ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE
INGENIERÍA

IMPLEMENTACIÓN DE UN SISTEMA DE MEDICIÓN Y MONITOREO DE TRÁFICO IP BASADO EN SOFTWARE LIBRE, CON EL FIN DE REALIZAR UNA PLANEACIÓN ADECUADA DE LAS CAPACIDADES DE LA RED WAN DE LA EMPRESA ALIANZANET S.A.

JORGE ALBERTO TAPIA CABRERA

Sangolquí - Ecuador
2009

CERTIFICACION

En calidad de Director y Codirector del presente proyecto de tesis, “Implementación de un sistema de medición y monitoreo de tráfico IP basado en software libre, con el fin de realizar una planeación adecuada de las capacidades de la red WAN de la empresa ALIANZANET S.A.”; realizado por el Sr. Jorge Alberto Tapia Cabrera, certificamos la realización del proyecto bajo nuestra dirección y tutoría

_____
Ing. Carlos G. Romero
DIRECTOR

_____
Ing. Alejandro Castro C.
CODIRECTOR

RESUMEN

El presente proyecto basa su desarrollo en la implementación de 3 herramientas, implementadas bajo GNU/Linux, para la medición y monitoreo del tráfico, que circula sobre la red WAN del ISP.

Dichas herramientas Nagios, MRTG y NTOP, estarán encargadas de la administración de la red, medición del consumo de los clientes, y caracterización del tráfico, respectivamente, de la red de la empresa, el resultado y la interacción de dichas herramientas entre sí, han contribuido entregando sus resultados, para el planteamiento de la solución adecuada a los problemas presentes, en la red de la empresa.

Estos denominados problemas, recaen en tres aspectos esenciales:

- Sobredimensionamiento de las capacidades de la red WAN de la empresa
- Erróneos o casi nulos criterios del monitoreo y planificación del crecimiento de la red.
- Total y completa falta de criterios de seguridad y caracterización, en cuanto al tráfico real que circula dentro de la red.

Luego del análisis de los resultados, se llega a plantear una solución a estos inconvenientes, cambiando completamente la topología de la red, a una estructura más ordenada, corrigiendo los puntos de saturación existentes dentro de la misma, implementando criterio de seguridad y control del tráfico generado por los clientes, y sentando la base de un sistema de monitoreo, automático, eficaz y proactivo.

DEDICATORIA

Este proyecto va dedicado a mi padre, sin cuyo ejemplo de lucha y carácter, esta etapa de mi vida no hubiera llegado a su feliz término, se lo dedico además a todas aquellas personas que creyeron en mí, y apoyaron las dediciones tomadas por mi persona, durante la realización del mismo.

AGRADECIMIENTO

Agradezco a mi madre y a mi hermano, por la paciencia y la comprensión que supieron demostrar a lo largo de toda mi carrera, un agradecimiento especial al grupo humano de la empresa Alianzanet S.A., en la persona del jefe de departamento técnico, por su apoyo y la apertura brindada para la realización de este proyecto de tesis.

PROLOGO

Un buen sistema de monitoreo de los enlaces dentro del área de cobertura de la red, faculta al proveedor ISP, para brindar el servicio que ofrece con eficacia, versatilidad y profesionalismo.

La internet basa su funcionamiento en el protocolo TCP/IP, mismo protocolo que posee innumerables ventajas, una de las principales, es que su control y monitoreo puede ser realizado de múltiples maneras, utilizando diferentes herramientas que permiten conocer el estado de las redes involucradas en el tráfico de datos:

- Flujo de protocolos
- Estabilidad del enlace
- Puntos de Saturación
- Consumo interno y externo

En estos puntos fundamentales recae la verdadera importancia de un sistema de monitoreo con el fin de controlar de manera total y personalizada el servicio brindado.

Se procederá en primera instancia a realizar un análisis de la red WAN de ALIANZANET S.A., tomando en cuenta su ingeniería actual. Para esto se realizará un análisis, sobre las ventajas y desventajas de algunos de los sistemas de monitoreo y control de tráfico más utilizados, con el fin de determinar su adaptabilidad a la ingeniería actual de la red WAN de ALIANZANET S.A. Posterior a esto se instalaran las herramienta en un servidor, configurando las herramientas seleccionadas, integrándolas a la red WAN de ALIANZANET S.A. Luego de recogidos los resultados, se procederá a plantear la solución adecuada de la red WAN de ALIANZANET S.A., y una proyección sobre las posibles mejoras a implementarse dentro de la misma.

INDICE DE CONTENIDOS

CAPITULO 2

2. LA RED DE ALIANZANET

INDICE DE TABLAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

CAPITULO 5

INDICE DE FIGURAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 5

INDICE DE HOJAS TECNICAS

CAPITULO 1

ESTRUCTURA DE UN ISP

1.1. INTRODUCCION

El servicio principal que brinda un ISP (*Internet Service Provider*) es el de proveer, a clientes particulares y corporativos, públicos y privados, de un enlace de datos para comunicarse y acceder a información a nivel mundial. Cuando se implementan redes de área extendida WAN, como la implementada en este caso por un ISP, es normal en muchos de los casos experimentar tiempos de respuesta altos o "pobres" dentro de la red, sea en usuarios específicos o en grupos enteros pertenecientes a una u otra trocal, este tipo de problemas suelen producirse por diferentes factores, entre los cuales se encuentra el crecimiento acelerado o anárquico de la red, este crecimiento debe ser planificado, con el fin de que no se den los problemas antes mencionados.

Estos inconvenientes hacen que se vea afectado el desempeño de la red, causando pérdidas inmensas que se traducen más en el ámbito económico y productivo, no solo de la empresa, sino de sus clientes. Es por esta razón que un buen sistema de monitoreo se convierte en una herramienta poderosa al momento de diagnosticar y prevenir este tipo de inconvenientes.

Cabe recalcar que las herramientas de *hardware* y *software* implementadas en este proyecto, son precisamente eso, herramientas, que utilizadas de la manera correcta, influirán en la planificación y correcta administración de la red WAN de la empresa.

1.2. REDES INVOLUCRADAS EN EL PROYECTO

La red [1]WAN de un ISP es aquella donde se sustenta todo el trafico de sus clientes de vista macro, debido al acelerado crecimiento en tecnologías de la información y telecomunicaciones, tecnologías que se implementaron para la conectividad a nivel local, regional, nacional e internacional, van que dando atrás, para dar paso a nuevas y mejores tecnologías, sin embargo este cambio en la ingeniería de redes, se da de manera paulatina, existiendo siempre un tema de compatibilidad.

Esta compatibilidad produce que, en una misma red, se complementen y convivan, diferentes tipos de tecnología, haciendo la administración de la red un tema bastante diverso, ya que el comportamiento y el tratamiento que se le da a uno u otro sistema son, en la forma más no en el fondo, diferentes.

1.2.1. Red *Frame Relay*

Frame Relay es una técnica de comunicación mediante retransmisión de tramas, para redes de circuito virtual, introducida por la [2]UIT a partir de 1988, su principal utilidad es la creación sencilla de circuitos virtuales punto-a-punto o punto-a-multipunto, manejando velocidades de hasta 2Mbps.

En este tipo de circuitos, los usuarios o puntos de la red, experimentan una comunicación directa entre los dos extremos, aunque las técnicas de conmutación de paquetes no están diseñadas para trabajar con conexiones físicas directas entre dos puntos de la misma. Frente a soluciones de circuitos físicos dedicados, *Frame Relay* es una opción más económica haciendo un uso más eficiente del ancho de banda, puesto que varios circuitos virtuales pueden compartir una misma línea de datos.

1.2.1.1. Funcionamiento de *Frame Relay*.

Como se dijo anteriormente, la red basa su función en el uso de circuitos virtuales, un circuito virtual (VC por sus siglas en inglés) es un sistema de comunicación por el cual los datos de un usuario origen pueden ser transmitidos a otro usuario destino a través de más de un circuito de comunicaciones real durante un cierto periodo de tiempo, pero en el que la conmutación es transparente para el usuario. Un ejemplo de protocolo de circuito virtual

1 WAN: Red de area extendida o *Wide Area Network*
2 UIT: Unión Internacional de Telecomunicaciones

es el ampliamente utilizado TCP (Protocolo de Control de Transmisión). Un *Data Link Connection Identifier* (DLCI) es el identificador de canal del circuito establecido en *Frame Relay*. Este identificador se aloja en la trama e indica el camino a seguir por los datos, es decir, el circuito virtual establecido.

El DLCI puede valer normalmente entre 0 y 1023 (10 bits), los valores del 0 al 15 y del 992 en adelante están reservados para funciones especiales, un DLCI tiene significado local, es decir, en el circuito virtual cada extremo puede tener un identificador de circuito diferente para identificar el mismo circuito.

El establecimiento de un VC es una forma de comunicación mediante conmutación de paquetes, en la cual la información o datos son empaquetados en bloques que tienen un tamaño variable a los que se les denomina paquetes. El tamaño de los bloques lo estipula la red. Los paquetes suelen incluir cabeceras con información de control. Estos se transmiten a la red, la cual se encarga de su encaminamiento hasta el destino final. Cuando un paquete se encuentra con un nodo intermedio, el nodo almacena temporalmente la información y encamina los paquetes a otro nodo según las cabeceras de control. Es importante saber que en este caso los nodos no necesitan tomar decisiones de ruteo, ya que la dirección a seguir viene especificada en el propio paquete.

Las dos formas de ruteo de paquetes son: datagramas y circuitos virtuales. Este artículo está centrado en el segundo.

En los circuitos virtuales, al comienzo de la sesión se establece una ruta única entre las ETD (entidades terminales de datos) o los host extremos. A partir de aquí, todos los paquetes enviados entre estas entidades seguirán la misma ruta.

Dentro la red *Frame Relay*, las conexiones o circuitos virtuales pueden ser de dos tipos:

a) Permanentes, mediante un PVC (*Permanent Virtual Circuit*), los cuales proporcionan un circuito dedicado entre dos puntos. Un PVC es un circuito virtual establecido para uso repetido por parte de los mismos equipos de transmisión. Los

Circuitos permanentes eliminan la necesidad de configuración y terminación repetitivas para cada llamada. Es decir se puede usar sin tener que pasar por la fase de establecer ni liberar las conexiones. El circuito está reservado a una serie de usuarios y nadie más puede hacer uso de él. Una característica especial que en el SVC no se daba es que si dos usuarios solicitan una conexión, siempre obtienen la misma ruta.

b) Conmutadas, mediante un SVC (*Switched Virtual Circuit*), estos por lo general se crean por defecto y de forma dinámica para cada llamada o conexión, y se desconectan cuando la sesión o llamada es terminada. Como ejemplo de circuito virtual conmutado se tienen los enlaces [3]ISDN. Se utilizan principalmente en situaciones donde las transmisiones son esporádicas. En terminología [4]ATM esto se conoce como conexión virtual conmutada. Se crea un circuito virtual cuando se necesita y existe sólo durante la duración del intercambio específico.

Por su versatilidad y mejor desempeño, en la mayoría de redes de área metropolitana, se utilizan los circuitos permanentes o PVC, de hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red.

Un ejemplo sencillo de esto sería:

1.- La [5]ETD A solicita el envío de paquetes a la ETD E.

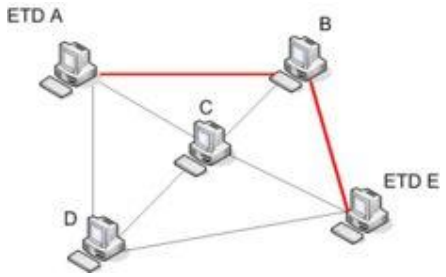


Figura. 1.1 Paso 1 Establecimiento del Circuito Virtual

2.- Cuando la conexión ya está establecida se comienzan a enviar los paquetes de forma ordenada por la ruta uno tras otro.

3 ISDN: Red Digital de Servicios Integrados
4 ATM: Modo de Transmisión Asíncrono
5 ETD : Entidad Terminal de Datos

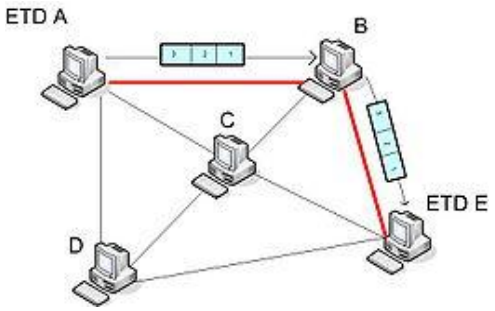


Figura. 1.2 Paso 2 Establecimiento del Circuito Virtual

3.- Cuando la ETD E recibe el último paquete, se libera la conexión, por lo que el circuito virtual deja de existir.

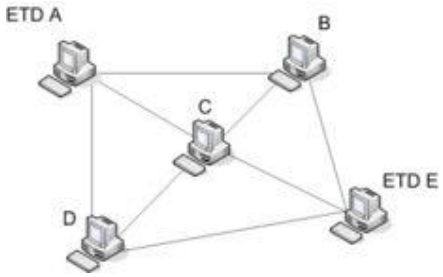


Figura. 1.3 Paso 3 Establecimiento del Circuito Virtual

1.2.1.2 **Estructura de *Frame Relay.***

El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red, puede manejar tanto tráfico de datos como de voz.

Al contratar un servicio Frame Relay, se contrata un ancho de banda determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (*Commited Information Rate*). Esta velocidad, surge de la división de Bc (*Committed Burst*), entre Tc (el intervalo de tiempo). No obstante, una de las características de *Frame Relay* es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, adaptándose muy bien al tráfico en ráfagas, pero en media en el intervalo Tc no deberá superarse la cantidad estipulada Bc

Estos Bc bits, serán enviados de forma transparente. No obstante, cabe la posibilidad de transmitir por encima del CIR contratado, mediante los Be (*Excess Burst*). Estos datos que superan lo contratado, serán enviados en modo [6]*best-effort* o el mejor esfuerzo, activándose el bit DE de estas tramas, con lo que serán las primeras en ser descartadas en caso de congestión en algún nodo.

