ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

OPTIMIZACIÓN DE LA RED WAN DE PETROCOMERCIAL MEDIANTE ENLACES PDH Y EL USO DEL PROTOCOLO ETHERNET EN LOS EQUIPOS DE BORDE CON PLATAFORMA CON SERVICIOS INTEGRADOS

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN ELECTRONICA Y REDES DE INFORMACIÓN

MAURO DANILO RON LARCO
mdron@com.eppetroecuador.ec

DAVID FERNANDO SILVA VIZCARRA
dsilva@com.eppetroecuador.ec

DIRECTOR: ING JACK VIDAL
vidal.net@gmail.com

Quito, Mayo 2011

DECLARACIÓN

Nosotros, Mauro Danilo Ron Larco y David Fernando Silva Vizcarra, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Mauro Danilo Ron Larco David Fernando Silva Vizcarra

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Mauro Danilo Ron Larco y David Fernando Silva Vizcarra, bajo mi supervisión.

ING. JACK VIDAL.
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Al Ing. Jack Vidal por apoyarnos en el desarrollo del proyecto de grado, a todos los compañeros de PETROECUADOR por la apertura y acceso a la información brindada.

A la Escuela Politécnica Nacional y a todos aquellos que nos acompañaron durante nuestros años universitarios, a todos nuestros profesores, compañeros y amigos.

Mauro Ron y David Silva

DEDICATORIA

A Dios por haber iluminado mi camino, a mis hermanos por ser el pilar de mi vida en especial a mi hermano Diego por siempre haberme apoyado, a mi madre por estar conmigo, a mi novia Jhadira por estar a mi lado en los momentos más difíciles.

Mauro Danilo Ron Larco

DEDICATORIA

A Dios por ser mi guía y confidente en todo momento, A mis Padres, Miguel y Janet, que gracias a su apoyo, paciencia y amor estoy alcanzando un logro más en la vida, A mi ñaña Jane y mi novia Majo que siempre me brindan su apoyo y cariño, A mis Abuelitos, Vicente y Norita, Ángel y Maritza, que doy las gracias de tenerlos junto a mí. Y a toda mi familia y amigos.

David Fernando Silva Vizcarra

RESUMEN

El presente proyecto realiza el diseño de la optimización de la red WAN de PETROCOMERCIAL, basado en el uso del protocolo Ethernet y la integración de servicios en los ruteadores, teniendo como fin una mejor utilización de los recursos de red y de las capacidades de ancho de banda de los enlaces.

En el Capítulo I, se revisan los conceptos, principios, protocolos y tecnologías, necesarios para el diseño de la solución, luego se describen los modelos de gestión de red, que permitirán desarrollar un modelo para los equipos de enrutamiento propuestos de la red WAN, finalmente se indican los conceptos de la integración de servicios en equipos Cisco.

En el capítulo II, se describe la situación actual de la red de PETROCOMERCIAL enfocado a las capas: aplicación, red, enlace de datos y física de acuerdo al modelo ISO/OSI, incluyendo las topologías de las capas de red, enlace de datos y física, este estudio permitirá un dimensionamiento adecuado de la solución planteada en el proyecto, además se realiza un análisis de tráfico para determinar el estado actual de los enlaces existentes. Al final del capítulo se presenta una descripción de los equipos utilizados actualmente.

En el capítulo III, con la información recopilada en los capítulos I y II se realiza el diseño de la topología lógica planteada para el presente proyecto. En base al diseño propuesto y al requerimiento de las aplicaciones se procede a dimensionar la capacidad de los enlaces. Con los cálculos realizados se indican los equipos necesarios para implementar el proyecto y sus características. Al determinar los equipos requeridos se establece un costo referencial del proyecto. Finalmente se

elabora un plan de migración para reducir los efectos negativos en el desempeño de la empresa.

En el capítulo IV se presenta el modelo de configuración de los equipos, tanto para el enrutamiento de datos como para telefonía IP, que será utilizado en un prototipo empleando el programa GNS3 y equipos físicos, además se desarrolla el modelo de gestión necesario para los ruteadores propuestos. Y en la parte final de este capítulo se plantea un plan de recuperación de fallas.

En el capítulo V se establecen las conclusiones y recomendaciones del proyecto, además en los anexos se presentan las configuraciones finales de los equipos y los diagramas de la red de PETROCOMERCIAL.

PRESENTACIÓN

Debido a la evolución de los equipos y medios de transmisión, Ethernet ha pasado de ser un protocolo destinado a redes de área local a redes que cubren extensiones territoriales considerables. La evolución de la fibra óptica y el desarrollo de radios microondas con soporte para Ethernet permiten cubrir extensiones en el orden de las decenas y centenas de Km.

El principio de funcionamiento de Ethernet, es la utilización de un método de acceso al medio que permite su uso conforme sea requerido, de esta forma el medio es aprovechado de mejor forma en ambientes en los cuales existe tráfico a ráfagas.

El presente proyecto está orientado a plantear una solución, para permitir la optimización de los recursos de red, utilizando el protocolo Ethernet para una mejor utilización de la capacidad de los enlaces WAN de PETROCOMERCIAL.

El desarrollo de la integración de servicios se da principalmente gracias a la introducción de los sistemas LINUX, los cuales ofrecen una amplia variedad de servicios de red en una misma plataforma, teniendo la ventaja de ser un sistema operativo robusto y de libre distribución y como desventaja el poco soporte técnico que se puede obtener en problemas que se puedan presentar.

Es común encontrar equipos que ofrecen una gama de servicios de red (Correo, Servidor WEB, Firewall) que corren sobre LINUX, integrando en un solo equipo físico varias funcionalidades de red.

Como respuesta a este abrumador crecimiento de equipos basados en LINUX, las marcas convencionales de equipo de internetworking han buscado soluciones

orientadas a integración de servicios, la solución que ofrece CISCO integra servicios en sus equipos de enrutamiento.

Los equipos CISCO que soportan integración de servicios, ofrecen funcionalidades de Telefonía IP, Firewalls, etc. Para la solución de Telefonía IP CISCO integra en sus equipos de enrutamiento una central telefónica IP, llamada CISCO CALL MANAGER, existiendo dos tipos de versiones, la versión EXPRESS orientada a las pequeñas y medianas empresas, y la versión ENTERPRISE orientada a grandes empresas.

El presente proyecto plantea la utilización de integración de servicios aprovechando el hardware adquirido para el enrutamiento de datos, con el fin de ofrecer adicionalmente el servicio de telefonía IP.

Los modelos de Gestión de redes permiten monitorear, gestionar y controlar los recursos de una red, por lo que su implementación en toda red debería ser imprescindible, por lo que el proyecto plantea un modelo de gestión de red para los ruteadores propuestos de la red WAN de PETROCOMERCIAL, considerando que no existe un modelo de gestión de red en la empresa.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ANEXOS

CAPÍTULO I

1. INTRODUCCIÓN

El presente capítulo tiene el objetivo de exponer el fundamento teórico necesario para el desarrollo del proyecto propuesto. En un comienzo se estudia el modelo ISO/OSI y la arquitectura de red TCP/IP. Luego se detallan las tecnologías de capa enlace de datos y de transporte de información. Además se revisan conceptos y funcionamiento de los modelos de gestión, y por último se detallará la integración de servicios.

1.1. MODELOS DE REFERENCIAS Y ARQUITECTURAS DE RED

Existen dos modelos de referencia en el que se puede basar el diseño de una arquitectura de red, los modelo ISO/OSI y TCP/IP, este último también se lo considera como una arquitectura.

1.1.1. MODELO ISO/OSI

Modelo de referencia desarrollado por la ISO, separa las funciones que se deben realizar en niveles o capas, cada capa realiza una función y se comunica solo con su capa par en el dispositivo con el que se realiza la comunicación, cada capa ofrece servicios a la capa superior a través de interfaces o sap (puntos de acceso al servicio). Define siete niveles o capas, que se indican en la figura 1.1.

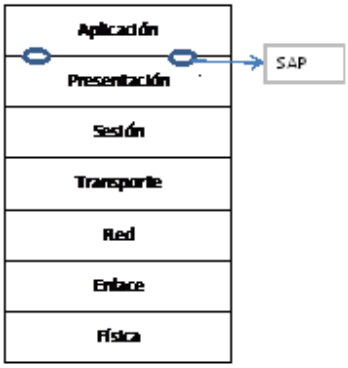


Figura 1.1 Capas del modelo OSI

1.1.2. MODELO Y ARQUITECTURA TCP/IP

TCP/IP después de su desarrollo se convirtió prontamente en un estándar de facto gracias a su gran aceptación. Define los protocolos que se utilizan en cada capa, por lo que se lo considera además de ser un modelo como una arquitectura de red.

1.1.2.1. Introducción

TCP/IP fue desarrollado y presentado por el Departamento de Defensa de EE.UU en 1972 y fue aplicado en ARPANET (Advanced Research Projects Agency Network), red que conectaba las computadoras de oficinas gubernamentales y universitarias. Funciona bajo el concepto de cliente servidor, lo que significa que alguna computadora pide los servicios de otra computadora; la primera es el cliente y la segunda el servidor. ARPANET evolucionó a lo que hoy en día se conoce como INTERNET.

La estructura fundamental de la arquitectura TCP/IP es la de un sistema de conmutación de paquetes. Esta conmutación consiste en la división de datos a transmitirse en pequeños fragmentos denominados paquetes, los cuales se los conmuta individualmente a través de diferentes caminos mediantes ruteadores. Entre las ventajas de conmutación de paquetes tenemos que permite multiplexar en una

misma conexión varias comunicaciones. Pero la desventaja es que no ofrece una capacidad garantizada.

1.1.2.2. Capas de la arquitectura TCP/IP

El conjunto de protocolos TCP/IP se estructura en cuatro capas como se indica en la figura 1.2:

- Aplicación
- Transporte
- Internet
- Interfaz de red (Acceso a red)

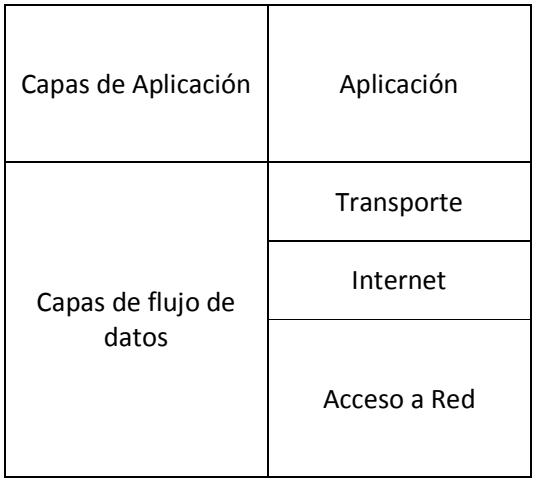


Figura 1.2 Modelo TCP/IP

1.1.2.2.1. Capa Aplicación

La capa aplicación interactúa con la capa transporte entregándole y recibiendo de ésta los mensajes requeridos por la aplicación. Los protocolos de capa de aplicación de TCP/IP son aquellos que permiten el envío y recepción de la información del usuario. Estos protocolos determinan las reglas para el intercambio de información de control y el formato necesario para muchas de las funciones de comunicación. Algunos de los protocolos de la capa aplicación son: DNS, HTTP, SMTP, Telnet, FTP.

1.1.2.2.2. Capa transporte

La capa transporte realiza la comunicación extremo a extremo entre procesos pares de capa aplicación en host diferentes. Puede proveer un transporte confiable asegurándose de que los datos lleguen sin errores y en la secuencia correcta.

La capa de transporte provee de dos protocolos que permite a las aplicaciones comunicarse independientemente del tipo de red (es decir, independientemente de las capas inferiores), estos protocolos son UDP y TCP.

1.1.2.2.2.1. Protocolo de datagramas de usuario (UDP)

UDP es un protocolo no orientado a conexión, descrito en la RFC 768. Puede enviar datos sin utilizar muchos recursos. Las unidades de datos de protocolo (PDU) en UDP se llaman datagramas, y son enviados en base al mejor esfuerzo. Cada datagrama de UDP posee 8 bytes de carga en el encabezado, encapsulando los datos de la capa de aplicación. En la figura 1.3 se indica los campos que conforman el encabezado de un datagrama UDP.

Las aplicaciones que utilizan UDP incluyen: Sistema de nombres de dominio (DNS), Streaming de video, Voz sobre IP (VoIP).

Puerto de Origen 16 bits	Puerto dedestino 16 bits
Longitud 16 bits	Checksum 16 bits
Datos de la capa aplicación (tamaño variable)	

Figura 1.3 Encabezado UDP

1.1.2.2.2.2. Protocolo de control de transmisión (TCP)

El protocolo de control de transmisión es orientado a la conexión y está descrito en el RFC 793. TCP utiliza recursos adicionales para realizar funciones de control. Estas funciones son la entrega confiable y el control de flujo. Cada segmento de TCP posee como mínimo 20 bytes de carga en el encabezado, encapsulando los datos de la capa de aplicación. En la figura 1.4 se observa los campos de un datagrama TCP.

Las aplicaciones que utiliza el TCP son: Exploradores Web, Correo electrónico, Transferencias de archivos.

<table>
<tr><td colspan="3">Puerto de Origen 16 bits</td><td>Puerto dedestino 16 bits</td></tr>
<tr><td colspan="4">Número de Secuencia 32 bits</td></tr>
<tr><td colspan="4">Número de Acuse de recibo 32bits</td></tr>
<tr><td>Longitud de encabezado 4 bits</td><td>Reservado 6 bits</td><td>Bits de código 6 bits</td><td>Ventana 16 bits</td></tr>
<tr><td colspan="3">Checksum 16 bits</td><td>Urgente 16 bits</td></tr>
<tr><td colspan="4">Opciones 0 0 32 bits (Opcional)</td></tr>
<tr><td colspan="4">Datos de la capa aplicación (tamaño variable)</td></tr>
</table>

Figura 1.4 Encabezado TCP

1.1.2.2.3. Capa Internet

La capa internet es la encargada del movimiento de los paquetes, originarios de la capa transporte, de un equipo a otro a través de la red. Encapsula los segmentos en paquetes IP que serán enviados por la capa inferior. Además realiza la desencapsulación de las tramas recibidas, y los pasa a la capa transporte. Algunos ejemplos de protocolos en este nivel se indican a continuación:

- IP (Internet Protocol): Es un protocolo de envío de datos no orientado a conexión, no confiable.
- ICMP (Internet Control Message Protocol): Usado por IP para intercambiar mensajes de control y error entre nodos.
- IGMP (Internet Group Management Protocol): Utilizados para informar a un ruteador local que se desea recibir paquetes multicast.
- ARP (Address Resolution Protocol): Este protocolo permite relacionar la dirección física de un dispositivo con su correspondiente dirección IP.
- RARP (Reverse Address Resolution Protocol): Este protocolo funciona de forma inversa a ARP, lo que quiere decir que permite relacionar la dirección IP de un dispositivo con su correspondiente dirección física.

- Protocolos de Enrutamiento: Son un conjunto de reglas utilizadas por los ruteadores para aprender rutas y mantener actualizada su tabla de enrutamiento conforme cambia la red[1].

1.1.2.2.3.1. Datagrama IP

Un datagrama IP está formado por una cabecera y un campo de datos (Figura 1.5). En el campo de datos se encapsulan los paquetes: TCP, UDP, ICMP, IGMP, etc.

<table>
<tr><td colspan="2">Ver 4 bits</td><td>HLEN 4 bits</td><td>Tipo de servicio 8 bits</td><td colspan="2">Longitud Total 16 bits</td></tr>
<tr><td colspan="3">Identificación 16 bits</td><td>Banderas 3 bits</td><td colspan="2">Desplazamiento de Fragmento 13 bits</td></tr>
<tr><td colspan="2">TTL 8 bits</td><td>Protocolo 8 bits</td><td colspan="3">Checksum del encabezado 16 bits</td></tr>
<tr><td colspan="6">Dirección de origen 32 bits</td></tr>
<tr><td colspan="6">Dirección de destino 32 bits</td></tr>
<tr><td colspan="5">Opciones 24 bits</td><td>Relleno 8 bits</td></tr>
<tr><td colspan="6">Datos</td></tr>
<tr><td colspan="6">.....</td></tr>
</table>

Figura 1.5 Campos del Datagrama IP

- *Versión*: El campo versión ocupa 4 bits. Este campo hace que diferentes versiones del protocolo IP puedan operar en la Internet (versión 4 o versión 6).
- *Longitud de la Cabecera:* Este campo ocupa 4 bits, y representa el número de octetos de la cabecera dividido por cuatro.
- *Tipo de servicio:* Utiliza un valor binario de 8 bits que especifica como un protocolo de capa superior desea le sean enviados sus datagramas a través de la subred de comunicaciones[2].
- *Longitud Total:* Este campo se utiliza para identificar el número de octetos en el datagrama.

[1,2] Ings. Mónica Vinueza – Pablo Hidalgo, Folleto de Redes TCP-IP, Marzo 2008

- *Identificación:* El valor del campo identificación es un número secuencial asignado por el Host origen. Ocupa dos octetos.
- *Señalizador:* Campo de 3 bits que representan los señalizadores de control, MF (Señalizador de Más fragmentos) y DF (Señalizador de No Fragmentar)
- *Desplazamiento de fragmentos:* Cuando el tamaño de un datagrama excede el MTU (Unidad Máxima de Transmisión), éste se segmenta. El campo desplazamiento del fragmento permite ordenar los fragmentos del paquete en la reconstrucción.
- *Tiempo de Vida:* El campo tiempo de vida ocupa 8 bits y es usado para representar el número máximo de saltos que un datagrama puede existir en una red, antes de ser desechado. Un Datagrama puede existir un máximo de 255 saltos. Si el datagrama es descartado se envía un paquete ICMP al emisor.
- *Protocolo:* Valor binario de 8 bits, determina el tipo de dato que el paquete traslada. Permitiendo a la capa de red pasar los datos al protocolo apropiado de la capa superior. Valores de ejemplo son: 01 (ICMP), 06 (TCP), 17 (UDP)
- *Checksum*: El checksum proporciona un método de seguridad para determinar si el datagrama ha sido dañado o modificado. Este campo tiene una longitud de 16 bits. El checksum incluye todos los campos de la cabecera IP.
- *Dirección de Origen:* Este campo contiene un identificador de red (Netid) y un identificador de Host (Hostid). El campo tiene una longitud de 32 bits que representa la dirección del host de capa de red de origen del paquete.
- *Dirección de Destino:* El campo Dirección IP de destino contiene un valor binario de 32 bits que representa la dirección host de capa de red de destino del paquete.
- *Opciones:* Campo adicional para suministrar otros servicios, no se lo utiliza frecuentemente.
- *Relleno:* Campo para completar un datagrama IP

1.1.2.2.4. Capa Interfaz a Red (Host a Red)

La capa interfaz a red es la capa inferior de TCP/IP. Es la encargada de establecer la interfaz con el hardware de red. TCP/IP no define protocolos en esta capa por lo que deja abierto la utilización de cualquier tecnología que pueda transportar paquetes IP.

1.1.2.3. Funcionamiento de TCP/IP

En TCP/IP cada red maneja por separado los datos que se transportan dentro de la misma, pero los datos que se intercambian entre usuarios de redes diferentes deben ser enrutados entre ellas. TCP/IP interviene en el enrutamiento entre redes. En concreto, el protocolo IP es responsable de llevar los datos a través de toda la internet, en base a los protocolos de enrutamiento.

1.1.2.4. Direccionamiento en TCP/IP

El direccionamiento de capa de red es esencial ya que permite la comunicación de datos entre equipos de la misma red o de redes diferentes. El Protocolo de Internet (IP) se basa en un direccionamiento jerárquico.

Cada host de una red debe ser identificado en forma única. En la capa Internet, es necesario reconocer los paquetes que se intercambian en una comunicación, mediante el uso de las direcciones de origen y de destino de los dos sistemas involucrados.

192	168	10	1	Dirección Decimal
11000000	10101000	00001010	00000001	Dirección Binaria

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- *Dirección de red*: la dirección en la que se hace referencia a la red.
- *Dirección de broadcast:* una dirección especial que se utiliza para enviar datos a todos los hosts de la red.
- *Direcciones host:* las direcciones asignadas a los dispositivos finales de la red.

1.1.2.4.1. Prefijos de red

En una dirección de red IPv4, además de su dirección de red se le agrega una longitud de prefijo. La longitud de prefijo determina cuántos bits en la dirección pertenecen a la porción de red. Por ejemplo: en 192.168.4.0 /24, /24 es la longitud de prefijo e indica que los primeros 24 bits son la dirección de red y los restantes 8 bits, pertenecen a la porción de host.

1.1.2.4.2. Tipos de Comunicación

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

- Unicast: comunicación por la cual se envía un paquete de un host a otro host de manera individual.
- Broadcast: comunicación por la cual se envía un paquete de un host a todos los hosts de la red.
- Multicast: comunicación por la cual se envía un paquete de un host a un grupo seleccionado de hosts.

1.1.2.4.3. Direcciones Públicas, Privadas y Reservadas.

La gran mayoría de las direcciones IPv4 son direcciones públicas que se utilizan para acceder a Internet, sin embargo existen grupos de direcciones que se utilizan en redes que no acceden a Internet y son de uso privado. Además de las direcciones reservadas que no son utilizadas, salvo circunstancias específicas.

1.1.2.4.3.1. Direcciones públicas

Casi todas las direcciones IPv4 son direcciones públicas. Estas direcciones se crearon con el fin de utilizarlas en el acceso hacia Internet.

1.1.2.4.3.2. Direcciones privadas

Los bloques de direcciones privadas son:

- de 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8)

- de 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12)
- de 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16)

1.1.2.4.3.3. Direcciones reservadas

Las direcciones reservadas son grupos de direcciones que han quedado para un uso específico. Las más importantes son las siguientes:

- 0.0.0.0 (o la dirección .0 de cualquier subred). Esta es la dirección para referirse a la red.
- 255.255.255.255 (o la dirección .255 de cualquier subred). Esta es la dirección de broadcast. Equivale a todos los terminales de la red.
- 127.X.X.X Este es el rango de ip's de loopback. Son para referirse a nuestra máquina. También llamadas de diagnóstico.

1.1.2.4.4. Clases de redes

En el RFC1700 se determinan rangos de direcciones de tamaños específicos llamados direcciones de clase A, B y C. También define a las direcciones de clase D (multicast) y de clase E (experimental).

Las direcciones unicast de clases A, B y C especificaban redes con tamaños ya establecidos, en rangos determinados. El rango de redes classfull se observa en la tabla 1.1.

Clase de Dirección	Rango del primer octeto	Bits de primer octeto	Máscara
A	1-127	0	8
B	128-191	10	16
C	192-223	110	24
D	224-239	1110	-
E	240-255	1111	-

Tabla1.1 Rango de redes classfull

1.1.2.4.5. Subredes

Para elaborar varias redes lógicas de un solo grupo de direcciones se utiliza la división en subredes. Esto se lo realiza tomando uno o más de los bits de host como bits para dirección de la subred. Lo que se hace es tomar "prestado" algunos de los bits de la parte de la dirección que pertenece al host, con el propósito de tener bits de red adicionales. La subred puede variar de tamaño, dependiendo de cuántos bits de host se utilicen, mientras mayor sea la cantidad, mayor el número de subredes creadas.

Las técnicas de subdivisión de una subred, o el uso de VLSM (máscara de subred de longitud variable), se crearon para realizar un direccionamiento más eficiente. En contraparte, en la división tradicional en subredes, se asigna la misma cantidad de direcciones para cada subred, desperdiciando numerosas direcciones de host que probablemente no van a ser utilizadas.

1.1.2.5. Protocolos de Enrutamiento[3]

El enrutamiento determina la ruta que requiere un paquete a través de la red, para ser reenviado y llegar a su destino. Cada dispositivo de enrutamiento no requiere conocer toda la ruta hacia las distintas redes, sólo debe conocer el siguiente salto para reenviar el paquete hacia la red de destino final.

Los dispositivos de enrutamiento usan las tablas de enrutamiento para determinar por donde un paquete será enrutado. Para determinar estos saltos, la tabla de enrutamiento necesita presentar la situación actual de las rutas de red a la cual puede acceder el router.

La información que presenta las tablas de enrutamiento puede ser configurada de forma manual o de forma dinámica a partir de los protocolos de enrutamiento. Los protocolos de enrutamiento sirven para:

[3] CCNA V4, Módulo 1, Network Fundamentals, Cisco 2010

- Encontrar redes remotas.
- Conservar las tablas de enrutamiento actualizadas.
- Elegir el camino óptimo hacia las redes de destino.
- Escoger un camino nuevo si la ruta actual deja de estar disponible.

1.1.2.5.1. Enrutamiento Estático

Se llama enrutamiento estático a las rutas hacia redes remotas, configuradas manualmente en el router. Una ruta predeterminada puede configurarse estáticamente.

Para tener certeza de que los datos para los cuales no exista una ruta no sean desechados, se necesita tener una ruta predeterminada configurada. Debido a que los paquetes se reenvían en cada salto, cada dispositivo encargado del ruteo debe estar configurado con una ruta hacia los siguientes saltos.

1.1.2.5.1.1. Ventajas del enrutamiento estático

- Consumo de procesamiento bajo.
- Permite tener un mayor control de la red.
- Se configura fácilmente.

1.1.2.5.1.2. Desventajas del enrutamiento estático

- La configuración y el mantenimiento son largos.
- La configuración puede causar errores, especialmente si se configuran redes extensas.
- Es necesario de un administrador para cambiar información de rutas modificadas o nuevas.
- No es escalable fácilmente en redes en crecimiento; el mantenimiento se torna cada vez más complicado.
- Se necesita conocer completamente a la red para una correcta implementación.

1.1.2.5.2. Enrutamiento Dinámico

Es de suma importancia que los routers mantengan información actualizada de las rutas, pero a veces es muy complejo de hacerlo utilizando solo tablas de enrutamiento por configuración estática. Por eso, se utilizan los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento se conforman mediante un grupo de reglas por las que los routers comparten dinámicamente su información de enrutamiento.

Los routers están enterados de las modificaciones en las redes para las que actúan como puertas de enlace, o de los cambios en enlaces entre routers, toda esta información pasa a otros routers. Cuando a un router se le informa sobre rutas nuevas o modificadas, actualiza su tabla de enrutamiento y, a su vez, envía la información a otros routers. De este modo, se puede contar con tablas de enrutamiento actualizadas dinámicamente en todos los routers y así aprenden sobre nuevas rutas a redes remotas que se encuentran a varios saltos de distancia.

1.1.2.5.2.1. Ventajas del enrutamiento dinámico

- El mantenimiento en la configuración es menos complicado cuando se elimina o se añade redes.
- Se cometen menos errores en la configuración.
- Se adapta bien a redes en crecimiento.

1.1.2.5.2.2. Desventajas del enrutamiento dinámico

- Se utilizan más recursos de CPU, memoria y ancho de banda del enlace.
- Se requiere conocimientos más técnicos para la configuración de estos protocolos de enrutamiento.

1.1.2.5.3. Protocolo vector distancia

Los protocolos vector distancia para establecer el mejor camino hacia una red, usan por lo general el algoritmo Bellman-Ford. Con este algoritmo el router conoce sólo la

información de enrutamiento que recibió de sus vecinos y no sobre el estado concreto de una topología. Además, se encargan de transmitir actualizaciones regularmente de su información de enrutamiento.

Los protocolos vector distancia tienen un mejor desempeño en escenarios donde:

- La red no es jerárquica, más bien plana y simple.
- No se cuenta con personal que posea suficientes conocimientos como para configurar protocolos de link-state y resolver problemas en ellos,
- No tiene importancia en la red tiempos de convergencia altos.

1.1.2.5.4. Protocolo de estado de enlace

Un router que utiliza protocolos de estado de enlace usa su información para crear un mapa de la topología y seleccionar el mejor camino hacia todas las redes de destino. Los protocolos de enrutamiento de estado de enlace no usan actualizaciones periódicas. Luego de que la red ha convergido, las actualizaciones sólo se envían cuando se produce una modificación en la topología.

Los protocolos de estado enlace tienen un mejor desempeño en escenarios donde:

- Se tiene una red extensa y diseñada de manera jerárquica.
- Se posee personas capacitadas para configurar correctamente protocolos de estado de enlace.
- Es importante tener menores tiempos de convergencia.

1.1.2.5.4.1. Métrica

Se define métrica como un valor empleado por los protocolos de enrutamiento para determinar un costo de una ruta hacia su destino. Los valores utilizados como métricas en los protocolos de enrutamiento pueden ser: conteo de saltos, ancho de banda, carga, retardo, confiabilidad, costo, entre otros.

1.1.2.5.4.2. Distancia Administrativa

Indica el grado de confiabilidad que se le da a una ruta en función de su origen. La ruta con la menor distancia administrativa se la considerará como la más fiable. En la tabla 1.2 se muestran las distancias administrativas de los protocolos de enrutamiento.

Origen de la ruta	Distancia Administrativa
Directamente Conectada	0
Estática	1
Ruta sumarizada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Tabla1.2 Distancia Administrativa de protocolos de enrutamiento

1.1.2.5.5. Protocolo de Gateway Interior Mejorado (EIGRP)[4]

El protocolo de gateway interior mejorado (EIGRP), fue lanzado en 1992 con el IOS 9.21 de los equipos Cisco. A EIGRP se lo califica como un protocolo de enrutamiento vector distancia sin clase y fue una mejora de IGRP de Cisco (Interior Gateway Routing Protocol).

EIGRP fue desarrollado por Cisco con el fin de crear una versión sin clase de IGRP. EIGRP agrega muchas características que protocolos como RIP (RIPv1 y RIPv2) e IGRP no poseen. EIGRP es un protocolo de enrutamiento vector distancia, aunque en momentos puede desempeñarse como un protocolo de enrutamiento de estado de enlace.

[4] Rob Payne, Kevin Manweiler, Cisco certified internetwork expert : study guide, Segund Edición, 2003

EIGRP utiliza el Algoritmo de actualización por difusión (DUAL) con el cual puede implementar características que no se encuentran en los protocolos de enrutamiento vector distancia. En EIGRP las entradas de ruta no caducan, y sus actualizaciones no se envían periódicamente. En su lugar, EIGRP utiliza un protocolo Hello para conocer el estado de las conexiones con sus vecinos, por lo que, cuando se produce una modificación en la información de enrutamiento, tales como un nuevo enlace o un enlace que ha sido descartado, se produce una actualización. EIGRP utiliza vectores distancia transmitidos a equipos conectados directamente, para actualizar las tablas de enrutamiento.

1.1.2.5.5.1. Determinación de la ruta

En EIGRP el algoritmo DUAL conserva dos tablas por separado: la una contiene información de la topología y la otra información de enrutamiento, la tabla de enrutamiento incluye la mejor ruta hacia una red de destino y la ruta de respaldo que el algoritmo haya comprobado que no tiene lazos de enrutamiento. Sin lazos de enrutamiento quiere decir que un mismo paquete no pasa por un mismo ruteador más de una vez.

1.1.2.5.5.2. Paquetes RTP

RTP, protocolo de transporte confiable, es utilizado para transmitir y receptar paquetes de EIGRP. EIGRP no hace uso de UDP ni de TCP.

1.1.2.5.5.3. Protocolo de saludo

El protocolo de saludo sirve para que los routers que ejecutan EIGRP, puedan descubrir vecinos y establecer cercanías. Se debe descubrir a sus vecinos antes de poder transmitir o receptar paquetes EIGRP entre los routers. Los vecinos de EIGRP son otros routers que ejecutan EIGRP en redes conectadas directamente.

EIGRP utiliza los tiempos de espera para mostrar al router cuánto tiempo máximo esperar para recibir el próximo Hello antes de señalar al router vecino como destino inaccesible. Por defecto, el tiempo de espera es tres veces el intervalo Hello, o 15

segundos en la mayoría de las redes. Si el tiempo de espera caduca, EIGRP señalará la ruta como inactiva y DUAL buscará una nueva ruta mediante el envío de consultas.

1.1.2.5.5.4. Algoritmo DUAL

Al calcular una nueva ruta, el algoritmo DUAL actúa evitando lazos de enrutamiento. Esto ayuda que todos los routers involucrados en una modificación de topología se sincronicen al mismo tiempo. Todos los routers que no hayan sido modificados por los cambios en la topología no se los toma en cuenta en el recálculo. Debido a estos cálculos realizados por el algoritmo, existe un mayor tiempo de convergencia que con otros protocolos de enrutamiento vector distancia.

Es importante siempre que sea posible evitar realizar un recálculo del algoritmo DUAL, ya que consume muchos recursos del procesador. Por lo tanto, DUAL mantiene una lista de rutas de respaldo que ya ha determinado como sin lazos. Si la principal ruta hacia una red falla, la mejor ruta de respaldo se agrega de inmediato a la tabla de enrutamiento.

1.1.2.5.5.5. Métrica compuesta de EIGRP

Los valores empleados por EIGRP dentro de su métrica compuesta son: ancho de banda, retardo, confiabilidad y carga. La fórmula compuesta predeterminada y los valores de k predeterminados se aprecian a continuación:

Métrica= [K1 * ancho de banda + ((K2 * ancho de banda)/(256-carga))+ (K3 * retardo)]*[K5/(confiabilidad + K4)]

K1 (Ancho de banda) = 1; K2 (carga) = 0;
K3 (retardo) = 1 K4 (confiabilidad) = 0; K5 (confiabilidad) = 0

Por defecto los valores K2, K4 y K5 son 0, por lo que la ecuación de la métrica compuesta de EIGRP se reduce a:

Métrica= [ancho de banda + retardo]

Los valores de k pueden ser modificados para dar más peso a las métricas de EIGRP

1.2. TECNOLOGÍAS DE RED DE CAPA DOS

TCP/IP no define protocolos de la capa de acceso a red dejando abierto la utilización de cualquier tecnología que permita el transporte de paquetes IP. A continuación se detalla el funcionamiento de Frame Relay y Ethernet.

1.2.1. FRAME RELAY

1.2.1.1. Introducción

FRAME RELAY es una tecnología de red WAN, que trabaja en la capa dos del modelo ISO/OSI y basa su funcionamiento en la conmutación de paquetes, específicamente utilizando circuitos virtuales. Aparece en la década de los 90 y tiene sus orígenes en las especificaciones ISDN (Redes Digitales de Servicios integrados), las redes ISDN proveían un solo interfaz de red al usuario para conectarse a diferentes redes de servicios. El servicio Frame Relay dentro de ISDN fue diseñado para proveer alta velocidad en el transporte de datos con conmutación de paquetes, las redes ISDN no tuvieron mayor acogida por lo que Frame Relay empezó su desarrollo independiente como solución a los problemas de latencia generados en las redes X.25 (tecnología que predominaba en ambientes WAN).

Frame Relay solventa las deficiencia de X.25 estableciéndose como una tecnología ligera de transmisión de datos, que omite algunas funciones de control implementadas en X.25 y que a diferencia de su predecesora trabaja hasta la capa enlace de datos del modelo ISO/OSI.

En 1991 se crea el Forum Frame Relay con participación de vendedores (Cisco, Stratacom, Digital, Northern Telecom), portadores, usuarios y consultores, los cuales tenían como tarea definir las especificaciones para los estándares de la tecnología Frame Relay. En el mercado ecuatoriano Frame Relay tuvo aceptación para solventar conectividad en redes de área extendida privadas, debido a las características técnicas que se explican a detalle más adelante, y al costo que significaba implementar una red Frame Relay.

En la actualidad la tecnología Frame Relay ha sido desplazada por otras tecnologías como ATM e IP-MPLS que brindan mayores capacidades y mayor eficiencia.

1.2.1.2. Trama Frame Relay

En la figura 1.6 se indica el formato de la trama Frame Relay.

Bandera	Campo de Dirección	Datos	Secuencia de Chequeo	Bandera
1 byte	2-4 bytes	Variable	2 bytes	1 byte

Figura 1.6 Formato de la trama de la capa enlace de datos

- Bandera, su función es delimitar el principio y final de cada trama, debido a que no se maneja un tamaño de trama fijo, permitiendo al equipo que recibe la información sincronizar el flujo de tramas. El formato de la bandera es 01111110, el equipo que envía la información tiene que validar que no exista ninguna secuencia de bits igual a la bandera, y lo garantiza no permitiendo que exista una secuencia de más de cinco unos, en el caso de que exista dicha secuencia se inserta un cero después del quinto uno, en el receptor se realiza el proceso inverso, si se detecta una secuencia de cinco unos se verifica el siguiente bit si es un uno es la secuencia de bandera si es un cero se elimina.

- Campo de Dirección, encargado del direccionamiento de las tramas Frame Relay y otras funciones que se explican en el detalle de este campo (Figura 1.7).

Dirección						CR	EA
Dirección				FECN	BECN	DE	EA
8	7	6	5	4	3	2	1

Figura 1.7 Formato Campo Dirección

El campo de dirección se divide en los siguientes subcampos:

- Dirección, DLCI, Identificador de Conexión de Enlace de Datos (Data Link Connection Identifier), esta dirección representa el circuito virtual utilizado para el establecimiento de la conexión en capa 2, utiliza 10 bits por tanto el protocolo podría permitir como máximo 1024 direcciones de DLCI, como consecuencia se podrían establecer 1024 conexiones Frame Relay entre un par de nodos, pero este número disminuye debido a que existen números de DLCI reservados. Dependiendo del campo EA puede extenderse.
- CR, Comando-Respuesta, este bit es utilizado por el protocolo Frame Relay para indicar si es un mensaje de comando o respuesta.
- EA, Dirección Extendida, la trama básica de Frame Relay puede manejar diez bits para el direccionamiento a través de los DLCIs, el propósito de estos bits es de extender el formato del campo de dirección para soportar más bits para el direccionamiento. El bit EA se coloca en cero cuando existe otro octeto a continuación y se coloca en uno cuando es el último octeto.
- FECN, Notificación de Congestión Explícita hacia Adelante, este bit es utilizado por la red, no por el equipo que transmite la información, para

notificar que existe congestión para el tráfico en la dirección en la que viaja la trama.

- BECN, Notificación de Congestión Explícita hacia Atrás, este bit es utilizado por la red, no por el equipo que transmite la información, para notificar que existe congestión para el tráfico en la dirección contraria en la que viaja la trama.
- DE, Elegible para Descarte este bit tiene importancia en situaciones de congestión, indica qué trama puede o no ser tomada en cuenta para el proceso de descarte o de eliminación, puede ser seteado por la red o por el usuario. Es importante tener en cuenta que no tener seteado el bit DE no indica que la trama nunca va a ser descartada, debido a que se lo puede realizar por otras circunstancias en la red.

- Datos, este campo contiene la información propia del usuario, el campo consta de un número entero de octetos, el tamaño máximo del campo no se encuentra especificado y por tanto dependerá de la red (El Forum Frame Relay recomienda un máximo de 1600 octetos), el tamaño mínimo del campo es de un octeto.
- FCS, Secuencia de Chequeo de Trama, se utiliza para verificar que no se insertaron errores durante el proceso de envío de la información, este campo contiene un código de redundancia cíclica ($x^{16} + x^{12} + x^5 + 1$), FCS opera en todos los bits de la trama excluyendo las banderas.

En capa física Frame Relay se basa en los servicios ISDN. El fórum Frame Relay estableció que se permiten varias opciones: V.35, G.703, G.704 y X.21. No hay una recomendación específica para el interfaz físico.

1.2.1.3. Funcionamiento

La fortaleza de Frame Relay fue la de constituirse en un protocolo ligero de red (realiza menos funciones de control que X.25), el algoritmo que sigue el protocolo es bastante simple: si se recibe una trama válida debe ser enviada al destino por una

determinada ruta, si existen problema de congestión en la red, los nodos pueden descartar tramas para aliviar el problema (se toma en cuenta el bit DE), si recibe una trama inválida el nodo descarta la trama, sin notificar al usuario esta acción.

Una trama es inválida por las siguientes razones:

- No está delimitada por dos banderas.
- Tiene una longitud menor a cinco octetos entre las banderas.
- No tiene un número entero de octetos después del proceso de bit stuffing (proceso de extracción bits en cero que se insertaron para evitar que exista secuencias iguales a la bandera)
- Contiene un error FCS
- No contiene un campo de dirección valido
- Contiene un DLCI no soportado
- Excede el tamaño máximo acordado entre el usuario y la red.

1.2.1.4. Arquitectura

Frame Relay divide su arquitectura en dos planos, el plano de Control y el plano de usuario, definiendo canales diferentes para cada uno.

1.2.1.4.1. Plano de Control

Llamado también plano C encargado de funciones de señalización de control. En esta capa utiliza el protocolo LAPD (Q.921, realiza funciones de control de flujo y control de errores), para transportar la información de señalización de control (Q.933 Sistema de señalización de abonado digital).

En el plano C también se define LMI (Local Managment Interface) para acceder a funciones de administración.

1.2.1.4.2. Plano de Usuario

Llamado también plano U encargado de las funciones de transferencia de información entre los interfaces de usuario. Utiliza en capa dos el protocolo LAPF (Q.922) no realiza funciones de control de flujo y solo realiza detección de errores, se divide en dos subcapas.

La subcapa inferior 2.1 presente en los equipos terminales como en los nodos de la red, garantiza una alta velocidad de conmutación. La subcapa superior 2.2 se implementa solo en los equipos terminales.

1.2.1.4.3. LAPF (Link Access Procedure For Frame Relay)

Protocolo desarrollado para mejorar LAPD (Q.921) con capacidad para control de congestión, las funciones de LAPF son:

- Delimitación de trama
- Multiplexación y De-multiplexación de circuitos virtuales.
- Alineamiento de octetos.
- Chequeo de tamaños mínimos y máximos de tramas
- Detección de errores
- Control de congestión.

1.2.1.5. Circuitos Virtuales

Frame Relay utiliza conmutación de circuitos virtuales para el transporte de información.

1.2.1.5.1. LMI

Frame Relay como fue descrito, no permite ningún control local o manejo de las interfaces, no existe ninguna forma para que los extremos de la red determinen el estado de su conexión.

Por esta razón se incluyo mecanismos de señalización en el protocolo, pero que no implica su implementación necesaria para el funcionamiento del mismo, simplemente permite recibir información acerca del estado de la red.

Para los mensajes LMI se utiliza DLCI independientes de los utilizados para la transmisión de información (DLCI 0).La función principal de LMI es notificar al interfaz de usuario información del estado y configuración relacionada a la operación de los PVCs (Permanent Virtual Circuits).

1.2.1.5.1.1. Características

- Notificación de la adición, borrado o presencia de PVCs.
- Notificación de la disponibilidad de un PVC preconfigurado.
- Una secuencia de poleo para asegurar la continúa operación del enlace.

1.2.1.5.1.2. Trama LMI

- *Header,* es igual al Header de la trama Frame Relay (DLCI, C/R, FECN, BECN) solo que siempre se utiliza el DLCI 0 como se explicó anteriormente
- *Indicador de Trama no numerada,* el protocolo LMI está más cercanamente alineado con LAPD, indica que la trama no tiene secuencia y es impedida para la realización del control de flujo, de esta forma se permite la compatibilidad entre redes ISDN y no ISDN. Siempre se lo codifica con la secuencia 00000011.
- *Discriminador de Protocolo,* utilizado para compatibilidad con redes ISDN, en el que se lo utiliza para distinguir mensajes de control de otros mensajes.
- *Referencia de Llamada*, solo es utilizado durante el establecimiento de SVCs. Cuando el mensaje no está relacionado con el establecimiento o la finalización de la llamada el campo es colocado en 00000000.
- *Tipo de Mensaje,* determina el tipo de mensaje LMI que se está transmitiendo, no existe una codificación estandarizada para el contenido del campo.

- *Elementos de información,* contiene la información específica del mensaje LMI, debe existir mínimo un campo aunque es común encontrar más de uno. Contiene un número entero de octetos que depende del número de elementos de información que contenga el mensaje LMI.

1.2.1.5.2. PVC Circuito Virtual Permanente

Este tipo de configuración es la que se utiliza en la práctica, consiste en un trayecto establecido por el administrador de la red a través de la nube Frame Relay que conecta dos puntos finales. Se basa en el concepto de transferencia de información frecuente y constante entre dispositivos DTE a través de la red Frame Relay.

Este circuito predeterminado permanece activo continuamente y está garantizado, tiene como objeto proporcionar un nivel específico de servicio, que se ha negociado con el cliente, esta garantía se define por parámetros en el circuito virtual. Un circuito virtual se diferencia de la conmutación de circuitos, en que en un mismo circuito físico pueden existir varios circuitos virtuales. Los PVCs siempre operan en alguno de los siguientes estados:

- *Transferencia de datos*. Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.
- *Pasivo.* Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los SVCs, los PVCs no se darán por finalizados en ninguna circunstancia ya que se encuentran en estado pasivo.

En la figura 1.8 se observa el establecimiento de circuitos virtuales permanentes en una red WAN.

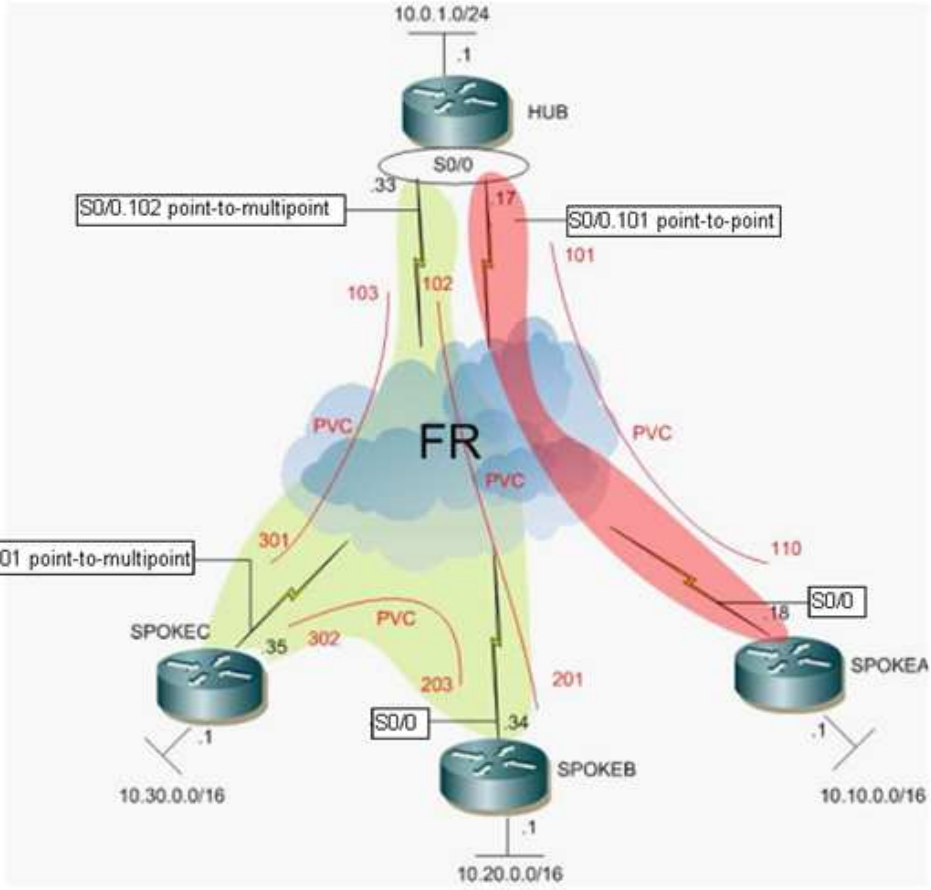


Figura 1.8 PVCs[5]

1.2.1.5.3. SVC Circuito Virtual Conmutado

Los circuitos conmutados se añadieron a finales de 1993, con poca aplicación y dejándolo prácticamente al plano teórico. Utilizan conexiones temporales bajo el concepto de transmisiones esporádicas de datos entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de cuatro estados:

- *Establecimiento de la llamada*. Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.
- *Transferencia de datos.* Los datos se transmiten ente los dispositivos DTE a través del circuito virtual.

[5] http://cciethebeginning.wordpress.com/tag/mgre/

- *Pasivo.* La conexión entre los dispositivos DTE aún está activo, sin embargo no hay transferencia de datos. Si un SVC permanece en estado pasivo por un periodo definido de tiempo, la llamada puede darse por terminada.
- *Terminación de la llamada.* Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Generalmente la infraestructura WAN es provista por un Carrier y el establecimiento, transmisión y cierre de la llamada consume recursos para cada transmisión de información por lo que se prefiere la utilización de PVCs.

1.2.1.6. Parámetros de Conexión

Con objeto de proporcionar un nivel específico de servicio, que se han negociado con el cliente, se establecen parámetros en los circuitos virtuales.

1.2.1.6.1. CIR, Tasa de Información Comprometida

Define la tasa a la cual el proveedor de servicio acuerda aceptar bits en el circuito virtual. Mientras el usuario no exceda este parámetro la entrega de las tramas estará garantizada.

1.2.1.6.2. EIR, Tasa de Información en Exceso

Define la tasa en que el usuario puede exceder el CIR, siempre y cuando la red no se encuentre congestionada, este concepto permite que la red se utilice de una forma eficiente en situación de baja carga en la red.

En situación de congestión de red el usuario se ve limitado al CIR debido a que si sobrepasa este parámetro todas las tramas que excedan el CIR serán descartadas.

1.2.1.6.3. Tc, Tiempo Comprometido

Intervalo de tiempo durante el cual el usuario está autorizado a enviar solamente la cantidad de información Bc y una cantidad excedente Be.

1.2.1.6.4. Bc, Ráfaga Comprometida

Número de bits comprometidos en el tiempo comprometido Tc.

1.2.1.6.5. Be, Ráfaga en Exceso

Número de bits adicional que el usuario puede enviar al Bc en el tiempo comprometido Tc.

1.2.1.6.6. AR, Tasa de Acceso

Velocidad del interfaz físico de acceso al cliente.

En la figura 1.9 se muestran todos los parámetros anteriormente indicados.

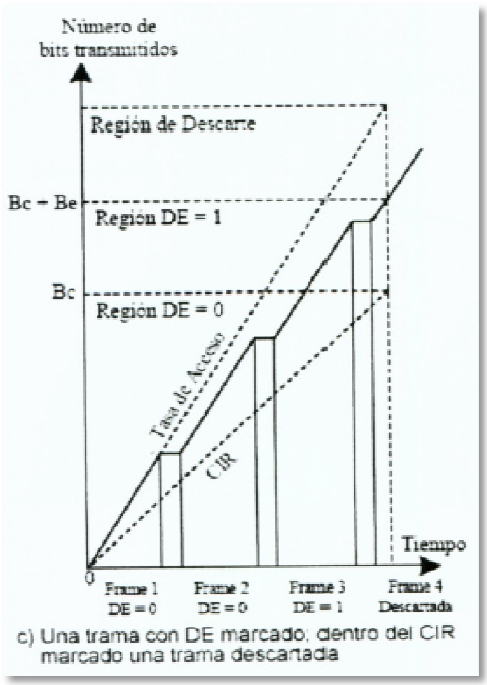


Figura 1.9 Parámetros de Conexión de Frame Relay[6]

[6] Soraya Sinche, Folleto de Redes de Área Extendida, 2009

1.2.1.7. Control de Tráfico y Congestión

1.2.1.7.1. Control de Tráfico

Al definir parámetros de conexión como el CIR y el EIR se necesita también definir mecanismos para realizar el control de los mismos. Frame Relay define los siguientes parámetros de control del tráfico:

Traffic Shaping. Vigila el trafico inyectado, éste nunca debe sobrepasar el CIR + EIR, y dependerá de las condiciones de carga de la red para que no deba sobrepasar el CIR.

Traffic Policing. Adopta medidas cuando se sobrepasan los caudales especificados, cuando se sobrepasa el CIR el bit DE será seteado para que sea elegible de descarte, si se sobrepasa el CIR + EIR la trama será descartada directamente. El Traffic Shaping y el Traffic Policing son aplicados en los puntos de entrada a la red.
El mecanismo en el que se implementan las técnicas de control de tráfico es el siguiente:

- El conmutador de entrada utiliza dos buffers con capacidad Bc y Be.
- El tráfico de entrada es almacenado en Bc y se envía con una tasa igual al CIR.
- Si el buffer Bc se llena es porque se está excediendo el CIR, y empieza a almacenar el tráfico excedente en el buffer Be, en el buffer Be las tramas son marcadas con el bit DE.
- Si el buffer Be se llena es porque se excedió el CIR + EIR y por tanto las tramas se pierden.

1.2.1.7.2. Control de Congestión Explícita

La función que cumplen los mecanismos de control de congestión explicita, es la de alertar a los sistemas finales ante la existencia de un crecimiento de congestión

dentro de la red y de esta forma tomar acciones para reducir la situación de congestión.

Existen dos puntos de vista para determinar dónde y la rapidez con la que ocurre la congestión.

- La congestión ocurre lentamente y se da principalmente en los conmutadores de acceso.
- La congestión ocurre rápidamente y se da en los conmutadores internos de la red Frame Relay.

Para la solución se utilizan dos tipos de control de congestión explícita: Forward y Backward, esto se implementa a través de dos bits reservados para este propósito en el campo Dirección de la trama Frame Relay, estos bits pueden ser seteados por cualquier nodo de la red Frame Relay.

1.2.1.7.2.1. BECN, Notificación Explícita de Congestión Hacia Atrás

El bit indica que existe congestión en el sentido opuesto al de la trama recibida, y que se deben tomar acciones para evitar la congestión.

Indica al usuario que las tramas que se envíen sobre esa conexión pueden encontrar recursos congestionados.

1.2.1.7.2.2. FECN, Notificación Explícita de Congestión Hacia Adelante

El bit indica que existe congestión en el sentido de la trama recibida, y que se deben tomar acciones para evitar la congestión. Indica al usuario que las tramas en esa conexión encontraron recursos congestionados.

El algoritmo que ejecutan los conmutadores de la red Frame Relay es el siguiente:

- Monitorizan continuamente el estado de las colas de salida en las interfaces para detectar la congestión lo antes posible.
- Descarta las tramas en las que se encuentra seteado el bit DE para solucionar la congestión.
- Si no se soluciona la congestión se identifica el circuito virtual que produce la congestión y el sentido en que se ocasiona.
- Una vez detectado el circuito virtual que causa la congestión y el sentido, el conmutador enviará tramas con señalización explicita de congestión utilizando los bits BECN o FECN según sean necesarios.

En la figura 1.10 se observa el sentido en el que viajan la señalización de congestión explicita, y se muestra que no necesariamente toda la red puede estar congestionada.

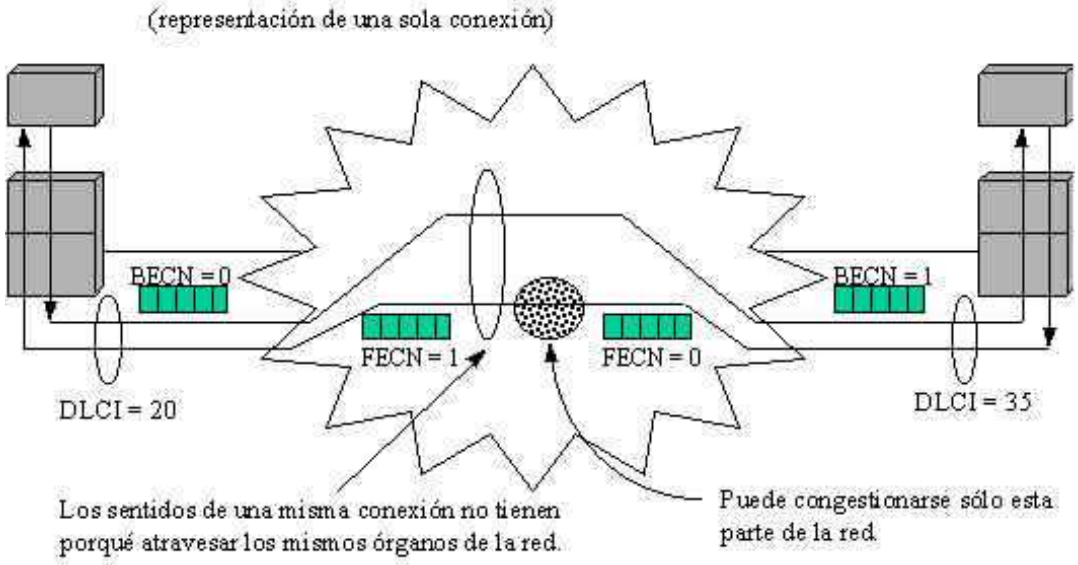


Figura 1.10 Control de Congestión Frame Relay[7]

[7] http://www.it.uc3m.es/~prometeo/rsc/apuntes/frame/frame.html

1.2.2. ETHERNET

1.2.2.1. Introducción

Muchas empresas, universidades y otras organizaciones tienen un gran número de computadoras que requieren interconexión en ambientes locales. Esta necesidad dio origen a la red de área local, siendo la más popular de ellas Ethernet. A pesar de que Ethernet nació como una tecnología LAN, el desarrollo de los medios de transmisión (fibra óptica) y la tecnología de los equipos de transmisión, ha permitido su utilización en ambientes geográficos más extensos.

1.2.2.2. Trama Ethernet

La trama Ethernet, utiliza encabezados y trailers para encapsular los paquetes recibidos de la capa 3, y poderlos enviar a su destino. Hay dos tipos de tramas de Ethernet: el estándar DIX Ethernet, que ahora es Ethernet II, y el estándar IEEE 802.3, que ha sido actualizado varias veces para incluir nuevas tecnologías.

Los dos estándares se diferencian principalmente por el agregado de un delimitador de inicio de trama (SFD) y el cambio del campo Tipo por un campo Longitud en el 802.3. En la figura 1.11 se compara la trama Ethernet y la trama 802.3

IEEE 802.3						
7	1	6	6	2	46-1500	4
Preámbulo	Delimitador de Inicio	Dirección de Destino	Dirección de Origen	Longitud	Encabezado y Datos 802.2	Secuencia de verificación

Ethernet					
8	6	6	2	46-1500	4
Preámbulo	Dirección de destino	Dirección de origen	Tipo	Datos	Secuencia de verificación

Figura 1.11 Comparación entre trama Ethernet y 802.3

1.2.2.2.1. Campos de la trama IEEE 802.3 [8]

- *Los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD) (1 byte).* Se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos ocho primeros bytes de la trama contienen el patrón de bits 10101010….1010 que se utilizan para permitir que el reloj del receptor se sincronice con el del emisor.
- *El campo Dirección MAC de destino (6 bytes).* Es el identificador del receptor deseado. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.
- *El campo Dirección MAC de origen (6 bytes).*Identifica la NIC o interfaz de origen de la trama.
- *Campo Longitud/tipo (2 bytes).* El campo Tipo de Ethernet II se incorporó a la actual definición de trama del 802.3. Cuando un nodo recibe una trama, debe analizar el campo Longitud para determinar qué protocolo de capa superior está presente. Si el valor de los dos octetos es equivalente a 0x0600 hexadecimal o 1536 decimal o mayor que éstos, los contenidos del campo Datos se decodifican según el protocolo EtherType indicado. Al contrario, si el valor es igual o menor que el hexadecimal de 0x05DC o el decimal de 1500, el campo Longitud se está utilizando para indicar el uso del formato de trama de IEEE 802.3.
- *Los campos Datos y Pad (de 46 a 1500 bytes)* contienen los datos encapsulados de una capa superior, que es una PDU de Capa 3 genérica. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, el Pad se utiliza para incrementar el tamaño de la trama hasta alcanzar el tamaño mínimo.
- *Campo Secuencia de verificación de trama (FCS) (4 bytes)* se utiliza para detectar errores en la trama. Utiliza una comprobación cíclica de redundancia (CRC). El equipo emisor incluye los resultados de la CRC en el campo FCS de

[8] CCNA V4, Módulo 1, Network Fundamentals, Cisco 2010

la trama. El equipo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, significa que no se produjo ningún error.

1.2.2.3. Funcionamiento

Ethernet trabaja, de acuerdo al modelo OSI, en las dos capas inferiores: la capa de enlace de datos y la capa física. La Capa 1 desempeña un rol importante en la comunicación que se produce entre los dispositivos. Ethernet en la Capa 1 se encarga de transportar los streams de bits, generar las señales y controlar los componentes físicos que transmiten estas señales a los medios.

La capa enlace de datos se separa en dos subcapas, con funciones específicas en cada una de ellas, estas dos subcapas son: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC).

Tanto la subcapa LLC como MAC, aportan en gran manera a la compatibilidad de tecnología y la comunicación con la computadora. La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

1.2.2.3.1. Estándar 802.2: control lógico de enlace.

Ethernet y los protocolos 802 brindan un servicio de datagramas de mejor esfuerzo. A veces, este servicio es el ideal. No obstante, hay servicios o aplicaciones en los que es deseable un protocolo de enlace de datos con control de errores y control de flujo, siendo LLC (Control Lógico del Enlace) la solución para estos requerimientos, LLC puede operar encima de todos los protocolos Ethernet y 802.

LLC es el responsable de brindar la comunicación entre el hardware que son las capas inferiores, con las capas superiores y el software de red. El protocolo de Control Lógico de Enlace tiene como mecanismo añadir información de control a los datos del protocolo de la red, que comúnmente son paquetes IPv4, para ayudar a entregar la información al dispositivo de destino.

El estándar 802.2 (LLC) se ejecuta en software y su implementación no depende del equipo físico. En un dispositivo terminal como una PC, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC).

1.2.2.3.2. Subcapa de control de acceso al medio (MAC)

MAC es la subcapa inferior de Ethernet en la capa de enlace de datos, es implementada en hardware, comúnmente en la tarjeta de interfaz de red (NIC) de la PC. Se encarga de dos actividades principalmente:

- Encapsulación de datos
- Control de acceso al medio

1.2.2.3.2.1. Encapsulación de datos

La encapsulación de datos proporciona tres funciones principales:

- Delimitación de tramas
- Direccionamiento
- Detección de errores

1.2.2.3.2.2. Control de acceso al medio

La subcapa MAC se encarga de enviar tramas en los medios. La función de la subcapa MAC, es la de administrar el control de acceso al medio, lo que incluye funciones como: el inicio de la transmisión de tramas y la recuperación por fallo de transmisión debido a colisiones.

En un ambiente de medios compartidos, todos los equipos pueden acceder a dicho medio, teniendo una misma prioridad para todos. Si más de un dispositivo desea enviar datos en un mismo instante, las señales físicas pueden colisionar lo que causa que la red falle y tenga que restaurarse para seguir con la comunicación. Para tratar de reducir estas colisiones, Ethernet hace uso del acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD), con lo cual puede detectar y

disminuir el número de colisiones, permitiendo una mejor administración en la reanudación de las comunicaciones.

Con el uso del esquema de coordinación distribuida (CSMA/CD), los dispositivos que hacen uso de Ethernet para comunicarse, pueden detectar si una computadora está transmitiendo, determinando si hay o no actividad eléctrica en el cable. Cuando una máquina determina que ninguna otra PC está enviando una trama o una señal portadora, la máquina podrá transmitir.

Detección de portadora

Los dispositivos que se comunican a través de Ethernet utilizan el método de acceso CSMA/CD, lo que conlleva que cada vez que deseen enviar información a la red, deben escuchar antes de transmitir. Si en el momento de escucha se descubre una señal de un dispositivo, la máquina que desea enviar datos deberá aguardar durante un período de tiempo determinado por el algoritmo de retroceso exponencial, antes de intentar transmitir otra vez.

Cuando no se “escuche” otra señal transmitiendo, el dispositivo podrá enviar datos a la red. Mientras se realiza la comunicación, el dispositivo continúa censando la señal para determinar si hay tráfico o colisiones en la LAN. Una vez que se completa la comunicación, la máquina vuelve a escuchar el medio si necesita transmitir información.

Detección de colisiones

Debido a que el dispositivo escucha el medio antes de transmitir, puede detectar cuando se produce una colisión. La colisión puede ser detectada debido a que los dispositivos están en la capacidad de determinar si existió un aumento de la amplitud de la señal que supere el nivel normal.

Señal de congestión y postergación aleatoria

Cuando se produce una colisión, los equipos transmisores, envían una señal de congestión de 32 bits, para que las máquinas de la LAN detecten la colisión. Esta señal de congestión se utiliza para notificar a los demás dispositivos sobre una colisión, de manera que las máquinas invocarán un algoritmo de postergación (algoritmo de retroceso exponencial).

El algoritmo de retroceso exponencial hace que los equipos dejen de transmitir durante un período aleatorio, lo que permite que las colisiones disminuyan.

Una vez que finaliza el periodo aleatorio, donde el dispositivo no transmite, dicho equipo vuelve al modo " de escucha" previamente a volver transmitir.

Algoritmo de retroceso exponencial[9]

Tras una colisión el tiempo se divide en ranuras discretas cuya longitud es igual al tiempo de propagación de ida y vuelta de peor caso en el cable (2t). Tomando en cuenta la ruta más larga permitida por Ethernet, el tiempo de ranura se estableció en 512 tiempos de bit, o 51,2 useg.

Tras la primera colisión, cada estación espera 0 a 1 tiempos de ranura antes de intentar transmitir nuevamente. Si dos estaciones entran en colisión y ambas escogen el mismo número aleatorio, habrá una nueva colisión. Después de la segunda colisión, cada una escoge 0, 1, 2 o 3 al azar y espera ese número de tiempos de ranura.

En general, tras i colisiones, se escoge un número aleatorio entre 0 y $2^i - 1$, y espera ese tiempo de número de ranuras. Sin embargo tras haberse alcanzado 10 colisiones, el intervalo de aleatorización se congela en un máximo de 1023 ranuras.

[9] Andrew S. Tanenbaum, Redes de Computadoras, 4ta Ed.

Tras 16 colisiones, el controlador informa de un fallo a la computadora. La recuperación posterior es responsabilidad de capas superiores.

1.2.2.4. Direccionamiento

Ethernet en sus inicios funcionaba con una topología de bus. En la cual los dispositivos de red se conectaban a un mismo medio compartido. El problema más importante que debía resolverse, en este tipo de redes, era cómo identificar cada uno de los dispositivos. Para ello se creó un identificador único, que se lo nombró como dirección de Control de acceso al medio (MAC), la cual sirve para identificar las direcciones de origen y de destino dentro de una red Ethernet, sin tomar en cuenta qué tipo de Ethernet se estaba utilizando.

La dirección MAC es agregada en la PDU de Capa 2. Esta dirección está compuesta por un valor binario de 48 bits expresado como 12 dígitos hexadecimales.

1.2.2.4.1. Estructura de la dirección MAC

Para asegurarse que la dirección MAC sea única la IEEE definió normas para los proveedores. La dirección MAC está conformada por un código de 3 bytes, denominado Identificador único organizacional (OUI), que es proporcionado por la IEEE a cada proveedor, y los restantes 3 bytes son códigos propios de cada proveedor.

1.2.2.4.2. Descripción del proceso de direccionamiento

Cuando un dispositivo envía datos en una red Ethernet, se adjunta la información del encabezado dentro de la dirección MAC. El dispositivo de origen envía los datos a través de la red. Cada tarjeta de interfaz de red de las PC, podrá visualizar la información para determinar si la dirección MAC coincide con su dirección física. Si no hay coincidencia, se descarta la trama. Si existe coincidencia, la trama es procesada.

Las direcciones de capa enlace de datos tienen significado solo local, y se utiliza para el transporte del paquete utilizando los medios locales a través de cada segmento.

1.2.2.5. Control de Flujo[10]

El funcionamiento full dúplex se introdujo inicialmente como una extensión no estándar por parte de varios fabricantes. Cuando en 1997 el subcomité 802.3x lo estandarizó incluyó además una nueva funcionalidad, el control de flujo, que en Ethernet se implementa mediante el comando PAUSE. El receptor puede en cualquier momento enviar al emisor un comando PAUSE indicándole por cuánto tiempo debe dejar de enviarle datos. Durante ese tiempo el receptor puede enviar nuevos comandos PAUSE prolongando, reduciendo o suprimiendo la pausa inicialmente anunciada. Con esto se pretende evitar el desbordamiento de los buffers del receptor con el consiguiente descarte de tramas, lo cual causaría errores mayores.

1.2.2.6. Estándares de Ethernet / IEEE 802.3[11]

Ethernet durante su evolución ha ido cambiando para ajustarse a las necesidades cambiantes y a las capacidades de los medios, significando ser la tecnología LAN de mayor éxito, en gran medida, debido a la simplicidad de su implementación, cuando se la compara con otras tecnologías. Ethernet también ha tenido éxito porque es una tecnología flexible que ha evolucionado para satisfacer las cambiantes necesidades y capacidades de los medios.

En la tabla 1.3 se visualiza los estándares de Ethernet.

[10] http://www.rediris.es/difusion/publicaciones/boletin/49/enfoque3.html
[11] CCNA V4, Módulo 1, Network Fundamentals, Cisco 2010

Estándares	Máxima velocidad de transmisión	Tipo de cable	Dúplex	Distancia Máxima
10Base-5	10mbps	Thick Coaxial	Half	500m
10Base-2	10mbps	Thin Coaxial	Half	185m
10Base-T	10mbps	UTP Cat3/Cat5	Full	100m
100Base-TX	100mbps	UTP Cat5	Full	100m
100Base-FX	100mbps	Fibra Multimodo	Full	400m
100Base-FX	100mbps	Fibra Multimodo	Full	2km
1000Base-T	1Gbps	UTP Cat5e	Full	100m
1000Base-TX	1Gbps	UTP Cat6	Full	100m
1000Base-SX	1Gbps	Fibra Multimodo	Full	550m
1000Base-LX	1Gbps	Fibra Multimodo	Full	5km
10GBase-CX4	10Gbps	Twinaxial	Full	15m
10GBase-T	10Gbps	UTP Cat6a/Cat7	Full	100m
10GBase-LX4	10Gbps	Fibra Multimodo	Full	300m
10GBase-CX4	10Gbps	Fibra Monomodo	Full	10km

Tabla1.3 Estándares de Ethernet

1.2.2.6.1. Ethernet de 100-Mbps (Fast Ethernet)

También conocido como Fast Ethernet. Las dos tecnologías que han adquirido relevancia son 100BASE-TX, que utiliza cable UTP y 100BASE-FX, que utiliza fibra óptica. Las características comunes a 100BASE-TX y a 100BASE-FX son los tiempos de transmisión de bit, el formato de trama y algunas partes del proceso de transmisión. El formato de trama de 100-Mbps es el mismo que el de la trama de 10-Mbps.

1.2.2.6.1.1. 100BASE-TX

100BASE-TX utiliza como medio de transmisión el cable UTP Cat. 5, hace uso de la codificación 4B/5B, para luego convertir la señal a 3 niveles de transmisión multinivel o MLT-3, transportando 100 Mbps de tráfico en modo half-dúplex y en modo full-dúplex, puede transmitir 200 Mbps de tráfico.

1.2.2.6.1.2. 100BASE-FX

Este estándar puede ser aplicado para lugares donde sea útil la fibra, como conexión de backbones o en entornos de gran ruido.

100BASE-FX utiliza la codificación 4B/5B y NRZI. Para las terminaciones de fibra se utiliza conectores ST o SC generalmente. Transmite a 100 Mbps y a 200 Mbps en modo full dúplex, gracias a la utilización de rutas individuales de Transmisión (Tx) y Recepción (Rx) en la fibra óptica.

1.2.2.6.2. Ethernet Gigabit

El estándar de Gigabit Ethernet puede ser usado en medios de transmisión de fibra o de cobre. El estándar utilizado en fibra es el 1000BASE-X (IEEE 802.3z), que puede transmitir 1 Gbps en transmisiones full-dúplex. El estándar para cable de cobre es 1000BASE-T (IEEE 802.3ab), con cables UTP de categoría 5 o mayor.

La trama de Gigabit Ethernet tiene el mismo formato que el utiliza en Ethernet de 10 y 100-Mbps. Las diferencias entre Ethernet estándar, FastEthernet y Gigabit Ethernet se encuentran en la capa física. Al aumentar la velocidad en cada estándar, los bits entran al medio en menor tiempo y con mayor frecuencia, por lo que es fundamental la temporización. A mayores frecuencias, existen mayores limitaciones de ancho de banda para los medios de cobre. Estas frecuencias producen que los bits sean más sensibles al ruido en los medios de cobre, demandando que Gigabit Ethernet utilice dos distintos pasos de codificación, que permiten mantener sincronización, hacer uso eficiente del ancho de banda y mejorar las características de la Relación entre Señal y Ruido.

1.2.2.6.2.1. 1000BASE-T

Para evitar los cuellos de botella producidos por Fast Ethernet en estaciones con anchos de banda cada vez mayores, se desarrolló 1000BASE-T (IEEE 802.3ab) que

provee un ancho de banda adicional. Una de las características fundamentales del estándar para 1000BASE-T es que es compatible con 10BASE-T y 100BASE-TX.

Para lograr transmitir confiablemente 1000 Mbps en el estándar Gigabit Ethernet se requirió de una serie de pasos que a continuación se detallan: el primer paso es utilizar los cuatro pares de hilos en lugar de los dos utilizados tradicionalmente por Ethernet y Fast Ethernet. Esto se consigue a través de un circuito complejo que permite la comunicación full dúplex en el mismo par de hilos, obteniendo como resultado 250 Mbps por par. Con la utilización de los cuatro pares de hilos, obtenemos los 1000 Mbps esperados.

En medios de transmisión de cobre se combina la codificación 8B10B con la codificación 4D-PAM5. 1000BASE-T se puede transmitir tanto en half-dúplex como en full-dúplex.

1.2.2.6.2.2. 1000BASE-SX y LX

Algunos parámetros idénticos en los estándares de Gigabit Ethernet son el tiempo de bit y el formato de trama. Dos tipos de codificación se establecen en la capa física. La codificación 8B/ 10B se aplica en los medios de fibra óptica.

El estándar Gigabit Ethernet en fibra emplea la codificación 8B/10B junto a la codificación de línea sin retorno a cero (NRZ). Las señales NRZ son enviadas hacia la fibra utilizando fuentes de luz de onda corta o de onda larga. La onda corta utiliza un láser de 850 nm. y en caso de fibra multimodo (1000BASE-SX) se utiliza una fuente LED. La onda corta es la más económica de las opciones pero cubre distancias más cortas. La fuente láser de 1310 nm de onda larga utiliza fibra óptica monomodo o multimodo (1000BASE-LX). Las fuentes de láser utilizadas con fibra monomodo pueden cubrir distancias de hasta 5000 metros.

1.2.2.6.3. 10-Gigabit Ethernet

Para transmitir señales de 10 Gbps en modo full dúplex en medios de fibra óptica se tuvo que desarrollar el estándar IEEE 802.3ae. A pesar de considerarse a Ethernet como una tecnología LAN, con el aparecimiento de 10 GigE se puede cubrir distancias de hasta 40 Km a través de una fibra monomodo como una compatibilidad con la red óptica síncrona (SONET) y con redes síncronas de jerarquía digital (SDH), haciendo de 10 Gigabit Ethernet como una tecnología MAN y WAN.

10 Gigabit Ethernet puede proveer mayores anchos de banda que tecnologías Ethernet precedentes, siendo su formato de trama y otras especificaciones de Capa 2 compatibles con estándares anteriores, garantizando su interoperabilidad con la infraestructura existente.

