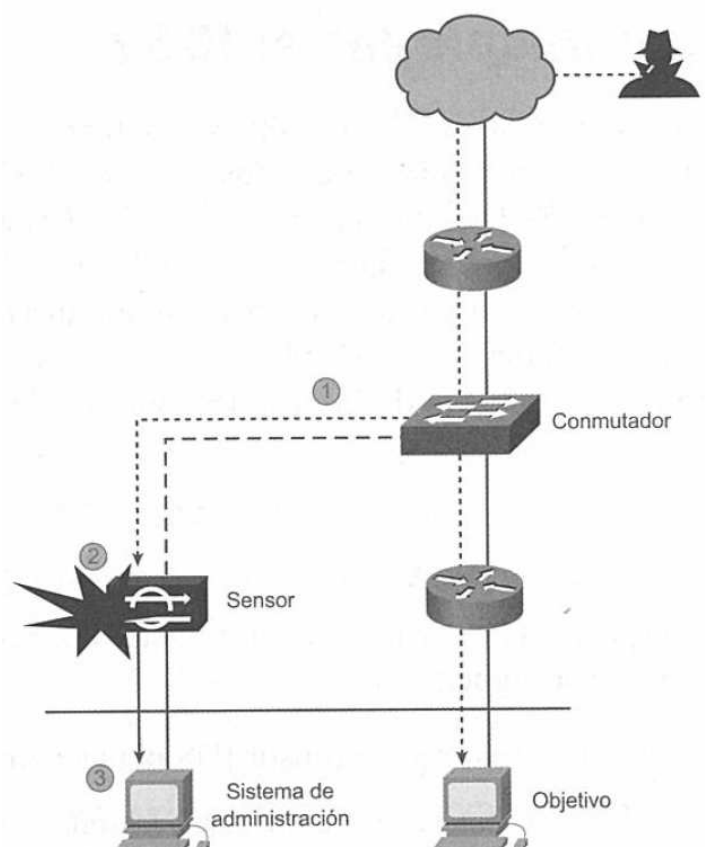


Figura 2.19 Tráfico de la red.

Control activo

El IPS controla activamente paquetes en línea en la red. En la figura 2.20 se pueden ver los pasos que hay que seguir:

1. El tráfico en la red no se copia sino que se envía a través del sensor IPS para su análisis.
2. Si el tráfico es compatible con una señal de intrusión la señal "arde".
3. El tráfico que es compatible con la señal es eliminada.
4. El sensor IPS también envía una alarma a la consola de gestión.

Con el IPS los paquetes que son parte del intento de intrusión son rechazados antes de llegar a su objetivo.

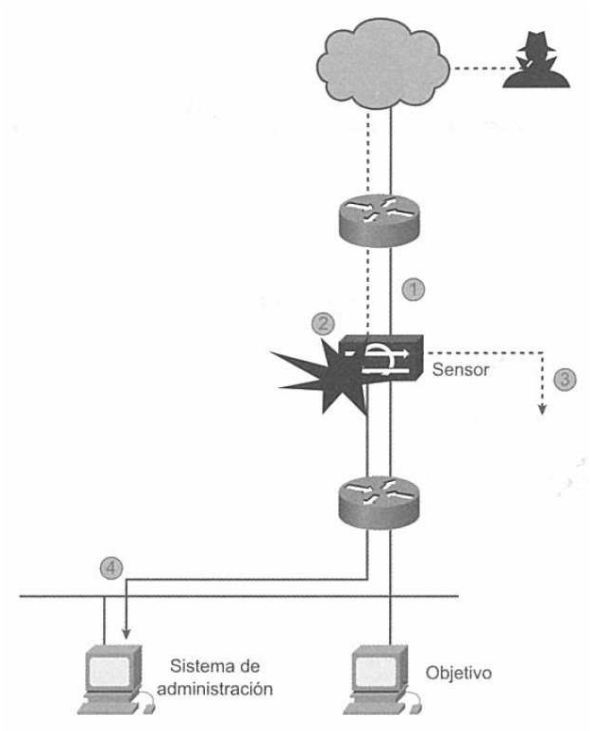


Figura 2.20 Control activo

Sistemas de Prevención de intruso (IPS)

El Sistema de Prevención de Intrusión (IPS) es similar a IDS. Ambos requieren una base de datos de señales de ataques conocidos para ser programadas en el dispositivo de red de IDS o IPS. Sin embargo mientas el IDS normalmente detecta intentos de intrusión y los impide o envía alertas al personal de red, el IPS normalmente opera "en línea! Dentro de la red e incluye medidas adicionales para detener los intentos de intrusión en tiempo real. A pesar de que podría parecer como si estas tecnologías fueran la misma cosa y que pudieran incluso reemplazar al firewall, hay que tener en mente que cada tecnología proporciona un nivel mayor de seguridad. Esta aproximación, que recibe el nombre de "defensa en profundidad" proporciona una aproximación de múltiple nivel a la seguridad asegurando que una brecha en el sistema no pone en peligro a toda la red.

Falsos positivos.

Uno de los mayores desafíos del IDS IPS consiste en distinguir ataques reales de positivos falsos. Éstos consisten en tráfico legítimo que hace saltar una alarma en un sensor IDS/IPS porque alguna de sus pautas encaja con una señal de ataque. Es como cuando se activa la alarma del auto.

Si se conecta diez veces en un día uno empieza a ignorarla y si se produce realmente el robo del auto nadie se da cuenta.

2.9 Redes virtuales privadas.

Las redes WAN[4] tradicionales requieren circuitos exclusivos que usen Transferencia de Tramas o líneas arrendadas. A pesar de que los precios han bajado, el coste de estos circuitos privados continúa siendo relativamente alto.

Como añadido a las redes WAN de uso exclusivo las corporaciones tenían que mantener grandes bancos de módems para llamadas (o dar la posibilidad externa de llamada al vendedor) de manera que los trabajadores pudieran acceder a la red corporativa con módems. En ambos casos, el objetivo era extender la red corporativa en la distancia hacia lugares e individuos lejanos.

Con la difusión del uso de Internet la posibilidad de conexión IP es accesible a los hogares y lugares públicos, como aeropuertos, cafeterías, etc. Los proveedores de servicio ven más efectivo a nivel de costes ofrecer WAN basada en IP antes que circuitos exclusivos. Las corporaciones tienen que ofrecer extensos servicios de Internet a sus empleados, socios y clientes para ser competitivas. Dada la confluencia del IP público y las redes corporativas, extender estas más allá del campo principal es más práctico y más barato.

Las redes virtuales (VPN) permiten a las corporaciones reemplazar sus redes privadas exclusivas (como Transferencia de Tramas, ATM o líneas arrendadas) con redes privadas "virtuales". Esto quiere decir que sus datos atraviesan las redes IP, pero es seguro debido a los sistemas de autentificación y encriptación. Debido al Internet, las redes proporcionadas por los proveedores de servicios de redes IP con una anchura de banda equivalente acaban siendo más baratas que los servicios exclusivos. Con la disponibilidad de conexión a Internet, las VPN permiten a los usuarios acceder a sus redes corporativas desde sus hogares, restaurantes, negocios, hoteles y otros lugares públicos: Las VPN también brindan la posibilidad de trabajar desde casa, creando teletrabajadores.

Con la convergencia de voz, video y datos, las VPN añaden valores que antes con los servicios de llamada y WAN no estaban disponibles. La conexión IP para la corporación elimina la necesidad de líneas separadas de fax, teléfono y video. Sin embargo, debido a que el uso de VPN implica mucho tránsito de datos para encriptar el tráfico, y los datos normalmente atraviesan el

[4] Una WAN es una colección de LAN, algunas de las cuales, o todas ellas, conectadas utilizando enlaces punto a punto que alcanzan distancias relativamente largas.

Internet público, se pueden producir retrasos impredecibles y los ajustes pueden afectar a la calidad de voz y video.

El término VPN realmente define dos conceptos distintos para redes virtuales. Para las corporaciones una VPN normalmente implica que el tráfico encriptado (usando IPsec) se envía a través de túneles por las redes públicas de IP. Para los proveedores de servicio, las VPN normalmente describen un servicio IP basado en intercambio de etiquetas que no implica encriptación. Esta discusión nos enfoca sobre las VPN basadas en IPsec.

Los cuatro tipos de conexiones de VPN son los siguientes:

- **Sitio a sitio**: Conecta lugares lejanos de la corporación a la red corporativa. El sitio lejano normalmente tiene varios usuarios compartiendo el acceso a la red corporativa.
- **Acceso remoto**: Los usuarios individuales consiguen acceso a la red corporativa tanto a través de servicio de llamadas o red de banda ancha. También se le llama teletrabajador.
- **Extranet**: Similar a sitio, excepto que la VPN conecta compañías distintas.
- **Verificación sin cables**: La tecnología de VPN también se puede utilizar para asegurar la identidad de usuarios sin cables en el entorno de una red corporativa.

Las preocupaciones por la seguridad se incrementan porque todas las compañías tienen que proteger sus redes de las otras. Debido a que atraviesan redes públicas, las VPN introducen consideraciones de seguridad que no eran tan importantes en redes WAN o de las redes privadas. En general proporcionar seguridad implica encriptar la información con destino a las corporaciones usando sistemas de verificación seguros. Para las VPN de sitia sitio, proporcionar seguridad normalmente implica añadir medidas de seguridad como cortafuegos, detección de intrusos y NAT/PAT. El IPsec proporciona un modo de manejar la encriptación entre muchos usuarios usando comunicaciones seguras.

Las VPN son sistemas de punto a punto, lo que implica que cada conexión tiene solo dos puntos finales. Un dispositivo sencillo puede tener muchos sitios lejanos, y los usuarios acabar sus conexiones en una caja, pero aun así hay solo una conexión (o túnel) por pareja.

Para cada túnel encriptado, los dos puntos finales deben primero verificar uno al otro y asegurarse de que el otro final es quien dice ser. En términos de encriptación, esto implica que cada punto final tiene que establecer una asociación segura (SA) con el otro. Esto implica esencialmente el intercambio confiable de información ente los dos usuarios que permite a cada uno verificar la identidad del otro. A este proceso se le conoce con el nombre de Intercambio de Claves de Internet (Internet Key Exchange, IKE). Después de que los dos sitios determinan que el

otro sitio es quien dice ser y que pueden confiar mutuamente en el otro, puede enviar datos encriptados a través de la VPN.