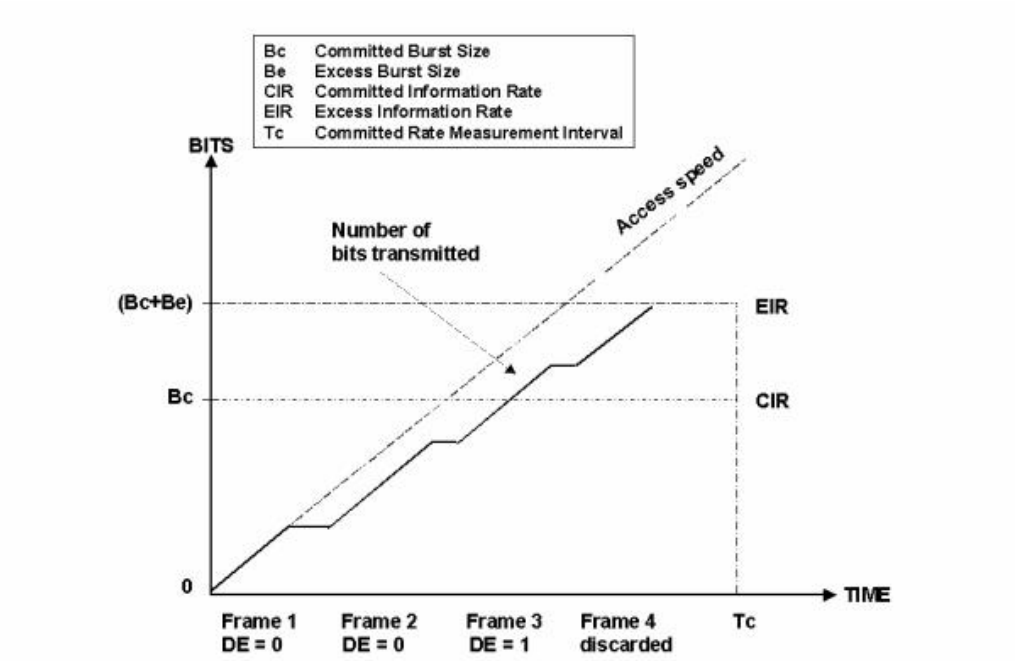


Figura. 1.4 Asignación de velocidad en tramas *Frame Relay*

Como se observa en la Figuera 1.4, las tramas que superen la cantidad de Bc+Be en el intervalo, serán descartadas directamente sin llegar a entrar en la red, sin embargo las que superan la cantidad Bc pero no Bc+Be se marcan como descartables (DE=1) para ser estas las primeras en ser eliminadas en caso de congestión.

Para realizar control de congestión de la red, Frame Relay activa unos bits, que se llaman FECN (*forward explicit congestion notification*), BECN (*backward explicit congestion notification*) y DE (*Discard Eligibility*). Para ello utiliza el protocolo [7]LAPF, un protocolo de nivel de enlace que mejora al protocolo [8]LAPD.

6 *best-effort:* Política implementada para trasmisión de datos sin corrección de errores con el mejo esfuerzo del sistema para evitarlos
7 LAPF: Mejora al procedimiento LAPD para enlces de acceso en ISDN.
8 LAPD: Implementación de *Link Access Pocedure* o Procedimiento para enlaces de acceso en el canal D para ISDN con señalización 7.

FECN se activa, o lo que es lo mismo, se pone en 1, cuando hay congestión en el mismo sentido que va la trama.

BECN se activa cuando hay congestión en el sentido opuesto a la transmisión. DE igual a 1 indica que la trama será descartable en cuanto haya congestión. Se utiliza el llamado Algoritmo del Cubo Agujereado, de forma que se simulan 2 cubos con un agujero en el fondo: Por el primero de ellos pasan las tramas con un tráfico inferior a CIR, el que supera este límite pasa al segundo cubo, por el que pasará el tráfico inferior a CIR+EIR (y que tendrán DE=1). El que supera este segundo cubo es descartado.

En cada nodo hay un gestor de tramas, que decide, en caso de congestión, a quien notificar, si es leve avisa a las estaciones que generan más tráfico, si es severa le avisa a todos. Siguiendo el algoritmo anterior, podríamos descartar en el peor de los casos el tráfico que pasa a través del segundo cubo. Este funcionamiento garantiza que se cumplen las características de la gestión de tráfico.

Por otro lado, no lleva a cabo ningún tipo de control de errores o flujo, ya que delega ese tipo de responsabilidades en capas superiores, obteniendo como resultado una notable reducción del tráfico en la red, aumentando significativamente su rendimiento. Esta delegación de responsabilidades también conlleva otra consecuencia, y es la reducción del tamaño de su cabecera, necesitando de menor tiempo de proceso en los nodos de la red y consiguiendo de nuevo una mayor eficiencia. Esta delegación de control de errores en capas superiores es debido a que *Frame Relay* trabaja bajo redes digitales en las cuales la probabilidad de error es muy baja.

1.2.1.3 **Ventajas y Aplicaciones.**

Las ventajas en la implementación del sistema *Frame Relay* sobre tecnologías antecesoras o contemporáneas como [9]X25, se listan a continuación, tomado en cuenta que es una tecnología que, actualmente es ya obsoleta.

- Reducción de complejidad en la red elecciones virtuales múltiples son capaces de compartir la misma línea de acceso.

9 X25: Red WAN de conmutación de paquetes aprobada por la UIT en 1980 para comunicación entre terminales de distintos fabricantes, se constituye como la primera red de conmutación de paquetes y es la base sobre la cual se implementaron FR y ATM.

- Equipo con costo reducido. Se reducen las necesidades de *"hardware"* y de *"software"* ya que el procesamiento es bastante simplificado.

- Mejora del desempeño y del tiempo de respuesta, la penetración es directa entre localidades con un bajo porcentaje de retardos en la red.

- Mayor disponibilidad en la red. Las conexiones a la red pueden redirigirse automáticamente a diversos cursos cuando ocurre un error.

- Se pueden utilizar criterios de Calidad de Servicio (QoS) basados o diseñados específicamente para el funcionamiento de *Frame Relay*.

- Mayor flexibilidad. Las conexiones son definidas por los programas. Los cambios hechos a la red son más rápidos y a menor costo si se comparan con otros servicios.

- Ofrece mayores velocidades y rendimiento, a la vez que provee la eficiencia de ancho de banda que viene como resultado de los múltiples circuitos virtuales que comparten un puerto de una sola línea.

- Los servicios de Frame Relay son confiables y de alto rendimiento. Son un método económico de enviar datos, convirtiéndolo en una alternativa a las líneas dedicadas.

- El Frame Relay es ideal para usuarios que necesitan una conexión de mediana o alta velocidad para mantener un tráfico de datos entre localidades múltiples y distantes.

1.2.2. **ATM (*Asincronous Transfer Mode)***

Asynchronous Transfer Mode (ATM) o Modo de Transferencia Asíncrona, se constituye como una tecnología desarrollada a finales de la década de los 80, para hacer frente a la gran demanda de capacidad de transmisión de servicios y aplicaciones, combinando la simplicidad de la multiplexación por división en el tiempo TDM (*Time Division Multiplex*), con la eficiencia de las redes de conmutación de paquetes, que manejan multiplexación estadística.

1.2.2.1. Funcionamiento de ATM.

A fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos por cable o radioeléctricos, en ATM la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes o celdas ATM de longitud constante, que pueden ser encaminadas individualmente mediante el uso de los denominados *canales virtuales* y *trayectos virtuales.*

En la Figura 1.5 se ilustra la forma en que diferentes flujos de información, de características distintas en cuanto a velocidad y formato, son agrupados en el denominado Módulo ATM para ser transportados a grandes enlaces de transmisión desde 155 Mbps hasta 622 Mbps, facilitados generalmente por sistemas de fibra óptica.

Una conexión ATM, consiste de celdas de información contenidas en un circuito virtual (VC). Estas celdas provienen de diferentes fuentes representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas variables tipo ráfagas como los datos. Cada celda compuesta por 53 bytes, de los cuales son para trasiego de información y los restantes para uso de campos de control (en la cabecera) con información de origen y destino la cual es identificada por un *virtual circuit identifier* VCI y un *virtual path identifier* VPI dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión. La organización de la cabecera (*header*) variará levemente dependiendo de sí la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son encaminadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local ya que pueden ser cambiados de interface a interface.

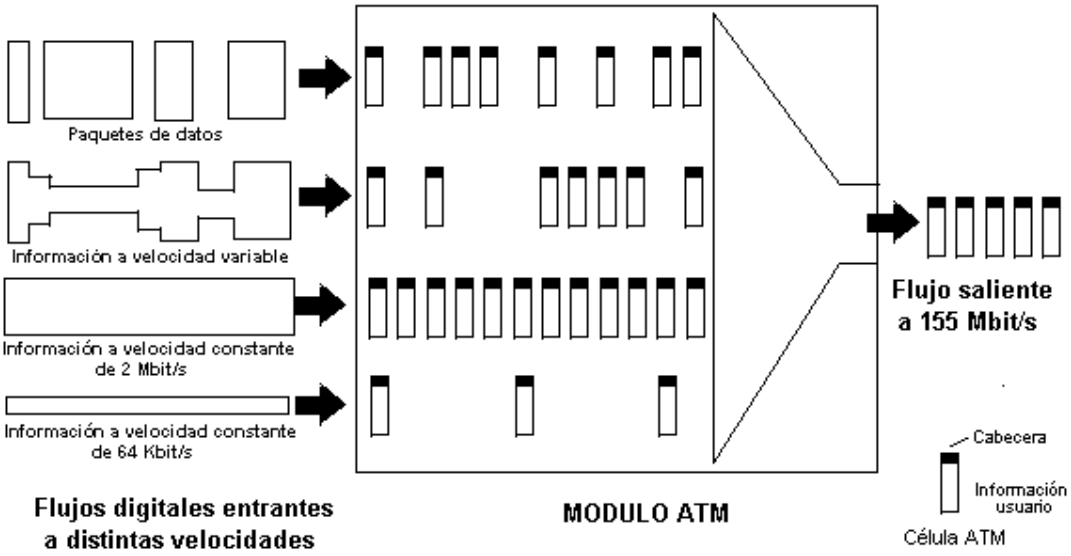


Figura. 1.5 Flujo de Información ATM

ATM multiplexa muchas celdas de circuitos virtuales en una ruta virtual colocándolas en particiones (*slots*), similar a TDM. Sin embargo, ATM llena cada slot con celdas de un circuito virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes. La Figura 1.6 describe el proceso de conmutación de ATM.

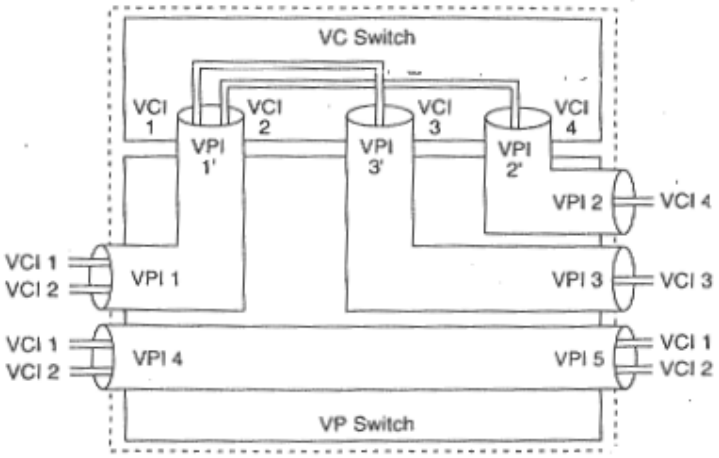


Figura. 1.6 Conmutación de rutas y circuitos virtuales en ATM

Los slots de celda no usados son llenados con celdas "idle", identificadas por un patrón específico en la cabecera de la celda. Este sistema no es igual al llamado "[10]bit stuffing" en la multiplexación Asíncrona, ya que aplica a celdas enteras.

10 *bit stuffing*: Procedimiento por el cual se agregan bits a la trama de datos de un sistema de comunicación, esta inserción de bits en l campo de datos se da únicamente cuando la rata de datos de la trama o de la ráfaga es inferior a la manejada en el resto de instancias del sistema.

Diferentes categorías de tráfico son convertidas en celdas ATM vía la capa de adaptación de ATM (AAL - ATM Adaptation Layer), de acuerdo con el protocolo usado.

1.2.2.2. Protocolo de transporte ATM. El protocolo ATM consiste de tres niveles o capas básicas, la *primera capa* llamada *capa física*, define los interfaces físicas con los medios de transmisión y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. A diferencia de muchas tecnologías LAN como Ethernet, que especifica ciertos medios de transmisión, (10 base T, 10 base 5, etc.) ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (*Synchronous Optical Network*), SDH (*Synchronous Digital Hierarchy*), [11] T1/E1, [12] T3/E3 o aún en modems de 9600 bps. Hay dos subcapas en la capa física que separan el medio físico de transmisión y la extracción de los datos, la *subcapa PMD (Physical Medium Depedent)* tiene que ver con los detalles que se especifican para velocidades de transmisión, tipos de conectores físicos, extracción de reloj, etc., Por ejemplo, la tasa de datos SONET que se usa, es parte del PMD.

La *subcapa TC (Transmission Convergence)* tiene que ver con la extracción de información contenida desde la misma capa física. Esto incluye la generación y el chequeo del *Header Error Corrección* (HEC), extrayendo celdas desde el flujo de bits de entrada y el procesamiento de celdas "idles" y el reconocimiento del límite de la celda. Otra función importante es intercambiar información de operación y mantenimiento (OAM) con el plano de administración.