Las tecnologías de 10 GigE son:

- 10GBASE-SR: Fibra multimodo, distancias de 26 m a 82 m.
- 10GBASE-LX4: En fibra multimodo permite distancias de 240 m a 300 m y en fibras monomodo de hasta 10 Km. Utiliza la multiplexación por división de longitud de onda (WDM).
- 10GBASE-LR y 10GBASE-ER: Admite distancias entre 10 km y 40 km en fibra monomodo.
- 10GBASE-SW, 10GBASE-LW y 10GBASE-EW: Conocidas colectivamente como 10GBASE-W. Su objetivo es trabajar con equipos WAN SONET/SDH para módulos de transporte síncrono (STM) OC-192.

1.2.2.6.4. 100 Gigabit Ethernet

La OTN (Optical Transport Network) estandarizado por la ITU-T en la serie G de recomendaciones, está basada en una jerarquía multiplexada de unidades ópticas de datos conocidas como ODUS, que son transportadas en unidades de transporte ópticos OTUS, existiendo 4:

1 – OTU1/ODU1: 2,5Gb/s
2 – OTU2/ODU2: 10Gb/s
3 – OTU3/ODU3: 40Gb/s
4 – OTU4/ODU4: 120 Gb/s

El OTU4 constituye el modelo de referencia de 100 Gigabit Ethernet. El estándar que se definió para 40-100 Gigabit Ethernet es 802.3ba utilizando WDM. Puede definir varios estándares de capa física soportados sobre fibra óptica monomodo y multimodo. En la tabla 1.4 se indica algunos detalles de las especificaciones de la capa física.

Distancia	40 Gigabit Ethernet	100 Gigabit Ethernet	Medio
10 m	40GBASE-CR4	100GBASE-CR10	COBRE
100 m	40GBASE-SR4	100GBASE-SR10	MMF OM3
125 m	40GBASE-SR4	100GBASE-SR10	MMF OM4
10 Km	40GBASE-LR4	100GBASE-LR4	SMF
40 Km		100GBASE-ER4	SMF

Tabla1.4 Estándar 100 Gigabit Ethernet

1.3. TECNOLOGÍAS DE TRANSPORTE DE INFORMACIÓN

Las tecnologías de transporte de información están asociadas con la capa 1 del modelo IOS/OSI y definen cómo la información es transportada en el medio. En este apartado se revisará la Jerarquía Digital Plesiócrona.

1.3.1. PDH

1.3.1.1. Introducción

PDH nace con la idea de transportar señales de canales digitales sobre un mismo enlace, usando técnicas de multiplexación por división de tiempo y equipos digitales

de transmisión. Las velocidades según el estándar Europeo de los canales a multiplexar son: 2 Mbps, 8.4 Mbps, 34 Mbps y 140 Mbps. Las velocidades según el estándar Norteamericano de los canales a multiplexar son: 1.5 Mbps, 6.3 Mbps, 45 Mbps y 274 Mbps.

1.3.1.2. Jerarquía PDH

PDH usa canales de 64 Kbps, a medida que aumenta el nivel de multiplexación se adicionan más números de canales sobre el medio físico. Por lo cual cada trama tiene su respectivo nivel, estructuras y duración.

En una trama PDH se agrega información de control, adicional a los canales de voz que viajan por estas tramas.

Los tres tipos de jerarquía PDH son: la europea, la norteamericana y la japonesa. Cada una de las cuales tienen sus propios esquemas de circuitos y velocidades en cada nivel jerárquico.

En la tabla 1.5 se muestran los distintos niveles de multiplexación PDH, según los estándares Norteamericano, Europeo y Japonés.

Nivel	Norteamericana			Europa			Japón		
	Circuito	Kbit/s	Denominación	Circuito	Kbit/s	Denominación	Circuito	Kbit/s	Denominación
1	24	1544	(T1)	30	2048	(E1)	24	1544	(J1)
2	96	6312	(T2)	120	8448	(E2)	96	6312	(J2)
3	672	44736	(T3)	480	34368	(E3)	480	32064	(J3)
4	2016	274176	(T4)	1920	139264	(E4)	1440	97728	(J4)

Tabla1.5 Jerarquía PDH

1.3.1.3. Jerarquía PDH según estándar Europeo

El primer nivel jerárquico de PDH, según la norma Europea es el E1, que es un flujo de datos de 2,048 Kbps. Un flujo PDH E1 se lo puede formar reuniendo un número de 30 canales de voz más 2 canales de 64 Kbps, que son empleados para la sincronización y señalización de los canales de voz. Los 64 Kbps de los canales PDH se obtienen mediante la digitalización de la señal de voz, usando una frecuencia de muestreo de 8 kHz (una muestra por cada 125 µs) y cada muestra se codifica con 8 bits con lo que da como resultado los 64 Kbps.

Los flujos de datos de la trama E1 se los controla mediante un reloj ubicado en el equipo que genera los datos. La velocidad entre flujo de datos puede variar ligeramente una de otra, aún permitiendo su funcionamiento normal.

La multiplexación de varios flujos de la trama E1 de PDH, se los realiza combinándolos en grupos de cuatro en un equipo multiplexor. La multiplexación se lleva a cabo intercalando un bit de cada flujo E1. También se agrega bits adicionales con el propósito de permitir al demultiplexor del equipo lejano identificar qué bits corresponden a cada flujo de E1 y así reconstruir los flujos originales. Estos bits añadidos se componen de los llamados bits de justificación o de relleno y de una mezcla fija de unos y ceros que es la denominada palabra de alineamiento de trama, que se transmite cada vez que se completa el envío de los 30+2 canales de cada uno de los 4 flujos de E1, que es lo que constituye una trama del orden superior (8 Mbps o E2).

1.3.1.4. Trama PDH (E1)

Cada trama tiene 32 slots de Tiempo TS (Time Slot), numerados de 0 a 31. Cada slot de tiempo transporta un Byte a una tasa de muestreo de 8 Khz, lo que genera una tasa de transmisión de 64 kbps, la duración de la trama es de 125 useg. Una multitrama está formada de 16 tramas numeradas de 0 a 15, que es la encargada de la organización temporal de los canales digitales.

El primer slot de tiempo, numerado como 0, se emplea para transmitir el alineamiento de trama e información de supervisión del enlace. El slot de tiempo número 16 se utiliza para Señalización Asociada al Canal. Los slots número 1 a número 15 y del slot número 17 al número 31 transportan los canales de telefonía digital o datos a 64 kbps. La combinación de los 32 canales (slots de tiempo) de 64 kbps conforman los 2048 kbps de una trama E1.

1.4. MODELOS DE GESTIÓN

La gestión de red es un proceso que incluye el despliegue, integración y coordinación tanto de los recursos de hardware, software y humanos con el fin de sondear, monitorizar, probar, configurar, evaluar, analizar y controlar los recursos de red con el fin de obtener los requerimientos de tiempo real, desempeño óptimo, calidad de servicio de la red, a un costo razonable.

Por lo tanto el proceso de gestión de red, es un proceso vital para el desempeño óptimo de una red, siendo importante la sistematización del mismo a través de un modelo que proporcione criterios para gestionar la red de forma eficaz y eficiente.

Los modelos de gestión se dividen en dos grupos, los modelos de gestión orientada a las redes y los modelos de gestión de telecomunicaciones, pero el proceso de integración de las redes y los sistemas de telecomunicaciones obliga a fusionar las mejores prácticas de varias modelos. Estos modelos se los puede observar en la figura 1.12.

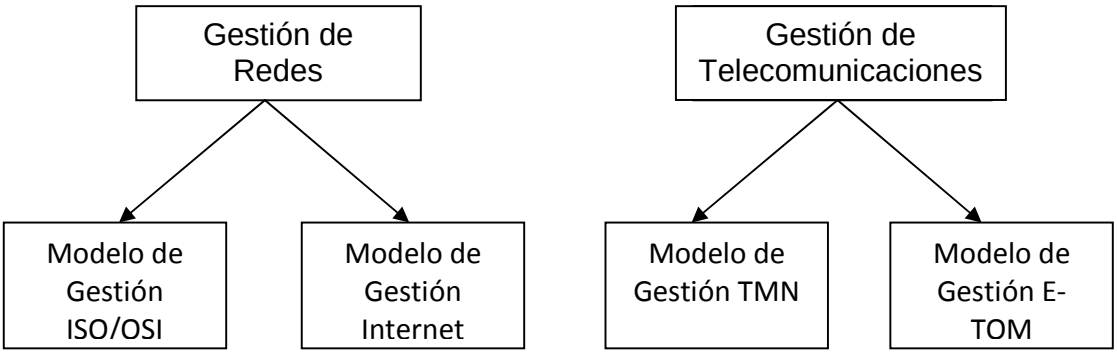


Figura 1.12 Tipos de Modelos de Gestión

1.4.1. MODELO DE GESTIÓN ISO/OSI

El modelo de Gestión ISO/OSI define 4 modelos básicos: Funcional, Organizacional, Comunicacional, Informativo.

1.4.1.1. Modelo Funcional

Define las tareas o funciones a las áreas de gestión de una red, esta lista de funciones se las conoce como modelo FCAPS.

F - Fallos
C – Configuración
A – Contabilidad
P – Rendimiento
S – Seguridad

1.4.1.1.1. Fallos

Tiene como objetivo la detección ubicación y recuperación de los problemas de la red, en base a tres tareas principales:

- Detección de fallas.
- Manejo de Alarmas.
- Corrección del problema y verificación.

1.4.1.1.2. Configuración

Proceso de obtención de requerimientos de la red y utilización de los mismos para incorporar, mantener y retirar los diferentes componentes y recursos de la red. Con tres tareas fundamentales:

- Recolección de datos sobre el estado de la red.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

1.4.1.1.3. Contabilidad

Tienen como objetivo la recolección de datos estadísticos de la red que permitan generar informes de tarifación, que reflejen la utilización de los recursos por parte de los usuarios. Con dos tareas fundamentales:

- Recolección de datos sobre la utilización de los recursos.
- Establecimiento de tarifas.

1.4.1.1.4. Rendimiento

Tiene como objetivo principal el mantenimiento de un buen nivel de rendimiento de la red, para esta tarea es necesario parametrizar el rendimiento de la red. Al realizarlo de una forma cuantitativa se puede estimar las acciones para mejorar o mantener el rendimiento de la red. Tiene cuatro tareas fundamentales:

- Recolección de datos sobre el rendimiento de la red.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales.
- Reporte programado de datos.

1.4.1.1.5. Seguridad

Tiene como objetivo establecer y aplicar mecanismos que permitan cumplir las políticas de seguridad, con cuatro tareas fundamentales:

- Identificación de la información a proteger y dónde se encuentra.
- Identificación de los puntos de acceso a la información.
- Protección de los puntos de acceso, detección de intrusos y políticas de seguridad.
- Respuestas a incidentes.

El modelo Funcional del modelo de gestión ISO/OSI es de amplia utilización, debido a que divide y asigna de forma muy clara las tareas de gestión.

1.4.1.2. Modelo Organizacional

Define los elementos que participan en la gestión de red y sus roles. Teniendo como arquitectura el modelo gestor-agente, agrupa los elementos administrados en grupos llamados Dominios.

Define un sistema administrador, que a través de un proceso realiza las peticiones y recibe las respuestas y notificaciones, también define un sistema administrable que recibe las notificaciones, las procesa y genera una respuesta, además de generar notificaciones.

El sistema administrable, se lo puede dividir en cuatro subsistemas, control de acceso, procesamiento de las operaciones, procesamiento de las notificaciones, generador de notificaciones. Interactúa con las bases de información para la administración (MIB) para obtener la información del agente.

1.4.1.3. Modelo Comunicacional

Define las características para realizar el proceso de comunicación entre los elementos de gestión de RED, definiendo el protocolo de comunicación CMIP (Common Management Information Protocol).

MIP tiene poca aceptación y su implementación es mínima por lo que no se ahondara en detalles del protocolo. Define las siguientes primitivas: M-EVENT-REPORT, M-GET, M-SET, M-CANCEL, M-DELETE, M-ACTION, M-CREATION.

1.4.1.4. Modelo Informativo

Se basa en el paradigma orientado a objetos, desarrollando su estructura a través del modelo organizacional. Define los objetos a través de sus atributos y métodos.

1.4.2. MODELO DE GESTIÓN TMN (TELECOMMUNICATIONS MANAGEMENT NETWORK)

Define 4 arquitecturas: Funcional, Física, Niveles, Informativa.

1.4.2.1. Arquitectura Funcional

Define tareas o funciones a realizar en la gestión de red basadas en bloques funcionales que son ejecutadas por los elementos físicos del modelo TMN. Define 5 bloques funcionales:

- Bloque de función de sistemas de operaciones (Operations Systems Function: OSF)
- Bloque de función de elemento de red (Network Element Function: NEF)
- Bloque de función de estación de trabajo (Worstation Function: WSF)
- Bloque de función de mediación (Mediation Function: MF)
- Bloque de función de adaptador Q (Q Adaptador Function: QAF)

Utiliza el concepto de puntos de referencia para definir relaciones entre los bloques funcionales.

1.4.2.2. Arquitectura Física

Define cómo se implementan los bloques funcionales. La M.3010 define los elementos físicos de TMN, siendo:

- Sistema de operaciones (Operations System: OS)
- Estación de trabajo (Workstation: WS)
- Elemento de red (Network Element: NE)
- Red de comunicación de datos (Data Communication Network: DCN)
- Dispositivo de mediación (Mediation Device: MD)
- Adaptador Q (Q Adaptor: QA)

La implementación de los puntos de referencia se los realiza a través de interfaces. En la figura 1.13 se indica las interfaces de la arquitectura física.

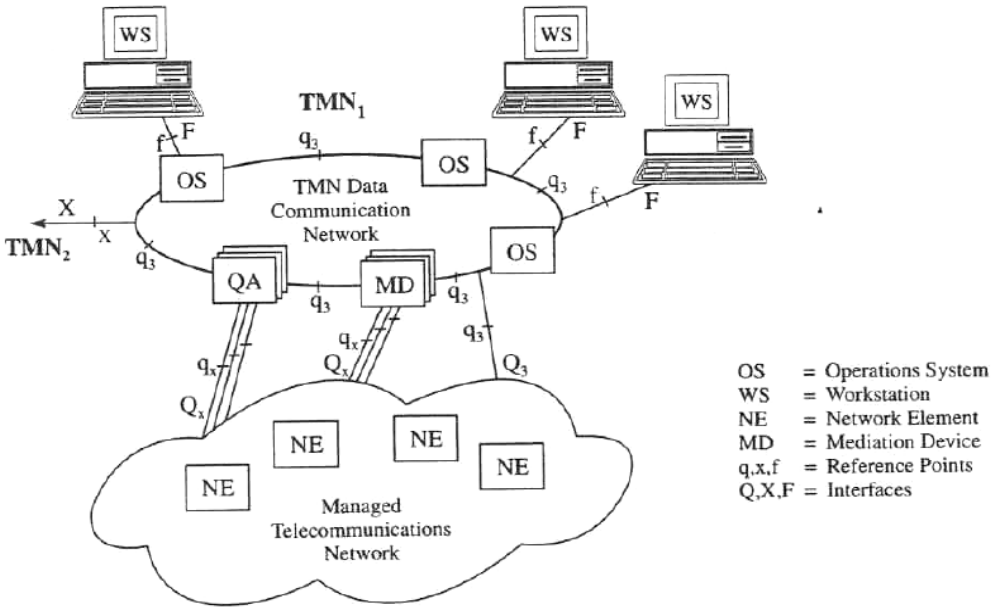


Figura 1.13 Interfaces de la Arquitectura Física[12]

[12] http://www.eie.fceia.unr.edu.ar/ftp/Tecnologiasdebandaangosta/Notas_sobre_TMN.pdf

1.4.2.3. Arquitectura lógica por niveles

Proporciona una jerarquización y estratificación de los servicios de la red. Esta arquitectura es el principal aporte del modelo de Gestión TMN debido a que integra en sus dos últimos niveles el negocio de la empresa y los tipos de servicios que ofrece. Define 5 niveles se gestión (figura 1.14): Negocio, Servicios, Red, Gestión de los elementos de red y Elementos de red.

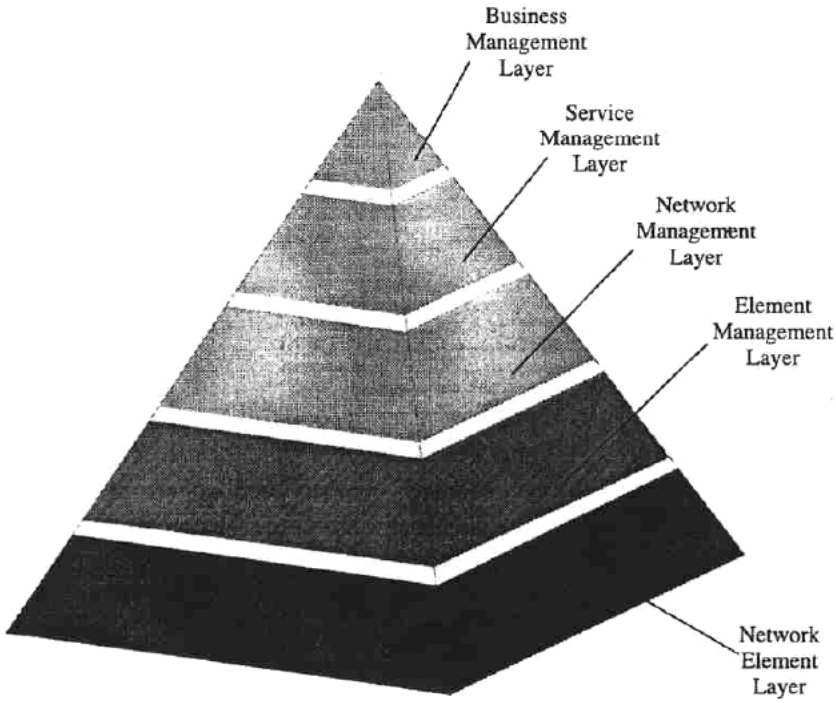


Figura 1.14 Niveles de Gestión TMN[13]

1.4.2.4. Modelo Informativo

El modelo de información es similar al modelo informativo en el modelo de gestión ISO/OSI, al igual que éste la arquitectura de información de TMN está basada sobre un modelo orientado a objetos, utiliza el modelo agente-gestor.

[13] http://www.eie.fceia.unr.edu.ar/ftp/Tecnologiasdebandaangosta/Notas_sobre_TMN.pdf

1.4.3. MODELO DE GESTIÓN E-TOM (ENHANCED TELECOM OPERATIONS MAP)

Es un modelo de mejora al modelo TMN. Con la diferencia que desarrolla las tareas de gestión a nivel de la capa de negocios y servicios.

1.4.4. MODELO DE GESTIÓN INTERNET

Está compuesto por 4 elementos: Gestores o NMS, Agentes, MIB y el protocolo de administración de red SNMP. En la versión 3 del protocolo SNMP no se maneja el concepto de agente, se define el agente Entidad y el agente NMS (Network Management System).

El NMS está definido como el software que permite realizar las peticiones de información de los recursos de un determinado dispositivo a través del protocolo SNMP, para su procesamiento.

El agente está definido como el software que permite acceder a la información de los recursos del dispositivo a través de las MIBs. MIB es el conjunto de todos los objetos posibles de un dispositivo, entendiendo por objetos las variables que describen el estado del dispositivo.

En la figura 1.15 se observa los elementos del modelo de Gestión Internet.

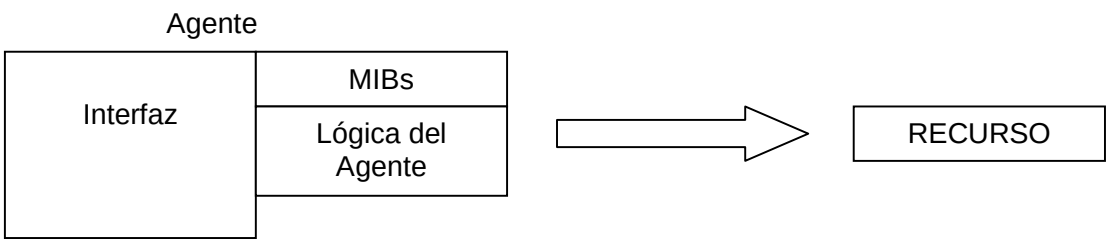


Figura 1.15 Modelo de Gestión Internet

1.4.4.1. Tipos de Agente

1.4.4.1.1. Agente Maestro-Subagente

Este agente se caracteriza por recibir peticiones a través de puertos bien conocidos y delegar tareas a los subagentes abriendo otros puertos de comunicación con los mismos, los subagentes son los que van a estar en contacto directo con las MIBs.

1.4.4.1.2. Agente Proxy

Este agente tiene como función principal mantener la transparencia para el usuario sin importar la versión de protocolo SNMP que se utiliza, el agente proxy es el encargado de hacer las traducciones necesarias entre las distintas primitivas de las versiones de protocolos.

1.4.4.2. Protocolo SNMP (Simple Network Management Protocol)

Protocolo de capa aplicación que permite el intercambio de información para la gestión de una red. SNMP como primera versión fue definida en el RFC 1157, convirtiéndose en el protocolo de administración de red con más aceptación. Permite que todos los dispositivos de networking y de comunicaciones permitan ser administrados independientemente del fabricante. El protocolo SNMP está orientado al modelo TCP/IP con 3 versiones disponibles.

El protocolo SNMP corre sobre UDP en los puertos 161 para peticiones y 162 para el envío de traps (PDU de generación asincrónica para notificar algún evento).

SNMP hace uso de un lenguaje de notación sintáctica abstracto (ASN) que independiza la plataforma del protocolo SNMP, para la representación de los objetos que manejan las MIB. ASN usa para su desarrollo las estructuras para la administración de información SMI.

Para el envío de mensajes, SNMP los empaqueta siguiendo las reglas de codificación básicas (BER) a través de los campos Tipo, Longitud, Valor (TLV).

1.4.4.2.1. SNMP Versión 1

Primera versión del protocolo SNMP, define grupos de dispositivos a ser administrados bajo el concepto de comunidades, además de 5 tipos de PDU (unidad de datos del protocolo). Las PDU que definen son:

GetRequest.- Realiza la petición de información del dispositivo a ser gestionado, a través del agente de cada dispositivo.

GetNextRequest.- Realiza la petición de información del siguiente dato solicitado del dispositivo a ser gestionado, a través del agente de cada dispositivo.

GetResponse.- Devuelve la información solicitada por el NMS.

SetRequest.- Permite modificar los datos del dispositivo gestionado.

Trap.- Envía notificaciones de tipo asincrónica cuando existe algún evento especifico en el dispositivo gestionado.

1.4.4.2.2. SNMP Versión 2

Mantiene la base de funcionamiento de la versión 1 añadiendo nuevas PDU que mejoran el desempeño de SNMP, mantiene el concepto de comunidades. Define 4 nuevas PDUs, que son:

GetBulkRequest.- Solicita información del agente del dispositivo a ser gestionado de forma eficiente, obteniendo la mayor cantidad de información, que depende de parámetros en el agente y las características de los objetos solicitados.

InformRequest.- Distribuye información de los dispositivos gestionados entre diferentes NMS.

TrapV2.- Genera notificaciones desde al Agente al NMS, se diferencia de la trap de la versión 1 por la estructura de la PDU.

Report.- PDU no implementada.

1.4.4.2.3. SNMP Versión 3

La principal implementación que se genera en la versión 3 del protocolo SNMP es la inclusión de niveles de seguridad, debido a que ésta era una de las mayores vulnerabilidades de sus predecesores al no implementar autenticación y transmitir la información en texto plano.

En la versión 3 ya no se maneja el concepto de comunidad, el manejo se lo realiza a través de usuarios, y la definición de NMS-Agente es sustituido por el de Entidad. El soporte a las versiones 1 y 2 es de forma transparente. Implementa 3 niveles de Seguridad:

- noAuth noPriv
- Auth no Priv
- Auth Priv

Para la implementación de mecanismos de autenticación se utilizan los algoritmos de hash MD5 y SHA, para la encripción se utilizan los algoritmos DES y AES.

1.4.4.2.3.1. Entidad

Una entidad está conformado por dos partes: la aplicación y el motor. La aplicación es la encargada de generar y procesar la información de o desde las MIBs, entre sus principales funciones y dependiendo si es una entidad agente o una entidad NMS están:

- Generar o recibir comandos, Generar o recibir notificaciones, funciones de proxy para la transparencia de la versión de SNMP.

El motor es el encargado de adaptar la información para su transmisión a través de la red, además de implementar los mecanismos de seguridad y control de acceso. La definición de motor en SNMP permite que se trabaje con más de un motor en un mismo dispositivo.

El mecanismo de seguridad que implementa SNMP 3 es USM (Modelo de seguridad de Usuario), basa su funcionamiento en usuarios, a los que se les definen los niveles de seguridad, es decir el tipo de autenticación que usará y el nivel de privacidad.

El mecanismo de control de acceso que implementa SNMP3 es VACM (Modelo de Control de Acceso por Vistas), basado en los niveles del árbol MIB, permite o deniega el acceso a la parte del árbol MIB que se configure. La figura 1.16 indica la arquitectura del protocolo SNMP v3.

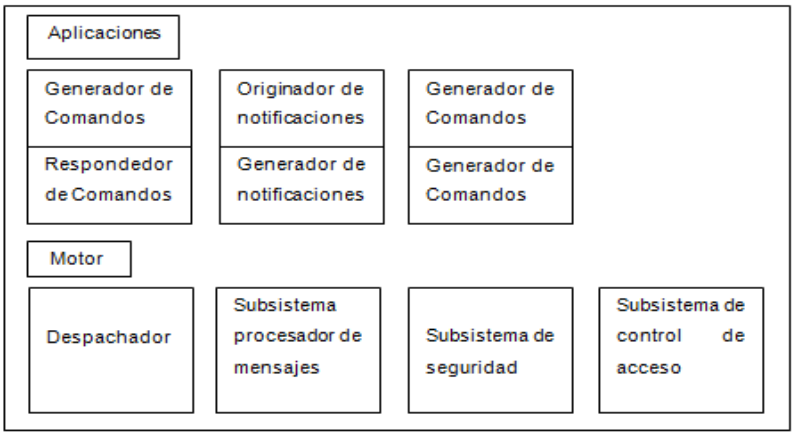


Figura 1.16 Arquitectura Protocolo SNMP v3

1.4.4.3. Monitorización Pasiva

La monitorización pasiva fue desarrollada para las plataformas UNIX pero su aceptación fue tal que en la actualidad se encuentra en todos los dispositivos de red y equipos computacionales, basa su funcionamiento en el envió de notificaciones llamados LOGs, disparados por eventos, permitiendo monitorizar cualquier estado del sistema. La arquitectura que emplea la monitorización pasiva es cliente-servidor

en la cual existe un servidor de LOGs que recibe la información de forma asincrónica de los clientes.

Maneja niveles de severidad para indicar que tan crítico es el LOG que es enviado al servidor, la mayoría de equipos utiliza 8 niveles de severidad.

- EMERGENCIA 0
- ALERTA 1
- CRITICO 2
- ERROR 3
- ADVERTENCIA 4
- NOTIFICACION 5
- INFORMATIVO 6
- DEPURACION 7

1.5. INTEGRACIÓN DE SERVICIOS

El concepto de integración de servicios se define como la inclusión, en un mismo dispositivo, de funciones o servicios adicionales de red, además de sus funciones básicas. Su desarrollo se da principalmente gracias a la potencialidad de los sistemas LINUX de ofrecer una amplia variedad de servicios de red en una misma plataforma, teniendo la ventaja de ser un sistema operativo robusto y de libre distribución y como desventaja el soporte técnico que se puede obtener en problemas que se puedan presentar.

Es común encontrar equipos que ofrecen una gama de servicios de red (Correo, Servidor WEB, Firewall) que corren sobre LINUX, integrando en un solo equipo físico varias funcionalidades de red.

Como respuesta a este abrumador crecimiento de equipos basados en LINUX, las marcas convencionales de equipo de internetworking han buscado soluciones orientadas a integración de servicios, la solución que ofrece CISCO integra servicios en sus equipos de enrutamiento.

Los equipos CISCO que soportan integración de servicios, ofrecen funcionalidades de Telefonía IP, Firewalls, etc. Para la solución de Telefonía IP CISCO integra en sus equipos de enrutamiento una central telefónica IP, llamada CISCO CALL MANAGER, existiendo dos tipos de versiones, la versión EXPRESS orientada a las pequeñas y medianas empresas, y la versión ENTERPRISE orientada a grandes empresas.

1.5.1. VoIP

VoIP permite que la voz viaje a través de una red de datos trasportada por el protocolo IP. La voz es digitalizada y transportada en paquetes.

La Voz sobre IP se diferencia de la Telefonía sobre IP, debido a que la VoIP es la *tecnología* que permite comunicar voz sobre el protocolo IP. A la telefonía sobre IP se le conoce como el servicio telefónico realizado con tecnología de VoIP.

1.5.1.1. Ventajas

Una de las principales ventajas del uso de este servicio, es la reducción drástica de los costos de la telefonía tradicional, esto se debe que se utiliza una misma red para transportar datos y voz. Esto se lo realiza especialmente cuando los usuarios de la red no utilizan toda la capacidad de esta, permitiendo enviar tráfico de voz sin un costo adicional.

Para optimizar el ancho de banda que requiere los paquetes de voz, se han desarrollado protocolos que permiten codificar estos paquetes de datos en tamaños cada vez más pequeños. Algunos de estos códecs se los revisa a continuación.

1.5.1.2. Protocolos de VoIP

Los protocolos establecen las reglas que permiten la comunicación entre los diferentes dispositivos VoIP. Su correcto uso determinará cuan eficaz y compleja será la comunicación. Algunos protocolos que se han desarrollado son:

- H.323 - Protocolo definido por la ITU-T;
- SIP - Protocolo definido por la IETF;
- Megaco (También conocido como H.248) y MGCP - Protocolos de control;
- Skinny Client Control Protocol - Protocolo propiedad de Cisco;
- MiNet - Protocolo propiedad de Mitel;
- CorNet-IP - Protocolo propiedad de Siemens;
- IAX - Protocolo original para la comunicación entre PBXs Asterisk
- Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype;
- IAX2 - Protocolo para la comunicación entre PBXs Asterisk, reemplazo de IAX;
- Jingle - Protocolo abierto utilizado en tecnología Jabber;
- SCCP- Protocolo propietario de Cisco;
- weSIP- Protocolo licencia gratuita de VozTelecom

1.5.1.2.1. H.323

H.323 define los protocolos para proveer sesiones de comunicación audiovisual sobre redes de datos. H.323 se aplica en Voz sobre IP y en videoconferencia basada en IP. Esta norma fue establecida por la ITU para determinar la señalización en redes IP, entre equipos, terminales y servicios. Este conjunto de protocolos establece un transporte de voz y datos no confiables y sin calidad de servicio. Además, es independiente de la topología de la red y permite utilizar gateways que ayudan a transmitir al mismo tiempo canales de voz, video y datos.

La arquitectura de red basada en H.323 está compuesta por los siguientes elementos:

- *Terminales*: Son los dispositivos finales utilizados por los usuarios, reemplazan a los teléfonos análogos. Pueden ser usados tanto en software como en hardware.
- Gatekeepers: Son el centro de las operaciones de VoIP. Se encargan de controlar las llamadas. Realizan las traducciones de direcciones, encaminar la señalización, además de monitorear el consumo de la central.
- Gateway: es el enlace a otras redes y a la red telefónica tradicional, se encarga de realizar funciones de codificación y traducción de señalización.
- MCU: Las Unidades de Control Multipunto sirven para soporte de multiconferencias. Son las encargadas de la negociación de las capacidades.

Dentro de las características principales de este protocolo tenemos las siguientes:

- Permite monitorear el tráfico de la red, evitando errores importantes que afecten su rendimiento.
- Es autónomo tanto de la red física que soporta como del hardware implementado.

1.5.1.2.2. SCCP (Skinny Client Control Protocol), Protocolo de Control de Cliente Ligero

Protocolo propietario de CISCO. Skinny es un protocolo ligero que permite una comunicación eficiente con un sistema Cisco Call Manager. Está diseñado para una utilización ligera de recursos de procesamiento y memoria.

El Call Manager puede actuar como un proxy de señalización para llamadas con otros sistemas que utilizan otro tipo de señalización como H.323, SIP, etc.

La comunicación con el Call Manager se da solo para el establecimiento de la llamada, el intercambio de mensajes de voz se da entre dispositivos finales, utilizando el protocolo RTP.

1.5.1.2.3. SIP (Session Initation Protocol), Protocolo de Inicio de Sesión

Protocolo de iniciación de sesión, es un protocolo de señalización, para crear, modificar y cerrar sesiones con uno o más participantes. Entre sus principales características tenemos:

- Simplicidad al utilizar mensajes en texto plano y formatos estándares como HTTP 1.1, esto hace que el protocolo sea relativamente sencillo.
- Eficiencia, consume poco ancho de banda, es muy eficaz en el tiempo de conexión de la llamada, debido a que toda la información que se pide para el establecimiento de la llamada está en el mensaje inicial.
- Escalabilidad, no se mantiene información del estado de las sesiones basadas en UDP en el SIP que procesan, por lo que un solo servidor puede manipular varios clientes, además prevé lazos de enrutamiento de mensajes.
- Flexibilidad, SIP usa SDP (Session Description Protocolo) para negociar los códecs, por lo que se puede utilizar cualquier códec registrado por la IANA.

1.5.1.2.3.1. Componente del Sistema

*Agentes de Usuario UA***.-** Son aplicaciones de punto final que reciben y envían peticiones SIP para beneficio de los usuarios. Los clientes de agentes del usuario envían peticiones SIP a la parte llamante, y los servidores de agentes de usuario reciben las respuestas de la parte llamada. Se asocia cada dirección SIP con cada agente del usuario.

Servidores Proxy.- Reciben peticiones SIP de clientes, e inician nuevas peticiones hacia los agentes del usuario de destino, son similares a los gatekeeper de H.323. Los servidores proxy SIP pueden tener reconocimiento local de los agentes de

usuario desde un registrador SIP. También pueden conocer varias alternativas para localizar a un agente de usuario.

Registradores.- Aceptan registros de los clientes que indican las direcciones en las que se les puede localizar.

1.5.1.2.3.2. Direccionamiento

Solo los usuarios y agentes de usuarios tienen direcciones SIP. Los servidores SIP (proxy, redirección y registradores) se identifican por sus respectivos sockets, los servidores SIP escuchan en los puertos TCP y UDP 5060.

Sintaxis de dirección SIP

Un URL SIP básico tiene el siguiente formato:
"sip:" [user [":" password] "@"] ((hostname | IP-address) [::port]

Ejemplo: sip:bob:secret@company.com:5060

Soporte SIP para direcciones E.164

SIP distingue los puntos finales E.164 de los puntos finales IP regulares, utilizando los parámetros del usuario en un URL SIP.

Ejemplo: sip:4199@192.168.0.1:5060;user=phone

URL de teléfono para direcciones E.164

La telefonía URLS proporciona tres alternativas al URL SIP: teléfono, fax y modem, además de codificar los números básicos, estos URLs también pueden indicar las capacidades de los dispositivos asociados a las secuencias especiales de las llamadas.

Ejemplo: tel:+14085551212;postd=w1234

El ejemplo indica con una instrucción post-dial, que se debería esperar un segundo tono de llamada después de marcar el número original, e introducir la extensión 1234.

Ubicación del servidor

SIP suele utilizar servidores proxy locales como próximo salto al punto de retraso para todas las solicitudes salientes. A fin de que los servidores proxy enruten apropiadamente las solicitudes SIP entrantes, pueden utilizar la información de un registrador SIP. Por lo que los clientes deberán localizar tanto los servidores proxy como los registradores.

Servidor Proxy

El método que se utiliza para que los clientes UA localicen dinámicamente los servidores SIP, aprovecha el registro de recursos SRV en DNS.

El cliente UA consulta al servidor DNS por el registro SRV con el tipo de servicio y el nombre de dominio DNS correcto. El servidor DNS responde con el nombre del host y el puerto del servidor SIP.

Otra opción es la de utilizar la opción 66 del servidor DHCP que permite dar una dirección para el servidor TFTP, para que el cliente descargue un archivo de configuración que contenga el nombre de dominio, o la dirección y puerto del servidor SIP.

Registrador

Los usuarios SIP se pueden configurar estáticamente con la dirección del registrador, o se lo puede encontrar a través de multidifusión, la dirección multicast reservada que se utiliza es la 224.0.1.75. Los agentes de usuarios SIP de su red pueden escuchar las direcciones multidifusión del registrador SIP para aprender de la presencia de otros agentes de usuario.

1.5.1.3. Códecs

Para la transmisión de señales de voz a través de la red es necesario el uso de códecs, éstos permiten la codificación y compresión del audio o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado se determinará el consumo de ancho de banda dentro de la red. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.

Entre los códecs utilizados en VoIP encontramos los G.711, G.723.1 y el G.729 (especificados por la ITU-T).

1.5.1.3.1. G.711

Estándar ITU conocido como PCM, digitaliza la voz a una tasa de muestreo de 8 Khz, utilizando 8 bits por muestra lo que genera una tasa de transmisión de 64 Kbps. No realiza compresión basada en la naturaleza de las conversaciones telefónicas.

1.5.1.3.2. G.729[14]

Estándar ITU, comprime la voz utilizando la técnica de compresión de fuente, por lo que se los conoce como vocoders, específicamente utiliza la técnica CELP (códec-excite linear prediction). Este codificador usa como señal de entrada tramas de 10 milisegundos, correspondientes a 80 muestras de voz, muestreadas a 8000 Hz. De cada trama de entrada, el codificador determina los coeficientes de predicción lineal, índices del libro de código (Usa un libro de códigos que es retroalimentado continuamente para predecir las formas de onda de la voz), y parámetros de ganancia, los cuales son codificados para su posterior envío. Estas piezas de información son transmitidas hasta el final en una trama conformada por 80 bits.

Tomando en cuenta que cada trama de 80 bits es procesada en 10 ms tenemos como resultado un códec con tasas de transmisión de 8 Kbps.

---

[14] Daniel Collins, Carrier grade voice over IP, McGraw-Hill Professional, 2002

G.729. Anexo A. El funcionamiento del códec G.729 es un poco complejo. Por lo que para reducir la complejidad de su algoritmo, se introdujo algunas simplificaciones en el Anexo A del códec. Alguna de ellas son: introducir rutinas de búsqueda del código de libro mucho más sencillas, simplificar los filtros posteriores al decodificador, entre otras. G.729A usa exactamente la misma estructura de trama transmitida por G.729, por lo tanto usa el mismo ancho de banda. Esto significa que el codificador puede funcionar de acuerdo a G.729, mientras que el decodificador puede funcionar usando G.729A o viceversa. G729A puede resultar en un códec con una calidad un tanto menor a la de G.729.

G.729 Anexo B. El anexo B de G.729 es una recomendación para la detección de actividad de voz (VAD voice activity detection), transmisión discontinua (DTX discontinuos transmission) y la generación de ruido confortable (CNG confort noise generation). VAD detecta si existe voz o ruido presente a la entrada. La detección se realiza en base a un análisis de varios parámetros de la señal de entrada, sin embargo este análisis no se lo hace fundamentándose simplemente en una trama, por el contrario, la decisión se toma basándose en la trama actual, más las dos tramas precedentes. Este mecanismo asegura que la transmisión ocurra para al menos dos tramas después que la persona pare de hablar.

Otra función realizada por VAD es la de decidir si enviar absolutamente nada o enviar una trama SID. La trama SID contiene cierta información que permite al decodificador generar ruido de confort que simula el ruido de fondo en el extremo de la transmisión. La trama SID de G.729B contiene 15 bits, significativamente más pequeña que la trama de voz de 80 bits.

Asumiendo que el silencio continúa por algún tiempo, el codificador se mantiene alerta al ruido de fondo. Si no hay ningún cambio significativo, nada es enviado y el decodificador continua generando ese ruido de confort. En cambio, si, el codificador nota un cambio significativo en la energía del ruido de fondo, una actualización de la trama SID es enviada para actualizar las características del ruido de fondo del

decodificador. Esto evita que el ruido de confort sea constante, y si persiste por un buen tiempo, sea molestoso para el oyente.

G.729 Anexo D. G.729 Anexo D fue desarrollado con el propósito de ser una extensión con menor tasa que la del algoritmo básico de G.729. Al igual que el algoritmo básico de G.729, el Anexo D opera con muestras de voz de 10 milisegundos. Sin embargo, en vez de enviar 80 bits por trama, el algoritmo del Anexo D, usa tramas de 64 bits, resultando en una tasa de bits de 6.4 Kbps.
G.729 Anexo D, provee una menor calidad que la proporcionada por el códec G.729 original, a cambio de obtener un ancho de banda más reducido.

G.729 Anexo E. G.729 Anexo E ofrece un mayor aumento en la tasa de bits que la producida en el algoritmo básico de G.729. El propósito de este aumento es la de proveer mayor robustez en presencia de ruidos de fondo significativos (particularmente música) a la entrada. G.729 usa un filtro de predicción lineal de décimo orden, lo que significa que el filtro contiene 10 coeficientes. El codificador de G.729E usa un filtro de 30 coeficientes. Además, el libro de código de G.729E es de 44 bits, en contraposición el de G.729 es de 35 bits. El efecto neto de estos cambios es que G.729E transmite 118 bits por cada 10 milisegundos de señal de entrada, resultando en una tasa de bits de 11.8 Kbps.

1.5.1.4. Retardo

Un retardo por debajo de los 150 ms se considera aceptable para la transmisión de VoIP.[15]

Una de las técnicas empleadas si una muestra de voz es perdida, es la de dejar un intervalo en el flujo de voz por parte de la terminal. Si muchos paquetes de voz se pierden, se puede aplicar un método de recuperación, que consiste en repetir muestras de voz previas. Esto se lo puede realizar solo si algunos paquetes se han

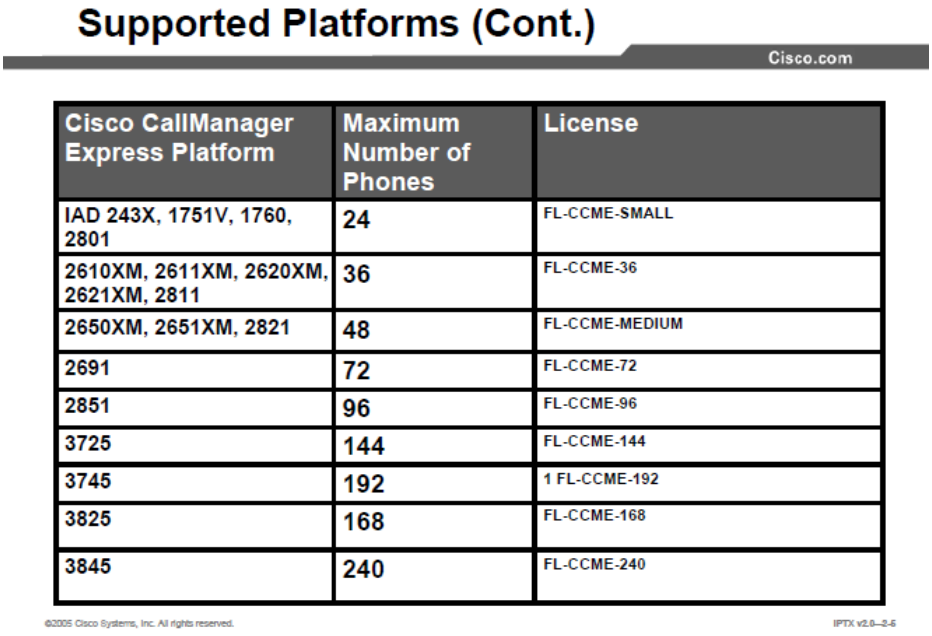
[15] Sistemas de telefonía, José Manuel Huidobro Moya, Rafael Conesa Pastor, Editorial Paraninfo, 2006

perdido. Si hay gran cantidad de errores, se utilizan generalmente técnicas de interpolación. Basándose en paquetes de voz previos, el decodificador predecirá los paquetes perdidos. Este método es conocido como Packet Loss Concealment (PLC).

1.5.2. CISCO CALL MANAGER EXPRESS (CCME)

El soporte otorgado para la central telefónica IP, lo da el IOS del equipo de enrutamiento, no todos los IOS para un mismo equipo soporta CCME, por ejemplo la versión CCME 3.2.1 requieren un IOS mínimo, el RELEASE 12. (11)T, que además debe soportar las funcionalidades de voz sobre IP, se puede utilizar los IOS ipadvancedservices.

Las versiones de Routers que soportan CCME con el número máximo de teléfonos se detallan a en la figura 1.17.



Supported Platforms (Cont.)

Cisco.com

Cisco CallManager Express Platform	Maximum Number of Phones	License
IAD 243X, 1751V, 1760, 2801	24	FL-CCME-SMALL
2610XM, 2611XM, 2620XM, 2621XM, 2811	36	FL-CCME-36
2650XM, 2651XM, 2821	48	FL-CCME-MEDIUM
2691	72	FL-CCME-72
2851	96	FL-CCME-96
3725	144	FL-CCME-144
3745	192	1 FL-CCME-192
3825	168	FL-CCME-168
3845	240	FL-CCME-240

Figura 1.17 Versiones de Routers que soportan CCME[16]

[16]Cisco, Studen Guide IP Telephony Express, 2005

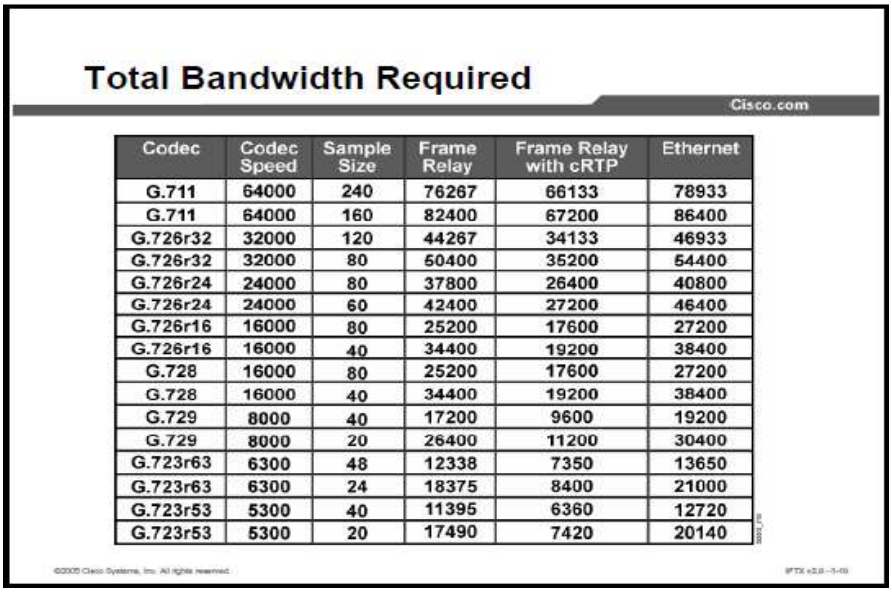
1.5.2.1. Funcionamiento

Teniendo como requisito la conectividad entre el teléfono y el CCME y que ya sea por DHCP o por configuración manual, el teléfono conozca la dirección del servidor TFTP, el primer paso que realiza el teléfono es descargarse o actualizar su firmware del servidor TFTP que puede ser configurado en el Router o puede ser un servidor externo; una vez el teléfono tenga su firmware, se registra en el CCME y se descarga el archivo de configuración que tenga asignado para el teléfono, el registro del teléfono se lo realiza por MAC-ADDRESS.

Una vez tenga el archivo de configuración el teléfono, puede realizar llamadas, el establecimiento de la llamada se lo realiza en el CCME utilizando el protocolo SSCP o SIP, una vez establecida la llamada el trafico de voz ya no pasa por el CCME, dándose directamente entre los teléfonos IP, utilizando el protocolo RTP.

1.5.2.1.1. Códecs

En la figura 1.18 se incluyen los valores de códecs de audio con la tasa de transmisión total, incluida las cabeceras.



Total Bandwidth Required

Cisco.com

Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with cRTP	Ethernet
G.711	64000	240	76267	66133	78933
G.711	64000	160	82400	67200	86400
G.726r32	32000	120	44267	34133	46933
G.726r32	32000	80	50400	35200	54400
G.726r24	24000	80	37800	26400	40800
G.726r24	24000	60	42400	27200	46400
G.726r16	16000	80	25200	17600	27200
G.726r16	16000	40	34400	19200	38400
G.728	16000	80	25200	17600	27200
G.728	16000	40	34400	19200	38400
G.729	8000	40	17200	9600	19200
G.729	8000	20	26400	11200	30400
G.723r63	6300	48	12338	7350	13650
G.723r63	6300	24	18375	8400	21000
G.723r53	5300	40	11395	6360	12720
G.723r53	5300	20	17490	7420	20140

Figura 1.18 Valores de códecs de audio[17]

[17] Cisco, Student Guide IP Telephony Express, 2005

1.5.2.2. DSP Digital Signal Processor (Procesador Digital de Señal)

Recurso que se utiliza principalmente para el transcoding (cambio de un códec a otro) entre dispositivos que manejan distintos códecs, generalmente se realiza el transcoding de G.711 a G.729. El recurso DSP tiene que ser registrado en el CCME para su utilización y es recomendable declarar solo los códecs que se utilizarán, debido a que el DSP soporta un número determinado de transcoding.

1.5.2.3. Dial Peers

Un dial peer es un direccionamiento a un punto final de una llamada, los dial peer establecen conexiones lógicas para completar una llamada end to end, la dirección es llamada destination pattern, para lo que se definen patrones de números como destino. CCME soporta dos tipos de dial peers, que son:

POTS. Conecta redes telefónicas tradicionales, tales como PSTN, PBX o teléfonos terminales. Provee una dirección para el dispositivo de borde, y apunta a un puerto específico de voz al que se conecta el dispositivo.

VOIP. Permite conexiones sobre una red de paquetes. Provee una dirección para el dispositivo de borde, asocia la dirección destino con el siguiente salto, que es la dirección del interfaz del siguiente router.

CAPÍTULO II

2. SITUACIÓN ACTUAL DE LA RED

En este capítulo se abarcan los aspectos más relevantes en cuanto a la topología de las capas física, enlace de datos y de red de PETROCOMERCIAL, de acuerdo al modelo ISO/OSI. También se explica los servicios de capa aplicación utilizados en la red de la empresa.

A través de toda esta información se presenta la situación actual en la que se encuentra la red de datos de PETROCOMERCIAL.

2.1. SERVICIOS DE CAPA APLICACIÓN

PETROCOMERCIAL utiliza diferentes aplicaciones y programas en su extensa red de comunicaciones para el manejo de la información (Datos, Voz, VoIP, video conferencia, video seguridad, aplicaciones, etc.). Debido a los diferentes grados de utilización de ancho de banda de las sucursales, PETROCOMERCIAL, hace uso de un segmentador de tráfico (Allot NetXplorer) con el que ofrece calidad de servicio a las aplicaciones, a los procesos internos y al acceso a Internet, de cada sucursal, permitiendo optimizar la comunicación tanto interna como externa.

Para el análisis de la situación actual de PETROCOMERCIAL se toma en cuenta la monitorización de la red, en un espacio determinado de tiempo, utilizando la herramienta NetXplorer. Además se presentará un estudio de los equipos activos en cada uno de los puntos tomados en cuenta para el presente Proyecto de Titulación

(Oyambaro, Corazón, Beaterio, Aeropuerto, Faisanes, Gasolinera, Sto. Domingo, Quito).

2.1.1. NÚMERO DE USUARIOS POR NODO

La recopilación de información del número de usuarios por nodo nos permitirá tener una visión muy cercana del tamaño de la red de comunicaciones manejada por PETROCOMERCIAL, además de proporcionarnos una noción aproximada del consumo de ancho de banda en cada nodo, que depende del número de máquinas activas y las aplicaciones que utilizan.

Para el estudio del número de estaciones por nodo utilizamos el programa Look@LAN que se explica a continuación.

2.1.1.1. Look@LAN[18]

Look@LAN es un programa que permite escanear la red, monitorizándola en un determinado rango de direcciones IP, especificado por el usuario. Con este software obtenemos información con datos útiles como nombre del host, sistema operativo, los servicios activos, NetBiosuser, NetBiosname, traceroute, tiempo de respuesta, SNMP, etc.

Las principales características de Look@LAN son:

- Monitoreo y recopilación de la información de la red.
- Notificaciones de los cambios ocurridos en cualquier nodo.
- Funcionamiento en tiempo real.
- Detección automática de las opciones de configuración de la red.
- Visualización de estadísticas y gráficas.
- Exportación de la información a diferentes formatos: HTML, Excel, Word.

[18] www.lookatlan.com

Para escanear una red debemos crear un nuevo perfil (como lo muestra la figura 2.1), luego escogemos el rango de direcciones IP a ser escaneadas (Figura 2.2).

Figura 2.1 Pantalla inicio de Look@LAN

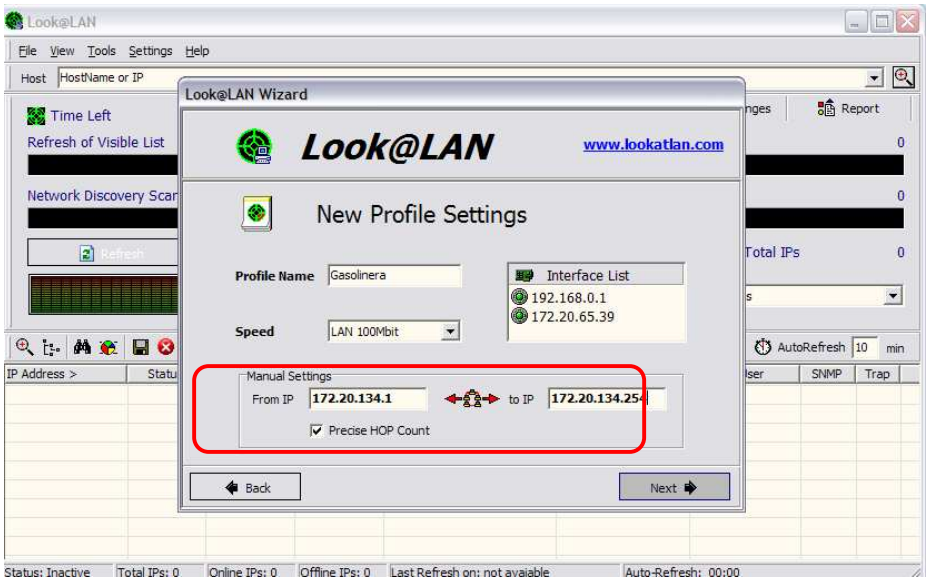


Figura 2.2 Configuración del rango de las direcciones IP

Una vez insertado el rango de direcciones IP el programa nos muestra las estaciones activas en tiempo real (Figura 2.3) proporcionándonos información de:

- Número de saltos o distancia hacia la máquina
- Sistema operativo
- Nombre de la máquina
- Servicio SNMP

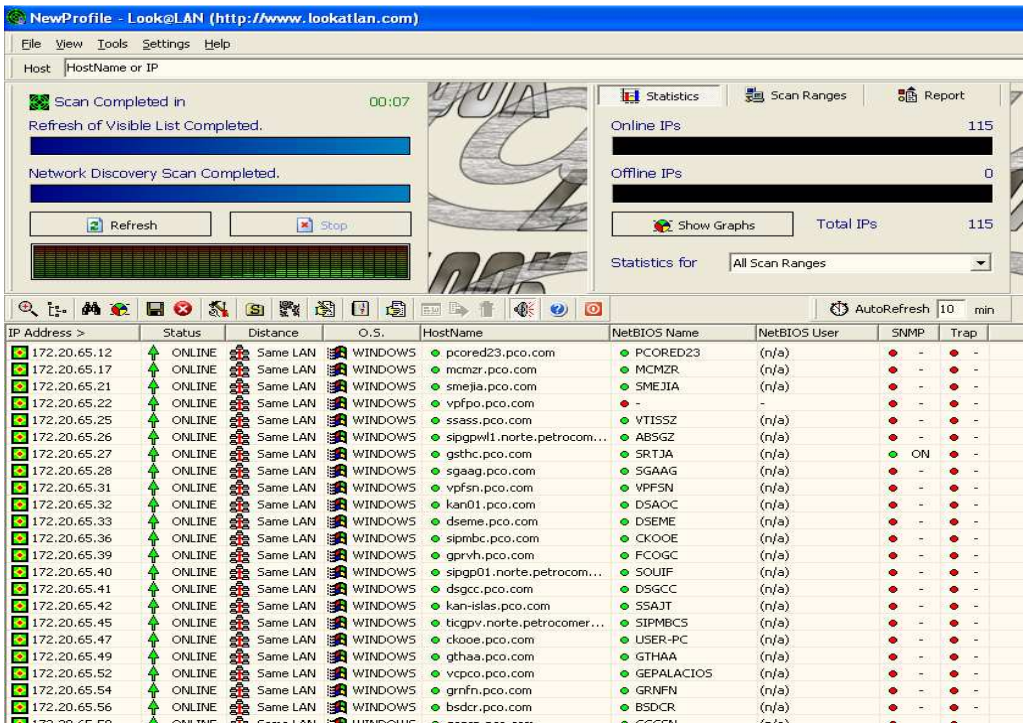


Figura 2.3 Escaneo de las máquinas activas en un rango de direcciones IP

Especificando el rango de direcciones IP de los nodos, podemos determinar el número de estaciones activas. Realizando este proceso con cada subred de las sucursales, se consiguió un número aproximado de los equipos conectados a la red.

El número de estaciones es considerado como una aproximación, debido a que las máquinas deben estar encendidas para ser registradas por el programa Look@LAN, por lo que puede variar el número de estaciones de un día a otro, siendo estas variaciones no considerables.

El número de estaciones promedio se encuentra registrado en la tabla 2.1.

Ubicación del Nodo	Subred	Número de equipos activos en promedio
AEROPUERTO	172.20.75.0/24	3
BEATERIO	172.20.129.0/25	53
CORAZÓN	172.20.77.0/24	3
GASOLINERA	172.20.134.0/24	21
FAISANES	172.20.141.0/24	5
OYAMBARO	172.20.76.0/27	6
QUITO	172.20.64.0/21	296
STO. DOMINGO	172.20.161.0/27	29
TOTAL		416

Tabla 2.1 Número de estaciones promedio por Nodo

2.1.2. ÍNDICE DE CRECIMIENTO DE LA EMPRESA

El estudio del índice de crecimiento de la empresa, tiene como objetivo determinar a un futuro el incremento del personal dentro de Petrocomercial. Este dato estadístico nos servirá más adelante, en el proyecto, para realizar diversos cálculos relacionados con el consumo de anchos de banda, uso de aplicaciones y dimensionamiento de equipos.

La información del Número de empleados de Petrocomercial durante los últimos años, presentada en la tabla 2.2, fue proporcionada por el área de Datos, a través del sistema de Recursos Humanos de Petrocomercial.

Año	Número de empleados ingresados / Año	Empleados Totales	Índice de Crecimiento
2004	49	2047	-
2005	27	2074	1,32%
2006	52	2126	2,51%
2007	35	2161	1,65%
2008	47	2208	2,17%
2009	41	2249	1,86%
2010	60	2309	2,67%

Tabla 2.2 Número de empleados de Petrocomercial durante los últimos años

Durante los últimos 5 años se puede observar un crecimiento constante dentro de la empresa, de acuerdo a la tabla 2.2 se puede promediar un crecimiento de 44.4 empleados por año. Con este dato podemos calcular el índice de crecimiento anual de la empresa:

$$c = \frac{(44.4)}{2309} * 100 = 1.92\%$$

Sin embargo para efectos del estudio del proyecto se considerará un periodo de cinco años, al tratarse de un proyecto tecnológico de mediano plazo, se considera este lapso adecuado como tiempo de vida del proyecto. El cálculo del índice de crecimiento para este período se realiza a continuación:

$$c = \frac{(235)}{2309} * 100 = 10.17\%$$

Para cálculos posteriores se utilizará un porcentaje de crecimiento dentro de 5 años del 10%.

2.1.3. SERVIDORES Y APLICACIONES

Dentro de la red de PETROCOMERCIAL, se cuenta con diversas aplicaciones que son manejadas por distintos servidores, las cuales permiten realizar las tareas diarias que requiere la empresa. Se cuenta con alrededor 63 servidores, de los cuales los principales se detallan en la tabla 2.3, indicando el nombre del servidor, aplicaciones instaladas y función que desempeña.

NOMBRE DEL SERVIDOR	APLICACIONES INSTALADAS	FUNCIÓN QUE REALIZA
PCORED01	IIS DIRECTORIO ACTIVO	Servidor de dominio principal
PCORED03V1 (PCOSAMETIME)	LOTUS DOMINO SERVER	Lotus SameTime (Domino - SameTime) Correo, chat.
PCORED03v2	BUSINESS OBJECT X1 RELEASE 2 IBM HTTP SERVER	Business Object 2.5 y DB2 Warehouse

	IBM WEB SPHERE	
PCORED04V1	LOTUS DOMINO SERVER	Correo
PCORED04V3		Anexo transaccional; SQL Server 2005; Eval. Ofertas
PCORED04V4	DOCUMENTAL LOTUS DOMINO	Aplicaciones Lotus Documentales
PCOPORTAL	DIRECTORIO ACTIVO NORTE IBM WEB SPHERE	Nuevo Portal
PCORED06	SERVIDOR DE IMPRESIÓN	Servidor de impresión
PCORED12	DIGITALIZACION	Repositorio software
PCORED13	IBM WEB SPHERE IBM RATIONAL IBM HTTP SERVER	WAS de desarrollo
PCORED18	Workflow	Aplicación PERMISOS; Aplicaciones Workflow
PCORED17	Warehouse	Base de datos del Data Warehouse
PCORED14	AQUA DATASTUDIO IBM WEB SPHERE PREMIUM SOFT	Portal PCO
PCORED20V1	OMNIVISTA	Omnivista
PCORED20V3	WHAT`S UP	WhatsUp
PCORED20V4	CONSOLA DE ADMINISTRACION VMWARE ESX SERVER	Consola de Administración Vmware ESX Server
PCORED20V5	CONSOLA DE ADMINISTRACION ARM	Consola de Administración ARM
PCORED22	VMWARE SERVER 1.9 SYMANTEC END PROTECTION MANAGER	Symantec End Protection Manager
PCORED23V1 **PCO-DC01**	DIRECTORIO ACTIVO	Controlador de Dominio Root
PCORED23V2 **PCODN-DC01**	DIRECTORIO ACTIVO	Controlador de Dominio Hijo
PCOSAMETIMESTD	LOTUS DOMINO SERVER	Lotus SameTime
PCOTSM	SERVER RAID MANAGER TIVOLI STORAGE MANAGER	Servidor de respaldos
PCOALLOT	NetXplorer	Servidor del Allot
SEG FIS 1		Servidor de Video Seguridad Almacenamiento

Tabla 2.3 Tabla de Servidores Principales de PETROCOMERCIAL

2.1.3.1. Aplicaciones y Servicios

A continuación se describen las principales Aplicaciones y Servicios utilizados en la red de PETROCOMERCIAL.

2.1.3.1.1. Microsoft Active Directory

Active Directory permite la implementación de seguridad en un entorno de computadoras distribuidas. El directorio activo utiliza distintos protocolos, entre ellos LDAP (Protocolo de Acceso al Directorio Ligero), el cual es utilizado en PETROCOMERCIAL. LDAP permite establecer una jerarquía, relacionando elementos de una red, como usuarios, individuales y grupales, conceder permisos, asignar recursos y establecer políticas de acceso.

Internamente *Microsoft Active Directory* se administra bajo dos dominios:

- PCO.COM
- PETROCOMERCIAL.COM

2.1.3.1.2. DHCP (Dynamic Host Configuration Protocol)

DHCP es un protocolo que permite asignar direcciones IP dinámicamente a equipos que se conecten a una determinada red. Su funcionamiento se basa en un servidor, el cual mantiene una lista de direcciones de red que va asignando a los dispositivos mediante peticiones de éstos. En la red de la empresa el DHCP asigna dinámicamente direcciones IP a los host de la red, los únicos equipos que tienen direcciones IP fijas son servidores, impresoras y equipos de interconectividad.

2.1.3.1.3. Correo Electrónico

El servicio de Correo Electrónico es proporcionado a través del programa cliente/servidor Lotus Notes y permite el envío tanto de mensajes instantáneos como correos electrónicos. Utiliza el protocolo SMTP para envío de correo electrónico y POP3 para descarga de mensajes.

2.1.3.1.4. Servicio Web[19]

Los servicios web son los aplicativos que se los manejan directamente desde el portal de EPPETROECUADOR (www.eppetroecuador.ec), ingresando a la pestaña de comercialización.

Algunas de estas aplicaciones son:
Aplicativos para uso de Funcionarios:

- *Control de Permisos:* Sistema automatizado de control y solicitud de permisos vía web. Con estos procesos se elimina el uso de las formas impresas y se redefine la cultura organizacional de aplicativos que benefician al personal.
- *Consultas a Recursos Humanos:* Sistema que permite revisar información personal y laboral que se encuentra ingresada en Recursos Humanos como información general, vacaciones, pagos, control de asistencia y trámites.
- *Acceso directo a EPR*: Aplicativo para el acceso al Observatorio digital para la planeación y gestión de desempeño de la empresa. Es un proceso dirigido para desarrollar el modelo de gestión de PETROCOMERCIAL, a través de talleres ejecutados en cada unidad operativa.
- *Aplicativos Workflow:* Sistema ágil y eficiente para el control de los procesos de contratación, compras locales y seguimiento de contratos.
- *Utilitarios Internos:* A través de este elemento, se verifica la funcionalidad de los procesos de facturación y recaudación, expuestos hacia la banca privada.
- *Mantenimiento Vehicular:* Sistema para el control del mantenimiento, consumo y permisos vehiculares. Permite al custodio registrar el consumo y mantenimiento dado al vehículo asignado, así como alertar del próximo mantenimiento preventivo.
- *Email:* Servicio que permite el ingreso a la cuenta de correo electrónico de los funcionarios a través de la web, sin la necesidad de tener el programa Lotus Notes instalado en la máquina.

[19] Tomado de la página web de Petroecuador (www.eppetroecuador.ec)

Aplicativos Empresariales de Comercialización

- *Sistema de Abastecimiento y Comercialización de Combustibles SACCO:* Sistema encargado de todo el proceso de negocio de la Abastecedora de PETROCOMERCIAL con las comercializadoras del mercado nacional, la Banca Privada y entes de control.
- *Sistema de Atención al Cliente:* A través de este sistema, PETROCOMERCIAL realiza actividades de mejoramiento del proceso de mercadeo. Monitorea la actividad de las estaciones de servicio, optimizando el control sobre los procesos realizados.
- *Sistema de Programación y Redistribución:* Sistema que mensualmente realiza la programación de despacho de combustibles y redistribución por parte de las comercializadoras.
- *Activos Fijos:* Encargado de todo el proceso de negocio de la Abastecedora de Petrocomercial con las Comercializadoras del mercado nacional, la Banca privada y entes de Control.
- *Gestión de Incautaciones:* Permite registrar a nivel nacional el detalle de los volúmenes, calidad y precio de los combustibles derivados de hidrocarburos, GLP y bienes, así como los antecedentes legales y destino final de estos productos y bienes incautados.
- *UCCV:* Sistema de monitoreo de metas operativas
- *Guía a terceros:* El Sistema de Guías de Remisión a Terceros es una herramienta diseñada para apoyar a que los Sujetos de control que participan en la cadena de comercialización y distribución de combustibles efectúen sus transacciones con otros sujetos de control.
- *Utilitarios Internos:* A través de este componente, se logra una verificación de la funcionalidad de los procesos de facturación, recaudación, y otros, expuestos hacia la banca privada, como procesos críticos para la venta de combustibles.

2.1.3.1.5. Internet

PETROCOMERCIAL cuenta con dos enlaces a Internet, el enlace principal tiene una velocidad de transmisión de 6 Mbps a través de CNT, el enlace alterno tiene una velocidad de transmisión de 6.5 Mbps a través de Telconet.

El equipo que permite la salida hacia Internet se encuentra en Quito, por lo que el tráfico de los demás nodos que requieran del servicio, pasarán por el nodo de Quito.

El servicio de Internet se brinda a través de un servidor Proxy que tramita las peticiones y direcciona el tráfico a través del firewall de la empresa. Cabe destacar que mediante el firewall se encuentran bloqueados sitios que no tengan relación en las actividades que realiza la empresa, así como los que incluyen descargas P2P o mensajería instantánea hacia Internet.

2.1.3.1.6. Real VNC (Virtual Networking Computing)

RealVNC es un software que permite remotamente ver e interactuar con el escritorio del sistema operativo de una computadora, que se encuentre distante, a través de la red.

VNC es utilizado por el área de Soporte a Usuario e Infraestructura para proporcionar ayuda remota a equipos que presenten problemas.

2.1.3.1.7. Telefonía IP

El sistema de telefonía en la Matriz se lo maneja a través de la central Telefónica Mitel, utilizando el protocolo propietario MINET; la central también permite manejar el protocolo estándar SIP, pero bajo un esquema de licenciamiento adicional. Por otra parte la telefonía analógica se lo maneja a través de ASUs, (Analogic Service Units).

En los nodos Beaterio y Santo Domingo se maneja el mismo sistema que en la Matriz. En los nodos Gasolinera y Oyambaro se maneja una central hibrida pero no se manejan extensiones IP.

En los nodos Corazón, Faisanes y Aeropuerto no se manejan centrales telefónicas, todas las sucursales se comunican con la matriz a través de líneas troncales.

En la tabla de 2.4 se detalla la situación actual de la red telefónica de PETROCOMERCIAL:

Descripción	Matriz	Beaterio	Sto. Domingo	Oyambaro	Gasolinera	Aeropuerto	Corazón	Faisanes
Líneas CNT	28	22	12	1	2	1	0	0
Troncales Internas desde Matriz	-	8	8	4	2	2	2	2
E1 desde Matriz	-	1	0	0	0	0	0	0
Bases Celulares	0	0	0	0	0	0	0	0
Fax existentes	14	7	6	2	2	1	1	1
Extensiones IP	160	42	30	0	0	0	0	0
Extensiones Analógicas	25	50	27	5	15	0	0	0
Contestadora Automática	Si	Si	Si	No	Si	No	No	No

Tabla 2.4 Telefonía PETROCOMERCIAL

La entrega de líneas troncales se lo realiza a través de E1 o fraccionales de los mismos, es decir se utilizan canales de 64 Kbps por canal de voz.

2.1.3.1.8. Video Conferencia

PETROCOMERCIAL con el propósito de disminuir costos y maximizar el uso del tiempo de sus funcionarios implementó el servicio de videoconferencia en varios nodos del país (Ambato, Pascuales, Riobamba, Shushufindi Sucursal, Esmeraldas Cabecera, Santo Domingo, Oyambaro, Osayacu, Beaterio, Guayaquil y Quito)

Este servicio permite una interactividad en tiempo real de los funcionarios, utilizando video y audio. En cada nodo que cuenta con el servicio de videoconferencia se encuentra instalados la solución POLYCOM que es un conjunto de equipos

conformado por una cámara, parlantes, micrófonos y un controlador, que permiten la conexión con uno o más equipos remotos, dependiendo del modelo.

2.1.3.1.9. Video Seguridad

Mediante el uso de cámaras de video seguridad PETROCOMERCIAL pretende brindar seguridad tanto a sus equipos físicos como a su personal humano, por lo que se realiza una constante monitorización de lugares críticos durante las 24 horas del día. Las cámaras de video seguridad utilizadas son de la marca Mobotix, las cuales se encuentran instaladas en los nodos Gasolinera, Beaterio y Quito. Permiten realizar un monitoreo online a través de exploradores web en tiempo real. Las imágenes capturadas son grabadas por sus respectivos servidores los cuales son manejados por el área de Seguridad Física.

2.1.3.1.10. Software Antivirus

Todas las computadoras de la empresa cuentan con el antivirus Symantec Endpoint, que periódicamente es actualizado a través de su servidor. El propósito del software es evitar el daño de las pc's causado por algún virus o malware.

2.1.4. CONSUMO DE ANCHO DE BANDA DE LOS NODOS

El análisis del ancho de banda utilizado por cada nodo nos permitirá conocer el estado en que se encuentra los enlaces de cada sitio remoto con la matriz (Quito), y determinar su consumo tanto en el tráfico hacia la red interna como hacia Internet.

El estudio estará dividido en tres partes: en primer lugar se presenta el ancho de banda que consume cada nodo hacia la red interna (aplicaciones, servidores) y hacia Internet, luego se mostrará los protocolos manejados por cada nodo en la red interna, especificando sus características, y por último se dará a conocer los protocolos de cada nodo utilizados en Internet.

Conociendo todos estos datos tendremos una visión más clara de la situación actual de la red de PETROCOMERCIAL, lo cual nos permitirá determinar los parámetros (ancho de banda) para el diseño e implementación planteados para el presente Proyecto de Titulación.

Para el estudio del ancho de banda consumido por los protocolos en cada nodo haremos uso de la Herramienta NetXplorer, que forma parte del segmentador de tráfico utilizado en PETROCOMERCIAL, a continuación se lo describe brevemente:

2.1.4.1. ALLOT NetXplorer[20]

El equipo, tanto de software como hardware, de ALLOT ayuda en la tarea de gestionar, monitorear y regular el tráfico de una red de comunicaciones. Su funcionamiento está basado en la metodología de inspección de paquetes a fondo (DPI)[21]. Gracias a esta técnica los paquetes son examinados a profundidad para determinar el tipo de información que contienen en la cabecera, permitiendo obtener un panorama desde la capa de transporte a la de aplicación, según el modelo OSI.

El elemento hardware en la solución de ALLOT lo conforma el llamado NetEnforcer, que es el encargado de aplicar las reglas y de obtener información de la red.

La parte software lo conforma NetXplorer, que permite una gestión centralizada de la red a ser monitoreada. Se encuentra conformada por una interfaz gráfica, por la cual se puede establecer las reglas de calidad de servicio y visualizar gráficamente estadísticas de varios parámetros de la red, tanto en tiempo real como en un espacio de tiempo.

[20] www.allot.com
[21] DPI es una forma de filtraje de paquetes en redes de computación que examina la sección de datos (y alternativamente también el encabezado) de paquetes, al pasar por un punto de inspección. (Tomado de www.allot.com)

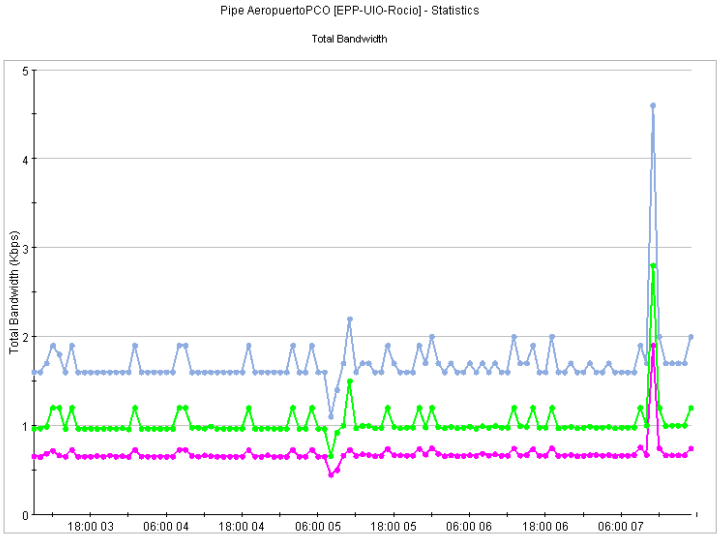
2.1.5. ANCHO DE BANDA UTILIZADO EN LA RED INTERNA E INTERNET

Utilizando la interfaz de usuario de NetXplorer conseguimos las gráficas posteriormente presentadas. El análisis de las gráficas son tomadas en un período de una semana, con una tasa de muestreo de 1 hora. En los gráficos se representa el consumo de AB máximo tanto hacia la red interna como hacia Internet y la capacidad en AB, de cada nodo.