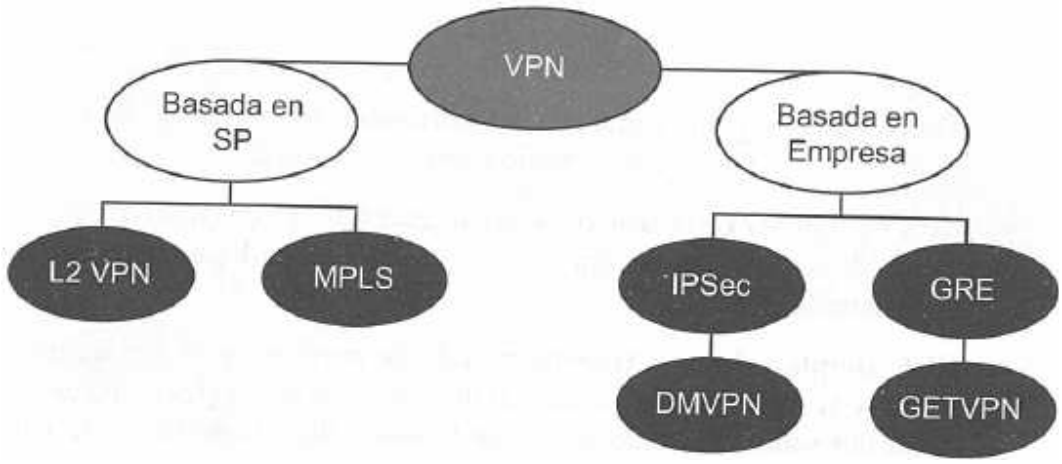


Figura 2.21 Clasificación de VPNs.

2.10 Almacenamiento en cache.

El auge de internet ha creado nuevos retos para los ingenieros de redes, existen varios problemas a resolver, por ejemplo obtener tiempo de respuesta más rápido, manejar enormes cantidades de usuarios, mayor rendimiento de sitios Web,.

El almacenamiento en caché de una red proporciona un medio para ubicar el contenido de la red más cerca de los solicitantes.

El almacenamiento en cache trabaja en cooperación con los puntos específicos de ahogo en una red. Se puede ubicar el tráfico colocando estratégicamente dispositivos de almacenamiento en cache en la red. La red almacena en caché de manera transparente contenidos visitados con frecuencia en unidades de almacenamiento interceptando las peticiones para esos contenidos almacenados y presentando la página del usuario. Por lo tanto la solicitud nunca llega al destino previsto, ahorrando ancho de banda y recursos del servidor.

Durante un aumento repentino de tráfico Web, un dispositivo de almacenamiento de caché puede ser sobrecargado, no siendo capaz de manejar peticiones Web adicionales. Para resolver este problema, los motores de caché determinan cuando éstos alcanzan un límite de carga concreto. En el punto de sobrecarga, el dispositivo de cache niega solicitudes adicionales y posteriormente envía directamente las peticiones a los servidores Web de destino para que estos las atiendan.

Una vez que el dispositivo de caché puede procesar las peticiones atrasadas, éste intercepta las peticiones nuevamente. Otra cuestión es mantener actualizado el contenido de caché. El dispositivo de caché se vuelve menos efectivo si éste no puede mostrar el mismo contenido que si el usuario visitara el servidor Web directamente.

2.11 La Capa de Sockets Seguros

Cuando la Web irrumpió a la vista pública, inicialmente sólo se utilizó para distribuir páginas estáticas. Sin embargo, pronto algunas compañías tuvieron la idea de utilizarla para transacciones financieras, como para comprar mercancía con tarjeta de crédito, operaciones bancarias en línea y comercio electrónico de acciones. Estas aplicaciones crearon una demanda de conexiones seguras.

En 1995, Netscape Communications Corp, el entonces fabricante líder de navegadores, respondió a esta demanda con un paquete de seguridad llamado SSL (Capa de Sockets Seguros). En la actualidad, este software y su protocolo se utilizan ampliamente, incluso por Internet Explorer.

SSL construye una conexión segura entre los dos sockets, incluyendo

1. Negociación de parámetros entre el cliente y el servidor.
2. Autenticación tanto del cliente como del servidor.
3. Comunicación secreta.
4. Protección de la integridad de los datos.

En la figura 2.22 se ilustra la posición de SSL en la pila de protocolos usuales. Efectivamente, es una nueva capa colocada entre la capa de aplicación y la de transporte, que acepta solicitudes del navegador y enviándolas al TCP para transmitir al servidor. Una vez que se ha establecido la conexión segura, el trabajo principal de SSL es manejar la compresión y encriptación. Cuando HTTP se utiliza encima de SSL, se conoce como HTTPS (HTTP Seguro), aunque es el protocolo HTTP estándar. Sin embargo, algunas veces está disponible en un nuevo puerto (443) en lugar de en uno estándar (80). Además, SSL no está restringido a utilizarse sólo con navegadores Web, pero ésa es la aplicación más común.

Figura 2.22. Capas (y protocolos) para una navegación de usuario doméstico con SSL.

SSL soporta una variedad de algoritmos y opciones diferentes. Entre dichas opciones se incluyen la presencia o ausencia de compresión, los algoritmos criptográficos a utilizar y algunos asuntos relacionados con la exportación de restricciones en la criptografía. La última es la destinada principalmente para asegurarse de que se utilice criptografía seria sólo cuando ambos lados de la conexión estén en los Estados Unidos

SSL consiste en dos subprotocolos, uno para establecer una conexión segura y otro para utilizarla. En la figura 2.23 se muestra el subprotocolo de establecimiento de conexión.

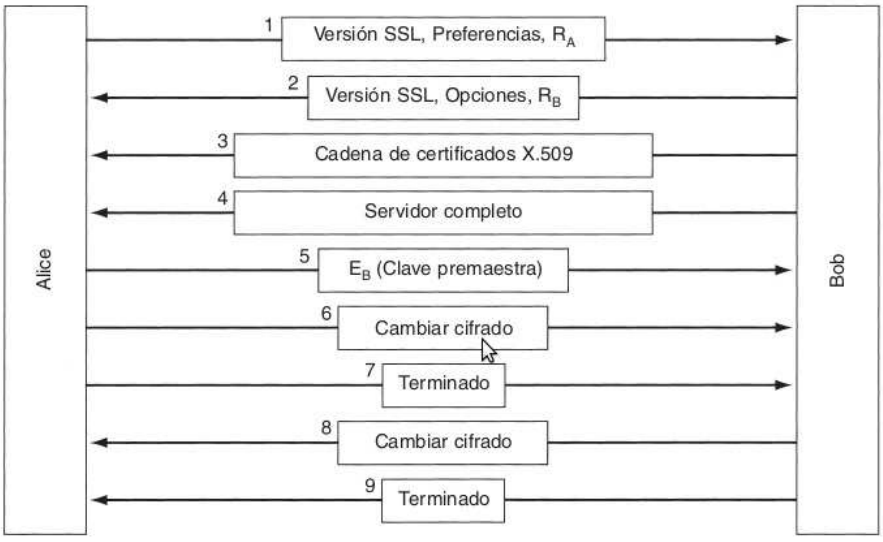


Figura 2.23. Una versión simplificada del subprotocolo de establecimiento de conexión SSL.

SSL soporta múltiples algoritmos criptográficos. El más robusto utiliza triple DES con tres claves separadas para encriptación y SHA-1 para la integridad de mensajes. Para las aplicaciones comunes de comercio electrónico, se utiliza RC4 con una clave de 128 bits para encriptación y MD5 se utiliza para la autenticación de mensajes. RC4 toma la clave de 128 bits como semilla y la expande a un número mucho más grande para uso interno. Después utiliza este número interno para generar un flujo de claves. Las versiones de exportación también utilizan RC4 con claves de 128 bits, 88 de los cuales se hacen públicos para que el cifrado sea fácil de romper.

Para un transporte real se utiliza un segundo subprotocolo, como se muestra en la figura 2.24. Los mensajes que provengan del navegador primero se dividen en unidades de hasta 16 KB. Si se activa la compresión, cada unidad se comprime por separado. Después de eso, se deriva una clave secreta a partir de las dos marcas aleatorias y la clave premaestra se concatena con el texto comprimido y al resultado se le aplica un hash con el algoritmo de hash acordado (por lo general MD5). Este hash se agrega a cada fragmento como el MAC. Después, el fragmento comprimido y el MAC se encriptan con el algoritmo de encriptación simétrico acordado (por lo general, aplicándole un OR exclusivo con el flujo de claves RC4). Por último, se agrega un encabezado de fragmento y el fragmento se transmite a través de la conexión TCP.

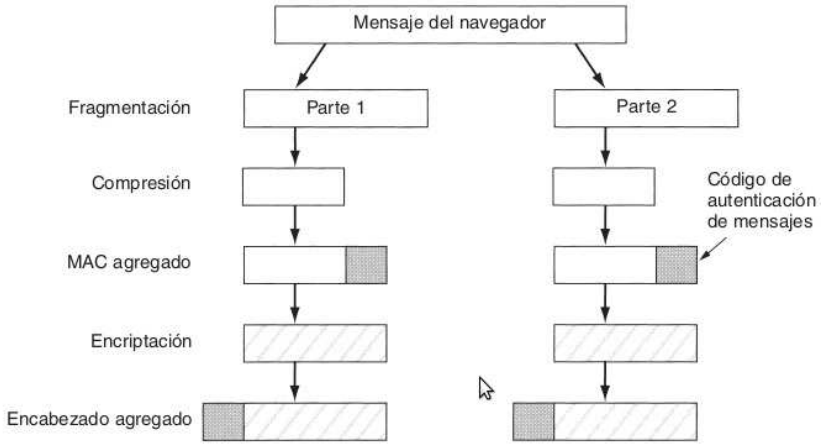


Figura 2.24. Transmisión de datos mediante SSL.

Sin embargo, es necesaria una advertencia. Puesto que se ha mostrado que el RC4 tiene claves débiles que pueden criptoanalizarse con facilidad, la seguridad de SSL mediante RC4 no es muy confiable (Fluhrer y cols., 2001). Los navegadores que permiten que el usuario elija el conjunto de cifrado deben configurarse para utilizar todo el tiempo triple DES con claves de 168 bits y SHA-1, aunque esta combinación es más lenta que RC4 y MD5.

En conclusión, en el marco teórico realizado en el presente trabajo, se abordan diversos temas vistos en los diversos módulos que integran el “Diplomado Integral de Telecomunicaciones” y que sirvieron como fundamentos para poder diseñar la propuesta que da solución a la problemática planteada por el Nacional Monte de Piedad: Dar salida a Internet a las aplicaciones PeopleSoft.

3. Conceptualización y modelado.

3.1 Entendimiento de la situación actual del sistema PeopleSoft.

Es importante conocer cómo es que el Monte de Piedad trabaja con el sistema Peoplesoft, ya que al tener clara la situación actual, Se pueda definir claramente de qué manera se integrará la solución planteada y los beneficios que su implementación traerán.

3.1.1 Entendimiento general.

Actualmente el Nacional Monte de Piedad tiene implementado PeopleSoft como la plataforma para comunicar las áreas funcionales de la empresa (contabilidad, compras, inventarios, recursos humanos, donativos, etc.), dicha herramienta es operada dentro de las instalaciones de la institución. Se requiere que la herramienta pueda ser utilizada en cualquier momento fuera de las instalaciones, con esta funcionalidad se pretende aumentar la eficiencia de los servicios.

- El sistema PeopleSoft Soluciones de Portal, PeopleSoft Finanzas y PeopleSoft Recursos Humanos, actualmente son utilizados por el siguiente tipo de audiencia: Empleados.
- Los empleados se encuentran ubicados en diferentes lugares de la República Mexicana.
- Cualquier usuario físicamente fuera de casa matriz requiere de un cliente de VPN para utilizar la aplicación.
- No existe una sólida estructura de seguridad.
- Proveedores deben de pasar por un proceso largo para cobrar pagos, abastecer productos.
- El procedimiento para la instalación del cliente de VPN puede durar varios meses.

