TRABAJO ESPECIAL DE GRADO

SELECCIÓN DE UN SISTEMA DE GESTIÓN DE RED PARA LA COMPAÑÍA BSP

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. García R. Juan F.
Para optar al Título de
Ingeniero Electricista

Caracas, 2005

TRABAJO ESPECIAL DE GRADO

SELECCIÓN DE UN SISTEMA DE GESTIÓN DE RED PARA LA COMPAÑÍA BSP

Prof. Guía: Ing. Dan El Montoya
Tutor Industrial: Lic. José Padulo

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Garcia R., Juan F.
Para optar al título de
Ingeniero Electricista

Caracas, 2005

CONSTANCIA DE APROBACIÓN

Caracas, 10 de noviembre de 2005

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller García R. Juan F., titulado:

"SELECCIÓN DE UN SISTEMA DE GESTIÓN DE RED PARA LA COMPAÑÍA BSP"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Luis Fernández
Jurado

Prof. Francisco Varela
Jurado

Prof. Dan El Montoya
Prof. Guía

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE
INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

DEDICATORIA

Ante todo a Dios y todos los Santos, por dame fuerza en los momentos de debilidad.

A mis PADRES que son mi inspiración, mis ojos, mi todo, por darme siempre su apoyo incondicional y enseñarme que no hay nada más importante que los estudios, lo más importante entre muchas cosas bellas que me van a dejar. Me ha costado mucho y se que sin ustedes no podría haber llegado hasta aquí, los quiero mucho.

A todos mis amigos que tanto han estado pendiente de mi, esperando se sientan tan orgullosos como yo de éste logro, y les sirva de inspiración de vida.

Aquí les dejo este regalo.

Juan F. García.

RECONOCIMIENTOS Y AGRADECIMIENTOS

Hago un especial reconocimiento a mis dos tutores por todo el apoyo, y dedicación ofrecida para la realización de éste Trabajo Especial de Grado. Gracias Prof. Montoya y Lic. José Padulo.

Agradezco a mis padres por la paciencia que me tienen.

A mí amigo Carlos por ese apoyo incondicional, no sabes cuanto me ayudaron las impresiones entre otras cosas.

A mi amigo Marco por toda la ayuda ofrecida para conseguir la pasantía.

A Ivan por sus correcciones y comentarios tan oportunos.

Y a todas esas personas que de una u otra forma pusieron un granito de arena para ayudarme a materializar este trabajo.

A todos muchísimas gracias.

Juan F. García.

García R., Juan F.

SELECCIÓN DE UN SISTEMA DE GESTIÓN DE RED PARA LA COMPAÑÍA BSP

Prof. Guía: Ing. Dan El Montoya. Tutor Industrial: Lic. José Padulo. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución. BSP. 2005. 99h + anexos.

Palabras claves: Gestión de Red; Análisis de Tráfico; Redes LAN y WAN.

Resumen: Se plantea la selección de un sistema de gestión de red enfocado en el análisis de tráfico de la compañía BSP. BSP es un ASP que ofrece servicios de outsourcing orientado a apoyar a sus clientes en las áreas administrativas, tecnología y nómina. Para prestar estos servicios con calidad, requiere que éste sistema de gestión de red le permita monitorear y detectar problemas en el tráfico de datos de su red LAN y enlaces WAN hacia sus clientes, para generar acciones correctivas oportunas. Después de estudiar exhaustivamente varios programas, se seleccionó *WhatsUp Professional* para el constante monitoreo y reportes de disponibilidad de los servidores y enlaces, *MRTG* para generar gráficas estadísticas del comportamiento del uso del ancho de banda de los enlaces WAN, *NTOP*, *Ethereal* y *Network Monitor* de SMS para analizar los protocolos, utilización de la red y establecer políticas de acceso y *Network Inspector* para el inventario de equipos de red y diagramación de la LAN.

INDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS Y GRÁFICAS

ACRÓNIMOS

ASCII: American Standard Code for Information Interchange.

AI: Artificial Intelligence. (Inteligencia artificial).

ANSI: American National Standards Institute.

ATM: Asynchronous Transfer Mode. (Modo de transferencia asíncrono).

BSP: Bussines Services Provider.

CATV: Cable Televisión. (Redes de televisión por cable).

CMIP: Common Management Information Protocol.

CNM: Customer Network Management.

CSMA/CD: Carrier Sense Multiple Access / Collision Detect.

DNS: Domain Name Server.

ERP: Enterprise Resource Planning. (Sistemas de planificación de recursos).

ETD: Equipo Terminal de Datos.

ETSI: European Telecommunications Standards Institute.

FTP: File Transfer Protocol.

HDLC: High-Level Data Link Control.

HTML: Hyper Text Markup Language. (Lenguaje de marcación de hipertexto).

HTTP: Hyper Text Transfer Protocol. (Protocolo de transferencia de hipertexto).

IAB: Internet Activities Board.

IEEE: Institute of Electrical and Electronics Engineers. (Instituto de Ingenieros Eléctricos y Electrónicos).

IETF: Internet Engineering Task Force. (Fuerza de Tareas de Ingeniería de Internet.)

IP: Internet Protocol, (Protocolo de Internet).

IPX: Internetwork Packet Exchange.

ISO: International Standardization Organization. (Organización Internacional para la Estandarización).

LAN: Local Area Network. (Red de área local).

MAN: Metropolitan Area Network. (Red de área metropolitana).

OAM&P: Operation, Administration, Maintenance and Provisioning.

OAM: Operation, Administration, Maintenance.

OSI: Open Systems Interconection. (Interconexión de sistemas abiertos).

PAN: Personal Area Network. (Red de área personal).

PC: Personal Computer. (Computador personal).

PDA: Personal Digital Assistant. (Ayudante personal digital).

POP: Post Office Protocol.

QoS: Quality of Service. (Calidad de servicio).

REDIRIS: Red para la interconexión de los recursos informáticos.

SGMP: Simple Gateway Monitoring Protocol.

SMFAs: Systems Management Functional Areas.

SMFs: Systems Management Functions.

SMTP: Simple Mail Transfer Protocol.

SNMP: Simple Network Management Protocol.

SPX: Sequenced Packet Exchange. (Intercambio secuenciado de paquetes).

SSH: Secure SHell.

TCP: Transmission Control Protocol. (Protocolo de control de transmisión).

TMN: Telecommunications Management Network.

UDP: User Datagram Protocol. (Protocolo de intercambio de datagramas).

UTP: Unshielded Twisted Pair. (Par trenzado no blindado).

VPN: Virtual Private Network, (Red Privada Virtual RPV).

WAN: Wide Area Network. (Red de área amplia).

INTRODUCCIÓN

La implantación de aplicaciones cliente servidor y sistemas cada vez más complejos y vitales tales como servicio ASP (Application Service Provider), mensajería interna (Ccmail, Notes y otros), correo electrónico, servicio de internet e intranet, y adicionalmente los compromisos con niveles de servicios cada vez más estrictos ofrecidos a los clientes de dichas aplicaciones en diversas empresas transnacionales, ha producido un repunte en la implantación de herramientas de gestión de redes y sistemas, que permitan una administración centralizada, detección de fallas en tiempo real y prevenciones de las mismas, minimizando los tiempos de resolución de dichos problemas y adicionalmente permitiendo medir la gestión de desempeño de la red en general.

En el presente trabajo de grado se realiza un estudio de las aplicaciones de gestión de red con el fin de seleccionar las más adecuadas para la red de BSP (Business Services Provider de Venezuela) que permita monitorear el tráfico de la LAN (Local Area Network) y enlaces WAN (Wide Area Network) hacia sus clientes, al igual que generar gráficas estadísticas del consumo de ancho de banda, reportes de la disponibilidad de sus servidores y servicios y por último analizar los protocolos y aplicaciones en circulación por su red, para que de ser necesario se apliquen políticas de acceso.

El estudio de estas aplicaciones se basa en la instalación, análisis y puesta a prueba de las mismas. Varias de estas son de licencia de uso público y otras son versiones de tiempo limitado dado que la licencia y uso comercial acarrea algún costo, y como se manifiesta en las limitaciones no se cuenta con el presupuesto para su adquisición inmediata.

Una vez seleccionadas las herramientas más idóneas, se hará uso de ellas para detectar debilidades y comportamientos que reflejen una actividad anormal en la red de la compañía, y finalmente se plantearán medidas correctivas.

CAPITULO I

1.1. Descripción de la compañía BSP.

Business Services Provide (BSP) es una Empresa que presta servicios de outsourcing cuyo objetivo es permitir a la gerencia de sus clientes dedicar una mejor atención hacia su negocio base, así como proveerlos de mejor y más oportuna información para apoyar la toma de decisiones.

La misión de ésta empresa es ser líder en el negocio de outsourcing con tecnología de avanzada, a través de los más altos niveles de calidad, competitividad y relación costo-beneficio, lo cual se traduce en una ventaja competitiva para sus clientes.

La visión de la empresa es estar siempre a la vanguardia en tecnología y mantener importantes alianzas estratégicas para la implantación de soluciones integrales de información y gestión a nivel nacional e internacional, buscando la mayor satisfacción de sus clientes.

Sus principales aliados son:

PeopleSoft es el software ERP que ofrece a sus clientes. *PeopleSoft* es uno de los proveedores líderes de software en sistemas integrados de información con más de 8.000 clientes en el mundo entero.

IBM es su plataforma de hardware. IBM es una de las corporaciones más grandes de la industria tecnológica, reconocida mundialmente.

IMPSAT es su proveedor de telecomunicaciones. Aporta soluciones integradas de voz, datos e Internet en banda ancha a empresas en toda Latinoamérica.

1.2. Planteamiento del problema.

Los ASP son proveedores que manejan y distribuyen servicios de software desde un mismo centro hacia sus diversos clientes. Una empresa que necesite un programa de contabilidad, en vez de comprar el software e instalarlo en cada una de las computadoras, puede rentar los programas a través de un ASP. De esta forma, la empresa se ahorra los gastos de implementación y el trabajo de realizar las actualizaciones, entre otras cosas.

La empresa BSP siendo un ASP, y en la búsqueda de ofrecer cada vez un mejor servicio, siente la necesidad de implantar herramientas para la gestión de su red LAN y WAN, tomando como ventaja el disponer de una estructura de red con equipos que manejan los protocolos SNMP (Simple Network Management Protocol), TCP/IP, y Frame Relay, siendo lo mínimo requerido por las tecnologías de gestión de redes y sistemas (System y Network Management).

Sintetizando se puede decir que los problemas principales que se quieren corregir mediante éste trabajo son: la falta de información oportuna (tráfico de la red) para la toma de decisiones, retraso en la detección y prevención de fallas, optimización del ancho de banda y falta de administración centralizada.

1.3. Objetivos.

1.3.1. Objetivo general.

El objetivo general de éste trabajo es seleccionar, configurar e implantar un sistema de gestión en la red LAN y WAN de la compañía BSP, con el fin de apoyar y

mejorar los servicios que ofrece como ASP, analizando el tráfico de datos, mejorando sustancialmente los tiempos de respuestas en la entrega de servicios, alertando y previniendo fallas.

1.3.2. Objetivos específicos.

Los objetivos específicos de este trabajo son:

- Estudiar la estructura de la red de BSP, para definir los límites y/o el alcance que tendrá la herramienta de gestión. En este punto se definirán las redes, subredes, dominios y equipos a monitorear: equipos de interconexión (conmutadores y enrutadores) y servidores.
- Seleccionar la(s) herramienta(s) de gestión a utilizar.
- Determinar el tráfico de las aplicaciones a ser ofrecidas.
- Estudiar las características técnicas y ubicación física del servidor central de gestión donde serán instaladas las herramientas y determinar las características de las consolas remotas de administración y supervisión
- Monitorear el desempeño de los enlaces WAN entre la compañía y los clientes.
- Detectar debilidades principalmente relacionadas al tráfico en la red LAN y WAN y plantear medidas correctivas para estas.

CAPITULO II

MARCO REFERENCIAL TEÓRICO

2.1. Redes.

Existen varias definiciones de una red, algunas de las cuales se mencionan a continuación:

- Conjunto de operaciones centralizadas o distribuidas, con el fin de compartir recursos "hardware y software".
- Sistema de transmisión de datos que permite el intercambio de información entre computadoras.
- Conjunto de nodos (computadoras) conectadas entre sí.[1]

2.2. Redes de datos.

Las redes de datos surgieron como resultado de las aplicaciones informáticas creadas para las empresas. Sin embargo, en el momento en que se desarrollaron estas aplicaciones, las empresas poseían computadores que eran dispositivos independientes que operaban de forma individual, sin comunicarse entre si. Esto puso de manifiesto que ésta no era la forma más eficiente ni rentable para operar en el medio empresarial. Las empresas necesitaban una solución que resolviera con éxito las siguientes tres preguntas:

- ¿Cómo evitar la duplicación de equipos informáticos y de otros recursos?

---

[1] Monografías.com [en línea]. <http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml> [Consulta: 2005]

- ¿Cómo comunicarse con eficiencia?
- ¿Cómo configurar y administrar una red?

Las empresas se dieron cuenta que podían ahorrar mucho dinero y aumentar la productividad con la tecnología de interconexión. Empezaron creando redes y expandiendo las existentes casi tan rápidamente como se producía la introducción de nuevas tecnologías y productos de red. Como resultado, a principios de los 80, se produjo una gran expansión de las tecnologías de red. Sin embargo, el temprano desarrollo de las redes resultaba caótico en varios aspectos.

A mediados de la década del 80, comenzaron a presentarse los primeros problemas de este crecimiento desordenado. Muchas de las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software distintas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones.

Una de las primeras soluciones a este problema fue la creación de redes de área local (LAN). Como estas conectaban todas las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio, permitieron que las empresas utilizaran la tecnología informática para compartir de manera eficiente archivos e impresoras.

A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. En un sistema LAN, cada departamento o empresa, era una especie de isla electrónica.

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino de una empresa a otra. Entonces, la solución fue la creación de redes de área

metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

2.3. Clasificación de la redes.

2.3.1. Redes según la escala.

Según el área geográfica que abarcan las redes se pueden clasificar en:

- PAN Redes de área personal (metro cuadrado; < 1 m.)
- LAN Redes de área local (cuarto, edificio, campus; < 1 Km.)
- MAN Redes de área metropolitana (ciudad; < 10 km.)
- WAN Redes de área amplia (país, continente; < 1000 km.) [2]

Las redes PAN (red de administración personal) son redes pequeñas, conformadas por no más de 8 equipos. Últimamente esta clasificación se está utilizando para una red local inalámbrica con un alcance muy limitado (hasta 10 metros). Las redes PAN se utilizan para conectar dispositivos, como asistentes personales digitales (PDA), teclados, ratones, impresoras, etc, que utiliza una persona con su computador. Al desaparecer los cables, estas redes permiten una interconexión más fácil. Bluetooth es una tecnología que se utiliza, por lo general, para formar una red personal.

LAN es un acrónimo inglés de Local Area Network (Red de Área Local), que se refiere a las redes locales de computadoras. La LAN más antigua y popular, ARCnet, fue lanzada en 1977 por Datapoint y fue originalmente diseñada para compartir múltiples discos de almacenamiento Datapoint 2200. Como todas las LANs antiguas, ARCnet era tecnología propietaria de hardware y software. Los esfuerzos de

---

[2] Wikipedia en Español [en línea].
<http://es.wikipedia.org/wiki/Redes_de_ordenadores/computadoras>. [Consulta: 2005]

estandarización por parte del IEEE (Institute of Electrical and Electronics Engineers) resultaron en la serie IEEE 802. Actualmente hay dos tecnologías comunes de cableado para LAN, Ethernet y Token Ring. Tecnologías sin cables también existen y son convenientes para usuarios de equipos móviles.

WAN es un acrónimo de Wide Area Network que en inglés significa (red de área amplia). Un ejemplo de este tipo de redes sería REDIRIS, la misma internet o cualquier red en las que no estén, en un mismo edificio, todos sus miembros (sobre la distancia hay discusión posible). Opera en la capa física y de enlace del modelo de referencia OSI (Open Systems Interconection). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado. Otras son construidas por los proveedores de internet (ISP) para ofrecer conexión a sus clientes.

Hoy en día internet proporciona WAN de alta velocidad. Como consecuencia de lo anterior la necesidad de redes privadas WAN se ha reducido drásticamente mientras que las redes privadas virtuales (VPN) que utilizan cifrado y otras técnicas para hacer esa red dedicada aumentan.

Entre las LAN y WAN se encuentran las MAN o Redes de área metropolitana. Por lo general se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos. Las redes de televisión por cable (CATV), son ejemplos de MAN analógicas para el caso de distribución de televisión.

2.3.2. Redes según la direccionalidad de los datos.

Según la direccionalidad de los datos las redes se clasifican en:

- Simplex unidireccionales, un ETD transmite y otro recibe
- Half-duplex bidireccionales, un sólo ETD transmite por vez
- Full-duplex ambos ETD pueden transmitir y recibir a la vez [3]

2.4. Mediciones de ancho de banda digital.

Las LAN y WAN, siempre han tenido algo en común: el uso del término ancho de banda para describir sus capacidades. El ancho de banda es la medición de la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado. Existen dos usos comunes del término ancho de banda: uno se refiere a las señales analógicas y el otro a las señales digitales. Bits por segundo es una unidad de ancho de banda. La siguiente tabla proporciona un resumen de las diversas unidades de ancho de banda:

Tabla 1. Diversas unidades de ancho de banda.

Unidad de ancho de banda	Abrev.	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1 kbps = 1.000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1.000.000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1.000.000.000 bps = 10^9 bps

2.5. Protocolos de redes.

Se le llama protocolo de red o protocolo de comunicación al conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación

[3] Wikipedia en Español [en línea].
<http://es.wikipedia.org/wiki/Redes_de_ordenadores/computadoras>. [Consulta: 2005]

entre entidades que forman una red. En este contexto, las entidades de las cuales se habla son programas de computadora o automatismos de otro tipo, como dispositivos electrónicos capaces de interactuar en una red.

Los protocolos de red establecen aspectos tales como:

- Las secuencias posibles de mensajes que pueden arribar durante el proceso de la comunicación.
- La sintaxis de los mensajes intercambiados.
- Estrategias para corregir los casos de error.
- Estrategias para asegurar la seguridad (autenticación, encriptación).

2.6. Estandarización.

Los protocolos que son implementados en sistemas de comunicación que tienen un amplio impacto suelen convertirse en estándares, debido a que la comunicación es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo pre-existente. Esto ocurre tanto de manera informal como deliberada. Existen consorcios empresariales, que tienen como propósito precisamente el de proponer recomendaciones de estándares que se deben respetar para asegurar la interoperabilidad de los productos.

Por ejemplo, la IEEE que propone varios estándares para redes físicas, o el W3C (World Wide Web Consortium) que gestiona la definición aceptada del HTTP (Hyper Text Transfer Protocol).

En el campo de las redes informáticas los protocolos se pueden dividir en varias categorías. Una de las clasificaciones más estudiadas es la OSI.

2.7. Modelo OSI.

El modelo OSI es la propuesta que hizo la Organización Internacional para la Estandarización (ISO) para estandarizar la interconexión de sistemas abiertos. Un sistema abierto se refiere a que es independiente de una arquitectura específica. El modelo se compone de un conjunto de estándares ISO relativos a las comunicaciones de datos.

Este modelo está dividido en las siguientes siete capas:

1. Capa física
2. Capa de enlace de datos
3. Capa de red
4. Capa de transporte
5. Capa de sesión
6. Capa de presentación
7. Capa de aplicación

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia

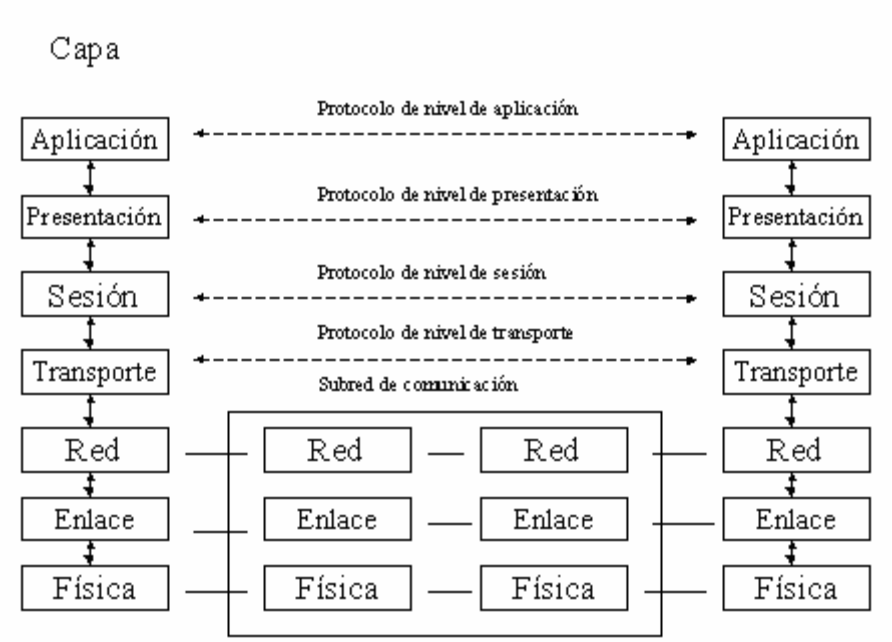


Figura 1. Arquitectura de red basada en el modelo OSI

En este modelo, solo las capas que tengan otra capa equivalente en el nodo remoto podrán comunicarse, esto es, solo las capas que son iguales entre si se comunican.

El protocolo de cada capa solo se interesa por la información de su capa y no por la de las demás, por ejemplo: El e-mail es un protocolo de aplicación que se comunica solo con otros protocolos del mismo tipo. Por lo tanto, la aplicación e-mail no se interesa si la capa física es una ethernet o un modem.

La información se pasa a las capas de abajo hasta que la información llega a la red. En el nodo remoto, la información es entonces pasada hacia arriba hasta que llega a la aplicación correspondiente. Cada capa confía en que las demás harán su trabajo, una capa no se interesa por el funcionamiento de las demás, lo único que es de interés es la forma en como los datos serán pasados hacia arriba o hacia abajo. La forma de lograr esto es empaquetando y desempaquetando información en los mensajes que se van a enviar, así el e-mail le da una información a la capa de TCP, la

cual agrega información y se la pasa a la capa de IP, la cual agrega más información y se la pasa a la de Ethernet, la cual agrega mas información y la transmite a la red. Si seguimos este método de empaquetar y desempaquetar llegará un momento en que a las capas mas altas casi no llega información, este es uno de los aspectos que la capa de transporte y sesión tienen que resolver.

2.7.1. Capa física.

La capa física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio (cable conductor, fibra óptica o inalámbrico); características del medio (por ejemplo tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) como a la forma en la que se transmite la información (codificación de señal, niveles de tensión/corriente eléctrica, modulación, tasa binaria, etc.) Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es unidireccional o bidireccional (simplex, duplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas. Se encarga también de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión y viceversa, es decir, transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Las principales funciones de la capa física se resumen a continuación:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

2.7.1.1. Codificación de la señal.

El nivel físico recibe una trama binaria que debe convertir a una señal electromagnética, de tal forma que a pesar de la degradación que pueda sufrir en el medio de transmisión vuelva a ser interpretable correctamente en el receptor. En el caso más sencillo el medio es directamente digital, como en el caso de las fibras ópticas, dado que por ellas se transmiten pulsos de luz. Cuando el medio no es digital hay que codificar la señal. En los casos más sencillos la codificación puede ser por pulsos de tensión (PCM o Pulse Code Modulatión). Otros medios se codifican mediante presencia o ausencia de corriente. En general estas codificaciones son muy simples y sacan provecho de la capacidad de medio. Cuando se quiere sacar más partido al medio se usan técnicas de modulación más complejas, y suelen ser muy dependientes de las características del medio concreto.

En los casos más complejos, como suelen ser las comunicaciones inalámbricas, se pueden dar modulaciones muy sofisticadas, este es el caso de los estándares Wi-Fi, con técnicas de modulación complejas de espectro ensanchado.

2.7.1.2. Medios compartidos y topologías más comunes.

Los medios compartidos más comunes son los siguientes:

Entorno de medios compartidos: Los entornos de medios compartidos se producen cuando múltiples nodos tienen acceso al mismo medio. Por ejemplo, si varios PC se encuentran conectados al mismo cable físico, a la misma fibra óptica, o si comparten el mismo espacio aéreo, entonces se dice que comparten el mismo entorno de medios.

Entorno extendido de medios compartidos: Es un tipo especial de entorno de medios compartidos, en el que los dispositivos de interconexión pueden extender el entorno para que se pueda implementar múltiple acceso o más usuarios.

Entorno de red punto a punto: se emplea típicamente para las conexiones de acceso telefónico a redes. Se trata de un entorno de interconexión compartido en el que cada dispositivo se conecta a otro dispositivo único a través de un enlace.

Indirectamente el tipo de conexión que se utiliza en la capa física puede influir en el diseño de la capa de enlace. Atendiendo al número de equipos que comparten un medio existen dos posibilidades:

- Conexiones punto a punto: que se establecen entre dos equipos y que no admiten ser compartidas por terceros
- Conexiones multipunto: en las que dos o más equipos pueden usar el medio.

Así por ejemplo la fibra óptica no permite fácilmente conexiones multipunto y por el contrario las conexiones inalámbricas son inherentemente multipunto. Hay

topologías como el anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto.

La técnica utilizada para lograr que los nodos sobre la red accedan al cable ó medio de comunicación y así evitar que dos o más estaciones intenten transmitir simultáneamente es realizada por la capa de enlace.

La topología de red es la disposición física en la que se conecta una red de computadoras. Si una red tiene diversas topologías se llama mixta.

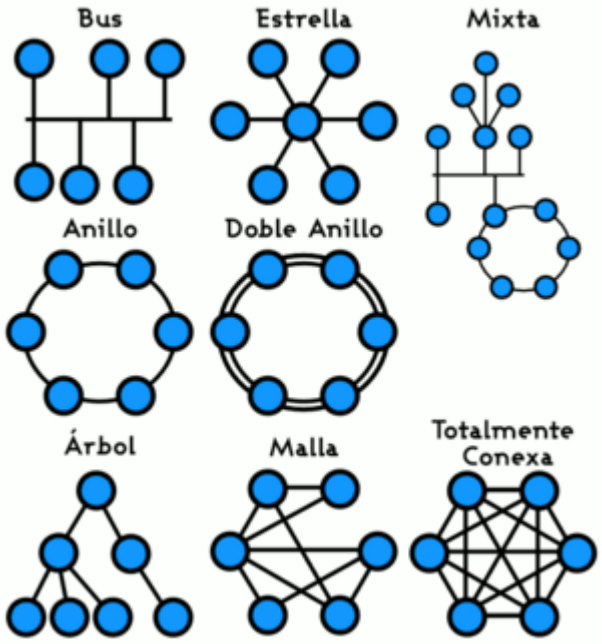


Figura 2. Topologías de red

La red en anillo es la topología de red en la que las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo. En este tipo de red la comunicación se da por el paso de un *token* o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de

información, de esta manera se evita la perdida de información debido a colisiones. Cabe mencionar que si algún nodo de la red se cae (termino informático para decir que esta en mal funcionamiento o no funciona para nada) la comunicación en todo el anillo se pierde.

