UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

MODELO DE OPTIMIZACION DE UNA RED DE SERVIDORES A NIVEL NACIONAL VIA IP

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

JOSE ALBERTO QUISPE CACERES

PROMOCIÓN
2004- I

LIMA – PERÚ

2010

MODELO DE OPTIMIZACIÓN DE UNA RED DE SERVIDORES A NIVEL NACIONAL VÍA IP

Este trabajo lo dedico de
manera muy especial
a mi familia, por el apoyo
y aliento que siempre
me han brindado dentro y
fuera de la universidad.

SUMARIO

El presente documento recoge los problemas de una empresa que tiene varias sucursales a nivel nacional, y se encuentra en expansión, por lo que tiene necesidad de mejorar la productividad y mantener la seguridad de su información.

Se plantea instalar equipos de comunicación con los cuales se realizara, la interconexión de las sucursales y a mejora en los servicios de red.

En el Capitulo I se describe los problemas una empresa en particular, el objetivo y los alcances para la solución del problema.

En el Capitulo II se define el marco teórico, en el cual se explican los conceptos de red para la solución propuesta.

En el Capitulo III se describe la metodología de la solución, indicando alternativas.

En el Capitulo IV se describe la ingeniería de proyecto, definiendo la solución de red.

En el Capitulo V se define los costos de proyecto para la solución planteada.

Finalmente, se presenta conclusiones.

INDICE

PROLOGO

El trabajo ha sido realizado, teniendo como objetivo dar la una solución de interconexión de sucursales de una empresa a nivel nacional, utilizado la red IP, teniendo como componentes en la solución un hardware, que soporta la medidas de seguridad necesarias como firewall, Vpn, IDS, IPS, Filtro de páginas web y muchas opciones más.

Anteriormente a esta solución se tenía implementado una solución piloto con servidores linux utilizando un software OPENVPN, podemos rescatar que la solución es buena, pero el problema en el manejo complejo para funciones avanzadas, además existen muy pocas personas que manejan a nivel de comandos servicios relacionados como firewall, vpn, Proxy sobre Software Libre.

Debido a las ventajas que ofrece el Equipo Hardware a través de la configuración Web, es más fácil tener la gestión y control de la red.

Capitulo I comprende la descripción del problemas de seguridad de una empresa, que no necesariamente puede necesitar la interconexión de sus sucursales. Se plantea también el objetivo, los alcances y las limitaciones.

Capitulo II se describe el marco teórico, donde se define los componentes que intervienen en una VPN, Red Lan y Red Wan, así también los servicios de correo y web.

Capitulo III se define las alternativas de solución, la solución propuesta, también se describe la situación actual de la infraestructura de red.

Capitulo IV se define la arquitectura de red propuesta, la cual brindara seguridad a la red Lan y a los servidores Correo y Web, de la misma forma la sucursales estarán protegidas, ante cualquier ataque desde la red de Internet, o Ataques de Denegación de Servicio, se considera la implantación de Antivirus Corporativo, y monitor de Red.

Capitulo V aquí se describe los costos del proyecto, tenemos los costo de inversión en infraestructura, en el cual tenemos los equipos de solución. (Router, Switch), y tenemos los costos de operación y mantenimiento.

Finalmente, se presenta las conclusiones del modelo planteado.

CAPITULO I
PLANEAMIENTO DE INGENIERIA DEL PROBLEMA

1.1 Descripción del Problema

Se tiene una empresa dedicada al rubro Ventas de Servicios de Telecomunicaciones (Empresa: Servicio Integral de Comunicaciones), que se ha expandido en el tiempo por motivos comerciales y estrategias de negocio, y debido a la rapidez implementa una administración de ventas descentralizada e independiente, observando que no hay control de ventas, comisiones, pagos , stock de almacén, etc.

Con respecto a los servicios que involucran la red de datos tenemos:

- Redes de las oficinas remotas expuestas a código malicioso de Internet (virus, spam, Spyware, etc).
- El firewall implementado en la Sede Principal, no tiene funciones de IPS.
- Falta de personal para la solución de problemas
- Perdida de productividad de empleados por no regulación del uso de Internet.
- Cada PC, realiza funciones de router para tener conectividad con determinados aplicativos
- El gabinete de equipos de comunicación, se observa que se guardan otros objetos, por ejemplo maletas.
- Desorden en el área de servidores.
- No se da el uso adecuado de los UPS y sistemas de backup (correo).
- Falta de definiciones claras de políticas de seguridad a los usuarios que normalicen el uso de las PCs y aplicaciones.
- En general, exposición a riesgo de disponibilidad de los aplicativos e información por desorden en la gestión de la tecnología que soporte al negocio y desconocimiento de sus debilidades.
- No existe una administración del Antivirus en la red.
- No existe un monitoreo de la Red, para los servidores y Aplicaciones.

1.2 Objetivos del Trabajo

Optimización de los servicios de red transmitiendo los estándares de instalación y

metodologías actualmente aplicadas, así como la Interconexión de la Red de Servidores. Caso: Empresa Servicio Integral de Comunicaciones Sac.

1.3 Alcances

El proyecto se aplicara para el local principal ubicado en lima y 13 locales remotos ubicados a nivel nacional, de los cuales se desarrollaran los componentes principales: conectividad, servicios de red: recomendaciones, políticas y procedimientos.

1.4 Evaluación del problema

Se ha visto el interés y el apoyo de la gerencia, administradores de agencias de solucionar todos los problemas y ver un mejor rendimiento de la red de datos y tener un manejo actualizado y centralizado de base de datos para tomar decisiones de administración y ventas.

Por lo tanto es necesario implementar una privada de comunicación entre las oficinas remotas y oficina principal a través de túneles por Internet, implementar políticas de acceso hacia Internet y administración del antivirus centralizado.

1.5 Limitaciones del trabajo

Se tiene como limitación en el proyecto, el aumento de ancho de banda, para los aplicativos de telefónica (atis,gestel,omega,finesse, silicon,citrix, etc), el cual se tiene acceso por una línea dedicada brindada por telefónica (servicio DIGIRED a 64kbps) la cual tiene como titular a Telefonioca del Peru y lo brinda a la empresa de forma gratituita por convenios de negocio.

CAPITULO II
MARCO TEORICO CONCEPTUAL

2.1 Redes Lan

2.1.1 Descripción

Consiste en un medio de transmisión compartido y un conjunto de software y hardware para servir de interfaz entre dispositivos y el medio, regulando el orden de acceso al mismo.

Las topologías usadas son anillo, bus, árbol y estrella; los medios de transmisión empleados son par trenzado, cable coaxial, fibra óptica y medios inalámbricos.

Características:

- Interconexión de equipos.
- Recursos Compartidos: impresoras, scanners, modems, discos, etc., que se usan como si estuvieran en el equipo local.
- Son redes de difusión. Canal de acceso múltiple.
- Red privada corporativa.
- Cobertura geográfica limitada.
- Velocidades de transmisión elevadas (de 1 a 100 Mbps).
- Tasas de error de transmisión muy bajas (10^9).
- Fácil instalación y explotación, con herramientas para su administración.

2.1.2 Estándares

Los estándares de redes de área local definidos por los comités 802 se clasifican en 16 categorías que se pueden identificar por su número acompañado del 802.X. Su objetivo principal es asegurar las compatibilidades, entre los productos de distintos fabricantes, definiendo las normas de las LAN. Muchas de ellas son también normas de ISO. Los comités 802 o proyecto 802, del IEEE, poseen el estándares de comunicación de dispositivos en una LAN.

El modelo IEEE, solo estandariza los niveles físico y de enlace:

- Nivel físico: igual que en el modelo OSI, trata lo relacionado con el medio de transmisión, la conexión, señales eléctricas, etc.

- Nivel de enlace: LLC (logical link control). Control de enlace lógico. Su objetivo es manejar distintos tipos de servicios de comunicación que se pueden ofrecer a través del medio. MAC (media access control). Control de acceso al medio. Ofrece la dirección física del equipo conectado a la red y los mecanismos utilizados para el uso del medio.

a) IEEE 802.2

Control de enlace lógico (logical Link Control). Relativo al establecimiento, mantenimiento y terminación de enlaces lógicos entre nodos de una comunicación.

Define el estándar general para el nivel de enlace de datos. El IEEE divide este nivel en dos subniveles: los niveles LLC y MAC. El nivel MAC varía en función de los diferentes tipos de red y está definido por el estándar IEEE 802.3.

b) IEEE 802.3

Ethernet, Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD, carrier-sense multipe access with collision detection).

Define el nivel MAC para redes de bus que utilizan Acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD, Carrier-Sense Multiple Access with Collision Detection). Éste es el estándar Ethernet. Se muestra en la Fig. 2.1, el formato de la Trama 802.3.

b.1) IEEE 802.3u

Fast Ethernet 100Base-X a velocidad de 100 Mbps.

Puede implementarse con las siguientes opciones:

- **100BASE-TX**:

  Forma predominante de Fast Ethernet, que trabaja sobre 2 pares de cobre, cada segmento de red puede tener una distancia máxima de 100 metros, en su configuración típica, 100BASE-TX utiliza un par de cables trenzados en cada dirección, proporcionando 100Mbits/s de throughput en cada dirección (full-duplex). La configuración de 100BASE-TX para la red es muy similar a 10BASE-T. Cuando es usado para una red de área local, los dispositivos de red (computadores, impresoras, etc.) son típicamente conectados a un hub o switch, creando la red estrella. Alternativamente es posible conectar dos dispositivos usando un cable crossover.

- **100BASE-FX**:

  Es una versión de Fast Ethernet sobre fibra óptica. Utilizando dos cables de fibra óptica, con comunicación dúplex de 100 Mbps. Utiliza 1300 nm de luz de longitud de onda de transmisión a través de dos lineas de fibra óptica, uno para recepción (RX) y el otro para trasmitir (TX).

- **100BASE-SX:**

Versión de Fast Ethernet sobre fibra óptica. Utiliza dos líneas de fibra óptica multi-modo para recibir y transmitir. Este es un menor costo al uso de 100BASE-FX, ya que utiliza una longitud de onda corta óptica, que son significativamente menos costosas.

b.2) IEEE 802.3ab

Ethernet 1000BASE-T, 1Gbit/s sobre par trenzado no apantallado.

El estándar 1000Base-T de Gigabit Ethernet emplea como medio de trasmisión un cable UTP, usando 4 pares de líneas de categoría 5 UTP.

b.3) IEEE 802.3z:

Ethernet 1000BASE-X, 1Gbit/s sobre fibra óptica.

En el estándar 1000Base-X la capa física es el Canal de Fibra.

El Canal de Fibra es una tecnología de interconexión entre workstation, supercomputadoras, dispositivos de almacenamiento de información y periféricos.

Hay 3 tipos de medios de trasmisión que son incluidos en el estándar 1000BaseX:

- 1000Base-SX: usa una fibra multi-modo, 850nm.
- 1000Base-LX: puede ser usada tanto mono-modo y multi-modo, 1300mn.
- 1000Base-CX: usa un cable par trenado de cobre (STP).

c) IEEE 802.11

Constituye un conjunto de estándares del sector para tecnologías de red de área local inalámbrica (WLAN) compartidas, de los cuales el que se utiliza con mayor frecuencia es IEEE 802.11b, también denominado Wi-Fi. IEEE 802.11b transmite datos a 1, 2, 5,5 u 11 megabits por segundo (Mbps) en el intervalo de frecuencias ISM (industrial, científico y médico) de banda S de 2,4 a 2,5 gigahercios (GHz). Otros dispositivos inalámbricos, como hornos microondas, teléfonos inalámbricos, videocámaras inalámbricas y dispositivos que utilizan otra tecnología inalámbrica denominada Bluetooth, también utilizan ISM de banda S.

c.1) IEEE 802.11a

Tiene una tasa de bits máxima de 54 Mbps y utiliza frecuencias del intervalo de 5 GHz, incluida la banda de frecuencias ISM de banda C de 5,725 a 5,875 GHz. Esta tecnología de velocidad mayor permite que las redes locales inalámbricas tengan un mejor rendimiento para aplicaciones de vídeo. Debido a que no se encuentra en las mismas frecuencias que Bluetooth o los hornos microondas, IEEE 802.11a proporciona una mayor tasa de datos.

c.2) IEEE 802.11g

Tiene una tasa de bits máxima de 54 Mbps y utiliza ISM de banda S. Todas las instrucciones de este artículo para configurar los nodos inalámbricos se aplican a las redes inalámbricas basadas en IEEE 802.11b, 802.11a y 802.11g.

Los estándares IEEE 802.11 especifican dos modos de funcionamiento: infraestructura y ad hoc.

- **El modo de infraestructura**

Se utiliza para conectar equipos con adaptadores de red inalámbricos, también denominados clientes inalámbricos, a una red con cables existente. Por ejemplo, una oficina doméstica o de pequeña empresa puede tener una red Ethernet existente. Con el modo de infraestructura, los equipos portátiles u otros equipos de escritorio que no dispongan de una conexión con cables Ethernet pueden conectarse de forma eficaz a la red existente. Se utiliza un nodo de red, denominado punto de acceso inalámbrico (PA), como puente entre las redes con cables e inalámbricas. En la figura 2.2 se muestra una red inalámbrica en modo de infraestructura.

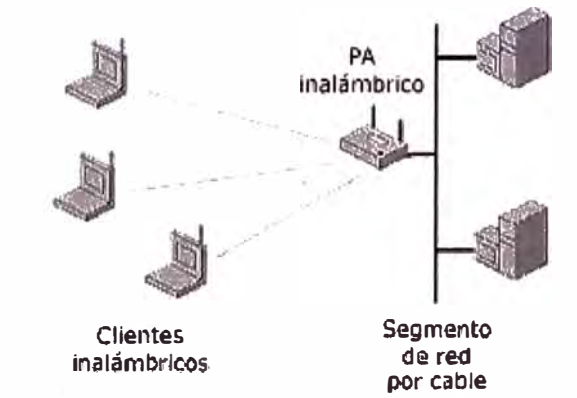


Fig. 2.2 Red inalámbrica en modo de infraestructura

En el modo de infraestructura, los datos enviados entre un cliente inalámbrico y otros clientes inalámbricos y los nodos del segmento de la red con cables se envían primero al punto de acceso inalámbrico, que reenvía los datos al destino adecuado.

- **Modo ad hoc**

El modo ad hoc se utiliza para conectar clientes inalámbricos directamente entre sí, sin necesidad de un punto de acceso inalámbrico o una conexión a una red con cables existente. Una red ad hoc consta de un máximo de 9 clientes inalámbricos, que se envían los datos directamente entre sí. En la figura 2.3 se muestra una red inalámbrica en modo ad hoc.

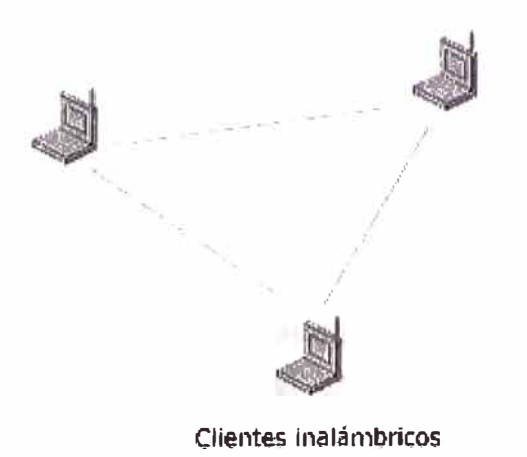


Fig. 2.3 Red inalámbrica en modo ad hoc

2.2 Redes Wan

2.2.1 Descripción

Una red de área amplia puede ser descripta como un grupo de redes individuales conectadas a través de extensas distancias geográficas. Los componentes de una red WAN típica (ver Fig. 2.4) incluyen:

- Dos o más redes de área local (LANs) independientes.
- Routers conectados a cada LAN
- Dispositivos de acceso al enlace (Link access devices, LADs) conectados a cada router.
- Enlaces inter-red de área amplia conectados a cada LAD

La combinación de routers, LADs, y enlaces es llamada inter-red.

La inter-red combinada con las LANs crea la WAN.

Un dispositivo de acceso al enlace (LAD) es necesario para convertir las señales para ser transmitidas desde la LAN en un formato compatible con el tipo de enlace de área amplia inter-red utilizado.

Las conexiones entre LADs pueden ser punto a punto o a través de la red intermedia de un proveedor de servicios de red.

En un enlace punto a punto, los LADs se comunican directamente entre sí sobre un circuito de telecomunicaciones. Este circuito puede ser temporal, como el de una red conmutada de telefonía pública, o permanente, por ejemplo una línea de datos dedicada contratada a un proveedor.

Nota: Una red intermedia se define como una red utilizada para conectar dos o más redes.

Algunos ejemplos de LAD incluyen:

- Modem.
- Data service unit/channel service unit (DSU/CSU).

- Terminal adapter (TA).
- Packet assembler/disassembler (PAD).
- Frame Relay access device (FRAD).

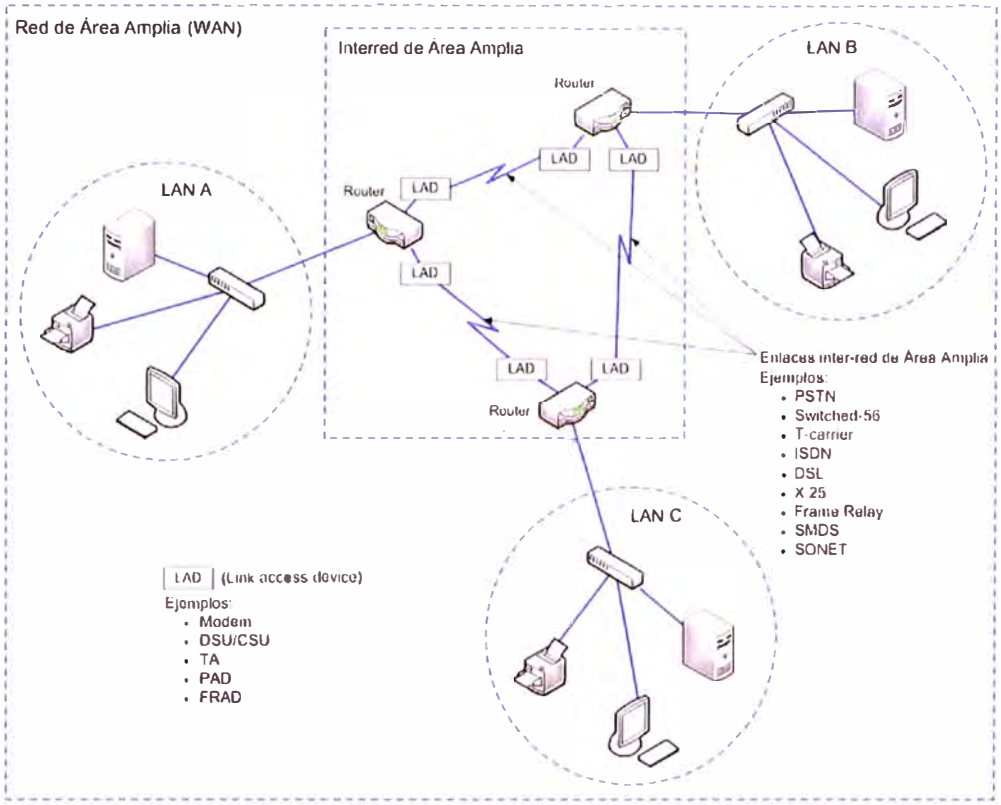


Fig. 2.4 - Red Wan

En un enlace de red intermedia, los LAD son conectados una red de transporte de datos, controlada y administrada por uno o más proveedores de servicios de red. Las conexiones al proveedor de servicios de red son realizadas usando enlaces punto a punto temporales o permanentes. Una vez que los datos son recibidos por el proveedor de servicios de red, son transferidos hasta la LAN de destino a través de una red de área amplia inter-red dedicada.

Los proveedores de servicio de red reciben múltiples flujos de datos en forma simultánea desde varias organizaciones. Todos los datos son transferidos un paquete a la vez por la red del proveedor de servicios, potencialmente con cada paquete tomando un camino diferente. El enrutamiento se basa en la información de direccionamiento incluida en el paquete.

Existen muchas conexiones y rutas posibles en la topología en forma de malla, de la red del proveedor. Varias tecnologías de enrutamiento y conmutación a alta velocidad son utilizadas por el proveedor de servicios de red para dirigir los paquetes hasta su destino. Dado que existen múltiples caminos, un paquete puede ser enrutado para evitar

cualquier falla o área congestionada de la red, el enrutamiento del paquete es dinámico.

Cuando se usan las redes de alta velocidad de un proveedor de servicios de red como enlaces de red intermedios, no existe un circuito predefinido de extremo a extremo entre las LAN comunicadas; es por ello que las tasas de transmisión de la inter-red pueden ser aumentadas o disminuidas según se requiera mediante acuerdos con el proveedor de servicios de red.

2.3 Redes Virtuales VLANs

2.3.1 Descripción

VLAN significa red de área local virtual, se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o en diferentes redes locales. Figura 2.5

2.3.2 Equipamiento

La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control mas inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

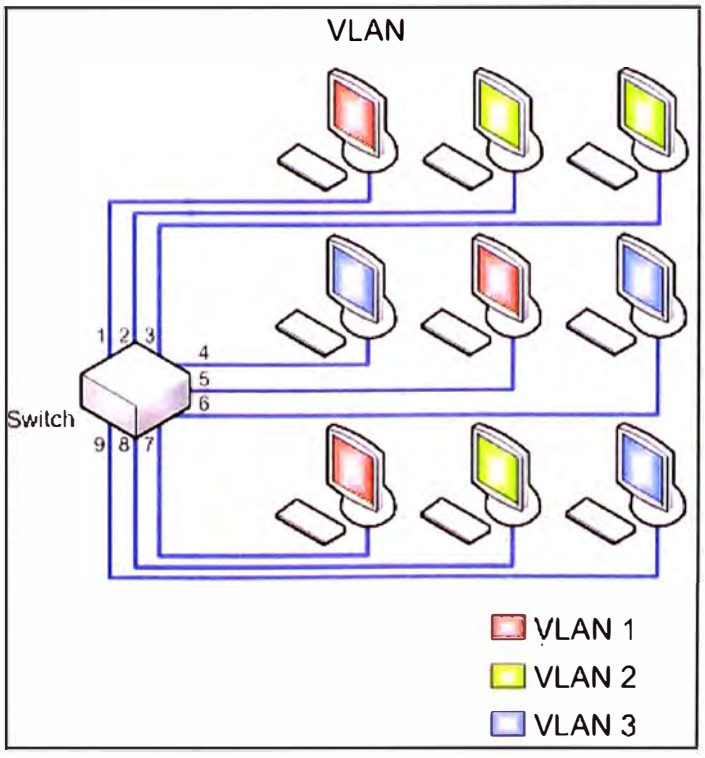


Fig. 2.5 – Red con VLAN

2.3.3 Segmentación

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica microsegmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

2.3.4 Ventajas

Reducción en el trafico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

2.3.5 Tipos de VLAN

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

- la **VLAN de nivel 1** (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador;
- la **VLAN de nivel 2** (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación;
- la **VLAN de nivel 3**: existen diferentes tipos de VLAN de nivel 3:
- **VLAN basada en la dirección de red,** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.
- **VLAN basada en protocolo,** permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

2.3.6 Vlan Trunk Protocol

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol (VTP) es el que se utiliza para esta conexión.

2.3.7 Estándares

a) IEEE 801.Q

El protocolo **IEEE 802.1Q** fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

2.4 VPN

2.4.1 Descripción

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Ejemplo Internet.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública, se implementan técnicas de seguridad para mantener la confidencialidad de los datos que circulen entre los usuarios. (Ver Fig. 2.6)

2.4.2 Arquitectura de las VPN

Dentro de las posibles arquitecturas que encontramos dentro de las VPN se pueden mencionar las siguientes:

- Proporcionada por un servidor de Internet: El proveedor de Internet puede instalar en su oficina un dispositivo que se encargara de la creación del túnel para la organización.
- Basadas en firewalls: De la misma forma en que las VPN trabaja en los niveles mas bajos del modelo OSI, el firewall actuará de la misma forma.
- Basadas en Caja Negra: Básicamente es un dispositivo con software, que utilizan algoritmos de tecnología VPN. Esto elementos son capaces de cumplir con la tarea de encriptación y desencriptación mas rápidamente que los servidores VPN.
- Basadas en Routers: Puede ser en este caso que el software de encriptación se añada al router ya existente o bien que se utilice una salida exclusiva de otro proveedor.
- Basadas en acceso remoto: El cliente tiene software por el cual se conecta al servidor de VPN de la corporación a través de un túnel encriptado.
- Basadas en Software: Por lo general se utiliza de un cliente a un servidor de VPN que esta instalado en alguna estación de trabajo. Es necesario tener procesos de administración de claves y un emisor de certificados.

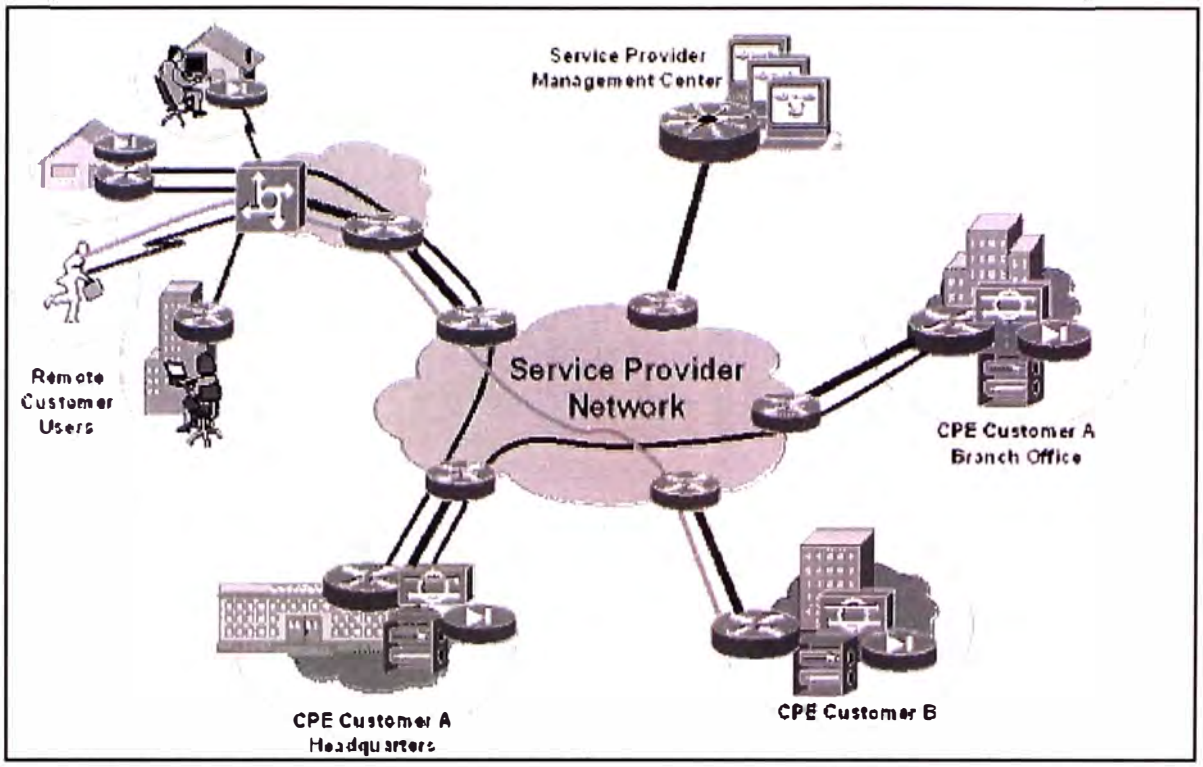


Fig. 2.6 – Red Privada sobre Internet

2.4.3 Tipos de conexiones VPN

a) Un usuario remoto que establece un tunel con la oficina principal. (client-to-site). Este es el caso de un vendedor o socio de negocios que requiere entrar a nuestra red.

b) Una sede remota (oficina) con varios usuarios que se une a la red central (site-to-site). Este es el caso de un almacén o sucursal remota que puede reemplazar un enlace privado costoso por una solución más económica. (Fig. 2.7)

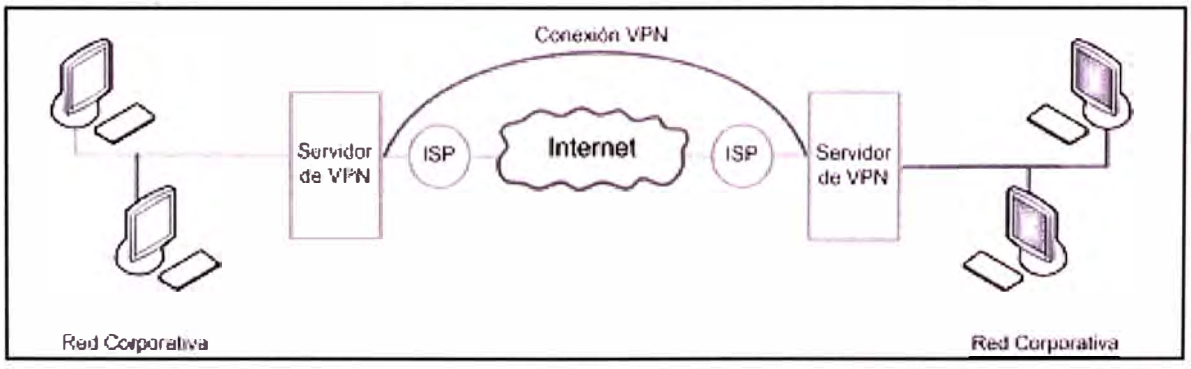


Fig. 2.7 – Tipos VPN

2.4.4 Tunneling

El túnel es un método por el cual se hace uso de una red intermedia para transferir datos de un extremo a otro.