Lo que se propone para poder dar acceso a internet a la aplicación PeopleSoft de manera segura y fácil, es utilizar una VPN SSL, es una red privada virtual (VPN) basada en SSL (Secure Sockets Layer) que promete una mayor sencillez a la hora de crear conexiones seguras por Internet, presente en la gran mayoría de navegadores Web, también promete ahorrar a los usuarios tiempo de administración al apoyarse en un hardware más fácilmente configurable y requerir poco o ningún software en las máquinas remotas.

Una VPN SSL puede tratar la mayor parte del tráfico que el resto de redes privadas virtuales. Y, al final, como siempre, todo dependerá de las funciones específicas de cada organización.

El protocolo SSL (utilizado en las transacciones monetarias por Internet) está presente en una gran mayoría de los PC corporativos dotados de navegadores Web. Para que estas máquinas remotas trabajen con VPN SSL no requieren ni software adicional ni mantenimiento. Además, SSL ofrece encriptación de 168 bits, la misma que la encriptación Triple-Des utilizada por IPSec.

Las nuevas firmas basan sus soluciones en la instalación de servidores entre esos PC remotos y el servidor de la LAN corporativa. Este servidor intermediario establece una conexión SSL en la máquina remota, dando a ese enlace Web un enlace al servidor de datos, haciendo accesible la red de la empresa desde Internet. El tráfico Web seguro llega a través del firewall corporativo por un único puerto SSL que puede ser configurado para que sólo permita acceder al servidor intermediario.

Esta solución tiene la ventaja de una mayor simplicidad y menos costos de mantenimiento, sin embargo, los productos no son tan baratos.

En general, esta solución tiene puntos fuertes y debilidades, pero es adecuada para aportar a NMP de enlaces a Internet seguros para compartir datos con sus usuarios comerciales. Incluso pueden ser muy útiles como sistema de respaldo.

NMP puede simplificar la creación de enlaces Internet seguros utilizando los nuevos productos que explotan el protocolo SSL ya presente en los navegadores, sin necesidad de instalar hardware VPN IPSec.

1- Un usuario remoto teclea la URL de un servidor proxy/SSL situado tras el firewall corporativo.
2- El usuario, una vez autenticado, recibe una lista de recursos disponibles.
3- El servidor SSL/proxy facilita la comunicación entre los servidores de aplicaciones y el usuario remoto.

Las ventajas de utilizar esto son:

- Se utiliza con un buscador Web estándar
- No requiere instalación de software especial en terminales
- Acceso a aplicaciones Web y conexiones de red interna de manera remota
- Mecanismo SSL para comunicación segura
- Bajo costo de mantenimiento

- Fácil administración

3.1.2 Seguridad.

Dentro de la topología de red distribuida del Nacional Monte de Piedad, actualmente no existe interacción entre sistema PeopleSoft con el exterior (Internet), es decir, la comunicación de los servidores de la PIA (PeopleSoft Internet Architecture) se da solo en la intranet. Finalmente, la seguridad para el acceso al sistema PeopleSoft es gobernada por el SD (Servicio de Directorio) AD (Active Directory) de Microsoft.

El siguiente grafo muestra la forma en la que AD interactúa con la PIA de PeopleSoft.

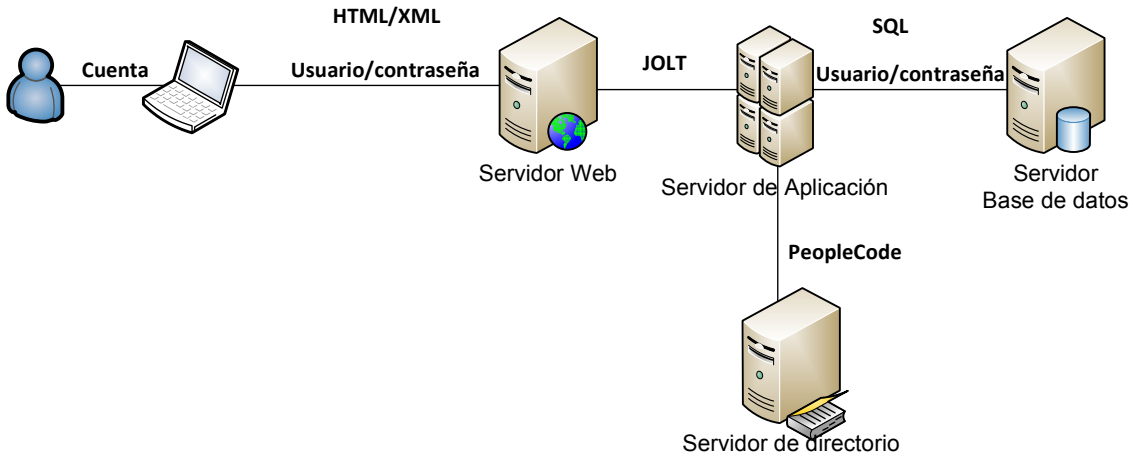


Figura 3.1. PIA PeopleSoft.

3.2 Requerimientos.

1. Dar acceso a través de internet a la aplicación PeopleSoft.
- 1.1 Infraestructura.
- 1.2 Redundancia
- 1.3 Seguridad.

3.3 Modelado.

Como resultado del análisis de las necesidades de Nacional Monte de Piedad se ha determinado que el siguiente diagrama es una representación gráfica del estado futuro de la red que le dará salida a la aplicación PeopleSoft.

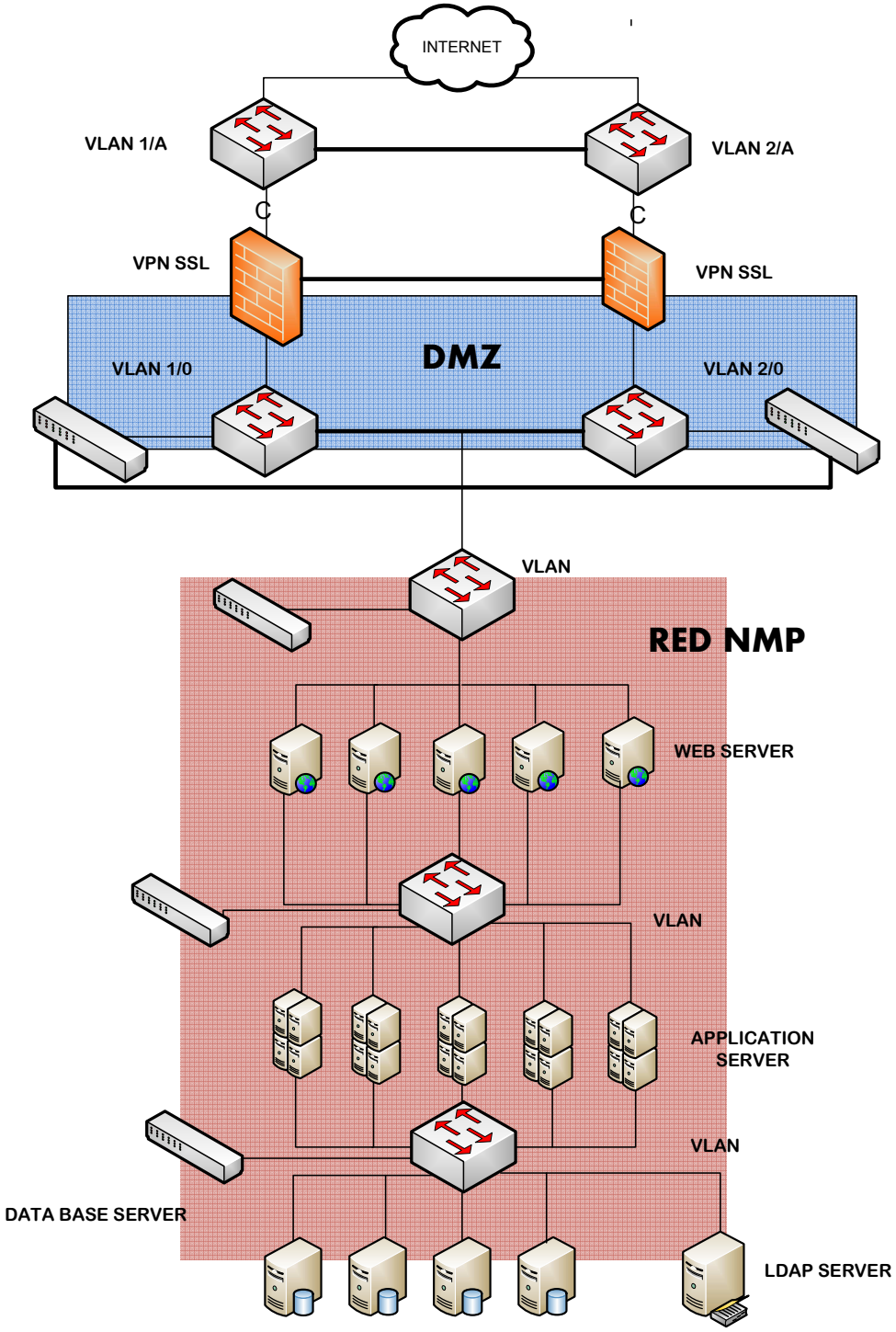


Figura 3.2. Modelo de red NMP.

4. Análisis y Diseño

El éxito de cualquier implementación consiste en poder brindar una solución acorde a las necesidades del cliente. El análisis nos permite tener una definición clara de las necesidades del cliente y el diseño, además de crear la solución acorde a esas necesidades. De ahí la importancia de estas etapas dentro del desarrollo de cualquier implementación.

4.1 Descripción de Requerimientos.

Las necesidades particulares para esta implementación están clasificadas en los aspectos relevantes para el requerimiento del Nacional Monte de Piedad, los cuales son: Infraestructura, Redundancia y Seguridad.

Requerimiento: Dar acceso a través de internet a la aplicación PeopleSoft. (Medios para dar acceso)

4.1.1 Infraestructura

A continuación se presenta una lista de componentes a utilizar durante la etapa de implementación de la red.

Componentes a considerar para el sistema:

- Conectividad de Internet.
- Ubicación física
- Routers.
- Switches/VLANS.
- Servidor VPN SSL.
- Balanceadores de carga (Reverse Proxy Servers).
- Servidores.
- Aplicación.
- Almacenamiento (Storage).
- Fuentes de alimentación.
- Planes de recuperación de desastres.
- IP Virtuales.
- IPs Homologadas.
- IPs No homologadas.
- Network Address Translation (NAT)
- Ubicación física para los componentes

4.1.2 Redundancia

Esta arquitectura planteada, maneja un esquema redundante de equipos para ofrecer una alta disponibilidad en caso de falla de algún dispositivo de red. Para ello se cuenta con un enlace dedicado con dos puntas RJ-45, dos switches, 2 equipos VPN SSL, y dos balanceadores de carga.