La red en malla es una topología de red en la que cada nodo está conectado a uno o más nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. La red de malla se utiliza cuando no debe existir ninguna interrupción en las comunicaciones.

La red en bus es la topología de red en la que todas las estaciones están conectadas a un único canal de comunicaciones por medio de unidades de interfaz y derivadores. Las estaciones utilizan este canal para comunicarse entre si.

En la red estrella las estaciones están conectadas directamente al servidor y todas las comunicaciones se han de hacer necesariamente a través de él. Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí. Esta red crea una mayor facilidad de supervisión y control de información ya que todos los mensajes deben pasar por el *hub* o concentrador, el cual gestiona la redistribución de la información a los demás nodos.

En la red en árbol los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es una serie de redes en estrella interconectadas. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones. Cuenta con un cable principal (backbone) al que hay conectadas redes individuales en bus.

2.7.2. Capa de enlace de datos.

La capa de enlaces de datos a partir de cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También debe incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor. Ejemplos de este tipo de capa son: Ethernet, Token Ring, ATM.

2.7.3. Capa de red.

La función de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir, se encarga de encontrar un camino, manteniendo una tabla de enrutamiento, para hacer llegar los datos al destino. Los equipos encargados de realizar este enrutamiento se denominan enrutadores o *routers*.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo degrada toda la red (similar a un atasco en un cruce importante en una ciudad). Ejemplos de esta capa de red son: IP e IPX.

2.7.4. Capa de transporte.

Esta capa acepta los datos de la capa de sesión, los divide si es necesario, y los pasa a la capa de red asegurándose que llegan bien a su destino. También aísla a las capas superiores de cambios en el hardware de comunicaciones. Es la parte

encargada de garantizar la calidad de la transmisión de datos. En ella podemos encontrar los protocolos UDP, TCP y SPX.

2.7.5. Capa de sesión.

El objetivo básico de la capa de sesión es gestionar una sesión de trabajo, es decir que debe dar un servicio orientado a conexión a pesar de las capas inferiores. Es la encargada de gestionar conexiones y reconexiones de manera que presente a las capas superiores una sesión sin interrupciones.

2.7.6. Capa de presentación.

La función de la capa de presentación es representar la información de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, unicode, EBCDIC), números (little-endian tipo intel, big-endian tipo motorola), sonido o imágenes, los datos lleguen de manera reconocible. Para conseguir este objetivo se describió una posible notación de sintaxis abstracta (ASN.1), que se utiliza internamente en los MIB de SNMP (protocolo de gestión de red, para supervisar equipos de comunicaciones a distancia). Otra sintaxis es el formato de representación de enteros (Network Byte Order) de la pila TCP/IP, que define los datos en orden bing-endian.

2.7.7. Capa de aplicación.

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de archivos. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece continuamente. Entre los protocolos más conocidos destacan:

- HTTP (HyperText Transfer Protocol)
- FTP (File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP (Post Office Protocol)
- SSH (Secure SHell)
- Telnet

Los siguientes protocolos de nivel de aplicación facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name Server)

2.8. Ethernet.

La norma o estándar Ethernet determina la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla de versiones futuras de 40 Gbps y 100 Gbps. Utiliza el protocolo de comunicaciones CSMA/CD (Carrier Sense Multiple Access / Collision Detect - Acceso múltiple con detección de portadora y detección de colisiones). Actualmente Ethernet es el estándar más utilizado en redes locales entre otras.[4]

Ethernet fue creado por Robert Metcalfe en Xerox Parc, centro de investigación de Xerox para interconectar computadoras. El diseño original

[4] Wikipedia en Español [en Línea] <http://es.wikipedia.org/wiki/Ethernet>. [Consulta: 2005].

funcionaba a 1 Mbps sobre cable coaxial grueso con conexiones vampiro (que "muerden" el cable). Para la norma de 10 Mbps se añadieron las conexiones en coaxial fino (10Base2), con tramos conectados entre si mediante conectores BNC, par trenzado categoría 3 (10BaseT) con conectores RJ45 mediante el empleo de *hubs* y con una configuración física en estrella e incluso una conexión de fibra óptica (10BaseF). Los estándares sucesivos (100 Mbps o Fast Ethernet, Gigabit Ethernet 10 Gbps) utilizan únicamente los cables de par trenzado sin apantallar (UTP - Unshielded Twisted Pair), de al menos categoría 5 y la fibra óptica.

IEEE 802.3 es el nombre de un comité de estandarización del IEEE y por extensión se denominan así los estándares por él producidos. La primera versión fue un intento de estandarizar ethernet aunque hubo un campo de la cabecera que se definió de forma diferente. Posteriormente hubo actualizaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits), redes virtuales, concentradores, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial). Los estándares de este grupo no reflejan necesariamente lo que se usa en la práctica, aunque a diferencia de otros grupos suele estar cerca de la realidad.

Las estaciones de una LAN de tipo CSMA/CD pueden acceder a la red en cualquier momento. Antes de enviar datos, las estaciones CSMA/CD escuchan a la red para determinar si se encuentra en uso. Si lo está, entonces esperan. Si la red no se encuentra en uso, las estaciones comienzan a transmitir. Una colisión se produce cuando dos estaciones escuchan para saber si hay tráfico de red, no lo detectan y, acto seguido transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde. Los algoritmos de postergación determinan el momento en que las estaciones que han tenido una colisión pueden volver a transmitir. Las estaciones CSMA/CD pueden detectar colisiones, de modo que saben en qué momento pueden volver a transmitir.

Las LAN Ethernet son redes de broadcast. Esto significa que cada estación puede ver todas las tramas, aunque una estación determinada no sea el destino propuesto para esos datos. Cada estación debe examinar las tramas que recibe para determinar si corresponden al destino. De ser así, la trama pasa a una capa de protocolo superior dentro de la estación para su adecuado procesamiento.

2.9. Hardware comúnmente utilizado en una red Ethernet.

El hardware comúnmente utilizado en una red Ethernet es el siguiente:

- NIC, o adaptador de red Ethernet: Permite el acceso de una computadora a una red. Cada adaptador posee una dirección MAC que la identifica en la red y es única.
- Una computadora conectada a una red se denomina nodo.
- Repetidor o *repeater*: Aumenta el alcance de una conexión física, disminuyendo la degradación de la señal eléctrica en el medio físico
- Concentrador o *hub*: Funciona como un repetidor, pero permite la interconexión de múltiples nodos, además cada mensaje que es enviado por un nodo, es repetido en cada punto el hub.
- Puente o *bridge*: Interconectan segmentos de red, haciendo el cambio de tramas (frames) entre las redes de acuerdo con una tabla de direcciones que dice en que segmento está ubicada una dirección MAC.
- *Switch* o conmutador: Funciona como el *bridge*, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los conmutadores pueden tener otras funcionalidades, como redes virtuales y permiten su configuración a través de la propia red.
- Enrutador o *router*: Funciona en una capa de red más alta que los anteriores, el nivel de red como en el protocolo IP por ejemplo. Realiza el enrutamiento de paquetes entre las redes interconectadas. A través de tablas y algoritmos de enrutamiento, un enrutador decide el mejor camino

que debe tomar un paquete para llegar a una determinada dirección de destino.

2.10. Colisiones y dominios de colisión.

Uno de los problemas que se pueden producir, cuando dos tramas se propagan al mismo tiempo en la misma red, es una colisión. En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadores envíen mensajes, cada uno por turnos. Esto significa que ambas pueden mandar mensajes, pero sólo podría haber una trama en el sistema. El problema es que en las grandes redes hay muchos computadores conectados, cada uno de los cuales desea comunicar miles de millones de bits por segundo.

Se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si todos los dispositivos de la red están interconectados por medio de un solo cable, aumenta la probabilidad de que se produzcan conflictos cuando varios usuarios intenten enviar datos al mismo tiempo. Lo mismo sucede si los segmentos de una red están conectados únicamente con dispositivos no filtrantes tales como repetidores. Ethernet permite que sólo un paquete de datos a la vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

En general, las colisiones degradan el rendimiento de la red. Sin embargo, una cierta cantidad de colisiones constituye una función natural de un entorno de medios compartidos (es decir, un dominio de colisión). Esto ocurre cuando una gran cantidad de computadores tratan de comunicarse entre sí al mismo tiempo utilizando el mismo cable.

El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión e incluye todos los entornos de medios compartidos.

Por ejemplo, un alambre puede estar conectado con otro a través de cables de conexión, paneles de conexión, repetidores e incluso concentradores. Todas estas interconexiones de capa 1 forman parte del dominio de colisión. Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

La historia de la forma en que Ethernet administra las colisiones y los dominios de colisión se remonta a las investigaciones que se llevaron a cabo en la Universidad de Hawai. En su intento por desarrollar un sistema de comunicaciones inalámbricas para las islas de Hawai, los investigadores universitarios desarrollaron un protocolo denominado Aloha. Este protocolo fue fundamental para el desarrollo de Ethernet. Los repetidores regeneran y retemporizan los bits, pero no pueden filtrar el flujo de tráfico que pasa por ellos. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. El uso de repetidor extiende el dominio de colisión, por lo tanto, la red a ambos lados del repetidor es un dominio de colisión de mayor tamaño.

Cualquier señal que entre a un puerto del concentrador se regenera, retemporiza y se envía desde todos los demás puertos. Por lo tanto, los concentradores, son útiles para conectar grandes cantidades de computadores ya que extienden los dominios de colisión. El resultado final es el deterioro del rendimiento de la red si todos los computadores en esa red exigen anchos de banda elevados, simultáneamente.

Si bien los repetidores y los concentradores son dispositivos de interconexión útiles y económicos, tienen la desventaja de extender los dominios de colisión. Si se extiende demasiado el dominio de colisión, pueden producirse demasiadas colisiones y puede verse afectado el rendimiento de la red. Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de

interconexión que dividan los dominios. Los puentes, conmutadores y enrutadores son ejemplos de este tipo de dispositivo de interconexión. Este proceso se denomina segmentación. Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación. El tráfico entre los dispositivos del mismo segmento no cruza el puente ni afecta a otros segmentos. Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado pesado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación.

2.11. Segmentación de la LAN Ethernet.

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, se congestionará rápidamente con tráfico y colisiones y virtualmente no ofrecerá ningún ancho de banda. La adición de dispositivos como, puentes, conmutadores y enrutadores dividen la LAN en dominios de colisión.

Un puente o conmutador reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico. Ambos dispositivos actúan como un *firewall* ante algunos errores de red potencialmente perjudiciales. También aceptan la comunicación entre una cantidad de dispositivos mayor que la que se soportaría en cualquier LAN única conectada al puente. Los puentes y los conmutadores amplían la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

Aunque los puentes y los conmutadores comparten los atributos más importantes, todavía existen varias diferencias entre ellos. Los conmutadores son

significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un conmutador. Los conmutadores pueden soportar densidades de puerto más altas que los puentes. Algunos conmutadores soportan la conmutación por el método *cut-through*, que reduce la latencia y los retardos de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). Por último, los conmutadores reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

La segmentación por enrutadores brinda todas estas ventajas e incluso otras adicionales. Cada interfaz del enrutador se conecta a una red distinta, de modo que al insertar el enrutador en una LAN se crean dominios de colisión y de *broadcast* más pequeños. Esto sucede porque los enrutadores no envían los *broadcasts* a menos que sean programados para hacerlo. Sin embargo, el enrutador puede ejecutar las funciones de puenteo y conmutación. El enrutador puede ejecutar la selección de mejor ruta, además, se puede usar para conectar distintos medios de interconexión y distintas tecnologías LAN simultáneamente. Los enrutadores pueden conectar las LAN que ejecutan distintos protocolos (IP vs. IPX vs. AppleTalk) y pueden tener conexiones seriales con las WAN.

Una LAN que usa una topología Ethernet de conmutación crea una red que funciona como si sólo tuviera dos nodos: el nodo emisor y el nodo receptor. Una LAN Ethernet conmutada permite que la topología LAN funcione más rápida y eficientemente que una LAN Ethernet estándar, ya que usa el ancho de banda de modo más eficiente. En una implementación Ethernet conmutada, el ancho de banda disponible puede alcanzar casi un 100%.

Es importante observar que aunque el 100% del ancho de banda puede estar disponible, las redes Ethernet tienen un mejor rendimiento cuando se mantiene por debajo del 40% de la capacidad total. Esta limitación se debe al método de acceso al medio de Ethernet (CSMA/CD). El uso de ancho de banda que supere el límite recomendado tiene como resultado un aumento en la cantidad de colisiones. El propósito de las LAN conmutadas es aliviar las insuficiencias de ancho de banda y los cuellos de botella de la red como, por ejemplo, los que se producen entre un grupo de PC y un servidor de archivos remoto. Un conmutador LAN es un puente multipuerto de alta velocidad que tiene un puerto para cada nodo o segmento de la LAN. El conmutador divide la LAN en microsegmentos, creando dominios libres de colisiones a partir de un dominio de colisión que antes era de mayor tamaño.

La Ethernet conmutada se basa en la Ethernet estándar. Cada nodo está directamente conectado a uno de sus puertos, o a un segmento que está conectado a uno de los puertos del conmutador. Esto crea una conexión de 100 Mbps entre cada nodo y cada segmento del conmutador. Un computador conectado directamente a un conmutador Ethernet está en su propio dominio de colisión y tiene acceso a los 100Mbps completos. Cuando una trama entra a un conmutador, se lee para obtener la dirección origen o destino. Luego, el conmutador determina cuál es la acción de conmutación que se llevará a cabo basándose en lo que sabe a partir de la información que ha leído en la trama. Si la dirección destino se encuentra ubicada en otro segmento, la trama se conmuta a su destino.

Los enrutadores son más avanzados que los puentes típicos. Un puente es pasivo (transparente) en la capa de red y funciona en la capa de enlace de datos. Un enrutador funciona en la capa de red y basa todas sus decisiones de envío en la dirección de protocolo de capa 3. El enrutador logra esto examinando la dirección destino del paquete de datos y buscando las instrucciones de envío en la tabla de enrutamiento. Los enrutadores producen el nivel más alto de segmentación debido a su capacidad para determinar exactamente dónde se debe enviar el paquete de datos.

Como los enrutadoress ejecutan más funciones que los puentes, operan con un mayor nivel de latencia. Los enrutadores deben examinar los paquetes para determinar la mejor ruta para enviarlos a sus destinos. Inevitablemente, este proceso lleva tiempo e introduce retardo.

2.12. Ethernet Half y Full Duplex.

Ethernet es una tecnología half duplex. Cada nodo de Ethernet verifica la red para comprobar si los datos se están transmitiendo. Si la red está en uso, la transmisión se retarda. A pesar del retardo de la transmisión, dos o más nodos Ethernet pueden transmitir al mismo tiempo, dando como resultado una colisión. Cuando se produce una colisión, el nodo que detecta primero la colisión envía una señal de atascamiento. Al escuchar la señal de atascamiento, cada nodo espera durante un lapso de tiempo aleatorio antes de intentar la transmisión. El algoritmo de postergación de la NIC genera este período al azar. A medida que más nodos se agregan a la red y empiezan a transmitir, es más probable que se produzcan colisiones.

Las LAN Ethernet se saturan porque los usuarios ejecutan software que utiliza intensamente la red, como aplicaciones cliente/servidor que hacen que las estaciones de trabajo deban transmitir con mayor frecuencia y durante períodos de tiempo más prolongados.

La Ethernet *full duplex* permite la transmisión y recepción de un paquete distinto al mismo tiempo. Esta transmisión y recepción simultánea requiere del uso de dos pares de hilos dentro del cable y una conexión conmutada entre cada nodo. Esta conexión se considera punto a punto y está libre de colisiones. Debido a que ambos nodos pueden transmitir y recibir al mismo tiempo, no existen negociaciones por el ancho de banda. La Ethernet full duplex puede utilizar un medio compartido existente siempre y cuando el medio cumpla con los estándares Ethernet mínimos.

Para transmitir y recibir de forma simultánea, se necesita un puerto dedicado para cada nodo. La conexiones full duplex pueden utilizar medios 10BASE-T, 100BASE-TX o 100BASE-FX para crear conexiones punto a punto. Las tarjetas de interfaz de red (NIC) ubicadas a ambos extremos deben tener capacidades full duplex.

El conmutador Ethernet full duplex aprovecha los dos pares de hilos que se encuentran dentro del cable. Esto se realiza creando una conexión directa entre el transmisor (TX) en un extremo del circuito y el receptor (RX) en el otro extremo. Con estas dos estaciones conectadas de esta manera, se crea un dominio libre de colisiones debido a que se produce la transmisión y la recepción de los datos en circuitos separados no competitivos.

Ethernet generalmente puede usar únicamente entre el 50% y el 60% del ancho de banda de 10-Mbps disponible debido a las colisiones y la latencia. Ethernet full duplex ofrece 100% del ancho de banda en ambas direcciones. Esto produce un rendimiento potencial de 20-Mbps: 10-Mbps TX y 10-Mbps RX.

2.13. Los Conmutadores interconectando LAN y WAN.

Es posible que dos o más LAN estén separadas geográficamente y estas se tengan que interconectar a través de un enlace WAN.

Hay varias situaciones donde aparecen estas situaciones:

- Una organización con múltiples localidades y múltiples usuarios en cada sitio, y todos requieren interconexión para varias aplicaciones.
- La empresa esta en una ubicación central y algunas sucursales u oficinas remotas necesitan conexión hacia la organización central.

- La organización necesita darle soporte individual a sitios remotos, como por ejemplo trabajadores remotos.[5]

Hay algunas diferencias entre las tecnologías utilizadas en las LAN y WAN y algunos de los factores importantes involucrados en la toma de decisiones en cuanto a las tecnologías a utilizar son las siguientes:

Tasa de Datos (Data Rate): En general, los enlaces WAN ofrecen bajas tasas de transmisión de datos para las LAN que interconectan. Mientras que las LAN operan a 10, 100 o 1000 Mb/s o más, el típico enlace remoto opera en el orden de 1 o 2 Mb/s (T1/E1/Frame Relay). Mientras la tasa del enlace aumenta en general los costos asociados a este aumentan también.

Tasa de Error (Error Rate): La tasa de error en los enlaces WAN por lo general es mayor que la que se presentan en las LAN, esto causa un impacto en los protocolos de las capas superiores y aplicaciones que están asumiendo la baja tasa de pérdida de tramas asociadas a los enlaces LAN.

Costos: En una LAN, el ancho de banda es esencialmente gratis. En una LAN operativa no causa costos el usar la capacidad disponible. Generalmente los enlaces WAN son entregados por un proveedor de servicios. El proveedor invierte capital en la instalación de las líneas y equipos para estos enlaces y necesita generar cargos para recuperar los costos agregados de mantenimiento. Mientras, que el ancho de banda de las LAN es gratis, el de las WAN cuesta dinero. Típicamente el costo es función de la tasa de datos y la distancia a ser cubierta

No hay forma directa de transformar una trama LAN en una trama WAN sin perder alguna información necesaria para entregar esta a sus destinatarios. Esto dio

---

[5] Seifert, Rich. The Switch Book, New Cork: Editorial John Wiley & Sons, Inc, 2000.

como resultado el encapsulado de las tramas de las LAN en un formato que permita la transmisión a través de la WAN.

Uno de los formatos más populares formatos para la transmisión de datos de forma serial sincrónica comúnmente usada en las WAN es el protocolo High-Level Data Link Control (HDLC), el cual provee un mecanismo para:

- Delimitar las tramas con el bit de sincronismo.
- Asignar dirección a las estaciones en el enlace
- Enlaces con control orientados a conexión, control de flujo y control de errores.

Las LAN ofrecen típicamente una tasa de error del orden de 10^{-12} o mejor, por la alta calidad de los cables y las relativas cortas distancias. Las WAN atraviesan largas distancias, y muchas veces atraviesan muchos equipos entre los puntos finales. Todos estos factores afectan negativamente la tasa de error de los enlaces WAN.

Las compañías proveedoras de los enlaces WAN ofrecen tasas de error peores que las que se encuentran en las LAN, y generalmente no hacen uso de algún esquema de detección y retransmisión como por ejemplo el control de errores de HDLC, por los retardos introducidos cuando los errores ocurren. En los enlaces con una tasa de error de pobre desempeño como por ejemplo los enlaces satelitales, se implementan esquemas de corrección de errores, donde dicha corrección ocurre transparente para el servicio usado en el canal, con un pequeño retardo a expensas de reducir la capacidad del canal.

La tasa de datos usada por las WAN son generalmente mucho menores que las LAN que interconectan, causando los siguientes efectos en el ancho de banda:

- El máximo ancho de banda en la conexión se reduce al del enlace WAN. No es posible mantener una transferencia de datos a una velocidad mayor que el enlace mas lento entre las estaciones.
- La entrega de tramas tiene un incremento en los retardos, causado porque la tasa de transmisión a través del enlace WAN es menor que en la LAN, traduciéndose en que se toma más tiempo en transmitir una trama en un enlace lento que en uno rápido. La trama más larga de Ethernet requiere 120µs para transmitirse en una red Ethernet 100Mb/s; en un enlace T1 la misma trama toma 7.9ms incrementándose por un factor de 66.
- Los enlaces WAN pueden ser un cuello de botella pues cuando el tráfico en las LAN aumenta los retardos se incrementan en los conmutadores al quedar en cola para salir en el conmutador remoto.

Algunos protocolos de las capas superiores están diseñados para operar en redes de área local y son sensibles a los retardos. Dos ejemplos de estos son Net-BIOS/NetBEUI y DEC LAT. Cuando se introduce un enlace WAN causa por lo general una falla general de estos protocolos. El comportamiento de aplicaciones que utilizan estos protocolos puede ser intermitente y difícil de diagnosticar.

2.14. Gestión de Red.

El término gestión (en inglés management) en general comprende los procesos de planeamiento, conducción, seguimiento y evaluación de un conjunto de decisiones y acciones, con el objeto de buscar la solución de distintos problemas y al mismo tiempo para lograr determinados objetivos en una organización. [6]

Gestión de Redes es un término muy amplio que implica coordinar recursos para planificar, organizar, diseñar, operar, contabilizar, controlar, analizar, evaluar y

[6] Mendillo Vincenzo, Material de apoyo, asignatura: Gestión de Redes. UCV, Noviembre 2.001.

expandir las redes de comunicaciones con el objeto de obtener niveles de servicio óptimos, a un costo razonable y con la máxima eficiencia.

Una actividad fundamental en la gestión de redes es la utilización de software y hardware para monitorear el estado de los equipos de la red y de los medios de transmisión, optimizando el desempeño de la red y tomando acciones para solucionar anomalías en el funcionamiento.

El campo de la gestión de redes históricamente ha estado atrapado entre dos tendencias que actualmente tienden a fundirse: gestión de redes de telecomunicaciones y gestión de redes de datos.

La primera tiene que ver con los equipos y sistemas de las redes de las compañías proveedoras de servicios, centrales telefónicas, líneas de abonados y troncales. La segunda tiene que ver con redes de computadoras (LAN y WAN) que incorporan enrutadores, conmutadores, modems, servidores, estaciones de trabajo, PCs, impresoras, etc. Pero actualmente es usual que las redes de computadores incluyan servicios de telecomunicaciones privados o públicos, al mismo tiempo que las redes de telecomunicaciones incluyen algunas capacidades de computación en PBXs, conmutadores y otros sistemas terminales. Por lo tanto el alcance de la gestión de redes ha ido unificando y ampliando ambas tendencias para así incluir equipos de telecomunicaciones, redes de datos, sistemas de computación y los servicios de transmisión y procesamiento de datos. El desarrollo acelerado de las tecnologías de redes, aunado a la coexistencia de productos de diferentes proveedores (ambientes multiproveedor), hacen que la gestión de redes sea cada vez más compleja. Por esta razón, las empresas y los propios proveedores de enlaces se han visto en la necesidad de implantar sistemas que faciliten la gestión.

Con la introducción del modelo de interconexión de sistemas abiertos tomado como base para la normalización abierta, se planteó la posibilidad de establecer criterios y procedimientos para la gestión de las redes.

En OSI se hace una clasificación de las funciones de gestión de la red en 5 áreas funcionales básicas para así facilitar el diseño e implantación de los sistemas de gestión. Estas funciones que se enumeran a continuación deberían ser parte de todo sistema de gestión inicial, con previsión para implantar funciones adicionales en el futuro:

1. Gestión de Fallas
2. Gestión de Configuración
3. Gestión de Desempeño
4. Gestión de Seguridad
5. Gestión de Contabilidad

Estas 5 áreas funcionales son conocidas y fácilmente recordadas en inglés como FCAPS (failure, configuration, accountability, performance, security)

2.15. Gestión de Fallas (Averías).

La gestión de fallas tiene que ver con la detección, aislamiento y corrección de operaciones anormales de la red. Una falla o alarma es el indicador de un desperfecto potencial o real que podría suscitarse como consecuencia de un evento, siendo el evento un cambio de estado producido en algún punto del dominio bajo gestión. Un evento puede generar el accionamiento de múltiples alarmas, pero el sistema de gestión debe tener la capacidad de discernir y presentar la multitud de alarmas como una sola alarma que identifica el problema en cuestión. El sistema de gestión debe tener la capacidad de permitir la configuración y reconfiguración de estas relaciones entre alarmas y eventos, según la preferencia de la empresa operadora

de la red, o en función de los cambios producidos en la estructura de la misma. Asimismo, el bloque de funciones de eventos debería tener la capacidad de registrar todos los eventos, pero presentando sólo los mensajes relevantes que conciernen a los diferentes niveles de administración.

2.16. Gestión de Configuración.

La gestión de configuración ofrece mecanismos para la gestión de los elementos de la red (también denominados entidades ú objetos), que se encuentran bajo el control del sistema de gestión. Se deberá contar con las posibilidades para realizar tareas como las siguientes:

- Modificar la configuración
- Inicializar objetos, apagarlos, ó ponerlos fuera de servicio
- Recopilar datos sobre el estado en forma periódica o no (por ejemplo, a petición del supervisor de la red).
- Proveer los servicios y recursos que se requieran para satisfacer la demanda de tráfico.

2.17. Gestión de Desempeño.

La gestión de desempeño tiene que ver con la evaluación del comportamiento de la red. Se encarga de recoger datos estadísticos, mediante el monitoreo, que puedan servir de base tanto para la planificación a largo plazo como para los pronósticos de tendencias a corto plazo.

