ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"DISEÑO E IMPLEMENTACIÓN DE UNA RED SEGURA Y CONVERGENTE EN LA UNIVERSIDAD COTOPAXI, BASADO EN TECNOLOGÍA 3COM"

HUGO SANTIAGO YÉPEZ CROW
MARCELO PAÚL ERAZO CARRIÓN

Sangolquí – Ecuador
2007

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado "Diseño e implementación de una red segura y convergente en la Universidad Cotopaxi, basado en tecnología 3Com." ha sido desarrollado en su totalidad por los señores Hugo Santiago Yépez Crow con C.C 060317947-4 y Marcelo Paúl Erazo Carrión con C.C 171312474-9, bajo nuestra dirección.

DIRECTOR

Ing, Gonzalo Olmedo

CODIRECTOR

Ing. Julio Larco

RESUMEN DEL PROYECTO

El diseño e implementación de una red segura y convergente en la Universidad Cotopaxi, basado en tecnología 3Com se lo realizó con elementos claves para manejar la convergencia, la cuál es dividida en tres partes: la primera es manejar un nivel bajo de colisiones para evitar aumentar latencia y errores sobre la red, a través del estándar 802.1Q también se puede implementar priorización de tráfico en capa 2. El segundo elemento es la calidad de servicio en donde se puede modelar el tráfico de la red para proveer prioridad a las aplicaciones que sean más sensibles a la latencia, jitter y pérdida de paquetes. El tercer elemento importante es poder manejar IEEE 802.3af para que los teléfonos IP sean alimentados de energía eléctrica directamente por el switch para que la telefonía siga operativa incluso ante la falla de energía ya que los UPS que alimentan los switches están centralizados facilitando la implementación del respaldo de energía eléctrica.

Para el diseño de la red segura y convergente se realizó la selección de los equipos de acuerdo a las características que presentan las dos marcas más importantes en *networking* como lo es *3Com y Cisco.* Se escogió a 3Com debido a su superioridad.

Para implementar el sistema de seguridad se consideró tres aspectos: alta disponibilidad, integridad de los datos y confidencialidad de los mismos. La Alta disponibilidad se puede manejar con mayor o menor nivel a través de los protocolos XRN, Link Aggragation, STP/RSTP/MSTP. La integridad de datos se puede lograr con IEEE 802.1X (autenticación AAA) e implementación de listas de acceso para que usuarios no autorizados sean imposibilitados de acceder a datos que no deben ser manipulados. La confidencialidad de los datos se puede lograr a través de túneles VPN a través del Internet y encripción también con el IPS que emplea la mejor defensa contra los hackers que lanzan ataques a las aplicaciones más importantes de la red.

.

DEDICATORIA

Este proyecto lo dedicamos en primer lugar a nuestros padres, por todo el apoyo, confianza y ayuda incondicional.

A nuestros hermanos, porque ellos son parte de nosotros y hemos estado juntos en todo momento.

A 3Com, por toda la información valiosa y a la Universidad Cotopaxi por confiar en nosotros para realizar este trabajo.

Finalmente a Dios, el pilar más importante de nuestras vidas, sin el cual nada de esto hubiera sido posible.

AGRADECIMIENTO

Quiero dejar testimonio de profunda gratitud a Dios, por permitirnos que se nos cumplan nuestras aspiraciones y esperanzas de ser unos buenos profesionales.

Agradecemos a nuestros padres por ser ejemplo de vida y superación.

También agradecemos a nuestros maestros por compartir sus conocimientos con nosotros.

PRÓLOGO

El objetivo del proyecto es, el diseño e implementación de una red segura y convergente basado en tecnología 3Com, ya que en la actualidad esta tecnología esta creciendo y desarrollándose de manera excepcional en el mercado de las redes, permitiendo a cualquier empresa alcanzar la excelencia en la velocidad de sus comunicaciones.

Este proyecto envuelve temas relacionados con la convergencia en la red de datos pero se enfoca también en indicar los grandes valores que se obtienen al migrar a una red con estas características, una de ellas es la seguridad, la integridad y la velocidad de los datos, que se emplean desde redes muy pequeñas como hogares hasta redes empresariales y corporativas.

El proyecto muestra el funcionamiento y las características de los equipos que se deben emplear al momento de diseñar redes seguras y convergentes, y también de los estándares que estos equipos utilizan para alcanzar a este tipo de redes.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE TERMINOS

A

Ancho de banda. Capacidad de transmisión de datos que tiene un medio determinado, generalmente cuantificado según el número de bits que se transmiten en un segundo.

Anillo. Topología de red en la que las estaciones se conectan físicamente a las adyacentes formando un anillo.

ANSI. American National Standarization Institute. Organismo nacional de estandarización y normalización de los Estados Unidos.

ARP. Address Resolution Protocol. Protocolo de nivel de red de la familia TCP/IP para la traducción de direcciones físicas de bajo nivel a direcciones de red.

ATM. Asynchrounous Transfer Mode. Protocolo estandarizado internacionalmente para transmisión de grandes volúmenes de datos a alta velocidad y basado en conmutación de paquetes. ATM emplea pequeñas celdas con un tamaño fijo de 53 bytes para enviar los datos en paquetes que pueden ser conmutados de forma ultrarápida a través de redes de telecomunicación de alto rendimiento. ATM es la primera tecnología que ha sido desarrollada desde el principio para que pueda soportar aplicaciones de transmisión de voz, video y datos. Se adapta bien a la naturaleza de las comunicaciones WAN. En la actualidad, ATM proporciona velocidades de transmisión desde 64Kbps hasta 622Mbps, pudiendo llegar a soportar en el futuro velocidades del orden de gigabits por segundo.

B

BRI. Interfaz de acceso básico a la RDSI. Ofrece dos canales B para datos a 64Kbps y un canal D de señalización a 16Kbps.

Bridge. Dispositivo que interconecta dos redes a nivel de enlace. El bridge monitoriza el tráfico en las redes que conecta y dirige los paquetes al destino apropiado.

Bus. Topología de red en la que las estaciones se conectan a un único cable.

C

Caudal garantizado. También conocido como CIR, es un parámetro que caracteriza a los circuitos virtuales permanentes en una red Frame Relay. Medido en bits por segundo, el CIR representa la capacidad media que el operador de la red debe reservar para el circuito virtual.

CCITT. Consultant Committee on International Telephone and Telegraph. Organismo internacional de estandarización y normalización en telecomunicaciones. En la actualidad ha cambiado su nombre a ITU-T.

Checksum. Método de detección de errores en la transmisión de datos. Antes del envío, se calcula un valor a partir de los datos que es transmitido junto a éstos. En recepción, se calcula el valor a partir de los datos recibidos y se compara con el generado en la transmisión. Si son distintos, es porque ha ocurrido algún error durante la transimisión que ha alterado el contenido de los datos.

Circuito virtual. Conexión lógica entre dos puntos.

Circuito virtual permanente. Abreviado como PVC, de Private Virtual Circuit. Es un circuito virtual que está siempre disponible para la transmisión y que es establecido por el operador de la red de forma administrativa.

Control de acceso al medio. Abreviado como MAC, de Medium Access Control, especifica el mecanismo utilizado para que distintas estaciones puedan utilizar un único medio compartido para transmitir sus datos.

Control del enlace lógico. Abreviado como LLC, de Logical Link Control. Es un conjunto de protocolos de nivel de enlace definido por el estándar IEEE 802.2 que puede ser utilizado para el intercambio de información a través de diferentes redes de área local.

CPA. Centro proveedor de acceso a Internet.

CSMA/CD. Carrier Sense Multiple Access with Collision Detection. Método de control de acceso al medio en el que los dispositivos que quieren transmitir deben primero comprobar que el medio está disponible. En ese caso, empieza a transmitir y comprueba que ninguna otra estación ha comenzado a enviar datos al mismo tiempo, en cuya caso ocurre una colisión. Si se detecta una colisión, los dispositivos esperan un intervalo aleatorio de tiempo antes de volver a intentar la transmisión.

CRC. Cyclic Redundancy Check. Método de detección de errores basado en códigos polinómicos.

D

Datagrama. Unidad de información que es transmitida por los protocolos de nivel de red.

DCE. Equipo de comunicaciones de datos.

DTE. Equipo terminal de datos.

E

EMI. Inteferencia electromagética.

Enlace. Conexión física entre dos nodos.

Estación. Sistema o dispositivo conectado a una red.

Ethernet. Tipo de red local diseñada originalmente para trabajar a 10Mbps sobre cable coaxial. Está basado en una topología en bus y es muy similar al estándar IEEE 802.3 que especifica el método CSMA/CD para control de acceso al medio.

F

Fast Ethernet. Evolución de Ethernet que aumenta el ancho de banda hasta 100Mbps.

FDDI. Fiber Distributed Data Interface. Tecnología LAN de alta velocidad basada en el empleo de fribra óptica como medio de transmisión. Está basada en una topología en doble anillo y soporta velocidades de 100Mbps.

Fibra óptica. Tipo de cable construido a partir de capas concéntricas de cristal o plástico que transmite señales de luz y proporciona anchos de banda mucho mayores que el cobre y además ofrece mayor fiabilidad y seguridad.

Frame Relay. Protocolo utilizado en la interfaz entre los dispositivos de usuario (routers, bridges, hosts) y equipos de red (nodos de conmutación) que posibilita la transmisión de los datos aplicando técnicas de conmutación de paquetes. Se caracteriza por confiar en la fiabilidad de los actuales medios transimisión, eliminando el nivel de red y reduciendo la funcionalidad del nivel de enlace.

Full Duplex. Enlace que es capaz de soportar la transmisión simultánea en ambos sentidos de la comunicación.

G

Gateway. Su acepción más común es la de dispositivo que interconecta redes a nivel de aplicación, haciendo las conersiones de protocolo necesarias. Dentro de la terminología de Internet, es cualquier dispositivo que interconecta redes.

H

HDLC. High-level Data Link Protocol. Protocolo de enlace orientado a bit estandarizado por la ITU-T y en el que están ampliamente basados la mayoría de los protocolos de enlace.

Host. En la terminología de Internet, un host es un equipo que tiene asignado una dirección IP y que no hace funciones de encaminamiento.

I

IAB. Internet Activities Board. Órgano coordinador de las actividades relacionadas con la estandarización de los protocolos de Internet.

IEEE. Institute of Electrical and Electronical Engineers. Asociación de profesionales de la ingeniería agrupados en diferentes comités para trabajar en diversas áreas. El comité 802 se dedica al desarrollo de estándares para redes locales.

IP. Internet Protocol. Protocolo de nivel de red de la familia TCP/IP.

IPCP. IP Control Protocol. Protocolo de control de IP sobre conexiones punto a punto utilizando el protocolo PPP.

Internet. Conjunto de redes estatales, universitarias y comerciales interconectadas entre sí que fue construida inicialmente por el Ministerio de Defensa Norteamericano para interconectar redes de investigación gubernamentales y universitarias.

ISO. Intenational Standarization Organization. Organismo de estandarización y normalización internacional. Creador del modelo de referencia OSI (Open Systems Interconection) y de los protocolos de comunicaciones asociados.

ITU-T. International Telecommunication Union - Telecommunication Standardization Sector. Organismo internacional de estandarización y normalización de las telecomunicaciones. Previamente denominado CCITT.

L

LAN. Local Area Network. Ver red de área local.

LCP. Link Control Protocol. Procolo de control del enlace en conexiones punto a punto con el protocolo PPP.

M

MAC. Control de acceso al medio.

Modelo de referencia OSI. Modelo arquitectónico definido por ISO que está compuesto por siete capas o niveles: físico, enlace, red, transporte, sesión, presentación y aplicación. Es el marco de trabajo para el desarrollo de estándares que permitan la comunicación entre sistemas de diferentes fabricantes.

MTU. Maximum Transfer Unit. Tamaño máximo de los datos de usuario que pueden viajar en un paquete de un protocolo determinado.

Multiplexación. Combinación de dos o más comunicaciones para ser enviadas por un único canal.

N

NCP. Network Control Protocol. Protocolo de control de red en conexiones punto a punto con el protocolo PPP.

O

OSI. Open Systems Interconnection. Término que se refiere a la comunicación entre sistemas abiertos, que son aquellos que proporcionan el soporte para los protocolos basados en el modelo de referencia OSI y que, por lo tanto, son capaces de comunicarse con otros sistemas abiertos.

P

Paquete. Unidad de información que viaja a través de una red.

PBX. Private Branch Exchange. Centralita privada de conmutación.

PDU. Protocol Data Unit. Porción de un paquete de un protocolo determinado que contiene los datos de usuario.

PRI. Interfaz de acceso primario a la RDSI. Proporciona en Europa 30 canales B a 64Kbps para datos y un canal D a 64Kbps para señalización.

Protocolo. Conjunto de reglas que rigen la interacción entre entidades que se comunican. Cada capa o nivel de una arquitectura define diferentes protocolos para soportar los diversos tipos de comunicación que llevan a cabo cada capa. Por ejemplo, los protocolos del nivel de enlace definen las reglas de interacción entre dos nodos conectados por un único enlace.

PPP. Protocolo punto a punto. Protocolo que proporciona un mecanismo estándar para transportar datagramas de diversos tipos de protocolos a través de un enlace punto a punto.

R

RDSI. Red Digital de Servicios Integrados.

Red de área extensa (WAN). Red en la que los sistemas se conectan mediante servicios de telecomunicaciones tales como líneas dedicadas, enlaces por satélite y enlaces de fibra óptica a través de distancias relativamente grandes.

Red de área local (LAN). Interconexión de estaciones relativamente poco separadas.

Red troncal (Backbone). Porción de una red, usualmente con gran ancho de banda, que proporciona el transporte utilizado para encaminar la información desde su origen al destino. Una red troncal puede ser empleada para interconectar otras redes.

RFC. Request For Comments. Documentos de libre difusión que sirven como medio de comunicación a la comunidad Internet para el desarrollo de estándares, o para divulgación de información de utilidad.

RTB. Red Telefónica Básica.

Router. Sistema que encamina información entre redes. Los routers operan a nivel de red y utilizan las direcciones de red para determinar hacia dónde encaminar la información.

S

SAS. Single Attachment Station. Estación en una red FDDI que se conecta a uno sólo de los dos anillos de fibra óptica que la componen.

SMT. Station Management. Parte de la especificación FDDI que define la capa de la estación de gestión donde se especifica la configuración de las estaciones FDDI, la configuración y las características del control del anillo.

Spoofing. Técnica de simulación empleada principalmente en los routers RDSI en la que en cada extremo de la conexión, los routers "convencen" a los dispositivos de la LAN de que la conexión WAN está activa permanentemente, aunque ésta sólo lo esté realmente mientras se transmiten los datos de usuario.

T

TCP. Transmission Control Protocol. Protocolo de nivel de transporte de la familia TCP/IP.

TCP/IP. Familia de protocolos definida para la operación en entornos interred.

Testigo. Trama especial que no transporta datos de usuario y que es pasada de una estación a otra en redes con acceso al medio por paso de testigo (Token Passing) para indicar qué estación es la que tiene el control sobre el medio.

Throughput. Capacidad de transmisión de un dispositivo. Se mide en bits por segundo.

Token passing. Método de control de acceso al medio que utiliza un testigo o token para llevar a cabo el control. Una estación sólo puede transmitir cuando está en posición del testigo.

Trama. Unidad de información que es transmitida por los protocolos de nivel de enlace.

Tráfico asíncrono. Modo de transmisión en el que las señales de entrada y de salida no guardan ninguna relación temporal entre sí.

Tráfico síncrono. Forma de transmisión en la que las señales de entrada y de salida tienen una relación temporal directa.

W

WAN. Wide Area Network. Ver Red de área extensa.

CAPÍTULO I

INTRODUCCIÓN

1.1. INTRODUCCIÓN A LA TELEFONÍA IP

Hace treinta años, el investigador Robert Metcalfe tuvo la visión de que habría alguna forma más económica de conectar computadoras para que la gente pudiera compartir mejor la información y ser más productiva. Su trabajo creó un cambio revolucionario en la tecnología de redes de computación: La tecnología Ethernet y una compañía multimillonaria, líder mundial en redes de computación: 3Com Corporation (Shuguang, 2002).

Hace seis años, se desarrollo un conjunto dedicado de productos de telefonía que pudieran operar confiablemente a través de las redes de datos. Este innovador sistema hoy se llama Telefonía sobre Redes. La Solución de Telefonía fue diseñada desde sus comienzos para aprovechar el poder, la flexibilidad y la economía de una red de datos, sin tener que sacrificar la confiabilidad y la familiaridad de los sistemas telefónicos tradicionales (Shuguang, 2002).

Hoy en día, se ofrece a los clientes una de las formas más económicas de utilizar redes Ethernet para mejorar sus comunicaciones telefónicas empresariales. Estas redes eliminan la necesidad de tener infraestructura de cables separados de voz y datos, y reducen enormemente los costos de instalación, operación y administración.

La Solución de Telefonía sobre Redes, soporta una amplia gama de configuraciones empresariales. Ya sea para oficinas sucursales más pequeñas o instalaciones de campos más grandes; estos sistemas ofrecen capacidades mejoradas y aplicaciones sofisticadas que cuestan menos y hacen mucho más que los sistemas telefónicos tradicionales.

La Solución de Telefonía sobre Redes tiene la inteligencia, el poder y la flexibilidad de administrar los requerimientos de las organizaciones más exigentes con oficinas en una o más localidades. Miles de empresas ya han descubierto que es una manera mejor de administrar sus comunicaciones de voz. Lo que hace que las soluciones de telefonía sobre redes sean tan atractivas es la habilidad de aprovecharse de la potencia y la flexibilidad de una red de datos sin sacrificar su confiabilidad. La confiabilidad se logra al aislar la funcionalidad del sistema telefónico de las funciones cotidianas asociadas con computadoras de escritorio y servidores. Los teléfonos comparten la red de datos con computadoras de escritorio y servidores, pero no utilizan a las computadoras de escritorio o a los servidores para el tráfico de voz. Es como manejar dos automóviles en la misma carretera; aún si la computadora falla, el tráfico de voz puede pasar sin obstrucciones.

El núcleo de la plataforma NBX yace en la alta disponibilidad del hardware de 3Com, así como en un sistema operativo en tiempo real tan confiable que es el que se utiliza en los marcapasos para el corazón humano. La más moderna tecnología del Procesador de Señales Digitales (DSP, por sus siglas en inglés) potencia teléfonos y otros de los componentes en el sistema NBX, asegurando que todos los dispositivos sean capaces de alcanzar su máximo rendimiento.

La mayoría de los sistemas telefónicos aparentan ser un misterio a los usuarios del diario y muchas veces al personal responsable de su administración. El resultado es la pérdida de productividad y de oportunidades.

Una interfaz administrativa increíblemente intuitiva le permite a los usuarios individuales y a los administradores personalizar por completo la solución para satisfacer sus requerimientos personales. Esta herramienta, basada en navegador y protegida por contraseña, ofrece menús desplegables personalizados a cada faceta del sistema. Las organizaciones más grandes encuentran herramientas para ahorrar tiempo que simplifican la creación de perfiles departamentales para administrar a sus usuarios telefónicos.

La tecnología de comunicaciones de voz elimina por completo los altos costos y los altos niveles de ansiedad que generalmente acompañan a las mudanzas de líneas telefónicas en las oficinas. Cualquier persona que haya tenido que esperar días por una costosa llamada de servicio, sólo para que le muevan el teléfono, apreciará profundamente las capacidades de autolocalización de los teléfonos NBX. Simplemente desconecte un teléfono de una localidad y conéctelo en el enchufe de otra red. El número de extensión del usuario, su correo de voz y las funciones personales se mudan con el teléfono.

La arquitectura comienza con una base Ethernet IEEE 802.3 que le permite a los usuarios conectar su teléfono IP en millones de puertos Ethernet alrededor del mundo. El sistema crece al añadir switches y routers de datos estándares en la industria, expandiendo el tamaño y las capacidades a medida que lo exige la demanda. Las organizaciones escogen el tipo de conectividad Ethernet que más les conviene, desde LANs inalámbricas a WANs multi-sitios.

Las soluciones usan un conjunto diverso de interfaces basadas en estándares, incluyendo:

· IMAP4 que permite que los usuarios vean y escuchen mensajes de voz con email clientes estándares (e.j., Microsoft Outlook, Eudora).
· TAPI para una integración de telefonía y computadoras (CTI, por sus siglas en inglés) que permite a los usuarios marcar números y manejar llamadas activas desde la pantalla de una computadora.
· TAPI/WAV que soporta conexiones inalámbricas a centros de llamada y aplicaciones de mensajería unificada.
· H.323 que se utiliza para conectar múltiples sitios o dispositivos de terceros. Además, soporta activamente a varios fabricantes terceros que crean aplicaciones de software para mejorar las capacidades de una plataforma NBX.

Las necesidades empresariales inevitablemente cambian; por lo tanto, la solución cuenta con actualizaciones de software, haciendo que sea fácilmente expansible y flexible. Las nuevas funciones, inclusive la documentación, pueden

obtenerse tan solo unos minutos después de estar disponibles, y puede distribuirse automáticamente a todo dispositivo del sistema y a cada usuario. Si las necesidades del negocio requieren de capacidades adicionales, éstas pueden añadirse con simples licencias de software.

1.2 OBJETIVO

El principal objetivo del proyecto es el Diseño e implementación de una red segura y convergente en la Universidad Cotopaxi, basado en tecnología 3Com.

1.3 OBJETIVOS ESPECÍFICOS

- Realizar un estudio del dimensionamiento de la red y establecer un direccionamiento IP de red adecuado.
- Planificar y determinar según las necesidades del cliente, la configuración mas adecuada para cada uno de los equipos adquiridos por la universidad.
- Identificar las características y ventajas de utilizar una red de telefonía sobre protocolo IP para la Universidad Cotopaxi.
- Analizar los protocolos que se utilizaran para lograr una red segura convergente sobre la Universidad Cotopaxi.
- Establecer e implementar los mecanismos de seguridad de la red de datos para la Universidad Cotopaxi.
- Programar el sistema de seguridad basado en el IPS X505 TippingPoint de 3Com.
- Realizar pruebas de calidad de servicio (QoS), interconectividad, operabilidad de la red de telefonía IP y seguridad.

1.4 ALCANCE DEL PROYECTO

En la red de la Universidad Cotopaxi resolveremos sus problemas de colisiones a través de VLANS y un direccionamiento adecuado de la red, que permitirá reducir el riesgo de downtime de servicios a través de alta disponibilidad, desarrollando un sistema adecuado de telefonía IP y protegiendo a la red con un adecuado sistema de prevención de intrusos. La ejecución de este proyecto permitirá realizar tanto el diseño como la implementación de todos los componentes que se requieren para obtener la

red segura tejiendo a la red con un adecuado sistema de prevención y convergente en esta Universidad, convirtiéndola en la pionera en poseer estos tipos de servicios en la provincia del Cotopaxi.

1.5 ANTECEDENTES

La red de datos de la Universidad Cotopaxi ha crecido de manera no planificada, esto ha provocado un aumento del dominio de *broadcast* y colisiones de la red teniendo como consecuencia la reducción en la velocidad de transmisión de datos.

Adicionalmente, debido a la construcción de una nueva infraestructura en la Universidad Cotopaxi, se requiere aumentar el número de usuarios telefónicos; sin embargo la central telefónica no permite este tipo de crecimiento por lo que se requiere implementar un sistema convergente de telefonía IP.

Esta red utilizará un equipo, que busca disminuir la brecha de ataques con respecto a nuevas vulnerabilidades emergentes. Los ataques al día de hoy se dan dentro de los puertos que no puede proteger el *firewall* como lo es el puerto 80, 25, 443; para lo cual requerimos un Sistema de Prevención de Intrusos (IPS) que proteja tanto aplicaciones, infraestructura y rendimiento de la red.

Se desea implementar una red configurable de forma fácil, con servicios convergentes como telefonía IP, con la capacidad de crecimiento en aplicaciones de movilidad, videoconferencia, presencia , *contact center* , y a la vez tener seguridad en todas estas aplicaciones.

1.6 TELEFONÍA ANALÓGICA

Los productos de PBX (*Private Branch Exchange*) tradicionales requieren que los clientes paguen dinero extra por una capacidad que tal vez nunca necesiten o por capacidades que sólo están disponibles en las plataformas más grandes. La solución ofrecida es una plataforma donde se paga a la medida que crece la red, que es económica para veinte usuarios y lo suficientemente poderosa para más de mil usuarios por localidad (3Com, 2006).

Muchas organizaciones enfrentan el desafío de tener que comunicarse entre personal y recursos que se encuentran distribuidos en varias localidades. Estos requerimientos pueden ser tan básicos como conexiones de oficinas al otro lado de la

calle, o tan sofisticados como enlazar múltiples campos en todo el mundo. Se ofrece un conjunto de soluciones económico y escalable para conectar a dos o dos mil localizaciones ininterrumpidamente.

Las soluciones de telefonía sobre redes permiten que las empresas reduzcan dramáticamente los cargos telefónicos de larga distancia dentro de la compañía, al tiempo que mejoran el servicio al cliente. Al aprovecharse de una red de datos que hoy en día sólo funciona para enviar email y archivos, los usuarios pueden hacer llamadas de una localidad a otra, transferir llamadas a otro lugar y enviar mensajes de voz a uno o más usuarios en múltiples oficinas. Estas capacidades ofrecen comunicaciones y servicios al cliente que son más rápidos, más fáciles y más eficientes.

Una arquitectura P.B.X. antigua podría incluir los siguientes componentes:

- P.B.X.
- Mensajería adjunta
- Funcionamiento Digital reservado
- Estación de dirección reservada o software reservado para los cambios de configuración

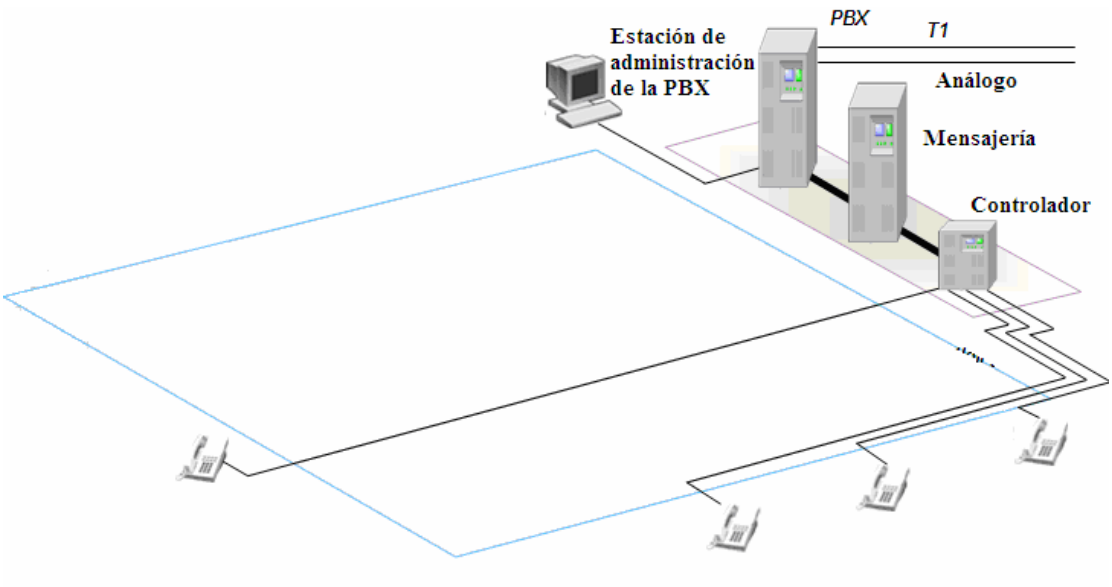


Figura 1.1. Arquitectura de los sistemas PBX tradicionales

Una red de datos consta de lo siguientes componentes:

LAN

- *Switchs*
- Puntos de acceso inalámbricos
- Computadoras personales
- Servidores
- Dispositivos de almacenamiento de la red
- Software de administración de la red

WAN

- Enrutadores

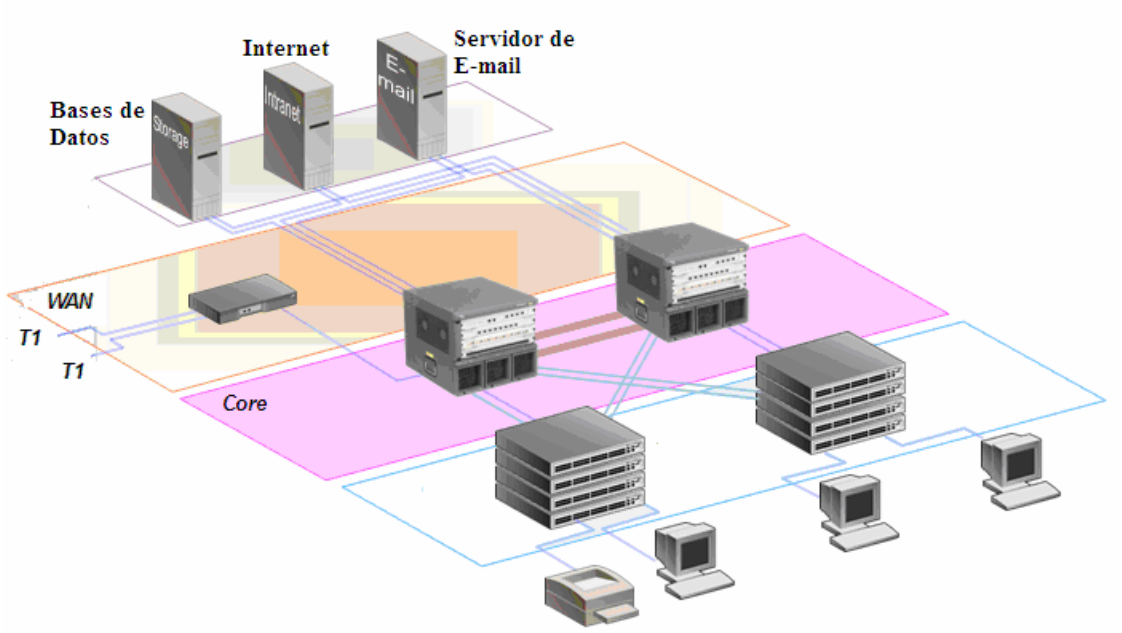


Figura 1.2. Componentes de una red LAN y WAN.

La figura 3 indica, cada área de trabajo tiene dos cables, uno para el teléfono y uno para la computadora personal.

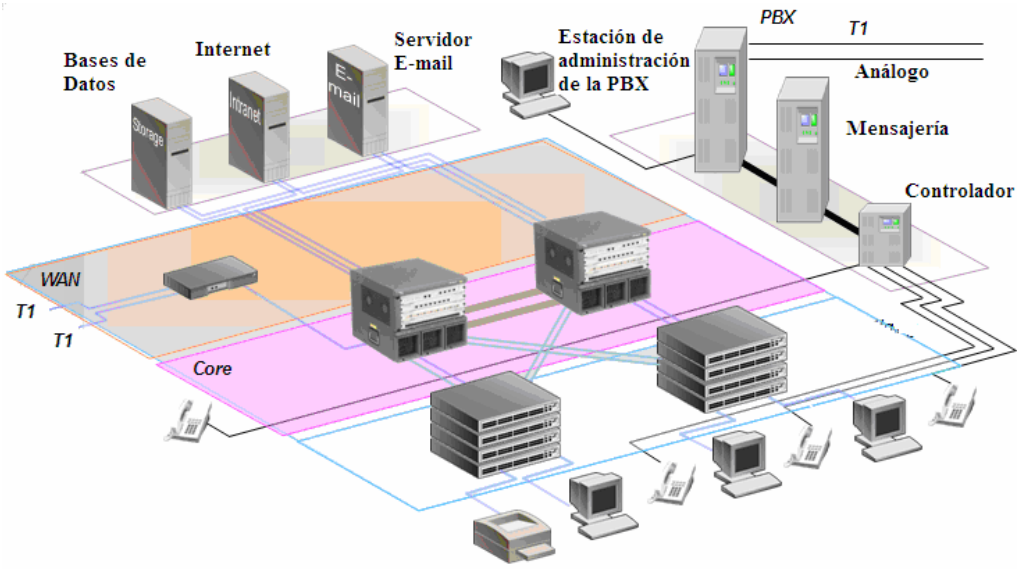


Figura 1.3. Red con dos cableados tanto para la telefonía como para la red de datos.

Hoy, la convergencia junta tanto teléfono y los sistemas de datos en una plataforma común usando una P.B.X. IP sobre la red de datos. En pocas palabras, el sistema de teléfono usa la misma infraestructura cableada como la red de datos, por lo tanto, permite que las llamadas telefónicas sean transmitidas sobre el mismo cable que solía transmitir datos.

Convergir los dos sistemas trae el valor adicional al cliente por no solamente reducir el cableado y gastos de mano de obra, pero un sistema de P.B.X. fácil de usar puede presentar nuevas características y funciones para mejorar la productividad.

En el ambiente competitivo de hoy, la productividad es a menudo la llave para diferenciar una empresa próspera.

El catalizador para la convergencia es la P.B.X. IP.

Una arquitectura de P.B.X. de IP podría incluir los siguientes componentes:

- Servidor de IP
- Servidor de Mensajería IP
- Servidor de conferencia IP

- IP Gateways
- Teléfonos IP
- Manejo de la interfaz integrada a través de un examinador web

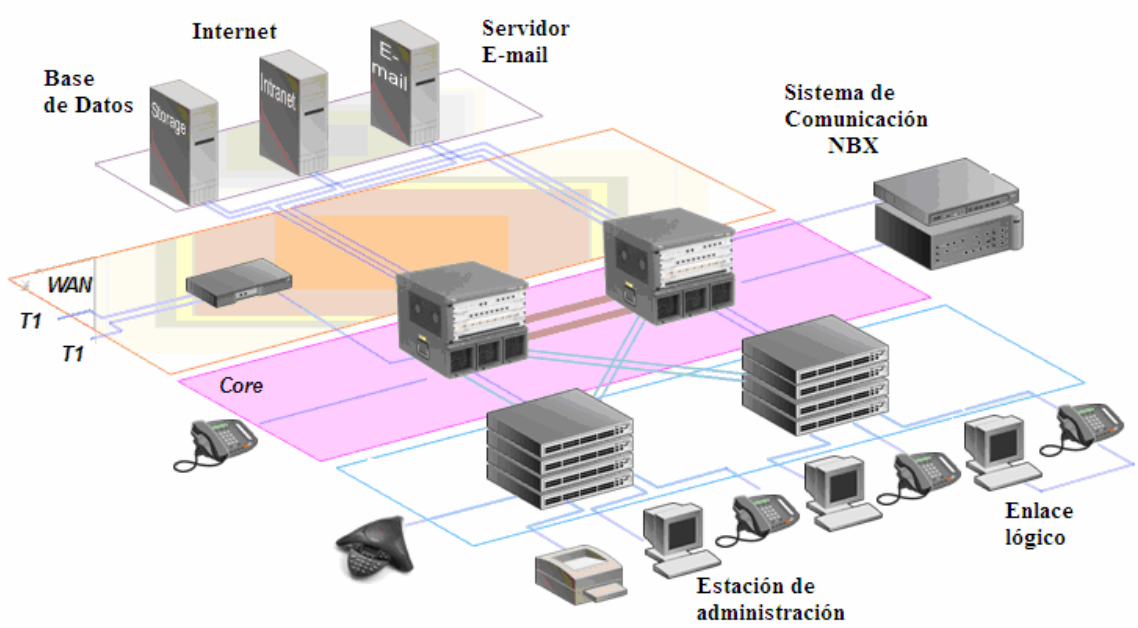


Figura 1.4. Muestra una red convergente, integrando telefonía y red de datos bajo una misma infraestructura.

Las Comunicaciones Unificadas llevan la convergencia más allá de la telefonía IP, integrando presencia, mensajería instantánea, mensajería unificada, conferencia WEB y videoconferencia, entre otras capacidades, en una plataforma común accesible desde cualquier medio. Sus ventajas, por tanto, son evidentes no sólo en cuanto al incremento de la productividad y la agilización de la toma de decisiones.

Es necesario optimizar las inversiones iniciales en la actualización de la infraestructura IP para aprovechar la nueva red a lo máximo, corriendo sobre ella nuevas aplicaciones, como audioconferencia, videoconferencia, y videoconferencia Web, presencia, mensajería instantánea (IM), integración de centro de contactos.
La inmensa mayoría de las organizaciones, gracias a Internet, han evolucionado hacia entornos extendidos y globales que conectan socios, clientes y proveedores.

En Estados Unidos, de acuerdo con las conclusiones de un reciente estudio de Nemertes Research, el 90% de los empleados trabaja fuera de las sedes centrales, una tendencia que en los últimos 5 años ha crecido un 800%, en el 2009 el número de empleados móviles en Europa representará un tercio del total de los trabajadores. Y en estos nuevos tipos de entornos laborales y de negocio, la comunicación y la colaboración en tiempo al que ofrecen las plataformas de Comunicaciones Unificadas adquieran su máximo sentido.

1.6.1 Tecnología Analógica

Entre una casa y la oficina de la compañía telefónica están pares de cables conectados con su teléfono que llevan una señal de análoga. Se escuchará el teléfono a menudo en su casa referido como un teléfono análogo.
Una señal análoga es una señal fluctuando continuamente.

En una señal análoga la frecuencia de vibraciones eléctricas por segundo (ciclos) es conocida como Hertz. Hertz es abreviado como Hz. Un hertz es igual a un ciclo por segundo.

1.6.2 Teléfonos

Los teléfonos son dispositivos sumamente simples. El principio básico para un teléfono no ha cambiado en más de 100 años. Los teléfonos tienen tres partes principales:

- Micrófono para la conversación
- Speaker para escuchar
- Hook Switch que conecta y desconecta al teléfono de la red

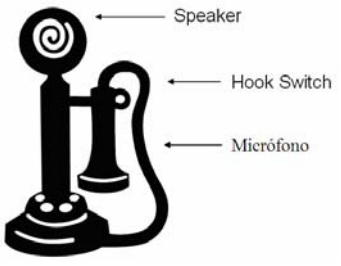


Figura 1.5. Muestra los componentes principales de un teléfono análogo.

Teléfonos modernos

Los teléfonos de hoy todavía tienen tres partes principales, pero componentes adicionales han sido añadidos:

- Duplex coil con el propósito de que no se escuche su propia voz.
- La campana o dispositivo de sonido con el propósito de conocer que se tiene una llamada entrante.
- Teclado de tacto - para marcar los números
- Generador de frecuencia para generar los tonos identificables para el equipo de proveedores.

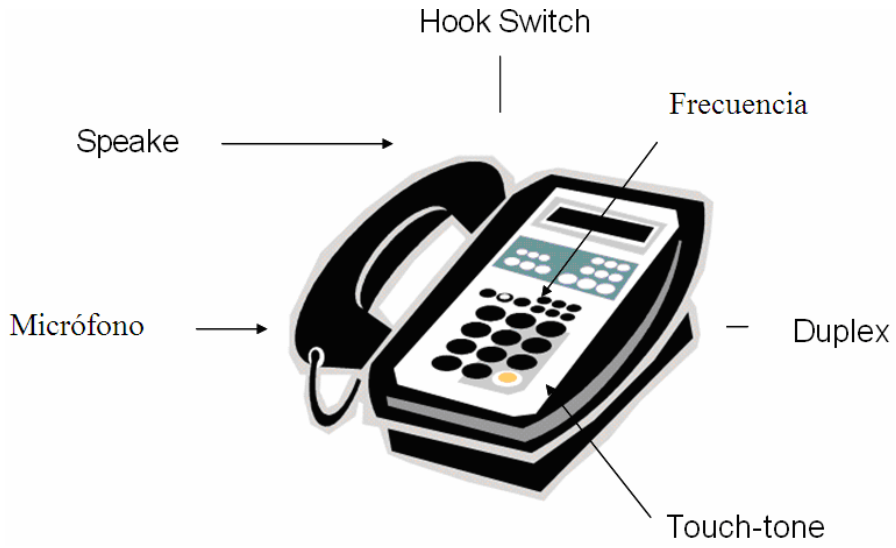


Figura 1.6. Componentes de los teléfonos modernos.

Teléfono analógico a operación digital

Un teléfono IP convierte ondas de sonido en señales eléctricas analógicas. Un procesador de señales digitales convierte el sonido análogo en datos digitales. Los datos son una trama de *Ethernet* y pueden ser encapsulados en IP, como se lo muestra en la figura 1.7.

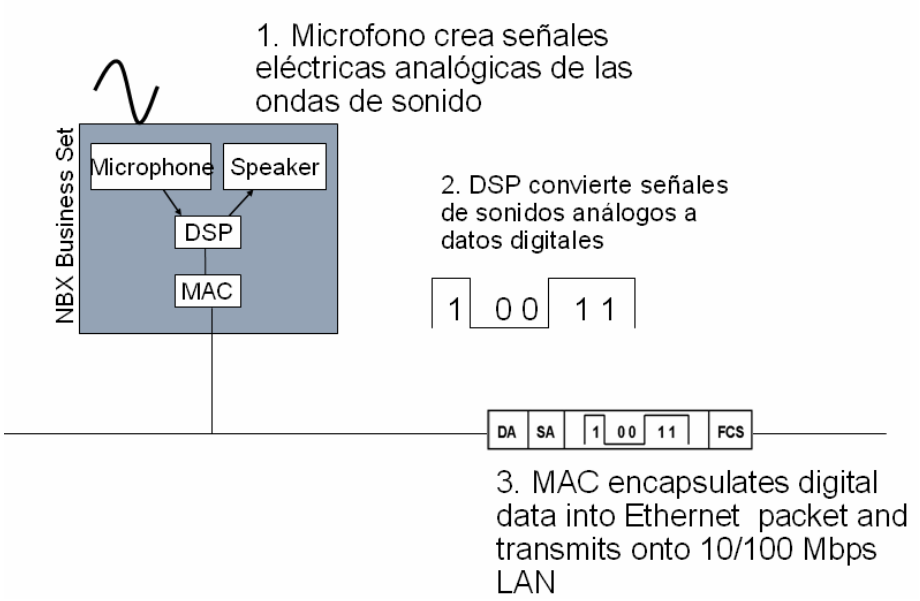


Figura 1.7. Proceso de funcionamiento de un teléfono IP.

1.6.3 Red Telefónica

La compañía telefónica aplica el voltaje a la línea. Esto es lo que lleva su voz. En Ecuador es 48VDC (voltios de corriente directa). Otros países podrían usar algo diferente. Como un ejemplo, Reino Unido usa 50VDC. Las otras áreas del mundo pueden usar hasta 150VDC.

Volts son una medida de la fuerza o presión. La corriente continua es una corriente eléctrica que viaja en una dirección.

La compañía telefónica hace su teléfono sonar enviando una forma de onda de CA. En los Estados Unidos, la frecuencia común es 20HZ. Otras partes del uso de mundo entre 20 y 40HZ. La CA o la corriente alterna es como la electricidad que viene de la central hidroeléctrica a su casa. Su dirección es invertida 60 veces por segundo en Ecuador y 50 veces por segundo en Europa.
Cuando toma su teléfono "Off-hook" el voltaje de línea baja de 48VDC a algún valor entre 3 y 9 voltios.

En Ecuador, dos cables de teléfono conectan su teléfono a la red telefónica. Estos cables son en general rojos y verdes. El cable verde es positivo y el cable rojo es negativo. El cable verde es llamado Tip y el cable rojo es llamado ring. Esto es la

terminología que se remontaba a las unidades terminales de centrales manuales que exigieron que un ser humano conecte cables para completar una llamada.

Aunque la compañía telefónica está proporcionando el poder a su equipo, su equipo no debe manejar más que 5 microamperios mientras el teléfono esta "On-hook". En el pasado, esto era lo suficientemente para almacenar en la memoria el último número marcado en la memoria de un teléfono. Hoy, la mayoría de los teléfonos tienen su propia batería interna para la memoria y brindan características más avanzadas.

Un amperio es una medición de la corriente eléctrica en un circuito. Es el número de electrones que pasan durante un período dado.

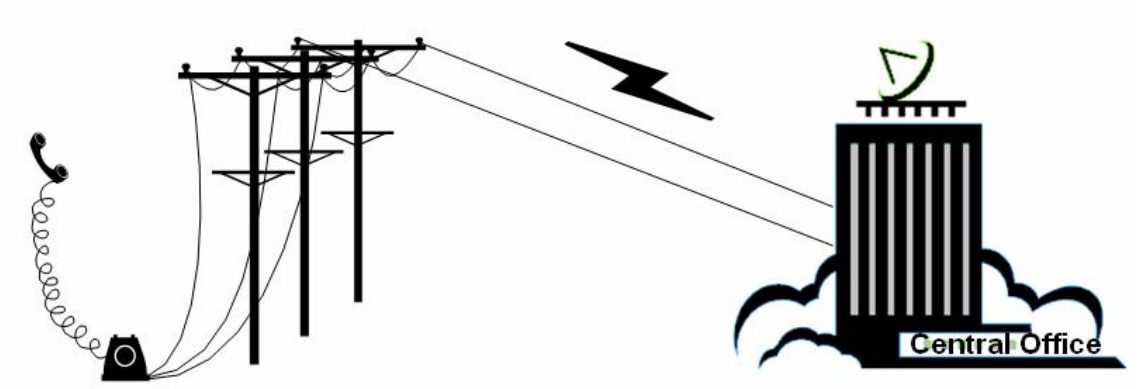


Figura 1.8. Muestra como un teléfono se conecta con la Oficina Central.

1.6.4 Cableado y Conectores

El puerto de conexión usual para el equipo de un cliente conectado a un circuito analógico es en general una conexión de RJ11. La jack de la pared tendrá un puerto RJ11 hembra, el dispositivo del cliente tendrá un puerto RJ11 macho, y unos 2 cables o 4 cables (straight through) con terminales machos. Los dos cables son generalmente usados para Tip y Ring (cables verdes y rojos) en general.

Conectores RJ12 machos sobre cables se han puesto en moda hoy. Un conector RJ12 macho se acomoda en un puerto RJ11 hembra cuando son del mismo tamaño físico.

En los últimos años, el cable UTP (Unshielded Twisted Pair) con 4 pares (8 cables) se ha llegado a ser muy común en la construcción de edificios. Éste es el resultado del desarrollo rápido con teléfonos digitales y redes Ethernet. Las conexiones de RJ45 son relacionadas con el Ethernet y algunos sistemas de teléfono digitales en general.

Un RJ11 conector macho cabrá en un puerto RJ45 hembra. Ethernet usa los pines 1,2,3, y 6 lo que deja a los cables de en medio pin 4 y 5 y los pines exteriores que son el 7 y 8 disponible para un uso alternativo. Pin 4 y 5 es usados para teléfonos a menudo como los pines del centro de un RJ11 / RJ12 alineación de conector macho precisamente con los conectores en un puerto de RJ45 hembra.

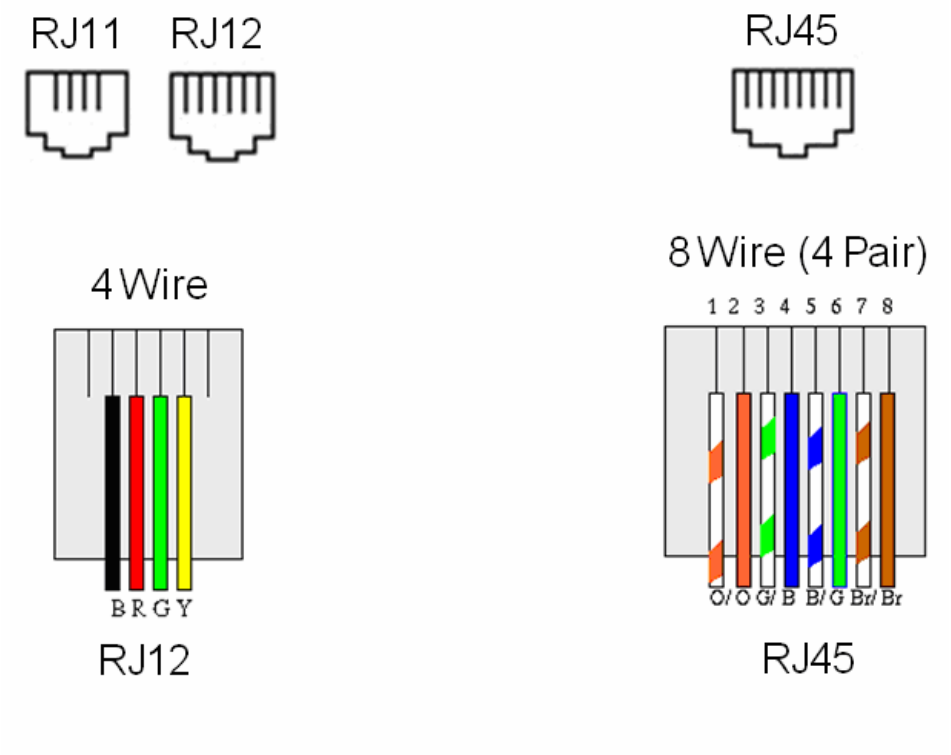


Figura 1.9. Conectores RJ11, RJ12 y RJ45.

La conexión de un teléfono a la red telefónica (oficina central) es generalmente aproximadamente de tres millas de longitud y está hecho de 22 pares trenzado de AWG. Esto es llamado el bucle local (local loop). El cableado de su casa u oficina es en general 4 cables, pero podría ser también un grupo de cables. La oficina central está donde la compañía telefónica mantiene su equipo de conmutación computarizado.

En Ecuador, 4 alambres de cable consisten en verdes, rojos, amarillos y negros. El verde y el rojo son generalmente los cables primarios usados. Amarillo y negro serían usados si usted tuviera una segunda línea de teléfono (como un ejemplo). En otras partes del mundo los colores usados son diferentes.

El cableado externo de un edificio puede ser subterráneo o aéreo. Cableado personal de casa o empresas podrían converger juntos en un grueso grupo de cables, en general 25 a 50 pares por cable, en una caja centralmente ubicada. La caja es referida como una caja de intercambio. Ese grupo seguirá a menudo a una caja más grande donde los grupos múltiples se combinan y se terminará posteriormente en la oficina central.

Hoy es común, las cajas de intercambio donde los grupos de cable múltiples convergen, tendrán un digitalizador. Esto toma los pares de cables y digitaliza todas las líneas con el propósito de que la voz puede ser llevada sobre juegos mucho más pequeños de cables (T1, E1, fibra).

En lugar de operadores que conectan líneas manualmente, hoy hay conmutadores controlados por computadora. Estos conmutadores controlados por computadora reconocen dos tipos de marcados; tonos y pulsos.

El pulso fue la tecnología original usada con conmutadores electro - mecánicos, en la actualidad usamos tonos. Esto es comúnmente referido a multi- frecuencia o Dual Tone Multi-Frequency (DTMF). En Europa es llamado multi- frecuencia (MF). La computadora intercambia reconociendo los diferentes tonos que fueron introducidos y hacen una conexión apropiada.

La red telefónica es conocida como Red Telefónica Conmutada Pública, Public Switched Telephone Network (PSTN), como se muestra en la figura 10.

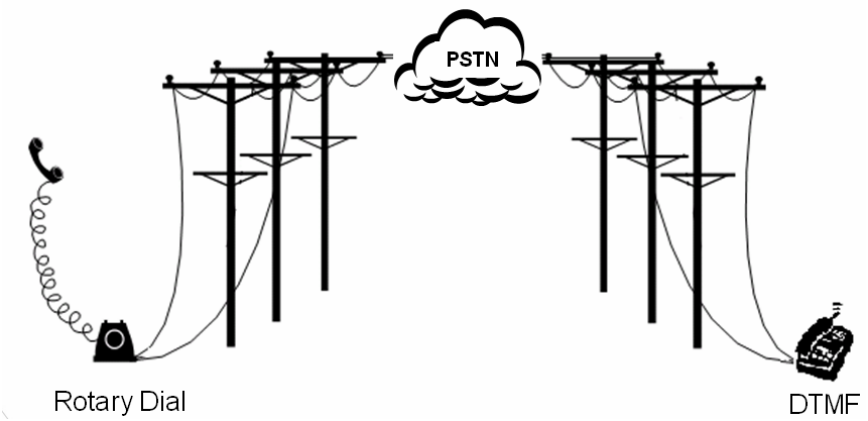


Figura 1.10. Red PSTN.

El sonido de tono de marcación que se escucha cuando se recoge el teléfono es una combinación de 350 Hz de tonos y 440 Hz de tonos generados por el conmutador controlado por computadora para dejarlo saber que esta listo para hacer una llamada. Cuando usted marca un número sobre el teclado de tacto, los tonos son combinado en el cual el conmutador controlado por computadora reconoce cual es el número.

	1209Hz	1336 Hz	1477 Hz
697Hz	1	2	3
770 Hz	4	5	6
852 Hz	7	8	9
941 Hz	*	0	#

Figura 1.11. Combinación de frecuencias de los tonos de marcación.

Cuando se habla, la red telefónica transmite las frecuencias de su voz entre 400 hertz y 3400 hertz. Cualquier sonido de arriba o debajo de estas frecuencias son extraídos y no llevados. Esto es hecho para admitir más llamados de larga distancia a ser transmitidas.

1.7 TECNOLOGÍA DIGITAL

Una señal análoga es una señal fluctuando continuamente. Una señal digital es una representación discreta de la señal. La señal análoga representa la circulación ininterrumpida de la información completamente, pero es propenso a la interferencia y es difícil repetir de un dispositivo a otro sin la pérdida o la introducción del ruido. La señal digital por otro lado no es tan propensa a la interferencia o al ruido y es mucho más fácil repetir de un dispositivo a otro. La señal digital puede suministrar una capacidad mucho más grande para la entrega de la información.

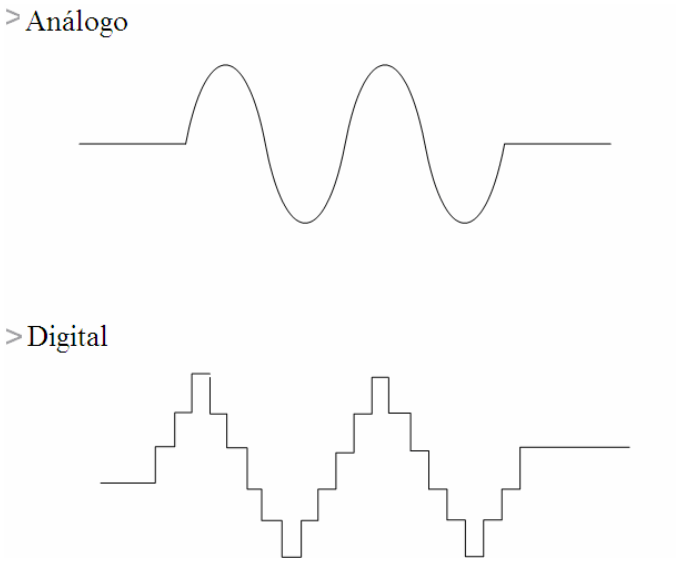


Figura 1.12. Señal Análoga y una señal Digital.

1.7.1 Red Telefónica Digital

Aunque los equipos de más uso para el cliente en la casa es el análogo, la red telefónica se ha puesto digital de la agregación de puntos de regreso a la oficina central y de oficina central a oficina central. Casi todo el tráfico de voz en la red telefónica hoy es digital. Esto permite que los varios proveedores complazcan un número más grande de comunicaciones al otro lado de la red telefónica y previene la degradación habitual en las señales analógicas.

En el caso de negocios, cuidan escoger líneas digitales directamente a sus instalaciones, como T1, E1s o ISDN. Estas líneas no sólo brindan la capacidad más grande sino también reducir gastos a la empresa.

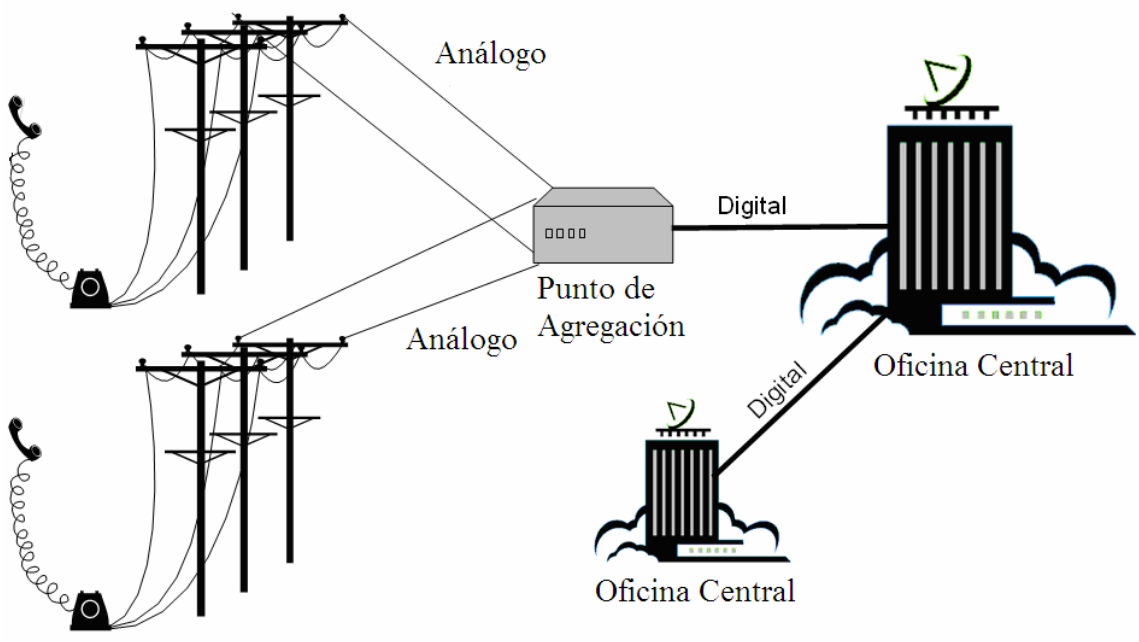


Figura 1.13. Conexiones análogas y digitales hacia la oficina digital.

T1

Un T1 es un circuito dedicado de la compañía telefónica en sus instalaciones. El T1 suministra 24 canales de voz digitalizados o un flujo de datos 1.544 Mbps. Podría constar de fibra o cobre de la oficina central a usted, pero el punto de demarcación en su edificio es en general de cobre.

El uso de T1 de cobre de dos pares (cuatro cables), 1 par para transmitir y 1 par para recibir.

En general, cuando un T1 lleva la voz se conecta a un sistema telefónico y cuando un T1 lleva los datos, se conecta a un router de la red.

Cada uno de los 24 canales de un T1 son de 64kbps y son referidos como un DS0. Los canales son creados usando frecuencias diferentes y usando multiplexión por división de tiempo con la información de tiempo siendo embebida para la transmisión de datos.

Debido a que no todos necesitan los 1.544 megabits de throughput que brinda el T1 los 24 canales de voz distintos, los proveedores permiten que el T1 sea comprado en incrementos de canal. Cualquier subdivisión de las 24 vías es llamada T1 fraccional.

Cuando se configura un T1, hay que consultar con el proveedor para los métodos de codificación y técnicas de entramado que serán configuradas en el equipo.

Se necesitará configurar la codificación y los métodos de entramado para las tarjetas de línea Digital de la NBX apropiadamente. Hay varios métodos de codificación diferentes usados sobre un T1:

- Inversión de Mark alterno (AMI)
- Bipolar con la sustitución de 8 bit (B8ZS)

Hay diferentes técnicas de entramado para un T1:

- D4 super trama
- Extended Superframe Framing (ESF)

La señal de *loopback* permite que un técnico ordene que el equipo remoto haga un lazo si este recibe una señal de regreso sobre el camino transmitido. Esto permite que el técnico inserte el equipo de prueba para *troubleshooting*. Se puede crear su propio loopback conectando los pines 1 a 4 y 2 a 5 sobre un plug RJ48.

E1

Un E1 es similar a un T1 excepto que ofrece 32 canales de 64 Kbps. Tiene un *throughput* de 2 mbps. Dos canales son reservados para señalización y control de la información que deja 30 canales para traer la voz o los datos. Esto es diferente de un T1, que lleva su señalización y control dentro del flujo de datos.

Cualquier subdivisión de los 30 canales es llamado un E1 fraccional.

Se debe consultar con el proveedor los métodos de codificación y técnicas de entramado para poder trabajar con la central telefónica.

El método de codificación dominante usado sobre E1 lo es:

- High-density bipolar-3 zeros

Existen diferentes técnicas de entramado de E1s:

- Double Frame
- Multi Frame

La Tabla 1.1 muestra las velocidades, servicios y nombres comunes par las líneas digitales E1y T1, utilizadas en diferentes continentes.

NORTE AMERICA			
Servicio	**Canales de Voz**	**Velocidad**	**Nombre Común**
DS0	1	64 Kbps	DSO
DS1	24	1.544 Mbps	T1
DS1C	48	3.152 Mbps	T1C
DS2	96	6.312 Mbps	T2
DS3	672	44.736 Mbps	T3
DS4	4032	274.176 Mbps	T4
EUROPA			
Servicio	**Canales de Voz**	**Velocidad**	**Nombre Común**
E1	30	2.048 Mbps	E1
E2	120	8.448 Mbps	E2
E3	480	34.368 Mbps	E3
E4	1920	139.264 Mbps	E4
E5	7680	565.148 Mbps	E5

1.8 CARACTERÍSTICAS DEL PROTOCOLO IP

El Protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico. IP es un protocolo de entrega no orientado a la conexión, poco confiable y de máximo esfuerzo. El término no orientado a la conexión significa que no se establece ningún circuito de conexión dedicado antes de la transmisión, como sí lo hay cuando se establece una comunicación telefónica. IP determina la ruta más eficiente para los datos basándose en el protocolo de enrutamiento. Los términos poco confiables y de máximo esfuerzo no implican que el sistema no sea confiable y que no funcione bien; más bien significan que IP no verifica que los datos lleguen a su destino. La verificación de la entrega no siempre se lleva a cabo.

A medida que la información fluye hacia abajo por las capas del modelo OSI, los datos se procesan en cada capa. En la capa de red, los datos se encapsulan en paquetes, también denominados datagramas. IP determina los contenidos de cada encabezado de paquete IP, lo cual incluye el direccionamiento y otra información de control, pero no se preocupa por la información en sí. IP acepta todos los datos que recibe de las capas superiores.

Existen dos tipos de servicios de envío: los no orientados a conexión y los orientados a conexión. Estos dos servicios son los que realmente permiten el envío de datos de extremo a extremo en una internetwork.

La mayoría de los servicios utilizan sistemas de entrega no orientados a conexión. Es posible que los diferentes paquetes tomen distintas rutas para transitar por la red, pero se reensamblan al llegar a su destino. En un sistema no orientado a conexión, no se comunica con el destino antes de enviar un paquete. Una buena comparación para un sistema no orientado a conexión es el sistema postal. No se comunica con el destinatario para ver si aceptará la carta antes de enviarla. Además, el remitente nunca sabe si la carta llegó a su destino.

En los sistemas orientados a conexión, se establece una conexión entre el remitente y el destinatario antes de que se transfieran los datos. Un ejemplo de redes orientadas a conexión es el sistema telefónico. Se realiza una llamada, se establece una conexión y luego se produce la comunicación.

Los procesos de red orientados a conexión se refieren comúnmente a procesos de conmutación de paquetes. Ya que los paquetes pasan de un origen a un destino, éstos pueden conmutar en diferentes rutas, y posiblemente lleguen en un orden diferente al que fueron enviados. Cada paquete contiene instrucciones, tales como direcciones y orden secuencial del mensaje, el cual coordina la llegada del mismo. Los dispositivos toman la determinación de la mejor ruta basados en diferentes criterios. Algunos parámetros son el ancho de banda disponible, el cual difiere de un paquete a otro.
Los procesos no orientados a conexión se refieren a procesos de conmutación de circuitos. Una conexión con el destino se establece antes de enviar información. Todos los paquetes deben viajar de manera secuencial a través del mismo circuito físico o virtual en una corriente continua.

La Internet es una red gigante no orientada a conexión en la cual la mayoría de la entrega de los paquetes la lleva a cabo IP. TCP añade la confiabilidad de la Capa 4 a servicios no orientados a conexión de comunicación con IP.

Los paquetes IP constan de los datos de las capas superiores más el encabezado IP. El encabezado IP está formado por lo siguiente:

Versión: Especifica el formato del encabezado de IP. Este campo de cuatro bits contiene el número 4 si el encabezado es IPv4 o el número 6 si el encabezado es IPV6. Sin embargo este campo no se usa para distinguir entre ambas versiones, para esto se usa el campo de tipo que se encuentra en el encabezado de la trama de capa 2.
Longitud del encabezado IP (HLEN): Indica la longitud del encabezado del datagrama en palabras de 32 bits. Este número representa la longitud total de toda la información del encabezado, e incluye los dos campos de encabezados de longitud variable.

Tipo de servicio (TOS): Especifica el nivel de importancia que le ha sido asignado por un protocolo de capa superior en particular, 8 bits.

Longitud total: Especifica la longitud total de todo el paquete en bytes, incluyendo los datos y el encabezado, 16 bits. Para calcular la longitud de la carga de datos reste HLEN a la longitud total.

Identificación: Contiene un número entero que identifica el datagrama actual, 16 bits. Este es el número de secuencia.

Señaladores: Un campo de tres bits en el que los dos bits de menor peso controlan la fragmentación. Un bit especifica si el paquete puede fragmentarse, y el otro especifica si el paquete es el último fragmento en una serie de paquetes fragmentados.

Desplazamiento de fragmentos: usado para ensamblar los fragmentos de datagramas, 13 bits. Este campo permite que el campo anterior termine en un límite de 16 bits.

Tiempo de existencia (TTL): campo que especifica el número de saltos que un paquete puede recorrer. Este número disminuye por uno cuando el paquete pasa por un Router. Cuando el contador llega a cero el paquete se elimina. Esto evita que los paquetes entren en un loop (bucle) interminable.

Protocolo: indica cuál es el protocolo de capa superior, por ejemplo, TCP o UDP, que recibe el paquete entrante luego de que se ha completado el procesamiento IP, ocho bits.

Checksum del encabezado: ayuda a garantizar la integridad del encabezado IP, 16 bits.

Dirección de origen: especifica la dirección IP del nodo emisor, 32 bits.

Dirección de destino: especifica la dirección IP del nodo receptor, 32 bits.

Opciones: permite que IP admita varias opciones, como seguridad, longitud variable.

Relleno: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits

Datos: contiene información de capa superior, longitud variable hasta un de máximo 64 Kb.

Aunque las direcciones de origen y destino IP son importantes, los otros campos del encabezado han hecho que IP sea muy flexible. Los campos del encabezado contienen las direcciones origen y destino del paquete y generalmente incluyen la longitud del mensaje. La información para enrutar el mensaje también está incluida en el encabezado de IP, el cual puede ser largo y complejo, como se lo muestra en la figura 1.14.

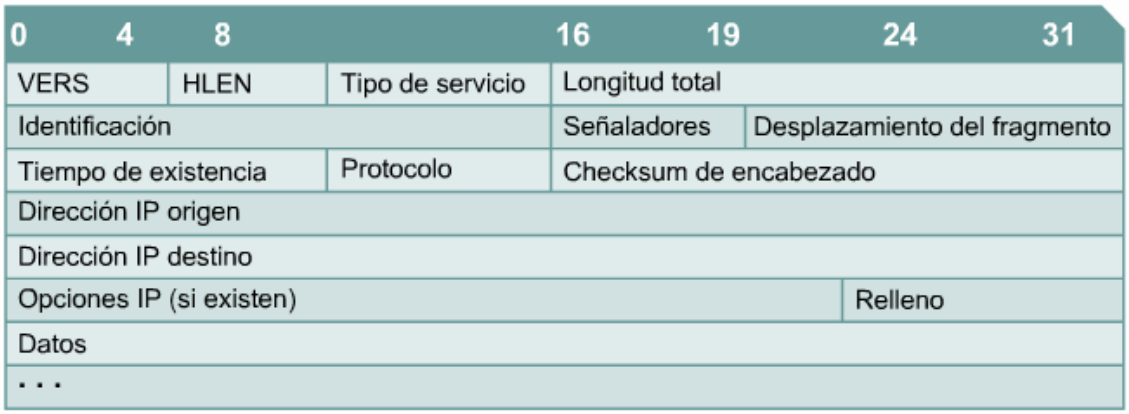


Figura 1.14. Componentes del encabezado IP.

1.9 VENTAJAS DE MIGRAR A TELEFONÍA IP

Dentro del desarrollo del mercado total de telefonía, la tecnología que tiene las mayores posibilidades de crecimiento es IP-Puro. Según las cifras de Gartner Group del 2004, la venta de líneas tradicionales (TDM) tenderá a cero en los próximos cinco años, la venta de líneas híbridas, aunque está pasando por un buen momento en la actualidad tenderá a decrecer ya que las líneas híbridas son simplemente un medio de llegar a la telefonía IP-Pura. Por último, la Telefonía IP pura es la única que se proyecta con crecimiento constante hacia el futuro y es la tecnología que va a tener la mayoría sino la totalidad de los puertos en 4 a 8 años (ComputerWorld, 2007).

Es interesante anotar que el "boom" de tecnología híbrida le está permitiendo a los jugadores de telefonía tradicional lograr ingresos adicionales a los percibidos si el enfoque fuera en telefonía IP híbrida. El costo total de propiedad, CTP, de un sistema de telefonía que cambia a híbrido y finalmente a IP puro es más alto que el CTP de un sistema que cambia a IP Puro sin pasar por el proceso de habilitarlo a IP a través de una tarjeta.

La principal razón que lleva a las empresas a migrar de sus soluciones de voz tradicionales a Telefonía IP, es el ahorro en costos (48% de los entrevistados), en la medida en que las empresas de todos los tamaños de la región tienen una presión fuerte para reducir sus inversiones en capital en telecomunicaciones y sus gastos operativos. Por esto la convergencia (integración de voz y datos en una misma red) emerge como una solución real para reducir costos y generar aumentos en productividad.

Entre el 37 % de las empresas que planean implementar Telefonía IP, el 46 % planean hacerlo en el 2004, el 28 % en el 2005 y el 4 % en el 2006 o luego. Un 22% de los encuestados no sabe cuándo implementará la solución.

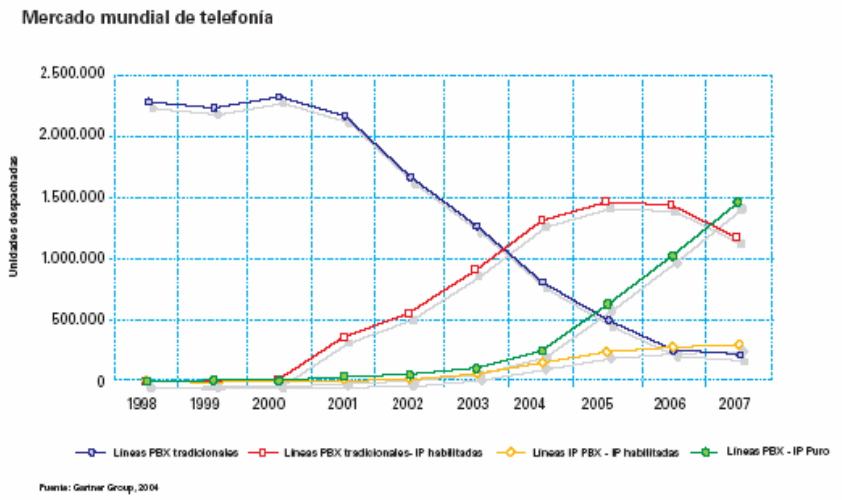


Figura 1.15. Mercado mundial de telefonía, en el cual el crecimiento de telefonía IP, va ha superar a cualquier sistema de telefonía tradicional.

El ambiente económico de hoy ha hecho más crucial para las personas responsables de adoptar decisiones para considerar qué tipo de rentabilidad pueden esperar de inversiones futuras de sus organizaciones. Las empresas que están invirtiendo en las comunicaciones IP tienen dos retornos principales en mente – reducción de costos de operación y mejorar la capacidad de comunicaciones de su organización.

La comunicación IP es una tecnología viable que puede ser implementada hoy convergiendo voz existente y datos conectados en una red basada en IP, una empresa puede bajar su coste total de la propiedad de la red reduciendo los gastos relacionados con equipo y el mantenimiento, la administración de la red, y los cargos por carrier de la red. Una red convergente también aumenta la capacidad de comunicaciones de una organización facilitando al empleado movilidad y suministrando un fundamento sólido para el despliegue de los servicios en estado avanzado, con muchas características y soluciones. Los beneficios de la convergencia son:

- Infraestructura de un solo cableado
- Costos reducidos
- Incremento de la productividad
- Mantenimiento reducido
- Manejo basado en WEB de forma integrada
- Movimiento de manera sencilla

Incremento de la productividad: con el sistema de comunicación las organizaciones de tamaño pequeñas a medianas pueden incrementar la eficiencia, aumentar la colaboración y mejorar las interacciones con los clientes. Las aplicaciones avanzadas y manejo instintivo, del navegador basada en WEB, pueden optimizar servicios y minimizar la necesidad para personal adicional. La plataforma brinda herramientas incorporadas y aumento de productividad como el correo de voz, la distribución de llamada automática (ACD), integración computador teléfono (CTI) vía clientes TAPI de correo voz / correo electrónico visuales (IMAP4), administración del escritorio, y detalle de llamadas que informa sobre las aplicaciones del (CDR).

Despliegue fácil: el diseño basado en estándares, incluyendo el soporte para el poder sobre Ethernet (Poe) de 802.3af de la IEEE, facilita la integración perfecta con la infraestructura de la red existente y provee la garantía de inversión de la evolución del sistema. Open Applications Protocol Interface (API) arquitectura que provee el acceso para mejorar aplicaciones con equipos terceros.

Escalabilidad práctica: las organizaciones pueden aumentar la capacidad y aumentar aplicaciones vía actualizaciones de software, sin la necesidad de adquisición de equipos físicos costosos. La concesión de licencia incrementa el ahorro de costos suministrando la escalabilidad de hasta 1,500 dispositivos (líneas / estaciones 720 líneas de PSTN máximas) y hasta 48 NBX IP Virtual Tie Lines (VTLs).

La operación reducida de costos: VoIP telefonía entrega una reducción de costos dramáticos para llamadas de larga distancia, plan de marcación multicitios unificado y hop-on/hop-off toll-bypass a través de una red de área amplia (WANs) entregando

inmediatamente ahorros. La opción de intercambio de mensajes multisitio entre equipos y perfiles de voz de terceras empresas Voice Profile for Internet Mail (VPIM)- Complementado con sistemas de mensajería de voz que ofrecen la economía de sistemas ínter operables a organizaciones de multi sitio.

Elecciones de teléfono IP: los teléfonos IP con características robustas dejan a las organizaciones optimizar sus inversiones en la infraestructura de comunicaciones. Las elecciones incluyen el Ethernet / teléfonos IP 10/100/1000 Mbps, los softphones, y las consolas de recepcionistas que soportan SIP o NBX control de llamada y Poe para la flexibilidad de empleo.

1.10 SERVICIOS ADICIONALES

1.10.1 Mejoras Primarias

1 Administración basada en web a través de una interfase intuitiva: Netset
2 Facilidad en la actualización de la versión con licenciamiento de software.
3 Clase de Servicio
4 Buzón de saludos múltiples
5 Auto Attendant
6 Conferencias
7 Zona de Paging
8 Operador Personal
9 Forzar y verificar códigos de cuenta.
10 Grupos HUNT
11 Grupos ACD
12 Notificación exterior
13 Soporta modo hibrido PBX
14 Capacidad de integración computador telefonía
15 Grabación detallada de llamadas
16 Supervisor monitor , Whisper y Barge-in
17 VTL

Clase de Servicio

La clase de servicio (CoS) es una configuración de los permisos de llamada que el administrador atribuye a usuarios a través de un identificador de grupos. Estos permisos están sujetos a los parámetros de Horas de trabajo de la empresa: como horas de actividad, abiertas, almuerzo, y otros. Por ejemplo, usted puede crear una clase que admite las llamadas interurbanas durante las horas de trabajo normales.

Consideraciones adicionales:

Las llamadas de emergencia (como las llamadas para el 911) no están sujetas a las restricciones de CoS. *System-wide Speed* dial no están sujetos a restricciones en la clase de servicio. Por ejemplo, si usted quiere permitir la llamada a un número específico a todos usuarios sin realizar ajustes en su CoS, cree un *Speed dial* para ese número.

Cuando se crea un nuevo perfil, el sistema asigna la CoS por defecto a menos que se especifique uno diferente, como se muestra en la figura 1.16. Si usted edita las propiedades CoS, verifique que contenga un mínimo de los permisos configurados. Se puede permitir o desactivar la notificación exterior en el nivel de sistema. *System -wide* tiene prioridad sobre el ajuste de CoS.

Un usuario puede contar con más CoS en un teléfono usando el *feature* 433. Por ejemplo, un usuario cuyo teléfono de la oficina asignado admite las llamadas para los números externos tiene que hacer una llamada para un número externo de un teléfono que tiene una CoS que no admite las llamadas externas. El usuario entra la clave del feature en el teléfono de habilitación de conferencia, y luego el sistema solicita el nombre de usuario y la contraseña antes de admitir la llamada.

Para configurar un código de cuenta forzado, se debe hacer un clic en *Force Acct Code* .

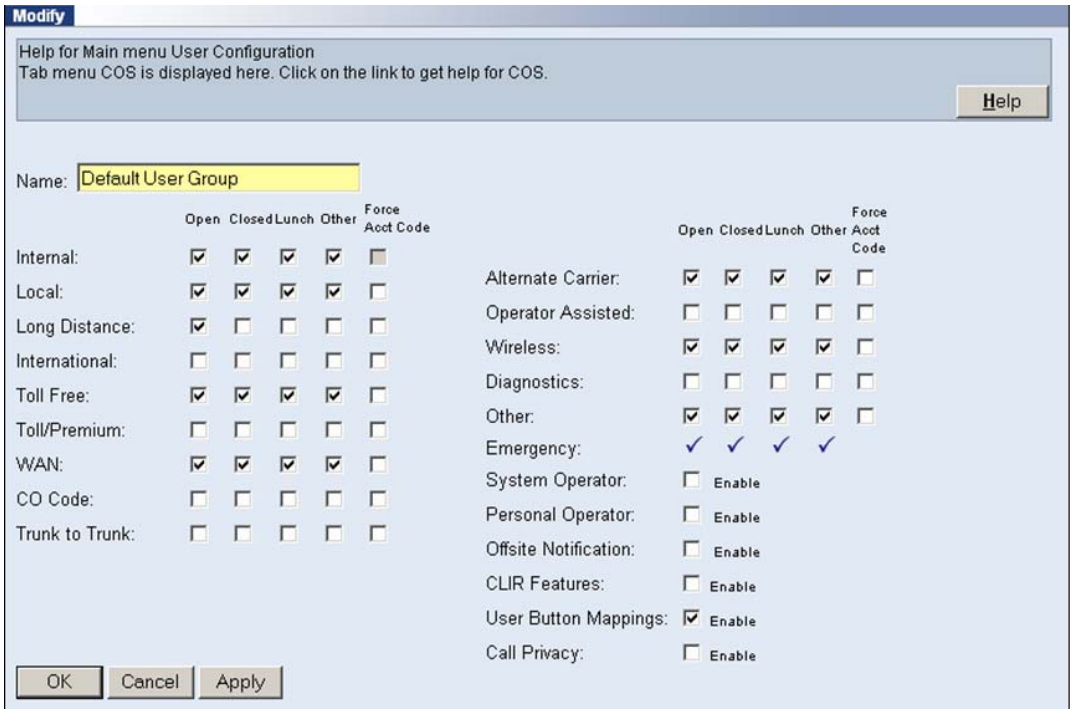


Figura 1.16. Muestra la pantalla para configurar la clase de servicio a los usuarios.