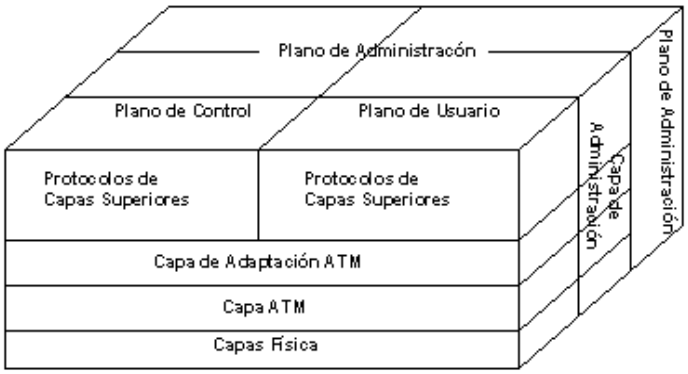


Figura. 1.7 Capas del protocolo ATM

La *segunda capa* es la *capa ATM*, esto define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del

11 T1/E1: T1 Línea de Trasmisión básica velocidad 1.544 Mbps para el sistema americano de transmisión de datos
E1 Línea de Trasmisión básica velocidad 2.048 Mbps para el sistema europeo de transmisión de datos
12 T3/E3:T3 Línea de Transmisión (LT) velocidad 44.736 Mbps (28 líneas T1); E3 LT velocidad 34.368 Mbps (16 líneas E1).

servicio. El formato de una celda ATM es muy simple. Consiste de 5 bytes de cabecera y 48 bytes para información.

Las celdas son transmitidas de manera serial y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una larga celda, que es muy eficiente para transmitir largas tramas de datos y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, vídeo y protocolos sensibles al retardo. A pesar de que no se diseñó específicamente para eso, la longitud de la celda ATM acomoda convenientemente dos *Fast Packets* [13]IPX de 24 bytes cada uno.

Los comités de estándares han definido dos tipos de cabeceras ATM: los *User-to-Network Interface* y la *Network to Network Interface.* La celda UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente, tal como hubs o routers ATM y la red de área extendida ATM (ATM WAN). La celda NNI define la interface entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interface entre una red ATM de un usuario privado y la red ATM de un proveedor público o carrier. La función principal de ambos tipos de cabeceras de UNI y la NNI, es identificar los *Virtual paths identifiers* (VPI) y los *virtual circuits* (VCI) como identificadores para el ruteo y la conmutación de las celdas ATM. En la Figura 1.8 se detalla el formato de las celdas UNI y NNI.

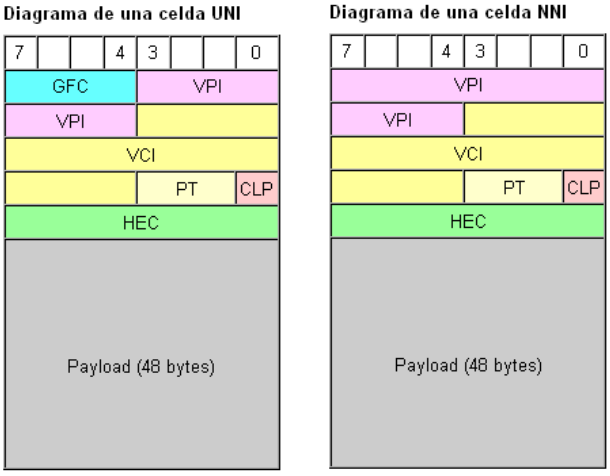


Figura. 1.8 Celdas UNI Y NNI de ATM

La *tercera capa* es la ATM *Adaptation Layer* (AAL). La AAL juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Específicamente, su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como emulación de circuitos,

vídeo, audio, *Frame Relay*, etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes.

La capa de Adaptación de ATM yace entre el ATM layer y las capas más altas que usan el servicio ATM. Su propósito principal es resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles del ATM layer. La capa de adaptación introduce la información en paquetes ATM y controla los errores de la transmisión. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes:

1. Que la información que está siendo transportada dependa o no del tiempo.

2. Tasa de bit constante/variable.

3. Modo de conexión.

Estas propiedades definen ocho clases posibles, cuatro se definen como B-ISDN Clases de servicios. La capa de adaptación de ATM define 4 servicios para equiparar las 4 clases definidas por B-ISDN:

- AAL-1
- AAL-2
- AAL-3
- AAL-4

La capa de adaptación se divide en dos subcapas:

a) *Capa de convergencia,* en esta capa se calculan los valores que debe llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el payload depende de la clase de información que va a ser transportada.

b) *Capa de Segmentación y re ensamblaje,* esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

1.2.2.3. Problemas en ATM. El Modo de Transferencia Asíncrona se planteó como herramienta para la construcción de redes de banda ancha (B-ISDN) basadas en conmutación de paquetes en vez de la tradicional conmutación de circuitos. El despliegue de la tecnología ATM no ha sido el esperado por sus promotores. Las velocidades para las que estaba pensada (hasta 622 Mbps) han sido rápidamente superadas. ATM se ha encontrado con la competencia de las tecnologías provenientes de la industria de la Informática, que con proyectos tales como la VoIP ofrecen las mejores perspectivas de futuro.

A diferencia de los mecanismos de control extremo a extremo que utiliza TCP, el explotar la capacidad de la red ATM al orden los Gpbs genera un juego de requerimientos necesarios para el control de flujo. Si el control del flujo se hiciese como una realimentación del lazo extremo a extremo, en el momento en que el mensaje de control de flujo arribase a la fuente, ésta habría transmitido ya algunos Mbytes de datos en el sistema, exacerbando la congestión. Y en el momento en que la fuente reaccionase al mensaje de control, la condición de congestión hubiese podido desaparecer apagando innecesariamente la fuente. La constante de tiempo de la realimentación extremo a extremo en las redes ATM (retardo de realimentación por producto lazo - ancho de banda) debe ser lo suficientemente alta como para cumplir con las necesidades del usuario sin que la dinámica de la red se vuelva impráctica.

Las condiciones de congestión en las redes ATM están previstas para que sean extremadamente dinámicas requiriendo de mecanismos de hardware lo suficientemente rápidos para llevar a la red al estado estacionario, necesitando que la red en sí, éste activamente involucrada en el rápido establecimiento de este estado estacionario. Sin embargo, esta aproximación simplista de control reactivo de lazo cerrado extremo a extremo en condiciones de congestión no se considera suficiente para las redes ATM.

1.2.2.4 **Red MPLS (*Multiprotocol Label Switching*).** MPLS se constituye como un mecanismo de transporte de datos estándar creado por *CISCO Systems* y repotenciado por la IETF (*Internet Engineering Task Force*), y definido en la RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI y fue diseñado para unificar el servicio de transporte de datos para las redes basadas en conmutación de circuitos y las basadas en conmutación de paquetes.

MPLS combina la flexibilidad de las comunicaciones punto a punto y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay, ATM, etc.

Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia todo esto en una red unificada.

Uno de los factores de éxito de la Internet actual está en la acepción de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones.

La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública de este siglo. Pero si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas.

Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort".

Si el modelo Internet ha de consolidarse como la red de datos del futuro, se necesita introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel best-effort y puedan proporcionar una respuesta más determinística y menos aleatoria.

Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (*Application Specific Integrated Circuits*), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS, sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF2 que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM; también como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"3); o bien, como una técnica para acelerar el encaminamiento de paquetes ... incluso, ¿para eliminar por completo el routing?. En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (enlace) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2.

Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del ruteo con la rapidez de la conmutación), MPLS ofrece nuevas posibilidades en la gestión de redes de interconexión, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

1.2.3.1 Origen de MPLS. Para poder crear circuitos virtuales análogo a lo que se hizo en ATM, se pensó en la utilización de etiquetas añadidas a los paquetes. Estas etiquetas definen el circuito virtual para su transporte a través de toda la red.

Estos ciruitos virtuales están asociados con un nivel de QoS determinado, según el SLA (*Service Level Agreement)*, inicialmente se plantearon dos métodos diferentes de etiquetamiento, en las capas 2 y 3 del modelo [14]OSI.

MPLS fue originalmente propuesto por un grupo de ingenieros de *Ipsilon Networks,* sin embargo esta tecnología, bautizada como tecnología de conmutación IP que fuera definido

14 OSI: Modelo de referencia creado en 1984 para la Interconexión de Sistemas Abiertos

solo para trabajar sobre infraestructura ATM, no alcanzó acogida en el mercado de las redes de transporte.

[15]CISCO Systems introdujo una propuesta relacionada con el trabajo de IN, sin restringir su trasmisión solo a ATM, llamada conmutación por marcas o "*Tag Switching*", y luego renombrada a conmutación por etiquetas o *"Label Switching"*, pasando a manos de la IETF, para su abierta estandarización. Una de las motivaciones principales fue la creación de s*witches* de alta velocidad, lo cual desde hace un buen tiempo era imposible, basado en el hecho de que no se podía realizar el transporte de estos paquetes a altas velocidades controlados solo hardware. Los avances de VLSI han contribuyeron al desarrollo de dichos *switches.*

Por esta razón las ventajas de MPLS radican principalmente en la habilidad de soportar múltiples modelos y plataformas de transporte basando su planificación e implementación en la Ingeniería de Tráfico.

Adicionalmente se implementó un amplio soporte en el aspecto de seguridad y robustez de la red, la cual va mas allá de la simple protección orecida por los sistemas SONET y SDH.

MPLS nace como la alternativa idónea para introducir ingeniería y transporte de tráfico IP sobre redes estructuralmente conmutadas por circuitos, este es el caso mencionado anteriormente para ATM.

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que las redes de backbone IP que los proveedores de servicio (ISP) habían empezado a desplegar en esos años, estaban construidos basados en routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los ISP fue el incremento del número de enlaces y de la capacidad de los mismos.

Del mismo modo, los ISP se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los

16 RSVP: Protocolo de Reserva de Recursos, los equipos pueden comunicar a otros nodos sobre sus requerimientos anchos de banda, retardos, etc.
17 PIM : Protocolo de Ruteo multicast que aprovecha la información entregada por las tablas de ruteo unicast.
18 BGP : *Border Gateway Protocol*, protocolo de enrutamiento para comunicación entre routers de border.

routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los ISP. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de ISP, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia.

Cada router se comunica con el resto mediante los circuitos virtuales permanentes (PVC) que se establecen sobre la topología física de la red ATM. Los PVC actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVC. Los routers ven los PVC como enlaces punto a punto entre cada par. En la Figura 1.9 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

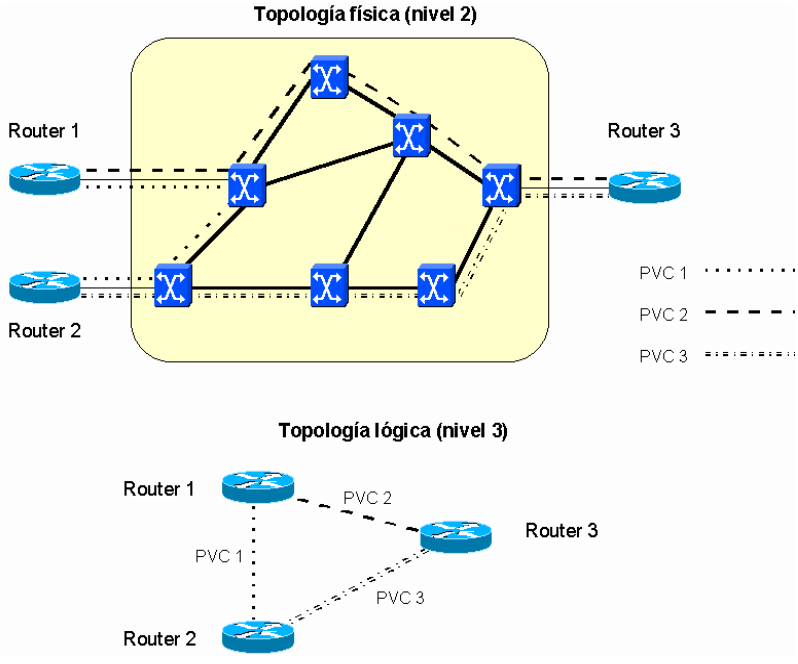


Figura. 1.9 IP sobre ATM

1.2.3.2 Funcionamiento de MPLS. Para entender el funcionamiento de MPLS se debe enunciar los elementos de la red:

- LER (*Label Edge Router*): Este elemento es el que inicia o termina el túnel formado para la comunicación en MPLS. Es decir, el elemento de entrada o salida a la red MPLS agregando o sustrayendo cabeceras. El router de entrada es conocido como *Ingress Router* y el de salida como *Egress Router*. Ambos forman el *Edge Label Switch Router* o routers de borde ya que se encuentran en los extremos de la red MPLS.
- LSR (*Label Switching Router*): Router conmutador de etiquetas.
- LSP (*Label Switched Path*): Este es el nombre designado para el camino que toma el tráfico, marcado como FEC *(Forwarding Equivalence Class)*, dentro de la red MPLS, tomado en cuenta que el túnel MPLS establecido entre los extremos LSP es unidireccional.
- LDP *(Label Distribution Protocol)*: Protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- FEC *(Forwarding Equivalence Class)*: Es el nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.
- Pila de etiquetas: un conjunto apilado de etiquetas que pueden circular con el paquete.

Es importante recalcar el hecho de que MPLS no se constituye por sí sola como una infraestructura de red WAN, su ingeniería de tráfico fue diseñada para aprovechar las redes ya implementadas como ATM o FR, para sobre estas transportar información de voz, datos, video, etc., de manera rápida, sencilla y eficaz, aprovechando la versatilidad de los protocolos TCP/IP.