Los paquetes que se transmiten se encapsulan sobre otro encabezado correspondiente al protocolo de túnel, este nuevo encabezado contiene la información necesaria para que el paquete atravesando la red intermedia llegue al destino correspondiente, una vez llegados a destino son desencapsulados y dirigidos al destino final.

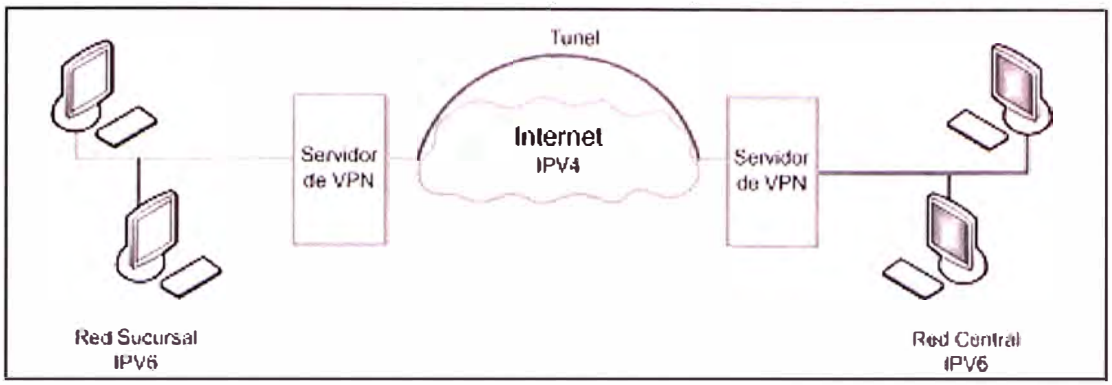


Fig. 2.8 – TUNEL VPN

Un túnel es un canal virtual, configurado entre dos sistemas remotos que se encuentran en diferentes redes, sobre una conexión real que involucra más de un nodo intermedio. Un túnel tiene dos extremos que son los extremos de la red intermedia, entre esos extremos se creará una conexión lógica con técnicas de seguridad que es por donde se hará el intercambio de paquetes de la comunicación. Ver Fig. 2.8

Se pueden destacar como requerimientos básicos de un protocolo de túnel que cumpla con las siguientes condiciones:

- Autenticación de usuario.
- Asignación dinámica de direcciones.
- Compresión de datos.
- Encriptación de datos.
- Administración de llaves.
- Soporte multiprotocolo.

2.4.5 Protocolos de Túnel

Los protocolos que se utilizan son a nivel de capa 2 o capa 3, se crea la conexión entre los dos puntos y se crea un túnel entre ellos como si pertenecieran a una misma red local. Además de los protocolos de capa 2, existen también los de capa 3 como el IPSec que encapsula paquetes de protocolo IP en otros de protocolo IP también.

Ejemplo de protocolos:

- L2F (Cisco's Layer Two Forwarding)
- PPTP (Microsoft's Point-to-Point Tunneling Protocol)
- L2TF

- IPSEC

2.5 TCP/IP

2.5.1 Descripción.

Bajo las siglas TCP/IP (Transfer Control Protocol/Internet Protocol) se agrupa un paquete de protocolos de comunicación de datos. El paquete toma este nombre por dos de los protocolos que lo integran, el TCP ó Protocolo de Control de Transferencia, y el IP, ó Protocolo de Internet, dos de los más importantes protocolos que podemos hallar en dicho paquete.

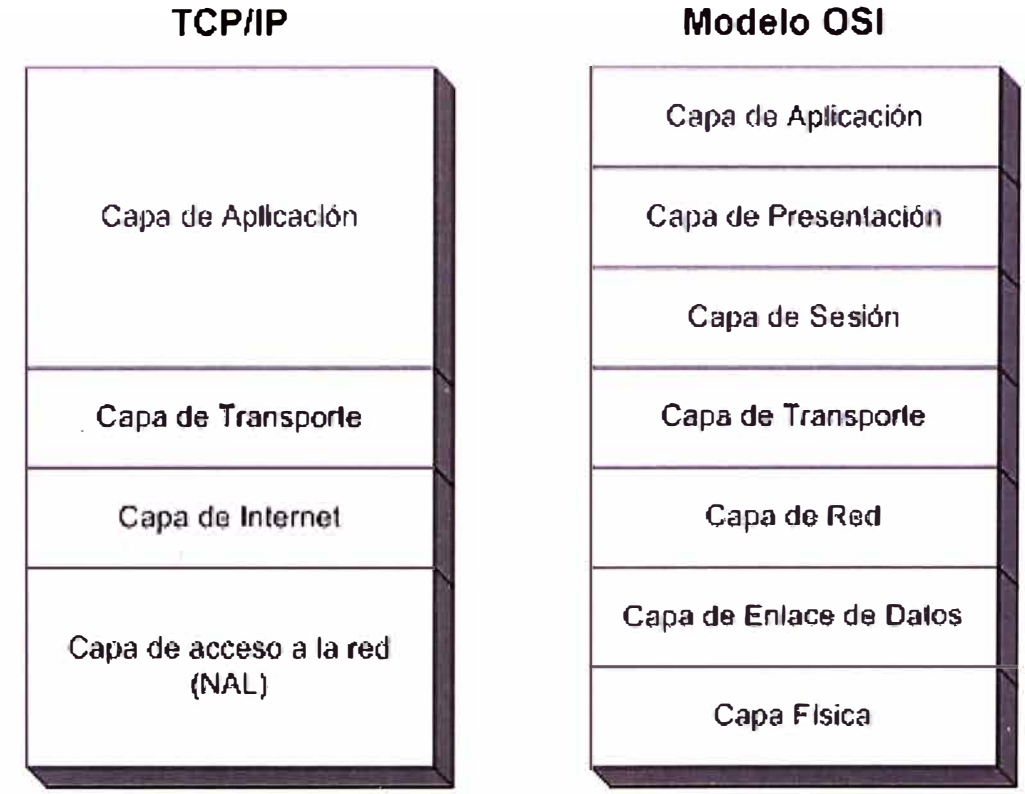


Fig. 2.9 - TCP/IP vs Modelo OSI

2.5.2 Características de TCP/IP

- Son estándares de protocolos abiertos y gratuitos. Su desarrollo y modificaciones se realizan por consenso, no a voluntad de un determinado fabricante. Cualquiera puede desarrollar productos que cumplan sus especificaciones.
- Independencia a nivel software y hardware Su amplio uso los hace especialmente idóneos para interconectar equipos de diferentes fabricantes, no solo a Internet sino también formando redes locales. La independencia del hardware nos permite integrar en una sola varios tipos de redes (Ethernet, Token Ring, X.25...)
- Proporcionan un esquema común de direccionamiento que permite a un dispositivo con TCP/IP localizar a cualquier otro en cualquier punto de la red.

- Son protocolos estandarizados de alto nivel que soportan servicios al usuario y son ampliamente disponibles y consistentes.
- TCP/IP permite que se comunique cualquier par de computadores conectados a ella. Cada computador tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de su fuente y de su destino. Los computadores intermedios de comunicación utilizan la dirección de destino para tomar decisiones de ruteo.

2.5.3 Arquitectura de los protocolos TCP/IP

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí.

El modelo de arquitectura de estos protocolos es mas simple que el modelo OSI, como resultado de la agrupación de diversas capas en una sola o bien por no usar alguna de las capas propuestas en dicho modelo de referencia.

De esta forma nos quedamos con una modelo en cuatro capas, tal y como se ve en la siguiente Fig. 2.9

2.5.4 Estándares de Protocolos de Aplicación

Además de los servicios básicos de nivel de transporte, los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto.

2.6 Servicios y Aplicaciones de Red

2.6.1 Correo electrónico y lista de distribución

Quizás la fórmula de comunicación de la red más utilizada y conocida. Con ella podemos establecer intercambio de datos entre dos personas -correo electrónico- y entre varias a la vez -lista de distribución-.

2.6.2 News

Los news son grupos de personas que utilizan la red para debatir sobre temáticas puntuales.

2.6.3 Telnet

Con esta tecnología nos permite disponer de un ordenador como si fuera un terminal conectado a otro ordenador que comparte con este sus programas y recursos.

2.6.4 Gopher y WWW

El acceso a la información en internet tiene por excelencia estas dos fórmulas de búsquedas. El gopher constituyó la primera herramienta que facilitaba la comunicación entre usuario e internet (interface), facilitándole a éste una recuperación de ficheros presentados con menús jerarquizados. Después, ha surgido WWW, y es en la actualidad el sistema más utilizado y eficaz que conocemos.

2.6.5 FTP

Es una herramienta que nos permite conectarnos con otros ordenadores y enviar o recibir ficheros.

2.7 Servidor

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

2.7.1 Servidor Web

Un servidor web es un ordenador que implementa el protocolo HTTP (HyperText Transfer Protocol), se ejecuta continuamente un programa o servicio, manteniéndose a la espera de peticiones por parte de un cliente (un navegador web) y que responde a estas peticiones adecuadamente, mediante una página web o página HTML, que se exhibirá en el navegador o mostrando el respectivo mensaje si se detectó algún error.

2.7.2 Servidor de Archivos

Tipo de servidor en una red de ordenadores cuya función es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este. Algunos protocolos comúnmente utilizados en servidores de archivos:

- SMB/CIFS (Windows, Samba en Unix)
- NFS (Unix)

2.7.3 Servidor de Correo

Un servidor de correo es una aplicación informática que nos permite enviar mensajes (correos) de unos usuarios a otros. Entre los más usados se encuentran Lotus Domino, Exchange Server, Postfix, Sendmail, etc. Para lograr la conexión se definen una serie de protocolos:

SMTP : Simple Mail Transfer Protocol
POP : Post Office Protocol
IMAP : Internet Message Access Protocol

2.7.4 Servidor Base de Datos

Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. Entre los servidores de bases de datos más potentes y fiables en entornos de alta disponibilidad y sistemas de archivos seguros, tenemos:

Oracle, SQL , MySQL, PostgreSQL, DB2, SAP, etc.

2.8 IDS

La detección de intrusos consiste en un conjunto de métodos y técnicas para revelar actividad sospechosa sobre un recurso o conjunto de recursos computacionales. Es decir, eventos que sugieran comportamientos anómalos, incorrectos o inapropiados sobre

un sistema; entendido como el ente que está siendo monitoreado (Estación de trabajo, dispositivos de red, servidores, firewalls, etc.).

2.9 IPS

Los IPS son dispositivos de hardware o software encargados de revisar el tráfico de red con el propósito de detectar y responder a posibles ataques o intrusiones. La respuesta usualmente consiste en descartar los paquetes involucrados en el ataque o modificarlos de tal manera que se anule su propósito. Es claro que este comportamiento los clasifica como dispositivos proactivos debido a su reacción automática a situaciones anómalas.

CAPITULO III
METODOLOGIA PARA LA SOLUCION DEL PROBLEMA

3.1 Alternativas de Solución

Con el objetivo de tener una red Interconectada a Nivel Nacional se tienen las siguientes soluciones:

3.1.1 Servicio IP-VPN

Para interconectar las sedes remotas, se podría contratar el servicio IP-VPN, con tecnología TDM, ADSL, F.O ofrecido por telefónica, con el cual tendríamos líneas dedicadas en todas las sedes, Lima y Provincia, este sistema de comunicación es privado y estable, se manejan equipos router cisco en cada Sucursal, los cuales son monitoreados por el Centro de Gestión de Telefónica con atención 7x24.

El problema de esta solución es el alto costo mensual, de las líneas dedicadas, y un costo adicional para que la sede principal se comunique con provincias, y las provincias se comuniquen con lima, definido por telefónica como ancho de banda LDN.

3.1.2 VPN sobre TCP/IP

Usando el servicio de Speedy ya instalado, y con facilidades técnicas de upgrade de velocidad, podemos configurar la conexión por VPN a través de Internet en todas las sucursales de la Empresa. Gracias a la técnica de tunneling, una Organización puede usar de forma segura una red pública, para comunicarse con sus sucursales remotas, ya que los paquetes son encriptados antes de ser enviados.

Esto nos ahorrara costos mensuales del servicio, tendremos el soporte del Servicio Speedy 24 hrs, y el monitoreo de los equipos y conexión VPN serian administrados por personal de la empresa.

3.2 Solución del Problema

3.2.1 Situación de las Telecomunicaciones en las Sucursales

Todas las sedes remotas se encuentran en cobertura del servicio Speedy disponible, las velocidades presupuestadas tienen las facilidades técnicas. También están los ISP como Telmex, Americatel disponibles, para las sedes de la ciudad de Lima, pero con otro tipo de acceso. Diferente Infraestructura.

También encontramos que en la ciudad de Lima se encuentra el servicio de Línea

dedicada, por parte de Telefónica Empresas, brindando servicio como IP-VPN, Internet Empresarial, también ofrecido para provincias.

Las empresas Americatel, Telmex, Global Crossing, también ofrecen servicio de datos dedicado, solo en Lima. En la tabla 3.1 se muestra los Locales donde se implantara la solución.

TABLA N° 3.1 SUCURSALES

Direcc. Comercial	Distrito o Provincia
Av. Gran Chimu 384 Zarate	SAN JUAN DE LURIGANCHO
Av. Gran Chimu 360 Zarate	SAN JUAN DE LURIGANCHO
Av. Venezuela 617 Chacra Colorada	BREÑA
Centro Comercial Megaplaza Los Olivos N° 80	LOS OLIVOS
Av. De los Herores 458 A	SAN JUAN
Plaza de la Solidaridad Mz ZC Sector 2 Grupo 15	VILLA EL SALVADOR
Av. Alfredo Mendiola 3693 Urb. Panamericana Norte	LOS OLIVOS
Mz B lt 14 Asoc El Porvenir	ATE VITARTE
Av. 28 de Julio 128	CHOSICA
Av. Gran Chimu 913 A Zarate SJL	SAN JUAN DE LURIGANCHO
Jr. 2 de Mayo 324 Imperial	CAÑETE
Jr. Ica 586	HUANCAYO
Calle Real 377	HUANCAYO
Plaza Carrion 181 -185	CERRO DE PASCO
Jr. Ancash 395	MERCED

3.2.2 Solución de Interconexión para la Empresa

De las alternativas de solución, se plantea como parte del trabajo realizar la VPN sobre TCP/IP, usando la infraestructura de Telefónica ADSL, mediante su servicio SPEEDY, para la interconexión de sucursales.

Se consideran cambios y adquisición de equipos de comunicación, para la solución, la seguridad de la red y mejor rendimiento de la misma, recomendaciones de los estándares de instalación de cableado estructurado y/o eléctrico.

Se considera como parte de la solución la restricción del acceso a Internet, por lo solo se permitirá el acceso a páginas relacionadas con el negocio, y acceso total a personal de gerencia. Se considera la centralización de un Antivirus a nivel corporativo.

Para la comunicación del Servidor de Correo, se considera excepcionalmente la contratación del servicio de Internet dedicado (INFOINTERNET), brindado por Telefónica.

Para la seguridad con respecto a los virus informáticos, se considera instalar un Antivirus Corporativo, a fin de mantener el control centralizado de este servicio, y verificar el estado actual de las PCs dentro de la red.

Para verificar la conectividad con todas las sucursales, servidores y servicios de red, se considera instalar un monitor de red, en este caso consideramos un servidor con SO. Linux, y con una aplicación conocida como Nagios.

Se recomienda la adquisición de servidores, con arreglo de discos RAID5, políticas de backup, a fin de mantener la continuidad del negocio y la integridad de la información en caso falle el hardware de los servidores.

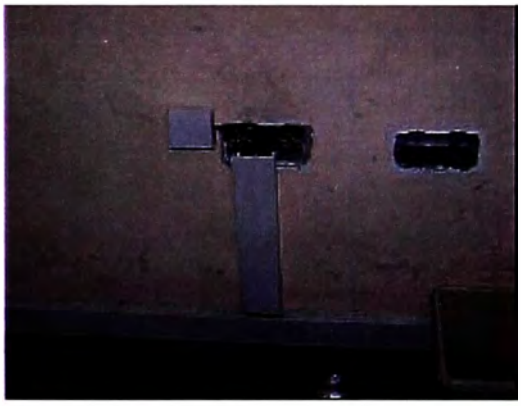
3.3 Situación Actual de la Infraestructura de la Red

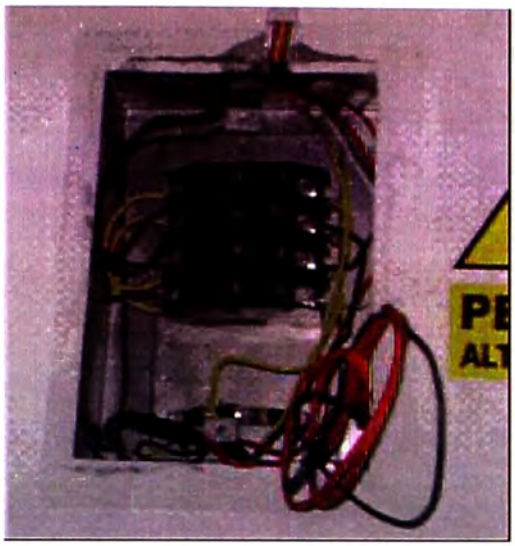
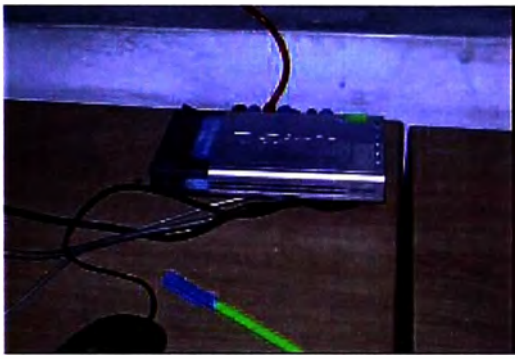
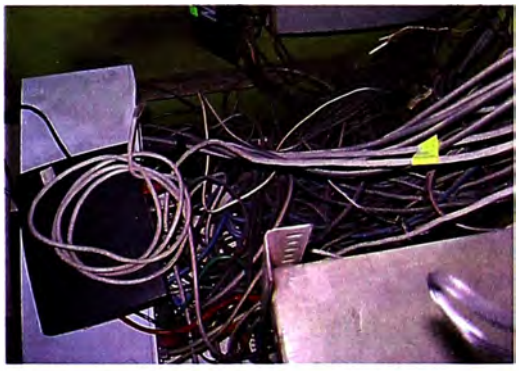
3.3.1 Muestreo de Sucursales

En virtud de verificar el status de las instalaciones eléctricas y el cableado estructurado, se efectuó un muestreo de algunas oficinas de Lima, encontrando algunas observaciones relevantes que podrían influir en el buen desenvolvimiento del trabajo.

En el ANEXO A detallamos las políticas y recomendaciones al respecto.

A continuación el estado de algunas sedes y sus instalaciones.

OFICINA PRINCIPAL	OBSERVACIONES DETECTADAS
	Riesgo de shock eléctrico al estar expuesta la caja empotrada. Falta de tapa ciega en las cajas empotradas. Ausencia de face plate en el tomacorriente deja visible cable eléctrico.
	No se cuenta con planos eléctricos y de cableado de datos. Altura de la caja de montaje eléctrica no recomendable Tablero de piso no garantiza seguridad al tener cables de corriente fuera del mismo. Falta de ajuste en los contactos de las llaves termo magnéticas puede producir corto circuito o desconexión temporal de equipos.

	Tablero eléctrico no cuenta con puerta y llave de seguridad. Pares de un mismo cable eléctrico tienen distinto calibre. Escasa seguridad en el manejo de las llaves termo magnéticas. Falta de identificación de llaves termo magnéticas no permite la rápida identificación del circuito.
	Ubicación inapropiada de equipos de comunicación puede originar la desconexión de alguno o todas las conexiones. Riesgo de manipulación o peligro de caída de equipo mismo lo cual podría dejarlo sin uso total.
	Exposición peligrosa de equipo por falta de rack para los equipos. Consecuencias derivadas podría ser la pérdida de la inversión por los activos y peor aún la desconexión e interrupción del servicio y horas hombre.
	Mejoramiento de las conexiones de los Patch Cords según las normas de cableado estructurado.

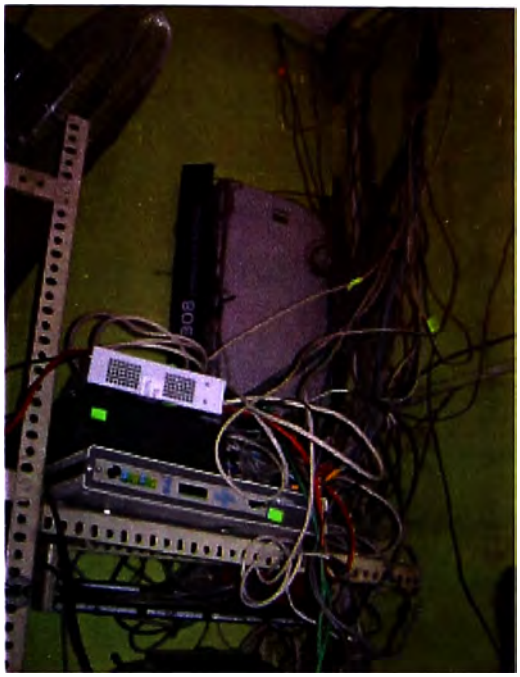
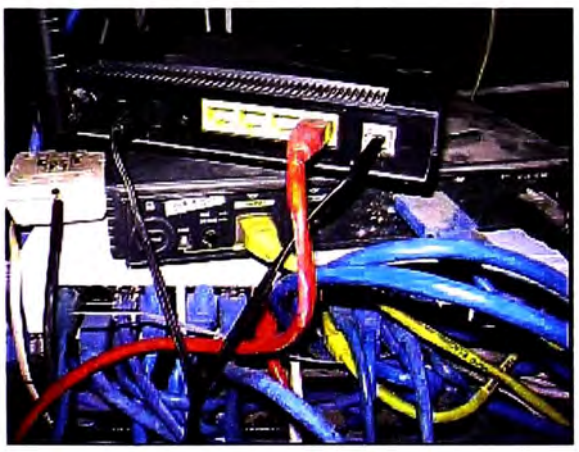
	Se detectó la falta de un Rack de comunicaciones. El actual no cumple con ninguna norma del estándar mundial. Es recomendable la instalación de un rack apropiado para salvaguardar la integridad de los equipos y evitar riesgo de pérdida fortuita de la comunicación.
	Falta de uso de ordenadores Acceso difícil para el mantenimiento y por ende la imposibilidad de realizar cambios inmediatos sin perjudicar la operatividad y continuidad del servicio de los usuarios y cliente.

Fig. 3.2 – Oficina Principal

OFICINA MEGAPLAZA	OBSERVACIONES DETECTADAS
	Tablero eléctrico accesible, no cuenta con llave de seguridad a fin de evitar la manipulación. Pobre etiquetado de llaves termo magnéticas.

	Objetos extraños ubicados en el área del rack (pegamento inflamable). Cabkes y Patch Cords no guardan el orden requerido. Baja identificación de los cables de conexión.

Fig. 3.1 – Oficina de Megaplaza

OFICINA SAN JUAN	OBSERVACIONES DETECTADAS
	Pobre ordenamiento de los Equipos. Baja administración del cableado estructurado debido a falta de ordenadores y patch panel. Difícil identificación de cables de conexión en caso de mantenimiento.
	Falta de mantenimiento preventivo que asegure la limpieza del ambiente fomentando el riesgo de deterioro de los equipos. Equipos de comunicación no adosados firmemente al rack o bandeja.

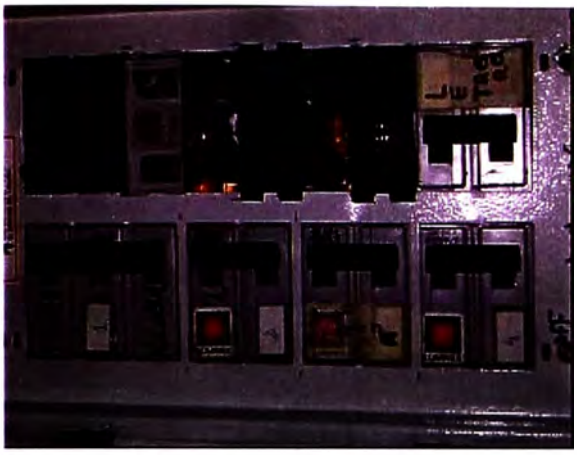
	Barras de cobre de conexión eléctrica visible por falta de tapa ciega de llaves termo magnéticas.

Fig. 3.3 – Oficina San Juan

OFICINA BREÑA	OBSERVACIONES DETECTADAS
	Pobre administración de los Patch Cords. Incorrecta instalación de equipos. Etiquetado de conexiones incompleta o no identificable. Mala ubicación de central telefónica.
	Presencia de objetos no idóneos (licencia de funcionamiento del local). Exposición inadecuada de cables eléctricos. Documentación irrelevante encontrada. Cables telefónicos expuestos. Excesivo polvo en los equipos.

Fig. 3.4 – Oficina Breña

OFICINA VILLA EL SALVADOR	OBSERVACIONES DETECTADAS
	Falta de protección de ranuras de llaves termo magnéticas.

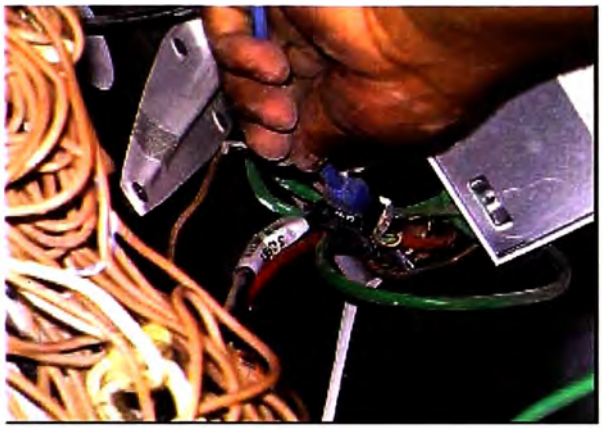
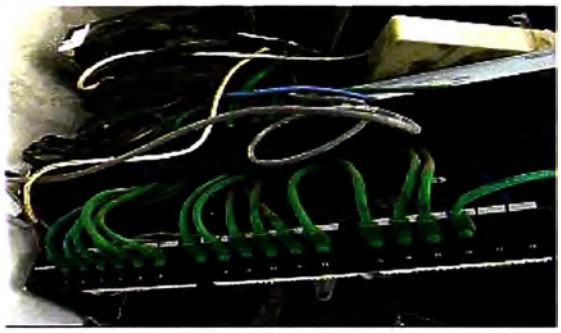
	Baja administración del cableado estructurado debido a falta de ordenadores y patch panel. Difícil identificación de cables de conexión en caso de mantenimiento. Pobre ordenamiento de equipo. Falta de mantenimiento preventivo que asegure la limpieza del ambiente fomentando el riesgo de deterioro de los equipos.
	Patch cord fuera del patch panel genera riesgo de desconexión y no cumple con las normas internacionales y buenas prácticas. Cable telefónico no conserva el orden adecuado.
	Equipos de comunicación no adosados firmemente al rack o bandeja. Falta de etiqueta e identificación de rutas de patch cords.

Fig. 3.5 – Oficina Villa Salvador

CAPITULO IV
INGENIERIA DEL PROYECTO

4.1 Red de Datos Actual

4.1.1 Descripción de la Topología actual

Actualmente en la oficina principal se cuenta con dos salidas a Internet provistos por Telefónica del Perú, cada uno con un modem Adsl de marca Zyxel. (Ver Fig. 4.1). Se usa dos servicios de Internet para separa el trafico entre dos grupos servidores y PCs.

El Internet1, es usado para los servidores para el acceso a Internet, y publicación de los Servicios Correo y Web.(Ver Fig. 4.1). El Internet 2, es usado para el acceso de todas la Computadores restantes.

Existen dos redes, una para acceder a Internet, y otra para ingresar a los sistemas de telefónica vía la línea dedicada.

Debido a que las redes son diferentes, existen dos tipos de computadoras, unas usan 2 tarjetas de red y otras con una sola tarjeta de red. Las PC con una tarjeta de red, para entrar a los aplicativos de telefónica, manejan una IP, y cambian la dirección IP por otra para acceder a Internet.

Las PC con dos tarjetas de red, utilizan dos direcciones IP, en cada tarjeta, y a su vez, dos direcciones como puerta de enlace.