Buzón de saludos múltiples

Los usuarios pueden tener hasta 5 saludos personales grabados. Cada uno puede ser activado a través de NetSet o el acceso de buzón de teléfono. Solamente un saludo personal puede estar activo a la vez, como se lo muestra en la figura 17.

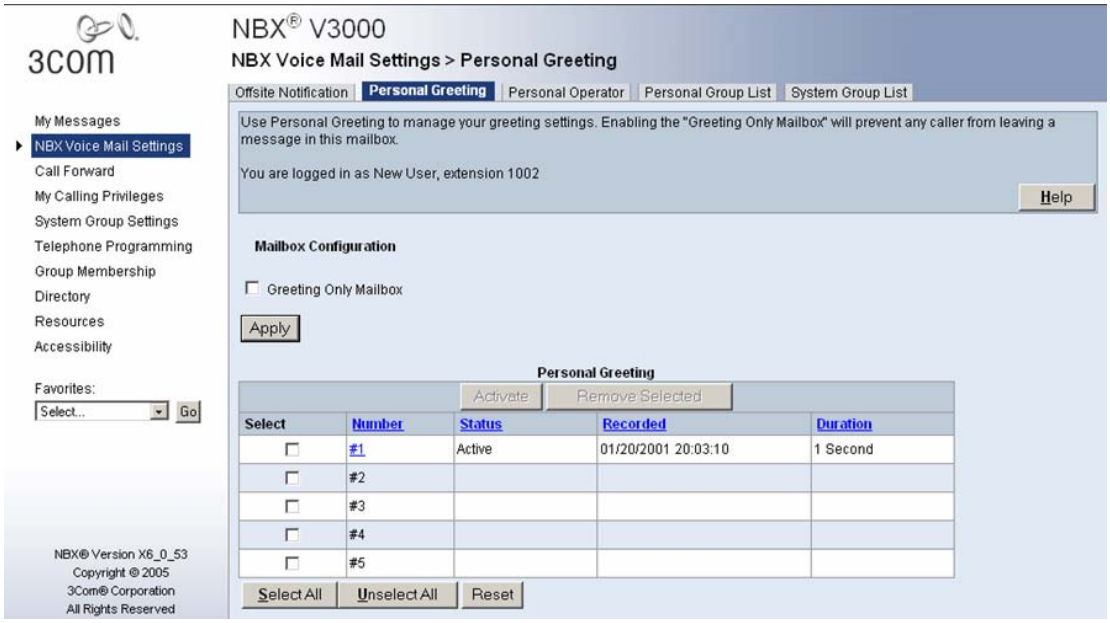


Figura 1.17. Configuración de saludos múltiples para los usuarios.

Operador Personal

Los usuarios pueden enviar sus llamadas a uno de los dos operadores configurable. Los operadores configurables son:

- Operador del Sistema - esto es el operador de sistema usual para su sitio.
- Operador Personal - éste es un destino aparte del operador de sistema por defecto que sería apropiado para una llamada hecha a usted. Por ejemplo, un operador personal podría ser su teléfono celular, o un Hunt group.

Operador de sistema y operador personal son configurados en el registro de entrada de un usuario, como se lo muestra en la figura 1.18.

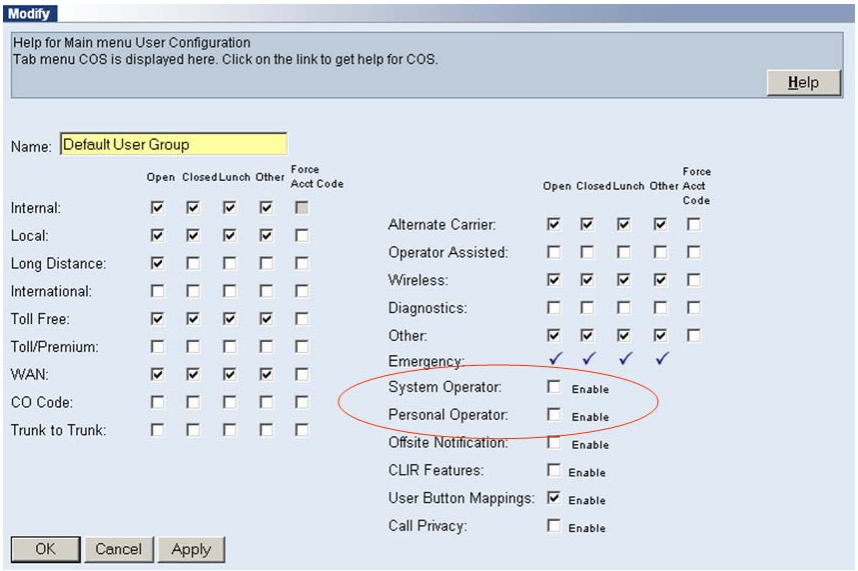


Figura 1.18. Pantalla para habilitar la configuración de operadores personales.

Notificación exterior

La notificación exterior permite que un usuario sea notificado sobre los mensajes que han sido dejados. Los usuarios pueden decidir ser notificados sobre todos los mensajes o sólo los marcados como urgentes, como se lo muestra en la figura 1.19.

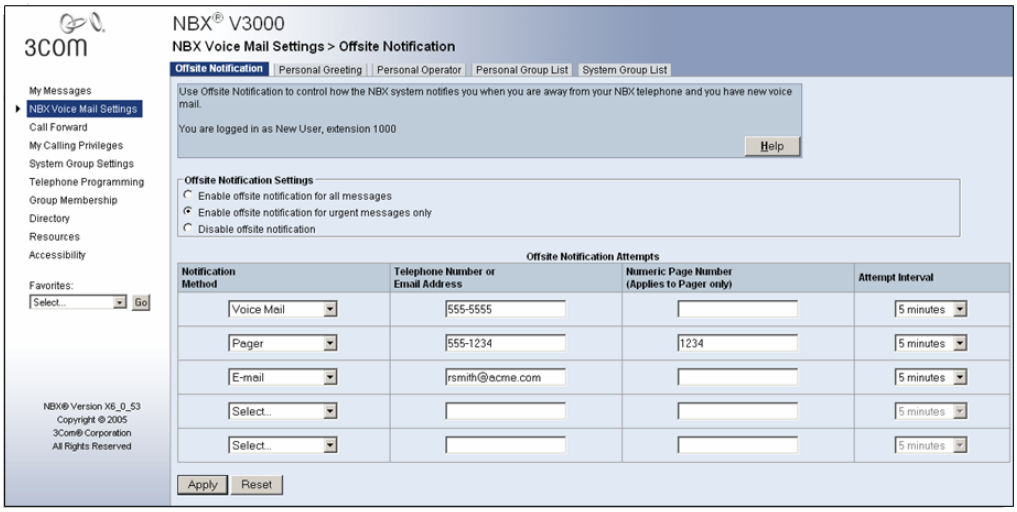


Figura 1.19. Muestra la configuración para la notificación exterior.

Zona de *Paging*

El *paging* es la habilidad de enviar un mismo mensaje a todas las estaciones, un mensaje de voz a través de los altoparlantes del teléfono o los sistemas de paginación externos que se conectan al sistema de NBX, como se lo muestra en la figura 1.20.

Figura 1.20. Muestra el proceso de *paging*.

La característica de zona paging permite que el administrador de NBX agrupe un número específico de dispositivos dentro del sistema como miembros de una zona. Los usuarios tienen la habilidad de llamar por megafonía a miembros de ese grupo. Un usuario puede llamar por megafonía el grupo a través de los parlantes del teléfono, o a través de parlantes externos. El administrador del sistema escoge el nombre y la extensión en uso.

El sistema de NBX admite múltiples zonas *paging* simultaneas. Sin embargo, un dispositivo que es actualmente de paginación o ser llamado por megafonía no responderá a otro pedido de *paging*.

El administrador puede arreglar una zona *paging* para ser accedido solamente a los miembros de la zona de *paging* o accesible para todos los usuarios.
El release 6 de la NBX (R6) soporta hasta 16 zonas de *paging* por el sistema. Cada uno tiene un nombre y extensión.

El *paging* puede ser desactivado sobre teléfonos individuales. Una extensión de dispositivo puede ser miembro de zonas de múltiples *paging.* Ningún límite sobre el número de dispositivos en una zona de paging.

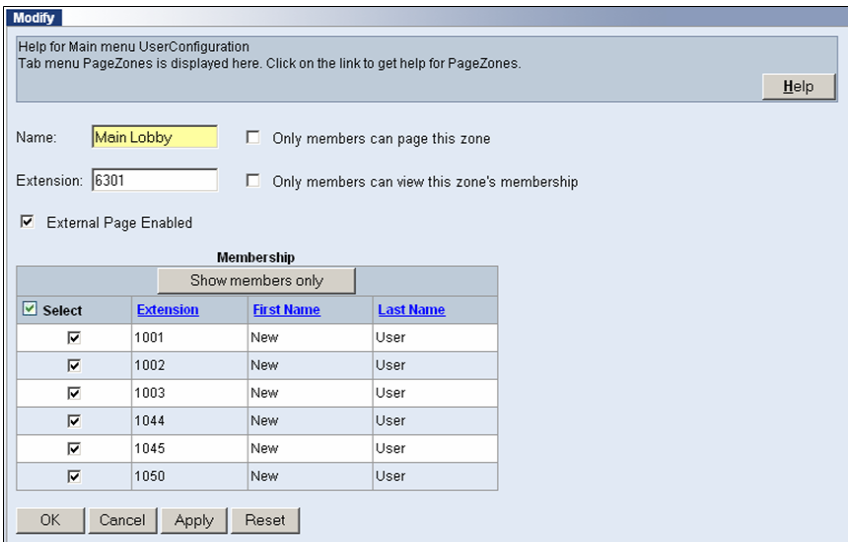


Figura 1.21. Muestra la configuración para las zonas de paging.

Atendedora Automática

Una Atendedora Automática es un servicio de contestador automático de teléfonos, usado en lugar de un encargado de atendimiento vivo. La NBX soporta hasta 100 Atendedoras Automáticas con 20 submenús cada uno.

El administrador puede configurar diferentes Atendedoras Automáticas basados en la hora del día y día de semana. Por ejemplo. Mañana, tarde o las horas después, como se lo muestra en la figura 1.22.

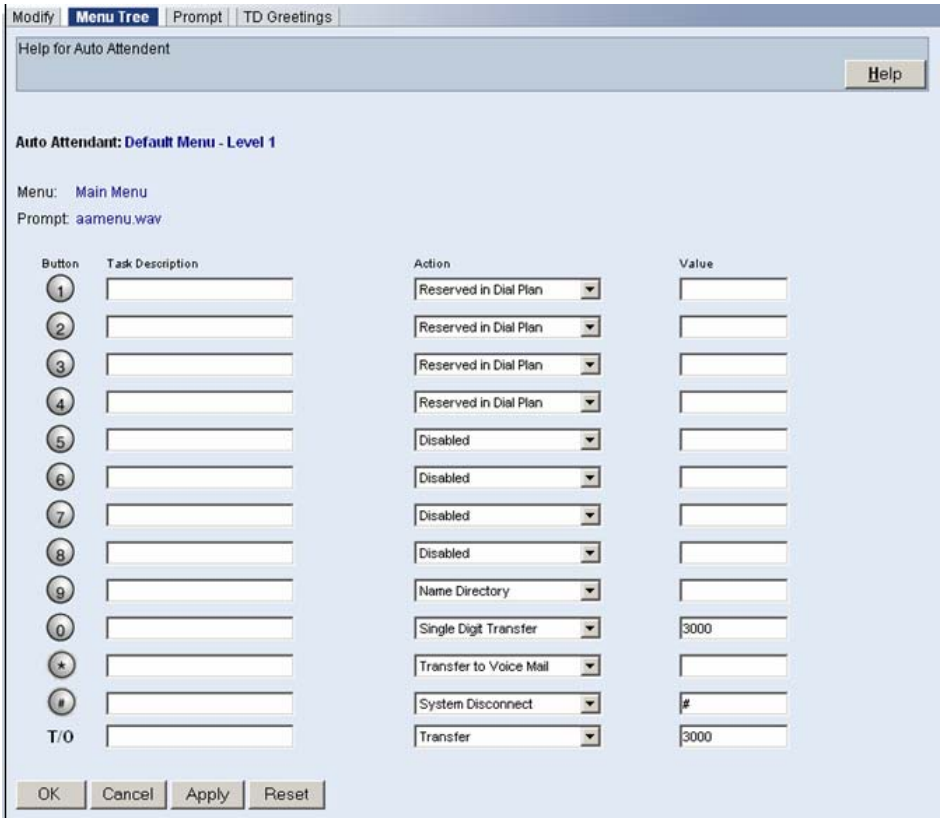


Figura 1.22. Muestra la configuración de la Atendedora Automática.

VTL

Virtual Tie Lines – es una conexión no tradicional, como lo es IP, establecido entre dos o más sistemas P.B.X.s permitiendo la comunicación entre ellas. Con sistemas de P.B.X. tradicionales, cuando la comunicación entre usuarios es requerido para múltiples sitios, o cuando los usuarios requieran acceso a la línea externa a través de las líneas de sitios distantes de la P.B.X.

Las líneas virtuales tie lines permiten algunos sistemas de NBX hacer las llamadas entre sí sin usar tarjetas análogas o líneas digitales. Esto causa marcaciones entre ubicaciones y es una alternativa viable a circuitos tie lines tradicionales entre ubicaciones.

El papel de la VTL es suministrar un mecanismo de señalización de llamadas para ser aprobado entre dos dominios del NCP, como se muestra en la figura 1.23.

La capacidad de VTL es convertida en un módulo de procesamiento de llamadas y ningún equipo físico adicional es requerido. VTLs mantienen QoS y suministran Tagging de IP - TOS de punta a punta.

Hasta 48 canales de VTL son soportados para la V3000. La concesión de licencia es vendida en incrementos de dos puertos. Una licencia de IP On-the-Fly usualmente es requerido en cada sistema de NBX.

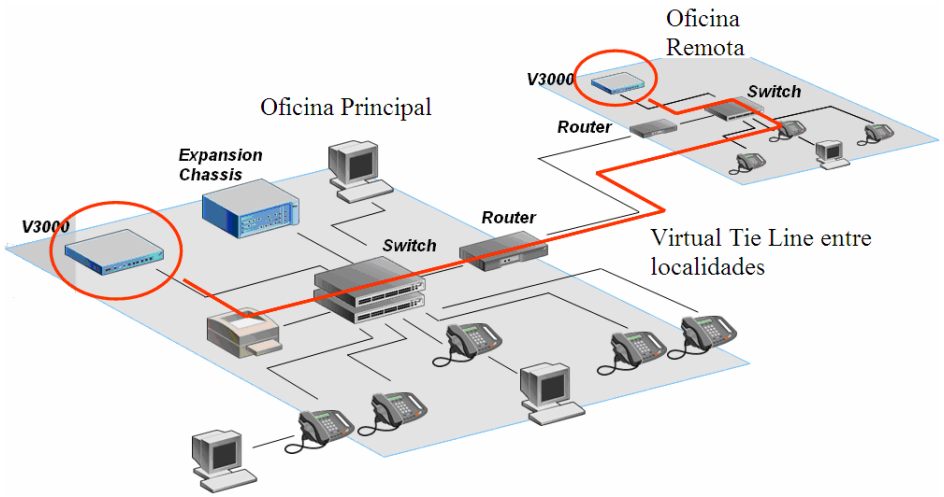


Figura 1.23. Muestra como se conectan las VTLs entre dos localidades diferentes.

Consideraciones

- Cantidad del volumen de llamada entre sitios.
- Número correcto de puertos de VTL y ancho de banda.
- Configuración del plan de marcación.

Consideraciones del ancho de banda

Cada llamada de VTL sin la compresión usa 87 kbps de ancho de banda en ambos sentidos

Cada llamada de VTL que usa compresión consume 55 kbps de ancho de banda en ambos sentidos.

Estar seguros de usar switches y routers que soporten calidad del servicio (capa 2 y 3).

- 802.1p / Q
- IP TOS / Diff Serv
- DSCP
- Multicast de IGMP

QoS Packet Tagging:

Cada paquete de voz es etiquetado con una prioridad estándar. El campo de prioridad de bits de los paquetes son leídos por switches y routers. Switches y routers colocan el tráfico dentro de buffers de transmisión de prioridad.

Es recomendado que una red privada sea usada en contra del Internet. Esto es porque IGMP no es soportado al otro lado de la Internet y el ancho de banda, la latencia y los asuntos de confiabilidad son comunes.

Compresión

Las configuraciones por defecto del software del sistema aseguran una buena calidad de audio bajo un rango de condiciones operativas. No se recomienda cambiar los ajustes de codificación estándar a menos que la calidad de sonido o la restricción de ancho de banda que no pueden ser resueltos a través de otros medios, como incrementar la capacidad de ancho de banda de la red (3Com, 2007).

La selección del codec no es aplicable a la música en espera, al correo de voz y Auto Attendant, que usan ADPCM solamente.

El ajuste de compresión afecta a todos los teléfonos, adaptadores de terminal analógicos, y la tarjeta de línea análoga y digital, al menos que la configuración sea diferente al nivel del dispositivo. No se puede configurar la compresión para VTLs

individuales, este ajuste es cambiado a nivel global. En un típico ambiente de red de área extendida, no se tiene control completo sobre el ancho de banda así que poner la compresión sobre las llamadas de VTL puede ayudar asegurar el tráfico de voz confiable sobre sus conexiones de VTL. El ajuste de compresión por defecto y compresión de sonido sobre las llamadas de VTL es - G711, como se lo muestra en la figura 1.24.

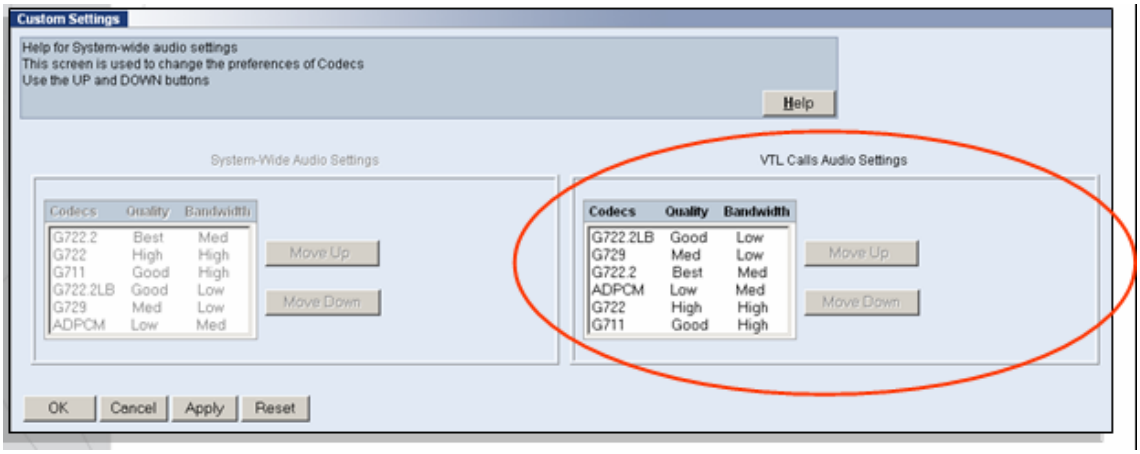


Figura 1.24. Muestra los Codecs de compresión de voz que se pueden emplear para las llamadas en VTLs.

Consideraciones WAN

El puerto 1040 del protocolo TCP y el rango de puertos UDP 2093 - 2096 son requeridos para hacer y recibir las llamadas de VTLs. Si su red tiene un cortafuegos o un aparato de seguridad instalados usted necesitará hacer los cambios de configuración apropiados para permitir la comunicación en estos puertos.

Traducción de dirección de red (NAT) es un estándar de Internet que permite que a una (LAN) de red de área local use un juego de direcciones IP para el tráfico interno y un segundo juego de direcciones para el tráfico externo. No se puede usar NAT con VTLs.

Es recomendado que usted usa una conexión de la red particular y no la Internet para VTLs. Estar seguro de sus equipos WAN y el proveedor permita el suficiente ancho de banda para las VTLs.

La NBX usa un rango específico de direcciones multicast. Estas direcciones son definidas dentro del NetSet y no deben ser cambiadas. Si multicast no está disponible al otro lado de la red de área extendida entonces las funciones como la llamada de conferencia son perdidas. Para funcionalidad multicast se debe respaldar, que todos los switches y routers del sistema de la NBX deben soportar multicast de IGMP.
Note que la música en espera no es soportada al otro lado de la VTL.

1.11 SISTEMA DE TELEFONÍA IP

El punto principal del sistema NBX es el procesador de llamada de la red (NCP). El NCP dirige los procesos de hacer y recibir las llamadas, proveer servicios de correo de voz y atendimiento automático, y responder a las solicitudes para servicios especiales, como el acceso para el servicio público de administración del NetSet de NBX, los servicios de integración teléfono computador (CTI), o el servidor de IMAP (el protocolo de Access de mensaje de Internet) del sistema.

1.11.1 Modos de operación de la NBX

La flexibilidad y la naturaleza robusta de la NBX permiten que él opere en algunos modos haciéndolo la elección correcta para casi cualquier tipo de solicitud:

- Modo de P.B.X.
- Modo KEY
- Modo híbrido

Modo PBX

En el modo de P.B.X. las líneas exteriores son juntadas y manejadas por el procesador de llamadas. Para llamar un número externo un usuario debe marcar para el acceso de línea típicamente el número 9. El procesador de llamada atribuye la próxima línea disponible al usuario.

Cuando una llamada es establecida el NCP deja la conversación.

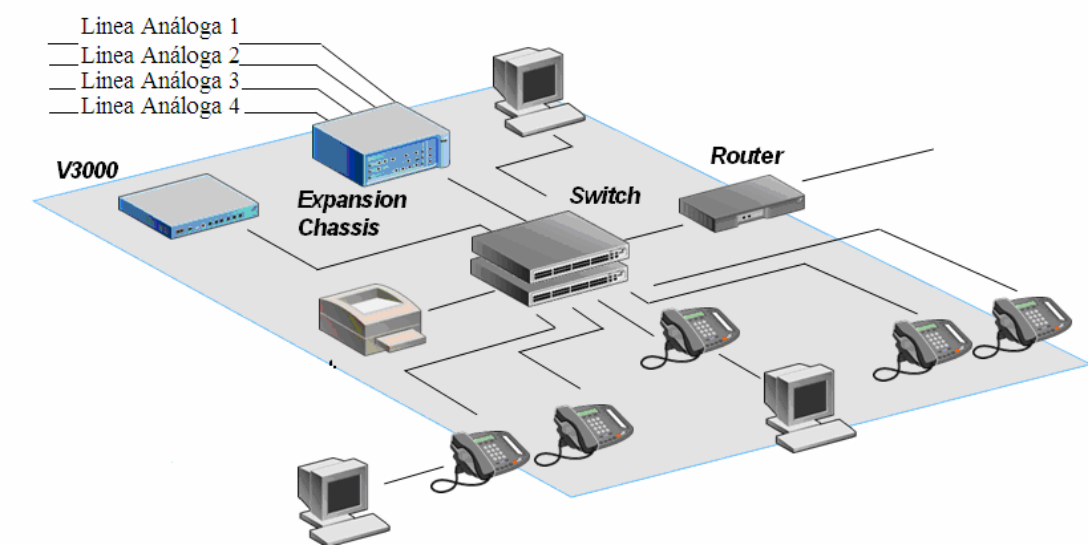


Figura 1.25. Muestra el modo de operación PBX de la NBX.

Modo KEY

En el modo KEY las líneas externas se mapean a botones individuales sobre los teléfonos. Los usuarios pueden compartir líneas, debido a que una línea puede ser mapeada a múltiples teléfonos. Las llamadas entrantes suenan en los teléfonos que tienen esa línea asignada.

El administrador puede definir una "Evolución sonante" para una línea mapeada a múltiples teléfonos. La llamada suena primero sobre un teléfono, y luego progresivamente sobre otros teléfonos. Ninguno de los teléfonos puede recoger la llamada incluso si ese teléfono especial no ha empezado a sonar

Modo Hibrido

En el modo híbrido algunas líneas exteriores son agrupadas mientras las otras líneas son distribuidas directamente a botones sobre teléfonos.

1.11.2 Procesador de llamadas en RED

El punto principal del sistema de NBX es el procesador de llamada de la red (NCP). El NCP es responsable de poner la comunicación entre puntos finales. Todos los modelos de NCP de NBX comparten muchos de los mismos puertos físicos:

- Alarma externa
- Página externa
- La música en espera (MoH)
- Consola
- Puertos de Ethernet

Note que los puertos de USB sobre los sistemas de NBX no están actualmente activos y se han reservado para futuro uso. La figura 1.26 muestra los componentes de la NBX.

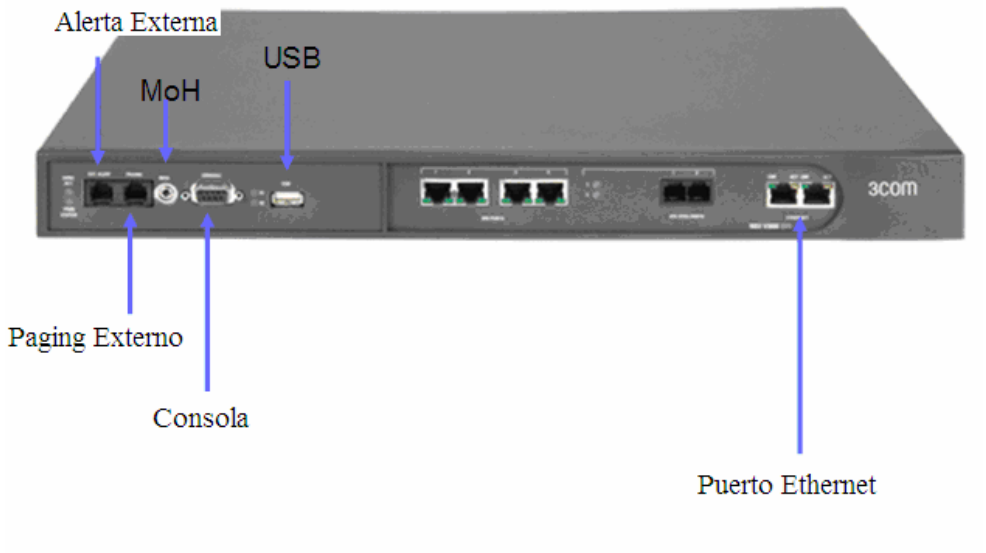


Figura 1.26. Componentes externos de la NBX.

Todos los procesadores de llamada de la red de NBX comparten los mismos componentes de equipos físicos básicos:

- Una o más unidades de discos
- Memoria
- Uno o dos suministros de energía
- Main Board

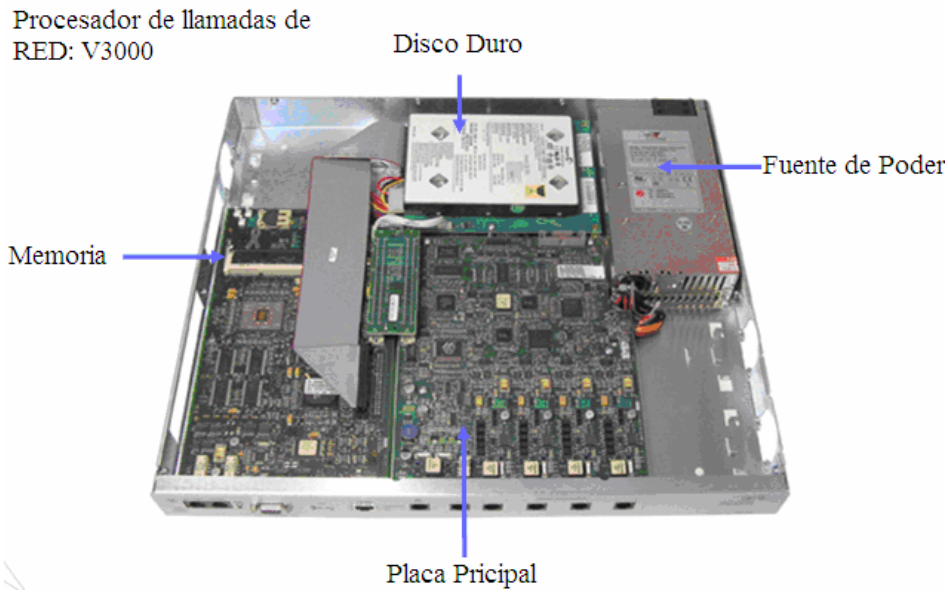


Figura 1.27. Muestra los componentes internos de la NBX.

Sistema de comunicación de V3000 de NBX

Soporta:

- 1500 dispositivos
- 375 tarjetas terminales analógicas
- 180 tarjetas de líneas analógicas
- 31 tarjetas de línea digital
- 90 tarjetas ISDN BRI-ST
- 100 Auto Attendants
- 72 puertos de voice mail
- 1500 mailboxes
- 1000 phantom mailboxes
- 12 conferencias de llamadas simultaneas
- 100 Hunt groups
- 48 Virtual Tie Lines

La central telefónica NBX V3000, integra cuatro puertos analógicos, un puerto de estación - equipo, y la interfaz de Ethernet 10/100 MB indispensable para dar un control de llamada completo y brindar una plataforma de acceso a pequeñas y medianas empresas. Para reducir costos eficazmente y permitir el crecimiento rápido, el sistema de V3000 incluye 400 hora de almacenamiento de correo de voz, cuatro auto attendant /

puertos de correo de voz, y el NetSet servicio público de administración a través de un navegador; la solución de V3000 de NBX puede ser ampliado para soportar no menos que 1,500 dispositivos, como se lo muestra en la figura 1.28.

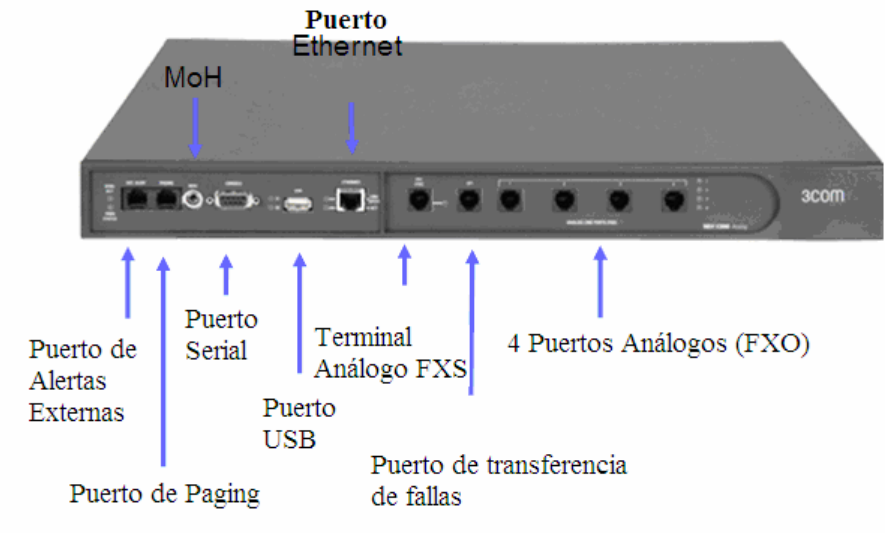


Figura 1.28. Muestra los componentes externos de la NBX V3000.

Expanción nbx 100 chasis de 6 slots

- Seis slots de tarjetas universales
- Puede ser usado para expandir cualquier sistema de comunicación NBX
- 10 Mb de backplane compartido
- Requerir la tarjeta de enlace ascendente para la conectividad de la red (cuando la NCP no esta presente)
- Fuente de poder única
- Requiere la interfaz de Ethernet propia de la tarjeta de enlace ascendente para la conexión de la red

NCP de NBX tiene 100 megabytes fullduplex de backplane. El NBX funciona en capa 2 (voz sobre Ethernet) y la plataforma de comunicaciones de capa 3 (voz sobre IP). Esto es una ventaja considerable sobre competidores que son estrictamente capaces de trabajar en capa 3. La voz sobre el Ethernet permite que el NBX sea instalado en ambientes más pequeños fácilmente sin la complejidad de la instalación de IP de capa 3.

Operación en capa 2

La NBX opera por defecto en capa 2. La operación de capa 2 es suficiente para los ambientes pequeños con una LAN sola donde el NBX y los teléfonos están en la misma LAN de Ethernet o VLAN.

Operación de capa 2 de Ethernet:

- Es barato, y fácil de implementar
- La dirección de destino es siempre una dirección Mac
- Todas las tramas transmitidas alcanzan cada dispositivo sobre la VLAN

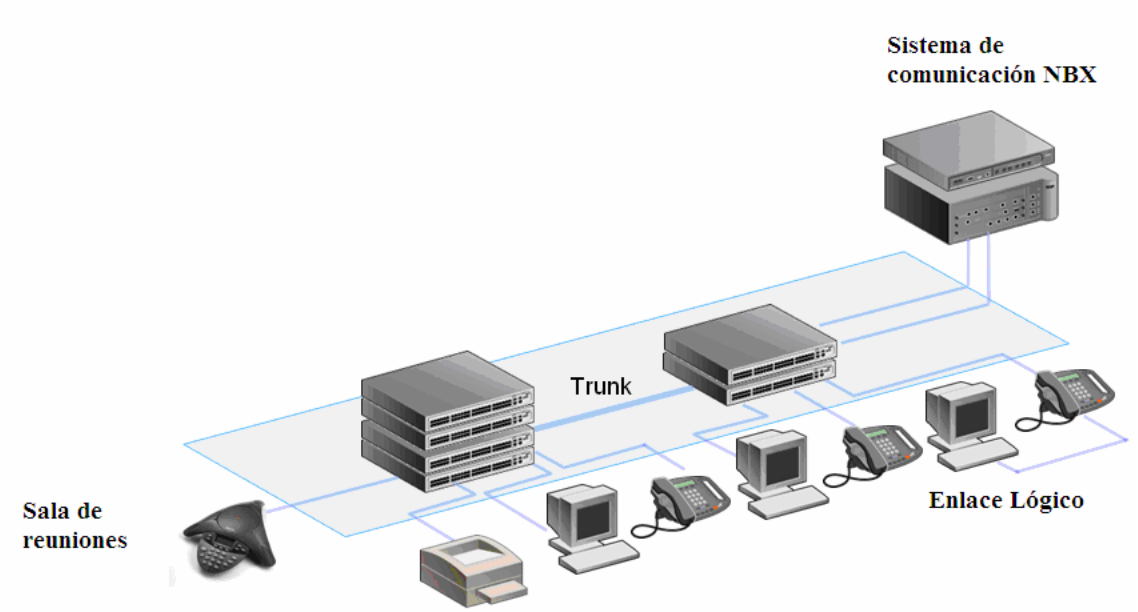


Figura 1.29. Funcionamiento de la Central Telefónica NBX en capa 2.

Operación en capa 3

La operación de capa 3 es requerida para ambientes con LAN múltiples donde la NBX y los teléfonos pueden estar sobre LAN de Ethernet diferentes, VLANS o al otro lado de redes de área extendidas

Usando IP (capa 3), un sistema de NBX solo puede soportar oficinas lejanas con varios teléfonos. Los teléfonos remotos funcionan como si estuvieran conectados como las extensiones locales.

El NCP en el sitio principal provee el control de llamada, el correo de voz, etcétera a los dispositivos remotos.

1.12 COMPONENTES DEL SISTEMA

Protocolos VoIP

Telefonía IP utiliza como soporte cualquier medio basado en routers y los protocolos de transporte UDP/ IP. El modelo de capas diseñado en 1981 para IP tenía prevista la voz sobre RTP/ IP; el modelo actual agrega UDP/ IP.

Existen varios organismos involucrados en los standards: el ITU-T (H.323 por ejemplo); el ETSI (con el proyecto Tiphon), el IMTC (International Multimedia Teleconferencing Consortium) y el IETF (que administra los protocolos de Internet).
Los protocolos de señalización utilizados en IP-Telephony son de diversos tipos. El ITU-T H. 323 es el primero aplicado para acciones dentro de una Intranet fundamentalmente. Es una cobertura para diversos protocolos H. 225, H. 245 y RAS que se soportan en TCP y UDP.

El IETF está definiendo otros tipos de protocolos: el MGCP para el control de las gateway a la red pública PSTN y los SIP/ SAP/ SDP hacia las redes privadas. Anterior a MGCP (trabaja sobre UDP) es el protocolo IPDC (IP Device Control) que trabaja sobre TCP y fue desarrollado por Level3 y el SGCP (Simple GCP) desarrollado por Bellcore.

La señal vocal se transmite sobre el protocolo de tiempo real RTP (con el control RTPC) y con transporte sobre UDP. El protocolo de reservación de ancho de banda RSVP puede ser de utilidad en conexiones unidireccionales. La señalización SS7 se utiliza hacia la red pública PSTN. De forma que se disponen de los protocolos ISUP/ SCCP/ TCAP que se transmiten sobre MTP en la PSTN y sobre TCP/ IP en la red de paquetes. El protocolo Q.931 (derivado de ISDN) se utiliza para establecer la llamada en H. 323.

1.12.1 Protocolo H323

ITU-T H. 323.

Esta norma del ITU-T data de 1996 (versión 1) y 1998 (versión 2) y ha sido generada para sistemas de comunicación multimediales basado en paquetes; redes que pueden no garantizar correctamente la calidad de servicio QoS. Esta tecnología permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. Es de suma importancia ya que los primeros servicios de voz sobre protocolo Internet (VoIP) utilizan esta norma. En la versión 1 del protocolo H. 323v1 del año 1996 se disponía de un servicio con calidad de servicio (QoS) no garantizada sobre redes LAN. En la versión 2 del año 1998 se definió la aplicación VoIP independiente de la multimedia. Una versión 3 posterior incluye el servicio de fax sobre IP (FoIP) y conexiones rápidas entre otros.

La versión H. 323v2 introduce una serie de mejoras sobre la H. 323v1. Algunas de ellas son: permite la conexión rápida (elimina parte de tiempo de solicitud de conexión); mediante H.235 introduce funciones de seguridad (autentificación, integridad, privacidad); mediante H. 450 introduce los servicios suplementarios; soporta direcciones del tipo RFC-822 (email) y del formato URL; mediante la unidad MCU permite el control de llamadas multi-punto (conferencia); permite la redundancia de gatekeeper; soporta la codificación de vídeo en formato H.263; admite el mensaje RIP (Request in Progress) para informar que la llamada no puede ser procesada por el momento; provee la facilidad que el gateway informe al gatekeeper sobre las disponibilidad de enlaces para mejorar el enrutamiento de llamadas; etc.

Tabla 1.2: Muestra las normas ITU-T APRA multimedia.

. Normas ITU-T para multimedia.

Norma ITU-T	Año	Aplicación	Vídeo	Audio	Múltiplex	Control
H.320	1990	ISDN	H.261	G.711	H.221	H.242
H.324	1995	POST	H.263	G.723	H.223	H.245
H.323	**1996/98**	**LAN**	**H.261/263**	**G.711**	**H.225**	**H.245**
H.310/321	1996	ATM	H.262	MPEG-1	H.222	H.245

Protocolos de H. 323

Descripción

Tráfico. -Codificación de audio: G. 711 a velocidad de 64 kb/ s; G. 722 para 48, 56 y 64 kb/ s; G. 728 para 16 kb/ s y G. 729 para 8 kb/ s. En tanto el ITU-T ratificó en 1995 a G. 729, el VoIP Forum en 1997 (liderado por Intel y Microsoft) seleccionó a G. 723.1 con velocidad de 6,3 kb/ s para la aplicación VoIP.

-Codificación de vídeo: de acuerdo con H. 263.

Señalización. -.H. 225. Son los mensajes de control de señalización de llamada que permiten establecer la conexión y desconexión. Este protocolo describe como funciona el protocolo RAS y Q. 931. H. 225 define como identificar cada tipo de codificador y discute algunos conflictos y redundancias entre RTCP y H. 245.

Q.931. Este protocolo es definido originalmente para señalización en accesos ISDN básico BRI (Basic Rate Interface). Se utiliza para señalización de llamada en la red IP (desde el GW hacia el terminal). Es equivalente al ISUP utilizado desde el GW hacia la red PSTN.

RAS (Registration, Admission and Status) utiliza mensajes H.225 para la comunicación entre terminal y gatekeeper GK. Sirve para registración, control de admisión, control de ancho de banda, estado y desconexión.

H. 245. Este protocolo de señalización transporta la información no-telefónica durante la conexión. Es utilizado para comandos generales, indicaciones, control de flujo, gestión de canales lógicos, etc. Se usa en la interfaz terminal-a-terminal y terminal-a-GK. H. 245 es una librería de mensajes con sintaxis es del tipo ASN. 1. En particular codifica los dígitos DTMF (Dual-Tone MultiFrequency) en el mensaje UserInputIndication.

H.235. Provee una mejora sobre H. 323 mediante el agregado de servicios de seguridad como autentificación y privacidad (criptografía). H.235 trabaja soportado en H.245 como capa de transporte. Todos los mensajes son con sintaxis ASN. 1.

Calidad de servicio. -Protocolo RTP (Real-Time Transport Protocol): usado con UDP/ IP para identificación de carga útil, numeración secuencial, monitoreo, etc. Trabaja junto con RTCP (RT Control Protocol) para entregar un feedback sobre la calidad de la

transmisión de datos. El encabezado de RTP puede ser comprimido para reducir el tamaño de archivos en la red.

Protocolo de reservación de ancho de banda RSVP usado para reservar un ancho de banda especificado dentro de la red IP. Téngase en cuenta que RSVP trabaja sobre PPP (o similar a HDLC) pero no trabaja bien sobre una LAN multiacceso.

Protocolo PPP *Interleaving* se utiliza para enlaces inferiores a 2 Mb/ s para fraccionar los paquetes de gran longitud y permitir el intercalado con paquetes de servicios en tiempo-real.

Direcciones -Dirección de red (*IP Address*). Se trata normalmente de direcciones privadas que identifican a cada componente. La asignación de direcciones puede ser fija o asignada en forma dinámica (protocolo DHCP).

Dirección TSAP. Corresponde al puerto TCP/ UDP. Permite la multiplexación de canales con la misma dirección de red. Algunos componentes, como el GK y el protocolo RAS, tienen una dirección de puerto fija (well-known). En otros, como los terminales, se asignan en forma dinámica.

Dirección de Alias. Se trata de alguna identificación como el número telefónico, dirección de email, nombre de usuario, etc. La resolución de direcciones alias se realiza en el gatekeeper.

1.12.2 Protocolo SIP

SIP

SIP es uno de los protocolos fundamentales de los sistemas de voz sobre IP. SIP significa protocolo de iniciación de sesión. Es un protocolo estándar de señalización para iniciar, modificar, y terminar las sesiones interactivas de los usuarios que involucran elementos de multimedia como el video, la voz, mensajera instantánea entre dos o más puntos en una red IP.

El protocolo es definido dentro del grupo de trabajo de la IETF SIP.

3Com es miembro del foro de debate de SIP y fue el primero en el mercado en dar completamente una funcionalidad SIP - P.B.X., el VCX de 3Com.

Figura 1.30. Muestra dos teléfonos SIP conectados.

SIP realiza seis pasos para ejecutar una conversación:

- Invite – Inicia la sesión
- Ack – Confirma el establecimiento de la sesión
- Bye – termina la sesión
- Cancel – cancela una invitación pendiente
- Options – capacidad de consultar
- Register – une una dirección a la ubicación del dispositivo

SIP es un protocolo basado en texto, similar a HTTP y al SMTP, para iniciar las sesiones de comunicación interactivas entre usuarios. Esto hace que SIP sea fácil localizar fallas, permite el rápido desarrollo de aplicaciones, y presenta un marco estable para establecer la interoperabilidad entre dispositivos, aplicaciones, controladores de llamada, y *gateways*.

SIP es diseñado para llevar a cabo la sesión de configuración independiente del flujo de comunicaciones. Los dispositivos finales hablan directamente con otros. Esto suministra un nivel más grande de flexibilidad, recuperación de fallas, y la escalabilidad.

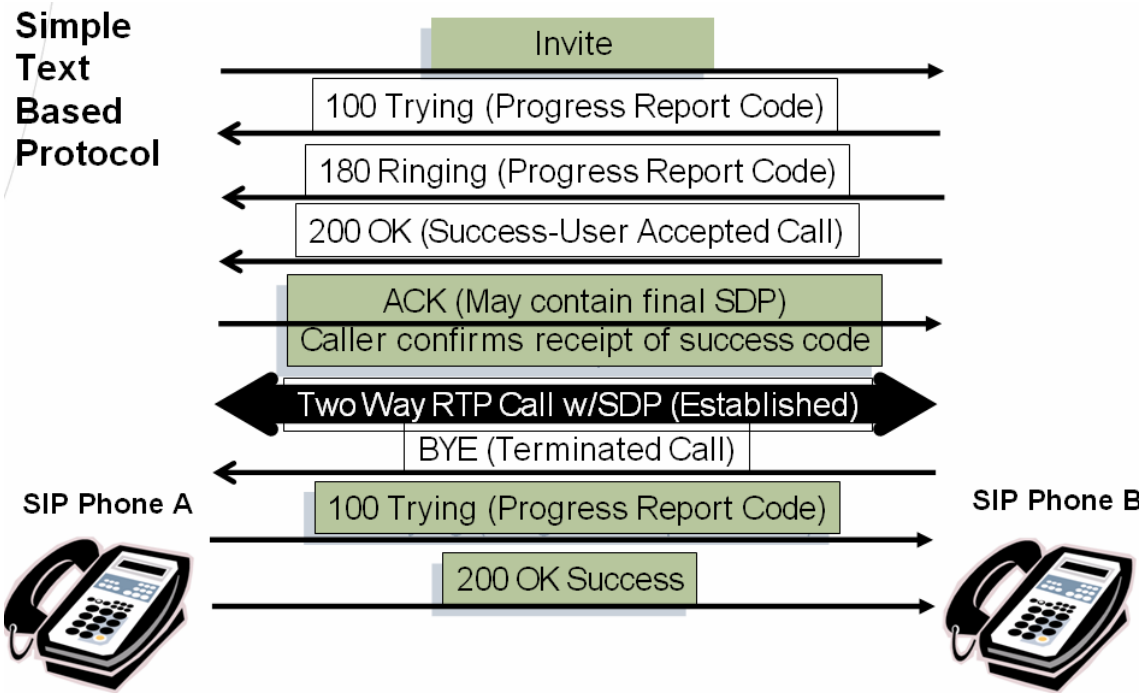


Figura 1.31. Muestra los pasos para realizar una llamada en modo SIP.

En una configuración de sesión SIP, un dispositivo SIP (como un teléfono SIP) envía una invitación a otro dispositivo SIP. El pedido es enviado a la dirección del usuario. El usuario envía una clave de respuesta. Hay varios tipos de respuestas codificas:

- 1yz respuestas informativas
- 100 probando
- 180 timbrando
- 181 la llamada esta siendo enviada
- 2yz Éxito
- 200 OK
- 3yz Redirección
- 300 opciones múltiples
- 301 movido permanentemente
- 302 movido temporalmente
- 4yz Error de cliente
- 400 solicitud mala
- 401 no autorizado
- 482 bucle detectado

- 486 ocupado aquí
- 5yz Servidor de fallas
- 500 servidor de error interno
- 6yz fracaso global
- 600 ocupado por todos lados

Cuando el Ack es enviado por el caller, la sesión está establecida. La llamada es terminada con BYE. Las claves de las respuestas son enviadas.

En un ambiente de P.B.X. en SIP, los mensajes no son enviados a un usuario directamente. Estos son enviados primero a un servidor proxy, que es el responsable de rutear primero el mensaje a la llamada que tomo parte. El proxy SIP también puede funcionar en un servidor de intercambio de mensajes, servidor de conferencias, y servidor de presencia creando rutas de llamada y llamadas de cobertura.

Esquema de dirección SIP

Sip usa un esquema de direccionamiento que es de lectura fácil y amena para los seres humanos (opuesta al sistema de notación decimal numerada). Una dirección SIP parece muy similar a una dirección de correo electrónico. Esto permite encontrar recursos a través de un servidor DNS.

Un ejemplo de una dirección de SIP es:
Sip:john.smith@3com.com

RTP y SDP

SIP depende de RTP para el transporte. RTP significa protocolo de transporte de tiempo real, un protocolo que soporta la transmisión en tiempo real de la voz y video. Un paquete de RTP reside sobre UDP. UDP es parte de la suite de protocolos de TCP/IP. Esta en capa 4, protocolo de entrega del mejor esfuerzo y mantiene servicios de la red sin conexión. UDP provee la información de sincronización en su encabezamiento para el reensamblaje correcto al final de la recepción.

El protocolo de descripción de sesión o SDP definen un formato de mensaje basado en texto para describir una sesión de multimedia. La información como el número de la versión, la información de contacto, el número de broadcast , audio y videoconferencia son incluidos en el mensaje. SDP es usado por algunos protocolos compitiendo como SIP, MGCP, y RTSP.

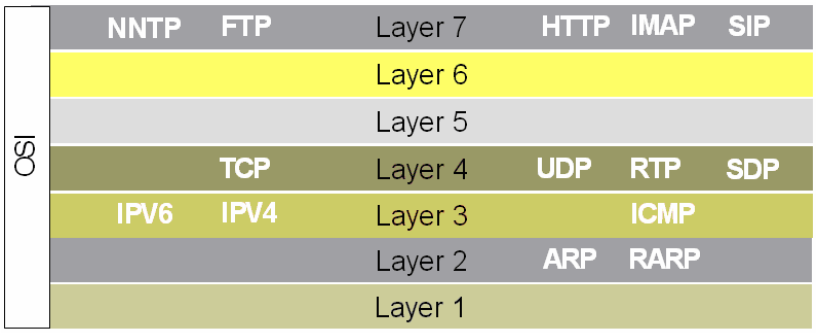


Figura 1.32. Muestra los protocolos usados en las capas del modelo OSI.

Arquitectura de la comunicación SIP (L3)

Cuando la comunicación es de un teléfono de la NBX a un teléfono SIP (local o remoto).

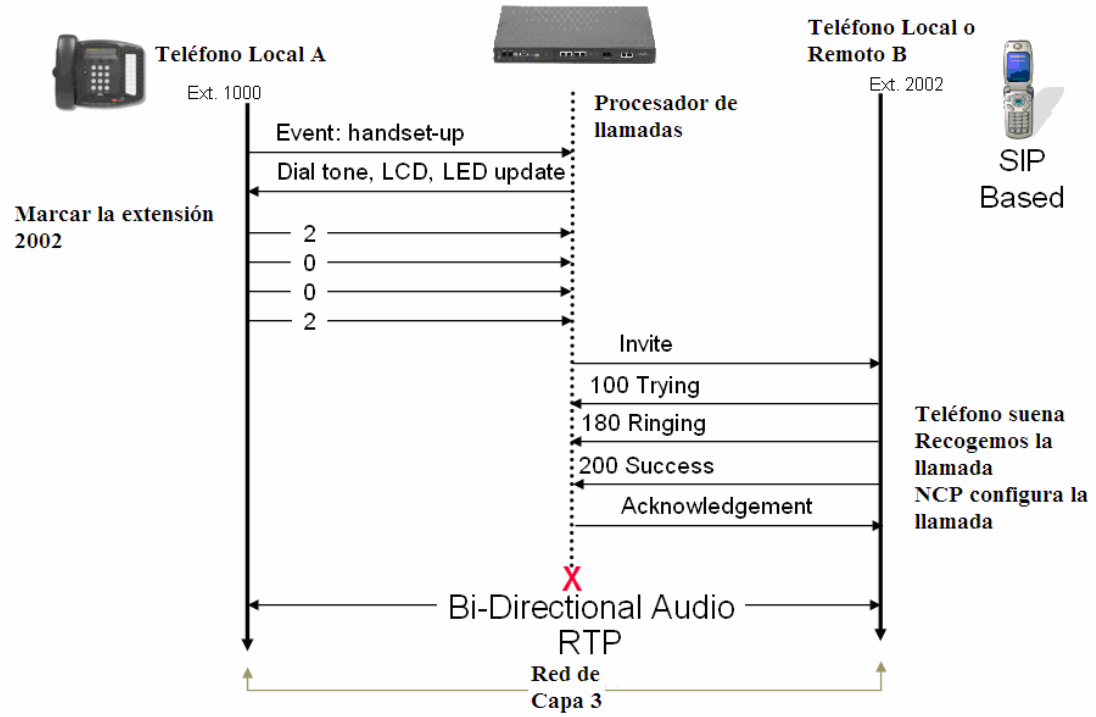


Figura 1.33. Muestra los procesos de comunicación entre dos teléfonos SIP en capa 3.

Detalles del modo SIP

Un sistema de NBX que trabaja en modo SIP puede interoperar con cualquier otro punto final de SIP, incluyendo gateways, dispositivos, y aplicaciones habilitadas en SIP.

Un sistema de NBX en modo de SIP usa estándar IP como el protocolo de red. Si se habilita SIP sobre un sistema de NBX que está usando modo de Ethernet o IP on the fly , el sistema cambia a IP Standard automáticamente. Típicamente se configura un servidor de DHCP para que provea la información de IP a dispositivos y configure la opción 184 sobre el servidor proveyendo la dirección IP del NCP.

La mensajería no está disponible sobre un sistema de NBX cuando se ejecuta el modo SIP. Para las características de mensajería, (correo de voz, auto attendant, música en espera, y anuncios retardados de ACD), se debe integrar un sistema mensajería externo, como el IP Messaging 3.0 de 3Com, que es vendido por separado. El sistema de NBX puede comunicarse con el sistema de mensajería IP de 3Com para crear buzones de mail automáticamente. El servidor de mensajería IP de 3Com puede ser configurado sincronizando periódicamente con el sistema NBX.

Paging es soportada sobre teléfonos de NBX con SIP activado pero: solamente teléfonos de NBX pueden iniciar un paging, solamente los teléfonos de NBX pueden recibir el paging, teléfonos SIP no pueden inicializar un paging solo lo pueden recibir.
Un usuario puede registrase en teléfonos diferentes (Hot Desking), pero solamente un registro de entrada a la vez esta admitido. Si un usuario está en una llamada, y luego ese usuario entra a otro teléfono, la primera llamada será desconectada. Esta característica no está disponible en un sistema de NBX que esta trabajando en el modo SIP.

Para las llamadas de 911 de emergencia, se puede arreglar que un teléfono de 3Com use que una vía de acceso de SIP alternativa que conecte las llamadas cuando el sistema de NBX está fuera de servicio. Teléfonos de 3Com no soportan la alternativa de DHCP para proveer una dirección de vía de acceso de SIP alternativo así que esta característica requiere la configuración manual.

La configuración de mapeo de botones no es soportada para el teléfono inalámbrico 3108 de 3Com o teléfonos SIP genéricos, es decir teléfonos de terceras empresas que soportan el protocolo SIP. No se puede mapear una línea de la Oficina Central a un teléfono SIP genérico o en el 3108 teléfono inalámbrico. Dispositivos SIP no pueden ser extensiones puente.

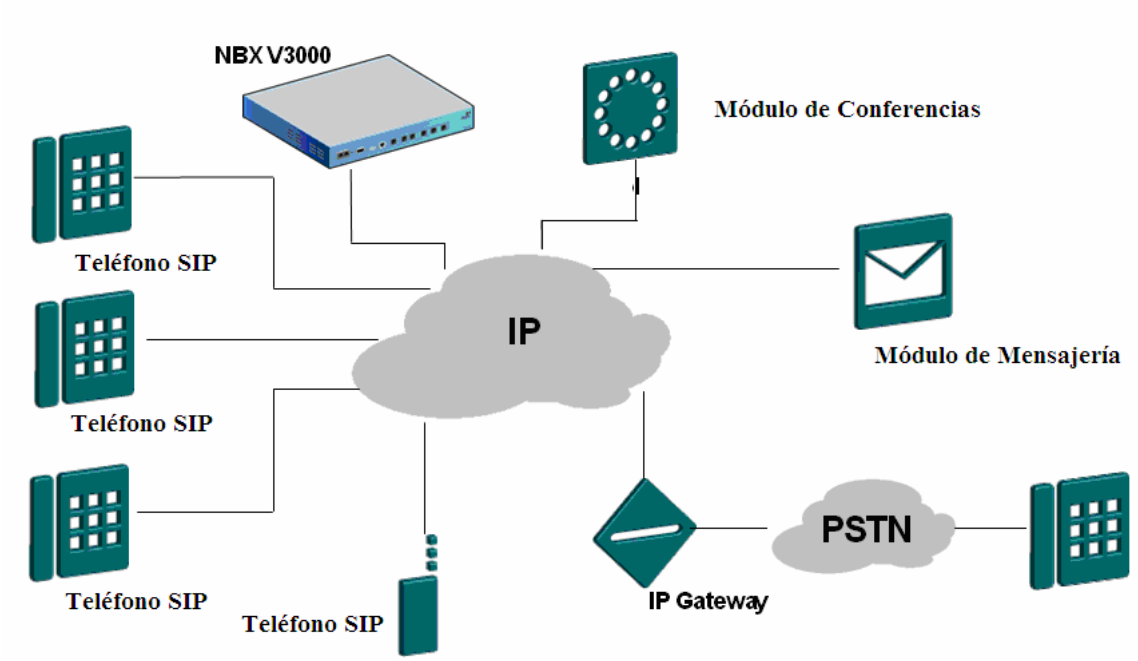


Figura 1.34. Muestra la central telefónica, trabajando en redes IP y en la PSTN.

Las conferencias pueden incluir hasta tres participantes, el creador de la conferencia, y los dos otros participantes de la conferencia interna o externa. El límite es cuatro participantes que no estén ejecutando el modo SIP en la NBX. Sin embargo, el número de sesiones de conferencia simultáneas (cada sesión = 4 participantes) soportado en modo no SIP, aumenta más allá del límite de la NBX en curso de 12. Para el soporte para las conferencias que requieren más de 3 participantes en una llamada se puede configurar opcionalmente un servidor de aplicación de conferencias de 3Com.

NBX Virtual Tie Lines no están disponibles sobre un sistema de NBX que se ejecuta en el modo SIP. Sin embargo, se puede conseguir el mismo resultado que, conectar a sistemas de NBX diferentes, configurando cada sistema de NBX que está corriendo el modo de SIP como una interfaz SIP de confianza. Una interfaz de SIP de

confianza puede incluir servidores proxys SIP, aplicaciones SIP, gateways SIP, AudioCodes gateways, y cualquier otro dispositivo de SIP de otra marca, incluyendo sistemas de telefonía de IP de VCX de 3Com.

Cuando se está usando un teléfono inalámbrico 3108 se puede cambiar de una subred y entrar a otra y así conseguir una dirección IP diferente (si DHCP es usado). El teléfono enviará un nuevo pedido de registro al sistema de NBX . Después de que el sistema de NBX valida el usuario, registra el usuario con la nueva dirección IP y retira la información de dirección IP previa, que permite que el usuario haga y reciba las llamadas. Sin embargo, si el teléfono consigue una nueva dirección IP durante una llamada, la llamada será desconectada. Una red inalámbrica planeada y cuidadosamente configurada bien puede aliviar este asunto.

Modo SIP sobre una NBX representa el estándar SIP (RFC 3261) con extensiones no propietarias a SIP. Teléfono de terceras empresas que no están en función de SIP, no funcionarán. Un sistema de NBX en el modo de SIP no soporta señalización segura SIP o seguro RTP. No soporta NAT, cortafuegos, o RTP relay. La comunicación está sobre UDP solamente. V3000 de NBX requiere una actualización de memoria de 512 megabytes para operar en el modo de SIP.

El plan de marcación de la NBX comprende las reglas que gobiernan los comportamientos de la llamada. Permitir SIP sobre un sistema de NBX requiere algunas nuevas anotaciones en el plan de marcación. Por defecto el plan de marcación necesita incluir adicionalmente entradas por defecto para puertos de conexiones SIP en la tabla de ruteo. Un puerto de conexión SIP identifica la ruta para que una llamada vaya a un gateway SIP o a otro dispositivo de confianza.

Cuando se añade el primer dispositivo SIP al sistema que usa el servicio público de NetSet de NBX, el sistema incita para la creación de una lista de extensión de defecto. Si se selecciona esa opción, una nueva lista de extensión es creada y la extensión de ese dispositivo es añadida a la lista de extensión. Se puede escoger añadir manualmente la lista de extensión y añadirle el nuevo dispositivo. También se debe

crear una ruta en la tabla de entrada asociada al plan de marcación con la lista de extensiones creadas para los dispositivos SIP. Se debe editar el plan de marcación para integrar al servidor IP de mensajería de 3Com y el servidor de aplicación de conferencias de 3Com con el sistema NBX. El administrador de la NBX debe añadir una lista de extensión al plan de marcación para soportar el direccionamiento de las extensiones para cada servidor externo.

1.13 Codificadores Decodificadores de voz (Codecs)

La configuración de audio permite que se reduzca el impacto de la red debido a los paquetes de audio permitiendo o desactivando la compresión y la supresión de silencio. Se puede permitir y desactivar estos ajustes para el sistema global o para dispositivos individuales.

Antes de que el tráfico de voz pueda ser transmitido sobre una red digital, la forma de onda del audio, en una señal de análoga, debe ser codificado en un formato digital. El audio digitalizado es paquetizado y entregado sobre la red hacia un destino, y luego decodificado de regreso en una forma de onda de voz. Software llamado CODEC (codificador / decodificador) convierte la información de sonido entre formatos digital y analógicos.

Los formatos de audio digitalizados tienen propiedades diferentes. Cada formato representa un compromiso entre el ancho de banda y calidad del audio, es decir alta calidad de audio requiere más ancho de banda de la red típicamente. La compresión de datos del audio digitalizado pueden ahorrar el ancho de banda con un pequeño acuerdo de la calidad del audio, pero la compresión requieren incrementos en gastos generales de procesamiento cuando se codifica y decodifica la información de sonido. Demasiado sobrecarga de procesamiento puede presentar demoras.

1.13.1 Codecs Soportados

G.711

Compresión ninguna

Un estándar de la Unión Internacional de Telecomunicaciones (ITU) para codificación de audio. La codificación y decodificación es rápida y el soporte es extendido. También llamado MULAW o μLaw. Una ley que es una pequeña variación, de los sistemas telefónicos europeos que usan. G.711 provee una buena calidad de audio a 64 kbps. Compañías telefónicas de todo el mundo usan la codificación G.711.

ADPCM

Compresión Media

Modulación en código de pulsaciones diferenciales adaptables (ADPCM) provee una buena calidad de audio en uno más baja transmisión de bits (32 kbps). El sistema usa la Asociación de multimedia internacional (IMA) versión de ADPCM.

G.729

Compresión alta

G.729, un estándar de la ITU , que emplea una técnica de compresión más sofisticado que ADPCM y es respaldada mundialmente. El codec G.729A comprime la información de audio a 8 kbps, aunque el procesamiento de la sobrecarga resulta verdaderos anchos de banda más grandes que 8 kbps.

G..722/G.722.2/G.722.2LB

Audio de banda ancha

G.722.2 es un estándar de la ITU - T para aplicaciones de voz de banda ancha y servicios. G.722.2 es un codec de banda ancha adaptable a multi-velocidades y usa rango de velocidades de bits de 6.6 a 23.85 kbps.

G.722 es un codec SB - ADPCM (modulación de código de pulso adaptable en sub banda). Opera ADPCM sobre ambas bandas la banda baja (0 - 4000 Hz.) y la banda alta (4000 - 8000). La velocidad de bit sin procesar (Sin los encabezamientos de paquete de la red) es de 64 kbps. G.722.2 es un codec basado en CELP (predicción lineal exitada en código). G.722 tiene una velocidad de 23.85 kbps. G.722.2 LB tiene una velocidad de 8.85 kbps.

El estándar fue diseñado para redes inalámbricas originalmente y las diferentes velocidades lo permiten adaptarse a condiciones de canales variantes.

Selección del Codec

Es importante recordar en no seleccionar el codec basado solo en compresión, hay que considerar tanto el ancho de banda como la calidad de audio.

1.14 CALIDAD DE SERVICIO QOS

1.14.1 Conmutación de ethernet y priorización

Cuando la voz y datos comparten la misma red, la conmutación suministra el mecanismo de priorización que asegura la calidad de voz. Hay algunas tecnologías de prioritización basadas en estándares disponibles:

- Dentro de la LAN: 802.1p de IEEE.
- Dentro de la red de área extendida: IP - TOS y DiffServ.

Para aprovechar la capacidad de priorización de datos sobre teléfonos IP, todos de los switches de la red que llevarán el tráfico de voz necesitarán soportar 802.1p.

Una VLAN es un subgrupo lógico dentro de una red de área local creado a través de software. VLANS operan en capa 2. Los dispositivos son agrupados por la función que por su ubicación física en general. El propósito de uno VLAN es aislar el tráfico dentro de la VLAN. Un puente de una VLAN a otra, un router o funcionalidades del enrutador son requeridos. Un enrutador trabaja en capa 3.

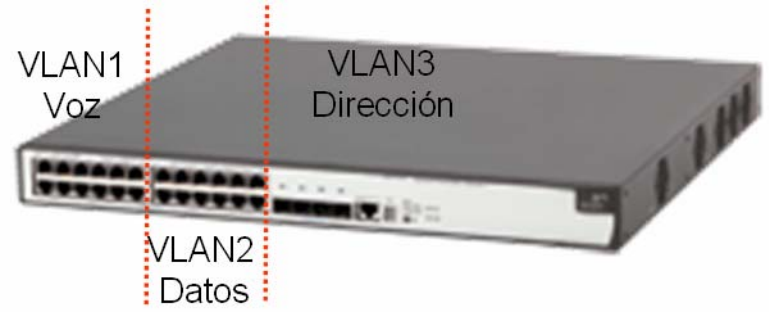


Figura 1.35. Muestra la creación de VLANS en un switch.

IEEE 802.1q

802.1q es un estándar de la IEEE que provee la calidad de servicio (QoS) en redes basadas en 802. Las etiquetas de VLAN están en todos paquetes de capa 2, pero no en paquetes que se originan en la NCP de capa 3 (ej: El control, HTTP, etcétera).

Cuatro bytes son añadidos a una trama de Ethernet, incrementando el tamaño de la trama máximo de 1518 a 1522 bytes.

Figura 1.36. Muestra el campo de 4 bits en el paquete IP, para dar calidad de servicio.

802.1p

802.1p es definido dentro de 802.1q. Tres bits son usados para permitir ocho niveles de prioridad (QoS) y 12 bits son usados para identificar hasta 4096 VLANS. 802.1p define el protocolo de registro de atributos genéricos (GARP) y el protocolo de registro de VLAN de GARP (GVRP). GARP deja a los clientes pedir la admisión en un dominio de multicast. GVRP los deja registrar en una VLAN.

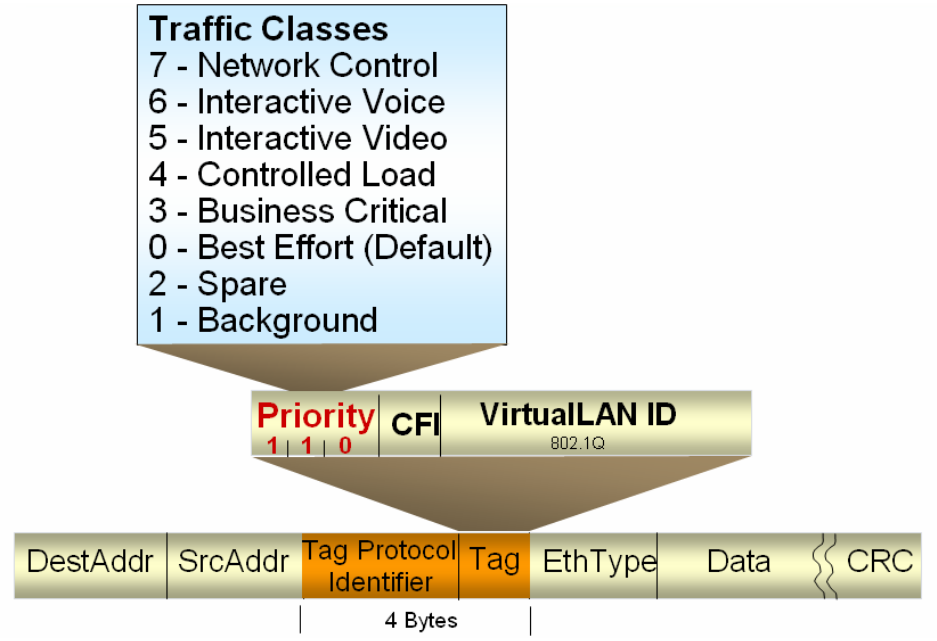


Figura 1.37. Muestra los ocho niveles para dar prioridad a la voz.

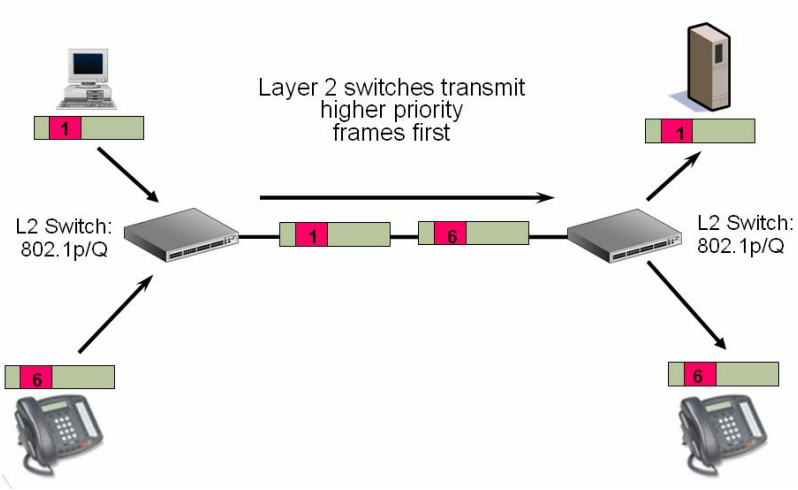


Figura 1.38. Muestra un ejemplo de cómo los paquetes de voz tienen prioridad sobre los paquetes de datos comunes.

Tipo de Servicio (ToS)

ToS de IP es usado para QoS y es invocado automáticamente cuando se selecciona VLAN tagging sobre la NBX. El encabezamiento IP tiene 3 partes de prioridad y 3 tipos de partes del servicio (delay, throughput y confiabilidad). Para funcionar en capa 3, los teléfonos de NBX insertan el valor hexadecimal B8 en el campo del ToS (decimal 184 = archivo binario 10111000). Los ruteadores de red de área extendida están esperando la configuración de prioridad de ToS de IP. TOS es usado en todos los paquetes, en ambas capas 2 y 3. Así que, todos paquetes son etiquetados en la VLAN excepto paquetes de control del NCP en capa 3, que son etiquetados con prioritización de ToS de IP.

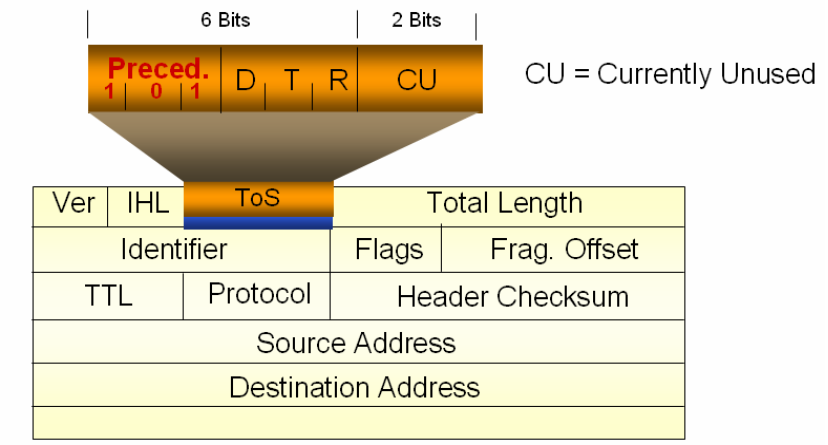


Figura 1.39. Muestra los 8 bits que son asignados para ToS para dar calidad de servicio a la red.

Differentiated Services (DiffServ)

El campo de DSCP bajo DiffServ reemplaza los campos de bits de ToS / prioridad campos de bits debajo de IP ToS. DiffServ fue desarrollado por la Agrupación de Ingeniería para Internet (IETF).

DiffServ proporciona un estándar de encabezamiento de paquete de IP a una manera usual de demostrar el nivel de prioridad en el tipo de servicio (ToS). Ruteadores usan DiffServ para leer paquetes de capa 3 para transmitir a través de teléfonos de la NBX el valor decimal 184 en el nivel de prioridad.

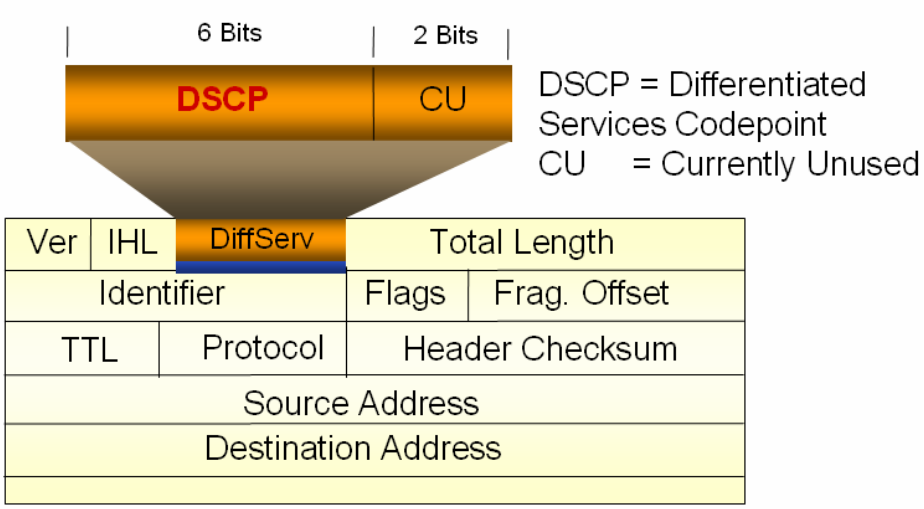


Figura 1.40. Muestra los 6 bits que son asignados para DSCP en el paquete IP.

1.14.2 Supresión de Silencio

El NBX puede retirar paquetes de una sesión que no contienen datos de voz y reemplazarlos con paquetes mucho más pequeños que contienen un indicador de silencio. Esto es llamado la supresión de silencios. El dispositivo receptor genera paquetes de ruido de Comfort durante las pausas de la conversación, como se lo muestra en la figura 1.41.

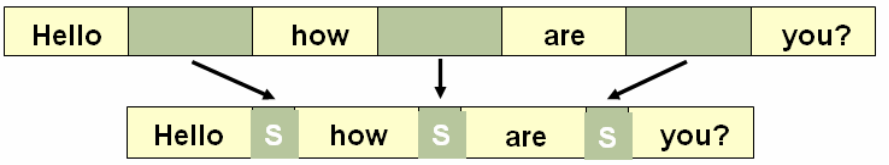


Figura 1.41. Muestra como es aplicada la supresión de silencios, en una llamada IP.

CAPÍTULO II

REDES LAN

2.1 PROTOCOLOS DE REDES LAN PARA IMPLEMENTAR CONVERGENCIA

Dado que la convergencia es la capacidad de una red de datos de soportar servicios de voz, datos y otros contenidos de valor, es importante entender los protocolos que deben ser implementados en la red con la finalidad de manejar calidad de servicio, evitar el aumento de niveles de colisiones en la red, evitar congestión de datos (la congestión equivale a pérdida de paquetes, debido a los buffers de tamaño limitado en las redes alámbricas) y garantizar disponibilidad de servicios.

Desde entonces hasta la actualidad, parecería que la única cosa que no se puede enviar por la red es la materia, con el incremento de servicios y aplicaciones sobre la red de datos, es importante preparar la red para modelar el tráfico de datos para evitar congestión y mantener servicios de calidad.

Nos remontamos a la historia debido a que los problemas de red tienen mucho que ver con su evolución así que iremos indicando los problemas que fueron surgiendo y los protocolos utilizados para resolverlos. Obviamente la resolución de estos inconvenientes logra tras la evolución de las redes, la capacidad de implementar convergencia.

Se lo debe modificar parámetros de la trama *ethernet* o el encabezado IP, manejando los puertos TPC/UDP, etc.

La primera regla para implementar redes convergentes es manejar estándares y no protocolos propietarios ya que estos dificultan la interoperabilidad, las modificaciones en los datos deben realizarse respetando los parámetros establecidos por la IEEE (IEEE corresponde a las siglas de *The Institute of Electrical and Electronics Engineers*, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación e ingenieros en telecomunicación) de tal forma que antes de empezar es importante entender la trama *ethernet*.

Nos referiremos al día de hoy al Standard IEEE 802.3 (tambièn referido como Ethernet II), es importante tener en cuenta que la trama *ethernet* es diferente a la trama IEEE 802.3 y ambas son incompatibles entre sí.

2.1.1.- IEEE 802.3

Ethernet usa un método de acceso al medio por disputa (*contention*). Las transmisiones son difundidas en el canal compartido para ser escuchadas por todos los dispositivos conectados, solo el dispositivo de destino previsto va a aceptar la transmisión. Este tipo de acceso es conocido como CSMA/CD.

El estándar IEEE 802.3 especifica el método de control del medio (MAC) denominado CSMA/CD por las siglas en ingles de acceso múltiple con detección de portadora y detección de colisiones (*carrier sense multiple access with collision detection*). CSMA/CD opera de la siguiente manera:

- Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.
- Si el medio esta tranquilo (ninguna otra estación esta transmitiendo), se envía la transmisión.
- Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.

- Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.
- Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión.
- Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión. Esto se conoce como el tiempo de *back off*.
- Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

Al hablar de convergencia, estamos aumentando el número de *hosts* en la red de datos, por lo tanto se aumenta la probabilidad de tener colisiones en la red, por lo tanto el primer protocolo que vamos a analizar es el relacionado con las redes virtuales (en adelante conocidas como VLANS). El estándar de la VLANS es IEEE 802.1Q. Estudiaremos este protocolo primero debido que a través de VLANS reducimos el dominio de colisiones en la red. O sea, podemos tener redes gigantes pero si están separadas por VLANS es como si tuviésemos redes muy pequeñas, al disminuir los dominios de colisiones evitamos tiempos de *back-off* y con ello evitamos que se aumente la latencia de la red. Es importante mantener la latencia (retardo de red) lo más pequeña posible debido a que las aplicaciones convergentes muchas veces requieren ser transmitidas a tiempo real.

Antes de entrar al estándar IEEE 802.1Q, hay un campo del formato de la trama IEEE802.3 que debemos tener en cuenta, esto es, el campo que indica si la información es *Unicast, multicast o Broadcast*.

Si la dirección se referencia a una sola estación, se conoce como *Unicast*, si se referencia a un grupo de estaciones limitado es *Multicast*, y si es a todos es *Broadcast*.

Al hablar de convergencia nos interesa manejar *muticast* para todo lo que son conferencias, paging, descubrimiento de nuevos teléfonos IP, etc. Por lo tanto debemos cuidarnos de que primero, el *musticast* no se transforme en *broadcast* (inundación de la

red) y segundo, que el *multicast* no sea cortado por los elementos activos. (por ejemplo, cuando usamos el protocolo de seguridad para túneles VPN, se utiliza IPSec, pero este protocolo no soporta *multicast*, por lo tanto hay que buscar la manera de convertir la información a *unicast* –una sola dirección-, transmitirla a través de IPSec y del otro lado convertir el *unicast* nuevamente en *multicast*, esto se lo logra a través de un protocolo llamado GRE, estos métodos y lo que configuramos en la solución se lo verá más adelante)

2.1.2 IEEE 802.1Q

Cuando crece el número de *hosts* en la red, aumenta el número de colisiones, por lo tanto aumenta el número de tiempo de *back-off´s* (tiempos aleatorios durante los cuales no se transmite información). El único mecanismo que existe para reducir el número de colisiones es dividiendo la red en redes virtuales VLANS

Como podemos ver en la figura 2.1 una red plana es aquella donde todos los computadores comparten un solo dominio de colisiones, entonces mientras más grande la red, mayor el dominio y mayor la latencia de la red (menor la velocidad).

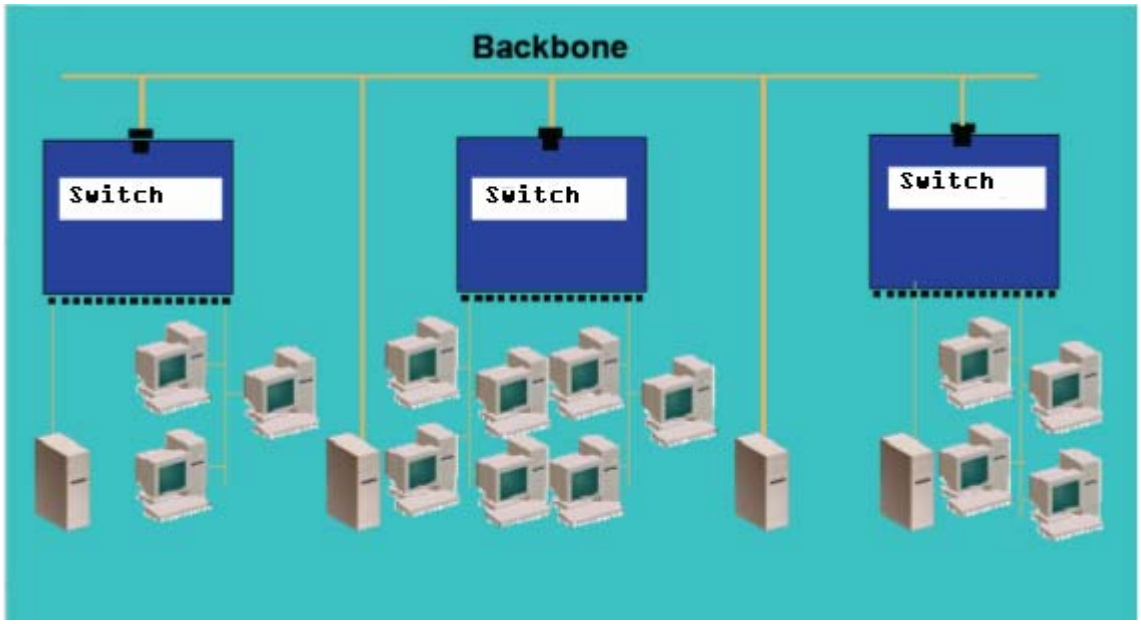


Figura 2.1. Muestra una red con un solo dominio de colisiones.

Lo que vamos a realizar ahora es dividir la red en 4 VLANS (figura 2.2), varios computadores estarán conectados a una VLAN específica, sin importar el lugar en el que estén, entonces los dominios de colisiones disminuyen porque no existe paso de datos entre las VLANS, sin embargo existen equipos que requieren ser vistos en todas las VLANS, parta ello, lo que hacemos es que pertenezcan a un puerto que pertenece a todas las VLANS, estos puertos son generalmente servidores especiales y enlaces entre switches, para que la VLAN 1 pueda conversar con la VLAN 2, 3 y 4 lo que se hace es realizar subredes, cada una con una puerta de enlace y a través de sus respectivas puertas de enlace se transmite la información entre VLANS de tal forma que si existen 4 VLANS, habrá 4 puertas de enlace que transmitirán la información entre subredes. Por ello, el switch que posea las puertas de enlace (en adelante las llamaremos *gateways*) debe ser muy robusto, y veloz, con alta disponibilidad y redundancia ya que toda la carga de la red estará sobre este dispositivo. Es importante que este switch principal, denominado switch de *CORE* posea enrutamiento basado en hardware para que no se degrade en nada la velocidad de la red al implementar VLANS y se mantenga la denominada velocidad de *wirespeed*.

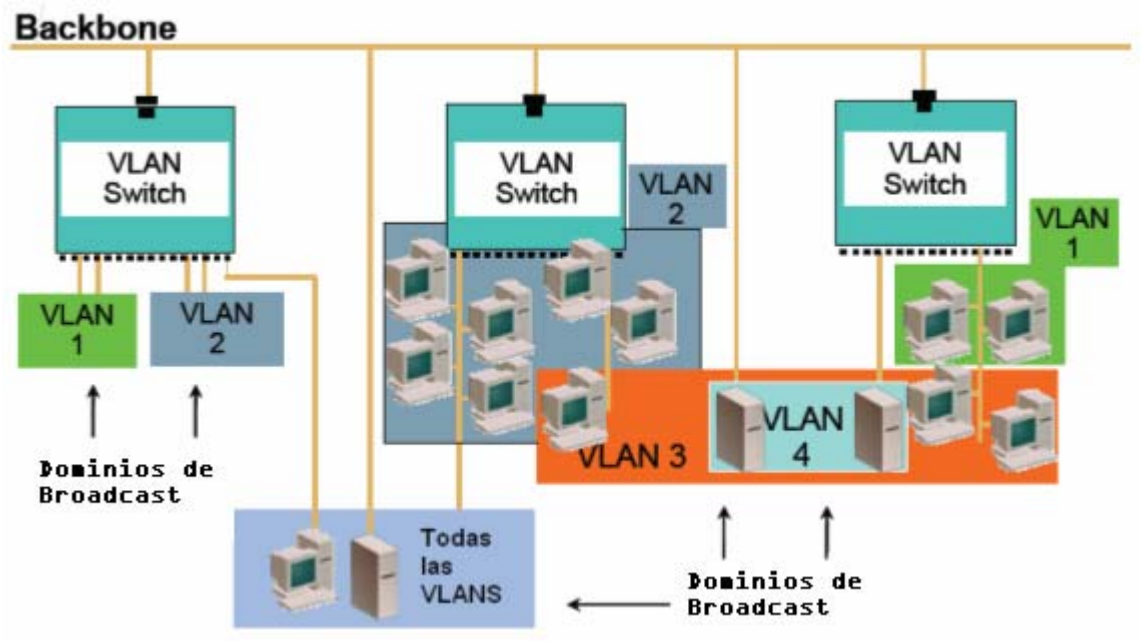


Figura 2.2. Muestra una red dividida en 4 VLANS.

En el ejemplo anterior, si requerimos 4 VLANS y un máximo de 30 hosts en cada VLAN usaremos una red de capa 3 clase C. (mayor información de estos cálculos, remontarse al capítulo de diseño de red).

La VLAN 1 tendrá el siguiente *gateway*: 192.168.0.33 con máscara 255.255.255.224
La VLAN 2 tendrá el *gateway*: 192.168.0.65
La VLAN 3 tendrá el *gateway*: 192.168.0.97
La VLAN 4 tendrá el *gateway*: 192.168.0.129

Por lo tanto un computador de la VLAN 1 tendrá la dirección 192.168.0.34 con máscara 255.255.255.224 y *gateway* 192.168.0.33

Un computador de la VLAN 2 tendrá la dirección 192.168.0.66 con máscara 255.255.255.224 y gateway 192.168.0.65

Cuando un computador de la VLAN 1 desea comunicarse con la VLAN 2 lo que hace es entregar la información al *gateway* de la VLAN 1, el *gateway* de la VLAN 1 se comunica con el *gateway* de la VLAN 2 y se entregan mutuamente la infomación, por lo tanto para comunicarse entre toda la red de 4 VLANS con 30 usuarios en cada una (total de 120 *hosts*) en lugar de esperar que los 119 *hosts* no estén transmitiendo datos para transmitir información, un PC tiene que esperar que tan solo los otros 29 no estén usando el canal y el *switch* de *core* a través de sus *gateway*s se encargan de transmitir la información de forma ordenada para que no existan colisiones en la red. O sea que hemos conseguido que una red de 120 *hosts* se vea (a nivel de dominio de colisiones y *broadcast*) como una red de 30 *hosts*. Mientras más pequeño el dominio de colisiones mayor la velocidad de la red. Debemos tener en cuenta que el número de *gateway*s utilizado debe también ser pequeño porque si aumentamos demasiado el número de VLANS consumimos mayores recursos de procesamiento en el hardware y podemos afectar el rendimiento de los equipos. Por lo tanto siempre hay que buscar un equilibrio.

Las VLANS poseen dos componentes denominados: membresía e identificador, los mismos que son definidos a continuación.
La membresía define la manera en que los miembros son seleccionados. Hay dos maneras de asociar a los miembros, etiquetado o no etiquetado.

Un miembro etiquetado posee bits adicionales en la trama que un miembro no etiquetado, como se lo muestra en la figura 2.3, por lo tanto si en un extremo hemos etiquetado el puerto, debemos etiquetar al otro lado también caso contrario se perderán todos los datos.

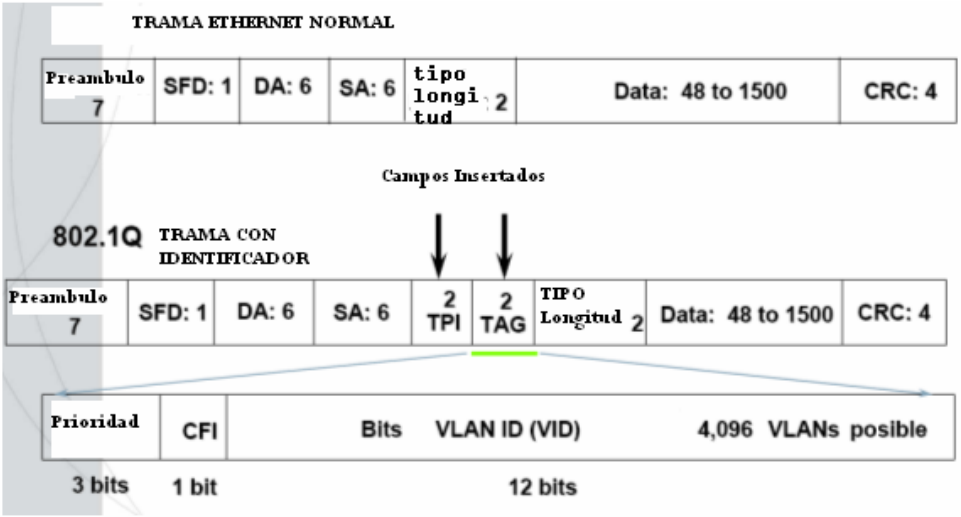


Figura 2.3. Muestra las tramas con y sin etiquetas.

La etiqueta es el número de la VLAN y solo dicha VLAN puede pasar por ese puerto. Cuando hemos etiquetado el puerto, todas las VLANS que han sido etiquetadas en el puerto podrán ser transmitidas por allí.

Por ejemplo si en el puerto son etiquetados las VLANS 2 y 3, puede pasar por ese puerto información de esas VLANS pero no podrá pasar información de la VLAN 4

Cuando un puerto ha sido no etiquetado, significa que puede pertenecer a una y solo una VLAN.

Un puerto que debe pertenecer a varias VLANS debe pertenecer a una VLAN de forma no etiquetada y las otras VLANS a las que pertenece deben estar puestas de forma etiquetada sobre el puerto.

Para realizar convergencia, se realizan diferentes VLANS para los usuarios basado en el número de *hosts*. Se crean VLANS diferentes para las aplicaciones, por ejemplo la telefonía IP estará en la VLAN 5, video en la VLAN 6 etc,

La convergencia significa compartir el medio físico, por lo tanto el punto de red servirá tanto para el teléfono IP como para el computador conectado como se muestra en la figura 2.4

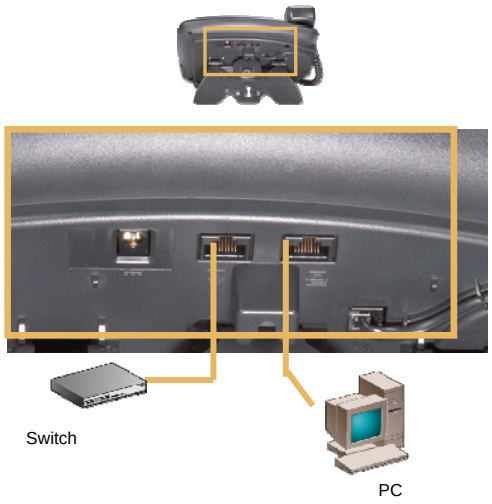


Figura 2.4. Puertos del teléfono IP, conexión al switch y al computador.

El puerto del *switch* debe estar etiquetado en la VLAN de telefonía (5) y debe pertenecer a la VLAN del PC en forma no etiquetada.

Ahora, existe la posibilidad de manejar los miembros dentro de dos tipos de VLANS: VLANS basadas en puerto y VLANS basadas en protocolo pero estos protocolos no interesan para la parte de convergencia, dentro de VLANS lo que nos interesa conocer es un mecanismo conocido como la VLAN automática. Esto se lo verá a continuación.

2.1.3 Asignación automática de la VLAN para telefonía IP y equipos de aplicaciones convergentes.

Si tenemos un teléfono IP, queremos que este se ubique en la VLAN de voz, sin importar la ubicación de este dispositivo, para realizar esto se puede configurar el switch para que detecte la dirección mac del dispositivo conectado y en caso de coincidir con la dirección mac del fabricante de la telefonía IP, el dispositivo será ubicado en la VLAN de voz sin perder la VLAN de datos porque al teléfono se le conectará un computador.

Para ello, el puerto del switch debe ser híbrido, y se debe pedir que detecte los 6 primeros caracteres hexadecimales que corresponden al fabricante OUI (número solicitado por los fabricantes a la IEEE, que les asigna un número de 3 octetos para, en adelante, identificar las tarjetas del fabricante; es el OUI "*Organizationally Unique Identifier*", también conocido como código de vendedor).

2.1.4 Asignación automática de VLAN según el usuario

En los switches, generalmente se configuran los puertos de los usuarios para pertenecer a una VLAN, sin embargo ha crecido la movilidad de los usuarios dentro de las empresas, debido a la proliferación de computadoras portátiles.
Por ejemplo, un usuario se conecta al puerto de la sala de reuniones, y esta está configurada como VLAN 4, tendrá todos los privilegios y restricciones de la VLAN 4, si este usuario es un gerente y la VLAN 4 no tiene acceso a la VLAN de gerencia, entonces el gerente perdió todos sus privilegios de red que tenía en su escritorio.

Por otro lado, una persona de recursos humanos encuentra un punto de red y se conecta, ese puerto estaba configurado en la VLAN de gerencia, entonces la persona de recursos humanos tiene acceso a recursos que no debería tener (los recursos de gerencia).

Existe un mecanismo llamado administración de acceso a la red NAM (*Network Access Management*), en donde el switch se comunica con el servidor de directorios activos (Active Directory de Microsoft). Esta comunicación sirve porque el directorio activo posee la información del nombre de usuario y contraseña de la persona, la VLAN a la que pertenece, el perfil de calidad de servicio y nivel de seguridad de debe tener,

entonces una vez que se registra en el directorio, el puerto del switch es automáticamente configurado para darle al usuario los privilegios y restricciones que debe tener, ni más ni menos.

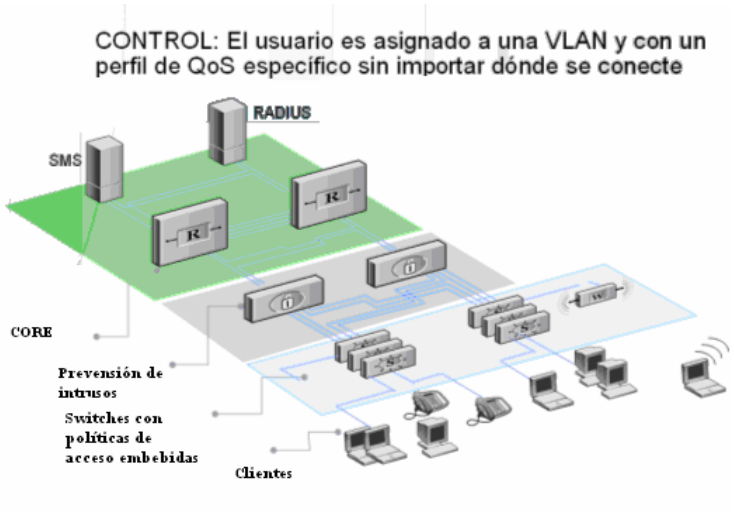


Figura 2.5. Manejo de acceso a la red, mediante el servidor de directorios activos.

Los teléfonos son colocados automáticamente en la VLAN de voz, los pc´s no tienen acceso de red hasta que sean autenticados, las impresoras de red por ejemplo son colocadas en la VLAN de impresoras y han sido identificadas por su dirección mac a través de RADA.

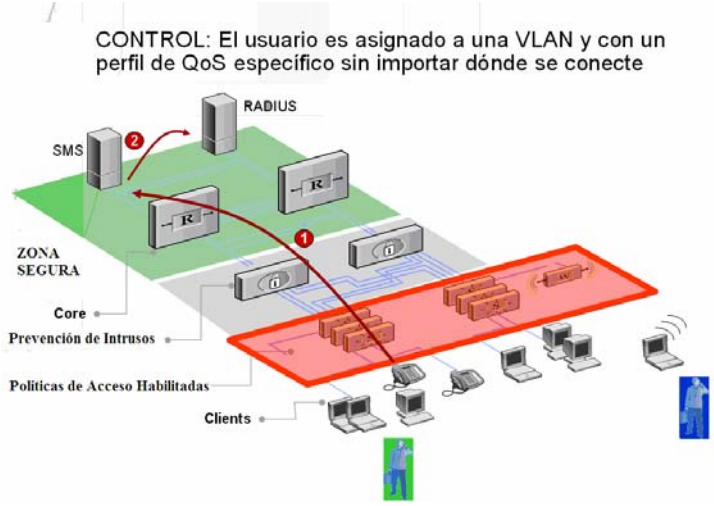


Figura 2.6. Muestra como un teléfono es autenticado en el servidor RADIUS.

El usuario conecta su computador a la red y es obligado a identificarse con su nombre de usuario y contraseña antes de entrar a la red. El nombre de usuario y

contraseña es analizado por el IAS del *Active directory* y se le asigna una VLAN, un perfil de calidad de servicio y un nivel de seguridad de forma automática.

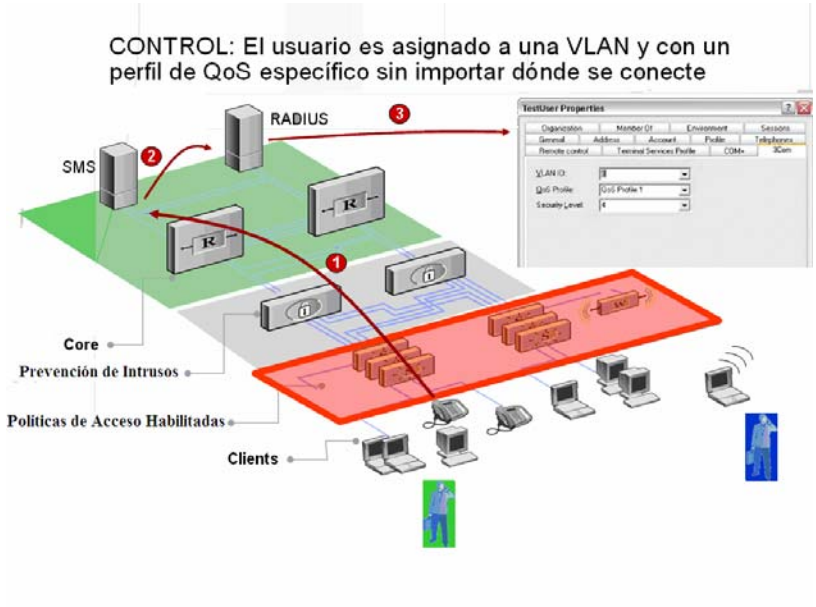


Figura 2.7. Muestra como un teléfono es autenticado en el servidor RADIUS, y como es asignado al perfil que pertenece.

El usuario tiene ahora sus permisos y restricciones, sin importar en que puerto de la red se encuentre, va a tener el mismo perfil.

2.2 PRIORIZACIÓN DE TRÁFICO Y CALIDAD DE SERVICIO EN LA RED

2.2.1 Perdida de paquetes, retardo y jitter.

Debido a la prioridad de flujo y a los picos de tráfico, los equipos de la red pueden perder paquetes de datos y producir retardos en la transmisión. Estos paquetes perdidos son retransmitidos y de este modo no se pierde información. Mientras las aplicaciones de datos no suelen verse afectadas, la voz sobre IP, si es muy sensible a estas perdidas. Concretamente, se ve muy afectada a partir de un 5% de paquetes perdidos.

El factor retardo, definido como el tiempo de transito de los paquetes desde el origen al destino y vuelta, influye asimismo en la calidad del servicio. A partir de cierto umbral puede empezar a ser incómodo mantener una conversación. Para una calidad

alta el retardo debería mantenerse por debajo de 150ms. Para una calidad media, por debajo de 400ms.

El jitter se define como la variación del tiempo de tránsito de los paquetes. No todos los paquetes sufren un retardo constante. Este retardo variable o jitter disminuye la calidad de la voz al superar el umbral de los 50ms.

La calidad de la voz resultante depende de la combinación de estos tres parámetros:

	Calidad Alta	Calidad Media	Calidad Baja
Pérdida de paquetes	1%	3%	5%
Retardo	150ms	400ms	600ms
Jitter	20ms	50ms	75ms

2.2.2 IEEE 802.1p CoS.

IEEE 802.1p es un estándar que provee modelamiento de tráfico y filtrado multicast a nivel de capa 2 (Mac Level)

La trama ethernet posee un campo de 3 bits por lo tanto hay 8 niveles diferentes de clases de servicio, estos bits se encuentran dentro del encabezado IEEE 802.1Q.

Todos los datos se tratan a través de la red con prioridad 000 conocida como mejor esfuerzo (best effort) y se puede cambiar estos parámetros para dar mayor prioridad de tal forma que un paquete identificado con los bits 111 tendrá más prioridad que uno marcado con 100 y este último tendrá mayor prioridad que el default 000.

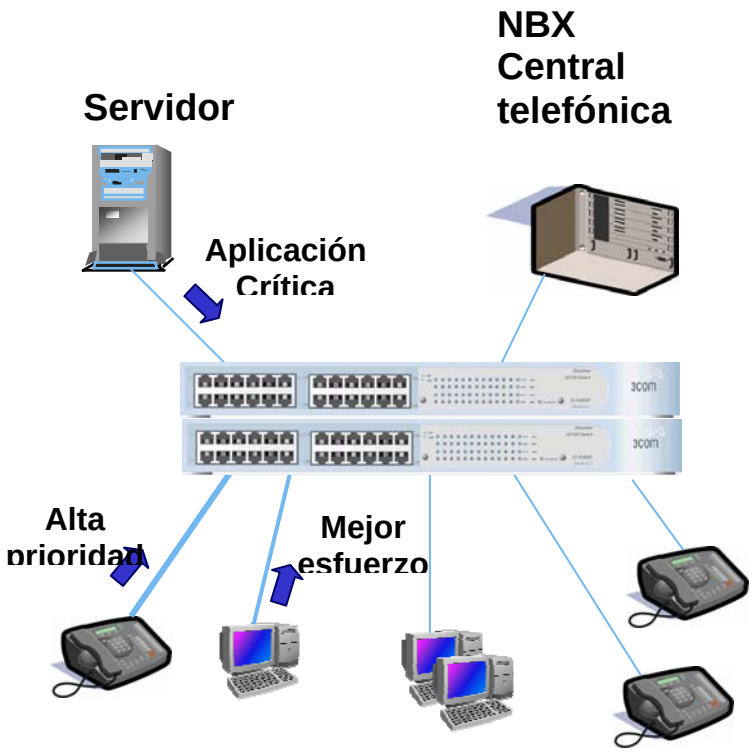


Figura 2.8. Niveles de clase de servicio de diferentes equipos en la red.

A continuación la Tabla 2.1 muestra los valores de priorización de tráfico cuando se utiliza CoS sobre la red.

TABLA 2.1

PRIORIDAD 0	DEFECTO: MEJOR ESFUERZO
PRIORIDAD 1	RESERVADO: "MENOR QUE" MEJOR ESFUERZO
PRIORIDAD 2	RESERVADO
PRIORIDAD 3	RESERVADO
PRIORIDAD 4	RETARDO SENSITIVO, NINGÚN SALTO
PRIORIDAD 5	RETARDO SENSITIVO, SALTOS DE 100 ms
PRIORIDAD 6	RETARDO SENSITIVO, SALTOS DE 10 ms
PRIORIDAD 7	CONTROL DE RED

CoS prioriza el tráfico pero no garantiza priorización de aplicaciones o rendimiento, para ello se requiere de QoS

2.2.3 Calidad de Servicio.

Según el comité de estándares industriales IETF, QoS provee la habilidad de priorizar tráfico basado en el nivel de servicio requerido. Este nivel de servicio puede

ser marcado en la infomación de cada paquete IP en el campo de Tipo de servicio (TOS).

Para configurar Calidad de servicio se deben definir los siguientes parámetros en los equipos activos:

- *Classifier*: clasifica el tráfico de la red por protocolo, aplicación, origen, destino, etc.
- *DiffServ Code Point (DSCP):* son los bits de priorización de tráfico dentro del encabezado IP, estos están codificados por cada aplicación específica e indican el nivel de servicio requerido en la red para esa aplicación.
- *Service Level:* define la prioridad que será entregada a un grupo de tráfico clasificado
- Policy: es una serie de reglas que son aplicadas a la red para que esta satisfaga las necesidades del negocio.
- QoS profile: son múltiples reglas que son asignadas a un puerto específico del equipo activo.

Para manejar Calidad de Servicio todos esos parámetros deben ser configurados en los equipos activos.

Hay dos mecanismos que se pueden usar para lograr lo anterior, estas no son mutuamente excluyentes y pueden ser utilizadas juntas:

2.2.4 Reservación de recursos.

IntServ es utilizado en la parte wan de la red para que sea una infraestructura robusta, los recursos de la red son reservados según el pedido de la apliación según lo que se haya configurado en los parámetros de QoS, para esto se utiliza el protocolo RSVP (Resource Reservation Setup Protocol)

Este modelamiento de tráfico se lo hace por cada flujo de la red (un data stream unidireccional e individual), se lo identifica porque cada una de estas caraterísticas:

protocolo de transporte, dirección de origen, número de puerto de origen, dirección destino, número de puerto del destino.

2.2.5 Priorización.

Es un método simple pero eficiente, 6 bits son introducidos en cada paquete y este campo toma el nombre de diffserv.

Funciona para varios flujos (consume menos recursos del sistema, por eso se considera más eficiente), se lo identifica porque cumple una o varias de estas caraterísticas: protocolo de transporte, dirección de origen, número de puerto de origen, dirección destino, número de puerto del destino.
Generalmente es implementado en la parte LAN de la red.

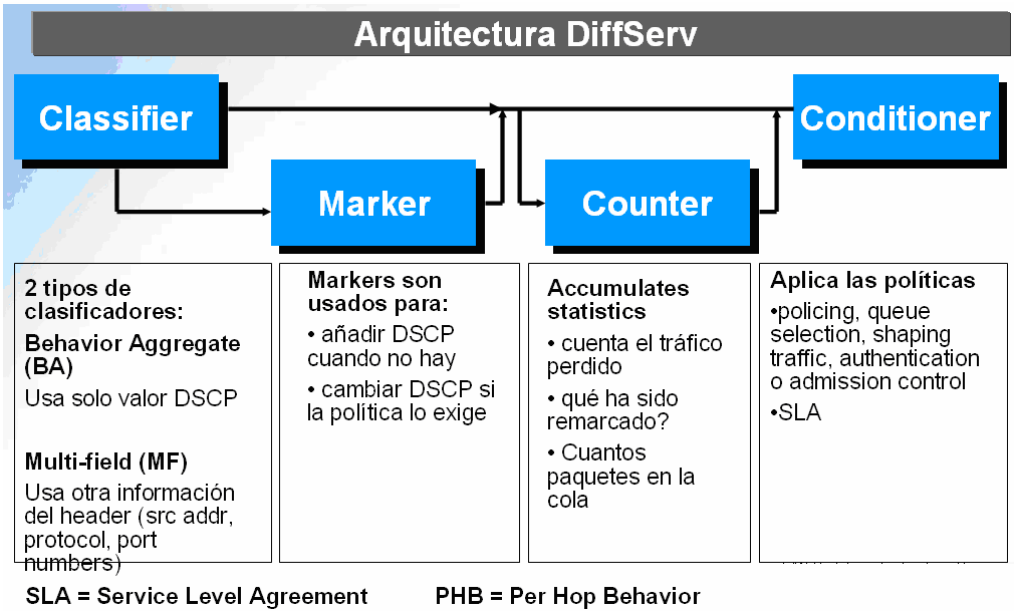


Figura 2.9: Funcionamiento de *DiffServ*

Componentes de la arquitectura de *DiffServ*:

DiffServ PHB.

Define el comportamiento de cada paquete, se refiere a la calendarización, encolamiento, políticas y modelamiento *(shaping).*

El PHB es el selector de clase y puede tener 2 tipos de uso, como AF y como EF

AF: Assured Forwarding, compuesto por 6 bits, definen la precedencia para hacer un dump de los paquetes como lo muestra la siguiente tabla:

Tabla 2.2 Muestra el nivel de precedencia en diferentes clases.

PRECEDENCIA DE CAIDAS	CLASE 1	CLASE 2	CLASE 3	CLASE 4
PRECEDENCIA DE CAIDAS BAJAS	OO1O1O	O1OO1O	O11O1O	1OOO1O
PRECEDENCIA DE CAIDA MEDIA	OO11OO	O1O1OO	O111OO	1OO1OO
PRECEDENCIA DE CAIDA ALTA	OO111O	O1O11O	O1111O	1OO11O

Donde la clase 1 es la de menor prioridad y precedencia de caidas bajas es la condición de menor prioridad, por lo tanto si la cola del buffer esta llena y hay que botar un dato, si los siguientes son los AF de los datos en la cola: 001010 010100 011110 el dato a ser eliminado es el que tenga el AF 001010

EF: ***Expedited Forwarding***

Compuesto por 6 bits que son siempre los mismos. Este parámetro puede ayudar a garantizar baja pérdida, baja latencia y bajo jitter. El valor es siempre 101110.

Podemos clasificar distintos tipos de aplicaciones, colocamos sobre la red voz, TACACS (autenticación de seguridad), SAP (aplicación de contabilidad muy usado en *retail*), *Oracle* (base de datos), *Lotus (e-mail)*, http (navegación de Internet), lo que pedimos al equipo activo es que meneje los paqutes de voz con la máxima prioridad, después *Oracle, TACAS* y *SAP*, después de ello la parte de seguridad de *Lotus Notes*, después el *e-mail*, la replicación de *Lotus Notes* y finalmente Internet, de tal manera que se puede tener degradación en la velocidad de navegación por web pero la telefonía IP siempre será a tiempo real en la red.

Tabla 2.3: Muestra los paqutes de voz con el valor de DSPC más alto, para asignar la prioridad más alta con respecto a otras aplicaciones.

PHB	Description	Traffic Type	DSCP Value (DEC)	DSCP Value (BIN)
EF	Expedited Forwarding	Voice	46	101110
AF11	High Priority Low Drop Precedence	TACACS, SAP, Orcale	10	001010
AF21	Medium Priority Low Drop Precedence	Lotus Notes (security)	18	010010
AF22	Medium Priority Medium Drop Precedence	Lotus Notes (normal email)	20	010100
AF23	Medium Priority High Drop Precedence	Lotus Notes (replication)	22	010110
AF31	Low Priority Low Drop Precedence	HTTP	26	011000

2.3 POWER OVER ETHERNET IEEE 802.3AF.

IEEE 802.3af Power obver ethernet es un mecanismo de brindar alimentación eléctrica sobre Ethernet para teléfonos IP y otros dispositivos que lo requieran como access points, cámars IP, etc. Los sistemas de alimentación ininterrumpida y las configuraciones desarrolladas de forma inteligente aumentan la fiabilidad y permiten el uso de tecnología en entornos de alta disponibilidad.

Hasta ahora, casi todos los equipos terminales compatibles en red tomaban la energía a través de una unidad de alimentación enchufada a una toma. Estos convertidores, que son de calidad inferior a la que provee un switch Power over ethernet, no sólo consumen una gran cantidad de electricidad debido a su limitado rendimiento, sino que restringen también la capacidad de ampliación del equipo terminal. Ello puede resultar caro. Por ejemplo, si no hay ningún enchufe en el lugar en el que desea instalar un punto de acceso WLAN, habrá que extender primero la red de alimentación. Adicionalmente que se requiere, para contingencia y respaldo de energía, UPS distribuídos y es mucho más sencillo respaldar únicamente el Switch a través de UPS centralizados.

Con el uso de esta tecnología se puede establecer una fuente de alimentación de energía a un equipo terminal compatible en red desde una unidad de alimentación

ubicada en el distribuidor del piso a través de cables Ethernet estándar. Junto con las fuentes de alimentación ininterrumpida en el distribuidor, esto no sólo asegura una mayor fiabilidad de funcionamiento, sino que también permite la instalación de puntos de acceso WLAN o cámaras de vídeo IP en lugares que antes resultaban inaccesibles.

Power over ethernet ayuda a aumentar la cantidad de elementos utilizados en una red convergente. Entre ellas cabe incluir los lectores RFID (Identificación por radiofrecuencia), dispositivos de seguridad como sistemas de alarma (detectores de humos), controles de acceso (por ejemplo, lectores de tarjetas de identificación) o escáneres de códigos de barras en cajas.

2.3.1 Alimentación a través de la red: el estándar PoE

El proceso de estandarización de la Telealimentación sobre Ethernet (PoE) comenzó en el año 1999, impulsado por empresas como 3Com, Intel, PowerDsine, Nortel, Mitel y National Semiconductor. En junio de 2003, los esfuerzos realizados por el Comité IEEE culminaron en la ratificación del estándar común 802.3af. Bajo "Equipo Terminal de Datos (DTE) accionado a través de una Interfaz Dependiente del Medio (MDI)", describe cómo la salida eléctrica se suministra a través de un cable LAN Ethernet al equipo terminal conforme con el estándar. Antes de este acuerdo sólo existían soluciones patentadas, por ejemplo del gigante en redes Cisco. Hoy día, el estándar PoE ha quedado estipulado para tecnologías Ethernet con velocidades de transferencia de datos de 10/100 MBit/s (Ethernet y Ethernet rápido). Puede descargar una copia gratuita en [http://standards.ieee.org/getieee802/download/802.3af-2003.pdf].

PoE se aprovecha de que el cobre puede conducir portadoras de carga eléctrica. Esto ofrece al cableado del piso una ventaja sobre las conexiones ópticas, ya que no sería posible suministrar energía al equipo terminal utilizando fibras ópticas. El 802.3af subdivide el equipo involucrado en el equipo de fuente de alimentación (PSE) y los consumidores o dispositivos alimentados (PD).

En la versión actual, con una tensión de CC de 48 voltios por puerto, se suministra una salida de 15,4 vatios. Dada la longitud máxima permitida del cable de

100 metros, parte de la tensión se pierde debido a la resistencia óhmica del cable de cobre, lo que significa que el equipo terminal conectado puede consumir un máximo de poco menos de 13 vatios (o, para ser más exactos, 12,95 vatios). Eso corresponde a un requisito de potencia máxima durante un funcionamiento continuo de 350 mA, si bien están permitidos 400 mA durante un corto período de tiempo cuando se enciende por primera vez el equipo.

El estándar PoE también establece un método de handshake conocido como "detección de potencia". Antes de que la unidad de alimentación encienda el equipo, comprueba, a través de la conexión de datos, si el equipo terminal conectado cumple el estándar 802.3af. Al equipo sólo se le suministra energía en caso de que la respuesta recibida sea afirmativa. De este modo, se puede evitar el peligro de fundir la tarjeta de red del PC, por ejemplo.

2.3.2 Midspan y endspan.

Un cable Ethernet tiene ocho conductores a modo de pares trenzados, y cada uno de los cuatro pares puede transmitir señales simétricas. No obstante, una Ethernet de 10/100 MBit/s sólo utiliza los hilos 1, 2, 3 y 6. Con el estándar PoE se pretende, por tanto, que se utilice el resto de las fibras para el suministro de CC. En un principio estaba previsto que los pares 4-5 se conectaran al polo positivo y los pares 7-8 al polo negativo de la fuente de tensión. De hecho, una adaptación del estándar significa ahora que pueda haber también una polaridad inversa.

En la PoE hay dos métodos de transmisión de energía:

El primero utiliza los pares no usados del cable TP, mientras que el segundo proporciona la energía a través de las líneas que trasmiten también el tráfico de datos.

La primera variante se utiliza en dispositivos "midspan": un controlador Midspan se puede comparar con un panel de conexiones mejorado de modo que incluya la opción de suministrar energía a través de una unidad de alimentación independiente a las líneas procedentes del conmutador y que llegan al equipo terminal. Al mismo

tiempo, aísla los componentes activos de la red (generalmente conmutadores) de la tensión de CC presente en el cable. Esto funciona a velocidades de hasta 100 MBit/s, a saber, para Ethernet rápida, y es adecuado para actualizar las instalaciones existentes o nuevas basadas en conmutadores Ethernet sin una funcionalidad PoE.

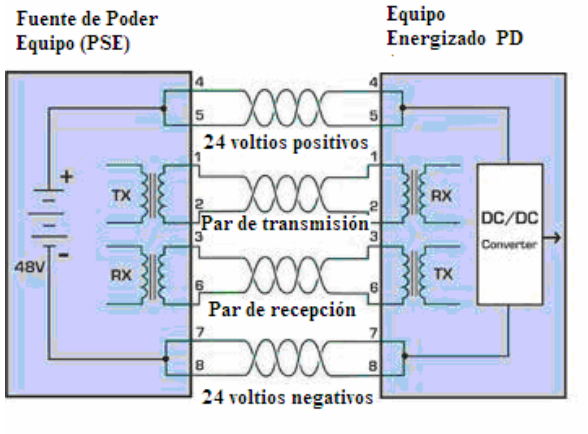


Figura 2.10: Suministro de energía PoE a través de un dispositivo Midspan

En la segunda variante, una fuente de tensión colocada directamente en el conmutador suministra energía a los pares del sistema de cables simétricos de 100 ohmios, que también lleva el tráfico de datos de la red. Las conexiones portadoras de datos 1-2 y 3-6 del cable Ethernet quedan aisladas galvánicamente de los contactos de los jacks presentes tanto en el conmutador como en el equipo terminal a través de unos transformadores. De este modo, la corriente continua puede ser alimentada fácilmente por el lado de salida del transformador. A esto se le denomina “endspan”.

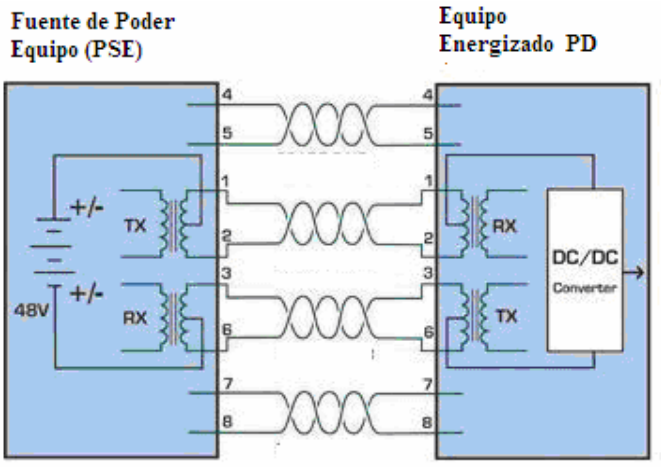


Figura 2.11. Suministro de energía PoE a través de un dispositivo Endspan.

Es muy importante tener en cuenta la potencia que soporta el switch y la potencia que consume cada uno de los teléfonos IP para poder dimensionar correctamente el equipo a ser adquirido. Por ejemplo los teléfonos IP para administradores (manager) ocupan mayor energía que los básicos y por ende si un switch va a tener sólo teléfonos básicos puede ser este más pequeño (hablando con respecto a la potencia que entrega) que uno que tenga que soportar todos los teléfonos tipo manager (que son a gigabit). Incluso a veces se requieren fuentes de poder redundantes externas para ciertas familias de switches.

2.4 PROTOCOLOS DE REDES LAN PARA IMPLEMENTAR SEGURIDAD

La importancia de la seguridad es garantizar 3 parámetros sobre la red: Integridad de los datos, Confidencialidad de la información y Alta disponibilidad de los servicios. Un parámetro adicional podría ser monitoreo.

Con la finalidad de garantizar estos parámetros se debe tener en cuenta los siguientes protocolos de extremo a extremo en la red de datos:

2.4.1 Protocolos que ayudan en la integridad de los datos:

Integridad significa que los datos no deben ser modificados de forma no autorizada. Ambientes con este atributo reforzado evitan esto tanto de atacantes como de errores que pueden cometer los usuarios.

Los principales problemas en seguridad son virus, bombas lógicas, back doors. Hay tres tipos de contaminación: corrupción, modificación maliciosa y reemplazo de datos válidos por errados.

Para combatir se provee sistemas de control de accesos, detección de intrusos y hashing. La mayor cantidad de compromisos a este parámetro se da por errores de los usuarios.

Al hablar de la red de datos (no de aplicaciones), los protocolos utilizados son los siguientes:

2.4.2 IEEE 802.1X.

Se utiliza en la capa de enlace de datos. Utilizado como control de accesos a los recursos de la red, permite la autenticación de dispositivos conectados a la red LAN, se pide una autenticación y en caso de ser verdadera, se establece una comunicación punto a punto, caso contrario se previene el acceso al puerto. De esta manera usuarios no autorizados no tendrán acceso a la red de datos.

2.4.3 ACL.

Las ACL son las Listas de Acceso, pueden ser configuradas en capas 2, 3 y 4, los parámetros utilizados para permitir o restringir recursos de la red sobre un perto específico son los siguientes:

- MAC address tanto de origen como de destino
- Tipo de trama ethernet
- Dirección IP tanto de origen o de destino
- Puerto TCP o UDP tanto de origen como destino
- Hora

De esta manera se puede llegar a la granularidad de permitir a un usuario ingresar desde la direccion IP 192.168.100.100 siempre y cuando la mac address sea 00:bb:1e:ff:14:46. Y tendra acceso al servidor 192.168.101.10 solamente usando la aplicación de video que maneja el puerto UDP 1234, si desea hacer un telnet o ftp a ese servidor, las peticiones serán negadas. Existe la capacidad de permitir esos parámetros por ejemplo desde las 12 am hasta las 6 pm (pero en el caso de la red que vamos a implementar no se soportarán listas de acceso basadas en horario por cuestión de presupuesto).

2.4.4 Protocolos que ayudan en la confidencialidad de los datos:

Confidencialidad significa que no es revelada información a quien no corresponda.

Mecanismos para romper este parámetro incluyen monitoreo de red, *shoulder surfing* (obtener información de las teclas aplastadas por algún usuario a través de

técnicas de espionaje), robo de archivos de contraseñas e ingeniería social (cuando se engaña a un usuario logrando que éste entregue información confidencial fingiendo ser una persona con derecho a dicha información).

La confidencialidad puede ser provista a través de encripción, *network traffic padding* (camuflaje de datos), control de acceso, clasificación de datos y entrenamiento al personal sobre los procedimientos apropiados.

Los protocolos que vamos a revisar corresponden a los de encripción y camuflaje de datos, estos protocolos son utilizados en redes inalámbricas y para acceso remoto de la red a través de Internet.

2.4.5 Protocolos de encripción de datos

WEP (incluído dentro de IEEE 802.11)

WEP (Wired Equivalent Privacy, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

El estándar IEEE 802.11 proporciona mecanismos de seguridad mediante procesos de autenticación y cifrado. En el modo de red Ad Hoc o conjunto de servicios avanzados, la autenticación puede realizarse mediante un sistema abierto o mediante clave compartida. Una estación de red que reciba una solicitud puede conceder la autorización a cualquier estación, o sólo a aquellas que estén incluidas en una lista predefinida. En un sistema de clave compartida, sólo aquellas estaciones que posean una llave cifrada serán autenticadas.

El estándar 802.11 especifica una capacidad opcional de cifrado denominada WEP (Wireless Equivalent Privacy); su intención es la de establecer un nivel de seguridad similar al de las redes cableadas. WEP emplea el algoritmo RC4 de RSA Data Security, y es utilizado para cifrar las transmisiones realizadas a través del aire.

Aunque los sistemas WLAN pueden resistir las escuchas ilegales pasivas, la única forma efectiva de prevenir que alguien pueda comprometer los datos transmitidos consiste en utilizar mecanismos de cifrado. El propósito de WEP es garantizar que los sistemas WLAN dispongan de un nivel de confidencialidad equivalente al de las redes LAN cableadas, mediante el cifrado de los datos que son transportados por las señales de radio. Un propósito secundario de WEP es el de evitar que usuarios no autorizados puedan acceder a las redes WLAN (es decir, proporcionar autenticación). Este propósito secundario no está enunciado de manera explícita en el estándar 802.11, pero se considera una importante característica del algoritmo WEP.

WEP es un elemento crítico para garantizar la confidencialidad e integridad de los datos en los sistemas WLAN basados en el estándar 802.11, así como para proporcionar control de acceso mediante mecanismos de autenticación. Consecuentemente, la mayor parte de los productos WLAN compatibles con 802.11 soportan WEP como característica estándar opcional

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un valor de comprobación de integridad (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha

sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden. WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red.

De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (*challenge*). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave.

Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

WPA.

En el estándar WPA se requiere autenticación 802.1x. En el estándar 802.11, la autenticación 802.1x era opcional. En entornos sin una infraestructura de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS), WPA admite el uso de una clave compartida previamente. En los entornos con una infraestructura RADIUS, se admiten el Protocolo de autenticación extensible (EAP) y RADIUS.

Con 802.1x, volver a teclear las claves de cifrado de unidifusión es opcional. Además, 802.11 y 802.1x no proporcionan ningún mecanismo para cambiar la clave de cifrado global utilizada para el tráfico de multidifusión y difusión. Con WPA es necesario volver a teclear las claves de cifrado de unidifusión y globales. Para la clave de cifrado de unidifusión, el protocolo de integridad de clave temporal (TKIP) cambia la clave para cada marco y el cambio se sincroniza entre el cliente inalámbrico y el punto de acceso inalámbrico (AP). Para la clave de cifrado global, WPA incluye una utilidad para que el punto de acceso inalámbrico anuncie la clave modificada a los clientes inalámbricos conectados.

WPA TKIP para el cifrado de los datos. Se trata de un protocolo de uso extendido que nuestro router Conceptronic soporta. TKIP (Temporal Key Integrity Protocol) genera claves dinámicamente para cada cliente conectado durante un tiempo predeterminado y para cada paquete que se envía desde o hacia el equipo (WEP utiliza una clave estática).

Para la autenticación utilizaremos el protocolo PSK (Pre-shared Key), una alternativa barata al uso de servidores Radius (encargados de autenticar a cada usuario) que aunque resulta una opción mucho más segura, necesita hardware adicional al punto de acceso (un ordenador con linux o Windows 2003 Server configurado y el software de servidor necesario).

Podemos optar por una clave hexadecimal (PSK Hex) o por una cadena de texto (PSK String) siendo esta última la más cómoda. La longitud no está definida, podemos introducir cualquier palabra, frase o combinación de caracteres que deseemos.

La primera opción 802.1x nos permite configurar la dirección IP, puerto y contraseña de acceso al servidor Radius de la red y que, como hemos comentado antes, está fuera del alcance de este texto.

Protocolos estándares de ULA (Upper Layer Protocol).

Estos protocolos proporcionan intercambio de autenticación entre el cliente y un servidor de autenticación.

EAP-TLS: basado en certificados tanto en el PC y el servidor. El certificado del PC debe ser establecido de forma manual (soportado por Windows XP)
PEAP: proporciona una autenticación basada en la contraseña, solamente el servidor necesita un certificado.

EAP-TTLS: proporciona autenticación únicamente en el servidor con la mejora en seguridades que provee seguridad en la capa de transporte a través de un túnel.

2.5 PROTOCOLOS DE TÚNELES VPN

2.5.1 PPTP.

Point-to-Point Tunneling Protocol fue desarrollados por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros.

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

2.5.2 IPSEC.

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.
ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway.

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

2.5.3 L2TP.

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles

y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

2.6 PROTOCOLOS QUE AYUDAN EN LA ALTA DISPONIBILIDAD

Como se puede ver en el siguiente estudio de Infonetics, la principal razón por la que existen renovaciones tecnológicas en las redes de datos es por la posibilidad de disminuir los tiempos de caída (*downtime*) de la red, esto es, la principal funcionalidad de los switches (sobretodo de core) es la alta disponibilidad.

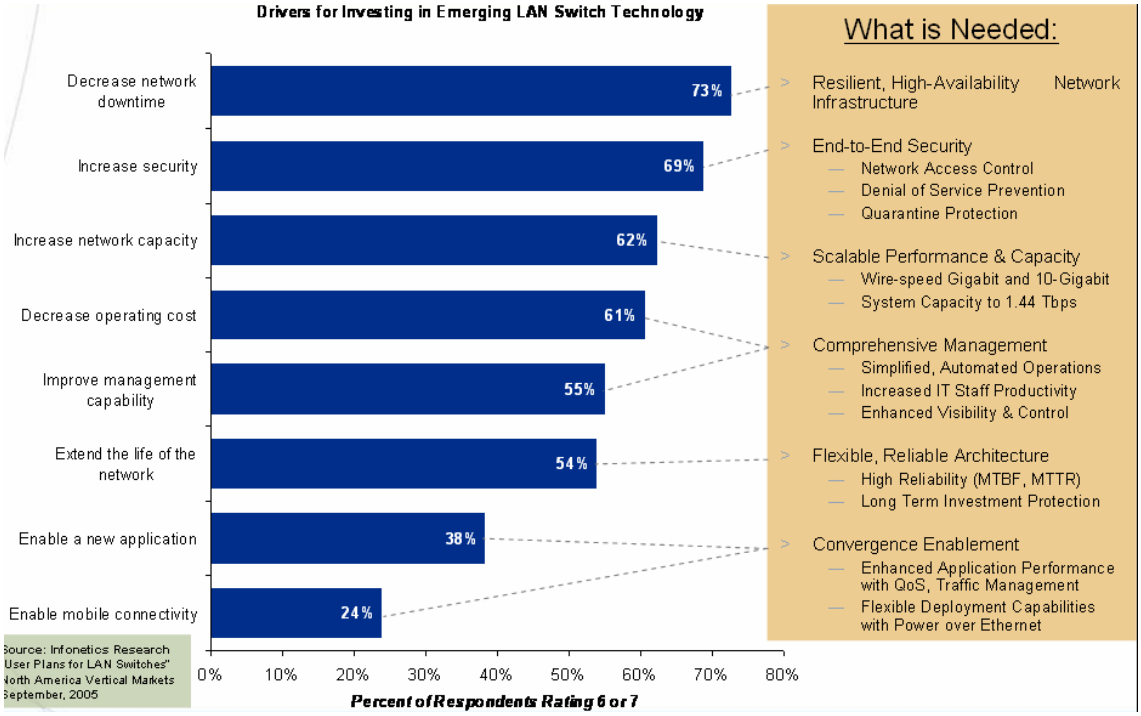


Figura 2.12. Factores por los que las empresas invierten en renovaciones de Switches.

Al día de hoy no se habla de un switch de core, sino de un sistema de core que debe tener la capacidad de presentar niveles altos de redundancia física, los aspectos mínimos a considerarse son los siguientes:

Para cambios rápidos de partes y piezas sin interrumpir la operación: los elementos deben ser hot-swap (capaces de ser removidos y colocados en caliente) sin que estos afecten la productividad y los servicios.

En el caso de las fuentes de poder, se debe poder retirar el equipo con la fuente dañada sin que esto afecte uno solo de las interfaces, procesadores, ventiladores etc.

Esto quiere decir que si la fuente falla debe existir internamente en el sistema fuentes activas que puedan soportar el peso eléctrico y potencia del equipo completamente operativo y cargado.

Incluso ante la falla de los ventiladores, se debe manejar el mismo esquema.

Con respecto a las interfaces de red, en caso de que exista una falla en una interfaz o cable, no debe existir interrupción en las aplicaciones, el estándar que se debe manejar es Link Aggregation IEEE 802.3ad para este efecto. Ahora, también existe la posibilidad que la falla se de en la tarjeta (todo el módulo) del switch por lo tanto las interfaces de enlace hacia servidores y otros switches deben poder implementar este estándar IEEE 802.3ad entre diferentes componentes del CORE como se muestra en la siguiente figura 2.13.

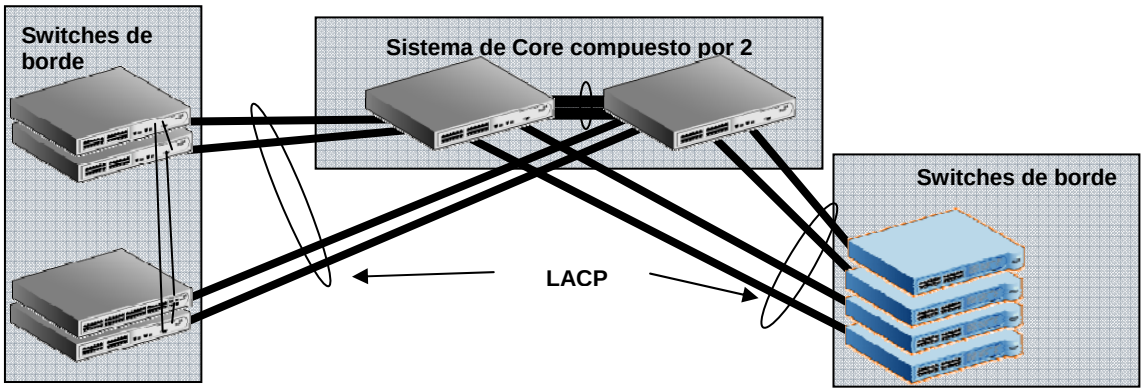


Figura 2.13. Sistema de CORE compuesto por 2 switches para manejar alta disponibilidad.

Para lograr que estos dos switches se transformen en un solo sistema de core, se utiliza una tecnología conocida como XRN, tecnología que la veremos un poco más adelante.

Los protocolos que estudiaremos serán en definitiva tres: Spanning Tree Protocol, Link aggregation y XRN.

2.6.1 STP (IEEE 802.1D), RSTP (IEEE 802.1w) y MSTP (IEEE 802.1S).

Hablaremos de estos tres protocolos de forma simultánea ya que manejan el mismo principio RSTP (*rapid spanning tree protocol*) es la evolución de STP (*Spanning Tree Protocol*) y MSTP (*Multiple Spanning Tree Protocol*) es lo mismo pero manejado dentro de VLANS a través de instancias.

En adelante para explicar los tres protocolos, se hablará de *Spanning tree* a menos que se especifique explícitamente que alguna funcionalidad aplique únicamente a STP, RSTP o MSTP.

Spanning tree es un protocolo que crea un ambiente libre de lazos en la red (un lazo provoca caída automática de todo el sistema).

Los lazos son convertidos en enlaces redunantes como se muestra en la figura 2.14.

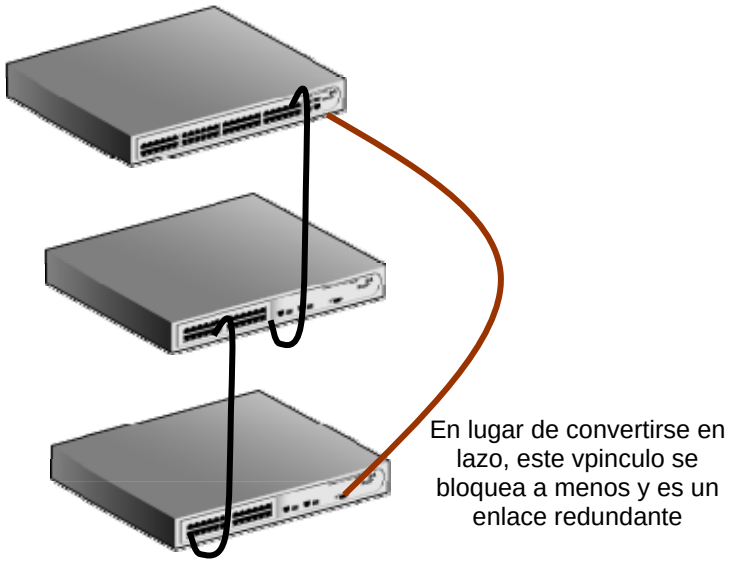


Figura 2.14. Funcionamiento de *spanning tree*

Este protocolo evita la duplicación de tramas, automáticamente se reconfigura después de una falla, puede operar sin ser configurado ya que todos los switches poseen este protocolo activado por defecto, permite interoperabilidad entre todas las marcas.

Los switches trabajan con unos paquetes llamados BPDU que son tramas que usa el switch principal (denominado *root bridge*) para verificar si los enlaces están activos y funcionando. El *root bridge* es aquel cuyo identificador sea el más bajo de todos los demás switches en la red, por defecto, todos los switches poseen el mismo número en el identificador por lo que el *root bridge* en este caso es el switch con la dirección mac más pequeña.

Para mandar información de un lugar a otro, los switches utilizan la ruta de menor costo, los enlaces a 100 Mbps son más costosos que un enlace a 1Gbps, cada enlace posee un valor, mientras más veloz el enlace, menor valor o costo tendrá.

Rapid Spanning Tree se demora 3 segundos en lograr la convergencia de la red (3 segundos de corte) mientras que Spanning Tree Protocol se demora 30 segundos.

Ninguno de los 2 protocolos consideran VLANS, si esto es requerido debe manejarse MSTP.

A veces, tenemos muchas VLANS implementadas en la red y un enlace entre un switch a otro podría manejar solamente una VLAN, en caso de un lazo, puede en ciertos casos bloquearse el enlace que coincidencialmente contiene esta VLAN especial, en este caso, esta VLAN queda aislada, para resolver este problema se usa MSTP porque con este protocolo se tomarían diferentes opciones para evitar el lazo y evitar que esa VLAN quede aislada.

MSTP se maneja por VLAN, esto quiere decir que cada VLAN podría tener su propio protocolo de Spanning Tree, esto permite manejar balanceo de carga.

STP no puede trabajar con RSTP, sin embargo MSTP si puede trabajar con uno de estos protocolos, por ejemplo en una red podemos tener STP y MSTP o lo que es mejor RSTP y MSTP juntos.

2.6.2 IEEE 802.3ad

IEEE 802.3ad se refiere a enlaces agregados y es conectar un switch con otro a través de múltiples enlaces con la misma velocidad como se muestra en la figura 2.15.

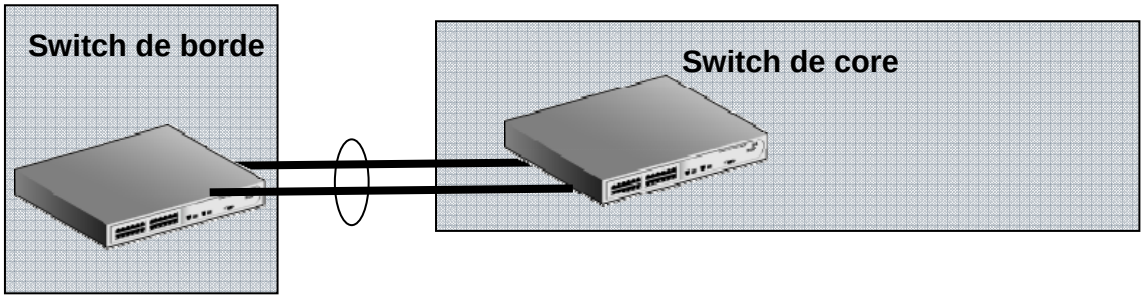


Figura 2.15. Muestra dos switchs conectados en enlaces agregados

De esta manera, en lugar de conectarnos por ejemplo a 1Gbps, podemos poner 2, 3, 4 o más enlaces de un switch a otro obteniendo 2, 3 y 4 Gbps de velocidad. Estos enlaces manejan balanceo de carga.

Todos estos enlaces sirven también como elementos de redundancia y son tratados como un solo enlace con respecto a spanning tree, enrutamiento, SNMP, etc.

Existen dos mecanismos manual y automático, en el automático el switch sensa hacia que dirección mac esta conectado el puerto y agrega los enlaces. El manual, el administrador es el encargado de indicar al switch cuales son los grupos, en este segundo método se ocupa menos recursos del procesador del switch pero una falla en la conexión de grupos de los link aggregations puede causar que los puertos se desactiven de forma automática.

La agregación de enlaces, o IEEE 802.3ad, es un término que indica el establecimiento de una red de datos que describe cómo utilizar varios enlaces Ethernet full-dúplex en la comunicación entre dos equipos, repartiendo el tráfico entre ambos. Se empezó a conocer a través de la empresa Kalpana, pero hoy son muchos los fabricantes que ofrecen esta funcionalidad para todas las velocidades de Ethernet. La mayoría de las implementaciones actuales se adecúan al apartado 43 del estándar de IEEE 802.3, designada informalmente como “802.3ad”.

2.6.3 XRN Red expandible resiliente (*Expandable Resilient Network*).

XRN es una tecnología por la cual 2 switches se convierten de forma lógica en uno solo, para ello se manejan tres funcionalidades DDM, DLA y DRR

2.6.4 DDM: Administración de dispositivos de forma distribuída.

Los dos equipos al ser conectados con un cable especial que maneja 24Gbps de velocidad, se convierten en dos unidades de un mismo sistema, esto quiere decir que son administrados por una sola IP.

El hecho de compartir una IP no es la única ventaja de DDM, ya que al poner switches en stack se logra la misma funcionalidad. Lo interesante de DDM es que adicionalmente cada equipo guarda dentro de sí una configuración realizada de tal manera que en esta configuración aparecen todas las funcionalidades de calidad de servicio, lista de acceso, rutas etc. De tal forma que si uno de los equipos es desconectado de la red, el otro funcionará con la configuración particular para ese equipo sin perder ninguna de las funciones configuradas en el equipo y sin que el administrador de red tenga que configurar estas funcionalidades en cada uno de los equipos, lo único que se debe hacer es configurar el sistema y cada equipo guarda su configuración especial de forma automática. A continuación se muestran ejemplos de configuraciones de la unidad 1 y unidad 2 de un mismo sistema XRN.

Ejemplo de la unidad 1 del sistema, se muestra en el Anexo A.

Como se puede observar en el Anexo A las configuraciones coinciden el nombre de las VLANS, las decripciones, los link aggregations pero al momento de indicar la información de cada puerto del switch, la unidad 1 indica los números 1/0/1 y la unidad 2 indica los números 2/0/1 donde 1/0/1 significa unidad 1 puerto 1 y 2/0/1 significa unidad 2 puerto 1.

Al lograr que los dos switches se transformen en forma lógica en un solo equipo, se logra que ambos equipos trabajen simultáneamente sobre la red, duplicando el nivel de procesamiento de paquetes por segundo, de esta forma estamos trabajando al doble

de velocidad y cuando muere uno de los equipos, se trabaja a la velocidad normal, en ambos casos se cumple la funcionalidad de manejar alta disponibilidad.

2.6.5 DLA Enlaces agregados de forma distribuída.

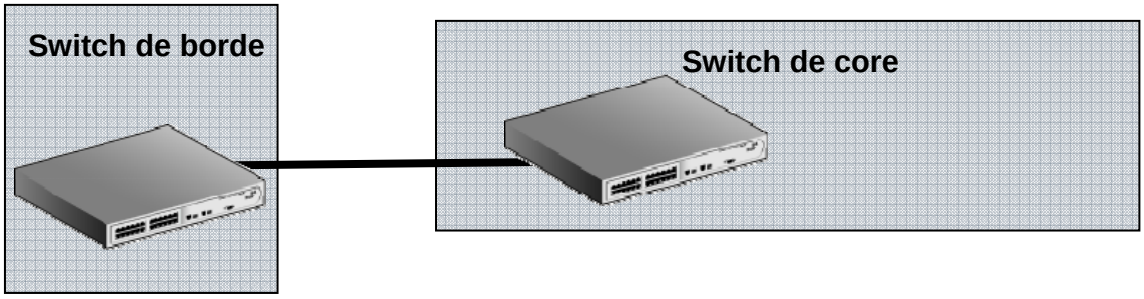


Figura 2.16. Switch de core conectado a un switch de borde

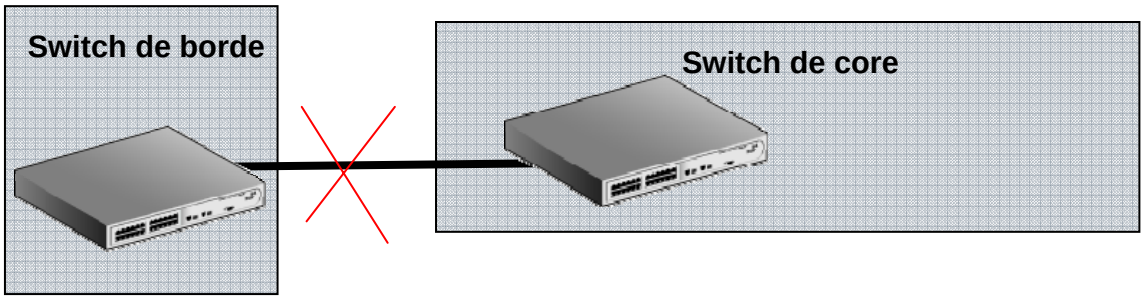


Figura 2.17. En caso de falla del enlace, quedamos sin conexión.

Por lo tanto, para alta disponibilidad se pone un segundo enlace redundante con el estándar 802.3ad enlace agragado (*link aggregation* o LACP)

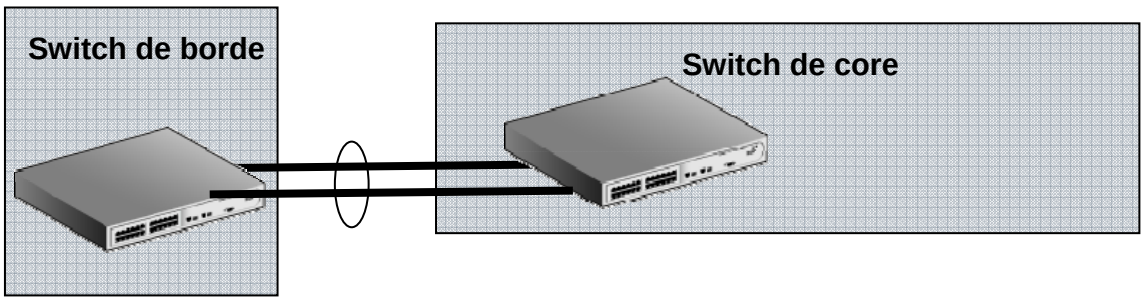


Figura 2.18. Enlace redundante con el estándar 802.3ad enlace agragado (*link aggregation* o LACP).

El estándar 802.3ad se maneja desde un equipo a otro, caso contrario se habla de otra tecnología como STP/RSTP/MSTP (*spanning tree protocol*), ahora, que sucede si falla el switch de core como en la siguiente figura:

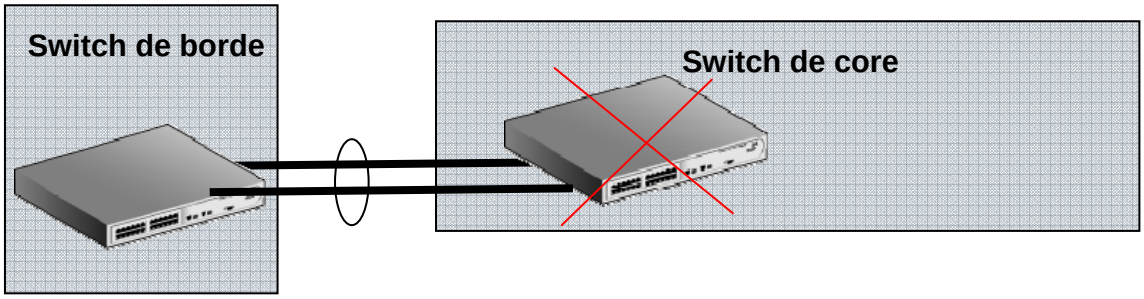


Figura 2.19. Falla del switch de core.

Como habíamos visto, gracias a la tecnología de XRN podemos hacer que dos switches se comporten como uno solo, esto es, podemos hacer *Link Aggregation* desde el switch de borde hacia el sistema de core compuesto por 2 unidades. Esta funcionalidad se llama DLA (*distributed link aggregation*) de esta manera si un switch falla la información fluye por el segundo enlace logrando así alta disponibilidad en la red.

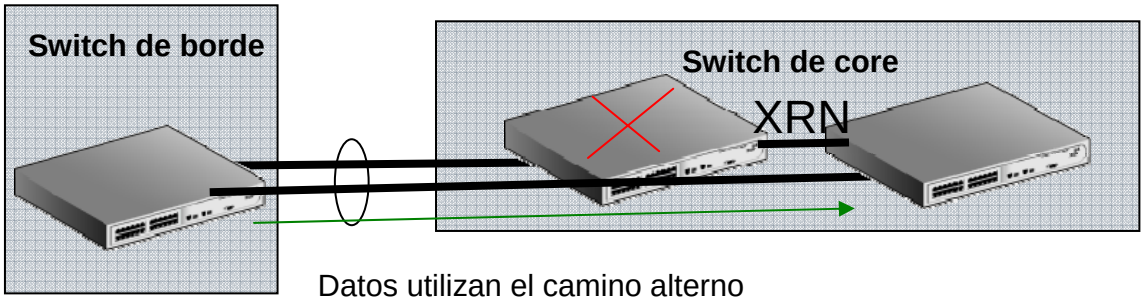


Figura 2.20. Tecnología XRN podemos hacer que dos switches se comporten como uno solo.

2.6.6 DRR (Enrutamiento resiliente distribuido).

La tercera funcionalidad de XRN es el enrutamiento resiliente de forma distribuída (DRR *Distributed Resilient Routing*) esta funcionalidad provee resiliencia sobre capa 3 al mismo nivel que lo haría un switch de chasis, este protocolo maneja enrutamiento local de capa 3 a través de RIP. XRN sincroniza las tablas de OSPF a

todos los *hosts* del sistema (*fabric*), toda la información de ACL es distribuída a todos las unidades del sistema.

La información de la sincronización de capa 3 (*routing*) es enviada a todas las unidades

El tráfico en capa 3 puede ser manejado de forma local por el switch y pasa de forma inteligente arriba o abajo del stack XRN, esto permite tener funcionalidades de capa 3 mucho más eficientes y rápidas sobre la red.

En definitiva, si uno de los switches muere, el otro posee toda la información de capa 3 de la red por lo que no existe interrupción del servicio.

Capitulo III

INTRODUCCIÓN A LOS SISTEMAS DE SEGURIDAD IPS

3.1 INTRODUCCIÓN

El objetivo de un IPS es detectar tráfico malicioso y no dejarlo pasar, por lo tanto un IPS debe ser proactivo. Un sistema de IPS debe ser colocado en línea, esto quiere decir que todo el tráfico que deseamos monitorear y destruir en el caso de que sea malicioso debe pasar por el equipo antes de que llegue a su destino (3Com, 2007).

El miedo de las empresas es que el equipo provoque cuellos de botella y se cree un punto de falla único.

Cada segmento del IPS posee dos puertos (uno de entrada y uno de salida).

El IPS protege la red ante:

- Anomalías de tráfico: estadísticos, anomalías de protocolos y aplicaciones, buffer overflow, paquetes ilegales o malformados, decodificación de peticiones web, evasión de filtros.
- Negación de servicios: ataques de inundación
- Ataques a las aplicaciones: protección del ancho de banda impidiendo p2p, protección ante nuevas vulnerabilidades de sistemas operativos.

Para definir el IPS más adecuado para la red, hay que tomar en cuenta tres factores importantes: si es capaz de proteger las nuevas vulnerabilidades emergentes, si estas vulnerabilidades han sido protegidas a tiempo, y finalmente que no genere latencia sobre la red.

Veamos ahora un estudio donde se muestran las vulnerabilidades que salieron para Microsoft en el año 2006, en el siguiente gráfico se muestran a todos los mayores fabricantes de IPS y la cobertura de las vulnerabilidades, se muestra claramente que el único fabricante que logró proteger el 100% de las vulnerabilidades fue TippingPoint como se muestra en la figura 3.1.

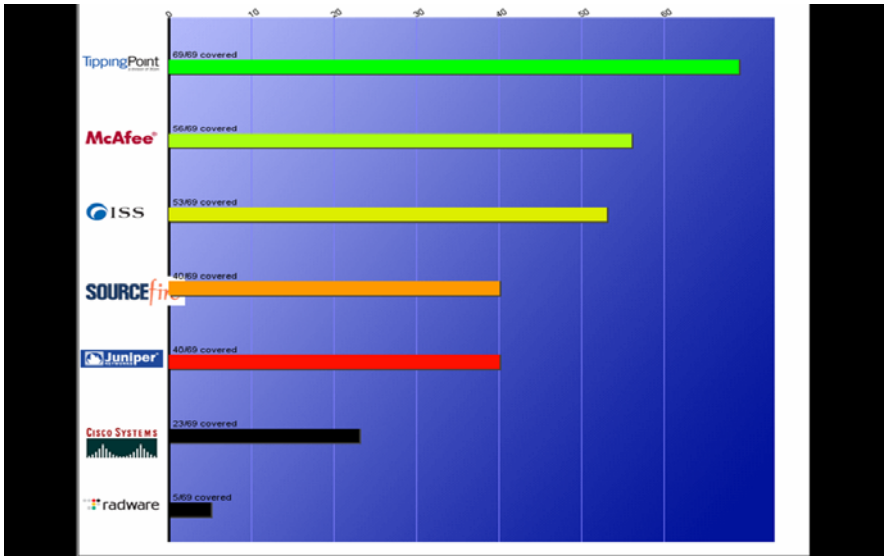


Figura 3.1. Muestra Tipping Point protegiendo 100% vulnerabilidades.

Ahora, el tiempo de reacción se mide en la sumatoria de días en los que el equipo protegió los ataques, por ejemplo, si la primera vulnerabilidad ha sido protegida 2 días antes se ponle número de -2 a una sumatoria total, si la siguiente vulnerabilidad ha sido protegida 3 días antes se suma el número -3, entonces -2-3 = -5.

Si el equipo protegió 1 día después se pone +1, si protegió 2 días antes se resta 2, por lo tanto +1-2= -1, el equipo más proactivo será el primero porque posee un número más lejano al día cero.

En este estudio se muestra como TippingPoint tiene el mejor tiempo de reacción frente al resto de fabricantes como se muestra en la siguiente fugura 3.2:

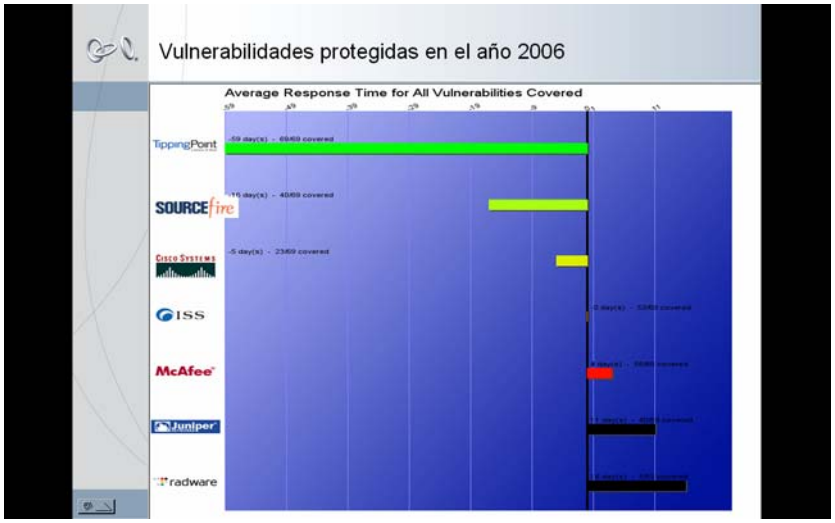


Figura 3.2. Tipping Point tiene el mejor tiempo de reacción.

Adicionalmente lo tercero que se debe revisar es la latencia, mientras menor latencia mejor es el equipo, se hizo un estudio con los 17 miembros de ICSA y solo 3 tuvieron menos de 500 microsegundos de latencia. TippingPoint fue el equipo que menor latencia tuvo, comprobándose que es el mejor IPS en el mercado.

Tipping Point con un *throughput* de 3 Gbps tuvo una latencia menor a 81 µs, en cambio Broad Web con un *throughput* de 100 Mbps genero una latencia de 441 µs.