En los gráficos de a continuación los colores representan lo siguiente:

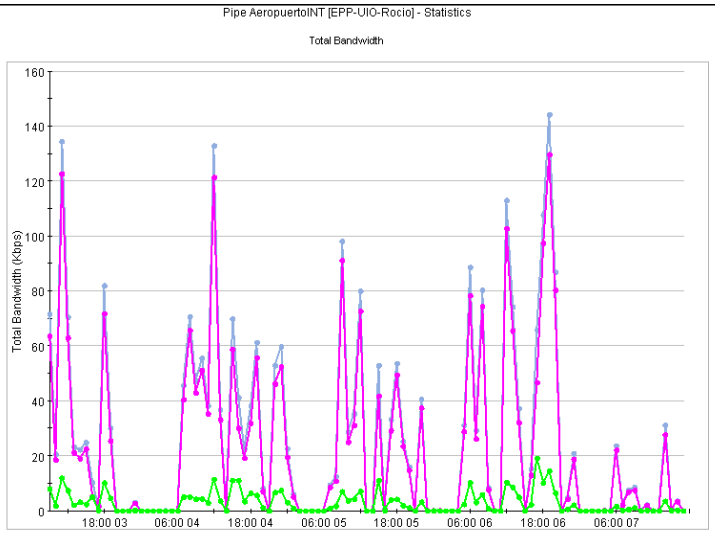
- Color Azul: Consumo de AB Máximo medido en Kbps
- Color Verde: Consumo de AB de Salida medido en Kbps
- Color Rosado: Consumo de AB de Entrada medido en Kbps

2.1.5.1. Aeropuerto



	Consumo de AB Máximo (Kbps)	Capacidad del Canal (AB en Kbps)
Red Interna total (color azul)	4.7	2048
Red Interna salida (color verde)	2.8	2048
Red Interna entrada (color rosado)	1.9	2048

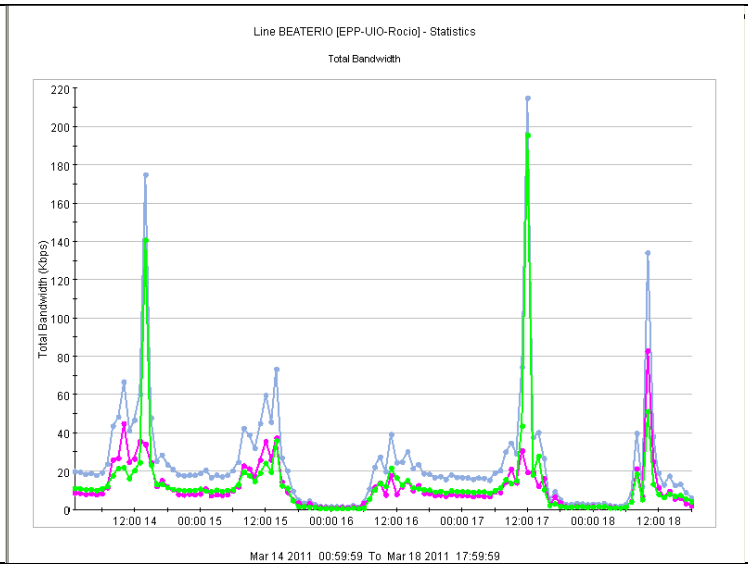
Figura 2.4 Consumo del AB Red interna del nodo Aeropuerto



	Consumo de AB Máximo (Kbps)	Capacidad del Canal (AB en Kbps)
Internet total (color azul)	142	2048
Internet salida (color verde)	20	2048
Internet entrada (color rosado)	130	2048

Figura 2.5 Consumo del AB Internet del nodo Aeropuerto

2.1.5.2. Beaterio



	Consumo de AB Máximo (Kbps)	Capacidad del Canal (AB en Kbps)
Red Interna Total (color azul)	210	2048
Red Interna salida (color verde)	205	2048
Red interna entrada (color rosado)	82	2048

Figura 2.6 Consumo del AB Red interna del nodo Beaterio

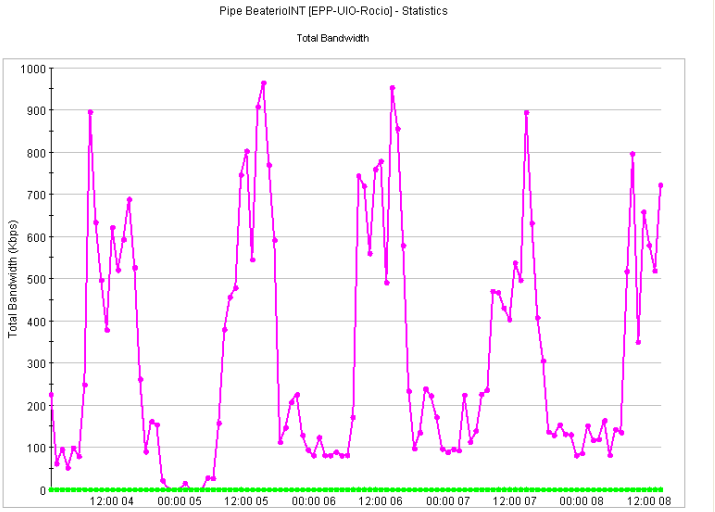
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet total (color azul)	970.03	2048
Internet salida (color verde)	970	2048
Internet entrada (color rosado)	0.03	2048

Figura 2.7 Consumo del AB de Internet del nodo Beaterio

2.1.5.3. Corazón

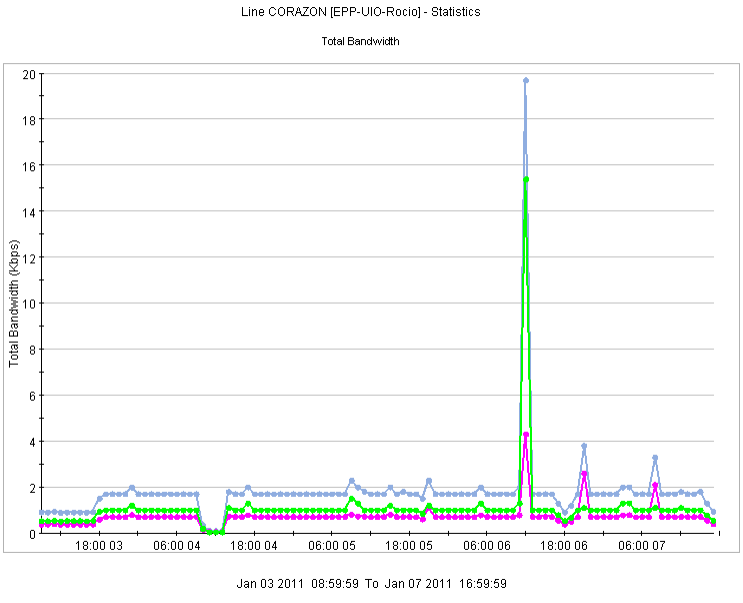
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Red Interna Total (color azul)	20	2048
Red Interna salida (color verde)	15.5	2048
Red interna entrada (color rosado)	4.5	2048

Figura 2.8 Consumo del AB Red interna del nodo Corazón

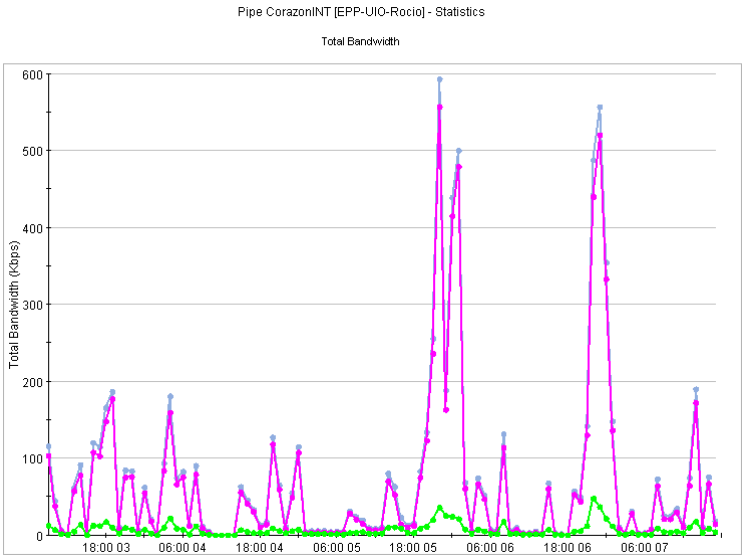
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet Total (color azul)	600	2048
Internet salida (color verde)	50	2048
Internet entrada (color rosado)	550	2048

Figura 2.9 Consumo del AB Internet del nodo Corazón

2.1.5.4. Gasolinera

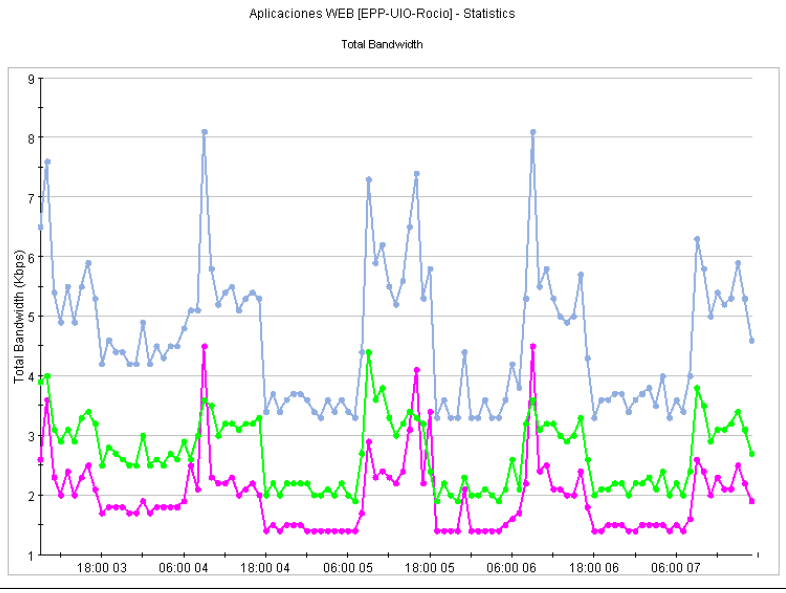
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Red Interna Total (color azul)	8.2	2048
Red Interna salida (color verde)	4.4	2048
Red interna entrada (color rosado)	4.5	2048

Figura 2.10 Consumo del AB Red interna del nodo Gasolinera

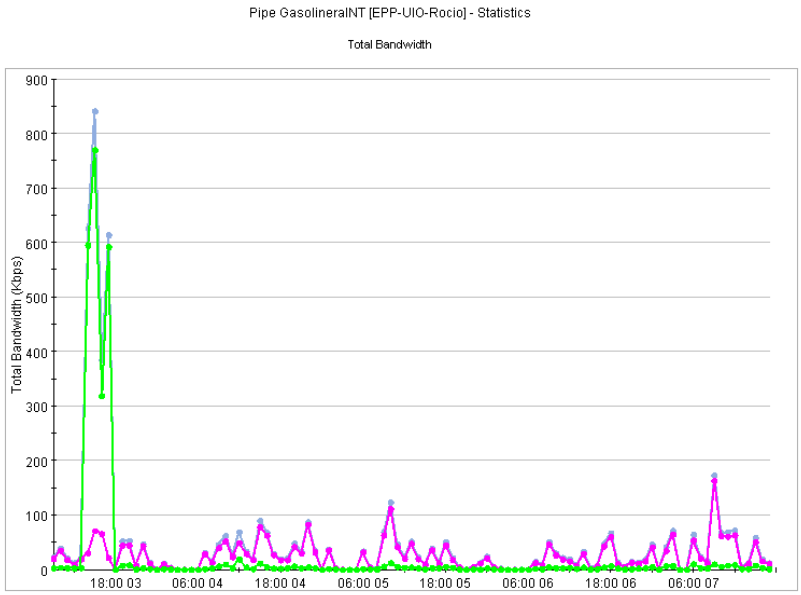
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet Total (color azul)	847	2048
Internet salida (color rosado)	160	2048
Internet entrada (color verde)	760	2048

Figura 2.11 Consumo del AB Internet del nodo Gasolinera

2.1.5.5. Faisanes

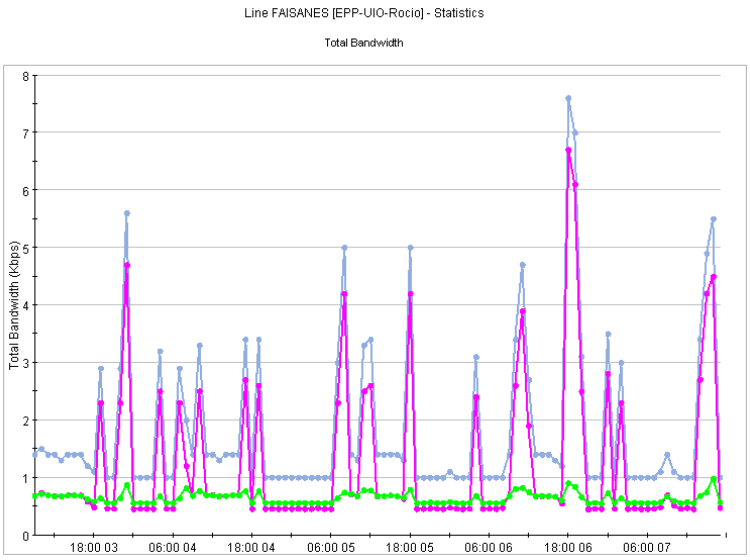
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Red Interna Total (color azul)	7,4	2048
Red Interna salida (color verde)	1	2048
Red interna entrada (color rosado)	6.8	2048

Figura 2.12 Consumo del AB Red interna del nodo Faisanes

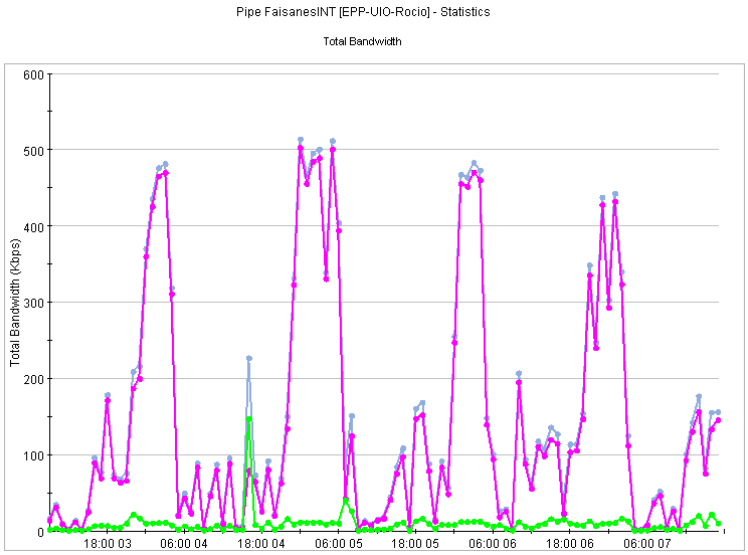
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet Total (color azul)	504	2048
Internet salida (color verde)	150	2048
Internet entrada (color rosado)	500	2048

Figura 2.13 Consumo del AB de Internet del nodo Faisanes

2.1.5.6. Oyambaro

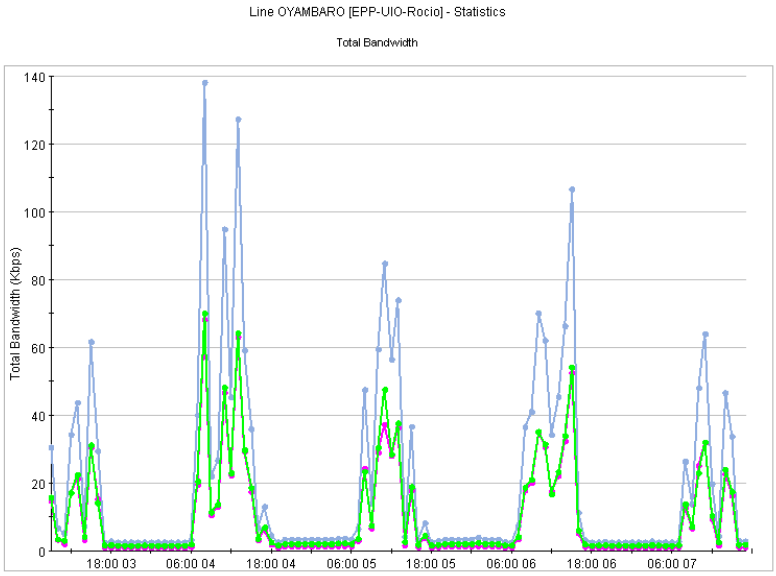
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Red Interna Total (Color Azul)	140	2048
Red Interna salida (color verde)	72	2048
Red interna entrada (color rosado)	68	2048

Figura 2.14 Consumo del AB hacia la Red interna del nodo Oyambaro

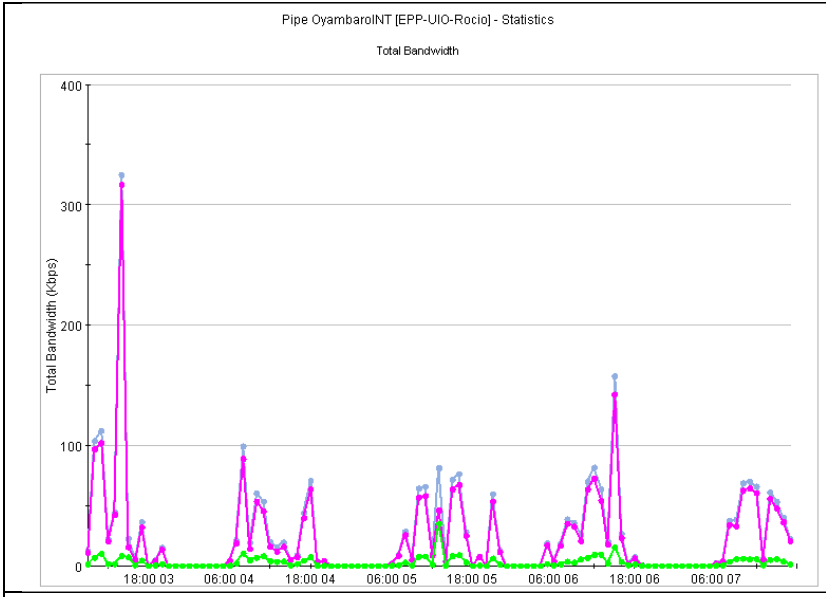
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet Total (color azul)	317	2048
Internet salida (color verde)	40	2048
Internet entrada (color rosado)	310	2048

Figura 2.15 Consumo del AB de Internet del nodo Oyambaro

2.1.5.7. Quito

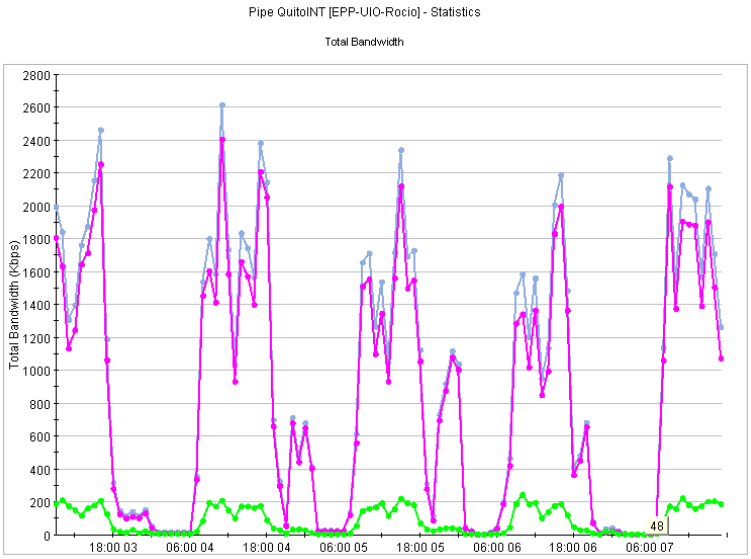
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet Total (color azul)	2614.3	6000
Internet salida (color verde)	240	6000
Internet entrada (color rosado)	2400	6000

Figura 2.16 Consumo del AB de Internet del nodo Quito

2.1.5.8. Sto. Domingo

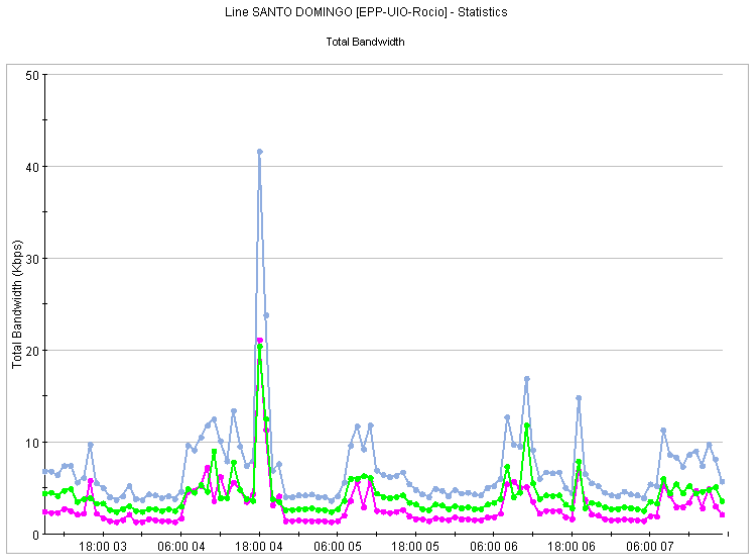
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Red Interna Total (Color Azul)	42	2048
Red Interna salida (color verde)	20	2048
Red interna entrada (color rosado)	22	2048

Figura 2.17 Consumo AB hacia Red Interna del nodo Sto. Domingo

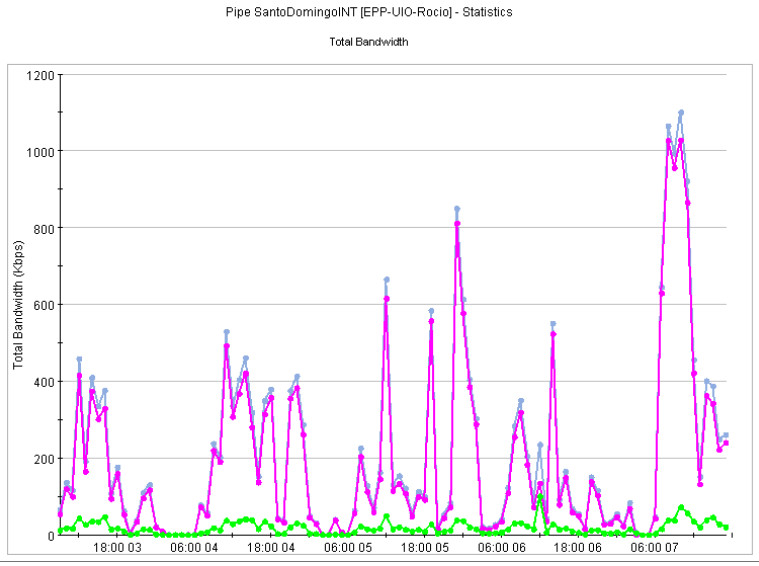
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Internet Total (color azul)	1100	2048
Internet salida (color verde)	150	2048
Internet entrada (color rosado)	1050	2048

Figura 2.18 Consumo AB hacia Internet del nodo Sto. Domingo

2.1.6. PROTOCOLOS DE MAYOR USO

En este apartado se presenta los protocolos más utilizados por los nodos, dentro de la red interna de PETROCOMERCIAL y hacia Internet.

En primer lugar se explica en forma breve el significado de los canales virtuales utilizados por NetXplorer, identificando los protocolos más activos y exponiendo de manera resumida los protocolos más representativos.

2.1.6.1. Creación de Canales Virtuales en Netxplorer

Los canales virtuales se utilizan para identificar las aplicaciones o servicios que demanda la red de la empresa.

A cada canal virtual se le asocia un catálogo de servicio (ya definido por la solución ALLOT). Las entradas de catálogo de servicio son usadas para clasificar el tráfico por aplicación o por protocolo. NetEnforcer usa la capacidad DPI (Explicado en el subcapítulo *2.1.3.1 ALLOT NetXplorer*) para identificar el tipo de protocolo o aplicación que circula por la red.

Dentro de los canales virtuales se pueden destacar aplicaciones o servicios como:

Aplicaciones y Servicios Internos.

- *Video Conferencia*: Asociado al tráfico IP generado por la subred de videoconferencia.
- *Video Seguridad*: Asociado al tráfico IP generado por la subred de videoseguridad.
- *Telefonía IP*: Está asociado al catálogo de servicios correspondientes a VOIP (contiene protocolos de telefonía IP como SIP, H 323, etc.).
- *Mail*: Está asociado al catálogo de servicios correspondientes a MAIL (contiene protocolos de correo electrónico como: POP3, SMTP, LOTUS NOTES, MS EXCHANGE, IMAP, etc.).

- *Administrativas*: Incluye al catálogo de servicios correspondientes a NETWORK OPERATION (contiene protocolos asociados a trabajos dentro de la red como: DNS, ARP, DHCP, ICMP, SNMP, RIP, RMON, etc.).
- *Aplicaciones Web*: Está asociado al catálogo de servicios correspondientes a WEB APPLICATIONS (contiene protocolos utilizados en la web como: HTTP, HTTPS, HTTP_PROXY, etc.).
- *Otros:* Es todo el tráfico IP que existe en la red.
- *Fallback*: Es todo el tráfico que no ha sido clasificado y asociado en los anteriores canales virtuales.

Aplicaciones y Servicios de Internet.

- *Descargas:* Está asociado al catálogo de servicios correspondientes a FILE TRANSFER (contiene protocolos utilizados en transferencia de archivos como: FTP, TFTP, HTTP_File_Transfer, etc.).
- *Descarga P2P:* Está asociado al catálogo de servicios correspondientes a P2P APPLICATIONS (contiene protocolos utilizados en transferencia peer-to-peer como: Ares, BitTorrent, eDonkey, Gnutella, iMesh, etc.).
- *HTTP:* Está asociado al catálogo de servicios correspondientes a WEB APPLICATIONS (contiene protocolos utilizados en la web como: HTTP, HTTPS, HTTP_PROXY, etc.).
- *Juegos:* Está asociado al catálogo de servicios correspondientes a GAMES (contiene protocolos utilizados en juegos como: CounterStrike, GTA, GuitarHero, PlayOnline, etc.).
- *Mail:* Está asociado al catálogo MAIL (contiene protocolos de correo electrónico como: POP3, SMTP, LOTUS NOTES, MS EXCHANGE, IMAP, etc.).
- *Messenger:* Está asociado al catálogo de servicios correspondientes a INSTANT MESSAGING (contiene protocolos utilizados en mensajería instantánea como: AOL, IRC, MSN, YAHOO, WEBEX, QQ CHAT, etc.).

- *Skype:* Está asociado al catálogo de servicios correspondientes a SKYPE (contiene protocolos propietarios utilizados por Skype).
- *SSL:* Está asociado al catálogo de servicios correspondientes a SECURITY (contiene protocolos de seguridad como: SSL, IPSEC, SUGP, GRE, etc.).
- *Streaming:* Está asociado al catálogo de servicios correspondientes a STREAMING APPLICATIONS (contiene protocolos de streaming como: IPTV, ITunes, MS Player, HTTP_Streaming, iPlayer etc.).

2.1.6.2. Protocolos más Utilizados en la Red Interna

De acuerdo a la figura 2.19 podemos especificar los protocolos más usados dentro de la red Interna de PETROCOMERCIAL.

A continuación se explica brevemente su funcionalidad y la relación que tiene con la red interna de la empresa.

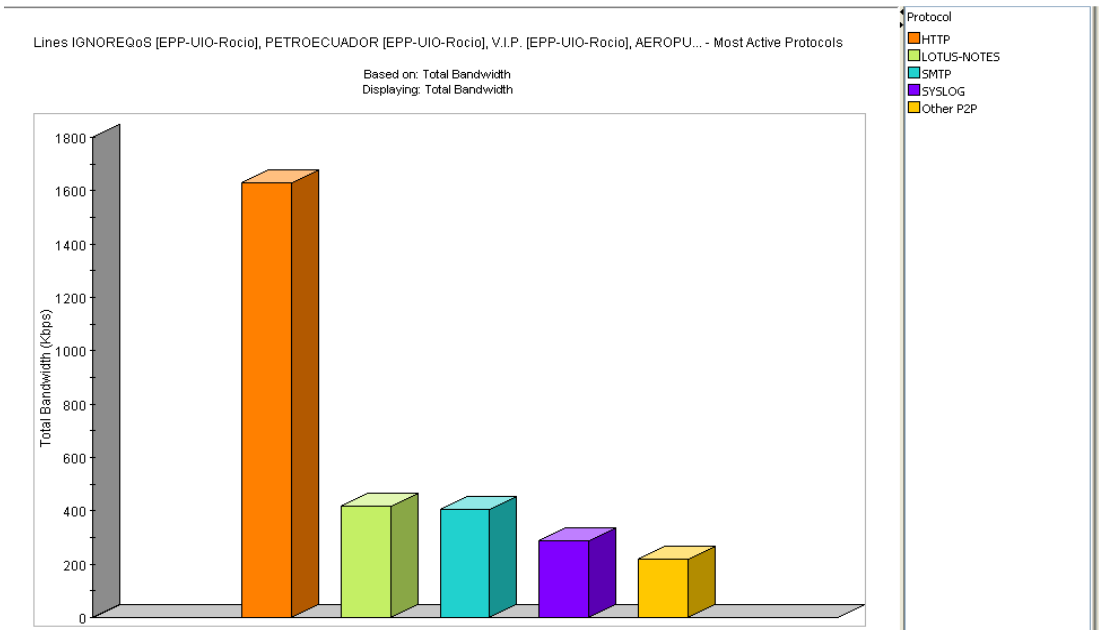


Figura 2.19 Protocolos de mayor uso en la Red Interna

2.1.6.2.1. HTTP

Dentro de la red Interna de la empresa se hace referencia al protocolo HTTP como el protocolo usado en cada transacción de la Web (WWW). Sin embargo no se relaciona con el envío de peticiones hacia o desde Internet.

Las peticiones HTTP más comunes se las hace hacia los servidores pcored, pcored14 y pcored22 entre los principales. El servidor pcored14 es el servidor web, allí se almacena la página web de la empresa. En la página Web se puede acceder a diferentes aplicaciones de uso común de los funcionarios de la institución.

2.1.6.2.2. Lotus-Notes

Lotus Notes se lo asocia dentro del software del segmentador de tráfico con los protocolos de transferencia de correos electrónicos, haciendo referencia al programa que se utiliza en la empresa como correo electrónico interno (Lotus Notes).

2.1.6.2.3. SMTP

Simple Mail Transfer Protocol (SMTP). Este protocolo es utilizado para el envío de mensajes de correo electrónico entre computadoras u otros dispositivos.

Este protocolo se debe diferenciar del protocolo Lotus-Notes, ya que el segmentador de tráfico (ALLOT) lo reconocerá como SMTP cuando sean utilizados por las demás aplicaciones de correo electrónico (Hotmail, Yahoo, Google, etc.). Todo el tráfico de correo electrónico generado desde Internet hacia el servidor LOTUS, el segmentador lo trata como tráfico SMTP.

2.1.6.2.4. Syslog

Este protocolo de red se lo utiliza para enviar mensajes registrando algún evento, sobretodo mensajes de seguridad del sistema. Entre los mensajes más utilizados encontramos los accesos a los sistemas, anomalías en el funcionamiento del equipo, información de actividad del equipo, errores varios de hardware y software. Sin embargo el registro más frecuente que se da en la red, utilizando syslog, es el de

recopilar información sobre el acceso que se hace a un servidor dentro de la red. Estos mensajes vienen junto a la fecha y hora del envío.

2.1.6.2.5. P2P

P2P se refiere al intercambio peer-to-peer, el cual se basa en una interconexión de igual a igual, entre computadoras, que sirve para intercambiar información.

Dentro de la red de PETROCOMERCIAL, este protocolo se utiliza para el intercambio de información y archivos entre computadoras de la red, esta práctica es muy común dentro de la red por lo que es uno de los protocolos más utilizados internamente. El trafico P2P hacia Internet está bloqueado.

2.1.6.3. Protocolos más Utilizados en Internet

En la figura 2.20 se indica los protocolos más utilizados en Internet por los nodos de PETROCOMERCIAL. A continuación se da una explicación de cada uno de ellos:

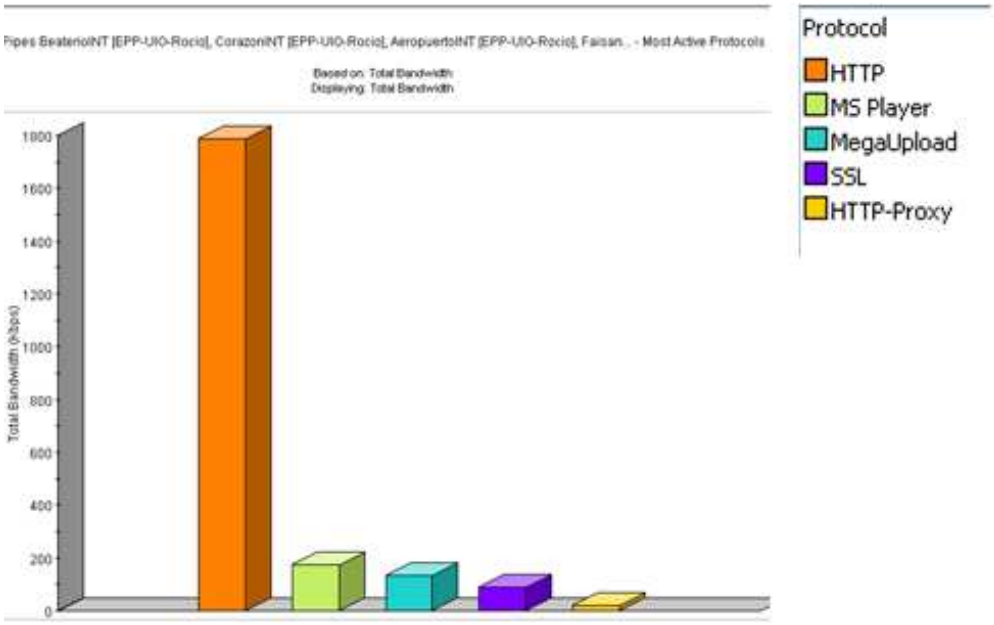


Figura 2.20 Protocolos de mayor uso en Internet

2.1.6.3.1. HTTP

La función de HTTP es la de permitir un intercambio de archivos entre un cliente (navegador) y un servidor web. Este protocolo es el más utilizado en Internet y por ende cuando una máquina o servidor de PETROCOMERCIAL intente conectarse a Internet lo más probable es que se haga uso de HTTP, por lo que es el protocolo de mayor uso de los nodos hacia Internet.

2.1.6.3.2. MS-Player

MS-Player se define dentro del catálogo del segmentador de tráfico, como un protocolo de Aplicaciones de Transmisión (*Streaming Applications*). Este protocolo consiste en la transmisión de audio y video por Internet. Se trata de escuchar o ver contenido multimedia sin tener que descargarlo previamente. Varias páginas web utilizan este tipo de aplicaciones dentro de su diseño.

2.1.6.3.3. Megaupload

El segmentador reconoce como protocolos a megaupload, este sitio de Internet brinda el servicio de carga y descarga de archivos. Esto protocolos sirven para la descarga directa, de cualquier tipo de archivo o información que se encuentre alojada en Internet, dentro de los servidores de las respectivas empresas.

2.1.6.3.4. SSL

SSL significa Protocolo de Capa de Conexión Segura, este protocolo implementa seguridad a través de la redes, permite encriptar las comunicaciones, brindando un entorno seguro para el intercambio de información, especialmente en Internet.

2.1.6.3.5. HTTP-Proxy

Define al puerto 8080 utilizado por el servidor proxy, todas las máquinas acceden a Internet a través del servidor proxy.

2.2. CAPA DE RED

La red WAN de PETROCOMERCIAL está conformada por 54 nodos o equipos de enrutamiento que brindan conectividad a nivel nacional a sus distintas sucursales (Ver anexo 1).

Estos nodos se encuentran distribuidos a lo largo de todo el territorio Ecuatoriano, divididos principalmente en dos regionales. La Regional Sur teniendo como matriz la ciudad de Guayaquil, y la Regional Norte teniendo como Matriz la ciudad de Quito, que por el alcance de este proyecto, es esta última regional en la que se centrará el análisis y diseño para el presente Proyecto de Titulación, específicamente en los ocho nodos (Aeropuerto, Beaterio, Corazón, Faisanes, Gasolinera, Oyambaro, Matriz, Sto. Domingo).

2.2.1. TECNOLOGÍA DE CAPA DE RED

En la capa 3 del modelo ISO/OSI, PETROCOMERCIAL utiliza IP en su versión 4 para el transporte de información, utilizando direccionamiento VLSM para las distintas subredes que se utilizan en la empresa, subneteando la red privada clase B 172.20.0.0 para sus distintas aplicaciones, exceptuando videoseguridad donde se subnetea la red 172.31.0.0 y la aplicación de control de válvulas de corte donde se utiliza la red 172.25.0.0.

Para la red de Telefonía se utiliza la red 172.10.0.0, lo cual es un error debido a que esta red se encuentra dentro del rango de direcciones públicas.

No utiliza protocolos de enrutamiento para la creación de tablas de rutas, se lo hace de manera estática, lo que involucra un proceso de creación manual de la ruta hacia cualquier subred nueva. Utiliza un equipo segmentador de tráfico en el punto central de la topología.

2.2.2. TOPOLOGÍA DE CAPA DE RED

Como se puede observar en el anexo 1 la red WAN de PETROCOMERCIAL forma en la capa red, dos estrellas en su topología lógica, la primera estrella se forma en la regional SUR, teniendo como centro de la estrella Cerro Azul ubicado en GUAYAS, y la segunda estrella se forma en la regional NORTE teniendo como centro de la estrella QUITO. Las dos estrellas se encuentran conectadas para una conectividad total.

La topología lógica obedece primero a la distribución organizacional de la empresa debido a que los nodos centrales son las matrices de las dos regionales en las que se encuentra divida la empresa. Al tener como centro de las dos estrellas las matrices de las Regionales se busca tener una administración centralizada de la red. Como se explicará en el direccionamiento, todo el trafico WAN tiene que pasar necesariamente por las puntos centrales, de esta manera todo el enrutamiento es manejado en los mismos.

Por el alcance de este Proyecto de Titulación se detalla la red WAN de la regional Norte.

2.2.3. DIRECCIONAMIENTO

El direccionamiento de la red de PETROCOMERCIAL se basa en la utilización de VLSM para subnetear las redes 172.20.0.0, 172.10.0.0, 172.31.0.0 y 172.25.0.0

2.2.3.1. Direccionamiento WAN

La subred que se utiliza para los enlaces WAN es la 172.20.36.X subneteada con máscara de 30 bits, para optimizar el uso de direcciones. En la tabla 2.5 se detalla el direccionamiento de la red WAN de PETROCOMERCIAL para los enlaces punto a punto, desde la matriz a las distintas sucursales.

DIRECCIONAMIENTO RED WAN				
Enlace	**Red**	**Máscara**	**Matriz**	**Sucursal**
Matriz-Sto.Domingo	172.20.36.8	255.255.255.252	172.20.36.9	172.20.36.10
Matriz-Beaterio	172.20.36.12	255.255.255.252	172.20.36.13	172.20.36.14
Matriz-Gasolinera	172.20.36.16	255.255.255.252	172.20.36.17	172.20.36.18
Matriz-Aeropuerto	172.20.36.20	255.255.255.252	172.20.36.21	172.20.36.22
Matriz-Corazón	172.20.36.36	255.255.255.252	172.20.36.37	172.20.36.38
Matriz-Oyambaro	172.20.36.168	255.255.255.252	172.20.36.169	172.20.36.170
Matriz-Faisanes	172.20.36.4	255.255.255.252	172.20.36.5	172.20.36.6

Tabla 2.5 Direccionamiento RED WAN

Toda la red WAN de PETROCOMERCIAL es manejada por routers marca VANGUARD cuyas características se detallan más adelante.

2.2.3.2. Direccionamiento Sucursales.

2.2.3.2.1. Matriz

En la tabla 2.6 se indican las distintas subredes que se manejan en la Matriz, la división en subredes se realiza en base a las aplicaciones.

MATRIZ			
Red	**No Vlan**	**Red IP**	**Máscara**
Datos	1	172.20.64.0	255.255.248.0
VideoSeguridad	7	172.31.64.0	255.255.255.128
Inalámbrica	8	172.20.72.0	255.255.255.192
Impresoras	9	172.20.63.0	255.255.255.0
Telefonía	1001	172.10.64.0	255.255.254.0
VideoConferencia	11	172.20.16.0	255.255.255.240

Tabla 2.6 Subredes Matriz

En la Matriz se cuenta con dos switches de core CISCO modelo 4507 que se encuentran entre la red LAN y los equipos, router VANGUARD y firewall ASTARO. Entre los equipos mencionados se encuentra un equipo segmentador de trafico

2.2.3.2.2. Beaterio

En la tabla 2.7 se detallan las distintas subredes que se utilizan en el Beaterio, la división en subredes se hace en base a las aplicaciones.

BEATERIO			
Subred	**No Vlan**	**Red**	**Mascara**
Datos 1	1	172.20.129.0	255.255.255.128
Datos 2	2	172.20.129.128	255.255.255.192
Telefonía	3	172.10.129.0	255,255,255,128
Industrial	4	172.20.129.192	255.255.255.192
Videoconferencia	5	172.20.16.16	255.255.255.224
Videoseguridad	7	172.31.129.0	255.255.255.128
Detec. Fugas Pol Q-A	8	172.31.129.128	255.255.255.192
Válvulas	10	172.25.129.0	255.255.255.0

Tabla 2.7 Subredes Beaterio

En el Beaterio se cuenta con un switch de capa 3 marca CISCO modelo 3560 entre la red y el router Vanguard.

2.2.3.2.3. Gasolinera

En la tabla 2.8 se detallan las distintas subredes que se utilizan en la Gasolinera, la división en subredes se hace en base de las aplicaciones.

GASOLINERA		
Descripción	**Red**	**Máscara**
Datos	172.20.134.0	255.255.255.0
Video Seguridad	172.31.134.0	255,255,255,128

Tabla 2.8 Subredes Gasolinera

En la red LAN de Gasolinera existen switches de capa 2 marca CISCO.

Adicional a las dos redes indicadas en la tabla, existen dos subredes más, la subred para impresión de notas de venta, y la subred para control de equipos de despacho de combustible, las cuales por motivos de seguridad y naturaleza de las dos aplicaciones son subredes solamente locales, lo que no influirá en la red WAN de PETROCOMERCIAL.

2.2.3.2.4. Aeropuerto

En la tabla 2.9 se indica la subred del aeropuerto.

AEROPUERTO		
Descripción	**Red**	**Máscara**
Datos	172.20.75.0	255.255.255.0

Tabla 2.9 Subred Aeropuerto

En la red local de Aeropuerto el switch que se utiliza es un equipo 3 COM no administrable que no soporta VLANs (802.1q).

2.2.3.2.5. Oyambaro

En la tabla 2.10 se detallan las distintas subredes que se utilizan en Oyambaro, la división en subredes se hace en base de las aplicaciones.

OYAMBARO			
Red	**No. Vlan**	**Red IP**	**Máscara**
Equipos Telecom	1	172.20.76.0	255.255.255.224
Libre	2	172.20.76.32	255.255.255.224
Datos	3	172,20,76,64	255,255,255,192
Libre	4	172.20.76.128	255.255.255.192
Industrial	5	172.20.76.192	255.255.255.128
Voz	6	172.10.76.0	255.255.255.128
Videoseg.	7	172.10.76.128	255.255.255.128
Videoconferencia	8	172.20.16.96	255.255.255.240
Válvulas	-----	172.25.76.0	255.255.255.0

Tabla 2.10 Subred Oyambaro

En Oyambaro se cuenta con un switch de capa 3 marca ALCATEL entre la red y el router VANGUARD.

2.2.3.2.6. Corazón

En la tabla 2.11 se detallan las distintas subredes que se utilizan en Corazón, la división en subredes se hace en base de las aplicaciones.

CORAZÓN		
Descripción	**Red**	**Máscara**
Datos	172.20.77.0	255.255.255.0
Válvulas	172.25.77.0	255.255.255.0

Tabla 2.11 Subredes Corazón

En la red de Corazón no existen VLANs por que el switch que se utiliza es un equipo 3 COM no administrable que no soporta el estándar 802.1q, por lo que se configuró el puerto del router con dos direcciones IP.

2.2.3.2.7. Faisanes

En la tabla 2.12 se detallan las distintas subredes que se utilizan en Faisanes, la división en subredes se hace en base de las aplicaciones.

FAISANES		
Descripción	**Red**	**Máscara**
Datos	172.20.76.0	255.255.255.0
Válvulas	172.25.76.0	255.255.255.0

Tabla 2.12 Subredes Faisanes

En la red de Faisanes no existen VLANs por que el switch que se utiliza es un equipo 3COM no administrable que no soporta el estándar 802.1q, por lo que se configuró el puerto del router con dos direcciones IP.

2.2.3.2.8. Santo Domingo

En la tabla 2.13 se detallan las distintas subredes que se utilizan en Santo Domingo, la división en subredes se hace en base de las aplicaciones.

SANTO DOMINGO			
Red	**No. Vlan**	**Red IP**	**Máscara**
Equipos Telecom	1	172.20.161.0	255.255.255.224
Libre	2	172.20.161.32	255.255.255.224
Datos	3	172.20.161.64	255.255.255.192
Libre	4	172.20.161.128	255.255.255.192
Industrial	5	172.20.161.192	255.255.255.192
Voz	6	172.10.161.0	255.255.255.128
videoseg	7	172.10.161.128	255.255.255.128
videoconferencia	8	172.20.16.48	255.255.255.240
Válvulas	10	172.25.161.0	255.255.255.0

Tabla 2.13 Subredes Santo Domingo

En Santo Domingo se cuenta con un switch de capa 3 marca ALCATEL entre la red y el router VANGUARD.

Como se puede observar el direccionamiento de las subredes, no fue diseñado para la sumarización de direcciones, por lo que es un problema que se tomará en cuenta en el diseño.

En los nodos terminales se maneja una ruta por defecto para que todo el tráfico WAN sea enviado al nodo central del Edificio el Rocío por lo que la creación de cualquier nueva subred es transparente para los mismos. De esta manera la administración del enrutamiento cae en el nodo central lo que permite tener un cierto control en la creación de nuevas subredes en los nodos terminales.

Este tipo de configuración genera una tabla de enrutamiento extensa creada manualmente en el nodo central, teniendo como ventaja que no hay consumo de ancho de banda de protocolos de enrutamiento.

2.2.3.3. Segmentador de Tráfico

PETROCOMERCIAL utiliza aplicaciones en tiempo real, por lo que cuenta con un equipo segmentador de tráfico que permite garantizar ancho de banda a las distintas aplicaciones, el equipo ALLOT se encuentra instalado en el Edificio el Rocío, matriz de la regional Norte, y cuenta con 4 interfaces, dos entrantes y dos salientes.

Como se observa en la figura 2.21, el primer par de interfaces se encuentra entre la red interna del edificio el Rocío y la RED WAN de PETROCOMERCIAL lo que permite monitorear y asignar políticas a los nodos terminales, el segundo par de interfaces se encuentra entre la red interna del edificio el Rocío y el Firewall que brinda salida a Internet, a los Enlaces de CNT, Clientes (Bancos) y hacia PETROECUADOR, lo que permite monitorear y controlar el tráfico que se genera a los puntos explicados.

La configuración actual no permite segmentar el tráfico que se genere entre los distintos interfaces del Firewall debido a que éste no pasará por el equipo, tampoco se segmentará en el caso de que los nodos terminales tengan conectividad sin pasar por el nodo central.

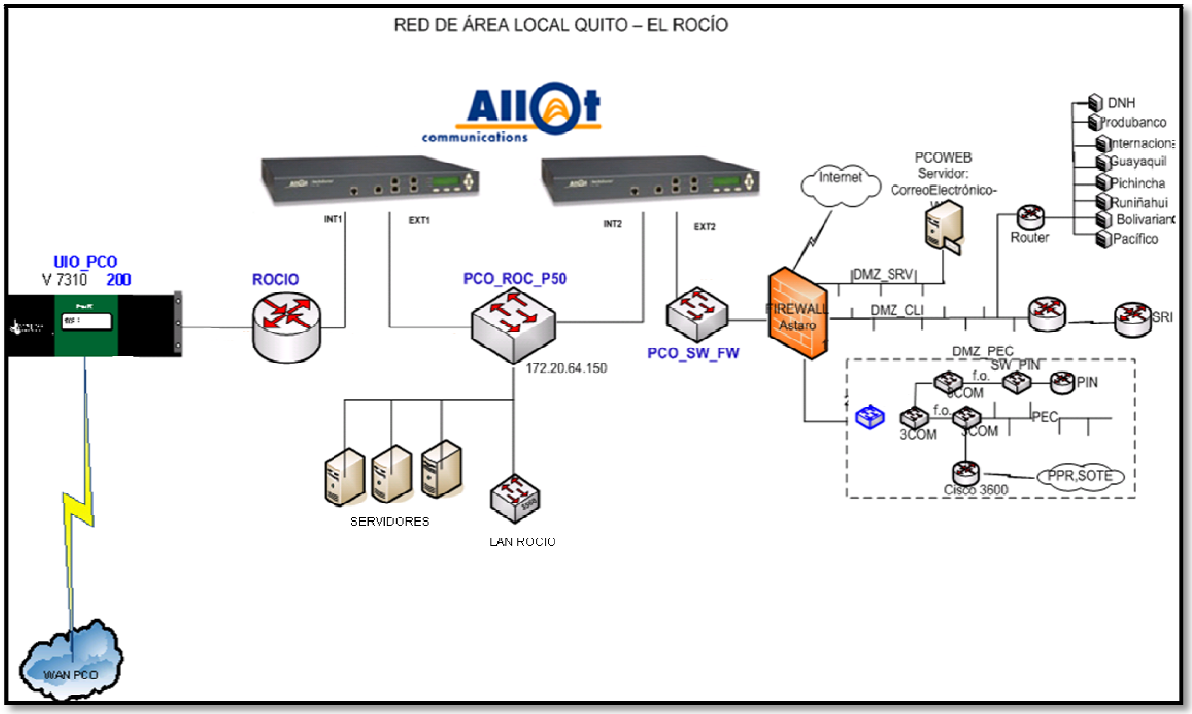


Figura 2.21 Diagrama Segmentador de tráfico

2.2.4. EQUIPOS DE ENRUTAMIENTO ACTUALES

Los routers que se utilizan en la red WAN de PETROCOMERCIAL son en su totalidad de la marca Motorola y del modelo Vanguard, a continuación se detallan las características de los distintos modelos y su ubicación.

2.2.4.1. Vanguard 7310[22]

Los equipos de enrutamiento Vanguard 7310 están destinados a soluciones de conectividad de datos y voz para medianas y grandes empresas.

2.2.4.1.1. Ubicación

Quito-Edificio El Rocío.

[22] http://www.vanguardnetworks.com/products-7300.htm

2.2.4.1.2. Especificaciones de software

Características para transporte de voz

- Compresión de Voz, códecs: G711, G723, G729a
- Señalización de VoIP soporte de H.323 versión 1 y 2.
- Voz sobre IP, Frame Relay, ATM. Broadcast de Voz
- Señalización Q.SIG
- PBX y conexiones a la PSTN.
- Broadcast de voz

2.2.4.1.3. Características de Routing y Administración

- Soporte a IPv4
- Protocolos de enrutamiento: RIP versión 1 y 2, OSPF, BGP4
- Routing Policies
- CIDR(Classless Inter-Domain Routing), Enrutamiento Entre Dominios sin Clase
- NAT (Network Address Traslation), Traducción de Direcciones de Red
- PAT (Port Address Traslation), Traducción de Direcciones de Puerto
- Múltiples direcciones IP por interfaz.
- Servidor DHCP.
- SOTCP (Serial Over TCP), Serial sobre TCP
- IGMP v2
- Qos, IP type of service, DiffServ

2.2.4.1.4. Seguridad

- Cliente Radius
- VPNs, IPsec.
- Soporte SNMP V1 y V3

2.2.4.1.5. Interfaces físicas

El router Vanguard 7310 da soporte para los siguientes tipos de interfaces:

- Interfaces LAN: Auto-selectable 10/100/1000BaseT, Ethernet y Gigabit Ethernet.
- Interfaces WAN de alta velocidad: DS-3/E3 ATM, ATM, Tasa de transmisión variable (VBR), Tasa de transmisión constante (CBR), Tasa de transmisión desconocida (UBR), RFC 1483 - Multiprotocolo sobre, ATM, RFC 1490 - Multiprotocolo over Frame Relay. Alta densidad, multicanal T1/E1 con CSU integrado.
- Puertos seriales de alta velocidad: 8/card, configurables para V.35, V.24, X.21, EIA530, selección automática vía cable DTE/DCE. ISDN Primary Rate Interface (PRI)

2.2.4.2. Vanguard 6841

Los equipos de enrutamiento Vanguard de la serie 6800 están destinados a soluciones de conectividad de datos y voz para medianas empresas.

2.2.4.2.1. Ubicación

Quito-Estación Beaterio, Santo Domingo-Estación Santo Domingo.

2.2.4.2.2. Especificaciones de Software

Características de voz

- PBX analógica y conexiones a PSTN.
- H.323 v2 gateway.
- SIP gateway
- Codecs: G.711, G.723.1, G.729a, and G.729b
- Broadcast de voz

2.2.4.2.3. Características de Routing y Administración

- Protocolos de enrutamiento: RIP versión 1 y 2, OSPF, BGP4
- Routing Policies

- CIDR (Classless Inter-Domain Routing)
- NAT (Network Address Traslation)
- PAT (Port Address Traslation)
- Múltiples direcciones IP por interfaz.
- Servidor DHCP.
- SOTCP
- 802.1 Q
- IGMP v2
- Qos, IP type of service, DiffServ
- Soporte SNMP V1 y V3

2.2.4.2.4. Seguridad

- Cliente Radius
- VPNs, IPsec.

2.2.4.2.5. Interfaces físicas

La familia 6800 tiene el mismo soporte de tarjetería que los modelos 7300

2.2.4.3. Vanguard 6455-6435

2.2.4.3.1. Ubicación

Quito-Estación de Servicio Gasolinera (6455), Pichincha-Estación Corazón (6435), Pichincha-Estación Faisanes (6435), Pichincha-Estación Oyambaro (6435), Quito-Aeropuerto (6435)

2.2.4.3.2. Especificaciones de Software

Características de voz

- PBX analógica y conexiones a PSTN.
- VoIP and VoFR Interoperability
- Codecs: G.711, G.723.1, G.729a, and G.729b
- Señalización H.323 versiones 1 y 2

- Broadcast de voz
- Tabla centralizada de switching de voz

2.2.4.3.3. Características de Routing y Administración

- Soporte a IPV4
- Protocolos de enrutamiento: RIP1/RIP2, OSPF
- Classless Inter-domain Routing (CIDR)
- Network Address Translation (NAT), Network Address Port Translation (PAT)
- IP Multicast/Broadcast
- Multiples direcciones IP por interfaz
- 802.1 Q
- IGMP v2
- Qos, IP tip de servicio, DiffServ
- Soporte SNMP V1 y V2

2.2.4.3.4. Seguridad

- VPNs, IPsec.

2.2.4.3.5. Interfaces físicas

La familia 6400 tiene el mismo soporte de tarjetería que los modelos 7300.

2.2.4.4. Configuración

En ningún ruteador se encuentra configurado un protocolo de enrutamiento, como se puede ver en la tabla 2.14 en la que se muestra la tabla de enrutamiento del ruteador del edificio el Roció, en este equipo se encuentran concentrado el direccionamiento estático, cuenta con un total de 116 rutas estáticas, por lo que es de tamaño considerable, cuenta con una ruta por defecto que envía el trafico al firewall para permitir la salida a internet y hacia otras empresas, en la tabla 2.15 se puede observar la tabla de enrutamiento en un nodo terminal, que cuenta con una ruta por defecto que envía todo el trafico al nodo El Rocío.

Número de Ruta	Red Destino	Máscara	Siguiente Salto	Distancia Administrativa
[1]	172.10.76.0	255.255.255.0	172.20.36.170	1
[2]	172.10.161.0	255.255.255.0	172.20.36.10	1
[3]	172.20.75.0	255.255.255.0	172.20.64.167	1
[4]	172.20.76.0	255.255.255.0	172.20.36.170	1
[5]	172.20.96.34	255.255.255.255	172.20.36.26	1
[6]	172.20.96.34	255.255.255.255	172.20.64.6	2
[7]	172.20.130.0	255.255.255.0	172.20.36.6	1
[8]	172.20.131.0	255.255.255.0	172.20.64.6	1
[9]	172.20.132.0	255.255.255.0	172.20.64.6	1
[10]	172.20.161.0	255.255.255.0	172.20.36.10	1
[11]	172.20.163.0	255.255.255.0	172.20.36.134	1
[12]	172.20.165.0	255.255.255.192	172.20.38.26	1
[13]	172.20.165.0	255.255.255.192	172.20.64.6	2
[14]	172.20.167.0	255.255.255.0	172.20.38.26	1
[15]	172.20.167.0	255.255.255.0	172.20.64.6	2
[16]	172.20.167.64	255.255.255.192	172.20.38.26	1
[17]	172.20.167.64	255.255.255.192	172.20.64.6	2
[18]	0.0.0.0	255.255.255.0	0.0.0.0	1
[20]	172.20.169.0	255.255.255.0	172.20.64.6	2
[21]	172.20.169.0	255.255.255.0	172.20.38.26	2
[22]	172.20.170.0	255.255.255.192	172.20.36.26	1
[23]	172.20.170.0	255.255.255.192	172.20.64.6	2
[24]	172.20.170.64	255.255.255.192	172.20.38.26	1
[25]	172.20.170.64	255.255.255.192	172.20.64.6	2
[26]	172.20.170.128	255.255.255.192	172.20.38.26	1
[27]	172.20.170.128	255.255.255.192	172.20.64.6	2
[28]	172.20.171.0	255.255.255.192	172.20.64.2	1
[29]	172.20.77.0	255.255.255.0	172.20.36.38	1
[30]	172.20.141.0	255.255.255.0	172.20.36.42	1
[31]	172.20.140.0	255.255.255.0	172.20.36.150	3
[32]	172.20.98.0	255.255.254.0	172.20.36.26	1
[33]	172.20.170.224	255.255.255.240	172.20.38.26	1
[34]	172.20.170.224	255.255.255.240	172.20.64.6	2
[35]	172.17.117.192	255.255.255.192	10.5.1.2	1
[36]	172.17.117.64	255.255.255.192	10.5.1.2	1
[37]	172.17.117.128	255.255.255.192	10.5.1.2	1
[38]	172.17.117.0	255.255.255.192	10.5.1.2	1
[39]	172.20.133.0	255.255.255.0	172.20.36.25	1
[40]	172.20.133.0	255.255.255.0	172.20.64.6	2
[41]	172.20.172.0	255.255.255.128	172.20.36.26	1
[43]	172.20.172.0	255.255.255.128	172.20.64.6	2
[44]	172.20.166.0	255.255.255.0	172.20.36.174	1
[45]	172.20.39.8	255.255.255.252	172.20.64.6	1
[46]	172.20.72.0	255.255.255.0	40.40.40.253	1
[47]	172.20.171.128	255.255.255.192	172.20.64.2	1
[48]	172.20.129.0	255.255.255.0	172.20.36.14	1
[49]	172.20.165.64	255.255.255.192	172.20.36.26	1
[50]	172.20.165.64	255.255.255.192	172.20.64.6	2

[51]	172.20.171.64	255.255.255.192	172.20.38.26	1
[52]	172.20.164.0	255.255.255.0	172.20.36.137	1
[53]	172.20.134.0	255.255.255.0	172.20.36.18	1
[54]	172.20.32.0	255.255.255.0	172.20.64.6	2
[55]	172.20.135.0	255.255.255.0	172.20.36.34	1
[56]	172.20.136.0	255.255.255.0	172.20.36.158	1
[57]	172.20.137.0	255.255.255.0	172.20.36.162	1
[58]	172.20.138.0	255.255.255.0	172.20.36.166	1
[59]	172.20.171.192	255.255.255.192	172.20.64.2	1
[61]	172.20.160.0	255.255.255.0	172.20.36.38	1
[62]	172.17.20.0	255.255.255.0	172.20.37.2	1
[63]	172.20.129.0	255.255.255.0	172.20.64.6	2
[66]	172.20.50.0	255.255.255.248	172.20.36.130	1
[67]	172.20.127.0	255.255.255.0	172.20.36.30	1
[68]	172.20.139.0	255.255.255.0	172.20.36.2	1
[70]	172.10.64.0	255.255.252.0	172.20.64.150	1
[71]	172.31.129.0	255.255.255.128	172.20.36.14	1
[72]	172.31.134.0	255.255.255.0	172.20.36.18	1
[73]	172.10.136.0	255.255.255.0	172.20.36.158	1
[74]	172.20.100.0	255.255.255.0	172.20.38.26	1
[75]	172.20.94.0	255.255.254.0	172.20.36.26	1
[76]	172.20.97.0	255.255.255.0	172.20.36.26	1
[77]	172.20.90.0	255.255.255.248	172.20.36.26	1
[78]	172.20.90.8	255.255.255.248	172.20.36.26	1
[79]	172.20.96.64	255.255.255.192	172.20.36.26	1
[81]	172.20.94.0	255.255.254.0	172.20.64.6	2
[82]	172.20.97.0	255.255.255.0	172.20.64.6	2
[83]	172.20.90.0	255.255.255.248	172.20.64.6	2
[85]	172.20.96.64	255.255.255.192	172.20.64.6	2
[86]	172.20.90.8	255.255.255.248	172.20.64.6	2
[90]	172.20.16.16	255.255.255.240	172.20.36.14	1
[91]	172.20.16.32	255.255.255.240	172.20.36.6	1
[92]	172.20.16.64	255.255.255.240	172.20.36.158	1
[93]	172.20.16.48	255.255.255.240	172.20.36.10	1
[94]	172.20.16.80	255.255.255.240	172.20.36.138	1
[95]	172.20.16.96	255.255.255.240	172.20.36.170	1
[96]	172.20.16.112	255.255.255.240	172.20.16.10	1
[97]	172.20.16.240	255.255.255.240	172.20.16.10	1
[98]	172.20.16.224	255.255.255.240	172.20.16.10	1
[99]	172.20.16.128	255.255.255.240	172.20.36.166	1
[100]	172.19.28.0	255.255.255.0	172.20.16.10	1
[101]	0.0.0.0	0.0.0.0	172.20.64.6	1
[102]	172.20.78.0	255.255.255.0	172.20.36.62	1
[103]	172.10.129.0	255.255.255.128	172.20.36.14	1
[104]	172.18.16.114	255.255.255.255	172.20.16.10	1
[105]	172.18.16.113	255.255.255.255	172.20.16.10	1
[106]	172.20.16.16	255.255.255.240	172.20.16.10	2
[107]	172.31.129.0	255.255.255.128	172.20.64.6	2
[108]	172.10.129.0	255.255.255.128	172.20.64.6	2
[109]	172.20.0.21	255.255.255.255	172.20.38.26	1

[110]	172.20.0.9	255.255.255.255	172.20.38.26	1
[111]	192.168.0.0	255.255.255.0	172.20.64.167	1
[112]	172.20.129.20	255.255.255.255	172.20.64.6	1
[113]	172.25.129.0	255.255.255.0	172.20.36.14	1
[114]	172.25.161.0	255.255.255.0	172.20.36.10	1
[115]	172.25.77.0	255.255.255.0	172.20.36.38	1
[116]	172.25.141.0	255.255.255.0	172.20.36.42	1

Tabla 2.14 Tabla de Enrutamiento Rocío

Número de Ruta	Red Destino	Máscara	Siguiente Salto	Distancia Administrativa
[1]	0.0.0.0	0.0.0.0	172.20.36.21	1

Tabla 2.15 Tabla de Enrutamiento Aeropuerto

Se encuentra configurado SNMP versión 1, para gestión y monitoreo de la red utilizando la comunidad Pco-Ec, tiene habilitada una sola línea remota a través de Telnet para su configuración.

2.3. CAPA ENLACE DE DATOS

La capa enlace de Datos es la responsable de la transferencia fiable de información a través de un circuito de transmisión de datos. Esta capa se relaciona con la capa de Red, anteriormente explicada, recibiendo peticiones de esta capa y utilizando los servicios de la capa física (se explica posteriormente).

2.3.1. TECNOLOGÍA DE CAPA ENLACE DE DATOS

En la capa 2 del modelo ISO/OSI la red de PETROCOMERCIAL hace uso de Frame Relay como medio de transporte de la información de la matriz (Quito) a sus nodos remotos (Aeropuerto, Beaterio, Corazón, Faisanes, Gasolinera, Oyambaro, Sto. Domingo).

Frame Relay se utiliza en PETROCOMERCIAL para brindar un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de las redes remotas con la matriz Quito.

Para la transmisión de datos a nivel WAN, Frame Relay, hace uso de los identificadores de conexión de enlace de datos (DLCI's) estableciendo los Circuitos Virtuales correspondientes. Más adelante en el direccionamiento se explicará más detalladamente los DLCI's de la red de PETROCOMERCIAL.

2.3.2. TOPOLOGÍA DE CAPA ENLACE DE DATOS

La topología de capa dos de PETROCOMERCIAL está formada por dos estrellas, como se explicó anteriormente (Véase *2.2.2 TOPOLOGÍA DE CAPA DE RED*), en las cuales se concentra todo el tráfico, a partir de estas dos estrellas, que se encuentran en la regional norte y regional sur, teniendo como centros a los nodos Quito y Guayaquil respectivamente. A partir de estos dos puntos concentradores se realiza la comunicación frame relay a nivel de capa 2 a los demás nodos. En el anexo 1 podemos observar el direccionamiento lógico de la red.

2.3.3. DIRECCIONAMIENTO [23]

Antes de explicar el direccionamiento de la red Frame Relay, se indican dos conceptos fundamentales dentro de la configuración de los routers Motorola Vanguard, los cuales son:

- *FRI* (*Frame Relay Interface, Interfaz Frame Relay*): Es la capacidad que se le asocia a un puerto físico o lógico, para que soporte la tecnología Frame Relay,

[23] Tomado del Proyecto de Titulación Rediseño de la red de área extendida de PETROCOMERCIAL con calidad de servicio, del Ing. René Damián Padilla Benítez, 2008

en todo caso, siempre un puerto lógico va a estar soportado sobre un puerto físico.

UN FRI puede soportar:

- Puertos con interfaces Frame Relay DTE en nodos Vanguard.
- Trasmitir y recibir tramas a través de nodos Vanguard, con Frame Relay T1.617 con Anexo G o sin él.
- Protocolos estándares ANSI, Anexo D, LMI (*Local Managment Interface, Interfaz de Administración local*), Q.933 Anexo A.

- *FRI Station* (*Frame Relay Interface Station, Estación de una Interfaz Frame Relay*): La estación es la encargada de generar un camino virtual y todo lo referente al mismo, sea éste conmutado o permanente, entre dos nodos Frame Relay, para que se puedan comunicar; por tanto una estación FRI sólo puede configurarse con un único DLCI y una Interfaz Frame Relay puede manejar máximo 254 estaciones FRI.

  Existen 2 tipos de Estaciones FRI que pueden ser creadas:

  - Una estación que maneje Anexo G, la cual soporta transmisión de datos encapsulados en X.25, y se refiere al mismo como un enlace lógico X.25.
  - Una estación Bypass, que transmite los datos siguiendo el RFC 1490 de la IETF, es decir Frame Relay puro utilizando solo LAPF.

De acuerdo a estos dos conceptos y teniendo presente que los DLCIs tienen significado local, el direccionamiento se lo puede expresar en función del puerto y la estación que está generando el circuito virtual, así para hablar de un enlace que se genera entre dos puntos en lugar de referirse a los DLCIs que lo forman, se hará referencia al puerto y la estación que lo generan utilizando el siguiente ejemplo:

El enlace entre Santo Domingo y Quito tiene la siguiente descripción: P100S1, lo cual representa que el puerto utilizado es el número 100 y la Estación es la número 1.

El DLCI por defecto en estos equipos es el número 16, esto no restringe el uso de otro DLCI en los nodos de la red.

En el anexo 1 se puede observar el direccionamiento de los demás nodo de la red de PETROCOMERCIAL, con la nomenclatura anteriormente explicada.

2.3.4. EQUIPOS DE CAPA ENLACE DE DATOS

Los nodos o ruteadores de la red de PETROCOMERCIAL son modelos Vanguard de la marca Motorola, como se indicó anteriormente.

2.3.4.1. Número de Nodos

Debido a que los equipos que realizan funciones de capa 3 y capa 2 son los mismos, el número de nodos y características de equipo, son los mismos que los descritos en la capa 3.

2.4. CAPA FÍSICA

A nivel de capa física PETROCOMERCIAL cuenta en su mayoría con infraestructura propia a través de un sistema de enlaces microondas, los restantes enlaces se los realiza a través de enlaces arrendados con la CNT (Ver Anexo 2).

2.4.1. TECNOLOGÍA DE CAPA FÍSICA

A nivel de capa física la red de PETROCOMERCIAL, utiliza la tecnología de transporte de información PDH. La distribución de los enlaces se lo realiza en la

regional norte desde el edificio el Rocío a través de E1 (estándar europeo) a las distintas sucursales.

La conexión entre el router y el equipo de transmisión, se lo hace a través de conversores de interfaces LAN a G.703, que son los interfaces que manejan el router y el radio respectivamente. Cada salida de los conversores se convierte en un tributario entrante al router. En la tabla 2.16 se detalla las capacidades de los enlaces existentes entre la Matriz y las sucursales.

ENLACE	CAPACIDAD	INTERFAZ DE RADIO
MATRIZ-BEATERIO	2 Mbps	G.703
MATRIZ-GASOLINERA	2 Mbps	G.703
MATRIZ-AEROPUERTO	2 Mbps	G.703
MATRIZ-OYAMBARO	2 Mbps	G.703
MATRIZ-CORAZON	2 Mbps	G.703
MATRIZ-FAISANES	2 Mbps	G.703
MATRIZ-SANTO DOMINGO	2 Mbps	G.703

Tabla 2.16 Capacidades de Enlaces PETROCOMERCIAL

2.4.2. TOPOLOGÍA DE CAPA FÍSICA

A nivel de capa física la red WAN de PETROCOMERCIAL cuenta con infraestructura propia con un sistema de microondas e infraestructura arrendada través de enlaces de CNT y Global Crossing para brindar conectividad a las distintas sucursales, para el propósito del presente Proyecto de Titulación se analizará los enlaces a los nodos especificados en capa 3, para todos los cuales se cuenta con enlaces microondas.

Se cuenta con tres puntos de concentración para los enlaces con las sucursales:

El cerro Pichincha a través del cual se permite enlazar Matriz-Gasolinera, Matriz-Aeropuerto, Matriz-Beaterio.

El cerro Atacazo a través del cual se permite enlazar Matriz-Oyambaro, Matriz-Corazón, Matriz-Chiguilpe.

El cerro Chiguilpe a través del cual se permite enlazar Chiguilpe-Santo Domingo, Chiguilpe-Faisanes.

Estos enlaces se los puede observar en el anexo 2. En la tabla 2.17 se detalla la ubicación de los puntos mencionados.

ESTACIÓN	PROVINCIA	CANTÓN	COORDENADAS		ALT (msnm)
			LATITUD	LONGITUD	
PICHINCHA	PICHINCHA	QUITO	00º09'53''S	78º31'18''O	3805
ATACAZO	PICHINCHA	QUITO	00º18'54''S	78º36'11''O	3851
CHIGUILPE	STO DOMINGO	STO DOMINGO	00º17'44''S	79º05'12''O	1178

Tabla 2.17 Ubicación puntos de concentración capa física

En la tabla 2.18 se detallan las características de los enlaces entre la matriz y las sucursales de PETROCOMERCIAL.

ENLACE	MARCA	MODELO	TECNOLOGÍA	DISTANCIA KM	CAPACIDAD DEL EQUIPO	CAPACIDAD INSTALADA
ATACAZO – ROCIO	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	19.48	STM1	8 E1
ATACAZO – CORAZON	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	8.96	STM1	1 E1
ATACAZO – OYAMBARO	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	30	STM1	1 E1
ATACAZO – CHIGUILPE	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	13	STM1	2 E1
CHIGUILPE – FAISANES	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	10	STM1	1 E1
CHIGUILPE – STO. DOMINGO	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	15	STM1	1 E1
PICHINCHA – BEATERIO	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	17.59	STM1	4 E1
PICHINCHA – ROCIO	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	7.98	STM1	8 E1
PICHINCHA – AEROPUERTO	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	4	STM1	1 E1
PICHINCHA - GASOLINERA	HARRIS	TRUEPOINT 5000	PORTADORA FIJA	4	STM1	1 E1

Tabla 2.18 Características enlaces PETROCOMERCIAL

2.4.3. EQUIPOS DE TRANSMISIÓN CAPA FÍSICA

En la actualidad se cuenta con equipos de transmisión marca Harris modelo TRUEPOINT 5000, dicho equipo cuenta con interfaces G.703 e interfaces LAN, las interfaces LAN no se encuentran utilizadas actualmente.

2.4.3.1. Truepoint 5000

Esquema de Modulación, QPSK a 256 QAM
Esquema de corrección de errores FEC.
Funciones de MULDEX (Multiplexer-Demultiplexer) integradas.

2.4.3.1.1. Soporte de interfaces

- 2 a16 E1 con actualización por clave de hardware
- 2 a16 E1 mezclados con 2 x 100BASE-T
- E3 + E1 con 2x 100BASE-T (Switch opcional).
- 21 E1 sobre empaquetado parcial STM-1–STM-1+E1 con 2 x 100-BASE-T (Switch opcional)

2.4.3.1.2. Puerto y Funcionalidades

- Canal de datos a 64 Kbps (V11 and/or G703)
- 10BASE-T Puerto sobre 64 Kbps
- Modem Dial-up
- Función de Puerto RTU (Canal de Datos (19.2 Kbps -RS232 Asynchronous)
- HDLC
- Keypad para la administración
- PPP para NMS y Web CIT (interoperabilidad con cualquier protocolo abierto de administración de red)

En la figura 2.22 se indica los componentes de un radio Harris Truepoint 5000.