Para que las PCs se comuniquen con los servidores, también se observa que los servidores manejan 2 tarjetas de red.

Para el Internet 1, la IP 192.168.1.1 y para el Internet 2, la IP 192.168.1.2 ambos como mascara 255.255.255.0

Las direcciones IP para la red de telefónica son: 172.26.14.224/27, teniendo como Gateway al router con IP 172.26.14.225.

Solo pueden acceder a la vez, al sistema de telefónica, 29 computadoras debido a la mascara de red usada, 255.255.255.224.

En todas las sedes remotas, no hay restricción de acceso a Internet.

4.1.2 Tipos de Sucursales

a) Tipo 1

Sucursales, incluida la sede principal, que cuentan con una línea dedica de

datos a 64kbps, para la conexión a los aplicativos de Telefónica. (Omega, Gestel, Atis, Aplicaciones de Telefónica Móviles, etc). La facturación de esta línea dedicada esta a nombre de Telefónica del Perú, este servicio lo tienen la mayoría de sucursales y están autorizados como centros de cobros de los productos de telefónica en general (pago de celulares, telefonía básica, Speedy, cable, etc), solo en algunas sucursales están autorizados el servicio Postventa Móviles.

La conexión a los aplicativos de telefónica es crítico, debido a que la pérdida de conexión afecta a las ventas de la empresa y al público debido a que no funciona el centro de cobros. (Ver Fig. 4.1)

b) Tipo 2

Este tipo de sucursales, no tienen una conexión dedicada, pero en su lugar tienen una conexión VPN a través de Internet para acceder a los aplicativos de Telefónica Móviles, por lo cual realizan ventas de equipos móviles, chips, etc. y en algunas sucursales Tipo 2, se tienen el servicio Postventa Móviles para el público.

Debido a este tipo de conexión a la red de telefónica, el acceso a Internet es crítico, así como el consumo innecesario de ancho de banda de Internet, perjudicando a las aplicaciones. (Ver Fig. 4.1).

c) Tipo 3

Llamados puntos de venta, que cuentan con 1 o 2 PCs, solo tienen Internet, para ingresar sus ventas o validarlas, tienen que comunicarse con alguna oficina remota o la Sede Principal.

4.1.3 Topología Actual

El diagrama de la red actual de datos, se muestra en la Fig. 4.1

4.2 Arquitectura de Red Solución

4.2.1 Componentes de la Solución

a) D-Link DFL-210 NetDefend

Para la oficina principal y sucursales será necesario instalar, el DFL-210 propuesto para la solución.

D-Link DFL-210 NetDefend, una nueva serie de soluciones de seguridad para empresas de tamaño medio y pequeño. Este Firewall de la línea Net Defend puede ofrecerle un alto retorno de inversión a través de las robustas características de seguridad, configuración flexible y máxima protección de la red. (Ver Anexo C)

Principales Características:

- 1 puerta WAN, 1 puerta DMZ (configurable) y 4 LAN

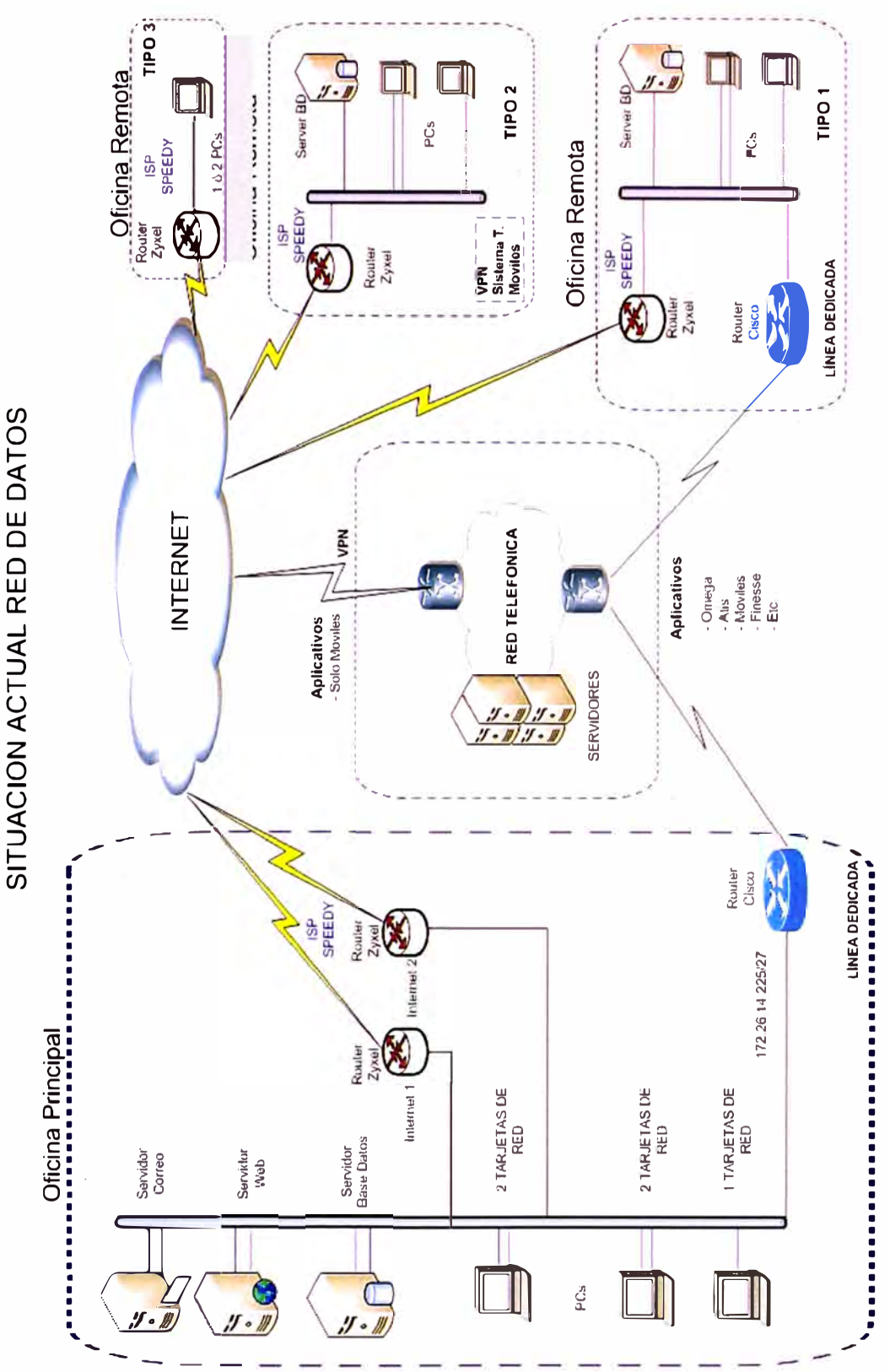


Fig. 4.1.- Diagrama de conexión de la red de datos actual

- Soporte hasta 12000 sesiones concurrentes
- Soporte de hasta 100 túneles VPNs, rendimiento hasta 25Mbps
- Administración del ancho de banda

- Balanceo de carga
- Filtrado de contenido
- Soporte IDS
- Protección DoS
- System Log y estadística en tiempo real

b) 3Com Baseline Switch 2226 Plus

Para tener un control de la Red y manejo de Broadcast, será necesario cambiar en las sedes a un switch administrable. (Ver Anexo C)

Este equipo se puede administrar vía web, además con la herramienta, 3Com Network Supervisor, podremos tener el diagrama de red, y asi poder identificar problemas. De esta forma podemos tener la administración de red de todos los equipos en las sucursales a través de la VPN.

c) Switch D-LINK DGS-3627, L3

Este Switch de Core, con funcionalidades de capa 3, será el que controle el trafico de la red LAN, enrutando la información hacia R1, R2 o R3 (Ver. Fig. 4.2). En la sede principal se tiene 80 PCs, distribuidos en 5 pisos, este equipo es el adecuado por su velocidad de conmutación. Ver Anexo C.

4.2.2 Conectividad

En la conectividad se contempla realizar una implementación de red segura mediante túneles por Internet entre las Oficinas Remotas y la Oficina Principal, también contempla revisión y configuración de conexiones hacia los aplicativos de Telefónica del Perú a través de sus líneas dedicadas. Contempla también la configuración de navegación a Internet de la Oficina Principal y Oficinas Remotas previa definición de políticas.

4.2.3 Infraestructura

La infraestructura WAN, donde estará implementada la solución de conectividad con los DFL-210, se considera para las sucursales el aumento de velocidad, a un Speedy 2000 (2048/512kbps) Negocios Avanzados al 25% y para la Oficina Principal se necesita 2 conexiones a Internet Speedy 2000 Negocios Avanzados al 25% (Una para acceso a Internet y otra dedica para las conexiones VPN) y una conexión dedica Infointernet de 512kbps 1:1 para el servicio Correo, Web y FTP.

Para la infraestructura de la red LAN será necesario cambiar a un switch administrable, y mantener este estándar, permitiendo tener una red con mayor velocidad de conmutación, fácil diagnostico de problemas y la posibilidad mediante las VLAN, separar el trafico de voz y de datos en caso se instale una central IP a futuro.

Actualmente se tienen instalado una central analógica en la sede principal, y en las sucursales líneas directas, la mayor comunicación de voz entre trabajadores es vía RPM

movistar corporativo, con plan ilimitado, el cual lo tienen el 90% de trabajadores.

Para el tipo de oficina 1, se tendrá un equipo cisco 1721, con un modem teldat para la conexión a los aplicativos, de telefónica. Para Internet se tendrá un modem zyxel.

4.2.4 Seguridad

El Firewall DFL-210 NetDefend, provee de una solución de garantía en seguridad para su red, con funciones integradas tales como firewall, balanceo de carga, tolerancia de fallas, filtro de contenidos, autentificación de usuarios, aplicaciones de bloqueo para mensajería instantánea y peer-to-peer*, protección Denial of Service (DoS), IDS, IPS, integracion de listas negras para el servicio SMTP y soporte para redes virtuales (VPN).

Para la protección contra los virus informáticos, se ha propuesto la instalación del Antivirus Panda en su versión Panda Office Proteccion, el cual nos da una administración centralizada desde una consola Web, así como reportes Ejecutivos de la Red.

4.2.5 Descripción de la Topología Final

El tráfico de Internet y VPN están separados porque se ha visto que el tiempo de respuesta aumenta considerablemente, si estos servicios se juntan en un solo router. El trafico en el servidor de correo, afecta considerablemente el performance para la solución VPN. (En el Anexo E se adjunta los procedimientos de pruebas piloto de la solución).

Se ha contratado el Servicio de Infointernet, debido a se tiene un mejor rendimiento en el envío y recepción de datos. Además que se esta garantizando el 100% de la velocidad contratada, y nuestro servidor de correo siempre estará enviando data.

En la red de la Oficina Principal, el default Gateway por defecto será la IP 192.168.150.1/24, este corresponde a un Swicth Core D-LINK DGS-3627, L3 de 24 puertos, este equipo tendrá configurado rutas estáticas.

Para salir hacia Internet se enruta el trafico hacia el router R2 con IP LAN 192.168.150.3 correspondiente a un DFL-210 con Speedy Negocios Avanzado de 2048/512 kbps. Ver Fig. 4.2.

Para el acceso a las VPN y conexión a los aplicativos de telefónica, se enruta el trafico hacia el router R3 con IP LAN 192.168.150.4 el cual corresponde a otro DFL-210 con Speedy Negocios Avanzado de 2048/512 kbps, este equipo es únicamente exclusivo para las VPN y redirección de trafico hacia los aplicativos de telefónica. Ver Fig. 4.2

Para el acceso al Servidor de Correo y Servidor Web, se enruta el trafico hacia el router R1 con IP LAN 192.168.150.2 el cual corresponde al tercer DFL-210, que tiene una zona DMZ, y servicio de Internet Dedicado a 512Kbps (INFOINTERNET).

Para el acceso desde Internet a los servicios de correo y web de la empresa, el router R1 enviara las peticiones de conexión hacia zona DMZ. Ver Fig. 4.2

Las Oficinas Remotas, tendrán un router DFL-210 el cual realizara la conexión VPN con

la sede principal, además se realizara el filtro de paginas web. Ver Fig. 4.2

Para el tipo 1 de Oficinas remotas, el router DFL-210 realizara la conexión a los aplicativos de telefónica a través de su interfaz DMZ. Ver Fig. 4.2

El router que maneja tráfico de menor importancia es el router R2, debido que solo es para acceder a Internet con las restricciones de páginas web permitidas. Ver Fig. 4.2

En caso de un ataque en cualquiera de las sedes, los router DFL-210 tienen activado su protección licenciada con un IPS que se actualiza constantemente, y en la sede principal el Switch de Core, para ayudar a la seguridad, el D-Link Safeguard Engine, identifica y prioriza el trafico que afecta al CPU, para disminuir el tráfico no deseado (DoS) y proteger el funcionamiento del switch, mientras las listas de acceso (ACL) mejoran el uso de la red.

4.2.6 Disponibilidad

Debido al uso del mismo equipo router DFL-210 en la Oficina principal, y considerando que LAN puede salir a Internet por cualquiera de los routers, en caso falle el servicio de internet o el hardware, se tienen los siguientes casos:

- Si falla el router R2, se enruta desde el switch core, el tráfico de Internet por R1.
- Si falla el router R1 (problema de hardware), se remplaza por el router R2 con la configuración backup del router R1, luego se enruta el tráfico de Internet, por R1.
- Si falla el router R3 (problema de hardware), se remplaza por el router R2 con la configuración backup del router R3, luego se enruta el tráfico de Internet, por R1.

Para las sedes remotas, se considera usar 01 equipo DI-804, ya existente como contingencia que cumple funciones de VPN y NAT, hasta el recuperación del DFL-210.

4.2.7 Topología Final

El diagrama de la red final de datos, se muestra en la Fig. 4.2

4.3 Componentes de Servicios de Red

Se adjunta en el Anexo D las recomendaciones, para un mejor servicio.

4.3.1 Situación Actual de la Infraestructura de Correo

El Diagrama de la Infraestructura del Sistema de Mensajería Microsoft Exchange 2003 Standard Edition de la empresa SIC es como se muestra en la Fig. 4.3

Las características de esta arquitectura son:

- Existe un único servidor Exchange 2003 Standard Edition trabajando en producción, éste se define como servidor Back-End.
- No existe servidor de contingencia y en caso de caída del servicio de mensajería MAIL, no habrá servicio de correo.
- El servidor MAIL que contiene el Exchange Server 2003 tiene instalado como antivirus para escaneo de correos el NOD32.

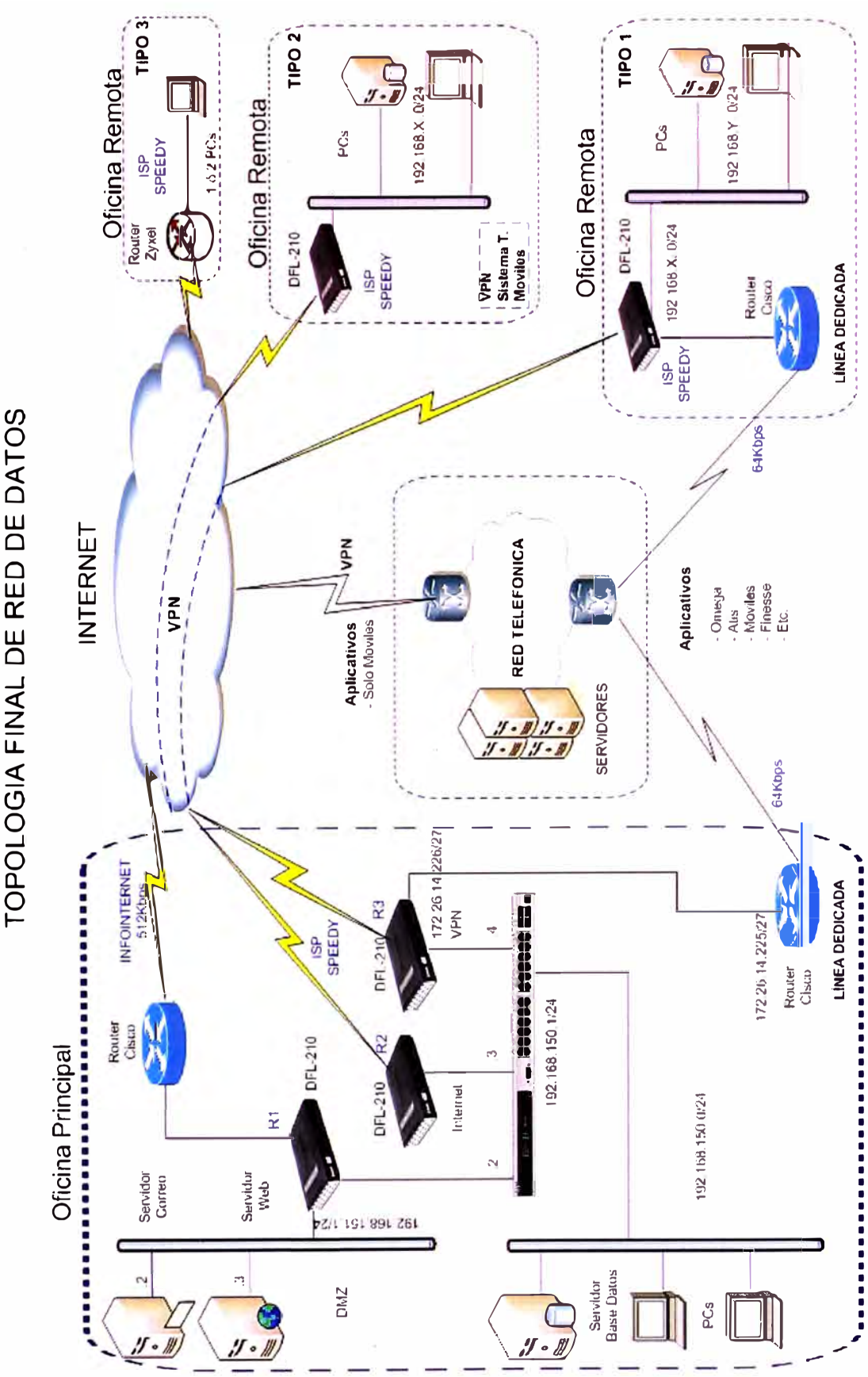


Fig. 4.2 Topología Final de la Red de Datos

Rol

El servidor Exchange 2003 Standard Edition MAIL se encuentra instalado en un

servidor independiente.

Fig. 4.3 – Diagrama de la Infraestructura de Mensajería

Carpetas Públicas

El uso de carpetas públicas se encuentra deshabilitado.

Modelo Jerárquico en la Organización de Exchange

En la Fig. 4.4 se muestra el modeló jerárquico del sistema de Mensajería Exchange 2003 y de los servicios instalados.

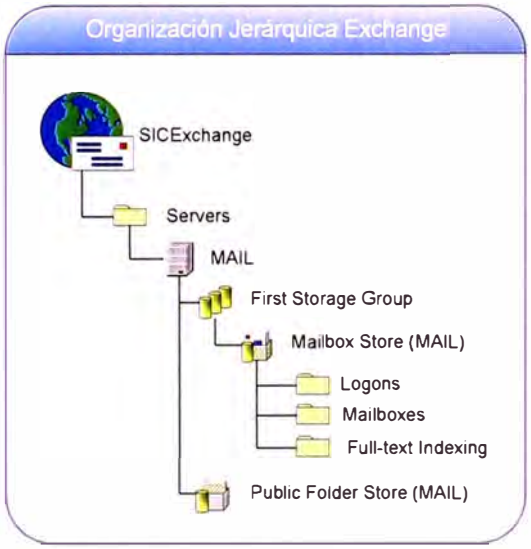


Fig. 4.4 – Organización Jerárquica Exchange

Base de Datos del Exchange:

Finalmente se tendrá la siguiente distribución, sobre los 300GB de disco duro

C: 20GB Operativo Windows Server 2003

D: 75GB Exchange Server 2003

E: 100GB BD Exchange 2003

F: 100GB Backup

Hardware usado del Servidor Exchange:

Características de Hardware:

4 GB de RAM

Intel (R) Xeon (TM) 3.00 GHz

HD: 300 GB

Cuenta con cinco particiones:

C: 20GB Operativo Windows Server 2003

D: 75GB Exchange Server 2003

E: 100GB BD Exchange 2003

F: 100GB Backup

Configuración de Red:

IP: 192.168.150.238/24

Gw: 192.168.150.244

DNS: 192.168.150.200

Flujo de Correos:

En la Fig. 4.5 se muestra la forma de envío de mensaje dentro del Sistema de Mensajería Exchange 2003 de la empresa SIC.

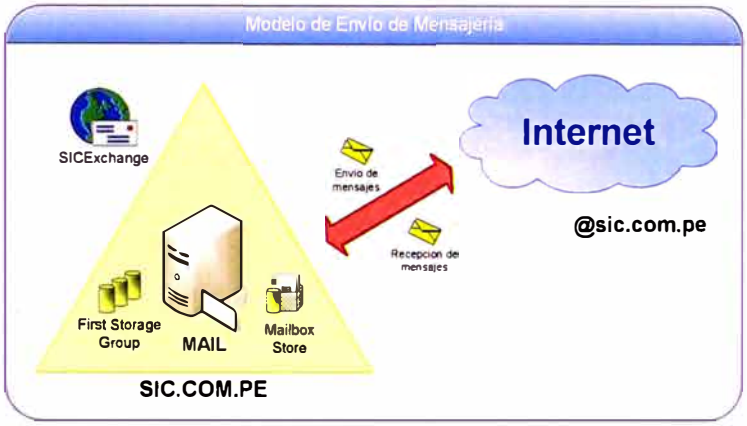


Fig. 4.5 – Modelo de Envío de Mensajería

- Los correos salen desde el servidor MAIL y de Internet llegan directamente al Servidor MAIL.
- Los usuarios pueden acceder a su correo vía OWA entrando a: http://mail.sic.com.pe/exchange. El acceso a su correo vía HTTP se realiza de forma no segura, porque no cuenta con ningún método de encriptación.
- Los usuarios acceden a su correo vía Outlook de forma local, conectándose al servidor Exchange.
- Los usuarios de la empresa SIC utilizan los siguientes clientes de mensajería Outlook 2003.

4.4 Instalación del Antivirus Corporativo

Panda Managed Office Protection es un servicio de suscripción basado en web. Libera a la pequeña y mediana empresa de tener que adquirir hardware adicional, personal de mantenimiento u otros recursos dedicados al Antivirus, manteniendo un alto nivel de

seguridad para todos sus PCs, portátiles y servidores, incluso los de oficinas remotas. (Ver Fig. 4.6).

Panda Manager Office Protection está complementado por auditorías de seguridad periódicas, beneficiándose de las tecnologías de Inteligencia Colectiva.

Al ser un Servicio Alojado (Hosted Service), la consola web siempre está disponible y permite gestionar la protección en cualquier momento desde cualquier lugar, incluyendo las oficinas remotas no conectadas a la LAN.

Ofrece Seguridad como Servicio a través de un portal de gestión y permite a las empresas delegar, si quieren, la gestión de su seguridad a proveedores de servicios especializados. Se adjunta en el Anexo F reportes del Antivirus.

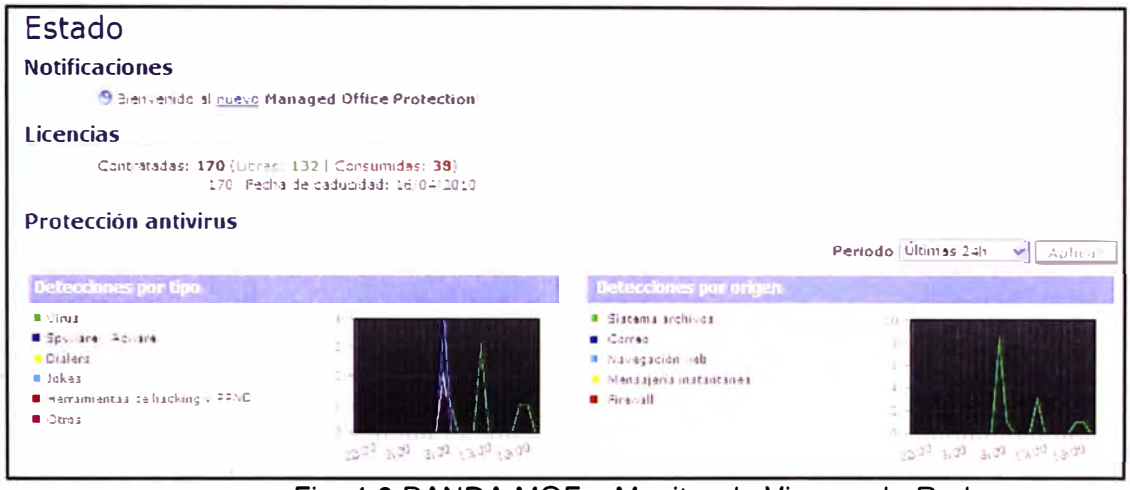


Fig. 4.6 PANDA MOF – Monitor de Virus en la Red.

4.5 Monitorización con Nagios

Nagios es un sistema open source de monitorización de redes ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados ó SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Permite la visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros, etc.

Se adjunta en el Anexo G, los reportes mostrados y grafica de estado, que se pueden obtener de esta herramienta Nagios, se usa otra configuración realizada, en otra empresa.

4.6 Tiempo de Respuesta de las Sucursales

Se muestra a continuacion en la tabla N° 4.1 los tiempo de respuesta, luego de la interconexion de sucursales, se considera escenarios sin trafico.

Para el caso de los aplicativos de telefónica: atis, gestel, omega, citrix, el tiempo de respuesta varia entre 40 mseg y 80 mseg, estos aplicativos no consumen mucho ancho de banda, por lo cual el enlace dedicado de 64 kbps es suficiente, incluso para los usuarios que se conectan remotamente. El promedio de utilizacion del BW de la línea dedicada es menor al 50%. Para el local ubicado en el Centro Comercial Megaplaza de los Olivos, que posteriormente tendra 30 ubicaciones de postventa Moviles, las cuales trabajaran en horario continuo de 10:00 - 22:00 hrs, se considera subir el BW a 512kbps, para que puedan trabajan sin demora en el tiempo de respuesta de la aplicaciones.

TABLA N° 4.1 Tiempo de Respuesta de la Sucursales.