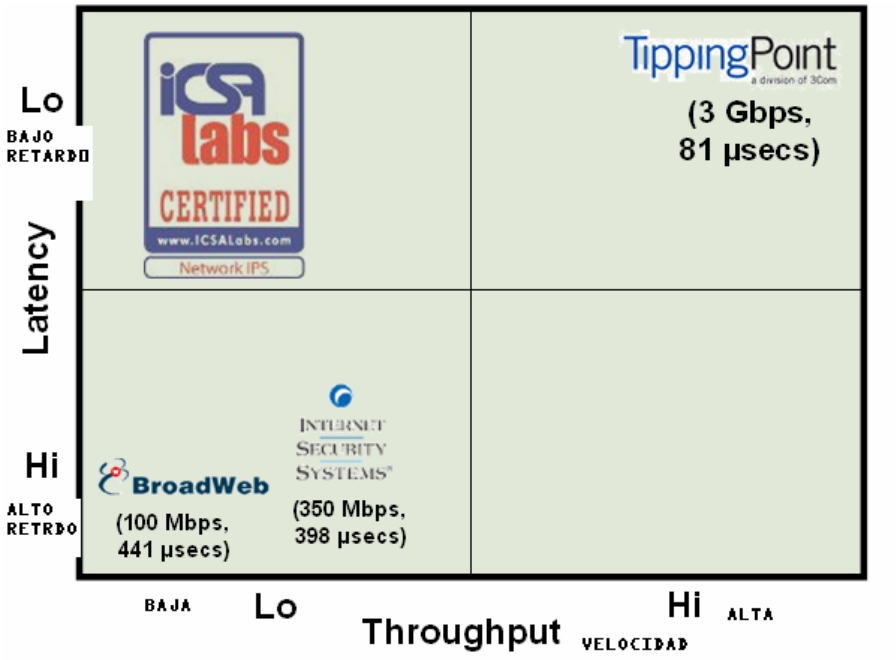


Figura 3.3: Tipping Point con un *throughput* de 3 Gbps tuvo una latencia menor a 81 µs.

3.2 FUNCIONALIDADES GENERALES

El equipo que vamos a colocar tiene las siguientes funcionalidades:

El equipo de seguridad es una plataforma de seguridad basada en IPS con funcionalidades VPN, *firewall* , administración de ancho de banda, calidad de servicio dentro de la VPN y filtrado de contenidos de web.

3.2.1 Especificaciones Operativas

El equipo opera en forma continua para detener y bloquear tráfico malicioso de gusanos, virus, troyanos, amenazas combinadas, DoS, intentos de *phishing*, *spyware*, amenazas de VoIP y otros.

Para garantizar una protección contra amenazas de última generación el equipo se actualiza en base a una vacuna digital que proporcione protección efectiva contra vulnerabilidades emergentes en sistemas operativos o aplicaciones conocidas como "Día Cero". Esta protección proporcionará protección preventiva contra diferentes tipos de ataques a la misma vulnerabilidad.

La vacuna digital proporcionará adicionalmente filtros nuevos para las amenazas emergentes que surjan como por ejemplo spyware, *phishing* y aplicaciones P2P.

Las actualizaciones de la vacuna digital se harán automáticamente cada semana o incluso antes cuando surjan amenazas y vulnerabilidades críticas.

El equipo cuenta con un conjunto de filtros y políticas preconfiguradas para bloquear ataques de forma precisa y automática., sin necesidad de ajustes para hacer eficiente el proceso de implementación.

El equipo cuenta con la funcionalidad de IPS y adicionalmente en el mismo dispositivo se ofrece la funcionalidad de VPN mediante IPSec, un firewall de inspección de estado de paquetes ("stateful packet inspección"), filtrado de contenidos

WEB y modelado de tráfico en base a políticas para control preciso de ancho de banda de tráfico entrante y saliente.

Es muy importante que estas funcionalidades sean interoperables es decir, el equipo debe permitir la aplicación de IPS y modelado de tráfico a un tunel IP Sec.

En relación al modelado de tráfico, el equipo permite controlar aplicaciones no críticas en la red tal como aplicaciones P2P, recuperando así ancho de banda para aplicaciones de misión crítica del negocio, como video-conferencias o voz IP para garantizar calidad de servicio.

El equipo deberá proporcionar servicio de filtrado de contenidos para controlar el acceso de los usuarios al WEB.

El equipo debe permitir tráfico de múlticast en los túneles para asegurar aplicaciones de teleconferencia.

El equipo permite la priorización de tráfico entrante y saliente tanto dentro como fuera de los túneles VPN.

En cuanto al filtrado de contenidos Web, la configuración de los filtros deberá ser sencilla e intuitiva mediante marcado de casillas ("*checkbox*") y categorías a restringir. La base de datos de sitios de Web que se utilizan en esta funcionalidad deberá residir en un servidor externo con balanceo de cargas y múltiples ubicaciones geográficas. El equipo deberá acceder a esta base en tiempo real, es decir evitará almacenar localmente estas bases de datos. Estas bases de datos externas deberán ser actualizadas constantemente.

Ofrece múltiples zonas de seguridad. Proporciona también niveles separados de aplicación de políticas, por sub-redes departamentales, por DMZ´s corporativas etc.

Adicionalmente deberá permitir la configuración de privilegios basados en la hora del día.

- Cuenta con un motor de políticas flexible que permita diversos objetos en la configuración de reglas tales como: Grupos de redes/zonas de seguridad/direcciones IP – privilegios basados en hora del dia, Aplicación de servicio, Calendario programado/hora del día, Túneles VPN.
- Cuenta con un control unificado de múltipes servicios como: filtrado de web, Modelado de Tráfico, autenticación de usuario y administración de dispositivos.
- Cuenta con funciones de Encriptación y autenticación tales como:
- Encriptación IPSec incluyendo DES, 3DES y AES acelerado mediante hardware.
- Autenticación de certificados digitales X.509 por autoridades certificadoras internas o de terceros.
- Grupos con múltiples privilegios
- Base de datos RADIUS integrada y externa.
- Proporciona filtrado de URL´s con listas configurables permitidas/denegadas asi como mediante la comparación de expresiones regulares de URL´s.
- Posee filtrado de contenidos web mediante un esquema de subscripción anual, este esquema de filtrado contará con 40 categorias de contenido y listas ilimitadas de URL´s.

Conectividad

El equipo cuenta con administración avanzada de tráfico y modelado de tráfico entrante y saliente incluyendo: VoIP, video conferencia, aplicaciones vitales para la empresa. Contará tambien con priorización de tráfico dentro y fuera de tuneles VPN, deberá contar controles flexibles y basados en políticas tales como Calendarios de horarios y tipos de servicio.

Posee soporte de cliente VPN directamente al sacarlo de la caja (sin licencias o hardware adicional), soportando diversos sistemas operativos tales como Microsoft, Apple.

Soporta protocolos estándar como PPTP, L2TP/IPSec, IPSec

El equipo integra y soporta funciones de cuarentena, es decir, tener la capacidad de bloquear o aislar a usuarios por medio de su dirección IP dependiendo de las políticas que se definan en el equipo, emitiendo al usuario puesto en cuarentena una página de aviso explicando la razón por la cual ha sido aislado. El administrador del equipo podrá revisar qué direcciones IP están en cuarentena y permitir que éstas vuelvan a conectarse a la red.

Tiene la capacidad de conectarse en diversos ambientes con diversos tipos de topologia asi como con diferentes esquemas de direcciones IP es decir, el equipo debera soportar los siguientes tipos de conexiones:

- Transparente, Enrutado, NAT (incluyendo servidor virtual y PAT)
- Combinados
- Ruteo dinámico (RIP V1 y V2)
- Etiquetado de VLAN 802.1q

Soporta ruteo de IP multicast sobre IPSec PIM-DM entre sitios sobre VPN IPSec, proporcionando soporte para aplicaciones de conferencia IP.

3.3 FUNCIONALIDADES DEL IPS

Dentro de los parámetros de IPS el equipo posee las siguientes característcas:

- El equipo ofrece protección a clientes y servidores impidiendo el ataque a sistemas operativos y aplicaciones vulnerables, también deberá proporcionar bloqueo a ataques multi modo.
- Proporciona protección en tiempo real utilizando una vacuna digital.
- Proporciona protección preventiva frente a amenazas a la red, será capaz de obtener automáticamente los filtros mas recientes, cuenta también con un grupo de filtros recomendados.

- Ofrece protección frente a spyware y aplicaciones P2P, impidiendo que los clientes se infecten de spyware, impidiendo la propagación de “walk-in-worms” en la red, (usualmente desde equipos portatiles)
- Bloquea aplicaciones y limitar el ancho de banda que ocupan tales como aplicaciones P2P y mensajería instantánea.
- El equipo deberá de tener filtros para detectar y bloquear spyware.
- El equipo deberá ser capaz de lboquear y/o administrar el ancho de banda que utilizan las aplicaciones P2P.
- El equipo deberá de soportar SNMP v1 y v2.
- El equipo deberá de contener MIBS que puedan ser utilizadas por cualquier sistema de administración de red.
- El equipo deberá de ser capaz de enviar traps al sistema de administración.
- El equipo deberá de soportar syslog para eventos de filtrado y administración de ancho de banda.
- El sistema debe de proporcionar un password de seguridad que solo puede ser cambiado por el Administrador mas importante del sistema.
- El sistema debe de proporcionar niveles jerárquicos de administración como por ejemplo operadores.
- El sistema debe de incluir un sistema propio de administración (common element manager).
- El sistema debe ser capaz de tener como mínimo 1700 filtros listos para ser utilizados por el equipo en caso de ser necesario y deberán de estar en un estado de default de fábrica que le indique al sistema que realice el bloqueo desde el primer día de operación sin necesidad de configurar nada en el equipo.
- El sistema deberá de proveer protección para las vulnerabilidades anunciadas o nuevas.
- El sistema deberá de ser capaz de operar en una red de gigabit con tasas altas de tráfico con todos los filtros activados sin tirar parquetes.
- El sistema deberá de proveer un sistema automático que permita actualizar al equipo en cuanto a las nuevas vulnerabilidades y ataques.
- El sistema deberá de soportar mecanismos de High Availability en eventos de errores en la red, errores internos el equipo o perdida completa del equipo.

- El sistema deberá tener diferentes niveles de acceso para su administración (superusuario, administrador y operador). El control de acceso se puede limitar por perfil, dispositivo o segmento de red.
- El sistema deberá de analizar todas las capas del modelo OSI.

En capa 3-4:

- checksums incorrectas.
- TCP *header flags* inválidas.
- IP fragments inválidos.
- TCP *reassembly* inválidos.
- Requerimientos no solicitados.

En capa 3-7:

- Argumentos muy largos que se pasan a comandos (buffer overflows para aplicaciones como HTTP, RPC, POP, IMAP, FTP, Telnet).
- Valores inválidos para Headers de Protocolos (desviaciones del RFC para la especificación del protocolo).
- Valores inválidos en la información de las aplicaciones (SQL Injection, shell meta-characters en valores de parámetros para requerimientos en el web).

El sistema deberá de poder identificar y bloquear lo siguientes ataques como mínimo:

- **Vulnerabilidades (mínimo 650 filtros)**
  - Sistema Operativo (Microsoft, Linux, Unix etc.), Aplicación (MSSQL, MS-Exchange, IIS, Oracle, Lotus Notes etc.), Protocolos (HTTP, SNMP, SMB, RPC, SMTP, POP, IMAP, SSH, FTP, HTTP).
- **Exploits (mínimo 450 filtros)**
  - MS-Blaster, Slammer, Welchia, Sobig, BugBear, Nimda, Code Red etc.
- **Políticas de Seguridad (150 filtros como mínimo)**
  - root access to Telnet, multi-session FTP, covert channel communications, ICMP options, application-specific access permissions).

- **Reconocimiento (Probes, escaneo de puertos, etc. – 300 filtros como mínimo)**
    - Escaneo de puertos.
- **Informacional (45 filtros mínimo)**
    - Actividad de protocolos de red (directory traversals, ICMP, login attempts, FTP commands etc).
- **DDOS (mínimo 5 filtros)**
    - SYN Floods, ataques amplificados.
- **Equipamiento de Red (25 filtros como mínimo)**
    - (routers/switches etc.) de ataques DoS e IP.
- **Normalización de Tráfico (30 filtros como mínimo)**
    - Limpiado de la red de paquetes que consumen recursos en la red (IP/TCP/UDP/ICMP/ARP).
- **Application Acceleration: Traffic Management (User Defined)**
    - Administración de tráfico por IP/TCP/UDP/ICMP, por protocolo o por dirección IP.
- **Application Acceleration: Misuse & Abuse (Peer to Peer - 95 Total)**
    - Manejo de 98% de protocolos.

El sistema debe ser capaz de bloquear propagación de gusanos y virus previniendo la infección de otros equipos y consumo de ancho de banda.

El equipo deberá ser capaz de reconocer anomalías de tráfico:

- Tráfico inusual
- Conexiones por segundo
- Umbrales de protocolos (paquetes, bytes, conexiones, etc.)
- Análisis de patrones de tráfico
- Análisis de utilización de aplicaciones
- Análisis de utilización de hosts

A falla del sistema, el sistema deberá ser capaz de dejar pasar el tráfico sin bloquearlo o tener que ejecutar alguna acción por el administrador.

A falta de energía eléctrica, el equipo debe de tener la opción de poder pasar el tráfico sin bloquearlo.

El equipo deberá de proveer protección contra:

- DoS y DDoS
- Protección contra vulnerabilidades
- Protección contra Zombie Recruitment
- Protección contra herramientas de ataque como TFN, Loki, etc..
- Protección de ancho de banda
- SYN Proxy
- Inundación por conexiones por segundo
- Inundación por conexiones establecidas

El equipo deberá de soportar 60,000 TCP SYNs.

El equipo deberá de hacer proxy de los TCP SYNs y se pueden hacer proxy por lo menos 60,000.

3.4 FUNCIONALIDADES AVANZADAS DEL IPS

Las funciones avanzadas están dirigidas a proteger la red para ser un complemento a sistemas de protección tradicionales.

Los IPS son importentes debido a que los siguientes dispositivos no son suficientes para la protección de la red:

Firewalls inspeccionan paquetes basados en los encabezados unicamente (políticas manejan por puertos y el SPI no se puede alterar para proteger de nuevas amenazas)

Anti X (sistemas reactivos NO PROACTIVOS que funcionan FUERA DE LINEA, no detienen el X antes de que se infecte una máquina al menos o se consuman recursos).

Políticas de parches: totalmente manual y no existe cobertura completa (muy poco tiempo para lograrlo) Síndrome de down (parchamos un sistema y se cae la aplicación).

Para combatir los ataques a vulnerabilidades se debe ver el contenido de los paquetes, los Firewalls no lo pueden hacer.

Que puede tener vulnerabilidades nuevas?
Protocolos (SIP, RFC)
Sistemas operativos (Linux, Unix, Windows, Cisco OS)
Aplicaciones (Pogramas, bases de datos)
Como se atacan las vulnerabilidades?
Virus, gusanos, troyanos
DoS, DDoS
Exploits que usan vectores para acceder a la vulnerabilidad (ataques directos)
Seguimiento a vectores que llevan al hole (espionaje, robo informacion)

El componente principal del IPS es el motor de supresión de amenazas (TSE), este elemento reconstruye e inspecciona el contenido de los flujos llegando a nivel de aplicación. Cada paquete es re-evaluado para buscar contenido malicioso. TSE es un motor de seguridad basada en flujos, la información analizada:

- Protocolo IP
- IP de origen
- Puertos de origen
- IP de destino
- Puertos de destino

Una vez clasificado, cada paquete es inspeccionado por el grupo apropiado de protocolos y filtros de aplicaciones. El motor de filtros del IPS combina procesamiento paralelo masivo a nivel de *hardware* garantizando así una mínima latencia en el orden de los microsegundos independientemente del número de filtros aplicados sobre el sistema.

Fuera de la caja el IPS provee una configuración recomendada de fábrica y los nuevos filtros que se incluyen en nuevas vacunas digitales también poseen configuraciones recomendadas de filtros. Por lo tanto podríamos dejar el equipo solo, sin configurar y estaría haciendo su trabajo. Sin embargo, esta no es la idea, lo que deseamos lograr con el IPS es cerrar lo mejor posible las brechas de seguridad de la

empresa. Para ello el primer paso será obtener la información de las aplicaciones y sistemas operativos que se manejan así como los protocolos utilizados en la red.

Haciendo un levantamiento de la información del cliente, conocemos que existe: Sistemas operativos basados en Windows, aplicaciones de bases de datos oracle, paquetes de video sobre la red (*stream* de video) con equipos marca sony que utilizan el protocolo H323 y H325, por lo tanto, como la configuración recomendada del cliente ya protege por defecto el sistema operativo y la base de datos, entonces tendremos que activar los siguientes filtros avanzados en el IPS (se incluye SIP por funcionalidades de Telefonía IP en este lenguaje):

2818: SIP: Method Anomaly
2819: SIP: URI Anomaly
2820: SIP: Version Anomaly
2821: SIP: Via Host Anomaly
2822: SIP: Via Version Anomaly
2823: SIP: Via Tag Anomaly
2824: SIP: From Field Anomaly
2825: SIP: Contact Field Anomaly
2827: SIP: Call-ID Field Anomaly
2829: SIP: Cseq Field Anomaly
2830: SIP: Content-Type Field Anomaly
2983: SIP: From Field Anomaly
2984: SIP: From Field Anomaly
2985: SIP: From Field Anomaly
2588: H.225: Source Address URL Length Anomaly
2590: H.225: Source Address h323-ID Length Anomaly
2591: H.225: Source Address h323-ID Value Anomaly
2592: H.225: Source Address dialedDigits Length Anomaly
2593: H.225: Source Address Email Length Anomaly
2595: H.225: Destination Address Choice Anomaly
2598: H.225: Destination Address h323-ID Length Anomaly
2599: H.225: Destination Address URL Length Anomaly

2600: H.225: Destination Address URL Value Anomaly
2601: H.225: Destination Address h323-ID Value Anomaly
2602: H.225: Destination Address dialedDigits Length Anomaly
2604: H.225: Source Address Choice Anomaly
2605: H.225: Protos Suite Attack

3.4.1 Elementos del IPS.

Los siguientes valores, temporizadores y tablas son elementos indispensables del sistema de IPS:

Tramas bloqueadas: todos los flujos miembros de un flujo principal que ya ha sido bloqueado, serán bloqueados sin análisis posterior para mejorar velocidad (es como si al capturar al líder de una pandilla y examinar lo que ha hecho la pandilla, capturamos a todos los miembros de la pandilla sin hacer averiguaciones de los mismos crímenes porque ya han sido analizados antes).

Tiempo de expiración: por defecto los flujos bloqueados en el punto anterior quedarán 1800 segundos en la tabla de seguirlos descartando antes de analizarlos nuevamente. (en el mismo ejemplo anterior, se apresará a todos los miembros de la pandilla durante el primer mes, a partir del segundo mes si es apresado alguno de ellos se volverá a hacer las mismas investigaciones). Esta variable en el IPS puede bajar hasta 30 segundos dependiendo del tipo de tráfico de la red, en nuestro caso esta variable no será alterada.

Variable simétrica o asimétrica: por defecto se entiende que el tráfico de una red es asimétrico, sin embargo en condiciones especiales (sobretodo de balanceo de carga) hay que indicar al equipo que el tráfico debe ser simétrico, caso contrario se trata de anomalía de tráfico. Esta variable tampoco será alterada en la red que estamos programando.

Filtros adaptativos: bajo condiciones raras y extremas, el equipo puede tener mucho trabajo que hacer (se congestiona), la congestión significa que debe hacer más lenta la red y procesar todos los paquetes como está programado el equipo o mantener la

velocidad de la red sin latencia pero para ello debe descartar muchos paquetes porque no hay suficiente tiempo para lidiar con todos.

En el caso del IPS de TippingPoint se utiliza un método muy interesante donde ninguna de las dos opciones es usada, lo que se logra en estos casos es mantener la velocidad de la red sin latencia y no descartar paquetes. La pregunta obvia es y cómo se logra esto y que hay que sacrificar (porque el equipo está con congestión), la respuesta es simple, el equipo siguie trabajando en proteger la red pero no dará ninguna estadística y reporte de ello.

Agregación adaptativa de filtros: en el caso anterior, el equipo no genera latencia ni descarta paquetes, ahora para no perder absolutamente toda la información del tipo de ataques que está manejando lo que se hace es poner un tiempo en el cual el equipo informa el numero de veces que protegio el ataque y cual era, pero esta información es desplegada después de que el problema ha sido superado.

CAPITULO IV

DISEÑO DE LA RED DE TELEFONÍA IP E IPS PARA LA UNIVERSIDAD COTOPAXI

4.1 INTRODUCCIÓN

"La clave para lograr un crecimiento sostenido en la productividad de las organizaciones no radica en lograr que los empleados trabajen más duro. Se trata de lograr que trabajen más inteligentemente", "Aquí es donde están las verdaderas mejoras en la productividad"(Rezk, 2004).

Una infraestructura de red basada en IP puede proporcionar un fundamento sobre el cual se puedan operar aplicaciones que les permitan a los empleados trabajar en forma más inteligente sin tener que realizar una configuración avanzada en el sistema. Las aplicaciones de Comunicaciones IP, que incluyen la telefonía IP, mensajería unificada, aplicaciones inalámbricas, aplicaciones para centros de contacto, al igual que video, son habilitadas mediante arquitecturas convergentes de red que entregan servicios sobre una red única.

En esta era del conocimiento, los empleados pueden utilizar la red y las tecnologías basadas en IP para colaborar más eficientemente y para comunicarse con mayor facilidad. Esta infraestructura también les permite trasladar datos, voz y vídeo a través de la red en forma más inteligente, por lo que pueden tomar decisiones más rápido, lo cual, a su vez, mejora la agilidad de la empresa, factores todos claves para mejorar la productividad.

Las características de la telefonía IP, tales como las llamadas de conferencia y los servicios integrados del directorio de empleados, son sensiblemente más fáciles de configurar y utilizar por parte de los empleados por sí solos, que las características convencionales del sistema telefónico PBX. Con frecuencia, la complejidad de

establecer y usar las características de los sistemas PBX lleva a los empleados a recurrir al personal de tecnología de la información y telecomunicaciones a pedir ayuda.

4.1.1Diseño de la Red

La Universidad Cotopaxi, requiere de los siguientes equipos para su implementación:

2 switchs 5500G conectados en XRN, para dar una alta disponibilidad al siwtch de Core, 12 switchs de borde 4500. Una central telefónica NBX V3000, con un chasis de expansión, y un sistema de protección de intrusos IPS X505.

La red de la Universidad Cotopaxi queda implementada de la siguiente manera:

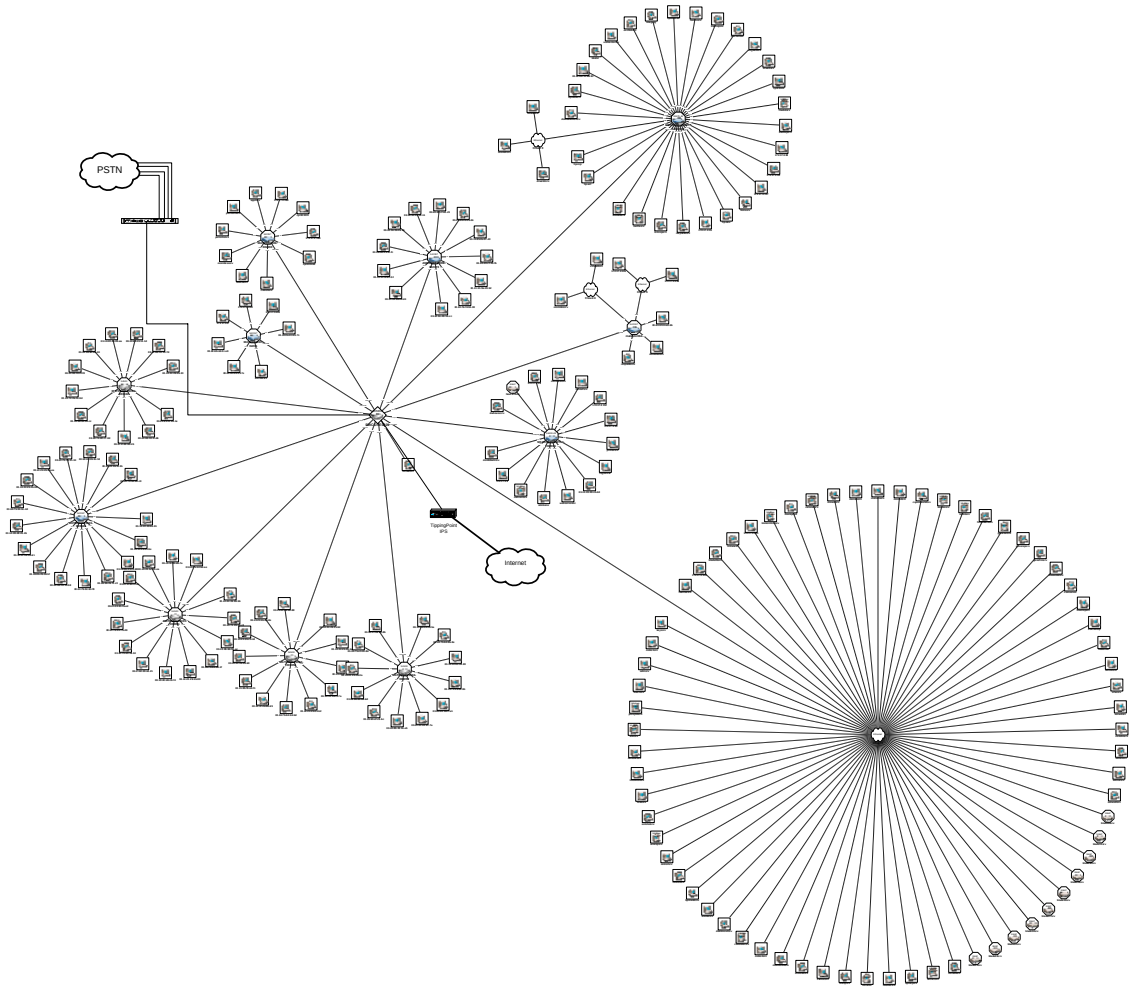


Figura 4.1. Red de la Universidad Cotopaxi

Procesos para el diseño de la Red

1.- Elegir una marca para trabajar

Dado que la red de la Universidad Cotopaxi implementará una red segura y convergente donde los componentes críticos del sistema son los siguientes:

- Telefonía IP
- Firewall
- IPS
- Switches de Core y Borde
- Programa de administración y monitoreo
- NAC /Control de Acceso a la Red)

Se requiere una marca que posea la solución de extremo a extremo para que la integración sea más sencilla, adicionalmente el soporte técnico se hará con un solo fabricante.

Analizando los diferentes fabricantes que puedan brindar esta solución encontramos a únicamente 2 que poseen la solución de extremo a extremo, Cisco y 3Com.

Entre las siguientes alternativas se ha elegido 3Com por las siguientes razones:

Con respecto a la telefonía IP

Los componentes de 3Com soportan el estándar G.722 (*Wideband audio*) para obtener mejor calidad del sonido de la voz sobre telefonía IP. Cisco no cumple con este requerimiento.

La telefonía SIP de 3Com es estándar mientras que Cisco usa Skinny que es propietaria y no es desarrollada de forma amplia lo que puede provocar problemas de compatibilidad e interoperabilidad a futuro.

Desde 1999 3Com usa un sistema operativo de tiempo real por lo que el desarrollo es muy maduro y robusto, Cisco hasta el call manager 4 manejó Windows y recién en el call manager 5 migró a Linux por lo que no es una plataforma madura.

Con respecto al IPS

Este sistema de seguridad protege de forma preventiva ante nuevas vulnerabilidades que suelen aparecer sobre protocolos, aplicaciones, sistemas operativos, equipos activos, central IP y los distintos componentes de la red.

Para mostrar el nivel de efectividad de las vacunas digitales, se ha recogido la información de las vulnerabilidades del año 2007 de la página web de Microsoft www.microsoft.com y vulnerabilidades del programa de día cero www.zerodayinitiative.org sobre amenazas a aplicaciones e infraestructura similaes a las utilizadas por la Universidad.

Los resultados muestran en la figura 4.2 que TippingPoint es el fabricante con mejor nivel de protección protegiendo el 95.83% de las vulnerabilidades.

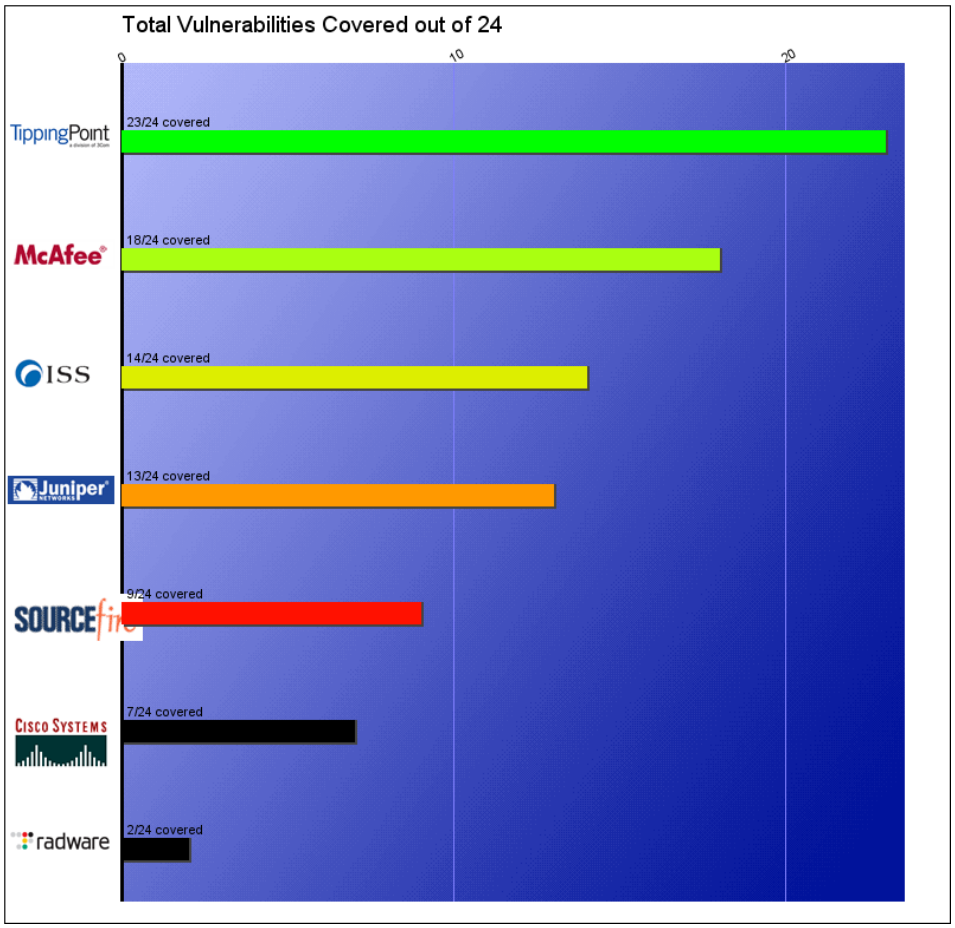


Figura 4.2. Resultados que muestran a TippingPoint como el mejor IPS

Con respecto a los Switches

El rendimiento en capa 2 de los switches propuestos (3Com Superstack 5500G) es superior a equipos similares de Cisco como lo muestra el siguiente estudio de Tolly group (www.tolly.com) en la figura 4.3.

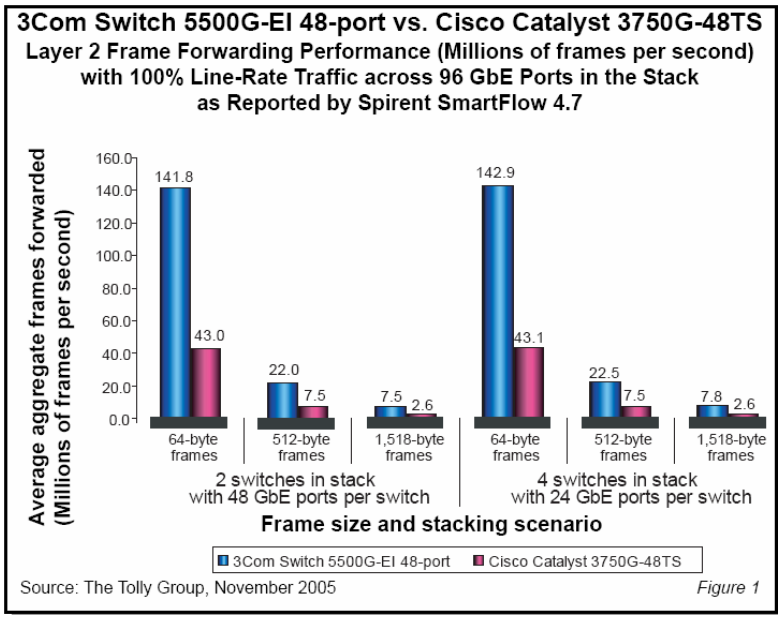


Figura 4.3. Muestra un reporte del Tolly Group sobre switchs 3Com y Cisco en capa 2.

El performance en capa 3 de los switches 5500G es muy superior a equipos similares de Cisco como se muestra en la siguiente figura 4.4 de Tolly Group:

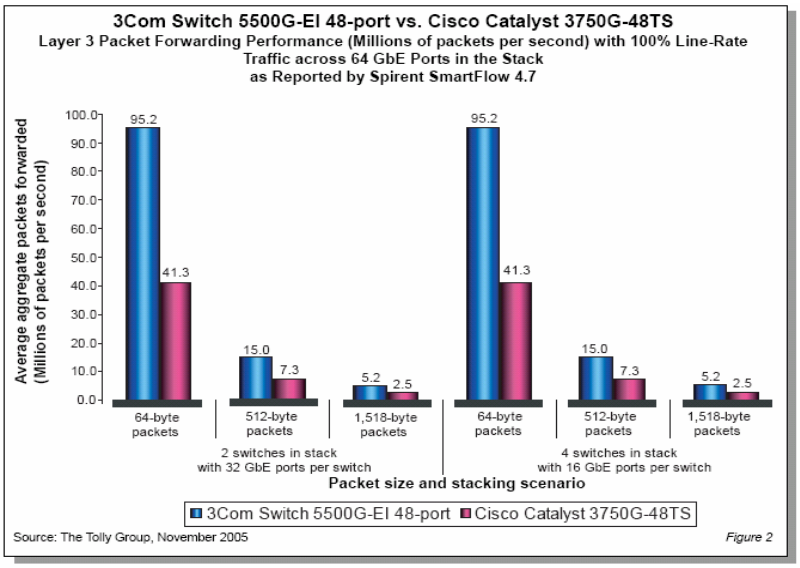


Figura 4.4. Muestra un reporte del Tolly Group sobre switchs 3Com y Cisco en capa 3.

2.- Cómo escoger los equipos más adecuados en la marca 3Com

Telefonía IP

Existen 2 teconologías posibles VCX y NBX, la primera se utiliza cuando se requiere niveles de redundancia y supervivencia altos, el segundo cuando lo que se busca es un sistema amigable y fácil de administrar, por lo que se ha elegido la plataforma NBX de 3Com.

Las opciones son V3000 y V3001R, ambas plataformas soportan un crecimiento de hasta 1500 puertos pero la segunda tiene fuente de poder y disco duro redundante.
Se ha elegido la opción de central telefónica V3000 porque es la que más se ajusta al presupuesto.

Switches

Los switches de core elegidos son 5500G debido a que son los únicos que soportan XRN a altas velocidades (hasta 96Gbps).

Los switches de borde se requieren que sus puertos sean 10/100, soporten vlans automáticas tanto en datos como telefonía IP, capas 2 y 3, capacidad de priorizar el tráfico de la red y soporte de enlaces agregados, los switches 4500 de 3Com son los más adecuados para esto.

Firewall/IPS

El equipo que posee estas dos funciones es el TippingPoint X505

Programa de administración

Existen 3 programas en 3Com, el más adecuado y sencillo de usar es el 3Com network Director ya que el 3Com Network Supervisor no posee funcionalidades de QoS y Vlans, por otro lado en programa EMS no maneja gráficos de topologías de red. El programa 3Com Network Director incluye un plug-in para Active Directory que permite manejar redes dinámicas con los switches 3Com.

3.- Diseño de la red

El siguiente cuadro corresponde a los equipos necesarios para red de la Universidad Cotopaxi.

Tabla 4.1: Cotización de equipos necesarios para la implementación.

Gig SFP Modules			Precio Unitari	Precio Total
1000BASE-SX SFP Transceiver	3CSFP91	2	$345	$ 690.00
LAN Switches				
3Com Switch 4500 Family				
Switch 4500 26-Port PWR	3CR17563-91	12	$1,500	$ 18,000.00
3Com Switch 5500 Family				
Gigabit Models				
Switch 5500G-EI 24 Port	3CR17250-91	2	$4,495	$ 8,990.00
Gigabit Model Additional Components				
Switch 5500G-EI Stacking Cable (65cm)	3C17262	1	$395	$ 395.00
Network Management				
Network Management Software				
3Com Network Director	3C15500	1	$3,495	$ 3,495.00
Security Solutions				
3Com X-Family				
3Com X506				
3Com X500 Digital Vaccine Subscription	3CX500-DV	1	$1,295	$ 1,295.00
3Com X506 Security Platform	3CRX506-96	1	$3,995	$ 3,995.00
Telefonía IP				
NBX V3000 Analog Platform	3C10600B-XX	1	$1,995	$ 1,995.00
NBX V3000 Four (4) Universal Card Slot Expansion Chassis	3C10605A-XX	1	$1,295	$ 1,295.00
NBX Analog FXO Line Card	3C10114C	2	$1,120	$ 2,240.00
NBX 3101 Basic Phone	3C10401B	20	$155	$ 3,100.00
3Com 3101SP Basic Phone with Speaker	3C10401SPKRB	20	$180	$ 3,600.00
3Com 3102 Business Phone	3C10402B	14	$240	$ 3,360.00
NBX 3105 Attendant Console	3C10405B	1	$225	$ 225.00
NBX Analog FXS Adapter	3C10400B-XX	4	$195	$ 780.00
NBX Group 1 Phone License	3C10411	40	$85	$ 3,400.00
			TOTAL	$ 56,855.00

La solución es de 60 teléfonos IP con 12 líneas troncales, 12 switches de acceso y 2 switches de Core, un Firewall/IPS y programa de administración.

4.- Parámetros para realizar la configuración de los equipos

El direccionamiento IP debe mantenerse el establecido previamente por la universidad por lo que se tendrán las siguientes redes, cada red corresponderá a una vlan diferente:

172.17.2.0 255.255.254.0

172.16.22.0 255.255.255.0

172.16.23.0 255.255.255.0

172.16.21.0 255.255.255.0

172.16.20.0 255.255.255.0

172.16.19.0 255.255.255.0

172.16.18.0 255.255.255.0

10.10.177.0 255.255.255.192

172.16.177.0 255.255.255.128

172.16.1.0 255.255.255.0

192.168.1.0 255.255.255.0

Las Vlans tendrán los siguientes nombres respectivamente:

VLAN 1: administracion

VLAN 2: Planta Baja

VLAN 3: 3er. Piso

VLAN 4: 1er. Piso

VLAN 5: Mezzanine

VLAN 6: 2do. Piso

VLAN 7: Anexo

VLAN 9: Red Wireless

VLAN 10: Red VIP

VLAN 11: VoIP

Con respecto a los enlaces agregados, habrá un enlace doble con cada uno de los switches de borde.

Central Telefónica NBX

Los siguientes cuadros se refieren a las clases de servicios que serán configurados en la central telefónica:

Class of Service	☒ = Default				
Default Route Point Group					
	Open	Closed	Lunch	Other	Forced Acct Code
Internal	☒	☒	☒	☒	

Local	☒	☒	☒	☒	☐
Long Distance	☒	☐	☐	☐	☐
International	☐	☐	☐	☐	☐
Toll Free	☒	☒	☒	☒	☐
Toll/Premium	☐	☐	☐	☐	☐
WAN	☒	☒	☒	☒	☐
CO/Phone Exchange Code	☐	☐	☐	☐	☐
Trunk to Trunk	☐	☐	☐	☐	☐
Alternate Carrier (Equal Access #)	☒	☒	☒	☒	☐
Operator Assisted	☐	☐	☐	☐	☐
Wireless	☒	☒	☒	☒	☐
Diagnostics	☐	☐	☐	☐	☐
Other	☒	☒	☒	☒	☐
Emergency (911 and E911)	✓	✓	✓	✓	
System Operator	Enabled ☐				
Personal Operator	Enabled ☐				
Off-site Notification	Enabled ☐				
CLIR Features	Enabled ☐				

Default User Group					
	Open	Closed	Lunch	Other	Forced Acct Code
Internal	☒	☒	☒	☒	
Local	☒	☒	☒	☒	☐
Long Distance	☒	☐	☐	☐	☐
International	☐	☐	☐	☐	☐
Toll Free	☒	☒	☒	☒	☐
Toll/Premium	☐	☐	☐	☐	☐
WAN	☒	☒	☒	☒	☐
CO/Phone Exchange Code	☐	☐	☐	☐	☐
Trunk to Trunk	☐	☐	☐	☐	☐

Alternate Carrier (Equal Access #)	☒	☒	☒	☒	☐
Operator Assisted	☐	☐	☐	☐	☐
Wireless	☒	☒	☒	☒	☐
Diagnostics	☐	☐	☐	☐	☐
Other	☒	☒	☒	☒	☐
Emergency (911 and E911)	✓	✓	✓	✓	
System Operator	Enabled ☐				
Personal Operator	Enabled ☐				
Off-site Notification	Enabled ☐				
CLIR Features	Enabled ☐				

Class of Service, continued ☒ = Default

Super User Group					
	Open	Closed	Lunch	Other	Forced Acct Code
Internal	☒	☒	☒	☒	
Local	☒	☒	☒	☒	☐
Long Distance	☒	☒	☒	☒	☐
International	☒	☒	☒	☒	☐
Toll Free	☒	☒	☒	☒	☐
Toll/Premium	☒	☒	☒	☒	☐
WAN	☒	☒	☒	☒	☐
CO/Phone Exchange Code	☒	☒	☒	☒	☐
Trunk to Trunk	☒	☒	☒	☒	☐
Alternate Carrier (Equal Access #)	☒	☒	☒	☒	☐
Operator Assisted	☐	☐	☐	☐	☐
Wireless	☒	☒	☒	☒	☐
Diagnostics	☒	☒	☒	☒	☐
Other	☒	☒	☒	☒	☐
Emergency (911 and E911)	✓	✓	✓	✓	

System Operator	Enabled ☒
Personal Operator	Enabled ☒
Off-site Notification	Enabled ☐
CLIR Features	Enabled ☐

Con respecto a los horarios de la central serán los siguientes:

Business Hours (Time of Day Service Modes)					
Open					
Open?		From		To	
☐	Monday	H:8	M:00	H:13	M:00
☐	Tuesday	H:8	M:00	H:13	M:00
☐	Wednesday	H:8	M:00	H:13	M:00
☐	Thursday	H:8	M:00	H:13	M:00
☐	Friday	H:8	M:00	H:13	M:00
☐	Saturday	H:8	M:00	H:13	M:00
☐	Sunday	H:8	M:00	H:13	M:00

Lunch					
Open?		From		To	
☐	Monday	H:13	M:00	H:14	M:00
☐	Tuesday	H:13	M:00	H:14	M:00
☐	Wednesday	H:13	M:00	H:14	M:00
☐	Thursday	H:13	M:00	H:14	M:00
☐	Friday	H:13	M:00	H:14	M:00
☐	Saturday	H:13	M:00	H:14	M:00
☐	Sunday	H:13	M:00	H:14	M:00

Other					
Open?		From		To	
☐	Monday	H:14	M:00	H:19	M:00
☐	Tuesday	H:14	M:00	H:19	M:00

☐	Wednesday	H:14	M:00	H:19	M:00
☐	Thursday	H:14	M:00	H:19	M:00
☐	Friday	H:14	M:00	H:19	M:00
☐	Saturday	H:14	M:00	H:19	M:00
☐	Sunday	H:14	M:00	H:19	M:00

El mapeo de los botones de los teléfonos ejecutivos será el siguiente

Button Mapping Groups, 3102 Business Telephones								
Default 3102 Business Group								
	Feature		Headset					
	Transfer to VMail							
	Call Park							
	Call Pickup							
	Paging							
	System							
	System							
	System		Release					

Con respecto al sistema de seguridad

Los parámetros básicos del firewall corresponden a los siguiente datos:

IP Services	Primary	Secondary	Tertiary
DNS Servers	200.31.6.34	200.31.6.38	

SNTP Server	200.31.6.34		

Email Server	172.17.2.23		

Default Route	200.31.6.31		

Static Routes

Interface	Route	Next Hop	Cost
172.17.2.0 255.255.254.0	172.17.2.1		60
172.16.22.0 255.255.255.0	172.17.2.2		60
172.16.23.0 255.255.255.0	172.17.2.3		60
172.16.21.0 255.255.255.0	172.17.2.4		60
172.16.20.0 255.255.255.0	172.17.2.5		60
172.16.19.0 255.255.255.0	172.17.2.6		60
172.16.18.0 255.255.255.0	172.17.2.7		60
10.10.177.0 255.255.255.192	172.17.2.8		60
172.16.177.0 255.255.255.128	172.17.2.9		60
172.16.1.0 255.255.255.0	172.17.2.10		60
192.168.1.0 255.255.255.0	172.17.2.11		60

Interfaces	WAN	LAN1	LAN2
Security Zone Name	WAN	LAN	
IP Address	200.31.6.32	172.17.2.254	
Mask	255.255.255.0	255.255.255.0	
DGW	200.31.6.30		

Host Name	Ucotopaxi

Host Location	RACK

4.1.2. Características del hardware a ser utilizado.

Plataforma telefónica IP NBX.

El procesador de llamadas de red (NCP), es quien maneja el tráfico de llamadas de la red, la mensajería, la información almacenada en el disco , fuente de poder, los conectores de red frontales y dispositivos externos.

La NBX V3000 viene con una memoria de 128 MB.

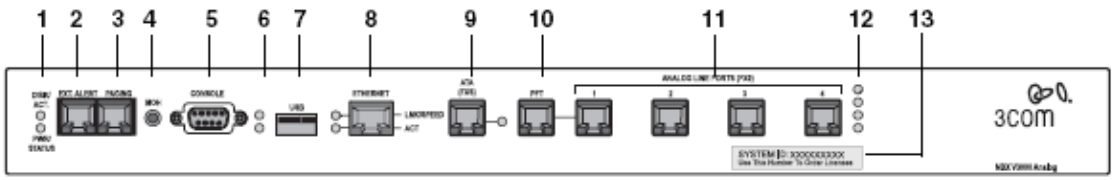


Figura 4.5. Muestra a los conectores y LEDS de la NBX V3000

1.- Estatus de la luz.- muestra la actividad del disco.

Estado:

Luz de color verde titilando.- El sistema se esta cargando

Luz de color rojo titilando.- El sistema tuvo una falla al cargar

Luz de color verde fija.- El sistema es operacional

2.- Alerta Externa.- reservado para uso futuro

3.- *Paging*.- conecta un amplificador analógico, a través de un conector RJ-11 de 600 Ohm.

4.- *MOH*.- Conecta un *mini-jack*, (3,5 mm mono o estéreo), que acepta música en espera (máximo 2V pico a pico), de una línea externa de un CD placer o de otro equipo reproductor de música.

5.- Consola.- Conector DB9 que provee un Terminal RS-232 (DCE) para la configuración vía consola.

6.- Estatus de Luz.- muestran el siguiente estatus.

Verde titilante.- La secuencia de inicio del sistema se ha inicializado.

Verde fijo.- La inicialización del disco esta completada.

7.- USB.- Reservado para usos futuros.

8.- *ETHERNET*.- conexión de puerto uplink ethernet 10/100 Mbps.

Los colores indican las siguientes velocidades:

Amarillo.- Velocidad de 10 Mbps.

Verde.- Velocidad de 100 Mbps.

Apagado.- No hay enlace.

Cuando titilan los leds indican actividad en el puerto.

9.- *ATA (FXS).-* Adaptador de Terminal analógica puerto RJ11 FXS (*Foreign Exchange Station),* dispositivo para conectar un terminal analógico, como un teléfono análogo o una máquina de fax, el led asociado con el puerto indica el estado del puerto.

10.- *Puerto PFT.-* Puerto de transferencia de falla de poder, el conector RJ11 acepta cualquier clase de teléfono analógico. Durante una falla de poder en la central telefónica, el puerto se activa y provee tono de marcado y servicio telefónico.

11.- *Puerto de líneas analógicas.-* 4 puertos RJ11 Foreign Exchange Office (FXO), puertos que conectan las líneas telefónicas a la oficina central.

12.- *Estatus de la luz.-* muestra el estado de cada puerto FXO.

Estado:

Luz titilando.- El puerto esta en actividad

Luz de color rojo titilando.- El puerto tuvo una falla al cargar

Luz de color verde fija.- El puerto es operacional

13.- Número de identificación.- Muestra el número del *System ID*, el número serial y la dirección MAC Address de los puertos analógicos.

4.1.3. Instalación de la NBX.

El acceso al sistema de la NBX se lo realiza vía puerto de consola y se tiene que modificar la dirección IP de la NBX en caso de que se encuentre en otra red.

Se tiene que realizar los siguientes pasos para la configuración inicial de la NBX:

- Retirar todos los módulos del chasis de la NBX.
- Conecte el cable de poder a la NCP de la NBX.
- Encienda el interruptor de poder
- Observe los LED sobre la parte frontal de la unidad. Esto indica la actividad durante el ciclo de inicialización de la NBX.
- Los LED serán la primera señal de indicación durante una instalación o durante el mantenimiento de la NBX.

- Fije una PC al puerto de consola de la NBX. Dependiendo de la NBX que usted está usando, podría tener más de un puerto de consola. Si esto es el caso, entonces coloque el cable de una PC al puerto de consola en el COM1.
- En un PC, inicie HyperTerminal (o el programa de emulación de terminal de su elección). Los parámetros de comunicaciones son 9600 bps, 8 bits de datos, sin paridad, y sin control de flujo.
- Dentro del Terminal de emulación escriba el comando nbxIpConfig (sensible a mayúsculas y minúsculas) y presione la tecla de "enter". Esto permitirá que usted ponga el nombre del host, la dirección IP, máscara de subred, *default gateway* para la NBX.
- La NBX de la Universidad Cotopaxi se configuró de la siguiente manera:

  Nbx3000->nbxIpConfig
  Change IP Configuration: (press ENTER to accept current values)
  hostname : nbx3000
  inet address : 192.168.1.190
  net mask : 255.255.255.0
  gateway inet : 192.168.1.254

- Configuración nueva IP:

  hostname : UCotopaxi
  inet address : 192.168.1.190
  net mask : 255.255.255.0
  gateway inet : 192.168.1.254

Cuando se realiza un cambio en el *Hostname*, dirección inet, mascara de red y Puerto de enlace, requiere que el sistema se reinicie.
Guardar cambios en el disco? (y/n) : n y
Cambio aceptado. La configuración IP ha sido guardada en el disco.
Nbx3000->

Se debe reinicializar la NBX con los nuevos ajustes. Presione la tecla de "Ctrl" y la tecla de "R" reinicializar su NBX simultáneamente. Durante esta inicialización, observe el NCP cargar el proceso sobre su computadora en HyperTerminal o el

programa final que se está usando. Cuando la siguiente cadena aparece sobre la pantalla, el proceso de boot ha terminado completamente: htfsLibSetSynchIO (1).

Se necesitará cambiar la dirección IP de su PC con el propósito de que esté en la misma subred con la NCP.

Inicie web explorer de su PC e ingrese la dirección IP del NCP. Seleccione el botón de administrador. Entre al sistema como el administrador. (*Login*: administrador y *passwords*: 0000), los registro de entrada y contraseñas son sensibles a mayúsculas y minúsculas.

Seleccione Mantenimiento del sistema del menú principal y borre los datos, como lo muestra la figura 4.3, al realizar esta acción borraremos toda la configuración que tiene la NBX. Seleccione el botón *Database*.

Figura 4.6. Pantalla para borrar los datos almacenados en la NBX.

Hacer clic en OK cuando pregunta, "Usted desea restaurar a *factory defaults*". Su sistema reinicializará ahora automáticamente. Una pantalla aparecerá desplegando el siguiente mensaje "El sistema ha sido reinicializado después de algunos minutos". Haga clic en cerrar.

Ingrese la información de la empresa, las horas de trabajo y Tiempo.

Mientras ingresa al *NetSet* como administrador, seleccione *System Wide Settings* y *Business Information* del menú principal.

Ingrese en los siguientes campos apropiados:

- Nombre de la empresa: Universidad Cotopaxi
- Dirección: Av Simón Rodríguez
- Ciudad: Latacunga
- Estado / provincia: Cotopaxi
- Código postal: 0
- País: Ecuador
- Contactos: Mauricio Cerda
- Teléfono: 032813156
- Fax: 032813157
- Email: mcerda@utc.edu.ec

Los datos ingresados es la información de la empresa que será exhibido en informes y en el plan de marcación.Hacer clic en aplicar.

Seleccione el tabulador de Horas de la empresa en lo alto de la pantalla, de información de la empresa, seleccione *System Wide Settings* y *Business Hours*.

Se ingreso las horas de trabajo de la Universidad Cotopaxi desde las 7:00 hasta las 21: 00, de lunes a viernes. Hacer clic en aplicar, como se lo muestra en la figura 4.7.

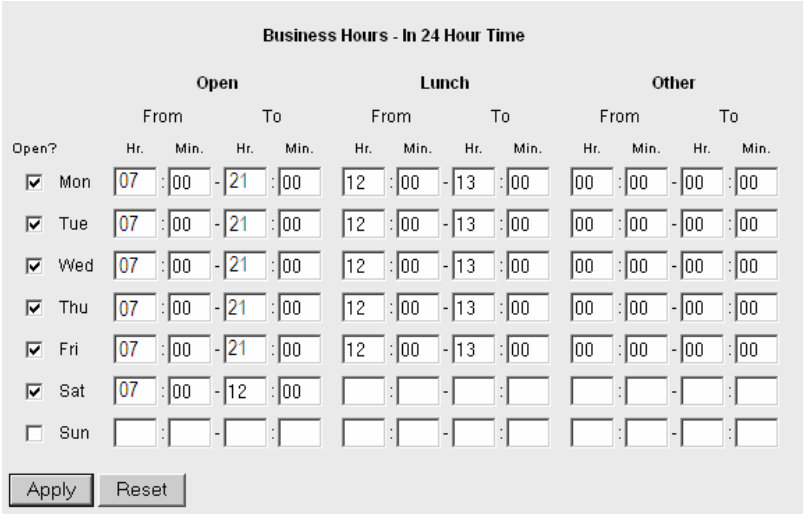


Figura 4.7. Pantalla para ingresar las horas de trabajo, *lunch,* y otros de la NBX.

Seleccione *System Wide Settings*, coloque la fecha y tiempo en el menú principal. Coloque la fecha y tiempo de la NBX, como se lo muestra en la figura 4.8.

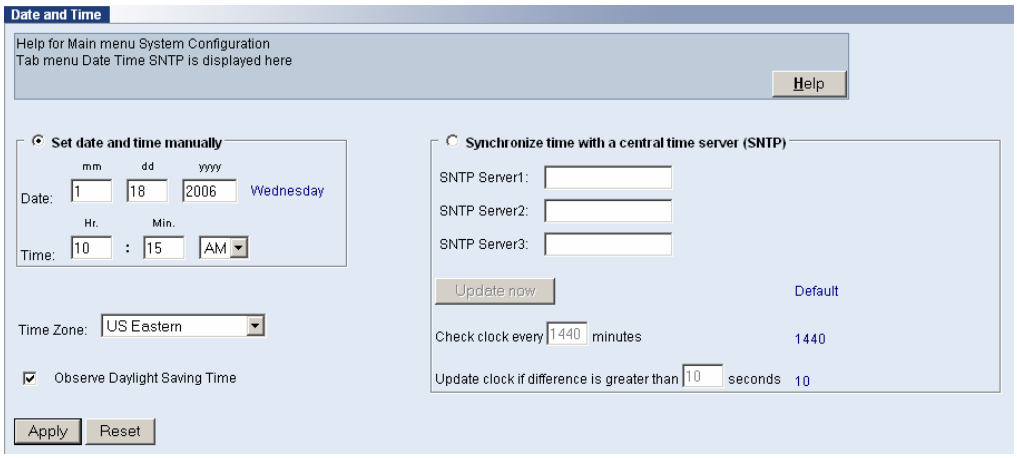


Figura 4.8. Pantalla para ingresar la fecha y hora de la NBX.

El software de NBX manejará los nuevos cambios de tiempo de DST. Además, los nuevos husos horarios serán añadidos:

• Canadá oriental
• Canadá central
• Montaña de Canadá
• Canadá Pacifico
• México central
• Montaña de México
• México Pacifico

Note que se puede sincronizar el tiempo con un servidor de hora central (SNTP).

4.1.4. Configuración básica de la NBX.

Instalación de teléfonos en la NBX y reemplazo.

- Del menu principal del NetSet de la NBX, seleccione *System Wide Settings*, y escoja *feature System Wide*, como se lo muestra en la figura 4.9.

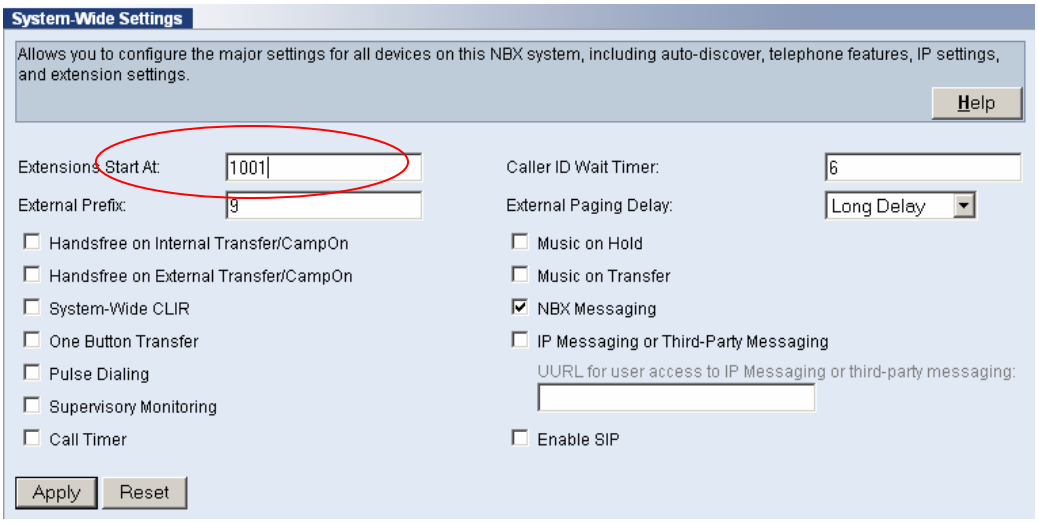


Figura 4.9. Pantalla que permite ingresar la configuración de *System Wide settings.*

- Las extensiones de la Universidad Cotopaxi inician desde la 1001.
- Hacer clic en aplicar.
- Del menu principal del NetSet , seleccione *System Wide Settings*, descubrimiento automático, como se lo muestra en la figura 4.10.

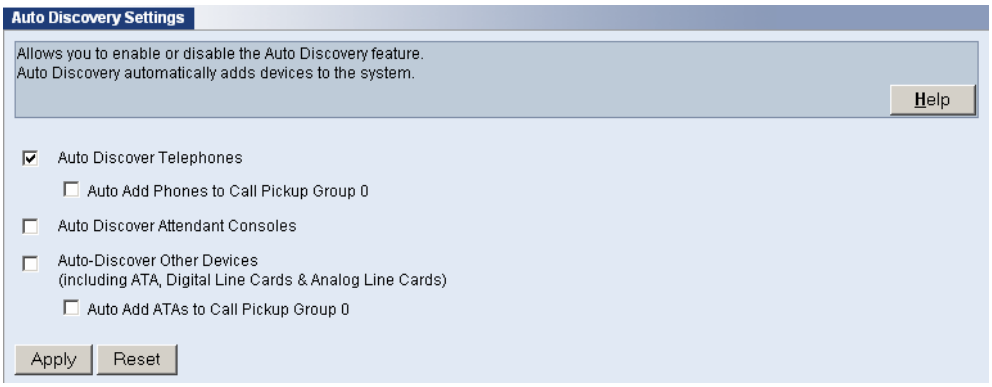


Figura 4.10. Pantalla que permite activar el descubrimiento automático de teléfonos.

- Seleccione descubrimiento automático de teléfonos.
- Hacer clic en aplicar.
- Usando un cable *Ethernet*, conecte el primer teléfono a la red *Ethernet*.
- La mayoría de los teléfonos de NBX son 802.3af y pueden recibir su poder de un interruptor de Poe de *Ethernet* directamente. Algunos teléfonos requieren el poder local.

- Observe los paneles de LCD de teléfonos. Demostrará su estado en curso y cuándo ha sido asignado una extensión.
- La extensión asignada debe ser 1001.
- Probar los teléfonos discando de teléfono a teléfono. Observe las luces de estado sobre el interruptor de Ethernet con el que los teléfonos están conectados. Observar las luces de estado cuándo:
    - Levanta el auricular del teléfono
    - Suena
    - Marca un simple digito
    - Habla
    - Colgado
    - Presiona el botón para hablar.
- Cambie de lugar el cable para uno de los teléfonos para otro puerto del *switch* para simular un usuario que se traslada a un nuevo escritorio.
- Llame otro teléfono de esa extensión. Note que todo trabaja como antes.
- Usted puede verificar el estado de teléfonos escogiendo configuración de teléfonos. El estado de los teléfonos deben estar "En línea", como se observa en la figura 4.11.

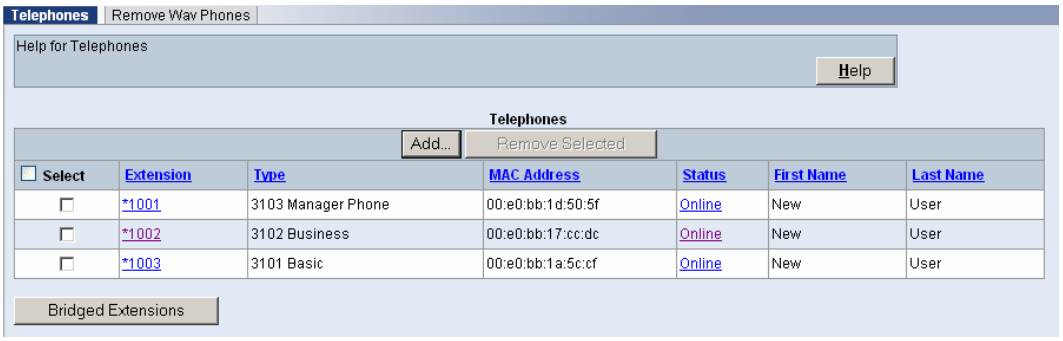


Figura 4.11. Muestra las extensiones telefónicas que fueron descubiertas y sus respectivos estados.

- Del menú principal del *Netset* de la NBX, seleccione *System Wide Configuration*.
- Deshabilite descubrimiento automático de teléfonos.
- Hacer clic en aplicar

- Es importante deshabilitar el descubrimiento de teléfonos después de una instalación para prevenir teléfonos intrusos, que son instalados en la NBX. Empezar con una extensión, por ejemplo la 1001, presionar el botón de mensajería. Seguir las instrucciones dictadas, y grabar un saludo como se lo desee.
- Existen dos formas de identificar nuevos teléfonos, por número de extensión o por su dirección MAC. Los teléfonos de la NBX muestran su número de extensiones sobre el LCD y este debe tener su dirección MAC en el mismo teléfono.
- Remover un teléfono descubierto, ingrese a Usuarios a través del menú principal del *Netset*, este teléfono es identificado, seleccione la extensión que se desea eliminar, y hacer un clic en remover lo seleccionado, como se lo muestra en la figura 4.12

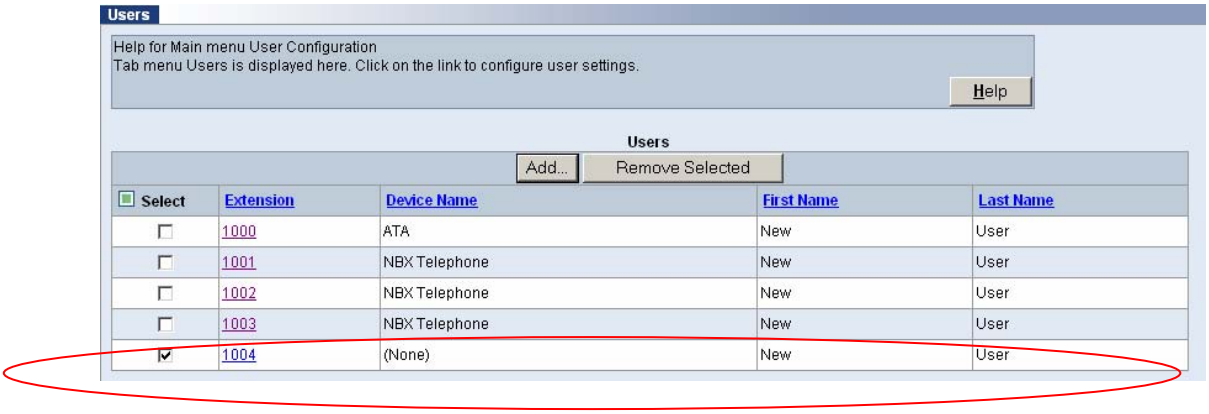
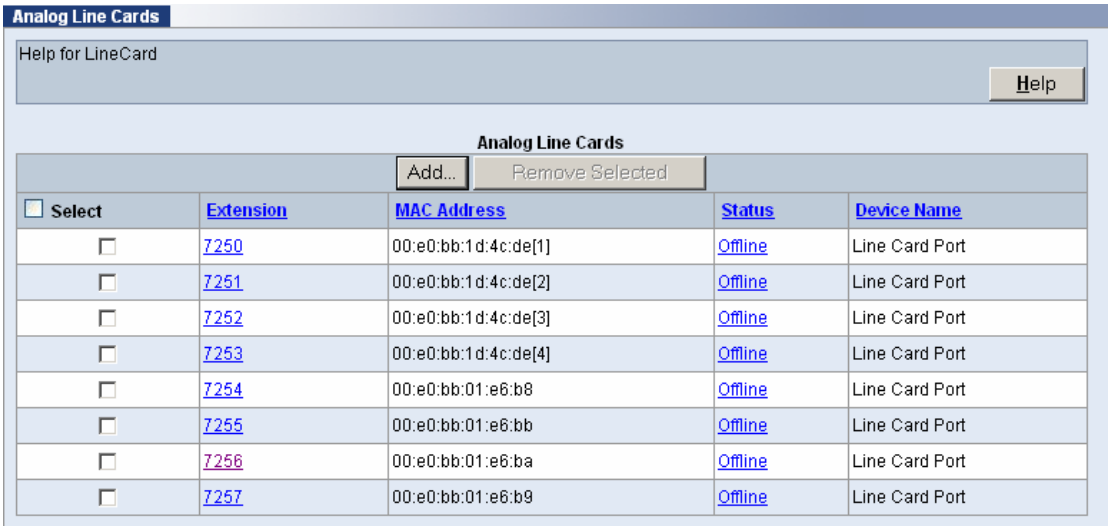


Figura 4.12. Muestra la lista de usuarios en la NBX.

Instalación de tarjetas de líneas analógicas (ALC).

- Del menú principal de la NBX, seleccione *System Wide Settings*, descubrimiento automático.
- Seleccione descubrimiento automático de otros dispositivos.
- Hacer clic en aplicar.
- Inserte el ALC en el chasis de la NBX y conecte el chasis a la red Ethernet.
- Verifique que el ALC haya sido descubierto escogiendo la configuración de Gateway de PSTN, las tarjetas de línea análogas del menú principal del NetSet. Vea la lista de ALCs en línea. Como lo muestra la figura 4.13.



Select	Extension	MAC Address	Status	Device Name
☐	7250	00:e0:bb:1d:4c:de[1]	Offline	Line Card Port
☐	7251	00:e0:bb:1d:4c:de[2]	Offline	Line Card Port
☐	7252	00:e0:bb:1d:4c:de[3]	Offline	Line Card Port
☐	7253	00:e0:bb:1d:4c:de[4]	Offline	Line Card Port
☐	7254	00:e0:bb:01:e6:b8	Offline	Line Card Port
☐	7255	00:e0:bb:01:e6:bb	Offline	Line Card Port
☐	7256	00:e0:bb:01:e6:ba	Offline	Line Card Port
☐	7257	00:e0:bb:01:e6:b9	Offline	Line Card Port

Figura 4.13: Muestra las extensiones de las tarjetas de líneas analógicas.

- Primero se mostrarán las extensiones propias de la NBX y luego las extensiones dadas por el chasis con las ALCs.
- Las direcciones MAC sobre el ALC están desde la más baja a la más alta de izquierda a derecha.
- Del menú principal de la NBX, seleccione configuración del *System Wide*, descubrimiento automático.
- Desactive el descubrimiento automático de otros dispositivos.
- Hacer clic en aplicar.

Clases de Servicio

La clase de servicio (CoS) es un juego de los permisos para llamadas que el administrador atribuye a sus usuarios. Estos permisos están sujetos a parámetros como Horas de trabajo de la empresa: Abierta, almuerzo, y otros.

Modificar Clase de Servicio para un grupo existente.

- Seleccione configuración de usuarios, clase de servicio del menú principal del *Netset*, como en la figura 4.14.

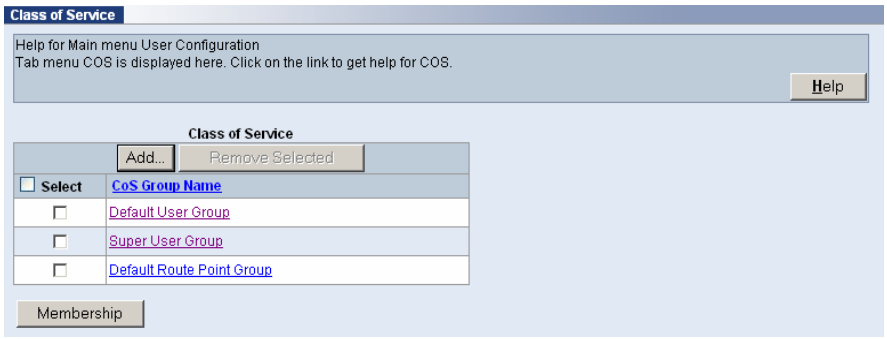


Figura 4.14. Muestra los grupos de clase de servicio creados.

- Hacer clic en *Default User Group*, y se les desplegará la siguiente pantalla mostrada en la figura 4.15.

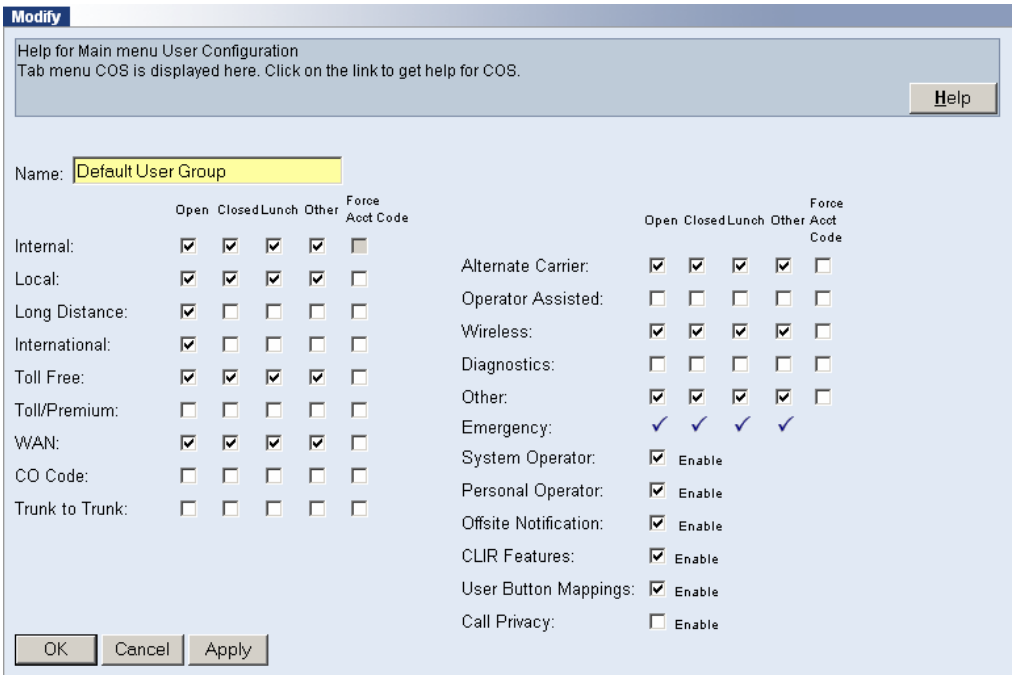


Figura 4.15. Muestra los permisos que tiene un grupo de usuarios.

- Para añadir un nuevo grupo de clase de servicio, ingrese a configuración de usuarios.
- .Hacer clic en añadir.
- Se crea la nueva clase de servicio, y se configura los privilegios del grupo según las necesidades de la Universidad, como se lo muestra en la siguiente figura 4.16.

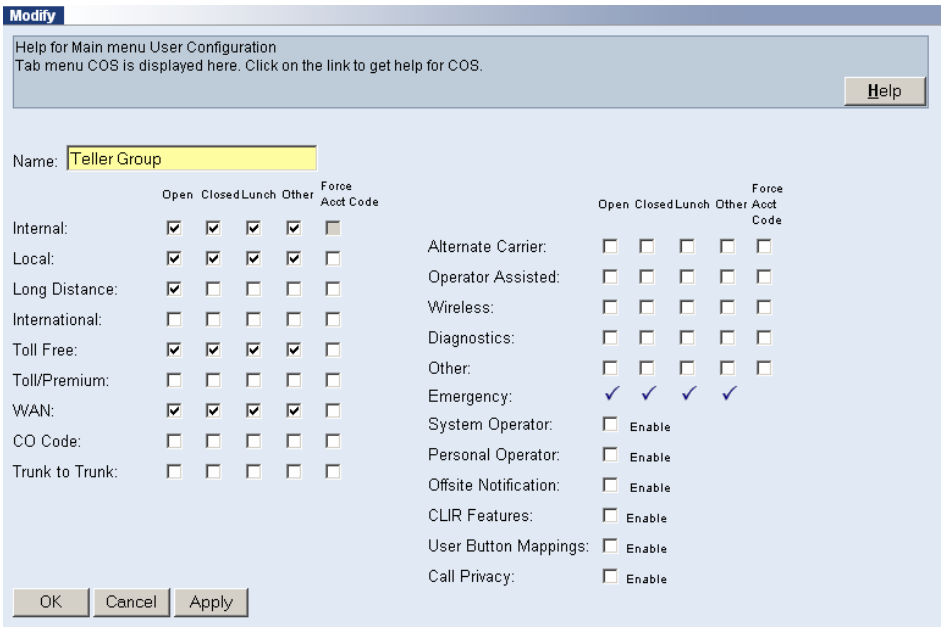


Figura 4.16. Muestra un nuevo grupo con sus respectivos permisos en su clase de servicio.

Configuración de Usuarios.

La configuración de usuarios para los teléfonos de la NBX ATA o ATC, descubiertos por la NBX, para la configuración de usuarios se tendrá que escribir la siguiente información: nombre, apellido, titulo, clase de servicio y localización.

Para la configuración de usuarios seguimos los siguientes pasos:

- Del menú principal de la NBX, seleccione Configuración de usuarios, Usuarios, dentro del cual se desplegará la siguiente figura 4.17.

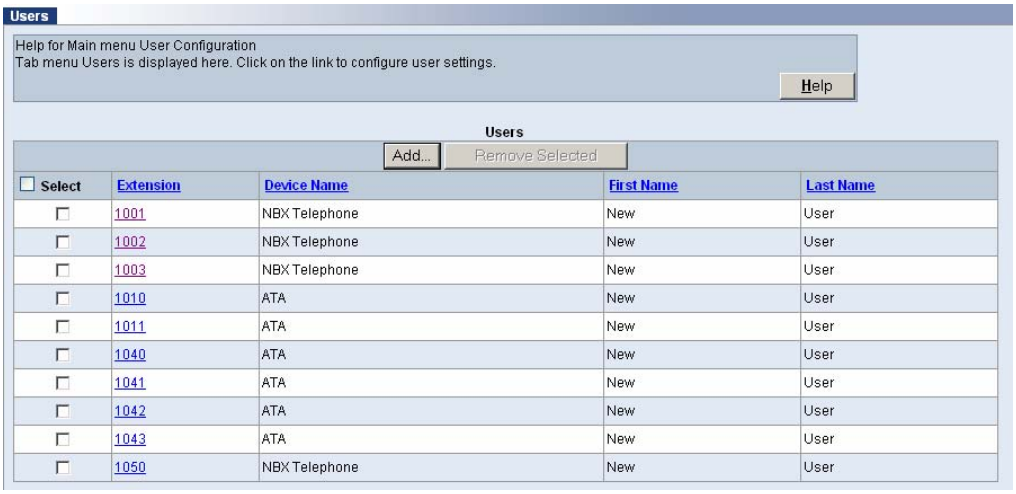


Figura 4.17. Muestra los usuarios conectados a la NBX.

- Configure cada usuario con los datos apropiados haciendo clic en su extensión. Revise que estén bien colocados los datos y haga clic en OK.

Mapeo de botones de los teléfonos IP.

Es necesario mapear botones en los teléfonos IP, debido a que facilitan el discado a los usuarios, y obtener rápidamente funcionalidades de la PBX.

Para realizar el mapeo de botones a los teléfonos realizamos los siguientes pasos:

- Del menú principal de la NBX, seleccione configuración telefónica y elija teléfonos.
- Seleccione la extensión 1001 o la extensión que usted desee mapear.
- Hacer clic en *Button Mapping*.
- Seleccione un botón que esta configurado con marcación personal rápida y cambie a directorio, como lo muestra la figura 4.18.
- Hacer clic en aplicar.