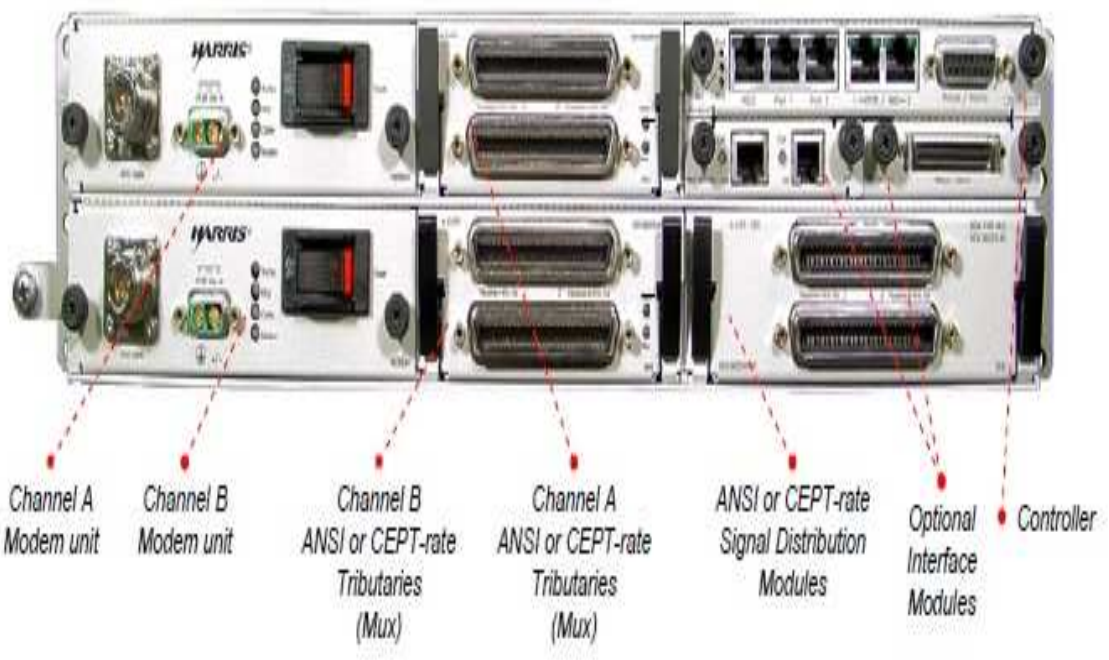


Figura 2.22 Radio Harris Truepoint 5000

CAPÍTULO III

3. DISEÑO DE LA RESTRUCTURACIÓN DE LA RED DE PETROCOMERCIAL

En este capítulo se realiza el diseño de la solución, para lo cual se indica la capacidad actual de los enlaces, con cuyos datos se calcula la capacidad requerida de acuerdo a la topología diseñada, se realiza el direccionamiento y dimensionamiento de los equipos necesarios para este proyecto, basándonos en los requerimientos de cada sucursal y de los enlaces. Se indica el modelo seleccionado de los equipos y su costo referencial en el proyecto. Además se elabora un plan de migración para los cambios a realizar.

3.1. TOPOLOGÍA

3.1.1. TOPOLOGÍA FÍSICA

Los puntos terminales de la red WAN, no se pueden modificar por obvias razones, los puntos de concentración en los cerros Pichincha y Atacazo son puntos estratégicos por lo que no existe razón para modificarlos, por lo tanto la topología física se debe mantener.

3.1.2. TOPOLOGÍA LÓGICA

Como se explicó en el capítulo 2, la topología lógica de la red WAN de PETROCOMERCIAL es una estrella que tiene como centro la Matriz en Quito, este diseño presenta la debilidad que si se necesita transmitir tráfico entre las sucursales necesariamente tiene que pasar por el nodo UIO de la Matriz. Tomando esto en cuenta se puede aprovechar la topología física de los equipos y diseñar la red WAN para que el centro de la estrella sea ahora los puntos de distribución de los enlaces, de esta forma si existe tráfico entre las sucursales dentro de una misma estrella será enviado sin consumir recursos de ancho de banda del enlace hacia la Matriz que es el enlace más crítico, para esta topología es necesario que exista un equipo de enrutamiento en los cerros Pichincha y Atacazo.

Otra ventaja de este diseño es que permite aprovechar de mejor forma el ancho de banda disponible en los enlaces de radiofrecuencia, debido a que la mayoría de PVC's entre la matriz y sus distintas sucursales tiene un CIR de 2Mbps, se utilice o no esta capacidad está reservada para el PVC y existen sucursales que debido al número de usuarios que maneja subutiliza esta capacidad.

Dichos recursos se pueden utilizar de forma más eficiente si se crea un ambiente de medio compartido en este enlace, por lo que el protocolo de capa dos utilizado para el diseño de la red WAN será Ethernet, de esta forma la capacidad del enlace entre la matriz y el cerro Pichincha o entre la matriz y el cerro Atacazo será dividido para el tráfico demandado por las sucursales, mientras más tráfico genere más recursos consumirá dichos enlaces.

Para la topología explicada existen dos opciones: que se eliminen los ruteadores de borde y los únicos equipos que realicen enrutamiento sean los equipos en los cerros Pichincha y Atacazo, de esta forma los gateways de cada red local serían los interfaces en estos equipos. El problema que genera esta topología es que los

broadcast que se generen en las redes locales consumirán recursos de los radioenlaces, por lo cual no es aplicable esta topología.

La segunda opción es la de mantener los ruteadores de borde y colocar equipos de enrutamiento en los cerros Pichincha y Atacazo creando subredes entre los interfaces de estos equipos y los equipos en enrutamiento en las sucursales, éste es la topología que se utilizará para la red WAN de Petrocomercial.

Gracias al soporte con el que cuentan los radios Harris TruePoint 5000 para Ethernet, al contar con dos interfaces que soportan esta tecnología, se puede realizar la comunicación con los equipos de borde a través de Ethernet, la comunicación por enlaces de radiofrecuencia pueden soportar hasta un STM 1 (155,52 Mbps).

Debido al requerimiento de números de puertos para el enrutamiento en los cerros Pichincha y Atacazo es conveniente usar un switch de capa tres para estas funciones, las características de estos equipos serán detallados más adelante.

Además es necesario brindar alta disponibilidad para las aplicaciones que utilizan la red, por lo que es necesario formar un anillo entre los nodos críticos de la red WAN, enlazando los cerros Pichincha y Atacazo.

Si bien por el alcance de este Proyecto de Titulación no se realiza un estudio de ingeniería para determinar la factibilidad del enlace propuesto, se indica la distancia entre los dos cerros y si se puede garantizar la primera zona de fresnel.

La distancia entre los dos puntos es de 18,931 km.

Para determinar si está garantizada la primera zona de fresnel se utilizo el software Radio Mobile, obteniéndose como resultado que con las torres que se cuenta en los cerros, se tiene línea de vista y está garantizada la primera zona de fresnel.

Las frecuencias asignadas por Senatel a Petrocomercial son de 14 Mhz, en la banda de 7 Ghz.

En la figura 3.1 se indica el resultado obtenido del programa Radio Mobile.

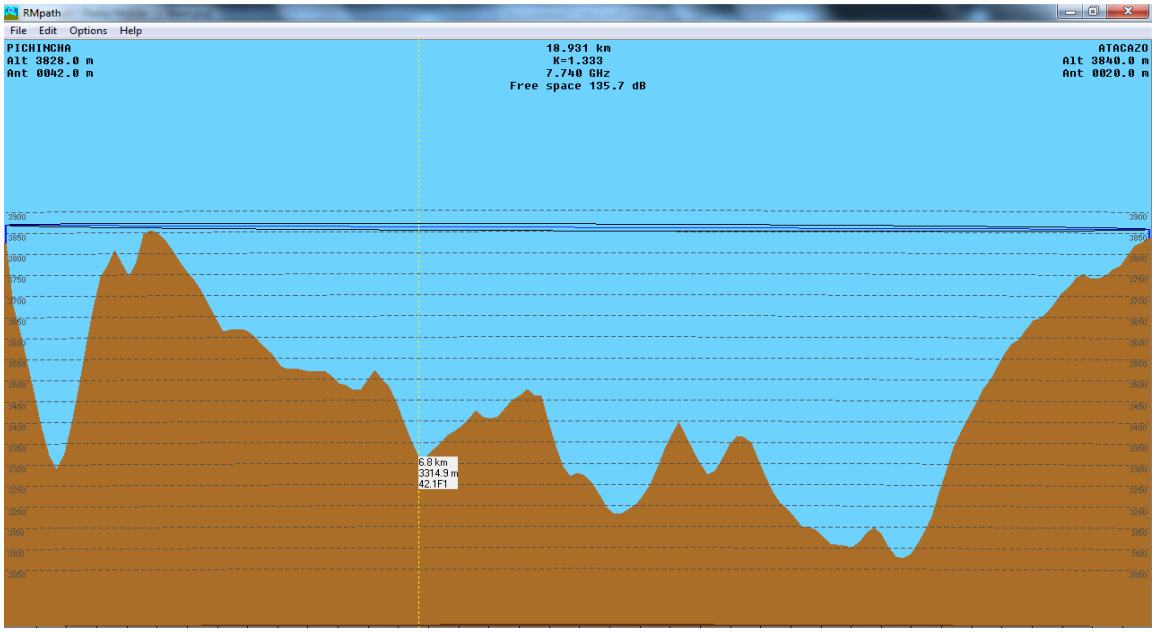


Figura 3.1 Enlace entre Atacazo Pichincha

La topología lógica propuesta para la red WAN de Petrocomercial se indica en la figura 3.2.

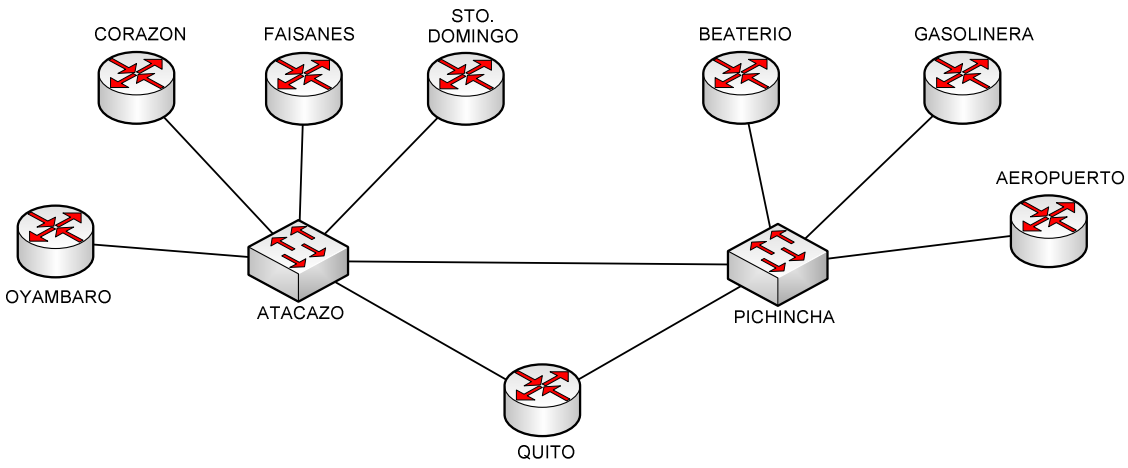


Figura 3.2 Topología lógica propuesta para la red WAN de PETROCOMERCIAL

3.2. CAPACIDAD DE ENLACES

PETROCOMERCIAL necesita optimizar el uso de sus enlaces hacia las distintas sucursales, debido al crecimiento de los requerimientos por parte de aplicaciones como videoconferencia, video seguridad, telefonía IP etc.

A continuación se analizan los anchos de banda necesarios para las aplicaciones, para lo cual se toma como base los datos estadísticos, obtenidos con la herramienta NetExplorer en el capítulo II.

3.2.1. CAPACIDAD UTILIZADA DE LOS ENLACES

En la tabla 3.1 se muestran las capacidades de los enlaces utilizados desde los distintos sitios remotos, obtenidos estadísticamente.

Ubicación	Red Interna (Kbps)	Internet (Kbps)	Utilizado (Kbps)	Capacidad del Enlace (Kbps)
Aeropuerto	2,8	130	132,8	2048
Beaterio	205	970	1175	4096
Corazón	15,5	550	565,5	2048
Faisanes	6,8	500	506,8	2048
Oyambaro	72	310	382	2048
Gasolinera	4,5	760	764,5	2048
Santo Domingo	22	1050	1072	2048
Matriz	-	2400	-	-
TOTAL	**328,6**	**6700**	**4598,6**	**-**

Tabla 3.1 Capacidad utilizada de los enlaces

Además de los datos estadísticos de los sitios remotos es necesario tomar en cuenta la línea de acceso a los servidores PCO1 y PCO8, con calidad de servicio Ignore QoS, como se muestra en la figura 3.3.

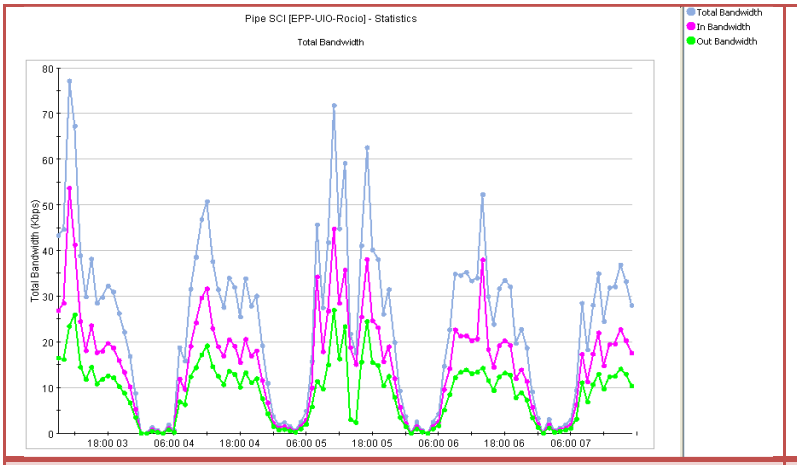
	**Consumo de AB Máximo (Kbps)**	**Capacidad del Canal (AB en Kbps)**
Red Interna Total (color azul)	80	2048
Red Interna salida (color verde)	28	2048
Red Interna entrada (color rosado)	54	2048

Figura 3.3 Acceso a servidores PCO1 y PCO8

Debido a que las aplicaciones de facturación que corren en los servidores PCO1 y PCO8, son accesados desde el nodo Gasolinera se tendrá un consumo en la red interna de 54 Kbps, y un consumo total de 818,5 Kbps en este nodo.

Los enlaces a dimensionar se indican en la tabla 3.2:

ENLACE
MATRIZ – PICHINCHA
MATRIZ – ATACAZO
PICHINCHA - ATACAZO
PICHINCHA – AEROPUERTO
PICHINCHA - BEATERIO
PICHINCHA – GASOLINERA
ATACAZO – CORAZÓN
ATACAZO – FAISANES
ATACAZO – STO. DOMINGO
ATACAZO – OYAMBARO

Tabla 3.2 Enlaces considerados para el cálculo de capacidad requerida

3.2.1.1. Capacidad utilizada en Cerro Pichincha

Para determinar la capacidad del enlace desde la matriz al cerro Pichincha, se lo realiza estadísticamente, utilizando la herramienta ALLOT, se crea una línea que contenga todo el tráfico hacia el cerro Pichincha (Gasolinera, Aeropuerto, Beaterio), tal como se lo muestra en la figura 3.4.

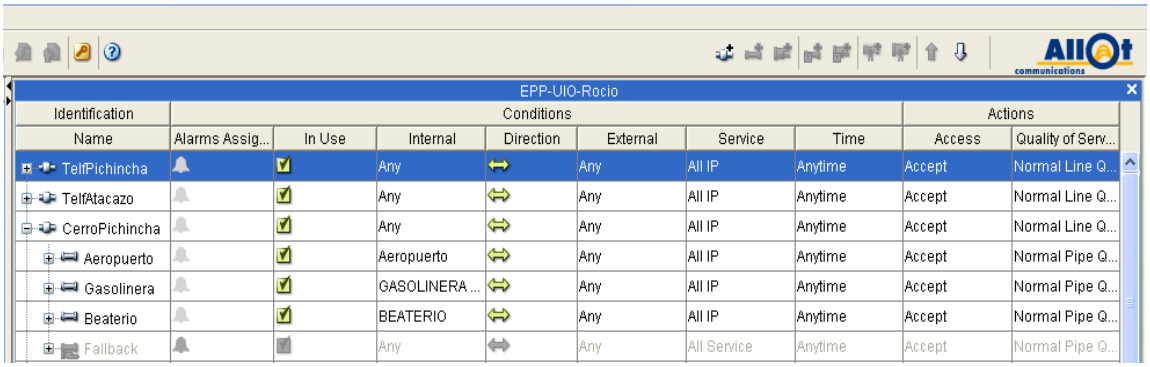


Figura 3.4 Línea creada en ALLOT para determinar la capacidad Cerro Pichincha

En la figura 3.5 se indica el ancho de banda total consumido por el enlace del Cerro Pichincha.

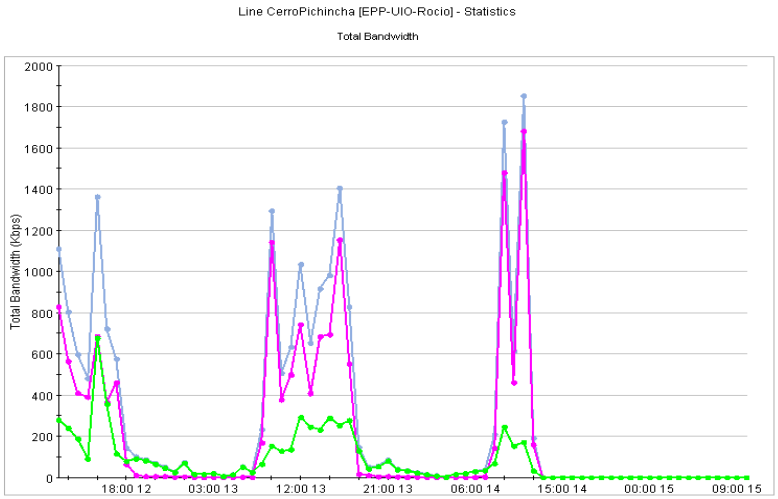


Figura 3.5 Capacidad Utilizada en Cerro Pichincha

Del gráfico se determina que el pico máximo correspondiente al tráfico de entrada es de 1721.2 Kbps

3.2.1.2. Capacidad utilizada en Cerro Atacazo

Para determinar la capacidad del enlace desde la matriz al cerro Atacazo, se lo realiza estadísticamente, utilizando la herramienta ALLOT, se crea una línea que contenga todo el tráfico hacia el cerro Atacazo (Corazón, Faisanes, Oyambaro, Santo Domingo), dicha línea se indica en la figura 3.6.

Beaterio		BEATERIO		Any	All IP	Anytime	Accept	Normal Pipe Q..
Fallback		Any		Any	All Service	Anytime	Accept	Normal Pipe Q..
CerroAtacazo		Any		Any	All IP	Anytime	Accept	Normal Line Q..
Corazon		Corazon		Any	All IP	Anytime	Accept	Normal Pipe Q..
Faisanes		Faisanes		Any	All IP	Anytime	Accept	Normal Pipe Q..
Oyambaro		OYAMBARO		Any	All IP	Anytime	Accept	Normal Pipe Q..
SantoDoming		SANTO DOMIN...		Any	All IP	Anytime	Accept	Normal Pipe Q..
Fallback		Any		Any	All Service	Anytime	Accept	Normal Pipe Q..
GALAPAGOS 1		Any		Any	All IP	Anytime	Accept	1024K Mx p4
IGNOREQoS		Any		Any	All IP	Anytime	Accept	Normal Line Q..

Figura 3.6 Línea creada en ALLOT para determinar la capacidad Cerro Atacazo

En la figura 3.7 se indica el ancho de banda total consumido por el enlace del Cerro Atacazo.

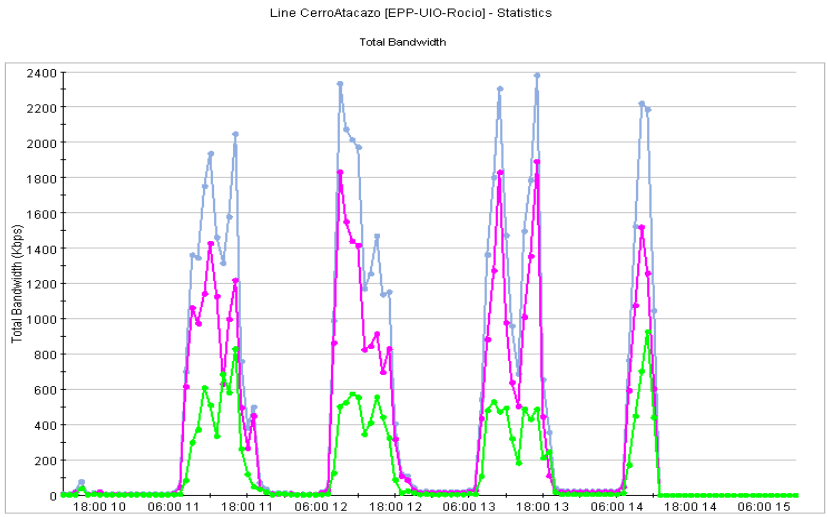


Figura 3.7 Capacidad Utilizada en Cerro Atacazo

Del gráfico se determina que el pico máximo correspondiente al tráfico de entrada es de 1935.2 Kbps

3.2.1.3. Capacidad Simultánea de los Cerro Pichincha y Cerro Atacazo

Debido al diseño lógico propuesto en la reestructuración de la red WAN, en donde se plantea formar un anillo entre los 3 nodos (Pichincha, Atacazo y Matriz), es necesario que en caso que uno de los enlaces de los Cerros hacia la Matriz falle, el otro soporte la demanda de tráfico de todos los nodos, para lo cual se determina la demanda simultánea de los dos enlaces, creando en el programa Allot una línea que contenga éste tráfico (Figura 3.8).

EPP-UIO-Rocio

Identification	Conditions							Actions	
Name	Alarms Ass...	In Use	Internal	Direction	External	Service	Time	Access	Quality of S...
Cerros_Pichincha_Atacazo		☑	Any	⇔	Any	All IP	Anytime	Accept	Normal Line...
Beaterio		☑	BEATERIO	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Aeropuerto		☑	Aeropuerto	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Gasolinera		☑	GASOLINER...	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Sto Domingo		☑	SANTO DOMI...	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Faisanes		☑	Faisanes	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Corazon		☑	Corazon	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Oyambaro		☑	OYAMBARO	⇔	Any	All IP	Anytime	Accept	Normal Pipe...
Fallback		☐	Any	⇔	Any	All Service	Anytime	Accept	Normal Pipe...

Figura 3.8 Línea creada en Allot del tráfico de todos los nodos

En la figura 3.9 se indica el ancho de banda total consumido por los Cerros Pichincha y Atacazo.

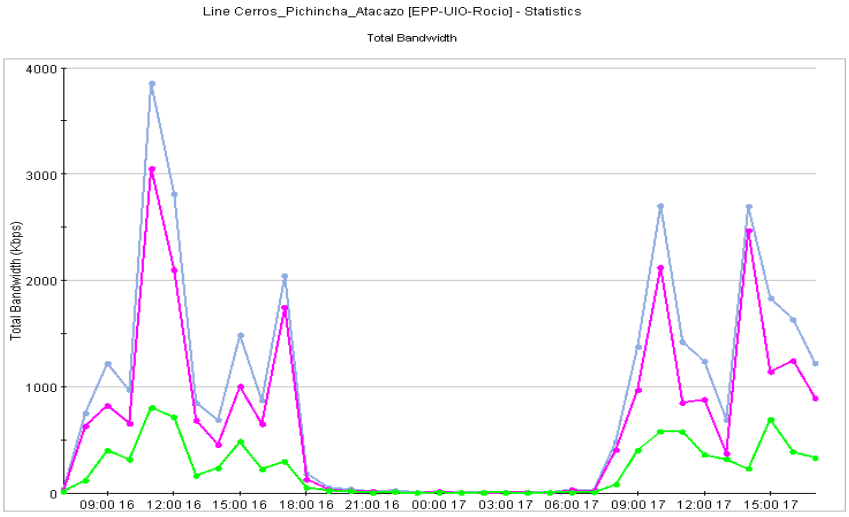


Figura 3.9 Capacidad Utilizada en los Cerros Pichincha y Atacazo en simultáneo

Del gráfico obtenemos un pico máximo debido al tráfico de entrada de 3152.2 Kbps.

3.2.1.4. Consumo de Ancho de Banda de Aplicaciones de uso no frecuente

La principal aplicación de uso no frecuente y que consume considerablemente recursos de ancho de banda, es la videoconferencia, además de que se debe tomar en cuenta que cada vez tiene más aceptación y utilización por parte de los usuarios.

La solución instalada en la red para el uso de videoconferencia, se la da con equipos Polycom, que trabaja bajo el estándar H.323, utilizando anchos de banda de 512 kbps, consiguiendo una calidad de imagen y sonido aceptables.

Los equipos de videoconferencia se encuentran instalados en los nodos: Beaterio (2 equipos), Sto. Domingo (1 equipo), Oyambaro (1 equipo) y Matriz (3 equipos). Se debe considerando que la planificación a futuro es cubrir todos los sitios remotos con equipos de Video Conferencia.

3.2.2. CAPACIDAD DE LOS ENLACES REQUERIDA

Debido a que en la capacidad monitoreada de los anchos de banda a los sitios remotos, está incluido el consumo de telefonía, y que se mantendrá el códec que se utiliza en la red, para determinar el ancho de banda necesario se utiliza la siguiente fórmula:

- *C(requerida)= C(utilizada)+ C(aplicaciones de uso no frecuente)*

3.2.2.1. Enlaces a sucursales

Para la tabla 3.3 se considera un crecimiento del 10 % de la capacidad utilizada actual (tomada de la tabla 3.1 del subcapítulo *3.2.1 CAPACIDAD UTILIZADA DE LOS ENLACES*). No se considera crecimiento para videoconferencia debido a que el consumo de ancho de banda es constante.

Ubicación	Utilizada (Kbps)	Uso no frecuente (Kbps)	Total (Kbps)	Enlace Necesario(Mbps)
Aeropuerto	132,8	512	673,37	1
Beaterio	1175	512	1687	2
Corazón	565,5	512	1194	1
Faisanes	506,8	512	1074,54	1
Oyambaro	382	512	1014,7	1
Gasolinera	818,5	512	1412,35	2
Santo Domingo	1072	512	1768,2	2

Tabla 3.3 Capacidad de los Enlaces Requerida en las Sucursales

3.2.2.2. Enlaces a Matriz

Para el cálculo de los enlaces a Matriz se tomó el dato obtenido del gráfico 3.9, debido a las consideraciones del punto 3.2.1.3 Capacidad Simultánea de los Cerro Pichincha y Cerro Atacazo, además se asume un 10% de crecimiento y una simultaneidad de 2 videoconferencias para los enlaces de los cerros hacia la Matriz, dando como resultado la tabla 3.4.

Ubicación	Utilizada (Kbps)	Capacidad Requerida para cierre de anillo (Kbps)	Videoconferencia (Kbps)	Total (Kbps)	Enlace Necesario (Mbps)
Enlace Pichincha	1721.4	3152.2	1024	4491.4	5
Enlace Atacazo	1.935.2	3152.2	1024	4491.4	5

Tabla 3.4 Capacidad de los Enlaces Requerida en los cerros Pichincha y Atacazo

3.2.2.3. Enlace Pichincha – Atacazo

Debido a que este enlace cerrará el anillo entre los 3 nodos (Pichincha, Atacazo y Matriz), éste deberá soportar en el peor de los casos, el tráfico del enlace de mayor consumo actual los cerros y la matriz (tabla 3.4), en este caso será el enlace Matriz – Atacazo.

Se asume un 10% de crecimiento y una simultaneidad de 2 videoconferencias para los enlaces de los cerros hacia la Matriz, obteniéndose la tabla 3.5.

Ubicación	Utilizada (Kbps)	Videoconferencia (Kbps)	Total (Kbps)	Enlace Necesario(Mbps)
Enlace Pichincha - Atacazo	1.935.2	1024	3152.72	3

Tabla 3.5 Capacidad del Enlace Requerida en los cerros Pichincha y Atacazo.

3.3. ÍNDICE DE SIMULTANEIDAD PARA TELEFONÍA

Para establecer los recursos necesarios para el transcoding en la red WAN, se debe precisar el índice de simultaneidad actual de llamadas de los nodos que se enlazan hacia el cerro Pichincha y Atacazo.

Para determinar el ancho de banda necesario en los enlaces, se requiere indicar además del ancho de banda utilizado, el consumo requerido por la telefonía. El códec que se utiliza en la WAN es G.729, con una tasa de transferencia de 8 Kbps sin cabeceras, la tasa de transferencia incluidos cabeceras se muestra en la tabla 3.6.

Codificador	Configuración del Codificador	Muestras de Voz	PPS	AB VoIP (Kbps)	Retraso Suavizado
G.723.1	5.3 K 5.3KB	1 2	33 17	14.25 10.06	40 - 300
G.723.1	6.3 K 6.3KB	1 2	33 17	15.31 11.15	40 – 300
G.729A	8GKB 8GKB3 8GKB4	2 3 4	50 33 25	21.6 16.89 14.80	40 - 300

	8GKB5	5	20	13.44	
CVSELP	8K 8KB	1 2	50 25	21.6 14.8	40 – 150
CVSELP	16K 16KB	1 2	50 25	29.6 22.8	40 – 150

Tabla 3.6 Ancho de Banda consumido por los códec en los equipos Motorola Vanguard[24]

3.3.1. CERRO PICHINCHA

Para determinar la capacidad del enlace desde la Matriz al cerro Pichincha utilizado por telefonía, se lo realiza estadísticamente, utilizando la herramienta ALLOT, se debe crear una línea que contenga todo el tráfico hacia el cerro Pichincha (Gasolinera, Aeropuerto, Beaterio), filtrándolo para obtener sólo el tráfico entre los ruteadores Vanguard. En la figura 3.10 se indica el ancho de banda consumido por la telefonía en el cerro Pichincha

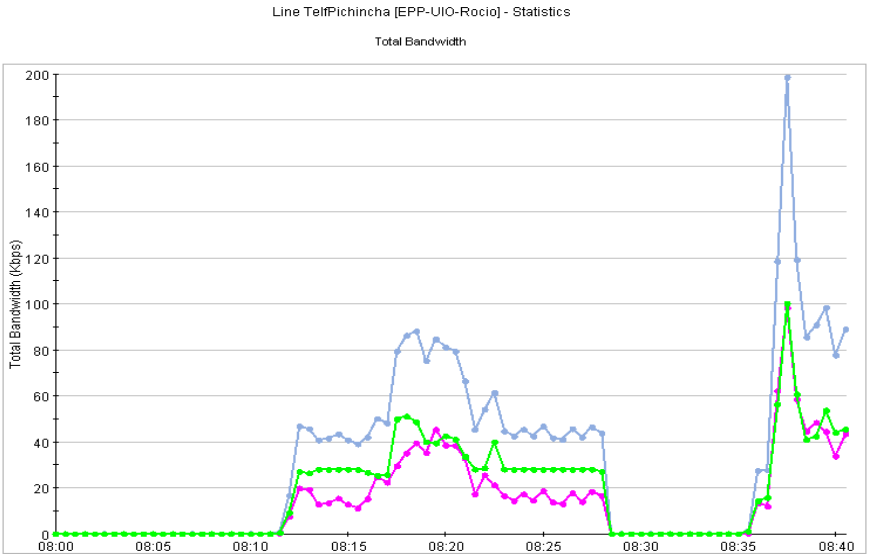


Figura 3.10 Consumo de telefonía en el Cerro Pichincha

Del gráfico se determina que existen picos de 202,6 Kbps.

[24] Vanguard Foundation Course, Folleto Euipo Motorola Vanguard (Anexo 7)

3.3.1.1. Simultaneidad de Telefonía Pichincha

Del manual de los equipos Vanguard se obtiene la utilización del códec G.729 incluido cabeceras es de 16,89 Kbps (Tabla 3.6).

Del pico de capacidad de la figura 3.10, se divide para 2, debido a que se muestra el tráfico en los sentidos, y este valor dividido para la tasa de trasferencia del códec G.729 incluyendo cabeceras.

$$i = \frac{202,6}{2 \text{ x } 16,89}$$

$$i = 6$$

Por tanto se tiene una simultaneidad de 6 llamadas.

3.3.2. CERRO ATACAZO

Para determinar la capacidad del enlace desde la Matriz al cerro Atacazo utilizado por telefonía, se lo realiza estadísticamente, utilizando la herramienta ALLOT, se debe crear una línea que contenga todo el tráfico hacia el cerro Atacazo (Corazón, Faisanes, Oyambaro, Santo Domingo), filtrándolo para obtener solo el tráfico entre los equipos de enrutamiento Vanguard.

En la figura 3.11 se indica el ancho de banda consumido por la telefonía en el cerro Atacazo.

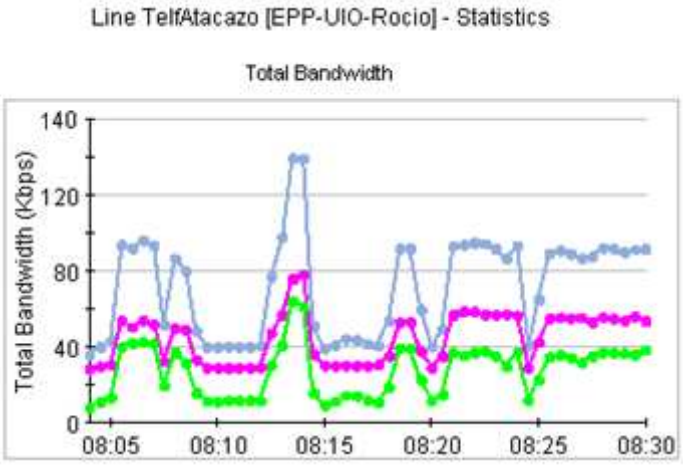


Figura 3.11 Consumo de telefonía en el Cerro Atacazo

Del gráfico se determina que existen picos de 129,7 Kbps.

3.3.2.1. Simultaneidad de Telefonía Atacazo

Del pico de capacidad de la figura 3.11, se divide para 2 debido a que se muestra el tráfico en los dos sentidos y este valor dividido para la tasa de trasferencia del códec G.729 incluyendo cabecera, se tiene el número de llamadas simultaneas.

$$i = \frac{129,7}{2 \text{ x } 16,89}$$

$$i = 4$$

Por tanto se tiene una simultaneidad de 4 llamadas.

3.4. DIRECCIONAMIENTO

El direccionamiento de la reestructuración de la red de PETROCOMERCIAL se realizará a partir de una dirección de red privada clase B, la cual se dividirá en subredes, cada una de las cuales dispondrá de dos direcciones IP válidas para ser asignadas a cada enlace WAN a diseñarse.

3.4.1. DIRECCIONAMIENTO WAN

El direccionamiento WAN se asignará, de acuerdo a la nueva topología lógica, en los nuevos ruteadores de borde ubicados en los nodos especificados para el presente Proyecto de Titulación (Aeropuerto, Beaterio, Corazón, Gasolinera, Faisanes, Oyambaro, Matriz y Sto. Domingo) y en las interfaces de switches de capa 3 ubicados en los dos puntos concentradores de la topología en estrella (Atacazo y Pichincha). Además el direccionamiento del enlace entre los cerros Pichincha y Atacazo.

Para el direccionamiento de los enlaces WAN se utilizará la red 172.20.35.0, la cual va a ser subneteada con máscara de 30 bits.

Cabe indicar que el direccionamiento de las LAN de cada nodo es el mismo que el explicado en el capítulo anterior (*2.2.3.2. Direccionamiento Sucursales*.)

3.4.1.1. Router Matriz

Al router a colocarse en el nodo Matriz se le va a asignar dos direcciones IP pertenecientes a dos subredes diferentes, una para cada enlace WAN con los puntos Pichincha y Atacazo respectivamente.

El nodo Matriz es un punto crítico en la red y cuenta con el mayor número de usuarios y aplicaciones críticas, el router ubicado en Quito va a servir como un punto de interconexión entre la red LAN de la Matriz y los nodos remotos (Aeropuerto, Beaterio, Corazón, Gasolinera, Faisanes, Oyambaro y Sto. Domingo), por lo cual va estar conectados a los switches en Atacazo y Pichincha.

En la tabla 3.7 se detalla el direccionamiento asignado a los enlaces entre el router Matriz (Quito) y los puntos concentradores Atacazo y Pichincha.

DIRECCIONAMIENTO RED WAN				
Enlace	**Red**	**Máscara**	**Quito**	**Sucursal**
Quito-Atacazo	172.20.35.60	255.255.255.252	172.20.35.62	172.20.35.61
Quito-Pichincha	172.20.35.12	255.255.255.252	172.20.35.14	172.20.35.13

Tabla 3.7 Direccionamiento WAN enlaces entre Quito y puntos centrales de la red

Cabe destacar que este dispositivo de ruteo tiene asignado una dirección de la red LAN de la Matriz para la vlan 1 de datos y administración y de la red de telefonía para la vlan 1001 de voz, estas direcciones IP se muestran en la tabla 3.8.

QUITO		
Interfaz Vlan	**Dirección IP**	**Máscara**
1	172.20.64.14	255.255.248.0
1001	172.10.64.4	255.255.255.0

Tabla 3.8 Direcciones IP de Vlans ruteador Quito

3.4.1.2. Switch Atacazo

Uno de los dos nuevos puntos concentradores en la topología lógica planteada en el Proyecto de Titulación es el Cerro Atacazo, debido al número de puertos que debe soportar para la conexión con los demás nodos, es conveniente el uso de un switch de capa 3.

Debido a la ubicación geográfica, se ha dividido a los nodos en dos grupos, un grupo conectado al switch en Atacazo y el otro grupo conectado al switch en Pichincha. Los nodos que van a ser conectados al switch Atacazo son: Corazón, Faisanes, Oyambaro y Sto. Domingo.

En la tabla 3.9 se describe el direccionamiento WAN del switch Atacazo con sus Nodos conectados directamente.

DIRECCIONAMIENTO RED WAN				
Enlace	**Red**	**Máscara**	**Atacazo**	**Sucursal**
Atacazo - Corazón	172.20.35.40	255.255.255.252	172.20.35.41	172.20.35.42
Atacazo - Faisanes	172.20.35.64	255.255.255.252	172.20.35.65	172.20.35.66
Atacazo - Oyambaro	172.20.35.32	255.255.255.252	172.20.35.33	172.20.35.34
Atacazo – Sto. Domingo	172.20.35.52	255.255.255.252	172.20.35.53	172.20.35.54
Atacazo - Pichincha	172.20.35.68	255.255.255.252	172.20.35.69	172.20.35.70

Tabla 3.9 Direccionamiento WAN de los enlaces entre los nodos y Atacazo

3.4.1.3. Switch Pichincha

Como se explicó en el anterior subcapítulo (Switch Atacazo), debido al número de puertos que deben soportar cada punto concentrador de la nueva topología lógica planteada en el Proyecto de Titulación, es útil en el cerro Pichincha el uso de un switch de capa 3.

Los nodos a ser conectados al equipo ubicado en el cerro Pichincha serán: Aeropuerto, Gasolinera y Beaterio.

En la tabla 3.10 se indica el direccionamiento asignado a los enlaces.

DIRECCIONAMIENTO RED WAN				
Enlace	**Red**	**Máscara**	**Pichincha**	**Sucursal**
Pichincha - Aeropuerto	172.20.35.8	255.255.255.252	172.20.35.10	172.20.35.9
Pichincha - Beaterio	172.20.35.0	255.255.255.252	172.20.35.1	172.20.35.2
Pichincha - Gasolinera	172.20.35.4	255.255.255.252	172.20.35.5	172.20.35.6
Pichincha - Atacazo	172.20.35.68	255.255.255.252	172.20.35.70	172.20.35.69

Tabla 3.10 Direccionamiento WAN de los enlaces entre los nodos y Pichincha.

3.4.2. PROTOCOLO DE ENRUTAMIENTO

Debido a la extensa red de PETROCOMERCIAL y a las múltiples subredes de direcciones IP, además del constante crecimiento de aplicaciones y por ende de subredes (lo que ocasiona una red con cambios constantemente), se hace necesaria la implementación de un protocolo de enrutamiento entre los diferentes routers que conforman la red.

En cuanto a los protocolos de enrutamiento que podemos usar para la configuración de los equipos a ser implementados, tenemos varias alternativas a ser seleccionadas.

Inicialmente, debido al tamaño de la red, es necesaria la implementación de un protocolo dinámico, el cual nos facilitaría en gran manera la configuración del enrutamiento. Establecido este primer requerimiento, ahora debemos discriminar entre un protocolo de puerta de enlace interior (IGP) y un protocolo de puerta de enlace exterior (EGP).

Debido que los dispositivos de enrutamiento, se encuentran en un mismo sistema autónomo, se va a elegir a un protocolo de enrutamiento de puerta de enlace interior (IGP), teniendo dentro de esta categoría varios tipos de protocolos.

Los dos grandes grupos de protocolos del tipo IGP son los protocolos por vector distancia y los protocolos de enrutamiento por estado de enlace. Al escoger algún protocolo de enrutamiento de uno de los dos grupos vamos a tener ventajas y desventajas de unos sobre los otros. Por lo que se escogió un protocolo híbrido que nos brinda lo mejor de los dos grupos, tanto de los protocolos por vector distancia como de los protocolos de enrutamiento por estado de enlace.

Por lo que el protocolo seleccionado para realizar el enrutamiento entre los routers y switches de capa 3 es EIGRP. Como se mencionó en capítulos anteriormente EIGRP

combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector de distancia, entre las razones por las que se escogió este protocolo tenemos:

- *Soporte para VLSM y CIDR*

A diferencia de otros protocolos como RIP versión 1, al usar el protocolo EIGRP nos brinda soporte para VLSM y CIDR, lo que representa una ventaja en la red de PETROCOMERCIAL, ya que sus diferentes subredes utilizan máscara variable.

- *Routers EIGRP convergen rápidamente por DUAL.*

Al tener una red extensa en PETROCOMERCIAL, es crítico que se utilice un algoritmo de enrutamiento en el cual sus tiempos de convergencia no sean altos, en caso de falla de alguno de los equipos, o en un cambio de la topología, es esencial que la red este operativa lo más pronto posible. EIGRP gracias a la utilización de DUAL permite una rápida convergencia en la red, esto lo puede hacer debido a que propaga rápidamente los cambios en el estado de los enlaces, como lo hace OSPF, pero con menos overhead, además de contar con una ruta de respaldo (siempre que sea posible).

- *Eficiente uso del ancho de banda.*

En las redes empresariales como la de PETROCOMERCIAL, un factor importante que siempre hay que tener en cuenta es el uso del ancho de banda, este factor no solamente tiene que ver con el consumo de las aplicaciones de la empresa o el uso del internet, sino también con la utilización del ancho de banda por parte de los protocolos de enrutamiento. Al utilizar protocolos de enrutamiento que consuman un significativo ancho de banda pueden provocar congestión innecesaria de la red. EIGRP, hace uso eficiente del ancho de banda, lo cual lo realiza mediante actualizaciones de enrutamiento que sólo se envían cuando se produce un cambio en la topología.

3.5. DIMENSIONAMIENTO DE EQUIPOS

3.5.1. ROUTERS

3.5.1.1. Características

Los equipos deben ser modulares, para crecimiento en interfaces de red y módulos de servicios especiales a nivel de hardware y de funciones especiales a nivel de software.

Como se detalló en el *punto 3.4.2* el protocolo de enrutamiento que se manejará es EIGRP, pero el equipo debe soporta adicional a éste protocolo, OSPF, que será necesario en el caso de cambiar de protocolo de enrutamiento o para permitir integrarse con equipos que no sean CISCO.

En el siguiente capítulo se realizará un modelo de Gestión para los routers para lo cual deberán soportar SNMP versión 1, 2c y 3 además de soportar RMON en las versiones I y II.

Para la comunicación entre los routers de borde y los radios Harris es necesario una comunicación Ethernet a 100 Mbps, por lo que el protocolo requerido sería IEEE 802.3u (Fast Ethernet). En los terminales en los que existe switches 3 COM no administrables, es conveniente reemplazarlos a través de una tarjeta que funcione como switch en los routers, esta deberá soportar el estándar de POE 802.3 af para alimentar teléfonos IP.

Deberá soportar 802.1q, para soporte de VLANS existente en las redes locales.

Deberá tener fuente redundante para asegurar el funcionamiento del equipo en caso de fallas de la fuente.

Para el cálculo del performance en el peor de los casos, se calcula en base a la utilización de los 3 puertos en modo dúplex, dos de ellos a la capacidad de los enlaces de radio requeridos (3E1 = 6144 Kbps), y uno a la velocidad del enlace de la red LAN (100 Mbps), por lo que siendo n el throughput y el peor de los casos se da cuando transmiten los 3 puertos en simultáneo:

$$n = \frac{(100000000 + 6144000 + 6144000) \text{ x } 2}{8 \text{ x } 64}$$

$$n = 0{,}438\ Mpps$$

Una de las ideas del presente Proyecto de Titulación es aprovechar el hardware de los routers para proporcionar servicios adicionales, bajo el concepto de servicios integrados, el principal servicio que se necesita actualmente es el de telefonía IP, por lo que todos los equipos deben soportar:

- Servicio de central telefónica IP para registro de teléfonos y procesamiento de llamadas.
- Servicio de mensajería de voz, integrable a cuentas de correo.

Además deberá soportar futuros servicios adicionales por módulos de hardware o upgrade del equipo como:

- Servicio de grabación y controladora de cámaras IP.
- Servicio de compresión de paquetes para reducciones de ancho de banda.

Se requiere que los equipos adquiridos además de las funcionalidades de manejar tráfico de datos, tenga funcionalidades de centrales telefónicas IP.

Los routers deberán soportar protocolos de señalización SIP, H.323 y protocolos propietarios de la central. Además deberán soportar la migración a configuración de

un sistema de supervivencia remoto con visión a futuro de adquirir una central dedicada de mayores prestaciones.

Los requerimientos para telefonía se muestran en la tabla 3.11:

Descripción	Matriz	Beat.	Sto. Domin.	Oyamba.	Gasol.	Aerop.	Corazón	Faisan
Líneas CNT	28	22	12	1	2	1	0	0
E1 CNT	1	0	0	0	0	0	0	0
Bases Celulares	0	0	0	0	0	0	0	0
Fax existentes	14	7	6	2	2	1	1	1
Extensiones IP	160	42	30	0	0	0	0	0
Extensiones Analógicas	25	50	27	5	15	2	2	2

Tabla 3.11 Requerimiento Telefonía PETROCOMERCIAL

Un códec que mantiene la calidad de la voz en niveles aceptables y reduce considerablemente el ancho de banda utilizado es g.729, que ocupa 8 Kbps sin cabeceras, por lo que se recomienda mantener el códec utilizado en la red WAN.

A nivel de LAN en las distintas sucursales y debido a la capacidad disponible no es inconveniente usar el códec g.711.

Debido al manejo de distintos códecs en los routers es necesario un recurso adicional que realice el transcoding. Para poder realizar llamadas entre teléfonos registrados en diferentes routers por lo que los equipos deben contar con módulos de procesamiento digital de señal integrado en hardware (Digital Signal Processor).

En la tabla 3.12 se muestra el número de extensiones IP que deben manejar los routers, se toma en cuenta un 10 por ciento de crecimiento.

Descripción	Matriz	Beaterio	Sto. Domingo	Oyambaro	Gasolinera	Aeropuert	Corazón	Faisanes
Extensiones IP	204	101	63	6	17	3	3	3

Tabla 3.12 Requerimientos extensiones IP

3.5.1.2. Tarjetería

3.5.1.2.1. Telefonía Analógica

Para la tarjetería FXO y FXS (son necesarias para líneas de CNT y faxes) se toma en cuenta un crecimiento en promedio del 10% y que para las sucursales Matriz, Beaterio y Santo Domingo se requieran tarjetas E1 para la migración de las líneas analógicas de CNT, los requerimientos de tarjetería de los routers se indican en la tabla 3.13:

Descripción	Matriz	Beaterio	Sto. Domingo	Oyambaro	Gasolinera	Aeropuerto	Corazón	Faisanes
FXO	-	-	-	2	3	2	0	0
FXS	16	8	7	3	3	2	2	2
E1	2	1	1	0	0	0	0	0

Tabla 3.13 Requerimientos de tarjetería de los routers

3.5.1.2.2. Transcoding

Los requerimientos para transcoding se calculan en base a las llamadas simultáneas obtenidas estadísticamente, debido a que serán las que necesitan un trascoding de G.711 a G.729, por tanto:

Cerro Pichincha

$$n = \frac{\text{Número de llamadas simultáneas}}{\text{Número total de extensiones}(\text{Beaterio} + \text{Gasolinera} + \text{Aeropuerto})}$$

$$n = \frac{6}{(92 + 15 + 2)} = 0{,}06$$

Cerro Atacazo

$$n = \frac{\text{Número de llamadas simultáneas}}{\text{Número total de extensiones}(\text{Sto. Domingo} + \text{ Oyambaro} + \text{ Corazón} + \text{Faisanes})}$$

$$n = \frac{4}{(57 + 5 + 2 + 2)} = 0{,}06$$

Multiplicando el factor de simultaneidad por el número de extensiones telefónicas se obtienen el número de llamadas simultáneas a la WAN que necesitarán recursos de transcoding.

Los canales de transcoding se indican en la tabla 3.14.

Descripción	Matriz	Beaterio	Sto. Domingo	Oyambaro	Gasolinera	Aeropuert	Corazón	Faisanes
Canales de transcoding	15	6	4	1	1	1	1	1

Tabla 3.14 Requerimientos Transcoding

3.5.1.2.3. Mensajería de Voz

Todos los routers deben contar con una tarjeta que permita manejar la funcionalidad de mensajería de voz con un soporte igual al número de extensiones IP en la matriz y cada sucursal.

3.5.2. SWITCHES

3.5.2.1. Características

Debido a los requerimientos de enrutamiento de los switches deben tener funcionalidades de capa 3 y soportar como se detalló en el punto 3.4.2 el protocolo de enrutamiento EIGRP, además de los protocolos RIP v2, OSPF, que serán necesarios en el caso de cambiar de protocolo de enrutamiento o para permitir integrarse con equipos que no sean CISCO.

La densidad de puertos que se utilizará en los switches será de 4 y 5 puertos en los switches Pichincha y Atacazo, y debido a que son puntos de concentración críticos, se necesitarán switches de 24 puertos con soporte a Ethernet a 100 Mbps IEEE 802.3 u (Fast Ethernet).

Deberá soportar 802.1q, para soporte de VLANS.

Debido al lugar de instalación de los switches (cerros Pichincha y Atacazo), deberán contar con alimentación DC, los mismos recibirán la energía través de los bancos de batería existentes, se utilizan bancos de batería y no UPS por el tiempo de consumo de energía que garantizan los mismo, que están en el orden de las decenas de horas mientras que los UPS en unidades de horas.

Para la capacidad de conmutación se realiza en base a los 24 puertos en modo full dúplex por lo tanto:

$$c = 100000000 \; x \; 24 \; x \; 2$$

$$c = 4{,}8 \; Gbps$$

Para el cálculo del performance en el peor de los casos, se calcula en base a la utilización de los 24 puertos en Fast Ethernet en modo dúplex por lo que siendo n el throughput y el peor de los casos se da cuando transmiten todos los puertos en simultáneo:

:

$$n = \frac{100000000 \text{ x } 24 \text{ x } 2}{8 \text{ x } (64 + 20)}$$

$$n = 7{,}14\ Mpps$$

3.6. MODELOS DE EQUIPOS

Se debe tomar en cuenta para escoger el modelo de equipos, además de los requerimientos, existe una política de la empresa de adquirir no más de dos modelos para un equipo, y como se explicó se necesita estandarizar la marca de equipos de networking.

3.6.1. ROUTERS CISCO 3845 Y 3825

Los equipos cuenta con dos interfaces 1000 base T y un modulo SFP, soportan 802.1q y los protocolos SNMP versión 1, 2 y 3 además de los estándares RMON I y II, son equipos modulares para permitir crecimiento, soporta los protocolos de enrutamiento EIGRP, RIP versión 1 y 2, OSPF, BGP, IS-IS.

Tiene un performance de 350 Kpps el modelo 3825 y 500 Kpps el modelo 3845.

La familia 3800 soporta el CME Bundle (Call Manager Express), solución de Cisco que permite integrar centrales telefónicas en los routers, permiten manejar los protocolos H.323, SIP y SSCP. El modelo 3845 tiene un soporte de 250 teléfonos IP, el modelo 3825 soporta 175 teléfonos. Además soportan el cambio a SRST sistema

de supervivencia remota, en el caso de centralizar el sistema de telefonía en una sola central de mayores capacidades.

Para el dimensionamiento de la memoria Flash se debe tomar en cuenta que información se guarda en la misma, entre las cuales se encuentra el IOS del Router que será el que más recursos consuma, el IOS tiene un tamaño aproximado de 50 Mbytes (c3845-advipservicesk9-mz.124-15.T12), además en la flash se guardan los archivos de configuración de los teléfonos, tonos, etc.

En la figura 3.12 se muestran los firmwares necesarios para los principales modelos de teléfonos.

- *ATA 186 ATA030100SCCP040211A.zup*
- *ATA 188 ATA030100SCCP040211A.zup*
- *7902G CP7902010200SCCP031023A.sbin*
- *7905G CP7905040000SCCP040701A.sbin and*
- *CP79050101SCCP030530B31.zup*
- *7910G+SW P00403020214.bin*
- *7912G CP7912040000SCCP040701A.sbin*
- *7914 S00103020002.bin*
- *7920 cmterm_7920.4.0-01-08.bin*
- *7935 P00503010100.bin*
- *7936 P00503010100.bin*
- *7940G P00303020214.bin or P00305000301.sbn*
- *7960G P00303020214.bin or P00305000301.sbn*

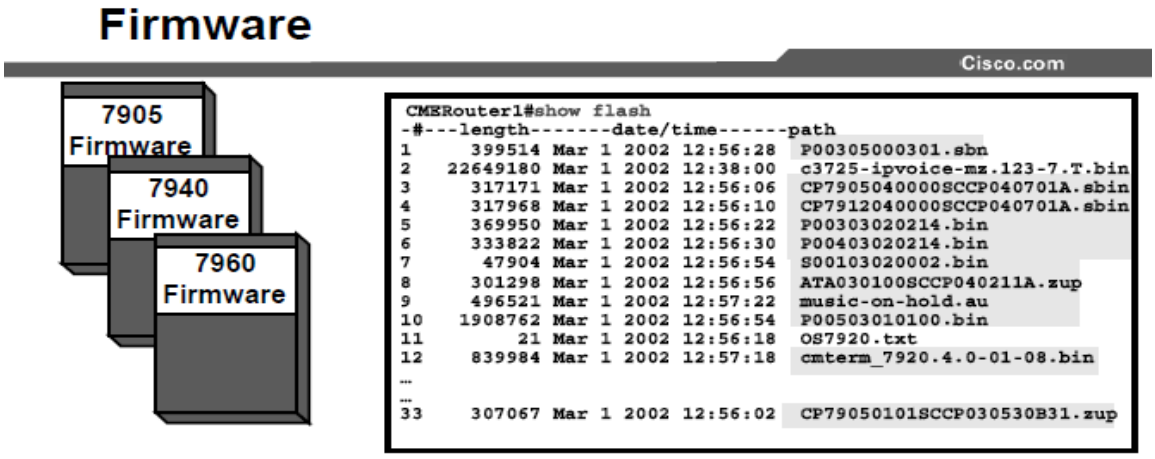


Figura 3.12 Firmware de los principales modelos de Teléfonos[25]

En la figura 3.13 se indica los firmwares necesarios para el funcionamiento de los modelos de teléfonos 7970G y 7971G-GE de la marca Cisco.

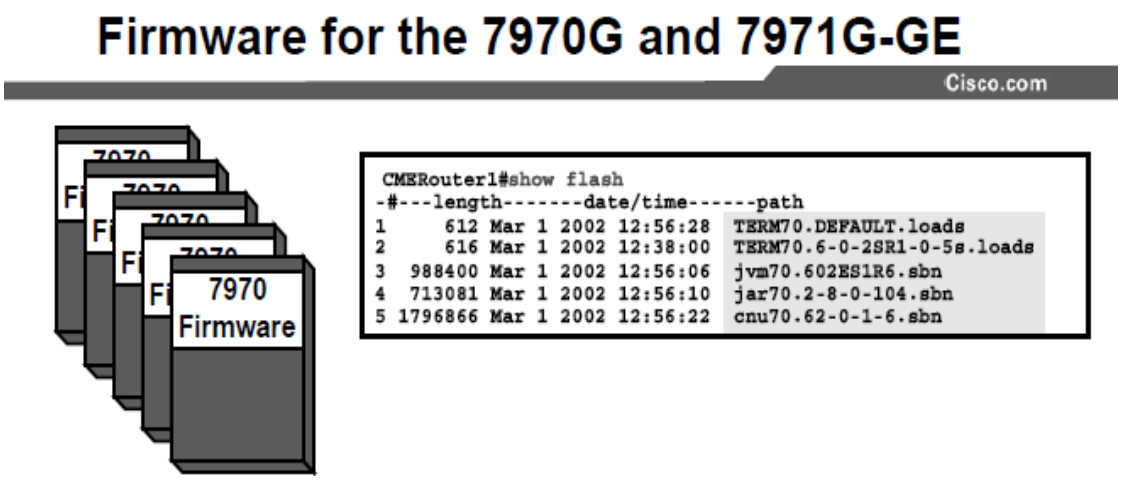


Figura 3.13 Firmware de los modelos de teléfonos 7970G y 7971G-GE[26]

En promedio los firmware ocupan un promedio de 10 Mbytes por modelo de teléfono si se manejan tres modelos de teléfonos ocuparían 30 Mbytes mas 50 Mbytes del IOS del router ocuparían una memoria de 80 Mbytes por lo que la memoria flash necesaria para los router sería de 128 Mbytes.

[25] Cisco, Student Guide IP Telephony Express, 2005
[26] Cisco, Student Guide IP Telephony Express, 2005

Cisco recomienda para aplicaciones de telefonía con 240 teléfonos y 720 extensiones, una memoria mínima de 64 Mbytes en flash y 256 en DRAM, se debe tomar en cuenta que los Routers correrán protocolos de enrutamiento dinámico por lo que necesitara más capacidad en DRAM por lo que el requerimiento de memoria DRAM en los routers será de 512 Mbytes.

3.6.1.1. Telefonía Analógica

En la tabla 3.15 se muestra el soporte para la tarjetería de la familia de router 3800, tanto para el modelo 3845 como 3825.

Cisco 3800 Series Features	Cisco 3825/3825-NOVPN	Cisco 3845/3845-NOVPN
Network-module slots: These slots can accommodate a standard network module, enhanced network module (NME), enhanced extended network module (NME-X), and high-density extension module (EVM-HD). The NME-X, when available, will have a wider form factor than the NME. You can combine two side-by-side NME slots to accommodate one double-wide network module (NMD) or when available, a double-wide enhanced extended network module (NME-XD).	• NM • NME • NME-X • NMD • NME-XD • EVM-HD	• NM • NME • NME-X • NMD • NME-XD • EVM-HD
Maximum number of network modules, NMEs, and NME-Xs supported	2	4
Maximum number of NMD/NME-XDs supported	1	2
Maximum number of EVM-HDs supported	1	2
Number of HWIC slots (These HWIC slots also support VICs, VWICs, and WICs.)	4	4
Number of fixed LAN ports (fixed RJ-45 port for 10/100/1000 connectivity)	2 Gigabit Ethernet (10/100/1000)	2 Gigabit Ethernet (10/100/1000)
Number of fixed Small Form-Factor Pluggable (SFP) ports (for SFP Gigabit Ethernet connectivity)	1	1
Number of AIM slots (for optional AIMs for offloading compute-intensive features)	2	2
Number of PVDM slots (for optional PVDM2s)	4	4
Number of USB 1.1 ports (for future use with USB flash memory, security tokens for secure Cisco IOS Software configuration distribution, and off-platform storage of VPN credentials)	2	2
Embedded VPN (hardware-based VPN encryption acceleration)	Yes*	Yes*
Number of console ports (up to 115.2 kbps)	1	1
Number of auxiliary ports (up to 115.2 kbps)	1	1
Memory: External Compact Flash and internal double-data-rate (DDR) synchronous dynamic RAM (SDRAM) with ECC**	• Default: 64-MB Compact Flash; 256-MB DDR SDRAM • Maximum: 512-MB Compact Flash; 1-GB DDR SDRAM	• Default: 64-MB Compact Flash; 256-MB DDR SDRAM • Maximum: 512-MB Compact Flash; 1-GB DDR SDRAM

Tabla 3.15 Soporte tarjetería Cisco 3845 y 382527

[27] Cisco, Folleto IP Telephony Express, 2005

3.6.1.1.1. Rocio (CISCO 3845)

El Router del nodo Rocío deberá contar con la siguiente tarjetería:

- Cisco High-Density Analog and Digital Extension Module for Voice and Fax con:
  - o EVM-HD-8FXS/DID 8 FXS para conexión de Faxes
  - o EVM-HD-8FXS/DID 8 FXS para conexión de Faxes

- VWIC2-2MFT-T1/E1 2 E1 para conexión con la CNT

3.6.1.1.2. Beaterio (CISCO 3825)

El Router del nodo Beaterio deberá contar con la siguiente tarjetería:

- VIC2-4FXS 4 FXS para conexión de faxes
- VIC2-4FXS 4 FXS para conexión de faxes

- VWIC2-1MFT-T1/E1 E1 para conexión con CNT

3.6.1.1.3. Santo Domingo (CISCO 3825)

El Router del nodo Santo Domingo deberá contar con la siguiente tarjetería:

- VIC2-4FXS 4 FXS para conexión de faxes
- VIC2-4FXS 4 FXS para conexión de faxes

- VWIC2-1MFT-T1/E1 E1 para conexión con CNT

3.6.1.1.4. Oyambaro (CISCO 3825)

El Router del nodo Oyambaro deberá contar con la siguiente tarjetería:

- VIC2-2FXO 2 FXO para conexión de líneas CNT
- VIC2-4FXS 4 FXS para conexión de faxes

3.6.1.1.5. Gasolinera (CISCO 3825)

El Router del nodo Gasolinera deberá contar con la siguiente tarjetería:

- VIC2-4FXO 4 FXO para conexión de líneas CNT
- VIC2-4FXS 4 FXS para conexión de faxes

3.6.1.1.6. Aeropuerto (CISCO 3825)

El Router del nodo Aeropuerto deberá contar con la siguiente tarjetería:

- VIC2-2FXO 2 FXO para conexión de líneas CNT
- VIC2-2FXS 2 FXS para conexión de faxes

3.6.1.1.7. Corazón y Faisanes (CISCO 3825)

Los Routers de los nodos Corazón y Faisanes deberán contar con la siguiente tarjetería:

- VIC2-2FXS 2 FXS para conexión de faxes

3.6.1.2. Transcoding

En la tabla 3.16 se muestra el soporte para el número de canales de transcoding según la complejidad para cada tarjetería

Name	Description*	Maximum Number of Channels in G.711	Maximum Number of Channels in High-Complexity Codecs	Maximum Number of Channels in Medium-Complexity Codecs
PVDM2-8	8-channel packet fax and voice DSP module	8	4	4
PVDM2-16	16-channel packet fax and voice DSP module	16	6	8
PVDM2-32	32-channel packet fax and voice DSP module	32	12	16
PVDM2-48	48-channel packet fax and voice DSP module	48	18	24
PVDM2-64	64-channel packet fax and voice DSP module	64	24	32

Tabla 3.16 Soporte tarjetería para transcoding serie 3800[28]

El códec que se manejará en la red WAN de PETROCOMERCIAL es G. 729 que es un códec de complejidad media. Además se debe considerar que el transcoding para un llamada se realiza en los dos sentidos por lo que los requerimientos mostrados en la Tabla 3.14 Requerimientos Transcoding, se duplican.

3.6.1.2.1. Rocío

El Router del nodo Rocío deberá contar con la siguiente tarjetería:

- PVDM2-64 Para 32 canales de transcoding (16 llamadas simultáneas).

3.6.1.2.2. Beaterio

El Router del nodo Beaterio deberá contar con la siguiente tarjetería:

- PVDM2-32 Para 16 canales de transcoding (8 llamadas simultáneas).

[28] Cisco, Studen Guide IP Telephony Express, 2005

3.6.1.2.3. Santo Domingo

El Router del nodo Santo Domingo deberá contar con la siguiente tarjetería:

- PVDM2-16 Para 8 canales de transcoding (4 llamadas simultáneas).

3.6.1.2.4. Oyambaro, Aeropuerto, Gasolinera, Corazón, Faisanes, Santo Domingo

Los routers deberán contar con la siguiente tarjetería:

- PVDM2-8 Para 4 canales de transcoding. (2 llamadas simultaneas)

3.6.1.3. Mensajería de Voz

En la tabla 3.17 se muestra el soporte de la tarjetería para mensajería de voz de la solución Cisco Unity Express.

	Cisco Unity Express Network Module (NME-CUE)			Cisco Unity Express Advanced Integration Module (AIM-CUE)		
License Level: Number of Mailboxes	GDMs	Hours of Storage	Concurrent Voicemail and Automated-Attendant Ports and Sessions	GDMs	Hours of Storage	Concurrent Voicemail and Automated-Attendant Ports and Sessions
12	5	300	8–24	5	14	6
25	10	300	8–24	10	14	6
50	15	300	8–24	15	14	6
100	20	300	8–24	Not supported		
150	25	300	8–24	Not supported		
200	25	300	8–24	Not supported		
250	25	300	8–24	Not supported		

Tabla 3.17 Soporte tarjetería CISCO 3800 para Transcoding29

Debido a que el número requerido de buzones de voz necesarios es igual al número de extensiones IP, la tarjetería y el licenciamiento es el siguiente.

[29] Cisco, IP Telephony Express, 2005

3.6.1.3.1. Rocío

El Router del nodo Rocío deberá contar con la siguiente tarjetería:

- NME-CUE Licenciado para 205 usuarios

3.6.1.3.2. Beaterio

El Router del nodo Beaterio deberá contar con la siguiente tarjetería:

- NME-CUE Licenciado para 105 usuarios

3.6.1.3.3. Santo Domingo

El Router del nodo Santo Domingo deberá contar con la siguiente tarjetería:

- NME-CUE Licenciado para 65 usuarios

3.6.1.3.4. Gasolinera

El Router del nodo GASOLINERA deberá contar con la siguiente tarjetería:

- AIM-CUE Licenciado para 20 usuarios

3.6.1.3.5. Oyambaro

El Router del nodo OYAMBARO deberá contar con la siguiente tarjetería:

- AIM-CUE Licenciado para 10 usuarios

3.6.1.3.6. Aeropuerto, Corazón, Faisanes

Los routers deberán contar con la siguiente tarjetería:

- AIM-CUE Licenciado para 5 usuarios

3.6.1.4. Tarjetería para Switch

Los routers que necesitan tarjetería para reemplazar los switches no administrables con los que cuentan, son AEROPUERTO, CORAZON y FAISANES, la tarjeta necesaria es:

- HWIC-D-9ESW-POE

3.6.2. SWITCH 3560-24TS-E

Los equipos cuentan con 24 interfaces 100 base T y cuatro módulos SFP, soportan 802.1q y los protocolos SNMP versión 1, 2 y 3 además de los estándares RMON I y II, soporta los protocolos de enrutamiento EIGRP, RIP V1 y 2, OSPF, BGP, IS-IS.

Debe contar con el sistema de alimentación redundante PWR-RPS2300 para permitir alimentación DC.

Cuentan con un MBTF 224,100 horas un Performance 6.5 Mpps y un backplane de 32 Gbps.

3.7. COSTO REFERENCIAL DEL PROYECTO

La idea del costo referencial del proyecto no es realizar un análisis de costo beneficio del mismo, sino dar una idea general del valor de los equipos del proyecto.

Los valores de los equipos son un promedio de los precio de lista de proveedores locales (DESCA, COMWARE, TOTALTEK).

3.7.1. CISCO ROCÍO

3845 VSEC Bundle with PVDM2-64, FL-CCME-250, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- Cisco High-Density Analog and Digital Extension Module for Voice and Fax con:
    - o EVM-HD-8FXS/DID 8 FXS para conexión de Faxes
    - o EVM-HD-8FXS/DID 8 FXS para conexión de Faxes

- VWIC2-2MFT-T1/E1 2 E1 para conexión con la CNT
- NME-CUE Licenciado para 205 usuarios
- Cisco Unity Express
- Cisco3845 redundant AC power supply

PRECIO= $ 28740

3.7.2. BEATERIO 3825

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- VIC2-4FXS 4 FXS para conexión de faxes
- VIC2-4FXS 4 FXS para conexión de faxes
- VWIC2-1MFT-T1/E1 E1 para conexión con CNT
- NME-CUE Licenciado para 105 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 23576

3.7.3. SANTO DOMINGO

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- VIC2-4FXS 4 FXS para conexión de faxes
- VIC2-4FXS 4 FXS para conexión de faxes
- VWIC2-1MFT-T1/E1 E1 para conexión con CNT
- NME-CUE Licenciado para 65 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 22176

3.7.4. GASOLINERA

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- VIC2-4FXO 4 FXO para conexión de líneas CNT
- VIC2-4FXS 4 FXS para conexión de faxes
- AIM-CUE Licenciado para 20 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 20689

3.7.5. OYAMBARO

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- VIC2-2FXO 2 FXO para conexión de líneas CNT
- VIC2-4FXS 4 FXS para conexión de faxes

- AIM-CUE Licenciado para 10 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 19189

3.7.6. AEROPUERTO

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- HWIC-D-9ESW-POE

- VIC2-2FXO 2 FXO para conexión de líneas CNT
- VIC2-2FXS 2 FXS para conexión de faxes

- AIM-CUE Licenciado para 5 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 17824

3.7.7. CORAZÓN

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- HWIC-D-9ESW-POE

- VIC2-2FXS 2 FXS para conexión de faxes
- AIM-CUE Licenciado para 5 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 17024

3.7.8. FAISANES

3825 VSEC Bundle with PVDM2-64, FL-CCME-175, Adv IP Serv, 128 MB Flash, 512 MB DRAM

- HWIC-D-9ESW-POE
- VIC2-2FXS 2 FXS para conexión de faxes
- AIM-CUE Licenciado para 5 usuarios
- Cisco Unity Express
- Cisco3825 redundant AC power supply

PRECIO= $ 17024

3.7.9. SWITCHES 3560-24TS-E

- **PRECIO= $ 5795**

3.7.10. COSTO TOTAL DEL PROYECTO

Se debe tomar en cuenta que los precios indicados son precios de lista de los que generalmente se obtiene un 25 al 30% de descuento.

Por lo que el costo aproximado del proyecto es de **$ 120.606** sin considerar impuestos.

3.8. PLAN DE MIGRACIÓN

Cuando se realiza algún cambio dentro de la topología de una red es necesario la realización de un plan de migración, para que el impacto de la implementación sea el menor posible. Un plan ordenado y detallado ayuda a que la operatividad de la red no sea afectada en gran medida, pudiendo resolver los problemas, si éstos sucedieran, de una manera más rápida.

3.8.1. ACTIVIDADES DE MIGRACIÓN

El presente subcapítulo describe las etapas que se consideran en el plan de migración, identificando las actividades que se deben efectuar.

3.8.1.1. Primera Etapa: Estudio

- Análisis de requerimientos
- Diseño de la nueva topología de la red
- Determinación de Direccionamiento
- Estudio de protocolos de enrutamiento más adecuado
- Análisis de equipos requeridos a ser instalados de acuerdo a la nueva topología
- Determinación de costos de equipos a ser instalados

3.8.1.2. Segunda Etapa: Pruebas

- Verificar la configuración propuesta
- Laboratorio de configuraciones routers Matriz, Aeropuerto y switch de capa 3 (Pichincha).
- Laboratorio de configuraciones routers Matriz, Corazón y switch de capa 3 (Atacazo).
- Backup de las configuraciones de todos los nodos a ser reemplazados.

Se escogió los nodos Aeropuerto y Corazón por ser los menos críticos.

3.8.1.3. Tercera Etapa: Instalación.

- Instalación de switch capa 3 en el cerro Pichincha.
- Instalación del router en nodo Matriz.
- Instalación de router en nodo Beaterio.
- Carga de configuraciones en los 3 puntos instalados.
- Configuración de protocolos de enrutamiento en switch de capa 3 Matriz y configuración de rutas estáticas Firewall Matriz.
- Conexión física de los equipos.
- Verificación de las nuevas configuraciones
- Detalle de incidentes y problemas
- Instalación de los routers en los nodos respectivos

3.8.1.4. Cuarta Etapa: Monitorización

- Verificación de las configuraciones
- Creación de Backups de las configuraciones
- Reporte de problemas post-instalación
- Monitorización de los equipos instalados
- Reporte de todo el trabajo realizado

3.8.1.5. Quinta Etapa: Configuración de Telefonía

- Laboratorio de configuraciones routers Matriz y Aeropuerto.
- Laboratorio de configuraciones para integración con la PSTN.
- Laboratorio de integración con la central MITEL
- Backup de todos los nodos.

3.8.1.6. Sexta Etapa: Instalación telefonía Rocío

- Carga de configuraciones en el nodo Rocío
- Instalación de Teléfonos.
- Conexión con la PSTN

3.8.1.7. Séptima Etapa: Monitorización Telefonía

- Verificación de las configuraciones
- Creación de backups de las configuraciones
- Reporte de problemas post-instalación
- Monitorización de los equipos instalados
- Reporte de todo el trabajo realizado

3.8.1.8. Octava Etapa: Instalación Telefonía sitios remotos

- Carga de configuraciones en los sitios remotos
- Instalación de Teléfonos
- Conexión con la PSTN
- Conexión con la Matriz y resto de sitios remotos

3.8.1.9. Novena Etapa: Monitorización Telefonía sitios remotos

- Verificación de las configuraciones
- Creación de backups de las configuraciones
- Reporte de problemas post-instalación
- Monitorización de los equipos instalados
- Reporte de todo el trabajo realizado
- Retiro de la central telefónica MITEL

CAPÍTULO IV

4. MODELO DE CONFIGURACIÓN DE EQUIPOS DE RED Y MODELO DE GESTIÓN

Este capítulo describe la configuración de los equipos tanto routers como switches, especificando sus configuraciones tanto de networking como de telefonía. La segunda parte del capítulo se enfocará en el desarrollo de un modelo de gestión, determinando sus componentes y la aplicación en el proyecto. Se presentarán los resultados de un prototipo del presente Proyecto de Titulación, usando el programa GNS3, equipos físicos y el programa What`s Up. En la parte final del capítulo se presenta un procedimiento para recuperación de fallas.

4.1. MODELO DE CONFIGURACIÓN ROUTERS

4.1.1. CONFIGURACIONES BÁSICAS

Las configuraciones básicas que se realizarán en los routers y switches, serán: nombre, mensaje de acceso, deshabilitación de resolución de nombres, usuarios con acceso al equipo, contraseña del enable, autenticación en la línea de consola y líneas vty por ssh para acceso remoto.

4.1.1.1. Nombre del Equipo

Tiene como objeto tener un identificativo del equipo al que se encuentra conectado.

Nombre del Router de Matriz : ROUTER_ROCIO
Nombre del Router de Beaterio: ROUTER_BEATERIO
Nombre del Switch del cerro Pichincha: SW_PICHINCHA

router >en
router #conf t
router(config)#hostname ROUTER_ROCIO
ROUTER_ROCIO(config)#end

4.1.1.2. Mensaje de acceso

Tiene como objeto alertar a usuarios no autorizados que intenten acceder al equipo.