Local	Departamento	IP Publica	IP LAN	Tiempo de Respuesta
Av. Venezuela 617 Breña	LIMA	201.240.17.48	10.25.4.130	21.54 ms
C.C Megaplaza Los Olivos	LIMA	190.41.32.211	172.26.31.130	20.20 ms
Av. Los Heroes 458 SJM	LIMA	200.48.135.185	172.26.22.226	23.42 ms
Pz. Solidaridad Villa el Salvador	LIMA	200.48.135.186	10.25.8.162	20.97 ms
Av. Alfredo Mendiola 3693 – Los Olivos	LIMA	190.40.222.180	172.26.22.130	19.55 ms
Mz B lt14 - El Porvenir Ate Vitarte	LIMA	190.40.221.165	10.25.8.130	20.13 ms
Av. 28 de Julio Chosica	LIMA	190.41.154.199	10.25.3.130	19.03 ms
Av. Gran Chimu 913 SJL	LIMA	190.41.175.118	192.168.170.2	25.67 ms
Jr. 2 de Mayo 324 Cañete	LIMA	190.41.247.41	172.26.45.34	22.18 ms
Jr. Ica 586	HUANCAYO	190.41.192.160	10.25.28.1	24.60 ms
Calle Real 377	HUANCAYO	190.41.188.1	192.168.163.3	22.53 ms
Pz. Carrion 181-185	CERRO DE PASCO	190.41.192.6	10.25.25.65	22.47 ms
Jr. Ancash 395	LA MERCED	190.41.97.140	10.25.27.1	22.61 ms

CAPITULO V
COSTOS DEL PROYECTO

5.1 Costo de Inversión

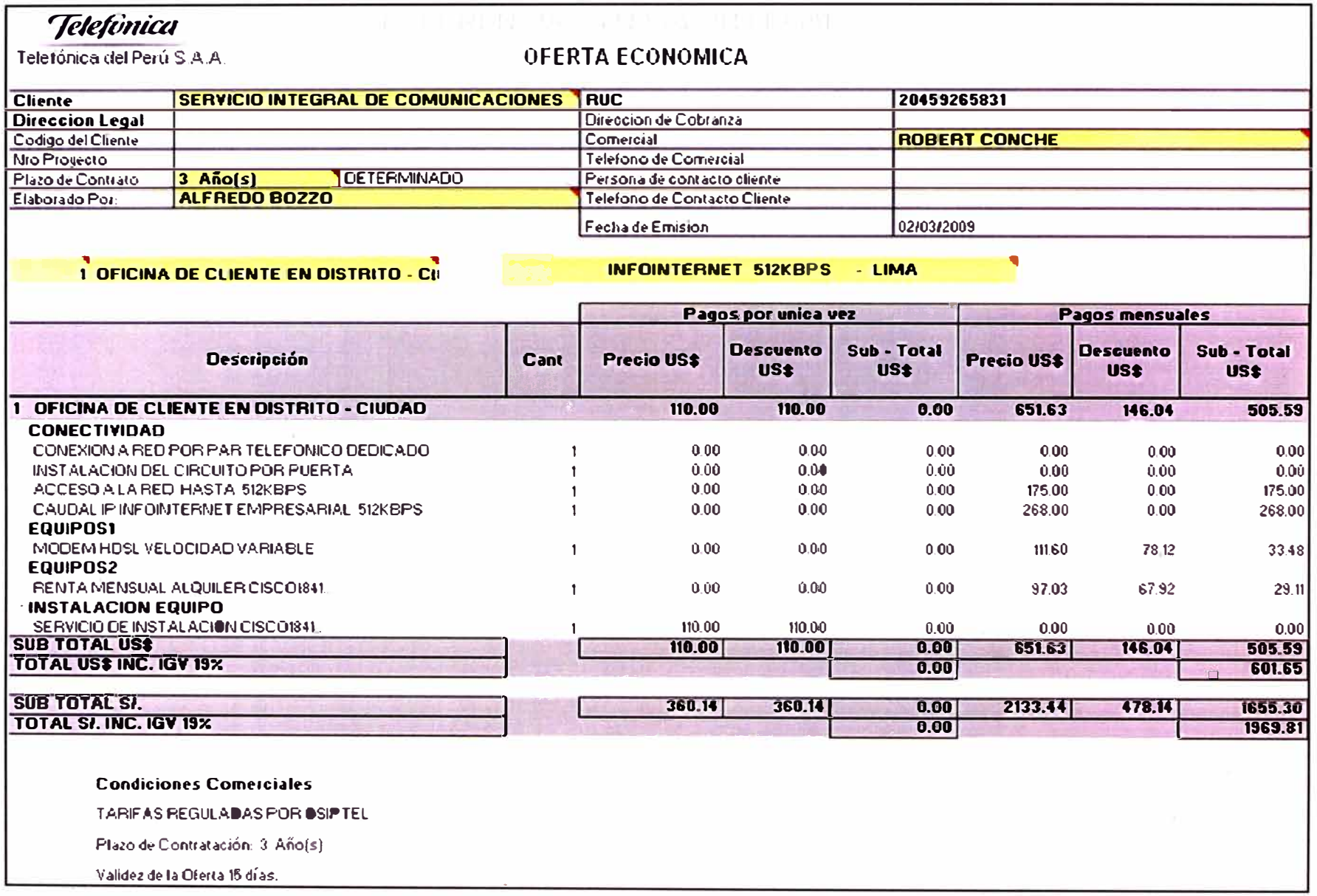
Tenemos como costo de Inversión los equipos de comunicación para la solución, así como los gabinetes para los mismos. Se muestra en la tabla N° 5.1 los costos de inversión.

TABLA N° 5.1 Costo de Inversión

Item	Descripcion	Ubicación	Cant.	Precio	Total
01	xStack® Managed 24-Port Gigabit Layer 3 Switch	Sede Principal	3	$ 1,800.00	$ 5,400.00
02	SWITCH 3COM BASELINE 2226 PLUS	Sede Principal	4	$ 189.41	$ 757.64
03	NetDefend DLink DFL210	Sede Principal	3	$ 420.00	$ 1,260.00
04	NetDefend DLink DFL210	Sucursales	13	$ 420.00	$ 5,460.00
05	SWITCH 3COM BASELINE 2226 PLUS	Sucursales	13	$ 189.41	$ 2,462.33
06	GABINETES PISO 600X600X2000 VIDR.S/MARCO	Sede Principal	1	$ 487.20	$ 487.20
07	GABINETE MURAL 6U FONDO 450. Puerta metalica vidriada	Sede Principal	4	$ 96.80	$ 387.20
08	GABINETE MURAL 6U FONDO 450. Puerta metálica vidriada	Sucursales	13	$ 96.80	$ 1,258.40
				SubTotal	$ 17,472.77
				Igv	$ 3,319.83
				Total	$ 20,792.60

Según la Fig. 5.1 también tenemos el costo de Instalación del Servicio INFOINTERNET requerido para la solución, por un monto igual a $110.00.

Este monto según la promoción puede tener costo $0.00



Telefónica

Telefónica del Perú S.A.A.

OFERTA ECONOMICA

Cliente	**SERVICIO INTEGRAL DE COMUNICACIONES**	**RUC**	**20459265831**
Direccion Legal		Direccion de Cobranza	
Codigo del Cliente		Comercial	**ROBERT CONCHE**
Nro Proyecto		Telefono de Comercial	
Plazo de Contrato	**3 Año(s)** DETERMINADO	Persona de contacto cliente	
Elaborado Por:	**ALFREDO BOZZO**	Telefono de Contacto Cliente	
		Fecha de Emision	02/03/2009

1 OFICINA DE CLIENTE EN DISTRITO - Cl **INFOINTERNET 512KBPS - LIMA**

Descripción	Cant	Pagos por unica vez			Pagos mensuales		
		Precio US$	Descuento US$	Sub - Total US$	Precio US$	Descuento US$	Sub - Total US$
1 OFICINA DE CLIENTE EN DISTRITO - CIUDAD		**110.00**	**110.00**	**0.00**	**651.63**	**146.04**	**505.59**
CONECTIVIDAD							
CONEXION A RED POR PAR TELEFONICO DEDICADO	1	0.00	0.00	0.00	0.00	0.00	0.00
INSTALACION DEL CIRCUITO POR PUERTA	1	0.00	0.00	0.00	0.00	0.00	0.00
ACCESO A LA RED HASTA 512KBPS	1	0.00	0.00	0.00	175.00	0.00	175.00
CAUDAL IP INFOINTERNET EMPRESARIAL 512KBPS	1	0.00	0.00	0.00	268.00	0.00	268.00
EQUIPOS1							
MODEM HDSL VELOCIDAD VARIABLE	1	0.00	0.00	0.00	111.60	78.12	33.48
EQUIPOS2							
RENTA MENSUAL ALQUILER CISCO1841	1	0.00	0.00	0.00	97.03	67.92	29.11
INSTALACION EQUIPO							
SERVICIO DE INSTALACION CISCO1841	1	110.00	110.00	0.00	0.00	0.00	0.00
SUB TOTAL US$		**110.00**	**110.00**	**0.00**	**651.63**	**146.04**	**505.59**
TOTAL US$ INC. IGV 19%				**0.00**			**601.65**
SUB TOTAL S/.		**360.14**	**360.14**	**0.00**	**2133.44**	**478.14**	**1655.30**
TOTAL S/. INC. IGV 19%				**0.00**			**1969.81**

Condiciones Comerciales

TARIFAS REGULADAS POR OSIPTEL

Plazo de Contratación: 3 Año(s)

Validez de la Oferta 15 días.

Fig. 5.1 Oferta Económica Infointernet 512 Kbps

5.2 Costo de Operación y Mantenimiento

Con respecto al servicio de Internet Actual en todas las sucursales se tiene la información en la Fig. 5.2

Costos y Velocidades Speedy / Año 2008

LOCAL	SPEEDY	Vel. kbps	Empresa	Tel. Speedy	Direcc. Comercial			Costo
CENTRAL	BUSINESS	2000	Lideres en Servicio Sac	376-1032	Av. Gran Chimu 384 Zarate	LIMA	San Juan Lurigancho	S/. 980.00
CENTRAL	BUSINESS	900	SIC	459-6646	Av. Gran Chimu 360 Zarate	LIMA	San Juan Lurigancho	S/. 309.99
BREÑA	BUSINESS	900	Lideres en Servicio Sac	331-1577	Av. Venezuela 617 Chacra Colora	LIMA	BREÑA	S/. 309.99
MEGAPLAZA	BUSINESS	1200	Lideres en Servicio Sac	521-4141	Centro Comercial Megaplaza Los	LIMA	LOS OLIVOS	S/. 439.99
SAN JUAN	BUSINESS	900	Lideres en Servicio Sac	2764484	Av. De los Herores 458 A	LIMA	San Juan Miraflores	S/. 309.99
VILLA	BUSINESS	900	Lideres en Servicio Sac	287-5322	Plaza de la Solidaridad Mz ZC Se	LIMA	Villa el Salvador	S/. 309.99
OLIVOS	BUSINESS	900	Lideres en Servicio Sac	486-7061	Av. Alfredo Mendiola 3693 Urb. P	LIMA	LOS OLIVOS	S/. 309.99
VITARTE	BUSINESS	1200	Lideres en Servicio Sac	351-8270	Mz B lt 14 Asoc El Porvenir	LIMA	ATE VITARTE	S/. 439.99
CHOSICA	CONVENCIOI	900	SIC	361-1747	Av. 28 de Julio 128	LIMA	Chosica	S/. 229.99
ZARATE 9	CONVENCIOI	900	Lideres en Servicio Sac	376-3517	Av. Gran Chimu 913 A Zarate SJL	LIMA	San Juan Lurigancho	S/. 229.99
CAÑETE	CONVENCIOI	900	SIC	284-7360	Jr. 2 de Mayo 324 Imperial	LIMA	CAÑETE	S/. 229.99
HYO ICA	BUSINESS	1200	SIC	64-214628	Jr. Ica 586	HUANCAYO	HUANCAYO	S/. 439.99
HYO REAL	BUSINESS	900	SIC	64-227758	Calle Real 377	HUANCAYO	HUANCAYO	S/. 309.99
CERRO DE PAS	BUSINESS	900	SIC	63-425238	Plaza Carrion 181 -185	CERRO DE PASCO	CERRO DE PASCO	S/. 309.99
LA MERCED	BUSINESS	1200	SIC	64-531169	Jr. Ancash 395	MERCED	MERCED	S/. 439.99
							TOTAL	S/. 5,599.86

Fig. 5.2 - Costos Actuales ISP antes del proyecto.

5.2.1 Costo Mensual por los servicios contratados al ISP

Se muestra en la Tabla N° 5.2 los precios finales y velocidades modificadas.

TABLA N° 5.2

Item	Descripción	Ubicación	Cant.	P. Unit. c/igv	Total
01	Speedy 2000 (2048/512kbps) N.Avanzado al 25%	Sede Principal	2	S/. 309.99	S/. 619.98
02	Infointernet 512kbps 1:1	Sede Principal	1	S/. 1,969.81	S/. 1,969.81
03	Speedy 2000 (2048/512kbps) N.Avanzado al 25%	Sucursales	13	S/. 309.99	S/. 4,029.87
				TOTAL	**S/. 6,619.66**

Este costo será el que finalmente se pague, de forma mensual, una vez finalizado el proyecto.

5.2.2 Costo de Mantenimiento por Servicios de Red y Soporte

Se considera para el mantenimiento de la red y supervisión de la misma, un total de 3 personas, quienes cumplirán las funciones según Tabla N° 5.3

TABLA N° 5.3

Item	Descripción	Ubicación	Total
01	Administrador de Red	Sede Principal	S/. 3,000.00
02	Jefe de Soporte	Sede Principal	S/. 1,500.00
03	Tec. Soporte	Sede Principal	S/. 1,000.00
		TOTAL	**S/. 5,500.00**

5.2.3 Costos de Software

Aquí se especifican los costos de software, pagos Anuales. Ver Tabla N° 5.4

Antivirus Corporativo, así como actualización del IPS.

TABLA N° 5.4

Item	Descripción	Cant.	P. U. c/igv	Total
01	Antivirus PANDA MOP	170	$ 16.95	$ 2,881.50
02	IPS Update Serv. x 12 meses DFL.210	16	$ 89.25	$1,428.00
			TOTAL	**$ 5,737.50**

CONCLUSIONES

El modelo en la arquitectura de red propuesto, es la mejor solución para Oficina Principal, debido a que se consideran todas las variables de conectividad, asegurando la disponibilidad del servicio, y eventualidad de falla un equipo router DF-210

La seguridad de la información se tomo como punto importante, y el equipo router al tener un Firewall activo, con la solución IPS estamos seguros que se responderá ante un ataque a la red.

Se cumplió el objetivo la instalación de un antivirus corporativo, PANDA Office Protección, es muy importante tener el control y el estado de la red con respecto a los virus, tenemos claro que es muy importante la Seguridad de la red perimetral, pero también es importante la seguridad desde las PCs con un antivirus y firewall personal, esto permite tener una barrera mas para proteger nuestra información.

La instalación de un antivirus corporativo, permitió un manejo ordenado de la red, nos indica que en sedes se esta propagando el virus, o código maliciosos, y podemos desde cual sitio conectado a Internet revisar la consola Web y ejecutar comando de limpieza.

Ahora con la interconexión de las Sucursales con la sede principal, y el apoyo del área de sistemas, es posible tener los reportes en tiempo real de las ventas de la empresa, el stock de los productos, las transferencias de mercadería, backup programado de la información de todas las sucursales que manejan un servidor de base de datos.

Gracias a la interconexión la empresa puede tomar decisiones de ventas y estrategias de negocio, ya que sabe en tiempo real el estado de producción de las sucursales, se permite un monitoreo a nivel de Ventas, ingreso y salida de caja. Esta información es muy valorada por la gerencia de ventas y gerencia general.

Las sucursales Tipo 3, llamados puntos de ventas, podrán realizar conexiones tipo PPTP (con Windows XP), hacia la sede principal o alguna sucursal, el router DFL-210, se encargara de enrutar, y que la usuario Remoto, pueda acceder solamente a los aplicativos de Telefónica.; ayudando así a verificar sus ventas.

Al tener un firewall en el cual se aplique reglas de salida a Internet, se aprovecha mayor el tiempo de trabajo del personal, ya que a veces utiliza mal los recursos. Esto genera mayor productividad por parte del personal, al no distraer su labor.

Gracias a la interconexión VPN, los programadores desde la sede principal, se pueden conectarse a los servidores de las sucursales, realizando tares de corrección, actualización, backup de base de datos, y otras transacciones.

Para el área de soporte técnico, la interconexión de sucursales ha ayudado a mejorar los tiempos de respuesta en atención, debido a que se conectan remotamente a las computadoras cliente, que tiene problema mediante una herramienta de control remoto VNC, diagnosticando el problema y procediendo a la solucion, para luego derivar si es necesaria la presencia de un técnico de soporte. Esto ahorra costo de movidad para el area de soporte y tiempo perdido; al trabajador le cuesta tiempo de trabajo al no contar con todos los servicios de red y aplicaciones operativos.

En líneas generales este mejora, al interconectar la sucursales y servidores a nivel nacional, ayuda a mejorar la productividad de la empresa, en todas sus áreas, gerencia, ventas, cajas, ahorrando costos como el área de soporte técnico y horas hombre.

Un tema muy importante, es tener un personal que se encargue la red de datos, debido a que se solucionan muchos problemas con conocimientos de ruteo, en este trabajo, se observa que son puntos básicos, el conocimiento de rutas estáticas y NAT, así como los procedimientos de reporte y seguimiento cuando falla una línea dedicada.

Muy importante también es tener los servicios publicados hacia Internet y tener a los servidores de Correo y Web en una Zona DMZ, en la cual si hubiera un caso de intrusión, no se vea perjudicada la red Lan.

Los tiempos de respuesta hacia todos los servidores a nivel nacional son aceptables, logrando realizar transacciones de forma exitosa, por el area de soporte sistemas, y aplicativos de administración, también el area de soporte realiza atenciones remotamente hacia todas las sucursales a nivel nacional sin problemas.

ANEXOS

ANEXO A
POLITICAS Y RECOMENDACIONES – CABLEADO ESTRUCTURADO

Fundamentos

El presente diseño proporcionará a las instituciones seleccionadas, un cableado estructurado de red que soportará la implementación de nuevas tecnologías, facilitando la incorporación de nuevos equipos. Para el diseño se ha contemplado los estándares mundiales de la norma EIA/TIA 568B.

Especificaciones del canal de comunicación

El sistema de cableado estructurado permitirá la integración de todos los dispositivos, proveyendo un canal de comunicación adecuado a las necesidades actuales y futuras. Este canal es de Categoría 6 de acuerdo a la EIA/TIA 568B. El sistema de conectorización soportado por el Patch Panel y el Jack RJ45 deberá cumplir con la norma T568A y T568B.

Especificaciones del cableado horizontal

Comprende el tendido del cable desde el RACK DE COMUNICACIONES ubicado en la Oficina Remota (preferentemente en el ambiente de cómputo) hasta cada estación de trabajo. El cable utilizado cumplirá la distancia máxima permitida por la norma de hasta 90 metros desde la terminación mecánica del medio en el Rack de comunicaciones hasta la toma de señal de datos. No se usarán empalmes para ningún tramo en el cableado horizontal. Los cables serán instalados a través de canaletas de PVC que permitan llegar hasta cada estación de trabajo.

En cada Rack de comunicaciones se implementará los paneles de distribución de acuerdo a la norma, y se usarán patch cords para conexión de estos paneles con los equipos de comunicación, Tanto los patch cords como los cables de conexión de las estaciones a las tomas de señal son de Categoría 6, se debería adjuntar las pruebas de Laboratorios Independientes (UL o ETL). Del mismo modo se debería incluir los valores obtenidos por el canal para cada frecuencia propuesta por el estándar TIA/EIA 568B

Metodología para la instalación del sistema de datos

- La **canalización** estará a cargo de SIC, debido a los ductos predispuestos en el diseño arquitectónico de cada institución. El cableado horizontal será llevado a
- través de ductos tomando en cuenta la supervisión de un especialista en cableado estructurado, para el cumplimiento de las normas y reglamentos de cableado tales como del 40 % de capacidad inicial, permitiendo un adicional; para una expansión futura, sobre la base del 60% de llenado máximo de ductos, tal como lo indica la norma EIA/TIA 569A. Asimismo, se deben tomar en cuenta los radios de curvatura para la fluidez del cableado.
- Los puntos de red y eléctrico se recomiendan instalarse a una distancia de 60 cm. del piso.

- Cada Oficina Remota debería llevar un Rack adosable con bisagra que permita su mantenimiento por la parte posterior. El Rack debería contener un concentrador (switch) de igual número de puertos que los equipos a conectarse más una holgura para expansiones futuras. Adicionalmente, debería instalarse un Patch panel con conectores RJ-45 Categoría 6 y su respectivo ordenador de cables.
- Se deberá, indicar mediante etiquetas identificadores los conectores de los paneles de distribución, y los cables deben estar señalizados en cada extremo con etiquetas adhesivas resistentes al polvo y humedad, codificados según estándares para su fácil identificación.
- Los responsables de Cableado Estructurado deberá, contar con la siguiente información una vez concluido el trabajo en cada oficina:

  Los planos en formato impreso y electrónico de los sistemas eléctricos y de datos detallados, donde se indicarán las rutas seguidas por el cableado de datos y cableado eléctrico, así como las ubicaciones de salidas, Rack y tableros de control eléctrico (los planos serán en blanco y negro).

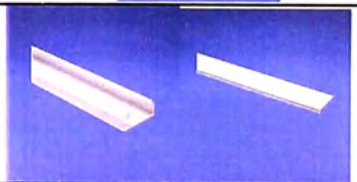
  Las hojas de evaluación en formato impreso y electrónico de todos y cada uno de los puntos del cableado estructurado, a fin de certificar su correcto funcionamiento e implementación según la categoría 6, para lo cual se realizará la certificación del cableado CAT6 punto por punto. Todos estos documentos deberían formar parte de un **acta de entrega de compromiso** al final de los trabajos.

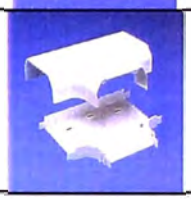
Materiales Recomendados

Descripción	**Bracket adosable**	
Beneficios	Permite el ordenamiento de equipos de comunicación: módems, ruteadores, switches, y la concentración de la red LAN.	
Descripción	**Patch Panel**	
Beneficios	Es un panel que cumple la función de permitir la inserción de los jacks RJ-45 que servirán para conectar las computadoras.	
Descripción	**Jack para Patch Panel**	
Beneficios	Módulo de conexión de datos, del tipo RJ-45 (patch panel) para datos. Pueden ser de Categoría 6 (recomendable), con 8 posiciones y 8 cables universales.	

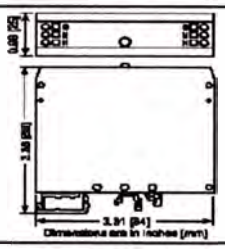
Descripción	**Ordenador**	
Beneficios	Ordenador de 2 UR	
Descripción	**Patch Cord**	
Beneficios	Patch Cord de 10 ft Cat 6 (Category 6 patch cord with *TX6™ PLUS* Modular Plug on both ends (10 ft))	

Accesorios de Cableado Horizontal

Descripción	**Cable UTP de 4 pares**	
Beneficios	Cable UTP de 4 pares. Categoría 6.	
Descripción	**CJ688TPBU**	
Beneficios	Módulo de conexión de datos, del tipo RJ-45 (patch panel) para datos. Recomendable si es de Categoría 6, con 8 posiciones y 8 cables universales	
Descripción	**Face Plate**	
Beneficios	Kit de Face Plate para 4 salidas de datos con tapa de cubierta atornillable.	
Descripción	**Caja de Montaje**	
Beneficios	Caja de Montaje para face plate de datos. (+ Caja de montaje eléctrica)	
Descripción	**Canaleta**	
Beneficios	Base y tapa de Canaleta de dos metros de longitud.	
Descripción	**Tabique divisor**	
Beneficios	Permite dividir una canaleta en dos rutas (datos y eléctrico)	
Descripción	**T70ICIW**	

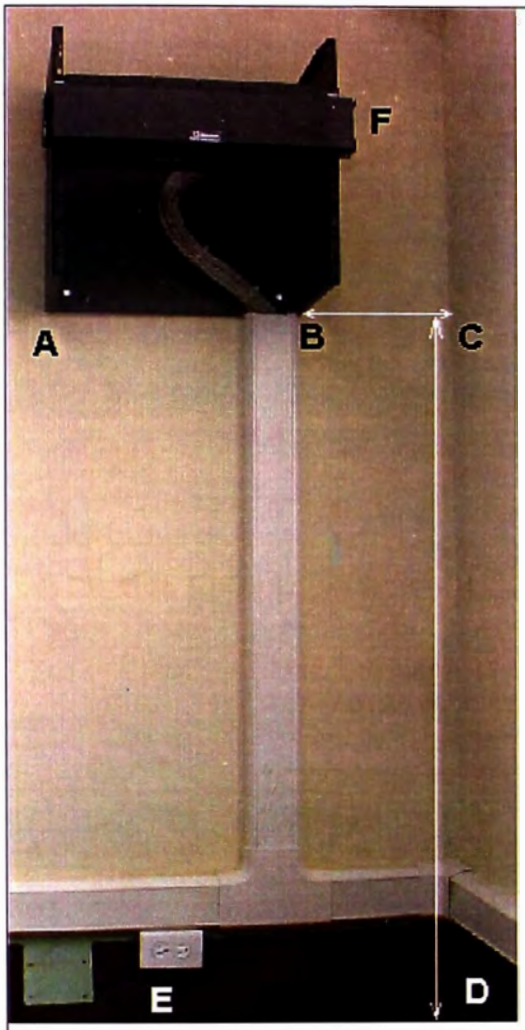
Beneficios	Inside Corner Fitting. Used to join sections of T-70 Raceway at inside corners	
Descripción	**Angulo Recto**	
Beneficios	Usado para unir dos secciones en ángulo recto.	
Descripción	**Tapa Final**	
Beneficios	Usada para las terminaciones de la canaleta.	
Descripción	**Tee de derivación**	
Beneficios	Usado para unir secciones de canaletas en intersecciones "T".	

Accesorios de Energía

Descripción	**Estabilizador**	
Beneficios	Proporciona una adecuada alimentación a los equipos de cómputo, controlando los niveles de voltaje.	
Descripción	**Supresor de Transitorios (TVSS)**	
Beneficios	Elemento electrónico que protege la red de computadoras bloqueando transitorios (os cilaciones intempestivas de voltaje y corriente)	
Descripción	**Tablero Eléctrico**	
Beneficios	Permite la organización de los circuitos eléctricos controlados por llaves termo magnéticas. Para el caso de cómputo se recomienda llaves de 20A para el control de 10 PC's estándar.	
Descripción	**Tomacorrientes**	
Beneficios	Tomacorrientes dobles y Placas tipo Leviton	
Descripción	**Indeco**	
Beneficios	Cable eléctrico TW#12 (rojo=33 mt, negro=33mt amarillo=33mt)	
Descripción	**Indeco**	
Beneficios	Cable eléctrico TW#6	

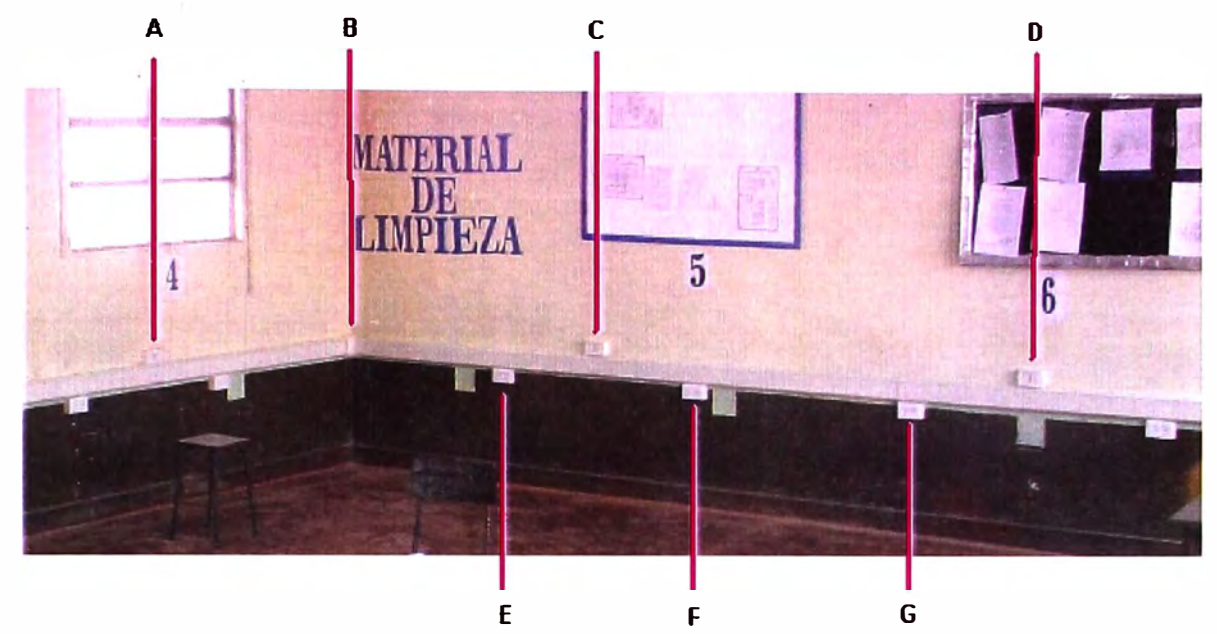
Estándares de Instalación

Rack de Comunicaciones



Caso	Descripción	Segmento	Dist.
1	Distancia del Rack hacia la esquina de la pared	B-C	0.30 mt.
2	Altura del Rack respecto al piso	C-D	1.80 mt.
3	Posición del tomacorriente que suministra energía al Rack	E	Entre A y B
4	Ubicación del Patch Panel	F	

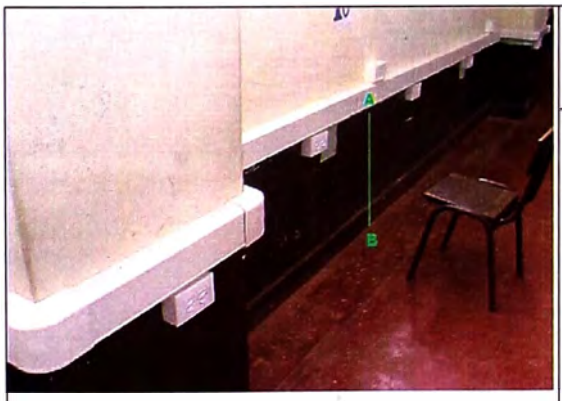
1	Eléctrico	tomacorrientes bipolares de doble toma con espiga conectada a tierra	



Distancias Referenciales entre las tomas de Datos y Eléctricas

Caso	Toma	Descripción	Distancia	Mínimo	Máximo
1	Datos	Distancia toma de datos hacia la esquina del ambiente	A-B	1.60 mt.	1.60 mt.
2	Datos	Distancia toma de datos hacia la esquina del ambiente	B-C	1.60 mt.	1.60 mt.
3	Datos	Distancia entre toma de datos	C-D	1.60 mt.	2 mt.
4	Eléctrica	Distancia entre tomas eléctricas	E-F	0.80 mt.	1 mt.
5	Eléctrica	Distancia entre tomas eléctricas	F-G	0.80 mt.	1 mt.