La configuración redundante de estos equipos se maneja en un esquema activo/pasivo, esto quiere decir que solo una punta del enlace, un switch, un equipo VPN SSL y un balanceador está funcionando y se denomina equipo activo, mientras que su contraparte permanece sin funcionar, como equipo pasivo, y solo entrará en funcionamiento si detecta que el equipo activo falla.

Para explicar el funcionamiento del diagrama, tomaremos el flujo a través de los equipos activos, ya que los dispositivos pasivos solo entran en caso de falla y cambiando su rol a activo.

El switch tiene configurado 2 VLAN, una de ellas tiene el segmento de direcciones IP homologadas donde en uno de sus puertos está conectado la punta del enlace dedicado, en otro puerto se conecta una de las interfaces del equipo VPN SSL.

En la Otra VLAN se tiene el segmento de direcciones IP no homologadas de la red en donde en uno de sus puertos tiene conectado el equipo VPN SSL, en otro puerto el balanceador y un último puerto donde se conecta un cable que permite la comunicación con un switch que alcance la red donde se encuentran los equipos con las aplicaciones PeopleSoft.

4.1.3 Seguridad

El Equipo VPN SSL permite que mediante un mecanismo de NAT, la comunicación de la red privada con Internet debido a que tiene puertos conectados en ambas VLAN's del switch. En este equipo se crean cuentas VPN para que los usuarios puedan conectarse a las aplicaciones PeopleSoft. También en este equipo se crea un pool de direcciones IP no homologadas, y cada vez que un usuario se conecte, se le asigna una dirección IP de dicho pool.

Dentro del mismo equipo se configuran los permisos que tienen los clientes que usen las direcciones IP del pool, para que se conecten solo a las direcciones IP virtuales que publica el equipo balanceador de carga, ya que solo podrán acceder a las aplicaciones a través de él.

El balanceador de carga también realiza las funciones de Proxy inverso, cache y aceleración Web. Este equipo se conecta a los servidores donde se encuentran las aplicaciones PeopleSoft y enmascara los servicios para que los usuarios lo consulten usando direcciones IP virtuales, por lo cual se configura para asociar las direcciones IP con las direcciones IP de los servidores donde se encuentran las aplicaciones PeopleSoft.

4.2 Ingeniería y diseño detallado de los requerimientos.

A continuación se hace una descripción más detallada de los elementos que formar parte de la implementación para dar solución a la problemática planteada, los cuales están clasificados en elementos de Infraestructura, redundancia y Seguridad.

NOTA: Las especificaciones técnicas de todos los equipo se encuentran en el Anexo A

4.2.1 Infraestructura

Requerimiento 1: Dar acceso a través de internet a la aplicación PeopleSoft. (Medios para dar acceso).

Ancho de Banda del enlace.

El ancho de banda promedio por usuario se estimo en 20 Kbps, teniendo en cuenta que se proyecta un máximo de 250 usuarios concurrentes, se requiere un enlace de 5Mbps para soportar la demanda en horas de mucha actividad. Aunque se recomienda tener un margen adicional del 10% para garantizar que no se sature dicho enlace proyectando crecimiento a mediano plazo.

Router.

Permitirá el acceso a todos los clientes externos a las aplicaciones PeopleSoft, asegura el enrutamiento de paquetes entre redes y determinar la ruta que debe tomar el paquete de datos. El Router ira conectado a través de fibra óptica al proveedor de servicio de internet. Sin embargo **NO** será parte de nuestra estructura, ni lo elegiremos nosotros, ya que estará dentro de la arquitectura del proveedor del enlace y éste nos entregará la salida que se conectará al switch y la dirección IP del Gateway.

Switch.

El switch servirá para la conexión de VLANs. Gracias al switch de nivel 3 se podrá gestionar la visibilidad entre las distintas VLAN y habrá una mejora en el rendimiento de la red ya que las broadcast de cada VLAN sólo llegarán a los equipos conectados a la misma. Los switches irán conectados al Gateway, al servidor VPN SSL y a los balanceadores de carga. Y se utilizará un SLM224G4S el switch Cisco SLM224G4S ofrece:

- La interfaz de configuración basada en navegador de este dispositivo elimina la complejidad del proceso de configuración.
- Obtiene datos de alto consumo de ancho de banda donde se necesitan con rapidez y sin errores.
- Protege los datos en la red contra el acceso no autorizado. Las funciones de seguridad avanzada, cifrado y autenticación mantienen alejados a los intrusos.
- Proporciona funciones de calidad de servicio y Power over Ethernet, entre otras, que facilitan la ampliación de las implementaciones de red avanzadas.
- Diversas opciones de puertos Fast Ethernet y Gigabit Ethernet.
- La función opcional Power over Ethernet, suministra energía con facilidad a los puntos de acceso inalámbrico, videocámaras y otros puntos terminales conectados a la red, con lo cual se reducen los costos, ya que se elimina la necesidad de instalar fuentes de alimentación independientes.
- Clúster flexibles, que permiten controlar los switches presentes y futuros mediante una sola interfaz común.
- Funcionalidad de seguridad que utiliza mecanismos de autenticación y filtrado avanzado para eliminar la amenaza de accesos no autorizados a la red.
- La seguridad protege el tráfico de la red para evitar el ingreso de usuarios no autorizados.

Modelo y uso		**Puertos disponibles**
	**SLM224G4S** • Conecte hasta 24 dispositivos en red (PC, impresoras, puntos de acceso y servidores) para compartir y transferir archivos y vídeos por la red • La tecnología de apilamiento flexible le	24 10/100, 4 10/100/1000 con 2 miniGBIC combinados

	permite administrar varios switches desde un solo menú de configuración	

Tabla 4.1 Especificación Switch.

Servidor VPN SSL

Citrix Access Gateway nos ayudará a dar acceso solo a las VPN SSL, es un dispositivo VPN SSL capaz de conceder acceso seguro a cualquier aplicación, con control basado en políticas SmartAccess. Proporciona a sus usuarios acceso seguro y sencillo a todas las aplicaciones y datos que necesiten para ser productivos y amplíe de manera rentable el acceso a las aplicaciones, manteniendo al mismo tiempo la seguridad mediante políticas a nivel de aplicación.

Access Gateway, hace frente con una buena relación calidad-precio a las demandas de acceso de trabajadores situados en cualquier punto. Esto permite aprovechar opciones de trabajo flexibles, facilita la externalización de servicios y el acceso de los no-empleados, permite mantener la continuidad de las operaciones y la disponibilidad de los recursos garantizando al mismo tiempo el más alto nivel de seguridad para la información.

- Su acceso “always-on” (siempre conectado) vuelve a conectar al usuario, sin interrupciones y automáticamente, cuando cambia de ubicación geográfica o de dispositivo, o si pierde la conectividad, reduciendo la sensación de frustración y mejorando la productividad.
- Su página de inicio basada en web otorga acceso fácil y rápido a recursos clave, permitiendo al usuario escoger entre una amplia variedad de dispositivos, incluyendo terminales portátiles.
- Su sistema integrado de comprobación de la seguridad del punto terminal garantiza que los dispositivos reúnen los criterios definidos por el administrador antes de conectarse a la red corporativa.
- El lector de punto terminal trabaja en tandem con Citrix® SmartAccess, que utiliza funcionalidades de “respuesta inteligente” no sólo para conceder o denegar el acceso a las aplicaciones, sino también para controlar las acciones de los usuarios, especificando qué les está permitido hacer con la información.
- Simplifica la administración y reduce costos.

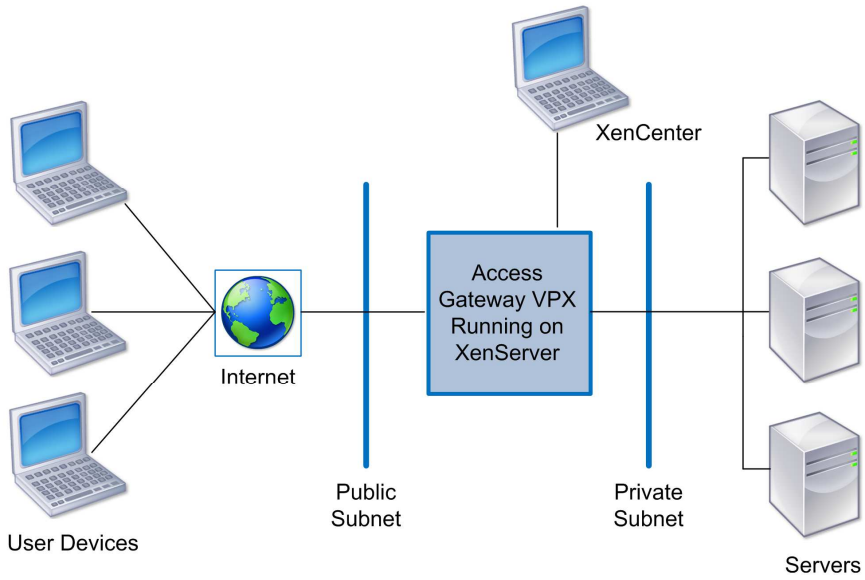


Figura 4.1 Conexión Gateway.

Balanceador de Carga.

Se requerirán de balanceadores de carga para la redundancia de los servicios. Dispositivo que se colocará al frente de un conjunto de servidores Web Logic que atienden una PeopleSoft, estos equipos asignan o balancean las solicitudes que llegan de los clientes a los servidores.

Figura 4.2 Balanceador de carga.

Como balanceador de carga proponemos un Citrix NetScaler que es un dispositivo de entrega de aplicaciones Web que acelera el rendimiento, proporciona administración de tráfico de niveles 4 a 7, ofrece un servidor de seguridad de aplicaciones integrado, y libera de cargas a los

servidores para garantizar la disponibilidad de las aplicaciones, mayor seguridad y una reducción sustancial de los costos. Reduce el costo total de propiedad (TCO) de la entrega de aplicaciones Web, optimiza la experiencia del usuario y hace que las aplicaciones se ejecuten cinco veces mejor.

Combina balanceo de carga y conmutación de contenido de alta velocidad con aceleración de aplicaciones, compresión de datos, almacenamiento de contenido en caché, aceleración SSL, optimización de redes y supervisión del rendimiento de las aplicaciones. A diferencia de otros enfoques que requieren múltiples productos puntuales, NetScaler es un dispositivo todo en uno, fácil de implementar y operar.

- Alivia la carga de redes sobrecargadas.
- Entrega más aplicaciones a mayor cantidad de usuarios con una notable reducción de los servidores y dispositivos de red, por lo tanto reducción de costo.
- Permite implementar nuevas aplicaciones Web 2.0 sin la necesidad de realizar cambios masivos en la infraestructura.
- Acelera el rendimiento de las aplicaciones Web hasta cinco veces o más.
- Envía el tráfico al servidor correcto con conmutación inteligente de contenido y aprovecha la compresión avanzada de múltiples niveles para lograr el mejor rendimiento posible y el mayor ahorro en ancho de banda de la red.
- El almacenamiento en caché de contenido dinámico entrega de manera instantánea el contenido solicitado con mayor frecuencia directamente desde NetScaler para mejorar aún más la experiencia del usuario.
- Bloquea los ataques y protege la información confidencial del acceso no autorizado. Evitando la pérdida de datos valiosos de las empresas y los clientes.
- Colaboran con el cumplimiento de normas como el estándar de seguridad de datos de la industria de pago con tarjetas PCI-DSS.
- Tiene capacidades integrales de autenticación, autorización y administración (AAA), combinadas con una poderosa protección contra ataques de negación de servicio (DoS), permiten el acceso remoto seguro y al mismo tiempo evitan el acceso no autorizado a la información confidencial.
- Proporciona detección y respuesta de sobrecarga para optimizar el uso de los recursos del servidor aun con tráfico impredecible. Al activar la capacidad on-demand, se reasignan los recursos automáticamente y se agregan o sustraen las capacidades del servidor en respuesta al volumen de tráfico sin interrumpir la aplicación o al usuario de la aplicación.
- El balanceo de carga de los niveles 4 a 7 garantiza un tiempo productivo del 100 por ciento para todos los usuarios y asegura que no haya ningún punto de falla.