ROUTER_ROCIO (config)#banner motd %

4.1.1.3. Deshabilitación de resolución de nombres

Tiene como objeto deshabilitar la función por defecto del ruteador de resolución nombres, ya sea local o través de un servidor DNS. Es importante indicar que los nombres de usuarios y contraseñas que se colocan en los ejemplos de configuración no son las que se manejan en PETROCOMERCIAL.

ROUTER_ROCIO (config)#no ip domain-lookup

4.1.1.4. Configuración de autenticación

4.1.1.4.1. Contraseña de enable

Tiene como objeto la protección del acceso al modo de privilegios. Además como se explicará en el modelo de gestión por política de seguridad, no se deberán manejar claves de menos de 8 caracteres.

ROUTER _ROCIO(config)#security passwords min-length 8
ROUTER _ROCIO(config)#enable secret s!stem@s2011

4.1.1.4.2. Usuarios con acceso al equipo

Tiene como objeto la creación de usuarios para autenticación local de acceso al equipo, se dará un nivel de privilegios de 15 que es el máximo dado para equipos CISCO. (Para el ejemplo de configuración por motivos de seguridad se dará un usuario ficticio).

ROUTER_ROCIO(config)#username usertics privilege 15 secret s!stem@s2011

Para evitar que las contraseñas sean almacenadas en el archivo de configuración en texto plano se utiliza el parámetro secret tanto en la contraseña del enable como en la de los usuarios, por tanto se aplica la función de hash MD5, y se muestra el resultado en los archivos de configuración. No se utiliza el comando service

password-encryption debido a que se utilizaría el algoritmo número 7 de CISCO que es un algoritmo más débil.

4.1.1.4.3. Autenticación de la línea de consola

Tiene como objeto proteger el acceso a configuración por consola.

ROUTER_ROCIO(config)#line console 0
ROUTER_ROCIO(config-line)#login local

4.1.1.4.4. Acceso remoto con SSH y autenticación.

Tiene como objeto permitir accesos remotos, con niveles de seguridad, la información que se intercambia no se transmite en texto plano.

ROUTER_ROCIO(config)#ip domain-name ROUTER_ROCIO.pco.com
(El nombre y dominio permite generar las claves RSA)

ROUTER_ROCIO(config)#crypto key generate rsa 1024
(Genera las claves RSA con un tamaño de 1024 bits)

ROUTER_ROCIO(config)#ip ssh time-out 30
(Configura el tiempo de espera antes de terminar la sesión)

ROUTER_ROCIO(config)#ip ssh authentication-retries 3
(Configura el número máximo de intentos fallidos)

ROUTER_ROCIO(config)#ip ssh version 2
(Habilita la versión 2 de SSH)

ROUTER_ROCIO(config)#line vty 0 4
ROUTER_ROCIO(config-line)#transport input ssh
ROUTER_ROCIO(config-line)#login local

(Habilita ssh para acceso remoto y autentica el acceso localmente)

4.1.1.5. Configuración de Interfaces

Las interfaces que se configuran son tanto internas como la de los enlaces WAN, conforme al diseño del capítulo 3.

4.1.1.5.1. Router MATRIZ

ROUTER_ROCIO(config)#interface GigabitEthernet0/0
ROUTER_ROCIO(config-if)#description ENLACE A SW_PICHINCHA - G0/5
ROUTER_ROCIO(config-if)#ip address 172.20.35.14 255.255.255.252
ROUTER_ROCIO(config)#interface GigabitEthernet0/1
ROUTER_ROCIO(config-if) #description ENLACE A SW_ATACAZO - F0/4
ROUTER_ROCIO(config-if)#ip address 172.20.35.62 255.255.255.252

ROUTER_ROCIO(config)#interface FastEthernet0/1/0
ROUTER_ROCIO(config-if) # description ENLACE A ALLOT EXTERNAL 1
ROUTER_ROCIO(config-if)#switchport mode trunk

ROUTER_ROCIO(config)#interface FastEthernet0/1/1
ROUTER_ROCIO(config-if) # description ENLACE A VANGUARD 172.20.64.11
ROUTER_ROCIO(config-if)#switchport mode trunk

Esta configuración permite que el tráfico entre la red WAN que pasa tanto por los ruteadores VANGUARD como por lo de los nuevos equipos CISCO sean monitoreados por el equipo ALLOT. El enrutamiento entre los equipos Vanguard y Cisco es estático.

ROUTER_ROCIO(config)#interface vlan 1
ROUTER_ROCIO(config-if) # description LAN_UIO
ROUTER_ROCIO(config-if) # ip address 172.20.64.14 255.255.248.0
(Interfaz VLAN para datos)

ROUTER_ROCIO(config)#interface vlan 1001
ROUTER_ROCIO(config-if) # description LAN_UIO_TELEFONIA
ROUTER_ROCIO(config-if) # ip address 172.21.64.4 255.255.255.0
(Interfaz VLAN para la telefonía IP)

4.1.1.5.2. Router BEATERIO

ROUTER_BEATERIO(config)#interface GigabitEthernet0/0
ROUTER_BEATERIO(config-if) #description ENLACE A SW_PICHINCHA G0/1
ROUTER_BEATERIO(config-if)#ip address 172.20.35.2 255.255.255.252
ROUTER_ BEATERIO(config)#interface GigabitEthernet0/1
ROUTER_ BEATERIO(config-if)#description ENLACE A SW_172.20.129.65

ROUTER_ BEATERIO(config)#interface GigabitEthernet0/1.1
ROUTER_ROCIO(config-if) # description LAN_BEA
ROUTER_ BEATERIO(config-if)#encapsulation dot1q 1
ROUTER_ BEATERIO(config-if)#ip add 172.20.129.14 255.255.255.0

ROUTER_ BEATERIO(config)#interface GigabitEthernet0/1.3
ROUTER_ROCIO(config-if) # description LAN_BEA_TELEFONIA
ROUTER_ BEATERIO(config-if)#encapsulation dot1q 3
ROUTER_ BEATERIO(config-if)#ip add 172.21.129.4 255.255.255.128

4.1.1.5.3. Switch PICHINCHA

SW_PICHINCHA(config)#interface GigabitEthernet0/1
SW_PICHINCHA (config-if)#description ENLACE A ROUTER BEATERIO Gi0/0
SW_PICHINCHA (config-if)#ip address 172.20.35.1 255.255.255.252

SW_PICHINCHA(config)#interface GigabitEthernet0/5
SW_PICHINCHA (config-if)#description ENLACE A ROUTER ROCIO Gi0/0
SW_PICHINCHA (config-if)#ip address 172.20.35.13 255.255.255.252

4.1.2. CONFIGURACIÓN DE EIGRP

Como se explicó anteriormente el protocolo de enrutamiento a ser configurado es EIGRP. Para evitar que se genere tráfico EIGRP por suplantación, ya sea provocado por error o por un ataque de seguridad, se utilizará autenticación, que protegerá la inserción de dispositivos no autorizados que generen tráfico EIGRP (existe una mayor probabilidad de este problema, debido a que se manejará EIGRP en los switches de capa 3 tanto del Beaterio como de la Matriz, a nivel de LAN).

4.1.2.1. Autenticación

Configuración de la cadena que contendrá el key del MD5 de autenticación

ROUTER_ROCIO(config)#key chain PETROEIGRP
ROUTER_ROCIO(config-keychain)#key 1
ROUTER_ROCIO(config-keychain-key)#key–string petro

Es necesario habilitar la autenticación en cada interfaz que envía o recibe trafico EIGRP.

ROUTER_ROCIO(config)#interface gi 0/0
ROUTER_ROCIO(config-if)#ip authentication mode eigrp 100 md5
ROUTER_ROCIO(config-if)#ip authentication key-chain eigrp 100 PETROEIGRP.

Se necesita habilitar la autenticación MD5 en los interfaces en el ruteador Rocío Gi0/0, Gi0/1 y VLAN 1. En el Router Beaterio en Gi0/0 y Gi0/1, en el SW Pichincha en el interfaz Gi0/1 y Gi0/5. Además es necesario habilitar EIGRP y su autenticación en los SW de Core de Matriz y Beaterio.

4.1.2.2. Enrutamiento

ROCÍO

ROUTER_ROCIO(config)#router eigrp 100
ROUTER_ROCIO(config-router)#network 172.20.0.0
ROUTER_ROCIO(config-router)#network 172.21.0.0

ROUTER_ROCIO(config-router)#no auto-summary

BEATERIO

ROUTER_BEATERIO(config)#router eigrp 100
ROUTER_BEATERIO(config-router)#network 172.20.0.0
ROUTER_BEATERIO(config-router)#network 172.21.0.0
ROUTER_BEATERIO(config-router)#no auto-summary

SW PICHINCHA

SW_PICHINCHA(config)#router eigrp 100
SW_PICHINCHA (config-router)#network 172.20.0.0
SW_PICHINCHA (config-router)#no auto-summary

Además es necesario la configuración en los switches de core de Matriz y Beaterio

ROUTER_MATRIZ(config-router)#router eigrp 100
ROUTER_ MATRIZ(config-router)#network 172.20.0.0
ROUTER_ MATRIZ(config-router)#network 172.31.0.0
ROUTER_ MATRIZ(config-router)#no auto-summary

ROUTER_PCOBEAT(config-router)#router eigrp 100
ROUTER_PCOBEAT(config-router)#network 172.20.0.0
ROUTER_PCOBEAT(config-router)#network 172.31.0.0
ROUTER_PCOBEAT(config-router)#network 172.25.0.0
ROUTER_ PCOBEAT(config-router)#no auto-summary

4.1.3. TELEFONÍA CISCO

La central telefónica CISCO CALL MANAGER EXPRESS permite la configuración tanto del protocolo propietario de CISCO SCPP como el estándar SIP.

4.1.3.1. Configuración de SCCP

El servicio que utiliza la configuración de SCCP es telephony-service, las líneas a configurar se denominan ephone-dn, y los teléfonos se denominan ephone.

ROUTER_ROCIO(config)# telephony-service
ROUTER_ROCIO (config-telephony)#ip source-address 172.21.64.4 port 2000
(Asocia el servicio con un socket (dirección IP y puerto), por defecto SCCP escucha en el puerto 2000)
ROUTER_ROCIO(config-telephony)#max-ephones 192
(Configura el número máximo de teléfonos a configurarse, el número depende del modelo de los ruteadores)

ROUTER_ROCIO(config-telephony)#max-dn 500
(Configura el número máximo de extensiones a configurarse, el número depende del modelo de los ruteadores, es mayor al número de ephones por que se puede asociar más de una extensión a un teléfono)

4.1.3.1.1. Configuración de Extensiones

ROUTER_ROCIO(config)#ephone-dn 1 dual-line
(Se le asigna una etiqueta numérica a la extensión (1), se configura como dual-line para que permita dos llamadas por botón, llamada saliente y entrante)

ROUTER_ROCIO(config-ephone-dn)#number 1001
(Se le asigna un número a la extensión)

ROUTER_ROCIO(config-ephone-dn)#name USER1
(Se coloca el nombre del usuario de la extensión)

ROUTER_ROCIO(config-ephone-dn)#label USER1
(Se coloca una etiqueta, opcional)

4.1.3.1.2. Configuración teléfono

ROUTER_ROCIO(config)#ephone 1
(Se le asigna una etiqueta numérica al teléfono)

ROUTER_ROCIO(config-ephone)#mac-address 0021.00E6.F0F2
(Permite el registro solo al cliente con la MAC configurada)

ROUTER_ROCIO(config-ephone)#button 1:1
(Asocia al botón 1 del teléfono la línea configurada como 1)
ROUTER_ROCIO(config-ephone)#type CIPC
(Configura el tipo de teléfono, 7911, 7940 etc. CIPC quiere decir CISCO IP COMUNICATOR).

4.1.3.2. Configuración de SIP

Debido a las limitaciones de los simuladores, y en el caso específico de éste Proyecto de Titulación el emulador GNS3, el cual no soporta el modelo del router CISCO 3845, el modelo que se utiliza es un modelo similar, el CISCO 3745 que no soporta algunas funciones del modelo escogido, por lo que la configuración de teléfonos a través de SIP se dejará determinada pero no se simulará.

El servicio que utiliza la configuración de SIP es voice register, las líneas a configurar se denominan dn, y los teléfonos se denominan pool.

ROUTER_ROCIO(config)#voice service voip

ROUTER_ROCIO(conf-voi-serv)#allow-connections sip to sip
(Permite las llamadas de extensiones sip a sip)

ROUTER_ROCIO(conf-voi-serv)#sip

ROUTER_ROCIO (conf-serv-sip)#registrar server expires max 1200 min 300
(Habilita el servicio para registro de extensiones SIP, configura un tiempo mínimo y máximo de expiración dado en segundos)

ROUTER_ROCIO(config)#voice register global

ROUTER_ROCIO(config-voice)#mode cme
(Habilita el registro de teléfonos a través del call manager express)
ROUTER_ROCIO(config-voice)#source-address 172.21.64.4 port 5060
(Asocia un socket al servicio de telefonía IP a través de SIP, el puerto por defecto de SIP es 5060)

ROUTER_ROCIO(config-voice)#max-dn 720

ROUTER_ROCIO(config-voice) #max-pool 262
(Se configura el número máximo de teléfonos y extensiones que depende del modelo del ruteador)

ROUTER_ROCIO(config-voice) #authenticate register
(Permite la autenticación de usuarios a través de usuario y contraseña)

ROUTER_ROCIO(config-voice) # create profile cfn
(Crea los archivos de configuración para los teléfonos)

4.1.3.2.1. Configuración de extensiones

Es muy similar a la configuración de extensiones de sccp.

ROUTER_ROCIO(config) #voice register dn 1
ROUTER_ROCIO(config-dn)# number 2001
ROUTER_ROCIO(config-dn)#name USER2
ROUTER_ROCIO(config-dn)#label USER2

4.1.3.2.2. Configuración de teléfonos

ROUTER_ROCIO(config)#voice register pool 1

ROUTER_ROCIO(config-pool)#id mac 0000.0000.0000
(Debido a que la autenticación se la realiza por usuario y contraseña este valor no es importante pero es necesario configurarlo)

ROUTER_ROCIO(config-pool)#number 1 dn 1
ROUTER_ROCIO(config-pool)#dtmf-relay sip-notify
Habilita la señalización por dual tone multifrequency dtmf.

ROUTER_ROCIO(config-pool)#username 1002 password petrosip
(Se configura el usuario y password que se configurarán en el cliente SIP)

ROUTER_ROCIO(config-pool)#codec g711ulaw
(Se indica el códec que utilizará el dispositivo final)

4.1.3.3. Configuración de dial-peers

Para el enrutamiento entre extensiones de distintas centrales es necesaria la creación de dial peer, con el patrón de las llamadas, y la dirección de la central remota

Se define un perfil de preferencias de códecs para los dial peer a utilizar.

ROUTER_ROCIO (config)#voice class codec 100
ROUTER_ROCIO (config-class)#codec preference 1 g729r8
ROUTER_ROCIO (config-class)#codec preference 2 g711ulaw

Se define el dial peer, con el patrón de llamadas que utiliza y la dirección de la central remota.

ROUTER_ROCIO(config)#dial-peer voice 100 voip
ROUTER_ROCIO (config-dial-peer)# destination-pattern 50..
ROUTER_ROCIO (config-dial-peer)#voice-class codec 100
ROUTER_ROCIO (config-dial-peer)# session target ipv4:172.21.129.4
ROUTER_ROCIO (config-dial-peer)# dtmf-relay h245-alphanumeric

Además es necesario configurar las tarjetas FXO que reciben las líneas analógicas de la PSTN.
Se define un grupo de líneas troncales y el patrón en que serán utilizadas.

trunk group PSTN
hunt-scheme sequential

voice-port 1/0/8
trunk-group PSTN
connection plar XXXX
Permite redireccionar a una determinada extensión la llamada de la troncal.

Dial-peer que se utiliza para las llamadas hacia la PSTN.
dial-peer voice 200 pots
trunkgroup PSTN
destination-pattern 2……
forward-digits 7

4.1.3.4. Configuración de DSP para transcoding

Los DSP serán utilizados para realizar el transconding entre códecs g711 y g729.
voice-card 0
(Identifica donde se ubica la tarjeta para DSP)

dspfarm
dsp services dspfarm

(Habilita el servicio dspfarm, que permitirá definir el perfil para el transcoding)

sccp local Vlan1001

(Asocia sccp a un puerto determinado del router)
sccp ccm 172.21.64.4 identifier 1
sccp

Se crea un grupo asociado a la aplicación sccp que luego se asociará al perfil del dspfarm
sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register mtpfcfbfb357d40

Se indica los códec que soportará el transcoding
dspfarm profile 1 transcode
codec g711ulaw
codec g729r8

Se configura el número máximo de sesiones simultáneas que puede soportar
maximum sessions 16

Se asocia a la aplicación que utilizará los dsp
associate application SCCP

4.1.3.5. Configuración para restricción de llamadas

trunk group PSTN
hunt-scheme sequential
Se crea el grupo troncal PSTN

voice-port 0/2/0

trunk-group PSTN
connection plar 1001
(Se le asocial al Puerto de voz el grupo creado)

dial-peer cor custom
name local
name regional
(Crea los nombres de restricción de las clases)

dial-peer cor list llamadaslocales
member local
(Asigna los miembros a las listas de restricciones de clases creadas)

dial-peer cor list llamadasregionales
member local
member regional
(Asigna los miembros a las listas de restricciones de clases creadas)

dial-peer voice 200 pots
trunkgroup PSTN
corlist outgoing llamadaslocales
destination-pattern 2.....
forward-digits 7
(Asigna la lista de restricciones a los dial peers, en este caso la lista *llamadaslocales* permite solo marcar a llamadas internas solo con el primer dígito 2)

dial-peer voice 201 pots
trunkgroup PSTN
corlist outgoing llamadasregionales
destination-pattern 0.....
forward-digits 9

(Asigna la lista de restricciones a los dial peers, en este caso la lista *llamadasregionales* permite solo marcar a llamadas fuera de la provincia)

ephone-dn 1 dual-line
corlist incoming llamadaslocales
(Asigna la lista de restricciones a los ephone-dns)

4.1.3.6. Configuración del Buzón de Voz

4.1.3.6.1. Configuraciones realizadas en el Router

interface Service-Engine0/0
description CUE
ip unnumbered Vlan1001
service-module ip address 172.21.64.2 255.255.255.0
service-module ip default-gateway 172.21.64.4
(Se le asigna una IP a la interfaz service engine con la cual se puede realizar una conexión entre el Cisco Unity Express (CUE) y el Cisco Call Manager (CCM))

ip route 172.21.64.2 255.255.255.255 Service-Engine0/0
(Se establece una ruta estática al módulo del Cisco Unity Express)

dial-peer voice 204 voip
*description **voicemail***
destination-pattern 1003
session protocol sipv2
session target ipv4:172.21.64.2
dtmf-relay sip-notify
codec g711ulaw
no vad

Se establece un dial peer para facilitar la comunicación entre el CUE y el CCM, los parámetros establecidos son:

- Destination pattern 1003: Especifica el número del buzón de voz al cual se va a redireccionar la llamada.
- session protocol sipv2: Establece a sipv2 como el protocolo de inicio de sesión entre el CUE y el CCM
- session target ipv4:172.21.64.2: Designa una dirección de red específica para recibir llamadas desde un dial peer de voz sobre IP.
- dtmf-relay sip-notify: Reenvía los tonos DMTF usando notificación sip
- códec g711ulaw: Especifica el código usado para los mensajes dejados en el Buzón de voz
- no vad: deshabilita VAD para permitir el funcionamiento del dial peer.

telephony-service
voicemail 1003
(Especifica en el telephone-service el número del correo de voz)

ephone-dn 1 dual-line
call-forward busy 1003
call-forward noan 1003 timeout 20
(Configura en el teléfono el reenvío de las llamadas al número 1003 que es el correo de voz, cuando se niega la llamada o no se contesta el teléfono)

4.1.3.6.2. Configuración en el Cisco Unity Express.

username USER1 create
(Se crea un usuario en el CUE)

username USER1 phonenumber "1001"
(Se le asigna la extensión del número telefónico perteneciente al usuario creado)

ccn application voicemail aa
description "Cisco voicemail"
enabled
maxsessions 4
script "voicebrowser.aef"
parameter "logoutUri" "http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
parameter "uri" "http://localhost/voicemail/vxmlscripts/login.vxml"
end application
(Se configura y habilita la aplicación del voicemail)

ccn trigger sip phonenumber 1003
application "voicemail"
enabled
maxsessions 4
end trigger
(Se configura el trigger sip de voicemail. Sirve para iniciar el proceso de correo de voz cuando se marca el número 1003)

voicemail mailbox owner "USER1" size 300
description "User1 mail box"
expiration time 10
end mailbox
(Se configura el correo de voz para el usuario creado anteriormente. Se especifica su tamaño en segundos y el tiempo, en días, en que expiran los mensajes almacenados).

4.1.4. CONFIGURACIÓN DE GESTIÓN DE RED

El protocolo que se utilizará para la gestión de red es SNMP versión 3.

4.1.4.1. Configuración de SNMP v3

ROUTER_ROCIO(config)#snmp-server view petroview 1.3.6.1.2.1 included
(Permite las MIB de MIB-2)

ROUTER_ROCIO(config)#snmp-server view petroview 1.3.6.1.4.1.9 included
(Permite las MIB de Cisco)

ROUTER_ROCIO(config)#snmp-server group petrogroup v3 priv read petroview
(Define el grupo al que va a pertenecer el usuario, utiliza snmp v3, utiliza autenticación y privacidad, además de permitir solo lectura, y asigna la vista definida anteriormente)

ROUTER_ROCIO(config)#snmp-server user petroadmin petrogroup v3 auth md5 petroaut3 priv des petro

(Define el usuario petroadmin, se le asigna al grupo petrogroup, y se dan las parámetros para la autenticación y encripción)

4.1.4.1.1. Configuración de Traps

ROUTER_ROCIO(config)#snmp-server enable traps
ROUTER_ROCIO(config)#snmp-server host 172.20.64.77 traps version 3 priv petroadmin

El servidor en el cual corre la aplicación Whats'UP tiene la dirección 172.20.64.77

4.1.4.1.2. Configuración de Logs

ROUTER_ROCIO(config)#logging on
ROUTER_ROCIO(config)#logging 172.20.64.77
ROUTER_ROCIO(config)#logging trap 3
(Habilita las traps de los niveles de 0 a 4, hasta el nivel de advertencia)

4.2. MODELO DE GESTIÓN DE RED

En consecuencia para el presente Proyecto de Titulación se elabora un modelo de gestión de red tomando en cuenta aspectos principales de los modelos de gestión explicados en el Capítulo I. Debido al alcance del proyecto el modelo de gestión de red se plantea para los equipos CISCO ubicados en los nodos anteriormente explicados. Se detallará la arquitectura del modelo de gestión de red, el modelo y la plataforma de gestión de red aplicados.

4.2.1. ARQUITECTURA DEL MODELO DE GESTIÓN

Un Modelo de gestión de red debe basarse en una arquitectura que le permita gestionar correctamente todos los elementos que estén involucrados en ésta. Para su correcto funcionamiento se debe tomar en cuenta una arquitectura centralizada que incluya un centro de gestión donde se controle todos los aspectos principales de los equipos integrados en la red de la empresa. Este centro debe estar conformado por lo siguiente:

- Modelo de gestión. Es el esquema que va a definir los pasos a realizarse en el control, verificación, y acción de los componentes de la red.
- Recursos humanos. Personal encargado del correcto funcionamiento del centro de gestión de red.
- Herramientas de gestión. Herramientas que facilitan las tareas de gestión a los operadores humanos y posibilitan minimizar el número de éstos.

En este capítulo se detalla el método de gestión, así como la herramienta que permitirá la gestión de los recursos de red. Debemos tomar en cuenta que todos los elementos anteriormente mencionados no tuvieran importancia sin la participación del recurso más importante en una empresa que es el humano. El personal encargado de gestionar la red debe ser el más calificado para esta área.

La estructura básica que utilizan los sistemas de gestión para tener un control total de los componentes a gestionar, se basa en el esquema de gestor-agente, el cual se indica en la figura 4.1.

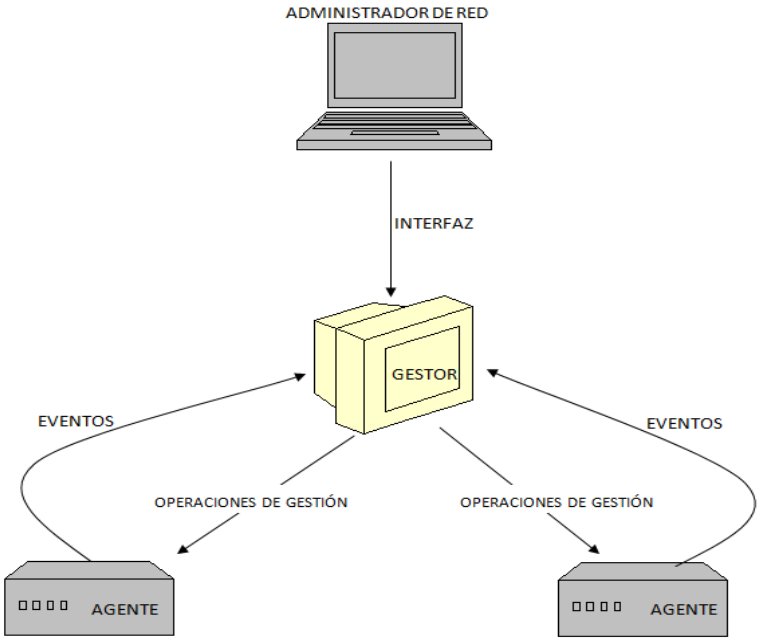


Figura 4.1 Esquema Gestor Agente

Para el presente proyecto se realiza un modelo de gestión tomando en cuenta los diferentes modelos que existen, y que han sido explicados en el Capítulo I del Proyecto de Titulación.

El modelo de gestión, estará basado en el modelo de gestión ISO/OSI, y el modelo de gestión Internet.

Del modelo de gestión ISO/OSI se ha tomado en cuenta el modelo funcional, y del modelo de gestión Internet se ha adoptado el protocolo de administración de red SNMP. La descripción del modelo de gestión de red para el Proyecto de Titulación se lo realizará más adelante.

En cuanto al uso del esquema de gestor-agente, se determinará como elementos para la gestión los siguientes:

- Gestor: Software de Gestión de redes What's Up, que se lo explicará en este capítulo
- Agente: Software de los Routers Cisco.
- Protocolo de gestión de red: SNMP v3, elemento que forma parte del modelo de gestión Internet.

4.2.2. HERRAMIENTA DE GESTIÓN

La herramienta de gestión a utilizarse es el programa What´s Up. A continuación se da una pequeña introducción.

4.2.2.1. Introducción

WhatsUp Gold, es una potente solución de monitorización de red diseñada para ayudar a proteger la infraestructura de comunicaciones de PETROCOMERCIAL. WhatsUp Gold ofrece la posibilidad de monitorear y controlar cualquier dispositivo de red, servicio o aplicación en TCP / IP y redes Windows.

Whats Up Gold permite descubrir los dispositivos en la red, iniciar el estado de comunicación de los dispositivos, y ejecutar las acciones basadas en cambios de estado del dispositivo, para poder identificar los fallos de la red.

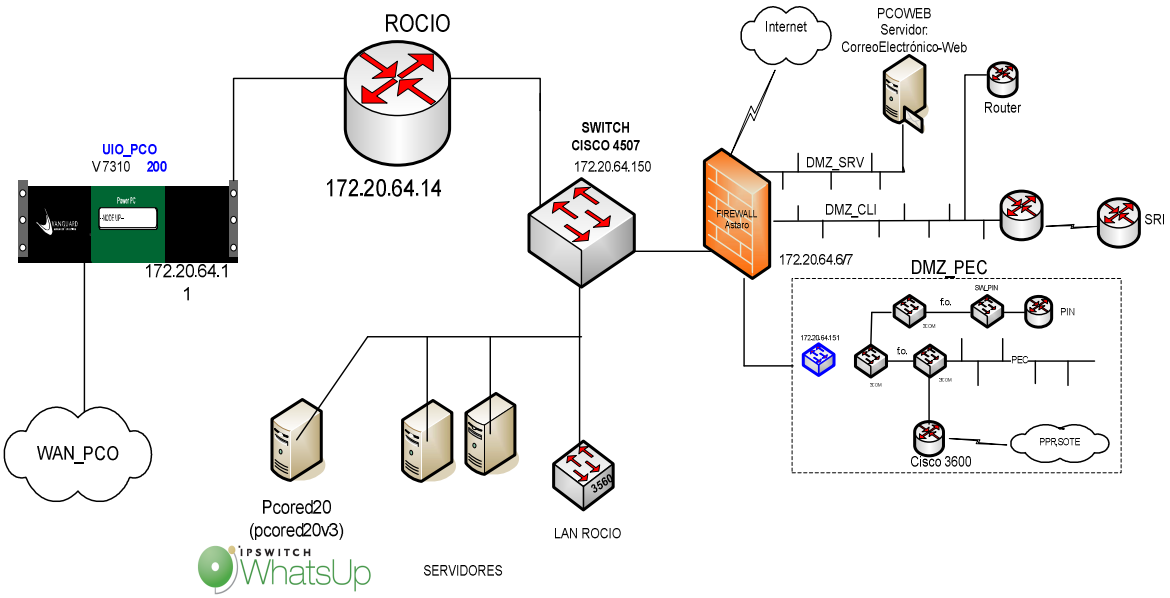


Figura 4.2 Esquema de Conexión de WhatsUp

Como se puede observar en la figura 4.2 el servidor donde se encuentra instalada la herramienta de monitoreo Ipswitch WhatsUp Gold se encuentra físicamente instalado en la LAN de SERVIDORES de la red de PETROCOMERCIAL, es importante indicar que este servidor debe tener configurada las políticas correspondientes en el Firewall para poder realizar ping a todos los dispositivos de la red. A continuación se indican las características y parámetros configurados en el servidor:

- Máquina Virtual con VMware Server 1.9
- Memoria Virtual: 4 GB
- Procesador Virtual: Intel Xeon de 3.00 GHz
- Sistema Operativo: Windows Server 2003 R2
- Hostname: pcored20v3
- IP: 172.20.64.77
- URL de Administración: http://172.20.64.77:8000
- Software Ipswitch WhatsUp Gold v14.0 Central Site Edition
- Microsoft SQL Server 2005 Express Edition

4.2.2.1.1. Requerimientos

Requisitos mínimos de software.

- Sistema Operativo Windows XP Professional SP2 o posterior; Windows Server 2000 Professional SP4 o, Windows Server 2003.
- Microsoft Internet Explorer 6.0 o Firefox 1.5x o superiores.
- Microsoft Windows Scripting Host v5.6 o posterior. (Requerido para la interfaz web de WhatsUp, y para ejecutar secuencias de comandos para las capacidades de Active Scripting "en monitores activos y acciones.)

Requisitos mínimos de hardware.

- Intel Pentium-compatible con los ordenadores, 550 MHz o superior (2 GHz o superior recomendado)
- 256 MB de memoria (RAM) (1-2 GB de RAM recomendado)
- 256 MB de espacio en disco
- Unidad de CD-ROM
- Tarjeta de Red

4.2.2.1.2. Consola de WhatsUp

La consola de administración de WhatsUp es la interfaz principal que nos permite la configuración, gestión de la aplicación y la base de datos con la que trabaja.

En esta parte se describe las diferentes partes de de la consola, la manera de navegar por la interfaz, y lo que se necesita saber para empezar a utilizarla.

Introducción a la Consola

En la figura 4.3 se indica las características principales que se encuentran en la consola Gold WhatsUp.

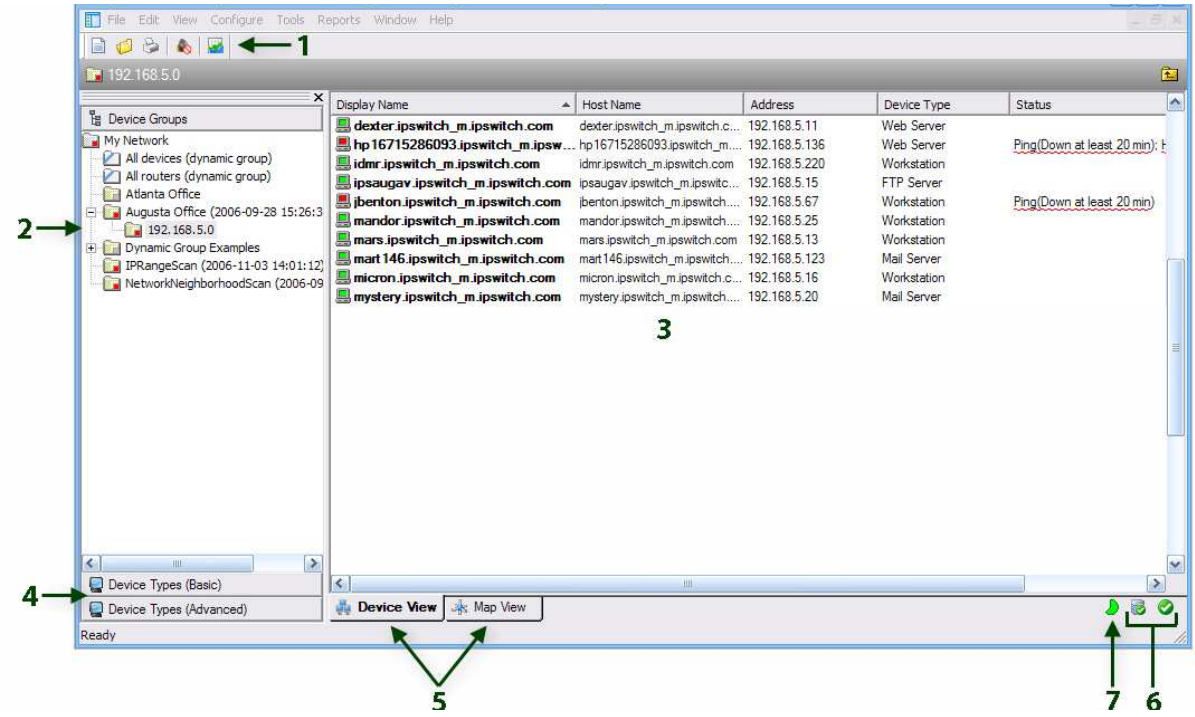


Figura 4.3 Elementos de la consola de What´s Up

1. La barra de herramientas de WhatsUp: Los iconos de esta barra de herramientas cambian según la distribución de que está utilizando actualmente. Los iconos de la barra de herramientas adicionales se pueden habilitar para la vista de mapa seleccionando.

2. Dispositivo de Grupo Árbol: Ésta es una lista de todos los grupos de dispositivos creados a través de WhatsUp. Al realizar un descubrimiento de exploración, WhatsUp crea una carpeta de nivel superior. Todas las subredes descubiertas se crean en los subgrupos, pero se pueden organizar, eliminado o cambiado el nombre para adaptarse a sus necesidades.

3. Panel de vista: Este panel muestra el grupo de dispositivos seleccionados en base a la vista escogida (ver dispositivos o Ver Mapa).

4. Tipos de grupos de dispositivos: Permite ver los tipos de dispositivos contenida en la selección de grupo. Estos tipos pueden ser arrastrados en el panel de vista para crear un nuevo dispositivo basado en el tipo de dispositivo seleccionado.

5. Ver los selectores: Permite elegir la forma en que desea ver sus grupos de dispositivos.

- Ver los dispositivos: Esta perspectiva ofrece una visión general de cada dispositivo y en un subgrupo de dispositivos seleccionados.
- Ver Mapa: Esta vista muestra una representación gráfica de los dispositivos y de los subgrupos de dispositivos seleccionados.

6. Pool de Indicador de Iconos: Estos iconos indican el estado actual de la máquina. Los íconos indicadores del estado de la máquina se muestran en la figura 4.4.

Poll engine is connected Poll engine is not connected Polling is enabled Polling is disabled

Figura 4.4 Indicadores del estado de la máquina

7. Indicador de tamaño de base de datos: Este icono muestra el tamaño actual de su base de datos. Los cambios de color y forma, se dan según los umbrales del tamaño de la base de datos:

Verde - el 49% y por debajo
Amarillo - 50% a 74%
Rojo - 75% y superiores.

4.2.2.1.3. Configuración

Asistente para descubrir dispositivos.

El Asistente para descubrir dispositivos escanea la red, usando el protocolo(s) y configuración que se elija, utiliza las credenciales configuradas. Después los dispositivos encontrados pueden ser agregados para su monitoreo, seleccionamos los que desea supervisar y WhatsUp Gold los crea en la base de datos.

El asistente se inicia por defecto tras la instalación. Después de este descubrimiento inicial, se puede ejecutar otro Descubrimiento en cualquier momento desde la consola, hacer clic en Archivo> Descubrir Dispositivos (Figura 4.5).

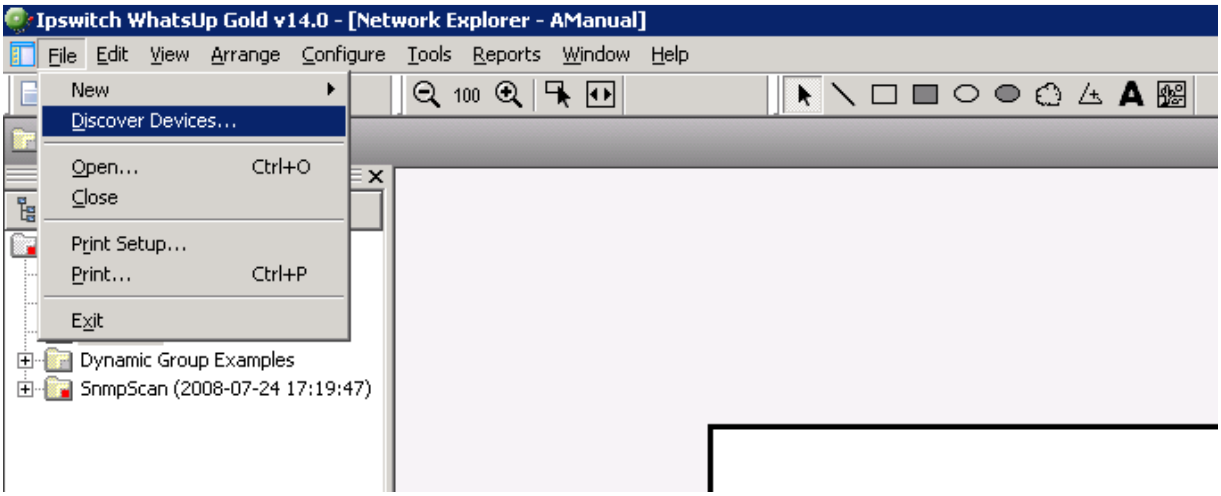


Figura 4.5 Descubrimiento de dispositivos

Seleccionamos el tipo de Scan:

En este caso seleccionamos IP RANGE SCAN y definimos el rango 172.20.64.0 a 172.20.64.255 y damos clic en SCAN (Figura 4.6).

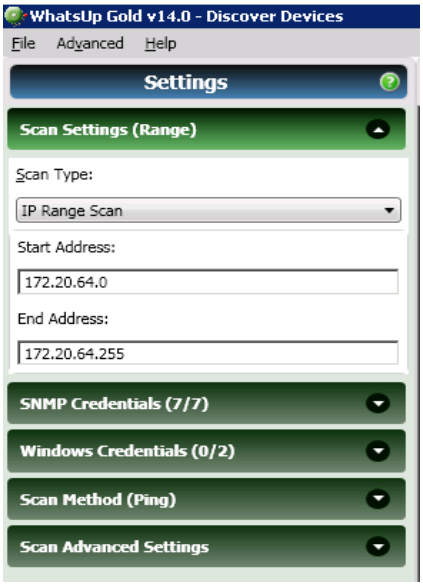


Figura 4.6 Escaneo de Dispositivos

Como resultado obtendremos un resumen de todos los host que fueron encontrados en el escaneo con su respectiva información como IP, hostname, Marca, Modelo, Sistema Operativo, etc. (Figura 4.7).

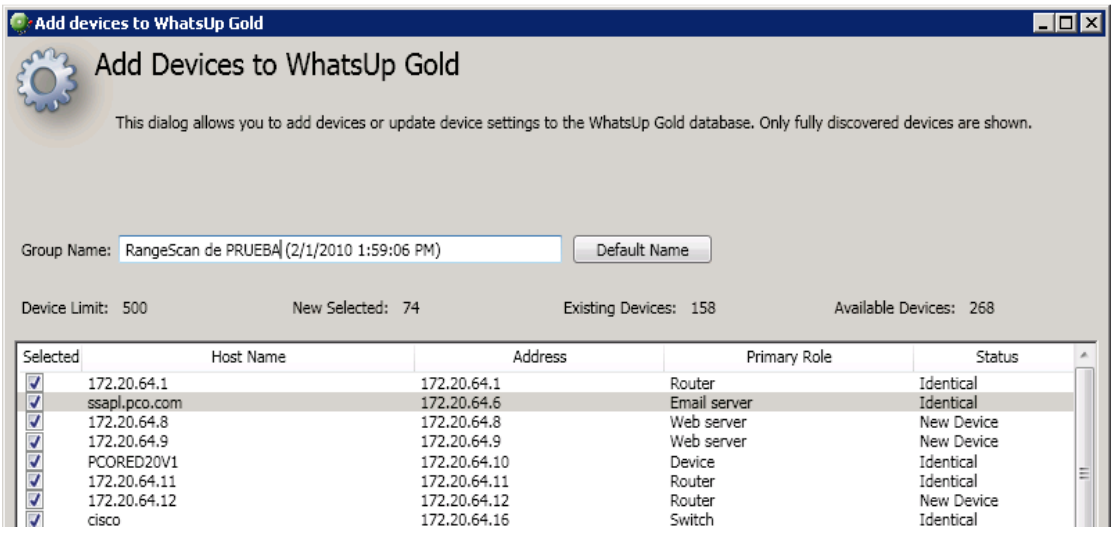


Figura 4.7 Dispositivos encontrados

En la figura 4.8 se visualiza gráficamente los dispositivos encontrados.

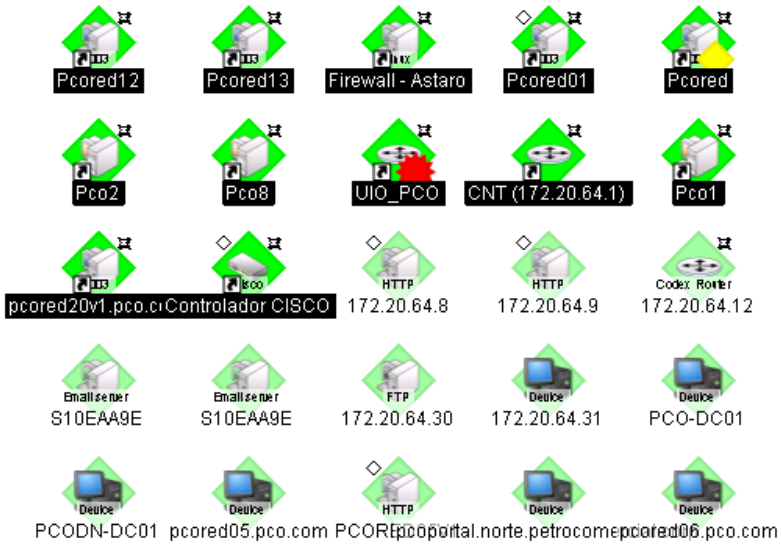


Figura 4.8 Dispositivos encontrados

Los dispositivos también pueden ser agregados de forma manual.

4.2.2.1.4. Uso de la Interfaz Web de WhatsUp

Acceder a la Interfaz Web de WhatsUp.

Se puede conectar a la interfaz web de WhatsUp desde cualquier navegador, pero se recomienda que sea por Internet Explorer, el acceso se lo realiza a través de la dirección IP y puerto del servidor en el cual se encuentra instalado y configurado para nuestro caso será http://172.20.64.77:8000 (Figura 4.9).

Figura 4.9 Ingreso a la interfaz web

En la pantalla que nos aparece (figura 4.10) ingresamos el respectivo USER y PASSWORD asignado.

Figura 4.10 Interfaz de Ingreso

Si la autentificación tiene éxito aparecerá la siguiente pantalla (figura 4.11), con el área de trabajo.

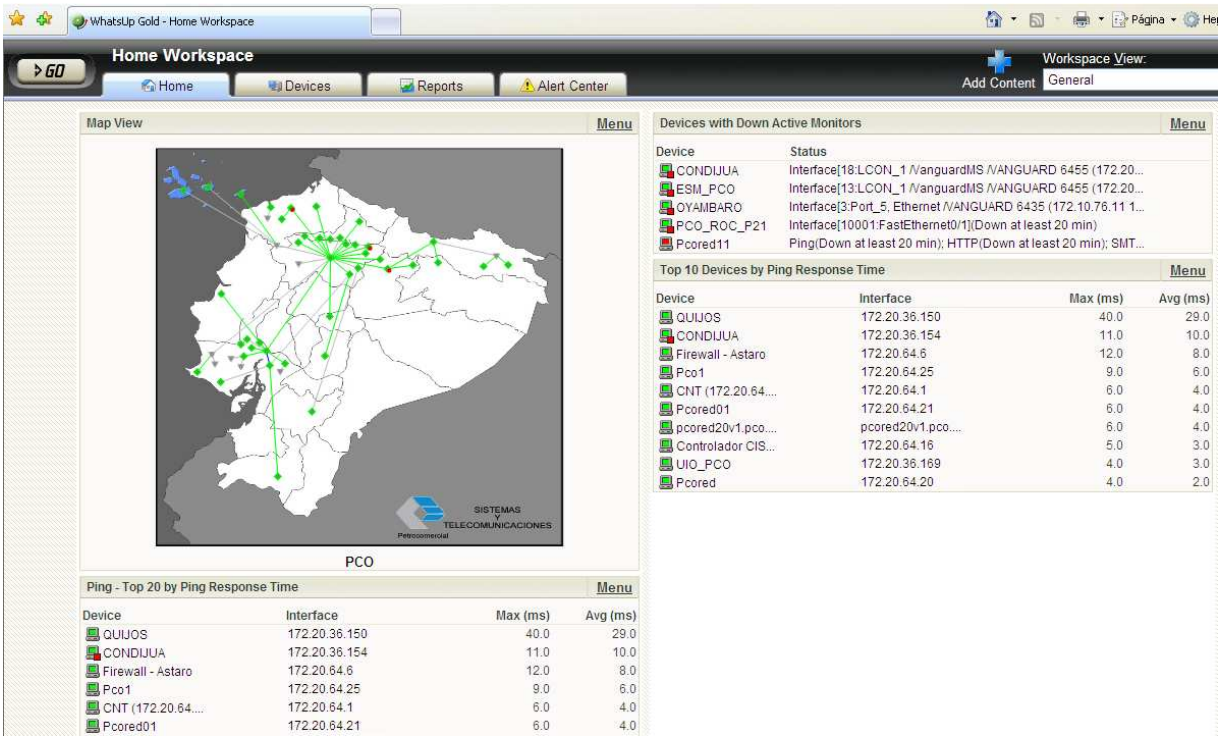


Figura 4.11 Interfaz de Inicio

Navegación a través de la interfaz web

El menú principal de la interfaz web está alojado en el botón GO (figura 4.12), ubicado en la parte superior izquierda del navegador. El menú GO es visible desde cualquier lugar dentro de la interfaz web.

Figura 4.12 Menú principal

Gestión de Dispositivos

En el sistema de monitoreo WhatsUp, los dispositivos son representaciones virtuales de los recursos (ordenadores, servidores, hubs, etc.) que están conectados a través de la red. Cuando los recursos de la red no pueden ser alcanzados por WhatsUp, el dispositivo se lo considera que está abajo y se puede configurar una acción para ser disparada cuando sucedan estos casos.

Acerca de la vista de Dispositivos

Esta perspectiva ofrece una visión general de cada dispositivo en un grupo seleccionado. El icono de cada dispositivo proporciona información sobre su tipo y estado. Además, la columna Estado indica el servicio específico y la duración de la interrupción. Cuando la entrada en la lista de dispositivos es una carpeta de grupo, la columna Estado muestra el número de dispositivos en el grupo con un desglose, indicando el número de dispositivos en cada estado.

Información acerca de las propiedades de dispositivos

Se puede modificar las propiedades de dispositivos individuales haciendo clic derecho en un icono de dispositivo ya sea en Ver Dispositivo o Ver Mapa, a continuación, se selecciona Propiedades (figura 4.13).

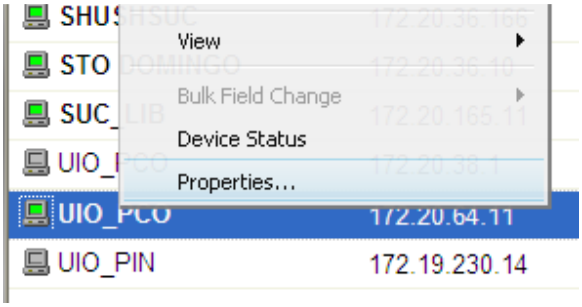


Figura 4.13 Acceder a propiedades de los equipos

Las propiedades que podemos encontrar en los dispositivos se las analizará más a detalle en el modelo de gestión implementado.

4.2.3. FUNCIONES DE GESTIÓN DE RED

Como se lo explicó anteriormente, el modelo a implementarse será una combinación de los modelos de gestión ISO/OSI e Internet. Se tomará el protocolo de gestión de red utilizado en el modelo Internet, SNMPv3, como medio de gestión para evaluar los parámetros indicados en el modelo funcional de ISO/OSI.

El modelo de Gestión ISO/OSI define 4 modelos básicos: Funcional, Organizacional, Comunicacional, Informativo. Para el modelo de gestión a desarrollarse se toma en cuenta el modelo funcional.

El modelo Funcional permite realizar las tareas de administración de la red, utilizando un conjunto de categorías generales conocidas como Fallos, Configuración, Contabilidad, Rendimiento y Seguridad (FCAPS por sus siglas en inglés). Cabe

destacar que en organizaciones de no-facturación, como es nuestro caso, *Contabilidad* se substituye a veces por *Administración*.

Utilizando un gestor como el software What's up y utilizando las mib's del protocolo SNMP, podemos brindar información acerca de las cinco capas funcionales de FCAPS, que se explican a continuación:

4.2.3.1. Administración de Fallas

Este apartado tiene como objetivo principal, mediante las herramientas de gestión, la detección y corrección de fallas que se den en los routers y switches a gestionarse en este proyecto.

Las áreas abarcadas en esta sección son:

- Detección de fallas.
- Manejo de Alarmas.
- Corrección del problema y verificación.

4.2.3.1.1. Detección de Fallas

La detección de errores es una tarea conjunta entre los dispositivos que actúan como agentes, en este caso los routers y switches, y la plataforma que actúa como gestor, en nuestro caso el software What's Up. Esta plataforma de gestión permite monitorear algunos parámetros de los routers y switches, como los observados en la figura 4.14, mediante el intercambio de mensajes snmp, y otras herramientas de detección de errores como ping o escaneo de puertos abiertos.

Los encargados de generar las respuestas a los parámetros indicados son los dispositivos Cisco y la herramienta de gestión What's Up es la responsable de recolectar esta información.

Monitor	State
Fan	Up at least 5 min
Ping	Up at least 5 min
Power supply	Up at least 5 min
Telnet	Up at least 5 min
Temperature	Up at least 5 min

Figura 4.14 Parámetros a monitorizar

El estado de estos parámetros se los puede representar gráficamente de la siguiente manera:

- Indicador Verde: El parámetro está activo por al menos 5 minutos.
- Indicador Amarillo: El parámetro está inactivo por al menos 2 minutos.
- Indicador Rojo: El parámetro está inactivo por al menos 5 minutos.

En la figura 4.15 se muestra los tipos de indicadores de estado.

Tue 12/07 1:06 PM	Interface (37) - Voice Over IF	Down at least 20 min
Tue 12/07 12:51 PM	Interface (37) - Voice Over IF	Down at least 5 min
Tue 12/07 12:49 PM	Interface (37) - Voice Over IF	Down at least 2 min
Tue 12/07 12:47 PM	Interface (37) - Voice Over IF	Down
Tue 12/07 11:12 AM	Telnet	Up at least 5 min
Tue 12/07 11:12 AM	HTTP	Up at least 5 min

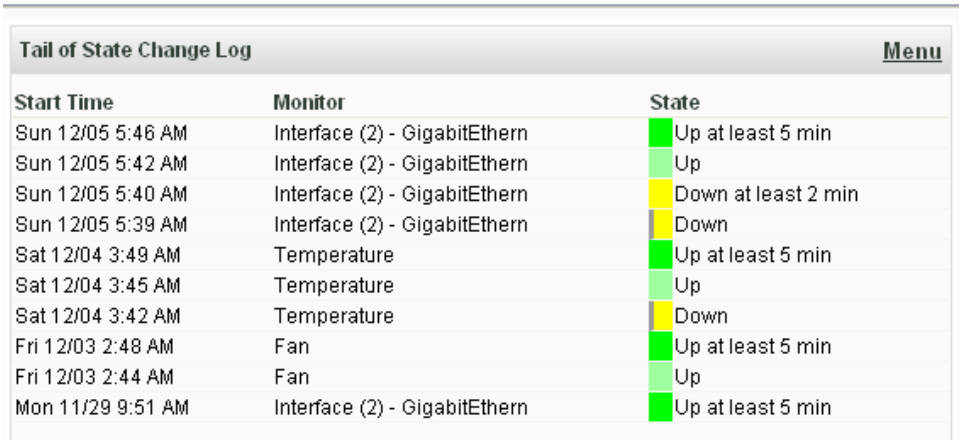
Figura 4.15 Indicadores de Estado

Una falla en los dispositivos gestionados puede estar asociada con los siguientes parámetros:

- Fan: Monitorea si está activo o no el ventilador del equipo
- Ping: Verifica la conectividad del equipo.
- Power Supply: Proporciona información sobre si está en funcionamiento la fuente de poder del equipo.
- Temperature: Muestra si el indicador de temperatura está activado.

Uno de los parámetros a ser monitorizados con mayor prioridad es el ping. La herramienta de gestión utilizada en este modelo nos permite comprobar la conectividad a nivel de la capa IP mediante mensajes ICMP (pings). Éste es un mecanismo básico pero eficaz para determinar la disponibilidad de un equipo o de su enlace.

En el workspace de What's Up podemos encontrar el log de las interfaces monitoreadas (figura 4.16) y los estados en que se encuentran (figura 4.17).



Tail of State Change Log — Menu

Start Time	Monitor	State
Sun 12/05 5:46 AM	Interface (2) - GigabitEthern	Up at least 5 min
Sun 12/05 5:42 AM	Interface (2) - GigabitEthern	Up
Sun 12/05 5:40 AM	Interface (2) - GigabitEthern	Down at least 2 min
Sun 12/05 5:39 AM	Interface (2) - GigabitEthern	Down
Sat 12/04 3:49 AM	Temperature	Up at least 5 min
Sat 12/04 3:45 AM	Temperature	Up
Sat 12/04 3:42 AM	Temperature	Down
Fri 12/03 2:48 AM	Fan	Up at least 5 min
Fri 12/03 2:44 AM	Fan	Up
Mon 11/29 9:51 AM	Interface (2) - GigabitEthern	Up at least 5 min

Figura 4.16 Tabla de los cambios de estados de las interfaces

Device Active Monitor States — Menu

Monitor	State
Interface (1) - ## LINK TO SW_ATACAZO - F0/0 ## (172.20.35.34	Up at least 5 min
Interface (10) - FastEthernet0/1/7	Unknown
Interface (11) - FastEthernet0/1/8	Unknown
Interface (13) - SSLVPN-VIF0	Up at least 5 min
Interface (14) - Null0	Up at least 5 min
Interface (15) - Vlan1	Unknown
Interface (2) - GigabitEthernet0/1 (172.20.76.14)	Up at least 5 min
Interface (3) - FastEthernet0/1/0	Unknown
Interface (4) - FastEthernet0/1/1	Unknown
Interface (5) - FastEthernet0/1/2	Unknown
Interface (6) - FastEthernet0/1/3	Unknown
Interface (7) - FastEthernet0/1/4	Unknown
Interface (8) - FastEthernet0/1/5	Unknown
Interface (9) - FastEthernet0/1/6	Unknown

Figura 4.17 Estado de las interfaces Monitoreadas.

Los dispositivos a ser monitorizados y sus interfaces se muestran en la tabla 4.1:

DISPOSITIVO	LUGAR	INTERFAZ	DESCRIPCIÓN
ROUTER CISCO 3845	ROCÍO	GigabitEthernet0/0	LINK TO SW_PICHINCHA - F0/5
		GigabitEthernet0/1	LINK TO SW_ATACAZO - F0/4
		FastEthernet0/1/0	LINK TO Pco_Roc_P50 - G5/42
		Vlan1	DATOS
		Vlan1001	VOZ
ROUTER CISCO 3825	BEATERIO	Vlan100	VLAN
		GigabitEthernet0/0	LINK TO SW_PICHINCHA - F0/1
		GigabitEthernet0/1	LAN
		FastEthernet0/1/0	VLAN 100
ROUTER CISCO 3825	STO. DOMINGO	GigabitEthernet0/0	LINK TO SW_ATACAZO - F0/5
		GigabitEthernet0/1	LAN
ROUTER CISCO 3825	GASOLINERA	GigabitEthernet0/0	LINK TO SW_PICHINCHA - F0/2
		GigabitEthernet0/1.1	LAN
		GigabitEthernet0/1.7	VIDEOSEG
ROUTER CISCO 3825	OYAMBARO	GigabitEthernet0/0	LINK TO SW_ATACAZO - F0/0
		GigabitEthernet0/1	LAN
ROUTER CISCO 3825	AEROPUERTO	GigabitEthernet0/0	LINK TO SW_PICHINCHA - F0/3
		Vlan1001	VOZ
		FastEthernet0/1/0	VLAN 1001
		Vlan1	DATOS
ROUTER CISCO 3825	CORAZON	GigabitEthernet0/0	TO SWITCH ATACAZO
		GigabitEthernet0/1	LAN
ROUTER CISCO 3825	FAISANES	GigabitEthernet0/0	TO SWITCH ATACAZO
		GigabitEthernet0/1	LAN
SWITCH CISCO	PICHINCHA	FastEthernet0/1	LINK TO BEATERIO - G0/0
		FastEthernet0/2	LINK TO GASOLINERA - G0/0
		FastEthernet0/3	LINK TO AEROPUERTO - G0/0
		FastEthernet0/4	LINK TO ATACAZO – Fa0/6
		FastEthernet0/5	LINK TO ROCIO - G0/0
SWITCH CISCO	ATACAZO	FastEthernet0/1	TO FAISANES
		FastEthernet0/2	TO OYAMBARO
		FastEthernet0/3	TO CORAZON
		FastEthernet0/4	TO UIO
		FastEthernet0/5	TO STO. DOMINGO
		FastEthernet0/6	TO PICHINCHA

Tabla 4.1 Interfaces a ser Monitoreadas

Todas las interfaces expuestas anteriormente de los equipos van a ser monitorizadas. Con el uso de la herramienta de monitoreo podemos detectar en qué dispositivo se produjo una falla y en que interfaz sucedió, lo que conlleva a la generación de alarmas que se explicara a continuación.

4.2.3.1.2. Manejo de Alarmas.

Una alarma se produce cuando algún parámetro monitorizado por la Herramienta de Gestión deja de estar activo o no responde. Una vez que se produjo la falla la herramienta alerta al administrador generando automáticamente un tipo de alarma predeterminado con anterioridad.

Con la plataforma de gestión What's Up tenemos la posibilidad de generar algunos tipos de alarmas, entre los principales están:

- Web Alarm: Esta alarma envía un sonido de alerta a la plataforma de administración en el web browser
- E-mail Action: Envía un E-mail al administrador indicando el problema ocurrido
- Sound Action: Envía un sonido a la consola donde esté instalado la herramienta de gestión.

Las alarmas aplicadas a los dispositivos implementados en este proyecto son: Sound Action, Web Alarm y E-mail Action. Con estas tres alarmas el administrador de red, que esté monitorizando los equipos a través de la web, recibirá una alerta sonora y por escrito, con el fin de que una vez haya sido informado sonoramente de un error en la red, puede verificarlo a través del mail, identificando el dispositivo involucrado y el tipo de error.

4.2.3.1.3. Corrección del Problema y Verificación.

Una vez que nos hemos ayudado con la herramienta de gestión para detectar la falla y manejar las alarmas producidas, el siguiente paso es la corrección del error, para ello debemos seguir algunas acciones.

Para los parámetros monitorizados como: FAN, Power Supply y Temperature se ha dispuesto los siguientes pasos a seguir para corregir el problema (figura 4.18):

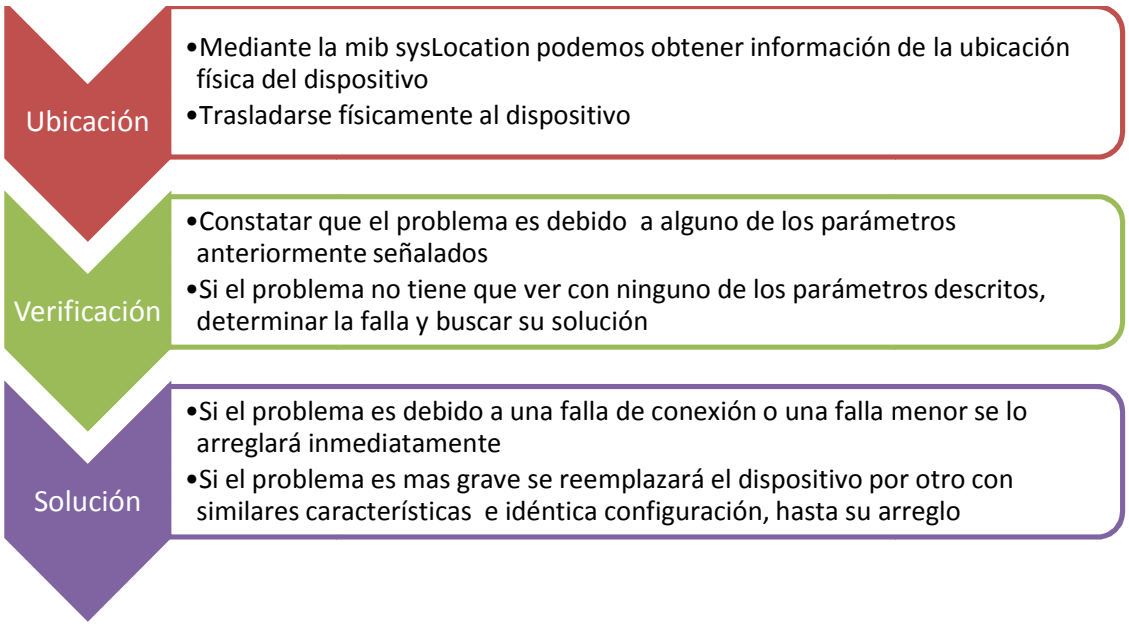


Figura 4.18 Pasos a seguir en la corrección del problema

Al realizarse estos pasos se procede a verificar su funcionamiento normal, fijándose en el estado de los parámetros que se muestra en el workspace del What's Up. Si el estado sigue sin ningún cambio (indicador de estado en rojo) se realizará nuevamente las acciones de la figura 4.18.

A diferencia de los parámetros anteriores que están ligados al hardware del equipo, el parámetro Ping, identificado como responsable del monitoreo de la conectividad, tiene varios factores a ser verificados para su corrección. Las soluciones a tomar son las siguientes (figura 4.19):

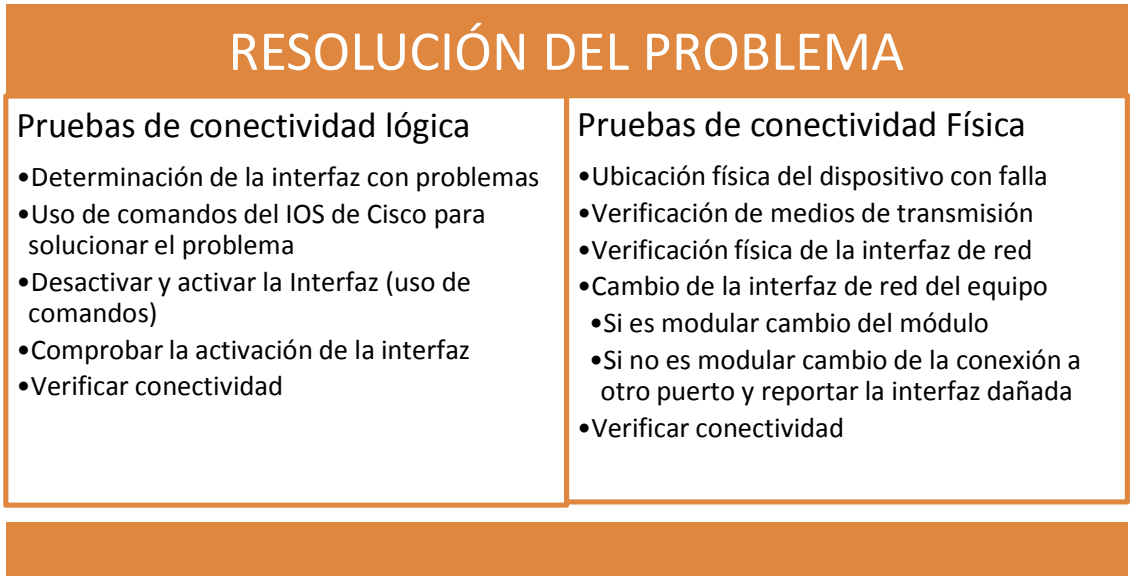


Figura 4.19 Pasos para la resolución de los problemas de conectividad

El procedimiento de recuperación de fallas se lo analizará a detalle más adelante.

4.2.3.2. Administración de Configuración

El objetivo de la administración de configuración permite la obtención de requerimientos de la red y utilización de los mismos para incorporar, mantener y retirar los diferentes componentes y recursos de la red.

La administración de configuración se basa en tres etapas:

- Recolección de datos sobre el estado de la red.
- Cambio en la configuración de los recursos.
- Almacenamiento de los datos de configuración.

4.2.3.2.1. Recolección de datos sobre el estado de la red

La recolección de datos de la red se lo puede realizar mediante dos herramientas de What´s Up, la primera el *autodescubrimiento* (*auto-discovery*) y la segunda la *autotopología* (*auto-mapping*).

Con la primera herramienta, como su nombre lo dice, podemos realizar un descubrimiento de los elementos activos de la red y determinar alguna de sus características más relevantes. Y con la segunda herramienta, la *autotopología*, conoceremos la forma en que están interconectados.

Auto-discovery

Utilizando la interfaz de What's Up logramos descubrir los elementos a ser gestionados, en este caso, los equipos de marca Cisco, routers y switches.

El procedimiento de auto-descubrimiento se lo realiza fácilmente a través de las herramientas de what's up, los pasos a seguir son los siguientes:

1. Click derecho en la interfaz, seleccionar *new device*
2. En la pantalla que aparece debemos tipear la dirección o el nombre del equipo en la opción *Ip address or host name of the device*
3. Si la información registrada es correcta, el dispositivo aparecerá en la interfaz de What's Up

La figura 4.20 indica el procedimiento auto-discovery de What's Up.

Figura 4.20 Procedimiento auto-discovery de What's Up

Esta herramienta de Gestión permite que se realice un almacenamiento centralizado de la información de los dispositivos de red, tal como nombre del dispositivo, descripción, número de serie, fabricante, ubicación física, contacto, cantidad de interfaces, etc.

A través de su mecanismo de auto descubrimiento (auto-discovery), la aplicación encuentra automáticamente las características básicas de un dispositivo, las que posteriormente pueden ser editadas manualmente desde la administración Web actualizando los registros.

La aplicación What's Up permite recolectar información del grupo MIB SYSTEM, que puede ser usada para la configuración de los dispositivos o para resolver problemas. Los grupos Mib de System recolectados son:

- sysDescr: Muestra la Descripción del dispositivo, incluyendo la marca del equipo, el tipo de software utilizado y su versión.
- sysObjectID: Muestra el identificadores de objeto del equipo
- sysUpTimeInstance: Indica el tiempo desde el cual ha estado activo el equipo, desde su descubrimiento.
- sysLocation: Indica la ubicación física del equipo
- sysContact: Señala la persona responsable del equipo
- sysName: Indica el nombre que ha sido configurado en el equipo.

En la figura 4.21 se muestra los grupos MIB encontrados en el auto-descubrimiento.

Figura 4.21 Características encontradas en el auto-descubrimiento.

Las mibs descritas en el grupo system, no son todas las que se puede recolectar con la herramienta auto-discovery de what's up. Por lo que utilizando el grupo mib de IP, específicamente el ipv4InterfaceTable, podemos obtener información importante para propósitos de configuración como la dirección IP del equipo. En la figura 4.22 se indica la información recolectada por la MIB ipv4InterfaceTable de IP.

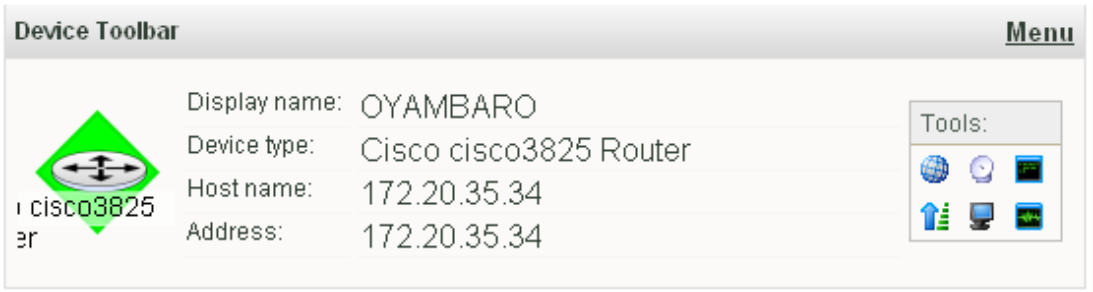


Figura 4.22 Información de la dirección IP del equipo

Adicionalmente What's Up emplea la mib Interface para determinar las interfaces del equipo y de qué tipo son: Ethernet, Fastethernet, GigabitEthernet. Además del tráfico generado por las interfaces. En la figura 4.23 se indica las interfaces descubiertas en el equipo.

Interface (2) - GigabitEthernet0/1 (172.20.76.14)	Up at least 5 min
Interface (3) - FastEthernet0/1/0	Unknown
Interface (4) - FastEthernet0/1/1	Unknown
Interface (5) - FastEthernet0/1/2	Unknown
Interface (6) - FastEthernet0/1/3	Unknown
Interface (7) - FastEthernet0/1/4	Unknown
Interface (8) - FastEthernet0/1/5	Unknown
Interface (9) - FastEthernet0/1/6	Unknown

Figura 4.23 Interfaces descubiertas en el equipo

Todos los parámetros revisados son de importante conocimiento ya que permiten mantener información de los equipos. Estos indicadores pueden ser utilizados para determinar qué tipo de equipos se encuentran en la red.

Auto-mapping

En este caso el auto-mapping se lo efectúa de forma manual ya que por defecto What's Up no lo realiza. Sin embargo su ejecución es fácil. Lo pasos a realizar son:

1. Click derecho en el dispositivo a interconectar
2. Seleccionar *Link to,* como indica la figura 4.24

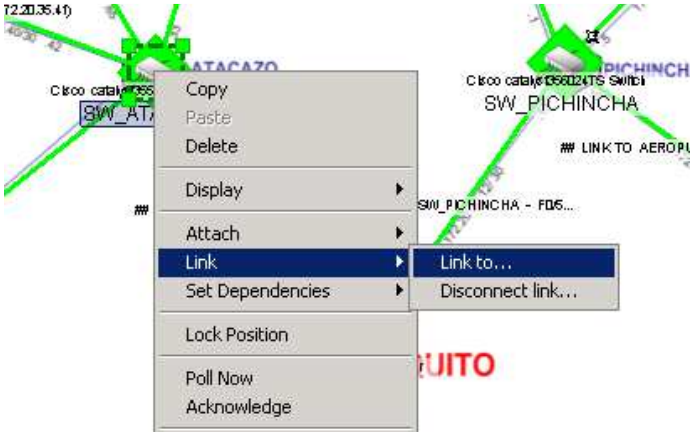


Figura 4.24 Paso 2 para el auto-mapping

3. Escoger la interfaz correcta a ser conectada con el otro dispositivo (figura 4.25).

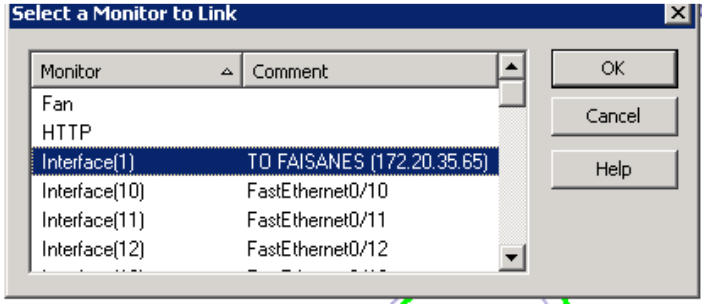


Figura 4.25 Paso 3 para el auto-mapping

4. Dar click en el otro dispositivo con el que se desea interconectar (figura 4.26).

Figura 4.26 Paso 4 para el auto-mapping

Las interfaces a conectarse entre equipos para la realización del auto-mapping son las indicadas en la tabla 4.2:

DISPOSITIVO	LUGAR	INTERFAZ LOCAL	A CONECTARSE CON
ROUTER CISCO 3845	ROCÍO	GigabitEthernet0/0	SW_PICHINCHA - F0/5
		GigabitEthernet0/1	SW_ATACAZO - F0/4
		FastEthernet0/1/0	SW_CORE - G5/42
ROUTER CISCO 3825	BEATERIO	GigabitEthernet0/0	SW_PICHINCHA - F0/1
ROUTER CISCO 3825	STO. DOMINGO	GigabitEthernet0/0	SW_ATACAZO - F0/5
ROUTER CISCO 3825	GASOLINERA	GigabitEthernet0/0	SW_PICHINCHA - F0/2
ROUTER CISCO 3825	OYAMBARO	GigabitEthernet0/0	SW_ATACAZO - F0/2
ROUTER CISCO 3825	AEROPUERTO	GigabitEthernet0/0	SW_PICHINCHA - F0/3
ROUTER CISCO 3825	CORAZON	GigabitEthernet0/0	SW_ATACAZO – F0/3
ROUTER CISCO 3825	FAISANES	GigabitEthernet0/0	SW_ATACAZO – F0/1
SWITCH CISCO	PICHINCHA	FastEthernet0/1	BEATERIO - G0/0
		FastEthernet0/2	GASOLINERA - G0/0
		FastEthernet0/3	AEROPUERTO - G0/0
		FastEthernet0/4	ATACAZO – Fa0/6
		FastEthernet0/5	ROCIO - G0/0
SWITCH CISCO	ATACAZO	FastEthernet0/1	FAISANES - G0/0
		FastEthernet0/2	OYAMBARO - G0/0
		FastEthernet0/3	CORAZON - G0/0
		FastEthernet0/4	ROCIO - G0/1
		FastEthernet0/5	STO. DOMINGO - G0/0
		FastEthernet0/6	PICHINCHA – FA0/4

Tabla 4.2 Interfaces a conectarse entre equipos

Como resultado del auto-discovery y del auto-mapping obtenemos un mapa topológico como se muestra en la figura 4.27.