El monitoreo de la calidad de funcionamiento exige mantener registros de entidades y estados, con el fin de detectar posibles problemas (por ejemplo congestión), así como para efectuar el ajuste de los recursos de la red en respuesta a las tendencias observadas. Por lo tanto a partir de estos datos o registros se podrán

realizar estimaciones de la calidad de servicio (QoS, Quality of Service). Otra función de la gestión de desempeño es la utilización de los datos históricos para pronosticar fallas en los equipos y enlaces con el fin de aplicar medidas de mantenimiento preventivo para aumentar la disponibilidad de la red.

2.18. Gestión de Seguridad.

Esta se puede dividir en tres partes principales:

- La seguridad física, que tiene que ver con la seguridad de los equipos y de las edificaciones donde ellos residen.
- La seguridad de acceso, que se ocupa de permitir el acceso por parte de los usuarios autorizados y controlar lo que les está permitido hacer.
- La seguridad de datos, que involucra el resguardo de los datos contra daños.

2.19. Gestión de Contabilidad.

Se trata del conjunto de funciones que permite la identificación de los recursos utilizados y la cuantificación de los costos para el eventual cobro a los usuarios en virtud de la utilización hecha de los servicios y de los recursos de la red. En las redes públicas la gestión de contabilidad participa en la elaboración de las facturas para los clientes y en el seguimiento de los pagos. También tiene que ver con la venta de los recursos de la red.

Si bien el esquema de OSI en áreas funcionales es útil desde el punto de vista conceptual, existen otros esquemas que se utilizan más a menudo en la práctica.

En los Estados Unidos es muy popular el esquema de ANSI (American National Standards Institute) conocido como OAM&P (Operation, Administration, Maintenance and Provisioning).

En Europa se usa el esquema de ETSI (European Telecommunications Standards Institute) y conocido como OAM (Operation, Administration and Maintenance), el cual es ligeramente distinto de OAM&P, ya que el aprovisionamiento forma parte de las áreas de servicio y de negocio.

Un tercer esquema es el CNM (Customer Network Management), el cual originalmente era un subconjunto de las funciones de TMN (Telecommunications Management Network) relativas a los clientes y usuarios.

2.20. Modos Operacionales.

Las actividades de la gestión de redes se pueden agrupar en dos modos operacionales:

Control de red: se refiere a la alteración de parámetros en los diferentes dispositivos de la red y a la ejecución de acciones predeterminadas para esos dispositivos. Debido a consideraciones de seguridad, por lo general esta función no está a libre disposición de los usuarios de las redes.

Monitoreo de la red: se refiere a la observación y análisis del estado y comportamiento de los componentes de la red. Es fundamental para la gestión de la red.

2.21. Estándar de gestión.

Virtualmente todos los sistemas distribuidos incluyen equipos de múltiples fabricantes. Para controlar costos y hacer práctica la gestión integrada de la red, es necesario contar con facilidades de gestión estandarizadas que puedan ser utilizadas en ambientes multiproveedor y una amplia gama de tipos de productos (enrutadores,

puentes, estaciones de trabajo, etc). En respuesta a esto, se han desarrollado 2 estándares básicos:

Familia SNMP: Tiene que ver con el conjunto de estándares para gestión de redes del ambiente internet e incluye protocolos, y especificaciones de la estructura de bases de datos del conjunto de definiciones de objetos gestionados. SNMP es el estándar adoptado para las redes TCP/IP desde 1989. A mediados de 1988, el Consejo de Actividades de Internet (Internet Activities Board - IAB) se reunió para elaborar las recomendaciones para el desarrollo de un protocolo de gestión. Los resultados de esta reunión fueron publicados en el RFC 1052. Ese mismo año la Fuerza de Tareas de Ingeniería de Internet (Internet Engineering Task Force - IETF) designó un grupo que comenzaría a trabajar en el desarrollo de tal protocolo. A finales de 1988, la IETF publicó en el RFC 1098, las especificaciones del nuevo protocolo: SNMP (Simple Network Management Protocol. Con esta herramienta a disposición, diferentes proveedores de sistemas de computación (IBM, Hewlett-Packard, Racal, AT&T, Novell, etc) iniciaron labores para desarrollar sistemas de gestión basados en ese protocolo y a finales de la década de 1980 y comienzos de los 90s, fueron lanzados al mercado los primeros sistemas comerciales.

Sistema de gestión OSI: Desarrollado por ISO, se refiere a un amplio y complejo conjunto de estándares que definen una variedad de aplicaciones de gestión de propósito general, de los cuales el más nombrado es CMIP (Common Management Information Protocol). Debido a su complejidad y la lentitud en el proceso de estandarización, el sistema de gestión OSI ha ido ganando aceptación muy gradualmente. OSI tiene una visión más ambiciosa que SNMP. Además de definir una base de información de gestión y un protocolo, OSI define: las funciones básicas que utilizan al protocolo y la base de datos (Systems Management Functions - SMFs) y las cinco áreas funcionales de gestión (Systems Management Functional Areas - SMFAs).

2.22. Tecnologías aplicables.

Un gran número de tecnologías están adquiriendo importancia en el diseño y desarrollo de sistemas de gestión. Entre ellas se encuentran:

Tecnología orientada a objetos: proveen una herramienta poderosa para modelar recursos a ser administrados y para brindar soporte a la gestión distribuida. Con la creciente incorporación de capacidades orientadas a objeto en los sistemas operativos, el uso de esta tecnología en sistemas de gestión va a aumentar.

Inteligencia artificial: las técnicas de AI (Artificial Intelligence), en especial técnicas de sistemas expertos, pueden aligerar la carga de los administradores de red.

Simulación y modelado: en el área de desempeño, el administrador usualmente se encuentra sobrecargado con exceso de datos. Las herramientas de modelado y simulación permiten a los administradores utilizar estos datos para obtener una medida del rendimiento actual del sistema y predecir futuros comportamientos.

2.23. SNMP (Simple Network Management Protocol).

El protocolo SNMP se originó en 1988 a partir del protocolo SGMP (Simple Gateway Monitoring Protocol). Definido en RFC-1098, SNMP fue diseñado para optimizar el procesamiento de funciones simples sobre las que se construye el manejo de la red.

La arquitectura de SNMP incluye los siguientes componentes básicos:

MIB: base de datos de información de gestión.

Agente: software residente en el equipo a ser gestionado. Cada agente almacena datos de gestión y responde a las peticiones de datos por parte de la estación de gestión. Los agentes ejecutan dos funciones básicas: inspección y modificación de variables MIB. Usualmente, la inspección de variables significa examinar los valores de contadores, umbrales, estados y otros parámetros, mientras que modificar significa cambiar los valores de las variables que inspecciona.

Manager (gestor): software residente en la estación de gestión la red. El gestor hace solicitudes al agente utilizando los comandos de SNMP. Los gestores ejecutan las funciones de la estación de gestión de la red y usualmente proveen una interfaz gráfica con el usuario, presentando un mapa de la red. Típicamente, almacenan datos MIB para análisis de tendencias. Algunos gestores pueden controlar simultáneamente múltiples agentes, mediante compiladores y exploradores de MIBs).

SNMP es un protocolo simple que contiene sólo dos comandos (GET y SET) para permitir a los gestores obtener el valor de una variable o almacenar un valor en una variable. La simplicidad de SNMP permite que las implantaciones de gestión de la red fueran llevadas a cabo rápidamente para satisfacer las necesidades inmediatas de Internet. Esta simplicidad permite además, que las implantaciones en los agentes sean más compactas y eficientes, permitiendo que los agentes utilicen la mayor parte de la memoria y recursos de procesamiento disponibles en llevar a cabo sus funciones primarias en vez de procesar peticiones del administrador.

No obstante su simplicidad, SNMP es un protocolo robusto, que se desenvuelve exitosamente ante condiciones adversas de la red. Es más importante para la gestión de una red trabajar bajo condiciones adversas que bajo condiciones normales, particularmente para gestión de fallas y desempeño, mientras se diagnostican y rectifican las causas que generaron tales condiciones.

Estas características de SNMP permiten que sea orientado a datagrama y basado en transacción. Siendo orientado a datagrama, permite la utilización de UDP como mecanismo de transporte y así se elimina la necesidad de establecer una conexión antes de la operación del protocolo. Además (por ser orientado a datagrama) no tiene conexión que pueda fallar bajo condiciones adversas. En contraparte, la orientación a datagrama impone que los mensajes SNMP sean enviados completamente en un datagrama, lo que se traduce en una limitante para la longitud de los mensajes.

SNMP utiliza dos puertos UDP: el puerto 161 lo abren los agentes para escuchar las peticiones del administrador y viceversa. El administrador también abre el puerto 162 para recibir los datos de los agentes.

2.24. Productos de gestión de red.

A continuación se va a hacer una presentación de las aplicaciones o subsistemas que se investigaron y estudiaron para conformar el sistema de gestión de red para la compañía BSP.

2.24.1. WhatsUp Professional.

Ipswitch WhatsUp Professional proporciona monitoreo detallado de la disponibilidad de la red y de su rendimiento. La encuesta proactiva de los dispositivos, desde una lista centralizada de los mismos, permite que el administrador monitoree el estado de la red, además de la aplicación de políticas alterables a gusto y alarmas. Entre las capacidades de monitoreo se incluyen:

- Servicios Windows (en sistemas NT, 2000, XP)
- Monitoreo de Puertos TCP/UDP

- Monitoreo de los recursos como el CPU, espacio de disco y memoria
- Registro de Eventos Windows y Syslog
- Capturas de SNMP
- El estado de los dispositivos puede ser codificado por color, ayudando a que el administrador se entere de algún problema con una simple mirada

Este paquete permite enterarse rápidamente de fallos en la red o de degradación del rendimiento con alertas alterables a gusto y políticas de acción. Envía alertas cuando surgen problemas o acelera aún más la resolución de los mismos con opciones como "reiniciar un dispositivo" o "iniciar un programa automáticamente". Permite maximizar el tiempo que la red está totalmente disponible, de las siguientes formas:

- Alertas vía e-mail, Pager, celular, SMS o alertas de audio
- Alertas en la bandeja de Tareas del Sistema
- Reenvío/Redirección de Capturas de SNMP
- Reinicio del servicio automático
- Visualización del estado o cambios del mismo desde cualquier explorador web (acceso remoto seguro tiene codificación SSL 128-bit)

Los ayudantes de instalación intuitivos, activan en el *WhatsUp Professional* buscadores de enrutadores, conmutadores, servidores, impresoras y cualquier otro dispositivo del entorno de red. Toda esta información es, entonces, almacenada dentro de una base de datos relacionable, para una fácil administración de los dispositivos y creación de los reportes. A su vez se puede personalizar para que:

- El administrador pueda crear grupos lógicos de los dispositivos y redes, para así ayudar en el monitoreo de áreas específicas de la red

- El administrador pueda visualizar la topología de su red en una lista o en un mapa.
- El administrador pueda alterar la manera en que visualiza su red a su gusto, con solo arrastrar y soltar, múltiples grupos de dispositivos y utilidades de diseño

WhatsUp Professional proporciona reportes en tiempo real y con opciones de formato histórico HTML, para fácil acceso y ajuste a gusto. El administrador puede compartir reportes detallados de disponibilidad o rendimiento para grupos de dispositivos o dispositivos específicos. Reportes flexibles pueden mostrar datos por mes, semana, día u hora. Entre las opciones de reportes se incluyen:

- Reporte de Disponibilidad (porcentaje de tiempo de respuesta)
- Reporte de Rendimiento (atraso en servicio o dispositivo)
- Reporte de Salud (reporte-resumen del status actual)
- Cronología de Cambio de Estado (histórico reciente de cambios en los dispositivos)

Los requerimientos de este sistema de gestión son:

- Servidor Windows 2003, Windows XP SP1 o superior, o Windows 2000
- 200 MB de espacio de disco
- 256 MB RAM
- Para utilizar la opción de notificación/alerta vía buscapersonas, es necesario un modem local y línea telefónica.

El costo de *Ipswitch WhatsUp Professional* es de $1495 e incluye la licencia del producto y 12 meses de soporte y actualizaciones. Su dirección web es http://www.ipswitch.com/products/whatsup/professional/index.asp

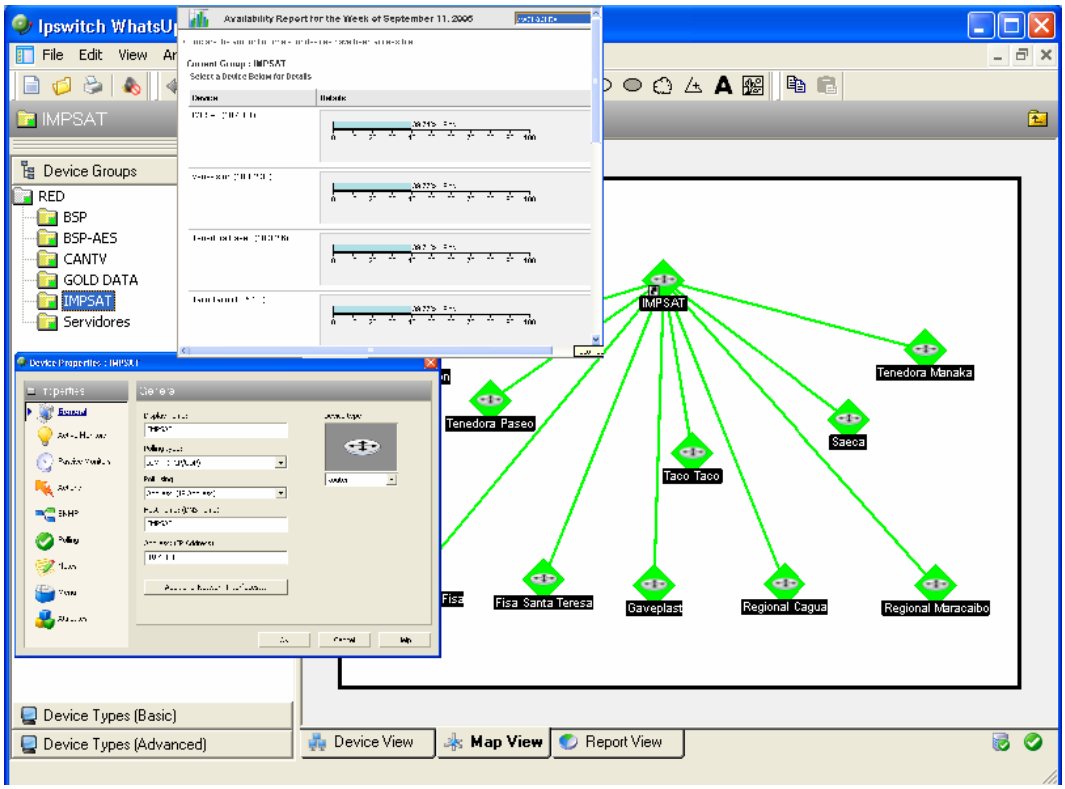


Figura 3. Pantalla de la aplicación “WhatsUp Professional”

2.24.2. Ethereal.

Ethereal es un potente analizador de protocolos de redes libre, para máquinas Unix o Windows. Permite capturar los datos directamente de una red u obtener la información a partir de una captura en disco (puede leer más de 20 tipos de formato distintos). Destaca también por su impresionante soporte de más de 300 protocolos, gracias sin duda a la licencia GPL y a sus más de 200 colaboradores de todo el mundo.

Permite examinar datos de una red en directo o de un archivo de captura en disco. Se pueden mostrar los datos capturados interactivamente, además de ver el resumen y el detalle para cada paquete. *Ethereal* tiene varias características muy

potentes, tales como un rico lenguaje de filtrado de salida de datos y la capacidad de ver un flujo de datos reconstruido de una sesión TCP.

Los requisitos de instalación son los siguientes: se necesita contar con una máquina que trabaje sobre tecnología NT; es decir, se tiene que ejecutar Ethereal-XTRA sobre un PC con Windows NT4, 2000 o XP en cualquiera de sus variantes. A través de un concentrador o switch gestionable con un puerto redirigido (mirroring), se debe obtener una copia de todos los paquetes que se mueven por la red.

Este software ofrece soporte para:

- Ethernet
- FDDI
- PPP
- Token-Ring
- IEEE 802.11 (redes inalambricas)
- Classical IP over ATM
- Loopback interfaces.

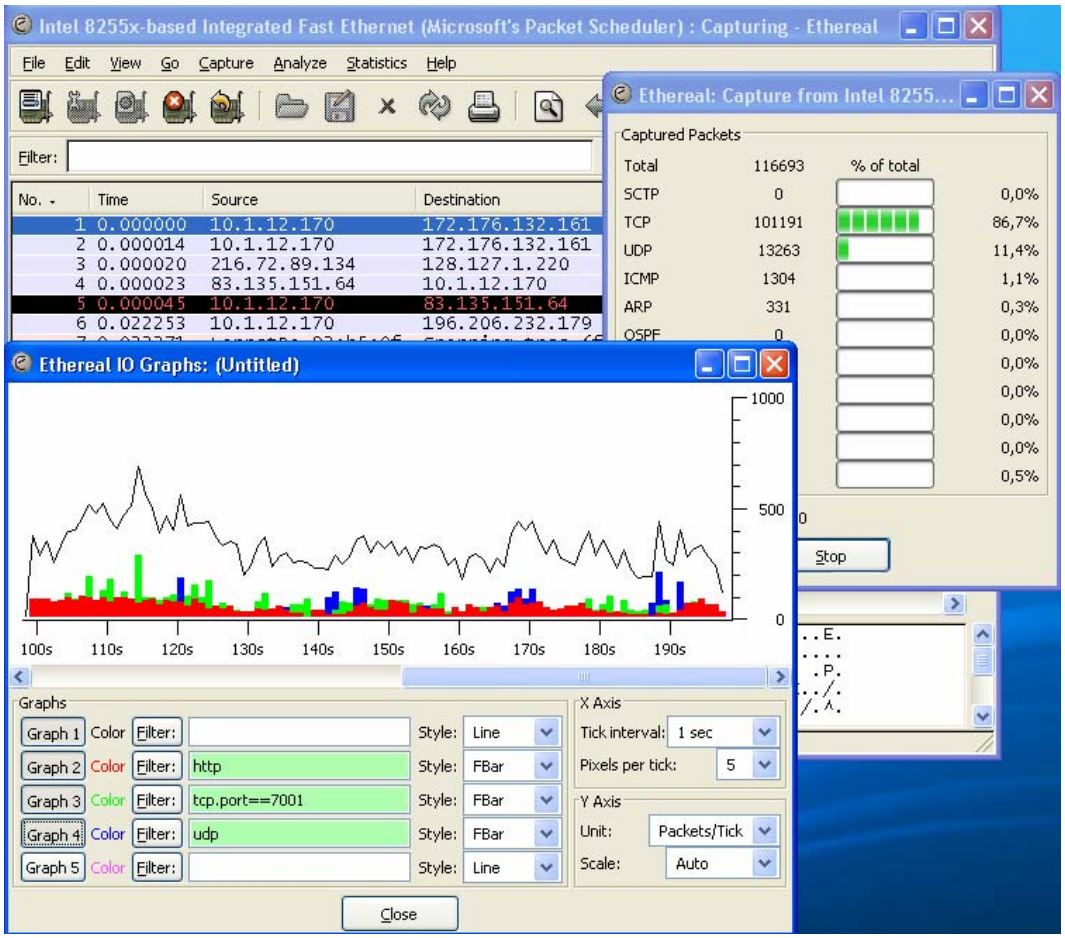


Figura 4. Pantalla de la aplicación Ethereal

2.24.3. Network Monitor 2.0 (SMS).

Network Monitor es una herramienta administrativa que permite monitorear el tráfico de la red en su paso por el cableado. Los analizadores de protocolo integrados en la herramienta, organizan el tráfico en paquetes de modo que éstos resulten más fáciles de analizar, y suministran información para localizar problemas con aplicaciones de red, estaciones de trabajo mal configuradas y protocolos innecesarios instalados en estaciones de trabajo, impresoras y servidores.

Network Monitor incluye diversos filtros de visualización, como una ayuda para colocar información específica en grandes trazados de red, filtros de captura para

limitar la información que captura la herramienta y activadores que permiten indicar al sistema qué acción debe emprender basándose en el contenido de un paquete.

Network Monitor para Windows 2000 se ofrece en dos versiones: una versión Lite, distribuida con Windows 2000, y una versión completa, que forma parte de Systems Management Server versión 2.0 (SMS o Servidor de administración de sistemas) y que también se puede instalar en Windows NT 4.0. La versión Lite sólo controla el tráfico local. La versión completa captura todo el tráfico de la red y, al conectarse a otro servidor o estación de trabajo en los que esté instalado el controlador de *Network Monitor*, permite controlar sistemas remotos. El controlador de *Network Monitor* se distribuye con Windows 2000 y no requiere la instalación de SMS. Para utilizar la versión completa de Network Monitor sin instalar SMS, se debe ejecutar el programa setup.exe del directorio \nmext del CD-ROM de Microsoft Systems Management Server 2.0.

2.24.4. NTOP.

Ntop significa Network TOP, y muestra el uso de la red. Es uno de los programas más completos en el monitoreo de redes, y además es GNU.

Los protocolos que es capaz de monitorear son: TCP, UDP, ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

Una vez instalado se puede ver lo que pasa por la red visitando la página web http://localhost:3000/, o httpS://localhost:3003/. El menú de navegación principal se encuentra en el marco de arriba, y permite ver las siguientes opciones:

- About: Muestra una explicación del programa, así como los créditos de las personas que lo han hecho.

- Data Rcvd, Data Sent: Enseña que datos se han recibido/transmitido.
- Stats: Es el apartado de estadísticas, enseña información muy completa acerca del estado de la red. Muestra si el tráfico es unicast, o multicast, la longitud de los paquetes, el TTL (tiempo de vida del paquete), y el tipo de tráfico que viaja (todo ello en porcentajes). También saca un listado de dominios, y qué plugins podemos activar o desactivar.
- IP Traffic: Da información acerca del sentido del tráfico, si va de la red local a una red remota, o viceversa.
- IP Protocolos: Da estadísticas del uso de los protocolos en tránsito, discriminando por grupos locales o remotos de los host.
- Admin: Sirve para poder cambiar la interfaz de red, crear filtros, y un mantenimiento de usuarios.

Resumiendo es una herramienta que no puede faltar al administrador de red, porque además de monitorear todo lo que pasa en la red, es capaz de ayudar a la hora de detectar malas configuraciones de algún equipo (esto salta a la vista porque al lado del *host* sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio.

2.24.5. Network Inspector (Fluke Networks).

Network inspector es una solución que realiza un seguimiento y diagnostico de forma activa de los problemas en entornos TCP/IP, IPX y NetBIOS. Network Inspector, esta diseñado para redes Ethernet LAN; identifica rápidamente si el problema se encuentra en un servidor, cliente, conmutador, enrutador o impresora gracias a la rápida detección y la clara visualización de la red. Con tan sólo pulsar un botón, se puede conseguir un informe de inventario de los dispositivos IP, IPX o NetBIOS, así como de los servicios que éstos ofrecen.

Network Inspector detecta rápidamente los dispositivos del dominio de difusión. Con esta detección de dispositivos se puede visualizar:

- Tipo/Nombres: Nombres de equipos DNS, y NetBIOS¨
- Direcciones: todas las direcciones IP asociadas al nodo y a la dirección MAC
- Servicios disponibles: conmutación, enrutamiento, correo electrónico, web e impresión
- Interfaces: velocidad y tipo
- Protocolos: IP, IPX y NetBIOS
- Configuración de la interfaz del dispositivo incluyendo velocidad, tipo, MTU, ranura y el conmutador más empleado y los puertos de enrutamiento, así como los dispositivos de cada puerto de conmutación.

La detección de dispositivos de Network Inspector también ofrece:

- Registro continuo de errores y cambios de los dispositivos de la red para aislar rápidamente los problemas
- Soluciones para los problemas de la red
- Notificación de sucesos por correo electrónico o buscapersonas
- Informes de inventario impresos en formato HTML, incluyendo IP, IPX y NetBIOS.

Network Inspector utiliza una arquitectura de agente/consola que le permite ubicar un agente en un segmento remoto y observar la información recopilada por dicho agente mediante una consola ubicada localmente. Sólo es necesario contar con un agente en cada dominio de difusión. Los datos se almacenan en una base de datos Microsoft Access. Otros profesionales de redes pueden tener acceso a la misma información mediante las consolas Network Inspector desde sus puestos de trabajo.

Los datos detectados se recogen, se exportan de forma automática a Microsoft Visio y se crea un mapa de la red, en el que se muestran los enlaces de los servidores, enrutadores y los PC hacia los conmutadores y concentradores. La creación de diagramas de la red resulta rápida y sencilla.

Los mapas que puede realizar (NetMap) son los siguientes:

- Conexiones del servidor en una red
- Conexiones de enrutador en una red conmutada
- Diagrama del conmutador (en forma de árbol)
- Indicador de conmutador único
- Impresoras conectadas
- Ordenadores centrales conectados
- Enrutadores, conmutadores y servidores conectados
- Conexiones de impresora en una red conmutada

Los requisitos mínimos para este sistema son:

- Windows 98 2nd Edition, Windows Millennium, Windows NT 4 (Service Pack 5 o superior), Windows 2000 (Service Pack 1 o superior) o Windows XP Professional Edition
- Procesador Pentium II 200 MHz
- 64 MB de RAM
- 150 MB de memoria virtual
- 100 MB de espacio disponible en disco

El licenciamiento ya no se encuentra disponible. Ha sido reemplazado por un nuevo producto (Optiview Console) de la misma compañía Fluye Networks, ofreciendo solo unas pocas mejoras.

2.24.6. MRTG.

Multi Router Traffic Grapher (MRTG) es la más importante de las aplicaciones de monitorización de tráfico que encontramos para servidores Linux. Programado por Tobias Oetiker y Dave Rand en Perl y C, muy meticulosamente para alcanzar una gran compatibilidad multiplataforma entre las cuales se pueden nombrar las siguientes:

- Linux 1.2.x, 2.0.x, 2.2.x, 2.4.x (Intel, Alpha, Sparc y PowerPC)
- Linux MIPS, Linux S/390
- SunOS 4.1.3
- Solaris 2.4, 2.5, 2.5.1, 2.6, 7, 8
- AIX 4.1.4, 4.2.0.0, 4.3.2
- WindowsNT 3.51, 4.0, 2k, XP
- IRIX 5.3, 6.2, 6.5
- BSDI BSD/OS 2.1, 4.x, 3.1
- NetBSD 1.5.x
- FreeBSD 2.1.x, 2.2.x, 3.1, 3.4, 4.x
- OpenBSD 2.x, 3.x
- Digital Unix 4.0
- SCO Open Server 5.0
- Reliant UNIX
- NeXTStep 3.3
- OpenStep 4.2
- Mac OS X 10.1

En el caso más general, MRTG usa SNMP (Simple Network Management Protocol) para recolectar los datos de tráfico de un determinado dispositivo (routers o servidores). Los gráficos generados con MRTG, además de una vista diaria detallada, representan también el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible porque MRTG mantiene un archivo de todos los datos que ha obtenido del dispositivo de red. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. Todo esto se realiza de una manera eficiente.