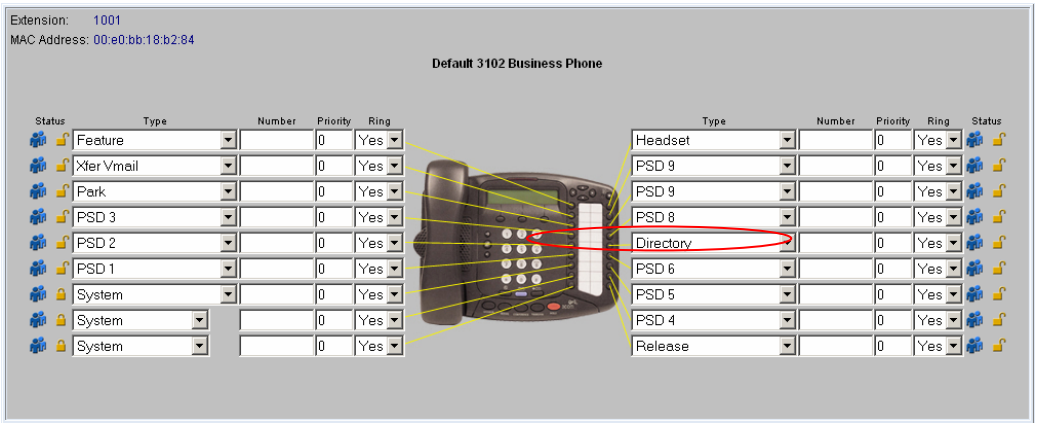


Figura 4.18. Muestra los botones disponibles en los teléfonos para dar una aplicación.

- Al presionar el botón programado como directorio, se puede observar en el LCD del teléfono todos los usuarios que se encuentran en la NBX.

Mapeo de botones para grupos de teléfonos.

Para mapear botones por grupo de teléfonos, realizamos los siguientes pasos:

- Del menú principal de la NBX, seleccione configuración telefónica y grupos de teléfonos.

- Seleccione los teléfonos 3102 *Business Group*.
- Hacer clic en mapeo de botones.
- Seleccione un botón que este configurado con PSD y cámbielo a directorio, como se lo muestra en la figura 4.19.

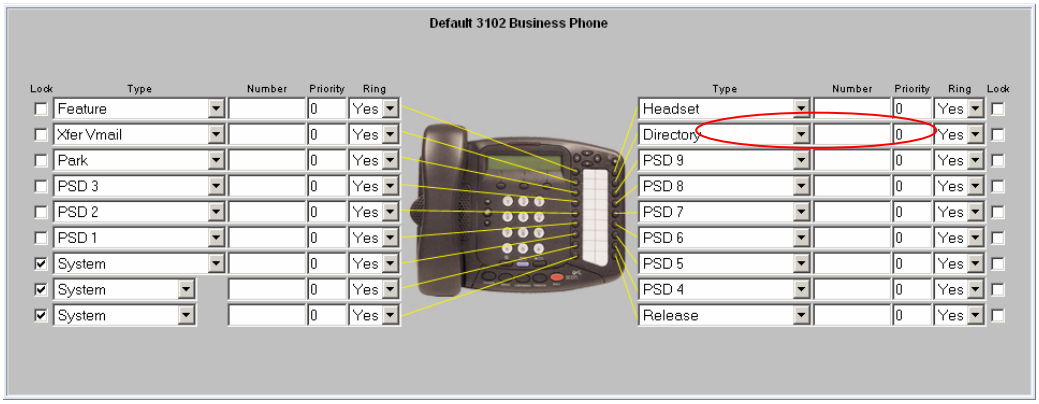


Figura 4.19. Muestra el mapeo de los botones del teléfono 3102.

- Hacer clic en aplicar
- Evalué este ajuste sobre todos sus teléfonos 3102 presionando el botón de programado sobre cada uno y vea el LCD.

Marcación rápida del sistema y personal.

Los administradores pueden crear hasta 100 sistemas de marcación rápida para el acceso rápido a los números comunes marcados. Los administradores también pueden arreglar la marcación rápida del sistema a través de la clase del servicio del usuario. Los números de marcación rápida del sistema no están sujetos a restricciones de servicio (CoS) así que un número de marcación rápida al realizar una llamada interurbana está asequible a los usuarios incluso si sus CoS no admite las llamadas interurbanas.

Usuarios también pueden crear las definiciones de marcación rápida personal y asignar a grupos de teléfono. No confunda los códigos de marcación rápida con números de extensiones. Cualquier teléfono en un grupo de teléfonos tiene acceso para las mismas definiciones de botones. Los usuarios pueden crear marcación personal rápida para botones que no han sido configurados. Los usuarios también pueden

cambiar las definiciones para cualquier botón como botón de marcación personal rápida, incluso si esos botones son definidos como en un grupo de botones mapeados. Los números de marcación personal rápida están sujetos a CoS.

Marcación rápida del sistema.

- Del menú principal de la NBX, selecione *Feature Settings*, marcación rápida del sistema.
- Verifique la primera opción que corresponda con la identificación 700.
- Ingrese el número 92554444 para marcación rápida.
- En el campo de comentarios puede ingresar el nombre de la persona o institución a la que esta llamando, como se muestra en la figura 4.20.
- Hacer clic en aplicar.

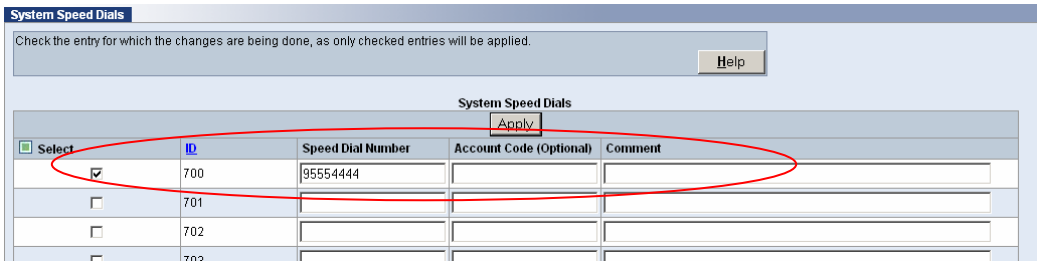


Figura 4.20. Pantalla que permite ingresar números telefónicos , con su código de cuenta y comentarios, para el sistema de marcación rápida.

- Seleccione el grupo de teléfonos 3102 Business.
- Hacer clic en mapeo de botones.
- Seleccione un botón que este configurado con PSD y cámbielo a SSD 0.
- Hacer clic en aplicar.
- La marcación rápida del sistema empieza desde el 700 al 799. El SSD 0 hasta el 99 corresponde con el último número o los últimos dos números de la identificación. Ejemplos; la marcación rápida con la identificación 709 será el SSD 9 de SSD, marcación rápida del sistema con el ID 712 será el SSD12.
- Verifique que el botón haya sido programado con marcación rápida del sistema presionándolo sobre cualquiera de los grupos de teléfonos. Los números se visualizarán sobre el LCD.

Marcación Rápida Personal.

Para la marcación rápida personal realizamos la siguiente configuración.

- Abrir una nueva ventana de navegador
- Entre al sistema como usuario 1002 con contraseña 1234.
- Del menú principal seleccione Directorio.
- Seleccione marcación rápida personal.
- Seleccione la extensión 601.
- Ingrese el número 90945551234 en el campo de marcación rápida, como lo muestra la figura 4.21.
- Hacer clic en aplicar.

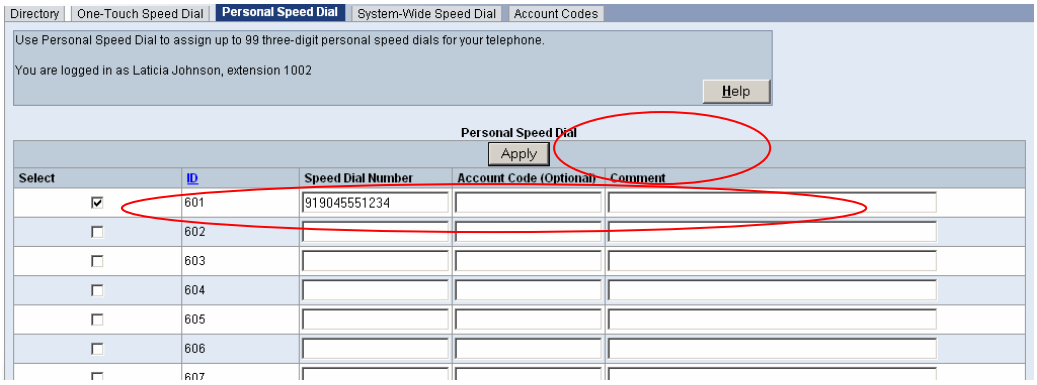


Figura 4.21. Pantalla que permite ingresar números telefónicos, con su código de cuenta y comentarios, para la marcación rápida personal.

- Del menú principal de la NBX, seleccione programación del teléfono.
- Hacer clic en mapear botones.
- Ubique un botón que este configurado con PSD1. Si no hay uno, configuré un botón.
- Sobre el teléfono físico asignado la extensión 1002, presione ese botón. El teléfono debe realizar la marcación rápida a ese número. El número se visualizará sobre el LCD.
- Las identificaciones de marcado personal rápido empiezan desde el número 601 hasta el 699. Por ejemplo, la identificación 601 se deberá mapear el botón con PSD1, los PSD corresponden al último o a los dos últimos números de la identificación.

Apariencia de estación puente.

La apariencia de estación de puente es usada entre un director y un subordinado para la cobertura de llamadas a menudo. Para configurar la apariencia de estación puente realizamos los siguientes pasos.

- Del menú principal de la NBX, seleccione configuración telefónica, teléfonos.
- Seleccione la extensión 1001.
- Hacer clic en mapeo de botones.
- Configure 3 botones programables como extensiones de puente mapeadas a la extensión 1001, como se los muestra en la siguiente figura 4.22.

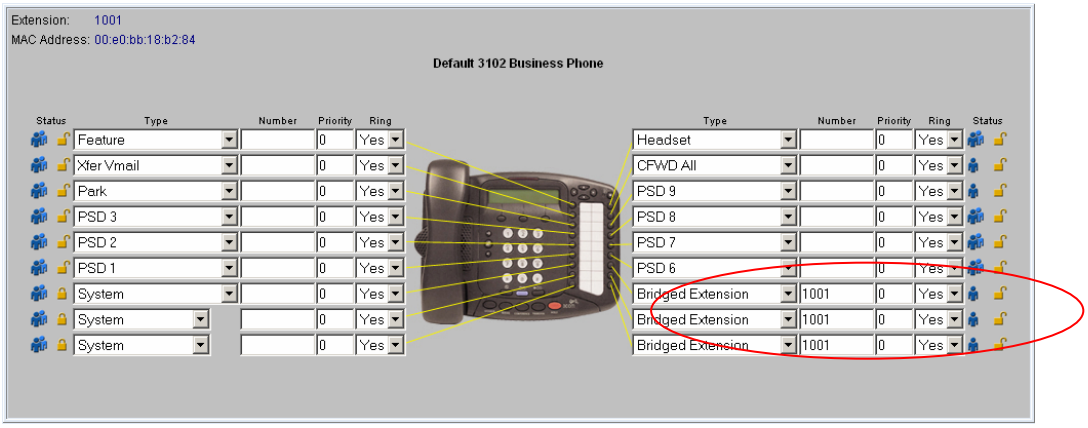


Figura 4.22. Mapeo de botones para que tengan la funcionalidad de extensión puente.

Correo de Voz

Recuperación de correo de voz para usuarios.

Los mensajes de correo de voz pueden ser recuperados a nivel local o remotamente. (Presionar el botón de mensajes que es un ejemplo de recuperación local. Para conectarse con la NBX desde una línea exterior y presionar ** para hacer un *bypass* a la atendedora automática y escuchar los mensajes de voz, son un ejemplo de la recuperación lejana de los mensajes de voz). Para recuperar los mensajes de voz realizamos los siguientes pasos:

- Abra una nueva ventana de un navegador.
- Hacer clic en el botón de usuario.
- Entre al sistema con la extensión 1002 y coloque su contraseña por ejemplo1234.

- Sobre el registro de entrada estará mis mensajes, en el buzón de voz. Se podrán observar los mensajes que han sido dejados para usted.
- Seleccione uno de los mensajes de correo de voz.
- Haga clic en play. Su reproductor preferido de sonido empezará a reproducir el archivo, como se lo muestra en la siguiente figura 4.23.

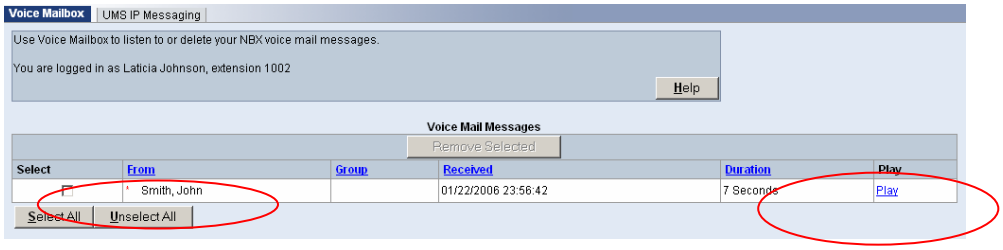


Figura 4.23. Pantalla para reproducir los mensajes dejados en las extensiones.

Contraseña perdida.

Es común que los usuarios olviden sus contraseñas del buzón de voz. Para borra el *password* de los usuarios realizamos los siguientes pasos:

- Del menú principal de la NBX, seleccione mantenimiento del sistema y la administración de contraseñas.
- Seleccione contraseña de usuario.
- Hacer clic en *ir*.
- Una lista de las extensiones aparecerá, como lo muestra la figura 4.24.
- Seleccione por ejemplo la extensión 1002.
- Hacer clic en el botón de reset contraseña.

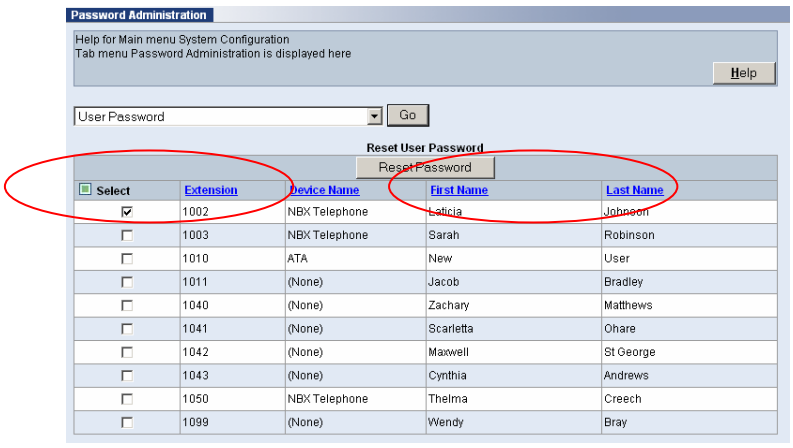


Figura 4.24. Muestra las extensiones que su *password* puede ser reseteado.

- Hacer clic en OK en la notificación de la contraseña para 1 usuario con éxito, como se lo muestra en la figura 4.25.

Figura 4.25. Muestra que se ha reseteado el *password* con éxito.

- Verifique la nueva contraseña presionando el botón de mensaje en la extensión 1002.
- Coloque un password nuevo en la extensión 1002.

Notificación al exterior.

La notificación exterior puede ser vía teléfono, *pager* o correo electrónico. Antes que un usuario pueda hacer la configuración a exterior, el administrador debe hacer cambios en la clase de servicio del usuario y permitir la notificación exterior para el intercambio de mensaje

s de NBX. No se podrá recibir una notificación exterior si su clase de servicio no tiene acceso para una línea externa.

- Del menú principal de la NBX, seleccione configuración de usuario, clase de servicio.
- Seleccione Default User Group.
- Verifique que la notificación exterior esté activada. Si no lo es, colocar un visto en notificación al exterior, como se lo muestra en la figura 4.26.
- Hacer clic en OK.

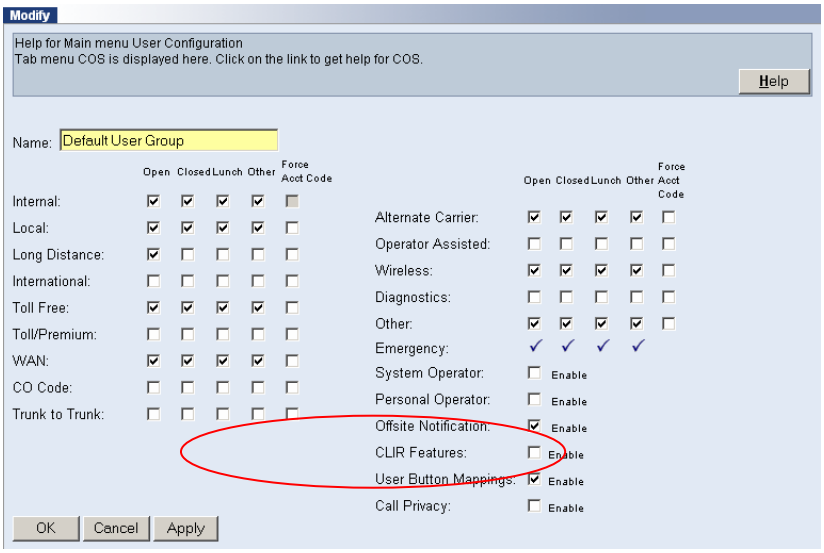


Figura 4.26. Configuración en la clase de servicio para que los usuarios puedan realizar notificación al exterior.

- Del menú principal de la NBX, seleccione intercambio de mensajes de NBX, y configure.
- Seleccione la ventana de notificación exterior.
- Verifique que este activada, como lo muestra la figura 4.27.
- Hacer clic en aplicar.

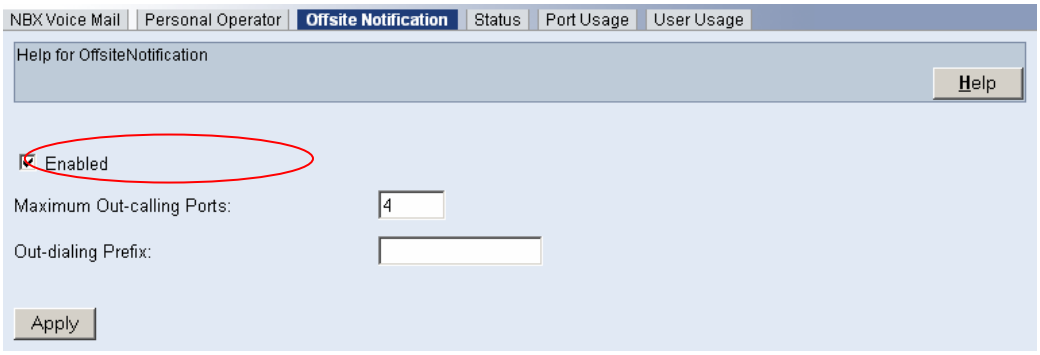


Figura 4.27. Muestra la habilitación de notificaciones hacia el exterior.

- Abra una nueva ventana de navegador.
- Entre al sistema como usuario a la extensión 1001 e introduzca la contraseña.
- Del menú principal del Netset como usuario, seleccione ajustes de correo de voz.
- Verifiqué que este habilitado las notificaciones al exterior, solamente para mensajes urgentes, como lo muestra la figura 4.28.

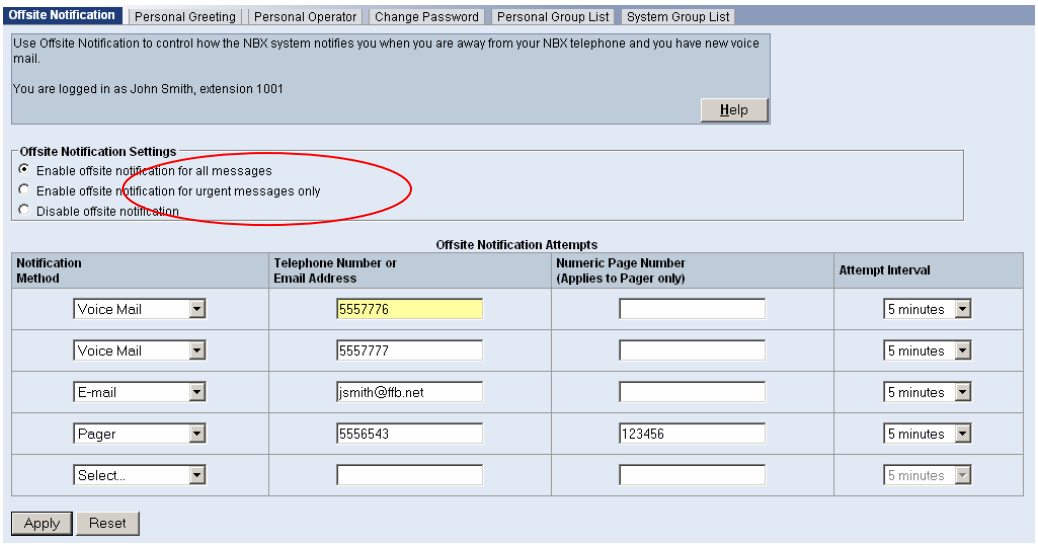


Figura 4.28. Muestra la configuración de notificación al exterior solo para mensajes urgentes.

- Las notificaciones deben estar marcadas como correo de voz. Para que se pueda ingresar un número de teléfono que la NBX pueda marcar, como un número de teléfono celular.
- La segunda columna ingrese el número telefónico que la NBX pueda marcar.
- Si la notificación está marcada como e-mail, ingrese una dirección e-mail por ejemplo jsmith@ffb.net.
- Si la notificación está marcada como pager, esta debe estar configurada con el número de pager 555-6543 y el número de pin 123456.
- Hacer clic en OK.

Configuración de saludos múltiples para usuarios vía telefónica.

Para la configuración de saludos múltiples para los usuarios seguimos los siguientes pasos:

- Levante el teléfono y presione el botón de mensaje sobre la extensión 1003.
- Escriba la contraseña, seguido de la tecla #.
- Seleccione opciones de buzón de voz presionando la tecla 9
- Seleccione 1 para revisar o hacer los cambios para su anuncio de nombre o saludo personal.
- Seleccione 2 para revisar o hacer los cambios para su saludo personal.
- Se le anunciará cuántos saludos grabados tiene usted. Escoja 9 para grabar un nuevo saludo.

- Usted escuchará el saludo de grabación número x (donde x es el próximo número de saludo).
- Grabe un nuevo saludo y presione la tecla #.
- Presione 1 para mantener su saludo.
- Presione 1 para hacer el saludo activo.
- Cuelgue el teléfono

Configuración de saludos múltiples para usuarios vía Netset.

Para configurar múltiples saludos para los usuarios via Netset, el software de administración de la NBX, siga los siguientes pasos:

- Abra una nueva ventana del navegador.
- Entre al sistema como Usuario ingrese a la extensión 1003 y escriba la contraseña.
- Del menú principal del Netset como usuario seleccione ajustes de correo de voz.
- Seleccione saludo personal.
- Seleccione un saludo inactivo colocando un visto en el saludo, como se lo muestra en la figura 4.29.
- Hacer clic en el botón de activar.

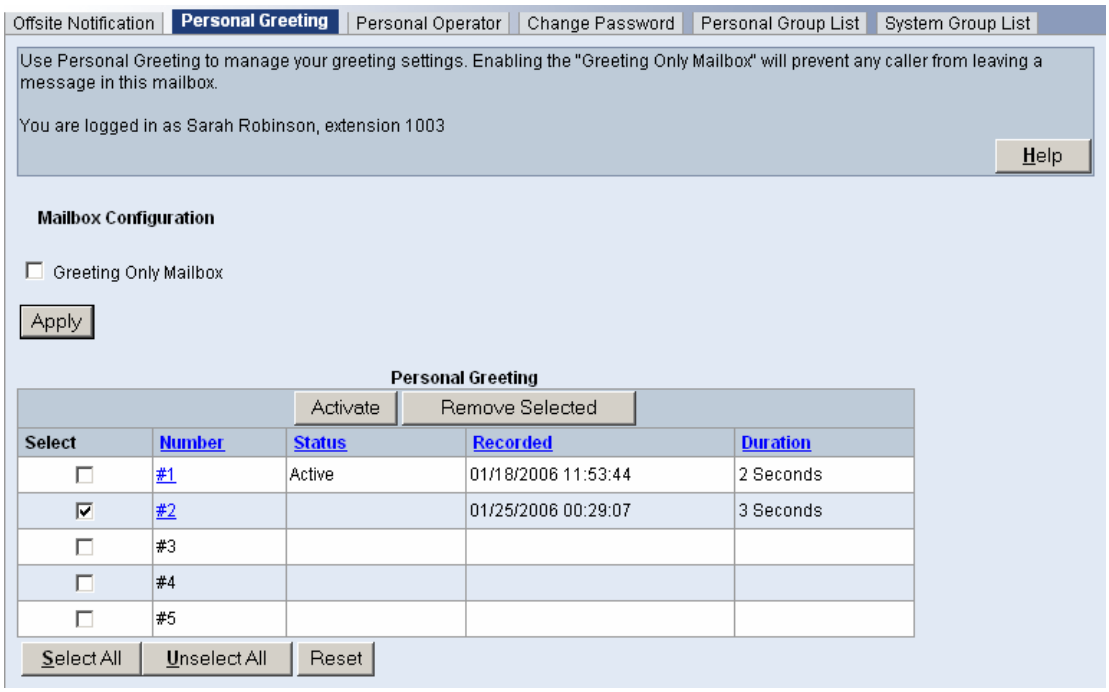


Figura 4.29. Muestra los múltiples saludos personales que tiene el usuario.

Configuración del teléfono para no interrumpir.

Para configurar el teléfono en modo de no interrumpir realizamos la siguiente configuración:

- Del menú principal del NetSet, seleccionamos configuración de teléfono y teléfonos.
- Seleccionamos la extensión 1001.
- Hacer clic en el mapeo de botones.
- Seleccione donde este un botón configurado como marcación rápida personal y cámbielo por *Do Not Disturb*, como se lo muestra en la siguiente figura 4.30.
- Hacer clic en aplicar.

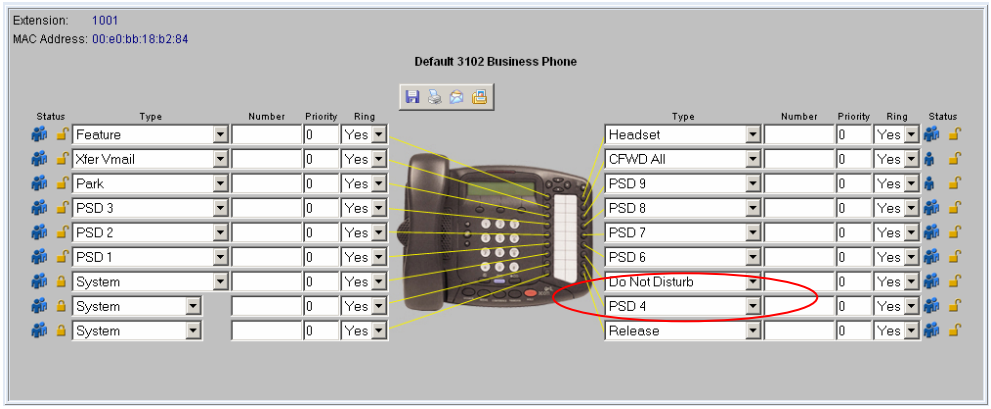


Figura 4.30. Muestra la configuración del teléfono en modo no interrumpir.

Correo de voz fantasma.

Para la configuración de correos de voz fantasmas realizamos la siguiente configuración:

- Del menú principal del *NetSet*, seleccione configuración de usuarios, y elija usuarios.
- Hacer clic en el botón añadir.
- Use la siguiente tabla 4.2 y arregle este usuario que no trabaja en la oficina o en la casa y esté viajando siempre.

Tabla 4.2 Datos de una extension fantasma

Extensión	Nombre	Apellido	Título	Contraseña de

				correo vocal
1098	Wendy	Pinto	Ingeniera	1234

- De un teléfono de la NBX, marque 500. Cuando escucha la atendedora automática presione la tecla **. Siga los pasos de configuración para el correo de voz del usuario y contraseña que usa la información.
- Saludos solamente al buzón de voz.
- Para realizar saludos solamente al buzón de voz, vamos a crear un anuncio de cómo llegar a la Universidad Cotopaxi.
- Del menú principal del NetSet, seleccione configuración de usuarios, usuarios.
- Hacer clic en el botón añadir
- Use la siguiente tabla 4.3 para la configuración de una extensión que proveerá las instrucciones para llegar a la Universidad. Recuerde especificar "Nada" para la extensión del usuario.

Tabla 4.3 Crea una extensión para grabar la dirección de la Universidad Cotopaxi.

Extensión	Nombre	Apellido	Contraseña de correo vocal
1099	Universidad	Instrucciones	1234

- Excluya a este usuario del Directorio de LCD.
- Excluya a este usuario del nombre de directorio.
- Estar seguro de los cambias en su configuración y hacer clic en OK.
- Del menú principal del Netset, hacer clic en la configuración de usuarios, usuarios.
- Seleccione la extensión 1099.
- Hacer clic en *Setting Tab*. Usted es llevado al portal de NetSet como usuario.
- De usuario NetSet de nivel seleccione ajustes de correo vocal de NBX.
- Seleccione saludo personal.
- Verifique dando la bienvenida a solamente al Mailbox.
- Hacer clic en aplicar.

- Hacer clic en su navegador hacia atrás para regresar al administrador portal del NetSet.
- De cualquier teléfono de NBX, marque 500. Cuando usted escuche la atendedora automática presione las teclas **. Siga la configuración de correo de voz y una contraseña. Grabe una descripción breve de cómo llegar a la Universidad Cotopaxi donde usted grabaría su mensaje de saludo normalmente.

Añadir un grupo de correo de voz al sistema.

Para añadir un grupo de correo de voz al sistema, seguimos los siguientes pasos:

- Del menú principal del Netset, seleccione mensajería de NBX, Lista de grupo de sistema.
- Hacer clic en añadir, como se lo muestra en la figura 4.31.

Figura 4.31. Muestra la pantalla para añadir un grupo de correo de voz al sistema.

- Cree un grupo con la identificación 02 y con un nombre de grupo de directores. Añada a miembros 1002 y 1003, como se lo muestra en la figura 4.32.

Figura 4.32. Muestra el nuevo grupo creado con las extensiones asociadas.

- Hacer clic en OK.
- Regrese a la ventana de lista de grupo del sistema. Seleccione el enlace con la identificación 02 haciendo clic sobre él.
- Hacer clic en la grabación por nombre.
- Ingrese la extensión para grabar.
- Hacer clic en el botón de grabación y grabe el nombre de este grupo; directores. Regresa a la ventana de lista de grupo del sistema.
- Presione el botón de mensaje sobre la extensión 1001. Entre al sistema con la contraseña configurada previamente.
- Presione 2 para grabar un mensaje (presione # cuando finalizo la grabación).
- Presione 1 para enviar su mensaje
- Presione *02 # para escoger grupo del sistema 2
- Presione # otra vez para transmitir.
- Añadir un grupo de correo de voz personal
- Abra una nueva ventana del navegador.
- Entre al sistema como usuario 1002 con su contraseña por ejemplo 1234.
- Del menú principal del Netset como usuario, seleccione configuración de correo de voz.
- Seleccione lista de grupo personal, como se lo muestra en la figura 4.33.
- Seleccione un saludo inactivo colocando un visto en la caja.
- Hacer clic en añadir

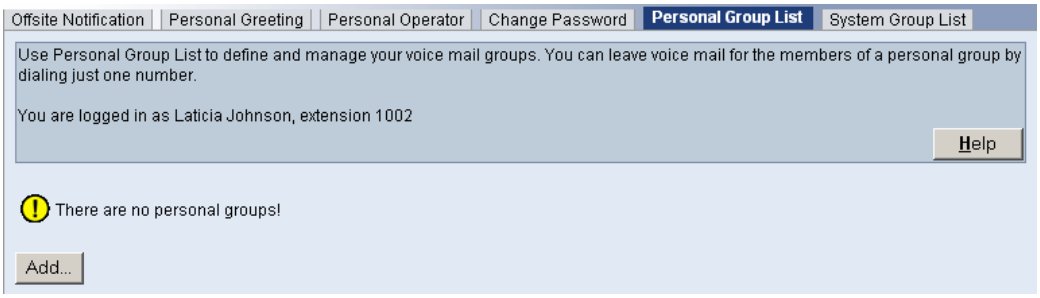


Figura 4.33. Muestra la lista de grupo personal, para añadir las extensiones que se van asociar.

- Cree un grupo con identificación 01 y con un nombre de grupo de equipo de profesores.
- Añada las extensiones 1001, 1003 y 1050.

- Hacer clic en OK.
- Presione el botón de mensaje sobre la extensión 1002 (o levantar el auricular y presione el botón de mensaje).
- Presione el botón de mensaje sobre la extensión 1001. Entre al sistema con contraseña 1234.
- Presione 2 para grabar un mensaje (presione # cuando este grabado).
- Presione 1 para enviar su mensaje
- Presione 01 # para escoger grupo personal 1
- No se utiliza * para grupos personales.
- Presione # otra vez para transmitir.
- Vamos a crear un segundo grupo personal ahora la instalación es a través del teléfono.
- Presionar el botón de mensaje sobre la extensión 1002 y entre al sistema.
- Presione 9 para opciones de buzón.
- Presione 3 para listas de grupo.
- Presione 1 para escuchar una lista completa de sus grupos.
- Presione 2 para crear un nuevo grupo.
- Ingrese el número de grupo de dos dígitos 02.
- Diga el nombre del grupo, todos los empleados y presione # cuando este completo.
- Presione 1 para aceptar su nombre de grupo grabado.
- Ingrese el mailbox de las extensiones 1002 , 1003, y 1005.
- Acepte el grupo presionando 1,
- Cuelgue el teléfono.

Réplica de mensajes.

Para realizar réplicas de mensajes realizamos los siguientes pasos:

- De la extensión 1001, deje un mensaje para la extensión 1003.
- Acceda al correo de voz para la extensión 1003.
- Presione 1 para escuchar el nuevo mensaje.
- Presione 4 para responder el mensaje.
- Grabe su mensaje y presione #.

- Presione 1 para enviar su mensaje.
- Presione 3 para eliminar el mensaje.
- Cuelgue.

Seguimiento de mensajes.

Para realizar seguimiento de mensajes realizamos los siguientes pasos:

- De la extensión 1002, deje un mensaje para la extensión 1003.
- Acceda al correo de voz para la extensión 1003.
- Presione 1 para escuchar el nuevo mensaje.
- Presione 5 para enviar el mensaje.
- Grabe un mensaje de introducción y presione # cuando este grabado.
- Presione 1 para enviar el mensaje a uno o más receptores.
- Ingrese el número de buzón de voz 1001.
- Presione # para enviar el mensaje.
- Presione 3 para eliminar el mensaje.
- Cuelgue.
- Elimine el mensaje enviado a la extensión 1001.

Seguimiento de llamadas.

El usuario puede usar seguimiento de llamadas para especificar un número telefónico cuando no se encuentre dentro de la oficina, también puede incluir mensajes de voz, otros números, o la atendedora automática y el usuario puede escoger desconectar las llamadas. Seguimiento de llamadas a través de teléfono.

Para realizar seguimiento de llamadas a través de teléfono realizamos los siguientes pasos:

- En la extensión 1003, desplácese hacia abajo a través del menú hasta que se consigue hacer un CFWD todo.
- Presione la tecla de #.
- Presione la tecla de # otra vez.
- Ponga la extensión 1001 para que envié todo "Envie todo a:".

- Presione la tecla de #. Todas llamadas serán enviadas al nuevo número ahora. Note que la LCD muestra CFWD; 1001.
- Marque de la extensión 1003 a la extensión 1002 . ¿1001 sonó?
- En la extensión 1003, desplácese hacia abajo a través de la carta hasta que se consigue a CFWD todo.
- Presione la tecla de #.
- Presione la tecla de # otra vez. El traslado de llamadas es cancelado ahora para este teléfono.

Seguimiento de llamadas a través del mapeo de botones.

Recuerde que se puede programar los botones como administrador o como usuario.

Para realizar seguimiento de llamadas a través del mapeo de botones realizamos los siguientes pasos:

- Del NetSet principal de la NBX, escoja configuración de usuarios.
- Seleccione la extensión 1002.
- Seleccione el tabulador de ajustes.
- De la visualización del usuario, seleccione la programación de teléfono.
- Seleccione button mapping tab.
- Configure los tres botones programables inferiores con *CFWD all, CFWD Busy, y CFWD No Answer*, como se lo muestra en la figura 4.34.
- Hacer clic en aplicar.

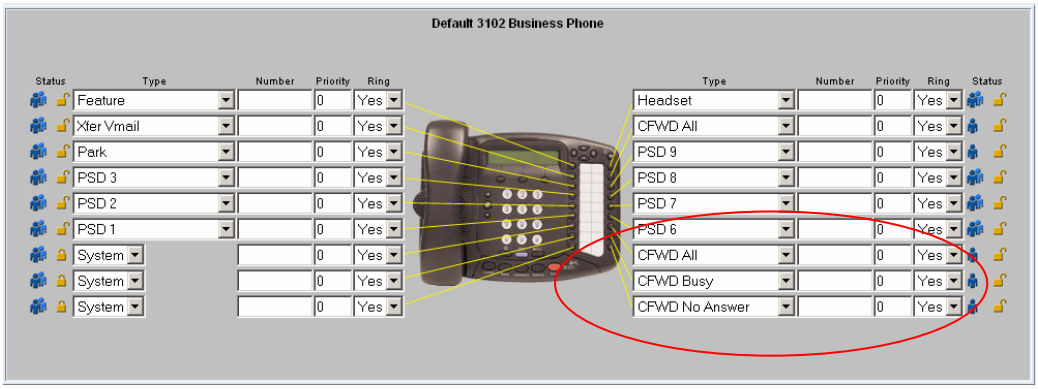


Figura 4.34. Muestra la configuración de botones para hacer un seguimiento de llamadas.

Operadores Configurables.

Un típico uso de operadores configurables es desviar a llamadores a un destino alternativo a través de un atendedor automático o mail de voz. Por ejemplo un grupo de llamadas puede ser configurable con "9" para ir a su teléfono celular. Hay dos destinos para todos los usuarios que pueden estar habilitados o inhabilitados. Estos son el operador de sistema y el operador personal. Las configuraciones por defecto del sistema son: "0" para el operador del sistema y "9" para el operador personal. Esto puede ser cambiado a cualquier dígito 0-9.

Para realizar la configuración de operadores personales, realizamos los siguientes pasos:

- Ingrese al NetSet como administrador, seleccione configuración de usuarios, clase del servicio.
- Hacer clic en Default User Group.
- Modifique el *Default User Group* para que el operador personal este permitido.
- Hacer clic en OK.
- Del menú principal del NetSet seleccione mensajería de la NBX y configure.
- Seleccione la operadora personal.
- Cambie el operador destino del sistema a 1003.
- Verifique que su dígito de acceso sea el "0".
- Verifique que el operador de destino personal sea el dígito “9”
- Hacer clic en aplicar.
- Abrir una nueva ventana del navegador.
- Entre al sistema como usuario 1002 con contraseña 1234 por ejemplo.
- Del menú principal del NetSet como usuario seleccione configuración de mensajes de voz.
- Seleccione operadora personal.
- Ingrese un número telefónico conocido precedido de un 9 (ejemplo; un número de teléfono). Como se lo muestra en la siguiente figura 4.35.

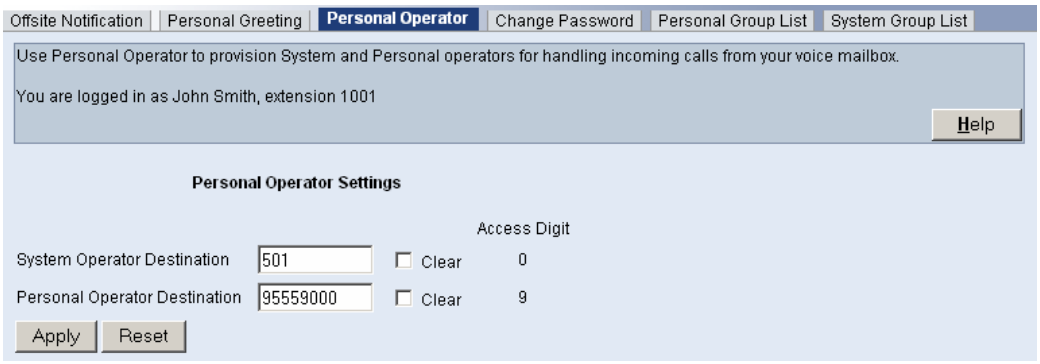


Figura 4.35. Muestra la configuración de la operadora personal.

- Hacer clic en aplicar
- Acceda a la mensajería para la extensión 1002 presionando el botón de mensaje y entre al sistema.
- Presione 9 para opciones de buzón.
- Presione 1 para hacer los cambios para su saludo personal.
- Presione 2 para hacer los cambios para sus saludos personales.
- Presione 9 para grabar un nuevo saludo.
- Grabe por ejemplo el siguiente saludo personal:
- Usted ha llegado al buzón de voz de Michelle Yépez. Su llamada es importante para mí así que por favor déjeme un mensaje y devolveré su llamada lo antes posible. Para hablar con alguien ahora, presione "0". Si usted tiene que contactarme urgentemente, presione 9 para contactarme a mi teléfono móvil.
- Presione # cuando este grabado el mensaje.
- Presione 1 para guardar este saludo.
- Presione 1 para hacer este saludo activo.
- Cuelgue.

Indicador de mensaje de espera.

El indicador de mensaje de espera (MWI), es una mejora que permite indicar sobre otro teléfono, que realice una llamada de regreso sobre el teléfono. El mensaje MWI se enciende sobre el teléfono.

Para la configuración de MWI realizamos la siguiente configuración:

- Del menú principal del Netset ingresamos a la configuración de teléfono, y elegimos grupo de teléfonos.
- Seleccionar los grupos que representan a la extensión 1001 y 1002 (ejemplo. *Default 3102 Business Telephone Group, Default 3103 Manager Group*).
- Hacer clic en el mapeo de botones clic en el tabulador de correspondencia de botón para el grupo o los grupos.
- Mapear 3 botones como muestra en la figura 4.36 para la extensión 1001 y 1002.

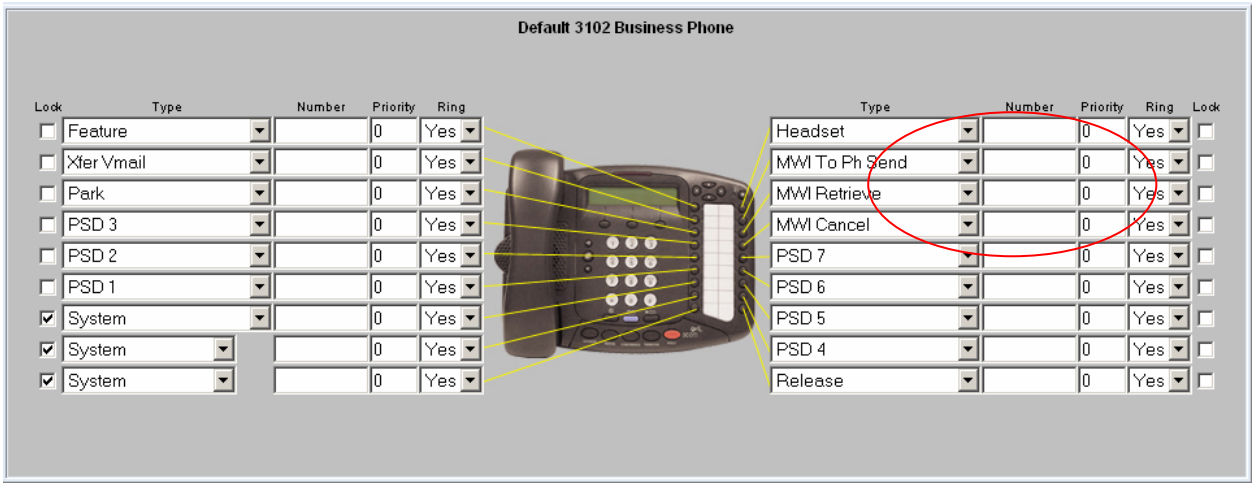


Figura 4.36. Muestra la configuración de los botones de los teléfonos para el modo de indicador de mensaje en espera.

Envió de un MWI.

En la extensión 1001, presione en el teléfono el botón MWI de envío y presione la extensión 1002#. El teléfono se descuelga automáticamente vía manos libres. Cuelgue.

Ver en la extensión 1002. El LED del botón de Retrieve de MWI es encendido.

Recuperar un MWI.

Para recuperar un MWI enviado, realizamos la siguiente configuración**:**

- Sobre la extensión 1002, presione el botón de Retrieve de MWI. Desplácese hacia abajo para ver la información. Note la identidad del remitente, la fecha y el tiempo en la visualización. Note que el Retrieve LED de MWI se activado para indicar que los mensajes de MWI han sido vistos.

- Desplácese hacia abajo hasta la extensión 1001 y presione llamar. Recoja la llamada y cuelgue.

Cancelar un mensaje enviado.

Vamos a cancelar un mensaje enviado:

- Realice el envió de un mensaje. El *LED* de *Retrive* de la extensión 1002 es encendido otra vez.
- En la extensión 1001, presione el botón de Cancelar *MWI*. Ingrese 1002 # y cuelgue. Note que la luz de MWI se apaga sobre la extensión 1002.
- Presione el botón de *Retrieve* de *MWI* en la extensión 1002. El mensaje cancelado dejó un *log*.
- Escoja eliminar todo.
- Del menú principal del *NetSet*, seleccione configuración de teléfono, elija grupos de teléfonos.
- Seleccione los grupos que representan la extensión 1001 y 1002.

Atendedora Automática.

La atendedora automática es la unidad central del sistema de correo de voz. Es importante crear y configurar atendedoras automáticas, y poder grabar o importar mensajes y saludos para dirigir las acciones de los *llamadores*.

Estos pasos son representativos de la configuración que ajustes hicieron a sistemas de NBX durante las instalaciones verdaderas y el mantenimiento.

Modificar el saludo del sistema.

Para modificar el saludo del sistema realizamos los siguientes pasos:

- Ingresamos al *NetSet* como administrador, seleccione mensajería de la NBX y atendedora automática del menú principal.
- Seleccione saludo del sistema, como se lo muestra en la figura 4.37.

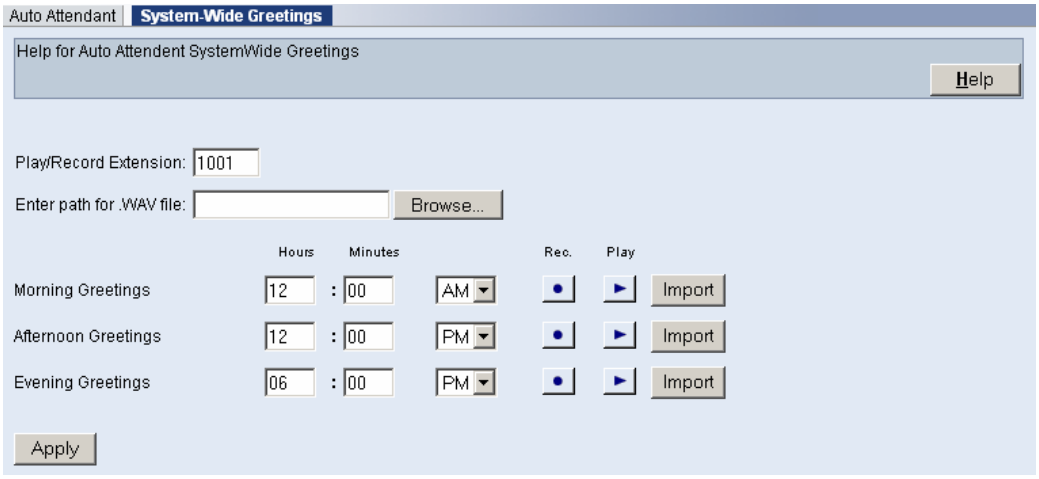


Figura 4.37. Muestra los saludos del sistema de la atendedora automática.

- Ingrese un número de extensión en el cual vamos a grabar un nuevo saludo al sistema, también se pueden importar saludos para el sistema.
- Hacer clic en play en cada uno de los tres saludos y así escuchara los saludos que se encuentran en el sistema, en la extensión telefónica que se seleccione previamente.
- En la Universidad Cotopaxi grabamos un nuevo saludo, por que es recomendable que tanto la voz de los saludos y de la atendedora automática sea la misma y de preferencia que sea la voz de una mujer, debido a la delicadeza de su voz, y que tenga experiencia como locutora.
- Presionamos # cuando finalizamos la grabación y 1 para guardar el mensaje. Luego colgamos el teléfono.
- Hacemos clic en play para escuchar los tres saludos del sistema.
- Al terminar, hacemos clic en aplicar.

Configuración de la atendedora automática.

Para la configuración de la operadora automática realizamos los siguientes pasos:

- Ingresamos al NetSet como administrador, seleccionamos mensajería de la NBX.
- Seleccionamos la atendedora automática, como lo representa la figura 4.38.

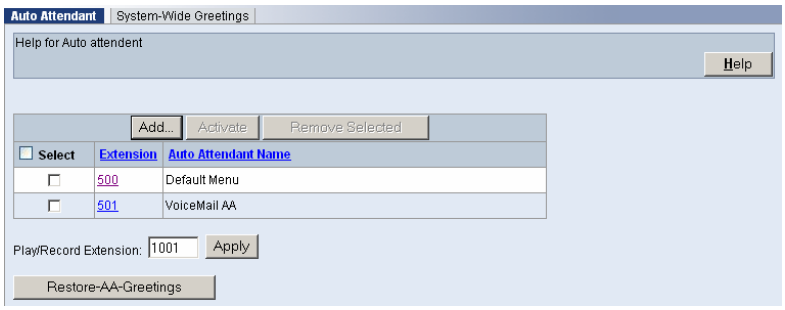


Figura 4.38. Muestra las extensiones de la atendedora automática.

- Hacer clic en aplicar.
- Hacer clic en el botón añadir.
- En la pantalla hacemos clic en añadir, e ingresamos el siguiente nomre FSB_MAIN. Colocamos la extensión 5501 y el número máximo de las repeticiones puntuales en 3, como se lo muestra en la figura 4.39.

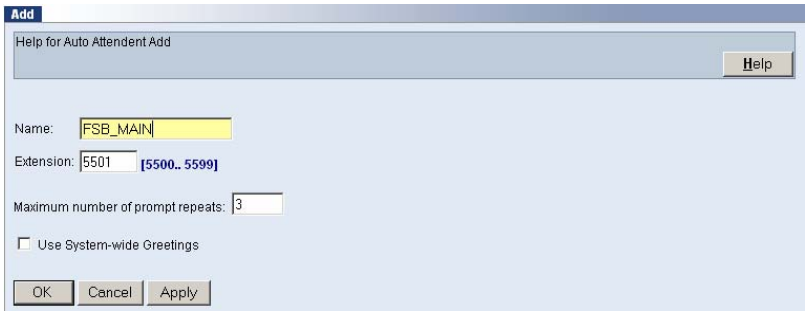


Figura 4.39. Muestra la nueva configuración de la atendedora automática.

- Hacer clic en OK.
- Bajo la atendedora automática se desplegará la configuración realizada, como se lo muestra en la figura 4.40.

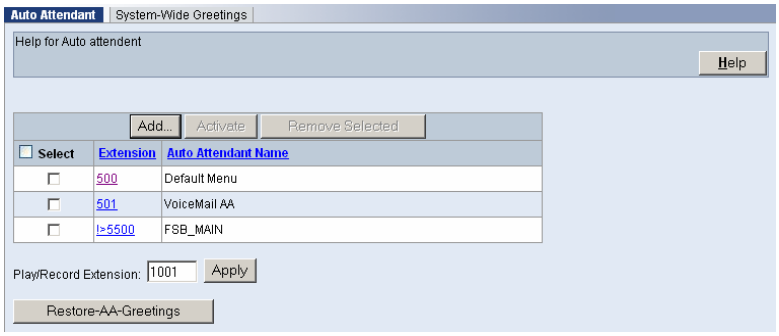


Figura 4.40. Muestra las extensiones de la atendedora automática.

- Seleccione la extensión 5500 haciendo clic en ella.
- Seleccione el menú *tree* y lo configuraremos como se lo muestra en la tabla 4.4.

Tabla 4.4 Configuración de dígitos de la atendedora automática

Botón	Descripción de tarea	Acción	Valor
1	4 dígitos internos	Reservado en el plan de marcación.	
2	4 dígitos internos	Reservado en el plan de marcación.	
3		Dejar incapacitado	
4		Dejar incapacitado	
5	Instrucciones	Transferencia a un simple dígito	1099
6		Dejar incapacitado	
7	Departamentos	Submenú	
8		Dejar incapacitado	
9	Directorio de nombres	Directorio de nombres	
0		Transferencia a un simple dígito	1003
*		Transferencia para el correo de voz	
#		Desconectar el sistema	#
T / O		Transferencia	1003

- Hacer clic en aplicar.

- Seleccionamos el *Prompt.*
- Colocamos un nuevo nombre en el *Prompt*: FSBmain
- Hacemos clic en el botón grabar. El teléfono designado sonará, y grabamos el siguiente mensaje.

Gracias por llamar a la Universidad Cotopaxi. Si usted conoce la extensión márquelo ahora. Para obtener información de la dirección de la Universidad marque 5. Para la lista de departamentos y hablar con un administrador del departamento presione 7. Para búsqueda por nombre en el directorio presione 9. Para hablar con la atendedora presione 0 o permanezca en línea y será atendido. Gracias por su llamada.

- Presione # cuando termine de grabar el mensaje y presione 1 para guardar, luego cuelgue el teléfono.
- Seleccione FSBmain colocando un visto en la ventana.
- Hacer clic en OK.
- Ingresamos al menú *tree* de la extensión 5501 e ingresamos el submenú presionando el botón de flecha para abajo, como se lo muestra en la figura 4.41.

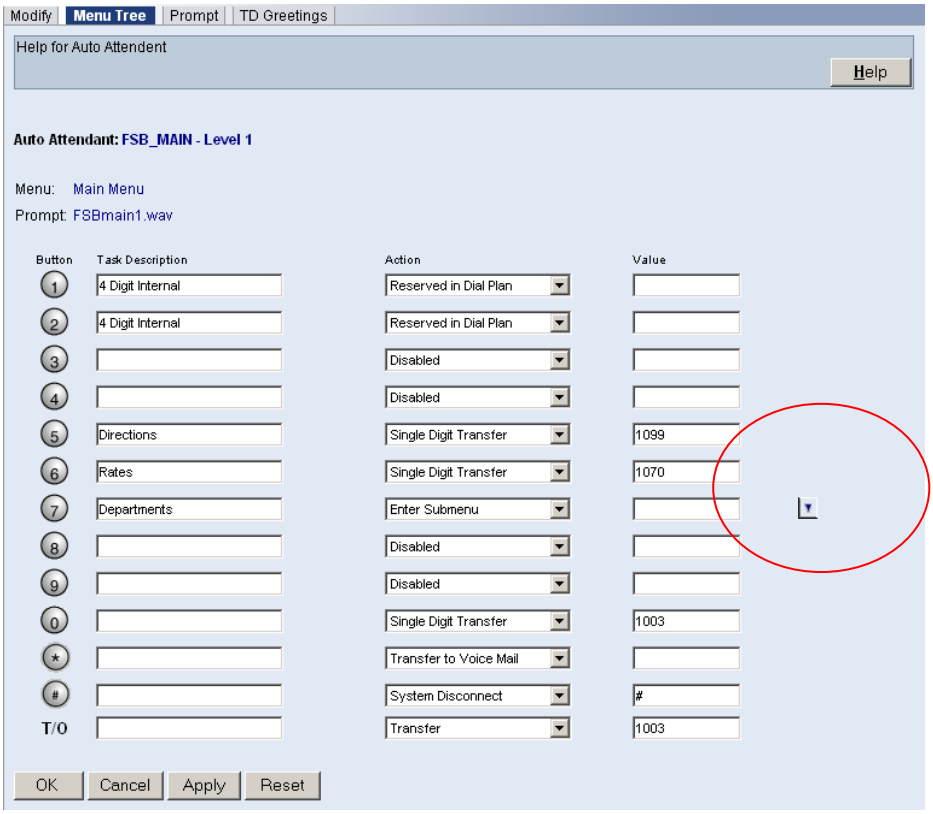


Figura 4.41. Muestra la configuración de digitos de la atendedora automática

- Ingresamos al submenú.

Usamos la tabla 4.5 para la programación de los botones:

Tabla 4.5 Submenú de la atendedora automática

Botón	Descripción de tarea	Acción	Valor
1	Administrativos	Transferencia de un simple dígito	1002
2	Sistemas	Transferencia de un simple dígito	1003
3	FIE	Transferencia de un simple dígito	1004
4	FIME	Transferencia de un simple dígito	1005
5	Automotriz	Transferencia de un simple dígito	1006
6	Civil	Transferencia de un simple dígito	1007
7	Regrese al menú principal	Carta de salida	
8			
9			
0	Información	Transferencia de un simple dígito	1010
*		Transferencia para el correo vocal	**
#		Disconnect de sistema	#
T / O	Información	Transferencia	1010Bottom of Form

- Hacer clic en aplicar.
- Seleccione el *Prompt*.
- Hacer clic en el botón grabar. El teléfono designado sonará. Grabamos el siguiente mensaje:

Para hablar con el área administrativa marque 1. Para departamento de sistemas marque 2. Para departamento de ingeniería electrónica marque 3. Para departamento de mecânica marque 4. Para departamento automotriz marque 5. Para departamento de ingeniería civil marque 6. Regresar al menú principal marque7. Contactar con información presione 0 o permanezca en la línea.

- Hacer clic en OK.
- Activamos la atendedora automática configurada.
- Dentro del menú principal de la NBX, seleccione *PSTN Gateway*, líneas análogas.
- Seleccionamos las líneas analógicas disponibles, y colocamos en la auto extensión 5501 para horas de trabajo, *lunch y otros*

Plan de Marcación.

El plan de marcación de la NBX, es la parte fundamental de la central telefónica, y revisaremos en las siguientes secciones, las partes fundamentales del plan de marcación. En la primera sección del plan de marcación de la NBX, notamos que la central telefónica genera en texto plano la dirección IP, el nombre, la fecha y hora de la central telefónica NBX, como se lo muestra en el Anexo B.

En el menú principal del Netset, ingresamos al plan de marcación y lista de extensiones, como se lo muestra en la figura 4.42.

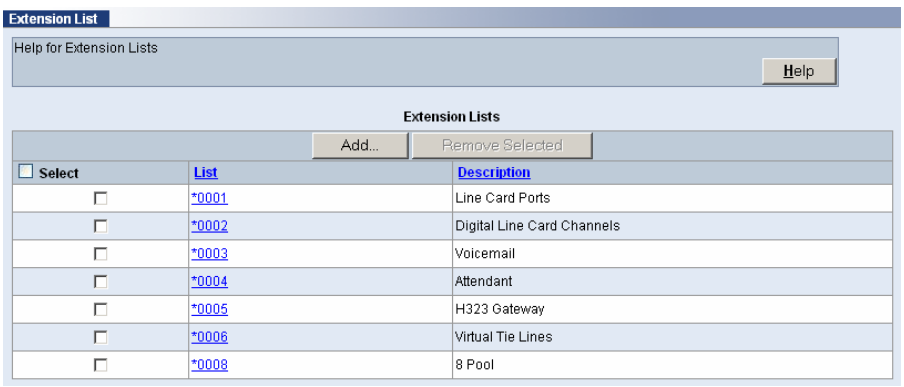


Figura 4.42. Muestra la lista de extensiones.

Se puede añadir nuevas listas o modificar la admisión para una lista existente. Hacer clic en OK y finalizar

Grupos *HUNT*.

Un grupo Hunt es un grupo de usuarios que pueden ser accedidos con la marcación de una simple extensión. La llamada es enrutada al grupo de extensiones *Hunt,* para que cualquier miembro del grupo pueda recibir la llamada. Un grupo *Hunt* estático hace que todos los miembros estén permanentemente conectados al sistema (bloqueados). Un grupo *Hunt* dinámico es donde los usuarios pueden estar conectados al sistema y afuera del grupo, el administrador puede permitir que los usuarios entren o salgan del grupo, usando contraseña de grupos *Hunt*.

Un grupo de llamada es un tipo especial de grupos *Hunt*. Una llamada entrante suena sobre todos los teléfonos en el grupo simultáneamente. Después de que el valor del tiempo muerto total es alcanzado, una llamada que todavía está sin respuesta es encaminada al punto de cobertura de llamada del grupo. Un *call pick up* permite que a cualquier usuario que es miembro del grupo de *pick up* pueda recoger la llamada que suena en cualquier teléfono del grupo.

Configuración del Grupo *Hunt.*

Para realizar la configuración de un grupo *Hunt,* realizamos los siguientes pasos:

- Ingresar al NetSet como administrador, seleccionar grupos de distribución de llamadas, grupos *Hunt,* como se lo muestra en la figura 4.43.

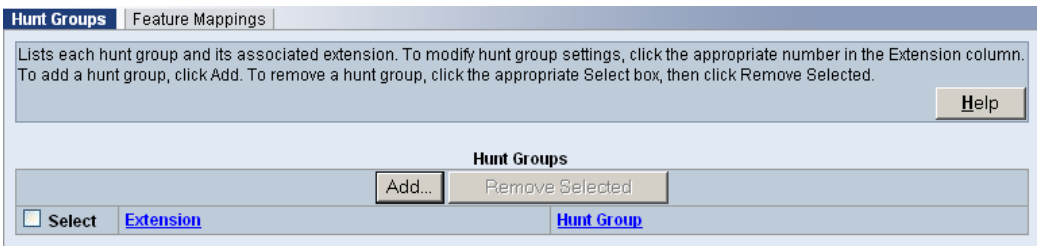


Figura 4.43. Muestra la extensión del grupo Hunt.

- Hacer clic en el botón añadir.

- Configure el grupo *Hunt* de la siguiente manera, como se lo muestra en la figura 4.44.

Name: línea directa del cliente

El tipo: grupo de Hunt lineal

Asigne la extensión: automáticamente

Por el tiempo muerto de dispositivo: 10

Salga del sistema si no hay respuesta: sí

Sume el tiempo muerto: 18

Contraseña: 0000

La cobertura de llamada: correo de voz por defecto

Miembros: 1001, 1002

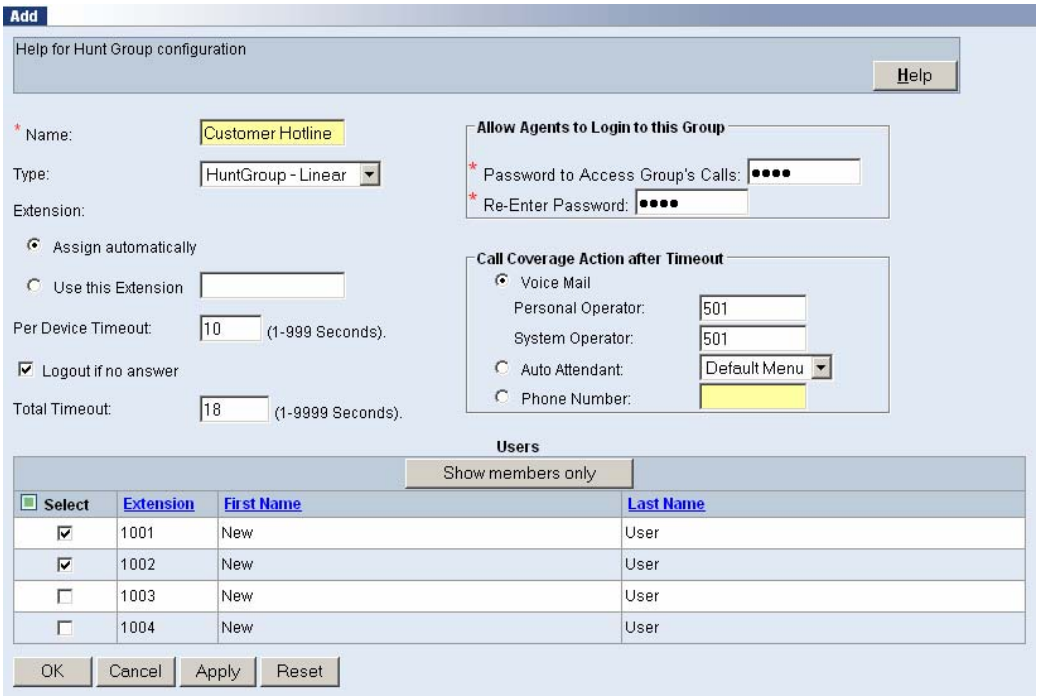


Figura 4.44. Muestra la configuración del grupo Hunt y las extensiones asignadas.

- La extensión asignada automáticamente será la 4000.
- Registro de entrada y salida de los grupos *Hunt* , con clave característica
- Para el registro de entrada y salida de los grupos Hunt, realizamos la siguiente configuración:
- Ingresar al *NetSet* como administrador, seleccionar grupos de distribución de llamada selectos, grupos *Hunt*.

- Seleccionamos la tabla de mapeo.
- Configure la línea directa del grupo Hunt, con la clave característica 850, para seleccionar línea directa a la extensión 4000.
- Hacer clic en aplicar.
- Desde la extensión 1001, presionamos el botón *speaker* , luego presionamos el botón de *feature,* ingresamos la clave característica 850 y el *password* del grupo *Hunt* , y de esta manera la extensión 1001 estará registrada en el grupo *Hunt*.
- Tambien se puede realizarlo mapeando los botones del teléfono del usuario, seleccionando en cualquier botón libre disponible *'grp login/out0'*.

Configurar Call Pick Up.

Para la configuración de *call pick up* realizamos los siguientes pasos:

- Ingresar al *NetSet* como administrador, seleccionamos *Feature Settings, Call Pickup,* como se lo muestra en la figura 4.45.

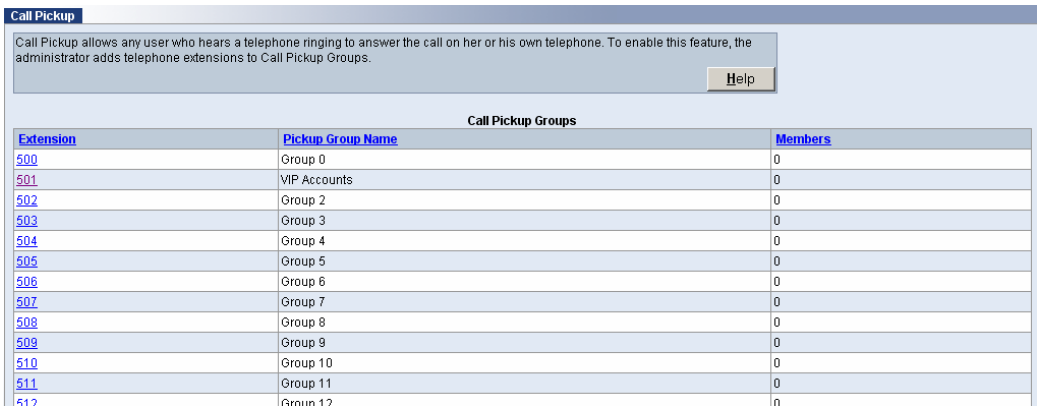


Figura 4.45: Muestra el grupo de extensiones de *Call Pickup*.

- Hacer Clic en 501 para el grupo 1.
- Cambiamos el nombre del grupo por *VIP Accounts,* como lo muestra la figura 4.46.

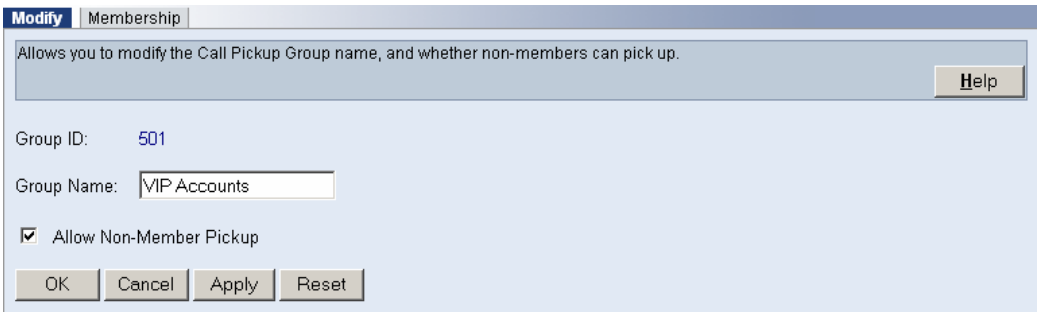


Figura 4.46. Muestra el nombre y la extensión del *pickup* seleccionado.

- Revisar cuales van a ser miembros del grupo de call pick up.
- Hacer clic en aplicar.
- Hacer clic en *Membership*, seleccionamos las extensiones del grupo, como se muestra en la figura 4.47.

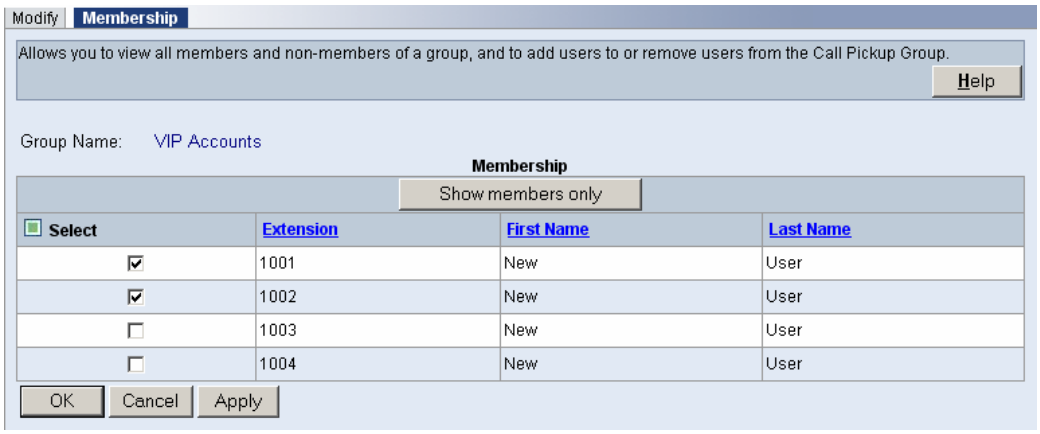


Figura 4.47. Muestra las extensiones añadidas a la extensión del pick up.

- Seleccionar la extensión 1001 en la configuración de teléfonos y mapear un botón libre con el nombre de ´pg501´.

Distribución Automática de llamadas (ACD).

Una central telefónica en términos general se refiere a cualquier sistema que acepta las llamadas entrantes para un sitio, asegura que esas llamadas sean enviadas al destino correcto dentro del sitio, y dirige los registros de base de datos en la actividad de llamada y la distribución. La central telefónica puede ser usado, por ejemplo, como un mostrador de ayuda, un mostrador de reservaciones, una línea directa de información, o un centro de servicio al cliente. Un centro de llamada telefónica dirige colecciones de

las extensiones de teléfono que son vinculadas con una base de datos centralizada típicamente.

El ACD distribuye las llamadas para Agentes y colas para las llamadas que no han sido respondidas antes de que un punto de tiempo predeterminado expire. El ACD también lleva anuncios grabados a los *callers*, dirige agentes de ACD individuales y grupos de Agentes, y provee información de la base de datos sobre tanto llamadas como Agentes.

El sistema de NBX soporta los siguientes grupos de ACD:

Grupo Lineal ACD. - El sistema NBX puede distribuir las llamadas para el grupo en modo lineal. La llamada entrante va hacia el agente clasificado primero y, si el Agente no está disponible, va al agente de segundo rango, el proceso continúa de este modo hasta que el sistema termina el rango, si no responde nadie a la llamada comienza otra vez el ciclo.

Grupo Circular ACD. - El sistema NBX puede distribuir las llamadas para el grupo en forma circular. El sistema intenta poner el llamado entrante con el agente cuyo rango sigue al agente que consiguió la última llamada primero. Si este Agente no está disponible, el llamado va hacia el próximo agente de categoría. Si el segundo Agente no está disponible, el sistema de NBX de ese punto en adelante trata la llamada como lineal.

Agente del grupo más ocioso del ACD.- El sistema NBX puede distribuir las llamadas para el grupo a base del tiempo muerto; es decir el sistema dirige la llamada al agente que tiene el tiempo más largo sin haber respondido a una llamada, si no responde va al agente que tiene el próximo tiempo más largo. Si la llamada no es respondida por el segundo Agente, el sistema NBX maneja la llamada como lineal.

Cuenta de llamadas mínima en la distribución de llamadas ACD.- Se emplea esta opción de distribución de llamada, cuando el sistema NBX distribuye las llamadas para

miembros de un grupo de ACD de acuerdo con el número de las llamadas tratado por cada agente. El agente que ha tratado al menor número de llamas, recibe la próxima llamada.

Distribución de llamadas de grupo ACD - Se emplea esta opción de distribución de llamadas, cuando una simple llamada suena sobre todos los teléfonos del grupo de ACD hasta que un miembro responde a la llamada o la llamada en tiempo fuera es encaminada a la cobertura de llamada del grupo. Esta alternativa envía solamente una llamada a la vez de la cola del ACD al grupo.

Creación de anuncios ACD.

Para la configuración de anuncios de ACD realizamos los siguientes pasos:

- Ingresar NetSet como administrador, del menú principal seleccionar grupos de distribución de llamadas, anuncios de ACD, como se muestra en la figura 4.48.

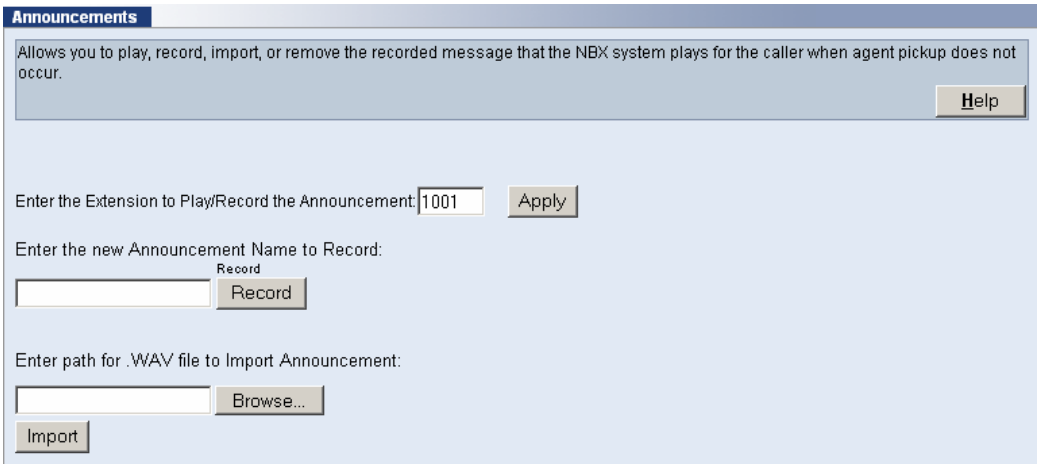


Figura 4.48. Muestra la creción de anuncios para un ACD.

- Ingresar a la extensión 1001, para la grabación del anuncio.
- Hacer clic en aplicar.
- Ingrese un nuevo nombre en el anuncio por ejemplo “Gracias por llamar”. Grabe lo siguiente:

Gracias por llamar a la Universidad Cotopaxi, una persona de información estará con usted en breve. Cree otro anuncio llamado "Su llamada", y grabe lo siguiente:

Su llamada es muy importante para nosotros, por favor permanezca en línea.

Cree un tercer anuncio, intente vía *WEB*. Grabe lo siguiente:

"¿Esperó demasiado tiempo? Porque no pruebe nuestra página web para el servicio inmediato, en www.utc.edu.ec/

Añadir Agentes a la Lista.

Para añadir Agentes a la lista del ACD, realizamos los siguientes pasos:

- Ingresar al NetSet como administrador, en el menú principal seleccione grupos de distribución de llamadas, agentes de ACD, como se muestra en la figura 4.49.

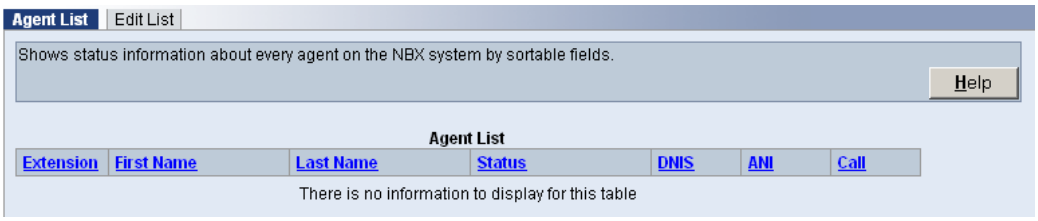


Figura 4.49. Muestra los agentes que se encuentran en el ACD.

- Hacer clic en editar lista, como se muestra en la figura 4.50.

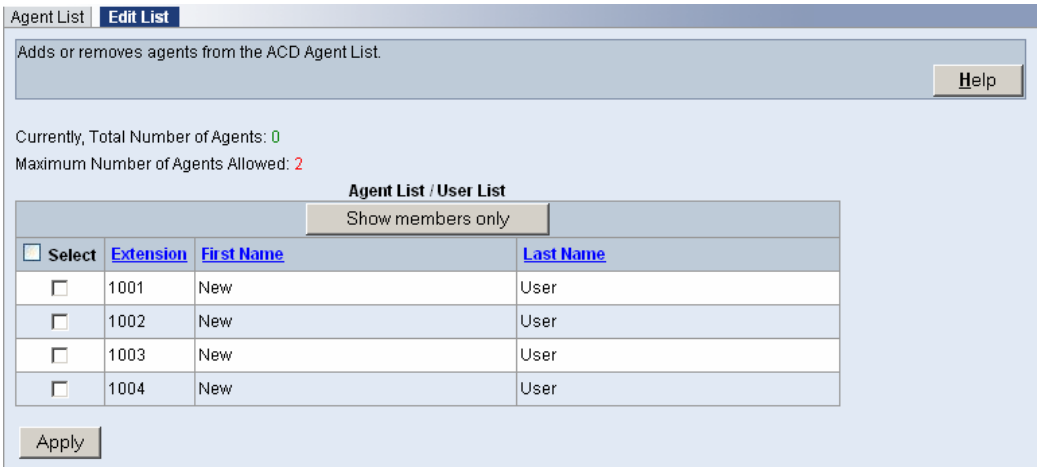


Figura 4.50. Muestra las extensiones de los agentes.

- Elegir las extensiones 1001, 1002, y 1003.
- Hacer clic en aplicar.

Crear un grupo ACD.

Para configurar un grupo ACD realizamos los siguientes pasos:

- Ingresar al NetSet como administrador, en el menú principal seleccione grupos de distribución de llamadas, grupos de ACD.
- Hacer clic en el botón *Add*. Como lo muestra la figura 4.51.