- El Balanceo de carga global de servidores (GSLB) garantiza que las aplicaciones estén disponibles para los usuarios en todo el mundo y constituye un elemento clave para las estrategias de recuperación ante desastres.

Servidores

Los Servidores estarán conectados como se encuentran actualmente en Nacional Monte de Piedad a un switch, no se planea hacer modificaciones a esa sección de la red. Se conectará el switch al que están conectados los servidores al Switch de la DMZ.

Son 5 Servidores Windows para el Web Server.

- 5 servidores Windows para el Application Server.
- 4 servidores Windows para las bases de datos
- 1 para el LDAP.

Aplicación.

PeopleSoft es la aplicación que se desea tener acceso fuera de las instalaciones de la casa Matriz del Nacional Monte de Piedad. PeopleSoft es un ERP como la plataforma para comunicar las áreas funcionales de la empresa (contabilidad, compras, inventarios, recursos humanos, donativos, etc.), dicha herramienta es operada dentro de las instalaciones, su arquitectura es la siguiente:

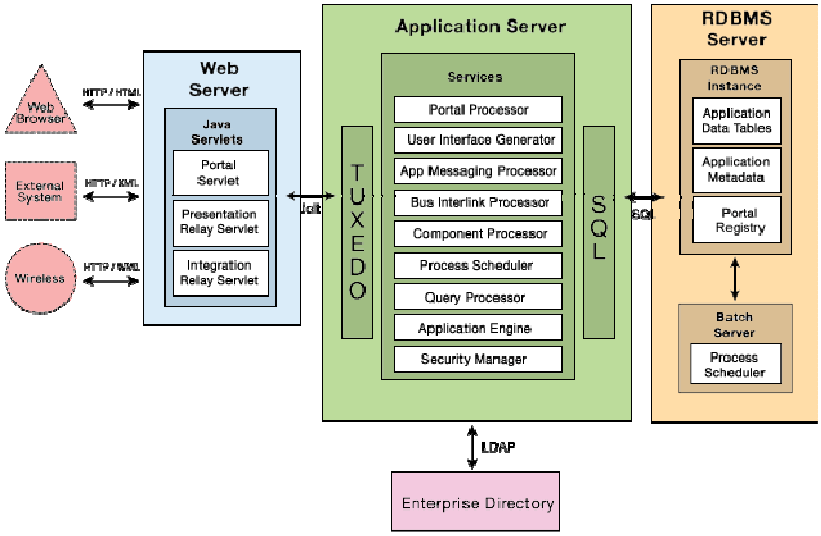


Figura 4.3 Arquitectura PeopleSoft.

Almacenamiento (Storage).

El almacenamiento de Nacional Monte de Piedad consta de:

- 4 servidores Windows para las bases de datos. (2 Servidores para las bases de datos de Finanzas y Portal y 2 Servidores de bases de datos para Recursos Humanos),
- 1 Servidor para el LDAP.

Fuentes de alimentación.

Requerimos fuentes de alimentación para los diferentes equipos de nuestra arquitectura con las que podamos garantizar el buen funcionamiento de los equipos, también para asegurar la disponibilidad del servicio, y para evitar fallas por la mala energía. Para saber la energía total necesaria tomaremos en cuenta los consumos de los equipos nuevos implementados para saber si es suficiente con la alimentación que ya se tiene.

Los consumos de energía total de cada uno de los equipos se muestran a continuación.

1. Switch SLM224G4S

Input Voltage	Input Current	Maximum Power	Heat DisipationBTU/hr
100 – 240 V	1.45 A @ 115 V 0.65 A @ 220 V	160 W	512 BTU/hr

2. Citrix Access Gateway VPX2000

Input Voltage	Input Current	Maximum Power	Heat DisipationBTU/hr
100 – 240 V	3 A	190 W	648 BTU/hr

3. Netscaler **VPX-200**

Input Voltage	Input Current	Maximum Power	Heat DisipationBTU/hr
90 – 264 V	ND	335 W	ND

Planes de recuperación de desastres.

El objetivo es evitar la negación del servicio, que siempre esté disponible para los usuarios, sin importar los problema que se pueden presentar, esto se logra a través de la creación de políticas en donde se especifique los procedimiento que se tienen que realizar para asegurar el servicio, también procedimientos para prever posibles fallas , un ejemplo de éste caso es incluir en el diseño redundancia como es nuestro caso o incluir algún respaldo, también la elección del equipo óptimo que cumpla las necesidades del cliente y que garantice disponibilidad y protección.

Los planes de recuperación de desastres DRP) cubren desde lo más sencillo a lo más complejo, dependiendo de las necesidades y las amenazas potenciales.

IP's Virtuales

Las direcciones IP Virtuales (VIP) se utilizaran en el equipo balanceador de carga de tal manera que enmascaren las direcciones IP de los servidores, de esta manera los clientes nunca tienen acceso directo a los servidores, y en caso de que se agreguen mas servidores para realizar un balanceo, o se llegue a cambiar, para el usuario será transparente.

IPs Homologadas.

Para la implementación de esta solución necesitaremos 2 IP´s homologadas, para que desde cualquier navegador se pueda acceder al servicio, una IP se ocupa para el puerto que va del Switch al Gateway y otra para el puerto del Switch que va al Servidor VPN SSL.

IPs NO Homologadas.

En el caso del resto de la red, se ocuparan ip´s privadas, solo la comunicación será interna, no necesitarán ser reconocidas desde cualquier punto.

NAT

El mecanismo de NAT será utilizado por el equipo VPN SSL para poder establecer la comunicación entre el segmento de direcciones Homologadas y no homologadas. El equipo

balanceador de carga utiliza NAT para poder enmascarar los servicios de las aplicaciones, este NAT se realiza con direcciones privadas del mismo segmento de red.

Ubicación para los componentes.

NMP ya cuenta con su centro de datos, en condiciones para el buen desempeño de los equipos, sólo hay que tomar en cuenta que el espacio requerido que es :

Equipo	Espacio (UR)
Access Gateway	1
Access Gateway	1
NetScaler	2
NetScaler	2
Switch	1
Switch	1

Tabla 4.2 Equipos requeridos.

Menos de la mitad de un Rack por lo que no implicará algún gasto mayor.

4.2.2 Redundancia.

La redundancia consiste en duplicar elementos de la arquitectura u ofrecer alternativas al flujo de la implementación para garantizar el funcionamiento del servicio o aplicación por si alguno de los componentes falla.

En la arquitectura redundante de la DMZ con NAT, la DMZ ocupa un espacio de direcciones de internet privadas y no ruteables. Los balanceadores de carga rutean los paquetes a los servidores Web en la misma red.

La redundancia la utilizaremos en la implementación de la red de Nacional Monte de Piedad para incrementar la fiabilidad y la capacidad de mantenimiento del sistema PeopleSoft. Se utilizará la redundancia por ser un sistema de red con alta disponibilidad. El tipo de redundancia que presentará el sistema es un esquema Activo/Pasivo.

La redundancia consistirá en que los activos redundantes entrarán en servicio cuando se producen fallos. Mientras tanto, están inactivos.

La fiabilidad y capacidad del mantenimiento son factores de la disponibilidad del servicio que se definen en términos de defectos y fallos de uno o más de los activos subyacentes del servicio.

Múltiples canales de servicio incrementar el de nivel de redundancia incrementan la zona de contacto y distribuyen la carga de trabajo en todo el sistema. Podrá mantenerse la calidad del servicio cuando cualquiera de los canales sufra interrupciones o una degradación del rendimiento.

El mantenimiento y la tolerancia a fallas son factores claves para el diseño de una red.

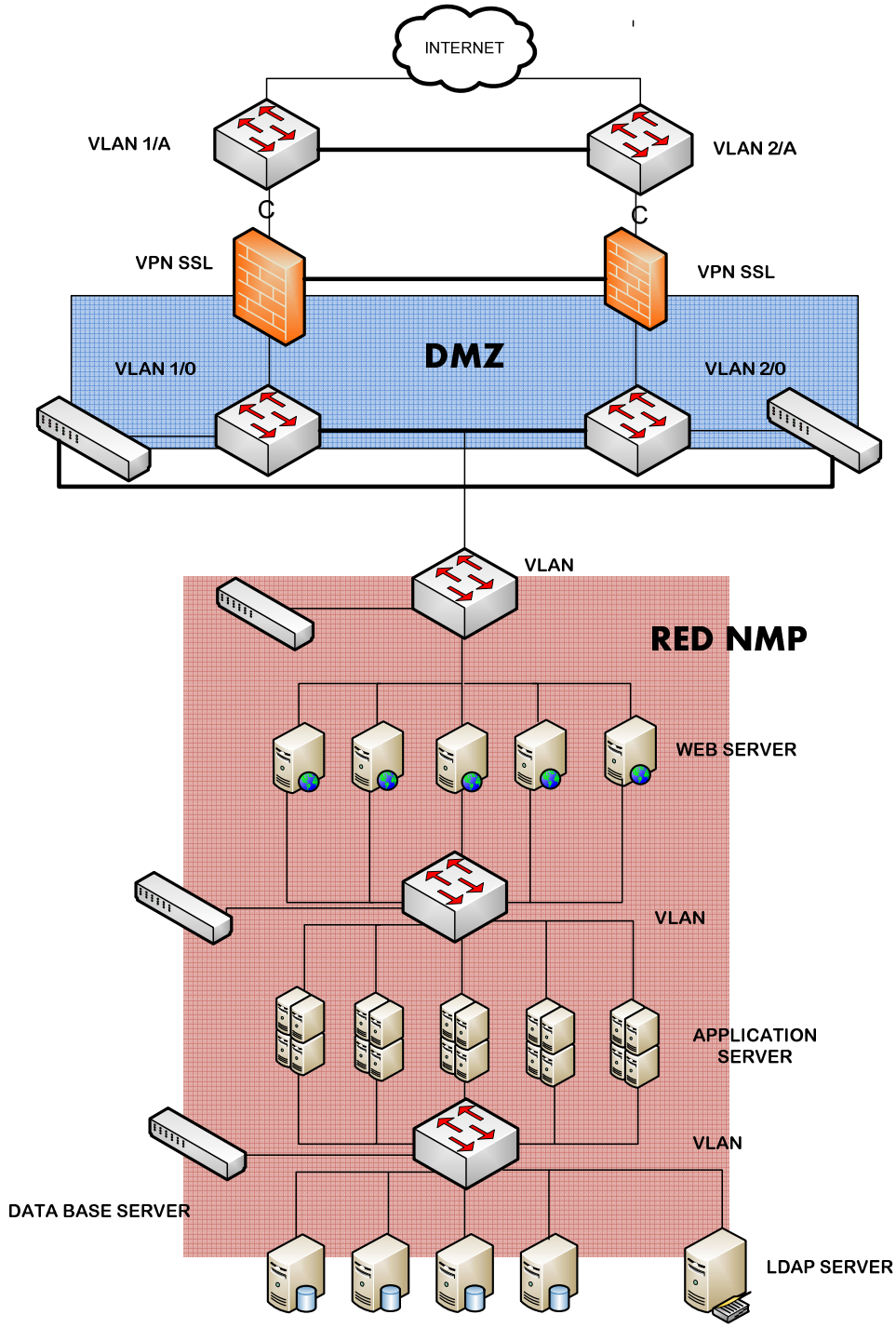


Figura 4.4. Arquitectura para dar salida a una aplicación PeopleSoft.