MRTG es una herramienta versátil, ya que si se profundiza un poco en sus posibilidades de configuración, se pueden monitorear parámetros tan interesantes como el número de usuarios conectados a nuestros sistemas, o el número de hosts trabajando en un cluster. Un ejemplo de las estadísticas que genera el programa *MRTG* se puede apreciar en el anexo Nº2.

(ver aneo Nº2)

2.24.7. PRTG Traffic Grapher.

PRTG es un software fácil de utilizar en Windows para supervisar el uso del ancho de banda la red así como otros parámetros como memoria y la utilización del CPU. Provee a los administradores de redes, las lecturas en vivo y las tendencias periódicas del uso de líneas dedicadas, enrutadores, cortafuegos, servidores, y de muchos otros dispositivos de red.

Con PRTG se puede saber el ancho de banda y datos del uso de la red que ayudan a optimizar la eficacia de la misma. El saber el consumo del ancho de banda permite:

- Evitar los embotellamientos en el funcionamiento del acceso a los servidores
- Planear mejoras estratégicas de la infraestructura.
- Entregar una mejor calidad del servicio a los usuarios de forma proactiva
- Reducir los costos por compra de ancho de banda y hardware según la carga real

La edición del freeware del PRTG está totalmente libre para el uso personal y comercial y se puede descargar gratis. Se requieren las ediciones comerciales si se desea supervisar más de un dispositivo. Las licencias comienzan en un costo de $49.95

El PRTG puede funcionar en una máquina con Windows en red por 24 horas durante todos los días y registrar constantemente los parámetros del uso de la red. Los datos registrados se almacenan en una base de datos interna para una futura referencia.

Posee una interfaz para Windows fácil de usar donde se pueden configurar los sensores de supervisión así como crear informes de usos. PRTG cuenta con un servidor web incorporado para proporcionar el acceso a los gráficos y a las tablas de forma remota.

Se apoya en todos los métodos comunes para la adquisición de datos como:

SNMP: El Simple Network Management Protocol, método básico de recopilar ancho de banda y datos del uso de la red. Puede ser utilizado para supervisar el uso del ancho de banda de enrutadores y switch puerto-por-puerto así como lecturas del dispositivo como la memoria, la carga del CPU etc.

Packet Sniffing: PRTG puede examinar todos los paquetes de datos que pasan por una tarjeta de red. Se puede supervisar solamente el tráfico de la máquina donde funciona PRTG o todo el tráfico de la red usando un switch con capacidad de supervisión o *mirroring* en sus puertos.

Netflow: El protocolo de Netflow es soportado por la mayoría de los enrutadores Cisco para medir uso del ancho de banda. Aunque es más complejo de instalarlo es también el método de más alcance y conveniente para alto tráfico de redes.

Con el packet sniffing y el netflow se puede medir el tráfico por direccion IP o protocolo mientras que la medida basada SNMP es basado solamente en un puerto.

Funciona en todas las versiones de Windows y con la mayoría de los productos de Cisco, HP, 3Com, Linksys, Nortel, etc., y con los dispositivos otros (e.g. las PC de Windows o las impresoras de la red).

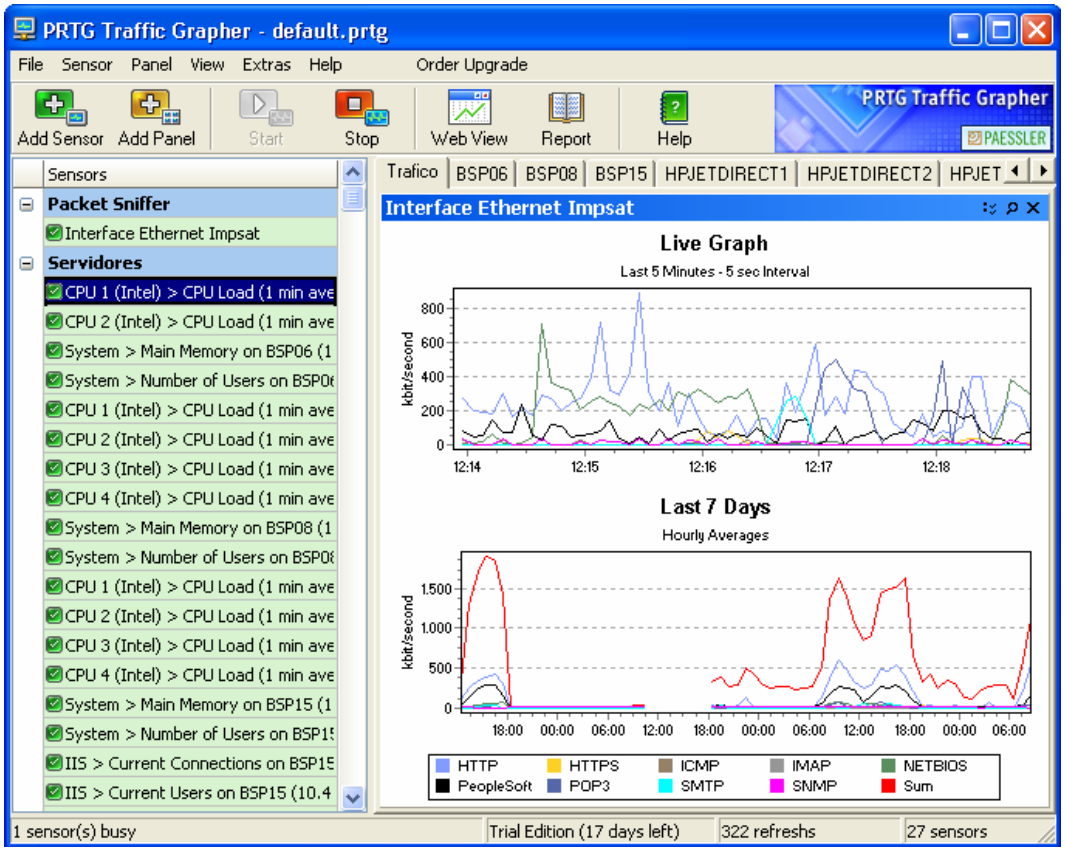


Figura 5. Pantalla de la aplicación PRTG

CAPITULO III

METODOLOGÍA

3.1. Tipo de Metodología.

La metodología utilizada se basó en la investigación, evaluación y selección de un sistema viable para solucionar los problemas planteados. Las etapas de ésta son el diagnóstico, planeamiento y fundamentación teórica, experimentación, análisis y conclusiones sobre la viabilidad y realización del proyecto.

3.2. Marco Metodológico.

El proyecto se estructuró en tres (3) etapas fundamentales:

- Etapa de Desarrollo
- Etapa de Implantación
- Etapa de Evaluación

A continuación se describirán brevemente cada una de las etapas, y se presenta un diagrama de Gantt donde se visualizan las actividades realizadas y sus tiempos estimados de ejecución.

3.2.1. Etapa de Desarrollo.

En esta etapa se llevo a cabo toda la parte investigativa previa a la implantación, donde se recopiló información sobre las condiciones actuales de la red

LAN y enlaces WAN con los clientes de BSP. Se elaboró un informe detallado de la red. Se realizó un análisis y se seleccionó el sistema que cumplía con las características que requería la estructura y necesidades de la compañía.

3.2.2. Etapa de Implantación.

Esta etapa consistió en la instalación y puesta en funcionamiento de las aplicaciones que conforman el sistema de gestión de red seleccionado previamente. Se instalaron consolas y agentes recolectores de información, los agentes remotos y herramientas de publicación como servidores y páginas web para la visualización remota de los mismos.

3.2.3. Etapa de Evaluación.

Una vez instalado el sistema de gestión de red, se realizó el monitoreo del ancho de banda de servidores y enlaces para luego caracterizar los mismos. Una vez configurados estos equipos de acuerdo a la topología de la red se recolectaron datos estadísticos como disponibilidad, tiempos y generación de alarmas en las caídas de los servidores y enlaces. Se analizó el tráfico de la red, discriminando por protocolos y aplicaciones, y se evaluó y estimó el consumo de ancho de banda de algunas aplicaciones ofrecidas por la compañía BSP.

3.2.4. Diagrama de Gantt.

DIARAMA DE GANTT EN PROYECT

CAPITULO IV

ETAPA DE DESARROLLO

4.1. Selección y Análisis del Sistema de Gestión.

Para la selección de una herramienta de gestión en BSP, se analizaron 7 programas o subsistemas existentes en el mercado: *WhatsUp Professiona*l de IpSwitch, *Ethereal*, *Network Monitor* de Microsoft, *NTOP*, *Network Inspector* de Fluye Networks, *MRTG* y *PRTG*. El análisis se realizó en función de las necesidades que presentaba la compañía BSP delimitados en el alcance del proyecto; esto permitió seleccionar las herramientas más convenientes en relación costo/beneficio. En esta etapa se realizaron las siguientes actividades:

4.1.1. Recolección e informe detallado de la red, computadores y recursos.

A continuación se detallarán los elementos y recursos de la red BSP.

4.1.1.1. Red LAN.

Topología: Estrella Extendida

Dispositivos:

- Host: Aproximadamente 76
- Servidores: 18
- Servidores de Impresión: 3 HP JETDIRECT
- Switch: 1 Stack conformado por 4 Módulos 144 puertos (AVAYA R333, P333 y 2*P334), con capacidad para manejar SNMP y actualmente habilitado.
- Router: 4 (IMPSAT, EAS, CANTV, GOLDATA)

Medios: 100BASE-TX, UTP Cat5

Tecnología: Ethernet IEEE 802.3

Dirección de RED:	10.4.1.0	
Mascara	255.255.255.0	
Broadcast	10.4.1.255	
DHCP:	BSP-03	10.4.1.13
Default Gateway	IMPSAT	10.4.1.1
PROXY:	BSP-04	10.4.1.14:8080
DNS:	BSP-01	10.4.1.11
	BSP-02	10.4.1.12
WINS:	BSP-02	10.4.1.12
SQL Server:	BSP-11	10.4.1.21
	BSP-12	10.4.1.22
Ms Exchange:	BSP-03	10.4.1.13
Controlador Primario de dominio	BSP-01	10.4.1.11
Controlador Respaldo de dominio	BSP-02	10.4.1.12
	BSP-03	10.4.1.13
Servidores IBM Bses de Datos	ODCREG1	10.4.1.33
	ODCVENE1	10.4.1.31
	ODCVENE2	10.4.1.32

Seguridad:

Firewall: Nokia 330

Telefonía:

Central telefónica: AVAYA-LUCENT, Definity

Un diagrama de la red LAN se puede apreciar en el anexo Nº 3.

(ver anexo Nº 3)

4.1.1.2. Red WAN.

Tabla 2. Equipos y descripción por cada enlace.

Router	Modelo	Dirección IP	Interfaces	Maneja SNMP	Activado SNMP
Impsat	Cisco 3600	10.4.1.1	3 Serial 1 Ethernet	Si	Si
AES	Cisco 3600	10.4.1.4	1 Serial 1 Ethernet	Si	No
CANTV	Cisco MC 3800	10.4.1.7	2 Serial 1 Ethernet	Si	No
Gold Data	Computador Dell LINUX	10.41.8	2 Ethernet	Si	Si

Tipos de Enlace:

Impsat: Frame Relay, Fibra Optica desde BSP hasta la la sede Impsat.

AES: Fibra Óptica desde BSP hasta el Cliente.

CANTV: HDLS desde BSP al Cliente.

Gold Data: Enlace de radio Spread Spectrum desde BSP al Cliente. (ver anexo Nº 4)

Tabla 3. Clientes y Anchos de Banda

Localidad	Canales de Voz	Ancho de Banda (Kbps)	Ancho de Banda Red Privada (CIR's en Kbps)	Ancho de Banda Internet (CIR's en Kbps)	Ancho de banda Canales de voz (CIRS's en Kbps)	Cantidad de Canales de Voz	Tipo de Enlace	Proveedor
BSP	30	4096	6144	256	330	30	Fibra Optica	IMPSAT
Tenedora de Valores	2	384	128	256	88	8	Radio	IMPSAT
Taco Taco Caracas	6	256	128	128	66	6	Radio	IMPSAT
Leones de Caracas	2	128	128	128	22	2	Radio	Gold Data
Saeca	2	256	256	256	22	2	Radio	IMPSAT
Fisa	2	256	128	128	22	2	Radio	IMPSAT
Venevisión		768	384	384			Fibra Optica	AES
Venevisión	12	1024	1024	1024	132	12	Radio	IMPSAT
Gaveplas	2	256	256	128	22	2	Radio	IMPSAT
Regional Cagua	5	1024	1024	256	88	8	Radio	IMPSAT
Regional Maracaibo	8	512	768	256	88	8	Radio	IMPSAT
Uniplast		128/256	256				Satelite	IMPSAT
Internet BSP		2048		2048			Fibra Optica	IMPSAT
FAACA		512		512			HDSL	CANTV
AFILCON		256		256			HDSL	CANTV

4.1.1.3. Servidores

Tabla 4. Servidores y su principal descripción.

Nombre	Dir. IP	Sistema Operativo	Modelo	Serial	Ethernet 10/100 Mbits	FO Gigabits	Servicios
BSP-01	10.4.1.11	Windows Server 2003 Enterprise Edition	IBM XSeries 350 8682-5RY	23F6973	1	1	DNS, Controlador Primario de Dominio
BSP-02	10.4.1.12	Windows Server 2003 Enterprise Edition	IBM XSeries 350 8682-5RY	23F7070	1	1	DNS,WINS, Controlador Resplado de Dominio
BSP-03	10.4.1.13	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7158	1	1	DHCP, MS EXCHANGE
BSP-04	10.4.1.14	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7052	2	1	PROXY
BSP-05	10.4.1.15	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7059	1	1	Impresión
BSP-06	10.4.1.16	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7077	1	1	Pruebas
BSP-07	10.4.1.17	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7076	2	1	PEOPLESOFT
BSP-08	10.4.1.18	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7165	3	1	PEOPLESOFT
BSP-09	10.4.1.19	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F6903	3	1	PEOPLESOFT
BSP-10	10.4.1.20	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F6989	1	1	PEOPLESOFT
BSP-11	10.41.21	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F7171	1	1	
BSP-12	10.4.1.22	Windows 2000 Advanced Server	IBM XSeries 350 8682-5RY	23F6992	1	1	
BSP-13	10.4.1.23	Windows Server 2003 Enterprise Edition	IBM XSeries 350 8682-5RY	23F7095	1	1	WEBSERVER
BSP-14	10.4.1.25	Windows Server 2003 Enterprise Edition	Dell Power Edge 2600		2	1 Ethernet Gigabits	WEBSERVER
BSP-15	10.4.1.104	Windows 2000 Advanced Server	Dell Power Edge 2600		2	1 Ethernet Gigabits	PEOPLESOFT
BSP-16	10.4.1.28						PEOPLESOFT
ODCVENE1	10.4.1.31	AIX	IBM RS/6000 S700 S7A				BASE DE DATOS
ODCVENE2	10.4.1.32	AIX	IBM RS/6000 S700 S7A				BASE DE DATOS
ODCREG	10.4.1.33	AIX	IBM RS/6000 M80				BASE DE DATOS
BSP P5A		AIX	IBM RS/6000 P5-570				BASE DE DATOS
BSP P5B		AIX	IBM RS/6000 P5-570				BASE DE DATOS

4.1.1.4. Sistema Operativo existente y disponible.

Se dispone de una plataforma Microsoft Windows NT/2000/2003/XP.

4.1.2. Carencias o necesidades.

Las necesidades de la red se enumeran a continuación:

- Se requiere un inventario de direcciones MAC e IP.
- Se requiere la detección de fallas de configuración de direccionamiento.
- Se requiere el inventario de los protocolos que se están utilizando en la red, para hacer una buena administración de los mismos.
- Se requiere la diagramación automática de la estructura de la red.
- Se requiere detectar eventos que representen la ocurrencia de un problema como la interrupción de un servicio o caída de un servidor
- Se requiere la generación de alarmas ante la detección de eventos
- Se requiere obtener estadísticas de los equipos de red o de algún equipo en especial a través de SNMP para medir y evaluar su comportamiento.
- Se requiere de un sistema que permita la generación de reportes y gráficas que sirvan para la evaluación de la red, los servidores, puertos del switch, ancho de banda utilizado, impresoras u otro componente de red.
- El área de Comunicaciones requiere de un sistema que le permita la visualización remota de las estadísticas, reportes y eventos.

4.1.3. Características de las aplicaciones de gestión de red.

En esta fase se analizaron las características de cada subsistema de gestión de red y se y se contrastaron con los requisitos técnicos mínimos exigidos por la red de la compañía. En la siguiente tabla se presenta este estudio comparativo:

Tabla 5. Comparación de las principales características de los subsistemas en estudio.

Requerimiento Técnico	WhatsUp	Ethereal	Network Monitor	NTOP	Network Inspector	MRTG	PRTG
Detección automática de dispositivos de red	Si	Si	Si	Si	Si		
Inventario direcciones MAC e IP	Si	Si	Si	Si	Si		
Detección de fallas de direccionamiento			Si	Si	Si		
Detección de protocolos		Si	Si	Si	Solo IP, IPX		Si
Detección de tráfico de aplicaciones específicas		Si		Si			
Diagramacion de la red	Si				Si		
Detección de eventos como caidas de servicios	Si				Si		
Generación de alarmas	Si				Si		
Generacion de estadisticas SNMP	Si			Si		Si	Si
Reportes de disponibilidad y rendimiento	Si			Si		Si	Si
Visualización remota	Si			Si	Si	Si	Si
Costo	$1495	No	No	No	Descontinuado	No	$49,5

4.1.4. Evaluación de la Relación Costo Beneficio.

De la evaluación técnica se obtuvo como resultado que los 7 subsistemas evaluados cumplen cada uno con una o más de las características y requisitos necesarios por BSP, esto lleva a considerar el aspecto económico, de lo que se puede decir lo siguiente:

- En su mayoría los programas son de domino público por ser de licencia GPL, que no acarrea ningún costo; los únicos que tienen costo por la licencia son *WhatsUp Professional* y *PRTG*. El programa *Network Inspector* ha sido descontinuado por la compañía fabricante.

- Analizando las características de cada uno de los subsistemas de licencias gratuitas se concluye que tienen características complementarias, por lo tanto se sugiere la instalación de los siguientes programas: *Ethereal, Network Monitor, NTOP* y *MRTG*.

- El programa *PRTG* es una versión modificada y amigable de *MRTG*. Dado que acarrea costos de licencia (aproximadamente $49) no se consideró necesario la adquisición e instalación del mismo.

- El programa *Whats Up Professional* aunque acarrea costo de licencia (aproximadamente $1450) es un programa que ofrece beneficios que ninguna de las otras aplicaciones provee, como por ejemplo: la generación de reportes de disponibilidad y generación efectiva de alarmas en caso de caídas del sistema. Por lo antes expuesto se sugiere su adquisición e implantación

- Dado que la versión disponible en Internet de *Network Inspector* es de uso limitado (30 días), aunado a que actualmente esta descontinuada por parte de la compañía fabricante y que su utilidad es muy puntual (el inventario de direcciones Ip, distribución de equipos en el Switch principal y diagramación de la red LAN), se recomienda su instalación por 30 días para dar solución a eventuales cambios en la red

4.2. Alcances de Sistema de Gestión de Red Seleccionado.

La implantación de los subsistemas anteriormente seleccionados en conjunto, formarán un sistema de gestión de red que permitirá lo enumerado a continuación:

- Inventario de direcciones MAC e IP.
- Diagramación automática de la estructura de la red
- Detección de fallas de configuración en el direccionamiento IP.
- Inventario de los protocolos que se están utilizando en la red.
- Detección de aplicaciones o protocolos que hagan uso indebido de la plataforma de red.
- Detección de problemas como la interrupción de un servicio o caída de un servidor
- Generación de alarmas ante la detección de eventos, por correo electrónico, o mensajes emergentes en pantalla y sonidos.
- Estadísticas del consumo de la red de los equipos en la LAN y WAN.
- Análisis de los tiempos de respuesta, tiempo de vida de los paquetes de las aplicaciones en ejecución
- Caracterización de la utilización de los enlaces hacia los clientes.
- Visualización remota de las estadísticas, reportes y eventos.

4.3. Selección de servidor y equipos remotos para la implementación.

Los requisitos mínimos del servidor para la instalación de todos los subsistemas son los siguientes:

- Pentium II 600 Mhz
- Servidor Windows 2003, Windows XP SP1 o posterior, o Windows 2000
- 200 MB de espacio de disco
- 256 MB RAM

Los requisitos mínimos necesarios para implementar en los computadores remotos, la supervisión, captura y análisis de tráfico son los siguientes:

- Pentium II 600 Mhz
- Windows XP SP1 o posterior
- 200 MB de espacio de disco
- 256 MB RAM

4.3.1. Servidor Seleccionado.

En base a los requisitos de los subsistemas, las especificaciones presentes en el servidor y su disponibilidad se decidió hacer la instalación de los sistemas de gestión de red en el siguiente servidor:

Tabla 6. Descripción del servidor seleccionado.

Marca	IBM
Modelo	X Series 350
Nombre	BSP-06
CPU	Pentium II XEON 700Mhz
RAM	2Gb
Disco Duro	Capacidad 4Gb, Disponible 500 Mb
	Capacidad 30Gb, Disponible 13.7 Gb
Tarjeta de Red	Gigabit Ethernet Sx Server Adapter
	IBM Netfinity Fault Tolerance PCI Adapter

4.3.2. Equipos Remotos.

En base a los requisitos de los subsistemas para el monitoreo remoto, las especificaciones presentes en las estaciones de trabajo y los recursos humanos disponibles para ejecutar tal labor, se implantaron los sistemas de gestión en las siguientes computadoras:

Tabla 7. Descripción de los equipos remotos seleccionados.

Marca	IBM
Modelo	NetVista
Nombre	JFGARCIA
CPU	Pentium IV 1.8Ghz
RAM	256 Mb
Disco Duro	Capacidad 40Gb Disponible 33 Gb
Tarjeta de Red	Intel PRO/100 VE
Marca	Dell
Modelo	OptiPlex 170L
Nombre	JBRITO
CPU	Pentium IV 2.6Ghz
RAM	512 Mb
Disco Duro	Capacidad 80Gb Disponible 60 Gb
Tarjeta de Red	Intel PRO/100 VE

CAPITULO V

ETAPA DE IMPLANTACIÓN

5.1 MRTG.

5.1.1. Instalación de MRTG.

Previamente a la instalación se procedió a descargar el software necesario. La página en Internet donde se descargó el software MRTG fue http://www.mrtg.cz/. El archivo fue mrtg-2.12.2.zip correspondiente a la versión 2.12.2 para Windows. También fue necesaria una copia de Perl para Windows que se descargó de la dirección http://www.ActiveState.com versión 5.6.

Se procedió a descomprimir el archivo descargado de MRTG en la carpeta c:\mrtg en el servidor seleccionado para su ejecución. Se instaló la versión de Perl en el mismo servidor y se verificó que el directorio de los archivos ejecutables de Perl se encontrara en el PATH del sistema, en este caso C:\Perl\bin;%SystemRoot%\system32;%SystemRoot%.

5.1.2. Configuración de MRTG.

Para la configuración de MRTG se verificaron las direcciones IP de los enrutadores y conmutadores a monitorear, los cuales fueron: AVAYA 10.4.1.30, Impsat 10.4.1.1, GoldData 10.4.1.8, AES 10.4.1.4 y CANTV 10.4.1.7. También se verificó que estuviera activo el servicio SNMP en el puerto estándar en cada uno, junto con sus respectivos nombres de la comunidad.

Se creó el archivo de configuración de MRTG con la ayuda de la herramienta *cfgmaker* incluida en el paquete anteriormente mencionado. La sintaxis utilizada para generar el archivo de configuración fue la siguiente:

“perl cfgmaker BSP@10.4.1.1 --global "WorkDir: c:\www\" --output mrtg.cfg”

donde BSP es el nombre de la comunidad para el enrutador de Impsat 10.4.1.1, c:\www es el directorio donde se almacenarán las estadísticas y el archivo de configuración generado tendrá el nombre mrtg.cfg. Esto creo un archivo de configuración inicial para el dispositivo. En este archivo todas las interfaces del enrutador serán almacenadas por número y descripciones de interface. Una vista parcial del archivo generado se puede observar en el anexo 1. (ver anexo Nº 1)

5.1.3. Ejecución continua de MRTG.

Se colocó una opción especial en el archivo de configuración de MRTG para que su ejecución fuera continua, esperará 5 minutos y entonces se ejecutara de nuevo. La opción agregada al archivo mrtg.cfg fue: RunAsDaemon: yes

Para ejecutarlo se realizó la siguiente instrucción:
start /Dc:\mrtg-2.9.18\bin perl mrtg --logging=eventlog mrtg.cfg

De encontrarse con problemas avisaría a través del visor de sucesos. Para detener MRTG, se puede abrir el administrador de tareas y terminar el proceso <perl.exe>. Para que se inicie automáticamente al reiniciar el servidor se colocó un acceso directo en la capeta de inicio del mismo con la siguiente configuración:
Destino: perl mrtg --logging=eventlog mrtg.cfg
Iniciar en: c:\mrtg\bin

5.2. Instalación de NTOP.

Se procedió a descargar el archivo de instalación NTop_XTRA_3_17_0.exe de la dirección en Internet http://www.openxtra.co.uk/products/ntop-xtra.php. Seguidamente de ejecutó dicho archivo en el servidor seleccionado para su instalación. Se inició el asistente de instalación, se siguieron las instrucciones mostradas en pantalla y se aceptó la ruta de instalación propuesta, en este caso "C:\Archivos de programa\OPENXTRA\NTopWin32". Al finalizar el proceso de copia de archivos, se agregó automáticamente un icono en la barra de tareas, desde el cual se puede desplegar un menú donde se activa o detiene el servicio correspondiente a la aplicación NTOP, e igualmente se puede acceder a la página principal de visualización del mismo que por defecto es http://localhost:3000, quedando de una vez configurado para capturar el tráfico circulante por la interface de red del servidor.

5.3. Instalación de Ethereal.

Se procedió a descargar el archivo de instalación Ethereal_setup_0.10.12.exe versión 0.10.12 para Windows de la dirección en Internet http://www.ethereal.com/download.html. Este paquete de instalación incluye el software WinCap, que permite capturar (Sniffing) todos los paquetes que transitan por la interface de red donde se desea ejecutar el analizador de protocolos *Ethereal*. Se procedió a ejecutar el archivo anteriormente mencionado, y se inició el asistente de instalación donde la información solicitada fue la ruta de destino de la instalación; para nuestro caso en el servidor seleccionado y quipos remotos para captura descentralizada "C:\Archivos de programa\Ethereal\".