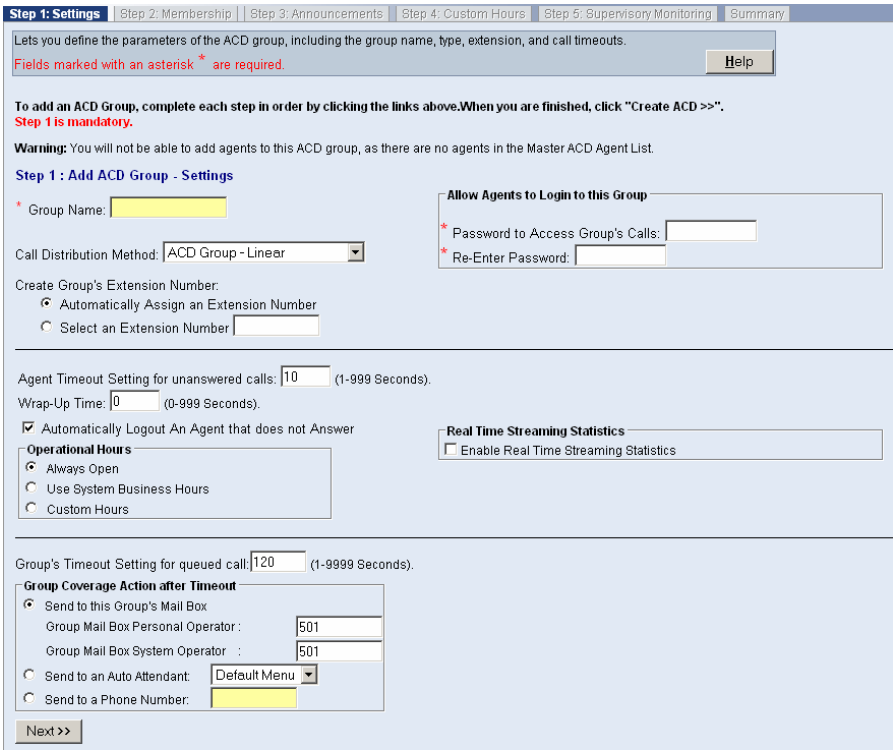


Figura 4.51. Muestra la pantalla para crear un nuevo grupo de ACD.

- Ingrese en el nombre de grupo “Información Cotopaxi”
- En el método de distribución de llamadas, deje el valor por defecto de grupo de ACD lineal.
- La extensión asignada automáticamente será la 4002.
- Permitir que los Agentes entren al sistema a este grupo" e inserte contraseña "2480". Vuelva a ingresar "2480" para confirmar.
- Colocar el ajuste del tiempo muerto del agente para las llamadas sin respuesta a 6.
- Deje el reloj automático en 0.
- Desactive la salida del sistema para un Agente que no da respuesta.
- Ponga el ajuste del tiempo muerto de grupo para la llamada dispuesta en cola de espera a 120.
- Observe, y permita que el resto de la configuración este por defecto.

- Hacer clic en siguiente
- Asignar miembros al grupo ACD.
- Asignamos los anuncio creados, como se lo muestra en la figura 4.52.

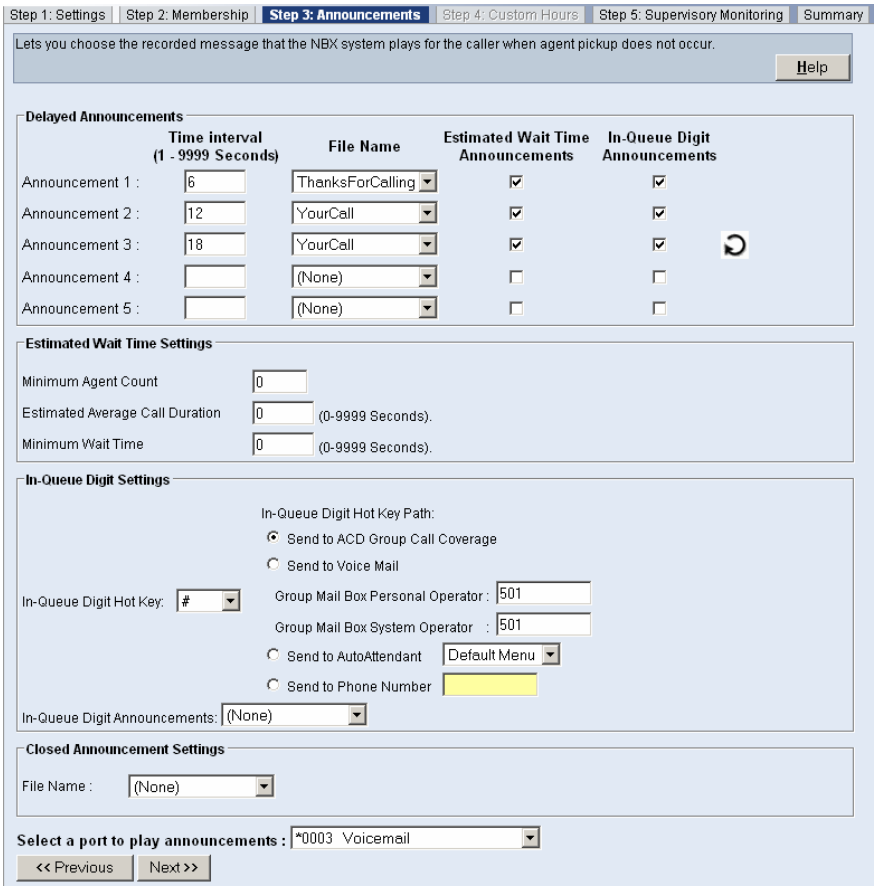


Figura 4.52. Muestra la pantalla para ingresar los anuncios grabados.

- Asigne 6 segundos para el anuncio uno.
- Asigne 18 segundos para el anuncio 2.
- Asigne 30 segundos para el anuncio 3.
- La configuración In-Queue Digit debe ser agrupada, para enviar a la extensión telefónica 1003.
- Coloque el anuncio de dígitos de In-Queue a "intente vía web".
- Deje los otros parámetros por defecto.
- Hacer clic en siguiente.
- Para finalizar asignamos la extensión del ACD a una línea analógica del *Gateway* de la PSTN.

Monitoreo de Supervisor.

El monitoreo de supervisor permite la observación de llamadas de toda clase (llamadas entrantes, salientes, *ACD*, grupos *Hunt* pueden ser monitoreados).

La función de monitor silencioso de la observación supervisora permite la observación sin el conocimiento de un Agente. La función de *Whispering* observación supervisora permite que a un supervisor hable a un agente sin el conocimientos del cliente. La función de *Barge-In* permite que al supervisor en una llamada hable tanto al agente como al cliente.

El anuncio por tonos pueden ser configurado para que el agente y el cliente conozca si el supervisor esta monitoreando la llamada, con *Barge-In* y *Whispering*. Con la observación supervisora simplificada, un dominio define agrupaciones lógicas de los agentes que son exigidos a ser monitoreados para un arreglo específico de personas. La NBX V3000 puede soportar hasta 101 dominios. Alguien que tiene una contraseña legítima puede monitorear a miembros del dominio. El administrador de la NBX crea dominios de observación supervisores que definen la siguiente información:

• El nombre único y la contraseña del dominio de observación supervisor
• Lo clases de llamadas que pueden ser controladas (grupo de llamadas entrantes solamente o todas la llamadas)
• Los grupos de llamada (ACD, Grupos *Hunt*, o TAPI), pueden ser monitoreados
• Los agentes (usuarios) pueden ser monitoreados
• El anuncio de monitoreo silencioso a través de tonos.

La privacidad de llamada permite que un usuario impida una llamada a ser monitoreada. Los usuarios de teléfono de NBX pueden activar y desactivar la privacidad de llamada para bloquear o aceptar la observación supervisora sobre una base de llamada. Por contraste, la admisión en el dominio de lista de privacidad puesto por el administrador de NBX asegura que todas las llamadas relacionadas con este usuario no pueden ser monitoreadas. Si el administrador de NBX destina un usuario a un grupo de clase de servicio que admite la privacidad de llamada, el usuario puede usar la clave de característica 428 para que impida una llamada en curso de ser monitoreado de la siguiente manera:

• Se puede activar la característica de privacidad de llamada antes de una llamada, o durante una llamada. Si se activa la privacidad de llamada mientras una llamada está siendo monitoreada, la sesión de monitoreo es terminada. Los paneles de visualización de teléfono muestran "*CALL PRIVACY ON*" cuando esta característica es activada.

• Cuando una sesión de privacidad de llamada activa termina, (por ejemplo: usted activa la privacidad de llamada, inicia una llamada, y luego sale de la llamada) los ajustes de privacidad de llamada no son más aplicables y la próxima llamada está abierta al monitoreo.

Mapeo de botones para el monitoreo de supervisor

Para realizar el mapeo de botones para supervisar realizamos los siguientes pasos:

- Ingresar al NetSet como administrador.
- Del menu principal del Netset, seleccione configuración de Teléfonos, teléfonos.
- Seleccionamos la extension 1001 para el monitoreo de las demás extensiones.
- Seleccionamos el mapeo de botones.
- En cualquier botón libre del teléfono seleccionamos *Supervisory Monitoring*.
- Hacer clic en el botón OK.
- Para habilitar el monitoreo de supervisor ingresamos como administrador, al menú principal y seleccionamos *System Wide Settings,* y habilitamos la opción de monitoreo de supervisor, como lo muestra la figura 4.53.

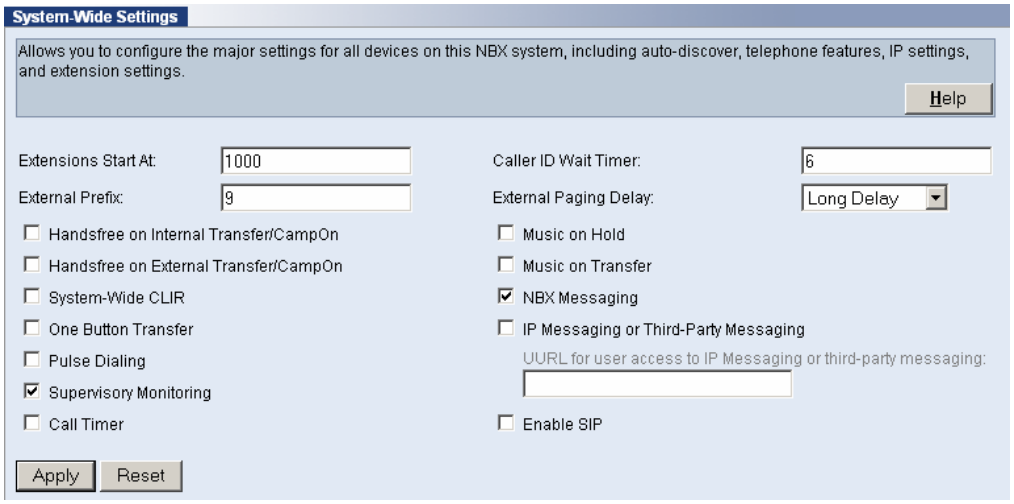


Figura 4.53. Muestra la habilitación de monitoreo de supervisor.

Creación del dominio del monitoreo del supervisor.

Para crear un dominio para el supervisor realizamos los siguientes pasos:

- Ingresar al Netset como administrador, del menu principal selecionar *Feature Settings*, y elegimos *Supervisory Monitoring*, como se muestra en la figura 4.54.

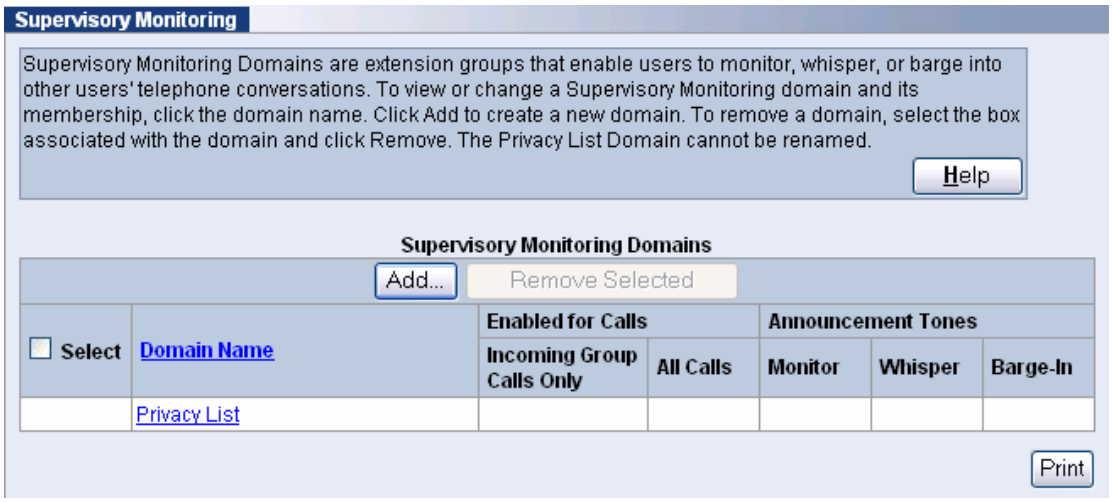


Figura 4.54. Muestra el dominio del monitoreo del supervisor.

- Hacer clic en el botón añadir, y se despliega la siguiente pantalla, figura 4.55.

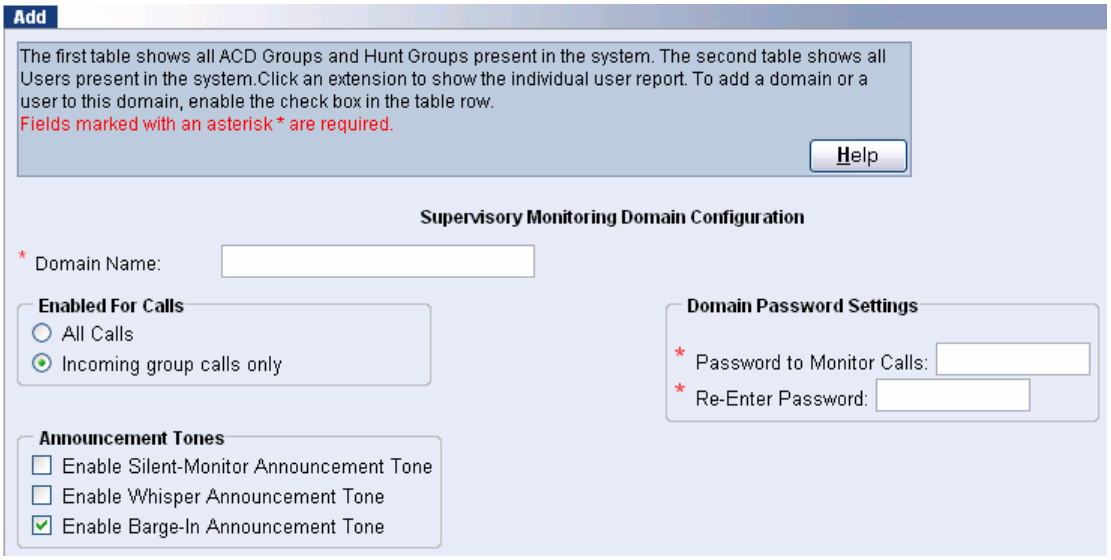


Figura 4.55. Muestra la pantalla para la creación de un nuevo dominio de supervisor.

- Ingrese el nombre del dominio: Jefe superior.
- Habilitar monitoreo del supervisor para todas las llamadas.

- Ingrese el *password* del dominio 123456.
- Seleccione *Barge-In Announcement Tone*.
- En el grupo del dominio y usuarios miembros del area del dominio, seleccione todas las extensions.
- Hacer clic en el botón OK.

WhisperPage.

La característica de WhisperPage permite que se marque una extensión de la NBX que está involucrado en una conversación con otra persona y hable a esa persona sin que la otra persona en la llamada pueda ser capaz de escucharlo.

Para la configuración de *WhisperPage,* realizamos los siguientes pasos:

- Entre al sistema como administrador del NetSet.
- Del menú principal del NetSet seleccione *Feature Settings*, y elija WhisperPage, como se muestra en la figura 4.56.

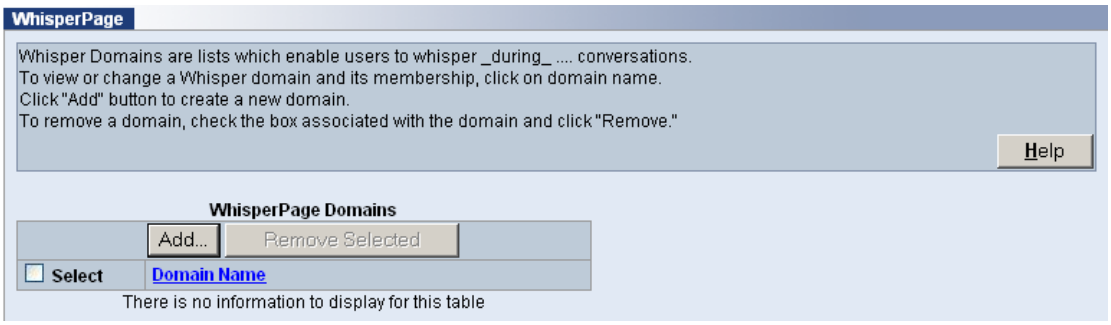


Figura 4.56. Muestra el dominio para *WhisperPage*

- Hacer clic en el botón de añadir.
- En la pantalla de WhisperPage cree el nombre del dominio, *Cotopaxiwhisper*.
- Escoja la extensión 1001 como hablante.
- Escoja la extensión 1002 como oyente, como se muestra en la figura 4.57.

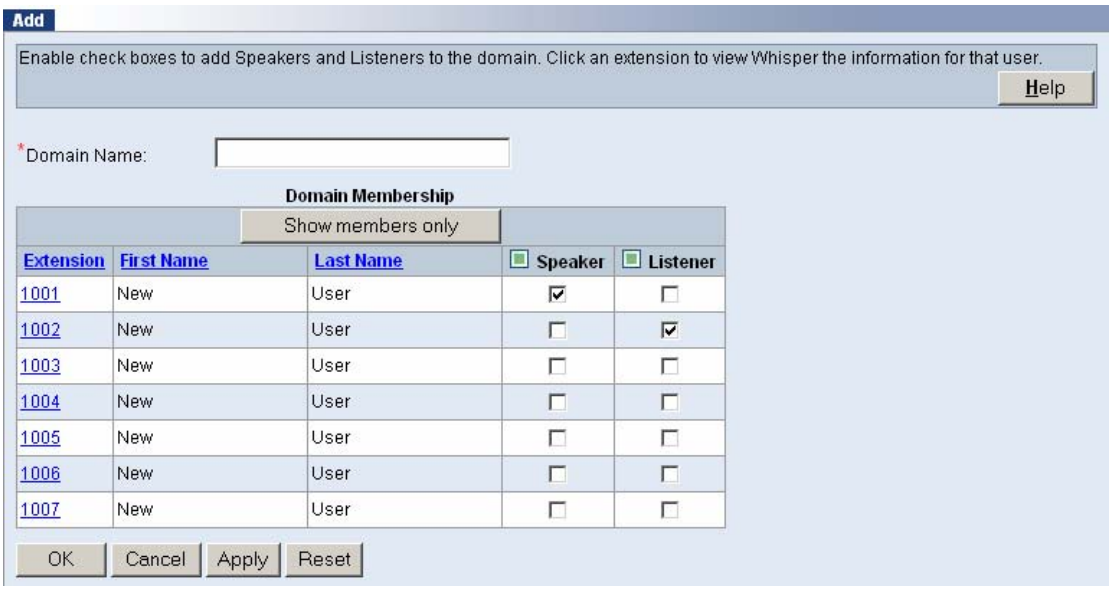


Figura 4.57. Miembros de WhisperPage.

- Hacer clic en el botón Aceptar.
- Hacer clic en OK cuando la ventana de terminación aparece.

Camp On.

Camp on permite que se coloque en una cola de espera una llamada transferida a una extensión de destino que ya está en uso. Cuándo la extensión se pone disponible, el sistema toca esa extensión automáticamente. Para la configuración de Camp on realizamos los siguientes pasos:

- Ingrese al *NetSet* como administrador.
- Del menú principal del *NetSet* , seleccione teléfonos, grupo de teléfonos.
- Seleccione los teléfonos 3102 Business Group
- Seleccionar mapeo de botones.
- Configure uno de los botones libres como *Camp on*.
- Hacer clic en el botón OK.

Llamada automática de regreso.

Callback automático permite que usted pida una llamada de regreso de una extensión de destino que esta en uso o sin respuesta. La NBX del sistema intenta conectarlo cuando la llamada destino se pone disponible. Sobre un teléfono de NBX, la característica de *Callback* automática es atractiva cuando la persona a quien se está

llamando está en otra llamada y usted quiere que el sistema genere una llamada hacia atrás tan pronto como esta persona este disponible. Para configurar *Callback* automático realizamos los siguientes pasos:

- Ingrese al *NetSet* como administrador.
- Del menú principal del *NetSet* , seleccione teléfonos, grupo de teléfonos.
- Seleccione los teléfonos 3102 *Business Group* Seleccionar mapeo de botones.
- Configure uno de los botones libres como *Call Back* automático.
- Hacer clic en el botón OK.

Claves de cuenta.

Claves de cuenta son los números adicionales que los usuarios marcan para asociar llamadas con funciones específicas, origen, o destino.

Verificar claves de cuenta es un ajuste de configuración global, diferente a imponer claves por clase de servicio. Si la configuración de la clase de servicio impone una clave de cuenta para un tipo de llamada especial, un usuario de teléfono de NBX debe ingresar una clave de cuenta antes de que el sistema de NBX encamine la llamada. Para la configuración de claves de cuenta realizamos los siguientes pasos:

- Entre al *NetSet* como administrador.
- Del menú principal del *NetSet* seleccione *feature setting*, códigos de cuenta, como se muestra en la siguiente figura 4.58.

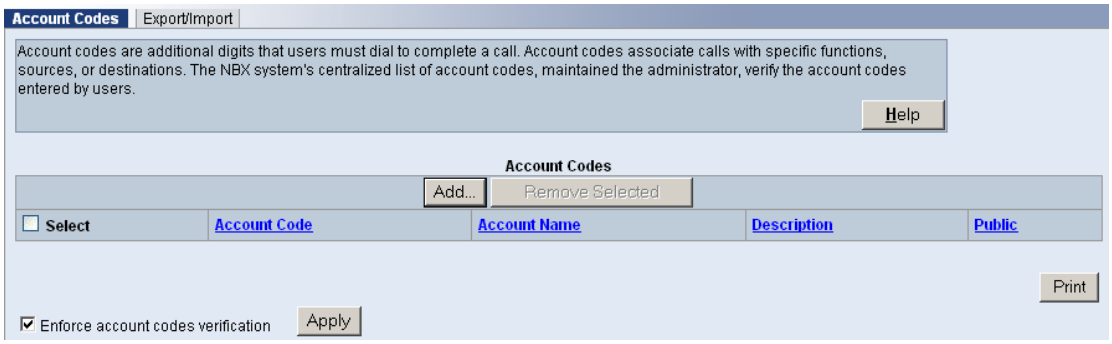


Figura 4.58. Códigos de Cuenta.

- Hacer clic en el botón añadir.
- En la pantalla de añadir clave del código de cuenta, ingrese la clave 2480.

- Nombre de la cuenta : dos por 80.
- Ingrese la descripción: dos para ochenta.
- Habilite que la clave de cuenta se visualize para todos los usuarios, como se lo muestra en la figura 4.59.

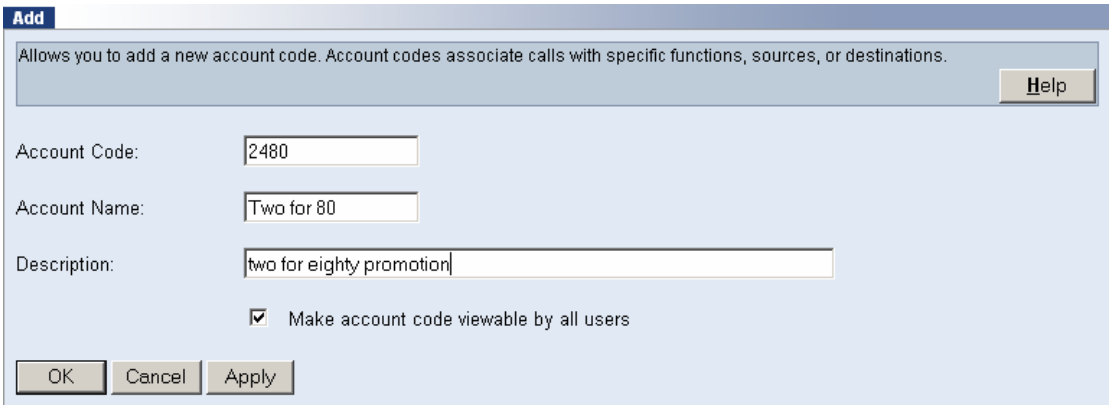


Figura 4.59. Muestra como añadir un nuevo código de cuenta.

Forzar códigos de cuenta a través de clase de servicio.

Para forzar claves de cuenta a través de la configuración de CoS, realizamos los siguientes pasos:

- Del menú principal del *NetSet*, seleccione configuración de usuarios, escoja clase de servicio.
- Seleccione Default User Group.
- Habilitar códigos de cuenta para llamadas locales.
- Hacer clic en OK.

Page Zones.

La característica de *Page Zone* permite que un subconjunto de dispositivos dentro del sistema como miembros de una zona. Los usuarios tienen la habilidad de llamar por megafonía a miembros de ese grupo solamente. El software de sistema de NBX soporta hasta 16 zonas de *paging* por el sistema. El sistema de NBX admite páginas de zona simultáneas múltiples. Sin embargo, un dispositivo que es actualmente la paginación o ser llamado por megafonía no responderá a otro pedido de página.

Creación de Zonas de *Paging*.

Para la creación de zonas de *paging*, realizamos los siguientes pasos:

- Ingresar al NetSet como administrador, seleccione *feature settings*, y elija *Page Zones,* como en la figura 4.60.

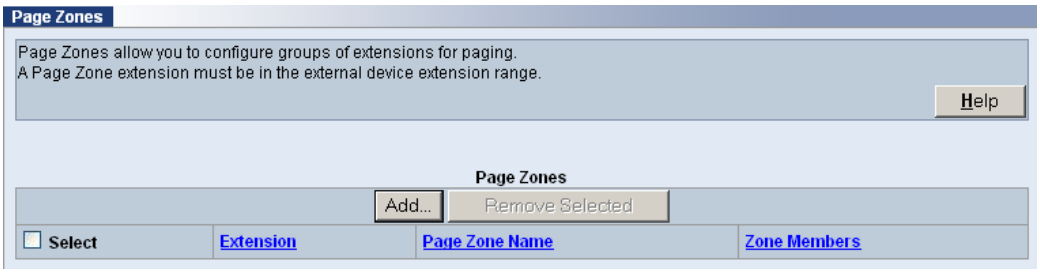


Figura 4.60. *Page Zones.*

- Seleccione añadir.
- Especifique en el nombre del campo *PageZone1*.
- Extensión de uso será la 6301.
- Seleccionemos las extensiones que "Solamente serán miembros que pueden llamar por megafonía a esta zona".
- Las extensiones selectas son 1001 y 1002, como se lo muestra en la figura 4.61.

Figura 4.61. Miembros de PageZone1.

Software de complemento de atendedora (CAS).

NBXTSP fue desarrollado por 3Com para permitir que a una aplicación TAPI interactúe con el teléfono de NBX del usuario sobre el PC de un usuario. Se puede configurar un número máximo de clientes de TAPI en el sistema. También se puede exigir que usuarios ingresen contraseñas para dispositivos de TAPI.

NBXTSP es un requisito esencial para la instalación de software de aplicación como CAS, *executive assistant* , etc. CAS proporciona en general una recepcionista a usuarios de NBX con el control de llamada desde el escritorio de la PC basado para el manejo de llamada rápido. CAS incluye un directorio de sistema más una "Lista rápida" personalizable y directorio personal. CAS complementa el 1105 de NBX y 3105 encargado funciones de consola y servicios. CAS funciona en PC con sistema operativo XP/2000 / NT / de Windows 95/98 multimedia. CAS incluye el control multi- sitio centralizado ahora.

Reporte detallado de llamadas.

Para el reporte detallado de llamadas, realizamos los siguientes pasos:

- Ingrese al NetSet como administrador.
- Seleccione mantenimiento de sistema, y elija *Call Reporting,* como lo muestra la figura 4.62.

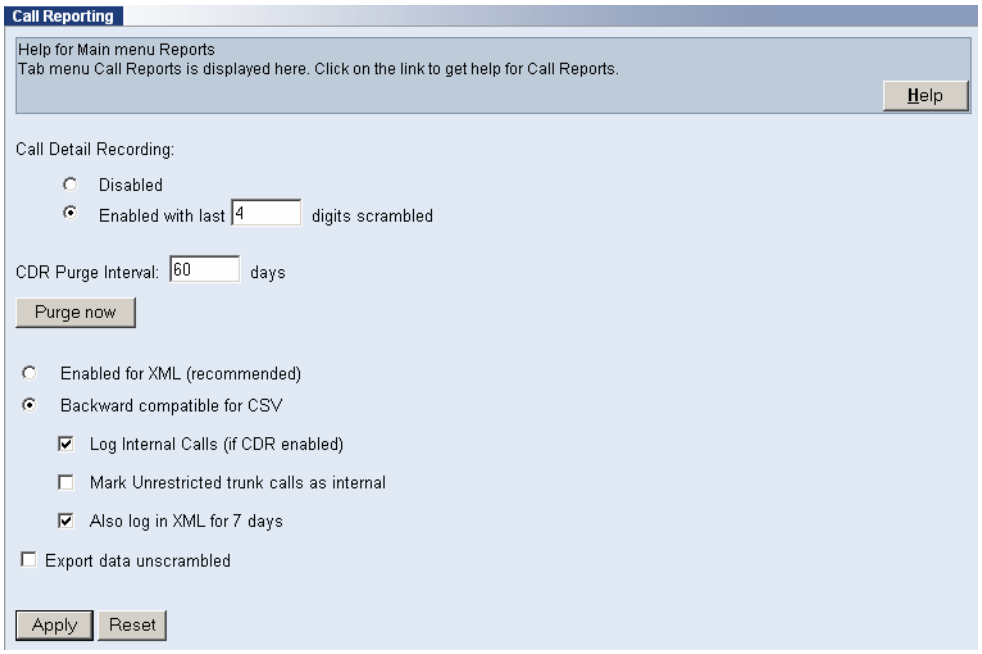


Figura 4.62. Reportador de llamadas.

- Permita CD con la 4 dígitos.
- *Purgar* el CDR en 60 días.
- Seleccione la compatibilidad con versiones anteriores para CSV.
- Seleccione log de llamadas internas (si CDR esta habilitado).
- Seleccione también Log en XML durante 7 días.
- Hacer clic en el botón Aplicar.
- Del menú principal del NetSet seleccione descargas, aplicaciones, como lo muestra la figura 4.63.

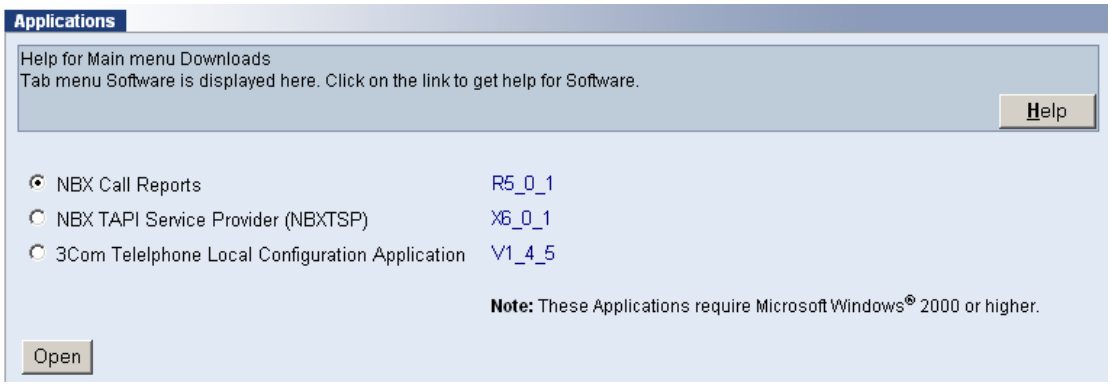


Figura 4.63. Aplicación de reportes.

- Seleccione informes de llamada de NBX.
- Hacer clic en Abrir y decida correr o guarde y luego ejecute el archivo.
- Siga todos los pasos para instalar el software sobre su PC. Será necesario colocar la dirección IP de la NBX y su contraseña.

4.1.5 Funcionalidades de central avanzada.

La central telefónica ofrece funcionalidades de central avanzada a través de *Telephony Applications Programming Interface* (TAPI), de esta manera se permite trabajar a la NBX como *Contact Center, IVR, etc.*

TAPI es una interface estándar para la integración de sistemas de telefonía y software basado en Windows que suministra control de llamadas entre la NBX y el servidor de aplicaciones, a través de la red de datos.

El Audio es llevado mediante archivos WAV entre la NBX y el servidor de aplicaciones a través de la red de datos, es un método eficiente y óptimo para interconectarse con las aplicaciones a un costo razonable.

TAPI 3.0 es una API evolutiva que proporciona convergencia de la telefonía tradicional PSTN y la telefonía IP. La telefonía IP constituye un conjunto de tecnologías emergentes que hace posible la colaboración de voz, datos y vídeo a través de las redes LAN, WAN e Internet existentes. TAPI 3.0 habilita la telefonía IP en los sistemas operativos de Microsoft® Windows® al proporcionar métodos sencillos y genéricos para realizar conexiones entre dos o más equipos y obtener acceso a cualquier flujo de medios que participa en la conexión.

TAPI 3.0 es compatible con conferencias H.323 basadas en estándares y conferencias de multidifusión IP. Utiliza el servicio *Active Directory* del sistema operativo Windows 2000 para simplificar la distribución en una organización e incluye soporte técnico de calidad de servicio (QoS, *Quality-of-Service*) para mejorar la calidad de las conferencias y la administración de la red.

Telefonía IP.

La telefonía IP constituye un conjunto de tecnologías emergentes que hace posible la colaboración de voz, datos y vídeo a través de las redes LAN, WAN e Internet existentes basadas en IP.

Específicamente, la telefonía IP utiliza los estándares abiertos IETF e ITU para transportar el tráfico multimedia a través de cualquier red que utilice IP y ofrece a los usuarios flexibilidad en los medios físicos (por ejemplo, líneas POTS, ADSL, ISDN (RDSI), líneas concedidas, cable coaxial, satélite y par trenzado) y en la ubicación física. Como resultado, se pueden utilizar las mismas redes ubicuas que transportan Web, correo electrónico y datos para conectarse con personas, compañías, organizaciones de enseñanza y gobiernos de todo el mundo.

TAPI 3.0 es una API evolutiva que permite la convergencia de la telefonía tradicional PSTN y la telefonía a través de redes IP.

Introducción a TAPI 3.0.

A medida que la telefonía y el control de llamadas son más frecuentes en el equipo de escritorio, es necesaria una interfaz de telefonía general que habilite aplicaciones para obtener acceso a todas las opciones de telefonía disponibles en cualquier equipo. Los medios o los datos de una llamada también deben estar disponibles para las aplicaciones de forma estándar.

TAPI 3.0 proporciona métodos sencillos y genéricos para realizar conexiones entre dos o más equipos, y obtener acceso a cualquier flujo de medios que participa en la conexión. Abstrae la funcionalidad de control de llamadas de forma que admita protocolos de comunicación diferentes, aparentemente incompatibles, para exponer una interfaz común a las aplicaciones.

TAPI 3.0 integra control de secuencias multimedia con la telefonía heredada. Asimismo, representa una evolución de la API TAPI 2.1 al modelo COM, que permite que las aplicaciones TAPI se escriban en cualquier lenguaje, como C/C++ o Microsoft® Visual Basic®.

Además de ser compatible con proveedores de telefonía clásicos, TAPI 3.0 es compatible con conferencias H.323 y conferencias de multidifusión IP estándar. TAPI 3.0 utiliza el servicio Active Directory de Windows® 2000 para simplificar la instalación en una organización y admite características de calidad de servicio (QoS) para mejorar la calidad de las conferencias y la administración de la red, como lo muestra la figura 4.64.

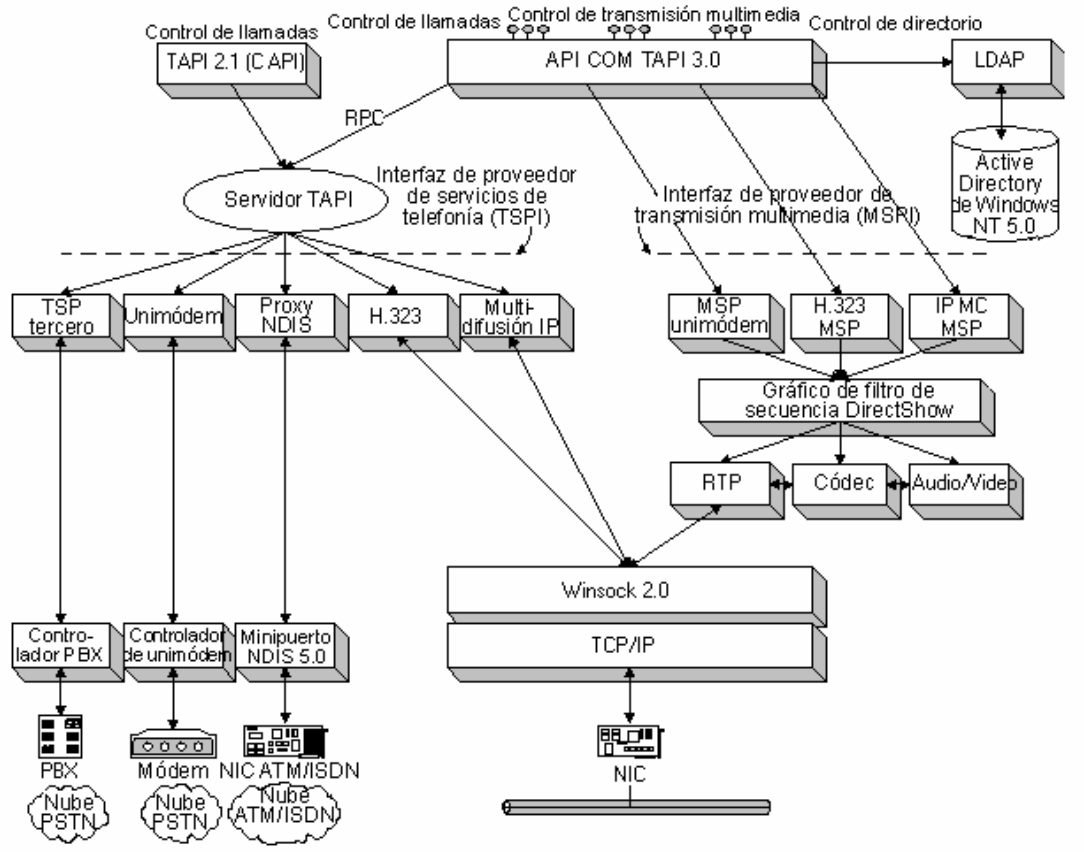


Figura 4.64. Arquitectura de TAPI

Interoperabilidad con bases de datos.

*S*istema de respuesta de Voz Interactivo (IVR) que maneja la gestión automática de llamadas entrantes y salientes sin la intervención de un Agente. El Cliente es quien, a través de comandos de voz o tonos de su teléfono (DTMF), solicita información o realiza transacciones.

Este producto, integrado a los sistemas de información corporativos, libera recursos humanos sustituyéndolos por un sistema *self-service* para el consumo masivo de información, generando de esta forma, un rápido retorno de la inversión.

El IVR incluye funciones de *e-mail-on-demand* y *fax-on-demand*, con las que el cliente puede recibir informaciones tales como balances de cuenta, reporte de transacciones o catálogos de productos y servicios. Entre las principales marcas de interoperabilidad con bases de datos, tenemos a *inConcert, Braxtel, Esnatech,* entre otros.

Funcionalidades

IVR: Sistema de respuesta de Voz Interactivo

Es una aplicación que acepta una combinación de entradas de voz y teclas provenientes del teléfono y brinda respuestas apropiadas en forma de voz, fax o e-mail.

El IVR invita a seleccionar opciones de un menú, solicitar la identificación y contraseña de un cliente o reconocerlo y validarlo mediante su timbre vocal, para luego suministrarle información que se encuentra en las bases de datos de la organización y permitirle realizar transacciones en forma interactiva.

El IVR también puede transferir la llamada a un Agente del *Contact Center* o enviar un *e-mail* o *fax* con información de la consulta realizada.

Debido a su flexibilidad, el IVR puede soportar el desarrollo y la implementación de complejas aplicaciones, para lo cual se deben desarrollar flujos de control a través de herramientas gráficas, como se lo muestra en la figura 4.65.

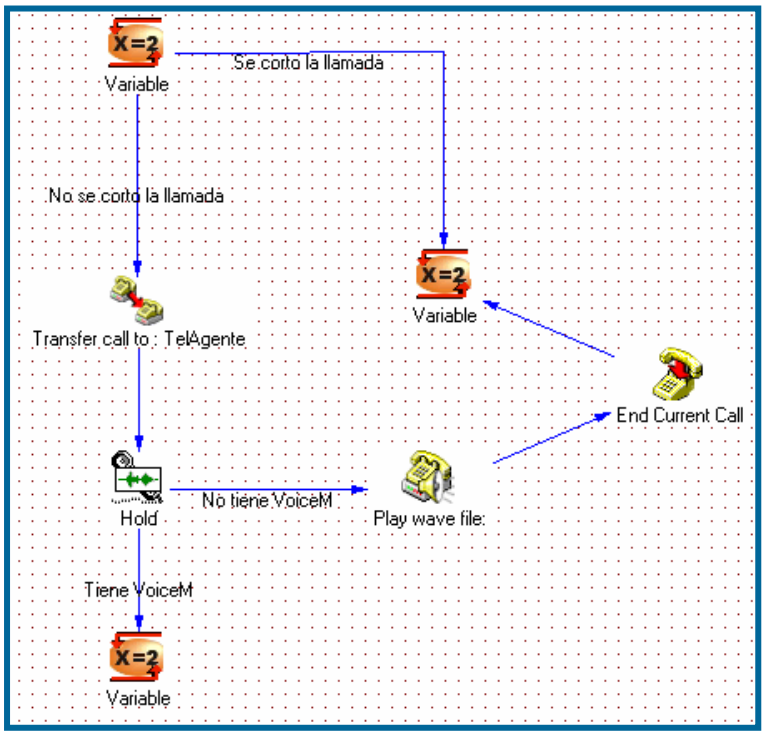


Figura 4.65. Muestra el control de flujos de un IVR.

EAI: Enterprise Application Integration.

El IVR incluye en su arquitectura una potente herramienta de integración *middleware* de última generación que le permite, de manera fácil y transparente, integrarse con aplicaciones de negocio (EAI) y con sistemas heredados ("Legacy Systems"), intercambiar información con sistemas de mensajería y acceder a bases de datos, como se lo muestra en la figura 4.66.

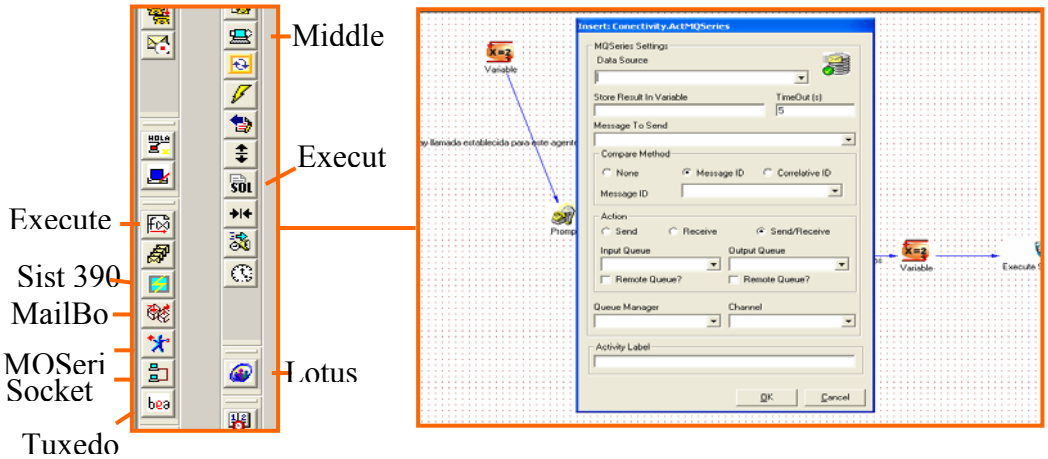


Figura 4.66. Muestra el intercambio de información entre bases de datos, correo electónico, etc.

CTI: Computer Telephony Integration.

La tecnología CTI que permite realizar el *Screen Pop* desplegando automáticamente la información del Cliente recabada desde el IVR, en la pantalla del Agente.

MODULOS.

La solución de las marcas de IVR, además del módulo IVR Server, se componen de otro módulo llamado Administrador.

Administrador.

Desde el módulo de Administrador se definen y mantienen, de manera simple y ágil, todos los parámetros de las campañas (unidades de trabajo del IVR). Adicionalmente se realiza la definición y mantenimiento de los usuarios del IVR (administradores y diseñadores) y la administración de los recursos (asociación de puertos de audio a las diferentes campañas implementadas).

Reportes.

Los módulos de administración de los IVRs tienen disponible los siguientes reportes que proveen información estadística sobre los niveles de productividad y servicio del IVR, como lo muestra la tabla 4.6.

Tabla 4.6 Reportes de los IVRs

	INBOUND IVR CALLS
Reporta	Todas las llamadas hechas al IVR y la *duración* de la misma, por *día* entre dos *fechas*, para la Campaña especificada.

	SUMMARY OF DAILY INTERACTIONS
Reporta	Resumen de llamadas hechas al IVR por Hora en un determinado rango de fechas para una determinada Campaña
Formato	*Cantidad* de llamadas al IVR hechas en una hora, el *porcentaje* que dichas llamadas representan sobre el total de llamadas realizadas y el *promedio* de duración de las mismas para el día determinado.

	OUTBOUND IVR CALLS
Reporta	Todas las llamadas realizadas, por *día y hora* entre dos *fechas*, proporcionando información de la duración total, el número destino y el resultado de la llamada, para la Campaña especificada.

	IVR INTERACTIOS QUERY
Reporta	Todas las llamadas de una determinada Campaña, producidas en un determinado rango de fechas y que cumplen con una determinada condición de filtrado. Todos estos datos son ingresados por el usuario que realiza la consulta.
Formato	Nombre y versión del Proceso (Flujo - IVR utilizado); fecha y hora de comienzo, fecha y hora de finalización, y duración total de la llamada, ordenado según la fecha de comienzo de la llamada.

Para una aplicación practica de IVR en la NBX de la Universidad Cotopaxi, sería realizar un proceso de matriculas vía telefónica. Este proceso se lo realiza de la siguiente manera:

En la central telefónica cambiamos la configuración de la atendedora automática, nos dirigimos al mapeo de botones y configuramos que cuando pulsen 5 se enrute a la lista de extensiones del IVR, para que el usuario pueda realizar su proceso de matricula vía telefónica.

Luego en el IVR nos creamos una lista de extensiones, en la cual va a estar las extensiones requeridas, por ejemplo la lista de extensiones es la *0020 y la cual contiene las siguientes extensiones 7550, 7551, 7552, 7553. Una vez creado este proceso el IVR esta activo para funcionar, cuando el usuario llama a la Universidad y pulsa el botón 5 que es para matricularse, la llamada se enruta al IVR, y en este proceso le van a pedir al cliente ingresar su número de cedula, el cual es enviado por medio de pulsos DTMF al IVR, que va a transformar estos pulsos en datos, y luego el IVR envia estos datos a la base de datos, por ejemplo Oracle, la base de datos ejecuta el pedido enviado por el IVR, este le envía una respuesta al IVR, el IVR transforma los datos devueltos a voz, y este es enviada por último a la NBX, en el cual el cliente va a recibir una respuesta del IVR.

Requerimientos de infraestructura LAN.

Conexión de la NBX a la PSTN y a la red LAN. Conexión de red (Switch) LAN Ethernet 10/100 Mbits para servidores y estaciones de trabajo de Agentes.

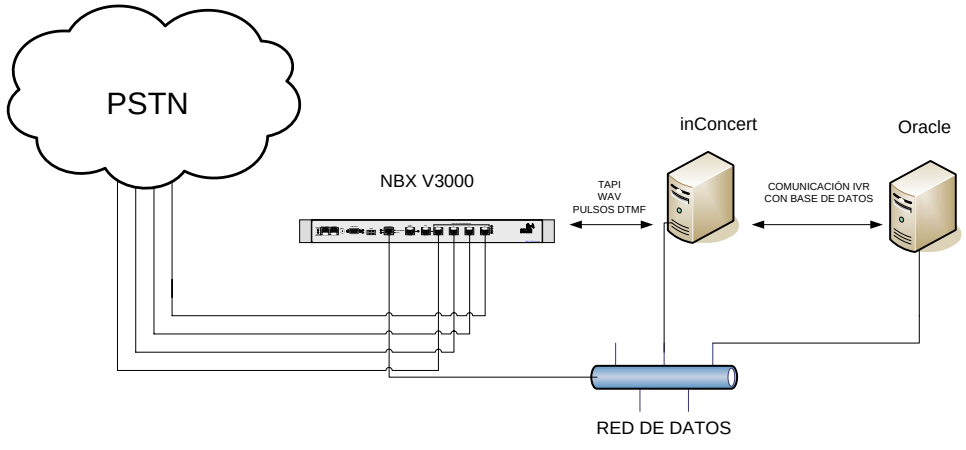


Figura 4.67. Ejemplo de interoperabilidad de la NBX con un IVR.

Aplicación con software de terceros.

Multimedia Contact Center, es un producto multimedia, robusto y especialmente pensado para organizaciones que administran su propio Centro de Contactos y para proveedores de servicios (OutSourcing).

Incorpora tecnología diseñada para soportar un alto tráfico (más de 5.000 interacciones por hora) y operar en modalidad 24 X 7. Multimedia Contact Center realiza el manejo de interacciones a través de múltiples canales de comunicación, tales como teléfono, voz sobre IP (VoIP), e-mail, Chat, portales web, y otros.

La NBX es compatible con diferentes marcas de Contac Centers como lo es inConcert, Exchange, entre otros.

FUNCIONALIDADES.

ACD: Distribución Automática de Llamadas.

Los algoritmos de ACD, que establecen la manera en que serán distribuidas las interacciones multimedia a los agentes, permiten aplicar reglas de negocio complejas en las decisiones de distribución de tráfico.

Existen múltiples criterios de distribución de llamadas (circular, balanceo de carga, balanceo de carga inverso, distribución en base a parámetros de las campañas y distribución basada en las habilidades de los Agentes).Todos ellos pueden ser combinados y están disponibles.

Se puede parametrizar también el tiempo máximo de búsqueda de agente libre y las condiciones de salida a dicha espera. Es posible anunciarle al cliente el tiempo promedio que tendrá de espera mientras se libera un operador e incluso ejecutar subprocesos en caso de desbordamiento.

CTI: Computer Telephony Integration.

Los *Contact Center* permiten la tecnología CTI que realiza el *Screen Pop* desplegando automáticamente la información del Cliente en la pantalla del Agente

Call Blending.

Los agentes pueden asociarse a múltiples campañas, entrantes y/o salientes, obteniéndose estadísticas de productividad discriminadas por tipo de servicio. Las prestaciones de Call Blending provistas por los Contact Center son válidas para todo tipo de interacciones multimedia, como se lo muestra en la figura 4.68.

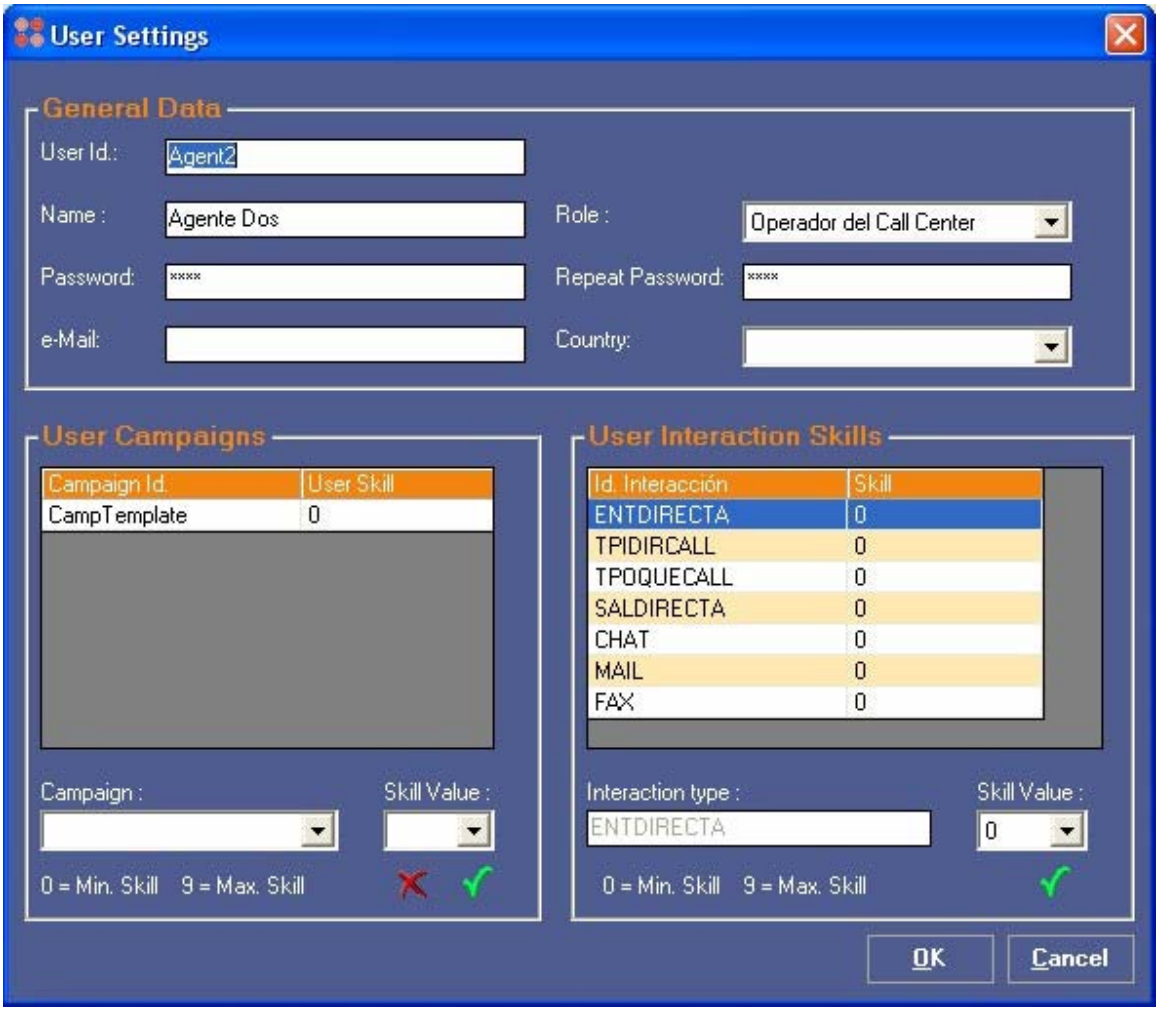


Figura 4.68. Muestra como un agente puede asociarse a multiples campañas.

EAI: Enterprise Application Integration.

Los Contact Center proveen en su arquitectura una potente herramienta de integración *middlewar e* de última generación que le permite, de manera fácil y transparente, integrarse con aplicaciones de negocio (EAI) y con sistemas heredados

("Legacy Systems"), intercambiar información con sistemas de mensajería y acceder a bases de datos, como se lo muestra en la figura 4.69.

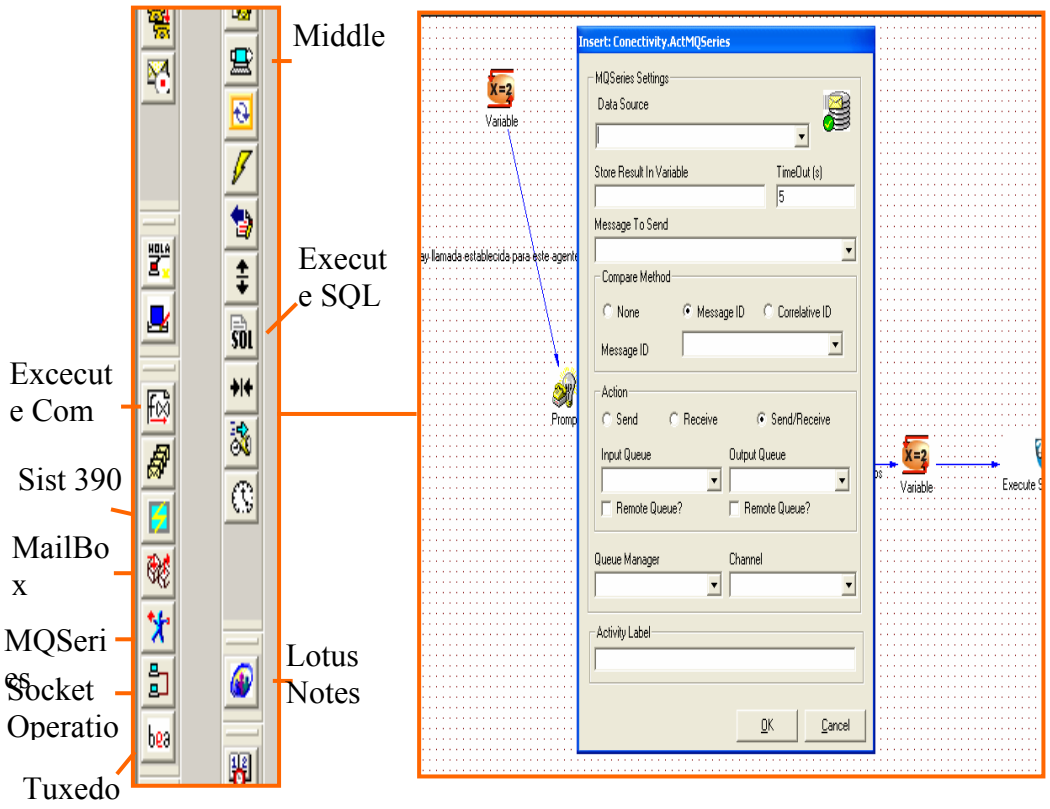


Figura 4.69. Integración con aplicaciones de negocios.

MODULOS.

Los Contact Center por lo general trabajan con módulos, para brindar un mejor trabajo al Contact Center y estos son:

- Agentes
- Supervisor
- Administrador

Agentes

El módulo es utilizado por los operadores del Contact Center. Es una aplicación compatible con Windows 2000 Professional y Windows XP. Opcionalmente, los Agentes podrán disponer de teléfonos físicos o por software.

Se instala fácilmente en la estación de trabajo del Agente y mediante una interfase ergonómica y simple provee todas las funcionalidades para que éste conduzca eficientemente las interacciones con los clientes.

Permite que los operadores manejen todos los tipos de interacciones, provenientes de múltiples canales, desde una misma herramienta y en un mismo PC lo que facilita la obtención de altos niveles de rendimiento y servicio.

Supervisor.

El módulo de supervisión está especialmente diseñado para el o los Supervisores del Centro de Contactos, orientada a incrementar la productividad y controlar el cumplimiento de los niveles de servicio para todo tipo de interacciones (Telefonía, Chat, eMail, VoiceMail, CallBack, etc.)

El módulo de Supervisor, permite monitoreo en tiempo real de distintas entidades, ya sean físicas o lógicas (interacciones del Cliente que arriban por los múltiples canales, agentes, campañas, grabaciones, etc.), proporcionando información estadística en vistas y gráficos configurables y de fácil acceso para quien opera la herramienta.

Cada Supervisor podrá tener un vista asociada a su perfil, de este modo se pueden segmentar los recursos a monitorear con sus atributos y valores actualizados.

Las alertas visuales proporcionadas al supervisor mediante cambios de colores, le permiten detectar inmediatamente situaciones críticas de acuerdo a los parámetros de nivel de servicio establecidos por la empresa, como se muestran en la siguiente figura 4.70.

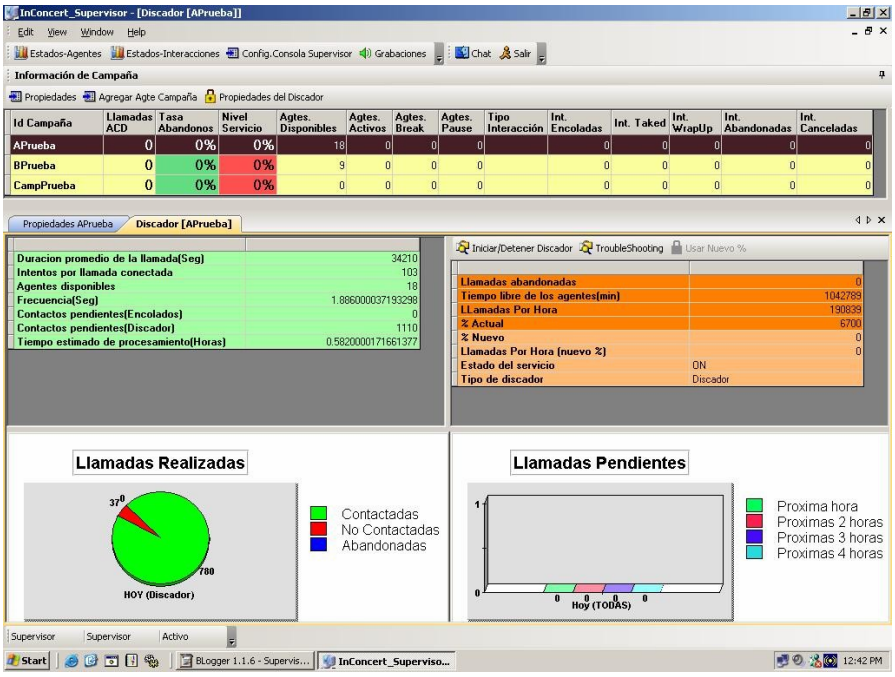


Figura 4.70. Muestra las interacciones con los clientes de forma estadística.

Administrador.

Desde el módulo de Administrador se definen y mantienen, de manera simple y ágil, todos los parámetros de las campañas (unidades de trabajo del Centro de Atención). Adicionalmente se realiza la definición y mantenimiento de los usuarios del CallCenter (supervisores, administradores, diseñadores y agentes) y la administración de los recursos (asociación de puertos de audio, agentes, supervisores, etc., a las diferentes campañas implementadas).

Desde el módulo Administrador, es posible el acceso a los reportes históricos y estadísticos del centro de contactos.

Reportes.

El Administrador tiene disponible los siguientes reportes que proveen información estadística sobre los niveles de productividad y servicio del Contact Center.

Reportes por Agente.

Detalle de Llamadas Entrantes

Detalle de Llamadas Salientes

Detalle de LogIn/LogOut. de Agente
Resumen de Llamadas
Resumen de Llamadas por Día
Resumen de Llamadas por Mes
Resumen de Llamadas Entrantes
Resumen de Llamadas Entrantes por Día
Resumen In. Llamadas por Mes
Resumen de Llamadas Salientes
Resumen de Llamadas Salientes por Día
Resumen de Llamadas Salientes por Mes

Reportes por Campaña.
Detalle de Llamadas Salientes
Detalle de Llamadas Salientes
Detalle de LogIn/LogOut de Agente por Campaña
Resumen de Llamadas Abandonadas
Resumen de Llamadas Abandonadas y Tomadas
Resumen de Llamadas
Resumen de Llamadas por Día
Resumen de Llamadas por Mes
Resumen de Llamadas Entrantes
Resumen de Llamadas Entrantes por Día
Resumen de Llamadas Entrantes por Mes
Resumen de Llamadas Salientes
Resumen de Llamadas Salientes por Día
Resumen de Llamadas Salientes por Mes

Requerimientos de infraestructura lan.
Conexión de la NBX a la PSTN y a la red LAN.
Conexión de red (Switch) LAN Ethernet 10/100 Mbits para servidores y estaciones de trabajo de Agentes, como se lo muestra en la figura 4.71.

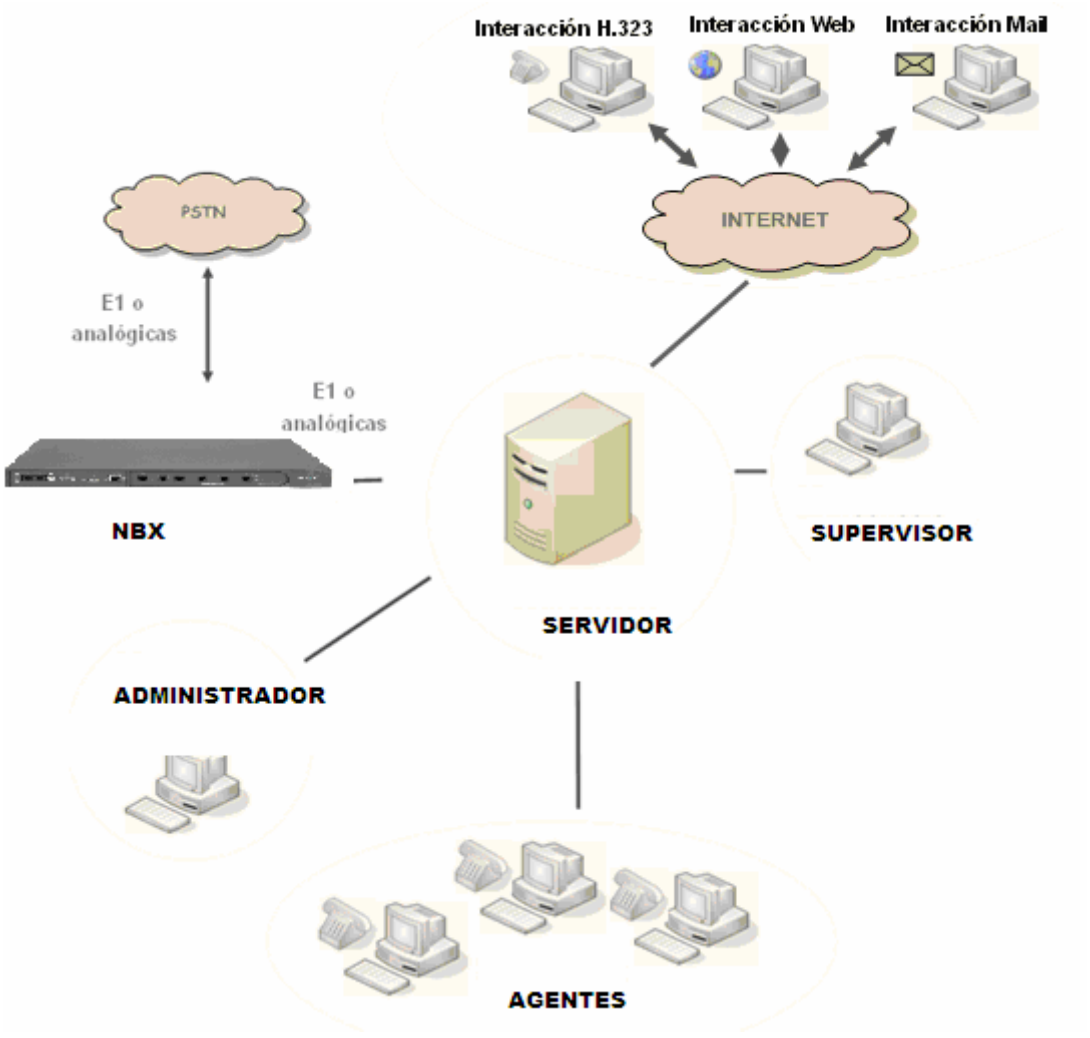


Figura 4.71: Ejemplo de interoperabilidad de la NBX con un Contact Center.

4.2 CONFIGURACIÓN DEL IPS

Como vamos a implementar una red convergente, vamos a realizar la configuración del TippingPoint X505 con la finalidad de poder manejar Múltiples NBX localizadas en las sedes de la empresa (actualmente existe solo un *campus* pero existe la proyección de tener más localidades). Por lo tanto configuraremos al X505 para que maneje calidad de servicio y *multicast* dentro de túneles VPN para que usuarios remotos puedan usar telefonía IP con todos sus beneficios. (con la configuración que realizaremos a continuación, un usuario puede ir a cualquier parte del mundo y poner un teléfono IP hacia Internet y conectarse a la NBX de la universidad con las respectivas seguridades).

Con respecto a las reglas de Firewall, se dejarán las que vienen por defecto en el equipo y se añadirán una cuantas para permitir túneles VPN y manejar filtrado de contenido de Internet.

4.2.1 Configuración de políticas de seguridad basado en puertos e interfaces.

Este escenario se construirá para implementar sobre el TippingPoint X505 un enlace VPN a través de IPSec. A través del túnel pasará información con calidad de servicio de telefonía IP para usuarios remotos. El protocolo de enrutamiento que será utilizado es estático y se configurará el equipo para dejar pasar *multicast* de tal manera que se puede hacer telefonferencias desde lugares remotos.

Para que tanto *multicast* como enrutamiento dinámico pasen por el X505, se utilizará GRE (encapsulamiento genérico de rutas). Este protocolo embebe el contenido del paquete con el contenido GRE para que se pueda transferir *multicast*, este link lo llamaremos túnel GRE.

El X505 soporta el uso de GRE sobre IPSec (GRE/IPSec) logrando que túneles GRE puedan ser establecidos en túneles VPN que usan IPSec.

En la configuración el equipo que actualmente tenemos será llamado “X505_1” y soportará túnels VPN desde cualquier lugar del mundo.

Los procedimientos que se realizarán son los siguientes:

- Establecer conectividad básica de la unidad (no detallado en este documento porque es rutinario, pero para este paso hay que establecer las interfaces virtuales, configurar los servidores DHCP en cada equipo y crear políticas en el Firewall para permitir el PING desde la WAN hacia el X505
- Establecer el tunnel VPN por IPSec. Para esto usaremos el modo VPN que tiene el equipo por defecto.
- Convertir el tunnel IPSec en GRE/IPSec
- habilitar *multicast*
- Pruebas de funcionamiento (que serán detalladas en un capítulo posterior)

Configuración de los teléfonos de la NBX (expuesto en el punto anterior de esta tesis).

Lo primero que vamos a hacer es el OBE (configuración inicial del equipo). Prendemos el equipo y conectamos a través de un cable de consola serial a 115200 de velocidad usando el programa tera term (se puede usar también hyperterminal de Windows).

Lo primero que nos va a pedir el equipo es poner el nivel de seguridad, pondremos la opción más segura que es la 2 (siendo 0 la menos segura), como se lo muestra en la figura 4.72.

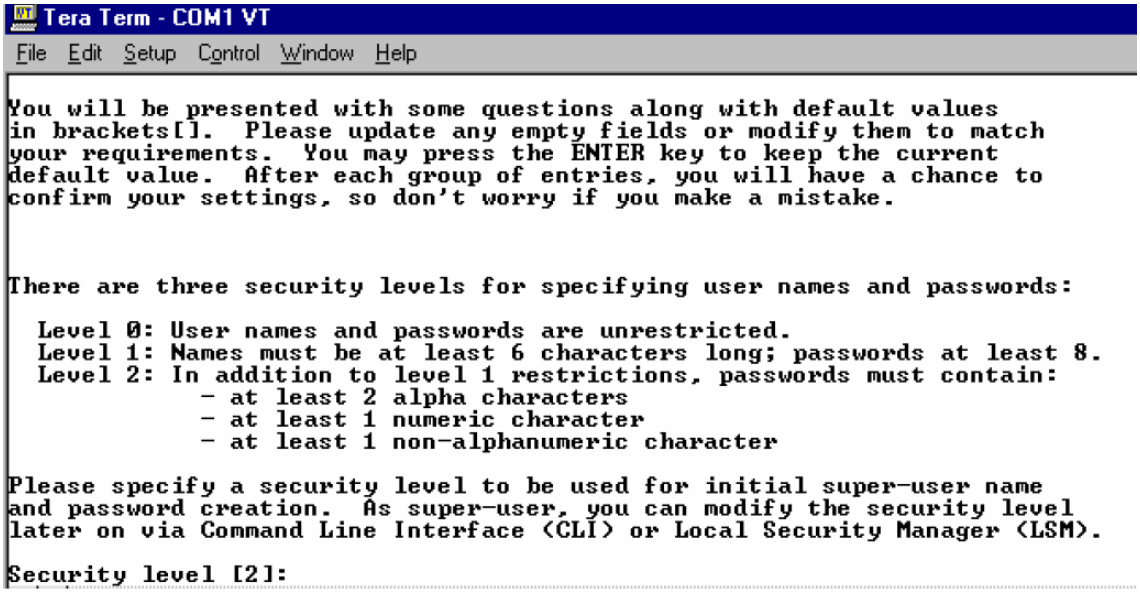


Figura 4.72. Muestra el nivel de seguridad de *password* que se va a elegir.

Después pondremos el nombre de usuario y contraseña al equipo, como se lo muestra en la figura 4.73.

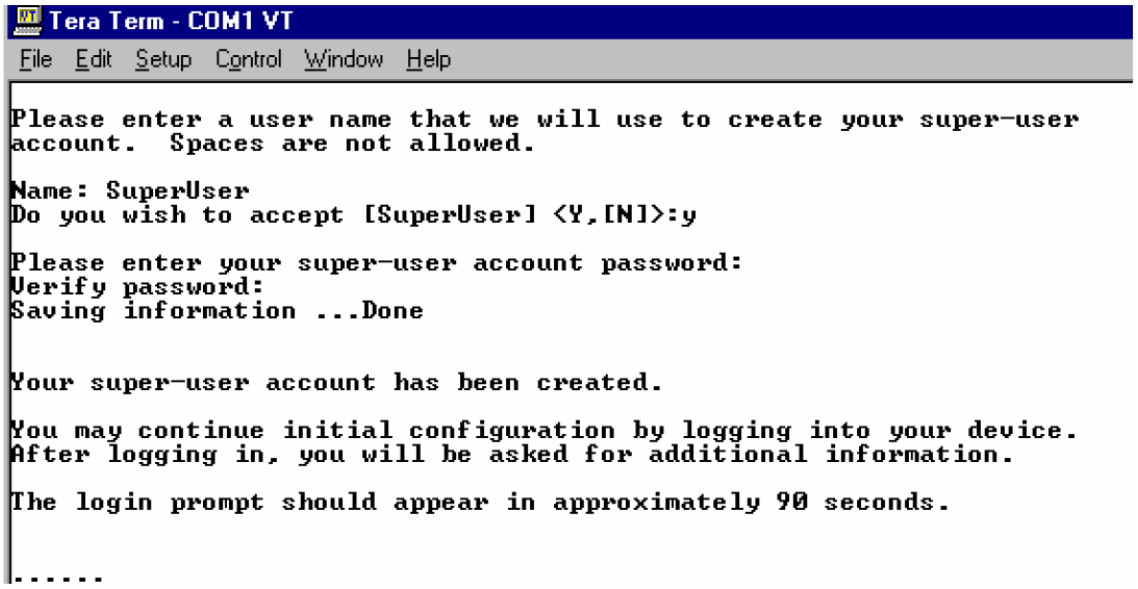


Figura 4.73. Pantalla para ingresar el *password*.

Después ponemos la IP del puerto de administración, como se muestra en la figura 4.74.

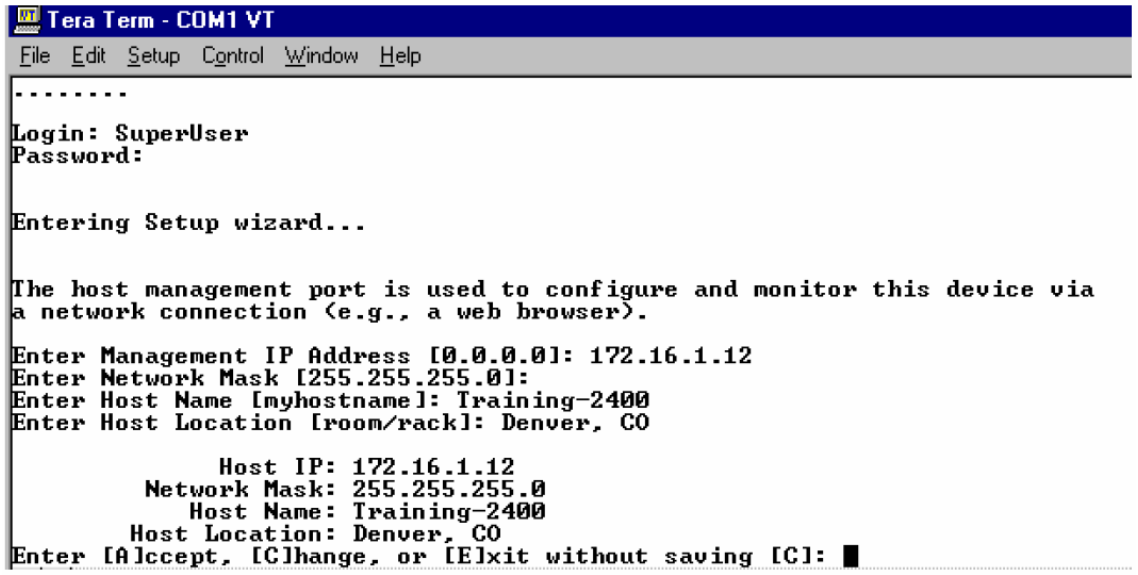


Figura 4.74. Pantalla que permite ingresar la dirección IP del equipo.

Al resto de opciones elegimos NO porque lo configuraremos después de forma gráfica. (con esta configuración ya están automáticamente creadas las reglas del corafuegos, HHCP habilitado, lo único que debemos hacer es ir a un *web browser* como Internet Explorer 6.0 y poner https://172.16.1.12)

Nota, se cambiara la IP de la Lan a 192.168.3.1 (por esta razón más adelante veremos los túneles con direcciones internas 192.168.3.x), dentro del explorador elegir Network- IP – y poner las IPs que nos dio el ISP, se se desea se puede allí mismo cambiar el nombre de las interfaces.