La conmutación de etiquetas en un LSR a la llegada de un paquete MPLS sigue el siguiente proceso:

- Se examina la etiqueta del paquete entrante y la interfaz por donde llega
- Se procede a consultar la tabla de etiquetas
- El sistema determina la nueva etiqueta y la interfaz de salida para el paquete

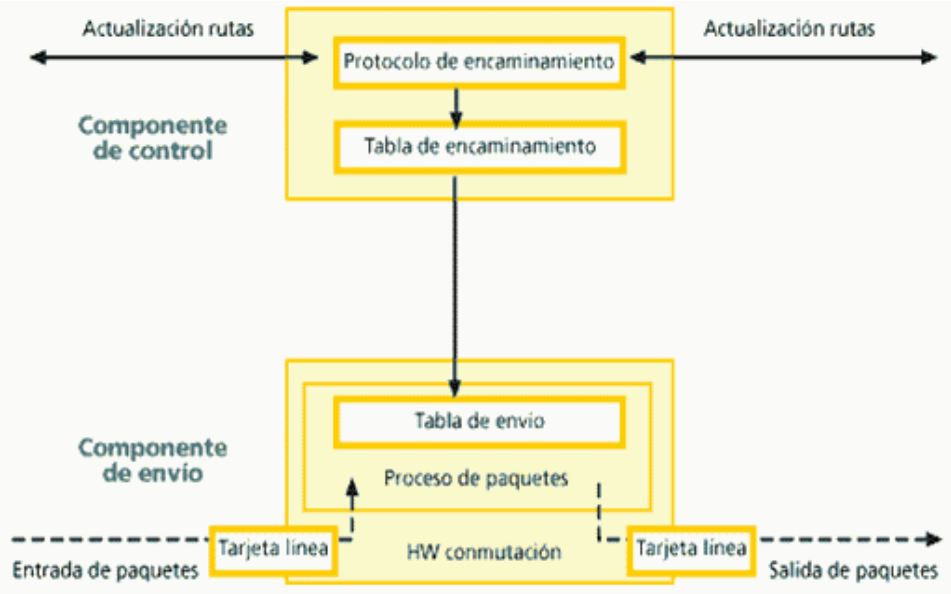


Figura. 1.10 Conmutación de Etiquetas en MPLS

En cuanto a MPLS sobre ATM, para soportar conmutación de etiquetas, un switch ATM debe implementar la componente de control de conmutación de etiquetas, como se observa en la Figura 1.10 Esta trabaja básicamente sobre la localización, distribución y procedimientos de mantenimiento de las etiquetas.

La información de enlace de etiquetas es comunicada mediante varios mecanismos, destacando el Protocolo de Distribución de Etiquetas o LDP. En muchos casos, se emplean otros protocolos diferentes para este cometido, como pueden ser: [16]RSVP, [17]PIM o [18]BGP. Siendo necesaria la participación de un LSR de ATM para llevarlos a cabo.

En la Figura 1.11 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (anteriormente llamado CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (*time-to-live*) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

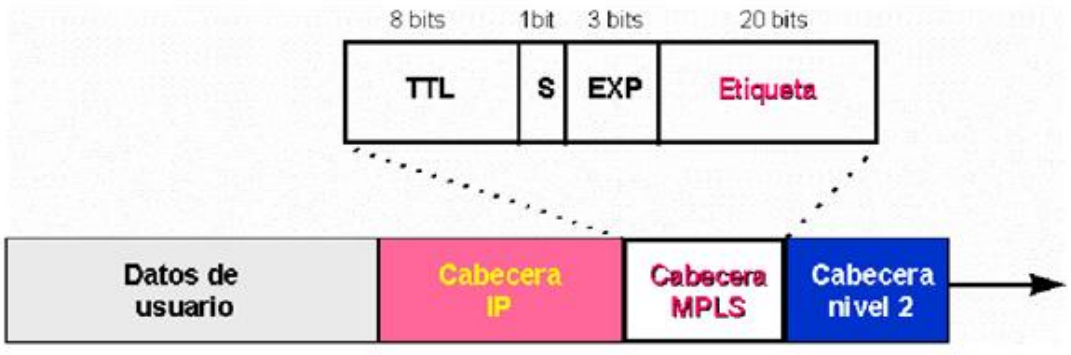


Figura. 1.11 La cabecera genérica de MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la Figura 1.12, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVC ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSP (puede haber más de uno para cada par de routers). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

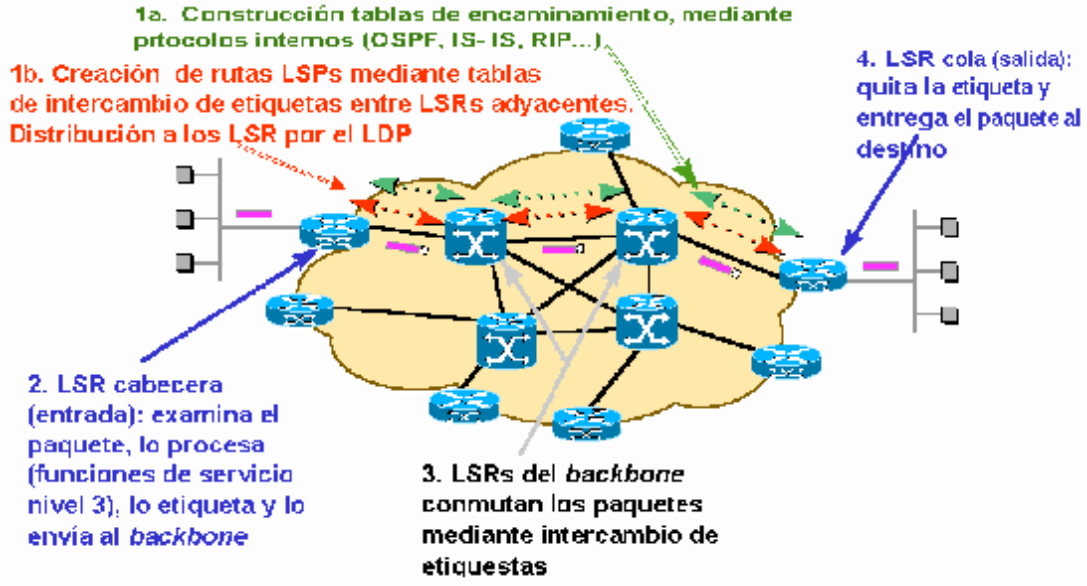


Figura. 1.12 Funcionamiento Global de MPLS

1.2.3.3 Aplicaciones de MPLS. Las aplicaciones y ventajas más relevantes que ofrece MPLS en la actualidad se listan a continuación:

· *Ingeniería de tráfico.* El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más

congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

- *Diferenciación de niveles de servicio mediante clases (CoS).* MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo [19]*DiffServ* del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, *DiffServ* permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en *DiffServ* como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP, de este modo, una red MPLS puede transportar distintas clases de tráfico.
- *Servicio de redes privadas virtuales (VPN).* Las redes privadas vistuales son conexiones entre puntos distantes dentro de la misma red o en redes distintas, con el objetivo de compartir información y recursos. Una VPN se sustenta sobre túneles IP, el objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de túneles privados por las que no puede entrar nadie que no sea miembro de esa IP VPN. Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:
  - En el nivel 3, mediante el protocolo IPSec10 del IETF.
  - En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros)

  Sobre la red WAN de un ISP.

  Estos dos tipos de túneles conocidos sobre redes *ATM/Frame Relay* presentan diferentes tipos de inconvenientes, entre los más relevantes el hecho de que se tienen que establecer conexiones punto a punto permanentes, su gestión es complicada, adicionalmente no se pueden establecer márgenes aceptables de calidad de servicio.

  Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el

modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre las distintas

19 *Diffserv:* Estándar para diferenciación de tráfico al establecer parámetros de calidad de servicio.

instancias de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo.

Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

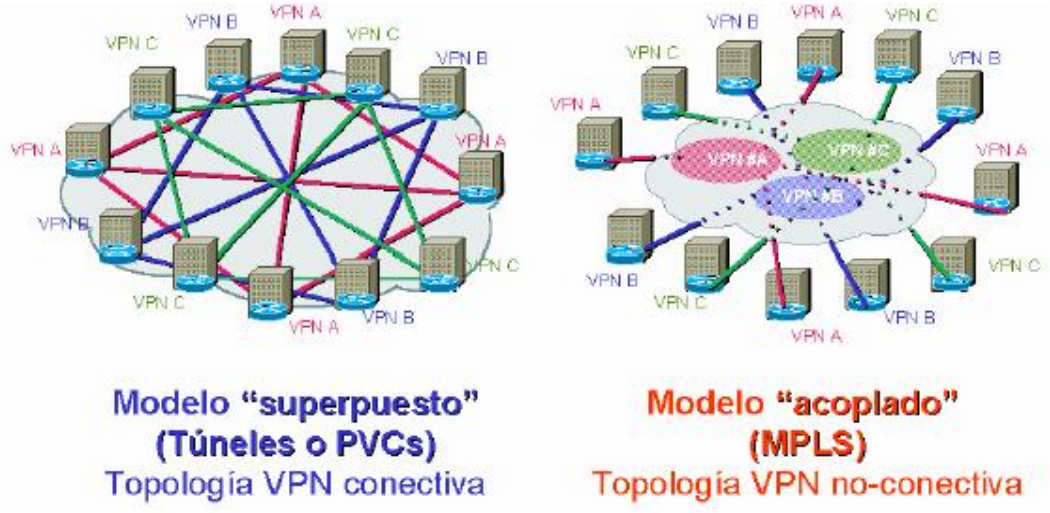


Figura. 1.13 Modelo VPN ATM/FR vs. Modelo Acoplado MPLS

1.2.4 ETHERNET (IEEE 802.3)

La red Ethernet o conocida también por el estándar IEEE 802.3, se constituye como un una infraestructura de red y protocolos establecidos para la comunicación entre terminales, sean estos equipos activos o pasivos, con el fin de intercambiar información y recursos.
El medio a través del cual se comunican los terminales es compartido por los mismos y varía dependiendo el segmento de red, las redes Ethernet han tenido un gran auge debido a la facilidad de su configuración y la eficacia de su desempeño en redes de área local o LAN.

1.2.4.1 Historia. A principios de los años 70 a un grupo de ingenieros de Palo Alto Research Center, dependiente de Xerox Company, se les encargó desarrollar 'La Oficina del Futuro'. Este grupo fue el creador del mouse, la idea de 'ventana' y un entorno de programación orientado a objetos (Smalltalk). Bob Metcalfe, uno de los ingenieros de este grupo, recibido en el MIT, dio el concepto básico que hoy utilizan todas las redes Ethernet. La idea de este sistema es la de difundir los paquetes de información, con facilidad de reenviar los paquetes que se pierdan, para asegurar el arribo seguro de los mismos.

En 1973 la red ya tenía todas las características esenciales de la Ethernet actual. Empleaba CSMA/CD para minimizar la probabilidad de colisión, y en caso de que ésta se produjera se ponía en marcha un mecanismo denominado retroceso exponencial binario para reducir gradualmente la 'agresividad' del emisor, con lo que éste se adaptaba a situaciones de muy diverso nivel de tráfico. Tenía topología de bus y funcionaba a 2,94 Mb/s sobre un segmento de cable coaxial de 1,6 km de longitud. Las direcciones eran de 8 bits y el CRC de las tramas de 16 bits. El protocolo utilizado al nivel de red era el PUP (Parc Universal Packet) que luego evolucionaría hasta convertirse en el que luego fue XNS (Xerox Network System), antecesor a su vez de IPX (Netware de Novell).

En vez de utilizar el cable coaxial de 75 ohms de las redes de televisión por cable se optó por emplear cable de 50 ohms que producía menos reflexiones de la señal, a las cuales Ethernet era muy sensible por transmitir la señal en banda base (es decir sin modulación). Cada empalme del cable y cada acoplador instalado producía la reflexión de una parte de la señal transmitida. En la práctica el número máximo de 'pinchos' vampiro, y por tanto el número máximo de estaciones en un segmento de cable coaxial, venía limitado por la máxima intensidad de señal reflejada tolerable.

20 SS7: Protocolo de Señalización Nº7 llamado también "fuera de banda" creado para controlar enlaces de voz dentro de la red ISDN en un canal paralelo a la transmisión de la señal, este canal SS7 es sicrónico.

En 1975 Metcalfe y David Boggs describieron Ethernet en un artículo que enviaron a *Communications of the ACM (Association for Computing Machinery)*, publicado en 1976. En él ya describían el uso de repetidores para aumentar el alcance de la red. En 1977 Metcalfe, Boggs y otros dos ingenieros de Xerox recibieron una patente por la tecnología básica de Ethernet, y en 1978 Metcalfe y Boggs recibieron otra por el repetidor. En esta época todo el sistema Ethernet era propiedad de Xerox.

Conviene destacar que David Boggs construyó en el año 1975 durante su estancia en Xerox PARC el primer router y el primer servidor de nombres de la Internet. La primera versión fue un intento de estandarizar ethernet aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

Los estándares de este grupo no reflejan necesariamente lo que se usa en la práctica, aunque a diferencia de otros grupos este suele estar cerca de la realidad.

1.2.4.2 Nivel Físico. Los estándares IEEE 802.3 siguen la nomenclatura XbaseY, donde X es la velocidad de transmisión en Mbps e Y puede hacer referencia a la distancia máxima en centenares de metros, al tipo de medio de transmisión, o alguna otra característica (F: fibra, T:par trenzado, X:full duplex, etc). En la Figura 1.13 se presenta un resumen de los estándares que han ido dando vida al sistema.

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5e ó 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

Figura. 1.14 Nivel Físico Ethernet

Ethernet basa su funcionamiento en el transporte de tramas de datos en las capa 2 y 3 del modelo OSI, en la figura 1.14 se muestra el formato de la trama Ethernet con todos sus campos.

Trama IEEE 802.3	Preámbulo	SOF	Destino	Origen	Longitud	Datos	Relleno	FCS
	7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

Figura. 1.15 Trama 802.3

Los campos de trama Ethernet 802.3 son los siguientes:

- *Preámbulo.* Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es:

  10101010 10101010 10101010 10101010 10101010 10101010 10101010

  Estos bits se transmiten en orden, de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

- *SOF (Start Of Frame) Inicio de Trama.* Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de dirección MAC de destino.

Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

- *Dirección de destino.* Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo multicast o la dirección de broadcast de la red. Cada estación examina este campo para determinar si debe aceptar la trama (si es la estación destinataria).

- Dirección de origen. Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 desde la que se envía la trama. La estación que deba aceptar la trama conoce por este campo la dirección de la estación origen con la cual intercambiará datos.

- *Tipo.* Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con la trama o, en su defecto, la longitud del campo de datos. La capa de enlace de datos interpreta este campo. (En la IEEE 802.3 es el campo longitud y debe ser menor o igual a 1526 bytes.)

- *Datos.* Campo de 0 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

- *Relleno.* Campo de 0 a 46 bytes que se utiliza cuando la trama Ethernet no alcanza los 64 bytes mínimos para que no se presenten problemas de detección de colisiones cuando la trama es muy corta.

- *FCS (Frame Check Sequence - Secuencia de Verificación de Trama).* Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (Control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo re calcula, si el valor calculado es 0 la trama es válida.

Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el *checksum* de verificación de la trama, comprueba que los datos corresponden a un mensaje IP y entonces lo pasa a dicho protocolo (capa de red-Internet) para que lo procese.

Hay que destacar que las direcciones utilizadas por Ethernet no tienen nada que ver con las direcciones de Internet. Las de Internet se le asignan a cada usuario, mientras que las de Ethernet vienen de incluidas de fábrica en la tarjeta de red (NIC).

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

CSMA/CD opera de la siguiente manera:

- Una estación que tiene un mensaje para enviar escucha al medio para ver si otra estación está transmitiendo un mensaje.
- Si el medio está tranquilo (ninguna otra estación está transmitiendo), se envía la transmisión.
- Cuando dos o más estaciones tienen mensajes para enviar, es posible que transmitan casi en el mismo instante, resultando en una colisión en la red.
- Cuando se produce una colisión, todas las estaciones receptoras ignoran la transmisión confusa.
- Si un dispositivo de transmisión detecta una colisión, envía una señal de expansión para notificar a todos los dispositivos conectados que ha ocurrido una colisión.
- Las estaciones transmisoras detienen sus transmisiones tan pronto como detectan la colisión.
- Cada una de las estaciones transmisoras espera un periodo de tiempo aleatorio e intenta transmitir otra vez.

La detección de portadora es utilizada para escuchar al medio (la portadora) para ver si se encuentra libre. Si la portadora se encuentra libre, los datos son pasados a la capa física para su transmisión. Si la portadora está ocupada, se monitorea hasta que se libere.

Luego de comenzar la transmisión, continúa el monitoreo del medio de transmisión. Cuando dos señales colisionan, sus mensajes se mezclan y se vuelven ilegibles. Si esto ocurre, las estaciones afectadas detienen su transmisión y envían una señal de expansión.

La señal de expansión de colisión asegura que todas las demás estaciones de la red se enteren de que ha ocurrido una colisión.

El estándar CSMA/CD de la IEEE define un modelo hecho de hasta seis funciones. Tres de estas funciones están relacionadas con el envió de datos y las otras tres de la recepción de datos. Las funciones de recepción funcionan en paralelo con las de envío, la función de encapsulación y desencapsulación de datos es llevada a cabo por la subcapa MAC. Este proceso es responsable de las funciones de direccionamiento y del chequeo de errores.
El encapsulado por otro lado es realizado por la estación emisora. El encapsulado es el acto de agregar información, direcciones y bytes para el control de errores, al comienzo y al final de la unidad de datos transmitidos. Esto es realizado luego que los datos son recibidos por la subcapa de control de enlace lógico (LLC). La información añadida es necesaria para realizar las siguientes tareas:

- Sincronizar la estación receptora con la señal.
- Indicar el comienzo y el fin de la trama.
- Identificar las direcciones tanto de la estación emisora como la receptora.
- Detectar errores en la transmisión.

El desencapsulado es realizado por la estación receptora. Cuando es recibida una trama, la estación receptora es responsable de realizar las siguientes tareas:

- Reconocer la dirección de destino y determinar si coincide con su propia dirección.
- Realizar la verificación de errores.
- Remover la información de control que fue añadida por la función de encapsulado de datos en la estación emisora.

La función de administración de acceso al medio es realizada por la subcapa MAC.
En la estación emisora, la función de administración de acceso al medio es responsable de determinar si el canal de comunicación se encuentra disponible. Si el canal se encuentra disponible puede iniciarse la transmisión de datos. La función de administración es responsable de determinar que acción deberá tomarse en caso de detectarse una colisión y cuando intentará retransmitir, en la estación receptora la función de administración de

acceso al medio es responsable de realizar las comprobaciones de validación en la trama antes de pasarla a la función de desencapsulado.

La función de codificación/decodificación es realizada en la capa física. Esta función es responsable de obtener la forma eléctrica u óptica de los datos que se van a transmitir en el medio.

La codificación de datos es realizada por la estación emisora. Esta es responsable de traducir los bits a sus correspondientes señales eléctricas u ópticas para ser trasladadas a través del medio. Adicionalmente, esta función es responsable de escuchar el medio y notificar al la función de administración de acceso al medio si el medio se encuentra libre, ocupado o se ha detectado una colisión.

La decodificación de datos es realizada en la estación receptora. Esta es responsable de la traducción de las señales eléctricas u ópticas nuevamente en un flujo de bits.

Trama de transmisión CSMA/CD

Se defina a una trama de transmisión como el grupo de bits en un formato particular con un indicador de señal de comienzo de la trama. El formato de la trama permite a los equipos de red reconocer el significado y propósito de algunos bits específicos en la trama. Una trama es generalmente una unidad lógica de transmisión conteniendo información de control para el chequeo de errores y para el direccionamiento.

El formato de la trama CSMA/CD (IEEE 8023.3) se encuentra a continuación:

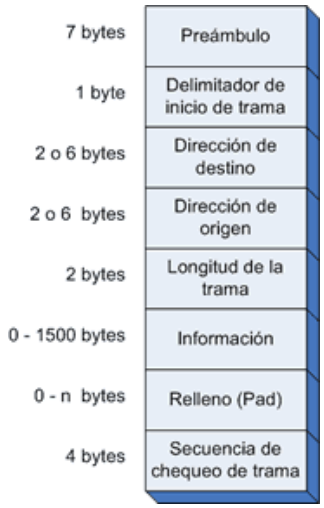


Figura. 1.16 Trama CSMA/CD

1.2.4.4 Dominio de colisión. Un dominio de colisión es un segmento Fisico de una red de computadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

A medida que aumenta el número de nodos que pueden transmitir en un segmento de red, aumentan las posibilidades de que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos nodos, que se conoce como colisión. Conforme aumenta el número de colisiones disminuye el rendimiento de la red.

El rendimiento de la red puede ser expresado como

$$Rendimiento(\%) = \left(1 - \frac{Colisiones}{Paquetes\ Totales}\right) * 100$$

Figura. 1.17 Rendimiento de Ethernet

Un dominio de colisión puede estar constituido por un solo segmento de cable Ethernet en una Ethernet de medio compartido, o todos los nodos que afluyen a un concentrador Ethernet en una Ethernet de par trenzado, o incluso todos los nodos que afluyen a una red de concentradores y repetidores.

A partir de las capas del modelo OSI es posible determinar qué dispositivos extienden o componen los dominios de colisión.

- Los dispositivos de la capa 1 OSI (como los concentradores y repetidores) reenvían todos los datos transmitidos en el medio y por lo tanto extienden los dominios de colisión.
- Los dispositivos de la capa 2 y 3 OSI (como los conmutadores) segmentan los dominios de colisión.
- Los dispositivos de la capa 3 OSI (como los routers) segmentan los dominios de colisión y difusión (*broadcast*).

Con Ethernet, si se tienen más de cuatro concentradores en una red, entonces probablemente ya se ha extendido el dominio de colisión más de lo deseado.

1.2.4.5 Redes *Fast* y *Gigabit* Ethernet. En la actualidad se manejan dos niveles de velocidad de manera generalizada, para trasmisión de datos a nivel local:

- ***Fast Ethernet*** *o* Ethernet de alta velocidad, es el nombre de una serie de estándares de IEEE de redes Ethernet con tasas de transmisión de 100 Mbps (megabits por segundo). En su momento el prefijo fast se le agregó para diferenciarla de la versión original Ethernet de 10 Mbps.

Debido al incremento de la capacidad de almacenamiento y en el poder de procesamiento, los DTE actuales tienen la posibilidad de manejar aplicaciones de vos y video de alta resolucion. Cuando estos ficheros son almacenados y compartidos en una red, las transferencias de un cliente a otro producen un gran uso de los recursos de la red.
Un adaptador de fast Ethernet puede ser dividido lógicamente en una parte de control de acceso al medio (MAC; media access controller), que se ocupa de las cuestiones de disponibilidad y una zona de capa física

La capa MAC se comunica con la física mediante un interfaz de 4 bits a 25 MHz de forma paralela síncrona, conocida como MII.
El interfaz MII establece como tasa máxima de bits de datos una velocidad de 100Mbit/s para todas las versiones de *Fast Ethernet.*
Se puede observar que actualmente en redes reales la cantidad de datos que se envían por señal está por debajo de este máximo teórico. Esto es debido a que se añadan cabeceras y colas en cada paquete para detectar posibles errores, a que ocasionalmente se puedan "perder paquetes" debido al ruido, o al tiempo de espera necesario para que cada paquete sea recibido por el otro terminal.
Existen subdivisiones dentro de *Fast Ethernet,* que dependen del tipo de medio utilizado y de la manera en la que se transmiten los datos:

§*100BASE-TX,* es el estándar más común dentro de este tipo de Ethernet es 100BaseTX, y es soportado por la mayoría del hardware Ethernet que se produce actualmente, utiliza 2 pares de cobre trenzado de categoría 5 o superior (un cable de categoría 5 contiene 4 pares, por lo que puede soportar 2 enlaces 100BASE-TX).

En una configuración típica de 100Base-TX se utiliza un par de cables trenzados en cada dirección (full-duplex). La configuración de una red 100Base-TX es muy similar a una de tipo 10Base-T. Cuando utilizamos este estándar para crear una red de área local, los componentes de la red (ordenadores, impresoras, etc) suelen estar conectados a un switch o un hub, creando una red con topología de estrella. Alternativamente, es posible conectar dos componentes directamente usando cable cruzado.

§*100BASE-T4*, fue una de las primeras implementaciones de Fast Ethernet. Se requiere de cuatro pares de cable trenzado, pero estos deben ser de categoría 3 en lugar de ser categoría 5 que es la exigida por TX. De los cuatro pares, un par esta reservado para transmitir, otro para recibir, y los dos restantes llevan datos de control.

§*100BASE-T2*, en este estándar los datos se transiten sobre dos pares de cobre, 4 bits por símbolo. En primer lugar, un símbolo de 4 bits se amplia en dos símbolos de 3 bits cada uno mediante un procedimiento complicado de codificación basado en un registro lineal de retroalimentación (ver el estándar para obtener más información). Esto es necesario para aplanar el ancho de banda y el espectro de la señal. El mapa de bits original que representa al código, no es constante en el tiempo y tiene un largo periodo (se podría decir que aparece con una frecuencia aleatoria).
§*100BASE-FX*, es una versión de Fast Ethernet sobre fibra óptica. Utiliza un tipo de luz 1300 (NIR; nm near- infrared) que es transmitida a través de dos líneas de fibra óptica, una para recepción (RX) y la otra para transmitir (TX). Para estos casos, la longitud máxima que abarca es de 400 metros para las conexiones half-duplex (para asegurar la detección de colisiones) o 2 kilómetros para full-duplex sobre fibra óptica multimodo (en comparación con los 100 metros sobre cable de cobre). En cuanto al tipo de codificación utilizada, 100BASE-FX utiliza la misma codificación 4B5B y NRZI que usaba 100BASE-TX.

§100BASE-SX, utiliza dos líneas multimodo de fibra óptica para recibir y transmitir. Se trata de una alternativa de menor coste que 100BASE-FX, ya que usa una longitud de onda más corta, que es mucho menos costoso que la longitud de onda larga utilizada en 100BASE-FX. 100BASE-SX puede trabajar a distancias de hasta

300 metros, utiliza la misma longitud de onda que la versión de fibra óptica 10BASE-FL. Debido a la corta longitud de onda utilizada (850 nm), se necesitan componentes ópticos menos costosos (LEDs en lugar de láseres), lo que hace que sea una opción atractiva para aquellos que actualicen de 10BASE-FL y los que no exigen largas distancias.

§*100BASE-BX*, trabaja a través de una sola línea de fibra óptica (a diferencia de 100BASE-FX, que utiliza un par de fibras). Debido a que contamos con una solo línea, se utiliza un multiplexor que divide la señal en dos longitudes diferentes de onda, una para transmitir, y otra para recibir.

- ***Gigabit Ethernet,*** también conocido como GE, es una ampliación de Ethernet estandarizada por IEEE 802.3ab y 802.3z, que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a una rata de transmisión de 1000 megabits por segundo. Su principal atributo reside, precisamente, en basarse en una tecnología tan convencional como Ethernet.

IEEE 802.3ab, ratificada en 1999, define el funcionamiento de Gigabit Ethernet sobre cables de cobre del tipo *Unshielded Twisted Pair* (UTP) y categoría 5, 5e o 6 y por supuesto sobre fibra óptica. De esta forma, pasó a denominarse 1000BASE-T. Se decidió que esta ampliación sería idéntica a Ethernet desde la capa de enlace de datos hasta los niveles superiores, permitiendo el aprovechamiento de las posibilidades de la fibra óptica para conseguir una gran capacidad de transmisión sin tener que cambiar la infraestructura de las redes actuales. Uno de los retrasos con el estándar fue la resolución de un problema al emitir con láser sobre fibra multimodal, ya que en casos extremos se podía producir una división del haz, con la consiguiente destrucción de datos. Esto era debido a que la fibra multimodal fue diseñada pensando en emisores LED, no láser y fue resuelto prohibiendo que en este estándar el láser dirigiera su haz hacia el centro de la fibra.

Gigabit Ethernet puede ser utilizada de diversas formas, para conectar conmutadores entre sí equipos que manejen un alto flujo de datos, para conectar servidores de acceso generalizado dentro de una red, para conectar estaciones finales a concentradores, etc.

En 2002, IEEE ratificó una nueva evolución del estándar Ethernet, 10 Gigabit Ethernet, con un tasa de transferencia de 10.000 megabits/segundo (10 veces mayor a Gigabit Ethernet).

1.3 INFRAESTRUCTURA DE UN ISP

ISP son las siglas en ingles para *Internet Service Provider*, el proveedor de servicios de internet, físicamente, Internet está compuesto por routers interconectados por enlaces de comunicación. Las redes IP más simples están formadas por unos pocos routers de propósito general interconectados por enlaces propios o alquilados. A medida que las redes se vuelven más complejas, con un número mayor de elementos, se requiere más infraestructura. Los elementos se especializan en sus aplicaciones, la gestión y la seguridad adquieren mayor importancia, la localización física es un factor a tener en cuenta, y la capacidad de manejar altas densidades de clientes es crítica. Como los routers trabajan con direcciones de nivel 3, que tienen una estructura, al imponer una estructura jerárquica a una red los routers pueden usar caminos redundantes y determinar rutas óptimas incluso en una red que cambia dinámicamente. Las estructuras de red jerárquicas también facilitan la separación de dominios de difusión.