Alcanzar un alto porcentaje de disponibilidad es simple: alcanza un alto tiempo entre fallas (Mean Time Between Failure MTBF) y un tiempo muy pequeño de reparación de fallas (Mean Time To Repair MTTR). El cálculo es MTBF/(MTBF+MTTR)x100%.

Es vital asegurar que el tiempo medio de reparación (MTTR) de un sistema se mantenga al mínimo si la alta disponibilidad es alcanzada

4.2.3 Seguridad

El otro elemento considerado dentro de la implementación del Nacional Monte de Piedad es lo relacionado a aspecto de protección de la información y mecanismos de seguridad que protejan la comunicación. Es por ello que se hace uso de las siguientes caracterísitcas dentro de la solución:

SSL.

- Protección Web.
- Definiciones de seguridad en la aplicación PeopleSoft.
- Autenticación a las aplicaciones por medio de LDAP.
- Single Sign On.

SSL.

El Monte de Piedad simplifica la creación de enlaces seguros utilizando el protocolo SSL ya que está presente en los diversos navegadores Web del mercado, de esta manera ofrece la misma seguridad sin necesidad de configurar un cliente VPN en cada equipo cliente.

Protección Web.

El equipo Netscaler ofrece protección adicional a las aplicaciones Web, ya que detecta patrones de posibles ataques Web, y puede tomar diversas acciones dependiendo el tipo de amenaza, desde enviar una notificación al administrador de red hasta bloquear el servicio a la dirección IP de donde proviene la amenaza.

Definiciones de seguridad en la aplicación PeopleSoft.

Las tres principales definiciones de seguridad de PeopleSoft son:

- Perfiles de usuario. (Conjunto de datos que describen un determinado usuario de PeopleSoft).
- Roles. (Objetos intermedios que unen los perfiles de usuario a las listas de permisos).
- Listas de permisos. (Conjunto de páginas y de las acciones admisibles en esas páginas).

La jerarquía que se debe seguir para implementar la seguridad de usuario es: Definición de las listas de permiso, seguido por la creación de los papeles y, finalmente, la asignación de estas funciones a los perfiles de usuario.

LDAP.

LDAP es un protocolo de Internet utilizado para acceder a un listado de directorio. Nacional Monte de Piedad almacena perfiles de usuario en un servidor de directorio, que sirve a la información del usuario para PeopleSoft y otras aplicaciones que lo requieran.

Las listas de permisos y roles se mantendrán con la seguridad de PeopleSoft. Sin embargo, los perfiles de usuario son definidos en el servidor de directorio LDAP. En el servidor de directorio se habilita el mantenimiento de un único perfil, el usuario centralizado se puede utilizar en todas las aplicaciones PeopleSoft y no PeopleSoft. Este enfoque reduce el mantenimiento redundante de información de usuario almacenada separadamente a través de la Nacional Monte de Piedad, y reduce la posibilidad de obtener información del usuario fuera de sincronización. Además, permite que los perfiles de usuario sean fácilmente creados, mantenidos y autenticados.

Single Sign On.

PeopleSoft ofrece la solución de autenticación más común. Esto ahorra el trabajo de desarrollo de soluciones y ahorra tiempo con la implementación de seguridad, las soluciones que ofrece PeopleSoft soportan autenticación a través de SSL, autenticación LDAP y Single Sign On. Como las aplicaciones de PeopleSoft están diseñados para el despliegue de Internet, muchos sitios hay que aprovechar de los servicios de autenticación que existen a nivel del servidor web. PeopleSoft se aprovecha de HTTPS, SSL y certificados digitales para garantizar la transmisión de datos desde el servidor web al navegador web del usuario final y también para proteger la transmisión de datos entre servidores de PeopleSoft y servidores de terceros (para el negocio a negocio procesamiento) a través de Internet.

PeopleSoft es compatible con Single Sign On entre las instancias de PeopleSoft. En el contexto del sistema PeopleSoft, el inicio de sesión único (Single Sign On) significa que cuando un usuario ha sido autenticado por un servidor de aplicación de PeopleSoft, este usuario puede acceder a un segundo servidor de aplicaciones de PeopleSoft, sin tener que teclear un login o una contraseña. Aunque el usuario está realmente el accediendo a diferentes aplicaciones y bases de datos, el usuario navega a la perfección a través del sistema.

5. Construcción e implementación.

En esta etapa se hace la integración de todos los elementos definidos, logrando así plasmar en un proyecto real y tangible el requerimiento hecho por el Nacional Monte de Piedad.

Objetivo.

Para la implementación de la red nos debemos asegurar de contar con una plataforma tecnológica que soporte todos los procesos importantes para la operación de Nacional Monte de Piedad. Estos procesos, que de detenerse ocasionarían pérdidas económicas se conocen como operaciones de misión crítica. Y se vinculan, por poner sólo algunos casos, tanto al sistema de compra y venta.

De los componentes tratados en la sección anterior vamos a configurar algunos diseños comunes en los sistemas de PeopleSoft. Los diseños de sistema tendrán escalabilidad, disponibilidad y seguridad. Los supuestos básicos de diseño y las políticas que se han considerado son:

Escalabilidad:

- Sistema debe ser capaz de escala con la demanda tanto como sea posible sin necesidad de cambio de la arquitectura.
- Utilizar equipos estándares siempre que sea posible.
- Escala con solución más rentable.
- El enfoque ha sido sobre todo para lograr mayor escalabilidad para el servidor Web y de appserver niveles.

Disponibilidad:

- El sistema no debe tener ningún punto único de fallo en la arquitectura.
- La mayoría de fallo único no deberá reducir la capacidad del sistema.
- Lo peor error de solo caso no debe reducir la capacidad en más del 50%.
- Cuando hay varias opciones disponibles para la elección de la disponibilidad, el método más sencillo es adoptado.
- Activo/Pasivo es seleccionado en lugar de más compleja Activo/Activo de configuración de la redundancia.
- Energía ininterrumpida como los UPS

La *disponibilidad* de los sistemas se refiere a la probabilidad que un sistema falle durante un tiempo determinado con el correspondiente mantenimiento correctivo*,* la *disponibilidad* es menor al porcentaje de *confiabilidad* de cualquier sistema.

Se construirá un sistema que proporcionará disponibilidad 24x7 con telecomunicaciones superior al 99.999%, es decir servicio de calidad.

La diversidad en equipamiento activo acoplado a los sistemas de transmisión, sugiere la implementación de más rutas de transmisión para evitar la discontinuidad del servicio; esto con el objetivo de aumentar la *confiabilidad* del sistema central y aumentar como consecuencia la *disponibilidad* de las redes de acceso hacia los usuarios.

Seguridad:

- Implementación de una VPN SSL
- El sistema no debe tener ningún punto único de protección en la arquitectura, esto representa una falta de seguridad.
- Por lo menos un nivel de NAT (Network Address Translation) desde la red exterior al nivel de servidor web.
- Las rutas estáticas serán utilizan dentro del sistema siempre que sea posible
- Implementación de Seguridad en la Aplicación PeopleSoft

5.1 Proceso de Implementación.

1. Colocación de equipos de comunicación.
   1.1 Montar Switches en rack.
   1.2 Montar equipo VPN SSL en rack
   1.3 Montar balanceadores de carga en rack.
2. Configuración del switch.
   2.1 Creación de VLANs (Segmento público y privadas).
   2.2 Conectividad con la intranet.
   2.3 Hacer pruebas de conectividad.
3. Configuración del equipo VPN SSL
   3.1 Conexión del equipo VPN SSL al segmento público y privado del Switch.
   3.2 Configuración del NAT.
   3.3 Se hacen pruebas de conectividad y de filtrado de servicios.
4. Configuración del balanceador.

4.1 Creación de nodos, servicios y servidores virtuales.
4.2 Pruebas de conectividad.

5. Configuración de las aplicaciones PeopleSoft.
   5.1 Cambio en direcciones IPs para dar salida a Internet.

Nota. En este proceso ya se tiene relación de direcciones IP para cada dispositivo.

5.2 Pruebas y certificación.

Para validad el correcto funcionamiento se deben realizar diversas pruebas a fin de garantizar y certificar el correcto funcionamiento según las necesidades definidas, para esto se realizarán 2 tipos de pruebas

- Pruebas integrales (conectividad).
- Pruebas de estrés.

Objetivo.

El objetivo de las pruebas es garantizar que los elementos de red que integran la nueva arquitectura puedan comunicarse de manera correcta con los elementos de la red del Nacional Monte de Piedad, para lo cual se realizaran pruebas de conectividad y estrés de acuerdo a la cantidad de usuarios que se tiene dimensionado soportar.

Actividades:

- Verificación que exista comunicación entre los equipos.
- Se hacen pruebas de conexión de los servicios.
- Para probar el Web Logic. Me conecto al URL donde está el servicio
- Al switch hacer pruebas para ver si alcanza el Gateway, y tiene salida a Internet
- Utilización de ping y trace route.
- Verificar tabla ARP con el comando arp -a
- En el equipo VPN SSL prueba para ver si alcanzo el Gateway.
- Utilización de ping y trace route.
- Verificar tabla ARP con el comando arp –a
- Verificación de servicios.

5.3 Operación y diagnostico.

Una vez que el proyecto se haya implantado con éxito, es necesario contar mecanismos que permitan verificar su correcto funcionamiento a lo largo del tiempo, es por ello que se requiere apoyarse en herramientas que ayuden a tener un diagnostico a fin de evitar que la implementación tenga algún problema

Monitoreo y análisis de la red.

El monitoreo permite detectar fallas en los dispositivos y servicios de red, así como el modo en que se están utilizando dichos recursos, de tal manera que permitan al administrador de la red tomar decisiones para garantizar la disponibilidad de la infraestructura de red. Para el proyecto de Nacional Monte de Piedad utilizaremos las siguientes herramientas:

MRTG

(Multi Router Traffic Grapher) es una herramienta que se utiliza para supervisar la carga de tráfico de interfaces de red. MRTG genera un informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo.