4.2.2 Establecimiento del túnel IPSec.

Una vez que hemos realizado el OBE (Experiencia fuera de caja, en donde ponemos una IP al equipo, ponemos el nombre de usuario y contraseña, habilitamos el servidor DHCP y ponemos nombres a las interfaces), seguimos los siguientes pasos:

Paso 1: Configurar los parámetros de IPSec:

```
X505_1# conf t vpn ike local-id email universidad@3com.com
X505_1# conf t vpn ike local-id domain universidad
```

Usar la propuesta IKE que viene en el equipo por defecto (IKE proposal 3DES-SHA1-PSK):

```
X505_1# show conf vpn ike
vpn ike local-id email universidad@3com.com
vpn ike local-id domain universidad
vpn ike add 3DES-SHA1-PSK
vpn ike proposal 3DES-SHA1-PSK phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-PSK phase1-integrity sha1
vpn ike proposal 3DES-SHA1-PSK phase1-dh-group 2
vpn ike proposal 3DES-SHA1-PSK phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-PSK auth-type psk
vpn ike proposal 3DES-SHA1-PSK aggressive-mode disable
vpn ike proposal 3DES-SHA1-PSK local-id-type ip
vpn ike proposal 3DES-SHA1-PSK peer-id-type ip
vpn ike proposal 3DES-SHA1-PSK ca-cert ANY
vpn ike proposal 3DES-SHA1-PSK nat-t disable
```

vpn ike proposal 3DES-SHA1-PSK dpd enable
vpn ike proposal 3DES-SHA1-PSK auto-connect disable
vpn ike proposal 3DES-SHA1-PSK tight-phase2-control enable
vpn ike proposal 3DES-SHA1-PSK phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-PSK phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-PSK phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-PSK pfs disable
vpn ike proposal 3DES-SHA1-PSK phase2-dh-group 2

Paso 2: Definir el SA (asociación de seguridad) y atarlo a la propuesta de IKE:
Ojo: cuando ponemos la dirección 0.0.0.0 decimos que el tunel se genera desde cualquier dirección IP

X505_1# conf t vpn ipsec add site1_sa
X505_1# conf t vpn ipsec sa site1_sa key ike proposal 3DES-SHA1-PSK shared-secret testtest
X505_1# conf t vpn ipsec sa site1_sa transport enable
X505_1# conf t vpn ipsec sa site1_sa peer 0.0.0.0
X505_1# conf t vpn ipsec sa site1_sa enable

Paso 3: Habilitar IPSec:

X505_1# conf t vpn ipsec enable

Paso 4: para pruebas se puede usar un PC u otro firewall con los mismos parámetros

Una vez que se haya hecho un túnel con un PC, revisar que el tunnel se haya configurado bien:

X505_1# show vpn ipsec

Name	Peer	Local ID	Peer ID	Status
---	---	---	---	---

site1_sa	200.31.6.40	200.31.6.31	200.31.6.40	Phase 1 Idle
		200.31.6.31 -	200.31.6.40 -	Phase 2 Idle
		200.31.6.31	200.31.6.40	

X505_1# ping 200.31.6.40
64 bytes from 200.31.6.40: icmp_seq=3. time=0. ms
64 bytes from 200.31.6.40: icmp_seq=4. time=0. ms
64 bytes from 200.31.6.40: icmp_seq=5. time=0. ms
64 bytes from 200.31.6.40: icmp_seq=6. time=0. ms
----200.31.6.40 PING Statistics----
7 packets transmitted, 4 packets received, 42 percent packet loss
round-trip (ms) min/avg/max = 0/0/0

4.2.3 Establecimiento del tunel GRE/IPSec.

Paso 1: crear un GRE virtual

X505_1# conf t interface virtual add 3 gre
X505_1# conf t interface virtual gre 3 local-ip 192.168.3.2
X505_1# conf t interface virtual gre 3 remote-endpoint-ip 200.31.6.40

X505_1# conf t interface virtual gre 3 sa site1_sa
X505_1# conf t interface virtual gre 3 remote-endpoint-ip 0.0.0.0
X505_1# conf t interface virtual gre 3 peer-ip 192.168.3.1
X505_1# conf t interface virtual gre 3 zone add VPN

Paso 2: Como el túnel termina en una zona llamada VPN, debemos permitir que la información del túnel VPN llegue sin restricciones a la LAN en donde está la NBX, como hay 10 reglas por defecto en el equipo, esta será la regla número 11 (el resto de reglas serán 12, 13 14 etc)

X505_1# conf t policy rule update 11 allow LAN VPN ANY
X505_1# conf t policy rule move 11 before 8
X505_1# show policy rules

ID	Action	Source	Destination	Service	En.
1	allow	LAN	WAN	ANY	X
2	allow	LAN	this-device	sms-conf..	X
3	allow	LAN	this-device	icmp-ping	X
4	allow	LAN	this-device	secure-m..	X
5	allow	LAN	this-device	dhcp-ser..	X
6	allow	LAN	this-device	dns	X
7	allow	ANY	this-device	vpn-prot..	X
11	allow	LAN	VPN	ANY	X
8	allow	WAN	this-device	sms-conf..	
9	allow	this-device	ANY	ANY	X
10	deny	ANY	ANY	ANY	X

Paso 4: Definir alguna polítias en la reglas del cortafuegos para que se pueda pasar a través de GRE el ping (ya que lo usaremos como herramienta de monitoreo)

X505_1# conf t policy rule update 11 allow LAN VPN ANY

X505_1# conf t policy rule move 11 before 8

X505_1# conf t policy rule update 12 allow VPN ANY ANY

X505_1# conf t policy rule move 12 before 8

X505_1# show policy rule

ID	Action	Source	Destination	Service	En.
1	allow	LAN	WAN	ANY	X
2	allow	LAN	this-device	sms-conf..	X
3	allow	LAN	this-device	icmp-ping	X
4	allow	LAN	this-device	secure-m..	X
5	allow	LAN	this-device	dhcp-ser..	X
6	allow	LAN	this-device	dns	X
7	allow	ANY	this-device	vpn-prot..	X
11	allow	LAN	VPN	ANY	X

12	allow	VPN	ANY	ANY	X
8	allow	WAN	this-device	sms-conf..	
9	allow	this-device	ANY	ANY	X
10	deny	ANY	ANY	ANY	X

4.2.4 Habilitar *Multicast* (IGMP, PIM-DM).

Se debe habilitar IGMP y PIM-DM, esto se lo hace a través de los siguientes comandos:

X505_1# conf t routing multicast igmp enable

X505_1# conf t routing multicast pim-dm enable

X505_1# conf t interface virtual internal 1 igmp enable

X505_1# conf t interface virtual internal 1 pim-dm enable

X505_1# conf t interface virtual gre 3 igmp enable

X505_1# conf t interface virtual gre 3 pim-dm enable

X505_1# conf t policy rule update 13 allow LAN this-device igmp

X505_1# conf t policy rule move 13 before 8

X505_1# show policy rules

ID	Action	Source	Destination	Service	En.
1	allow	LAN	WAN	ANY	X
2	allow	LAN	this-device	sms-conf..	X
3	allow	LAN	this-device	icmp-ping	X
4	allow	LAN	this-device	secure-m..	X
5	allow	ANY	this-device	vpn-prot..	X
6	allow	WAN	this-device	sms-conf..	
7	allow	this-device	ANY	ANY	X
9	allow	LAN	this-device	dhcp	X
10	allow	WAN	this-device	icmp-ping	
11	allow	LAN	VPN	ANY	X
12	allow	VPN	ANY	ANY	X
13	allow	LAN	this-device	igmp	X

8	deny	ANY	ANY	ANY	X

Para revisar que todo esté bien:

X505_2# show routing multicast

IGMP Querier Status

Interface IP Address Querier Groups

--- --- --- ---

1 172.17.2.254 172.17.2.254

2 200.31.6.31

3 192.168.3.2 192.168.3.2 (nota: esta es una IP diferente a la red para evitar conflictos de IP).

PIM-DM Neighbor Table

Neighbor Interface Uptime Expires Version

--- --- --- --- ---

192.168.3.1 3 3 102 2

Configuración de filtros de IPS con políticas basadas en cierre de brechas de seguridad.

Para cerrar las brechas de seguridad hay que cambiar los filtros del IPS, las políticas que se manejarán serán cerrar spyware, virus, gusanos, troyanos, P2P y proteger las bases de datos Oracle que posee la empresa, por esta razón se cambiarán los filtros a bloquear y modificar como aparecen en la siguiente tabla:

Tabla 4.7 Muestra los filtros cambiados en el TPX505

Time	Name	Category	Type	Src. Addr.	Src. Port	Dst. Addr.	Dst. Port	VLAN	Device	Segment
10/3/06 4:39:...	0657: FTP: ...	Exploits	Block	10.0.30.117	1382	10.0.30.118	21		2.5 IPS	
10/3/06 4:39:...	0657: FTP: ...	Exploits	Block	10.0.30.115	39182	10.0.30.116	21		2.5 IPS	
10/3/06 4:39:...	1129: HTTP: I...	Vulnerabilities	Block	10.0.30.119	33036	10.0.30.120	80		2.5 IPS	
10/3/06 4:39:...	2064: SMB: ...	Exploits	Block	10.0.30.111	1039	10.0.30.112	139		2.5 IPS	
10/3/06 4:39:...	1698: HTTP: ...	Exploits	Block	10.0.30.107	35421	10.0.30.108	80		2.5 IPS	
10/3/06 4:39:...	0321: Nmap ...	Reconnaissa...	Block	10.0.30.105	52682	10.0.30.106	1		2.5 IPS	
10/3/06 4:39:...	1129: HTTP: I...	Vulnerabilities	Block	10.0.30.109	32781	10.0.30.110	80		2.5 IPS	
10/3/06 4:39:...	0260: HTTP: ...	Exploits	Block	10.0.30.103	4253	10.0.30.104	80		2.5 IPS	
10/3/06 4:39:...	0657: FTP: ...	Exploits	Block	10.0.30.99	39159	10.0.30.100	21		2.5 IPS	
10/3/06 4:39:...	1450: MS-RP...	Vulnerabilities	Block	10.0.30.101	4752	10.0.30.102	135		2.5 IPS	
10/3/06 4:39:...	1323: HTTP: I...	Vulnerabilities	Block	10.0.30.97	1038	10.0.30.98	80		2.5 IPS	
10/3/06 4:39:...	0588: DNS: I...	Exploits	Block	10.0.30.95	57785	10.0.30.96	53		2.5 IPS	
10/3/06 4:39:...	2143: LPR: L...	Vulnerabilities	Block	10.0.30.91	59850	10.0.30.92	515		2.5 IPS	
10/3/06 4:39:...	1450: MS-RP...	Vulnerabilities	Block	10.0.30.93	51477	10.0.30.94	135		2.5 IPS	
10/3/06 4:39:...	2143: LPR: L...	Vulnerabilities	Block	10.0.30.89	59854	10.0.30.90	515		2.5 IPS	
10/3/06 4:39:...	0588: DNS: I...	Exploits	Block	10.0.30.87	57787	10.0.30.88	53		2.5 IPS	
10/3/06 4:39:...	0238: HTTP: ...	Exploits	Block	10.0.30.81	2095	10.0.30.83	80		2.5 IPS	
10/3/06 4:39:...	0657: FTP: ...	Exploits	Block	10.0.30.79	39182	10.0.30.80	21		2.5 IPS	

CAPITULO V

EVALUACIÓN DEL SISTEMA

5.1 PRUEBAS DE LA RED LAN

Tras la implementación del sistema, se ha recogido la topología de la red mediande un software de administración de redes llamado *3Com Network Director,* la red de la Universidad Cotopaxi queda de la siguiente manera:

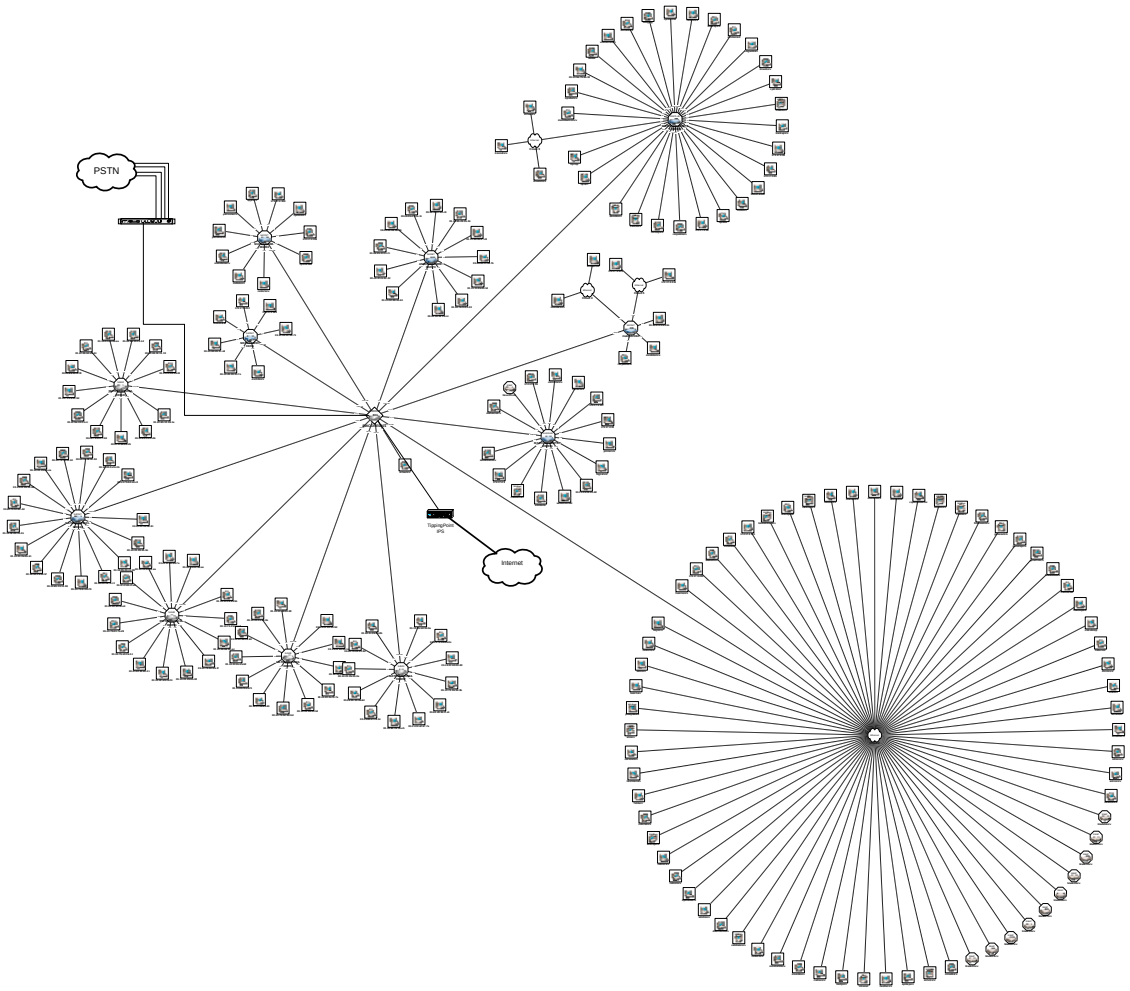


Figura 5.1: Red de la Universidad Cotopaxi.

El sistema Core está compuesto por 2 switches 5500G en XRN, cada uno tiene colocado 12 enlaces con link aggregation a switches y un enlace simple a 1Gbps. Lo primero que debemos probar es que el funcionamiento de DLA funcione correctamente, para ello utilizamos el programa de administración 3Com Network Director para comprobar que cada uno de los enlaces de *Link Aggregation* funcione correctamente y estén activos logrando balanceo de carga:

ANEXO C: Comprobación de cada uno de los enlaces 802.3ad:

Una vez que hemos comprobado que los *Link Aggregation* funcionan correctamente, debemos cerciorarnos que las VLANS también lo hagan, para ello se usará un computador que será movido a distintas VLANS y se probarán las aplicaciones de los servidores y de un servidor que será colocado en distintas VLANS. En la figura 5.2 mostrada a continuación, se muestran los 2 switches que conforman el CORE, los puertos 1/0/21, 1/0/22 y 2/0/22 son conectados a un *blade* de servidores (es un solo equipo con muchos servidores internos) por lo tanto es un link aggregation de 3 enlaces, aquí están todas las aplicaciones importantes de la universidad por lo tanto debe existir conectividad desde todas las VLANS. Se han graficado 2 de los switches conectados con Link Aggregation hacia el sistema de CORE y su utilizan 2 computadoras que serán utilizados como cliente y como servidor para realizar varias pruebas. Desde la PC de la VLAN 6 se comprobo la respuesta del ping a la direccion 172.17.2.10 (los blades de servidores) y se tiene respuesta, de igual manera todas las aplicaciones funciona de la mejor manera sin ningún conveniente (incluso ante alto tráfico en la red).

Para probar conectividad con todas las VLANS se ejecuta los siguientes comandos en el puerto del switch 4500 donde está conectado el PC:

[4500]VLAN 2

[4500-VLAN2]port ethernet 1/0/10

Coloca el puerto en la VLAN 2

El PC se pone en símbolo del sistema (CMD):

Ipconfig /release

Ipconfig /renew

Esos comandos hacen que el PC libere la dirección IP y la pida nuevamente al servidor DHCP, como ahora el PC se encuentra en la VLAN 2, el servidor DHCP, a través del DHCP RELAY del switch (configuración que hace que el switch le indique al servidor el rango de direcciones que le debe dar al PC) le otorga la siguiente dirección al PC: 172.16.22.2 y se realizan las mismas pruebas anteriores teniendo éxito nuevamente. Lo mismo se hace para las demás VLANS hasta llegar a la 10 comprobando el funcionamiento correcto del sistema. Con esto confirmamos que a nivel de conectividad, está funcionando el sistema sin problemas.

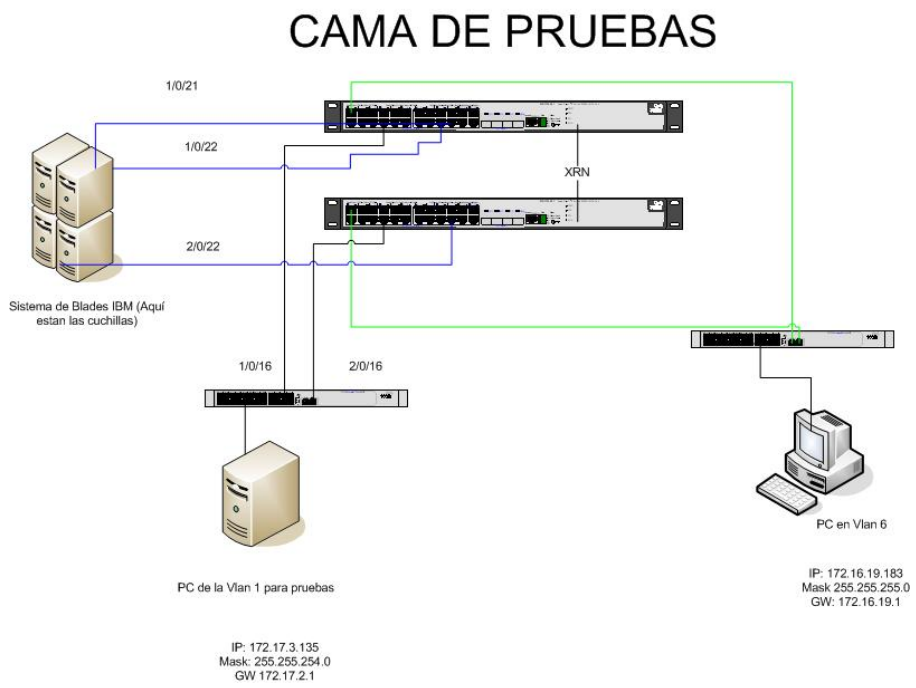


Figura 5.2: Switch de Core de la Universidad Cotopaxi.

Posteriormente se revisa que sucede con respecto a la alta disponibilidad.

Las pruebas que se realizarán serán las siguientes:

1) Hacer reboot de todo el sistema CORE (los 2 switches 5500G) y cronometrar el tiempo en el que se vuelve a tener operativo el sistema
2) Hacer reboot de la unidad 1 y cronometrar los tiempos de reconexión del sistema
3) Hacer reboot de la unidad 2 y cronometrar los tiempos de reconexión del sistema
4) Desconectar el XRN y cronometrar los tiempos de reconexión del sistema
5) Desconectar uno de los enlaces de link aggregation y cronometrar los tiempos de reconexión del sistema

Los resultados se muestran en la siguiente tabla 5.1:

Tabla 5.1. Resultados de las pruebas.

Número de prueba	tiempo Corte por caída (segundos)	tiempo corte por sincronización al levantarse el equipo caído
1	196	15
2	30	15
3	30	15
4	30	15
5	3	0

Luego del monitoreo de 30 días del equipo se recogieron los resultados de latencia, estabilidad, latencia de los servicios, entre otros, en el sistema de blades principal. Con esto comprobamos que la red esté funcionando eficientemente (en las aplicaciones de la red), los resultados se presentan en la siguiente figura 5.3, la misma que presenta un reporte propio del software de administración de 3Com.

3Com® Network Director

Monitoring History Report

This report shows historical graphs for the device "OMNI4760" over time. Gaps in the graphs indicate t is no collected data for that period.

Report created: 30 Mayo de 2007 11:48
Map: cortesupjust

Daily Graphs (5 minute average)
Weekly Graphs (30 minute average)
Monthly Graphs (2 hour average)
Yearly Graphs (1 day average)

Daily Graphs (5 minute average)

DNS Service

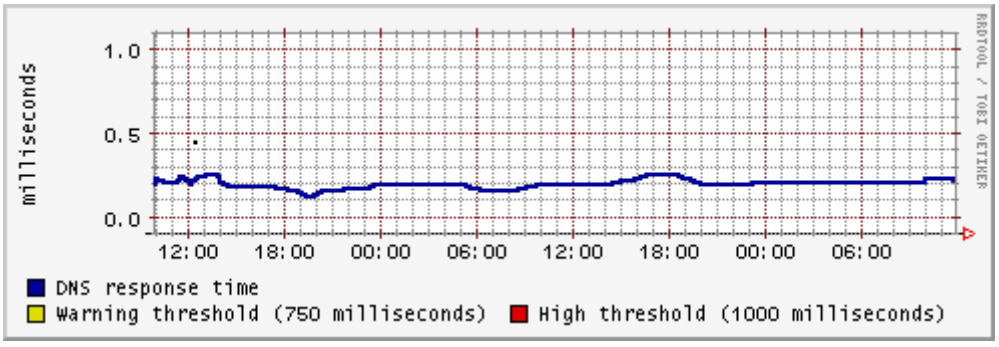


Figura 5.3: Resultado del servicio de DNS.

Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

La figura 5.3 muestra la aplicación DNS, en el dominio del tiempo, esta figura muestra que tiene latencias muy bajas que van entre 0,1 ms hasta 0,3 ms que es la más alta. De esta manera podemos ver que la aplicación del servicio de DNS, esta trabajando de una manera optima.

ANEXO D: Resultado de los servicios con 3Com Network Director.

En resumen, todos los servicios funcionan a velocidad de *wirespeed*. Comprobando que el sistema está funcionando de la manera en la que se esperaba.

Incluso durante unos días se utilizaron DNS externos en lugar de los internos y la latencia bajó considerablemente, demostrando que por medio de la red no se genera latencia, la latencia se genera por medio de las aplicaciones de los servidores.

5.2 PRUEBAS DE SEGURIDAD DE LA RED

Para esta prueba se utiliza el esquema de conectividad mostrado en la figura 5.4, cuyo procedimiento se basa en los siguientes puntos:

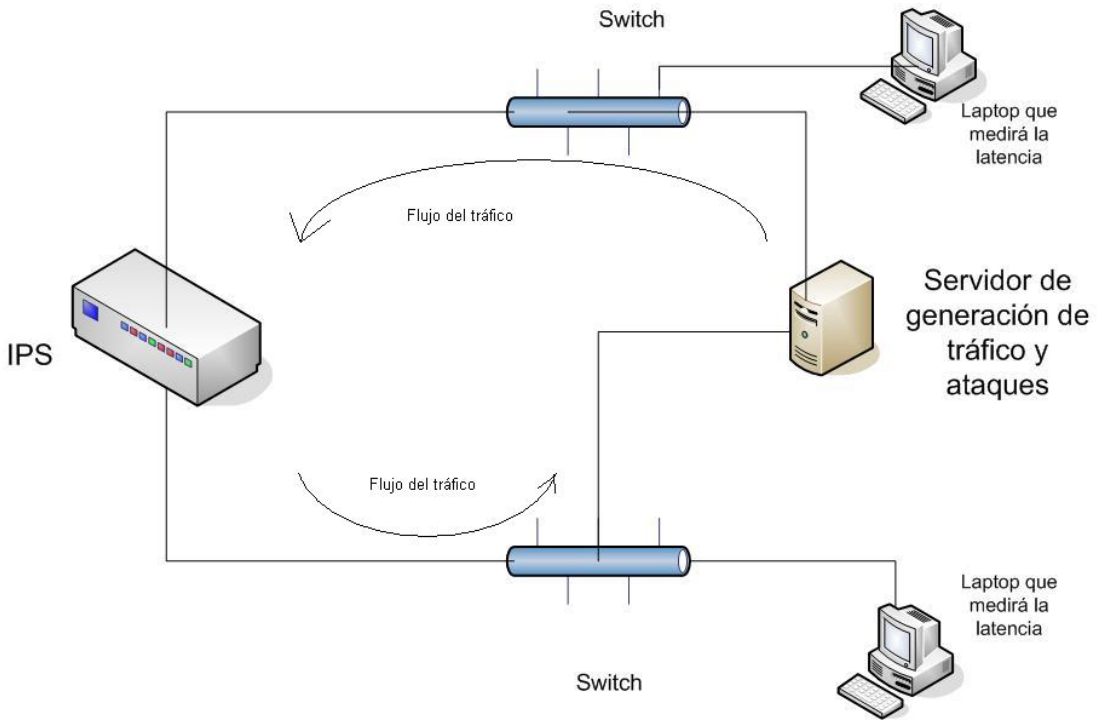


Figura 5.4: Esquema de conectividad para pruebas de seguridad de la Universidad Cotopaxi.

Control de Aplicaciones y tráfico

1. Prueba de control de ancho de banda (rate Limiting) por Puerto y dirección IP

Para esto se implementó una regla de firewall que indica un máximo de ancho de banda de 20Kbps para telefonía y el PcXSet (un softphone utilizado para esta prueba) pudo registrarse en el equipo pero la voz no podía ser transmitida, después se cambió a ancho de banda garantizado de 80Kbps (por el codec G711 utilizado en la prueba) y la voz se podía escuchar claramente y a tiempo real.

2. Prueba de Prueba de control de ancho de banda (rate Limiting) para aplicaciones P2P. Resultado: satisfactorio, se bloqueó emule, y msn de forma satisfactoria como se muestra en la siguiente figura 5.5.

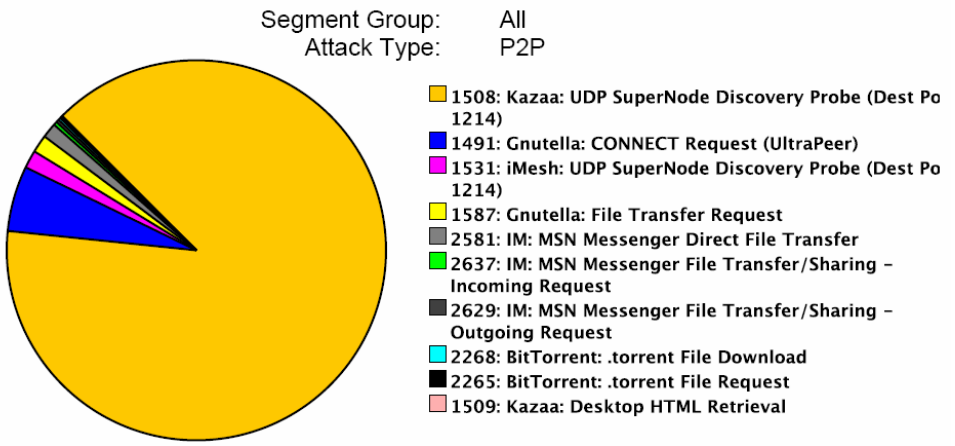


Figura 5.5: Apliacaciones P2P bloqueadas por el TippingPoint

Pruebas de administración y Políticas de Seguridad

1. Verificar que el IPS venga desde la fábrica con una política de protección amplia y precisa, “Recommended Settings”. Verificar que estos “Recommended Settings” tengan por lo menos 950 filtros habilitados en modo block con alertas.

Resultado: Comprobado, en resumen tenemos lo siguiente en la vacuna digital 2.5.074 de https://tmc.tippingpoint.com

Vulnerabilidades (712 filtros)
Exploits (456 filtros)
Políticas de Seguridad (159 filtros)
Reconocimiento (Probes, escaneo de puertos, etc. – 300 filtros)
Informacional (45 filtros)
Equipamiento de Red (60 filtros)
Normalización de Tráfico (37 filtros)

2. Crear una nueva política de seguridad y distribuirla en línea mientras que el IPS este en modo de protección.

a. Monitorear el CPU del equipo y verificar latencia durante la distribución.

El comando en el IPS para ello es: show np tier-stats

El uso no sobrepasa el 20% (11% cuando no hay carga)

b. Verificar la latencia durante este proceso.

No fue afectada la latecia, el ping se mantiene constante, como lo muesra la figura 5.6.

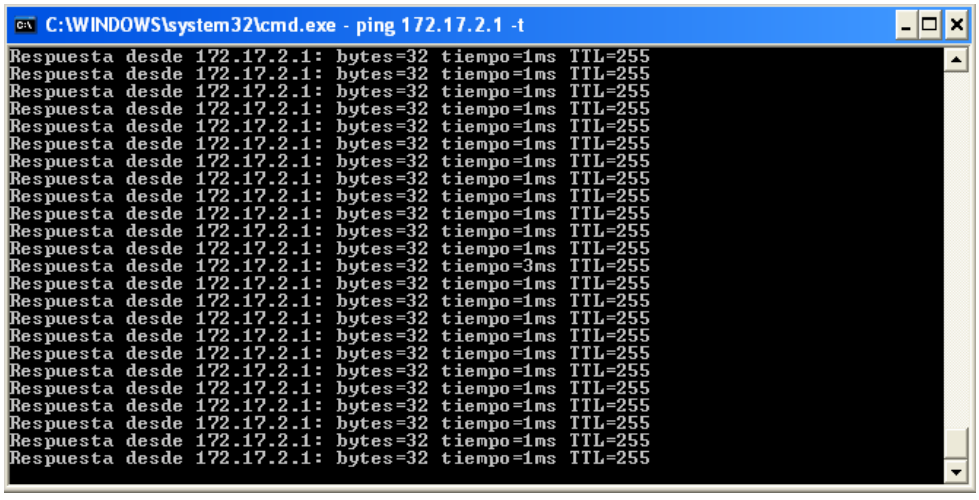


Figura 5.6: Muestra que el ping no es afectado con latencia.

3. Buscar un grupo de filtros por nombre como por ejemplo: Trojans y cambiar la política de seguridad de su default y luego hacer la distribución de estos cambios.

a. Monitorear el CPU del equipo y verificar latencia durante la distribución, como se lo muestra en la figura 5.7.

El gráfico muestra cómo se realizó ese procedimiento.

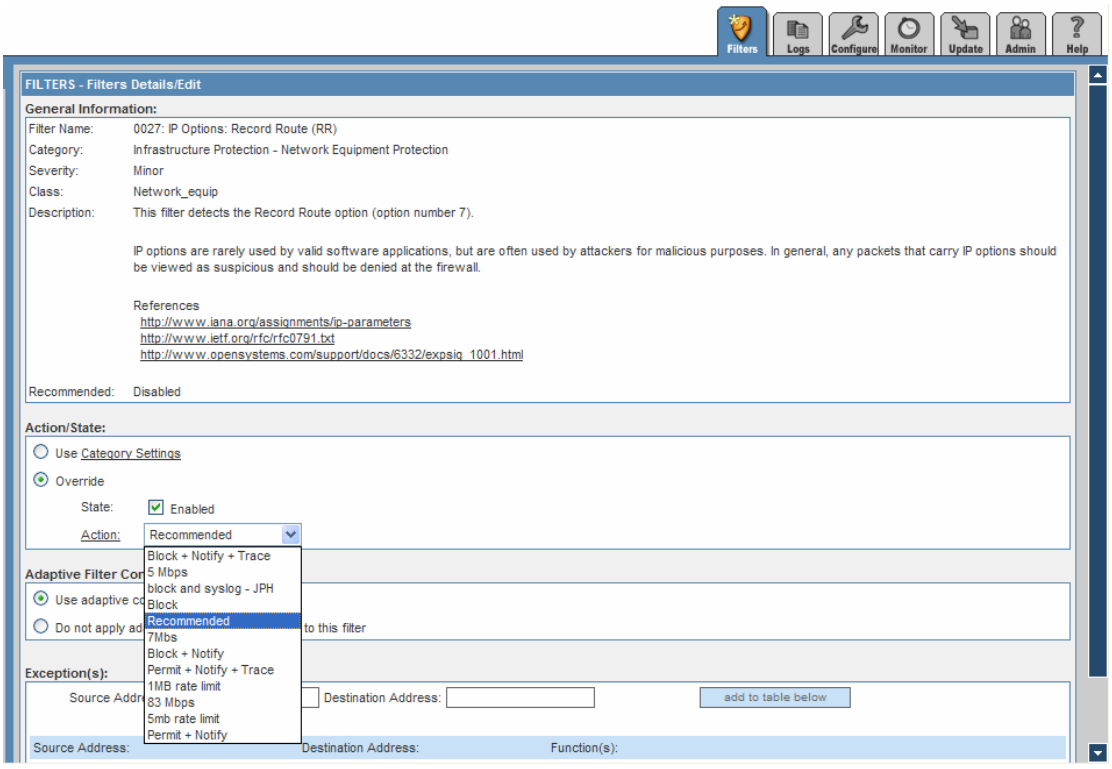


Figura 5.7: Distribución de filtros en el TippingPoint

El uso no sobrepasa el 20% (11% cuando no hay carga)

b. Verificar la latencia durante este proceso

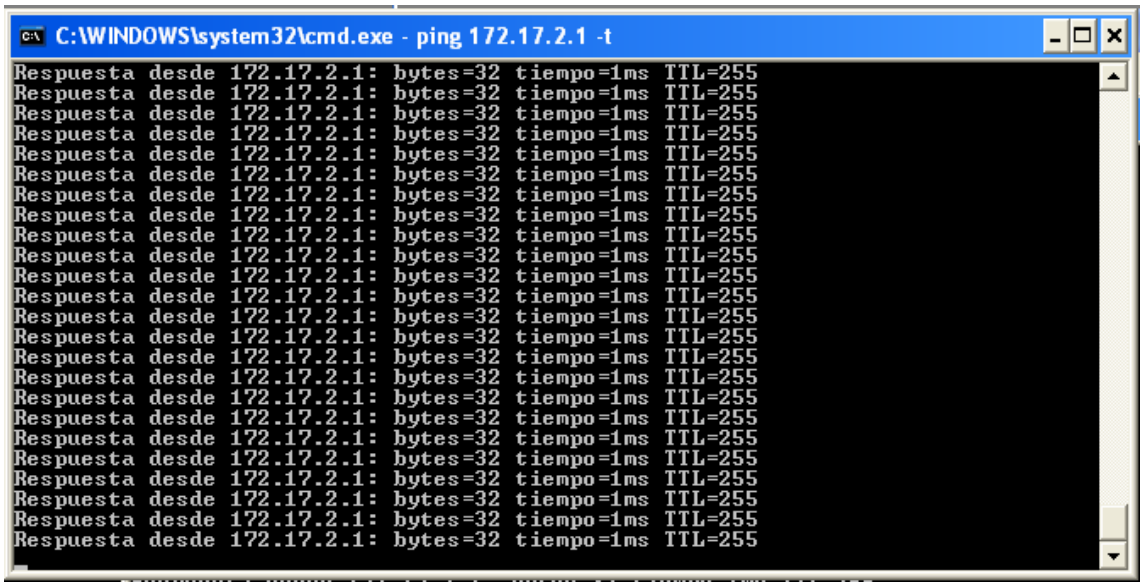


Figura 5.8: Latencia no afectada

5.3 Pruebas de Rendimiento

1. Utilizar el servidor de generación de tráfico y ataques.

Para esto vamos a utilizar un servidor de tráfico llamado Tomahawk. Se anexa el procedimiento exacto de cómo armarlo, instalarlo y configurarlo.

Para medir la latencia utilizamos el ping desde un servidor hasta otro

Av155% ping 172.17.2.200

Generar tráfico http y medir la latencia

av154% perf_http
av155% perf_http

Latencia sin IPS	
Prueba	Tiempo
1	0.311 us
2	0.313 us
3	0.314 us
Promedio	0.31266667 us
Latencia con IPS	
Prueba	Tiempo
1	0.481 us
2	0.443 us
3	0.448 us
Promedio	0.45733333 us
Latencia generada por el IPS	
Prueba	Tiempo
1	0.17 us
2	0.13 us
3	0.134 us
Promedio	0.14466667 us

Como vemos la latencia solo aumentó un 0.15 microsegundos, por lo que el equipo está trabajando a velocidad de wirespeed.

2. Probar latencia del IPS bajo carga de diferente tipo de Tráfico

Vamos a probar con tráfico ftp, el comando en los equipos es perf ftp y los resultados se muestran en el siguiente cuadro:

Prueba	Tiempo promedio
1	4 us
2	4 us
3	4 us
Promedio	4 us
Latencia con IPS	
Prueba	Tiempo
1	6 us
2	6 us
3	5 us
Promedio	5.66666667 us
Latencia generada por el IPS	
prueba	Tiempo
1	2 us
2	2 us
3	1 us
Promedio	1.66666667 us

Ahora, adicionalmente ingresaremos tráfico UDP a la prueba con el comando perf udp. Los resultados se muestran en el siguiente cuadro:

Prueba	Tiempo
1	4 us
2	4 us
3	4 us
Promedio	4 us
Latencia con IPS	
Prueba	Tiempo
1	6 us
2	6 us
3	6 us
Promedio	6 us
Latencia generada por el IPS	
Prueba	Tiempo de diferencia
1	2 us
2	2 us
3	2 us
Promedio	2 us

Sin ataques, el IPS genera latencias no mayores a 2 microsegundos, lo cual es realmente extraordinario (250 veces más rápido que la velocidad mínima para considerar que un equipo que trabaja en línea).

3. Probar el rendimiento y desempeño de las conexiones por segundo que el IPS puede generar en producción y en línea.

Para manejar esta prueba se deben generar los siguientes comandos en uno de los equipos:

av154% cps
time to create 250,000 connections:
real 0m3.268s
user 0m0.040s
sys 0m0.120s

El resultado es la cantidad de tiempo que le tomó al equipo el responder a 250000 conexiones. En este ejemplo, le tomó 3.268 segundos, que corresponde a 250,000/3.268 = 76,500 conexiones por segundo. Se hicieron pruebas de este rendimiento con y sin IPS para medir el número de conexiones por segundo que se pueden obtener con el IPS.

Conexiones por segundo SIN IPS	
Número de conexiones	250,000
Segundos necesarios para realizarlo	7.505
TOTAL conexiones por segundo	**33,311**

Conexiones por segundo SIN IPS	
Número de conexiones	250,000
Segundos necesarios para realizarlo	9.45
TOTAL conexiones por segundo	**26,455**

El equipo soporta entonces 26455 conexiones por segundo (el numero de conexiones por segundo de la universidad para acceso simultaneo de los 1500 usuarios es de 17.64 conexiones por cada usuario).

4. Probar el rendimiento del IPS en línea simulando ataques

Se debe ejecutar el scrip en los servidores: /usr/local/qa/bin/attacks

av154% attacks

Esta prueba posee 32 ataques básicos, sin embargo para hacer la prueba más interesante, vamos a repetir los ataques mil veces con el siguiente comando**:**

av154% attacks 1000

Los resultados de la prueba se muestran en la siguiente tabla 5.2:

Latencia de la red sin IPS estando bajo ataques		
prueba	Tiempo	
1	13,516 s	
2	13,626 s	
3	13,737 s	
Promedio	13,6263333 us	
Latencia de la red con el IPS bajo ataques		
Pass	Average Time	
1	15,769 s	
2	15,723 s	
3	15,44 s	
Total avg	15,734 us	

Número de ataques detenidos	32000
Número de ataques burlados	0
Efectividad 100%	

Con esto se demuestra un 100% de efectividad con latencia no mayor a 2 microsegundos.

De esta manera hemos revisado 2 parámetros importantes del IPS

1) que no genera latencia, eso se comprobó porque el ping entre las 2 laptops conectadas en el esquema no se alteró en más de 1ms al aumentar el tráfico en el servidor generador de tráfico y ataques

2) que no detiene las aplicaciones reales y no deja pasar ataques, en el servidor de ataques tenemos colocados 32 diferentes tipos de ataques y 0 de ellos pasaron a través del IPS.

Tras colocar el IPS en línea, después de 1 mes de producción en la red de la universidad se encontró que se detuvieron los siguientes ataques:

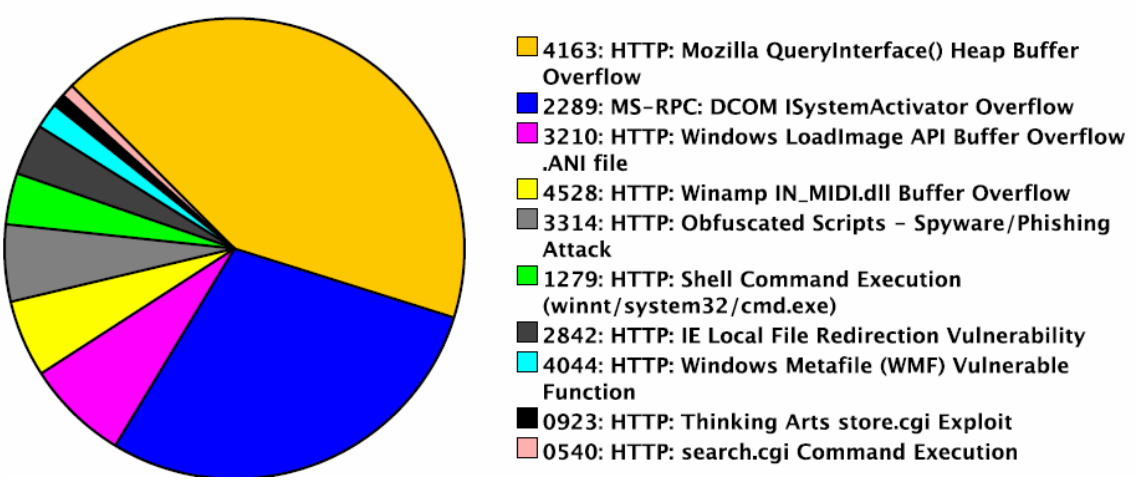


Figura 5.9: Los 10 ataques más críticos.

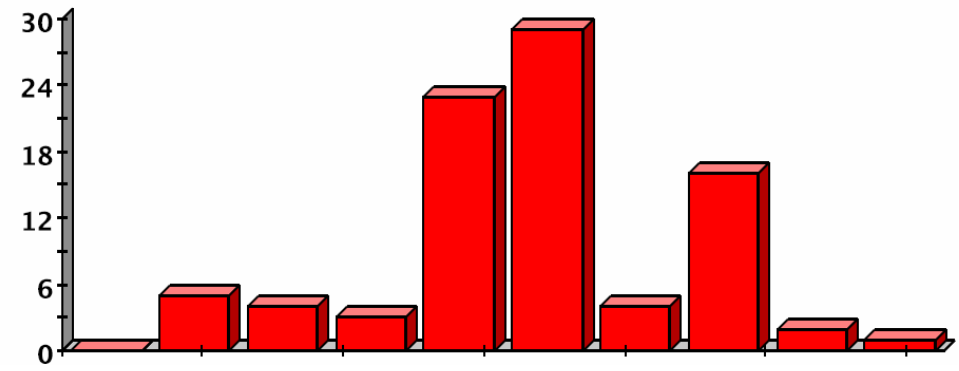


Figura 5.10: Cantidad de ataques críticos diarios.

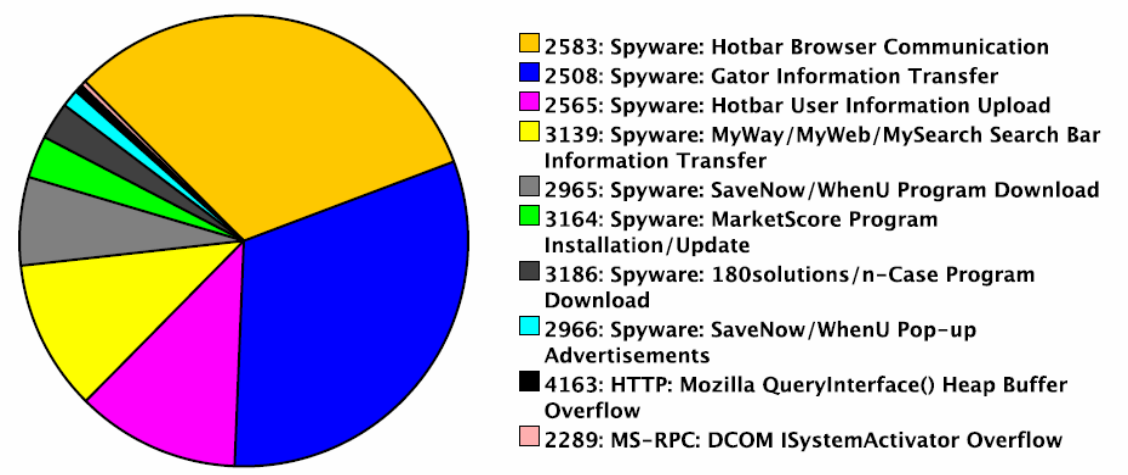


Figura 5.11: 10 ataques más recurrentes en la red.

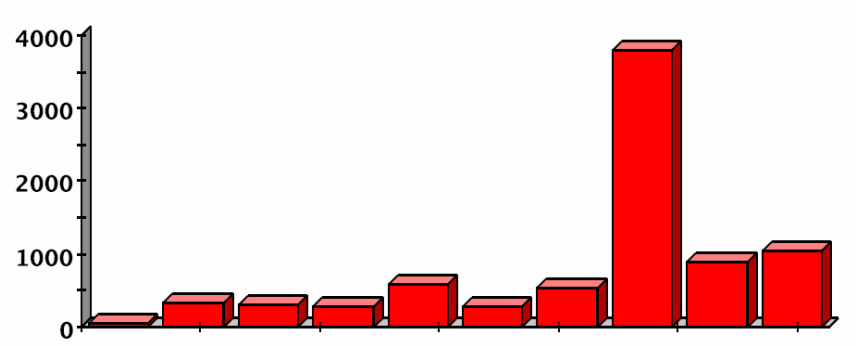


Figura 5.12: Cantidad de ataques diarios.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

- La red de datos es hoy en día pilar fundamental de la operación y funcionamiento de la Universidad Cotopaxi, siendo el vehículo de comunicación por excelencia, además del canal de acceso a todos los recursos de información. Las actuales y extendidas ventajas en materia de ancho de banda, calidad de servicio, alta disponibilidad, seguridad y confiabilidad de las redes de datos han conducido, casi naturalmente, a su convergencia con las de voz.
- El mayor valor de migrar a telefonía IP, para la Universidad Cotopaxi, no reside en los ahorros de costos derivados de la reducción del importe de las facturas telefónicas y de la convergencia de las redes de voz y datos en una única infraestructura. Su mayor potencial se encuentra en que la voz, al convertirse en una aplicación más sobre la red IP, puede ser gestionada como tal e integrarse con otras aplicaciones, dando lugar a nuevas formas de comunicación y colaboración en tiempo real.
- Debido a la convergencia de la Universidad Cotopaxi, aumentamos el número de *hosts*, y esto aumenta la probabilidad de tener colisiones en la red, por lo tanto es necesario trabajar con VLANS (IEEE 802.1Q) debido que a través de VLANS reducimos el dominio de colisiones en la red. Es decir, podemos tener redes gigantes pero si están separadas por VLANS es como si tuviésemos redes muy pequeñas, al disminuir los dominios de colisiones evitamos tiempos de *back-off* y con ello evitamos que se aumente la latencia de la red.
- Es importante configurar QoS en todos los equipos de la red de la Universidad Cotopaxi debido a que provee la habilidad de priorizar tráfico basado en el nivel de servicio requerido. Este nivel de servicio puede ser marcado en la información de cada paquete IP en el campo de Tipo de servicio (TOS).

- Monitoreo: muchas veces es importante redireccionar cierto tipo de tráfico hacia un analizador (sniffer) para descubrir cierta información importante sobre la red (para hacer troubleshooting, auditoría etc.) sin embargo al hacer port mirroring se obtiene a veces demasiada información y es casi imposible encontrar la información buscada. Los switchs poseen la capacidad de hacer ACLs a puertos de mirror (donde se colocará el sniffer) de tal forma que se redirecciona sólo cierto tipo de tráfico para facilitar este estudio. El port mirroring puede ser configurado 1 a 1, varios puertos a 1 e incluso VLAN a 1 o puerto mirror remoto.
- La Telefonía en Redes que utiliza la Universidad Cotopaxi es la tecnología que permite incorporar tráfico de voz sobre redes de datos basadas en paquetes como Ethernet, Frame Relay, IP o ATM, Satisfaciendo sus necesidades al mejorar las comunicaciones y reducir sus costos.
- La telefonía IP de la Universidad Cotopaxi aprovecha la infraestructura existente para Datos, los dispositivos (teléfonos, troncales, etc) son otros elementos de la red de Datos, la voz viaja en forma discreta en unidades de información denominadas paquetes, los cuales utilizan algoritmos de compresión que compensan retrasos, errores y exceso de tráfico en la red a fin de garantizar la calidad del servicio y también ofrece una plataforma abierta para el desarrollo de nuevas aplicaciones.
- Un solo cableado implica para la Universidad Cotopaxi la eliminación del costo del cableado telefónico (US$450 por punto), eliminación del costo del mantenimiento del cableado (US$2000 al año), llamadas de larga distancia por la red con eliminación de costos de larga distancia (US$3000 aprox. año).
- Un solo staff de soporte unificado para la Universidad Cotopaxi, permite que un solo grupo administre y de soporte a las redes de datos/telefonía, con un ahorro de gastos de (US$12000 año) y la administración también puede ser remota.
- Mantenimiento interno permite a la Universidad Cotopaxi, la eliminación de contratos de mantenimiento (US$5000) al año, la eliminación de costos por visita de técnicos (US$150) y la eliminación de requisitos de mantenimiento de usuario (Aumento de la eficiancia del usuario y departamento técnico - No tiene precio).

- La Universidad Cotopaxi tiene la integración con software tradicional como lo es Outlook, Lotus notes, Mensajería Unificada, Call Center.
- Los productos de IPS de la Universidad Cotopaxi, siempre se están renovando para proteger contra vulnerabilidades y ataques cibernéticos más recientes, por medio de Vacunas Digitales que se instalan automáticamente a través de la red**.**
- Las organizaciones saben que mantener los parches apropiados para sus sistemas es una tarea de nunca acabar. En los ambientes de computación móvil ubicua, las computadoras portátiles a veces se contagian de gusanos y virus que se pueden propagar vertiginosamente en una red, infectando a todas las máquinas vulnerables. El IPS de la Universidad Cotopaxi mitiga la necesidad de aplicarle parches a los sistemas al detener ataques en la red con Parches Virtuales de Software, antes de que lleguen a los sistemas vulnerables**.**
- Es necesario proteger el núcleo de la red de la Universidad Cotopaxi, no sólo el perímetro. Los IPS filtran el tráfico malo del Internet, así como de los segmentos internos críticos con infraestructura crítica (routers, switches, servidores de VOIP, servidores DNS, servidores de e-mail, bases de datos) cuya protección siempre debe estar asegurada y cuya disponibilidad debe ser casi un 100%. Según datos del FBI/NIPC, 60% de las violaciones reportadas fueron ataques internos, por lo que es evidente que proteger el interior de su red es tan importante como proteger su perímetro**.**
- El IPS de la Universidad Cotopaxi marca un impacto considerable en el uso de su banda ancha y optimizan la utilización de la red al limpiar tráfico "basura" como runts, giants y otro tráfico que no es válido en la red. Se pueden bloquear o moldear las velocidades de las aplicaciones de uso recreativo, cuya finalidad no está relacionada con los negocios (P2P, IM, Spyware), para readquirir el ancho de banda y fortalecer su puesto de seguridad, al cerrar los canales que se pueden usar para ataques o la propagación de infecciones**.**
- El IPS de© la Universidad Cotopaxi emplea la mejor defensa contra los hackers que lanzan ataques que consisten de paquetes (SYN floods, CPS floods, EST floods) cuyo objetivo es hacer rebosar y sacar de servicio a las aplicaciones más importantes de su red (HTML, bases de datos, e-mail, FTP, DNS, VOIP)**.**

6.2. RECOMENDACIONES

- La solución de voz sobre IP ayuda a los negocios a permanecer en movimiento y a crecer. Con este sistema es posible obtener diversos beneficios, desde el manejo de simples llamadas hasta mensajería unificada, integrada en el mismo sistema; desde la identificación de llamadas hasta la búsqueda en bases de datos al instante (CTI); desde la red del área local (LAN) y la red del área extensa (WAN) hasta el acceso a Internet.
- La administración del sistema es igual de fácil, utilizando el concepto de Web Management de 3Com. Los administradores pueden agregar usuarios nuevos y realizar cambios en todo el sistema —de manera simple y accesible— utilizando un navegador estándar de Web, como *Netscape Navigator* o *Microsoft Internet Explorer*.
- Buscar un sistema de telefonía IP que permita la Automatización del proceso de Negocio a través de *Hunt Groups*, Tratamiento personalizado de llamadas con *AA / Voicemail*, *Suite* para el incremento de productividad: CTI, TAPI dialer, Netset, Contabilidad Financiera con CDR, Distribución Integrada en Atención del cliente – CAS, Ubicador Productivo – Paging / CallPark
- La instalación de un IPS no debe impactar el desempeño de la red cuando se instala.
- El IPS debe contar con características de alta disponibilidad, su uso debe ser transparente para las aplicaciones y los componentes de red que ya existen en el entorno.
- Debe tener herramientas de diagnóstico para facilitar el desempeño del IPS.
- El IPS debe ser reconocido y probado por entidades y laboratorios independientes.
- Su arquitectura y diseño deben ser desde el inicio IPS, no basado en arquitectura IDS.
- Debe contar con varias técnicas y tecnologías de detección.
- Filtros de Vulnerabilidad(no sólo firmas de SNORT).
- Capaz de detectar y parar DOS y DDOS.
- El rendimiento no debe de bajar con la subida de Amenazas.
- El IPS no se debe degradar bajo carga y ataques.

- El sistema de administración del IPS debe ser amigable y poderoso
- Sin “punto único de falla”
- Descarga automática de vacunas digitales.
- El departamento de vacunas digitales debe se reconocido a nivel mundial y efectivo que asegurando protección completa contra los últimos ataques y “exploits”.

ANEXOS

ANEXO A: PROGRAMACIÓN DEL SWITCH 1

```
#
 sysname SWCORE0201
#
 undo password-control aging enable
 undo password-control length enable
 undo password-control history enable
 password-control login-attempt 3 exceed lock-time 120
#
 local-server nas-ip 127.0.0.1 key 3com
#
 dhcp-server 0 ip  172.17.2.143
#
 igmp-snooping enable
#
 link-aggregation group 1 mode manual
 link-aggregation group 2 mode manual
 link-aggregation group 3 mode manual
 link-aggregation group 4 mode manual
 link-aggregation group 5 mode manual
 link-aggregation group 6 mode manual
 link-aggregation group 7 mode manual
 link-aggregation group 8 mode manual
 link-aggregation group 9 mode manual
 link-aggregation group 10 mode manual
 link-aggregation group 11 mode manual
 link-aggregation group 12 mode manual
 link-aggregation group 13 mode manual
#
radius scheme system
#
```

```
domain system
#
local-user admin
 service-type telnet terminal
 level 3
local-user manager
 password simple manager
 service-type telnet terminal
 level 2
local-user monitor
 password simple monitor
 service-type telnet terminal
 level 1
#
acl number 3997
 rule 0 permit ip dscp ef
 rule 1 permit tcp destination-port eq www
 rule 2 permit udp destination-port eq snmp
 rule 3 permit udp destination-port eq snmptrap
 rule 4 permit ip dscp cs6
 rule 5 permit ip dscp cs7
#
acl number 4999
 rule 0 permit type 8868 ffff
 rule 1 permit source 00e0-bb00-0000 ffff-ff00-0000
 rule 2 permit source 0003-6b00-0000 ffff-ff00-0000
 rule 3 permit source 00e0-7500-0000 ffff-ff00-0000
 rule 4 permit source 00d0-1e00-0000 ffff-ff00-0000
 rule 5 permit source 0001-e300-0000 ffff-ff00-0000
 rule 6 permit source 000f-e200-0000 ffff-ff00-0000
 rule 7 permit source 0006-b900-0000 ffff-ff00-0000
 rule 8 deny dest 0000-0000-0000 ffff-ffff-ffff
#
qos-profile default
```

```
 packet-filter inbound link-group 4999 rule 8
 traffic-priority inbound ip-group 3997 rule 0 cos voice
 traffic-priority inbound ip-group 3997 rule 4 cos network-management
 traffic-priority inbound ip-group 3997 rule 5 cos network-management
 traffic-priority inbound link-group 4999 rule 0 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 1 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 2 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 3 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 4 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 5 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 6 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 7 dscp ef cos voice
#
VLAN 1
 igmp-snooping enable
#
VLAN 2
 description Planta Baja
#
VLAN 3
 description 3er. Piso
#
VLAN 4
 description 1er. Piso
#
VLAN 5
 description Mezzanine
#
VLAN 6
 description 2do. Piso
#
VLAN 7
 description Anexo
#
```

```
VLAN 9
 description Red Wireless
#
VLAN 10
 description Red VIP
#
VLAN 11
 description Red VoIP
#
interface VLAN-interface1
 ip address 172.17.2.1 255.255.254.0
#
interface VLAN-interface2
 ip address 172.16.22.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface3
 ip address 172.16.23.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface4
 ip address 172.16.21.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface5
 ip address 172.16.20.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface6
 ip address 172.16.19.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface7
 ip address 172.16.18.1 255.255.255.0
```

```
 dhcp-server 0
#
interface VLAN-interface9
 ip address 10.10.177.1 255.255.255.192
#
interface VLAN-interface10
 ip address 172.16.177.1 255.255.255.128
 dhcp-server 0
#
interface VLAN-interface11
 ip address 192.168.1.1 255.255.255.0
 dhcp-server 0



#LOCCFG. MUST NOT DELETE
#
interface Aux1/0/0
#
interface GigabitEthernet1/0/1
 stp edged-port enable
 port link-type trunk
 port trunk permit VLAN all
 broadcast-suppression pps 3000
 undo jumboframe enable
 port link-aggregation group 3
 apply qos-profile default
#
interface GigabitEthernet1/0/2
 stp edged-port enable
 port link-type trunk
 port trunk permit VLAN all
 broadcast-suppression pps 3000
 undo jumboframe enable
```

```
 port link-aggregation group 9
 apply qos-profile default
#
interface GigabitEthernet1/0/3
 stp edged-port enable
 port link-type trunk
 port trunk permit VLAN all
 broadcast-suppression pps 3000
 undo jumboframe enable
 port link-aggregation group 5
 apply qos-profile default
```

Ejemplo de parte de la configuración de la unidad 2 del sistema de XRN:

```
#
 sysname SWCORE0201
#
 undo password-control aging enable
 undo password-control length enable
 undo password-control history enable
 password-control login-attempt 3 exceed lock-time 120
#
 local-server nas-ip 127.0.0.1 key 3com
#
 dhcp-server 0 ip  172.17.2.143
#
 igmp-snooping enable
#
 link-aggregation group 1 mode manual
 link-aggregation group 2 mode manual
 link-aggregation group 3 mode manual
 link-aggregation group 4 mode manual
```

```
 link-aggregation group 5 mode manual
 link-aggregation group 6 mode manual
 link-aggregation group 7 mode manual
 link-aggregation group 8 mode manual
 link-aggregation group 9 mode manual
 link-aggregation group 10 mode manual
 link-aggregation group 11 mode manual
 link-aggregation group 12 mode manual
 link-aggregation group 13 mode manual
#
radius scheme system
#
domain system
#
local-user admin
 service-type telnet terminal
 level 3
local-user manager
 password simple manager
 service-type telnet terminal
 level 2
local-user monitor
 password simple monitor
 service-type telnet terminal
 level 1
#
acl number 3997
 rule 0 permit ip dscp ef
 rule 1 permit tcp destination-port eq www
 rule 2 permit udp destination-port eq snmp
 rule 3 permit udp destination-port eq snmptrap
 rule 4 permit ip dscp cs6
 rule 5 permit ip dscp cs7
#
```

```
acl number 4999
 rule 0 permit type 8868 ffff
 rule 1 permit source 00e0-bb00-0000 ffff-ff00-0000
 rule 2 permit source 0003-6b00-0000 ffff-ff00-0000
 rule 3 permit source 00e0-7500-0000 ffff-ff00-0000
 rule 4 permit source 00d0-1e00-0000 ffff-ff00-0000
 rule 5 permit source 0001-e300-0000 ffff-ff00-0000
 rule 6 permit source 000f-e200-0000 ffff-ff00-0000
 rule 7 permit source 0006-b900-0000 ffff-ff00-0000
 rule 8 deny dest 0000-0000-0000 ffff-ffff-ffff
#
qos-profile default
 packet-filter inbound link-group 4999 rule 8
 traffic-priority inbound ip-group 3997 rule 0 cos voice
 traffic-priority inbound ip-group 3997 rule 4 cos network-management
 traffic-priority inbound ip-group 3997 rule 5 cos network-management
 traffic-priority inbound link-group 4999 rule 0 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 1 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 2 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 3 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 4 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 5 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 6 dscp ef cos voice
 traffic-priority inbound link-group 4999 rule 7 dscp ef cos voice
#
VLAN 1
 igmp-snooping enable
#
VLAN 2
 description Planta Baja
#
VLAN 3
 description 3er. Piso
#
```

```
VLAN 4
 description 1er. Piso
#
VLAN 5
 description Mezzanine
#
VLAN 6
 description 2do. Piso
#
VLAN 7
 description Anexo
#
VLAN 9
 description Red Wireless
#
VLAN 10
 description Red VIP
#
interface VLAN-interface1
 ip address 172.17.2.1 255.255.254.0
#
interface VLAN-interface2
 ip address 172.16.22.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface3
 ip address 172.16.23.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface4
 ip address 172.16.21.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface5
```

```
 ip address 172.16.20.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface6
 ip address 172.16.19.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface7
 ip address 172.16.18.1 255.255.255.0
 dhcp-server 0
#
interface VLAN-interface9
 ip address 10.10.177.1 255.255.255.192
#
interface VLAN-interface10
 ip address 172.16.177.1 255.255.255.128
 dhcp-server 0
#LOCCFG. MUST NOT DELETE

#
interface Aux2/0/0
#
interface GigabitEthernet2/0/1
 stp edged-port enable
 port link-type trunk
 port trunk permit VLAN all
 broadcast-suppression pps 3000
 undo jumboframe enable
 port link-aggregation group 3
 apply qos-profile default
#
interface GigabitEthernet2/0/2
 stp edged-port enable
 port link-type trunk
```

```
 port trunk permit VLAN all
 broadcast-suppression pps 3000
 undo jumboframe enable
 port link-aggregation group 9
 apply qos-profile default
#
interface GigabitEthernet2/0/3
 stp edged-port enable
 port link-type trunk
 port trunk permit VLAN all
 broadcast-suppression pps 3000
 undo jumboframe enable
 port link-aggregation group 5
 apply qos-profile default
```

ANEXO B: PROGRAMACIÓN DE LA CENTRAL TELEFÓNICA

```
////////////////////////////////////////////////////////////////////////////
/
/ Archivo de configuración de plan de disco de marcar de NBX
/ Generar de V3000 192.168.1.190  de máquina por apreciado cliente 0
/ Generó 07 11:12 el martes feb.:18 2007
/
////////////////////////////////////////////////////////////////////////////
```

Al revisar la siguiente sección del plan de marcación de la NBX, el propósito es borrar la configuración del sistema durante el reinicio de carga de la información del plan de marcación.

```
/ Primero, elimine toda información del dialplan existente
Eliminar tabla *
Eliminar Ruta de destino *
Eliminar rutas temporizadas *
Eliminar PreTranslator *
/ Creamos toda la información del dialplan
```

El plan de marcación consta de 4 dígitos, y a continuación se muestra el rango de extenciones para los diferentes tipos de aplicaciones.

//

/ Ajustes. Nota: los rangos de ACD incluyeron la categoría en HuntGroup.

//

Longitud de la extensión	4
Rango de extensiones de los teléfonos	1000 1999
Rango de extensiones de parqueo	6000 6199
Rango de extensiones de la atendedora automática	5000 5999
Rango de extensiones de *HuntGroup*	4000 4999
Rango de extensiones externas	6000 7999

//

/ La configuración del rango de extensiones externa debe incluir el rango /de extensiones de parqueo.

/ Si el rango de parqueo de llamadas esta fuera del rango de parqueo de /las extensiones externas, la funcionalidad de parqueo de llamadas no /funcionará.

//

//

/ Tablas del plan de marcación

//

La tabla 1 controla llamadas que realiza la NBX. La tabla 2 controla las llamadas entrantes a la NBX. Tabla 3 es la ruta de menor costo.

Información de la tabla 1. El ID de la columna demuestra todo 1s, es decir representa a la primera tabla. Note que la segunda columna de entrada está en orden secuencial y sirve para representar los diferentes tipos de entradas de dígitos de marcación. La columna de dígitos especifica el número exacto que se va a ingresar en el teléfono, cuando se va a realizar una marcación. El mínimo y máximo se refiere al número de los dígitos que el sistema espera recibir cuando un usuario realiza una llamada. La clase es una descripción fija que admitirá o negará la marcación basado en la clase de servicio el usuario. La columna de prioridad no es usada. La ruta especifica que ruta tomará el número marcado. Las rutas tienen su propia sección en el plan de marcación.

Tabla 1 crea extensions internas de 4 dígitos

```
/               Id Entry  Digits      Min Max Class         Prio Route
/               -- -----  ----------- --- --- ------------  ---- -----
TableEntry Create  1     1  0           1   1 Internal        0     4
TableEntry Create  1     2  1           4   4 Internal        0     0
TableEntry Create  1     3  2           4   4 Internal        0     0
TableEntry Create  1     4  3           4   4 Internal        0     0
TableEntry Create  1     5  4           4   4 Internal        0     0
TableEntry Create  1     6  5           4   4 Internal        0     3
TableEntry Create  1     8  6           4   4 Internal        0     0
TableEntry Create  1     9  7           4   4 Diagnostics     0     0
TableEntry Create  1    10  9           8   8 Local           0     1
TableEntry Create  1    11  90          2  64 Operator        0     1
TableEntry Create  1    12  901         4  64 International   0     1
TableEntry Create  1    13  91          9  12 International   0     1
```

La información de la tabla 2. La columna de identificación demuestra todo 2s, esto significa que estamos manejando la tabla 2. La columna de entrada está en orden secuencial que sirve para diferencial los diferentes tipos de llamadas entrantes. La columna de dígitos especifica el número exacto que está siendo presentado. El mínimo y máximo se refiere al número de dígitos que el sistema debe esperar recibir para una cadena de números antes de tomar una acción. La clase de servicio es una descripción fija que admitirá o negará la marcación de un número en el teléfono basado en la configuración de la clase de servicio. La prioridad no es usada. La ruta especifica que ruta tomará el número marcado. Por lo general no se recomienda cambiar la configuración de la tabla 2, es preferible dejarla como viene por defecto.

Tabla 2 llamadas entrantes y Atendedora Automática.

```
/               Id Entry  Digits      Min Max Class         Prio Route
/               -- -----  ----------- --- --- ------------  ---- -----
TableEntry Create  2     1  0           1   1 Internal        0     4
TableEntry Create  2     2  1           4   4 Internal        0     0
```

```
TableEntry Create   2     3  2          4   4 Internal        0     0
TableEntry Create   2     4  3          4   4 Internal        0     0
TableEntry Create   2     5  4          4   4 Internal        0     0
TableEntry Create   2     6  5          4   4 Internal        0     3
```

LA ruta de menor costo no es requerido para la mayoría de los clientes. Cuando LCR es usado el tráfico hacia afuera pasa primero por la tabla 1. La tabla LCR maneja el tráfico cuando es aplicable. Por lo demás, el tráfico es manejado por otras tabla (Tabla 1 o Tabla 2 por defecto)

La tabla 3 crea rutas de menor costo

En la sección de rutas, se tiene tres partes principales; la descripción de ruta, las entradas para una ruta, las operaciones ha ser ejecutadas.. Ejemplo; la ruta de destino creada 1. El campo de descripción es completamente personalizable para ayudarlo identificar la ruta. Usted verá una o más entradas para cada ruta. La entrada de ruta destino crea la ruta 1, la entrada 1 y la extensión destino. Para terminar, las operaciones o las modificaciones del plan de marcación antes que un número sea enviado como un ejemplo, la PSTN. La operación de ruta de destino, crea la ruta con la entrada 1 y operación con la identificación 1, y la operación que puede ser (añadir, anteponer, quitar y reemplazar) y el número de los dígitos para la acción.
La operación que se ejecuta es crear una ruta de destino creada, como se lo muestra a continuación.

```
////////////////////////////////////////////////////////////////////////////
/       Routes
////////////////////////////////////////////////////////////////////////////

/                   Route Description
/                   ----- -----------
DestinationRoute Create     1 LocalCO
DestinationRoute Create     2 LocalCONoStrip
DestinationRoute Create     3 Voice Application
DestinationRoute Create     4 Attendant
DestinationRoute Create     5 H323 ConneXtions Ports
```

DestinationRoute Create 8 8 Pool

Luego se escoge una entrada en la ruta de destino, los cuales son lineas de extensiones que tienen asociados las líneas análogas..

```
/                    Route Entry DestinationExtension
/                    ----- ----- --------------------
DestinationRouteEntry Create   1    1 *0001
DestinationRouteEntry Create   1    2 *0002
DestinationRouteEntry Create   2    1 *0001
DestinationRouteEntry Create   2    2 *0002
DestinationRouteEntry Create   3    1 *0003
DestinationRouteEntry Create   4    1 *0004
DestinationRouteEntry Create   5    1 *0005
DestinationRouteEntry Create   8    1 *0008
```

Luego elegimos la operación que se va a realizar con la llamada discada, por ejemplo en la ruta 1 que esta asociada a una llamada local, el usuario ingresa 9 para poder llamar a cualquier número de la red PSTN, pero el número 9 que marca el usuario no debe salir en la llamada, por lo que se escoge la opción de stripLead 1 (quitar 1), con esta operación eliminamos el número 9 en una llamada hacia la red pública conmutada, y de esta manera terminamos con la configuración del plan de marcación .

```
/                      Route Entry OperId Operation  Value
/                      ----- ----- ------ ---------  -----
DestinationRouteOperation Create   1    1     1 stripLead  1
DestinationRouteOperation Create   1    2     1 stripLead  1
DestinationRouteOperation Create   8    1     1 stripLead  1
```

/ End of configuration

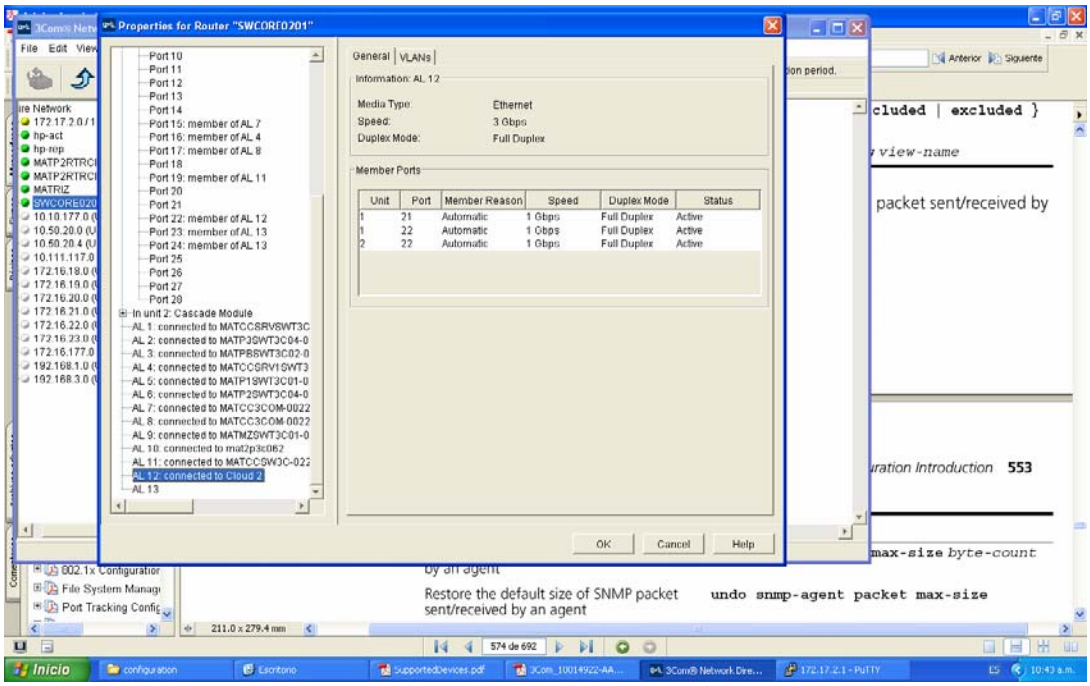
```
/       10. szExtension *0001 is the default Line Card Port extension list
/       11. szExtension *0002 is the default T1 extension list
/       12. szExtension *0003 is the default Voicemail extension list
/       13. szExtension *0004 is the default Attendant extension list
/          (The lowest telephone extension that is Auto-discovered will
```

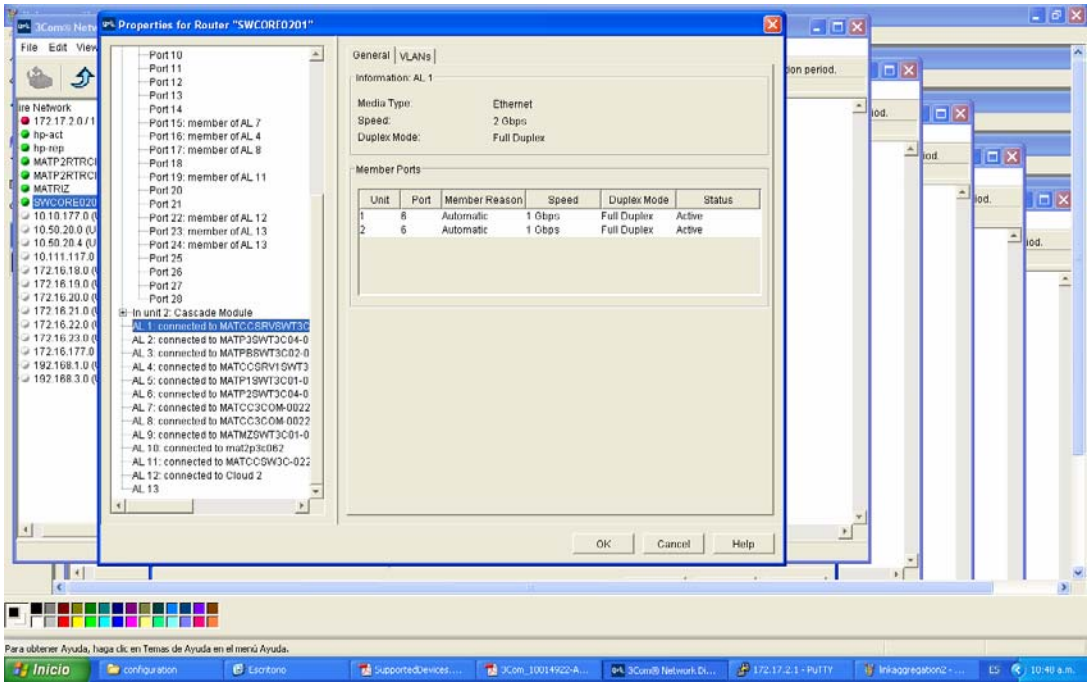
/ populate)

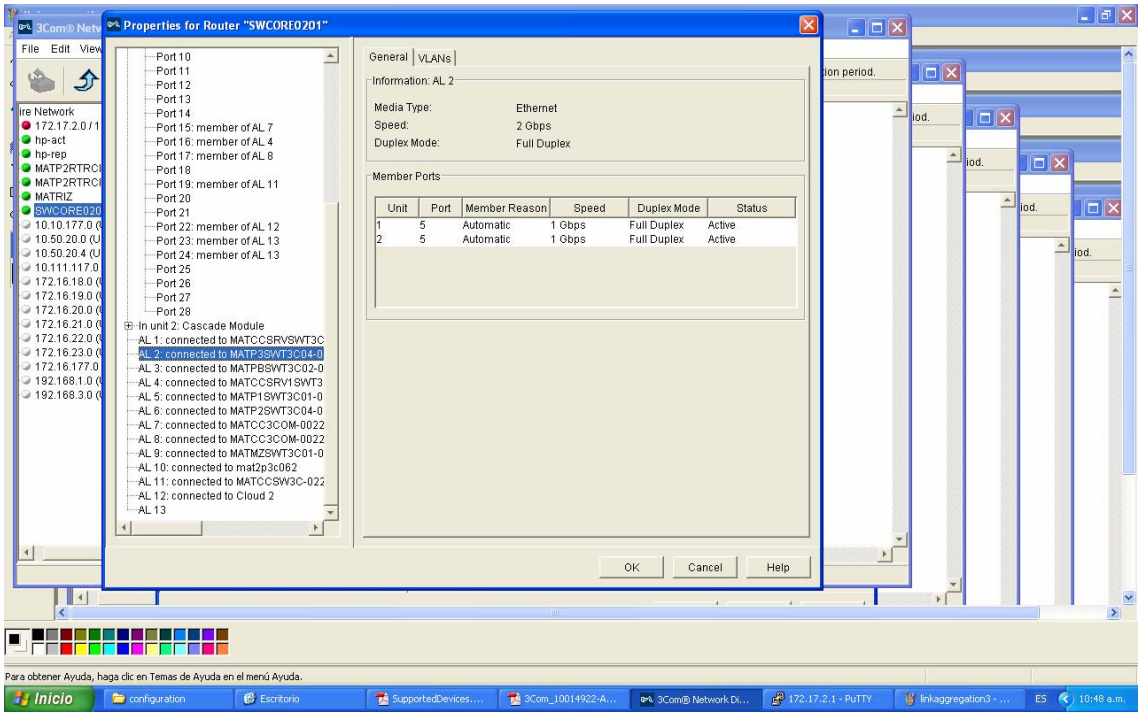
/ 14. szExtension *0005 is the default H323 extension list

/ 15. szExtension *0008 is the default 8 Pool extension list

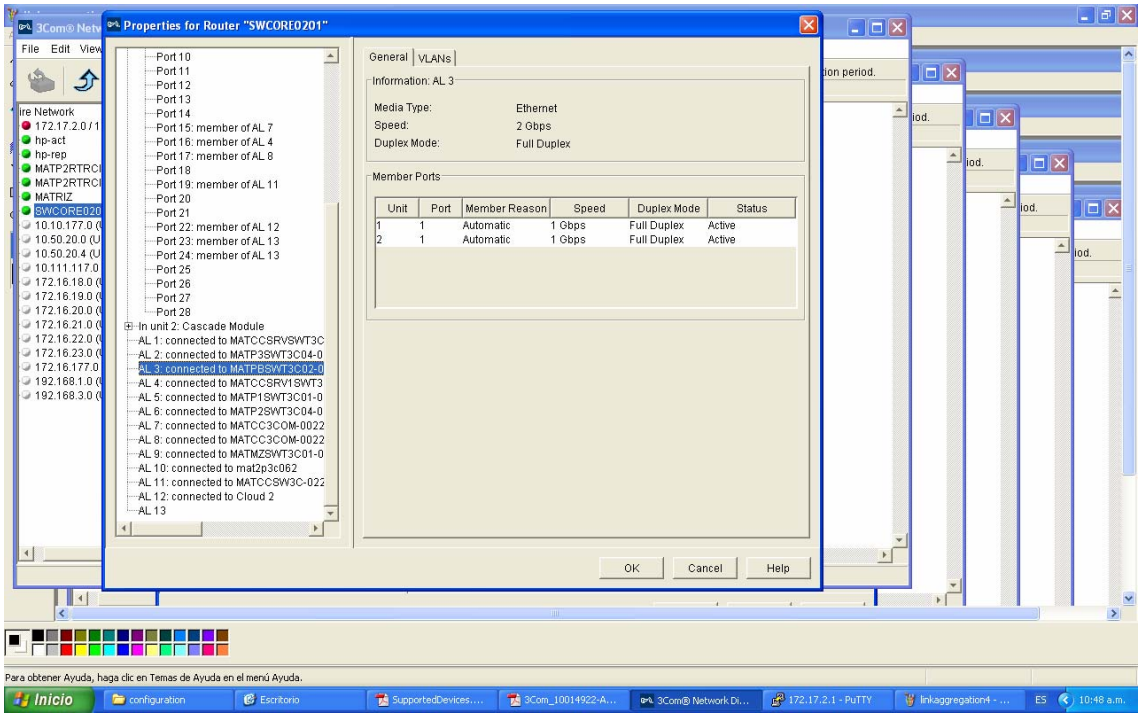
ANEXO C: COMPROBACIÓN DE CADA UNO DE LOS ENLACES 802.3AD

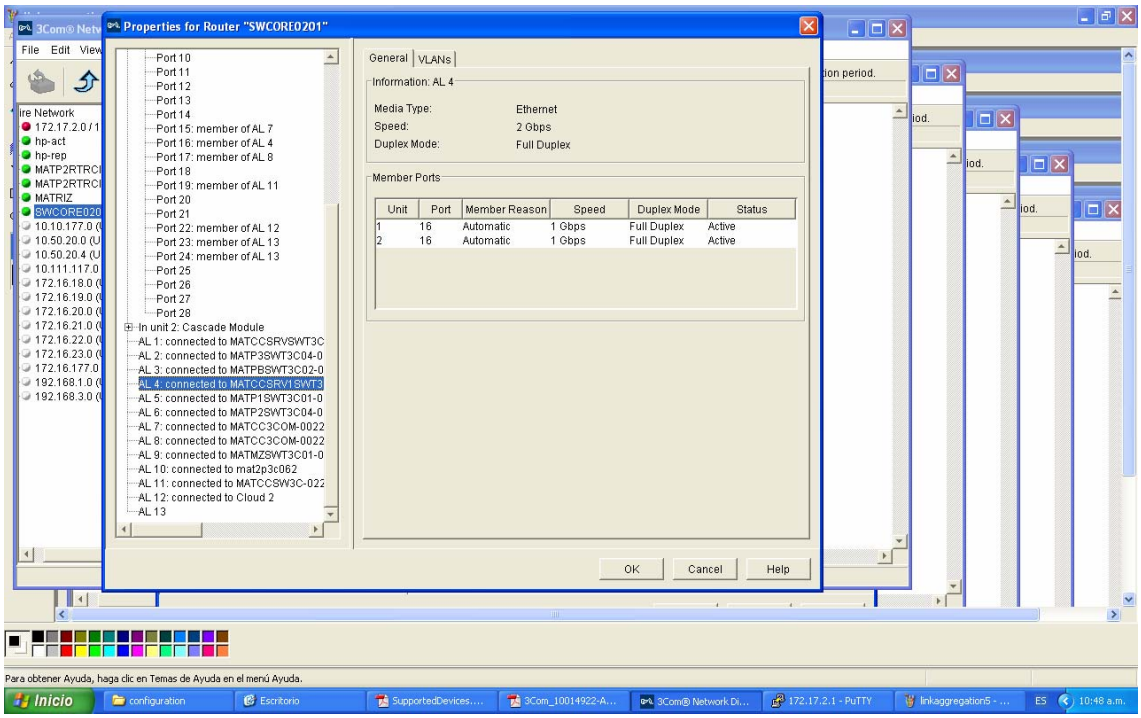


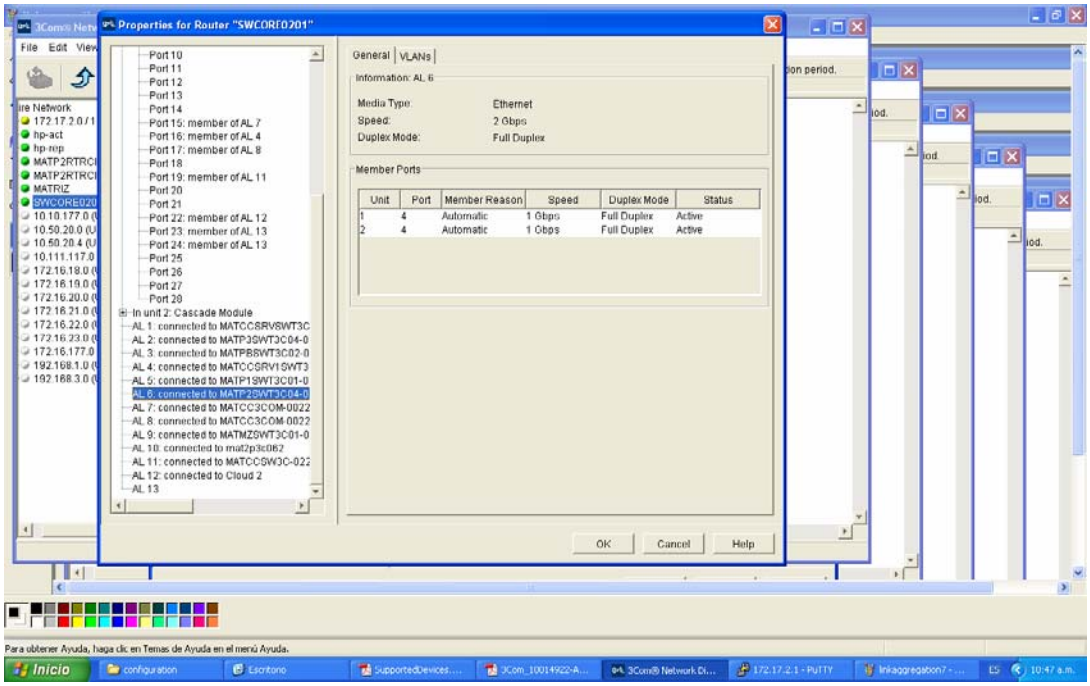

Properties for Router "SWCORE0201"
General
VLANs
Information: AL 1
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 6 Automatic 1 Gbps Full Duplex Active
2 6 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation2 - ...
10:40 a.m.