La configuración para la recolección de datos puede ser realizada manualmente para obtener solo ciertos parámetros deseados.

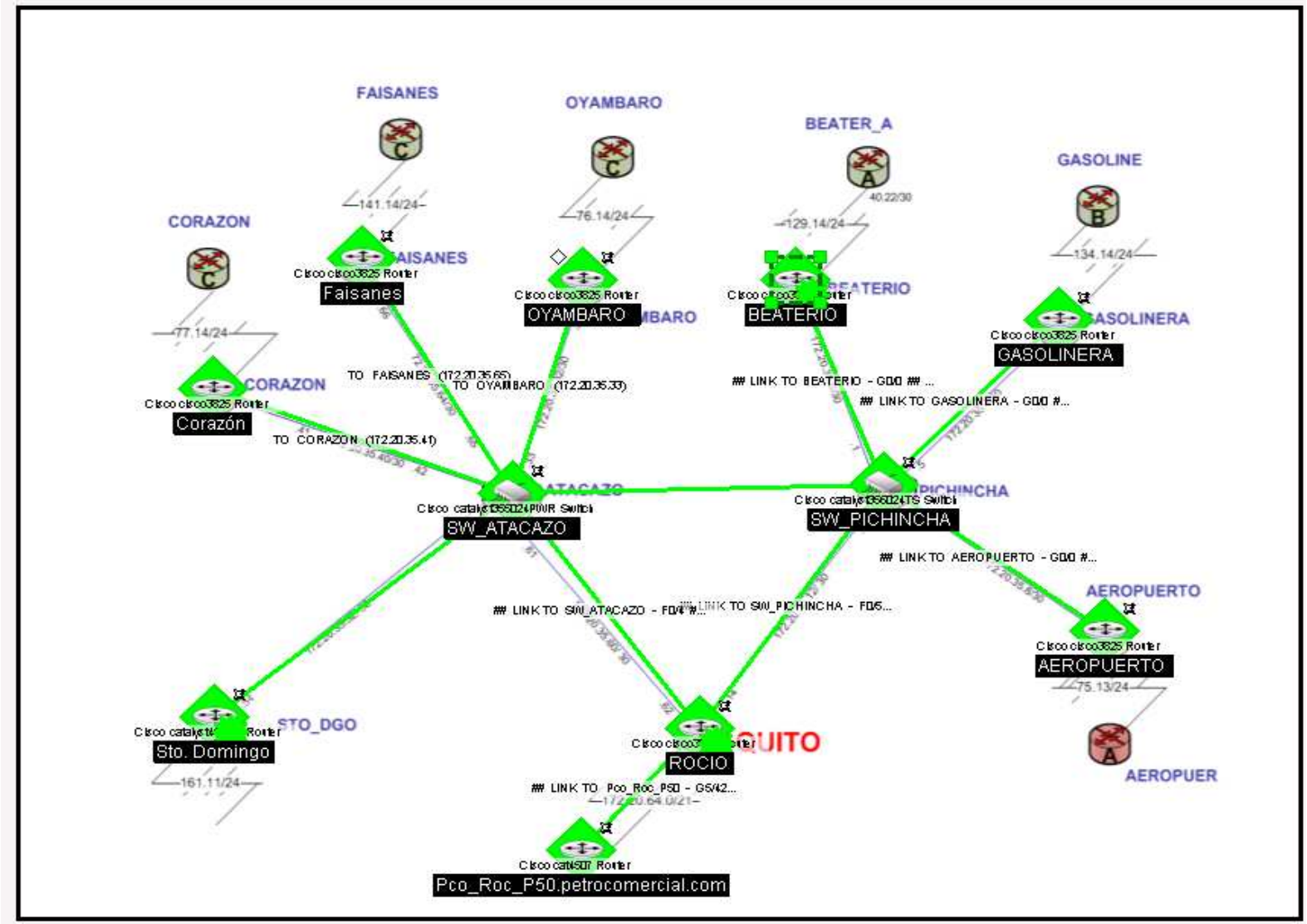


Figura 4.27 Mapa topológico utilizado en What's Up

4.2.3.2.2. Cambio en la Configuración de los Recursos.

Con la información obtenida del punto anterior, se determinarán los cambios necesarios a realizarse en las configuraciones (de ser necesario), además se determinara si un cambio solicitado por el área usuario de los servicios de red, es necesario.

Antes de cualquier cambio de configuración es obligatorio realizar un backup de la configuración actual.

Además es importante documentar los cambios realizados en la configuración de los equipos. El problema de no tener documentado los cambios realizados en los equipos de red, radica cuando se tiene un grupo de personas encargadas de la administración de la red, y se realiza un cambio sin que se ponga en conocimiento al resto del grupo, lo que puede causar confusiones en la administración del equipo, derivando en problemas de funcionamiento y hasta errores de conectividad.

La finalidad de este procedimiento es mantener una información de configuración de la red actualizada y que ayude a una mejor administración de los dispositivos de la red, ayudando a disminuir los tiempos de respuesta en caso de errores o cambios en la configuración de los equipos que ayuden a mejorar el desempeño de los dispositivos en la red.

En la figura 4.28 se muestra el documento de registro de los cambios realizados en los equipos de red.

EP PETROECUADOR

REGISTRO DE CONFIGURACION **FO-TIC'S-001**

Nro.: Fecha:

Técnico:_____Unidad:_____Área:_____

Descripción del equipo

Marca y Modelo: _____

Nombre del equipo:_____

Dirección IP:_____

Hora de reporte: _____ Hora de Inicio:_____

Hardware: ☐ Software: ☐

Técnico Responsable

_____ _____

Nombre Firma

Propósito de la configuración:

Configuración realizada:

Figura 4.28 Hoja tipo para registrar cambios realizados en la configuración

4.2.3.2.3. Almacenamiento de los Datos de Configuración.

Las hojas de registro de configuraciones deben ser digitalizadas y almacenadas tanto en una carpeta de acceso general como en un repositorio digital.

El objetivo de esta práctica es el de mantener en un mismo lugar y de manera ordenada las configuraciones de todos los equipos de la red, con el propósito de que en un eventual fallo de un equipo o cambio de configuración, permita una respuesta más rápida y con toda la información necesaria.

Para respaldar las configuraciones de los equipos se utilizó el programa Cisco TFTP Server v1.1, instalado en una máquina que servirá como repositorio de todas las configuraciones. El procedimiento para respaldar las configuraciones es el siguiente:

1. Ingresar al equipo que se desea respaldar la configuración, al modo EXEC privilegiado.

2. Verificar conectividad con el servidor TFTP, utilizando el comando:
*ping 172.20.64.xxx(*Dirección IP de la máquina que actua como servidor TFTP*).*

3. Copiar la configuracion del equipo utilizando el comando en el modo EXEC privilegiado:

En la figura 4.29 se indica los pasos a realizar para copiar la configuración al tftp.

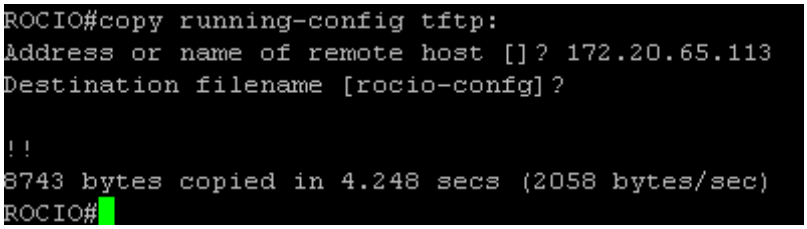


Figura 4.29 Comandos para copiar la configuración al tftp

La figura 4.30 indica que el archivo ha sido copiado en el equipo repositorio.

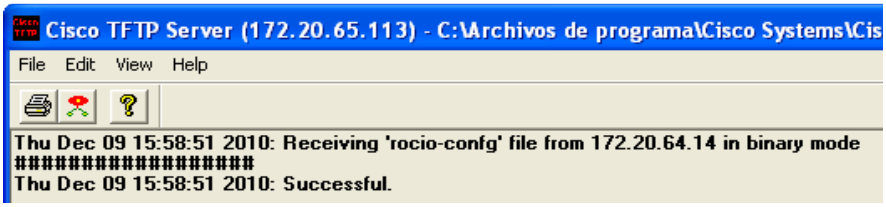


Figura 4.30 Archivo copia exitosamente en el equipo repositorio

4. Guardar la configuración del router o switch, en la máquina que actua como repositorio, en una carpeta con el nombre del router o switch y la fecha de realización del respaldo.

Además de los backup que se realicen cuando exista un cambio en la configuración se debe realizar el respaldo de todos los equipos cada 2 semanas. Además se debe sacar copias físicas de los respaldos de las configuraciones cada 2 meses.

La práctica adecuada y constante de este proceso de respaldo, garantiza una mejora en la administración de los recursos de red y reduce el riesgo de una pérdida total de la información contenida.

4.2.3.3. Administración de Rendimiento

Utilizamos la administración de rendimiento para mantener un estado óptimo de la red y sus dispositivos, asegurando que en todo momento esté operando eficientemente. Las tareas que se realizan en la administración de rendimiento son:

- Recolección de datos significativos que indiquen los niveles de rendimiento como, el throughtput de la red, tiempo de respuesta y latencia, utilización de las interfaces, entre otros.
- Análisis de los datos para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.

4.2.3.3.1. Indicadores de Niveles de Rendimiento

Dentro de los indicadores que permiten medir el rendimiento de los dispositivos en la red, la herramienta de gestión What´s Up, nos brinda algunos parámetros como son:

- CPU Utilization: Permite monitorear la utilización de CPU del dispositivo
- Interface Utilization: Muestra el porcentaje de utilización de cada Interfaz
- Memory Utilization: Indica el porcentaje de utilización de la memoria del equipo
- Ping Latency and Availability: Permite monitorear la latencia y disponibilidad de los mensajes ping.

En la figura 4.31 se muestran los indicadores de nivel de rendimiento definidos por What`s Up.

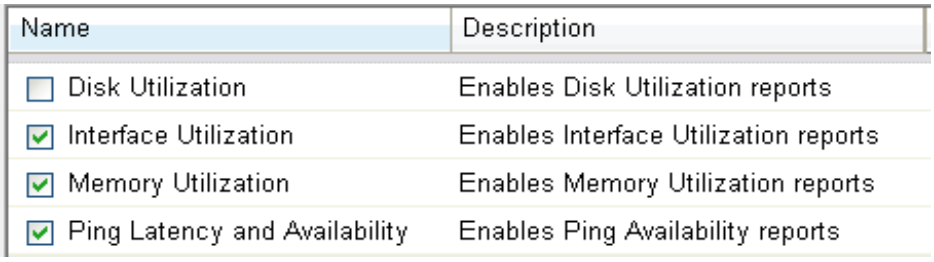


Figura 4.31 Parámetros definidos por What´s Up para medir el rendimiento

CPU Utilization.

Este parámetro indica el porcentaje de utilización de cpu, de los equipos de la red, se lo puede monitorear tanto en tiempo real como en un determinado periodo de tiempo. Los valores que son recolectados por la herramienta de gestión son: porcentaje mínimo de utilización, porcentaje máximo de utilización y un porcentaje promedio de utilización. La figura 4.32 indica el parámetro para medir el rendimiento, CPU utilization.

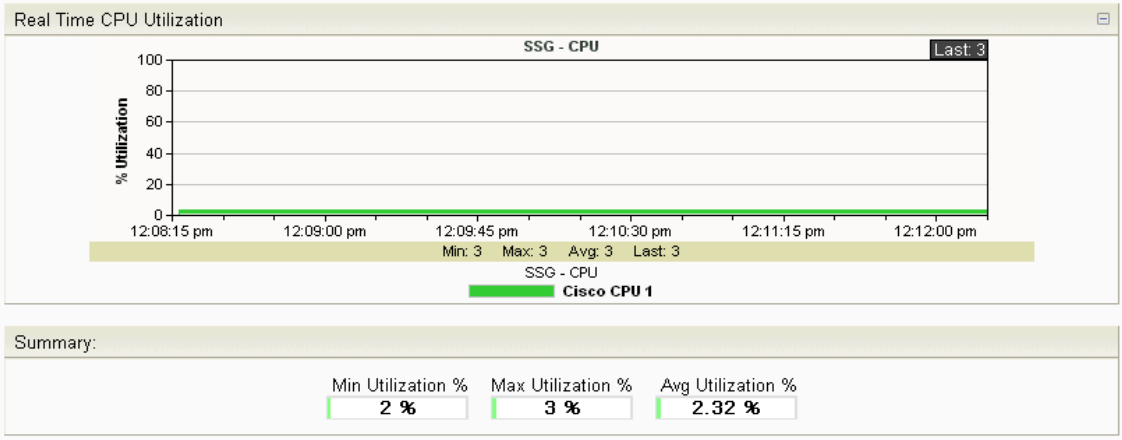


Figura 4.32 Indicador de la utilización de CPU de un equipo de red

Interface Utilization

Este parámetro utiliza la mib IfInOctects para determinar la cantidad de bites de recepción, y la mib IfOutOctects para determinar la cantidad de bites de transmisión, con estos valores generados por las mibs y recolectados por What´s Up, determinamos el tráfico que cruza por las interfaces y el porcentaje de utilización de las mismas, destacando los valores máximo, mínimo y promedio. Se lo monitorea en tiempo real y en un periodo de tiempo determinado. La monitorización de las interfaces se lo realiza de manera individual. La figura 4.33 indica el parámetro para medir el rendimiento, Interface utilization.

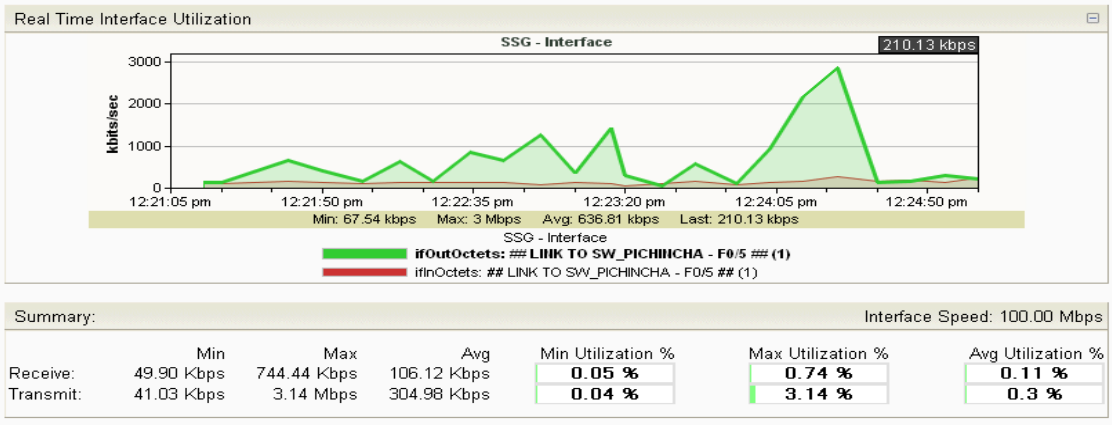


Figura 4.33 Indicador del porcentaje de utilización de las interfaces y su tráfico

Memory Utilization

Este indicador de rendimiento muestra el porcentaje de utilización de la memoria del equipo de red tanto de la memoria del procesador como de la memoria de entrada y salida. Su monitorización se lo realiza en tiempo real y en un periodo de tiempo determinado. Los valores mostrados por este parámetro son: el tamaño total de la memoria en MB, su espacio máximo, mínimo y el promedio utilizado, además del porcentaje de utilización mínimo, máximo y promedio. La figura 4.34 indica el parámetro para medir el rendimiento, Memory utilization.

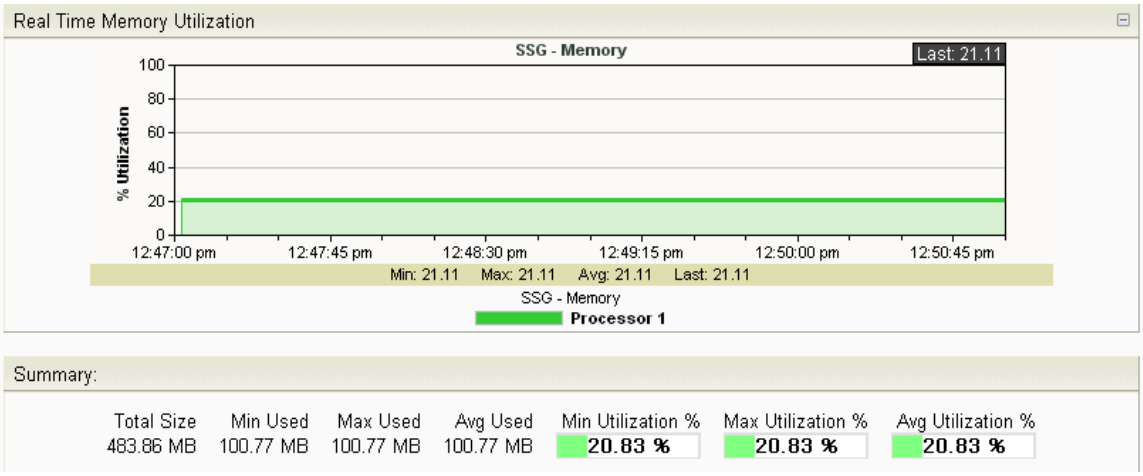


Figura 4.34 Indicador de la utilización de Memoria y el porcentaje.

Ping Latency and Availability

Estos parámetros muestran dos valores importantes correspondientes al ping, el primero es la disponibilidad y el segundo corresponde al tiempo de respuesta o latencia del ping.

El indicador de latencia del ping se lo puede monitorear en tiempo real y nos indica valores como el tiempo de respuesta mínimo, el tiempo máximo de respuesta y el tiempo de respuesta promedio. En la figura 4.35 se indica todos estos parámetros.

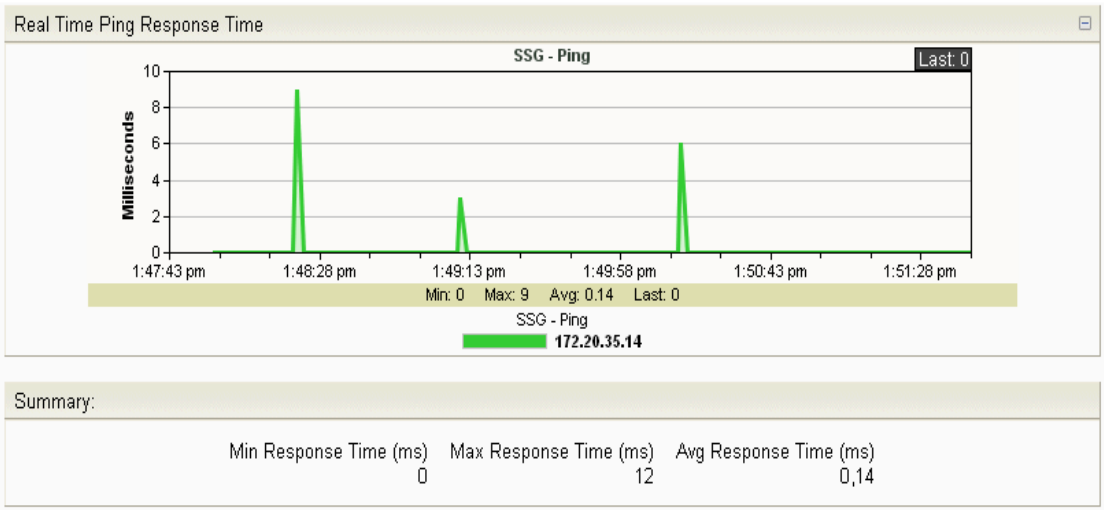


Figura 4.35 Indicador de la Latencia del ping en un equipo de red

El indicador de disponibilidad del ping muestra valores como: los paquetes que han sido enviados durante un periodo de tiempo, los paquetes perdidos, porcentaje de paquetes perdidos, el tiempo en que se ha realizado los pings, el tiempo que no ha estado disponible y el porcentaje de disponibilidad. En la figura 4.36 se indica todos estos parámetros.

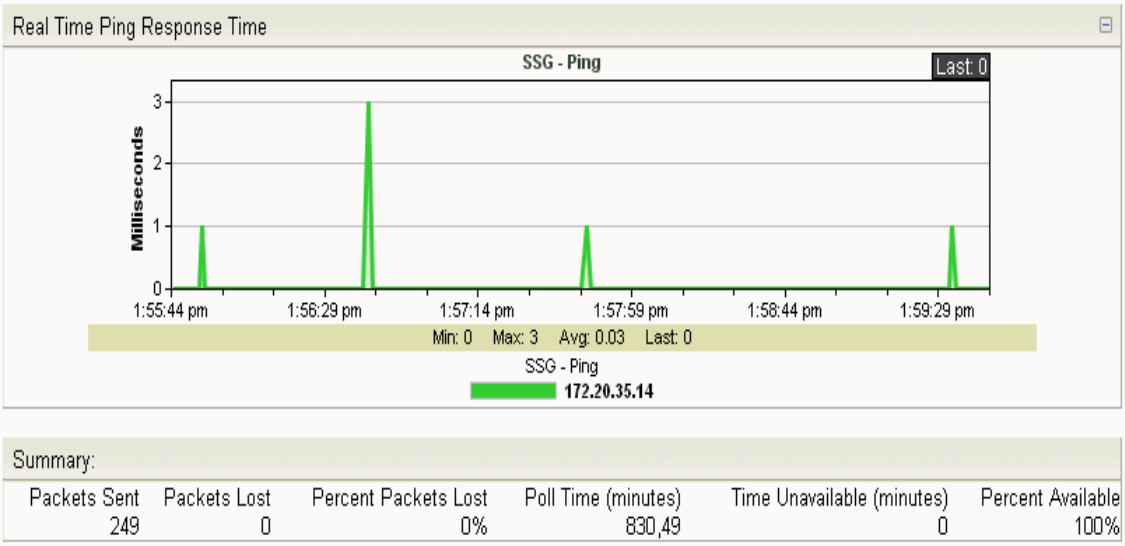


Figura 4.36 Indicador de disponibilidad del ping en un equipo de red

4.2.3.3.2. Alarmas de niveles de rendimiento

Las alarmas de rendimiento son disparadas cuando se sobrepasan los umbrales configurados, se notifica al administrador de red mediante correo electrónico, con tres niveles de escalamiento. Cuando la alarma es disparada es notificado en la cuenta de correo del técnico encargado de la red WAN, si en 10 min no es resuelto el problema es notificado en la cuenta del técnico líder, si en 30 min no es superado el problema es notificado en la cuenta del supervisor de infraestructura de comunicaciones, la notificación en la escala 3 es enviado cada hora hasta que se solucione el problema.

4.2.3.3.3. Análisis de los Datos

Utilizando los parámetros de rendimiento de los dispositivos, se consigue generar varios reportes, los cuales ayudarán para el establecimiento de umbrales de algunos indicadores de rendimiento y servirán para una recopilación continua de los datos. Estos dos últimos puntos se los revisará más adelante.

Los reportes que pueden ser generados, se derivan de los indicadores de rendimiento, por lo que estos registros incluyen los analizados en el punto anterior, pero además incluyen otros reportes como:

- Active Monitor Availability
- Interface Discard
- Interface Errors
- State Change Timeline

<u>Active Monitor Availability</u>

Permite monitorear en tiempo real el estado de una interfaz de algún equipo de la red. Muestra durante un periodo de tiempo el porcentaje en el que la interfaz estuvo

disponible, en mantenimiento, sin estado, no disponible y su disponibilidad actual. La figura 4.37 indica el monitor de disponibilidad de la interfaz.

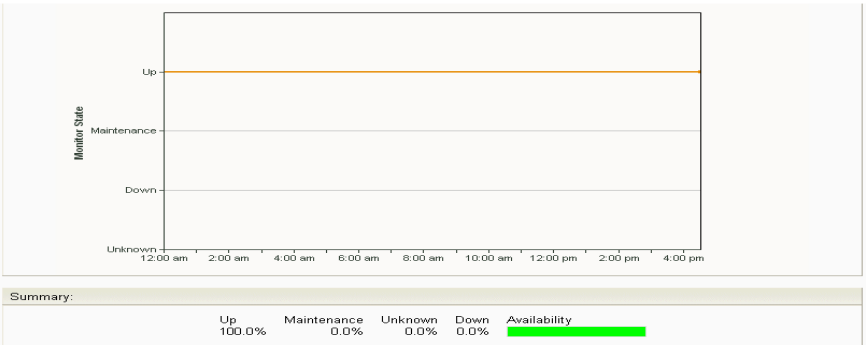


Figura 4.37 Monitor de disponibilidad de la interfaz

Interface Discard

Este monitor muestra el número de interfaces descartadas durante un minuto, tanto en transmisión como en recepción. Sus valores de descarte de interfaces son el mínimo, máximo y un promedio durante un periodo de tiempo. La figura 4.38 indica el monitor de Interface Discard.

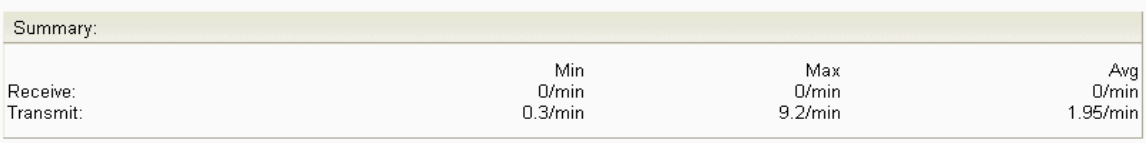


Figura 4.38 Monitor Interface Discard

Interface Errors

Permite observar el número de interfaces con error en un periodo de un minuto, tanto para recepción como para transmisión. Los valores indicados son: mínimo, máximo y un promedio de los errores de interfaces por minuto. En la figura 4.39 se indica el monitor de Interface Errors.

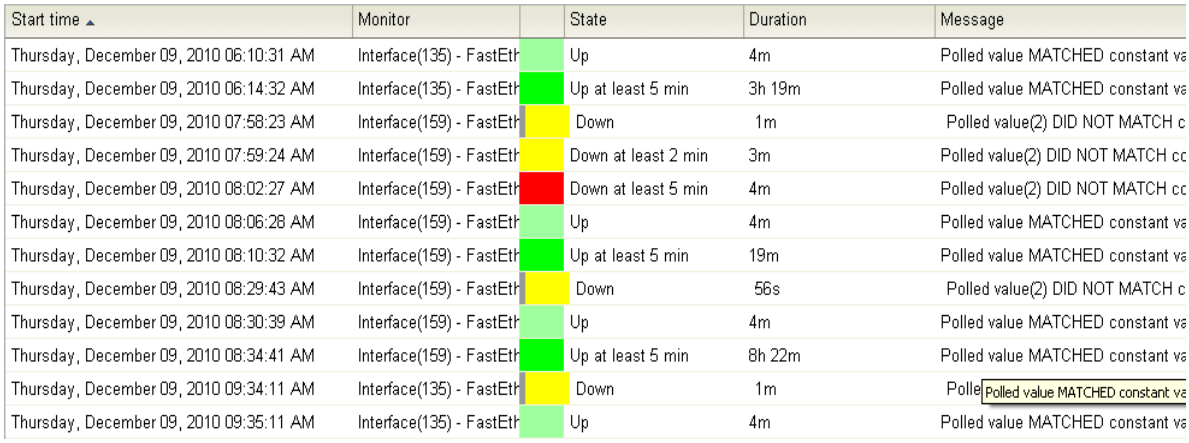
Summary:

	Min	Max	Avg
Receive:	0/min	0.1/min	0/min
Transmit:	0/min	0/min	0/min

Figura 4.39 Monitor Interface Errors

State Change Timeline

Este reporte indica los cambios de estado que ha tenido una interfaz en particular durante un periodo de tiempo. Muestra la fecha y hora en que se produjo el cambio de estado, que interfaz, el estado, cuánto tiempo duró en ese estado y su mensaje. En la figura 4.40 se indica el monitor State Change Timeline.



Start time	Monitor		State	Duration	Message
Thursday, December 09, 2010 06:10:31 AM	Interface(135) - FastEth		Up	4m	Polled value MATCHED constant va
Thursday, December 09, 2010 06:14:32 AM	Interface(135) - FastEth		Up at least 5 min	3h 19m	Polled value MATCHED constant va
Thursday, December 09, 2010 07:58:23 AM	Interface(159) - FastEth		Down	1m	Polled value(2) DID NOT MATCH c
Thursday, December 09, 2010 07:59:24 AM	Interface(159) - FastEth		Down at least 2 min	3m	Polled value(2) DID NOT MATCH cc
Thursday, December 09, 2010 08:02:27 AM	Interface(159) - FastEth		Down at least 5 min	4m	Polled value(2) DID NOT MATCH cc
Thursday, December 09, 2010 08:06:28 AM	Interface(159) - FastEth		Up	4m	Polled value MATCHED constant va
Thursday, December 09, 2010 08:10:32 AM	Interface(159) - FastEth		Up at least 5 min	19m	Polled value MATCHED constant va
Thursday, December 09, 2010 08:29:43 AM	Interface(159) - FastEth		Down	56s	Polled value(2) DID NOT MATCH c
Thursday, December 09, 2010 08:30:39 AM	Interface(159) - FastEth		Up	4m	Polled value MATCHED constant va
Thursday, December 09, 2010 08:34:41 AM	Interface(159) - FastEth		Up at least 5 min	8h 22m	Polled value MATCHED constant va
Thursday, December 09, 2010 09:34:11 AM	Interface(135) - FastEth		Down	1m	Polle Polled value MATCHED constant va
Thursday, December 09, 2010 09:35:11 AM	Interface(135) - FastEth		Up	4m	Polled value MATCHED constant va

Figura 4.40 Monitor State Change Timeline

4.2.3.3.4. Establecimiento De Umbrales

La necesidad de establecer umbrales en ciertos recursos de los dispositivos, está relacionada con el propósito de mantener un desempeño óptimo de los dispositivos de la red.

Es importante mantener umbrales en indicadores críticos como el ping para establecer conectividad, además estos umbrales manejan alarmas que alertan de

posibles errores en los equipos, antes de que estos sucedan, permitiendo al administrador de red tener un tiempo prudencial para la resolución del problema.

Las principales alarmas de umbrales son:

- Performance Ping Availability Falls Below 96,67%
  La base de tiempo en el que se toma la medida es 5 min, el tiempo de tolerancia de pérdida de enlace es de 10 segundos por tanto:

$$d = \frac{290\ X\ 100}{300}$$

$$d = 96{,}67\ \%$$

- Performance Ping Response Time Exceeds 10 ms
  Debido a que el cálculo del tiempo de respuesta de ping depende de los tiempos de: transmisión, propagación, recepción y latencia en los equipo y que calcular los tiempos de latencia es sumamente complejo, se determinará el valor estadísticamente, el lugar más distante y por ende más crítico es Santo Domingo estadísticamente el tiempo de respuesta de un paquete de ping con los parámetros normales es de 10 ms.

  Para el uso de recursos se utiliza un umbral del 80%:

- Performance Memory Utilization Exceeds 80%
- Performance Interface Utilization Exceeds 80%
- Performance CPU Utilization Exceeds 80%

Performance Ping Availability Falls Below 96,67%

Esta alarma de umbral alerta al administrador de red cuando el promedio de disponibilidad de ping de algún elemento de la red, es menor del 96,67 por ciento en un rango de 5 minutos. En la figura 4.41 se indica los dispositivos alarmados debido al umbral de la disponibilidad del Ping.

Performance Ping Availability Falls Below 98.33%

Description: Average Ping Availability during the past 30 minutes falls below 98%

Device	Interface	Percent Available	Time Alerted
AEROPUERTO	172.20.35.9	66,7 %	Wed 12/08 6:17 PM
Pco_Roc_P52	172.20.64.152	51,4 %	Tue 12/07 11:38 AM
Pco_Roc_P51	172.20.64.151	51,4 %	Tue 12/07 11:38 AM
Pco_Roc_P20	172.20.64.140	51,4 %	Tue 12/07 11:38 AM
Pco_Roc_P21	172.20.64.141	51,4 %	Tue 12/07 11:38 AM
Pco_Roc_P22	172.20.64.142	51,4 %	Tue 12/07 11:38 AM
Pco_Roc_P01	172.20.64.132	51,4 %	Tue 12/07 11:38 AM
PCORED01	172.20.64.21	51,4 %	Tue 12/07 11:38 AM

Figura 4.41 Dispositivos alarmados debido al umbral de la disponibilidad del Ping

Performance Ping Response Time Exceeds 10 ms

Esta alarma surge cuando un dispositivo ha excedido los 10 ms como tiempo de respuesta promedio en los últimos 30 minutos. En la figura 4.42 se indica los dispositivos alarmados debido al umbral de Respuesta del Ping.

Performance Ping Response Time Exceeds 10 ms

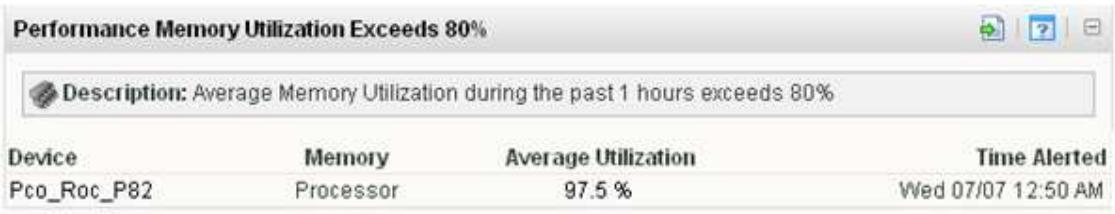
Description: Average Ping Response Time during the past 30 minutes exceeds 10ms

Device	Interface	Response Time Average	Time Alerted
PRO_CORREO	172.16.49.31	73,99 ms	Wed 12/08 3:08 PM
172.19.40.5	172.19.40.5	72,33 ms	Wed 12/08 2:50 PM
SEG_FIS_ SISTEMAS	172.31.64.14	50,71 ms	Wed 12/08 6:58 AM
172.20.129.9	172.20.129.9	54,37 ms	Wed 12/08 6:58 AM
172.19.231.57	172.19.231.57	303,55 ms	Tue 12/07 1:48 PM
ROCIO	172.20.64.14	61,30 ms	Thu 11/11 2:08 PM
www.google.com	74.125.67.105	91,03 ms	Thu 11/11 10:02 AM
GASOLINE	172.20.134.11	58.00 ms	Sun 10/10 2:26 PM
VANG_GASO	172.20.134.11	52.67 ms	Sun 10/10 1:26 PM

Figura 4.42 Dispositivos alarmados debido al umbral de Respuesta del Ping

Performance Memory Utilization Exceeds 80%

Esta alarma de umbral se da cuando un dispositivo excede en un 80 por ciento la utilización de memoria de su equipo durante la última hora. En la figura 4.43 se indica los dispositivos alarmados debido al umbral de Utilización de Memoria.



Performance Memory Utilization Exceeds 80%

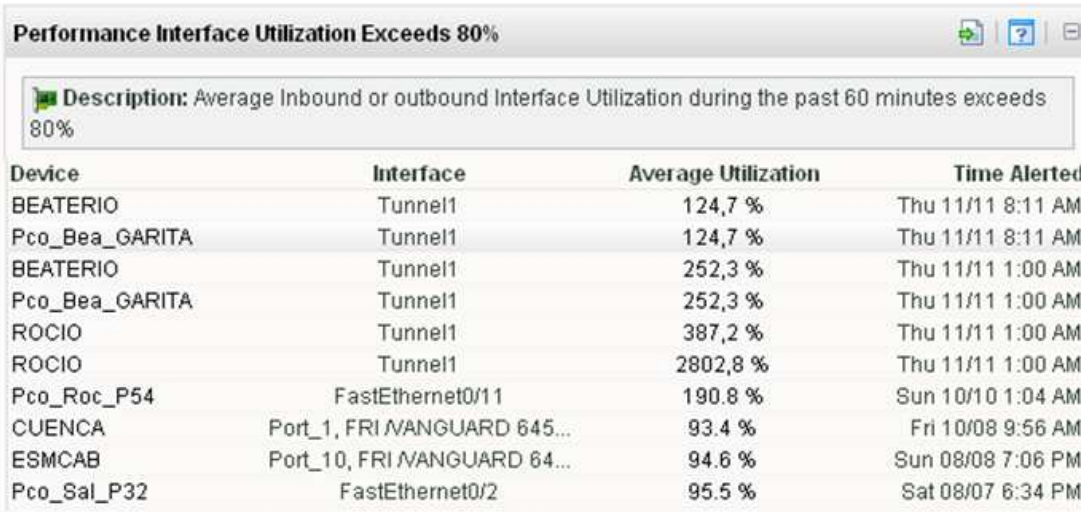
Description: Average Memory Utilization during the past 1 hours exceeds 80%

Device	Memory	Average Utilization	Time Alerted
Pco_Roc_P82	Processor	97.5 %	Wed 07/07 12:50 AM

Figura 4.43 Dispositivos alarmados debido al umbral de Utilización de Memoria

Performance Interface Utilization Exceeds 80%

El administrador de red recibe esta alarma cuando la utilización de una interfaz en alguno de los dispositivos de red excede al 80 por ciento de utilización. En la figura 4.44 se indica los dispositivos alarmados debido al umbral de Utilización de la Interfaz.



Performance Interface Utilization Exceeds 80%

Description: Average Inbound or outbound Interface Utilization during the past 60 minutes exceeds 80%

Device	Interface	Average Utilization	Time Alerted
BEATERIO	Tunnel1	124,7 %	Thu 11/11 8:11 AM
Pco_Bea_GARITA	Tunnel1	124,7 %	Thu 11/11 8:11 AM
BEATERIO	Tunnel1	252,3 %	Thu 11/11 1:00 AM
Pco_Bea_GARITA	Tunnel1	252,3 %	Thu 11/11 1:00 AM
ROCIO	Tunnel1	387,2 %	Thu 11/11 1:00 AM
ROCIO	Tunnel1	2802,8 %	Thu 11/11 1:00 AM
Pco_Roc_P54	FastEthernet0/11	190.8 %	Sun 10/10 1:04 AM
CUENCA	Port_1, FRI /VANGUARD 645...	93.4 %	Fri 10/08 9:56 AM
ESMCAB	Port_10, FRI /VANGUARD 64...	94.6 %	Sun 08/08 7:06 PM
Pco_Sal_P32	FastEthernet0/2	95.5 %	Sat 08/07 6:34 PM

Figura 4.44 Dispositivos alarmados debido al umbral de Utilización de la Interfaz

Performance Cpu Utilization Exceeds 80%

Esta alarma de umbral se da cuando un dispositivo excede en un 80 por ciento la utilización del CPU de su equipo durante los últimos 30 minutos. En la figura 4.45 se indica si algún dispositivo está alarmado debido al umbral.

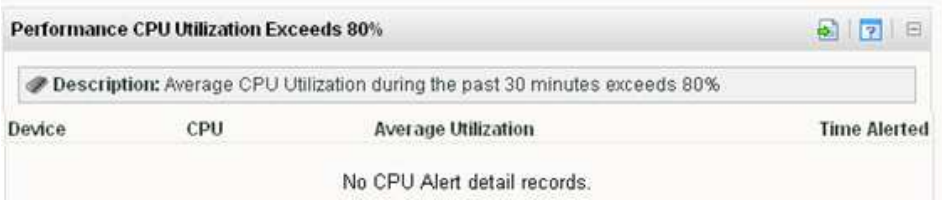


Figura 4.45 Muestra si algún Dispositivo está alarmado debido al umbral

4.2.3.3.5. Recopilación De Datos

Se puede establecer una recopilación programada de datos, que ayudará a mantener información de la red actualizada, sin la necesidad que intervenga el administrador. Los principales reportes programados son:

- System: Se visualiza los logs y los diagnósticos de datos para todos los dispositivos.
- Group: Compara la disponibilidad y el rendimiento de un grupo de dispositivos específicos.
- Device: Reporta acerca de la disponibilidad y rendimiento pero solo de un dispositivo a la vez, sus reportes son similares al de Group.
- Alert Center: En este tipo de reporte se puede observar los datos generados por las alarmas de umbral
- Performance: Brinda reportes de rendimiento tanto de los dispositivos grupalmente como individualmente.
- Problem Areas: Se puede observar reportes de alertas a través de toda la red y su solución aplicada.
- General: Muestra los reportes de What's Up gold más generales

4.2.3.4. Administración de Contabilidad

En un principio la administración de contabilidad tiene como objetivo recopilar información de la red para luego establecer una cuota de los servicios ofrecidos, y determinar un precio que deban pagar los usuarios por la utilización de dichos recursos. Este procedimiento se lo realiza en empresas o instituciones de lucro.

Dado el caso que el Proyecto de Titulación se lo realiza en una empresa pública en un área que no tiene como objetivo lucrar de los servicios ofrecidos, este apartado de administración de contabilidad no se aplica, sin embargo para departamentos sin fines de lucro se puede utilizar la administración de contabilidad para recopilar información y mantener un inventario.

La gestión de contabilidad es importante para mantener documentada toda la información detallada de la red de datos; información tal como: topología, configuraciones, indicadores de rendimiento, registro de fallas entre otros.

Para llevar la contabilidad se determinan parámetros que sirven para mantener un registro de la red totalmente claro y ordenado. Los siguientes son puntos a tomar en cuenta en la realización del inventario:

- Tráfico entrante y saliente de las interfaces más importantes de los equipos de red.
- Cantidad de ocupación de la capacidad de disco y de memoria de los equipos.
- Porcentaje de uso del procesador del equipo, permite determinar si un equipo está o no en óptimas condiciones.
- Porcentaje de paquetes enviados y perdidos en una interfaz monitoreada de un equipo. Ayuda a determinar el problema de la interfaz y buscar posibles soluciones.

- Registro de las alarmas generadas por los equipos. Permite mantener un reporte de los errores sucedidos en los dispositivos, para determinar sus soluciones en el menor tiempo posible.
- Reportes de fallos.
- Reportes de configuración.
- Inventario de medidas de seguridad de los equipos.

Todos los datos recopilados, ya sean estadísticas, reportes o gráficos se los deberá incluir en el inventario. Estos datos serán de gran ayuda para el administrador de red, que deberá evaluarlos para poder determinar soluciones óptimas y precisas en caso de errores o tomar decisiones de planeación para la red y en general para determinar el estado de la red.

El inventario será almacenado en un servidor de gran capacidad de disco duro con permisos de acceso solo para el administrador de red.

4.2.3.5. Administración de Seguridad

La administración de seguridad tiene mucha relevancia en el modelo de gestión, debido a que sin la aplicación correcta de este, todas las demás actividades del modelo funcional de ISO/OSI, no tuvieran relevancia.

El aplicar correctamente este modelo de administración de seguridad, beneficia a las demás capas de administración del modelo funcional de ISO/OSI. Su relevancia es alta debido a que sin este modelo las demás capas de administración pueden funcionar incorrectamente, ya sea por un ataque a los equipos de una persona externa o interna, que comprometa el uso de la red y por ende la administración de fallas, la administración de configuración, la administración de rendimiento, la administración de contabilidad y evidentemente la administración de seguridad.

La administración de seguridad se la utiliza para evitar ataques tales como:

- Abuso interno de acceso a la red
- Denegación de servicio
- Acceso no autorizado al sistema
- Detección de passwords.

Aspectos de Seguridad de los Routers:

- Seguridad en la parte física.
- Actualización del IOS de los equipos cuando sea necesario.
- Copia de seguridad de la configuración y del IOS de los equipos.
- Control de los componentes de los equipos para evitar el uso no autorizado de los puertos y servicios.

Para proporcionar seguridad física, se debe ubicar los equipos en un lugar cerrado, donde sólo pueda ingresar personal autorizado. El lugar debe poseer todos los parámetros adecuados para el correcto funcionamiento de los equipos, ya sean estos controles de temperatura y humedad o protecciones para interferencias electrostáticas y magnéticas. Además para reducir la posibilidad de denegación de servicio en los equipos debido a una falla en la energía eléctrica, se debe instalar una fuente de energía ininterrumpible (UPS) y mantener los repuestos disponibles.

Los pasos a seguir para proteger a un router son[30]:

1. Administración de la seguridad de los routers.
2. Proteger el acceso administrativo a los routers.
3. Registrar la actividad de los routers.
4. Proteger los servicios y las interfaces de los routers vulnerables.
5. Proteger los protocolos de enrutamiento.
6. Manejo de IOS de los equipos

[30] CCNA V4, Módulo 4, Accesing the WAN, Cisco 2010

4.2.3.5.1. Administración de la Seguridad de los Routers

Para tener una administración segura de routers se debe aplicar correctamente las recomendaciones dadas a continuación:

- Evitar el uso de palabras de diccionario, pueden ser vulnerables a los ataques de diccionario.
- Combinar letras, números y símbolos.
- Escribir mal una contraseña a propósito. Por ejemplo podría ser Sistemas escrita 5!steM@s.
- Crear contraseñas largas. Deberá tener, como mínimo, ocho caracteres. Se deberá modificar las contraseñas cada mes. Debe tener una política que defina cuándo y con qué frecuencia se deben modificar las contraseñas
- Contraseñas con frases

A través del IOS de Cisco podemos optar por dos modelos de protección de contraseñas:

Las contraseñas deberán ser protegidas mediante el algoritmo de hash MD5, como se explico en la configuración se utilizará la palabra clave *password* por *secret*.

A partir del IOS de Cisco 12.3 en adelante, se puede definir longitudes mínimas en las contraseñas creadas, se recomienda que un password tenga como mínimo 8 caracteres. El comando para establecer este parámetro es: *security passwords min-length.*

4.2.3.5.2. Protección del Acceso Administrativo a los Routers

Para la autenticación a todas las líneas se utilizarán bases de datos locales de usuarios en los routers.

Para la administración remota de los routers, ninguno deberá tener habilitado telnet, el acceso remoto solo se lo realizará por SSH. Solo se deberá permitir 3 intentos de autenticación y el tiempo de inactividad para cerrar la sesión será de 30 segundos.

4.2.3.5.3. Actividad de Registro de los Routers

La configuración del registro (syslog) en el router se debe realizar con cuidado. Se debe enviar los registros del router a un host de registro designado. Los logs deberán ser registrados en el Whats UP y solo los niveles de 0 a 4, es decir hasta el nivel de advertencia

4.2.3.5.4. Proteger los servicios y las interfaces de los routers vulnerables

Los routers Cisco admiten una gran cantidad de servicios de red en las capas 2, 3, 4 y 7, sin embargo, la mayoría de los servicios utilizados no son necesarios. La tabla 4.3 describe servicios generales de los routers vulnerables y enumera las mejores prácticas asociadas a esos servicios.

Característica	Descripción	Predeterminado	Recomendación
Protocolo de descubrimiento de Cisco (CDP)	Protocolo de capa 2 patentado entre dispositivos de Cisco.	Habilitado	El CDP no se necesita casi nunca, deshabilítelo.
Servidores pequeños TCP	Servicios de red TCP estándar: echo, chargen, etc.	>=11.3: deshabilitado 11.2: habilitado	Es una característica de versiones anteriores; deshabilítela de manera explícita.
Servidores UDP pequeños	Servicios de red UDP estándar: echo, discard, etc.	>=11.3: deshabilitado 11.2: habilitado	Esta es una característica de versiones anteriores; deshabilítela.
Finger	Servicio de búsqueda de usuario UNIX, permite listado remoto de usuarios.	Habilitado	Personas sin autorización no deben conocer esto; deshabilítelo
Servidor HTTP	Algunos dispositivos de Cisco del sistema operativo Internetwork (IOS) ofrecen configuración basada Web	Varía según el dispositivo	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Servidor BOOTP	Realice el mantenimiento para permitir que otros routers arranquen desde éste.	Habilitado	Esto se necesita con poca frecuencia y puede abrir un agujero en la seguridad; deshabilítelo.

Carga automática de la configuración	El router intentará cargar su configuración mediante TFTP.	Deshabilitado	Esto se utiliza con poca frecuencia; deshabilítelo si no se encuentra en uso.
Enrutamiento IP de origen	Característica IP que permite que los paquetes especifiquen sus propias rutas.	Habilitado	Esta característica, muy poco usada, puede ser beneficiosa en ataques; deshabilítela.
ARP proxy	El router actuará como un proxy para una resolución de dirección de capa 2.	Habilitado	Deshabilítelo salvo que el router esté funcionando como puente LAN.
Broadcast dirigido IP	Los paquetes pueden identificar un LAN objetivo para broadcasts.	>=11.3: habilitado	El broadcast dirigido se puede utilizar para ataques; deshabilítelo.
Comportamiento del enrutamiento sin clase	El router enviará paquetes que no tengan una ruta concreta.	Habilitado	Ciertos ataques se pueden beneficiar de éste; deshabilítelo salvo que su red lo solicite.
Notificaciones de IP inalcanzables	El router notificará a los emisores, de manera explícita, acerca de direcciones IP incorrectas.	Habilitado	Puede ayudar con la asignación de red; deshabilitado en interfaces para redes que no son confiables.
Respuesta de la máscara IP	El router enviará una máscara de dirección IP de la interfaz en respuesta a una solicitud de máscara del protocolo de mensajes de control de Internet (ICMP).	Deshabilitado	Puede ayudar con la asignación de dirección IP; deshabilítela explícitamente en interfaces de redes que no son confiables.
Redirecciona-mientos IP	El router enviará un mensaje de redirección ICMP en respuesta a ciertos paquetes IP ruteados.	Habilitado	Puede ayudar con la asignación de red; deshabilítelo en interfaces no confiables.
Servicio NTP	El router puede actuar como un servidor de tiempo para otros dispositivos y hosts.	Habilitado (siempre que NTP esté configurado)	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Protocolo de administración de red simple	Pueden admitir consulta y configuración remota del protocolo de administración de red simple (SNMP).	Habilitado	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Servicio de nombres de dominio	Realizan la resolución de nombre servicio de nombre de dominio (DNS).	Habilitado (broadcast)	Configure la dirección del servidor DNS de manera explícita o deshabilítelo

Tabla 4.3 Servicios vulnerables en el router.[31]

[31] CCNA V4, Módulo 4, Accessing the Wan, Cisco 2010

Los servicios como: echo, discard y chargen se los puede desactivar utilizando el comando no service tcp-small-servers o no service udp-small-servers. Otros servicios como Bootp, Finger, HTTP, se los puede desactivar de la siguiente manera:

- no ip bootp server.
- no service finger.
- no ip http server.

Otros servicios que pueden causar un agujero para una intrusión no autorizada y que se los puede deshabilitar son:

- Protocolo de descubrimiento de Cisco (CDP): con el comando no cdp run.

Igual que los servicios proporcionados en el router pueden causar fallas de seguridad, las interfaces del router pueden ser más seguras si se utilizan determinados comandos en el modo de configuración de interfaz:

- Interfaces no utilizadas: con el comando shutdown.
- Enrutamiento ad hoc: con el comando no ip proxy-arp.

Otros servicios que deberían estar desactivados son NTP y DNS debido a:

- NTP: El NTP deja los puertos de escuchas abiertos y vulnerables
- DNS: Puede ayudar a los atacantes a conectar las direcciones IP a nombres de dominio.

4.2.3.5.5. Protección del Protocolo de Enrutamiento: EIGRP

El protocolo de enrutamiento usado en el actual proyecto es EIGRP, por lo que para protegerlo se debe realizar algunas configuraciones de autenticación. La configuración de la cadena que contendrá el key del MD5 de autenticación es:

ROUTER(config)#key chain PETROEIGRP
ROUTER(config-keychain)#key 1
ROUTER(config-keychain-key)#key–string petro

Se deberá configurar autenticación en todas las interfaces en las que se envíen o reciban información de EIGRP, se deberá utilizar el algoritmo MD5. La configuración es:

ROUTER(config)#interface gi 0/0
ROUTER(config-if)#ip authentication mode eigrp 100 md5
ROUTER(config-if)#ip authentication key-chain eigrp 100 PETROEIGRP.

4.2.3.5.6. Manejo de IOS de los Equipos

Dentro de este apartado podemos realizar algunas funciones tales como:

Mantenimiento de las imágenes del IOS de cisco.

Para el mantenimiento de las imágenes de IOS de Cisco se realiza lo siguiente:

Primer paso

- Confirmar el tamaño de la actualización.
- Planificar la actualización en un periodo con poca actividad.

Segundo Paso

- Desactivar las interfaces que no se utilizan.
- Realizar una copia de respaldo de la configuración en ejecución y de las imágenes de IOS de Cisco TFTP.
- Ejecutar las transferencias de archivos.
- Probar la función de actualización y activar las interfaces desactivadas.

Administración de las imágenes del IOS de cisco.

Una buena práctica para mantener la disponibilidad del sistema es asegurarse de tener siempre copias de seguridad de los archivos de configuración y de los archivos de imagen del IOS. Por tanto se deberá realizar el respaldo de la configuración cada vez que se realice un cambio en la misma, y cada 2 meses. Los IOS de los routers deberán ser respaldados cada vez que se los actualice.

4.3. PROTOTIPO DEL PROYECTO DE TITULACIÓN

En el prototipo diseñado para el presente Proyecto de Titulación se realizará la simulación en un ambiente híbrido (equipos virtuales y equipos físicos), en la cual se presenta la conexión entre el nodo Matriz y el nodo Beaterio. Para indicar la comunicación entre los dos nodos se elaborará un ambiente en el que se representen los equipos existentes en Matriz, Beaterio, y el Cerro Pichincha. Además se mostrará la conectividad entre los dos nodos y se probará los servicios integrados que proporcionan los equipos, específicamente telefonía IP. Utilizando el programa What´s Up se indicará el modelo de gestión aplicado a los routers. Toda esta información se encuentra documentada a continuación.

4.3.1. ELEMENTOS DEL PROTOTIPO

El prototipo consta de los siguientes elementos:

- Router Beaterio: Emulado con el programa GNS3 (instalado en laptop 1). En la Figura 4.46. se indica el programa GNS3 instalado en una computadora.

Figura 4.46 Programa GNS3 instalado.

- Router Rocío: Equipo físico, Router Cisco 3825 (Figura 4.47 y 4.48).

Figura 4.47 Router Cisco 3825 vista frontal

Figura 4.48 Router Cisco 3825 vista posterior

- Switch Pichincha: Equipo físico. Switch Cisco 3560 (Figura 4.49).

Figura 4.49 Switch Cisco 3560

- Telefonía IP Rocío
    - Teléfono IP físico, Cisco IP Phone 7961 (Figura 4.50).

Figura 4.50 Cisco IP Phone 7961

- Teléfono IP físico, Cisco IP Phone 7911 (Figura 4.51).

Figura 4.51 Cisco IP Phone 7911

- Telefonía IP Beaterio
  - Softphone, Cisco IP Communicator 2.1.1.0 (Figura 4.52).

Figura 4.52 Cisco IP Communicator 2.1.1.0

- Herramienta de Gestión: What´s Up Gold v14.4 (instalado en laptop 2) (Figura 4.53).

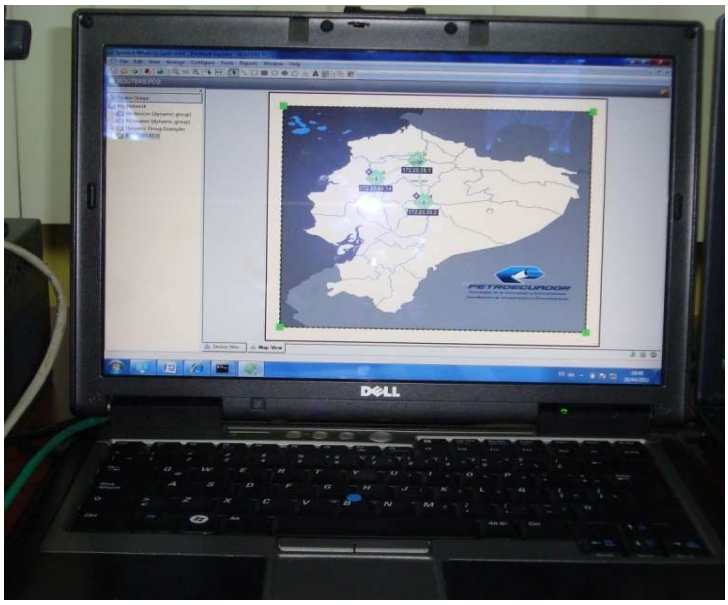


Figura 4.53 Programa What´s Up instalado

- Servidor de Correo: Kerio Connect 7.1.3 (instalado laptop 3) (Figura 4.54).

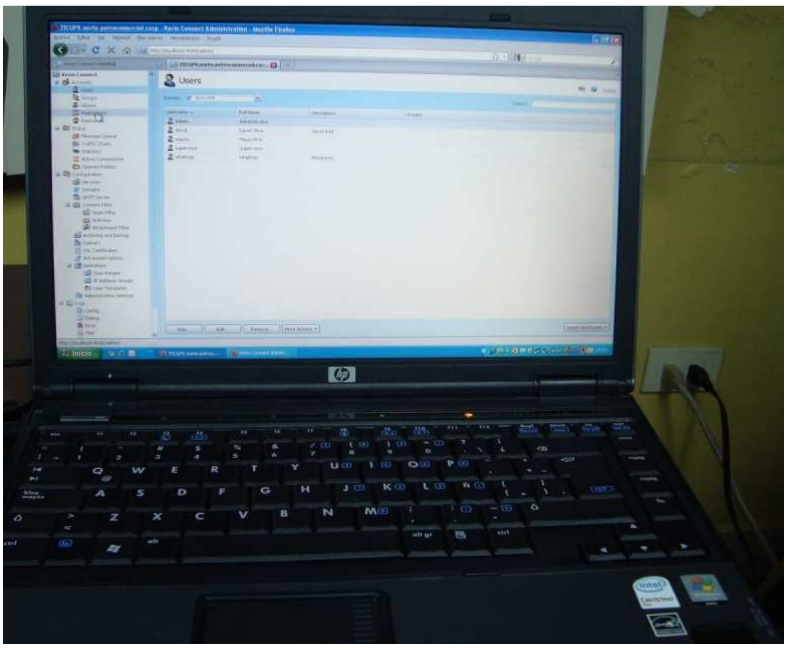


Figura 4.54 Programa Kerio instalado

En la figura 4.55 se muestra los elementos que conforman el prototipo.

Figura 4.55 Elementos que conforman el prototipo

4.3.2. TOPOLOGÍA DEL PROTOTIPO

El esquema de conexión del prototipo se muestra en a figura 4.56.

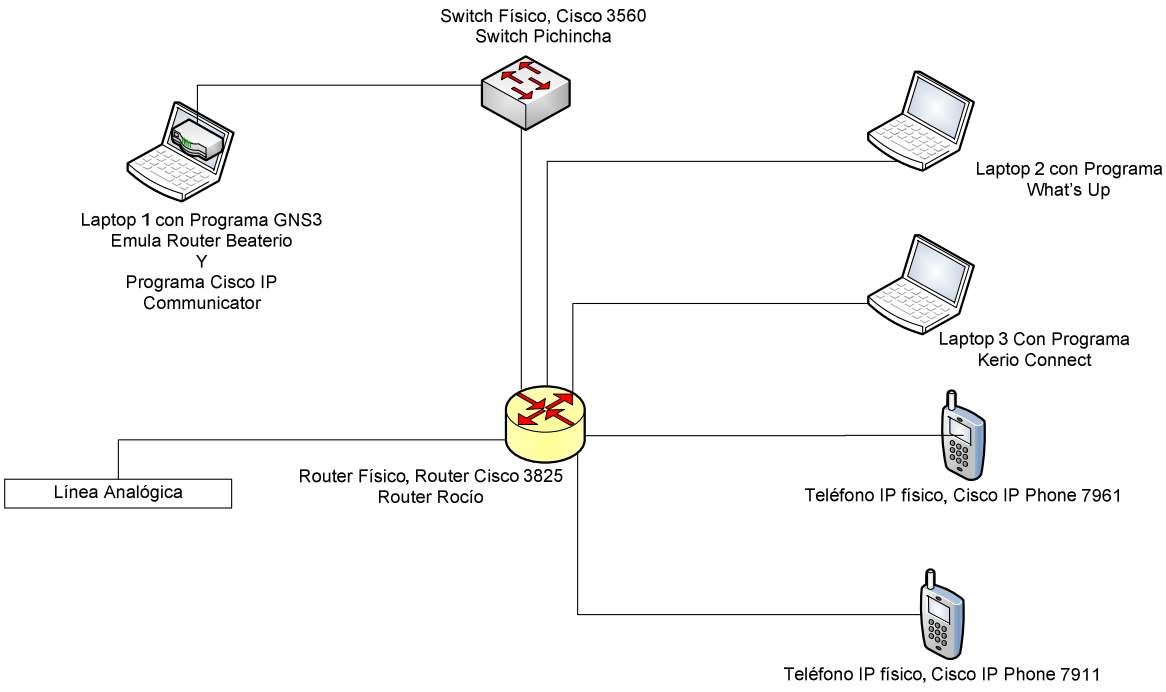


Figura 4.56 Esquema de Conexión del Prototipo.

El esquema de conexión del Prototipo se encuentra conformado por:

Laptop 1, donde se encuentra el Programa GNS3 que emula el router Beaterio. La tarjeta de red de área local, de la pc, emula la interfaz del ruteador con la que se conectará al switch Pichincha. La tarjeta de red inalámbrica de laptop 1, emula la interfaz del router que se conectará con la LAN de Beaterio. En la figura 4.57 se indica el esquema de conexión en el programa GNS3.

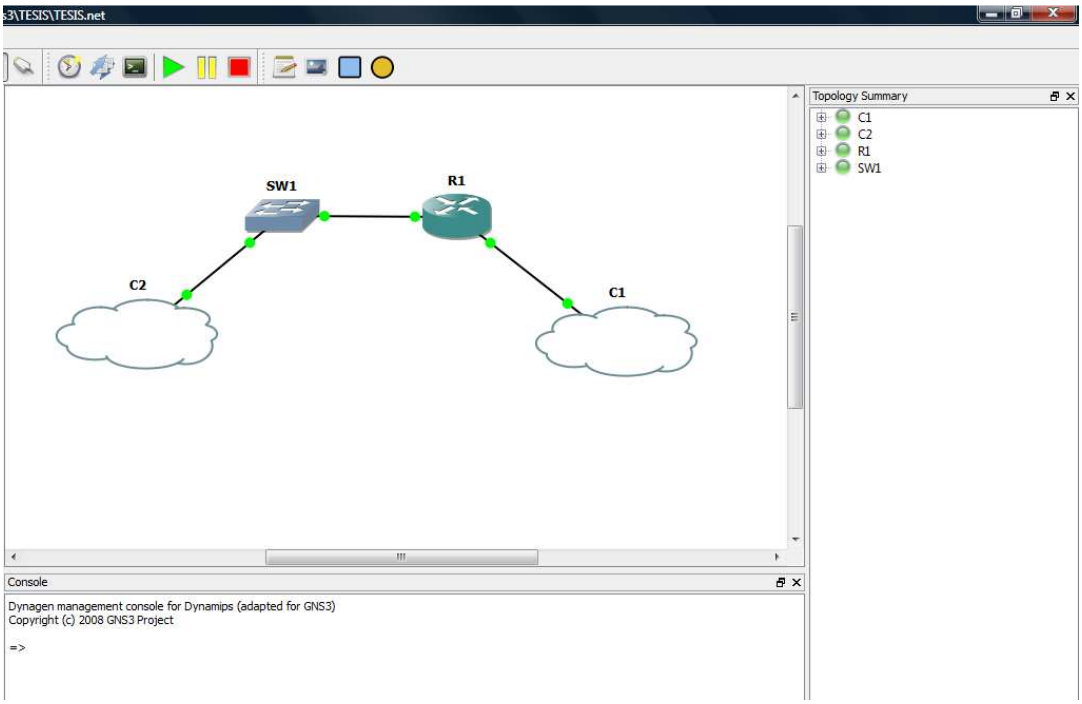


Figura 4.57 Esquema de conexión en GNS3

Adicionalmente se encuentra instalado el programa Cisco IP Communicators, que emulará a un teléfono IP físico, y a su vez a la telefonía IP del nodo Beaterio. En la Figura 4.58 se muestra las interfaces gráficas de los programas instalados en laptop 1.

Figura 4.58 Interfaces gráficas de los programas instalados en laptop 1

El switch Pichincha se conecta al router Beaterio y al router Rocío.

El router Rocío se conecta al switch Pichincha. Además al router Rocío se conecta laptop 2 que tiene instalado el programa Whats Up el cual servirá para monitorear el modelo de gestión aplicado a los equipos de enrutamiento. También conectado al equipo de enrutamiento del nodo Rocío está laptop 3, en la cual está instalado el programa Kerio Connect que funciona como servidor de correo y se encargará de enviar los correos electrónicos a los administradores de red informando acerca de algún problema en los equipos, de acuerdo a las alarmas configuradas previamente en el programa What's Up.

Finalmente al equipo del Rocío están conectados teléfonos IP físicos, que emulan la conexión del router Rocío con su LAN y a su vez con la parte de telefonía IP, también a una interfaz de la tarjetería FXO del equipo, está conectado una línea analógica,

que permitirá a los teléfonos IP comunicarse con la PSTN y realizar llamadas a líneas de CNT.

4.3.3. DOCUMENTACIÓN DEL PROTOTIPO

A continuación se encuentra documentada la información recopilada del prototipo.

4.3.3.1. Documentación de enrutamiento

Se presenta información referente al protocolo de enrutamiento EIGRP en los equipos de enrutamiento utilizados en el prototipo, así como de las interfaces de cada equipo.

4.3.3.1.1. Router Rocío

Interfaces activas en el equipo

En la tabla 4.4 se indican las interfaces utilizadas en el Router Rocío.

DISPOSITIVO	INTERFAZ	DESCRIPCIÓN
ROUTER ROCÍO	Service- Engine 0/0	Interfaz donde se realiza la configuración de los servicios de telefonía
	GigabitEthernet0/1	Interfaz para conectarse con el switch Pichincha
	FastEthernet0/1/0	Conexión con el teléfono IP Cisco 7961
	FastEthernet0/1/1	Conexión con laptop 2 (Programa What´s Up)
	FastEthernet0/1/2	Conexión con laptop 3 (Programa Kerio Connect)
	Voice-port 0/2/1	Conexión con la línea analógica

Tabla 4.4 Interfaces conectadas al Router Rocío

En la figura 4.59 y 4.60 se muestran las interfaces conectadas en el Router Rocío tanto de forma físico como mediante la interfaz de comandos respectivamente.

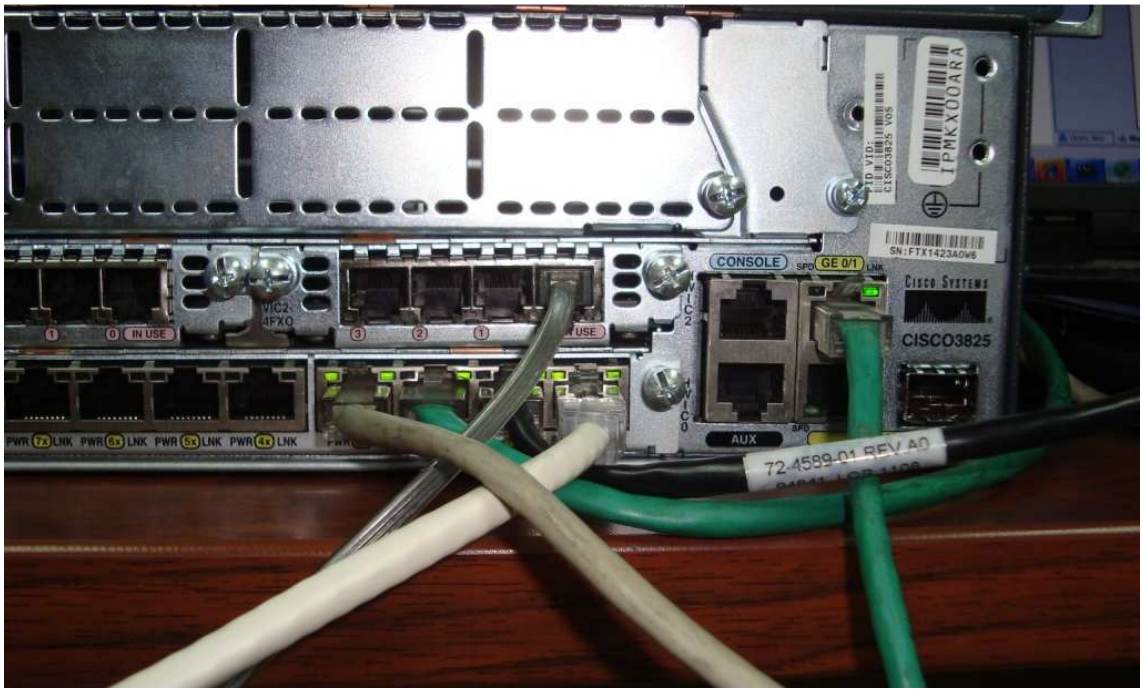


Figura 4.59 Interfaces conectadas al Router Rocío físicamente

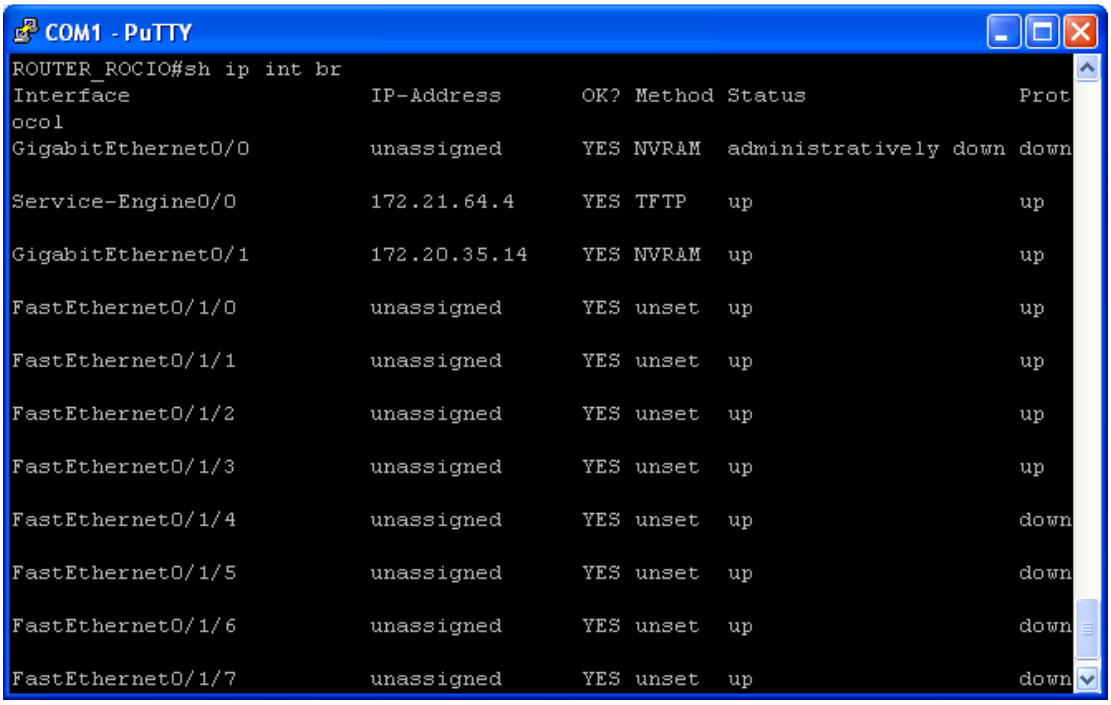


Figura 4.60 Interfaces activas visualizadas a través de línea de comandos del Router Beaterio

Vecinos EIGRP

En la figura 4.61 se indica el establecimiento de vecinos a través del protocolo de enrutamiento EIGRP. En la figura 4.62 se muestra la tabla de vecinos descubiertos a través de EIGRP, del router Rocío.

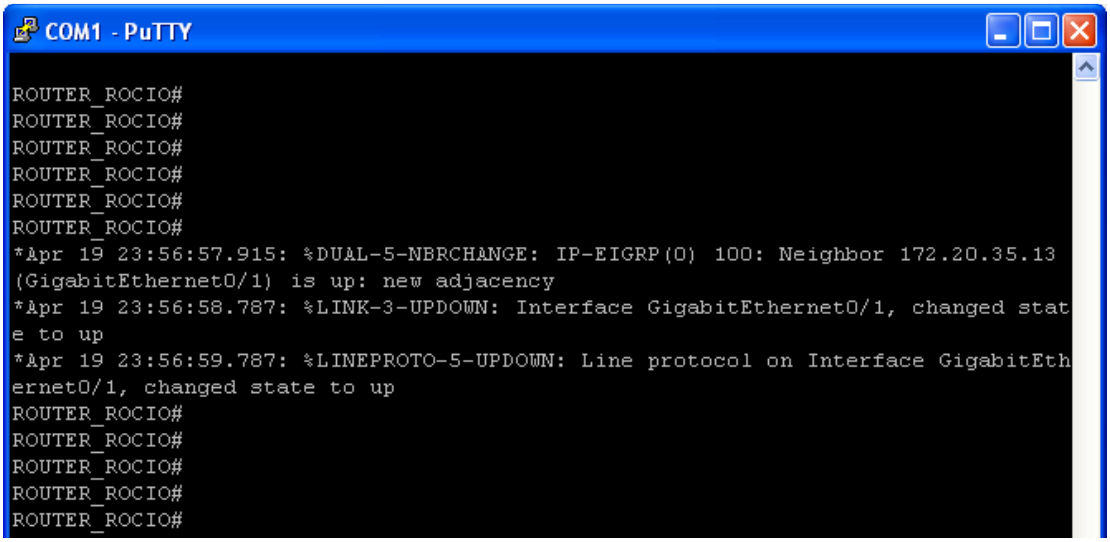


Figura 4.61 Establecimiento de vecinos EIGRP en Router Rocío

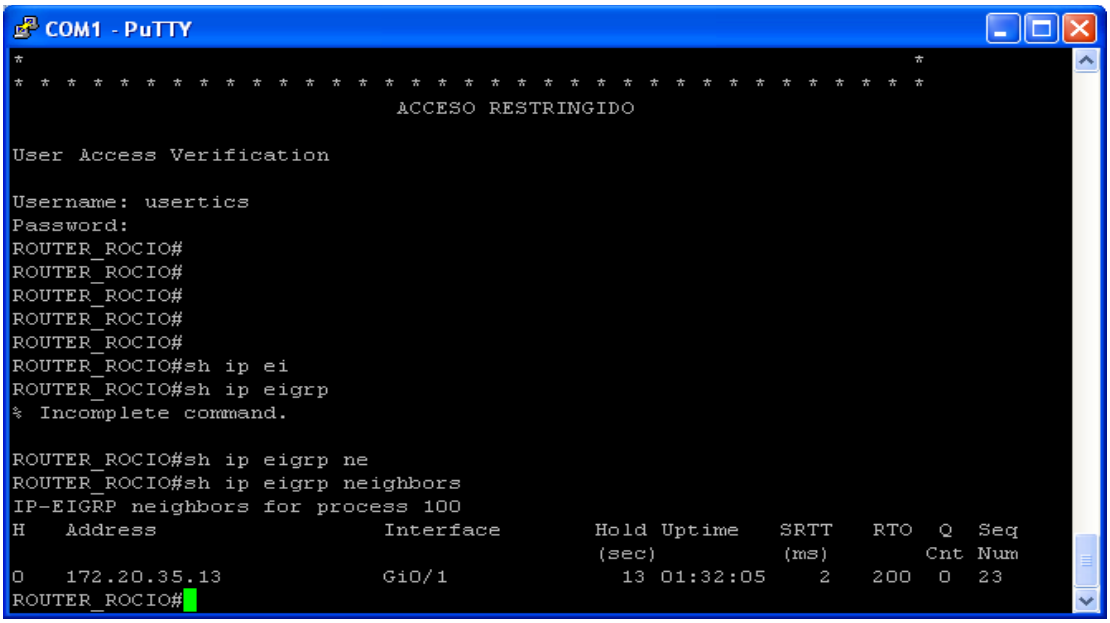


Figura 4.62 Tabla de Vecinos EIGRP en router Rocío

Tabla de enrutamiento EIGRP

En la figura 4.63 se indica la tabla de enrutamiento del router Rocío, aprendida mediante el protocolo de enrutamiento EIGRP.