Por otro lado, el mecanismo de enrutamiento del protocolo IP es el enrutamiento salto-a-salto (*hop-by-hop*) sin estado basado en el destino, que tiende intrínsecamente a agregar tráfico en las principales rutas troncales, lo que justifica la implementación de una estructura jerárquica, esta estructura basa su espina dorsal en tres segmentos fundamentales:

- Red de Border
- Red de Core
- Red de distribución

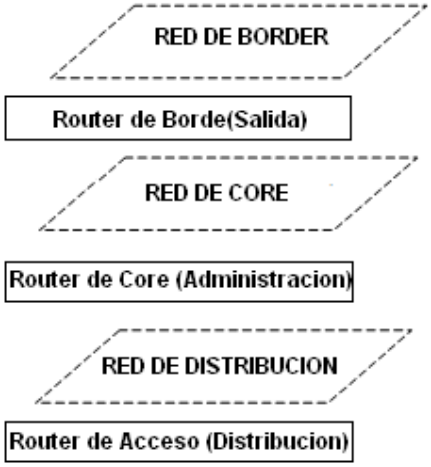


Figura. 1.18 Niveles jerárquicos ISP

1.3.1 Red de acceso

La red de acceso es la encargada de recoger todas las conexiones de acceso entregadas por la red de distribución del proveedor de última milla, a través de enlaces de fibra óptica, cobre, etc. En este segmento de la red se realiza la administración directa de los clientes distribuyéndolos entre las diferentes interfaces del router de acceso de la red.

Existen diferentes tipos de enlaces de acceso en la red de distribución, dependiendo de la tecnología utilizado para este objetivo.

· **Líneas conmutadas o dial-up.** Este tráfico (sobre enlaces portadores bajo [20]SS7) llega al Punto de Interconexión del operador de acceso, que está conectado con nuestra central de conmutación. La central toma como argumento el número de destino y saca en interfaces primarios (ISDN PRI) el tráfico de Internet. Estos primarios se suministran a los equipos RAS (*Remote Access Server*) situados en los POP de la Red de Datos. El usuario final dispone de un equipo de cliente (modem o router) que establece una sesión PPP con el RAS. El RAS es un dispositivo de acceso remoto que dispone de un pool de módems y que realiza funciones

20 SS7: Protocolo de Señalización Nº7 llamado también “fuera de banda” creado para controlar enlaces de voz dentro de la red ISDN en un canal paralelo a la transmisión de la señal, este canal SS7 es sicrónico.

de cliente RADIUS, autentificando al usuario y terminando la sesión PPP. RADIUS es un estándar de Internet adoptado de manera generalizada en las situaciones en las que un dispositivo de acceso remoto necesita autenticar a un usuario de acceso conmutado frente a un servicio de directorio. La salida del RAS se enlaza con un router concentrador de acceso mediante [21]VLAN (*Vritual Local Area Network*). Para incrementar el nivel de servicio se realiza un diseño redundante, en el que cada RAS tiene dos salidas, una *Fast Ethernet* y otra *Ethernet*, conectadas a dos VLAN diferentes. Cada una de las VLAN tiene conexión con dos routers concentradores de acceso diferentes.

Los RAS tendrán dos rutas por defecto. La ruta por defecto a través de la interfaz Ethernet tendrá una métrica superior a la ruta a través de la interfaz *Fast Ethernet.* Los [22]*gateways* SS7 realizan las funciones de un RAS pero se pueden conectar directamente con señalización SS7 al punto de Interconexión, eliminando la necesidad de puertos de conmutación y de interfaces primarios. Además estos equipos permiten reducir la congestión de red y aumentar las tasas de conexión. La figura 1.18 representa el escenario de un proveedor con un Gateway SS7:

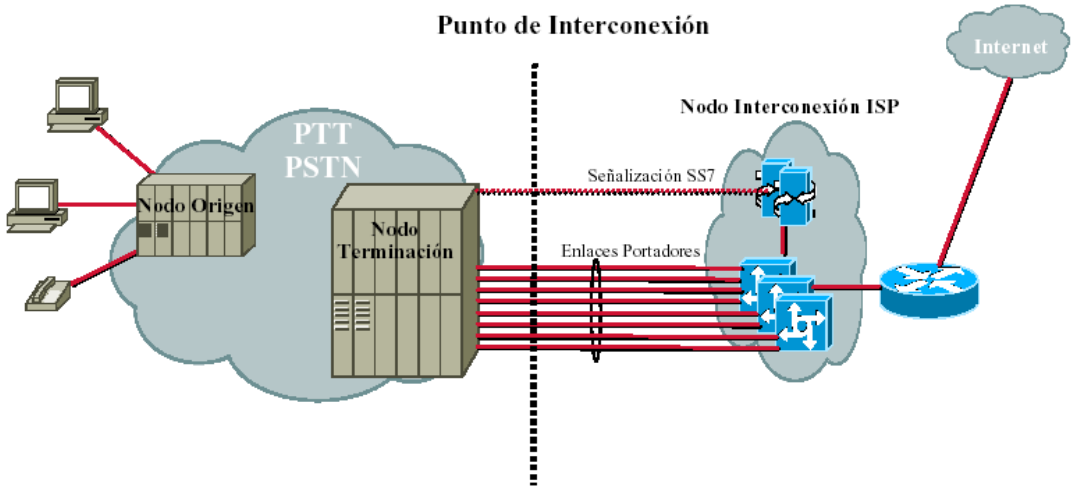


Figura. 1.19 ISP conectado a *Gateway* SS7

21 VLAN*:* Red local virtual, son redes dentro de una misma red LAN, separadas en subredes por el protocolo 802.1q que coloca etiquetas en los paquetes de estas redes para identificarlas y tratarlas como redes distintas.
22 *gateway:* Puerta de enlace, equipo que une un segmento de red con otro próximo en camino a una red de acceso a Internet.

1.3.1.2 Líneas dedicadas. Uno de los componentes de más rápido crecimiento del acceso a Internet es la conectividad entre negocios mediante líneas alquiladas. El tráfico de líneas alquiladas se define como DSO, N*64, E1, E3 ó STM-1.

En este caso los clientes disponen de un router que se enlaza directamente mediante una línea dedicada con un router concentrador de acceso, por el que entra a la red de datos del proveedor. El router concentrador de acceso realiza la agregación del tráfico procedente de líneas alquiladas. El enlace entre el router de cliente y el router concentrador se soporta actualmente sobre anillos de fibra óptica de área metropolitana. Los POPs diseñados antes de la generalización de los interfaces SDH en los routers requerían una multitud de bastidores de DSU (data service units) para terminar E1 sobre pares de cobre tradicionales. Los routers concentradores de acceso actuales proporcionan una alta densidad de terminaciones para conexiones DS1 y DS3, de modo que una sola tarjeta de línea puede terminar cientos de circuitos DS1 transportados sobre una sola fibra.

1.3.1.3 Líneas ADSL. Permiten a los clientes disponer de acceso permanente de banda ancha sobre una línea telefónica convencional. El usuario es provisto de un equipo de cliente que incluye un módem ADSL. Este equipo se conecta al punto de terminación telefónica en el domicilio del usuario. En el otro extremo del par de cobre se localiza el DSLAM (Digital Subscriber Line Access Multiplexer), encargado de terminar las conexiones ADSL de nivel físico de múltiples usuarios y de conmutar las celdas ATM transportándolas hacia la red de acceso. El ISP de Internet se conecta mediante un enlace ATM al Punto de Acceso Indirecto (PAI) del operador de acceso, que establece un PVC (circuito virtual permanente) de ATM entre el usuario y el PAI.

Para soportar el acceso por líneas ADSL es necesario introducir en la red de datos un nuevo elemento denominado BAS o *Broadband Access Server*. Este equipo concentra el tráfico y actúa como border entre los niveles 2 y 3, teniendo funcionalidades de enrutamiento, autenticación y control de tráfico.

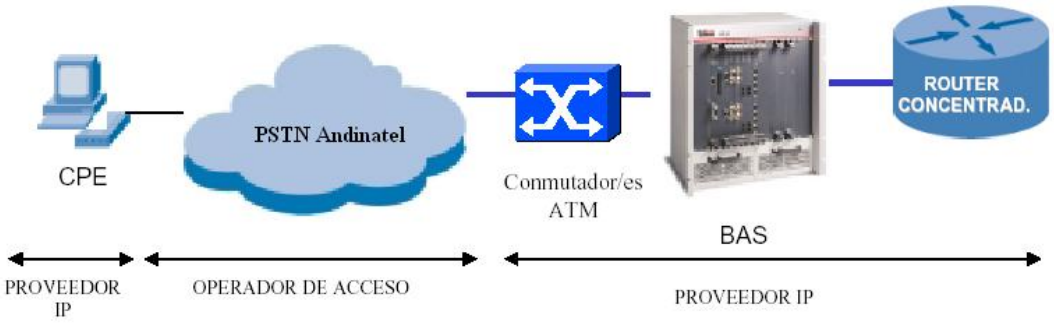


Figura. 1.20 ISP conectado a *Gateway* SS7

En las redes de ISP se tiende actualmente a desplegar ATM únicamente en el borde de la red, con la misión de agregar tráfico ADSL de los [23]DSLAM, así como servicios de *Frame Relay*, en equipos switch ATM. La mayor parte de los ISP ya no despliegan ATM en la red troncal, que está basada íntegramente en IP. La demanda de servicios de ADSL exige que los conmutadores ATM tengan capacidad para soportar un número elevado de VC (circuitos virtuales). Los conmutadores ATM no estaban diseñados inicialmente para soportar múltiples DSLAM, que pueden tener cientos de circuitos virtuales por cada circuito DSLAM-conmutador. Adicionalmente la introducción de las redes MPLS en el mercado de los carrier presenta un reto para los proveedores de internet al obligarlos a cambiar su infraestructura y el diseño de su red a la ingería de trafico propuesta por MPLS.

1.3.2 Red de *Core*. Constituye el segmento de la red más importante para la gestión y funcionamiento del ISP, la red de core se encarga de :

- Agregar el tráfico procedente de las redes de acceso y border.
- Interconexión de todos los [24]POP de la Red.
- Interconexión a otras Redes, proveedores de tránsito y puntos neutros.
- Aloja al Centro de Proceso de Datos, segmento de la red donde se encuentran funcionando los servidores de datos del ISP, nombres, correo, proxy, monitoreo, etc.

Parte indispensable dentro de la red de core es el router de core, equipo encargado de gestionar todas las tareas mencionadas anteriormente de la manera más eficiente, a través del router de core circula todo el tráfico de la red, por lo que realiza diversas funciones como:

23 DSLAM: Multiplexor de acceso para líneas digitales de suscriptor, estos equipos de hallan en la red de distribución del ISP.
24 POP: Punto de Presencia del Proveedor, estos puntos se encuentra diseminados en la *edge* del proveedor o red de acceso, son los encargados de concentrar el acceso de clientes en los distintos puntos de cobertura del ISP.

- *Gestión de nubes de compartición,* para las diferentes clases de enlaces gestionados por el ISP, sean estos residenciales o corporativos, en compartición 1:X, donde X representa un numero múltiplo de 2, que indica el nivel de compartición de la nube, dado que el uso del internet pasa por un tema estadístico, donde los usuarios de determinado canal no utilizan todo el ancho de banda todo el tiempo, un enlace 1:8, representa un canal compartido para ocho usuarios dentro de la nube, por lo que se garantiza la octava parte de la velocidad, en el caso extremo de que estén accediendo a la red todos los usuarios, al mismo tiempo, lo cual en la práctica, no sucede.
- *Criterios de balanceo de carga y enrutamiento,* tomando en cuenta que todo el trafico del ISP es gestionado por el segmento de core, la decisión de que vía de salida tomaran los datos generados por los enlaces de distribución, las toma la red de core, es así que, de ser el caso que el proveedor posea más de un canal de salida al internet, con más de un proveedor, como es el caso de los enlaces de ***backup,*** el router de core encaminará el tráfico de los diferentes clientes a través de los diferentes enlaces, no solo en el caso de que existan problemas en alguno de estos, sino cuando el administrador de la red decida balancear la carga en alguno de estos enlaces, cuando se encuentren saturados.
- *Procesos de autenticación,* estos procesos se llevan a cabo en la red de core, cuando el ISP brinda enlaces, tanto banda ancha como en Dial up, a través del sistema PPP *Point to Point Protocol,* este tipo de acceso establece conexiones punto a punto, independiente de la velocidad, al cliente se le confiere un nombre de usuario y una contraseña, los mismo que son validados en un servidor de validación, este servidor puede correr aplicaciones como [25]CHAP, [26]TACACS o [27]RADIUS, para dar el acceso a estos enlaces, en la actualidad el sistema más utilizado es RADIUS por sus ventajas al hablar de movilidad IP.
- *Alojamiento y conectividad para servidores de datos,* en la red de core se alojan los servidores de datos parte de la red del ISP, entre estos equipos están los servidores DNS, servidor de nombres, encargado de la resolución de direcciones IP a nombres de internet, SMTP, servidor de transferencia de correo, encargado de gestionar correo saliente de la red del ISP hacia el internet, RADIUS, servidor de autenticación para enlaces PPP, etc. estos servidores se hallan conectados a la red

25 CHAP: *Challenge Handshake Authentication Protocol,* es un protocolo de autenticación por desafío mutuo entre los terminales.
26 TACACS: *Terminal Access Controller Access Control System,* es un protocolo de autenticación remota que se usa en redes Unix
27 RADIUS: *Remote Authentication Dial-In User Server*, es un protocolo de autenticación para aplicaciones de acceso y movilidad IP.

de core el ISP con el objetivo de que todos los usuarios parte de la red del mismo puedan acceder a sus servicios.