Distancias referenciales entre las canaletas y el nivel de piso



Item	Descripción	Seg-mento	Normal	Variación
Canaleta	Distancia desde el piso hasta el nivel inferior de la canaleta	A-B	0.6 mt	+/- 0.15 mt

ANEXO B
POLÍTICAS Y RECOMENDACIONES GENERALES

Capítulo: INSTALACIONES ELECTRICAS

Previo a la instalación de equipos informáticos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

Para equipos de cómputo es conveniente disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

Deberá disponerse de un pozo a tierra (cuya resistencia no debe ser mayor a 5 ohmios), conectado al Sistema Eléctrico que alimenta los equipos de cómputo. Asimismo se etiquetará el cableado, las extensiones y los tableros de distribución eléctrica.

Asegurar un suministro de energía eléctrica de voltaje estable con la ayuda de sistemas de estabilización de voltaje, supresores de picos y unidades de potencia contra cortes fluidos (UPS).

Mantener en lugar visible los procedimientos de maniobras de encendido de emergencia.

Evitar los cableados sueltos o dispersos, éstos deberán entubarse.

Es necesario establecer puntos centrales de corte de fluido eléctrico, a nivel edificio o piso.

Capítulo: INSTALACIONES DE AGUA Y DESAGUE

Se recomienda que los sistemas de agua y desagüe se encuentren a niveles inferiores al Centro de Cómputo. Se verificará periódicamente el estado de las griferías y cañerías a fin de evitar posibles inundaciones.

Capítulo: INSTALACIONES DE AIRE ACONDICIONADO

Es recomendable contar con servicio de aire acondicionado, evitando que esté próximo a material inflamable, asimismo contará con las instrucciones de operación visibles.

Verificar que el aire acondicionado esté alimentado con agua refrigerada de un suministro confiable. Caso contrario se considerará la posibilidad de un sistema de refrigeración de agua y bombas de circulación alternativas.

Asegurar que las tomas de aire de los equipos se encuentren ubicados en zonas no susceptibles de ser obstruidas.

Capítulo: PROTECCIÖN CONTRA INCENDIOS

Capacitar al personal en el uso y mantenimiento del equipo contra incendio.

Disponer de un plano que contenga todas las fuentes de suministros posibles de agua, con su capacidad estimada en cada caso.

Evitar que las paredes, pisos y techos contengan material inflamable, recomendándose instalar equipos de alarma detectores de humo.

Para combatir los incendios producidos por equipos eléctricos se deben utilizar

extintores, hechos preferentemente de bióxido de carbono, productos químicos secos y líquido vaporizado. Estos estarán al alcance inmediato, preservando la vigencia química del extintor, e identificando su localización en el respectivo plano.

Es recomendable que exista suficiente iluminación en los alrededores del edificio, las ventanas o mamparas se protegerán de manera que se evite el impacto de piedras o material incendiario.

Capítulo: POLÍTICAS GENERALES

Es recomendable que el acceso a los centros de cómputo sea restringido al personal autorizado, contándose con un registro de entradas y salidas de visitantes.

Recomendamos mayor vigilancia y control. Se deben incorporar guía de salida de equipos a fin de tener un control estricto de los activos.

Que los procedimientos de limpieza de los ambientes eviten:

- Levantar el polvo en áreas donde existan éstos.
- Golpear los módulos o muebles de computadora.
- Utilizar material inadecuado para la limpieza de los equipos.

Se ha observado una excesiva cantidad de polvo en ambientes críticos por las comunicaciones e información que se maneja.

Los equipos de cómputo no deberán estar encendidos si no van a ser utilizados.

Las microcomputadoras y terminales tendrán un soporte logístico, que permita un apropiado mantenimiento preventivo (filtros para pantalla y kits limpieza). Es conveniente, asimismo que las microcomputadoras tengan instalado un software de protección de pantalla.

Se recomienda que el servicio de mantenimiento de los equipos de cómputo lo realice un proveedor que garantice las buenas prácticas.

No es conveniente el ingreso de alimento y bebidas en las salas que cuentan con equipos de cómputo.

Disponer de los medios físicos adecuados y suficientes, así como la capacitación y reglamentación para prevenir siniestros y/o minimizar sus efectos.

Contará con un plan de contingencia, así como con estrategias adecuadas para hacer frente a los desastres. Entre el área de cómputo y las demás áreas, se establecerán acuerdos acerca de las condiciones bajo las cuales el plan de contingencia ha de ser activado, considerándose la duración probable de la falta de servicio, y la pérdida (total o parcial) de la capacidad de procesamiento en una o varias instalaciones etc.

Considerar una de las oficinas remotas como NODO DE RESPALDO (NOC), para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad y disponibilidad.

Constituir un Comité de Seguridad a nivel institucional, que velará por el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Jefe de Cómputo u otro funcionario de nivel equivalente

Capítulo: MEDIDAS DE AHORRO DE ENERGÍA

En iluminación, la medida más efectiva es el apagado de las luces que no se utilizan. Se recomienda utilizar lámparas de bajo consumo (LFC) en todos aquellos lugares en que las lámparas incandescentes sean de más de 40W y estén prendidas más de 4 horas por día. Si bien las LFC son más caras, el gasto se ve compensado por un menor consumo eléctrico y una mayor vida útil (consumen el 20 % de lo que consume una incandescente y duran alrededor de 4 veces mas).

Seleccione adecuadamente el reemplazo de la lámpara incandescente. Idealmente deberá sustituir aquellas de mayor potencia y tiempo de uso. Generalmente estas lámparas se ubican en la cocina, comedor o sectores iluminados durante toda la noche.

Sólo utilice LFCs en ambientes en donde las lámparas no estén sometidas a muchos encendidos y apagados en poco tiempo. (p.e. no en baños)

Muchos aparatos, entre ellos los TVs, videos, microondas, equipos de audio, equipos de aire acondicionado, computadoras personales (PCs), etc. continúan consumiendo energía eléctrica aún cuando parezca que se encuentran apagados. La suma de estos pequeños consumos pueden alcanzar un valor significativo. Desenergícelos completamente cuando no los utilice.

Utilizar adecuadamente el modo de ahorro de energía que tienen las computadoras, las mismas que se desactivan cuando no están siendo utilizadas

Capítulo: AMBIENTE

Tanto en el caso de los equipos de aire acondicionado, como en el de las estufas eléctricas (también a gas) las medidas más efectivas para economizar el consumo energético son:

- No sobrecaliente ni sobreenfríe los ambientes.
- Mantenga cerradas las puertas del ambiente que está climatizando, evitando así desperdiciar energía en ambientes en donde no Ud. se encuentra.

Los equipos de aire acondicionado tienen distintas eficiencias. A veces un precio algo más elevado al comienzo tiene una amplia recompensa en su factura de energía eléctrica. Asesórese al respecto.

Evite las excesivas infiltraciones de aire por puertas y ventanas sellándolas adecuadamente.

ANEXO C
DATOS TECNICOS DE LOS EQUIPOS

DFL-210	INFORMACIÓN TÉCNICA
PUERTAS	LAN : 04 Ports 10/100 Base-TX Autosensing WAN : 01 Port 10/100 Base-TX Autosensing DMZ : 01 Port Configurable 10/100 Base-TX Autosensing Serial : RS-232 (9 pines)
CPU	Risc 266 MHz
SDRAM	128MB
FLASH	128MB
RENDIMIENTO Y CAPACIDADES MÁXIMAS	
FIREWALL PERFORMANCE	80 Mbps
AES/3DES PERFORMANCE	25 Mbps
CURRENT SESSION	12,000
NEW SESSION/SECONDS	2,000
POLÍTICAS	500
USUARIOS SOPORTADOS	150
MODOS DE OPERACIÓN FIREWALL	
LAYER 3 MODE	Modo Route y NAT
LAYER 2 MODE	Modo Transparente
NAT (NETWORK ADDRESS TRASLATION)	Sí
PAT (PORT ADDRESS TRASLATION)	Sí
POLÍTICAS BASADAS EN NAT	Sí
PORT FORWARDING	Sí
CONFIGURACIÓN DE POLÍTICAS PROGRAMABLES EN EL TIEMPO	Sí
VIRTUAL NETWORK PRIVATE (VPN)	
PROTOCOLO IPSEC	AH, ESP
MODO IPSEC	Túnel y Transporte
MÉTODO ENCRIPTACIÓN	DES/3DES/AES/Twofish/Blowfish/ CAST-128/NULL
ALGORITMO AUTENTICACIÓN	MD5, SHA-1
GRUPO PFS	Perfect Forward Secrecy (DH Group): Group 1, 2, 5
SERVIDOR VPN	PPTP/L2TP/IPSec
SERVIDOR PPTP	Encriptación MPPE
VPN SITE TO SITE	Sí
REMOTE ACCESS FOR IPSEC	Sí
TÚNELES DEDICADOS	100
MODO IKE	Main, Aggressive
ADMINISTRACIÓN DE LLAVES	Pre-share key X.509 v3 Manual Key* Soporte IKE v2
IPSEC NAT TRANSVERSAL	Sí

SELECCIÓN DE POLÍTICAS VPN	Routing / Policy-Base Routing
DEAD PEER DETECTION	Sí
VPN TUNNEL KEEP ALIVE	Sí
PREVENCIÓN CONTRA REPETICIÓN DE ATAQUES (REPLAY ATTACK)	Sí
SOPORTE VPN ESTRELLA (HUB AND SPOKE)	Sí
DIRECCIONAMIENTO IP & ROUTING	
STATIC IP ADDRESS	Sí
MODOS	PPPoE para xDSL Cliente PPTP para xDSL Cliente DHCP para interface WAN BigPond Cable, Telia compliance
SERVIDOR DHCP INTERNO	Sí
DHCP RELAY	Sí
DHCP SOBRE IPSEC	Sí
IP ALIAS	Sí
STATIC ROUTES	Sí
RUTEO BASADO EN POLÍTICAS	Sí
NETWORKING	Sí
SOPORTE DE MÚLTIPLES ENLACES WAN	Hasta 8 VLANs
SOPORTE DE VLAN IEEE 802.1Q	Sí
IP INTERFACE	8 items
IP MULTICAST	IGMP 2*, IGMP snooping*
H.323 NAT TRAVERSAL	Sí
SOPORTE DE ALG (APPLICATION LAYER GATEWAY)	HTTP, FTP, H.323 SMTP*, SIP*, DNS*
ADMINISTRACIÓN DEL SISTEMA	
ASISTENTE DE INSTALACIÓN	Sí
CONSOLA INTERFACE	Sí
WEB UI INTERFAC	Sí
COMMAND LINE INTERFACE (CLI)	Sí
SECURE COMMAND SHELL (SSH)	*
SOPORTE DE SISTEMA DE ADMINISTRACIÓN CENTRAL	Sí
PROTECCIÓN DE CPU Y MEMORIA	*
SNTP Y UDP TIME SYNCHRONIZATION	Sí
ADMINISTRACIÓN DE USUARIOS Y EQUIPO	
MÚLTIPLES ADMINISTRADORES	Soportado en el sistema Administración Central
CONTROL DE PERMISOS DE USUARIO DE MULTI-NIVE	Soportado en el sistema Administración Central
CUENTA ADMINISTRATIVA SOLO LECTURA (READ ONLY)	Sí
ACTUALIZACIÓN DE SOFTWARE, CONFIGURACIÓN	Web UI TFTP*

BACKUP/RESTORE	
DEFINICIÓN DE HOST CONFIABLE PARA ADMINISTRACIÓN REMOTA	Sí
AUTENTICACIÓN DE USUARIO	
BASE DE DATOS LOCAL	150 items
BASE DE DATOS EXTERNA	RADIUS, LDAP*, Active Directory
AUTENTICACIÓN EN LÍNEA CON BASE DE DATOS INTERNA O EXTERNA	Sí
AUTENTICACIÓN DE USUARIOS POR GRUPOS	Sí
SOPORTE DE MÚLTIPLES SERVIDORES DE AUTENTICACIÓN AL MISMO TIEMPO	Máximo 3 Servidores
IP Y MAC ADDRESS BINDING	Hasta 64 items
XAUTH (EXTENDED AUTHENTICATION)	Para autenticación IPSec
LOGGING Y MONITOREO	
CAPACIDAD DE LOGS INTERNO	500 records
VISUALIZADOR LOG	Sí
NOTIFICACIÓN POR EMAIL	Sí
SOPORTE DE SERVIDOR LOG EXTERNO	Syslog server
FORMATO DE EXPORTACIÓN LOG	CSV (Soportado en el sistema Administración Central)
MONITOREO DE RENDIMIENTO EN TIEMPO REAL	Sí
LOG DE EVENTOS Y ALARMAS	Sí
ADMINISTRACIÓN DE MENSAJES DE LOG	Sorting/Filtering/Search*
SOPORTE SNMP V1, V2C	Sí
SNMP TRAP	*
SNMP STANDARD MIB-II Y CUSTOM MIB	*
MONITOREO DE TÚNEL VPN	Sí
ADMINISTRACIÓN DE ANCHO DE BANDA	
ANCHO DE BANDA GARANTIZADO	Sí
ANCHO DE BANDA MÁXIMO	
UTILIZACIÓN PRIORIDADES ANCHO DE BANDA	Sí
POLÍTICAS BASADAS EN TRAFFIC SHAPING	Sí
TRAFFIC SHAPING PROGRAMABLES EN EL TIEMPO	Sí
ADMINISTRACIÓN ANCHO DE BANDA EN EL TÚNEL VPN	Sí
ALTA DISPONIBILIDAD (AH)	
WAN FAILOVER	Sí
SISTEMA DE DETECCIÓN DE	

INTRUSO (IDS)	
PATRONES NIDS AUTO ACTUALIZABLES	Sí
PROTECCIÓN CONTRA ATAQUES DOS Y DDOS	Si
DETECCIÓN DE ATAQUES NIMDA, CODERED	Si
LISTA NEGRA DE IP	Support 128 IP/subnet items*
ALARMA DE ATAQUE POR NOTIFICACIÓN DE CORREO	Si
FILTRO DE CONTENIDO	
FILTRO DE CONTENIDO	Filtro URL, Filter Keyword*, Exempt list
SCRIPTS	Java Applet, Java Scripts, VB Scripts, Cookies, Active X
EMAIL*	Black list, Keyword, Exempt list
BLOQUEOS DE PROGRAMAS P2P	Sí
BLOQUEOS DE PROGRAMAS IM	*
BALANCEO DE CARGA DE TRÁFICO	
BALANCEO DE CARGA DE TRÁFICO DE SALIDA	*
ALGORITMO DE BALANCEO DE CARGA	Round Robin Connection Rate
TRÁFICO REDIRIGIDO CUANDO FALLA ALGUNA CONEXIÓN	Sí
LEDS INDICATORS POR DISPOSITIVO	
POWER	Sí
STATUS	Sí
WAN	Sí
LAN	Sí
DMZ	Sí
CARACTERÍSTICAS FÍSICAS	
ALIMENTACIÓN ELÉCTRICA	5V / 3A External AC to DC Switching Power Adaptor
DIMENSIONES	235 x 162 x 36 mm. Desktop Size
TEMPERATURA OPERACIÓN	0° C a 40° C
TEMPERATURA ALMACENAJE	-20° C a 70° C
HUMEDAD	5% a 95% No Condensado
EMISIÓN (EMI)	- FCC Class A - CE Class A - C-Tick
SEGURIDAD	- UL - LVD (EN60950) - TUV

3COM BASELINE SWITCH 2226 P	**CARACTERISTICAS**
MARCA	3COM
MODELO	BASELINE 2226 PLUS

NUMERO DE PARTE	3CBLSF26
PUERTOS	26 PUERTOS 24 PUERTOS 10/100 2 PARES DE PUERTOS GIGABIT DE USO DUAL (CONFIGURABLE COMO 10/100/1000 ó SFP)
SEGURIDAD	IEEE 802.1X
CAPAS	CAPA 2 full-rate nonblocking on all ports, full-/half-duplex autonegotiation, flow control, IEEE 802.1Q VLAN support, IEEE 802.1p traffic prioritization, IGMP snooping
ESPECIFICACIONES ADICIONALES	CONVERGENCIA: 4 hardware queues per port; IEEE 802.1p Class of Service/Quality of Service (CoS/QoS); auto-VLAN assignment for voice traffic SWITCH MANAGEMENT: Web-based configuration, SNMP management, Compact CLI for initial switch configuration
VOLTAJE DE ALIMENTACION	AUTO VOLTAJE (110-220 VAC)

DI 804
Principales Características y Facilidades
· Internet y VPN Server
· Soporte VPN Site-to-Site o Client-to-Site
· Soporte VPN pass-through para IPSec, PPTP y L2PT
· Funcionalidades de Firewall, tales como Stateful Packet Inspection (SPI), Domain Filtering, y URL Filtering
· Soporte de una DMZ-Host
· Soporte Ruteo IP, RIP-1/RIP-2
· Puerta serial para Dial Backup vía ISDN o módem análogo
· Administración Web y DHCP Server
· Diseño innovador
· Fácil configuración (UnPn) y alto rendimiento.

Swicth D-LINK DGS-3627, L3	INFORMACIÓN TÉCNICA
MARCA	D-LINK
MODELO	DGS-3627
Método de Switching	Store-and-forward
Flash Memory	- Prom: 512 KBytes - Runtime: 16 Mbytes
Switching Capacity	108 Gbps
Estándares	- IEEE 802.3 - IEEE 802.3u - IEEE 802.3x, Flow Control - IEEE 802.3ab - IEEE 802.3ae - IEEE 802.3z - ANSI/IEEE 802.3 Nway auto-negotiation
PUERTOS	24 X 10/100/1000BASE-T PORTS 4 SFP PORTS COMBO WITH LAST 4 10/100/1000BASE-T 3 OPEN SLOTS FOR OPTIONAL 10GE MODULES 1 RS-232, CONSOLA
Stackability	Virtual Stacking: - SIM v1.6 - All DGS-3600 Series support software virtual stacking to single IP manage up to 32 devices - Bandwidth up to 20G (Depends on the stacking interface you used). Physical Stacking: * - Via optional CX4 (or XFP) module provide bi-directional redundant stacking topology - Up to 12 devices - Bandwidth up to 40G - Topology Linear/Ring
VOLTAJE DE ALIMENTACIÓN	INTERNA UNIVERSAL 100 A 240 VAC, 50/60 Hz
Funciones de Administración	Administración - Single IP Management: SIM v1.6 - LLDP * - SNMP v.1, v.2C, v.3 RFC 1157, 1901, 1908, 2570, 2575 - Web-based GUI RFC 2068 - CLI (command line interface) - RMON v1: Support 4 groups RFC 2819 - RMON v2: Support Probeconfig group - sFlow : IP address/UDP port No. * - Boot/DHCP client RFC 951, 1542 - DHCP Auto-Configuration

	- DHCP relay option 82 RFC 3046 - DHCP Server * - Telnet Server RFC 854 - Telnet Client * - TFTP client RFC 783 - SNTP - SYSLOG RFC 3164, 3195 - Trap/Alarm/Log Severity Control - Dual Image - Dual Configuration - Flash file system - Port Description - Editable Login Banner - Editable System Prompt - Virtual Interface: Same like Cisco Loopback interface * - 0.0.0.0 IP Setting - Web GUI Traffic Monitoring - Web MAC address Browsing - CPU Monitoring Web/CLI/SNMP - SNMP Trap on MAC Notification MIBs Soportadas - MIB-II RFC 1213 - Bridge MIB RFC 1493 - SNMP v.2 MIB 1907 - RMON MIB 2819 (Previo RFC 1757) - RMONv2 MIB RFC 2021 - Ether-like MIB 2665 (Previo RFC 1643, 2358) - 802.3 MAU MIB RFC 2668 - 802.1Q VLAN/802.1p MIB (RFC 2674) - IF MIB RFC 2863 (RFC 2233) * - RADIUS Authentication Client MIB 2618 - IGMPv3 MIB - RIPv2 MIB RFC 1724 - OSPFv2 MIB RFC 1850 - IP Forwarding Table MIB (CIDR) RFC 2096 - VRRP MIB RFC 2787 - IPv4 Multicast Routing MIB RFC 2932 - PIM MIB for IPv4 RFC 2934 - RADIUS Accounting Client MIB 2620 - Ping MIB * - Trace out MIB * - L2 Specific MIB - L3 Specific MIB - Private MIB RMON Groups 1, 2, 3, 9 (Alarm, Statistics, History, Event)
Funciones L3	- Policy Based Route - RIP v1/v2 - RIPng (IPv6)

	- OSPF v2 - OSPF Passive Interface - OSPF NSSA (Not SoStubby Area) - OSPF Equal Cost Route - Number of IP Interface: 64 - Number of IP Interface : 256 * - Multiple IP Interface per VLAN: 5 - Multiple IP Interface per VLAN: 256 * - Multi Path Routing: Equal Cost (EC) and Weighted Cost (WC) - VRRP - IPv6 Ready Phase 1 - DVMRP v3 - PIM DM : IPv4 - PIM SM : IPv4
Floating Static Route	- IPv4 Floating Static Route - IPv6 Floating Static Route
L3 Forwarding Table Size	- Total 8K L3H/W forwarding entries(both IPv4/6 IP forwarding) - Max 8K entries for IPv4 - Max 4Kentries for IPv6
Seguridad para el Acceso a la Red	- Port security (hasta 16 MAC's por puerto) - 802.1x: Port/MAC-based Access Control - RADIUS Auth. For Mgmt Access -TACACS+ Auth. for Mgmt - SSL v3 - SSH v2 - Web-based Access Control * - MAC-based Access Control * - JWAC: Support NTT and OKI authentication server * - Microsoft NAP: Support Microsoft NAP function via 802.1X guest VLAN - Broadcas/Multicast Storm Control - Traffic Segmentation - IP-MAC Binding: 500 address per device - IP-MAC-port Binding: Modos ARP y ACL - IP-MAC-Port Binding Enhancement: DHCP snooping/filtering - D-Link Safeguard Engine - D-Link Safeguard Engine Enhancement *
ACL (Access Control List)	- Maximum Mask/profiles: 8 Profiles, Max. 1792 rules - Based on Switch Port - Based on VLAN ID - Based on 802.1p priority - Based on MAC address - Based on IPv4/v6 address - Based on DSCP - Based on protocol type - Based on IPv6 traffic class - Based on IPv6 flow label

	- Based on TCP/UDP port - Based on User Defined Packet Content - Time Based ACL - ACL Statistic * - CPU interface filtering
QoS (Calidad se Servicio)	- 802.1p Priority Queues - Max. N° de colas por puerto: 8 - Bandwidth Control: Por puerto rangos de 64 Kbps - Per flor bandwidth control: Rangos de 64 Kbps - Queue handling: WRR/Strict mode - CoS Based On Switch Port - CoS Based On VLAN ID - CoS Based On 802.1p priority - CoS Based On MAC Address - CoS Based On IPv4/v6 address - CoS Based On DSCP - CoS Based On protocol type - CoS Based On IPv6 traffic class - CoS Based On IPv6 flow label - CoS Based On TCP/UDP port - CoS Based On User Defined Packet Content
Consumo	72,3 Watts max.
Optional Redundant Power Supply	DPS-500
Tamaño	Montable en rack estándar de 19", 1 U
Dimensiones	441mm x 389mm x 44mm
Peso	5,51 Kg
LEDs indicadores	- Power - Console - RPS - Stacking ID Por puerto 10/100/1000 : - Speed Mode - Link/Act Por puerto SFP : - Link/Act Por 10G Open Slot: - Link/Act

ANEXO D
RECOMENDACIONES PARA SERVICIOS DE RED

El Diagrama de la Infraestructura Recomendada se muestra en la Fig. D.1

Nota:

Dentro del estándar usado por Microsoft nos pide que cada Servidor Domain Controller tenga solo su propia funcionalidad, es por ello que se requiere un servidor que cumpla únicamente la función de Domain Controller.

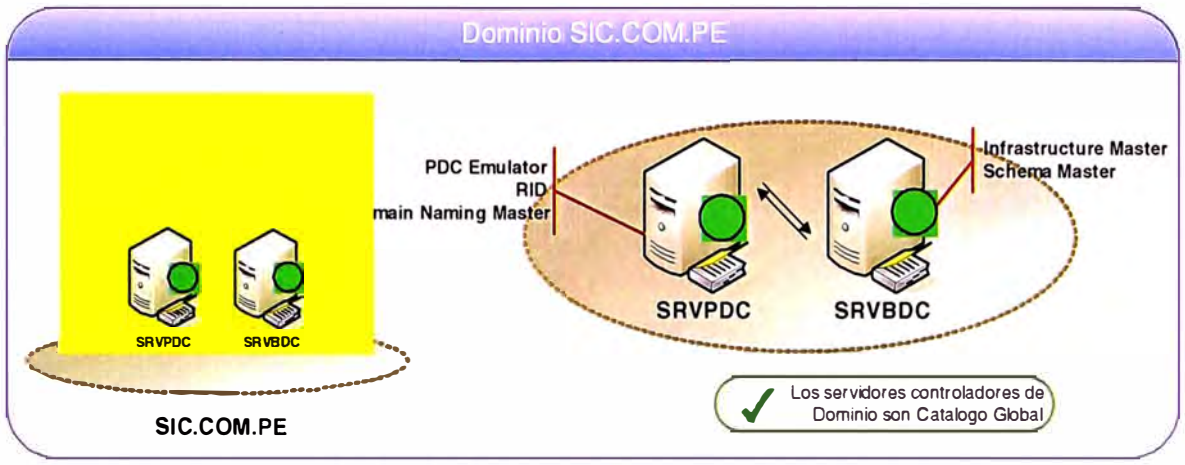


Fig. D.1– Diagrama de Infraestructura de Correo Final

Hardware del nuevo Domain Controller recomendado, verTabla N° D.1

TABLA N° D.1 – Hardware Mínimo Recomendado para Domain Controller

Características:
1 GB de RAM
Mínimo Dual Core
HD: 80GB
Cuenta con dos particiones:
C: 20 GB (Instalación de Sistema Operativo)
D: 60 GB

Nueva Arquitectura:

En los servidores Domain Controller se dividirán los Roles FSMO, el servidor SRVPDC contará con 3 roles FSMO y el servidor SRVBDC contará con 2 roles FSMO, tales como se detalla en la siguiente tabla N° D.2

TABLA N° D.2 – Roles FSMO

Nivel del Rol	**Nombre de Rol**	**Dueño**
Nivel de Bosque (Forest)	Schema	SRVBDC
	Domain Naming	SRVPDC
Nivel de Dominio(Domain)	PDC	SRVPDC
	RID	SRVPDC
	Infrastructure	SRVBDC

Nota:

Esta división de Roles se efectúa según las buenas prácticas usadas por Microsoft, para que halla un balanceo de roles en los domain controller para que cuando un DC colapse el otro servidor ingrese sin ningún problema.

- Los servidores Domain Controller **SRVPDC** y **SRVBDC** serán Global Catalog, para que cuando algún usuario del dominio haga una búsqueda de objetos, se encuentre el objeto más rápido. Ver Fig. D.2

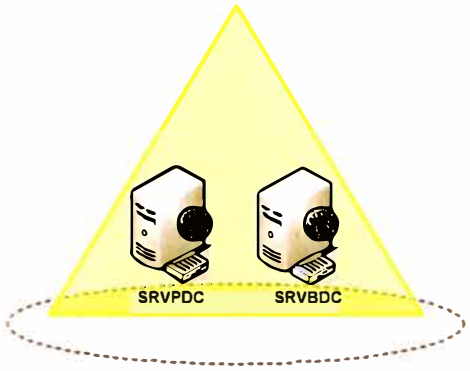


Fig. D.2 - Global Catalog SIC.

- Las Unidades Organizacionales serán modificadas. La nueva estructura de las OU's serán creadas por Áreas, las cuales serán las áreas con que cuenta la empresa SIC, esta nueva estructura será tanto para usuarios como para computadoras. En la Fig. D.3 se detalla un ejemplo de la nueva estructura de Unidades Organizacionales.
- En el servidor **SRVPDC** que tiene el servicio de DNS, deberán de borrar todos los registros huérfanos (registros que ya no existen) para que así no existan problemas al unir una computadora al dominio y no tenga registros iguales.

  Nota:

  Esta nueva estructura se esta realizando para poder aplicar las políticas a nivel de OU's, Para que las políticas restringidas sean por áreas, tanto computadoras como usuarios.
- Es recomendable que las computadoras que son parte del Dominio **SIC.COM.PE** tengan un sistema operativo estándar, el más recomendable actualmente es **Microsoft Windows XP SP3**, la cual contaría con el cliente de mensajería **Microsoft Outlook 2003** que es el más usado actualmente y recomendado. Con el cliente Outlook instalado en las computadoras se configurará sus cuentas de

correo electrónico de la empresa SIC, para que puedan guardar todos sus correos en .PST en su propia máquina.

- La cuenta de servicio **BackupSic** usuario del grupo Backup Operators, deberá ser usada para los backup programados diariamente. En este servidor se realizará el backup del System State de cada Domain Controller **SRVPDC** y **SRVBDC**.