La herramienta utiliza el protocolo SNMP (Simple Network Management Protocol). Este protocolo proporciona la información en crudo de la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida. Esta cantidad bruta deberá ser tratada adecuadamente para la generación de informes

Esta herramienta puede instalarse en ambientes Windows/Linux, Los pre-requisitos son que se tenga instalado el lenguaje PERL y un Servidor Web donde publicar los resultados . La propuesta incluirá la instalación de esta herramienta para monitorear el consumo de ancho de banda de los distintos dispositivos en la red, como son Switches, Equipo VPN SSL, Balanceadores y Servidores.

http://oss.oetiker.ch/mrtg/

WMI Monitor

Las funciones de WMI (Windows Management Instrumentación) son un componente importante para la administración de sistemas Windows . Permiten, además, una monitorización detallada de estos entornos, WMI Monitor es una herramienta para monitorear el desempeño y

disponibilidad de los servidores Windows así como de sus aplicaciones, es una herramienta gratuita ideal para ambientes Windows.

http://www.solarwinds.com/register/index.aspx?Program=937&c=70150000000Ezdb

AWStats

Es una poderosa herramienta que genera estadísticas avanzadas de manera gráfica, Analiza las bitácoras de servidores Web y es compatible con WebLogic, por lo que se podrán generar reportes diarios sobre la utilización de PeopleSoft.

http://awstats.sourceforge.net/

5.4 Mejora Continua

Se propone un sistema y un procedimiento de mejora continua en la implementación y operación del sistema, creemos que este punto es importante para garantizar a nuestro cliente que tendrá la mejor solución a su problema y garantizar que con ayuda de nuestra tecnología siempre será capaz de mantener el servicio, poder dar acceso remoto a las aplicaciones PeopleSoft de Nacional Monte de Piedad con gran eficiencia y muy buena calidad.

Para lograr éste punto proponemos:

- Actualizaciones de Software de manera continua.
- Monitoreo constante del número de usuarios que hacen uso de éste servicio, para asegurar que la infraestructura sea capaz de soportar a tal número.
- Hacer mantenimiento preventivo en los equipos para evitar las fallas y que el rendimiento sea el adecuado.
- Evitar mantenimiento correctivo.
- Con ayuda de las herramientas de monitoreo ver la eficiencia de la red para ver que la eficiencia aumente, poder medirla y a la vez tener control sobre ella.

Para asegurar que se lleve a cabo se realizará un programa con dichas actividades, en donde se especifique las fechas, los procedimientos detallados que se tendrán que realizar.

5.5 Costos.

Uno de los aspectos importantes para el éxito de la implementación, es que los recursos necesarios se encuentren dentro del presupuesto asignado por el Nacional Monte de Piedad, para ello se evaluaron distintos equipos de diversos proveedores a fin de encontrar los elementos que mejor se adapten en una relación costo-beneficio. De ello, se desprende la siguiente relación de equipo de comunicaciones y enlace dedicado requerido, así como el costo asociado a su adquisición.

Equipo de Comunicaciones

Producto	Cantidad	Precio unitario	Total
Switch 24 Puertos CISCO SLM224G4S	2	$5,300	10,600
Citrix Access Gateway 2000	2	$25,350	$50,700
NetScaler VPX-200	2	$65,000	$130,000
Costo Total			191,300

Enlace Dedicado 5 Mbps

Costo de Instalación	$20,000
Renta Mensual	$10,000
Costo Total Primer Año	$140,000

* Precios expresados en pesos mexicanos sin IVA

5.6 Cronograma General del Proyecto.

Para desarrollar todas las actividades involucradas en este proyecto se contempla un total de 12 semanas, dividida en diferentes etapas, las cuales se ejecutaran de acuerdo al siguiente cronograma:

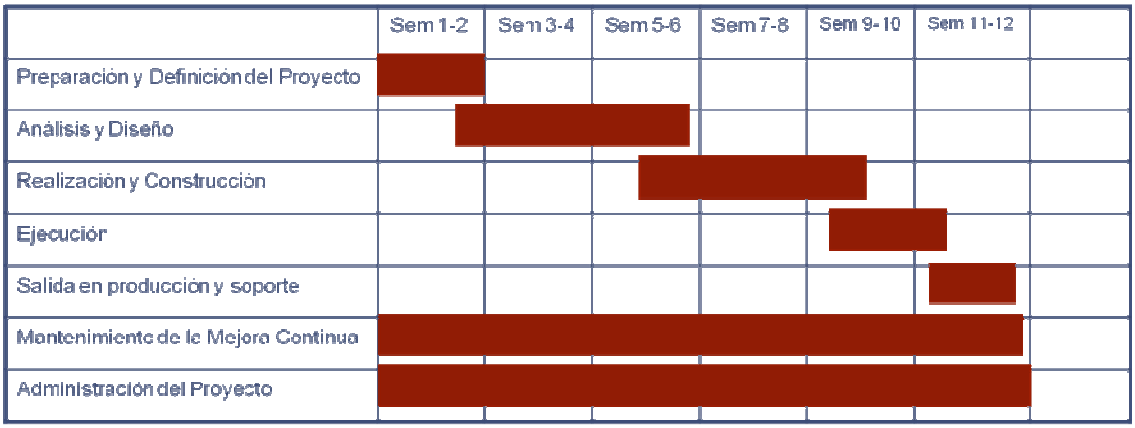


Figura 5.1 Cronograma.

Conclusiones.

La adopción de la arquitectura de acceso a la aplicación PeopleSoft mediante el uso de VPN SSL, permitirá al Monte de Piedad administrar de manera más fácil, eficiente y con el mismo nivel de seguridad, a los diversos usuarios que la utilizan.

Al tener los dispositivos de conectividad en un esquema redundante, se ofrece una alta disponibilidad de acceso a las aplicaciones, ya que al detectarse una falla en algún equipo de comunicación, existe en espera, un equipo idéntico al de la falla, que ahora toma el control de manera transparente, de tal manera que los clientes nunca perciben la falla.

Con la adopción de técnicas como el Single Sign On se agiliza el acceso a usuarios de una forma homogénea y segura a las aplicaciones.

A pesar de que podría parecer como si tecnologías como el IPS e IDS pudiera reemplazar a los firewall, hay que tener en cuenta que cada tecnología proporciona un nivel mayor de seguridad

Nacional Monte de Piedad pueden simplificar la creación de enlaces de Internet seguros utilizando los nuevos productos que explotan el protocolo SSL, el cual está presente en los navegadores sin necesidad de instalar hardware VPN IPSec.

Por ejemplo:

1. Un usuario remoto teclea la URL de un servidor proxy/SSL situado tras el firewall.
2. El usuario, una vez autenticado, recibe una lista de recursos disponibles.
3. El servidos SSL/proxy facilita la comunicación entre los servidores de aplicaciones y el usuario remoto.

Como parte de mis conclusiones personales quiero manifestar que el área de las telecomunicaciones es muy extensa sin embargo a través del Diplomando Integral de telecomunicaciones pude abarcar el estudio de cada una de ellas; en el presente trabajo tuve que limitar su estudio para poder aplicar los conceptos de un problema específico. Esto último es lo que se me complicó más en el desarrollo del proyecto: Poner límite, no obstante es lo que me causo la mayor satisfacción personal una vez encontrado.

Gracias al Diplomado y a los profesores que lo imparten pude mejorar mis habilidades en la toma de decisiones, comprendí la teoría de las telecomunicaciones, por ejemplo como viaja la señal por un cable, por el aire, conceptos, como asegurar las redes, elegir equipo de

telecomunicaciones según su aplicación, etc. Además a través de este ejercicio práctico desarrollé la planeación de un proyecto en el área de telecomunicaciones.

La propuesta me ha dejado grandes satisfacciones personales, y ha sembrado en mí la inquietud de estudiar Administración de Proyectos.

Glosario.

Ancho de Banda. Capacidad máxima de un medio de transmisión y/o enlace.

ERP. (Enterprise Resource Planning). El ERP es una herramienta que ayuda a integrar todos los procesos del negocio y a optimizar los recursos disponibles.

Balanceador. Es un dispositivo o programa que distribuye la carga de trabajo entre los servidores réplicas para lograr la velocidad máxima posible sirviendo páginas. Incluso, si por alguna razón uno de los servidores réplica tiene una avería y deja de funcionar, la página web seguiría siendo accesible, ya que el balanceador de carga se encargaría de dar la petición a alguno de los otros servidores.

Bridge. Puente. Dispositivo que interconecta redes de área local (LAN) en la capa de enlace de datos OSI. Filtra y retransmite tramas según las direcciones a Nivel MAC.

Browser. Navegador. Término aplicado normalmente a los programas que permiten acceder al servicio WWW

Cache. Es un conjunto de datos duplicados de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, respecto a la copia en la caché. Cuando se accede por primera vez a un dato, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor.

Cortafuego. Ver firewall.

Criptografía. La criptografía es la ciencia que trata la protección de la información mediante el desorden por transposición o sustitución (cryptós) de las letras (graphós) de un documento, con el objetivo de hacerlo confidencial.

CRM (Customer Relationship Management). Gestión de las Relaciones con los Clientes Sistemas informáticos de apoyo a la gestión de las relaciones con los clientes, a la venta y al marketing. Con este significado CRM se refiere al sistema que administra un data warehouse (almacén de datos) con la información de la gestión de ventas y de los clientes de la empresa.

Datagram (Datagrama). Usualmente se refiere a la estructura interna de un paquete de datos.

DMZ. Una DMZ (del inglés *Demilitarized zone*) o Zona DesMilitarizada. Una zona desmilitarizada (DMZ) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

DNS Domain Name System. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

Domain Dominio. Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda.

Ethernet. Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus Coaxial. Método de acceso es CSMA/CD.

Firewall. Cortina de Fuego. Router diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa (Software) ó router (Hardware) que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

Frame. También trama de datos. Grupo de bits transmitido de manera serial sobre un canal de comunicación. En Browsers de WWW como Netscape se refiere a una estructura de sub-ventanas dentro de un documento HTML

Frame Relay. Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

FTP. File Transfer Protocol. Protocolo de Transferencia de Archivos. Uno de los protocolos de transferencia de ficheros más usado en Internet.

Full Duplex. Circuito o dispositivo que permite la transmisión en ambos sentidos simultáneamente

Gateway. Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre sí dos redes normalmente de distinto protocolo o un Host a una red.

Hacker Experto en informática capaz de de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones.

Half Duplex. Un circuito que permite de manera alternante la transmisión y la recepción de señales, pero no de manera simultánea.

Header Cabecera. Primera parte de un paquete de datos que contiene información sobre las características de este.

Host. Anfitrión. Computador conectado a Internet. Computador en general.

HTML HyperText Markup Language. Lenguaje de Marcas de Hipertexto. Lenguaje para elaborar páginas Web actualmente se encuentra en su versión 3. Fue desarrollado en el CERN.

HTTP HyperText Transfer Protocol. Protocolo de Transferencia de Hipertexto. Protocolo usado en WWW.

Internet. Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

Intranet Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW. IP Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de internet. También se refiere a las direcciones de red Internet.