5.4. Instalación de Network Monitor.

El programa Network Monitor de SMS, se instaló en los equipos remotos para análisis de tráfico y protocolos. La forma de instalarlo fue ejecutando el programa setup.exe del directorio \nmext del CD-ROM de Microsoft Systems Management Server 2.0. Se inició un asistente de instalación y se aceptaron todos los valores que por defecto desplegó el mismo. Finalizado el asistente se tuvo a disposición un acceso directo en la barra de programas de Windows para acceder a dicha aplicación.

5.5. Instalación de Network Inspector.

En la dirección en Internet http://www.flukenetworks.com se descargó la versión 4.1 del programa Network Inspector. El archivo descargado fue NetInsp.exe. Se ejecutó este archivo en los equipos destinados a realizar el análisis de la red, y al solicitar la licencia se dejó en blanco como condición para instalarse en modo de prueba con tiempo de expiración 7 días. El mismo a su vez solicitó la ruta de instalación seleccionándose en cada caso el directorio "C:\Archivos de Programa\Fluke Networks\Inspector". El asistente de instalación se encargó de realizar la copia de los archivos correspondientes a la consola y agente, al igual que los accesos directos de los mismos. El agente queda configurado automáticamente para iniciarse cada vez que se reinicia el equipo capturando la información de la red y la consola despliega dicha información.

5.6. Instalación de WhatsUp Professional.

Primero se rellenó una planilla de solicitud de descarga del software en la pagina http://www.ipswitch.com, luego se recibió un correo de respuesta donde se especificaba la dirección de descarga http://visit.ipswitch.com/DownloadWU y se

procedió a la misma. El archivo que se descargó fue iwp.exe. Dicho archivo se ejecutó en el servidor seleccionado y se siguieron las instrucciones sugeridas por el asistente de la instalación. Una vez instalado, se realizó una detección automática del dominio de la red donde una vez detectados los principales equipos se agruparon de acuerdo a enrutadores, conmutadores y servidores. Los equipos que no se detectaron automáticamente por no pertenecer al dominio de red, como por ejemplo enrutadores remotos (los de los clientes) se agregaron de forma manual. Posteriormente se configuró para los servidores la opción de generar una alarma en el caso de que surja una caída de los mismos con un una duración mayor a 5 minutos en la modalidad de correo electrónico y avisos emergentes en pantalla donde los destinatarios fueron los administradores de la red y sus respectivos equipos. Se configuró una cuenta de administrador con todos los privilegios para visualizar y modificar las vistas y configuraciones de los equipos y cuentas para los administradores y gestores de red con acceso restringido a las modificaciones.

5.7. Instalación de IIS.

Los Servicios de Internet Information Server 5.0 se encontraban instalados en el servidor Windows 2000 de forma predeterminada. Estos fueron necesarios para publicar vía WEB las estadísticas creadas con MRTG además de una página WEB sencillamente desarrollada donde se resumieron los accesos de forma remota a todas las aplicaciones finalmente implementadas.

CAPITULO VI

ETAPA DE EVALUACIÓN.

6.1. Estudio de la red LAN.

A continuación se presenta un resumen de las observaciones y sugerencias realizadas sobre la red LAN de la compañía BSP una vez implementado el sistema de gestión de red seleccionado. Estas observaciones están enfocadas a nivel de hardware (estaciones de trabajo, impresoras, servidores y equipos de conmutación), a nivel de software (protocolos, ancho de banda y aplicaciones) y finalmente a nivel de topología (lógica y física).

6.1.1. Estudio de Hardware.

Con la ayuda del *Network Inspector*, se realizó un censo de los dispositivos de la red LAN, levantándose un inventario de los equipos detectados. La información obtenida fue la siguiente:

- Dirección IP y subnet a la que pertenece el dispositivo.
- Máscara de red.
- Dirección MAC.
- Servicios IP: SNMP, HTTP, EMAIL, IMPRESIÓN, DNS, DHCP.
- Tipo de equipo de red: Estación de trabajo, servidor, impresora, enrutador o conmutador.

El informe obtenido se puede observar en el anexo Nº 5, y el alcance del mismo fue el siguiente:

- Cuantificar el número total de equipos de red presentes
- Diferenciarlos por servidores, estaciones de trabajo, impresoras, enrutadores o conmutadores.
- Inventariar su dirección física (dirección MAC).
- Inventariar su dirección IP y máscara.
- Inventariar su identificación en la red.

Con el mismo *Network Inspector* se generó un reporte detallado del conmutador principal AVAYA. Dicho reporte se puede apreciar en el anexo Nº 6. El alcance de dicho reporte fue el siguiente:

- Identificar los dispositivos de red conectados a cada puerto de conmutador
- Características del puerto: Velocidad 10 o 100 Mbits, Full o Half Duplex
- Estado del puerto: Activo o inactivo.

Después de realizar un exhaustivo análisis de los informes se presentaron las siguientes observaciones y sugerencias:

- Se sugirió la instalación del protocolo SNMP en los enrutadores, conmutadores y servidores donde no estaba activo en el momento de levantar el informe. Se evidenció que algunos si lo tenían activado pero dado a que el identificador de la comunidad no era "*public"* o no se estaba en conocimiento de cual era el configurado estos aparecían como no activos. Esta sugerencia se hace ya que es necesario tener activado el protocolo SNMP en los equipos principales de red para elaborar las estadísticas.

- Se informó de las estaciones de trabajo que tenían configuradas direcciones de red y máscaras IP diferentes a las definidas en la red LAN BSP para su corrección.

- Se sugirió la unificación en la forma de asignar los nombres de red de las estaciones de trabajo, lo que ayudaría a la pronta identificación y asociación con su ubicación física y recursos humanos que la utilizan.

6.1.2. Estudio de Software.

La red LAN BSP está basada en el protocolo IP. Con la ayuda de *Network Monitor* se identificaron los equipos que tenían activo el protocolo IPX y se informó para su desactivación.

Usando *NTOP* se obtuvo las estadísticas que se pueden apreciar en el anexo Nº 7.

Después de analizar estos reportes (ver anexo Nº 7) se puede decir lo siguiente:

- El 1.2% del tráfico esta distribuido en Broadcast y Multicast, lo que se considera una condición normal.

- Los paquetes presentan un tamaño en promedio de 382 bytes siendo en un 31% menores a 64 bytes. Esto se considera positivo en una red LAN, dado que paquetes pequeños aseguran menos tiempo de utilización del medio y por ende menos probabilidad de colisión.

- En promedio el ancho de banda utilizado en la red LAN es de 377 Kbits lo que representa 0.38% de utilización del medio.

- El tiempo de vida (TTL) se encuentra por debajo de 160ms lo que indica que la mayoría de los paquetes llegan en corto tiempo a su destino evitándose la perdida de los mismos por latencia en el medio.

- El 99.9% del tráfico es IP, siendo la mínima diferencia el representado por el trafico (R) ARP que se encuentra en condiciones normales.

- De la capa 4 se aprecia que el 95% corresponde a TCP y la diferencia a UDP, lo que garantiza la retransmisión de la data en caso de problemas por el control de flujo de TCP.

- De las aplicaciones que hacen uso de TCP, se aprecia que la mayoría del tráfico corresponde a "Other TCP/UDP-based Protocols" que para la red LAN de BSP corresponde a las aplicaciones *PeopleSoft* que utilizan el puerto TCP 7001

- No se observó tráfico de aplicaciones maliciosas, o que pudieran estar haciendo un uso indebido del ancho de banda.

6.1.3. Estudio de Topología.

La topología física es en estrella, parte de un conmutador principal hacia los servidores, estaciones de trabajo e impresoras, en cableado UTP categoría 5. No se evidencian problemas de congestión en la red, pero dada la estructura y los diversos servicios que ofrece la organización, se realizaron las siguientes sugerencias en función de segmentar y optimizar la utilización de la misma:

- La dirección IP de la red es 10.4.0.0 máscara 255.255.0.0 donde los servidores están configurados con direcciones fijas en el rango que va desde 10.4.1.11 al 10.4.1.30 y de esta última dirección en adelante se asignan automáticamente las direcciones a las estaciones de trabajo por el DHCP. Se sugiere cambiar el direccionamiento IP, asignándole a los servidores el rango que va desde la 10.4.1.0 a la 10.4.1.254 y a las estaciones de trabajo las direcciones de la 10.4.2.0 a la 10.4.2.254; esto facilitará la aplicación de políticas de acceso en los enrutadores y cortafuegos ya que la segmentación de las direcciones IP permitirá diferenciar entre los mismos.

- Crear VLAN para cada departamento, por ejemplo, recursos humanos, administración, consultoría, desarrollo etc. Esto favorecerá a delimitar el tráfico de datos que es tan diferenciado entre los departamentos y aplicar mejores políticas de acceso a los servidores, lo que asegurará una descentralización de los focos de congestión.

- Configurar direcciones IP adicionales en los servidores, las cuales serán pertenecientes a otra red diferente a la red LAN de BSP; por estas se tendría el acceso vía WAN a los servidores y así se desvinculan los accesos remotos del direccionamiento interno de la LAN.

6.2. Estudio de la red WAN.

En este estudio se presenta un resumen de las observaciones y sugerencias realizadas sobre la red WAN de BSP una vez implementado el sistema de gestión de red seleccionado, principalmente enfocado hacia la utilización del ancho de banda y a nivel de protocolos descubriendo el tránsito de aplicaciones indebidas por la red.

6.2.1. Estudio de la utilización Ancho de Banda.

Después de configurado el MRTG para cada uno de los enlaces hacia los clientes, se tomaron estadísticas de la utilización del ancho de banda de cada uno por un período de alrededor de 2 meses, lo que permitió caracterizarlos. Por ejemplo se monitorearon valores máximos y promedios tanto de entrada como de salida, y en base a las necesidades se observó utilización instantánea. A continuación se presenta un cuadro resumen de estos valores para cada enlace:

Tabla 8. Resumen de la utilización del ancho de banda de los clientes.

Enlace	Ancho de banda del canal	Utilización					
		Máximo			Promedio		
		Entrada	Salida	Utilización Máximo %	Entrada	Salida	Utilización Promedio %
Ethernet Impsat	100 Mbits	1695,40	883,70	1,70	336,70	171,90	0,34
Regional Cagua	1024 kb/s	660,10	784,10	76,57	63,40	91,70	8,96
Regional Cagua Internet	256 kb/s	235,20	0,38	91,88	12,50	0,16	4,88
Regional Maracaibo	768 kb/s	400,60	672,00	87,50	19,40	99,30	12,93
Regional Maracaibo Inernet	256 kb/s	91,70	232,30	90,74	3,10	23,90	9,34
Fisa	128 kb/s	19,30	30,30	23,67	0,42	0,64	0,50
Fisa Internet	128 kb/s	10,70	109,60	85,63	0,40	2,42	1,89
Saeca	256 kb/s	51,70	38,20	20,20	2,53	3,92	1,53
Saeca Internet	256 kb/s	136,70	190,10	74,26	10,20	22,70	8,87
Gaveplast	256 kb/s	14,10	93,10	36,37	1,44	4,07	1,59
Gaveplast Internet	128 kb/s	62,80	0,31	49,06	1,31	0,06	1,03
Venevisión	1024,00	257,10	441,00	43,07	5,61	69,00	6,74
Venevisión Internet	384,00	379,20	364,30	98,75	191,60	13,70	49,90
Taco Taco	128 kb/s	76,10	123,20	96,25	1,58	3,67	2,87
Taco Taco Internet	128 kb/s	0,09	0,28	0,22	0,01	0,10	0,08
Tenedora	128 kb/s	17,00	80,30	62,73	0,56	1,08	0,84
Gold Data	128 kb/s	32,20	73,40	57,34	2,12	7,33	5,73
AES	768 kb/s	744,20	561,20	96,90	57,30	62,10	8,09
CANTV	512 kb/s	19,70	124,60	24,34	1,36	8,63	1,69

Analizando los enlaces en base a la máxima utilización de los mismos, se puede decir que en su mayoría hacen un uso eficiente del ancho de banda comprometido con el proveedor, encontrándose una máxima utilización de 96.90% que se acredita a instantes de tiempo donde existió la máxima concurrencia de usuarios en horas pico. Los bajos valores promedios se deben a que la utilización del

enlace por parte de los clientes es casi nula los fines de semana, y fuera de horarios de oficina, además de que el tráfico en su mayoría es HTTP, que es caracterizado por un consumo en ráfagas haciendo uso de toda la capacidad disponible del canal por cortos intervalos de tiempo.

Enlaces como FISA, Saeca, Gaveplast, Taco-Taco Internet, y FAACA (CANTV), están subutilizando el enlace contratado, pues su utilización máxima oscila entre 0.22% y 36.37 % y con valores promedio entre 0.08% y 1.69%. Dada estas circunstancias se sugiere ajustar el ancho de banda contratado a un valor cercano al máximo utilizado con el fin de reducir los costos de contratación. Los valores sugeridos son:

Tabla 9. Ancho de banda sugerido.

Enlace	**Ancho de banda actual**	**Ancho de banda Sugerido**
Fisa	128 kb/s	64 kb/s
Saeca	256 kb/s	128 kb/s
Gaveplast	256 kb/s	128 kb/s
Taco Taco Internet	128 kb/s	64 kb/s
FAACA	512 kb/s	256 kb/s

Dada la característica de utilización promedio elevada del enlace de Venevisión Internet, se realizó una investigación sobre el tráfico que circulaba a través de él. Con la utilización de *Ethereal*, se realizó la captura del tráfico que circulaba y se detectó la aplicación *Edonkey*, una aplicación P2P destinada al intercambio de archivos de diversos formatos de audio y video. Se tomó nota de los puertos origen y destino utilizados por esta aplicación y dado que el uso de dicho programa causa la degradación del enlace se aplicó una lista de acceso en el enrutador para no permitir la circulación a través de él de paquetes con estos puertos en sus cabeceras.

6.3. Estudio del ancho de banda utilizado por las aplicaciones ofrecidas.

La aplicación estudiada fue *PeopleSoft*, un sistema ERP (Enterprise Resources Managment) que en español significa un planificador de recursos empresariales. *PeopleSoft* proporciona soluciones de gestión, análisis y control empresarial, dentro de las áreas económico - financiera, gestión de materiales, distribución, gestión de la cadena de aprovisionamiento, fabricación y recursos humanos. Las soluciones empresariales de *PeopleSoft* están enfocadas al núcleo de la gestión de negocio, a los procesos comerciales de negocio tanto para organizaciones orientadas a productos como a servicios y a los requerimientos específicos de la industria. Las principales características se enumeran a continuación:

- Establece parámetros de gestión de acuerdo alcance de la empresa.
- Define estructuras de operación en los diferentes módulos que integran el sistema como cuentas por pagar, cuentas por cobrar, tesorería, inventario y compras.
- Establece la estructura contable, reglas contables.
- Estructura el árbol como la estructura organizacional y funcional.
- Define e identifica los proveedores, clientes, artículos y bancos.
- Establece controles, contables, administrativos, operativos y seguridad.
- Garantiza la información veraz, oportuna y confiable.

PeopleSoft crea la empresa en tiempo real; gracias a ello los clientes, proveedores, socios comerciales y empleados pueden acceder directamente a los procesos de gestión en cualquier momento y desde cualquier lugar. El funcionamiento de la empresa en tiempo real supone enormes ventajas de rendimiento: se eliminan intermediarios, los procesos de gestión son inmediatos, el rendimiento empresarial se somete a control continuo, toda la información pertinente se presenta en tiempo real y la respuesta a los cambios empresariales es inmediata.

PeopleSoft ofrece un completo conjunto de aplicaciones de empresa creado mediante Arquitectura Puro Internet. Los clientes, proveedores, socios comerciales, y empleados disponen de acceso directo a los procesos de gestión vía Internet. La carencia de código en las estaciones cliente permite el acceso a los procesos desde cualquier lugar, en cualquier momento y mediante cualquier dispositivo web, lo que aumenta considerablemente la productividad, al tiempo que se reducen los costos.

Las siguientes pruebas se realizaron con la intención de medir cual es el consumo de ancho de banda por usuario haciendo uso de la aplicación remotamente (Internet) y así tener estimaciones de los anchos de banda a contratar por los clientes en función del número de usuarios que necesiten tener acceso a la aplicación.

Las pruebas consistieron en la ejecución de varios módulos de la aplicación de forma remota, específicamente en el cliente *Gaveplast* realizándose la captura del tráfico generado y posterior análisis.

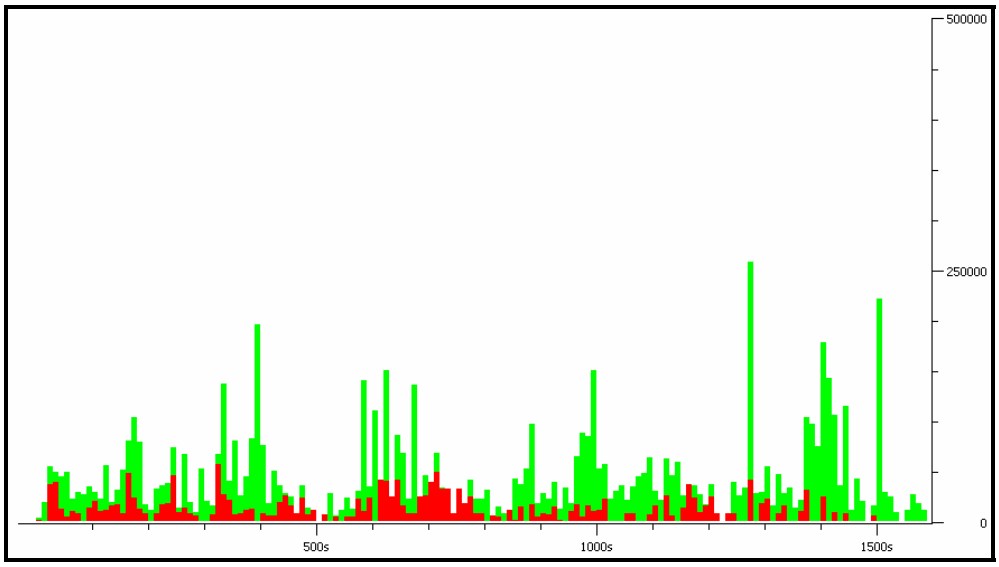
La prueba 1 se realizó el 10 Agosto 2005 entre 10:20:49 y 10:47:24 y mostró los siguientes resultados:

Tabla 10. Estadísticas del tráfico total con destino el servidor de la aplicación en la prueba 1.

Tiempo de Captura (seg):	1594.817
Paquetes:	19212
Average de Paquetes/seg	12.047
Average del tamaño del paquete(bytes)	375
Average de bytes/seg	4522.463
Average de kbits/seg	36.17

Tabla 11. Tráfico filtrado para la estación de trabajo en estudio en la prueba 1.

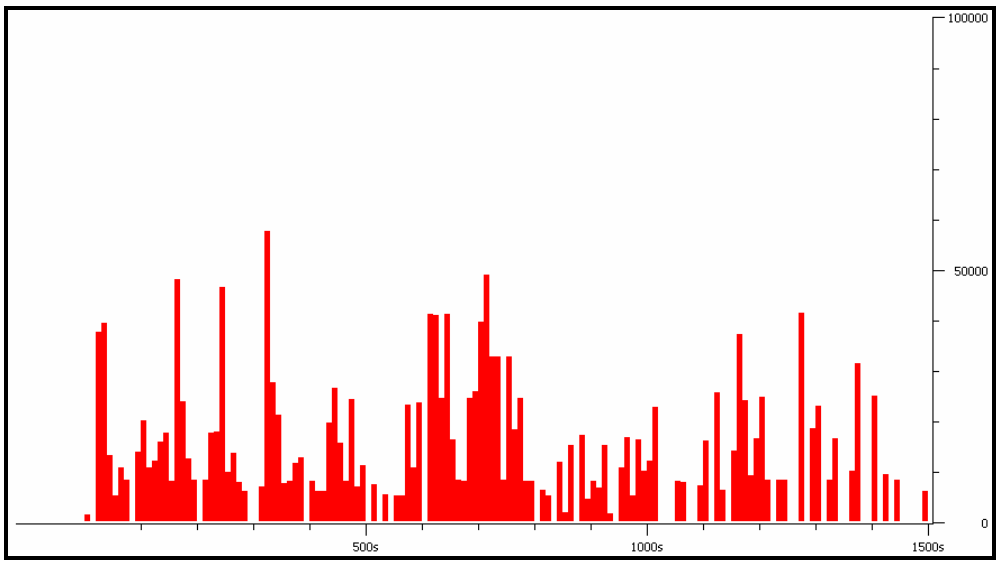
Tiempo de Captura (seg):	1594.817
Paquetes:	5509
Average de Paquetes/seg	3.67
Average del tamaño del paquete(bytes)	352.248
Average de bytes/seg	1295.858
Average de kbits/seg	10.36



Verde= Tráfico total hacia 10.4.1.17 **Rojo**= Tráfico de 10.7.1.53

Eje X: Intervalo de los pulsos=10 seg Eje Y: Bytes

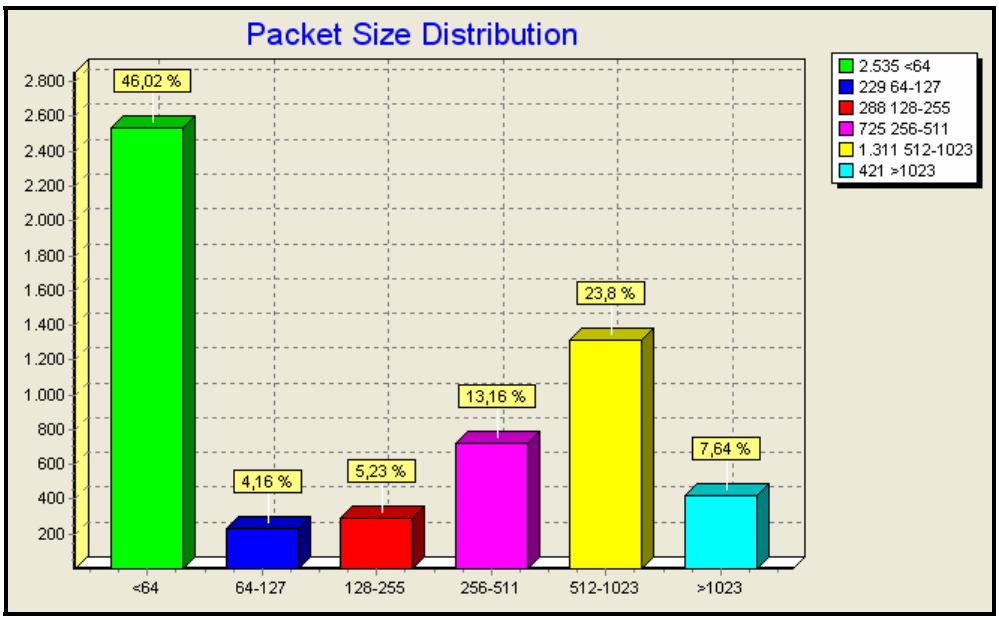
Gráfica 1. Tráfico diferenciado en función del tiempo en la prueba 1.



Eje X: Intervalo de los pulsos=10 seg Eje Y: Bytes

Máximo= 70000/(10*1000)=56kbits

Gráfica 2. Tráfico de la estación 10.7.1.53 en función del tiempo en la prueba 1



Gráfica 3. Distribución del tamaño de los paquetes en la prueba 1.

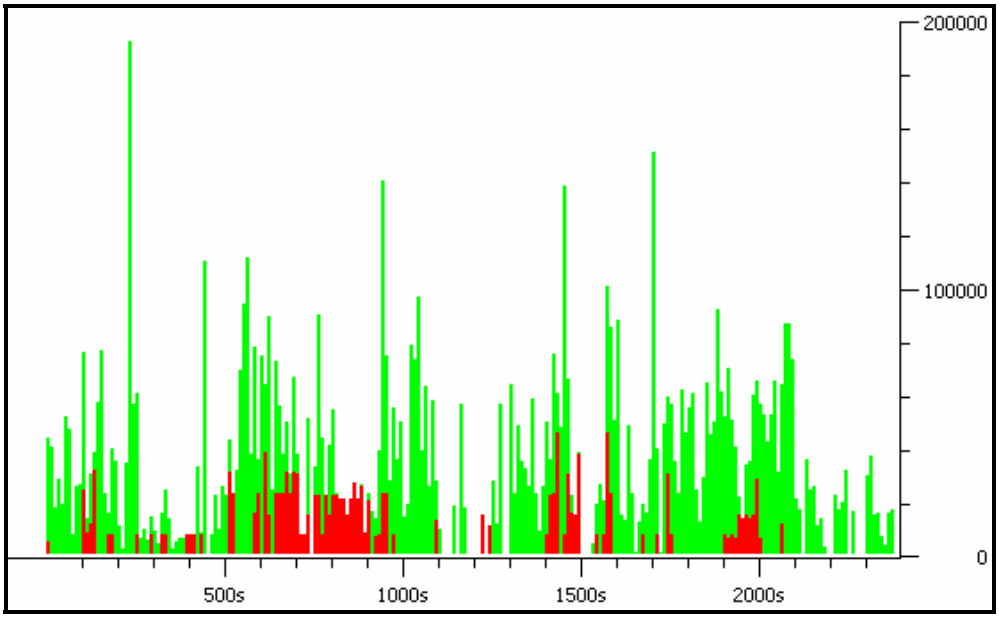
La prueba 2 se realizó el 10 Agosto 2005 entre 11:38:03 y 12:17:51 y mostró los siguientes resultados:

Tabla 12. Estadísticas del tráfico total con destino el servidor de la aplicación en la prueba 2.

Tiempo de Captura (seg):	2387.452
Paquetes:	22143
Average de Paquetes/seg	9.275
Average del tamaño del paquete(bytes)	374
Average de bytes/seg	3475.070
Average de kbits/seg	27.80

Tabla 13. Tráfico filtrado para la estación de trabajo en estudio en la prueba 2.