1.3.3 Red de border

La red de border gestiona el acceso de los usuarios al internet, esta red se encuentra en el *edge* o borde de la red como su nombre lo indica, se encuentra interconectado al proveedor de canal internacional del ISP, la comunicación entre los enrutadores de border se realiza a través del protocolo BGP, BGP o *Border Gateway Protocol* es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por lo tanto, los ISP registrados en Internet se componerse de varios sistemas autónomos, designando sistemas autónomos a cada uno de los segmentos parte de la red del ISP y para este caso es necesario el protocolo BGP.

Este intercambio de información de encaminamiento se hace entre los routers externos de cada sistema autónomo, estos routers deben soportar BGP, BGP se constituye como el protocolo más utilizado en redes con intención de configurar un EGP (*External Gateway Protocol*).

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomos. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP).

El protocolo de *gateway* fronterizo (BGP) es un ejemplo de protocolo de *gateway* exterior (EGP). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. BGP4 es la primera versión que admite encaminamiento entre dominios sin clase (CIDR) y agregado de rutas. A diferencia de los protocolos de Gateway internos (IGP), como [28]RIP u [29]OSPF, no usa métricas como número de saltos, ancho de banda, o retardo. En cambio, BGP toma decisiones de encaminamiento basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP

En conclusión, en la red de border se concentra todo el trafico del ISP desde la red de distribución, pasando por la red de core, y terminando en la red de border, en esta red se hallan además, interconectados varios enlaces de salida, no solo enlaces activos sino enlaces de backup.

28 RIP: *Routing Information Protocol*, protocolo de enrutamiento dinámico, intercambio de tablas de rutas entre routers aledaños.
29 OSPF: *Open Short Path First*, método de enrutamiento dinámico que designa la ruta más corta para el transporte de los paquetes origen – destino, de manera automática.

En la figura 1.19 se resume la estructura completa de un ISP, desde el acceso de los clientes, pasando por la red de core, y la salida hacia el internet.

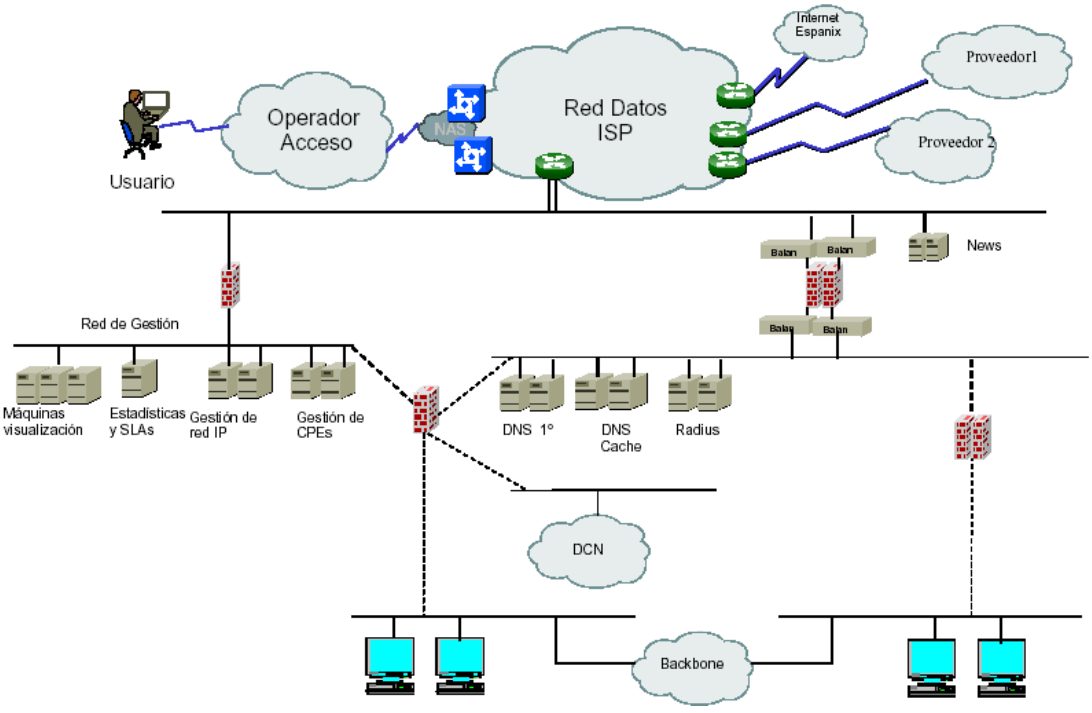


Figura. 1.21 Estructura ISP

CAPITULO 2

LA RED DE ALIANZANET

2.1 INTRODUCCION

Como uno de los puntos fundamentales del presente proyecto de tesis, se hace indispensable describir el estado actual de la red de Alianzanet, en el presente capitulo se presentará una visión global y detallada de la red del ISP Alianzanet, esto dará la pauta y colaborará en gran manera a la identificación de los problemas reales de la red, sus fortalezas debilidades y la posterior selección de la herramienta y solución adecuadas para el aprovechamiento eficiente de los recursos de la misma.

La red WAN de ALIANZANET S.A., basa su espina dorsal en tres segmentos fundamentales (Figura 1.17), que son:

1. Red de Border
2. Red de Core
3. Red de distribución

Estos tres segmentos se reproducen en los dos nodos con los que cuenta la empresa para su operación:

1. NODO CAROLINA (POP ANDINADATOS Carolina)
2. NODO IÑAQUITO (POP ANDINADATOS Iñaquito)

Es importante recalcar que en la actualidad los dos nodos trabajan independientemente, no existe interconexión física ni lógica entre ellos, su administración se realiza de manera remota desde las oficinas de ALIANZANET S.A.

Adicionalmente a esto, los equipos ubicados en los nodos Carolina e Iñaquito, físicamente se hallan constituidos por un solo ruteador CISCO2801 y CISCO1800 respectivamente, equipos que realizan en cada caso las labores de Core, Border y Distribución.

2.2 Red de Distribución

2.2.1 Descripción

Encargada de recoger circuitos virtuales y conexiones de acceso entregadas por el backbone de Andinadatos, en este segmento de la red se realiza la administración directa de los clientes distribuyéndolos entre las diferentes interfaces de acceso que posee el router de acceso de la red.

2.2.2 Componentes

La red de acceso está constituida de dos segmentos de igual importancia:

- La Infraestructura distribuida por toda la ciudad ([30]CNT), la cual sirve de interconexión entre los usuarios y el proveedor, en este caso ALIANZANET S.A., esta infraestructura convive con los dos tipos de ingeniería que utiliza CNT dentro de su ISDN, ATM/Frame Relay y MPLS (reciente).
- Router de Distribución, Acceso o *Edge Router*, es el encargado de anlcar a sus interfaces los enlaces de distribución provistos por CNT, entre los que están enlaces E1y T1 para ATM/FR y enlaces IP para MPLS.

El enlace de acceso es el enlace más importante y de mayor capacidad en la red de acceso, este enlace puede ser de varios tipos y velocidades dependiendo de la capacidad de proveedor (Figura 2.1).

ALIANZANET S.A. cuenta con seis enlaces de acceso distribuidos en los dos Routers de distribución:

Tabla 2.1 Enlaces de Acceso Alianzanet S.A.

ROUTER CISCO2801 (Nodo Carolina)	CAPACIDAD
Enlace ATM/FR E1 (Primera Troncal)	2,048 Mbps
Enlace ATM/FR E1 (Primera Troncal)	2,048 Mbps
Enlace ATM/FR T1/T1 (Tercera Troncal)	1,544 Mbps
Enlace Fast Ethernet (Troncal IP)	100 Mbps
ROUTER CISCO1800(Nodo Iñaquito)	
Enlace ATM/FR T1/T1 (Primera Troncal)	1,544 Mbps
Enlace ATM/FR T1/T1 (Segunda Troncal)	1,544 Mbps

2.2.3 Funcionamiento

La empresa llega hasta sus clientes en un 90% a través de líneas ADSL, este tipo de enlace permite a los clientes disponer de acceso permanente de banda ancha sobre una línea telefónica convencional, es decir un par de cobre diseñado originalmente para transportar canales de voz a 64 Kbps (DS0).

El usuario es provisto de un equipo de cliente CPE (*Customer Premises Equipment*) o módem ADSL.

Los CPE no son más que unidades terminales asociadas a equipos de telecomunicaciones, localizados en el lado del suscriptor y conectados al canal de comunicaciones sea, del proveedor de internet, o del carrier o portador de la información. El carrier en este caso viene a ser Andinadatos constituyéndose como el proveedor de servicios portadores de larga distancia.

En el caso del acceso ATM/Frame Relay el usuario es provisto de un CPE (Customer Premises Equipment) o módem ADSL, este se conecta al punto de terminación telefónica en el lugar designado por el usuario.

En el otro extremo del par de cobre se localiza el DSLAM (Digital Subscriber Line Access Multiplexer), propiedad de CNT, encargado de administrar las conexiones ADSL de nivel físico (capa 1 modelo OSI) y de conmutar las celdas ATM transportándolas hacia y desde la red de acceso, CNT se encarga de establecer un DLCI (Data Link Conection Identifier) entre el DSLAM y el PAI (Punto de Acceso Indirecto) .

Los enlaces de FO dentro del nodo de la empresa se interconectan a través del backbone de CNT con el (PAI), esta pasarela de acceso es conocida como *passport*.

El ISP (ALIANZANET S.A.) se conecta mediante conversores BNC a DB25 en el caso de estos enlaces Frame Relay y T1 dentro de los nodos de la empresa, anclando en sus interfaces seriales los DLCI de cada uno de los clientes.

Para el acceso MPLS el usuario es provisto de un CPE o módem ADSL, este se conecta al punto de terminación telefónica en el lugar designado por el usuario.
En el otro extremo del par de cobre se localiza el IP DSLAM, un equipo 100% IP, propiedad de CNT, encargado de administrar las conexiones ADSL de nivel físico (capa 1 modelo OSI) y de transformarlas en conexiones de capa 2, en este caso se establece una conexión bajo el estándar 801.1q (VLAN) para redes virtuales, CNT establece un canal IP dentro de su red de backbone, entre el IPDSLAM y el Router de Acceso del ISP, esta pasarela IP representa equipos de enrutamiento MPLS sobre líneas SDH, estos son los encargados de encaminar los datos del nivel 2 al nivel 3 de interconexión, nivel donde se establece la VLAN de acceso directa con la red de Alianzanet.

El ISP se conecta mediante conversores SFP a Fast Ethernet (FE), dentro del nodo de la empresa, anclando en sus interfaces FE L3 las VLAN por central, configuradas del lado de CNT.
El Router de Acceso por lo tanto, maneja una alta densidad de enlaces para conexiones T1, E1 y Fast Ethernet, de modo que, en la actualidad, cada tarjeta de línea alberga cientos de circuitos virtuales.

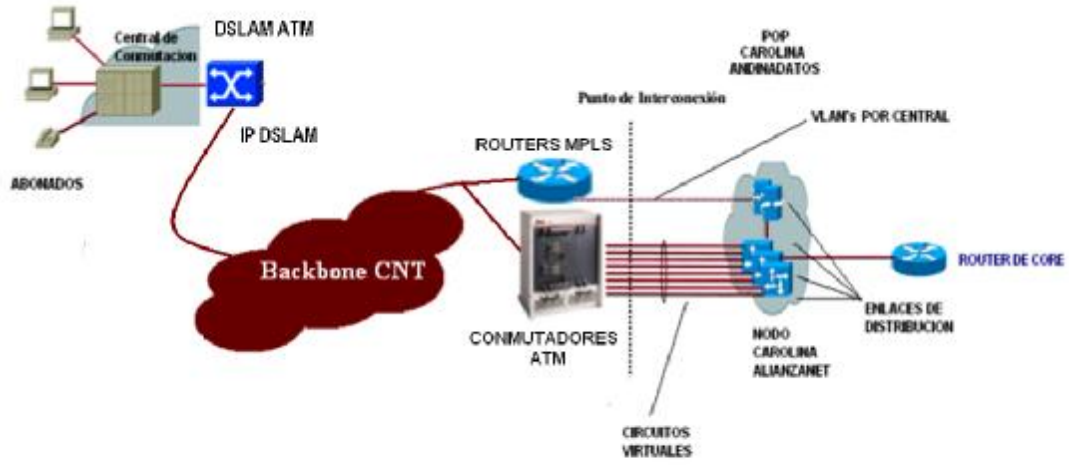


Figura. 2.1 Red de Acceso Nodo Carolina Alianzanet S.A.

2.3 Red de Core

2.3.1 Descripción

La Red de Core es la encargada de tramitar el flujo principal de datos entre las redes de Border y Distribución (Figura 2.2) en esta red se gestionan criterios de compartición, enrutamiento para el acceso desde y hacia la red de core y border además de alojar los servidores de la empresa.

2.3.2 Componentes

Este segmento de la red de ALIANZANET S.A. se compone principalmente de los siguientes elementos:

- Router CISCO 2801 Nodo Carolina Segmento de Core
- Router CISCO 1800 Nodo Iñaquito Segmento de Core
- Centro de Proceso de Datos CPD
    - Gestion y Monitoreo
    - DNS
    - SMTP
    - HOSTING

2.3.3 Funcionamiento

Las tareas para las cuales se halla configurada esta red son las siguientes:

- Enrutamiento estático

ALIANZANET => ANDINADATOS

ALIANZANET => RED DE DISTRIBUCION CNT.

- Traducción de direcciones NAT (Network Adress Translation), de la red privada hacia la red pública representada por la salida internacional.

MAN (*Metropolitan Area Network*) => SALIDA INTERNACIONAL

- Segmentación del canal de salida entre los usuarios de los diferentes circuitos virtuales gestionados por la red de acceso, principalmente en modulación TDM donde cada host obtiene la misma ranura de tiempo en la trama TDM. Estadísticamente nunca el 100% del número de usuarios de la red, emitirá peticiones de acceso al canal de salida (Salida Internacional) al mismo tiempo durante todo el día, a esto se le conoce como multiplexación estadística.