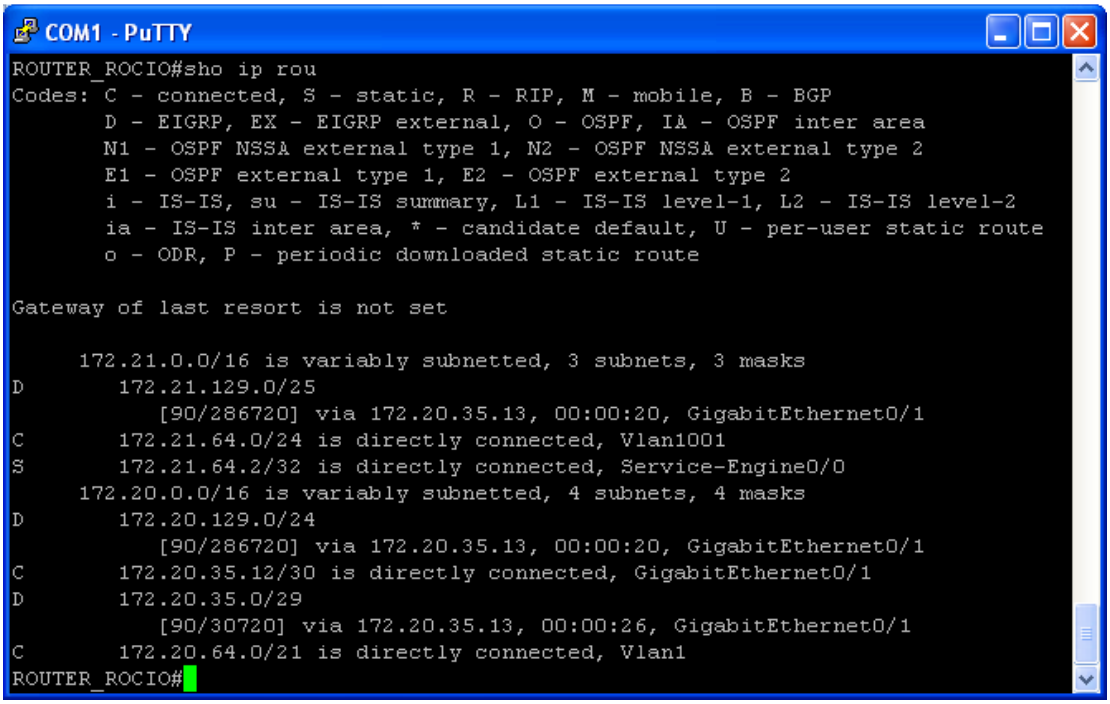


Figura 4.63 Tabla de Enrutamiento EIGRP en router Rocío

4.3.3.1.2. Router Beaterio

Interfaces activas en el equipo

En la tabla 4.5 se indican las interfaces utilizadas en el Router Beaterio.

DISPOSITIVO	INTERFAZ	DESCRIPCIÓN
ROUTER BEATERIO	FastEthernet1/0	Conexión con Switch Pichincha (Se conecta mediante la tarjeta física LAN de laptop 1)
	FastEthernet0/1.1	Conexión a la LAN de Beaterio (Se conecta mediante la tarjeta física Inalámbrica LAN de laptop 1)
	FastEthernet0/1.3	Conexión a la LAN de telefonía de Beaterio (Se conecta mediante la tarjeta física Inalámbrica LAN de laptop 1)

Tabla 4.5 Interfaces conectadas al Router Beaterio

En la figura 4.64 se muestran las interfaces conectadas en el Router Beaterio mediante la interfaz de comandos.

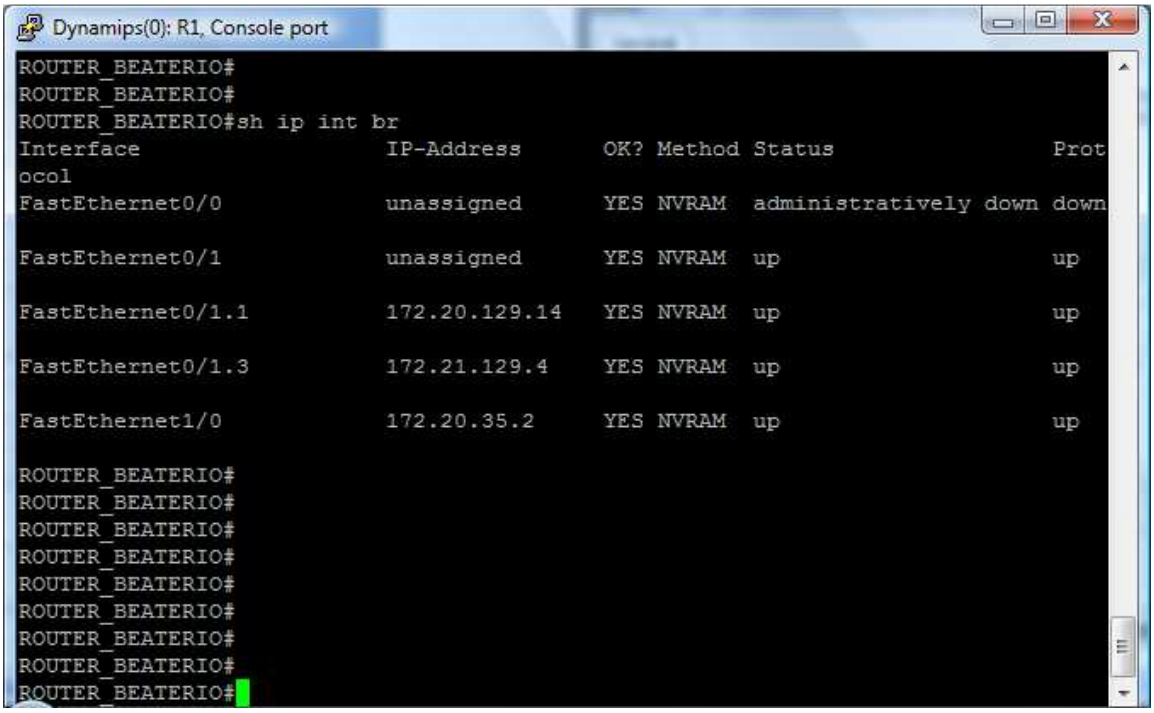


Figura 4.64 Interfaces Conectadas al Router Beaterio

Vecinos EIGRP

En la figura 4.65 se indica el establecimiento de vecinos a través del protocolo de enrutamiento EIGRP. En la figura 4.66 se muestra la tabla de vecinos descubiertos a través de EIGRP, del router Beaterio.

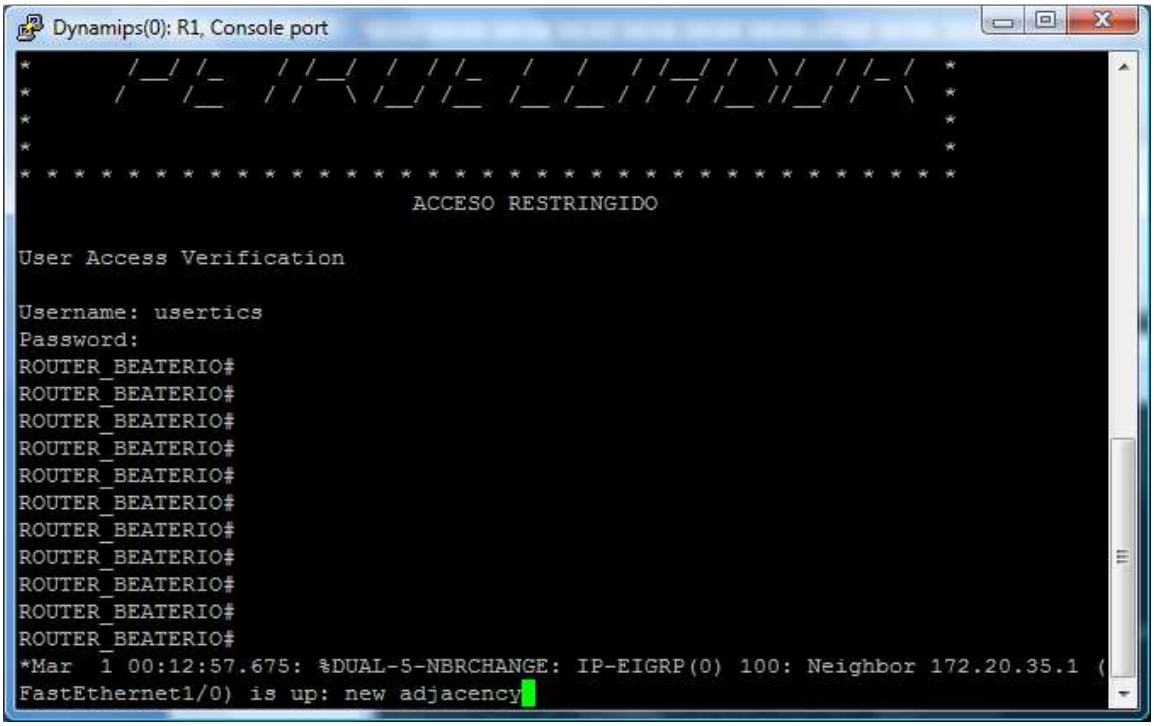


Figura 4.65 Establecimiento de vecinos EIGRP en router Beaterio

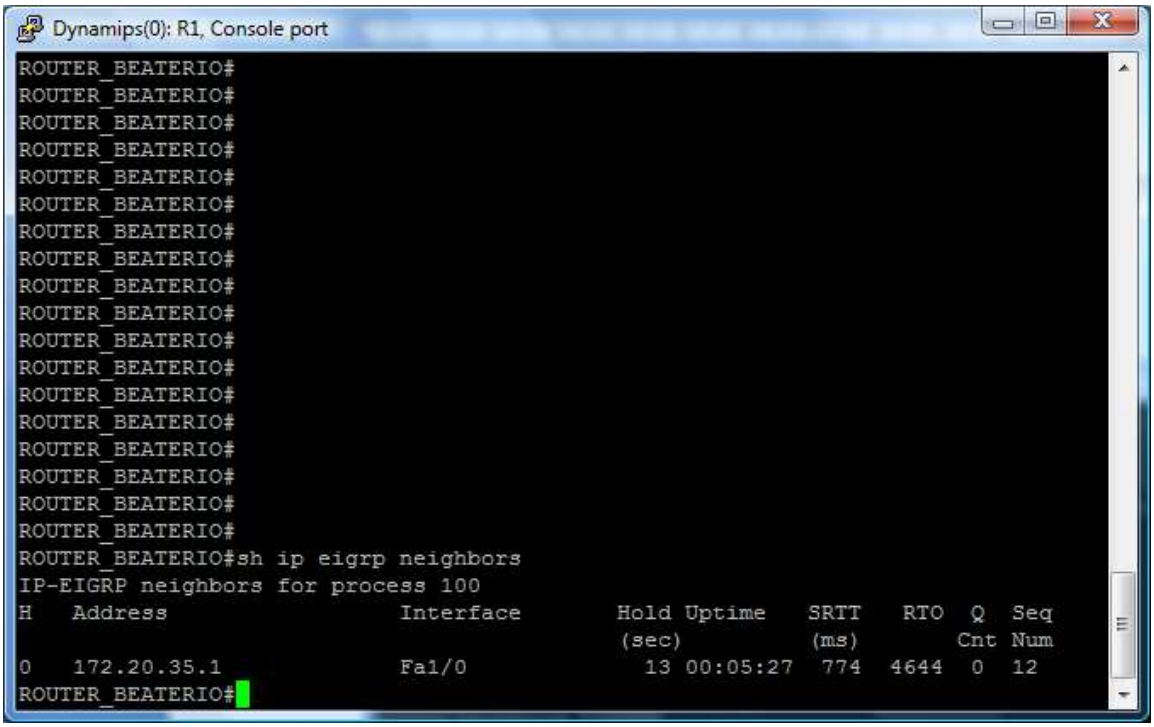


Figura 4.66 Tabla de vecino EIGRP en router Beaterio

Tabla de enrutamiento EIGRP

En la figura 4.67 se indica la tabla de enrutamiento del router Beaterio, aprendida mediante el protocolo de enrutamiento EIGRP.

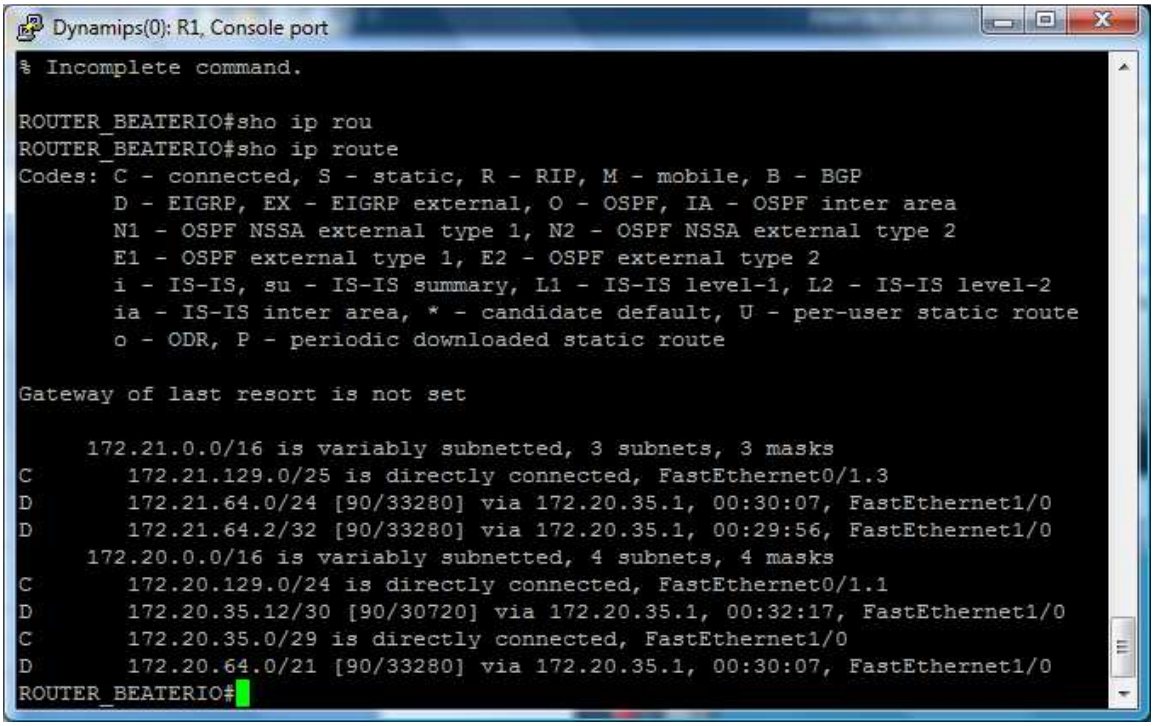


Figura 4.67 Tabla de Enrutamiento EIGRP en router Beaterio

4.3.3.1.3. Switch Pichincha

Interfaces activas en el equipo

En la tabla 4.6 se indican las interfaces utilizadas en el Switch Pichincha.

DISPOSITIVO	INTERFAZ	DESCRIPCIÓN
Switch Pichincha	FastEthernet0/1	Conexión a router Rocío
	FastEthernet0/2	Conexión a router Beaterio

Tabla 4.6 Interfaces conectadas al switch Pichincha

En la figura 4.68 y 4.69 se muestran las interfaces conectadas en el Switch Pichincha tanto de forma físico como mediante la interfaz de comandos respectivamente.

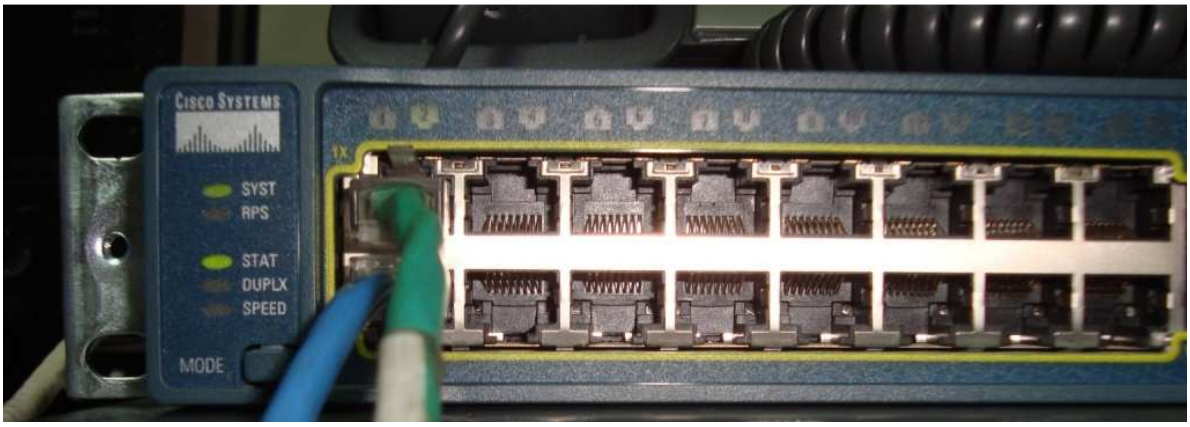


Figura 4.68 Interfaces conectadas al Switch Pichincha físicamente

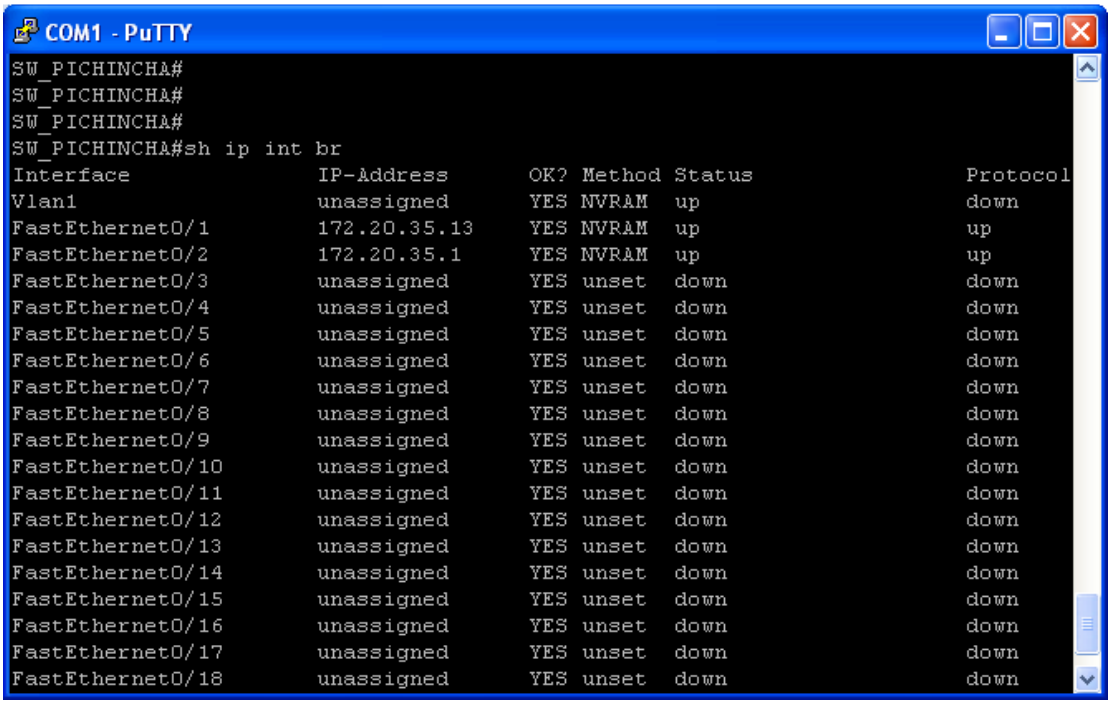


Figura 4.69 Interfaces activas visualizadas a través de línea de comandos del Switch Pichincha

Vecinos EIGRP

En la figura 4.70 se indica el establecimiento de vecinos a través del protocolo de enrutamiento EIGRP. En la figura 4.71 se muestra la tabla de vecinos descubiertos a través de EIGRP, del switch Pichincha.

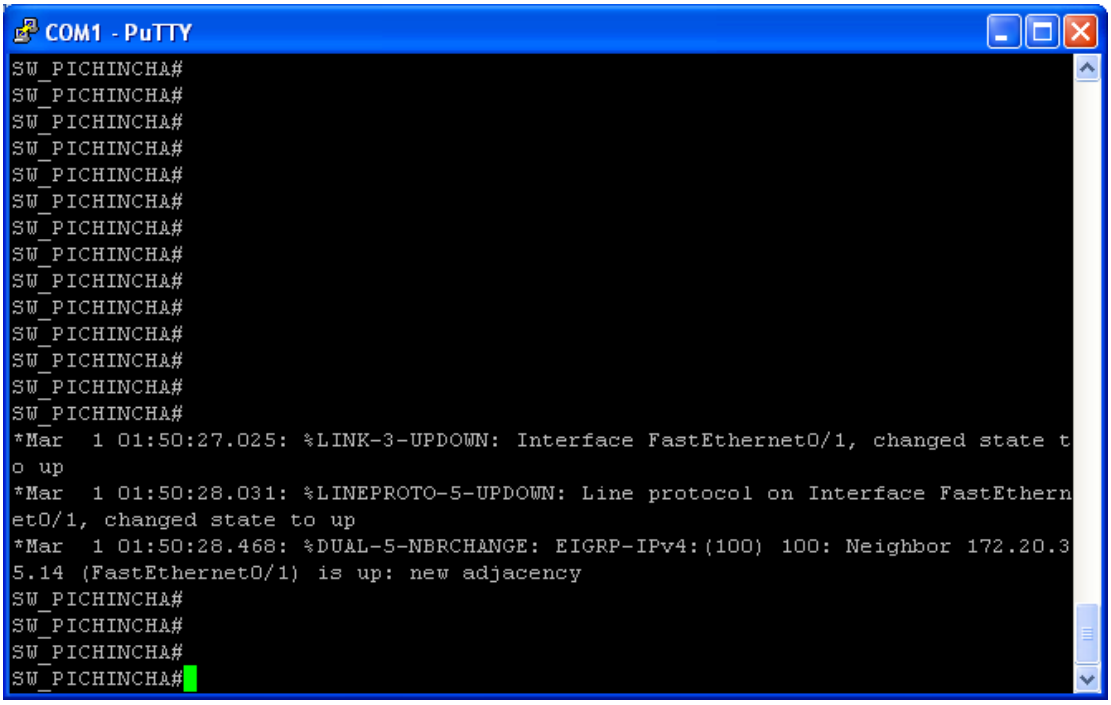


Figura 4.70 Establecimiento de vecinos EIGRP en switch Pichincha

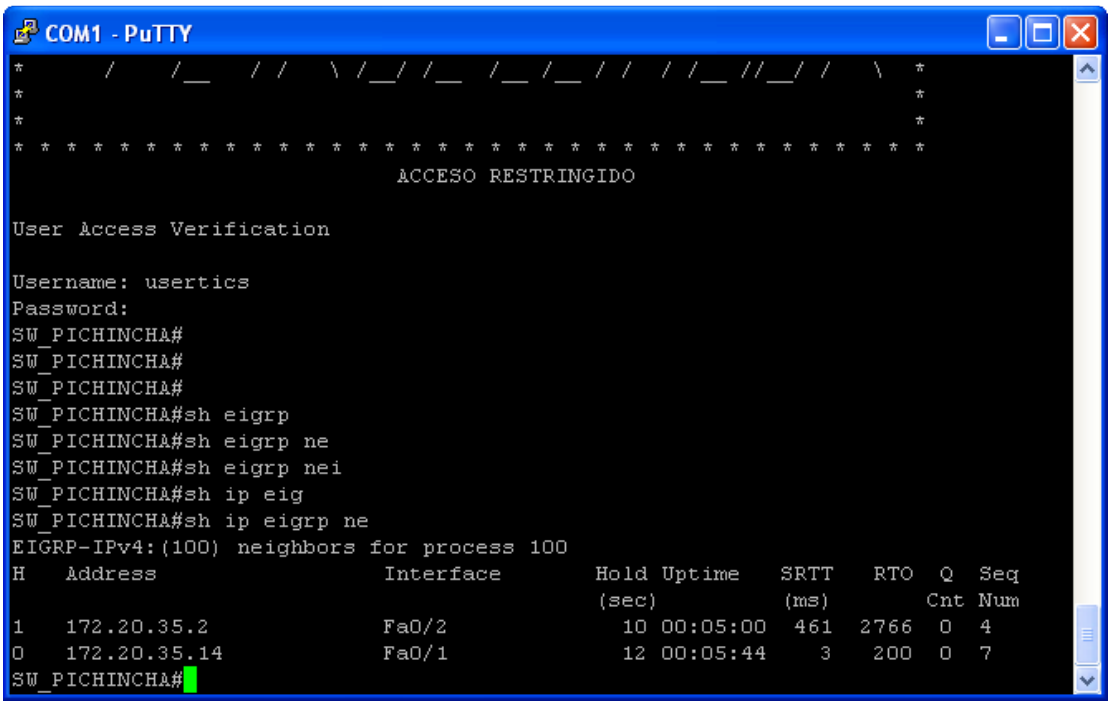


Figura 4.71 Tabla de Vecinos EIGRP en switch Pichincha

Tabla de enrutamiento EIGRP

En la figura 4.72 se indica la tabla de enrutamiento del switch Pichincha, aprendida mediante el protocolo de enrutamiento EIGRP.

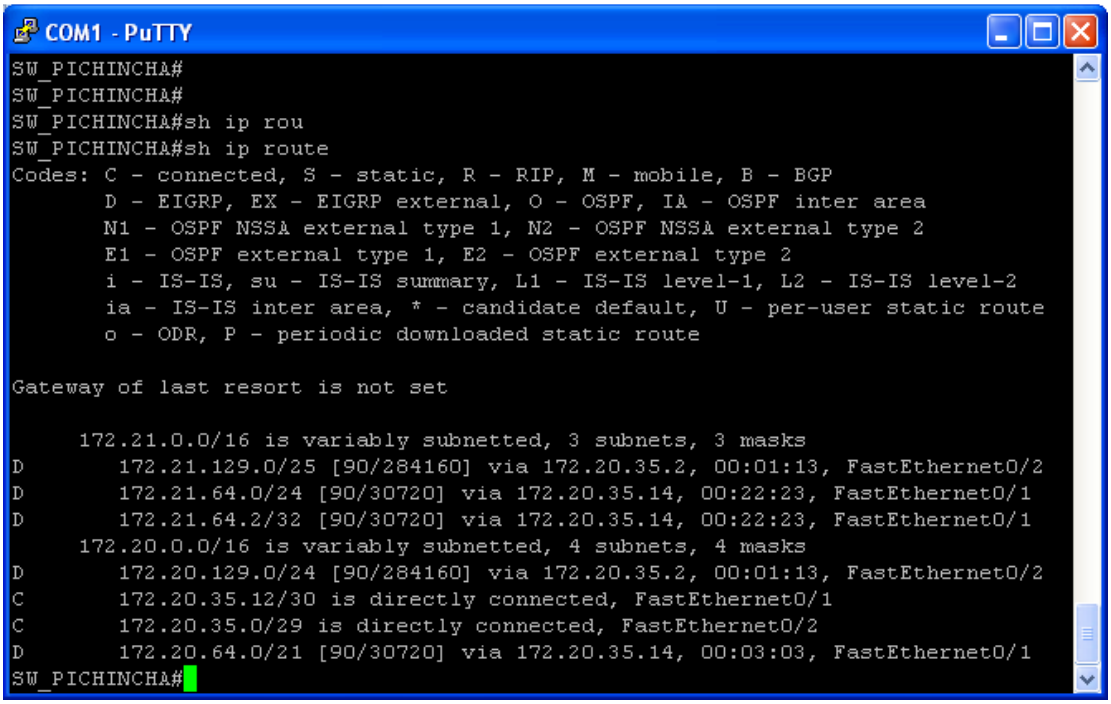


Figura 4.72 Tabla de Enrutamiento EIGRP en switch Pichincha

4.3.3.2. Documentación Telefonía

A continuación se indica la documentación de la telefonía IP en los routers Rocío y Beaterio.

4.3.3.2.1. Router Rocío

Teléfono Registrado

En la figura 4.73 se muestra el registro de un teléfono IP en el router Rocío.

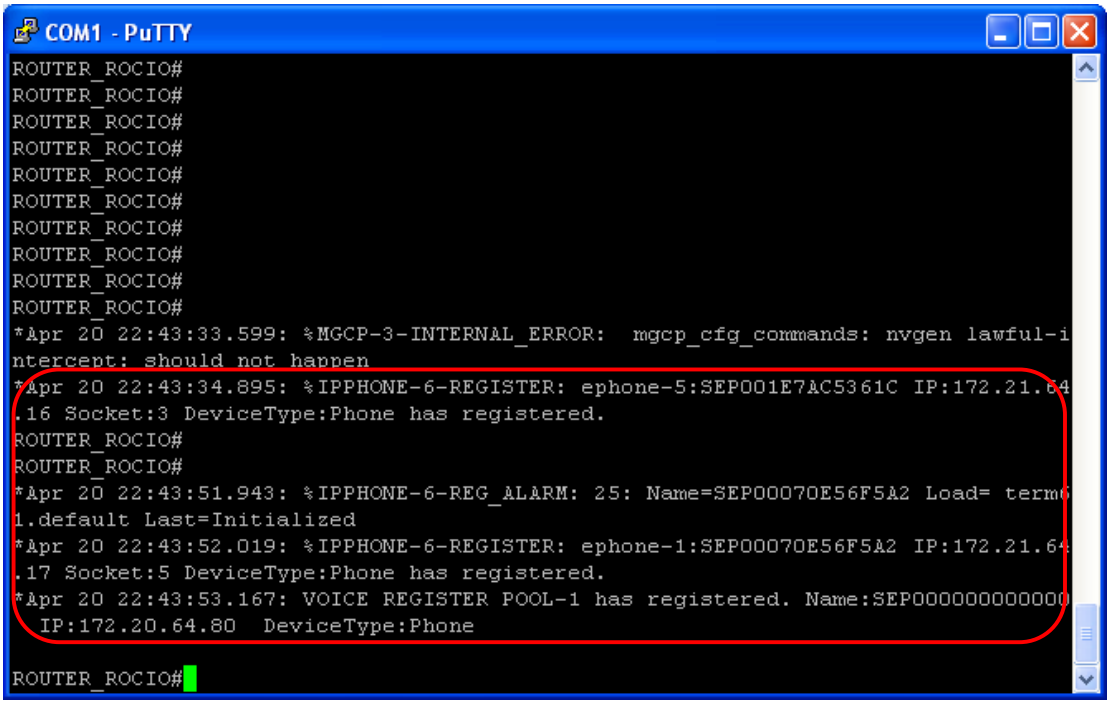


Figura 4.73 Registro de teléfono IP en router Rocío

Teléfonos utilizados en router Rocío

Los teléfonos utilizados en el router Rocío con sus nombres y número de extensión telefónica se muestra a continuación:

Cisco IP Phone 7961:

- Username: USER1
- Número de Extensión Telefónica: 1001

Cisco IP Phone 7911

- Username: USER2
- Número de Extensión Telefónica: 1005

En la figura 4.74 se indica los dos teléfonos usados en router Rocío

Figura 4.74 Cisco IP pone 7911 (Izquierda), Cisco IP Phone 7961 (Derecha)

Establecimiento de una llamada

En las figuras 4.75 y 4.76 se muestran los mensajes recibidos en la interfaz de línea de comandos del router Rocío establecimiento de una llamada entre USER1 y USER2.

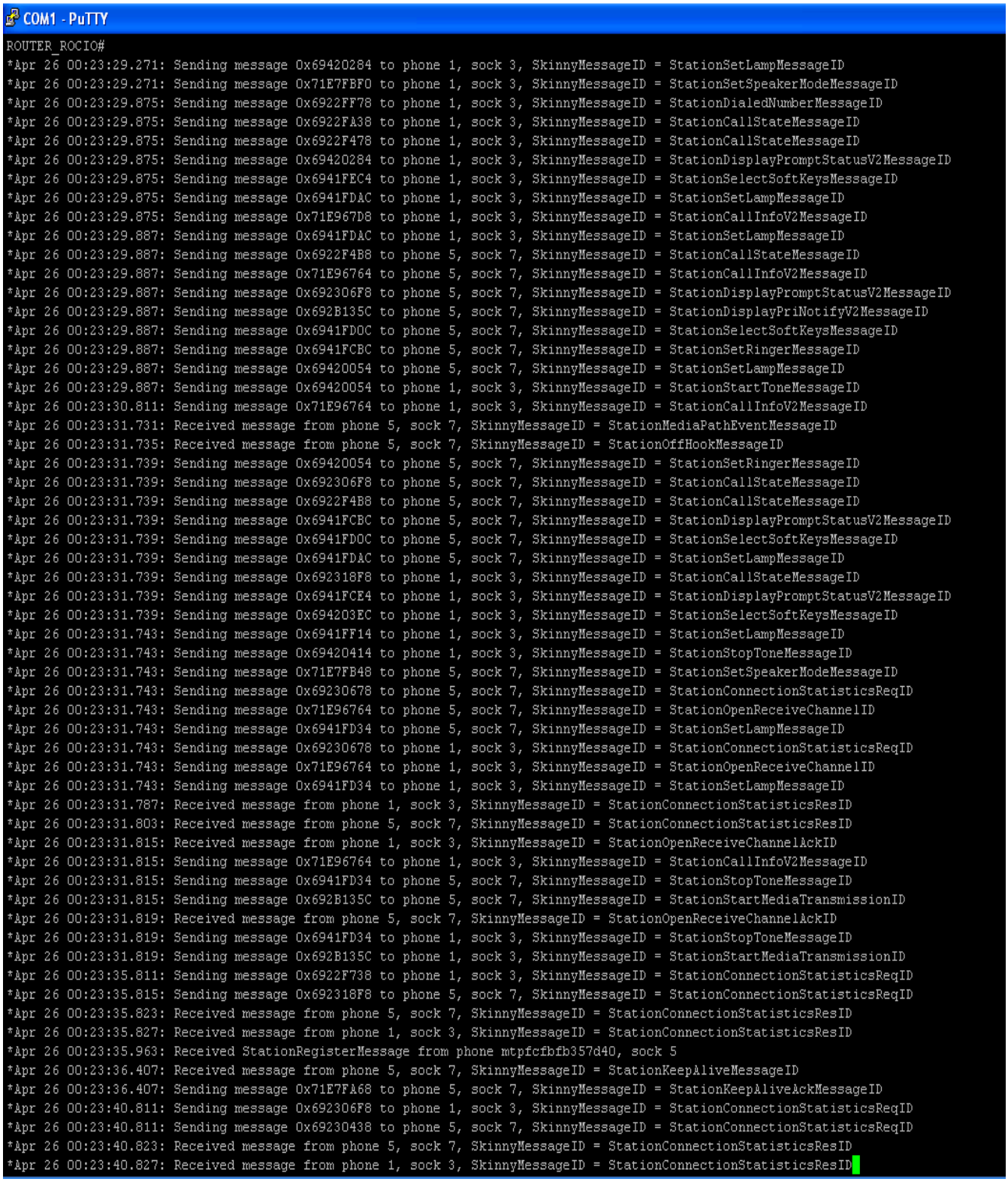


Figura 4.75 Mensajes recibidos al establecerse una llamada parte 1

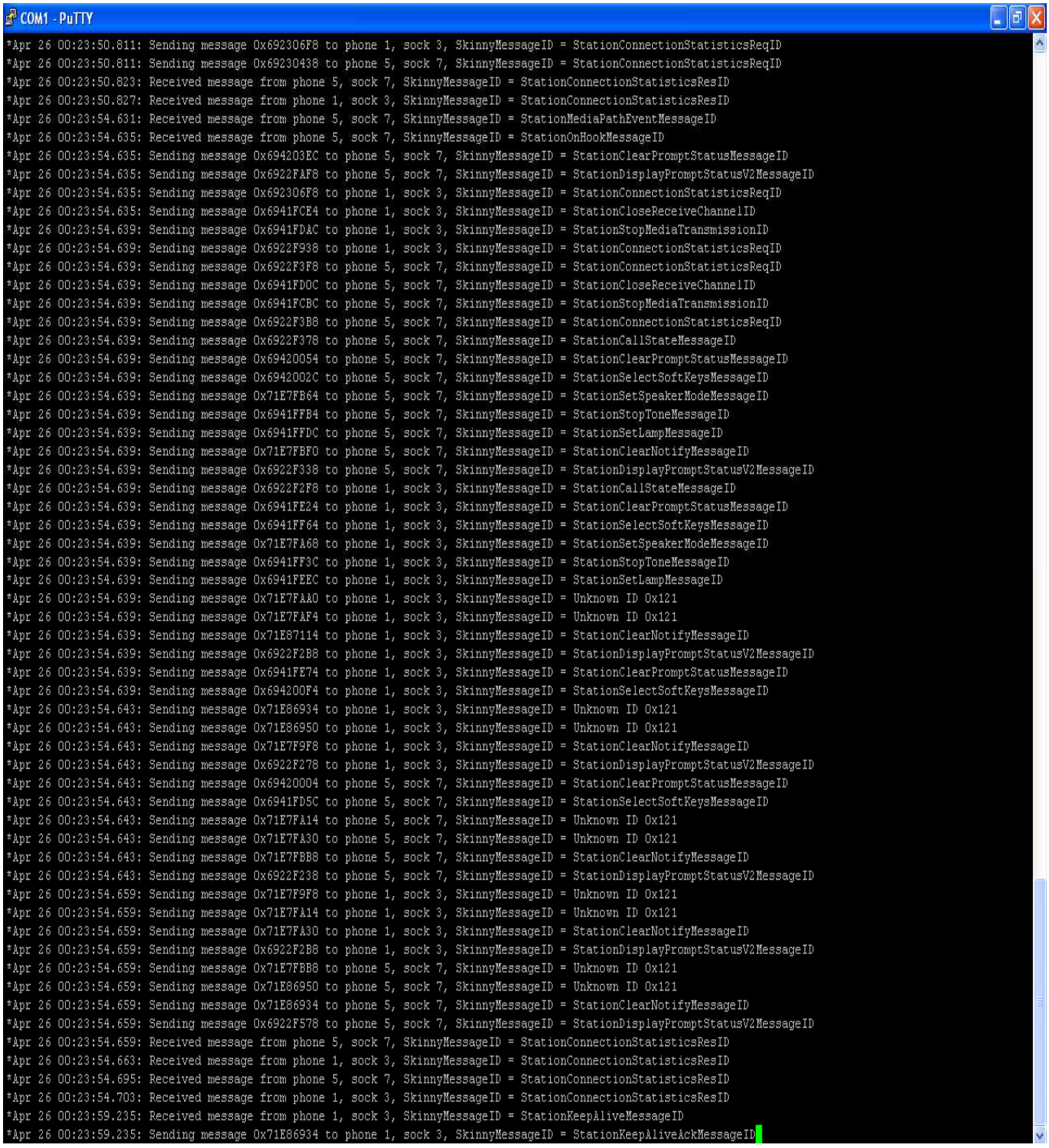


Figura 4.76 Mensajes Recibidos al establecerse una llamada parte 2

En las figuras 4.77 y 4.78 se indican de manera gráfica la realización de una llamada entre USER1 y USER2.

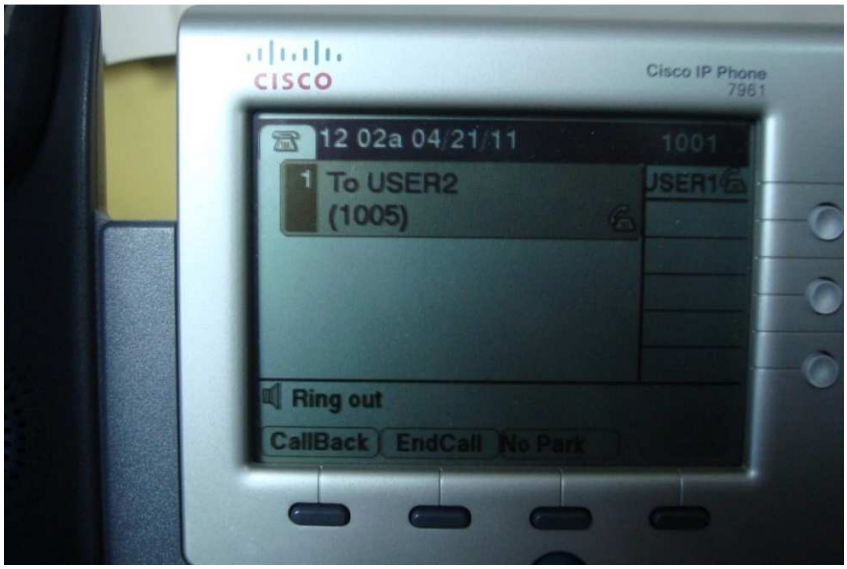


Figura 4.77 USER1 establece una llamada con USER2

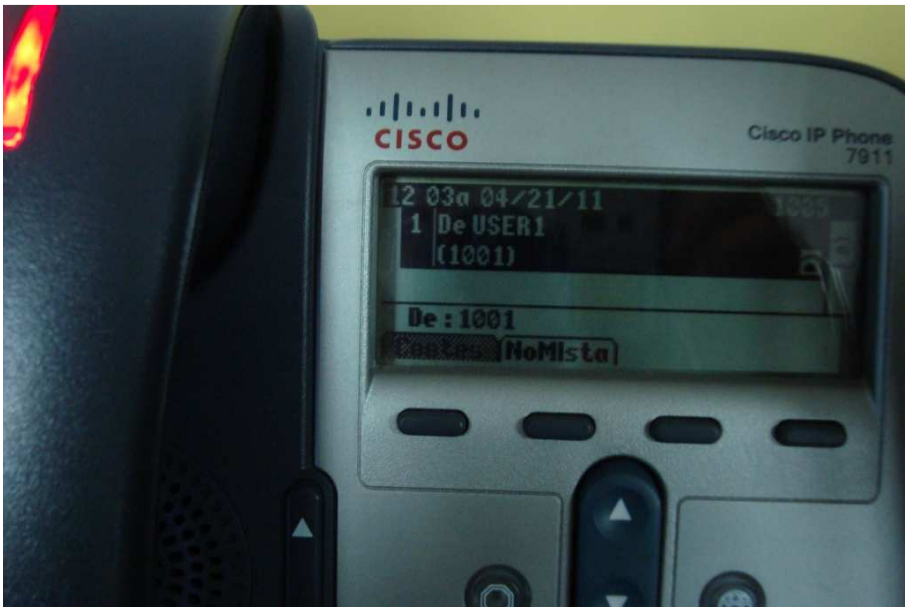


Figura 4.78 USER2 recibe la llamada de USER1

4.3.3.2.2. Router Beaterio

Teléfono Registrado

En la figura 4.77 se muestra el registro de un teléfono IP, específicamente del softphone de Cisco IP Communicator en el router Beaterio.

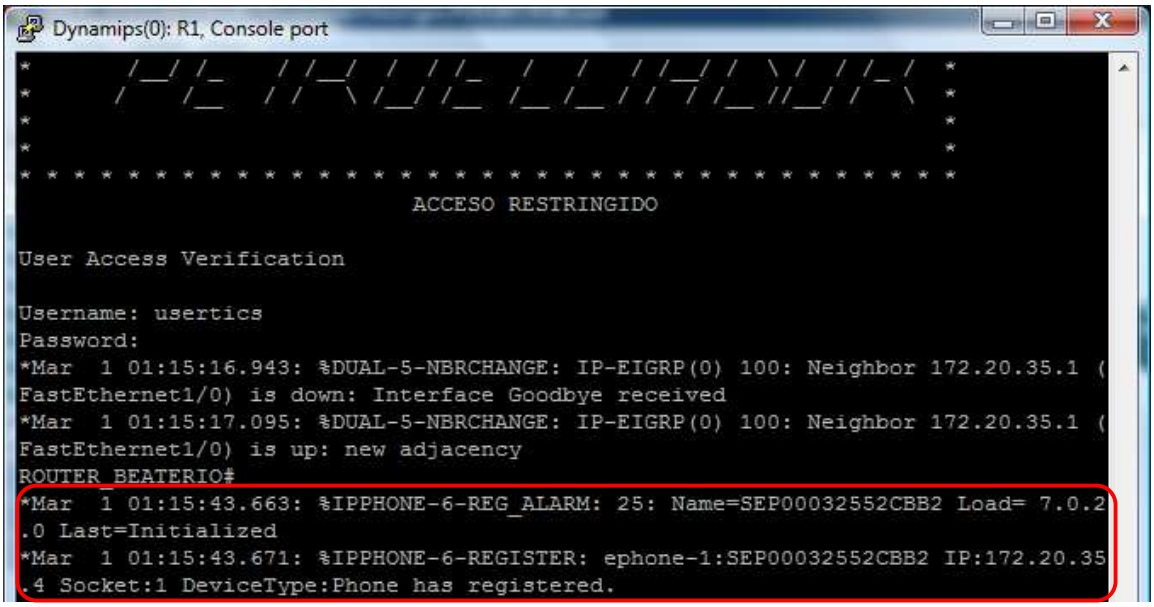


Figura 4.79 Registro de teléfono IP en router Beaterio

Teléfono utilizado en router Beaterio

El softphone de Cisco utilizado en el router Beaterio con su nombre y número de extensión telefónica se muestra a continuación:

Softphone, Cisco IP Communicator 2.1.1.0:

- Username: David
- Número de Extensión Telefónica: 2001

Figura 4.80 Softphone Cisco IP Communicator

Adicional a lo indicado en telefonía se configuro, correos de voz y restricción de llamadas ver anexo 5.

4.3.3.3. Documentación del Modelo de Gestión

Para administrar y monitorear el modelo de gestión aplicado a los routers y switch del prototipo se utilizó el programa What´s Up. A continuación se muestra la información documentada.

4.3.3.3.1. What´s Up

El programa What´s Up se utilizó para la monitorización y administración de los routers Rocío y Beaterio, y del switch Pichincha. En la figura 4.81 se indica la interfaz de monitoreo de estos equipos.

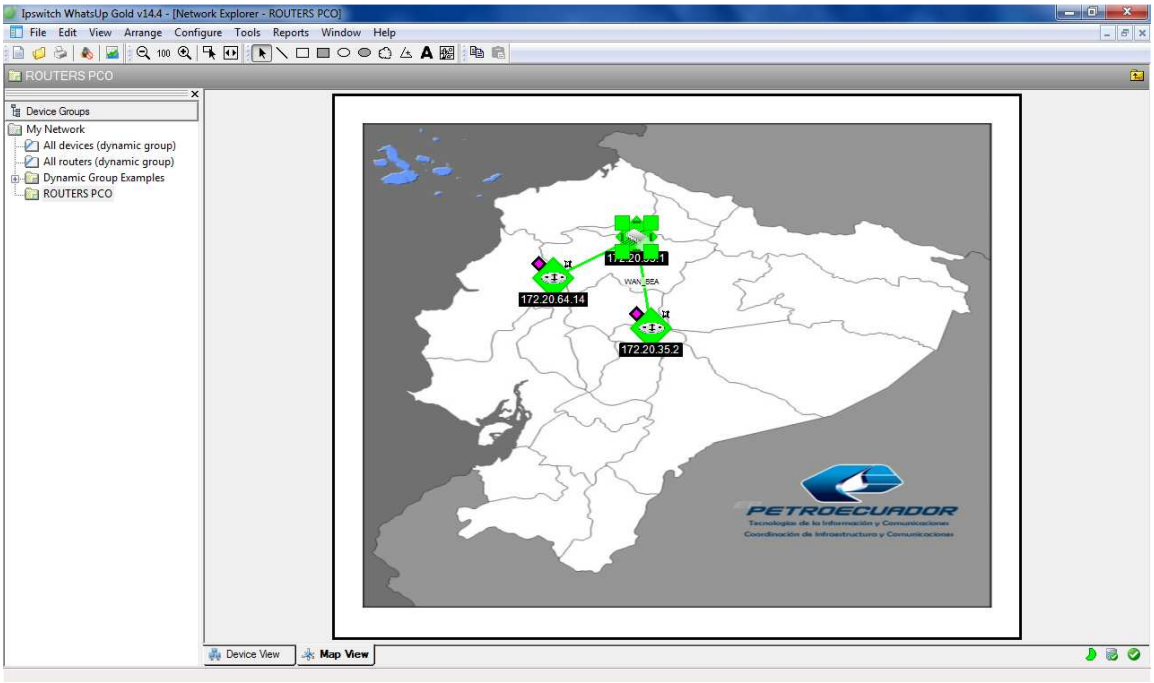


Figura 4.81 Interfaz de Monitoreo de What´s Up

Interfaz Web Home

El programa What´s Up permite un monitoreo de los dispositivos a través de navegadores web, facilitando su gestión desde cualquier máquina dentro de la red del prototipo.

En las figuras 4.82 y 4.83 se muestra la interfaz web principal para el monitoreo de los dispositivos. Dentro de esta interfaz se indica el mapa de los dispositivos monitoreados, el tiempo de respuesta del ping de los dispositivos, mostrados gráficamente, algunas estadísticas de los indicadores de rendimiento y de los dispositivos monitoreados en general.

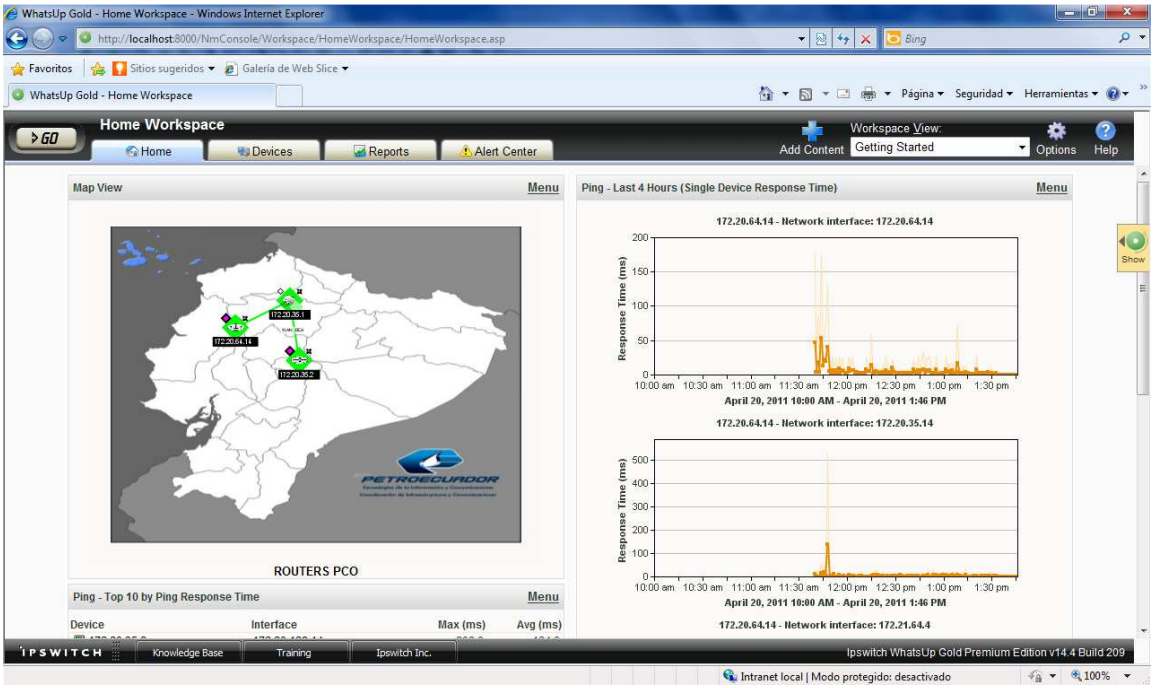


Figura 4.82 Interfaz Web principal parte 1

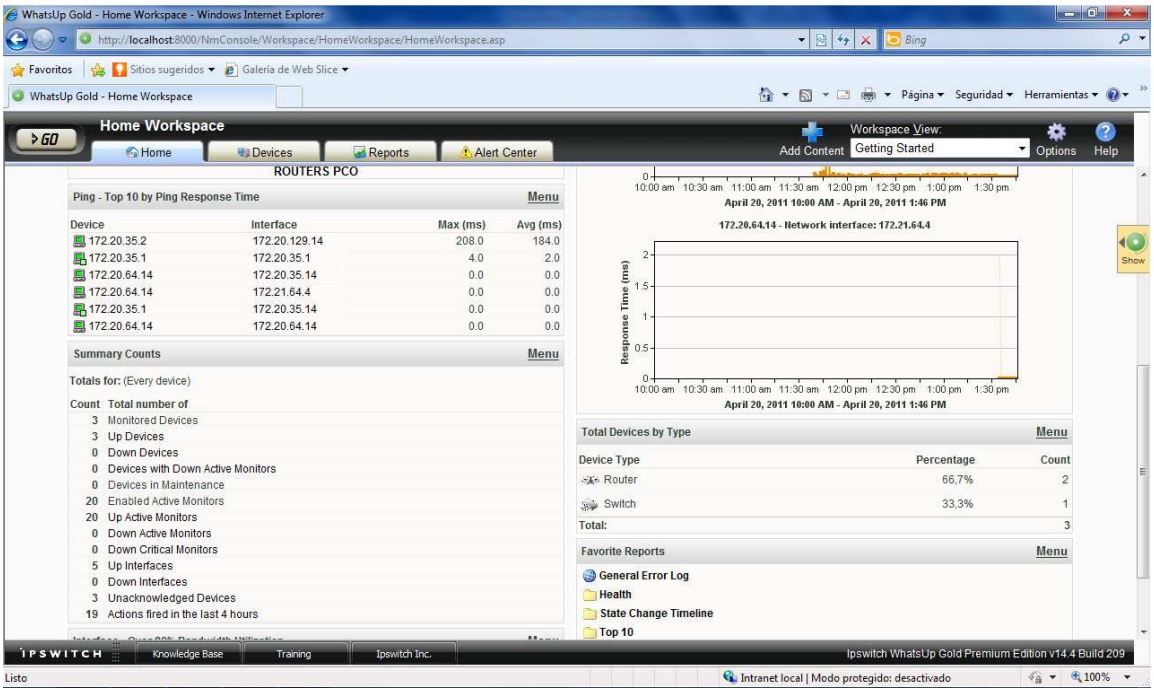


Figura 4.83 Interfaz Web principal parte 2

Interfaz de Monitoreo Web de router Rocío

En la figura 4.84 se muestra la interfaz web de monitoreo del router Rocío. En esta pantalla se indica información del router Rocío como: nombre del dispositivo, tipo de dispositivo, dirección IP, información del grupo system de snmp, una tabla con los cambios de estado de los parámetros monitorizados (Interfaces, ping, power supply, fan, temperatura), tiempos de respuesta del ping de forma gráfica. Además a través de esta interfaz web se puede observar los reportes de los parámetros de rendimiento, de las alarmas de nivel de rendimiento y de los demás parámetros ya indicados en el *subcapítulo 4.2.3.3 Administración de Rendimiento*

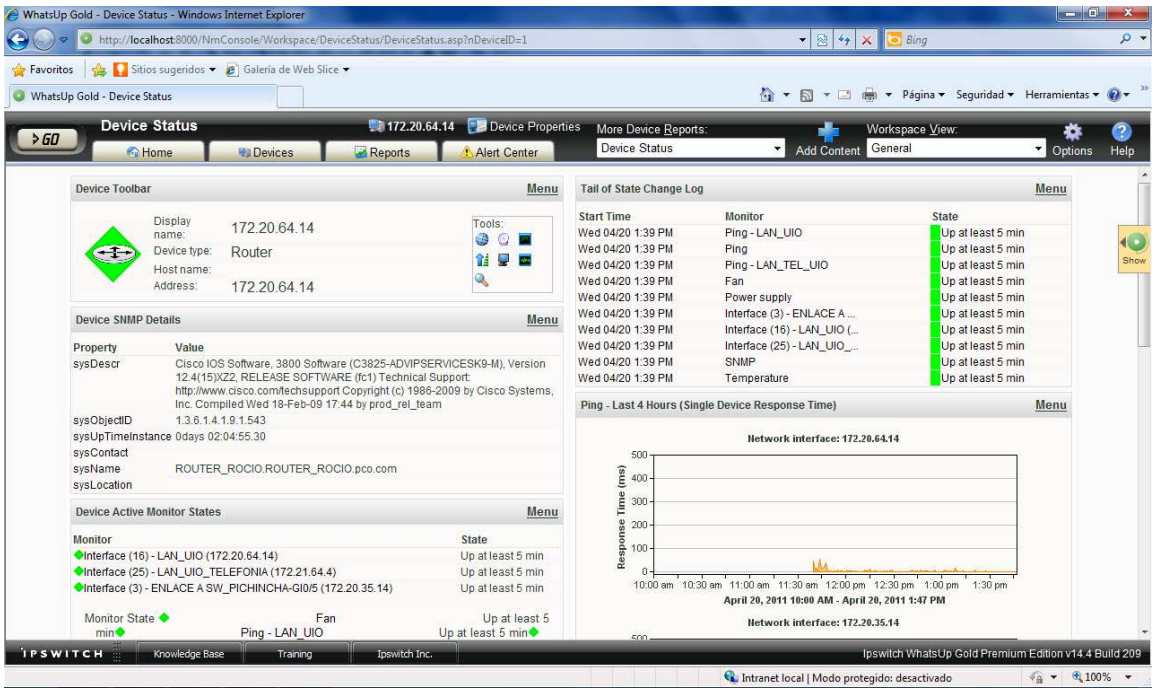


Figura 4.84 Interfaz web de monitoreo del router Rocío

Interfaz de Monitoreo Web de switch Pichincha

En la figura 4.85 se muestra la interfaz web de monitoreo del switch Pichincha. En esta pantalla se indica la información ya descrita en *Interfaz de Monitoreo Web de router Rocío.*

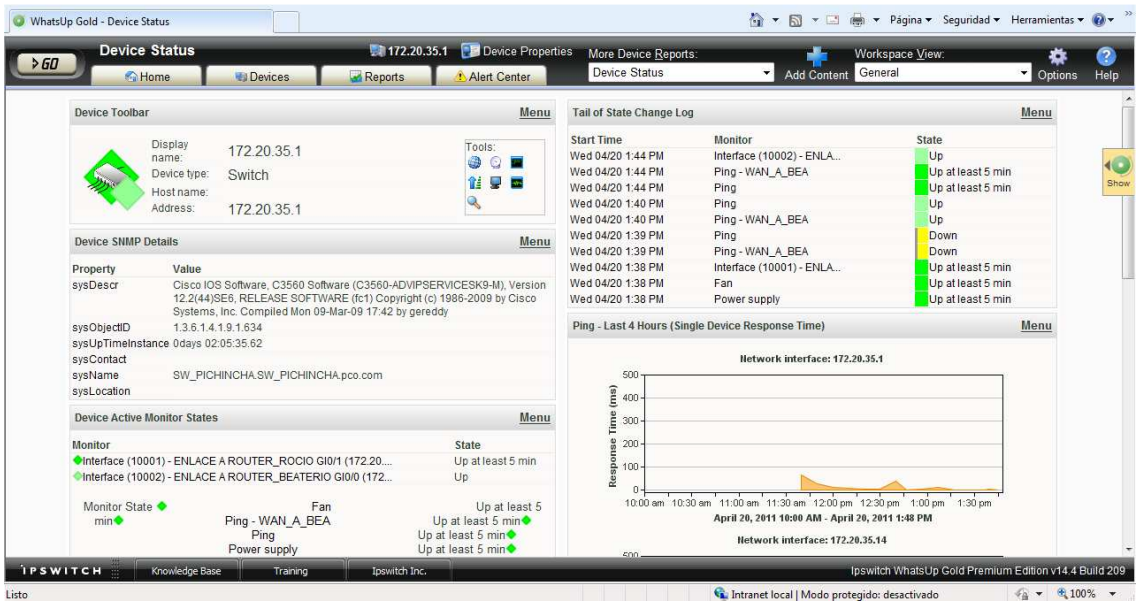


Figura 4.85 Interfaz web de monitoreo del switch Pichincha

Interfaz de Monitoreo Web de router Beaterio

En la figura 4.86 se muestra la interfaz web de monitoreo del router Beaterio. En esta pantalla se indica la información ya descrita en *Interfaz de Monitoreo Web de router Rocío.*

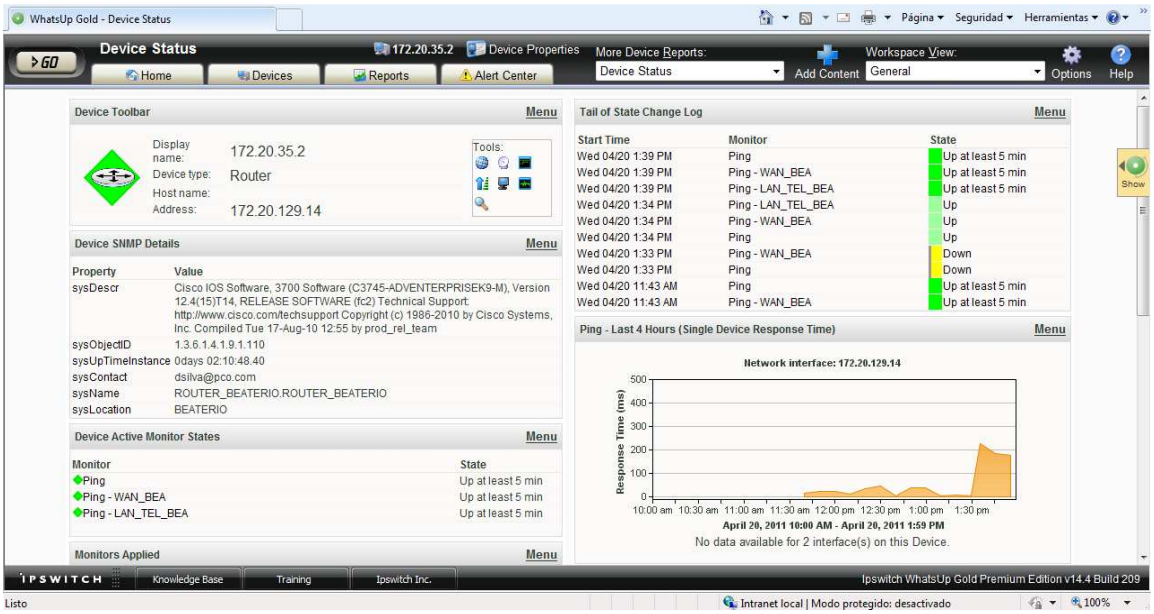


Figura 4.86 Interfaz web de monitoreo del router Beaterio

Monitoreo de los Parámetros de Rendimiento

En las figuras de a continuación se muestra gráficamente el monitoreo de algunos parámetros de Rendimiento de los equipos.

En la figura 4.87 se indica el monitor de la utilización de las interfaces del router Beaterio

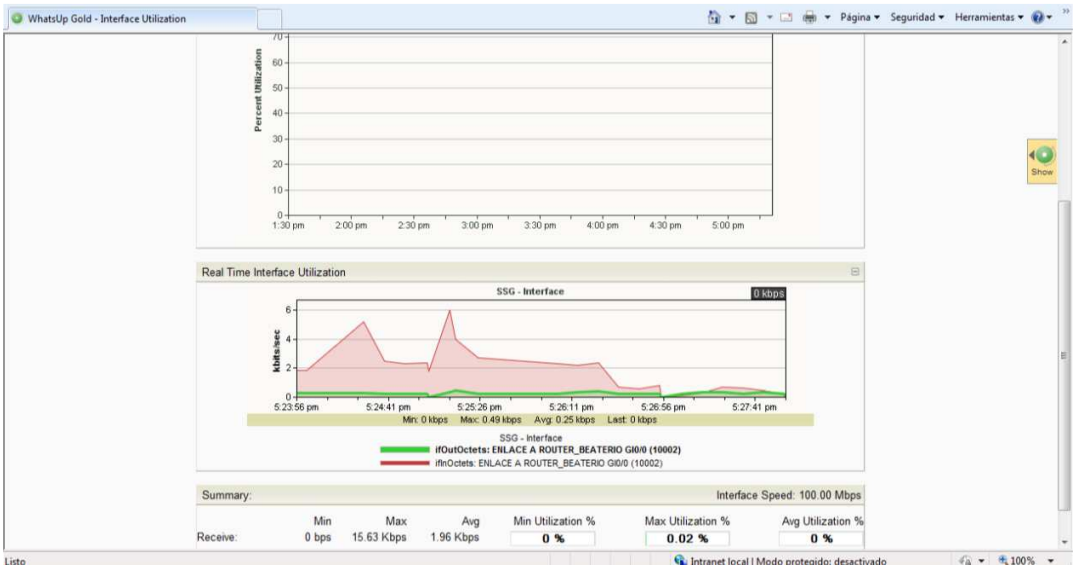


Figura 4.87 Monitoreo de las interfaces del router Beaterio

En la figura 4.88 se indica el monitor de la utilización del CPU del router Rocío

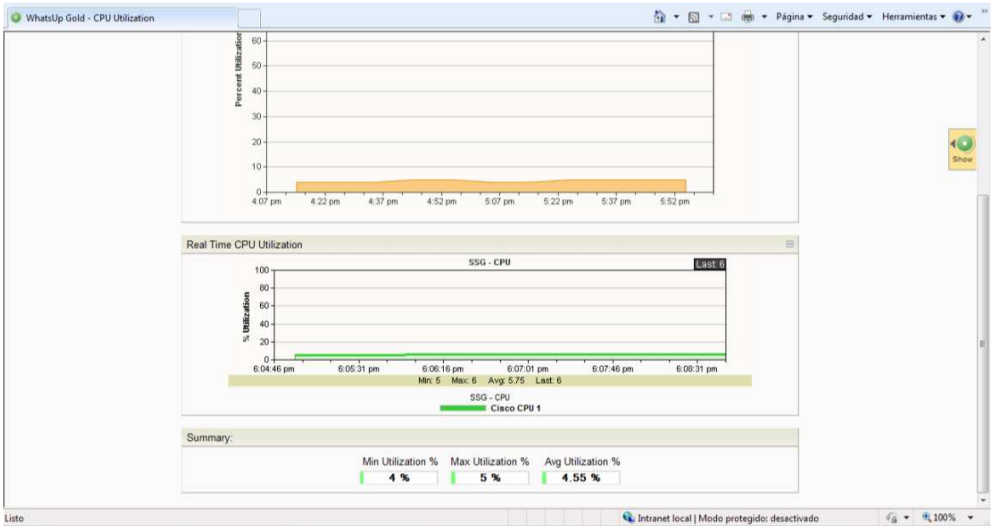


Figura 4.88 Monitoreo de la utilización de CPU del router Rocío

Estos parámetros y los ya descritos en el subcapítulo *4.2.3.3 Administración de Rendimiento* se encuentran monitorizados para los routers Rocío y Beaterio, y para el switch Pichincha del prototipo presentado.

Manejo de Alarmas

El manejo de alarmas se lo realiza a través de la interfaz web del Alert Center. En esta interfaz se indican los dispositivos que han sido alarmados debido a que han sobrepasado alguno de los umbrales configurados (véase subcapítulo *4.2.3.3.4 Establecimiento de Umbrales*) y si se ha tomado alguna acción a estas alarmas. En las figuras 4.89 y 4.90 se indica la interfaz del Alert Center.

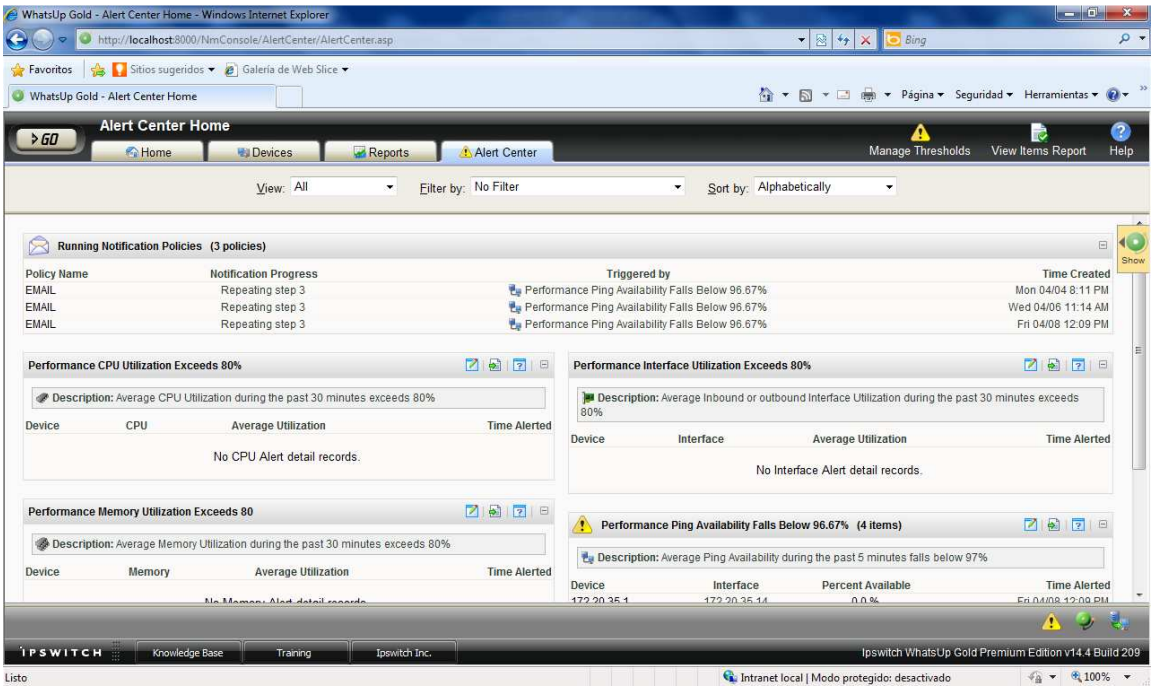


Figura 4.89 Interfaz del Alert Center parte 1

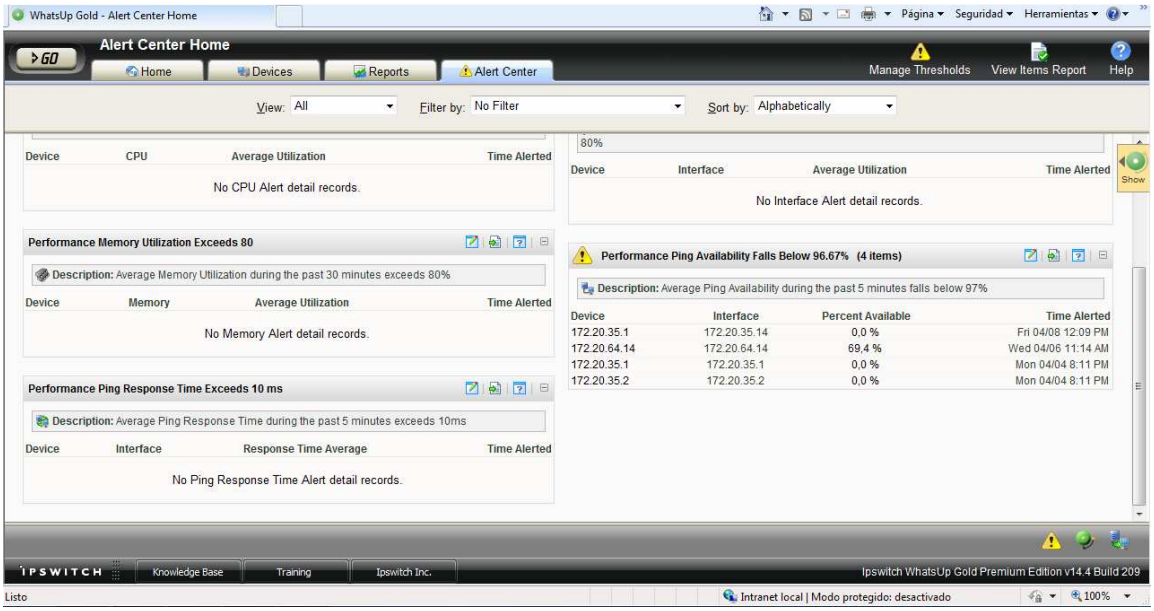


Figura 4.90 Interfaz del Alert Center parte 2

Además de visualizar la interfaz del Alert Center se ha configurado alarmas sonoras y visuales que se disparan inmediatamente si algún indicador de rendimiento de los dispositivos ha dejado de funcionar. En la figura 4.91 se indica una alarma visual disparada por algún parámetro de rendimiento que ha dejado de funcionar en uno de los dispositivos monitoreados.

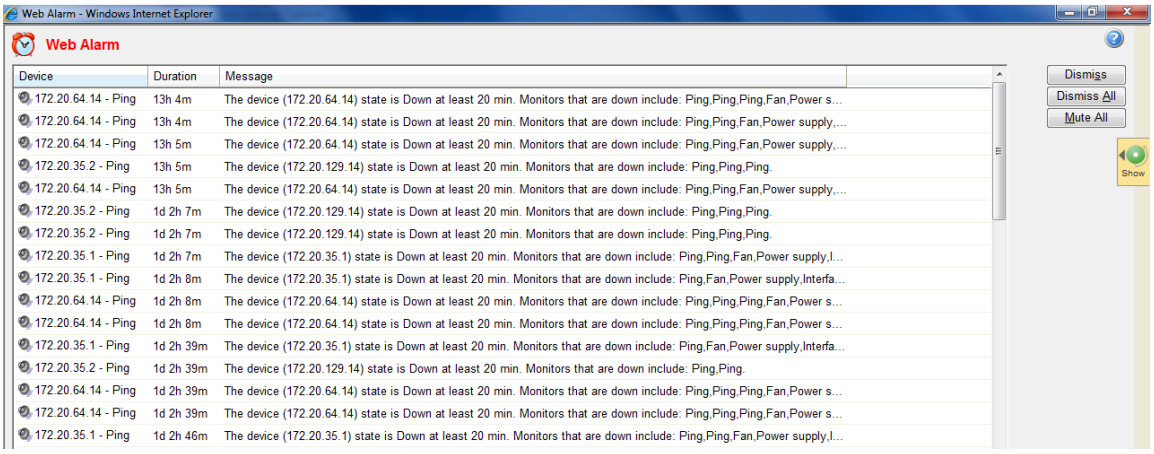


Figura 4.91 Alarma Visual indicando que parámetro a dejado de funcionar y en que dispositivo.

4.3.3.3.2. Kerio Connect

El programa Kerio Connect funciona como el servidor de correo de What´s Up y se encarga de enviar correos electrónicos a los administradores de red, indicando si algún dispositivo ha sobrepasado los umbrales configurados (véase subcapítulo *4.2.3.3.4 Establecimiento de Umbrales*).