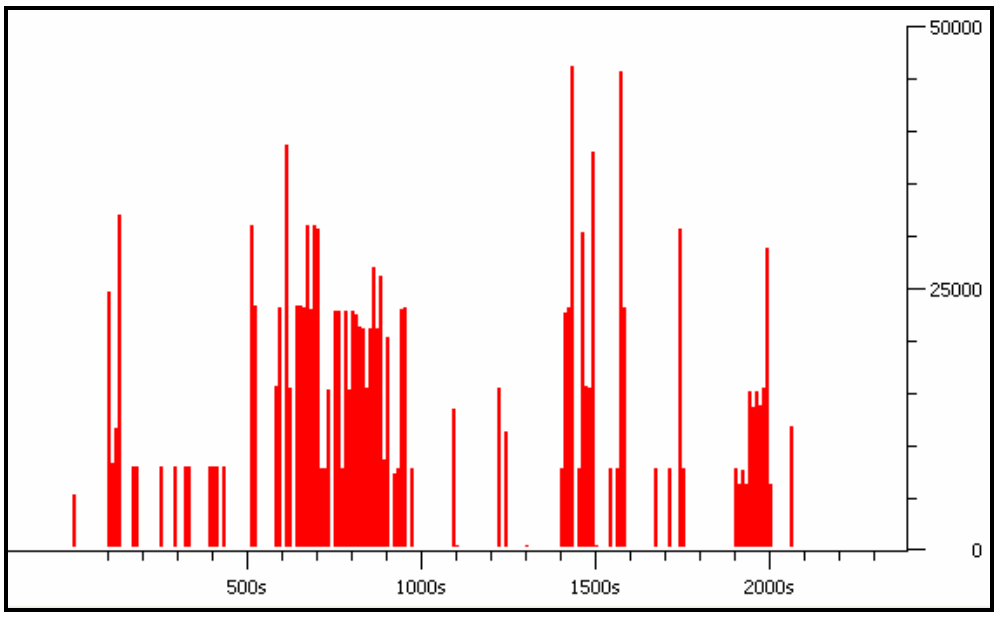
Tiempo de Captura (seg):	2056.522
Paquetes:	4353
Average de Paquetes/seg	2.117
Average del tamaño del paquete(bytes)	329.185
Average de bytes/seg	696.780
Average de kbits/seg	5.57



Verde= Tráfico total hacia 10.4.1.17 **Rojo**= Tráfico de 10.7.1.44

Eje X: Intervalo de los pulsos=10 seg Eje Y: Bytes

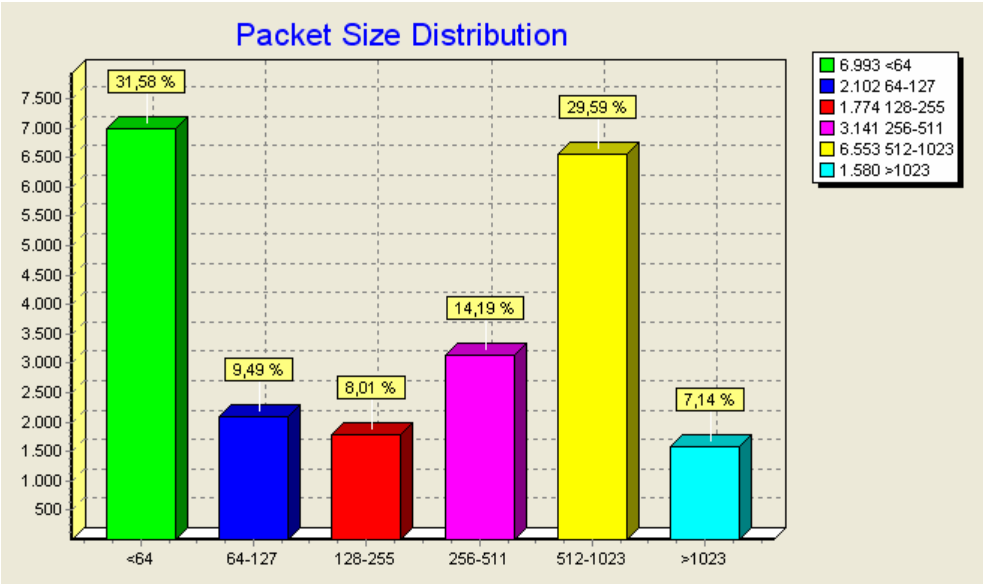
Gráfica 4. Tráfico diferenciado en función del tiempo en la prueba 2.



Eje X: Intervalo de los pulsos=10 seg Eje Y: Bytes

Máximo= 45000/(10*1000)=36kbits

Gráfica 5. Tráfico de la estación 10.7.1.44 en función del tiempo en la prueba 2.



Gráfica 6. Distribución del tamaño de los paquetes en la prueba 2.

De estas pruebas se puede decir lo siguiente:

- Se aprecia que el tráfico está caracterizado por ráfagas, esto por ser HTTP; lo anterior se traduce en lo siguiente: en cortos intervalos de tiempo se hace el mejor esfuerzo por utilizar al máximo la capacidad del canal.
- Dada la característica anterior se estimó el valor promedio del ancho de banda utilizado como función del promedio de paquetes por segundo (paquetes/segundo) y el promedio del tamaño del paquete (kbits/paquete), dando por resultado el ancho de banda promedio (kbits/segundo)
- En las dos pruebas se obtuvieron valores diferentes del ancho de banda promedio, dado que eran estaciones de trabajo y condiciones de estrés del servidor distintas. Como se aprecia en la prueba 1 se obtuvo una utilización del ancho de banda promedio de 10.36 kbits/seg que es mayor a la de la prueba 2 de 5.57 kbits/seg. Esto se debe a que en la primera prueba se recibió una relación mayor de paquetes por unidad de tiempo que en la segunda, y por lo consiguiente se concluye que en la prueba 1 se

hizo una mayor utilización del enlace y por ende se considera la condición de mayor estrés. Por lo antes expuesto se consideró como valor máximo de utilización del canal por cliente de la aplicación *PeopleSoft* el valor de 10.36kbits/seg.

CONCLUSIONES Y RECOMENDACIONES

Con el desarrollo y auge de las redes de datos se esperaba que la gestión de estas se simplificara con el paso del tiempo, sobre todo ahora que muchas de las antiguas tecnologías de red son obsoletas. Sin embargo administrar eficientemente una red es un problema complejo debido a los nuevos servicios que emergen constantemente y a las nuevas amenazas de seguridad que aparecen cada día. También se ha incrementado la importancia de facilitar el manejo de la red, pues las compañías necesitan cada vez más realizar operaciones en tiempo real y disponibilidad de aplicaciones críticas con menos supervisión.

También se debe añadir el hecho de que las compañías sufren recortes de presupuesto y reducciones en el número de empleados, lo que obliga a hacer más con menos medios, por lo que está claro que la gestión de red tiene un papel crítico a la hora de solucionar estos problemas. Las compañías necesitan que su sistema de gestión de red reduzca costos globales de funcionamiento, permitiendo que los recursos y la experiencia en tecnologías de información se emplee en ubicaciones más estratégicas.

Después de investigar los sistemas de gestión de red más comunes en el mercado como por ejemplo, Tivoli (IBM), SMS (Microsoft), Ominivista (Alcatel), OpenView (HP), SunNet Manager (SUN), CiscoWorks (Cisco) entre otros, BSP observó los altos costos asociados a la adquisición de los mismos. En vista de la limitación de presupuesto por parte de BSP para la implementación de estos a corto plazo, se consideraron productos de bajo costo o de licencias de uso público y/o gratuito, para realizar una primera evaluación de la infraestructura de red y cubrir las necesidades básicas de gestión, monitoreo y supervisión de la misma.

Fueron 7 en total los subsistemas evaluados para conformar el sistema de gestión de red de BSP. Uno a uno fueron analizados y estudiados. El enfoque estuvo orientado a sus funcionalidades respecto a los requerimientos del sistema al igual que el costo. Finalmente se elaboró un cuadro comparativo (ver tabla Nº5) en función de las necesidades y alcances del proyecto, especificando el cumplimiento o no de cada uno de ellos, al igual que se agregó un campo asociado al costo para las licencias no gratuitas.

De este cuadro comparativo se aprecia que cada subsistema ofrece por lo menos una funcionalidad no cubierta por los otros, en consecuencia, se decidió implementarlos todos a excepción de la aplicación *PRTG* cuyas características están cubiertas por el programa *MRTG*. La ventaja de usar *MRTG* es que su licencia es gratuita.

Una vez seleccionado el servidor y los equipos de supervisión remota en función de los requerimientos mínimos recogidos de la evaluación del sistema seleccionado, se procedió a la fase de implementación de los mismos, donde se configuraron y personalizaron sus diversas funcionalidades cubriendo las necesidades de BSP.

Una vez implementados los subsistemas se hizo uso de los mismos, obteniéndose lo siguiente:

- Se censaron e inventariaron los equipos que conforman la red de BSP en un informe detallado, permitiendo: dimensionar, detectar y corregir problemas en sus configuraciones y programar la instalación de los agentes SNMP para monitorearlos.

- Se estimó a 10.36 kbits/seg el consumo de ancho de banda de la aplicación ofrecida por BSP específicamente *Peoplesoft* por cliente remoto. Esto a su vez

sirvió para tener una primera aproximación del ancho de banda total de los enlaces WAN a ser contratado por los clientes.

- Se recogieron estadísticas de la utilización de los enlaces hacia clientes, servidores y principales equipos de interconexión de la red de BSP permitiendo hacer sugerencias en pro de obtener relaciones costo/beneficio óptimas basadas en el consumo de ancho de banda de los mismos.

- Se configuraron las aplicaciones para generar alarmas (en forma de correo electrónico y mensajes emergentes en pantalla) en caso de interrupción de los servicios, permitiendo realizar la atención de las fallas de forma oportuna.

- Se obtuvieron estadísticas de disponibilidad y reportes de tiempo fuera de servicio de los principales equipos de red, cuyo análisis permitió predecir y corregir fallas recurrentes.

- Se detecto el tráfico de aplicaciones que degradaban los enlaces al igual que la información de los puertos que estas utilizaban. Con esta información se aplicaron políticas de acceso que restringieron la circulación de las mismas por los enlaces.

Como comentario final y a manera de recomendación se puede decir que en el mercado existen productos dedicados a la gestión de red que cubren las necesidades de BSP y muchas funcionalidades más, pero implican una inversión significativa que conlleva a realizar un análisis más profundo de los costos en función de los beneficios. Estudios como los presentados en este trabajo pueden considerarse unas buenas prácticas previas a adquisición de soluciones de mayor envergadura de así requerirse.

REFERENCIAS BIBLIOGRÁFICAS

[1] Monografías.com [en línea]. <http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml> [Consulta: 2005]

[2] Wikipedia en Español [en línea]. <http://es.wikipedia.org/wiki/Redes_de_ordenadores/computadoras>. [Consulta: 2005]

[3] Wikipedia en Español [en línea]. <http://es.wikipedia.org/wiki/Redes_de_ordenadores/computadoras>. [Consulta: 2005]

[4] Wikipedia en Español [en Línea] <http://es.wikipedia.org/wiki/Ethernet>. [Consulta: 2005].

[5] Seifert, Rich. The Switch Book, New Cork: Editorial John Wiley & Sons, Inc, 2000.

[6] Mendillo Vincenzo, Material de apoyo, asignatura: Gestión de Redes. UCV, Noviembre 2.001.

BIBLIOGRAFÍAS

Libros.

Black Uyless. Tecnologías emergentes para redes de computadoras. México: Prentice-Hall Hispanoamericana, S.A., 1.999.

Mendillo Vincenzo. Material de apoyo, asignatura: Gestión de Redes. UCV, Noviembre 2.001.

Seifert, Rich. The Switch Book, New York: Editorial John Wiley & Sons, Inc, 2000.

Spurgeon, Charles. Ethernet The Definitive Guide, USA: Editorial O'Reilly&Associates, 2000.

Stallings, William. SNMP, SNMP v2, SNMP v3 and RMON 1 and 2. USA: Editorial Addison – Wesley Pub Co, 1998.

Tanenbaum, A. Redes de Computadoras. México: Editorial Prentice-Hall Hispanoamericana, S.A., 1.997.

Internet.

Monografías.com [en línea]. <http://www.monografias.com> [Consulta: 2005]

GLOSARIO

ARCnet: Red de recursos adjuntos. Un bus de token de 2.5 Mbps de LAN desarrollado a final de los 70 y a principio de los 80 por Datapoint Corporation.

Backbone: Parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de, y se destina a, otras redes.

Bit: Dígito binario utilizado en el sistema numérico binario. Puede ser 0 ó 1.

Bluetooth: Sistema de comunicación inalámbrica el cual permite la interconexión de diferentes dispositivos electrónicos (PCs, teléfonos fijos o móviles, agendas electrónicas, auriculares, etc.) de forma que presenta un estándar creado por importantes empresas de los sectores de la informática y las telecomunicaciones.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican mediante una dirección de broadcast.

Firewall: Router o servidor de acceso o varios routers o servidores de acceso designados como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de acceso así como otros métodos para garantizar la seguridad de la red privada.

Host: Sistema informático en una red. Similar al término nodo , salvo que host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y routers.

Hub: Por lo general, se usa este término para describir un dispositivo que sirve como centro de una red con topología en estrella. Dispositivo de hardware o software que

contiene múltiples módulos independientes pero que están conectados a los equipos de red y de internetwork. Los hubs pueden ser activos (cuando repiten señales enviadas a través de ellos) o pasivos (cuando no repiten las señales sino simplemente dividen las señales enviadas a través de ellos). En Ethernet y IEEE 802.3, un repetidor multipuerto de Ethernet que se conoce a veces como concentrador

IEEE: Instituto de Ingeniería Eléctrica y Electrónica. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares que predominan en las LAN de la actualidad.

Internet: Término utilizado para referirse a la internetwork más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. En un determinado momento se la llamó Internet DARPA. No debe confundirse con el término general internet.

internet: Abreviatura de internetwork.. No debe confundirse con la Internet. Ver internetwork.

Internetwork: Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (en general) como una sola red. A veces denominada una internet, que no se debe confundir con la Internet.

ISO: Organización Internacional para la Normalización. Organización internacional que tiene a su cargo una amplia gama de estándares, incluidos aquellos referidos a la networking. ISO desarrolló el modelo de referencia OSI, un popular modelo de referencia de networking.

GNU: fue iniciado por Richard Stallman con el objetivo de crear un sistema operativo completo libre. El 27 de septiembre de 1983 se anunció públicamente el proyecto por primera vez en el grupo de noticias net.unix-wizards. Al anuncio original, siguieron otros ensayos escritos por Richard Stallman como el "Manifiesto GNU", que establecieron sus motivaciones para realizar el proyecto GNU, entre las que destaca "retornar al espíritu de cooperación que prevaleció en los tiempos iniciales de la comunidad de usuarios de computadoras". GNU es un acrónimo recursivo que significa "GNU No es Unix". Para asegurar que el software GNU permaneciera libre para que todos los usuarios pudieran "ejecutarlo, copiarlo, modificarlo y distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en Inglés como copyleft (en clara oposición a copyright), y está contenida en la Licencia General Pública de GNU (GPL)

Multicast: Paquetes únicos copiados por la red y enviados a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de direcciones de destino.

Networking: Interconexión de cualquier grupo de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

OSI: interconexión de sistemas abiertos. Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

Router: Dispositivo de la capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Envía paquetes desde una red a otra basándose en la información de la capa de red. De vez

en cuando denominado gateway (aunque esta definición de gateway se está tornando obsoleta).

Switch: Dispositivo de red que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

Unicast: Mensaje que se envía a un solo destino de red.

[ANEXO Nº 1]

[Archivo generado por la herramienta de configuración *cfgmaker* de MRTG]

```
# Created by Juan F. García
# cfgmaker --output mrtg.cfg BSP@10.4.1.1
WorkDir: c:\www
### Global Defaults
#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits
EnableIPv6: no
######################################################################
# System: rt-odc-kpmg
# Description: Cisco Internetwork Operating System Software
# IOS (tm) 3600 Software (C3620-IS-M), Version 12.3(13),
# Technical Support: http://www.cisco.com/techsupport
# Copyright (c) 1986-2005 by cisco Systems, Inc.
#  Compiled Thu 10-Feb-05 09:16
#  Contact:
#  Location:
######################################################################
### Interface 1 >> Descr: 'FastEthernet0/0' | Name: 'Fa0/0' | Ip: '10.4.1.1' | Eth:
'00-b0-64-f0-45-01' ###
Target[10.4.1.1_1]: 1:BSP@10.4.1.1:
SetEnv[10.4.1.1_1]: MRTG_INT_IP="10.4.1.1"
MRTG_INT_DESCR="FastEthernet0/0"
MaxBytes[10.4.1.1_1]: 12500000
Title[10.4.1.1_1]: Traffic Analysis for 1 -- rt-odc-kpmg
PageTop[10.4.1.1_1]: <h1>Traffic Analysis for 1 -- rt-odc-kpmg</h1>
                    <div id="sysdetails">
                            <table>
                                    <tr>
                                            <td>System:</td>
```

```
                <td>rt-odc-kpmg in </td>
            </tr>
            <tr>
                <td>Maintainer:</td>
                <td></td>
            </tr>
            <tr>
                <td>Description:</td>
                <td>FastEthernet0/0  </td>
            </tr>
            <tr>
                <td>ifType:</td>
                <td>ethernetCsmacd (6)</td>
            </tr>
            <tr>
                <td>ifName:</td>
                <td>Fa0/0</td>
            </tr>
            <tr>
                <td>Max Speed:</td>
                <td>12.5 MBytes/s</td>
            </tr>

            <tr>
                <td>Ip:</td>
                <td>10.4.1.1 ()</td>
            </tr>

        </table>
</div>
```

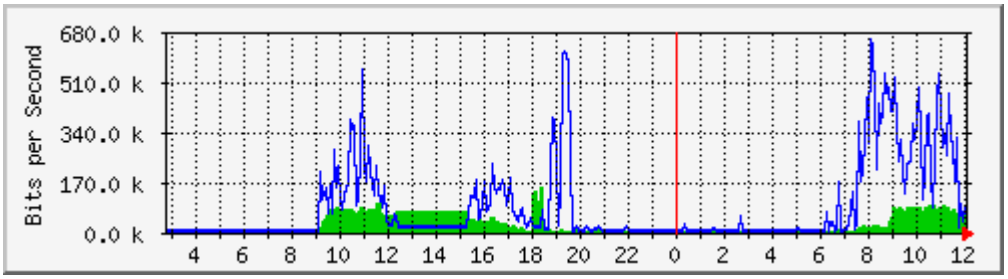
[ANEXO Nº 2]

[Estadísticas generadas por *MRTG*]

The statistics were last updated Tuesday, 13 September 2005 at 12:09,

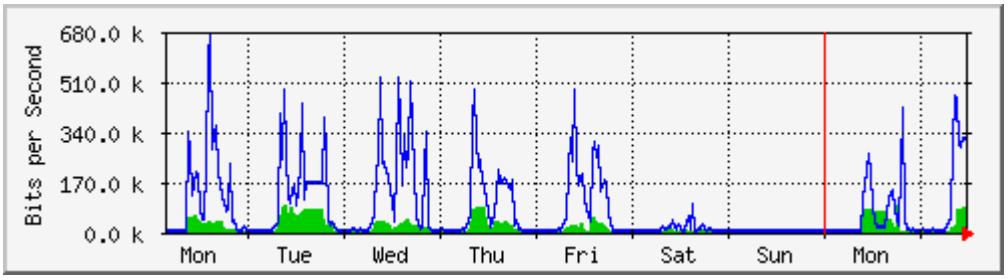
at which time 'rt-odc-kpmg' had been up for 107 days, 22:53:38.

`Daily' Graph (5 Minute Average)



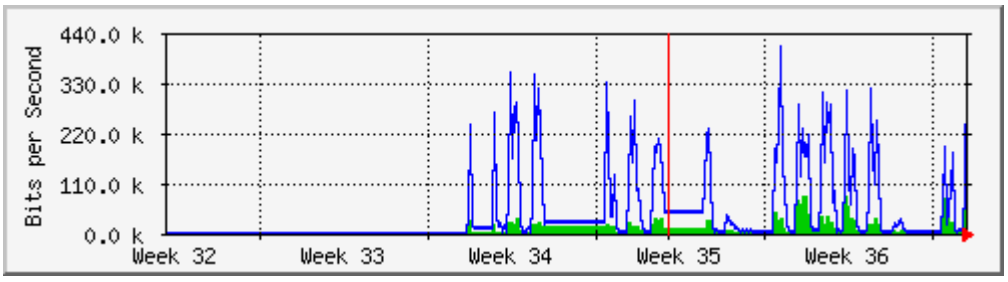
	Max	Average	Current
In	153.9 kb/s (20.0%)	25.6 kb/s (3.3%)	29.0 kb/s (3.8%)
Out	648.5 kb/s (84.4%)	81.9 kb/s (10.7%)	37.6 kb/s (4.9%)

`Weekly' Graph (30 Minute Average)



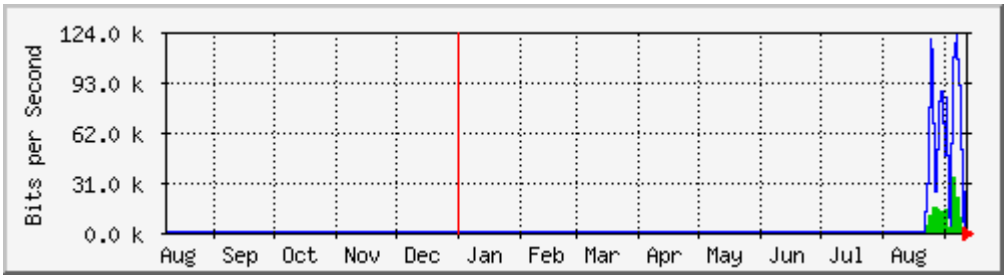
	Max	Average	Current
In	93.8 kb/s (12.2%)	16.0 kb/s (2.1%)	81.1 kb/s (10.6%)
Out	660.0 kb/s (85.9%)	76.3 kb/s (9.9%)	323.2 kb/s (42.1%)

`Monthly' Graph (2 Hour Average)

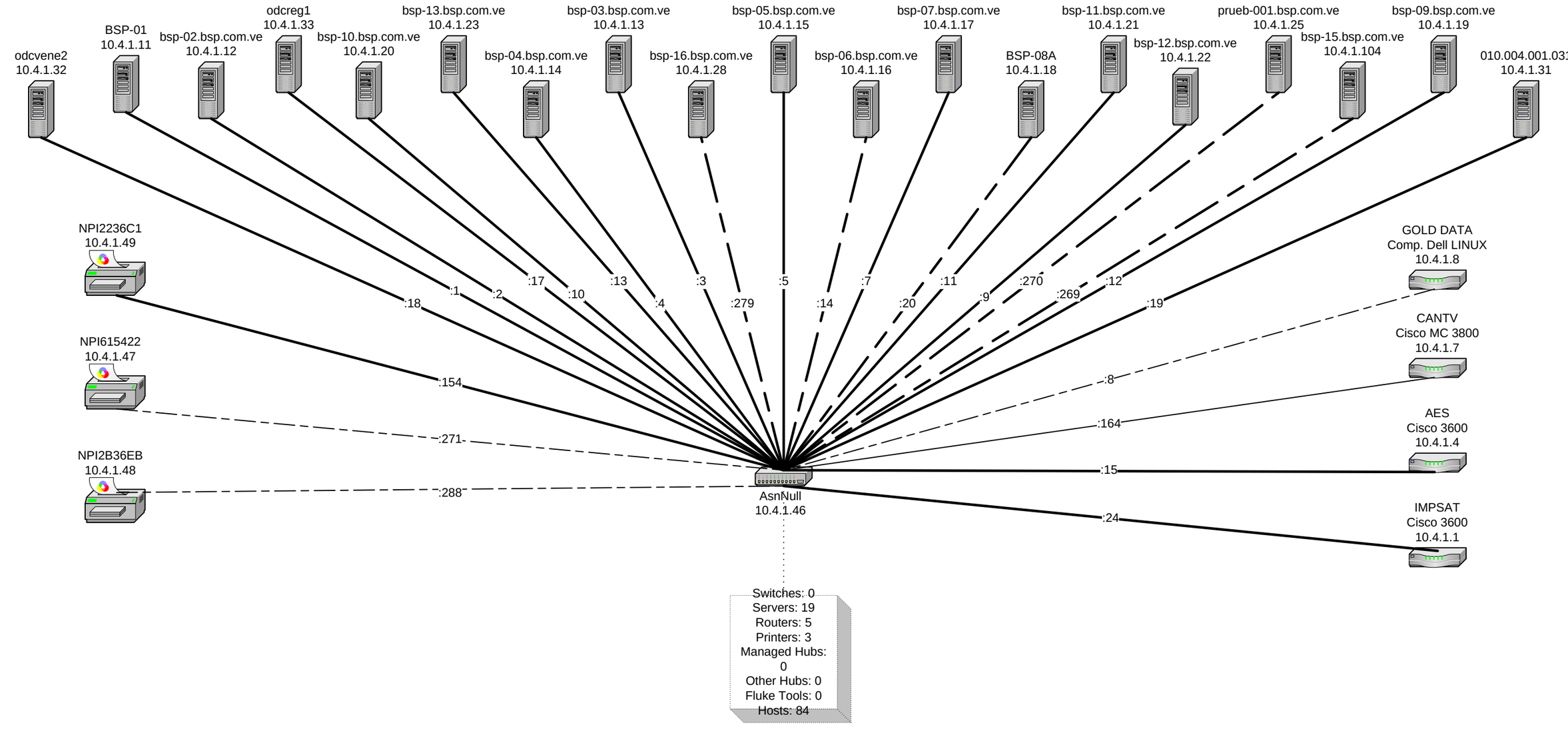


	Max	Average	Current
In	81.2 kb/s (10.6%)	12.1 kb/s (1.6%)	51.4 kb/s (6.7%)
Out	406.2 kb/s (52.9%)	64.6 kb/s (8.4%)	373.6 kb/s (48.6%)

`Yearly' Graph (1 Day Average)