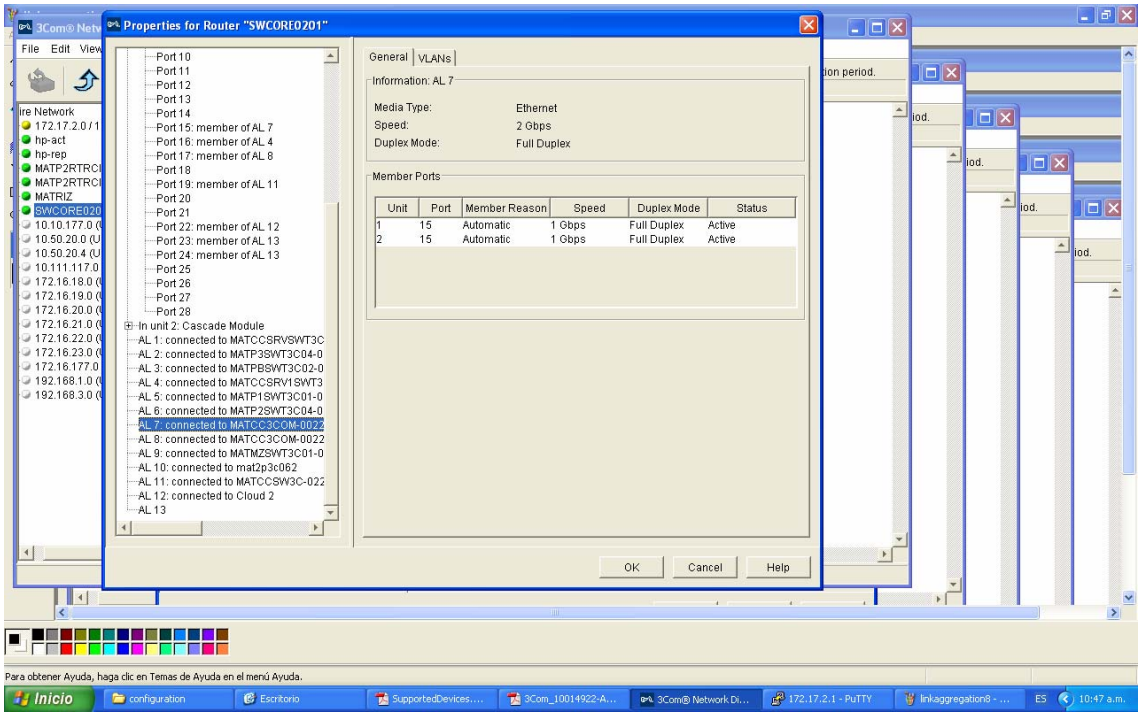

Properties for Router "SWCORE0201"
General
VLANs
Information: AL 2
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 5 Automatic 1 Gbps Full Duplex Active
2 5 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation3 - ...
10:48 a.m.

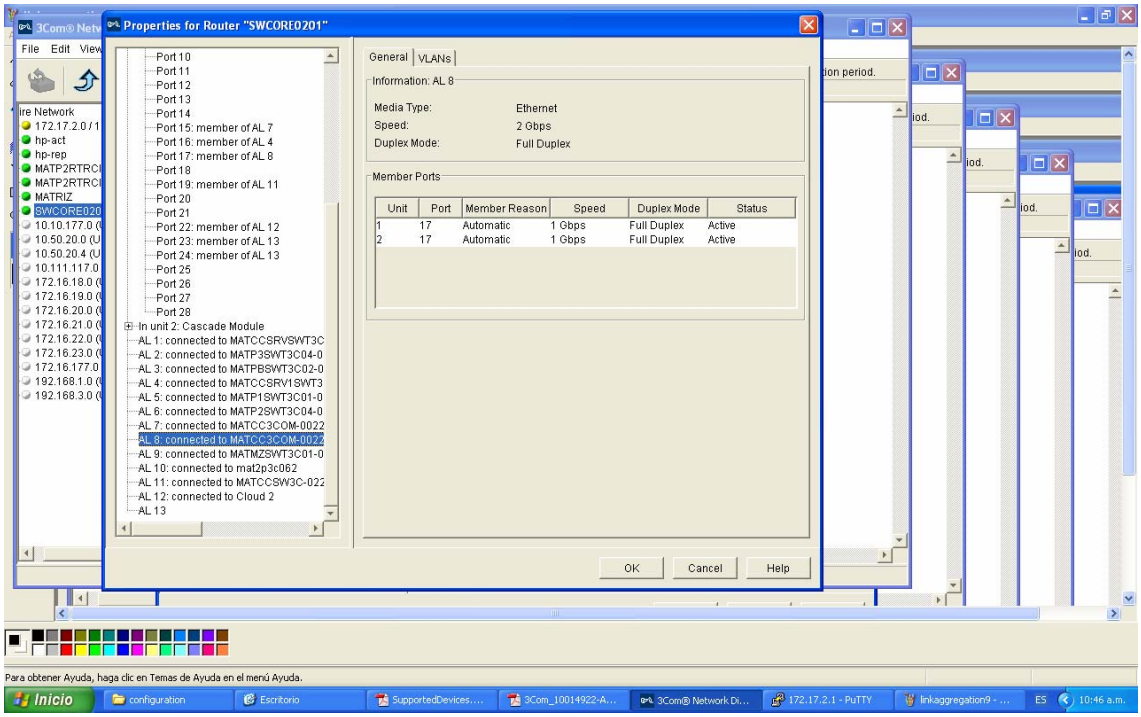
}

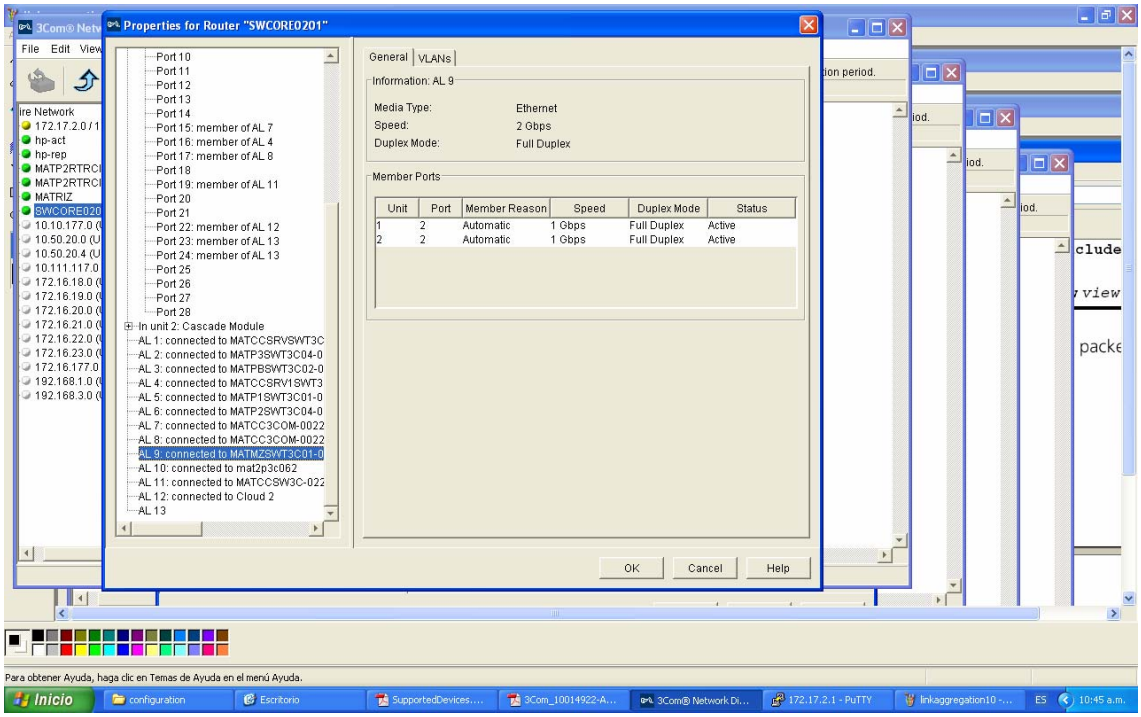

Properties for Router "SWCORE0201"
General
VLANs
Information: AL 3
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 1 Automatic 1 Gbps Full Duplex Active
2 1 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation4 - ...
ES
10:48 a.m.

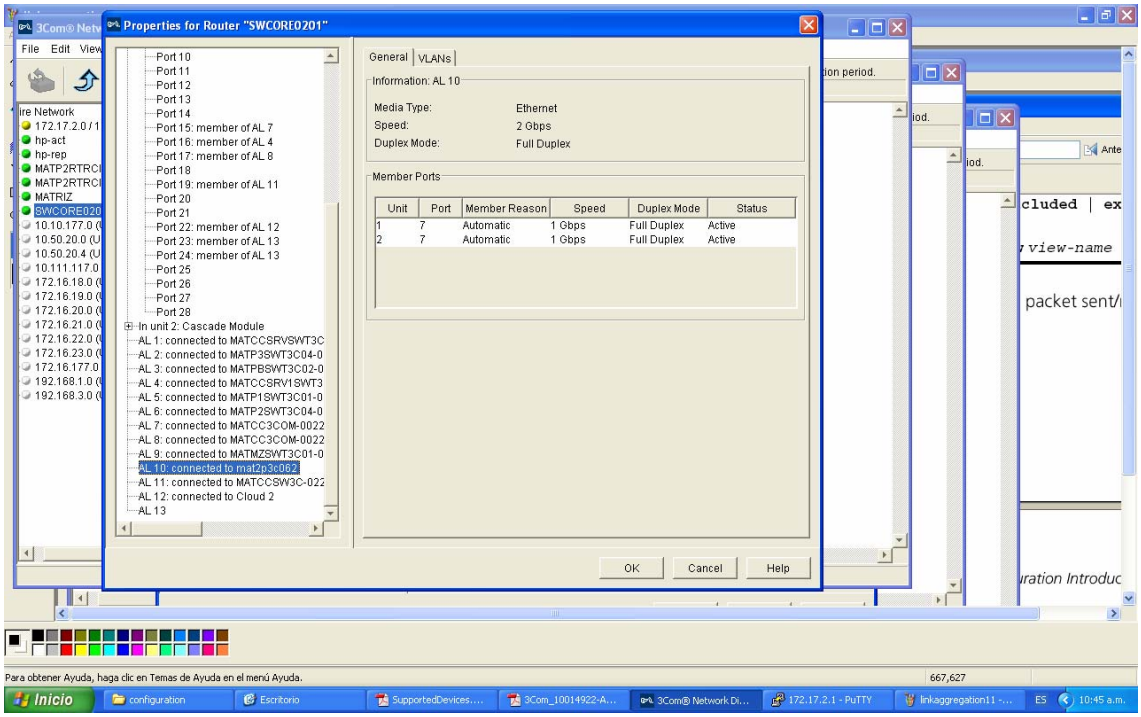

Properties for Router "SWCORE0201"
General
VLANs
Information: AL 4
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 16 Automatic 1 Gbps Full Duplex Active
2 16 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation5 - ...
ES
10:48 a.m.

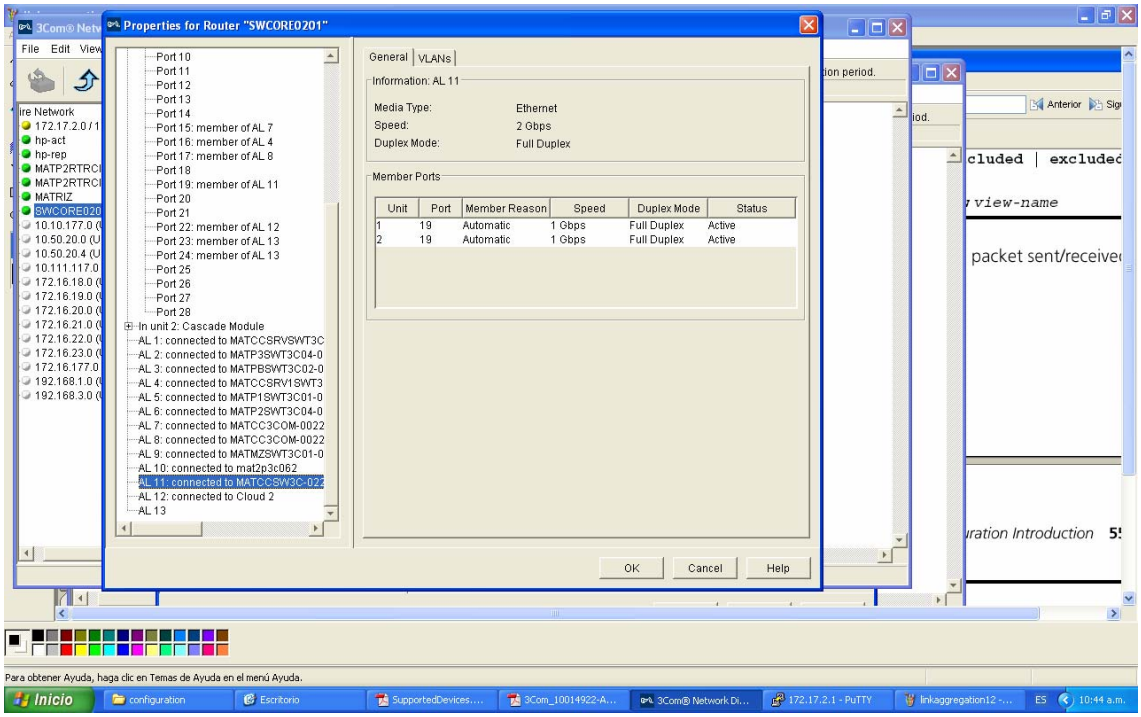

Properties for Router "SWCORE0201"
General
VLANs
Information: AL 6
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 4 Automatic 1 Gbps Full Duplex Active
2 4 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation7 - ...
ES
10:47 a.m.


Properties for Router "SWCORE0201"
General
VLANs
Information: AL 7
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 15 Automatic 1 Gbps Full Duplex Active
2 15 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation8 - ...
ES
10:47 a.m.


Properties for Router "SWCORE0201"
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
General
VLANs
Information: AL 8
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 17 Automatic 1 Gbps Full Duplex Active
2 17 Automatic 1 Gbps Full Duplex Active
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation9 - ...
ES
10:46 a.m.

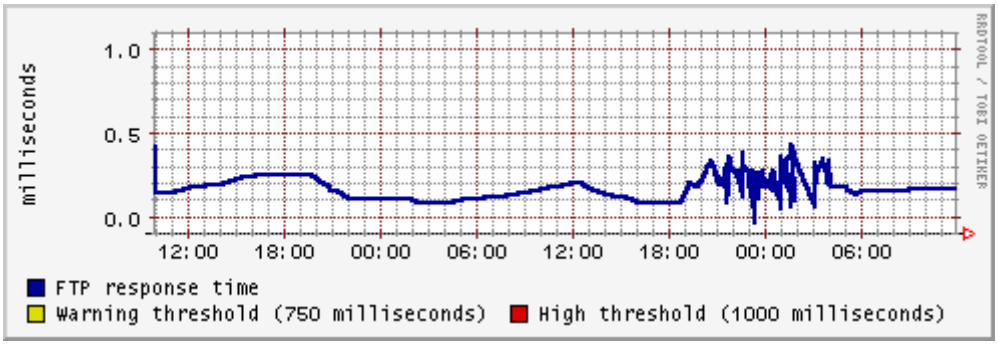

Properties for Router "SWCORE0201"
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
General
VLANs
Information: AL 9
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 2 Automatic 1 Gbps Full Duplex Active
2 2 Automatic 1 Gbps Full Duplex Active
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation10 -...
ES
10:45 a.m.


Properties for Router "SWCORE0201"
General
VLANs
Information: AL 10
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 7 Automatic 1 Gbps Full Duplex Active
2 7 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
667,627
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation11 -...
ES
10:45 a.m.


Properties for Router "SWCORE0201"
General
VLANs
Information: AL 11
Media Type: Ethernet
Speed: 2 Gbps
Duplex Mode: Full Duplex
Member Ports
Unit Port Member Reason Speed Duplex Mode Status
1 19 Automatic 1 Gbps Full Duplex Active
2 19 Automatic 1 Gbps Full Duplex Active
Port 10
Port 11
Port 12
Port 13
Port 14
Port 15: member of AL 7
Port 16: member of AL 4
Port 17: member of AL 8
Port 18
Port 19: member of AL 11
Port 20
Port 21
Port 22: member of AL 12
Port 23: member of AL 13
Port 24: member of AL 13
Port 25
Port 26
Port 27
Port 28
In unit 2: Cascade Module
AL 1: connected to MATCCSRVSWT3C
AL 2: connected to MATP3SWT3C04-0
AL 3: connected to MATPBSWT3C02-0
AL 4: connected to MATCCSRV1SWT3
AL 5: connected to MATP1SWT3C01-0
AL 6: connected to MATP2SWT3C04-0
AL 7: connected to MATCC3COM-0022
AL 8: connected to MATCC3COM-0022
AL 9: connected to MATMZSWT3C01-0
AL 10: connected to mat2p3c062
AL 11: connected to MATCCSW3C-022
AL 12: connected to Cloud 2
AL 13
OK
Cancel
Help
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
configuration
Escritorio
SupportedDevices....
3Com_10014922-A...
3Com® Network Di...
172.17.2.1 - PuTTY
linkaggregation12 -...
ES
10:44 a.m.

ANEXO D: RESULTADO DE LOS SERVICIOS CON 3COM NETWORK DIRECTOR.

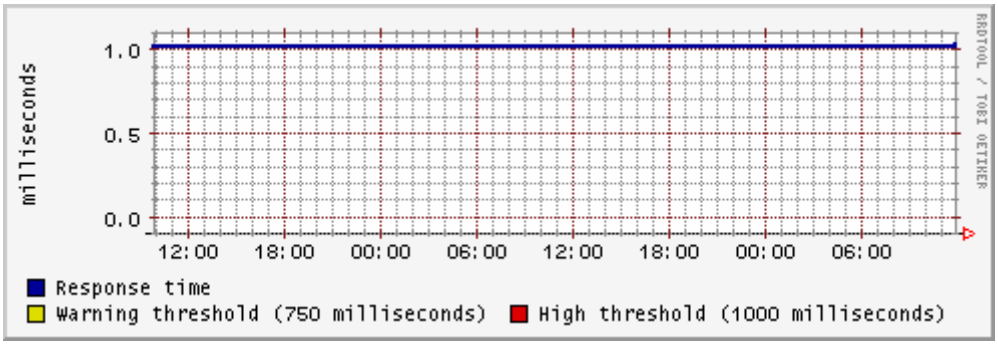
FTP Service



Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

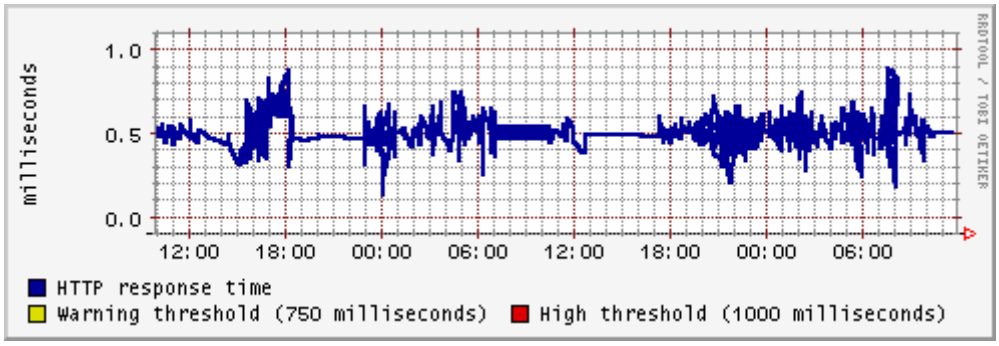
IP Ping Service



Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

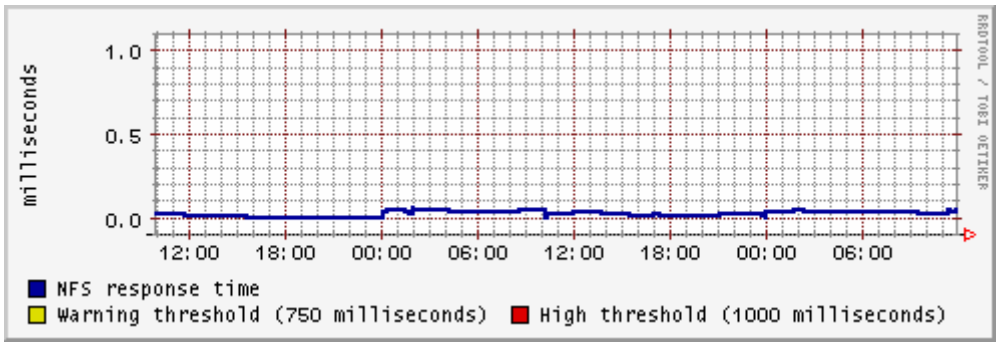
HTTP Service



Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

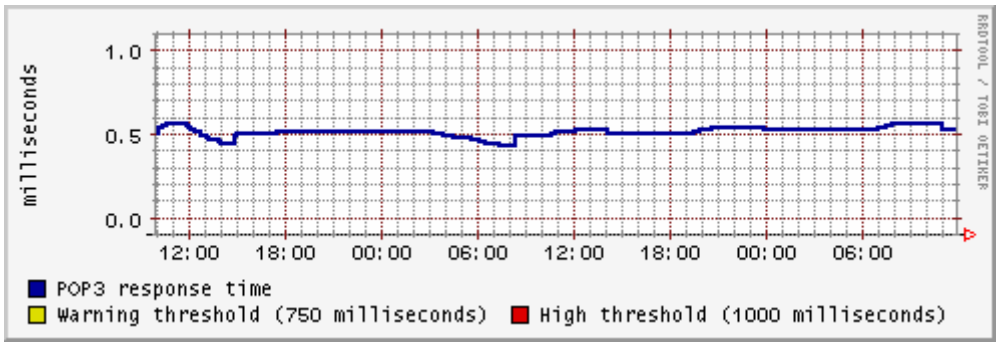
NFS Service



Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

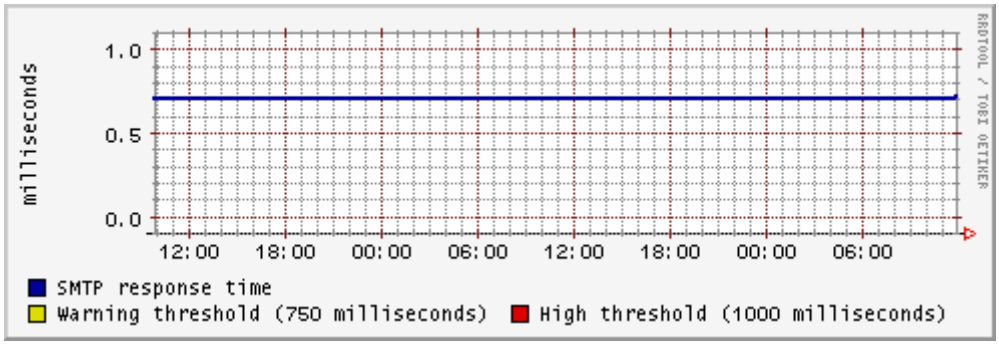
POP3 Service



Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

SMTP Service

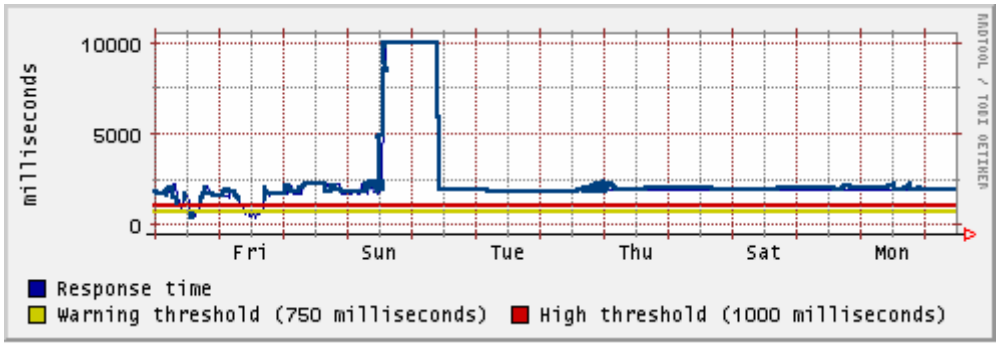


Data range: 29 de abril 2007 9:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

Weekly Graphs (30 minute average)

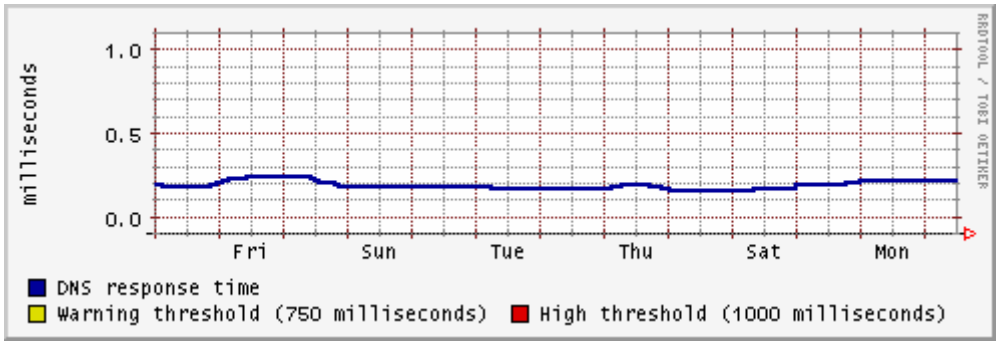
IP Ping Service



Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

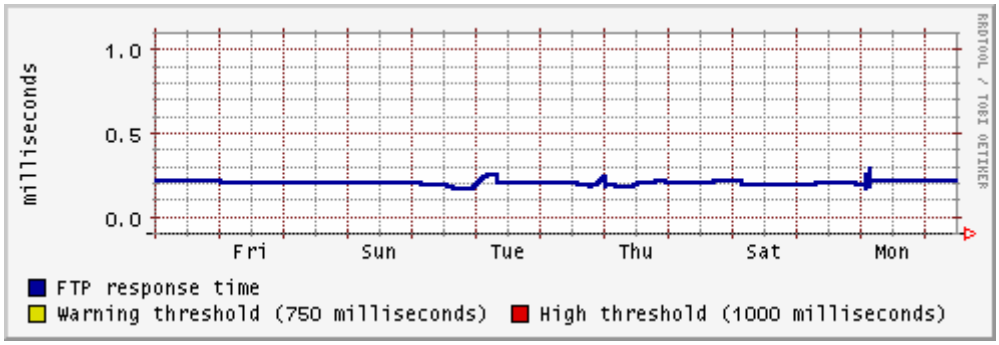
DNS Service



Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

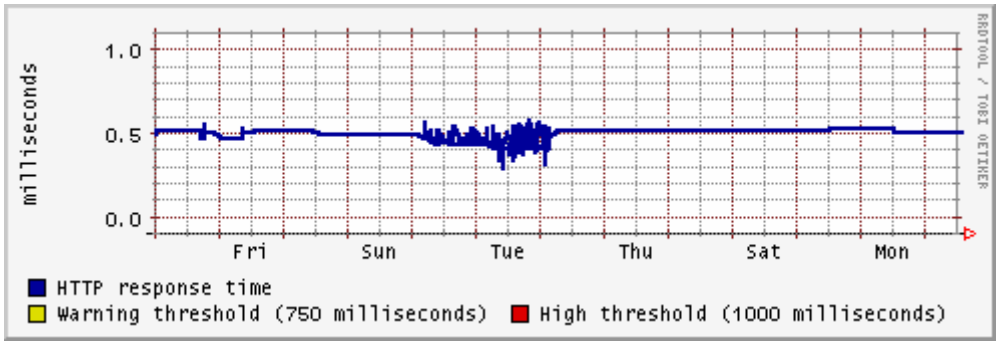
FTP Service



Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

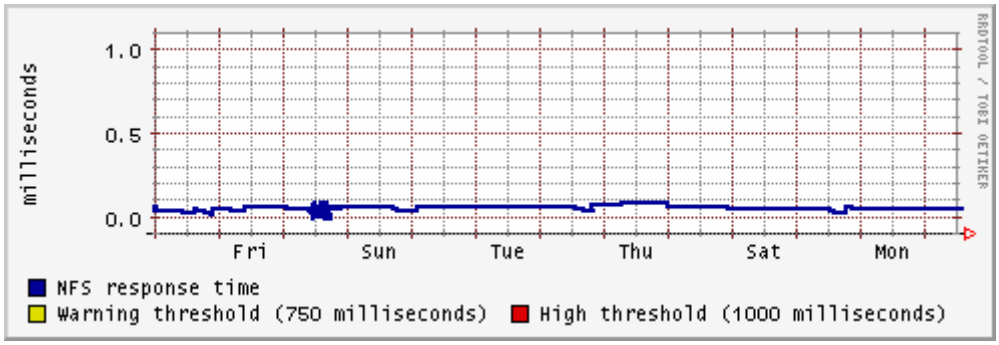
HTTP Service



Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

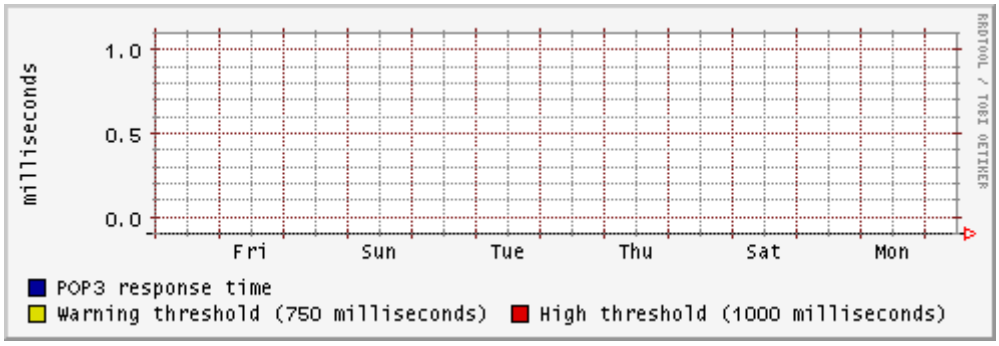
NFS Service



Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

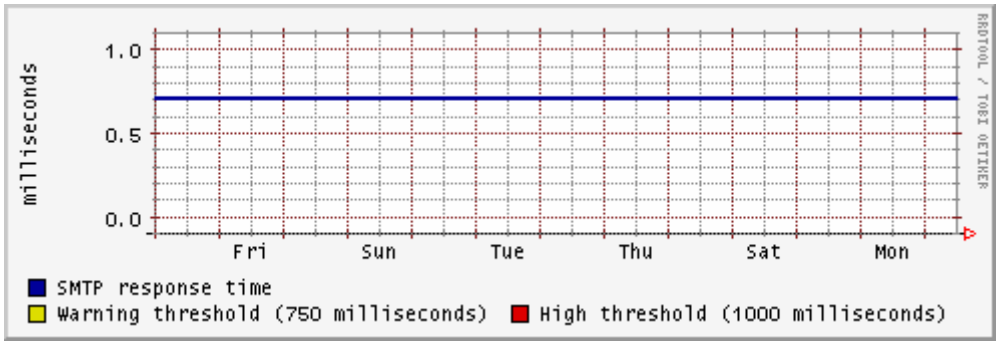
POP3 Service



Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

SMTP Service

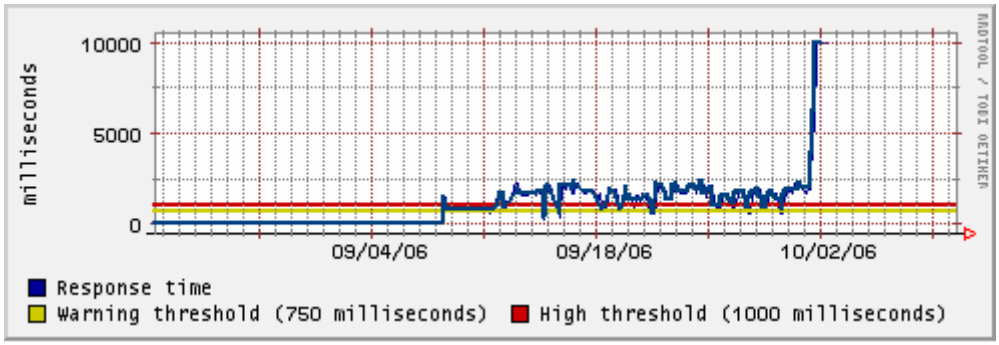


Data range: 29 de abril 2007 23:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

Monthly Graphs (2 hour average)

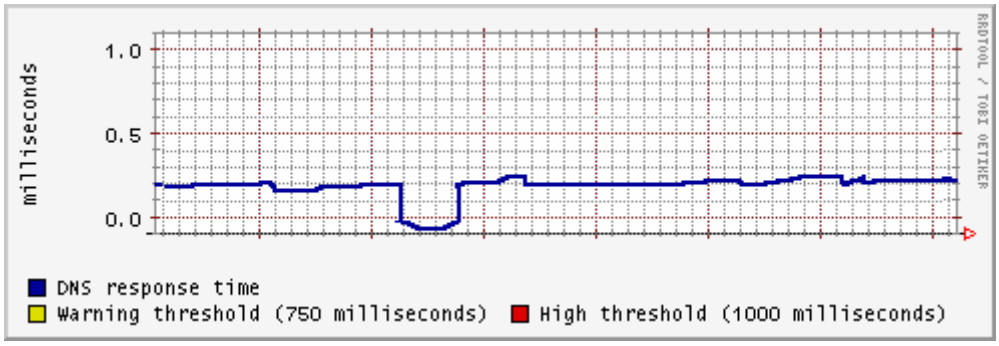
IP Ping Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

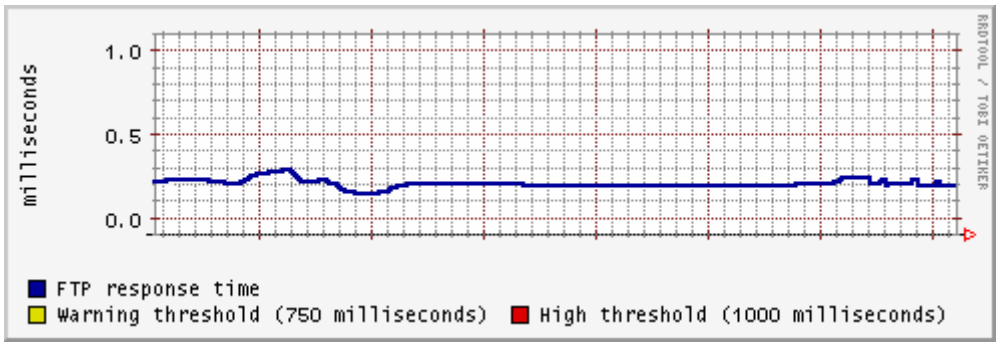
DNS Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

FTP Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

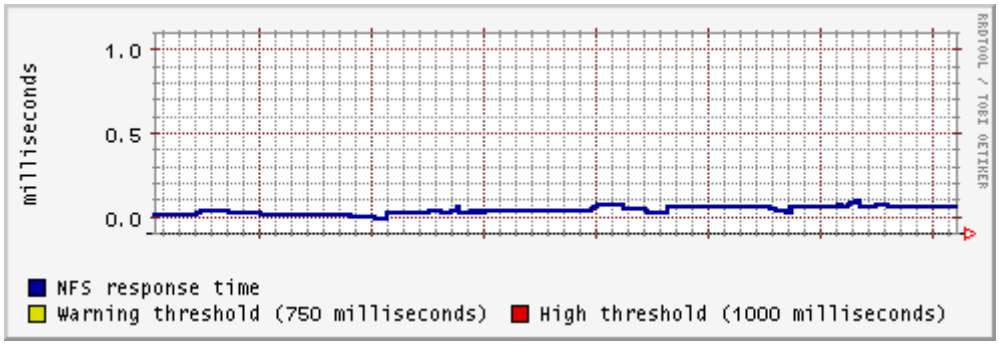
Click here to export this graph as CSV

HTTP Service

Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

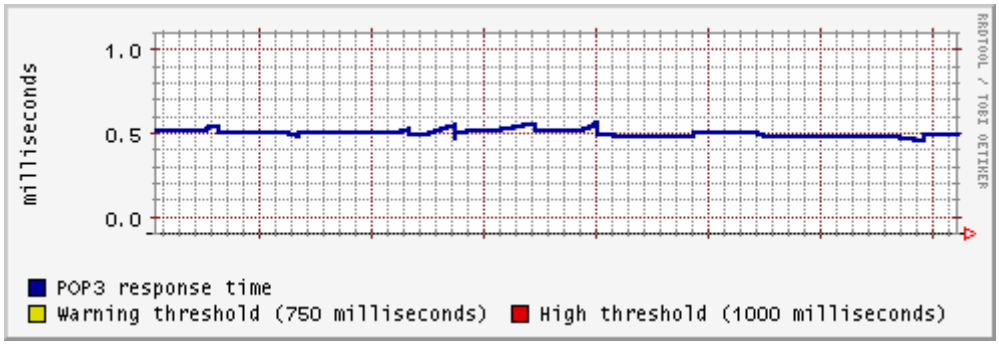
NFS Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

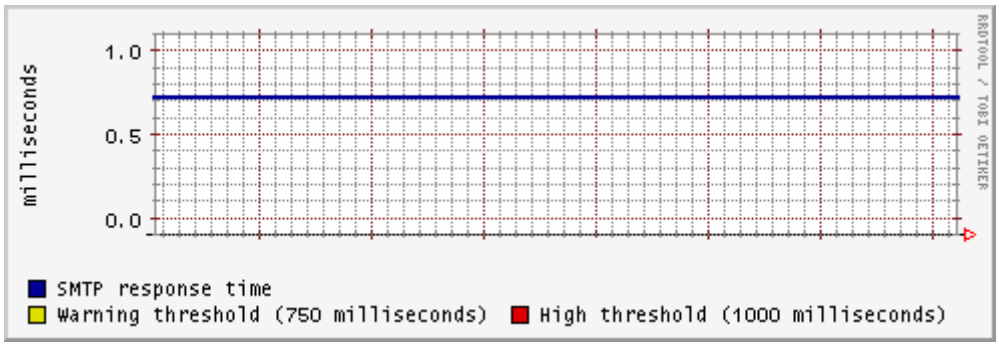
POP3 Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

SMTP Service

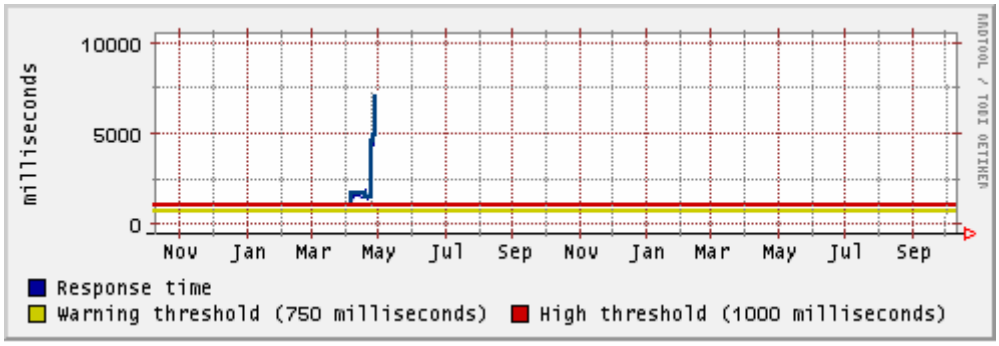


Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

Yearly Graphs (1 day average)

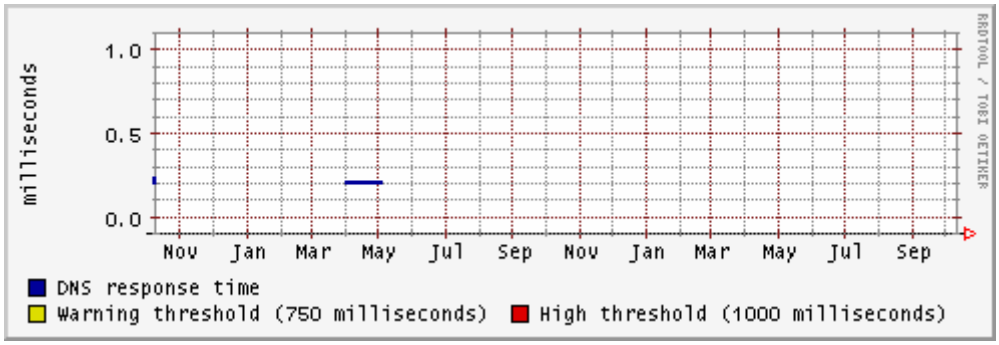
IP Ping Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

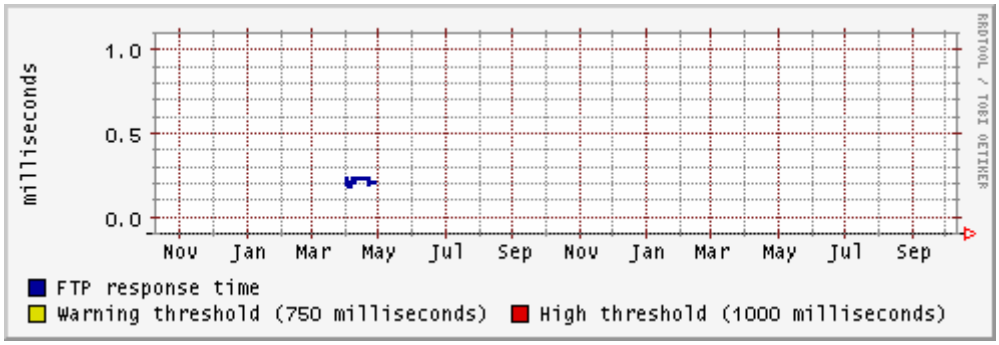
DNS Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

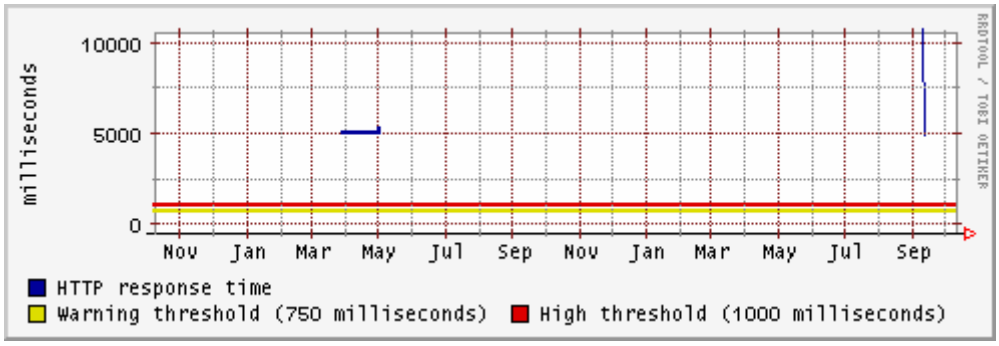
FTP Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

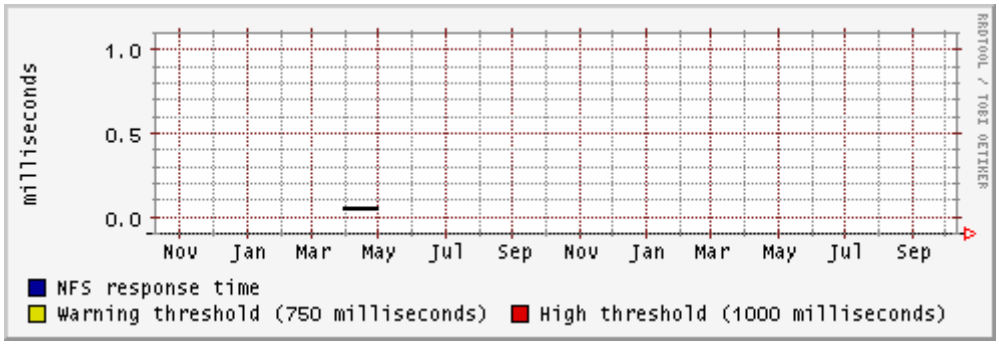
Click here to export this graph as CSV

HTTP Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

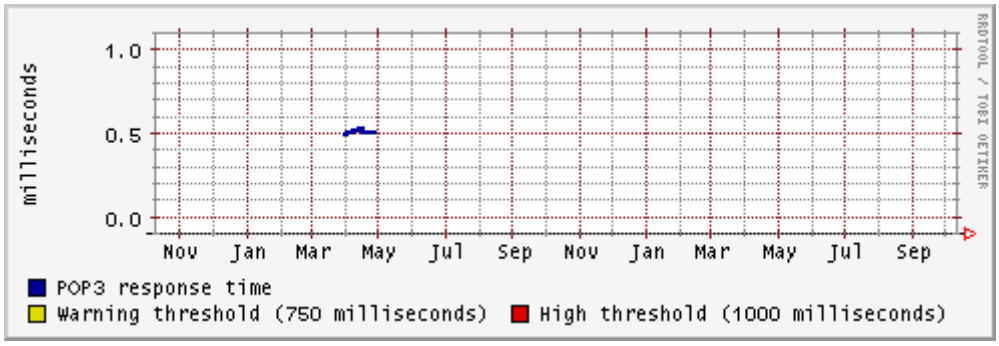
Click here to export this graph as CSV



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

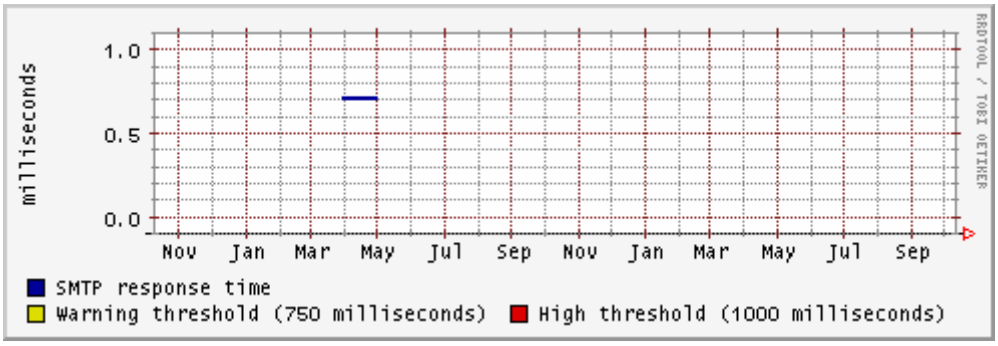
POP3 Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

SMTP Service



Data range: 29 de abril 2007 11:48 to 30 Mayo de 2007 11:48

Click here to export this graph as CSV

ANEXO E DATASHEET DE LA CENTRAL TELEFÓNICA IP NBX V3000

3com

3Com® NBX® V3000 Analog Platform R6.0

DATA SHEET

Economical, standards-based IP telephony platform with a range of built-in applications, full feature-set and analog central office trunk interfaces

OVERVIEW

The 3Com® NBX® V3000 Analog platform is a full-featured IP telephony solution designed for small- and medium-sized organizations moving to a Voice over Internet Protocol (VoIP) architecture. Its ease of use allows non-technical personnel to make individual or system-wide changes with the click of a mouse. The system's ability to scale up to 1,500 devices and to support standards-based protocols, including Session Initiation Protocol (SIP), gives organizations the confidence to choose the NBX solution for their current and future telecom needs.

With a built-in analog gateway interface, the platform can connect up to four analog loop-start central office (CO) lines directly to the Public Switched Telephone Network (PSTN), reducing configuration time and its related expense. Additionally, the NBX V3000 Analog solution—in combination with an NBX Expansion Chassis—accommodates further communications options via T1/E1, PRI, analog and BRI trunking.

To increase productivity and reduce operating costs, the solution also features a host of integrated applications, including voice messaging that provides a voice mailbox with auto-setup for every user, call center software that enhances the efficiency of agents in a queue, as well as easy to set-up hunt groups, auto-attendant, supervisory monitoring and call reporting. Email integration, supported on any IMAP4-compliant email system, offers the ability to share a common inbox for email and voice messages. Plus, V3000 Analog solutions let organizations centrally manage IP telephony services via the web with the 3Com NBX NetSet™ management application.

KEY BENEFITS

PROTECT INVESTMENT WITH MULTIPLE PROTOCOL SUPPORT

NBX V3000 Analog platforms with R6.0 and higher system software can operate in either of two modes: Standard NBX or SIP mode. **Standard NBX mode** utilizes the traditional protocol on which six generations of 3Com NBX applications have been built since 1998, while **SIP mode** allows the platform to communicate with third-party SIP-compliant devices and applications. 3Com's goal of ensuring its customers access to continuously evolving telecom standards, maximizes functionality and the return on investment (ROI) from NBX solutions.

ENABLE BUSINESS APPLICATIONS WITH SIP

SIP support unlocks access to advanced software that optimizes the productivity-enhancing benefits of VoIP technology and facilitates employee communications with collaborative tools such as IP Messaging and IP Conferencing applications.

Standards-based 3Com V3000 Analog platforms offer a comprehensive set of features, all in a compact form factor for particularly cost-effective and practical deployment.

FEATURE HIGHLIGHTS

- Support for traditional voice and multimedia communications
- Embedded applications including voice messaging, auto-attendant, and call center software
- Interoperability with SIP-compliant devices, applications and endpoints
- Browser-based NBX NetSet management tool to ease system setup and maintenance
- Compliance with Section 508 of the United States Rehabilitation Act that regulates electronic and information technology accessibility for persons with disabilities
- Management options that include SYSLOG, SNMP, SNTP, NBX Multisite Backup Tool and NBX Dial Plan Editor
- Inclusion of 15 phone licenses with base system purchase
- Multilingual NBX NetSet end-user support for United States English, Latin American Spanish, Brazilian Portuguese and Italian

SPECIFICATIONS

PLATFORM
Can operate in either Standard mode using the NBX call control protocol or in SIP mode with NBX R6.0 or higher software

SYSTEM REQUIREMENTS
100BASE-TX or switched Ethernet LAN

3Com NBX V3000 Analog platform

Minimum of two 3Com IP phones

SYSTEM CAPACITY
Support for up to 1,500 devices (lines/stations), including up to 720 PSTN CO lines and 48 Virtual Tie Lines (NBX Standard mode) or up to 300 SIP trunks (NBX SIP mode with R6.0 or higher software)

PSTN GATEWAY OPTIONS
Loop-start analog, T1/PRI, E1/PRI, ISDN BRI-ST, Q.SIG/PRI

Support for SIP analog and digital gateways in SIP mode with NBX R6.0 or higher software

PORT CONNECTIONS
WAN: via external router with IP-ToS support

LAN: one 10/100 uplink port

ANALOG DEVICES
Support for 2500 series-compatible analog devices, including cordless phones, fax machines, night bells and door ringers; one FXS port included on a V3000 platform with optional support for additional analog devices via the NBX Expansion Chassis and Analog Station card

NETWORK, PRIORITIZATION AND AUDIO COMPRESSION STANDARDS
H.323, G.711, G.729a/b, ADPCM, G.722, 802.1d, 802.1p, 802.1q, 802.2, 802.3af, 802.11, IP, IP-ToS, DiffServ, TCP/IP, UDP/IP, DHCP, DNS

APPLICATION STANDARDS
SIP, TAPI 2.1, TAPI/WAV, IMAP4, HTTP, H.323, SMTP/MIME, VPIM

MANAGEMENT
Built-in 3Com NBX NetSet utility; 3Com Network Supervisor support

NBX VOICEMAIL LANGUAGES/ DIALECTS
Chinese (Cantonese), Chinese (Mandarin), English (Australian), English (United Kingdom), English (United States), French (Parisian), German, Hebrew, Italian, Spanish (Castilian), Spanish (Latin American), Russian

POWER REQUIREMENTS
NBX V3000 Analog platform: 100-120 VAC, 50-60 Hz, 1A

220-240 VAC, 50-60 Hz, 0.5A

POWER DISSIPATION
NBX V3000 Analog platform: 50 W

IP Phones: 8 W (maximum)

CHASSIS/CALL PROCESSOR DIMENSIONS AND WEIGHT
Height: 4.445 cm (1.75 in)

Width: 48.815 cm (17.25 in)

Depth: 37.465 cm (14.75 in)

Weight: 5.68805 kg (11.54 lb)

ENVIRONMENTAL RANGES
Operating temperature: 0° to 40°C (32° to 104°F)

Storage temperature: -40° to +70°C (- 40° to +158°F)

Humidity: 5 to 85% noncondensing

NETWORK ACCESS STANDARDS
National Requirements FCC Part 68 (United States), CS03 (Canada), CTR4/A1 Commission Decision 98/520 (European Community)

SAFETY
UL/CUL 1950 Third Edition

IEC 60950: 1991 + A1, A2, A3, A4; National deviations for Europe and Australia

EMISSIONS
FCC Part 15 Class A and B

EN 55022: 1994/A1, 1995/A2, 1997/ Class A

VCCI Class A

AS/NZS 3548: 1995/Class A

RoHS-compliant

IMMUNITY
EN 55024: 1998

ANEXO F DATASHEET DEL IPS TIPPINGPOINT X505

TippingPoint
a division of 3Com

TippingPoint™ X505

DATASHEET

Building Intelligence Into The Network

The TippingPoint X505 is the first integrated security platform based on the award-winning TippingPoint Intrusion Prevention System architecture with the extended functionality of virtual private network (VPN) and firewall, bandwidth management, quality of service and Web content filtering.

The TippingPoint X505 is specifically aimed at addressing the needs of the extended enterprise, regional branch office or medium-sized business by leveraging the same award-winning TippingPoint Intrusion Prevention capabilities and Digital Vaccine® update service used to protect many large enterprises. The TippingPoint X505 is the industry's first comprehensive security solution at a performance and price point that makes it affordable for branch offices to have best-of-breed, enterprise-class security.

The TippingPoint X505 utilizes the award-winning capabilities of the TippingPoint Intrusion Prevention Systems to continually cleanse the network of malicious traffic--worms, viruses, Trojans, Phishing attempts, Spyware, VoIP threats and other harmful traffic. To ensure constant protection, TippingPoint's Digital Vaccine security team continually develops new attack filters, also known as virtual software patches, to pre-emptively protect against the exploit of new and zero-day vulnerabilities. These vulnerability filters are created to block multiple attack variants on a single vulnerability, providing zero-day protection from unknown threats. In addition to vulnerability filters, the Digital Vaccine service updates customers' TippingPoint X505 devices with a variety of new filters to protect against a comprehensive range of emerging threats such as Spyware, Phishing and P2P threats.

Digital Vaccine updates are automatically delivered to customers every week, or immediately when critical vulnerabilities and threats emerge. TippingPoint's "Recommended Protection Settings" provides preconfigured policies to automatically and accurately block attacks without any tuning, significantly reducing the amount of time and resources required to protect and maintain a healthy network.

In addition to the award winning IPS functionality, the TippingPoint X505 includes IPSec VPN, a stateful packet inspection firewall, Web content filtering, and policy-based traffic shaping, which provides fine grain bandwidth usage and control for both inbound and outbound traffic streams. One of the most compelling attributes of the X505 is that all of its functionalities are wholly interoperable. For example, IPS and traffic shaping can be applied within an IPSec VPN tunnel - effectively preventing the propagation of worms between enterprise branch locations, while simultaneously prioritizing site-to-site VoIP phone calls for enhanced VoIP quality.

The TippingPoint X505's bandwidth management capabilities are another unique differentiator. Non-critical applications, such as peer-to-peer file sharing can be throttled to reclaim valuable bandwidth. Conversely, mission-critical applications, such as video conferencing or voice over IP can be given priority to ensure Quality of Service. The TippingPoint X505 also provides a Web content filtering service that enhances productivity and reduces liability for organizations by enabling appropriate Web usage policy enforcement.

The TippingPoint X505 is supported by the TippingPoint Security Management System (SMS), an enterprise-class management platform, which provides intuitive management for multiple TippingPoint IPS or X505 devices. The TippingPoint SMS arrives with factory-installed software for

TECHNICAL SPECIFICATIONS

Performance
- 50+ Mbps IPS
- 50+ Mbps VPN (3DES/AES)
- 100+ Mbps Firewall
- 128,000 connections

Connectivity
- 4 x 10/100 data
- 1 x 10/100 management
- 1 x RS232/DB9 console
- 1 x USB (future)
- 1 x IEC AC power input

Capacity
- Unrestricted user license
- 50 Security Zones (4 physical)
- 250 IPSec Security Associations
- 1,000 concurrent Phase 2 IPSec VPN tunnels

Management
- Local Security Manager (HTTPS); CLI (local console, SSH); SNMP; TippingPoint SMS

VPN
- 3DES/DES/AES encryption
- X.509/Digital Certificates
- PPTP & L2TP/IPSec server for VPN client access

Firewall Deployment Mode
- Stateful packet inspection
- NAT (routed, transparent, mixed), NAT/PAT, port forwarding, and inter-zone firewall
- Time of day schedules
- Customizable services/groups

Content and URL Filtering
- On-box Web filtering
- Black/White URL lists
- Authenticated over-ride
- Subscription based Content Filter
  - 6 million categorized URLs
  - 40 content categories
  - 65 languages/200 countries
- Unlimited database size

Safety
- UL 60950-1, EN60950-1, CSA 22.2 No. 60950, IEC 60950

Emissions
- EN55022 Class A, FCC Part 15 Class A, ICES-003 Class A, VCCI Class A, ANSI C63.4 Class As

Power
- Input voltage: 100-240VAC
- AC Frequency: 50/60 Hz
- Current rating: 3 - 6 Amps (max)
- Power consumption: 200 W (max)

Environmental
- Operating Temperature: 0 to 40°C (32 to 104°F)
- Storage Temperature: -20 to 80°C (-4 to 176 °F)
- Humidity: 5 to 95% (non-condensing)

Dimensions
- 19" rack mountable
- Height: 2.0 in (51mm)
- Width: 17.25 in (438mm)
- Depth: 12.0 in (305mm)
- Weight: 12.7 lbs (5.8kg)

simplistic installation, and is the only IPS management system that boasts high availability (HA)/failover capabilities.

Proactive Network Security

The TippingPoint X505 leverages the same award-winning IPS engine and Digital Vaccine service used to protect thousands of enterprise-class networks throughout the world. By performing comprehensive deep packet inspection through Layers 2-7, the X505 delivers uncompromised security to eradicate attacks such as worms, viruses, Trojans, blended threats, DoS attacks, and a range of other threats. The TippingPoint IPS is the most-decorated in its field.

Maximize Business-Critical Applications

The TippingPoint X505 prioritizes real-time business-critical applications, including video conferencing, IP telephony and interactive distance-learning. Its innovative tunneling approach secures current and next-generation multicast conferencing applications as well as other business critical applications. In particular, the TippingPoint X505 can prioritize both inbound and outbound application traffic as well as inside and outside IPSec VPN tunnels. This unique feature offers high quality VoIP experiences to remote offices or users.

Enforce Acceptable Usage Policies with Content Filtering

The TippingPoint X505 can block or rate limit non-mission critical applications, and enforce acceptable Web-usage policies that improve productivity and reduce wasted bandwidth. This can ensure Internet access is being used for business-related activities, and provides protection from legal and social liabilities related to unacceptable Web content.

Web content filtering is simply a matter of check-marking the boxes in the categories to be restricted. The Web site filter database is a co-located geographically balanced hosted server, which is accessed in real time via the X505, eliminating the need to download an ever increasing database of unacceptable URLs, while ensuring your protection is always up to the minute because content is filtered through a continually updated database.

Digital Vaccine®: Constant Peace of Mind

TippingPoint's Digital Vaccine is an annual subscription service that ensures the TippingPoint X505 is constantly updated against the latest threats. Digital Vaccine also entitles access to TippingPoint's Threat Management Center (TMC), which serves as the central intelligence bureau for TippingPoint Intrusion Prevention Systems. The TMC searches for emerging vulnerabilities and continually develops new signatures and algorithms to block attacks on the network. TippingPoint's TMC Web site is the premier one-stop resource for TippingPoint X505 customers, providing up-to-date attack filter and software updates as well as product documentation.

SECURITY

Client and Server Protection
- Prevent attacks on vulnerable applications and operating systems
- Eliminate costly ad-hoc patching
- Multi-mode attack blocking

Digital Vaccine Real-Time Protection
- Pre-emptive protection against threats
- Automatic distribution of latest filters
- Recommended Settings

Spyware and Peer-to-Peer Protection
- Protect clients from becoming infected with spyware
- Prevent walk-in-worms (from infected laptops), from uploading data to the network
- Block or rate limiting Peer-to-Peer and Instant Messaging applications

Multiple Security Zones
- Separate levels of policy enforcement:
  - Departmental subnets
  - Corporate DMZs
  - Student/teacher networks
  - Time-of-day based privileges

Flexible Policy Engine
- Object-based policy rules:
  - Network/security zone/IP address group - Time-of-day based privileges
  - Service application
  - Schedules/time of day
  - VPN tunnels
- Unified control of multiple services:
  - Web filtering
  - Traffic shaping
  - User authentication
  - Device administration

Encryption and Authentication
- Next-generation IPSec encryption, including hardware-accelerated DES, 3DES, and AES
- X.509 Digital Certificate authentication from internal or third-party certificate authorities
- Web-based user authentication
- Multiple-privilege groups
- On-box and external RADIUS database

URL Filtering
- Configurable allow/deny URL lists
- Regular-expression URL matching

Web Content Filtering
- Annual subscription includes:
  - 40 content categories
  - Unlimited URL listings

CONNECTIVITY

Advanced Traffic Management
- Inbound and outbound traffic shaping:
  - VoIP
  - Video-conferencing
  - Business-critical applications
- Prioritization of traffic inside and outside VPN tunnels
- Flexible, policy based controls:
  - Time-based schedules
  - Type of service

Out-of-Box VPN Client Support
- Operating systems supported include:
  - Microsoft
  - Apple
- Standard protocols supported include:
  - PPTP
  - L2TP/IPSec
  - IPSec

Flexible Network Deployments
- Support for mixed environments irrespective of topology or IP addressing scheme:
  - Transparent
  - Routed
  - NAT (including Virtual Server and PAT)
  - Combined deployments
  - Dynamic Routing (RIP V1and 2)
  - 802.1Q VLAN Tagging

IP Multicast Routing over IPSec
- Support for PIM-DM IP multicast routing between sites over IPSec VPN, providing support for next-generation IP conferencing applications

TippingPoint
a division of 3Com

Corporate Headquarters:
75018 North Capital of Texas Hwy.
Austin, TX 78731
+1 512 681 8000
+1 888 TRUE IPS
www.tippingpoint.com

International Headquarters:
World Trade Centre Amsterdam
Zuidplein 36, H-Toren
1077 XV Amsterdam
The Netherlands
+31 20 799 7629

3com

ANEXO G DATASHEET DEL SWITCH 5500

3Com® Switch 5500 10/100 Family

DATA SHEET

- Advanced stackable switches for the enterprise edge
- Highly resilient 3Com® XRN® Technology stacking architecture, up to eight units high
- Standard and enhanced models for maximum choices
- Highest level of security and converged network features

Key Benefits

Scalability
An enterprise-class, high-end 10/100 Layer 2/3/4 switch portfolio that is stackable to up to eight units high and provides 384 Fast Ethernet ports, with additional Gigabit ports for stacking or uplinks.

Performance
28– and 52–port models deliver switching capacity of up to 12.8 and 17.6 Gbps, respectively, with wirespeed, line-rate performance delivered on all ports.

Flexibility
Standard image (SI) and enhanced image (EI) software give the widest choice of enterprise switch features at an optimal price. EI-models offer Layer 3 Open Shortest Path First (OSPF) routing, patented 3Com® XRN® technology, and IEEE 802.3af Power over Ethernet (PoE)—for advanced support of today's converged networks.

Network-Level Availability
XRN (eXpandable Resilient Networking) technology is a 3Com innovation that enables multiple interconnected and stackable Layer 3 switches to behave as a single management entity.

Automated stack and fabric setup delivers high resiliency and continuous availability without adding to network complexity. Once configured, all switches actively share network loads and routing intelligence and support ultra-fast failover recovery for lost or disconnected switches.

Multilayered Security
These advanced enterprise switches integrate distributed security enforcement and centralized network management features. Access Control Lists (ACLs) help safeguard access to key network resources from unauthorized access and data corruption. User-based authentication and DES 56-bit encryption help secure Layer 3 protocols and management controls, such as SSH and SNMP. IEEE 802.1X RADIUS Network Login and MAC-based authenticated RADIUS login enforce access control at the network's edge.

Priority for Converged and Business-Critical Traffic
Next-generation features—advanced, policy-based Class of Service/Quality of Service (CoS/QoS), eight priority queues, committed access rates, bandwidth limiting and filtering, and more—identify and prioritize time-sensitive traffic, including voice over IP (VoIP). For assured privacy, switches can be configured to isolate 3Com NBX® and other-vendor VoIP traffic through a voice-dedicated virtual LAN (VLAN).

Unique AC-/DC-Powered Operation
Support for AC- and direct DC-powered operation leverages your existing power schemes in data centers and switching infrastructures. The state-of-the-art Redundant Power System (RPS) is designed to work with the 3Com Switch 5500. This RPS can provide supplemental N+1 power across all PoE ports in the switch, provisioning up to 384 ports with a full 15.4W.

Future-Proof Investment
Standards-based switching—including IPv6 traffic filtering and classification—cabling support, and management features provide a networking solution that maximizes existing IT investment and supports emerging standards.

Powerful, Unified Management
Switches are powered by the 3Com Operating System, the same proven software shared across our premium enterprise products including the 3Com Switch 8800 and 7700 modular families. This consolidates administrative control over the entire switching infrastructure when using 3Com management application software such as 3Com Enterprise Management Suite and 3Com Network Director.

Specifications

All information in this section is relevant to all members of the 3Com Switch 5500 10/100 family, unless otherwise stated.

Connectors
24 or 48 auto-negotiating 10BASE-T/100BASE-TX ports configured as auto MDI/MDIX; 4 Gigabit SFP ports

24 auto-negotiating in-line power 10BASE-T /100BASE-TX ports configured as auto MDI/MDIX; 4 Gigabit SFP ports (28-port PWR only)

24 SFP ports, to be populated with 100BASE-X SFP transceivers with multi- or single-mode connectors; 2 Gigabit SFP ports; 2 auto-negotiating 10BASE-T/ 100BASE-TX/1000BASE-T ports configured as auto MDI/MDIX (28-port FX only)

Redundant power supply (-48 VDC) connector

RJ-45 console port

Security
RADIUS authentication

RADIUS session accounting

SSH v1.5

IEEE 802.1X network login

Access Control Lists (ACL)

Packet filtering

SNMP v3 encryption

Stacking
Up to 384 10/100 front panel ports

Stack Switch 5500 EI models only with other like units using XRN Technology via SFP ports.

Stack Switch 5500 SI models only with other like units using 'master/slave' via SFP ports.

Performance
28-port
12.8 Gbps switching capacity, maximum

9.5 Mpps forwarding rate, maximum

16,000 MAC addresses supported

52-port
17.6 Gbps switching capacity, maximum

13.1 Mpps forwarding rate, maximum

16,000 MAC addresses supported

Reliability
(MTBF @ 25°C)

28-port: 53 years (464,000 hours)

28-port PWR: 30 years (263,000 hours)

52-port: 44 years (385,000 hours)

52-port PWR: 21 years (184,000 hours)

28-port FX: 38 years (184,000 hours)

Dimensions
Height: 43.6 mm (1.7 in or 1U)

Width: 440 mm (17.3 in)

Depth:
Non-PWR models: 270 mm (10.6 in)
PWR models: 427 mm (16.8 in or 1U)

Weight:
Non-PWR models: 3.3 kg (7.3 lb)
PWR models: 6.3 kg (13.9 lb)

Power Supply
AC Line Frequency 50/60 Hz

Input Voltage 90-240 VAC

Current Rating:
1.0A maximum

Environmental Requirements
Operating temperature:
0° to 40°C (32° to 104°F)

Storage temperature:
-10° to 70°C (14° to 158°F)

Humidity (operating and storage):
10% to 95% non-condensing

Standard: EN 60068 (IEC 68)

Industry Standards Supported
IEEE 802.1D (STP)

IEEE 802.1p (CoS)

IEEE 802.1Q (VLANs)

IEEE 802.1S (MSTP)

IEEE 802.1w (RSTP)

IEEE 802.1X (Security)

IEEE 802.3 (Ethernet)

IEEE 802.3ad (Link Aggregation)

IEEE 802.3ab (1000BASE-T)

IEEE 802.3ae (10G Ethernet)

IEEE 802.3i (10BASE-T)

IEEE 802.3u (Fast Ethernet)

IEEE 802.3x (Flow Control)

IEEE 802.3z (Gigabit Ethernet)

IETF Standards
Management, Including MIBs Supported
RFC 1213/2233 (MIB II)

RFC 1253 (OSPF Version 2 MIB) (EI models only)

RFC 1724 (RIP Version 2 MIB Extension)

RFC 1907 (SNMP v2c, SMI v2 and Revised MIB-II)

RFC 2021 (RMON II Probe Config MIB)

RFC 2233 (Interfaces MIB)

RFC 2571 (FrameWork)

RFC 2571-2575 (SNMP)

RFC 2613 (Remote Network Monitoring MIB Extensions)

RFC 2665 (Pause control)

RFC 2668 (IEEE 802.3 MAU MIB)

RFC 2674 (VLAN MIB Extension)

RFC 2819 (RMON MIB)

Emissions / Agency Approvals
CISPR 22 Class A

FCC Part 15 Class A

EN 55022 1998 Class A

ICES-003 Class A

VCCI Class A

EN 61000-3-2 2000, 61000-3-3

Immunity
EN 55024

Safety Agency Certifications
UL 60950

IEC 60950-1

EN 60950-1

CAN/CSA-C22.2 No. 60950-1-03

Management
SNMP and Telnet support

Multiple agents with single management entry point

RMON-1, SMON

RMON Groups: Statistics, History, Alarms and Events

Statistics gathering and reporting

Command line interface

Management through 3Com management applications

- 3Com Network Supervisor

- 3Com Network Director

- 3Com Enterprise Management Suite

Warranty
Limited Lifetime Hardware Warranty, except for fans and power supply, which is 5 Year Limited. Limited Software Warranty for ninety (90) days. See www.3com.com/warranty for details.

Other Benefits
90 days of telephone technical support. Limited software updates.

See www.3com.com/warranty for more detail.

Register products at http://eSupport.3com.com.

Service
Americas:
www.3com.com/products/en_US/global_services

International:
http://emea.3com.com/globalservices

REFERENCIAS BIBLIOGRÁFICAS

[1] LAN Switching technologies, 3Com University, Sawn Newman

[2] IPS Training, Noboru Kamino, Intrusión Prevention System Product Training, Jim Hughes

[3] Información de seguridad: www.sans.org

[4] Tecnologias emergente en redes de comunicación de datos, Ulyses Black, quinta edicion 2005.

[5] 3Com University, *NBX Advanced technical Training R6.0, 1, Estados Unidos , Junio del 2006.*

[7] Documentación oficial de 3Com: http://www.3com.com

[8] Soluciones de Telefonía para empresas: http://www.inConcertCC.com

[9] Chambers, John, "El autentico valor de la convergencia", *COMPUTERWORLD, 176, 12, 15 de Febrero del 2007.*

[10] 3Com Corporation, *Securing Networks witch the 3Com X-Family, 1, 350 Campus Drive, Marlborough, Abril del 2007.*

[11] Greg Young, John Pescatore, "Magic Quadrant for Network Intrusión Prevention System Appliances, 2H06" Gartner RAS Core Research Note G00144735, 22 December 2006, R2130 12282007.

Sangolquí, _____

Elaborado por:

_____ _____

Hugo Yépez Crow Marcelo Erazo Carrión

Coordinador de la Carrera

_____

ING. GONZALO OLMEDO