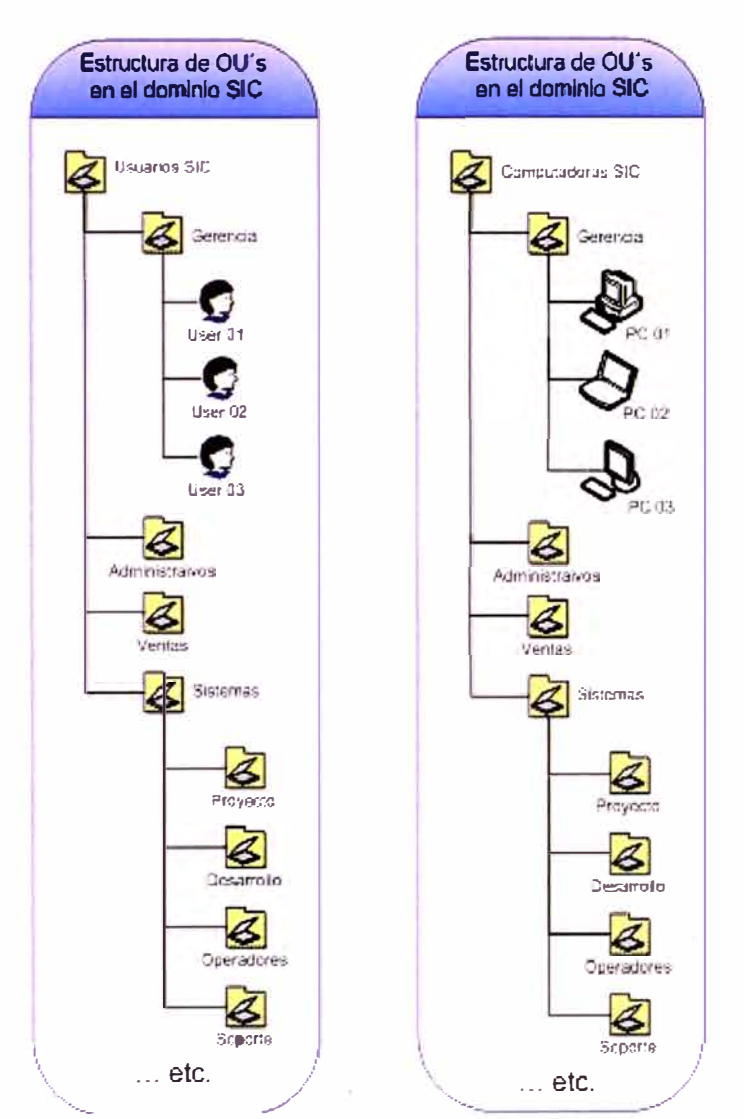


Fig. D. 3 - Estructura de OUs. Recomendada.

Políticas a configurar dentro de Dominio SIC.COM.PE:

Políticas de Cuentas

- La contraseña no puede contener menos de 06 caracteres.
- El tiempo de vida de una contraseña es máximo de 60 días.
- El tiempo de vida de una contraseña es mínimo de 01 día
- Las contraseñas se almacenan las últimas 05 contraseñas.

Políticas de envió y recepción de correo

Las Políticas del Sistema de Mensajería estarían en un principio limitadas de la siguiente manera:

Usuarios Gerencia:

- Tamaño máximo de envío : ilimitado
- Tamaño máximo de recepción : ilimitado
- Limite de recepción : ilimitado
- Advertencia : 450000 KB
- Prohibir el envío : 475000 KB
- Prohibir el envío la recepción : 500000 KB

Usuarios Ventas:

- Tamaño máximo de envío : 10MB
- Tamaño máximo de recepción : 10MB
- Limite de recepción : 10MB
- Advertencia : 75000 KB
- Prohibir el envío : 80000 KB
- Prohibir el envío la recepción : 85000 KB

Usuarios Administrativos:

- Tamaño máximo de envío : 5MB
- Tamaño máximo de recepción : 5MB
- Limite de recepción : 5MB
- Advertencia : 45000 KB
- Prohibir el envío : 47000 KB
- Prohibir el envío la recepción : 50000 KB

Usuarios Sistemas:

- Tamaño máximo de envío : 5MB
- Tamaño máximo de recepción : 5MB
- Limite de recepción : 5MB
- Advertencia : 45000 KB
- Prohibir el envío : 47000 KB
- Prohibir el envío la recepción : 50000 KB

Administración de mensajería

La administración del sistema de mensajería se realiza solo por parte del administrador de Red de la empresa SIC.

Nomenclatura para los buzones de correo

La creación de un buzón de correo se realiza de la siguiente forma:

Primera letra del primer nombre más el apellido paterno y si existiera casos de homónimos se adiciona la primera letra del segundo nombre después de la primera letra.

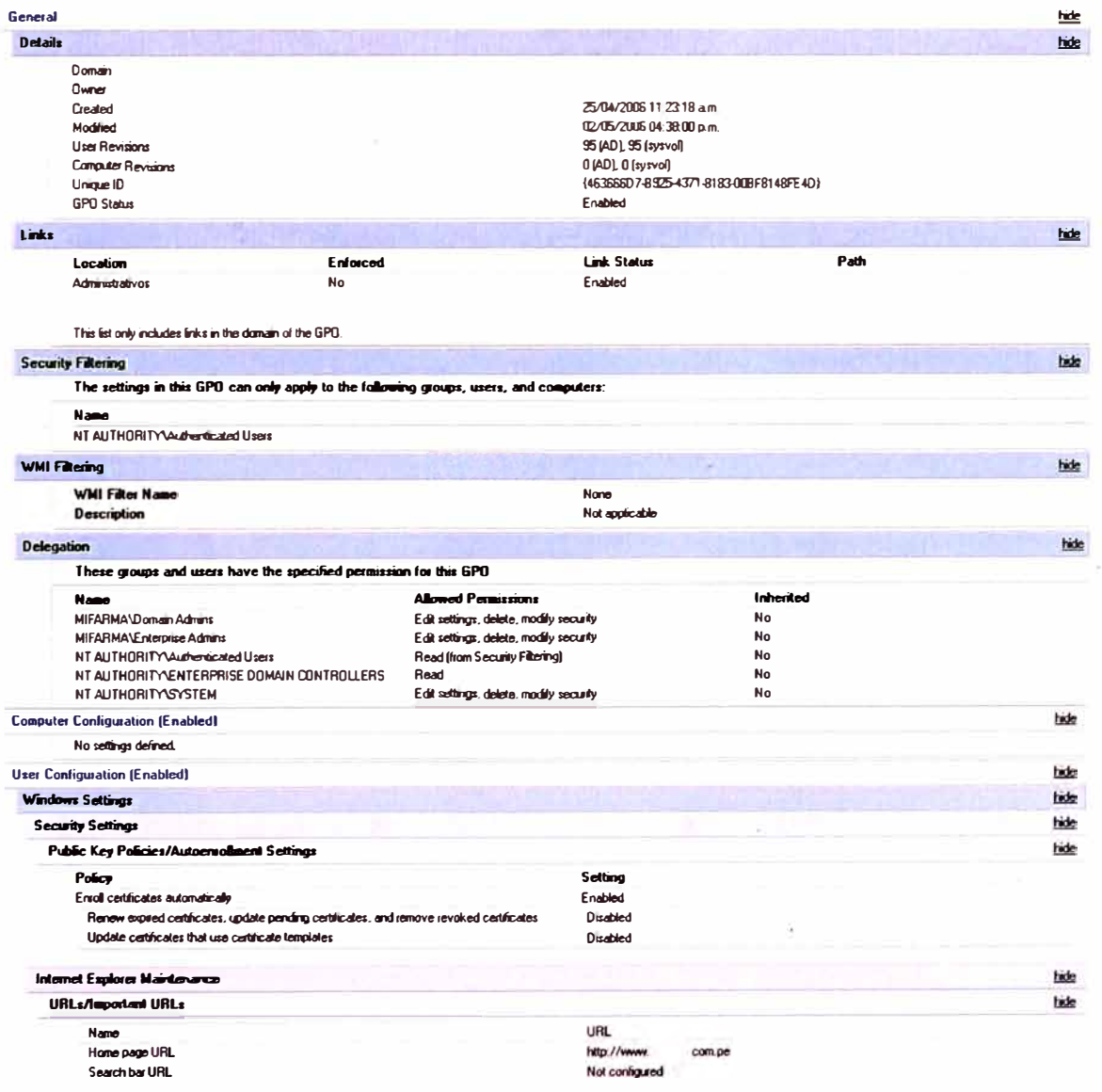
Por ejemplo: jquispe, arodriguez, jlperez, etc.

GPO – ADMINISTRATIVO POLICY

Sobre la política "Administrativo Policy" se han realizado cambios específicamente relacionados a la seguridad en Microsoft Internet Explorer, agregándose restricciones que se aplican a estaciones de trabajo Windows XP.

También se ha agregado una lista de aplicaciones, las cuales no se esta permitido que los usuarios puedan ejecutar, como por ejemplo: Aplicaciones que realizan búsquedas en Internet, para descargar contenido del tipo musical, juegos, videos entre otros.

A continuación se muestra un formato de políticas:



General — hide

Details — hide

Domain	
Owner	
Created	25/04/2006 11:23:18 a.m.
Modified	02/05/2006 04:38:00 p.m.
User Revisions	95 (AD), 95 (sysvol)
Computer Revisions	0 (AD), 0 (sysvol)
Unique ID	{4638680D7-B525-4371-8183-00BF8148FE4D}
GPO Status	Enabled

Links — hide

Location	Enforced	Link Status	Path
Administrativos	No	Enabled	

This list only includes links in the domain of the GPO.

Security Filtering — hide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

WMI Filtering — hide

WMI Filter Name	None
Description	Not applicable

Delegation — hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
MIFARMA\Domain Admins	Edit settings, delete, modify security	No
MIFARMA\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled) — hide

No settings defined.

User Configuration (Enabled) — hide

Windows Settings — hide

Security Settings — hide

Public Key Policies/Autoenrollment Settings — hide

Policy	Setting
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Internet Explorer Maintenance — hide

URLs/Important URLs — hide

Name	URL
Home page URL	http://www. com.pe
Search bar URL	Not configured

Online support page URL	Not configured

Administrative Templates hide

Control Panel hide

Policy	Setting
Prohibit access to the Control Panel	Enabled

Control Panel/Add or Remove Programs hide

Policy	Setting
Hide Change or Remove Programs page	Enabled
Remove Add or Remove Programs	Enabled

Control Panel/Display hide

Policy	Setting
Password protect the screen saver	Enabled
Remove Display in Control Panel	Enabled
Screen Saver	Enabled
Screen Saver executable name	Enabled
Screen Saver executable name	%SystemRoot%/System32/Logon.scr

Policy	Setting
Screen Saver timeout	Enabled
Number of seconds to wait to enable the Screen Saver	
Seconds:	900

Control Panel/Printers hide

Policy	Setting
Browse the network to find printers	Enabled
Prevent addition of printers	Enabled
Prevent deletion of printers	Enabled

Desktop hide

Policy	Setting
Do not add shares of recently opened documents to My Network Places	Enabled
Don't save settings at exit	Enabled
Hide My Network Places icon on desktop	Enabled
Prohibit adjusting desktop toolbars	Enabled
Prohibit user from changing My Documents path	Enabled

Desktop/Active Desktop hide

Policy	Setting
Enable Active Desktop	Enabled
Allows HTML and JPEG Wallpaper	

Policy	Setting
Prohibit changes	Enabled

Network/Network Connections hide

Policy	Setting
Ability to Enable/Disable a LAN connection	Disabled
Prohibit access to properties of a LAN connection	Enabled
Prohibit access to properties of components of a LAN connection	Enabled
Prohibit access to the Advanced Settings item on the Advanced menu	Enabled
Prohibit access to the New Connection Wizard	Enabled
Prohibit Enabling/Disabling components of a LAN connection	Enabled
Prohibit TCP/IP advanced configuration	Enabled

Start Menu and Taskbar hide

Policy	Setting
Add Logoff to the Start Menu	Enabled
Do not display any custom toolbars in the taskbar	Disabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove links and access to Windows Update	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Run menu from Start Menu	Enabled

System hide

Policy	Setting
Code signing for device drivers	Enabled
When Windows detects a driver file without a digital signature:	Warn

Policy	Setting
Don't display the Getting Started welcome screen at logon	Enabled
Don't run specified Windows applications	Enabled
List of disallowed applications	
emule.exe	
gnutella.exe	
kazaa.exe	
napster.exe	
winamp.exe	

Policy	Setting
Prevent access to registry editing tools	Enabled
Disable regedit from running silently?	Yes

Policy	Setting
Prevent access to the command prompt	Enabled
Disable the command prompt script processing also?	Yes

Windows Components/Internet Explorer hide

Policy	Setting
Disable changing Advanced page settings	Enabled

Disable changing Automatic Configuration settings	Enabled
Disable changing certificate settings	Enabled
Disable changing connection settings	Enabled
Disable changing default browser check	Enabled
Disable changing home page settings	Enabled
Disable changing Messaging settings	Enabled
Disable changing proxy settings	Enabled
Disable changing ratings settings	Enabled
Disable changing Temporary Internet files settings	Enabled
Disable Internet Connection wizard	Enabled
Do not allow AutoComplete to save passwords	Enabled
Search: Disable Search Customization	Enabled

Windows Components/Internet Explorer/Browser menus hide

Policy	Setting
Tools menu: Disable Internet Options... menu option	Enabled

Windows Components/Internet Explorer/Internet Control Panel hide

Policy	Setting
Disable the Advanced page	Enabled
Disable the Connections page	Enabled
Disable the Content page	Enabled
Disable the General page	Enabled
Disable the Privacy page	Enabled
Disable the Programs page	Enabled
Disable the Security page	Enabled

Windows Components/Task Scheduler hide

Policy	Setting
Hide Advanced Properties Checkbox in Add Scheduled Task Wizard	Disabled
Hide Property Pages	Enabled
Prevent Task Run or End	Enabled
Prohibit Drag-and-Drop	Enabled
Prohibit New Task Creation	Enabled
Prohibit Task Deletion	Enabled

Windows Components/Windows Explorer hide

Policy	Setting
Hide these specified drives in My Computer	Enabled
Pick one of the following combinations	Restrict A and B drives only

Policy	Setting
No "Computers Near Me" in My Network Places	Enabled
No "Entire Network" in My Network Places	Enabled
Prevent access to drives from My Computer	Enabled
Pick one of the following combinations	Restrict A and B drives only

Policy	Setting
Removes the Folder Options menu item from the Tools menu	Enabled
Turn on Classic Shell	Disabled

Windows Components/Windows Media Player/Networking hide

Policy	Setting
Hide Network Tab	Enabled
Streaming Media Protocols	Disabled

Windows Components/Windows Media Player/User Interface hide

Policy	Setting
Hide Security Tab	Enabled

ANEXO E
PRUEBAS PILOTO DE INTERCONEXIÓN DE SUCURSALES

Se desarrollará inicialmente por medio de un piloto de pruebas a fin de certificar la solución. A continuación el procedimiento del piloto a montarse.

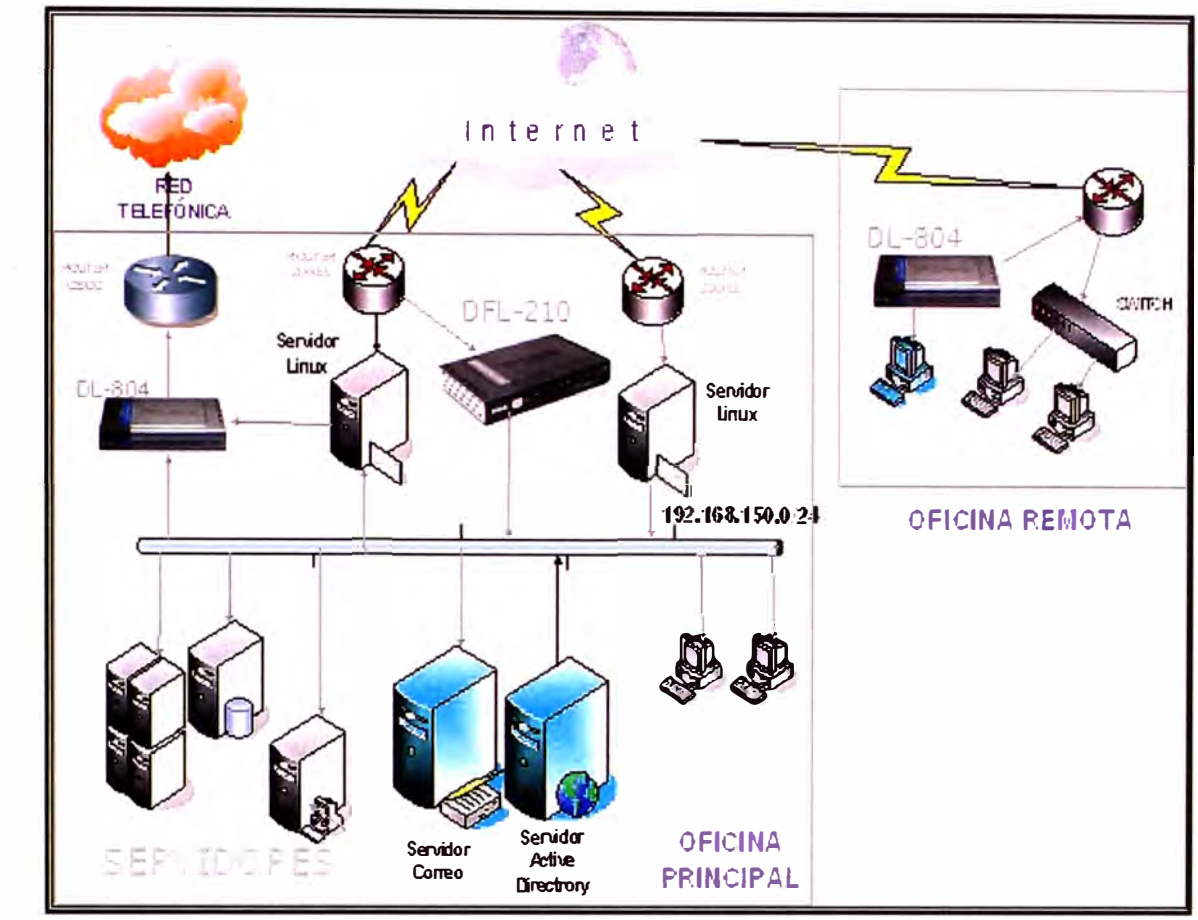
Desarrollo de Prueba Piloto

La implementación del piloto en donde se probarán las funcionalidades propuestas en el presente documento. Se realizará de la siguiente manera

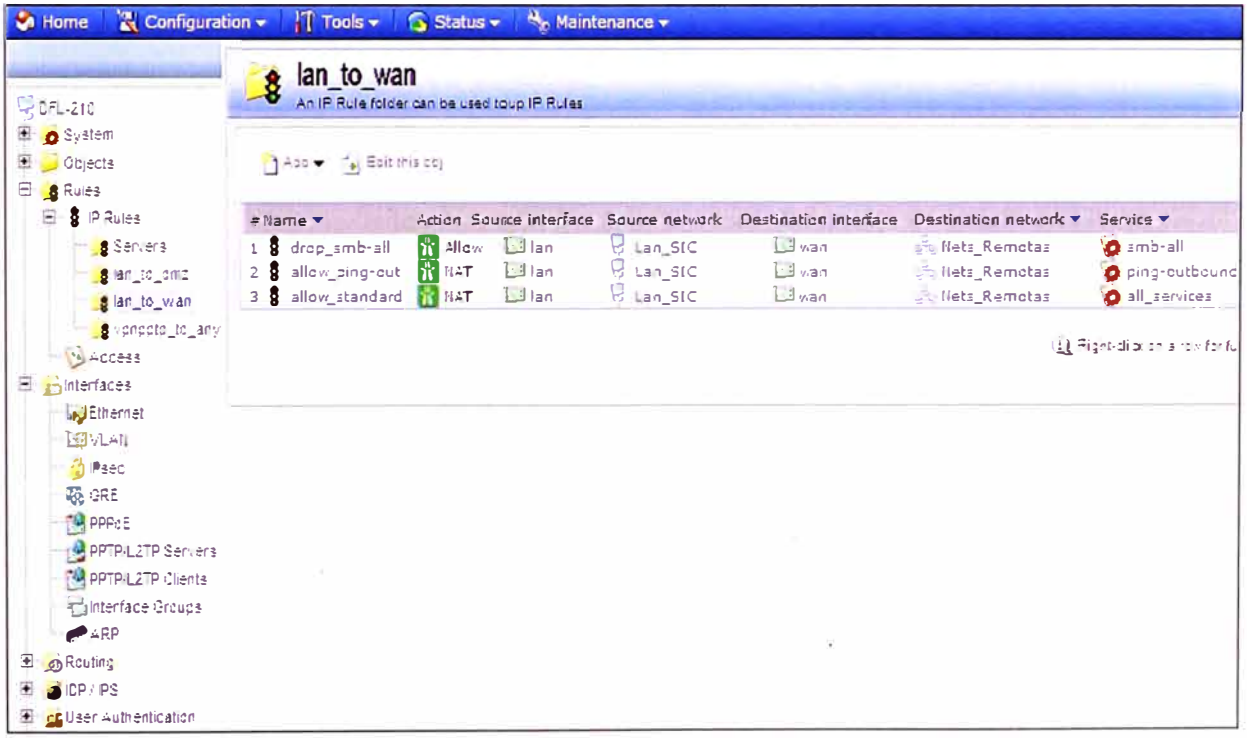
Formato de Prueba

Prueba1	**Prueba Piloto de Conectividad**
Actores Involucrados o Métricas de Información	Actores: Componente Solución de Túneles, Firewall y Filtro de Contenido
Objetivo	Probar las comunicaciones entre la Oficina Principal y la una Oficina Remota (Conexión entre el DFL-210 y el DI-804HV)
Pre-requisitos	Reservar puertos LAN y WAN en Oficina de Vitarte y Oficina Principal Contar con dos equipos PC'S enla oficina principal y un PC en la oficina remota
Descripción	La interfaz WAN del equipo Dlink DFL 210 se conectará al rango IP público 190.41.59.248/28, en donde se le asignará a este equipo una IP disponible de este rango. Asimismo, la interfaz LAN de este equipo se conectará al nuevo rango IP privado propuesto 192.168.150.0/24, en donde se le asignará la IP 192.168.150.1/24, a este mismo equipo a dos de sus puertos LAN disponibles se conectarán los nuevos servidores de Correo y Directorio Activo con las nuevas funcionalidades implementadas, los mismos que serán exclusivamente para las pruebas del piloto. En la oficina remota (se propone Vitarte) se instalará un equipo D-link DI-804HV conectando la interfaz WAN a uno de los puertos del Zyxel donde se le asignará una IP privada de ese rango Por otro lado, la interfaz Lan de este equipo se conectará al nuevo rango IP privado propuesto 192.168.11.0/24, en donde se le asignará la IP 192.168.11.1/24, a este mismo equipo a uno de sus puertos LAN se conectará una sola PC de la oficina remota el mismo que no requerirá conectarse a los aplicativos internos de SIC ni a los aplicativos de Telefónica del Perú.

Topología Propuesta para el Piloto



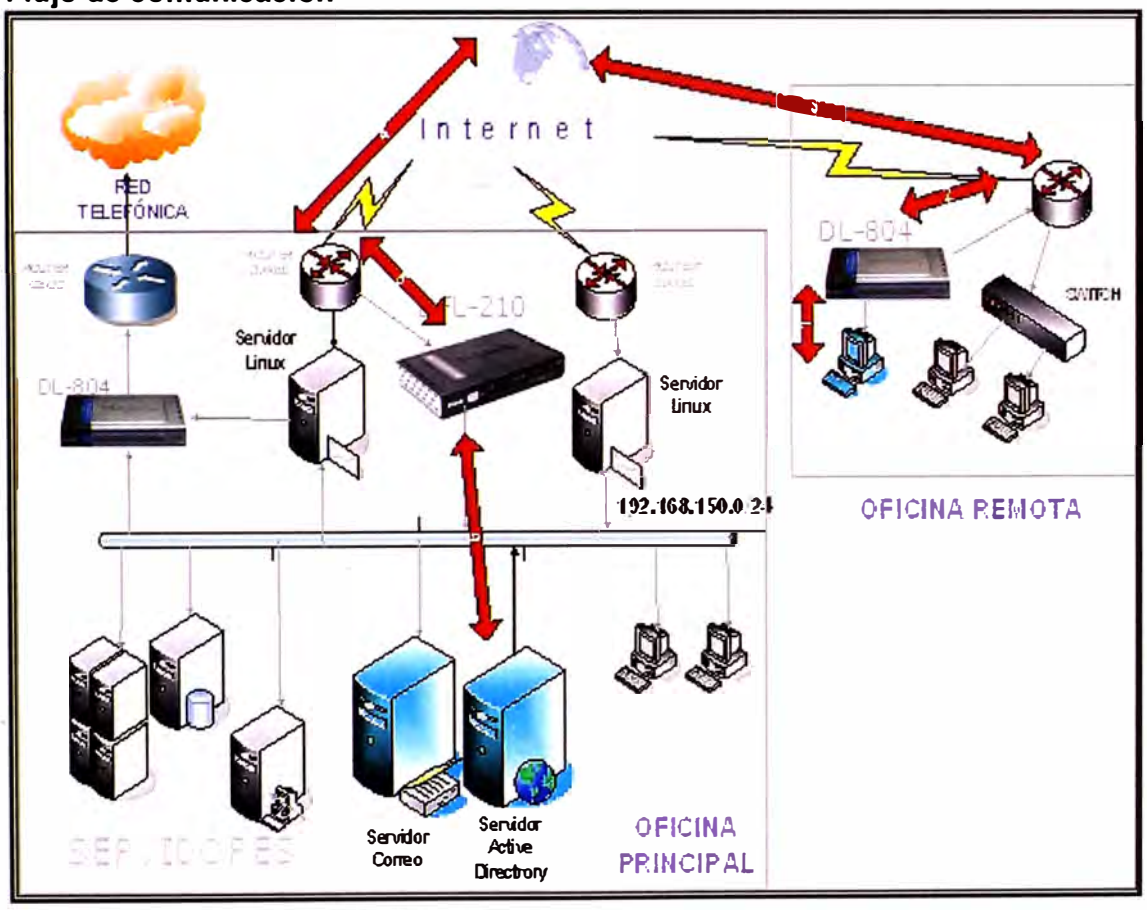
Aquí se muestra la venta de configuración del DFL 210



En el menú del lado derecho se muestran, todas las pestañas de configuración.

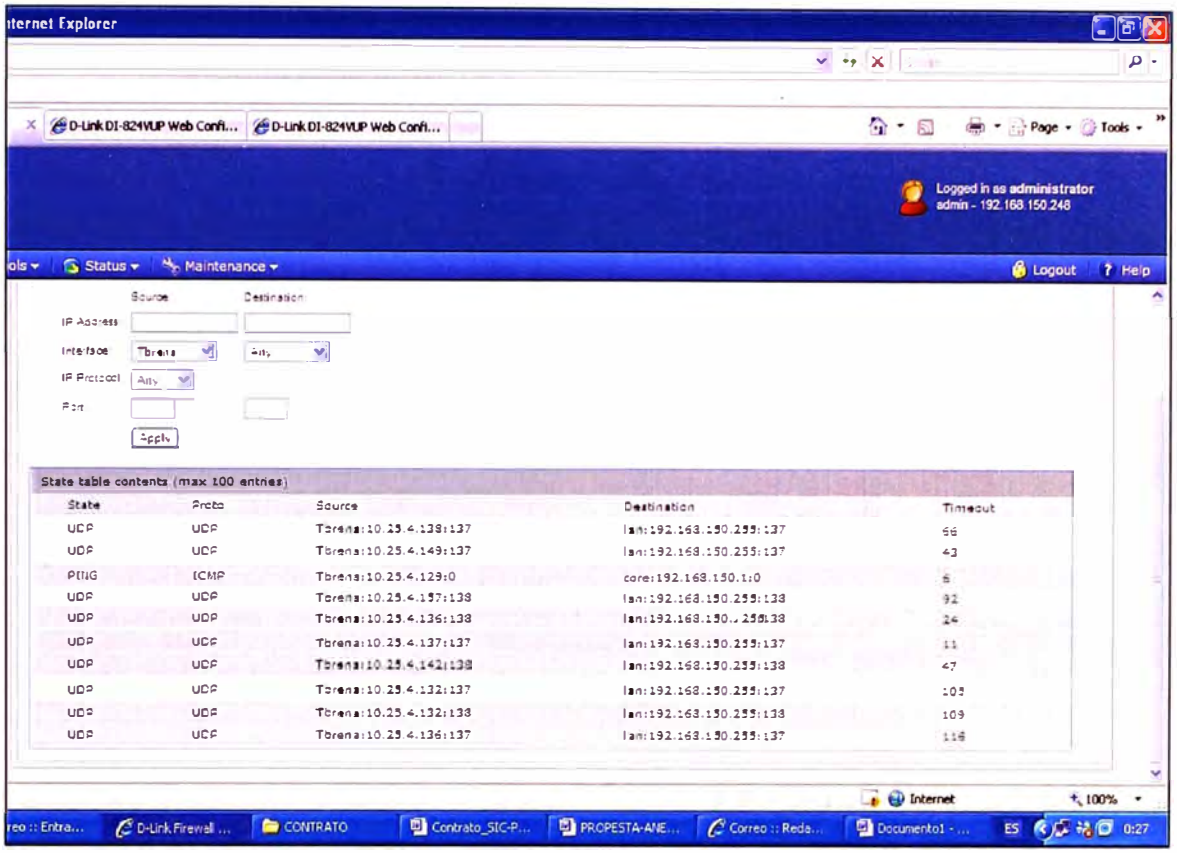
Act.	Acción	Resultado Esperado
1.1	**Prueba Piloto de la Solución Firewall** Se ha implementado en el Piloto una red aislada con la solución de Servidores a ser instalados en SIC, a fin de probar el funcionamiento en estado normal y en estado de configuración Firewall. Durante la prueba se simula la activación y desactivación de Firewall	Se observa que las politicas aplicadas, restringen las salidas hacia todos los puertos TCP y UDP.
1.2	**Prueba Piloto de la Solución de Túneles** Implantada la solución de Comunicaciones, se realiza una prueba usando los equipos instalados en el lado Principal y en el lugar Remoto que funcionan en la realidad	Se observa que se logra conectar con la sede principal mediente el tunel IPSEC.
1.3	**Prueba Piloto de Filtro de Contenidos** Solo se permitirá acceso ha ciertos dominios.	Se verifica el acceso restringido hacia Internet.