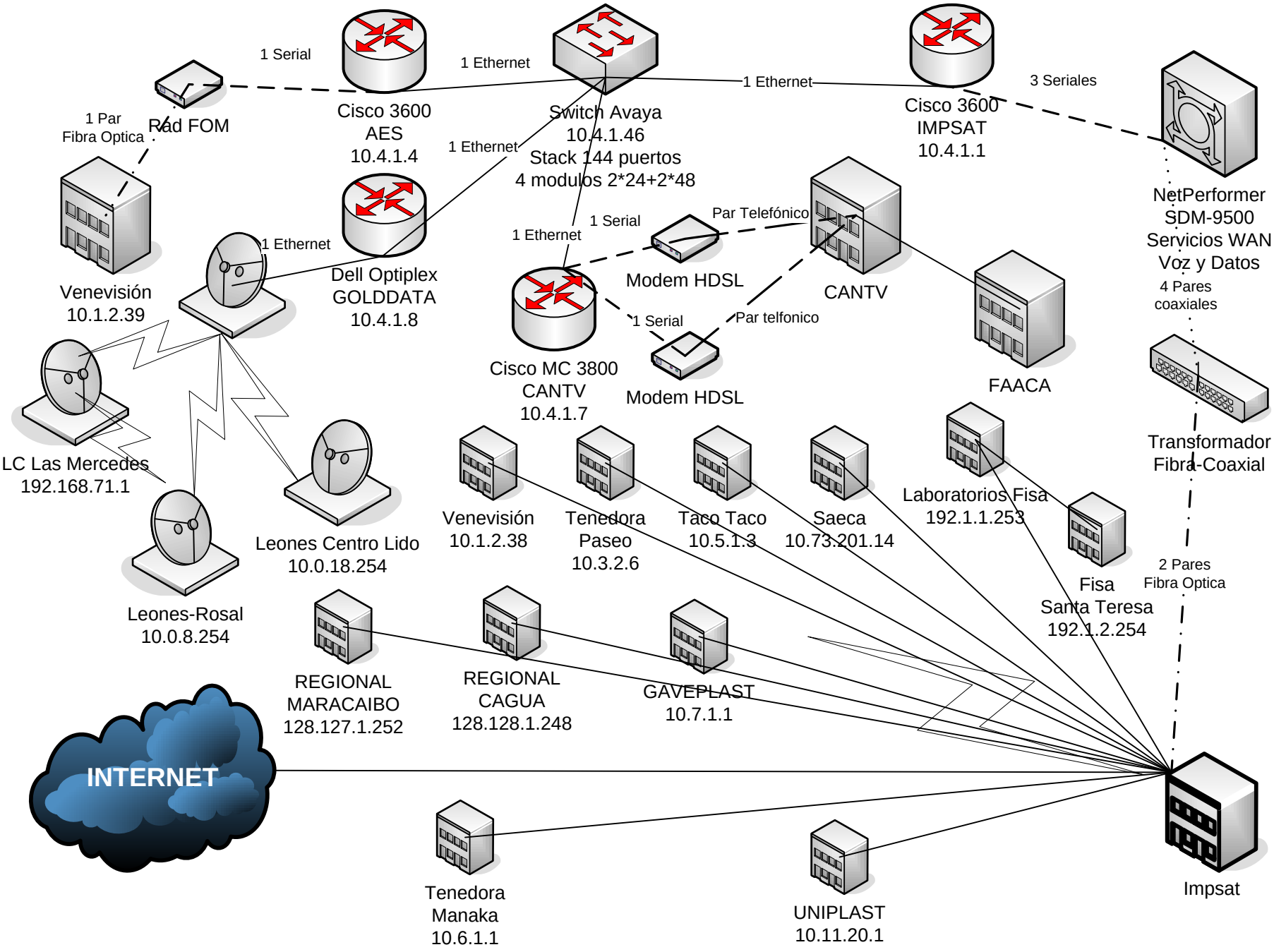


	Max	Average	Current
In	34.3 kb/s (4.5%)	11.7 kb/s (1.5%)	23.5 kb/s (3.1%)
Out	122.0 kb/s (15.9%)	62.2 kb/s (8.1%)	49.4 kb/s (6.4%)



Database: Inspector
Status as of: September 2, 2005 4:56pm

Generated by: Network Inspector - Fluke Networks, Inc. (www.flukenetworks.com)


1 Serial
1 Ethernet
1 Ethernet
3 Seriales
1 Par
Fibra Optica
Rad FOM
Cisco 3600
AES
10.4.1.4
Switch Avaya
10.4.1.46
Stack 144 puertos
4 modulos 2*24+2*48
Cisco 3600
IMPSAT
10.4.1.1
NetPerformer
SDM-9500
Servicios WAN
Voz y Datos
1 Ethernet
1 Ethernet
1 Serial
Par Telefónico
Venevisión
10.1.2.39
Dell Optiplex
GOLDDATA
10.4.1.8
Modem HDSL
CANTV
4 Pares
coaxiales
1 Serial
Par telfonico
Cisco MC 3800
CANTV
10.4.1.7
Modem HDSL
FAACA
Transformador
Fibra-Coaxial
LC Las Mercedes
192.168.71.1
Venevisión
10.1.2.38
Tenedora
Paseo
10.3.2.6
Taco Taco
10.5.1.3
Saeca
10.73.201.14
Laboratorios Fisa
192.1.1.253
Leones Centro Lido
10.0.18.254
Leones-Rosal
10.0.8.254
Fisa
Santa Teresa
192.1.2.254
2 Pares
Fibra Optica
REGIONAL
MARACAIBO
128.127.1.252
REGIONAL
CAGUA
128.128.1.248
GAVEPLAST
10.7.1.1
INTERNET
Impsat
Tenedora
Manaka
10.6.1.1
UNIPLAST
10.11.20.1

October 27, 2005
14:58:46

IP Inventory

Subnet/Name	MAC Address	IP Address	Subnet Mask	SNMP	IP Services: HTTP	IP Services: E-mail	IP Services: Print
Subnet: 010.004.001.000			**255.255.255.000**				
010.002.001.002	IBM-ded6a3	010.002.001.002					
010.002.001.003	IBM-3ed4c2	010.002.001.003					
010.004.001.001	00b064-f04501	010.004.001.001					
IP Services: EIGRP Router, Static Router, Proxy Arp Router							
010.004.001.003	Ipsiln-1f1444	010.004.001.003					
010.004.001.004	0008e3-b5a3a1	010.004.001.004			ü		
IP Services: Static Router, Proxy Arp Router, HTTP							
010.004.001.030	LANNET-f88800	010.004.001.030		ü	ü		
IP Services: 802.1d Switch, HTTP							
010.004.001.031	IBM-ded653	010.004.001.031			ü		
010.004.001.038	00096b-dd1bfa	010.004.001.038					
010.004.001.039	00096b-dd1aca	010.004.001.039					
apadron.bsp.com.ve	GATEWY-137894	010.004.001.175					
AsnNull	LANNET-8ad32c	010.004.001.046		ü	ü		
BSP	Dell-238551	010.004.001.008		ü			
IP Services: Static Router							
BSP-01	000255-fc3c26	010.004.001.011					
IP Services: DNS							
bsp-02.bsp.com.ve	000255-fc350d	010.004.001.012					
IP Services: DNS, WINS							
bsp-03.bsp.com.ve	000255-fc3502	010.004.001.013			ü		
IP Services: DHCP, DNS, HTTP							
bsp-04.bsp.com.ve	BBN-2eb01a	010.004.001.014			ü		
IP Services: DNS, HTTP							
bsp-05.bsp.com.ve	000255-fc2a70	010.004.001.015			ü		
bsp-06.bsp.com.ve	000255-fc23e5	010.004.001.016		ü	ü		
bsp-07.bsp.com.ve	3Com-2f2244	010.004.001.017			ü		
BSP-08A	000255-fc347a	010.004.001.018		ü	ü		
bsp-09.bsp.com.ve	3Com-2f223f	010.004.001.019			ü		
bsp-10.bsp.com.ve	000255-fc3bf1	010.004.001.020			ü		
bsp-11.bsp.com.ve	000255-fc3bfc	010.004.001.021					
bsp-12.bsp.com.ve	000255-fc350f	010.004.001.022			ü		
bsp-13.bsp.com.ve	000255-fc34c4	010.004.001.023			ü		
bsp-15.bsp.com.ve	000d56-fd8917	010.004.001.104		ü	ü		
bsp-16.bsp.com.ve	000e0c-372f20	010.004.001.028		ü			
bsp-27.bsp.com.ve	000f1f-6706a2	010.004.001.027					
bsp-acoello.bsp.com.ve	001143-626738	010.004.001.089			ü		
bsp-asalcedo.bsp.com.ve	GATEWY-3062de	010.004.001.161					
bsp-cgarcia.bsp.com.ve	000f1f-0c22ba	010.004.001.067			ü		
bsp-consulto14.bsp.com.ve	000e7b-34b629	010.004.001.086			ü		
BSP-CONSULTO15	000e7b-507a2a	010.004.001.109					
bsp-consulto23.bsp.com.ve	000103-7fc686	010.004.001.100					
bsp-consulto23.bsp.com.ve	000103-8a6a53	010.004.001.100					
bsp-consultor27.bsp.com.ve	000255-db668c	010.004.001.134					
bsp-ebustamante.bsp.com.ve	000255-db60de	010.004.001.121					
bsp-ecastillo.bsp.com.ve	GATEWY-3062fd	010.004.001.131					
bsp-eramirez.bsp.com.ve	000d56-cb9d75	010.004.001.173					
bsp-fehernandez.bsp.com.ve	000476-2ac5dc	010.004.001.179					
bsp-iazuaje.bsp.com.ve	00023f-7f224a	010.004.001.144					
bsp-jsolares.bsp.com.ve	000d56-1bd864	010.004.001.091					

IP Inventory

Subnet/Name	MAC Address	IP Address	Subnet Mask	SNMP	IP Services: HTTP	IP Services: E-mail	IP Services: Print
Subnet: 010.004.001.000			**255.255.255.000**				
BSP-LREGALADO	Sony-dc54de	010.004.001.098			ü		
bsp-lregalado.bsp.com.ve	000d60-5e1953	010.004.001.093					
bsp-malvarado.bsp.com.ve	000d56-1bdf8b	010.004.001.172					
bsp-msilva.bsp.com.ve	BBN-2b5143	010.004.001.169					
bsp-mvelasquez.bsp.com.ve	000f1f-0c21a3	010.004.001.090					
bsp-mvillav.bsp.com.ve	00023f-7bf76b	010.004.001.185			ü		
bsp-ocuevas.bsp.com.ve	GATEWY-306311	010.004.001.165					
bsp-rcabrera.bsp.com.ve	000255-db6195	010.004.001.148					
bsp-sbs.bsp.com.ve	000255-db64b5	010.004.001.098			ü		
bsp-ventrafil.bsp.com.ve	000255-db5f97	010.004.001.026					
bsp-xteran.bsp.com.ve	000f1f-0c22d7	010.004.001.124					
bsp-yhenriquez.bsp.com.ve	000255-db5d7c	010.004.001.136					
bsp-ysanchez-1.bsp.com.ve IP Services: DHCP	000255-db668b	010.004.001.174					
c1mcampo040204.peoplesoft.co IP Services: Static Router, HTTP	000d60-5e1dac	010.004.001.092			ü		
cartigas2.bsp.com.ve	001143-0af62e	010.004.001.069					
cbittar.bsp.com.ve IP Services: Static Router, Proxy Arp Router	000476-2b4803	010.004.001.166					
cdevia.bsp.com.ve	3Com-20bae6	010.004.001.141					
cgarcia_2.bsp.com.ve	000d56-1bdcff	010.004.001.156					
cgarcia-home.bsp.com.ve	000347-916e6b	010.004.001.088					
cmoreno.bsp.com.ve	BBN-2b47a7	010.004.001.160					
config-01.bsp.com.ve	000d60-b21613	010.004.001.102					
config-02.bsp.com.ve	000255-db53c3	010.004.001.132					
consul13.bsp.com.ve	000d56-1aa9cd	010.004.001.127			ü		
contral-03.bsp.com.ve	000255-db613f	010.004.001.181					
curso01.bsp.com.ve	BBN-d6c29a	010.004.001.152					
cvargas1	000255-db35fb	010.004.001.188			ü		
cvargas1.bsp.com.ve	001143-0a776e	010.004.001.064			ü		
d6j5bp61.bsp.com.ve	001143-1412e1	010.004.001.095					
edelgado1.bsp.com.ve	BolMan-5092a8	010.004.001.065		ü	ü		
edelgado1.bsp.com.ve	BBN-2ec5d0	010.004.001.184					
egonzalez-laptop.bsp.com.ve	000f1f-0c214b	010.004.001.158					
eguerra-ve.ve.oracle.com	AMBIT-26387d	010.004.001.097					
ejcampos.bsp.com.ve	001143-0ac9e8	010.004.001.146					
elparra.bsp.com.ve	00508b-ad26a5	010.004.001.110					
esarmiento.bsp.com.ve	INTEL-58a23e	010.004.001.135					
gbaptista.bsp.com.ve	000d56-1bd87b	010.004.001.122			ü		
gmartinez.bsp.com.ve	000d56-1be523	010.004.001.125			ü		
ibm-9grlr7g19pe.bsp.com.ve	AMBIT-d92edf	010.004.001.099			ü		
jcova.bsp.com.ve	001143-0ac0b2	010.004.001.151					
jmanuel.bsp.com.ve	000255-db5f8a	010.004.001.170					
jpadulo.bsp.com.ve	AMBIT-33de07	010.004.001.108					
jpadulo.bsp.com.ve	AMBIT-3409ed	010.004.001.187					
laptop	000e0c-372e68	010.004.001.101		ü	ü		
LAPTOPDELL1	000f1f-0c213f	010.004.001.087					
laptopdell3.bsp.com.ve	000f1f-0c2190	010.004.001.145			ü		
laptopdell4.bsp.com.ve	000f1f-0c25f9	010.004.001.103					
laptopdell7.bsp.com.ve	000f1f-0c2113	010.004.001.157					
larraiz1.bsp.com.ve	000255-db62a4	010.004.001.155					
mariavilla.bsp.com.ve	000d56-1be298	010.004.001.147					
mgutierrez.bsp.com.ve	BBN-d6c227	010.004.001.167					
mlucero.bsp.com.ve	000476-2b4c4b	010.004.001.168					
mrios-1.bsp.com.ve	000476-2ac40c	010.004.001.159					
mrondon.bsp.com.ve	000476-2b4e23	010.004.001.182					

IP Inventory

Subnet/Name	MAC Address	IP Address	Subnet Mask	SNMP	IP Services: HTTP	IP Services: E-mail	IP Services: Print
Subnet: 010.004.001.000			**255.255.255.000**				
mvelasquez.bsp.com.ve	BBN-d71095	010.004.001.178					
NPI2236C1	0001e6-2236c1	010.004.001.049	010.004.001.049	ü	ü		ü
NPI2B36EB	0001e6-2b36eb	010.004.001.048	010.004.001.048	ü	ü		ü
NPI615422	0001e6-615422	010.004.001.047	010.004.001.047	ü	ü		ü
oandrade.bsp.com.ve	BBN-2b4eb7	010.004.001.186					
odc-kwj2yinc499.bsp.com.ve	000d56-1be60d	010.004.001.230			ü		
odc-p0l6db24ete.bsp.com.ve	000255-db5c3d	010.004.001.138					
odcreg1	f00629-6c7be6	010.004.001.033	255.255.000.000	ü	ü		
odcvene2	IBM-3ed4ec	010.004.001.035		ü	ü		
odcvene2	f004ac-3ed4ec	010.004.001.032	255.255.000.000	ü	ü		
odiegidi-ve.ve.oracle.com	000d60-5e1972	010.004.001.094					
pasan001.bsp.com.ve	GATEWY-30636b	010.004.001.142			ü		
prueba1.bsp.com.ve	BBN-d6bd66	010.004.001.183					
rrhh10.bsp.com.ve	3Com-cecab7	010.004.001.150					
rrodriguezc.bsp.com.ve	000d56-1aa760	010.004.001.200			ü		
tec-2002.bsp.com.ve	0002b9-90511a	010.004.001.007					
tecno-1.bsp.com.ve	000255-db612f	010.004.001.123			ü		
tecno-15.bsp.com.ve	3Com-ac3da5	010.004.001.143					
tvca-gbolet.bsp.com.ve	BBN-2b47a1	010.004.001.137					
VFERRERI	001125-af899b	010.004.001.111					
WORKCENTRE	Xerox-656a83	010.004.001.041		ü	ü		
Subnet: 010.010.010.000			**255.255.255.000**				
010.010.010.010	LANNET-8ae09a	010.010.010.010					
010.010.010.010	LANNET-b17400	010.010.010.010					
Subnet: 010.011.020.000			**255.255.255.000**				
bsp-acoello.bsp.com.ve	001143-626738	010.011.020.013			ü		
bsp-cgarcia.bsp.com.ve	000f1f-0c22ba	010.011.020.019			ü		
bsp-consulto14.bsp.com.ve	000e7b-34b629	010.011.020.018			ü		
bsp-mvillav.bsp.com.ve	00023f-7bf76b	010.011.020.017			ü		
ibm-9grlr7g19pe.bsp.com.ve	AMBIT-d92edf	010.011.020.016			ü		
Subnet: 135.050.000.000			**255.255.000.000**				
c1mcampo040204.peoplesoft.co	000d60-5e1dac	135.050.004.253			ü		
IP Services: Static Router, HTTP							
Subnet: 169.254.000.000			**255.255.000.000**				
bsp-asalcedo.bsp.com.ve	GATEWY-3062de	169.254.200.218					
bsp-iazuaje.bsp.com.ve	00023f-7f224a	169.254.177.083					
bsp-rcabrera.bsp.com.ve	000255-db6195	169.254.164.252					
cdevia.bsp.com.ve	3Com-20bae6	169.254.051.238					
contral-03.bsp.com.ve	000255-db613f	169.254.069.247					
curso01.bsp.com.ve	BBN-d6c29a	169.254.248.223					
cvargas1.bsp.com.ve	001143-0a776e	169.254.034.205			ü		
edelgado1.bsp.com.ve	BBN-2ec5d0	169.254.212.204					
gmartinez.bsp.com.ve	000d56-1be523	169.254.054.025			ü		
ibm-9grlr7g19pe.bsp.com.ve	AMBIT-d92edf	169.254.148.226			ü		
jmanuel.bsp.com.ve	000255-db5f8a	169.254.068.166					
larraiz1.bsp.com.ve	000255-db62a4	169.254.163.003					
mgutierrez.bsp.com.ve	BBN-d6c227	169.254.156.044					
oandrade.bsp.com.ve	BBN-2b4eb7	169.254.253.037					
prueba1.bsp.com.ve	BBN-d6bd66	169.254.011.219					
Subnet: 192.168.000.000			**255.255.255.000**				
bsp-ysanchez-1.bsp.com.ve	000255-db668b	192.168.000.001					
IP Services: DHCP							

Switch Detail

010.004.001.030

MAC Address: LANNET-f88800
IP Address: 010.004.001.030
Subnet Mask: 255.255.255.000
Interfaces: 145
Up: 86
Down: 59

SNMP

Name:
Description: Avaya Inc. - P330 Stackable Switch, SW version 4.1.1
Location:
Contact:
Uptime: 25 days, 20 hours, 44 minutes
OID: 1.3.6.1.4.1.81.17.1.17
Comm. String: public

I/F Index 100

(Avaya Inc. - P330 Stackable Switch, SW version 4.1.1)

Interface: Up, Prop Virtual, RMON
Speed: 0 Bits/sec
MTU: 0

Port 1

(Avaya Inc. - P333R 10/100Base-Tx Port 1 on Unit 1)

Interface: Up, Ethernet, RMON
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.03%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-02.bsp.com.ve	000255-fc350d	010.004.001.012

Port 2

(Avaya Inc. - P333R 10/100Base-Tx Port 2 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
BSP-08A	000255-fc347a	010.004.001.018

Port 3

(Avaya Inc. - P333R 10/100Base-Tx Port 3 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-13.bsp.com.ve	000255-fc34c4	010.004.001.023

Port 4

(Avaya Inc. - P333R 10/100Base-Tx Port 4 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.05%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-12.bsp.com.ve	000255-fc350f	010.004.001.022

Port 5

(Avaya Inc. - P333R 10/100Base-Tx Port 5 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.65%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-04.bsp.com.ve	BBN-2eb01a	010.004.001.014

Port 6

(Avaya Inc. - P333R 10/100Base-Tx Port 6 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-06.bsp.com.ve	000255-fc23e5	010.004.001.016

Switch Detail

Port 7

(Avaya Inc. - P333R 10/100Base-Tx Port 7 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
laptop	000e0c-372e68	010.004.001.025
laptop	000e0c-372e68	010.004.001.101

Port 8

(Avaya Inc. - P333R 10/100Base-Tx Port 8 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.16%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-15.bsp.com.ve	000d56-fd8917	010.004.001.104

Port 9

(Avaya Inc. - P333R 10/100Base-Tx Port 9 on Unit 1)

Interface: Up, Ethernet
Speed: 10 MBits/sec
MTU: 1522
Utilization: 0.04%

Directly Connected Devices

Name	MAC Address	IP Address
tec-2002.bsp.com.ve	0002b9-90511a	010.004.001.007

Port 10

(Avaya Inc. - P333R 10/100Base-Tx Port 10 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
010.004.001.038	00096b-dd1bfa	010.004.001.038

Port 11

(Avaya Inc. - P333R 10/100Base-Tx Port 11 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.16%

Directly Connected Devices

Name	MAC Address	IP Address
010.004.001.039	00096b-dd1aca	010.004.001.039

Port 12

(Avaya Inc. - P333R 10/100Base-Tx Port 12 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.13%

Directly Connected Devices

Name	MAC Address	IP Address
010.004.001.004	0008e3-b5a3a1	010.004.001.004

Port 13

(Avaya Inc. - P333R 10/100Base-Tx Port 13 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.04%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-10.bsp.com.ve	000255-fc3bf1	010.004.001.020

Port 14

(Avaya Inc. - P333R 10/100Base-Tx Port 14 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.02%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-07.bsp.com.ve	3Com-2f2244	010.004.001.017

Port 15

(Avaya Inc. - P333R 10/100Base-Tx Port 15 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.38%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-03.bsp.com.ve	000255-fc3502	010.004.001.013

Switch Detail

Port 16

(Avaya Inc. - P333R 10/100Base-Tx Port 16 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-11.bsp.com.ve	000255-fc3bfc	010.004.001.021

Port 17

(Avaya Inc. - P333R 10/100Base-Tx Port 17 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.08%

Directly Connected Devices

Name	MAC Address	IP Address
BSP-01	000255-fc3c26	010.004.001.011

Port 18

(Avaya Inc. - P333R 10/100Base-Tx Port 18 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.11%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-09.bsp.com.ve	3Com-2f223f	010.004.001.019

Port 19

(Avaya Inc. - P333R 10/100Base-Tx Port 19 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.16%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-05.bsp.com.ve	000255-fc2a70	010.004.001.015

Port 20

(Avaya Inc. - P333R 10/100Base-Tx Port 20 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.07%

Directly Connected Devices

Name	MAC Address	IP Address
odcvene2	IBM-3ed4ec	010.004.001.032
odcvene2	f004ac-3ed4ec	010.004.001.032
odcvene2	IBM-3ed4ec	010.004.001.035

Port 21

(Avaya Inc. - P333R 10/100Base-Tx Port 21 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.04%

Directly Connected Devices

Name	MAC Address	IP Address
odcreg1	f00629-6c7be6	010.004.001.033

Port 22

(Avaya Inc. - P333R 10/100Base-Tx Port 22 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.11%

Directly Connected Devices

Name	MAC Address	IP Address
010.004.001.031	IBM-ded653	010.004.001.031

Port 23

(Avaya Inc. - P333R 10/100Base-Tx Port 23 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.73%

Directly Connected Devices

Name	MAC Address	IP Address
010.004.001.003	Ipsiln-1f1444	010.004.001.003

Port 24

(Avaya Inc. - P333R 10/100Base-Tx Port 24 on Unit 1)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 1.43%

Directly Connected Devices

Name	MAC Address	IP Address
010.004.001.001	00b064-f04501	010.004.001.001

Switch Detail

Port 129

(Avaya Inc. - P333T 10/100Base-Tx Port 1 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 130

(Avaya Inc. - P333T 10/100Base-Tx Port 2 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 131

(Avaya Inc. - P333T 10/100Base-Tx Port 3 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 132

(Avaya Inc. - P333T 10/100Base-Tx Port 4 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.08%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-16.bsp.com.ve	000e0c-372f20	010.004.001.028

Port 133

(Avaya Inc. - P333T 10/100Base-Tx Port 5 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 134

(Avaya Inc. - P333T 10/100Base-Tx Port 6 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
ejcampos.bsp.com.ve	001143-0ac9e8	010.004.001.146

Port 135

(Avaya Inc. - P333T 10/100Base-Tx Port 7 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-27.bsp.com.ve	000f1f-6706a2	010.004.001.027

Port 136

(Avaya Inc. - P333T 10/100Base-Tx Port 8 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 137

(Avaya Inc. - P333T 10/100Base-Tx Port 9 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
BSP	Dell-238551	010.004.001.008

Switch Detail

Port 138

(Avaya Inc. - P333T 10/100Base-Tx Port 10 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
010.002.001.002	IBM-ded6a3	010.002.001.002

Port 139

(Avaya Inc. - P333T 10/100Base-Tx Port 11 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
esarmiento.bsp.com.ve	INTEL-58a23e	010.004.001.135

Port 140

(Avaya Inc. - P333T 10/100Base-Tx Port 12 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 141

(Avaya Inc. - P333T 10/100Base-Tx Port 13 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 142

(Avaya Inc. - P333T 10/100Base-Tx Port 14 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 143

(Avaya Inc. - P333T 10/100Base-Tx Port 15 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.12%

Directly Connected Devices

Name	MAC Address	IP Address
jpadulo.bsp.com.ve	AMBIT-3409ed	010.004.001.108
jpadulo.bsp.com.ve	AMBIT-3409ed	010.004.001.187

Port 144

(Avaya Inc. - P333T 10/100Base-Tx Port 16 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.02%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-malvarado.bsp.com.ve	000d56-1bdf8b	010.004.001.172

Port 145

(Avaya Inc. - P333T 10/100Base-Tx Port 17 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.02%

Directly Connected Devices

Name	MAC Address	IP Address
cvargas1.bsp.com.ve	001143-0a776e	010.004.001.064
cvargas1.bsp.com.ve	001143-0a776e	169.254.034.205

Port 146

(Avaya Inc. - P333T 10/100Base-Tx Port 18 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
jcova.bsp.com.ve	001143-0ac0b2	010.004.001.151

Switch Detail

Port 147

(Avaya Inc. - P333T 10/100Base-Tx Port 19 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
elparra.bsp.com.ve	00508b-ad26a5	010.004.001.110
gbaptista.bsp.com.ve	000d56-1bd87b	010.004.001.122

Port 148

(Avaya Inc. - P333T 10/100Base-Tx Port 20 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 149

(Avaya Inc. - P333T 10/100Base-Tx Port 21 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 150

(Avaya Inc. - P333T 10/100Base-Tx Port 22 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 151

(Avaya Inc. - P333T 10/100Base-Tx Port 23 on Unit 2)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
tecno-1.bsp.com.ve	000255-db612f	010.004.001.123

Port 152

(Avaya Inc. - P333T 10/100Base-Tx Port 24 on Unit 2)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 257

(Lucent - Cajun P334T 10/100Base-Tx Port 1 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-consulto23.bsp.com.ve	000103-8a6a53	010.004.001.087
bsp-consulto23.bsp.com.ve	000103-8a6a53	010.004.001.100

Port 258

(Lucent - Cajun P334T 10/100Base-Tx Port 2 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.05%

Directly Connected Devices

Name	MAC Address	IP Address
jmanuel.bsp.com.ve	000255-db5f8a	010.004.001.170
jmanuel.bsp.com.ve	000255-db5f8a	169.254.068.166

Port 259

(Lucent - Cajun P334T 10/100Base-Tx Port 3 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-yhenriquez.bsp.com.ve	000255-db5d7c	010.004.001.136