IP (Internet Protocol). Protocolo de Internet Protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usadoen Internet. Los datos se envían en bloques conocidos como paquetes (datagramas) de un determinado tamaño. El envío es no fiable (conocido también como best effort o mejor esfuerzo); se llama así porque el protocolo IP no garantiza si un paquete alcanza o no su destino correctamente. Un paquete puede llegar dañado, repetido, en otro orden o no llegar. Para la fiabilidad se utiliza el protocolo TCP de la capa de transporte.

ISDN Integrated Services Digital Network. Red Digital de Servicios Integrados. Servicio provisto por una empresa de comunicaciones que permite transmitir simultáneamente diversos tipos de datos digitales conmutados y voz.

ISO International Standard Organization. Organización Internacional de Estándares

JOLT. Es un protocolo de comunicación de TUXEDO que es usado para facilitar las peticiones de usuarios a través del servidor de aplicaciones.

LDAP. Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios) Hace referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Middleware. Es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, software, redes, hardware y/o sistemas operativos.

NAT (Network Address Translation). Es un mecanismo utilizado por ruteadores para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

Paquete. En telecomunicaciones, un paquete es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo. Un paquete está generalmente compuesto de tres elementos: una cabecera (header en inglés) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload en inglés) que contiene los datos que se desean trasladar, y la cola (trailer en inglés), que comúnmente incluye código de detección de errores.

PeopleSoft. Software de Planificación de Recursos Empresariales (E.R.P. - Enterprise Resource Planning), gestión de Recursos Humanos , gestión de las Relaciones con los Clientes (CRM, customer relationship management) y Gestión de Nómina a grandes empresas.

Protocolo. Los protocolos de comunicaciones definen las reglas para la transmisión y recepción de la información entre los nodos de la red, de modo que para que dos nodos se puedan comunicar entre si es necesario que ambos empleen la misma configuración de protocolos.

Puerto. En los protocolos TCP/IP es un punto de conexión lógica. En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar a una computadora en red.

Servidor. En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Single Sign On. (SSO) Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación.

SSL. Secure Sockets Layer (SSL; protocolo de capa de conexión segura) y su sucesor Transport Layer Security (TLS; seguridad de la capa de transporte) son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Trama. Para las **telecomunicaciones**, una trama es una **unidad de envío de datos**. Este concepto es equivalente a la idea de paquete de datos en el nivel de enlace de datos del modelo OSI. La trama cuenta con una cabecera (que incluye campos de control de protocolo), datos (aquello que se quiere transmitir en un nivel de comunicación superior) y una cola (donde se establece un chequeo de errores).

TCP. (Transmission Control Protocol) Protocolo de Control de Transmisión Es un protocolo que proporciona una conexión segura que permite transferir corrientes de bits en ambos sentidos. Por este motivo se dice que TCP proporciona un servicio orientado a conexión o que proporciona canales virtuales. Se encarga del control de errores y del control de flujo. Si el mensaje es excesivamente largo, fragmenta la corriente entrante de bytes en mensajes discretos y entrega

cada uno de ellos al IP. También reordena los paquetes si estos llegan desordenados por seguir caminos diferentes en su transmisión.

Tuxedo. (Transactions for Unix, Extended for Distributed Operations) es una plataforma de middleware usada para gestionar procesos transaccionales distribuidos en entornos de computación distribuida. Tuxedo es un middleware orientado a transacciones. Actualmente es muy utilizado en instituciones financieras donde se tiene alto flujo transaccional. En conjunto con Weblogic logran ser una capa importante para el servicio a todos los medios electrónicos.

VPN. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WebLogic. Es un servidor de aplicaciones Java EE y también un servidor web HTTP desarrollado por BEA Systems posteriormente adquirida por Oracle Corporation. Se ejecuta en Unix, Linux, Microsoft Windows, y otras plataformas.

Bibliografía

Anderson, N (2008). Introducción a las redes Cisco. España: Ediciones Anaya.

Carballar, JA (2006), Firewall: La seguridad de la Banda Ancha. México: Alfaomega Grupo Editor

Tanenbaum A.S(2011), Redes de computadoras, México: Pearson Educación.

Referencias internet.

http://www.citrix.com

http://www.cisco.com/web/ES/index.html

http://www.oracle.com/us/products/applications/peoplesoft-enterprise/index.html

Anexos

ANEXO A. Especificaciones Técnicas

SWITCH CISCO SLM224G4S

Especificaciones	
Puertos	• 24 conectores RJ-45 para 10BASE-T/100BASE-TX • 4 conectores RJ-45 para 10BASE-T, 100BASE-TX y 1000BASE-T con 2 ranuras SFP compartidas y 2 puertos Gigabit
Botones	Ninguno
Tipo de cableado	Par trenzado no apantallado (UTP) Categoría 5 o superior para 10BASE-T/100BASE-TX, UTP Categoría 5 Ethernet o superior para 1000BASE-T
LED	Power, Link/Act, Speed
Rendimiento	
Capacidad de conmutación	12,8 Gbps, sin bloqueo
Tamaño de tabla MAC	8000
Número de VLAN	128
Clústeres de switches	
Funcionamiento de los clústeres de switches	• Tamaño máximo del clúster de switches: 192 puertos • Número máximo de unidades del clúster de switches: 6 (con Cisco SLM248G4S) • Inserción y retirada sin interrupción del servicio • Opciones de anillo y cadena • Maestro y maestro de copia de seguridad para un control de clústeres flexibles • Numeración automática o configuración manual de las unidades del clúster de switches
Gestión	
Interfaz de usuario para Internet	Interfaz de usuario de Internet incorporada para una sencilla configuración basada en el navegador (HTTP)
SNMP	Versiones 1, 2c y 3 del protocolo SNMP
MIB SNMP	RFC1213 MIB-2, RFC2863 MIB de interfaz, RFC2665 MIB de interfaz asociada a Ethernet, RFC1493 MIB de puente, RFC2674 MIB de puente ampliado (puente P, puente Q), RFC 2819 MIB de RMON (grupos 1, 2, 3 y 9 únicamente), RFC2737 MIB de entidad, RFC 2618 MIB de cliente RADIUS
RMON	El agente de software RMON integrado admite 4 grupos de RMON (historial, estadísticas, alarmas y eventos) para mejorar la gestión, supervisión y análisis del tráfico
Actualización del firmware	• Actualización con navegador de Internet (HTTP) • Actualización de TFTP (Trivial File Transfer Protocol, protocolo de transferencia de archivos trivial)
Otra gestión	• Registro de auditoría de switch • Cliente de protocolo de configuración dinámica del servidor (DHCP) • BOOTP • Protocolo de tiempo de red simple (SNTP) • Actualización Xmodem • Diagnóstico por cable • Replicación de puertos • Ping
Características de seguridad	
IEEE 802.1X	Autenticación 802.1X: RADIUS; protocolo EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security, protocolo de autenticación extensible: seguridad de capa de transporte de túnel), protocolo PEAP (Protected EAP, protocolo de autenticación extensible protegido), protocolo EAP-MD5, protocolo Cisco LEAP, protocolo EAP-TLS
Control de acceso	ToS/DSCP
Disponibilidad	
Agregación de enlaces	• Adición de enlaces utilizando el protocolo de control de adición de enlace (LACP) IEEE 802.3ad • Hasta 8 puertos en un máximo de 8 troncales
Control de tormentas	Difusión y multidifusión
Árbol de expansión	Árbol de expansión múltiple IEEE 802.1d, Fast Linkover
Snooping IGMP	El snooping IGMP (versiones 1 y 2) proporciona la unión y el abandono rápidos por parte de los clientes de las transmisiones multidifusión y limita el tráfico de vídeo de consumo elevado de ancho de banda a los solicitantes únicamente.
QoS	
Niveles de prioridad	4 colas de hardware
Programación	Asignación de prioridades de colas y turno rotativo ponderado (WRR)
Clase de servicio	• Basada en puerto • Basada en prioridad VLAN 802.1p • Precedencia/ToS/DSCP IP IPv4

Capa 2	
VLAN	• VLAN basadas en puertos y en 802.1Q • VLAN de gestión
Bloqueo de cabecera de línea (HOL)	Prevención de bloqueo de cabecera de línea
Trama Jumbo	Admite un tamaño de trama de hasta 10 KB
Normas	• 802.3 10BASE-T Ethernet • 802.3u 100BASE-TX Fast Ethernet • 802.3ab 1000BASE-T Gigabit Ethernet • 802.3z Gigabit Ethernet • 802.3x Control de flujo
Entorno	
Dimensiones **An x Al x F**	17,32 x 1,75 x 7,99 pulgadas (440 x 44,45 x 203 mm)
Peso de la unidad	5,29 lb (2,4 kg)
Alimentación	100–240 V 0,5 A
Certificación	FCC Parte 15 Clase A, CE Clase A, UL CSA (CSA22.2), marcado CE, CB
Temperatura de funcionamiento	32° a 104 °F (0° a 40 °C)
Temperatura de almacenamiento	-4° a 158 °F (-20° a 70 °C)
Humedad de funcionamiento	De un 20 a un 95%, sin condensación
Humedad de almacenamiento	De un 5 a un 90%, sin condensación
Contenido del paquete	
• Gigabit Smart Switch Cisco SLM224G4S de 24 puertos 10/100 y 4 puertos • Cable de alimentación CA • Kit de montaje en rack con fijaciones y hardware • CD con guía del usuario en formato PDF • Tarjeta de registro en línea • Cable para consola	
Requisitos mínimos	
• Utilidad basada en Web: Microsoft Internet Explorer (versión 5.5 o superior) • Cable de red Categoría 5 Ethernet	
Garantía del producto	
Garantía de hardware limitada de 5 años con devolución a fábrica para sustitución y una garantía de software limitada de 90 días	

ACCESS GATEWAY 2000

Especificaciones del dispositivo Access Gateway

Series	2000
Chasis Dimensiones: Peso:	 1,7" (4,3 cm) x 16,8" (42,6 cm) x 14,1" (35,8 cm) (rack de 1U) 23 lbs (10,4 kg)
Alimentación	100-240 VAC Gama completa 60-50 Hz, 260 W
Puertos interfaz	2 x 10/100/1000 BASE-T
Nº máx. usuarios VPN	500
Ediciones que soporta	Standard Edition Advanced Edition
Garantía, actualizaciones software y firmware	Incluye 12 meses, disponible plan adicional

NETSCALER VPX-200

NetScaler VPX Platforms

	VPX-200
Performance	
HTTP throughput	200 Mbps
SSL encrypted throughput	200 Mbps
HTTP compression throughput	200 Mbps
Application firewall throughput	200 Mbps
Max concurrent TCP connections[2]	5 million
New SSL requests/second	500
Max concurrent SSL VPN users[3]	300

Minimum requirements per physical host[4]	
Hypervisor	XenServer 5 Update 3 or later, VMWare ESX(i) 3.5 or above
Processor[5]	Dual core, Intel VTx or AMD-v
Memory[5]	2 GB
Hard drive	20 GB
Network interface	Hypervisor supported network interface card
Minimum requirements for additional NetScaler VPX virtual machines	
Processor	Dual core, Intel VTx or AMD-v
Memory	1GB
Hard drive	20 GB