Flujo de comunicación

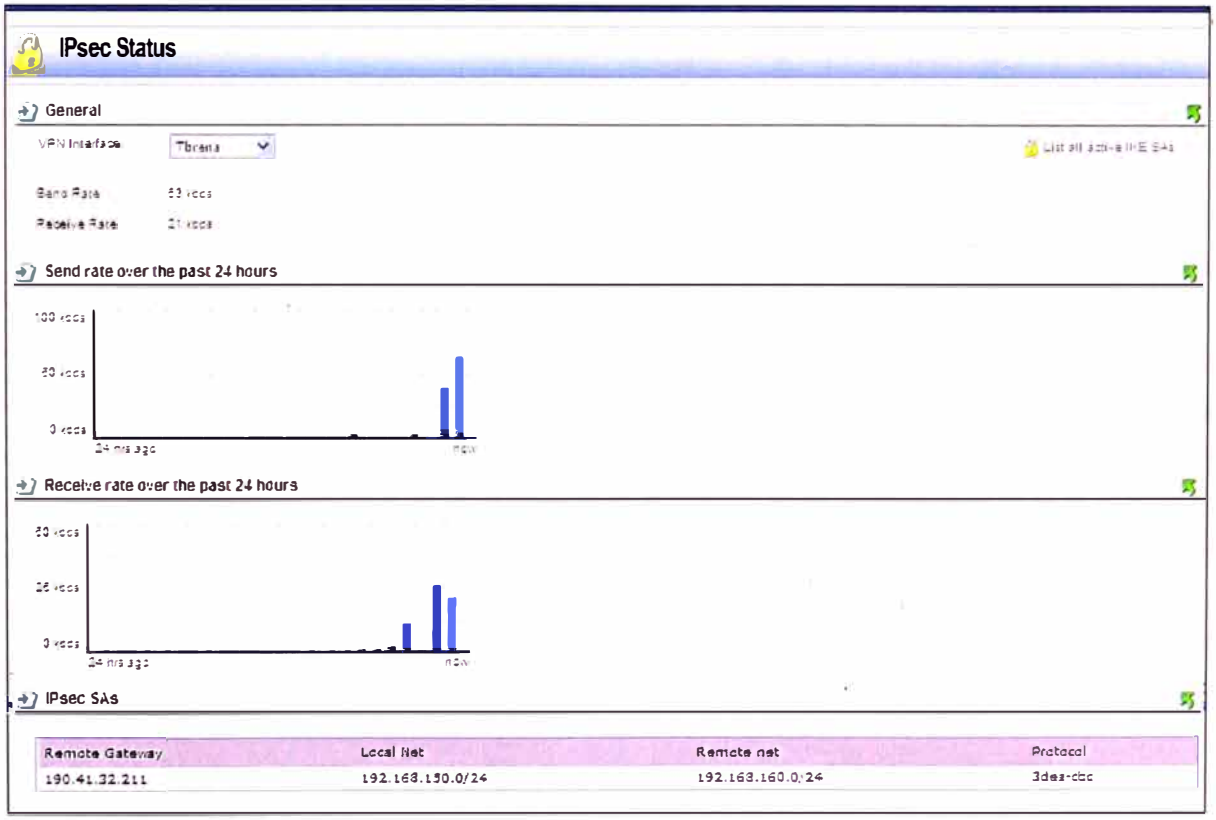


Una vez que se haya probado las facilidades satisfactoriamente se pasará a producción toda las PC`s de la oficina remota, para lo cual será necesario realizar configuraciones en el equipo Linux 1, donde básicamente se agregará una ruta estática de retorno que indique que para ir a la red remota ir por el Dlink DFL 210. De esta forma se agregara todos los locales, hasta terminar la fase de implantación. Al final se retiran los equipos Linux, y quedaran los Router Dlink DFL-210.

Se Adjunta Pantalla de prueba de conectividad con el switch Core.

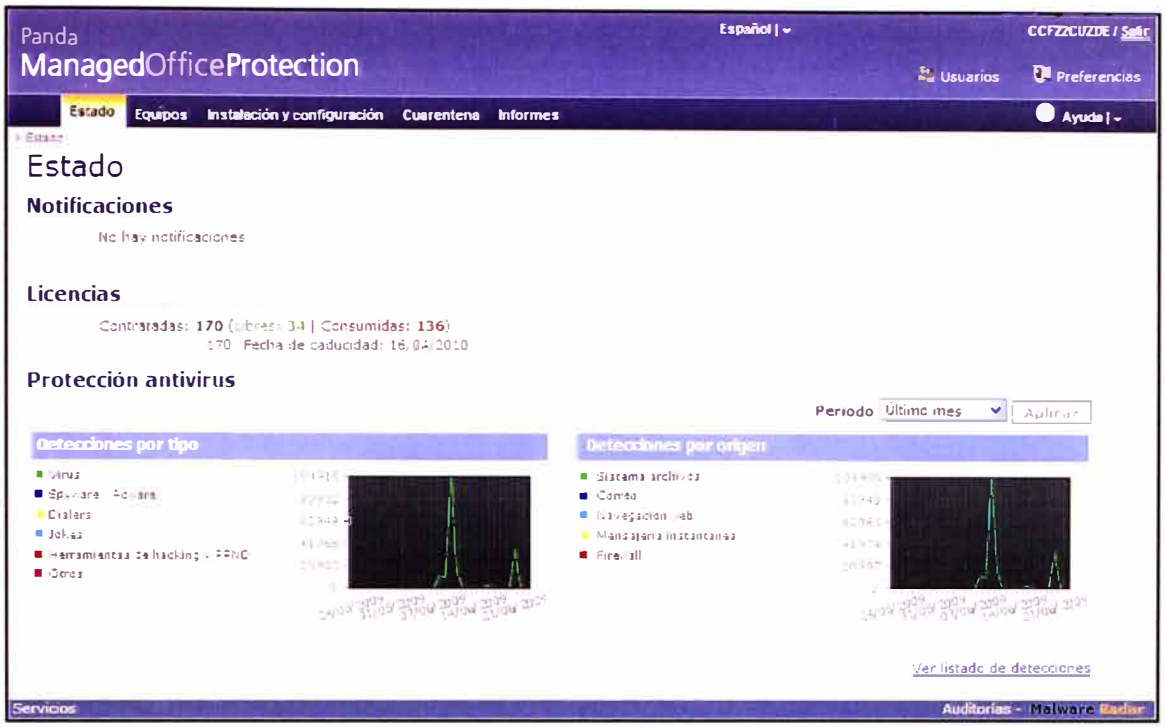


El la gráfica siguiente se muestra el estado de conexión de la VPN así como el tráfico.

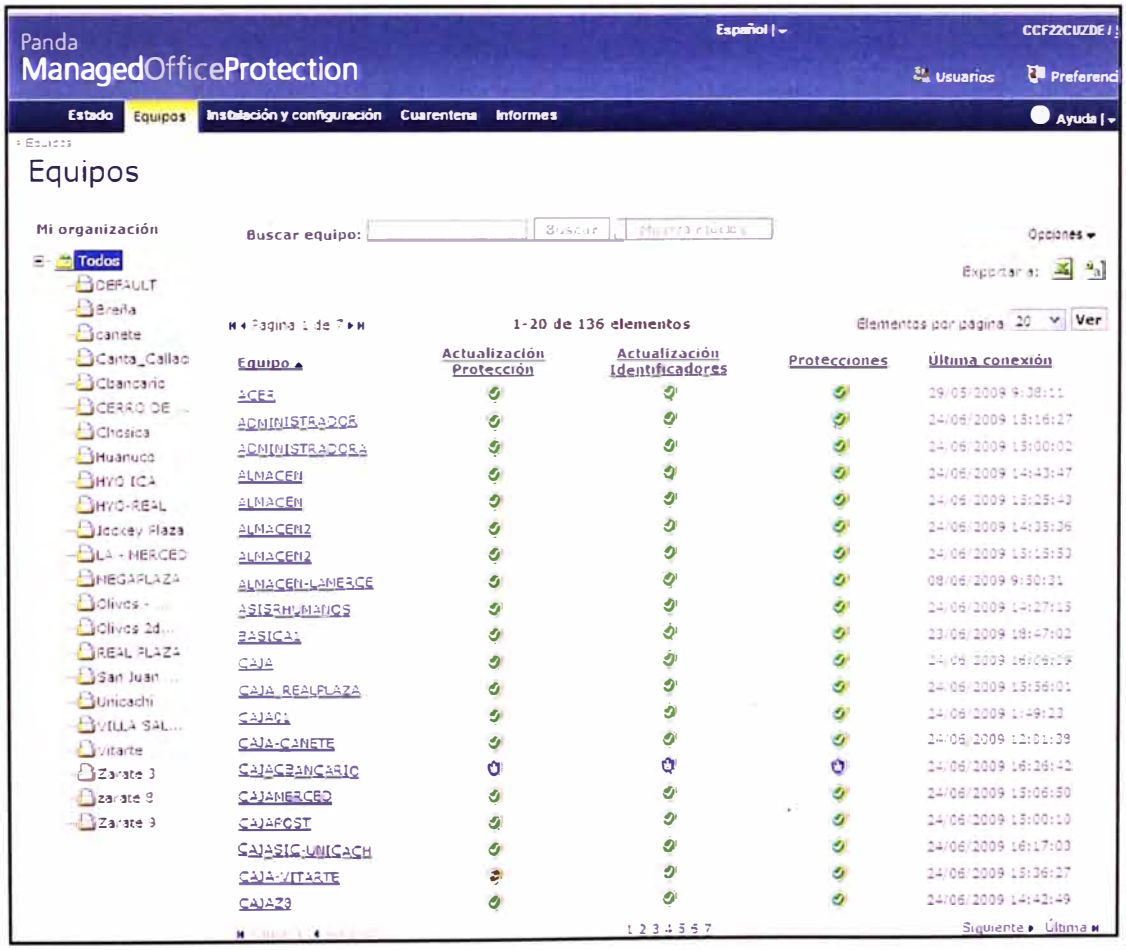


ANEXO F
REPORTES DE ANTIVIRUS CORPORATIVO

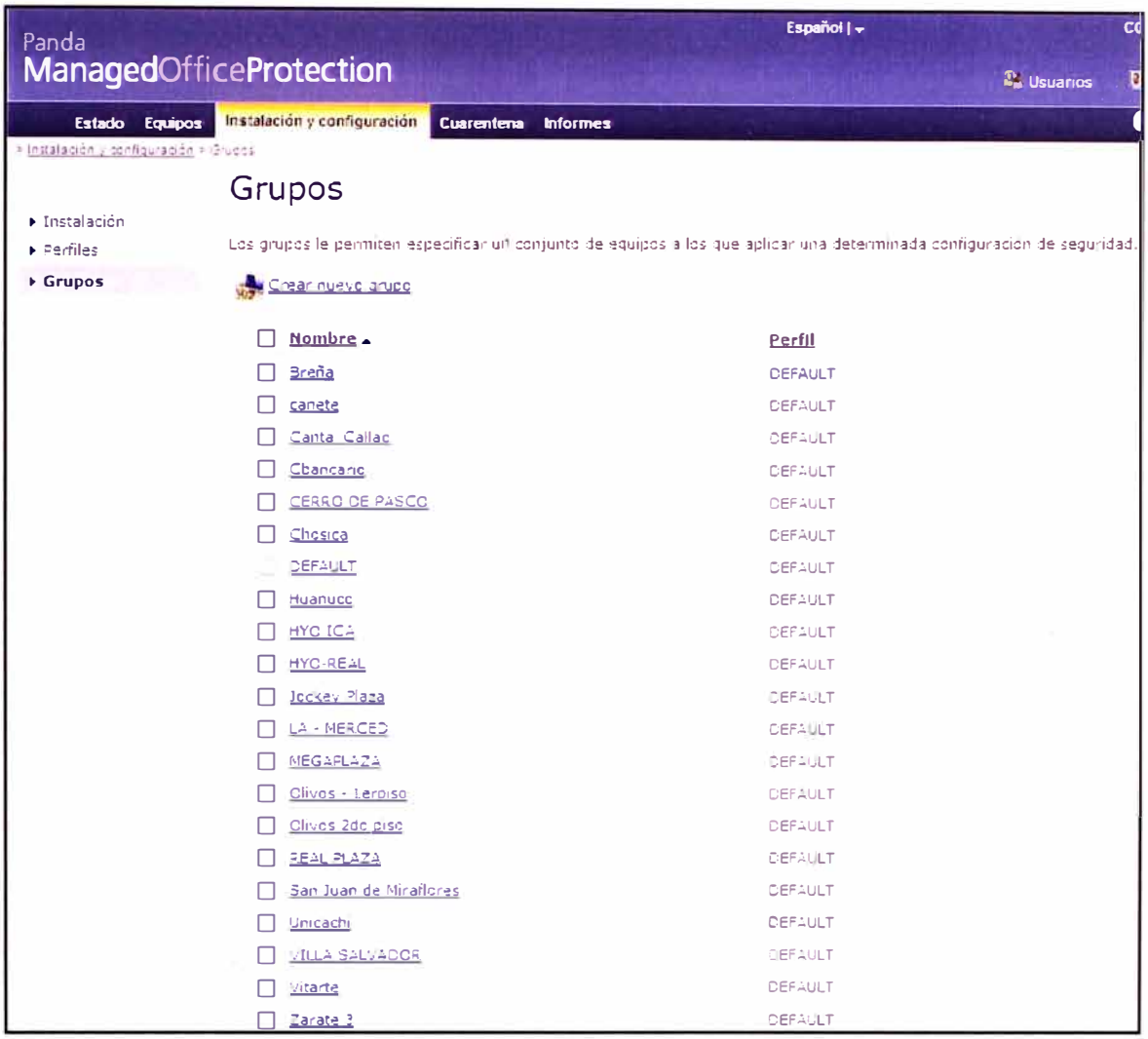
Aquí se muestra la ventana de inicio del Antivirus Corporativo MOF.
Como se ve en la imagen siguiente se tiene la grafica virus vs tiempo.



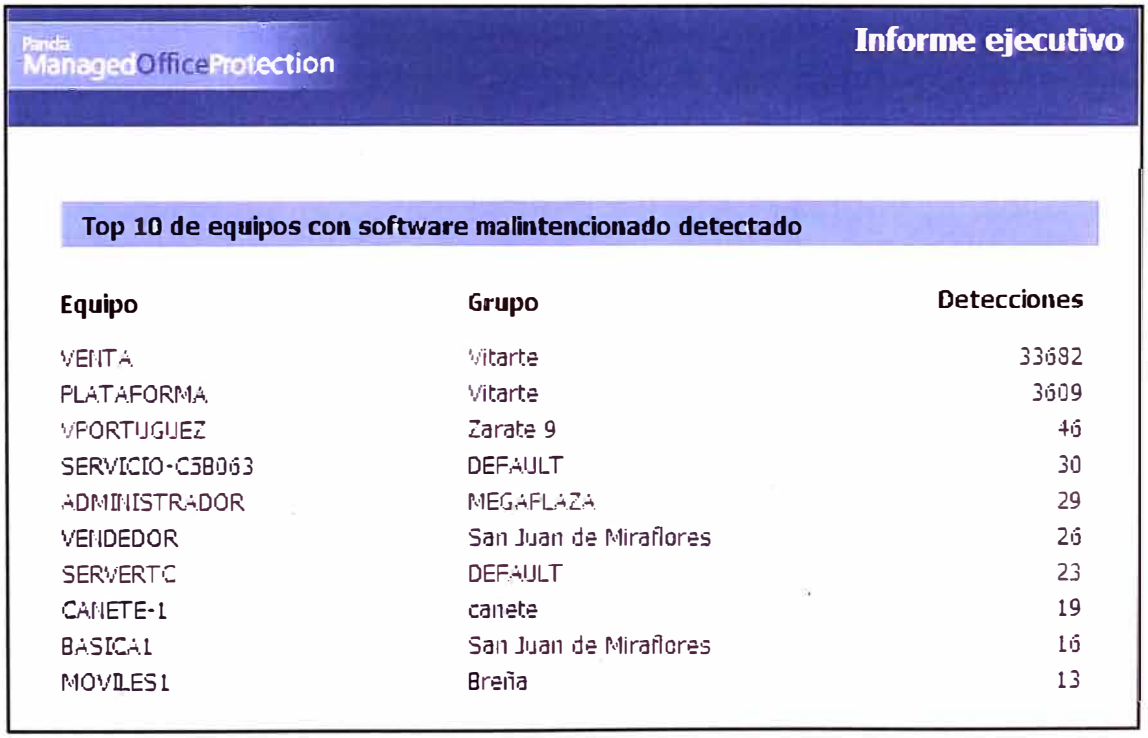
En la imagen siguiente vemos el estado de la protección de los equipos por grupos.



En la imagen siguiente vemos los grupos creados en la organización.



En la figura siguiente se muestra un reporte de TOP 10 de equipos con virus.



Aquí tenemos el estado de protección instalada en la organización.

Antivirus, Firewall o Antivirus + Firewall, así como el estado de actualización.

Panda Managed Office Protection — Informe ejecutivo

Alcance del Informe:

Todos los grupos de la organización

Datos obtenidos del 24/05/2009 al 24/06/2009

Estado de las protecciones

Protecciones instaladas

	Equipos	
Antivirus + Firewall	15	*(11,11%)*
Antivirus	120	*(88,89%)*
Firewall	0	*(0%)*
Total	**135**	

Actualización de las protecciones

	Equipos	
Actualizados	131	*(96,32%)*
Actualizados pendientes de reinicio	4	*(2,94%)*
Desactualizados	0	*(0%)*
Instalando protección	1	*(0,74%)*
Total	**136**	

Actualización del archivo de identificadores

	Equipos	
Actualizados	133	*(97,79%)*
Desactualizados	2	*(1,47%)*
No necesitan actualización	0	*(0%)*
Instalando protección	1	*(0,74%)*
Total	**136**	

En la imagen siguiente, un reporte ejecutivo mensual de los virus encontrados en la red, en la imagen anterior del TOP 10 podemos observar que la sede de vitarte es la que esta mas infectada por los virus y necesita una atención urgente por el área de soporte.

Office [illegible]ction

Informe ejecutivo

Detecciones:

Software malintencionado detectado

Virus	180462	(99,81%)
Spyware / Adware	230	(0,13%)
Dialers	0	(0%)
Jokes	1	(0%)
Herramientas de hacking y FFND	22	(0,01%)
Otros	95	(0,05%)
Total	**180810**	

Ataques bloqueados

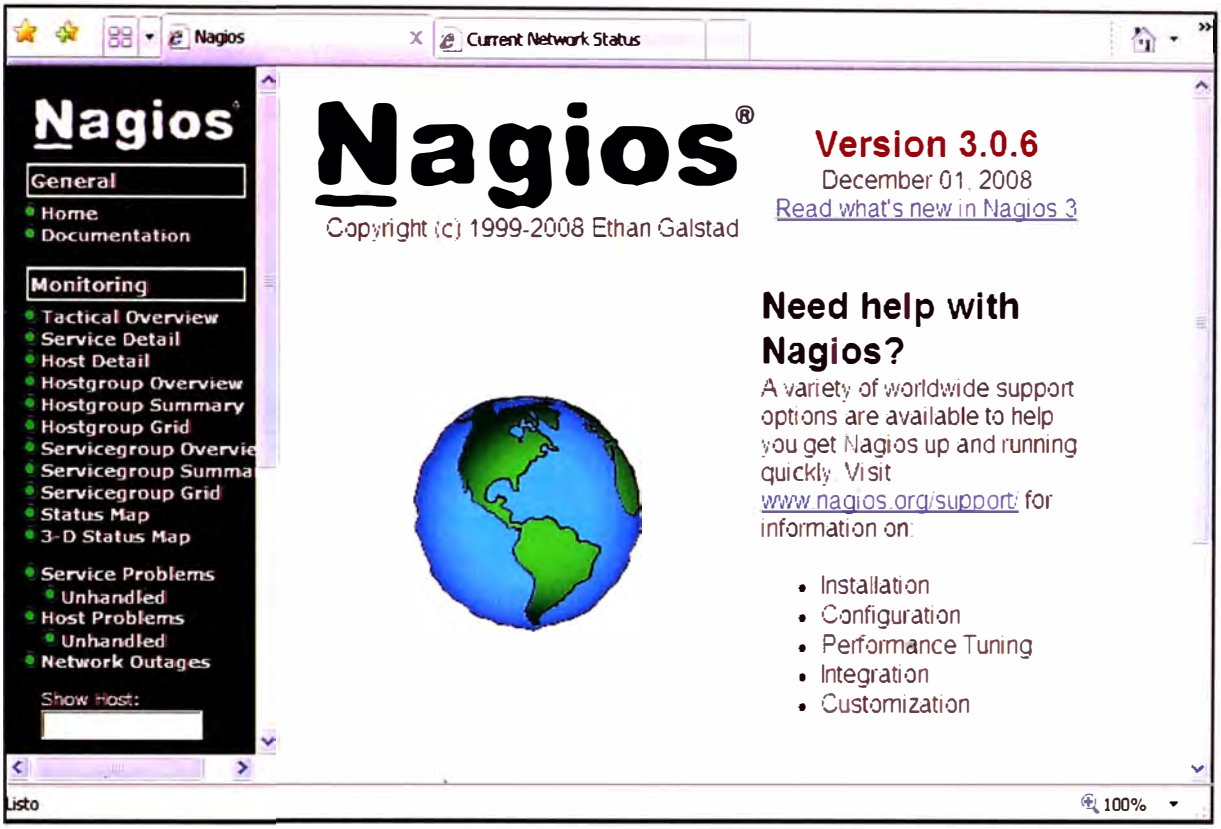
No hay suficiente información para mostrar esta sección

Paquete con cabecera inconsistente	0	(0%)
IP Spoofing	0	(0%)
Escaneo de puertos	0	(0%)
Combinación de indicadores TCP errónea	0	(0%)
Ataque de DoS	0	(0%)
Ataque LAND	0	(0%)
Ataques por fragmentación	0	(0%)
DHCP, DNS o WINS no solicitado	0	(0%)
Otros	0	(0%)
Total	**0**	

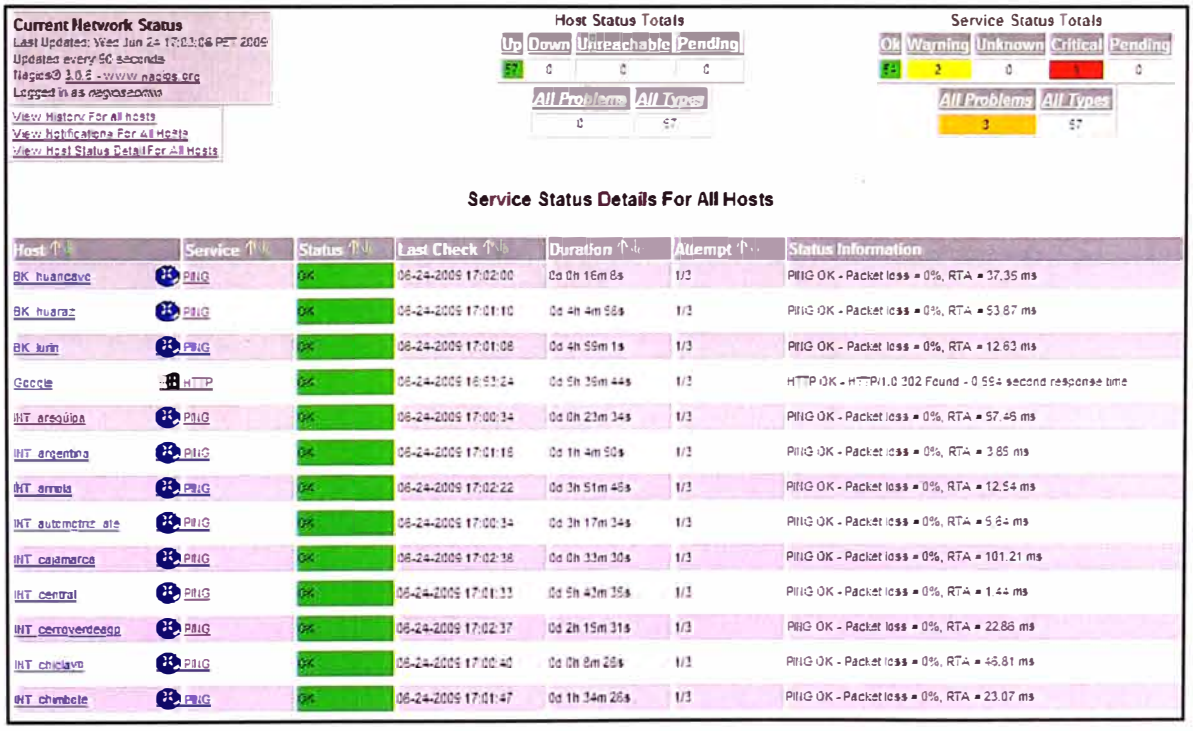
ANEXO G
MONITOREO CON NAGIOS

En la imagen siguiente observamos la pantalla inicial del software de monitoreo Nagios.

Como se ve en el menú de la derecha tiene varias opciones, de la cuales se describirán las mas importante.



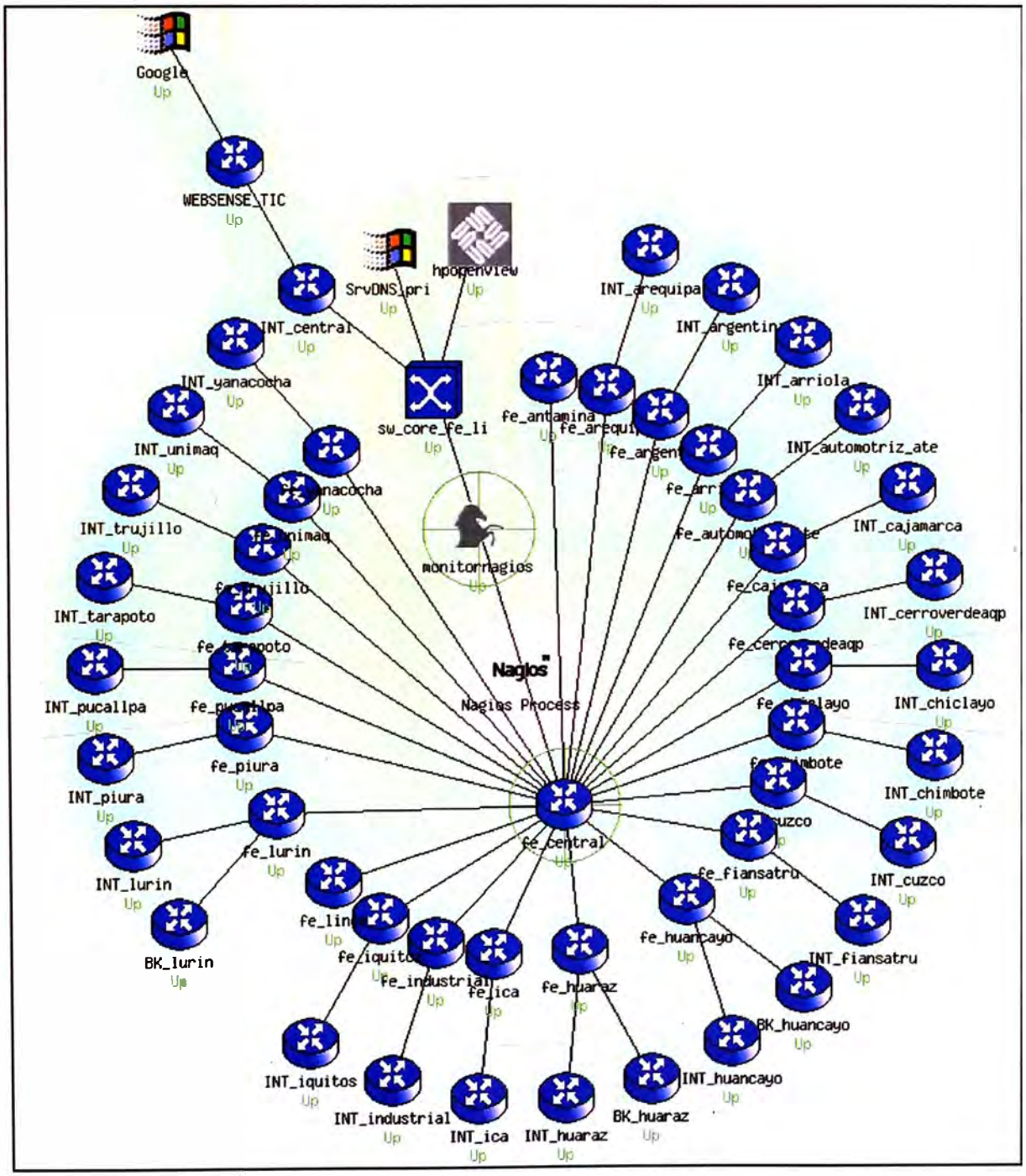
En la imagen siguiente observamos la opción Service Detail, en donde se muestran los servicios monitoreados, identificados por el host, servicio, estado, ultimo chequeo, duración, los intentos y la información del estado actual.