Interfaz Web de Kerio Connect

En la figura 4.92 se indica la interfaz web de administración del programa Kerio Connect

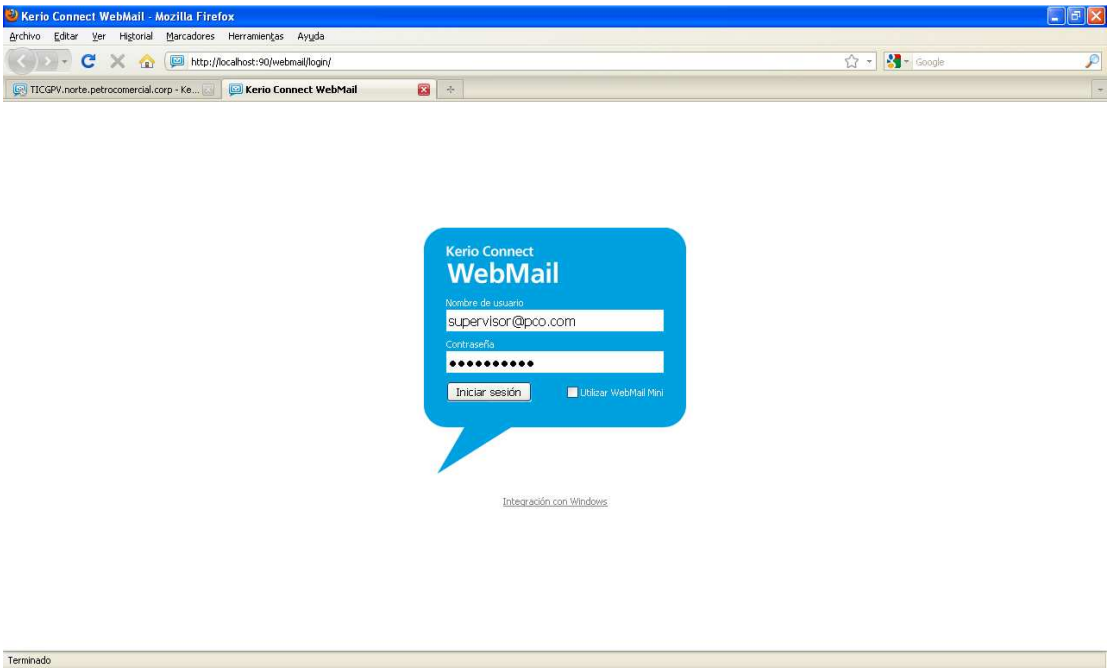


Figura 4.92 Interfaz de administración web de Kerio Connect

Mediante la interfaz web de administración del programa Kerio Connect se puede configurar las cuentas de correo, a la cual llegarán los mensajes de alarma de los dispositivos monitoreados (véase subcapítulo *4.2.3.3.2 Alarmas de Nivel de Rendimiento*). En la figura 4.93 se indican los usuarios de las cuentas de correo creadas.

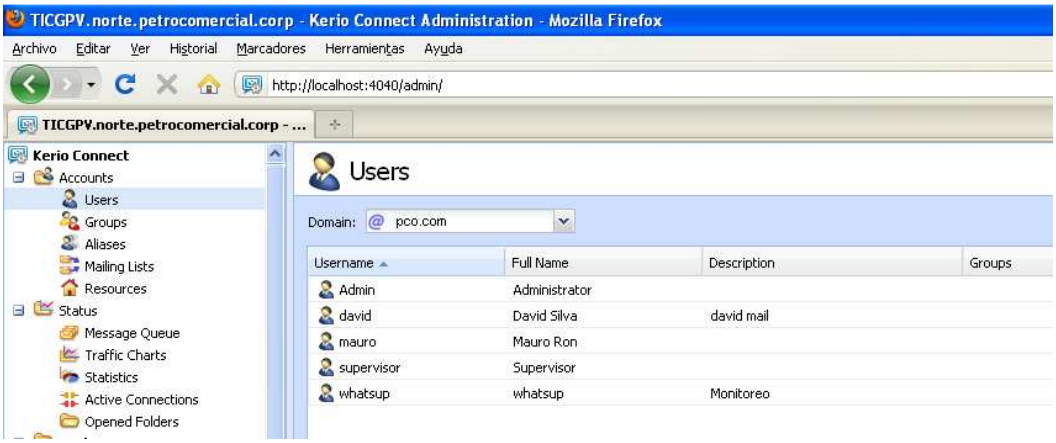


Figura 4.93 Usuarios de las cuentas de correo creadas

En la figura 4.94 se indica los servicios que están ejecutándose, con sus respectivos números de puerto, para el correcto funcionamiento de Kerio Connect.

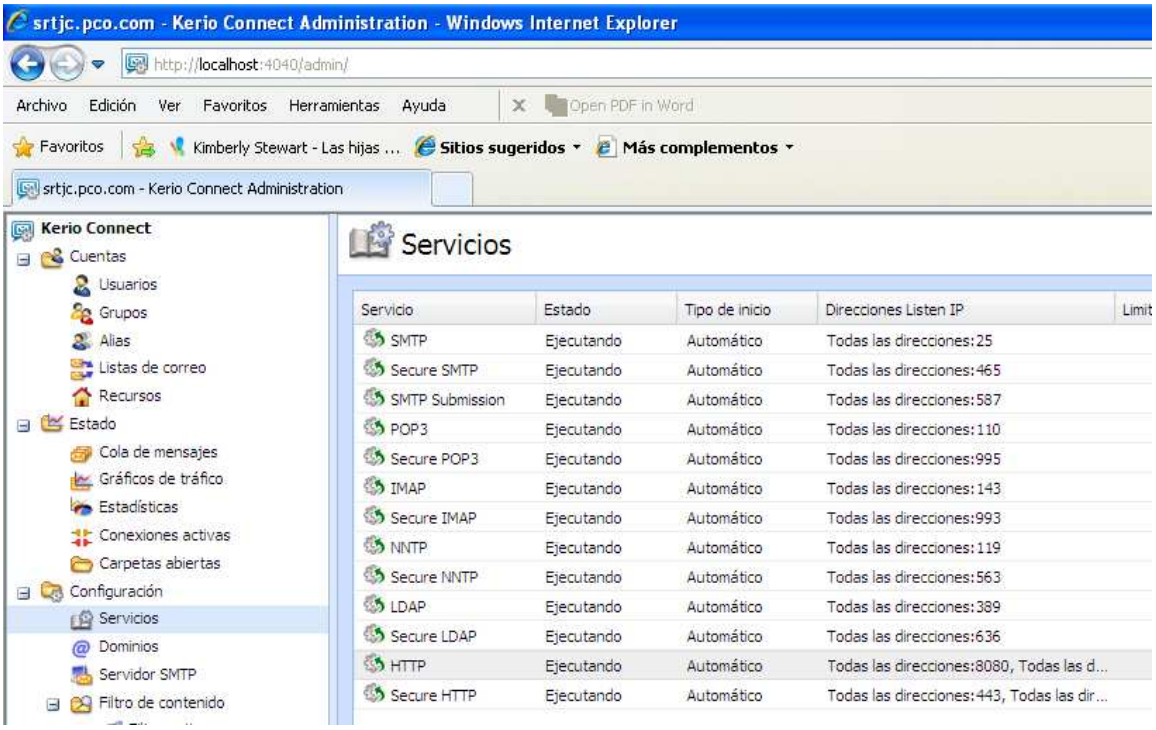


Figura 4.94 Servicios ejecutados en Kerio Connect

En la figura 4.95 se muestra el dominio configurado en el programa Kerio Connect. El dominio configurado es pco.com.

Figura 4.95 Dominio configurado en Kerio Connect

En la figura 4.96 se muestra el formato de uno de los mensajes recibidos en la cuenta de un usuario de correo debido a que un dispositivo se encuentra alarmado.

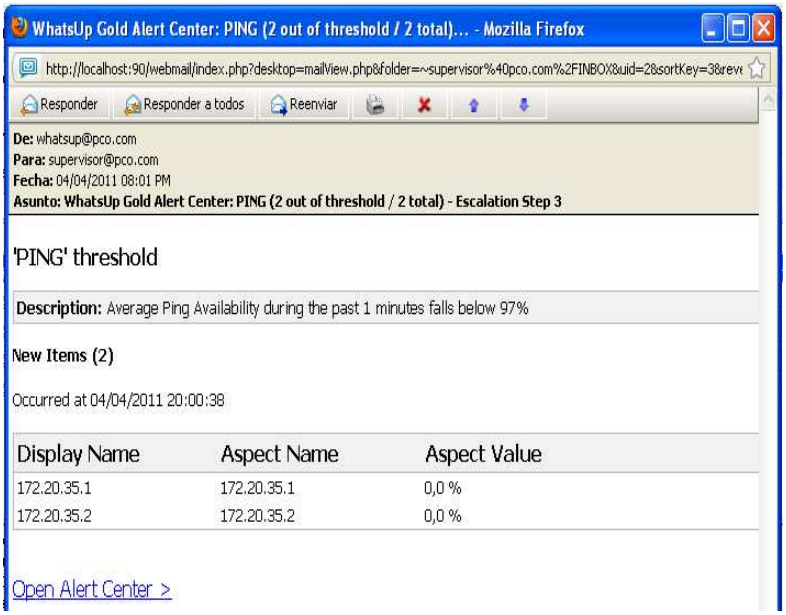


Figura 4.96 Formato del mensaje de correo recibido

4.4. PROCEDIMIENTOS PARA RECUPERACIÓN DE FALLAS

Las actividades realizadas por el área de TICS de PETROCOMERCIAL, tiene una relevancia importante dentro de la empresa, por lo que su red debe mantenerse completamente operativa. Cualquier fallo dentro de la red puede ser crítico, por lo cual se debe implementar un procedimiento de recuperación de fallas, que ayudaría, en caso de ocurrir un error, a restablecer el funcionamiento de la red lo más pronto posible. Las recomendaciones para este procedimiento son:

- Familiarizarse con el equipo, conocer su funcionamiento e identificar los indicadores de operación normal del equipo.
- Tener siempre actualizado tanto la topología lógica y física de la red. Registro de las conexiones, enlaces, interfaces, entre otros.
- Verificar los problemas de manera ordenada y paso a paso, se puede comenzar desde las capas más bajas del modelo OSI o TCP/IP, por lo general se comienza por la capa física que es donde se halla la mayoría de errores.
- Inspeccionar minuciosamente cambios en la configuración de los equipos, no saltarse pasos, y revisar desde la configuración más básica, direcciones ip, interfaces apagadas, etc., hasta lo más complejo, protocolos de enrutamiento, listas de acceso, etc.

4.4.1. FALLAS EN CONECTIVIDAD

Las interfaces de los dispositivos de red, routers y switches en nuestro caso, son uno de los principales elementos a revisar cuando suceden problemas de conectividad. El procedimiento a seguir para corregir estos problemas son:

4.4.1.1. Fallas de Configuración

Físicamente y visualmente este problema se lo identifica de acuerdo al color del puerto, en los switches, y la luz indicativa en los routers. Podemos asumir que una

falla ocurrió en un puerto de un switch cuando su indicador esté en color ambar, o cuando no haya una luz indicadora, en el caso de los routers. El procedimiento a seguir es:

- Verificar que el puerto no esté apagado
- Puede producirse un estado de no respuesta de la interfaz, el cual puede arreglarse apagando y encendiendo manualmente el puerto.
- Verificar la información de la interfaz, como dirección ip, máscara de subred, en el caso de los switches, verificar los parámetros de velocidad, modo troncal, dúplex, otros.
- Luego de examinar posibles problemas en la capa física, pasar a capas superiores para verificar problemas tales como configuraciones del modo troncal, vlans configuradas, servicios activados, configuraciones de enrutamiento, entre otros.

4.4.1.2. Fallas de Hardware

- Comprobar que realmente el indicador lumínico está correctamente funcionando, y no es problema de la interfaz.
- Verificar que a ambos lados de la conexión estén levantadas las interfaces, ya que si uno de los dos lados está desactivado, el enlace se mostrará como down.
- Utilización correcta de cables de red, cruzados, directos, y en el caso de la fibra, determinar si se utiliza multimodo o monomodo.
- Verificación del correcto funcionamiento de los patch cord, revisar parámetros como correcta utilización del código de colores, sin cortes en la longitud del cable, no sobrepasar la norma técnica sobre la distancia del cable. Pruebas como éstas se las puede realizar utilizando un probador de cable.
- Revisar posibles fallas en tarjetas NIC defectuosas, realizar pruebas con cables que se verifiquen que están funcionando correctamente, para descartar problemas de medios de transmisión.

4.4.1.3. Fallas del Equipo Físico

Si se han realizado tanto las pruebas de configuración como de hardware y el problema persiste, se puede considerar fallas del equipo físico tanto en hardware como en software.

- Tarjetas de red que presentan problemas
- Problemas con el IOS de los equipos, posiblemente versiones desactualizadas o con errores
- Posibles soluciones a problemas presentados en las interfaces de red son:
    - Apagar y prender la interfaz
    - Resetear el módulo
    - Reiniciar el equipo
    - Actualizar el IOS del equipo
- Si el problema continúa se recomienda reemplazar el equipo.

4.4.1.4. Problemas de Cableado y Medio Físico

En la figura 4.97 se indica algunos problemas y sus respectivas soluciones, con respecto al cableado y medio físico.

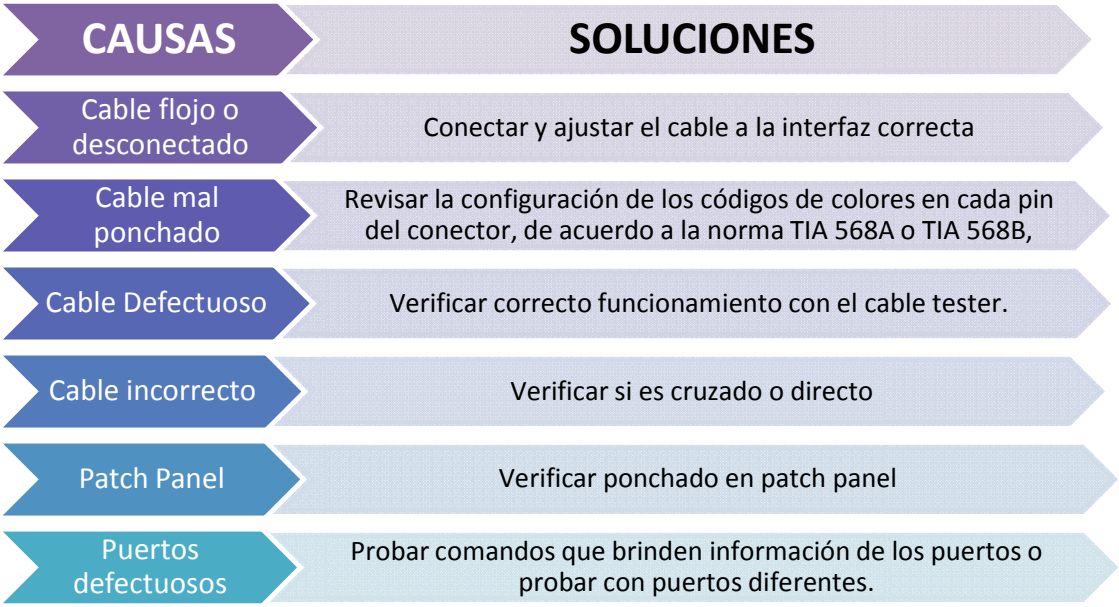


Figura 4.97 Causas y soluciones a problemas de cableado

Además de las pruebas a nivel de área local de cableado se deberá determinar, problemas a nivel de enlace microonda, para lo cual se deberá:

- Revisar alarmas locales o remotas.
- Revisar por consola las alarmas.
- Revisión y reemplazo de la parte que indique la alarma.
- Revisas estado de tributarios (disable).
- Hacer un LOOP lógico para verificar errores con el Datacom.
- Medir niveles de recepción AGC (Control Automático de Ganancia), deberá estar dentro de los umbrales 2.5V a 4 V, 73dB -45dB.
- Realizar una revisión al transmisor y a las antenas (alineación)
- Apagar un equipo y realiza la medición de AGC para determinar si existe interferencia.
- Revisar ID number.
- Reemplazar el equipo.

4.4.2. PASOS Y RECOMENDACIONES PARA EL PROCEDIMIENTO DE RECUPERACIÓN DE FALLAS

Como resumen de un procedimiento de recuperación de fallas tenemos la figura 4.98 que indica los pasos a realizarse si un equipo de red, en este caso un router, falla. En la figura 4.99 se detallan algunas recomendaciones para poner en práctica un procedimiento de recuperación de fallas.

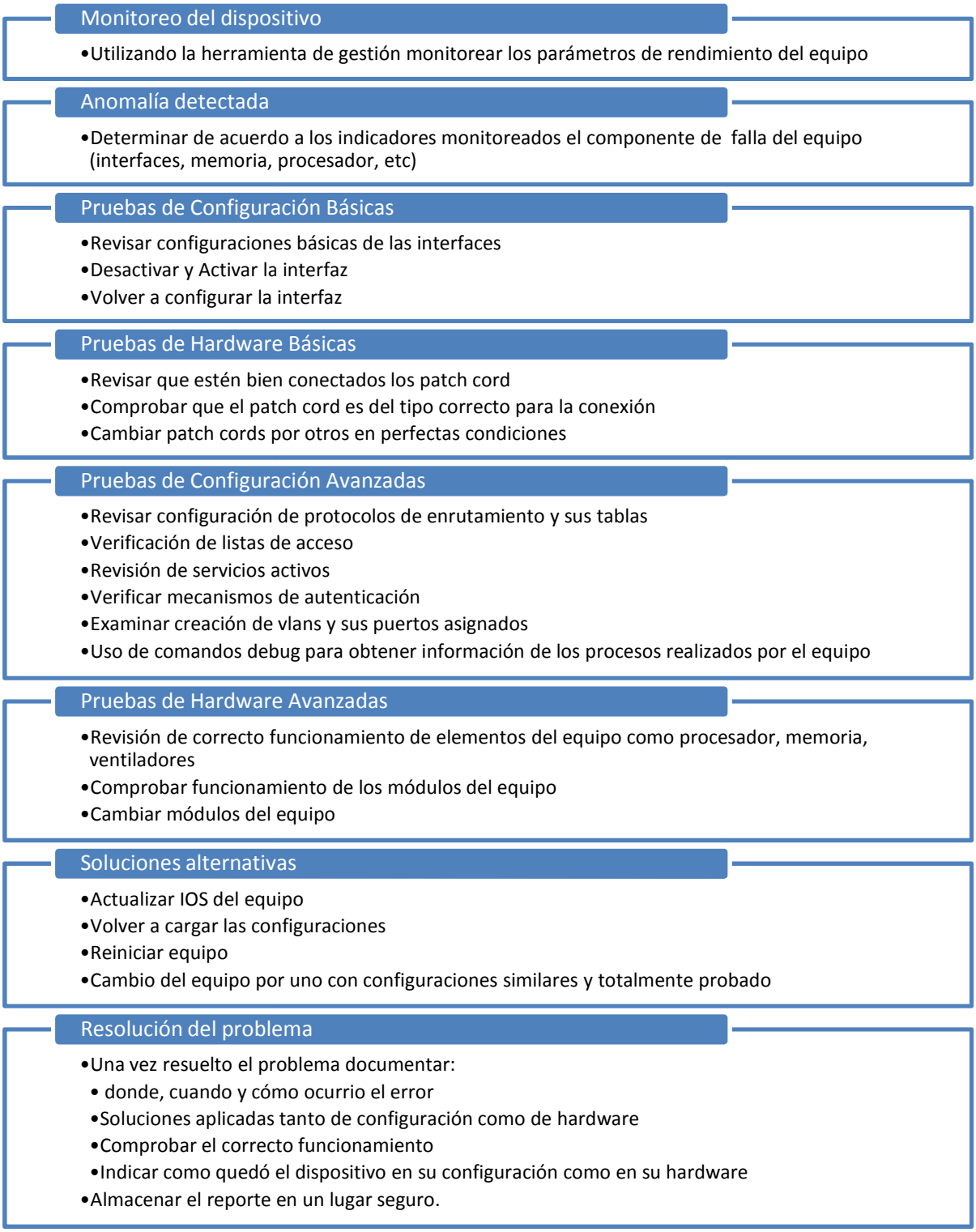


Figura 4.98 Procedimiento de recuperación de fallas de routers

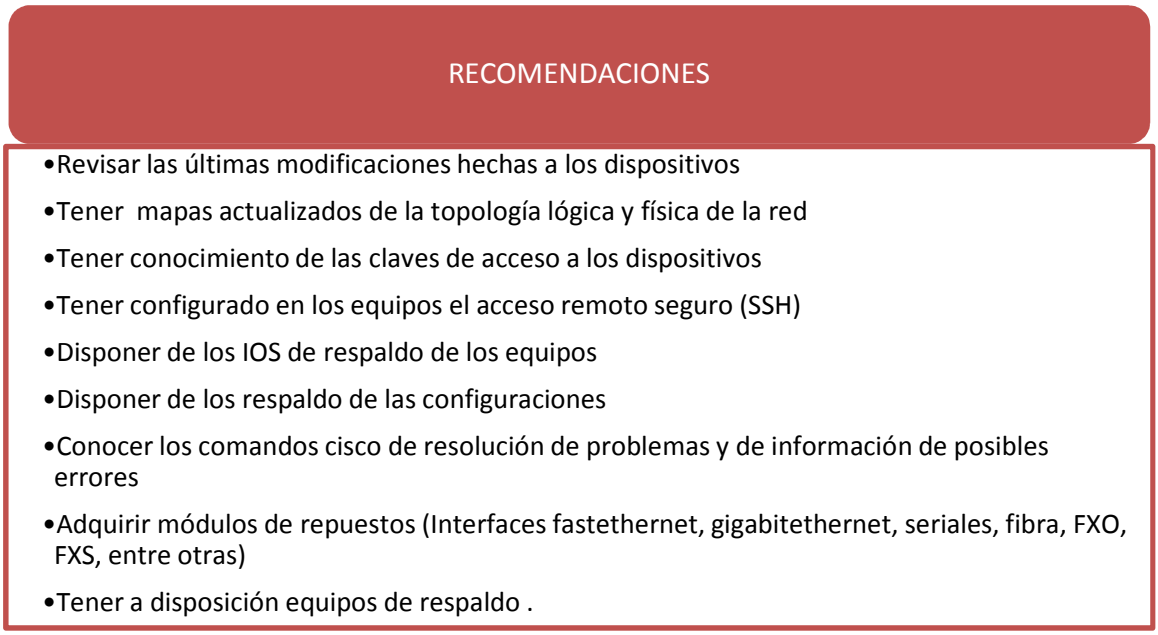


Figura 4.99 Recomendaciones para el procedimiento de recuperación de fallas

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Debido a la evolución de los equipos y medios de transmisión, Ethernet ha pasado de ser un protocolo destinado a redes de área local a redes que cubren extensiones territoriales considerables. La evolución de la fibra óptica y el desarrollo de radios microondas con soporte para Ethernet permiten cubrir extensiones en el orden de las decenas y centenas de Km.

- La complejidad y el tamaño considerable de la red de Petrocomercial, hace necesario el uso de un protocolo que no consuma excesivamente recursos de red, al considerar EIGRP como el protocolo de enrutamiento a implementar garantizamos una administración más eficiente, optimización del ancho de banda de los enlaces y tiempos de convergencia menores.

- En topologías en las cuales existan puntos de distribución, como los cerros Pichincha y Atacazo, es más eficiente utilizar protocolos que tengan un mecanismo de control de acceso al medio, que permita compartir los recursos conforme sean necesarios, al eliminar Frame Relay (con éste se eliminan los circuitos virtuales), se crea un solo canal de la matriz a los cerros Pichincha y Atacazo respectivamente, que se compartirá para todos los nodos remotos conectados a estos puntos, con esto se tiene un uso de los anchos de banda

de los enlaces más eficiente. La implementación de esta tecnología más los equipos y las políticas de calidad de servicio, permitirán utilizar de mejor forma los recursos de red de Petrocomercial.

- El análisis de tráfico realizado con la herramienta ALLOT, demostró que no es necesario un crecimiento exagerado en los Anchos de Banda de los enlaces de la red WAN de Petrocomercial, sino un mejor control y utilización de los mismos, lo cual se plantea conseguir con el protocolo Ethernet, los radios con interfaces Ethernet, los equipos planteados y los segmentadores de tráfico ya implementados.

- El constante crecimiento de la empresa y la inclusión de nuevos servicios tecnológicos, merece una consideración a la hora de calcular los requerimientos de ancho de banda, el porcentaje considerado para el mismo en los próximos cinco años es de 10%, lo que representa un incremento a futuro prudente, de acuerdo a las tendencias del índice de crecimiento de la empresa en los últimos años.

- El uso de equipos en los cuales existe convergencia de servicios, como en el caso de los ruteadores, los cuales manejan enrutamiento de datos, telefonía IP y en el algunos nodos DHCP, reduce costos, debido a que el hardware que se adquiere es uno solo para todos los servicios, pero se debe tomar en cuenta que los equipos adquiridos deben garantizar alta disponibilidad de los servicios, debido a que si el hardware falla todos se verían afectados.

- El modelo de Gestión de Red planteado, que se basa en la arquitectura FCAPS del modelo ISO/OSI, el protocolo SNMP v3 del modelo de Internet y el uso de la herramienta Whats'Up Gold, buscan mantener el control, administración, y gestión de los routers actuales adquiridos, además de reducir al mínimo los tiempos en los cuales el sistema no está disponible.

- La herramienta de gestión Whats'Up Gold nos permite implementar varias tareas del modelo de gestión planteado en el Proyecto de Titulación, las cuales están basadas en el modelo FCAPS, los parámetros configurados se basaron en cálculos y las políticas de rendimiento de los equipos.

- La determinación de un plan de migración permite conocer de forma ordenada y cronológica los pasos a seguir en la implementación de los equipos, disminuyendo el impacto en la utilización de la nueva tecnología y permitiendo manejar los errores de una manera más rápida y efectiva.

- Actualmente Petrocomercial no tiene implementado ningún procedimiento de recuperación de fallas, que permita gestionar de manera rápida y efectiva una falla de sus equipos. El plan de recuperación de fallas presentado en el proyecto, da los lineamientos básicos para que en un corto plazo se pueda elaborar una verdadera infraestructura aplicada a la recuperación de fallos en los equipos, que permita mantener una red confiable y disponible.

- La migración de la integración de las centrales telefónicas con la matriz que se lo realizaba por tarjetas fxo, a una integración a nivel de IP, aumenta la

escalabilidad de la solución, ya que no dependerá de la tarjetería y el número de extensiones, sino del ancho de banda con el que cuente el enlace.

- En telefonía las funciones adicionales como correo de voz o contestadora automática se las configura tanto en el IOS del equipo como en su módulo de servicios integrados, teniendo siempre en cuenta que se posea las licencias activas para dichos servicios.

- Para realizar el transcoding entre diferentes códecs o para realizar la conversión de protocolos de señalización (SCCP, SIP), es necesario el uso de recursos adicionales (DSP). Los ruteadores realizan estas conversiones en hardware por lo que genera menores tiempos de latencia.

5.2. RECOMENDACIONES

- Debido a un error en el diseño del direccionamiento de la red de PETROCOMERCIAL, es necesario migrar toda la red de telefonía, ya que está utilizando direccionamiento público, si bien la telefonía IP está funcionando, cuando los host de la red intenten acceder a una dirección publica dentro del mismo rango, se generan problemas debido a que los datos son enrutados a los teléfonos.

- Como se explicó en el capítulo III, existe una política en Petrocomercial que no permite colocar más de dos modelos de routers para el proyecto, la cual a nuestro criterio debe ser modificada debido a que por el número de usuarios en determinados nodos es necesario modelos de características inferiores.

- El mantener una sola marca de dispositivos dentro de la infraestructura de red puede generar ventajas y desventajas. Una desventaja es que la inversión inicial puede ser muy costosa, sin embargo a largo plazo se puede obtener un desempeño estable y robusto en la red, obteniendo un 100 % de compatibilidad entre todos los equipos.

- Debido a que en Petrocomercial no existe un modelo de Gestión de Red implementado y que el presente Proyecto de Titulación plantea el modelo de Gestión solo para los ruteadores adquiridos, es necesario desarrollar un modelo de Gestión para toda la red de Datos.

- Debido a que los ruteadores soportan tanto el protocolo SCCP como SIP, se pueden utilizar los teléfonos MITEL con los que se cuenta en la actualidad, debido a que soportan SIP, mas los teléfonos con soporte SCCP que se adquieran.

- Al realizar la compra de equipos con servicios integrados se recomienda que dentro de las especificaciones se detalle si los equipos vienen o no con licencias para realizar funciones específicas, en el caso de la telefonía, es necesario la activación de las licencias para brindar servicios de correo de voz o de contestadora automática.

- Es necesario que el modelo de Gestión planteado sea difundido a todos los técnicos que tengan participación directa en la configuración, mantenimiento o gestión de los ruteadores, para que el modelo sea de cumplimiento obligatorio.

- En el modelo de gestión planteado todos los puntos que éste abarca son importantes, sin embargo la gestión de seguridad es uno de los que se debería implantarse con mayor prioridad, ya que sin una adecuada administración de seguridad en los equipos, los demás puntos del modelo FCAPS se verían afectados negativamente, dando lectura falsas de sus indicadores, ya sea por ataques o errores.

- Para un correcto funcionamiento del modelo de gestión se debe trabajar con todas las tareas de administración en conjunto, considerando un monitoreo constante de los principales parámetros de cada una.

- Como el presente proyecto está pensado como una primera fase para la migración de la red de telefonía de Petrocomercial, para la segunda fase del proyecto se recomienda la adquisición de servidor de telefonía dedicado y la migración de IOS de los ruteadores adquiridos a sistemas de Supervivencia Remota.

REFERENCIAS BIBLIOGRÁFICAS

CAPÍTULO 1

▪ PÁGINAS WEB

1.1. Ethernet

- http://www.rediris.es/difusion/publicaciones/boletin/49/enfoque3.html

1.2. Frame Relay

- http://materias.fi.uba.ar/6621/material/framerelay/framerelay_ATM_fiuba.pdf
- http://www.it.uc3m.es/~prometeo/rsc/apuntes/frame/frame.html

1.3. Modelo de Gestión

- http://www.eie.fceia.unr.edu.ar/ftp/Tecnologiasdebandaangosta/Notas_sobre_TMN

▪ DOCUMENTOS ELECTRÓNICOS

1.4. Introducción a las Redes Digitales de Transmisión, Laboratorio de Comunicaciones II – 66.37 – Guillermo E. Gómez

1.5. Cisco, IP Telephony Express, 2005

- **LIBROS**

1.6. FRAME RELAY , Principles and Applications Philip Smith, ADDISON-WESLEY PUBLISHING COMPANY

1.7. Andrew S. Tanenbaum, Redes de Computadoras, 4ta Ed.

- **OTROS**

1.8. Folleto Ing. Soraya Sinche, Redes de Área Extendida, 2009

1.9. Folleto Ing. Pablo Hidalgo, Redes TCP/IP, 2008

1.10. Folleto Ing. Pablo Hidalgo, Redes LAN, 2008

1.11. Forum Frame Relay

1.12. Cisco CCNA v4, Módulo 1, Aspectos Básicos de redes, 2010

CAPÍTULO 2

- **PÁGINAS WEB**

2.1. Look at Lan

- *www.lookatlan.com*

2.2. Real VNC

- www.realvnc.com

2.3. Información de Petrocomercial

- www.eppetroecuador.ec

- **DOCUMENTOS ELECTRÓNICOS**

2.4. Allot: The Traffic Mangement Handbook, ALLOT Communications, 2006.

2.5. Rediseño de la red de área extendida de PETROCOMERCIAL con calidad de servicio, René Damián Padilla Benítez, 2008

2.6. Cisco, IP Telephony Express, 2005

- **OTROS**

2.7. Información de Servidores y Aplicaciones, recopilado en Petrocomercial.

CAPÍTULO 3

- **PÁGINAS WEB**

3.1. Características equipos Cisco

- *www.cisco.net*

- **DOCUMENTOS ELECTRÓNICOS**

3.2. Introducción a Student Guide IPTX (IP Telephony Express) V2.0

- **LIBROS**

3.3. Fundamentos de Routing, Eduardo Collado Cabeza, 2009

CAPÍTULO 4

- **PÁGINAS WEB**

4.1. Gestión de redes

- http:// www.ramonmillan.com/tutoriales/gestionred.php
- integrared.blogspot.com/.../las-cinco-capas-funcionales-de-la.html

4.2. What's Up

- www.whatsupgold.com

4.3. Modelo de Gestión

- http://www.eie.fceia.unr.edu.ar/ftp/Tecnologiasdebandaangosta/Notas_sobre_TMN.pdf

4.4. Configuración Voice Mail

- http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_configuration_example09186a00808f9666.shtml#configs

▪ DOCUMENTOS ELECTRÓNICOS

4.5. Gestión De Redes Con SNMP, Prof. Vincenzo Mendillo, 2009

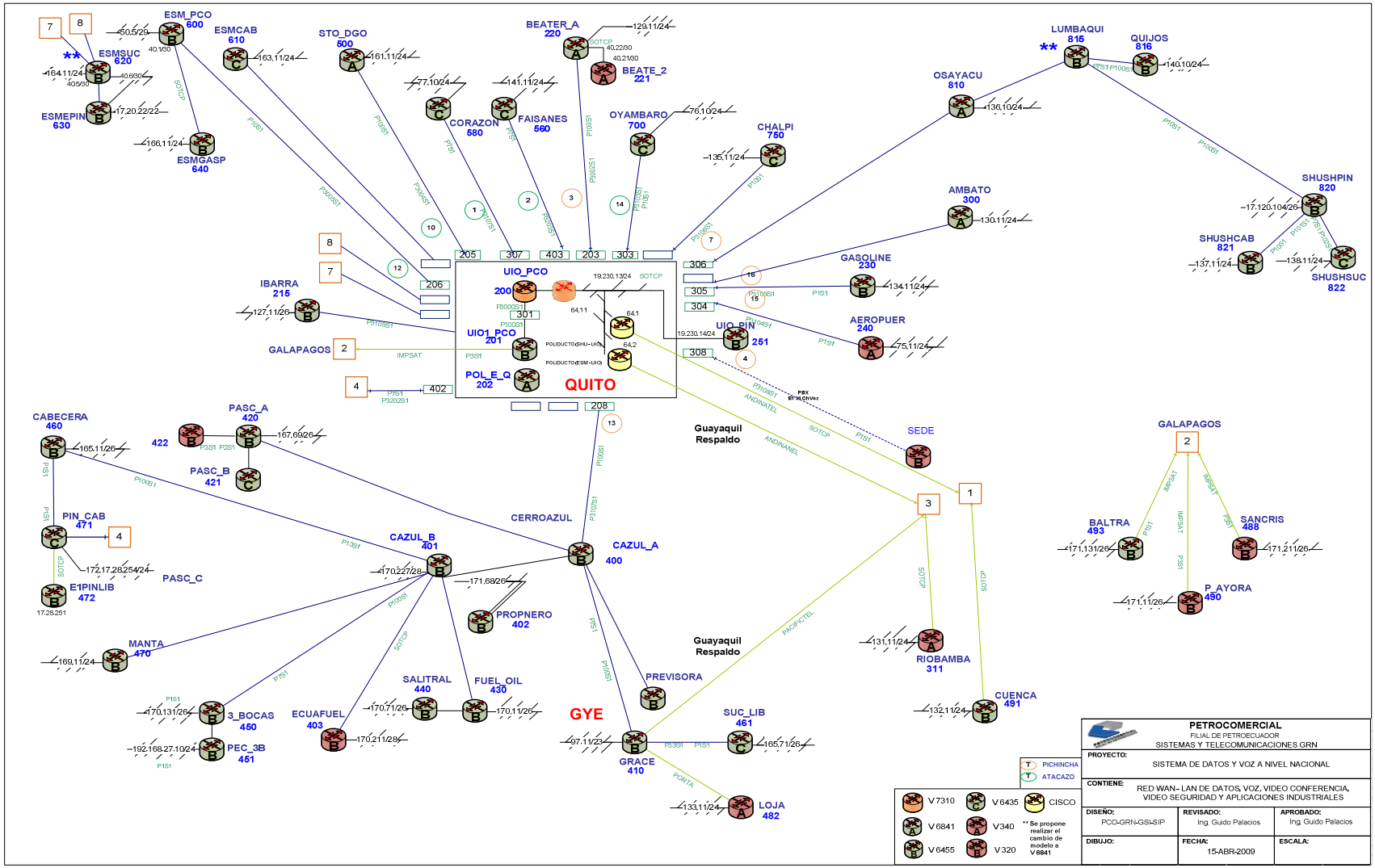
4.6. Cisco, IP Telephony Express, 2005

4.7. Manual de Usuario de What's UP GOLD

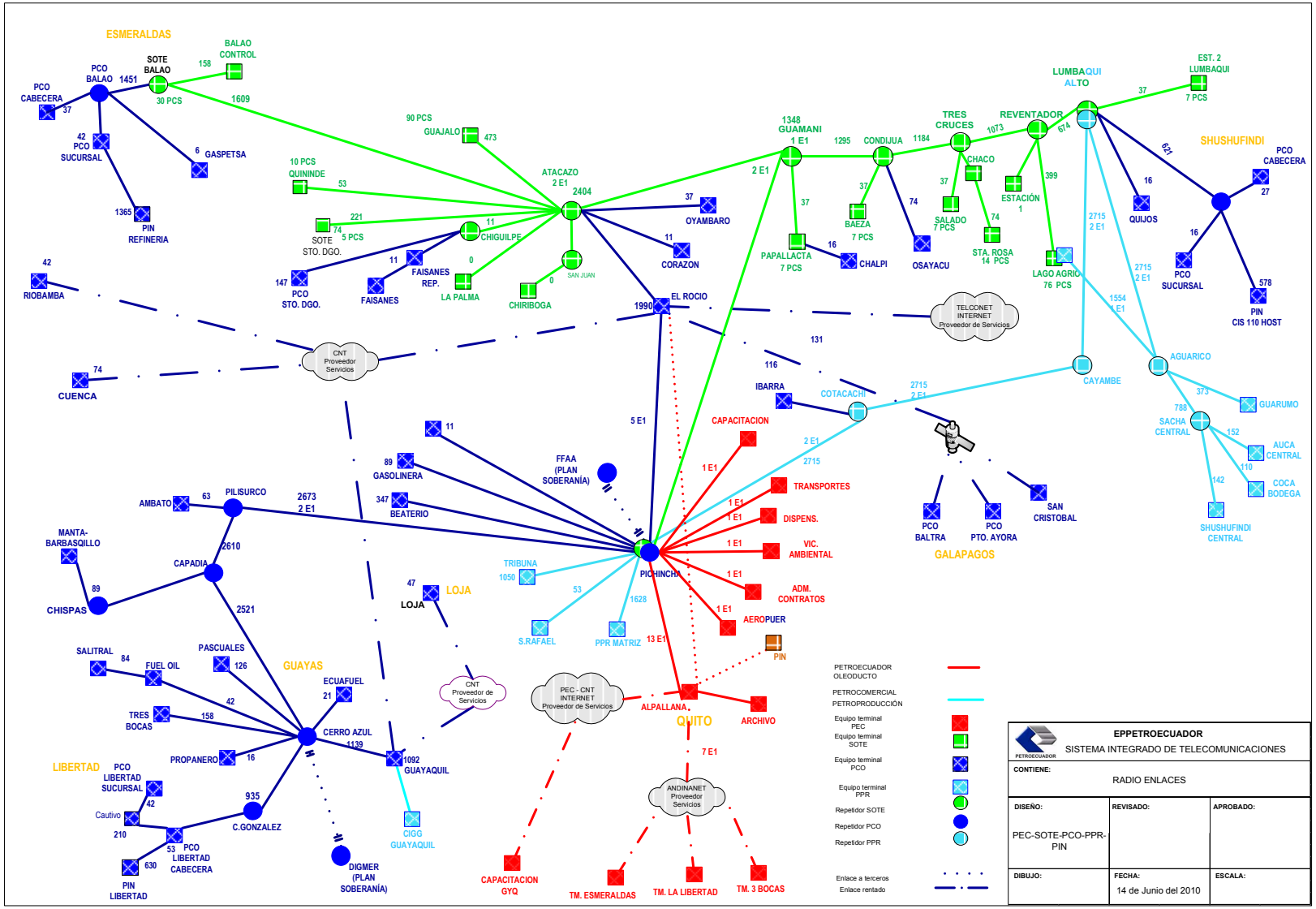
▪ OTROS

4.8. Cisco CCNA v4, Módulo 4, Accessing the Wan, 2010

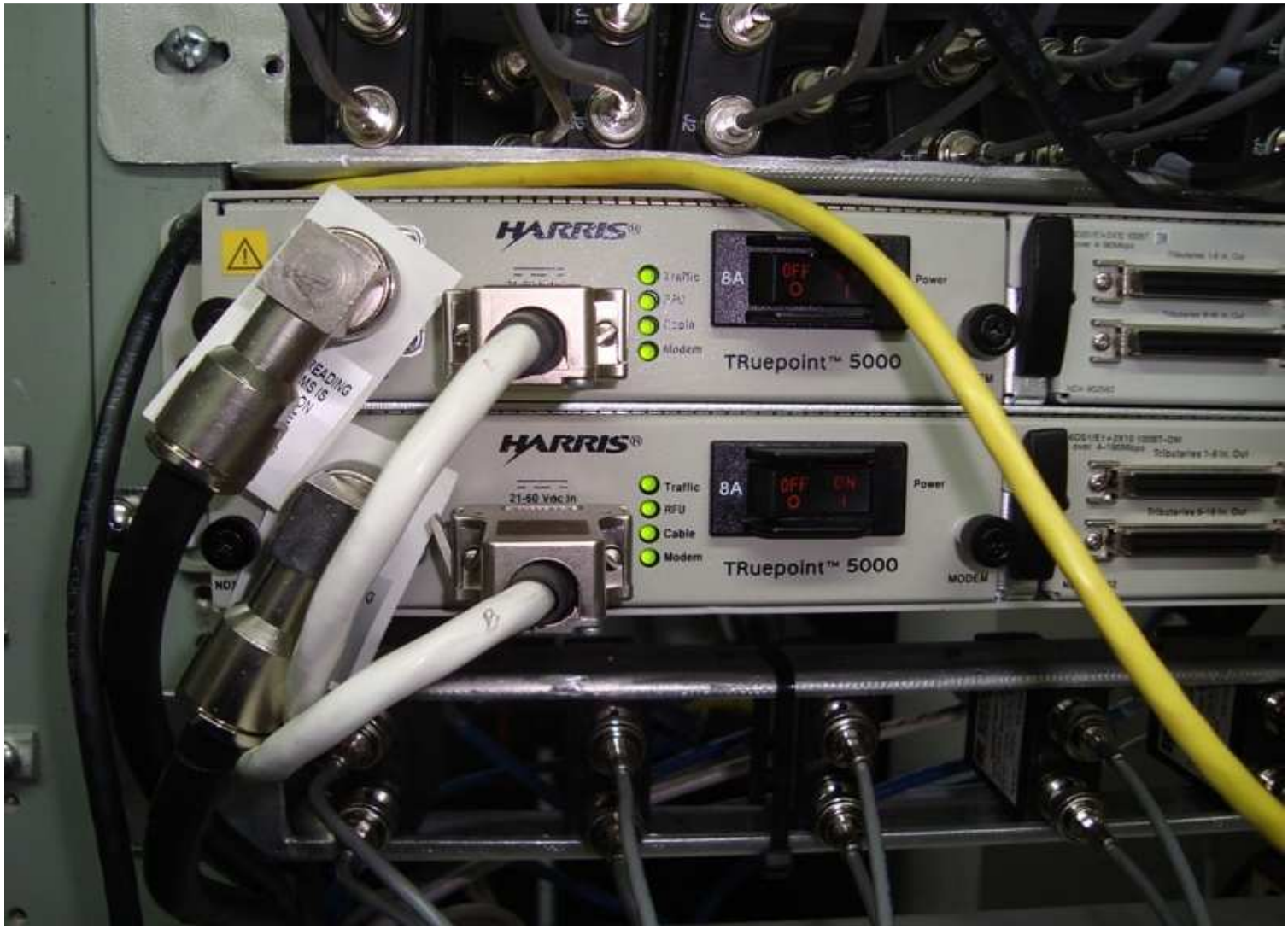
ANEXOS



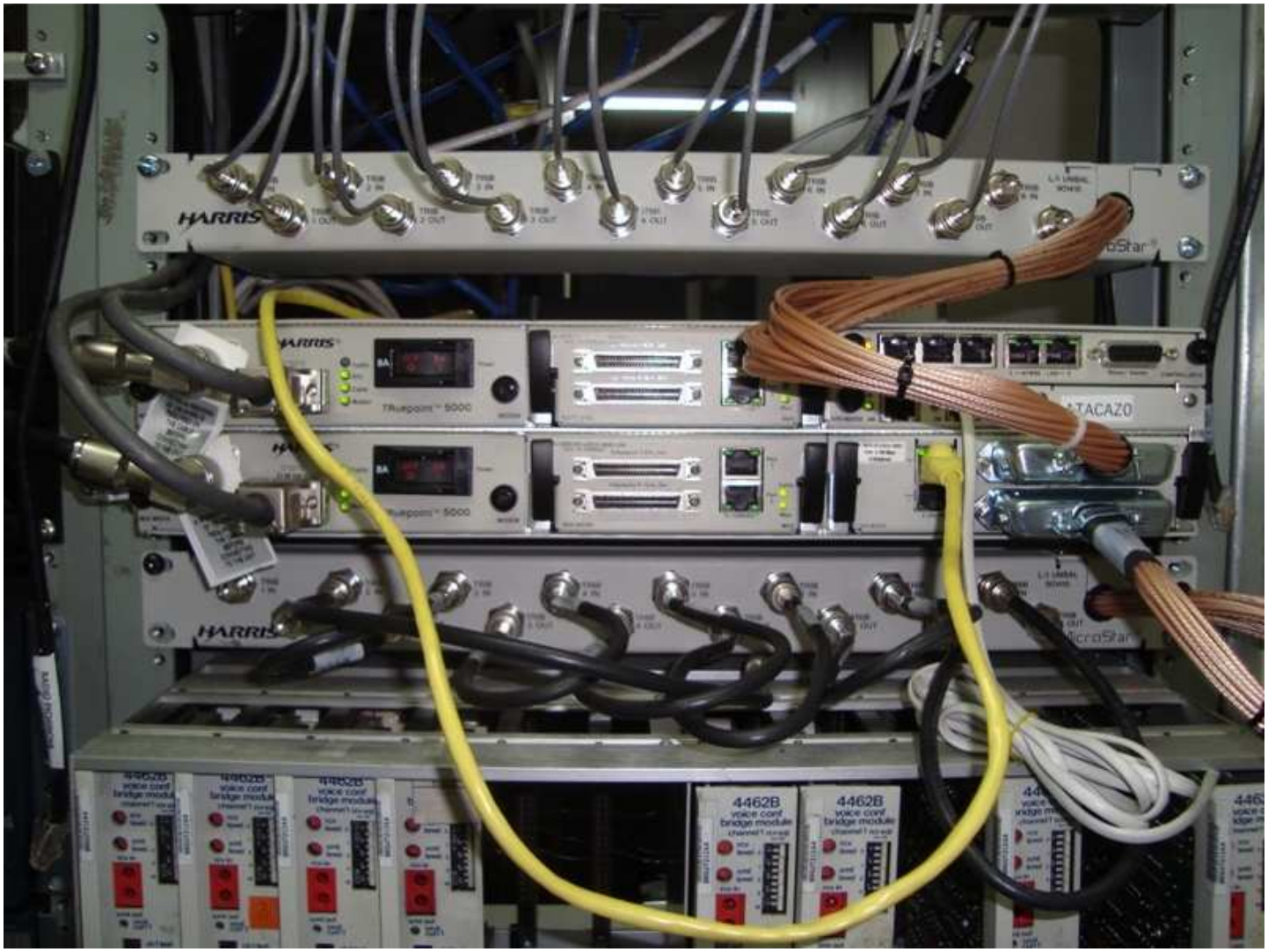
ANEXOS 1 RED WAN DE PETROCOMERCIAL



ANEXOS 2 DIAGRAMA DE ENLACES MICROONDA DE PETROCOMERCIAL



ANEXOS 3 EQUIPOS HARRIS INSTALADOS EN PETROCOMERCIAL



ANEXOS 4 EQUIPOS HARRIS INSTALADOS EN PETROCOMERCIAL 2

ANEXO 5

CONFIGURACIÓN DE EQUIPOS

CONFIGURACIÓN SWITCH PICHINCHA

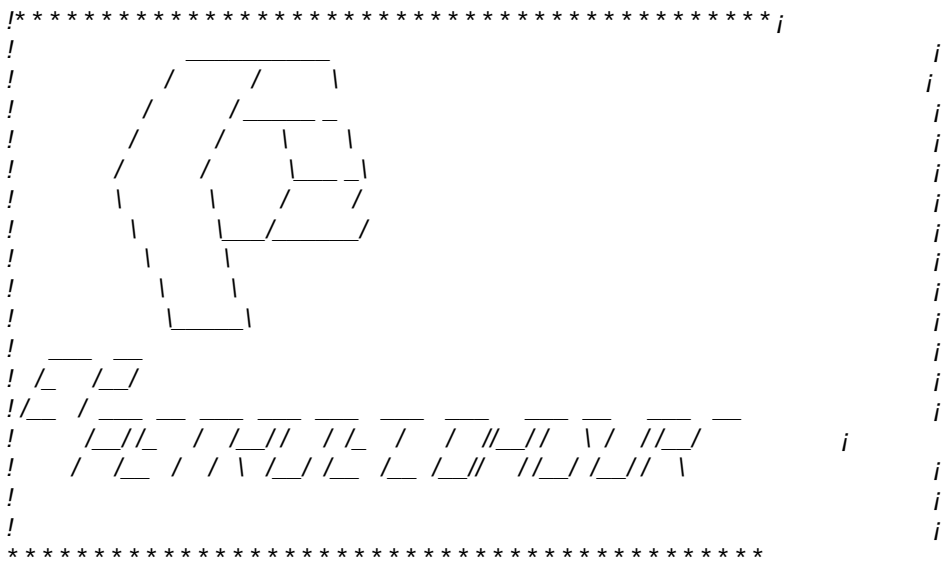
```
Current configuration : 6719 bytes
!
! Last configuration change at 02:49:46 UTC Sat Jan 1 2011 by usertics
! NVRAM config last updated at 02:54:17 UTC Sat Jan 1 2011 by usertics
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW_PICHINCHA
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$tt5g$EskihdUahMFJFNDaFck.f/
!
username usertics privilege 15 secret 5 $1$JAxI$NkZJLixBB3EQq.FeLAGRX.
no aaa new-model
system mtu routing 1500
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name SW_PICHINCHA.pco.com
!
key chain PETROEIGRP
 key 1
   key-string petro
!
archive
```

```
log config
hidekeys
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
ip ssh time-out 30
ip ssh version 2
!
interface FastEthernet0/1
 description ENLACE A ROUTER_ROCIO GI0/1
 no switchport
 ip address 172.20.35.13 255.255.255.252
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
!
interface FastEthernet0/2
 description ENLACE A ROUTER_BEATERIO GI0/0
 no switchport
 ip address 172.20.35.1 255.255.255.248
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
```

```
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
```

```
!
interface Vlan1
 no ip address
!
router eigrp 100
 no auto-summary
 network 172.20.0.0
!
ip classless
no ip http server
no ip http secure-server
!
logging trap errors
logging 172.20.64.77
no cdp run
snmp-server group petrogroup v3 priv read petroview notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF7F
snmp-server view petroview mib-2 included
snmp-server view petroview system included
snmp-server view petroview cisco included
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps transceiver all
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
```

```
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps vtp
 snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps bgp
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps mvpn
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 172.20.64.77 version 3 priv petroadmin
!
control-plane
!
banner motd ^C
```




```
!
line con 0
 login local
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

CONFIGURACIÓN ROUTER BEATERIO

```
Current configuration : 7907 bytes
!
! Last configuration change at 02:37:32 UTC Sat Jan 1 2011 by usertics
! NVRAM config last updated at 02:43:02 UTC Sat Jan 1 2011 by usertics
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_BEATERIO
!
boot-start-marker
boot-end-marker
!
security passwords min-length 8
enable secret 5 $1$BUol$efPDi8NERC1AXs9bZRuVE/
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 172.20.129.1 172.20.129.25
!
ip dhcp pool Beaterio_Lan
   network 172.20.129.0 255.255.255.0
   default-router 172.20.129.14
!
no ip bootp server
no ip domain lookup
ip domain name ROUTER_BEATERIO
!
multilink bundle-name authenticated
!
key chain PETROEIGRP
 key 1
   key-string petro
!
!
voice class codec 100
 codec preference 1 g729r8
 codec preference 2 g711ulaw
```

```
!
!
username usertics privilege 15 secret 5 $1$QeJ8$rsgVPXOkCcWvvV5kgqCv3.
archive
 log config
  hidekeys
!
!
ip ssh time-out 30
ip ssh version 2
!
!
interface FastEthernet0/0
 no ip address
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description ENLACE A SW_172.20.129.65
 no ip address
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 description LAN_BEA
 encapsulation dot1Q 1 native
 ip address 172.20.129.14 255.255.255.0
!
interface FastEthernet0/1.3
 description LAN_BEA_TELEFONIA
 encapsulation dot1Q 3
 ip address 172.21.129.4 255.255.255.128
```

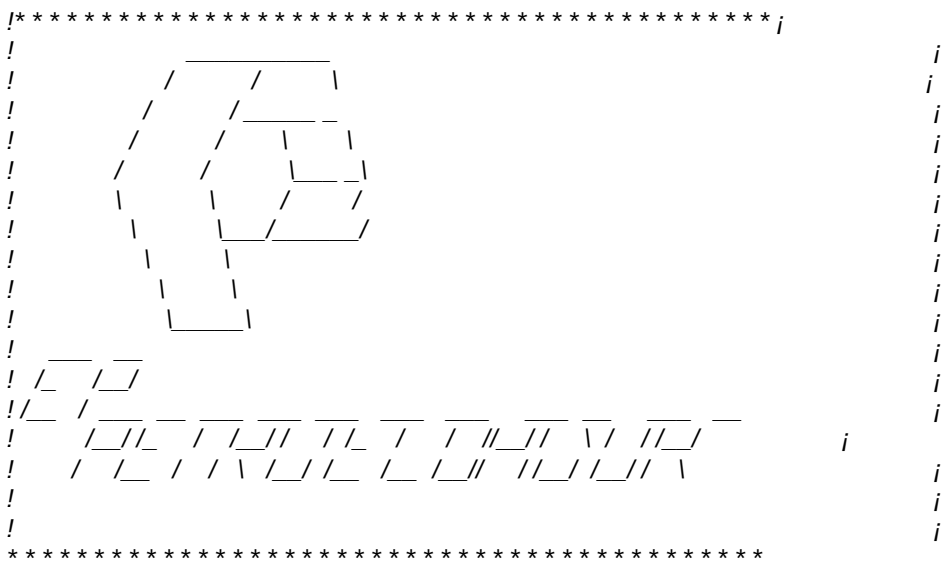
```
!
interface FastEthernet1/0
 description ENLACE A SW_PICHINCHA G0/1
 ip address 172.20.35.2 255.255.255.248
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
 duplex auto
 speed auto
!
router eigrp 100
 network 172.20.0.0
 network 172.21.0.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging trap errors
logging 172.20.64.77
snmp-server group petrogroup v3 priv read petroview notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF7F
snmp-server view petroview mib-2 included
snmp-server view petroview system included
snmp-server view petroview cisco included
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps xgcp
snmp-server enable traps flash insertion removal
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
```

snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bgp
snmp-server enable traps bstun
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps dial
snmp-server enable traps dlsw
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmobile
snmp-server enable traps ipmulticast
snmp-server enable traps mpls ldp
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls vpn
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit

snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps stun
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vsimaster
snmp-server enable traps vtp
snmp-server enable traps pw vc
snmp-server enable traps director server-up server-down
snmp-server enable traps firewall serverstatus
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps rf
snmp-server enable traps ccme
snmp-server enable traps srst
snmp-server enable traps voice
snmp-server enable traps dnis

```
snmp-server host 172.20.64.77 version 3 priv petroadmin
no cdp run
!
!
control-plane
!
!
dial-peer voice 100 voip
 destination-pattern 100.
 voice-class codec 100
 session target ipv4:172.20.64.14
 dtmf-relay h245-alphanumeric
!
dial-peer voice 200 voip
 destination-pattern 2.....
 voice-class codec 100
 session target ipv4:172.20.64.14
 dtmf-relay h245-signal
!
!
telephony-service
 max-ephones 192
 max-dn 500
 ip source-address 172.21.129.4 port 2000
 max-conferences 8 gain -6
 transfer-system full-consult
!
!
ephone-dn  1  dual-line
 number 2001
 label David
 name David
!
!
ephone  1
 device-security-mode none
 mac-address 0003.2552.CBB2
```

```
 type CIPC
 button  1:1
!
!
banner motd ^C
```




```
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input ssh
!
end
```

CONFIGURACIÓN ROUTER MATRIZ

```
Building configuration...

Current configuration : 11390 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_ROCIO
!
boot-start-marker
boot-end-marker
!
security passwords min-length 8
logging message-counter syslog
enable secret 5 $1$KC6b$ErJ/pzdLJlcUuVYhxFkEi/
!
no aaa new-model
memory-size iomem 5
!
dot11 syslog
ip source-route
ip dhcp excluded-address 172.21.64.1 172.21.64.15
!
ip dhcp pool VLAN_VOZ
   network 172.21.64.0 255.255.255.0
   default-router 172.21.64.4
   option 150 ip 172.21.64.4
!
!
ip cef
!
!
no ip bootp server
```

```
no ip domain lookup
ip domain name ROUTER_ROCIO.pco.com
!
no ipv6 cef
multilink bundle-name authenticated
!
!
!
trunk group  PSTN
 hunt-scheme sequential
!
!
key chain PETROEIGRP
 key 1
   key-string petro
voice-card 0
 dspfarm
 dsp services dspfarm
!
!
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 sip
  registrar server
!
!
voice class codec 100
 codec preference 1 g729r8
 codec preference 2 g711ulaw
 codec preference 3 g711alaw
!
voice register global
 mode cme
```

```
 source-address 172.21.64.4 port 5060
 max-dn 500
 max-pool 185
 authenticate register
 voicemail 1003
 create profile sync 0031556441720142
!
voice register dn  1
 number 1002
 call-forward b2bua mailbox 1003
 call-forward b2bua noan 1003 timeout 15
 name Prueba
 label Prueba
!
voice register pool  1
 id mac 0000.0000.0000
 number 1 dn 1
 dtmf-relay sip-notify
 username 1002 password petrosip
 codec g711ulaw
!
username usertics privilege 15 secret 5 $1$QaA7$/DIc5WhgFMi0ankRr9B4C/
archive
 log config
  hidekeys
!
ip ssh time-out 30
ip ssh version 2
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
interface Service-Engine0/0
```

```
 description CUE
 ip unnumbered Vlan1001
 service-module ip address 172.21.64.2 255.255.255.0
 service-module ip default-gateway 172.21.64.4
!
interface GigabitEthernet0/1
 description ENLACE A SW_PICHINCHA-GI0/5
 ip address 172.20.35.14 255.255.255.252
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
 duplex auto
 speed auto
 media-type rj45
!
interface FastEthernet0/1/0
 switchport access vlan 1001
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
 switchport access vlan 1001
!
interface FastEthernet0/1/4
!
interface FastEthernet0/1/5
!
interface FastEthernet0/1/6
!
interface FastEthernet0/1/7
!
interface FastEthernet0/1/8
!
interface Vlan1
 description LAN_UIO
 ip address 172.20.64.14 255.255.248.0
```

```
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
!
interface Vlan1001
 description LAN_UIO_TELEFONIA
 ip address 172.21.64.4 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 PETROEIGRP
!
router eigrp 100
 network 172.20.0.0
 network 172.21.0.0
 no auto-summary
!
ip forward-protocol nd
ip route 172.21.64.2 255.255.255.255 Service-Engine0/0
!
!
no ip http server
no ip http secure-server
!
logging trap errors
logging 172.20.64.77
snmp-server group petrogroup v3 priv read petroview notify
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFF7F
snmp-server view petroview mib-2 included
snmp-server view petroview system included
snmp-server view petroview cisco included
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps xgcp
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server enable traps authenticate-fail
```

snmp-server enable traps dot11-qos
snmp-server enable traps switch-over
snmp-server enable traps rogue-ap
snmp-server enable traps wlan-wep
snmp-server enable traps flash insertion removal change
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps license
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bgp
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp

snmp-server enable traps ipmulticast
snmp-server enable traps mpls ldp
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps pw vc
snmp-server enable traps firewall serverstatus
snmp-server enable traps ipmobile
snmp-server enable traps rf
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach

```
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ccme
snmp-server enable traps srst
snmp-server enable traps mpls vpn
snmp-server enable traps voice
snmp-server enable traps dnis
snmp-server host 172.20.64.77 version 3 priv petroadmin
!
control-plane
!
voice-port 0/2/0
 trunk-group PSTN
 connection plar 1001
!
voice-port 0/2/1
!
voice-port 0/2/2
!
voice-port 0/2/3
!
voice-port 0/3/0
!
voice-port 0/3/1
!
voice-port 0/3/2
!
voice-port 0/3/3
!
sccp local Vlan1001
sccp ccm 172.21.64.4 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register mtpfcfbfb357d40
```

```
!
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 maximum sessions 12
 associate application SCCP
!
dial-peer cor custom
 name local
 name regional
!
!
 dial-peer cor list llamadaslocales
 member local
!
dial-peer cor list llamadasregionales
 member local
 member regional
!
!
dial-peer voice 100 voip
 destination-pattern 200.
 voice-class codec 100
 session target ipv4:172.21.129.4
 dtmf-relay h245-alphanumeric
!
dial-peer voice 200 pots
 trunkgroup PSTN
 corlist outgoing llamadaslocales
 destination-pattern 2.....
 forward-digits 7
!
dial-peer voice 201 pots
 trunkgroup PSTN
```

```
 corlist outgoing llamadasregionales
 destination-pattern 0.......
 forward-digits 9
!
dial-peer voice 203 voip
 description **CUE autoattendant**
 destination-pattern 1004
 b2bua
 session protocol sipv2
 session target ipv4:172.21.64.4
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
dial-peer voice 204 voip
 description **voicemail**
 destination-pattern 1003
 session protocol sipv2
 session target ipv4:172.21.64.2
 dtmf-relay sip-notify
 codec g711ulaw
 no vad
!
telephony-service
 max-ephones 185
 max-dn 500
 ip source-address 172.21.64.4 port 2000
 max-redirect 10
 auto assign 1 to 5
 user-locale ES
 user-locale 1 ES
 user-locale 2 ES
 user-locale 3 ES
 user-locale 4 ES
 network-locale ES
 network-locale 1 ES
 network-locale 2 ES
```

```
 network-locale 3 ES
 network-locale 4 ES
 voicemail 1003
 max-conferences 12 gain -6
 transfer-system full-consult
 create cnf-files version-stamp 7960 Jan 01 2011 00:15:29
!
!
ephone-dn  1  dual-line
 number 1001
 label USER1
 name USER1
 call-forward busy 1003
 call-forward noan 1003 timeout 20
 corlist incoming llamadaslocales
!
!
ephone-dn  2
!
!
ephone-dn  5  dual-line
 number 1005
 label USER2
 name USER2
 call-forward busy 1003
 call-forward noan 1003 timeout 15
 corlist incoming llamadasregionales
!
!
ephone  1
 device-security-mode none
 video
 mac-address 0007.0E56.F5A2
 type 7965
 button  1:1
!
!
```

```
!
ephone  5
 device-security-mode none
 mac-address 001E.7AC5.361C
 type 7911
 button  1:5
!
!
banner motd ^CC

!*********************************************************************************************!
!                 ____________                                                                i
!              /       /       \                                                              i
!            /       /_______ _                                                              i
!           /       /      \     \                                                           i
!          /       /        \___ _\                                                          i
!          \        \       /     /                                                          i
!           \        \____/_______/                                                          i
!            \       \                                                                       i
!             \       \                                                                      i
!              \_____\                                                                       i
!   ___   __                                                                                 i
!  /_    /__/                                                                                i
! /__   / ___  __  ___  ___  ___   ___   ___    ___  __    ___  __                           i
!       /__/ /_    /   /__/ /    / /_   /     /   //__/ /    \ /   / /__/                  i
!      /    /__   /   /  \  /__/ /__   /__  /__//    //__/ /__/ /   \                       i
!                                                                                            i
!                                                                                            i

**********************************************************************************************
                        ACCESO RESTRINGIDO   ^C
!
line con 0
 login local
line aux 0
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 line vty 0 4
 login local
```

```
 transport input ssh
!
scheduler allocate 20000 1000
end
```

CONFIGURACIÓN CISCO UNITY EXPRESS DE ROUTER MATRIZ

```
clock timezone America/Guayaquil

hostname se-172-20-20-4

line console

system language preferred "es_CO"
software download server url "ftp://127.0.0.1/ftp" credentials hidden
"6u/dKTN/hsEuSAEfw40XlF2eFHnZfyUTSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk
2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

license agent max-sessions 9

privilege ViewRealTimeReports create
privilege vm-imap create
privilege ManagePublicList create
privilege manage-passwords create
privilege ManagePrompts create
privilege broadcast create
privilege ViewPrivateList create
privilege manage-users create
privilege ViewHistoricalReports create
privilege local-broadcast create

groupname BROAD create
groupname Broadcasters create

username Prueba create
username USER1 create
username USER2 create
```

username admin create

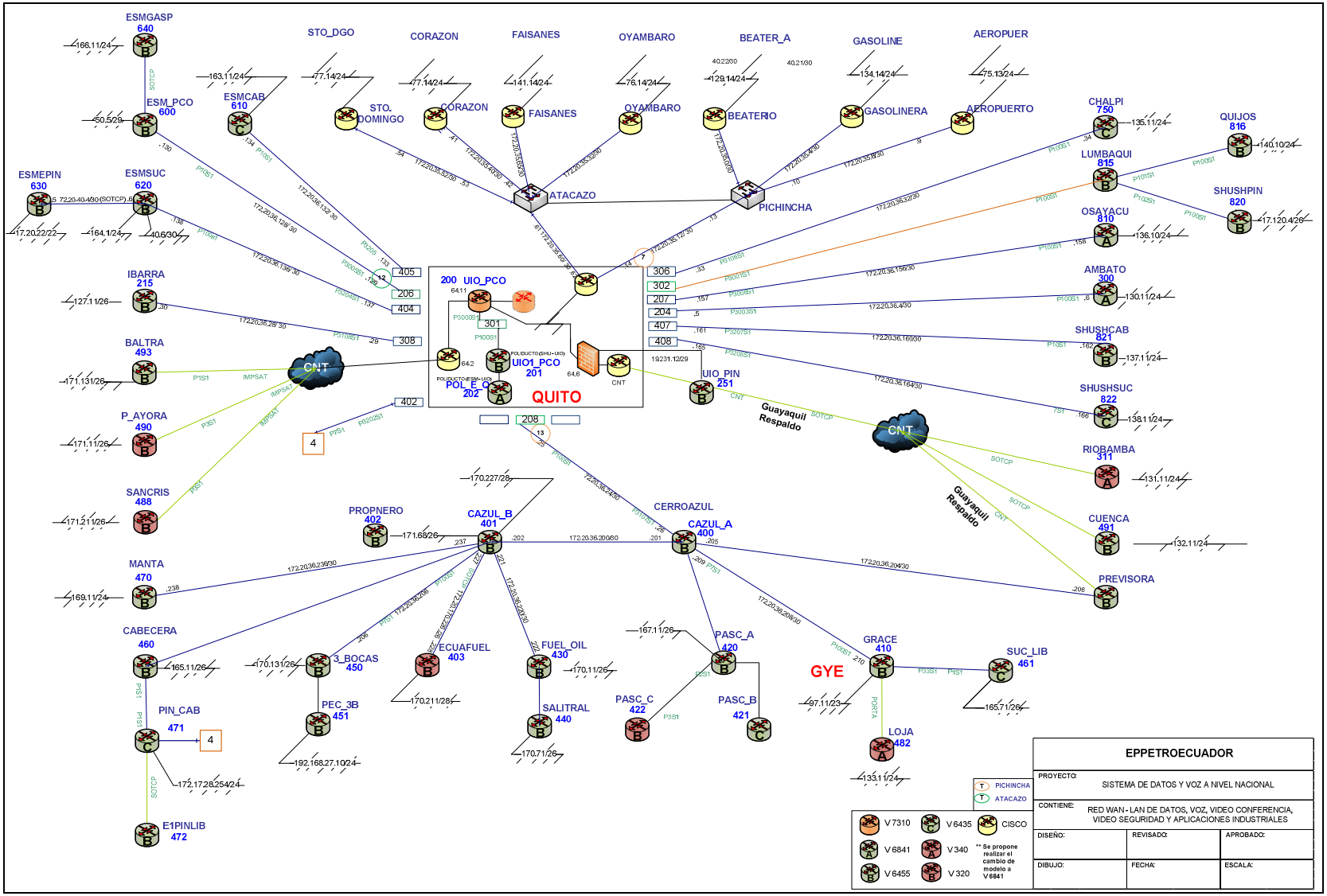
privilege ViewRealTimeReports description "Privilege to view realtime reports"
privilege vm-imap description "Privilege to manage personal voicemail via IMAP client"
privilege ManagePublicList description "Privilege to manage public lists"
privilege manage-passwords description "Privilege to reset user passwords"
privilege ManagePrompts description "Privilege to create, modify, or delete system prompts"
privilege broadcast description "Privilege to send local or remote broadcast messages"
privilege ViewPrivateList description "Privilege to view private list"
privilege manage-users description "Privilege to create, modify, and delete users and groups"
privilege ViewHistoricalReports description "Privilege to view historical reports"
privilege local-broadcast description "Privilege to send local broadcast messages"
privilege ViewRealTimeReports operation report.realtime
privilege vm-imap operation voicemail.imap.user
privilege ManagePublicList operation system.debug
privilege ManagePublicList operation voicemail.lists.public
privilege manage-passwords operation user.password
privilege manage-passwords operation user.pin
privilege manage-passwords operation system.debug
privilege ManagePrompts operation system.debug
privilege ManagePrompts operation prompt.modify
privilege broadcast operation broadcast.local
privilege broadcast operation broadcast.remote
privilege broadcast operation system.debug
privilege ViewPrivateList operation voicemail.lists.private.view
privilege manage-users operation user.mailbox
privilege manage-users operation user.password
privilege manage-users operation user.notification
privilege manage-users operation user.pin
privilege manage-users operation group.configuration
privilege manage-users operation user.configuration
privilege manage-users operation system.debug
privilege manage-users operation user.remote
privilege ViewHistoricalReports operation report.historical.view
privilege local-broadcast operation broadcast.local
privilege local-broadcast operation system.debug

```
groupname Administrators member admin
groupname Broadcasters privilege broadcast

username Prueba phonenumber "1002"
username USER1 phonenumber "1001"
username USER2 phonenumber "1005"

restriction msg-notification create
restriction msg-notification min-digits 1
restriction msg-notification max-digits 30
restriction msg-notification dial-string preference 1 pattern * allowed

backup server url "ftp://127.0.0.1/ftp" credentials hidden
"EWlTygcMhYmjazXhE/VNXHCkplVV4KjescbDaLa4fl4WLSPFvv1rWUnfGWTYHfmPSd8ZZNgd+Y9J3
xlk2B35j0nfGWTYHfmPSd8ZZNgd+Y9J3xlk2B35j0nfGWTYHfmP"

calendar biz-schedule systemschedule
 open day 1 from 00:00 to 24:00
 open day 2 from 00:00 to 24:00
 open day 3 from 00:00 to 24:00
 open day 4 from 00:00 to 24:00
 open day 5 from 00:00 to 24:00
 open day 6 from 00:00 to 24:00
 open day 7 from 00:00 to 24:00
 end schedule

ccn application autoattendant aa
 description "autoattendant"
 enabled
 maxsessions 6
 script "aa.aef"
 parameter "busClosedPrompt" "AABusinessClosed.wav"
 parameter "holidayPrompt" "AAHolidayPrompt.wav"
 parameter "welcomePrompt" "AAWelcome.wav"
 parameter "disconnectAfterMenu" "false"
 parameter "dialByFirstName" "false"
 parameter "allowExternalTransfers" "false"
```

```
 parameter "MaxRetry" "3"
 parameter "dialByExtnAnytime" "false"
 parameter "busOpenPrompt" "AABusinessOpen.wav"
 parameter "businessSchedule" "systemschedule"
 parameter "dialByExtnAnytimeInputLength" "4"
 parameter "operExtn" "0"
 end application

ccn application ciscomwiapplication aa
 description "ciscomwiapplication"
 enabled
 maxsessions 6
 script "setmwi.aef"
 parameter "CallControlGroupID" "0"
 parameter "strMWI_OFF_DN" "8001"
 parameter "strMWI_ON_DN" "8000"
 end application

ccn application msgnotification aa
 description "msgnotification"
 enabled
 maxsessions 6
 script "msgnotify.aef"
 parameter "logoutUri" "http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
 parameter "DelayBeforeSendDTMF" "1"
 end application

ccn application promptmgmt aa
 description "promptmgmt"
 enabled
 maxsessions 1
 script "promptmgmt.aef"
 end application

ccn application voicemail aa
 description "Cisco voicemail"
 enabled
```

```
 maxsessions 4
 script "voicebrowser.aef"
 parameter "logoutUri" "http://localhost/voicemail/vxmlscripts/mbxLogout.jsp"
 parameter "uri" "http://localhost/voicemail/vxmlscripts/login.vxml"
 end application

ccn engine
 end engine

ccn reporting historical
 database local
 description "se-172-20-20-4"
 end reporting

ccn subsystem jtapi
 ccm-manager address 0.0.0.0
 end subsystem

ccn subsystem sip
 gateway address "172.21.64.2"
 mwi sip unsolicited
 end subsystem

ccn trigger http urlname msgnotifytrg
 application "msgnotification"
 enabled
 maxsessions 2
 end trigger

ccn trigger http urlname mwiapp
 application "ciscomwiapplication"
 enabled
 maxsessions 1
 end trigger

ccn trigger sip phonenumber 1003
 application "voicemail"
```

```
 enabled
 maxsessions 4
 end trigger

ccn trigger sip phonenumber 1004
 application "autoattendant"
 enabled
 maxsessions 4
 end trigger

service voiceview
 enable
 end voiceview

voicemail default mailboxsize 2000
voicemail broadcast recording time 300
voicemail default messagesize 120
voicemail notification restriction msg-notification
voicemail operator telephone 1003
voicemail capacity time 600
voicemail mailbox owner "Prueba" size 300
 description "voicemail Prueba"
 expiration time 10
 end mailbox

voicemail mailbox owner "USER1" size 300
 description "User1 mail box"
 expiration time 10
 login pinless any-phone-number
 end mailbox

voicemail mailbox owner "USER2" size 300
 description "Voice mail User2"
 expiration time 10
 end mailbox
end
```



ANEXO 6 TOPOLOGIA IMPLEMENTADA EN LA RED WAN DE PETROCOMERCIAL