Switch Detail

Port 260

(Lucent - Cajun P334T 10/100Base-Tx Port 4 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-ebustamante.bsp.com.ve	000255-db60de	010.004.001.121

Port 261

(Lucent - Cajun P334T 10/100Base-Tx Port 5 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.02%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-ysanchez-1.bsp.com.ve	000255-db668b	010.004.001.174
bsp-ysanchez-1.bsp.com.ve	000255-db668b	192.168.000.001

Port 262

(Lucent - Cajun P334T 10/100Base-Tx Port 6 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.10%

Directly Connected Devices

Name	MAC Address	IP Address
prueba1.bsp.com.ve	BBN-d6bd66	010.004.001.183
prueba1.bsp.com.ve	BBN-d6bd66	169.254.011.219

Port 263

(Lucent - Cajun P334T 10/100Base-Tx Port 7 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
tecno-15.bsp.com.ve	3Com-ac3da5	010.004.001.143

Port 264

(Lucent - Cajun P334T 10/100Base-Tx Port 8 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
contral-03.bsp.com.ve	000255-db613f	010.004.001.181
contral-03.bsp.com.ve	000255-db613f	169.254.069.247

Port 265

(Lucent - Cajun P334T 10/100Base-Tx Port 9 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-rcabrera.bsp.com.ve	000255-db6195	010.004.001.148
bsp-rcabrera.bsp.com.ve	000255-db6195	169.254.164.252

Port 266

(Lucent - Cajun P334T 10/100Base-Tx Port 10 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 267

(Lucent - Cajun P334T 10/100Base-Tx Port 11 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
ibm-9grlr7g19pe.bsp.com.ve	AMBIT-d92edf	010.004.001.099
ibm-9grlr7g19pe.bsp.com.ve	AMBIT-d92edf	010.011.020.016
ibm-9grlr7g19pe.bsp.com.ve	AMBIT-d92edf	169.254.148.226

Port 268

(Lucent - Cajun P334T 10/100Base-Tx Port 12 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
curso01.bsp.com.ve	BBN-d6c29a	010.004.001.152
curso01.bsp.com.ve	BBN-d6c29a	169.254.248.223

Switch Detail

Port 269

(Lucent - Cajun P334T 10/100Base-Tx Port 13 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
config-02.bsp.com.ve	000255-db53c3	010.004.001.132

Port 270

(Lucent - Cajun P334T 10/100Base-Tx Port 14 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
VFERRERI	001125-af899b	010.004.001.111

Port 271

(Lucent - Cajun P334T 10/100Base-Tx Port 15 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
tvca-gbolet.bsp.com.ve	BBN-2b47a1	010.004.001.137

Port 272

(Lucent - Cajun P334T 10/100Base-Tx Port 16 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
BSP-CONSULTO15	000e7b-507a2a	010.004.001.094
BSP-CONSULTO15	000e7b-507a2a	010.004.001.109

Port 273

(Lucent - Cajun P334T 10/100Base-Tx Port 17 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
egonzalez-laptop.bsp.com.ve	000f1f-0c214b	010.004.001.158

Port 274

(Lucent - Cajun P334T 10/100Base-Tx Port 18 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 275

(Lucent - Cajun P334T 10/100Base-Tx Port 19 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 276

(Lucent - Cajun P334T 10/100Base-Tx Port 20 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
larraiz1.bsp.com.ve	000255-db62a4	010.004.001.155
larraiz1.bsp.com.ve	000255-db62a4	169.254.163.003

Port 277

(Lucent - Cajun P334T 10/100Base-Tx Port 21 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-ecastillo.bsp.com.ve	GATEWY-3062fd	010.004.001.131

Switch Detail

Port 278

(Lucent - Cajun P334T 10/100Base-Tx Port 22 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
edelgado1.bsp.com.ve	BBN-2ec5d0	010.004.001.184
edelgado1.bsp.com.ve	BBN-2ec5d0	169.254.212.204

Port 279

(Lucent - Cajun P334T 10/100Base-Tx Port 23 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.22%

Directly Connected Devices

Name	MAC Address	IP Address
mariavilla.bsp.com.ve	000d56-1be298	010.004.001.147

Port 280

(Lucent - Cajun P334T 10/100Base-Tx Port 24 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 281

(Lucent - Cajun P334T 10/100Base-Tx Port 25 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-asalcedo.bsp.com.ve	GATEWY-3062de	010.004.001.161
bsp-asalcedo.bsp.com.ve	GATEWY-3062de	169.254.200.218

Port 282

(Lucent - Cajun P334T 10/100Base-Tx Port 26 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
NPI2236C1	0001e6-2236c1	010.004.001.049
rrhh10.bsp.com.ve	3Com-cecab7	010.004.001.150

Port 283

(Lucent - Cajun P334T 10/100Base-Tx Port 27 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
pasan001.bsp.com.ve	GATEWY-30636b	010.004.001.142

Port 284

(Lucent - Cajun P334T 10/100Base-Tx Port 28 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
mrondon.bsp.com.ve	000476-2b4e23	010.004.001.182

Port 285

(Lucent - Cajun P334T 10/100Base-Tx Port 29 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 286

(Lucent - Cajun P334T 10/100Base-Tx Port 30 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
oandrade.bsp.com.ve	BBN-2b4eb7	010.004.001.186
oandrade.bsp.com.ve	BBN-2b4eb7	169.254.253.037

Switch Detail

Port 287

(Lucent - Cajun P334T 10/100Base-Tx Port 31 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-eramirez.bsp.com.ve	000d56-cb9d75	010.004.001.173

Port 288

(Lucent - Cajun P334T 10/100Base-Tx Port 32 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
mlucero.bsp.com.ve	000476-2b4c4b	010.004.001.168

Port 289

(Lucent - Cajun P334T 10/100Base-Tx Port 33 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 290

(Lucent - Cajun P334T 10/100Base-Tx Port 34 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-ocuevas.bsp.com.ve	GATEWY-306311	010.004.001.165

Port 291

(Lucent - Cajun P334T 10/100Base-Tx Port 35 on Unit 3)

Interface: Up, Ethernet
Speed: 10 MBits/sec
MTU: 1522
Utilization: 0.04%

Directly Connected Devices

Name	MAC Address	IP Address
edelgado1.bsp.com.ve	BolMan-5092a8	010.004.001.065

Port 292

(Lucent - Cajun P334T 10/100Base-Tx Port 36 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
cgarcia_2.bsp.com.ve	000d56-1bdcff	010.004.001.156

Port 293

(Lucent - Cajun P334T 10/100Base-Tx Port 37 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
mgutierrez.bsp.com.ve	BBN-d6c227	010.004.001.167
mgutierrez.bsp.com.ve	BBN-d6c227	169.254.156.044

Port 294

(Lucent - Cajun P334T 10/100Base-Tx Port 38 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
odc-p0l6db24ete.bsp.com.ve	000255-db5c3d	010.004.001.138

Port 295

(Lucent - Cajun P334T 10/100Base-Tx Port 39 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
consul13.bsp.com.ve	000d56-1aa9cd	010.004.001.127

Switch Detail

Port 296

(Lucent - Cajun P334T 10/100Base-Tx Port 40 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
rrodriguezc.bsp.com.ve	000d56-1aa760	010.004.001.200

Port 297

(Lucent - Cajun P334T 10/100Base-Tx Port 41 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-jsolares.bsp.com.ve	000d56-1bd864	010.004.001.091

Port 298

(Lucent - Cajun P334T 10/100Base-Tx Port 42 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.02%

Directly Connected Devices

Name	MAC Address	IP Address
gmartinez.bsp.com.ve	000d56-1be523	010.004.001.125
gmartinez.bsp.com.ve	000d56-1be523	169.254.054.025

Port 299

(Lucent - Cajun P334T 10/100Base-Tx Port 43 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-consultor27.bsp.com.ve	000255-db668c	010.004.001.134

Port 300

(Lucent - Cajun P334T 10/100Base-Tx Port 44 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.03%

Directly Connected Devices

Name	MAC Address	IP Address
cartigas2.bsp.com.ve	001143-0af62e	010.004.001.069

Port 301

(Lucent - Cajun P334T 10/100Base-Tx Port 45 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
odc-kwj2yinc499.bsp.com.ve	000d56-1be60d	010.004.001.107
odc-kwj2yinc499.bsp.com.ve	000d56-1be60d	010.004.001.110
odc-kwj2yinc499.bsp.com.ve	000d56-1be60d	010.004.001.230

Port 302

(Lucent - Cajun P334T 10/100Base-Tx Port 46 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
d6j5bp61.bsp.com.ve	001143-1412e1	010.004.001.095

Port 303

(Lucent - Cajun P334T 10/100Base-Tx Port 47 on Unit 3)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 1.51%

Directly Connected Devices

Name	MAC Address	IP Address
cvargas1	000255-db35fb	010.004.001.188

Port 304

(Lucent - Cajun P334T 10/100Base-Tx Port 48 on Unit 3)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
eguerra-ve.ve.oracle.com	AMBIT-26387d	010.004.001.097
jpadulo.bsp.com.ve	AMBIT-33de07	010.004.001.108

Switch Detail

Port 385

(Lucent - Cajun P334T 10/100Base-Tx Port 1 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 386

(Lucent - Cajun P334T 10/100Base-Tx Port 2 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 387

(Lucent - Cajun P334T 10/100Base-Tx Port 3 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 388

(Lucent - Cajun P334T 10/100Base-Tx Port 4 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 389

(Lucent - Cajun P334T 10/100Base-Tx Port 5 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 390

(Lucent - Cajun P334T 10/100Base-Tx Port 6 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 391

(Lucent - Cajun P334T 10/100Base-Tx Port 7 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 392

(Lucent - Cajun P334T 10/100Base-Tx Port 8 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 393

(Lucent - Cajun P334T 10/100Base-Tx Port 9 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Switch Detail

Port 394

(Lucent - Cajun P334T 10/100Base-Tx Port 10 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 395

(Lucent - Cajun P334T 10/100Base-Tx Port 11 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
BSP-LREGALADO	Sony-dc54de	010.004.001.093
BSP-LREGALADO	Sony-dc54de	010.004.001.098

Port 396

(Lucent - Cajun P334T 10/100Base-Tx Port 12 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 397

(Lucent - Cajun P334T 10/100Base-Tx Port 13 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 398

(Lucent - Cajun P334T 10/100Base-Tx Port 14 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 399

(Lucent - Cajun P334T 10/100Base-Tx Port 15 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
NPI615422	0001e6-615422	010.004.001.047

Port 400

(Lucent - Cajun P334T 10/100Base-Tx Port 16 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
apadron.bsp.com.ve	GATEWY-137894	010.004.001.175

Port 401

(Lucent - Cajun P334T 10/100Base-Tx Port 17 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-fehernandez.bsp.com.ve	000476-2ac5dc	010.004.001.179
bsp-msilva.bsp.com.ve	BBN-2b5143	010.004.001.169
mvelasquez.bsp.com.ve	BBN-d71095	010.004.001.178

Port 402

(Lucent - Cajun P334T 10/100Base-Tx Port 18 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Switch Detail

Port 403

(Lucent - Cajun P334T 10/100Base-Tx Port 19 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 404

(Lucent - Cajun P334T 10/100Base-Tx Port 20 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 405

(Lucent - Cajun P334T 10/100Base-Tx Port 21 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 406

(Lucent - Cajun P334T 10/100Base-Tx Port 22 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 407

(Lucent - Cajun P334T 10/100Base-Tx Port 23 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 408

(Lucent - Cajun P334T 10/100Base-Tx Port 24 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-cgarcia.bsp.com.ve	000f1f-0c22ba	010.004.001.067
bsp-cgarcia.bsp.com.ve	000f1f-0c22ba	010.011.020.019

Port 409

(Lucent - Cajun P334T 10/100Base-Tx Port 25 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
c1mcampo040204.peoplesoft.	000d60-5e1dac	010.004.001.092
c1mcampo040204.peoplesoft.	000d60-5e1dac	135.050.004.253

Port 410

(Lucent - Cajun P334T 10/100Base-Tx Port 26 on Unit 4)

Interface: Up, Ethernet
Speed: 10 MBits/sec
MTU: 1522
Utilization: 0.12%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-sbs.bsp.com.ve	000255-db64b5	010.004.001.098
bsp-ventrafil.bsp.com.ve	000255-db5f97	010.004.001.026
odiegidi-ve.ve.oracle.com	000d60-5e1972	010.004.001.094

Port 411

(Lucent - Cajun P334T 10/100Base-Tx Port 27 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
cbittar.bsp.com.ve	000476-2b4803	010.004.001.166

Switch Detail

Port 412

(Lucent - Cajun P334T 10/100Base-Tx Port 28 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 413

(Lucent - Cajun P334T 10/100Base-Tx Port 29 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 414

(Lucent - Cajun P334T 10/100Base-Tx Port 30 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.04%

Directly Connected Devices

Name	MAC Address	IP Address
WORKCENTRE	Xerox-656a83	010.004.001.041

Port 415

(Lucent - Cajun P334T 10/100Base-Tx Port 31 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 416

(Lucent - Cajun P334T 10/100Base-Tx Port 32 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
NPI2B36EB	0001e6-2b36eb	010.004.001.048

Port 417

(Lucent - Cajun P334T 10/100Base-Tx Port 33 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-mvelasquez.bsp.com.ve	000f1f-0c21a3	010.004.001.090

Port 418

(Lucent - Cajun P334T 10/100Base-Tx Port 34 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
laptopdell7.bsp.com.ve	000f1f-0c2113	010.004.001.157

Port 419

(Lucent - Cajun P334T 10/100Base-Tx Port 35 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 420

(Lucent - Cajun P334T 10/100Base-Tx Port 36 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
cgarcia-home.bsp.com.ve	000347-916e6b	010.004.001.066
cgarcia-home.bsp.com.ve	000347-916e6b	010.004.001.088

Switch Detail

Port 421

(Lucent - Cajun P334T 10/100Base-Tx Port 37 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
cdevia.bsp.com.ve	3Com-20bae6	010.004.001.141
cdevia.bsp.com.ve	3Com-20bae6	169.254.051.238

Port 422

(Lucent - Cajun P334T 10/100Base-Tx Port 38 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-xteran.bsp.com.ve	000f1f-0c22d7	010.004.001.124

Port 423

(Lucent - Cajun P334T 10/100Base-Tx Port 39 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.06%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-consulto14.bsp.com.ve	000e7b-34b629	010.004.001.086
bsp-consulto14.bsp.com.ve	000e7b-34b629	010.011.020.018

Port 424

(Lucent - Cajun P334T 10/100Base-Tx Port 40 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 425

(Lucent - Cajun P334T 10/100Base-Tx Port 41 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 426

(Lucent - Cajun P334T 10/100Base-Tx Port 42 on Unit 4)

Interface: Up, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.01%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-iazuaje.bsp.com.ve	00023f-7f224a	010.004.001.144
bsp-iazuaje.bsp.com.ve	00023f-7f224a	169.254.177.083

Port 427

(Lucent - Cajun P334T 10/100Base-Tx Port 43 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
laptopdell4.bsp.com.ve	000f1f-0c25f9	010.004.001.103

Port 428

(Lucent - Cajun P334T 10/100Base-Tx Port 44 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
bsp-acoello.bsp.com.ve	001143-626738	010.004.001.089
bsp-acoello.bsp.com.ve	001143-626738	010.011.020.013

Port 429

(Lucent - Cajun P334T 10/100Base-Tx Port 45 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
laptopdell3.bsp.com.ve	000f1f-0c2190	010.004.001.096
laptopdell3.bsp.com.ve	000f1f-0c2190	010.004.001.145

Switch Detail

Port 430

(Lucent - Cajun P334T 10/100Base-Tx Port 46 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Directly Connected Devices

Name	MAC Address	IP Address
LAPTOPDELL1	000f1f-0c213f	010.004.001.066
LAPTOPDELL1	000f1f-0c213f	010.004.001.087

Port 431

(Lucent - Cajun P334T 10/100Base-Tx Port 47 on Unit 4)

Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

Port 432

(Lucent - Cajun P334T 10/100Base-Tx Port 48 on Unit 4)

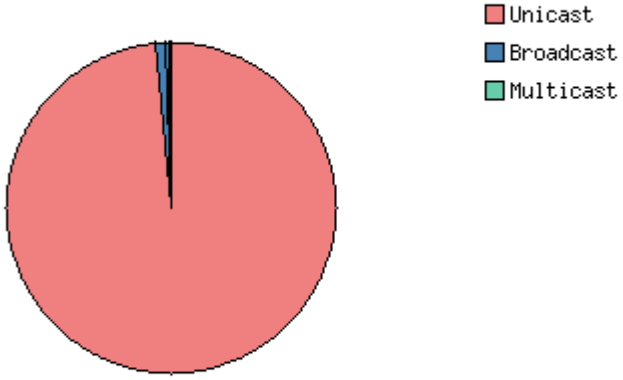
Interface: Down, Ethernet
Speed: 100 MBits/sec
MTU: 1522
Utilization: 0.00%

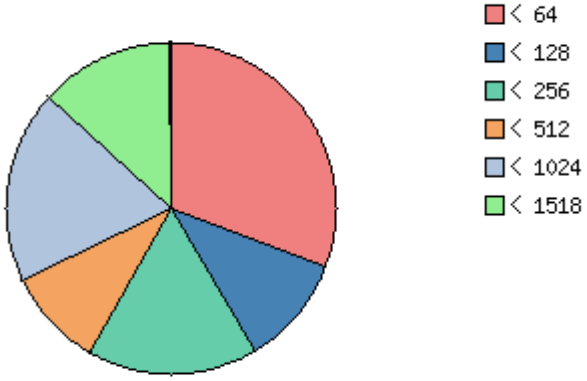
Directly Connected Devices

Name	MAC Address	IP Address
bsp-mvillav.bsp.com.ve	00023f-7bf76b	010.004.001.185
bsp-mvillav.bsp.com.ve	00023f-7bf76b	010.011.020.017

[ANEXO Nº 7]

[Estadísticas de NTOP]

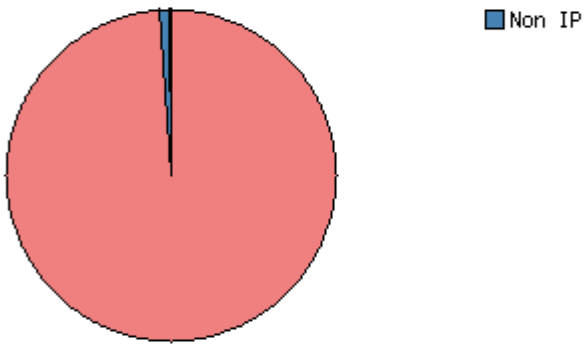
Packets	**Dropped (libpcap)**	6.6%	133,729
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		2,013,133
	Total Packets Processed		2,013,133
	Unicast	98.8%	1,989,133
	Broadcast	0.9%	18,291
	Multicast	0.3%	5,709
			
	Shortest		42 bytes
	Average Size		382 bytes
	Longest		1,514 bytes
	< 64 bytes	31.0%	623,417
	< 128 bytes	10.9%	218,914
	< 256 bytes	16.9%	340,801
	< 512 bytes	9.9%	198,645
	< 1024 bytes	19.2%	386,600
	< 1518 bytes	12.2%	244,756
	> 1518 bytes	0.0%	0



Packets too long [> 1514]	0.0%	0
Bad Packets (Checksum)	0.0%	0

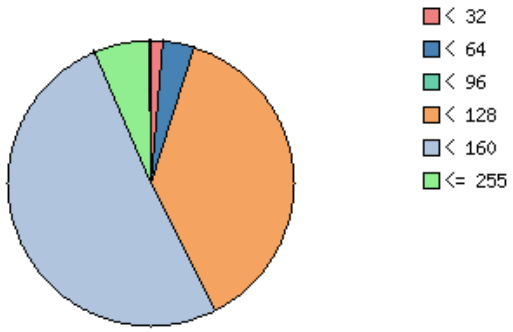
Traffic

Total	743.6 MB [2,013,133 Pkts]
IP Traffic	743.0 MB [743.0 MB Pkts]
Fragmented IP Traffic	1.6 MB [0.2%]
Non IP Traffic	668.8 KB

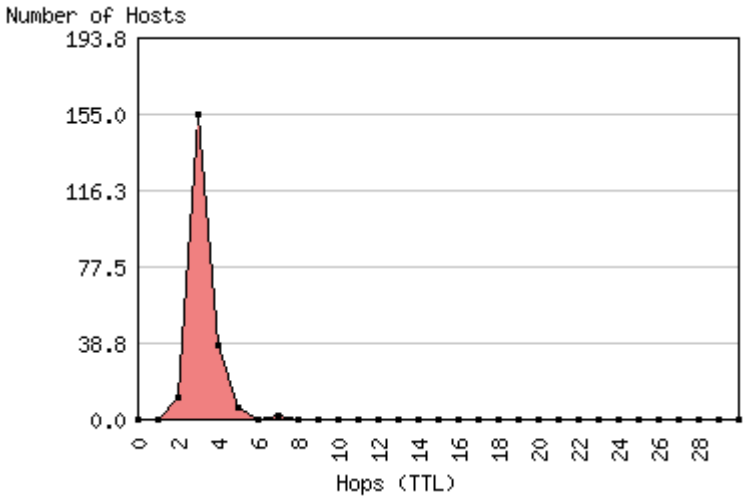


Average TTL		131
TTL < 32	1.4%	28,550
32 < TTL < 64	3.9%	79,332

	64 < TTL < 96	0.2%	4,772
	96 < TTL < 128	37.4%	753,484
	128 < TTL < 160	51.0%	1,026,189
	160 < TTL < 192	0.0%	0
	192 < TTL < 224	0.0%	0
	224 < TTL < 256	5.4%	109,271



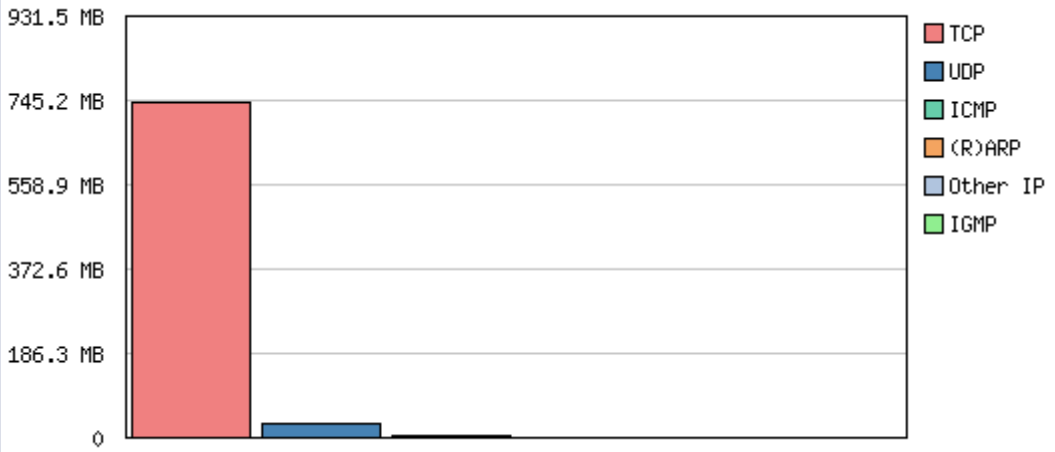
Remote Hosts Distance



Network Load	**Actual**	982.2 Kbps	273.6 Pkts/sec
	Last Minute	1.0 Mbps	270.5 Pkts/sec
	Last 5 Minutes	557.8 Kbps	144.9 Pkts/sec
	Peak	1.0 Mbps	273.6 Pkts/sec
	Average	377.9 Kbps	122.0 Pkts/sec

Global Protocol Distribution

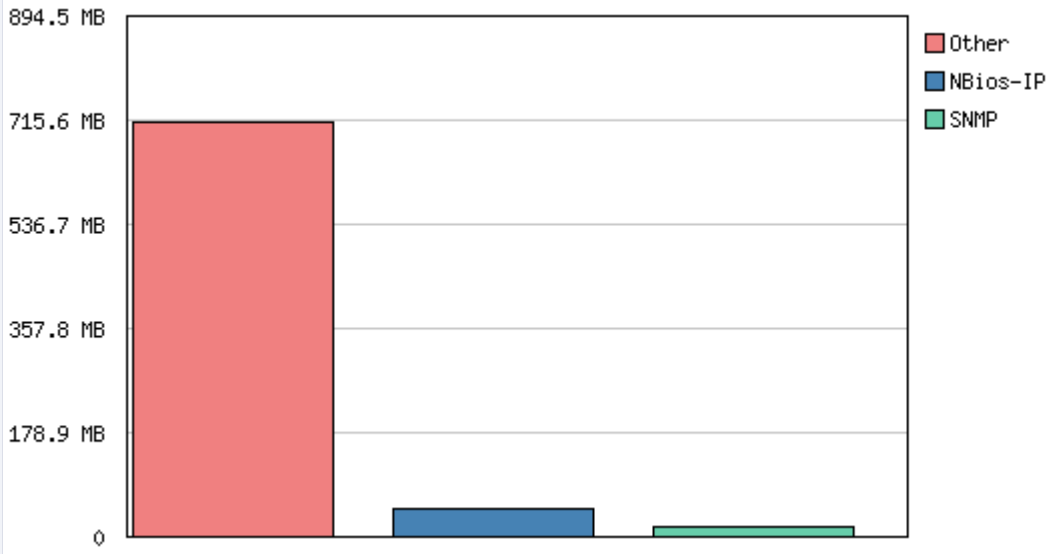
Protocol	Data	Percentage			
IP	743.0 MB	99.9%	**TCP**	707.2 MB	95 %
			UDP	30.5 MB	4%
			ICMP	4.9 MB	0%
			IGMP	0.3 KB	0%
			Other IP	346.0 KB	0%
(R)ARP	511.1 KB	0%			



Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Percentage
http	1.6 MB	0%
DNS	3.1 MB	0%
NBios-IP	38.3 MB	5%
Mail	556.7 KB	0%
DHCP-BOOTP	529.1 KB	0%
SNMP	17.3 MB	2%
NFS/AFS	305.1 KB	0%
Kazaa	30.9 KB	0%

eDonkey	13.8 KB	0%	
Messenger	174.0 KB	0%	
Other TCP/UDP-based Protocols	681.0 MB	91%	



TCP/UDP Traffic Port Distribution:

Last Minute View

TCP/UDP Port		Total	Sent	Rcvd
3139	3139	1006.2 KB	38.1 KB	968.1 KB
netbios-ssn	139	1002.2 KB	965.7 KB	36.5 KB
7001	7001	993.1 KB	807.3 KB	185.8 KB
8080	8080	416.4 KB	325.7 KB	90.7 KB
48373	48373	352.4 KB	30.3 KB	322.0 KB
445	445	206.4 KB	194.6 KB	11.8 KB
1080	1080	197.5 KB	5.2 KB	192.3 KB
2146	2146	131.2 KB	14.5 KB	116.7 KB