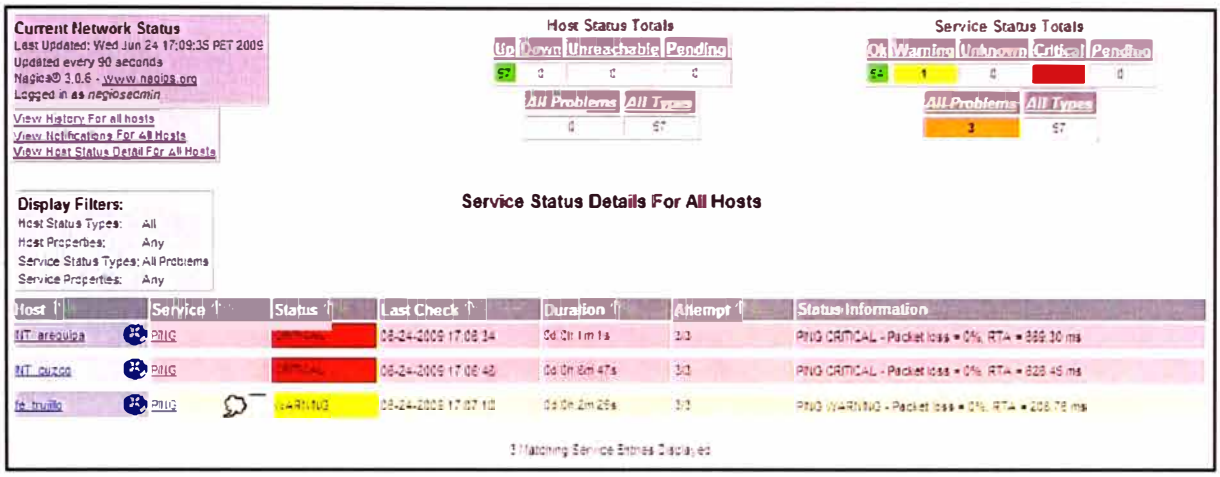
La imagen mostrada a continuación, es una de las más importantes, la opción usada es el status map, ubicada en el menú de la derecha.

Como se podrá observar, se agregan todos los equipos monitoreados: host, servidores, switch, router, y servicios de red.

Cuando ocurre un evento, el recuadro para a un estado de color rojo, indicado que existe un problema de comunicación con dicho equipo asociado.

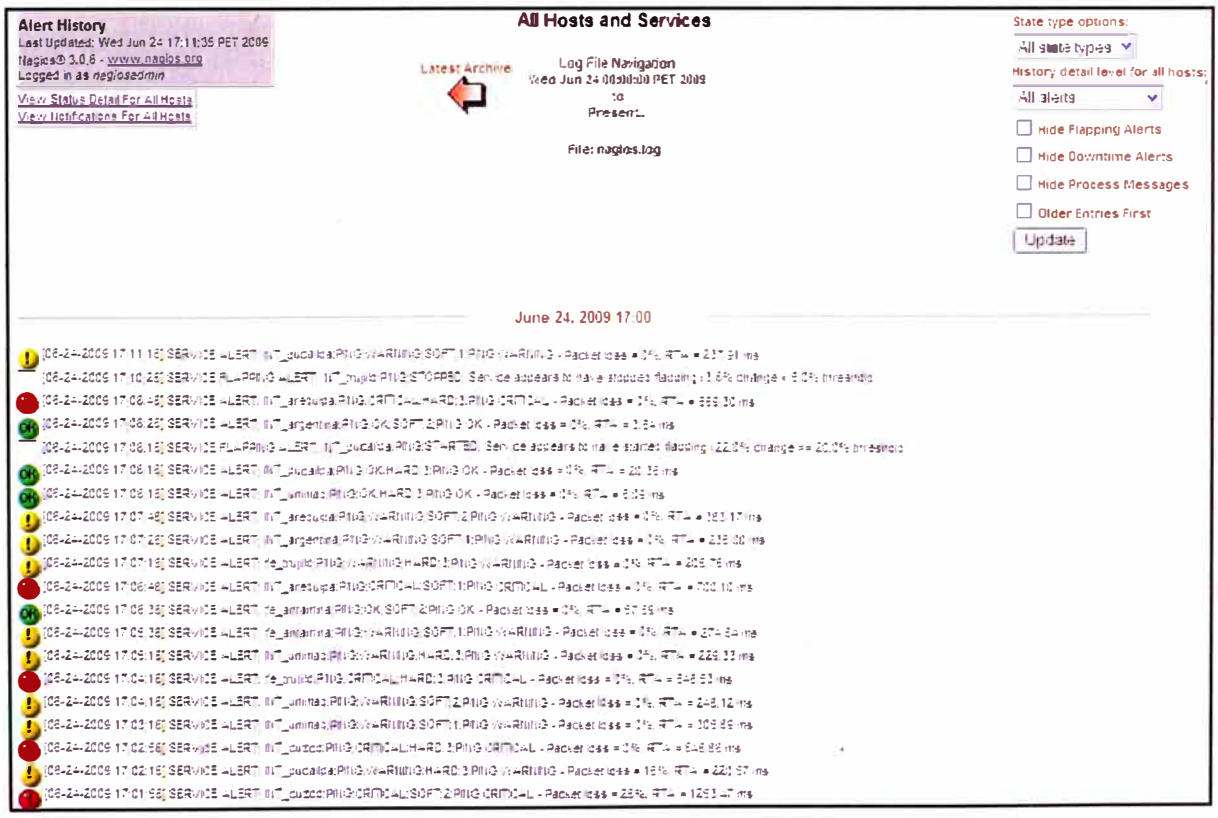


El menú siguiente Current Network Status, nos muestra los equipos encontrados en la red con el status marcado como Critical y Warning. Esto debido a que han pasado los umbrales definidos en la configuración.

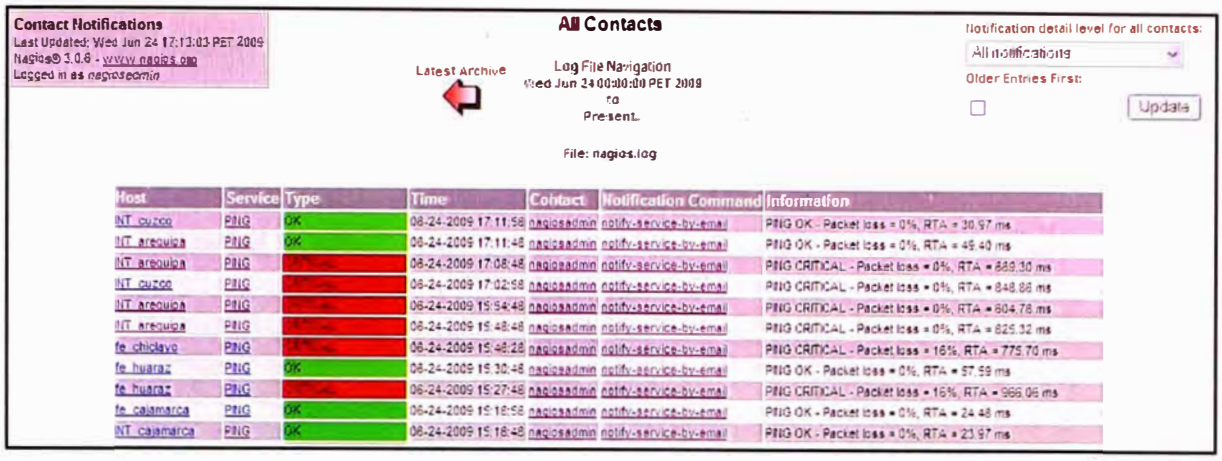


En la imagen siguiente se muestra el historial de alertas, identificados por un icono, así como la hora y fecha del equipo monitoreado.

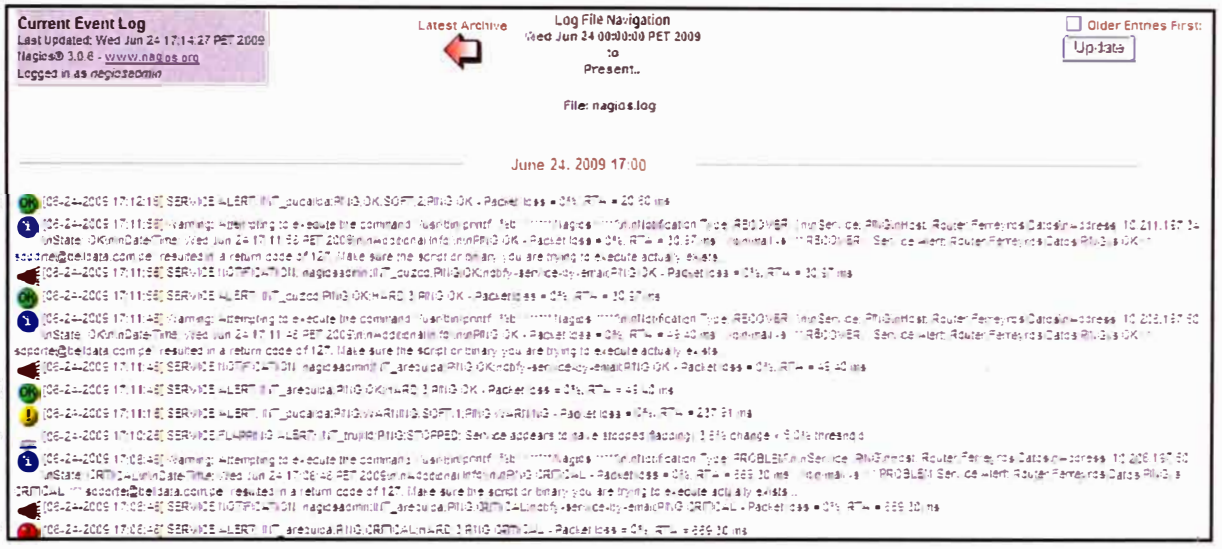
En este historial también se indica cuando el equipo ha vuelto a un estado normal, debajo del umbral configurado.



En la figura siguiente se muestra, las notificaciones realizadas a los contactos registrados, que puede ser un mensaje de correo por ejemplo a una cuenta establecida.



En la imagen siguiente se muestra los eventos de Log actuales.



Como se puede observar el software de monitoreo Nagios, se tiene varias ventanas con reporte de la red, tanto como un grafico de red, y registro en Log.

A continuación se muestra una parte de la configuración de los equipos asociados:

Como se ve en el cuadro de texto siguiente se define un servicio, luego se asocia a equipos de la red, por ejemplo: huanuco, SrvDns etc., seguidamente se tiene que especificar el servicio a monitorea, en nuestro caso el servicio PING, luego e importante es definir, los tiempo de chequeo, en este caso 3 minutos, y en caso se encontrara un equipo sin conexión se configura volver a verificar el servicio cada 1 minuto.

Se definen tres estados para la verificación del servicio:

CRITICO (CRITICAL) si el promedio de round trip (RTA) es mayor a 600 milisegundos o la pérdida de paquetes es 60% o más,

PRECAUCIÓN (WARNING) si el RTA es mayor a 200 ms o la pérdida de paquetes es 20% o más.

OK si el RTA es menor a 200 ms y la pérdida de paquetes es menor a 20%.

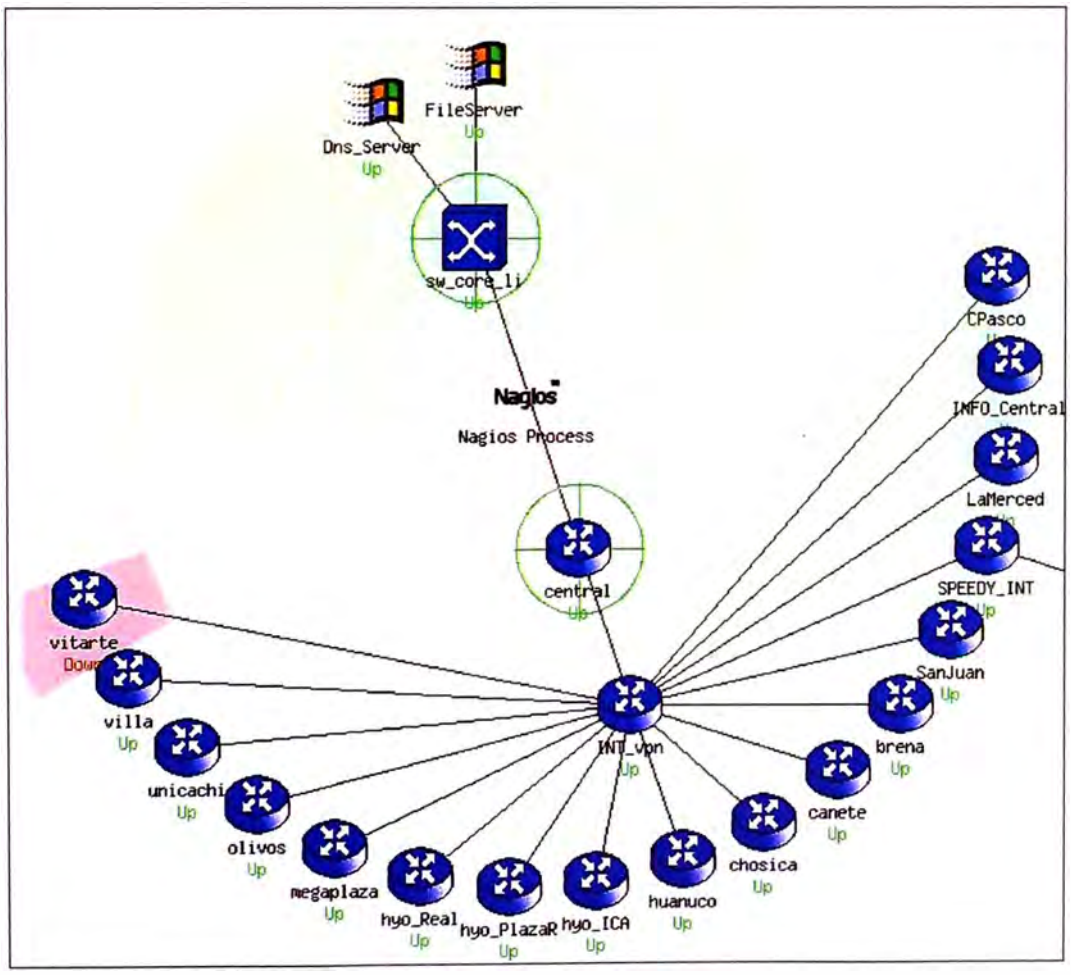
Muestra de los parámetros de la configuración

```
# Define a host for the local machine
define host{
Use     generic-switch
        Host_name    huanuco
        Alias        Router Huanuco SIC
        Address      10.28.25.1
        Hostgroups   switches
        Parents      central
        Icon_image   router.gif
        Status_image router.gd2
################################################################
define an optional hostgroup for Linux machines
define hostgroup{
        Hostgroup_name  switches
        Alias           network Switches
        }
define hostgroup{
      hostgroup_name  Dns_Server; The name of the hostgroup
      alias         Servidor PDC_DNS ; Long name of the group
      members       SrvDNS,servidorBD,mailserver;
      }
################################################################
# Define a service to "ping" the local machine
define service{
      use                     generic-service      ; Name of service template to use
      host_name                   SrvDNS,servidorBD,SrvMail;
      service_description         PING
      check_command               check_ping!100.0,20%!500.0,60%
      }
################################################################
define service{
      use                 generic-service ; Inherit values from a template
      host_name           chosica,canete,hyo_ica,vitarte,brena,olivos,huanuco,cpasco;
      service_description   PING          ; The service description
      check_command       check_ping!200.0,20%!600.0,60%  ; The command
used to monitor the service
      normal_check_interval  3            ; Check the service every 3 minutes under
normal conditions
      retry_check_interval   1           ; Re-check the service every minute until its
final/hard state is determined
      notifications_enabled  1           ;
      notification_options   c,r;
      }
################################################################
define service {
      host_name Google;
      service_description HTTP
      check_command check_http
      use generic-service;
      notification_interval 0
      notification_options   c,r
}
```

```
define service {
        use                     generic-services
        host_name               mailserver
        service_description     salida smtp
        is_volatile             0
        check_period            24x7
        max_check_attempts      3
        normal_check_interval 5
        retry_check_interval    1
        contact_groups          admins
        notification_period     24x7
        notification_options    c,r
        check_command           check_smtp
}
```

- **notification_options**: en las opciones de notificación, podremos indicar que muestre:
    - d (down): activo, devuelve el ping correctamente.
    - u (unreachable): inalcanzable, no devuelve solicitud de ping.
    - r (recovered): recuperado, activo tras una solicitud de ping unreachable

A continuación mostramos la gráfica de red de interconexión VPN de todas las sucursales con la sede Principal, para la empresa Servicio Integral de Comunicaciones.

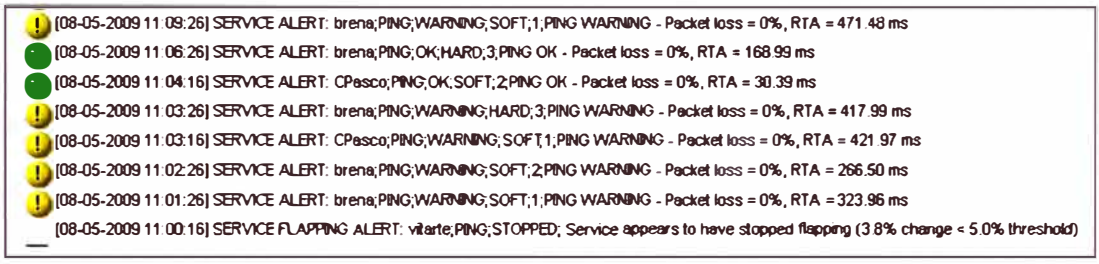


Se observa del grafico anterior que no hay conexión con la sede de vitarte, las conexiones a las demás sucursales se encuentra operativas, según mapa de red.

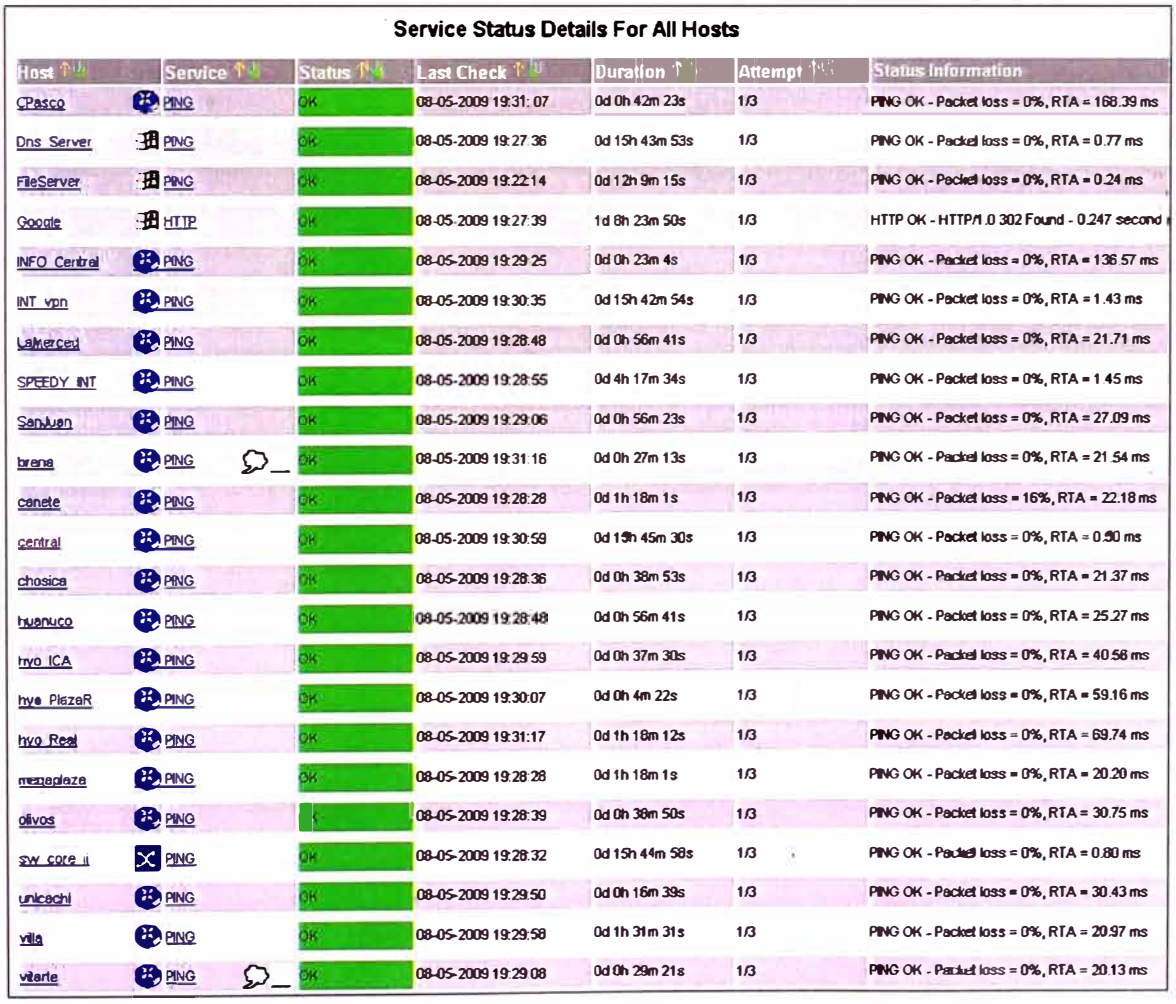
Al pasar el Mouse por encima del cualquier icono perteneciente a un equipo de la red monitoreada, se muestra más información, la cual es útil para tomar acción cuando existan problemas.

En la imagen siguiente vemos una parte del historial del estado de las conexiones con las sucursales a nivel nacional, como se puede observar, los tiempos de repuesta sin saturación de trafico se encuentra en promedio entre 21 mseg y 33 mseg.

Vemos también que se muestran las alarmas de warning al pasar los 200ms, también se muestran el registro OK, cuando se restablecen los parámetros debajo del umbral.



En la grafica mostrada a continuación se muestran los tiempos de repuesta:



Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
CPasco	PING	OK	08-05-2009 19:31:07	0d 0h 42m 23s	1/3	PING OK - Packet loss = 0%, RTA = 168.39 ms
Dns_Server	PING	OK	08-05-2009 19:27:36	0d 15h 43m 53s	1/3	PING OK - Packet loss = 0%, RTA = 0.77 ms
FileServer	PING	OK	08-05-2009 19:22:14	0d 12h 9m 15s	1/3	PING OK - Packet loss = 0%, RTA = 0.24 ms
Google	HTTP	OK	08-05-2009 19:27:39	1d 8h 23m 50s	1/3	HTTP OK - HTTP/1.0 302 Found - 0.247 second
INFO_Central	PING	OK	08-05-2009 19:29:25	0d 0h 23m 4s	1/3	PING OK - Packet loss = 0%, RTA = 136.57 ms
INT_vpn	PING	OK	08-05-2009 19:30:35	0d 15h 42m 54s	1/3	PING OK - Packet loss = 0%, RTA = 1.43 ms
LaMerced	PING	OK	08-05-2009 19:28:48	0d 0h 56m 41s	1/3	PING OK - Packet loss = 0%, RTA = 21.71 ms
SPEEDY_INT	PING	OK	08-05-2009 19:28:55	0d 4h 17m 34s	1/3	PING OK - Packet loss = 0%, RTA = 1.45 ms
SanJuan	PING	OK	08-05-2009 19:29:06	0d 0h 56m 23s	1/3	PING OK - Packet loss = 0%, RTA = 27.09 ms
brena	PING	OK	08-05-2009 19:31:16	0d 0h 27m 13s	1/3	PING OK - Packet loss = 0%, RTA = 21.54 ms
canete	PING	OK	08-05-2009 19:28:28	0d 1h 18m 1s	1/3	PING OK - Packet loss = 16%, RTA = 22.18 ms
central	PING	OK	08-05-2009 19:30:59	0d 15h 45m 30s	1/3	PING OK - Packet loss = 0%, RTA = 0.90 ms
chosica	PING	OK	08-05-2009 19:28:36	0d 0h 38m 53s	1/3	PING OK - Packet loss = 0%, RTA = 21.37 ms
huanuco	PING	OK	08-05-2009 19:28:48	0d 0h 56m 41s	1/3	PING OK - Packet loss = 0%, RTA = 25.27 ms
hyo_ICA	PING	OK	08-05-2009 19:29:59	0d 0h 37m 30s	1/3	PING OK - Packet loss = 0%, RTA = 40.58 ms
hyo_PlazaR	PING	OK	08-05-2009 19:30:07	0d 0h 4m 22s	1/3	PING OK - Packet loss = 0%, RTA = 59.16 ms
hyo_Real	PING	OK	08-05-2009 19:31:17	0d 1h 18m 12s	1/3	PING OK - Packet loss = 0%, RTA = 69.74 ms
mesapalaza	PING	OK	08-05-2009 19:28:28	0d 1h 18m 1s	1/3	PING OK - Packet loss = 0%, RTA = 20.20 ms
olivos	PING	OK	08-05-2009 19:28:39	0d 0h 38m 50s	1/3	PING OK - Packet loss = 0%, RTA = 30.75 ms
sw_core_ii	PING	OK	08-05-2009 19:28:32	0d 15h 44m 58s	1/3	PING OK - Packet loss = 0%, RTA = 0.80 ms
unicachi	PING	OK	08-05-2009 19:29:50	0d 0h 16m 39s	1/3	PING OK - Packet loss = 0%, RTA = 30.43 ms
villa	PING	OK	08-05-2009 19:29:58	0d 1h 31m 31s	1/3	PING OK - Packet loss = 0%, RTA = 20.97 ms
vitarte	PING	OK	08-05-2009 19:29:08	0d 0h 29m 21s	1/3	PING OK - Packet loss = 0%, RTA = 20.13 ms

BIBLIOGRAFÍA

1. W. Stallings, “Comunicaciones y Redes de Computadoras”, Prentice Hall, 1998.

2. Russel, Charlie y Crawford y Crwawford, Sharon y Gerend, Jason “Microsoft Windows Server 2003 Running”, McGraw-Hill, 2003.

3. Ernesto Ariganello, “Técnicas de configuración de router Cisco”, Ra-Ma, 2008.

4. Cisco Sytems, Inc “Guia del Segundo año. CCNA 3 y 4. Tercera Edición”, Pearson Educacion, 2004.

5. Justo Carrecedo Gallardo, “Seguridad en Redes Telematicas”, McGraw-Hill, 2004

6. Tony Howlett, “Software Libre: Herramientas de seguridad”, Grupo Anaya 2005.

7. Antonio Villalón Huerta, “Seguridad en UNIX y Redes”, http://www.scribd.com/reader/related/1739221 extraída el 12 de Diciembre del 2008

8. Sistema de Respaldo configuración DLINK, http://www.dlink-me.com/ftp/firewall/ConfigExamples/DFL-800_1600_2500-VLAN_and_route_failover.pdf , extraída el 11 de Marzo del 2009.

9. IPSEC, http://www.ipsec-howto.org/spanish/x161.html, extraído el 20 de Marzo del 2009.

10. Conceptos: Servicios de Red y Aplicaciones, http://www.ieev.uma.es/biblos/material/mater/0361.htm, extraído el 10 de Abril del 2009.

11. Servicios IP, http://docs.sun.com/app/docs/doc/820-2981/6nei0r0rq?l=es&a=view, extraído el 12 de abril del 2009.

12. Soluciones DLINk, http://www.dlink.com, extraído 12 de abril del 2009.

13. Soluciones Antivirus, Empresas, http://www.pandasecurity.com/spain/, extraído 15 de abril del 2009.

14. D-Link Network Security on-line http://www.dlink.com.tw/online_manual/security/dfl-210/, extraído 15 abril 2009.