2.3.3.1 Centro de Proceso de datos. Esta es una parte esencial de la red de CORE ya que alberga los servidores de gestión de red IP, gestión de equipos de cliente, DNS, SMTP.
Todos ellos se constituyen como sistemas de elevada disponibilidad y altamente escalables.
El CPD (Centro de Proceso de Datos) se conecta a la red de core a través de una pasarela *Fast Ethernet* y de un switch capa 2, donde se encuentran conectados los servidores parte del CDP, estos servidores albergan, valga la redundancia, los siguientes servicios:

- *Servidor de nombres DNS,* servicio crítico de la red encargado de la resolución de nombres de internet, este se encuentra configurado sobre un sistema Linux Ubuntu 8.04 y protegido contra intrusos y ataques externos por SNORT Y SELINUX, un sistema de detección de intrusos y un firewall de sofware basado en IPTABLES respectivamente.
- *Servidor de correo saliente smtp,* servidor encargado de tramitar el envio de correo electrónico desde la red de Alianzanet S.A. hacia el exterior, sin importar el dominio y el tipo de cuenta que utilice el usuario para llevar a cabo esta tarea. El servidor se halla configurado en un servidor Linux Ubuntu 8.04, para trabajar con el puerto estándar para dicho protocolo, el puerto 25, su configuración permite agregar usuarios a una lista de

accesos, por dirección IP, listando aquellos host dentro de la red de Alianzanet que tendrán acceso al servidor SMTP.

- *Servidor de Hosting*, encargado de administrar y albergar dominios de correo electrónico a clientes que así lo requieran, se halla configurado en un servidor Linux Ubuntu 8.04, el programa ZIMBRA es el encargado de crear y administrar las cuentas de los usuarios en los diferentes dominios.

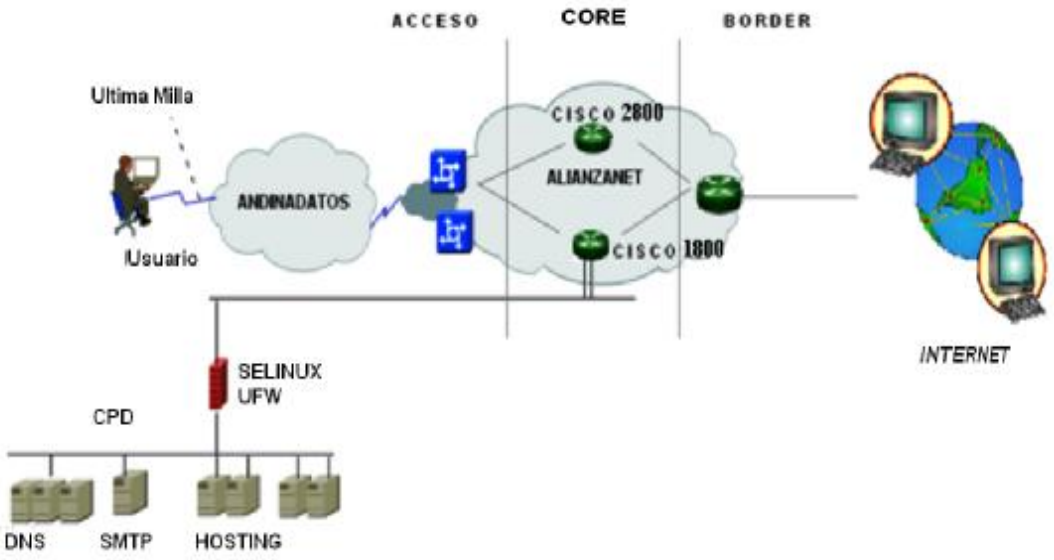


Figura. 2.2 Red de Core Alianzanet S.A.

2.4 Red de Border

2.4.1 Descripción

Esta red es la encargada de encaminar todo el trafico entregado por la red de core desde y hacia el internet (Figura 2.3) la red de border gestiona los enlaces de salida de la empresa se halla conectada a la red multi servicios de CNT, su componente principal es el router de border.

2.4.2 Componentes

Esta red ésta compuesta por los siguientes elementos puntuales:

- Router CISCO 2801 Nodo Carolina.
- Router CISCO 1800 Nodo Iñaquito.
- Canal Internacional.

2.4.3 Funcionamiento

La parte más importante y el cerebro de la red de Border es el router de border RB, mismo que, usando el protocolo EGP (*Exterior Gateway Potocol*) BGP, se encarga de comunicarse con el resto de routers "vecinos", intercambiando tablas de rutas y garantizando a la vez bucles libre de acceso para el trafico ip entregado por la red de Core.

El canal internacional constituye el enlace de acceso a internet, la capacidad de este enlace, así como su configuración se halla detallada en la siguiente tabla:

Tabla 2.2 Border Alianzanet

NODO	ROUTER	INTERFAZ	CAPACIDAD
CAROLINA	CISCO 2801	FastEthernet 0/1	6,144 Mbps (3 E1)
IÑAQUITO	CISCO 1800	FastEthernet 0/0	3,072 Mbps (1 E1 + 1024 Kbps)

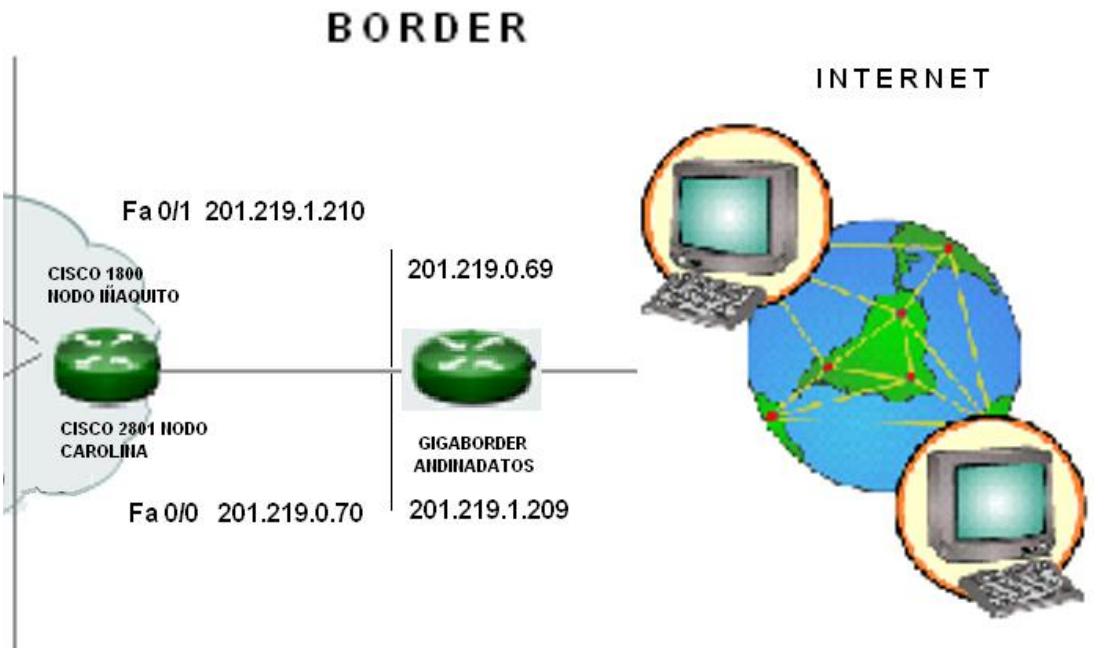


Figura. 2.3 Red de Border Alianzanet S.A.

2.5 Segmentos de Red

2.5.1 Introducción

En este punto del desarrollo es importante mencionar el hecho de que, por políticas de la empresa, se ha decidido orientar una parte del monitoreo, solo a aquellos clientes que generan altos réditos para la empresa, es el caso de los enlaces corporativos más importantes que maneja la empresa en la actualidad, la compresión de su importancia, así como la de su topología y demás datos informativos, marcará la pauta para la correcta comprensión, de la implementación y configuración de las herramientas.

Los clientes en este caso corporativos de la empresa se dividen en tres grupos:

- Empresas
- Conjuntos y Edificios

2.5.2 Empresas

A continuación se detallarán los host y servicios creados para el monitoreo de este grupo de clientes corporativos. Este grupo está conformado por enlaces con alto consumo de recursos dentro de la red, caracterizados por ciertos parámetros fundamentales:

- Anchos de banda superiores a los 512 Mbps en compartición 1:1.
- Rangos de direcciones IP públicas dentro de subredes con mascaras de 30 y 29 bits.
- Un flujo de tráfico preferentemente durante horas de oficina.
- Ultima Milla sustentada en enlaces de cobre o fibra óptica, anclados a la red de Alianzanet por medio de ruteadores marca CISCO brindando la ventaja de ser monitoreados y administrados vía protocolo SNMP.

2.5.2.1 Empresa Metropolitana Quito Turismo. El acceso a internet junto con los sistemas OTRS, Samba, NTOP, Cacti, fueron configurados por Alianzanet sobre un servidor basado en GNU/Linux, este servidor se halla también dentro del futuro plan de monitoreo, actualmente no se encuentra monitoreado. Cabe recalcar que estos sistemas son parte fundamental de la gestión de la red y sistemas involucrados con la labor de la empresa.

A continuación se detallan los datos más relevantes del enlace, así como un diagrama del acceso.

Tabla 2.3 Enlace EMQT

Ultima milla (Capa Física)	Fibra Óptica monomodo
Carrier	Telconet
Ancho de Banda	2048 Kbps
Compartición	1:1
Perta de Enlace	186.3.3.129
CPE	CISCO SERIE 800
Ubicación	El Dorado (Quito)

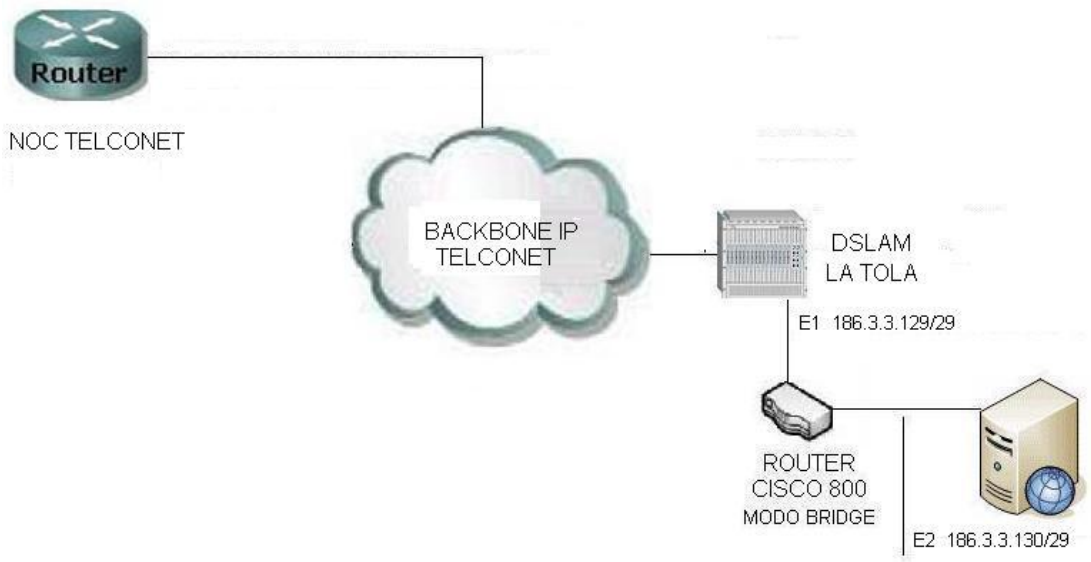


Figura. 2.4 Topología de Acceso EMQT

2.5.2.2 Broker Tecnológico Pedro Vicente Maldonado. Andinadatos se encarga de configurar una ruta simétrica desde el cliente ubicado en la población de Pedro Vicente Maldonado hacia la troncal metro de Alianzanet, sustentada para el acceso lógico, sobre una interfaz VLAN levantada sobre una de las interfaces Capa 3 Fast Ethernet, en el nodo Carolina de la empresa.

A continuación se detallan los datos más relevantes del enlace, así como un diagrama del acceso.

Tabla 2.4 Enlace PVM

ULTIMA MILLA (CAPA FISICA)	Cobre
CARRIER	Andinadatos
ANCHO DE BANDA	1024 Mbps
COMPARTICIÓN	1:1
PUERTA DE ENLACE	201.219.36.89

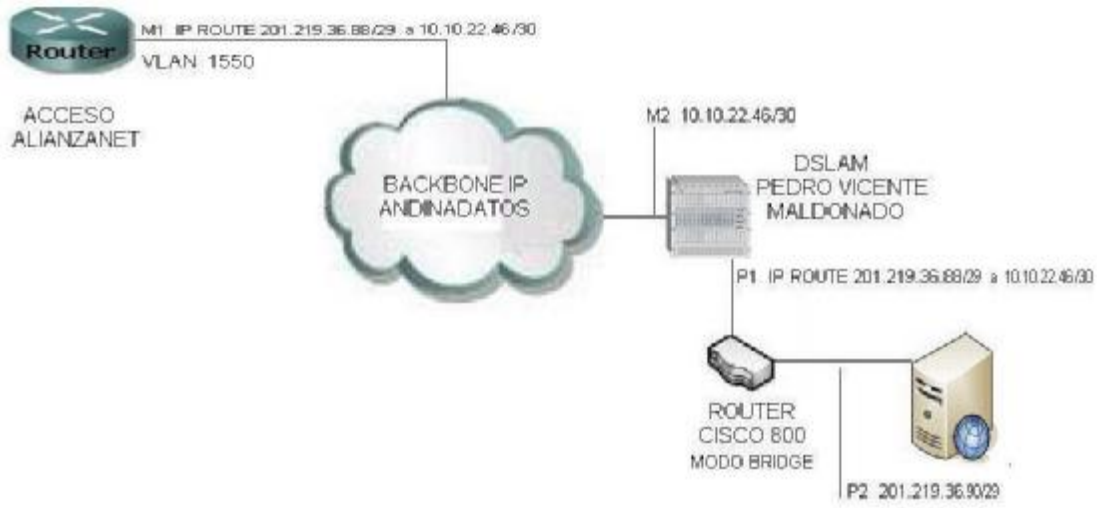


Figura. 2.5 Topología de Acceso PVM

2.5.2.3 WISP El Puyo. Alianzanet se encarga de configurar una ruta estática desde su red de acceso hacia el backbone IP de Andinadatos, sustentada sobre una VLAN, configurada en la interfaz FastEthernet 0/0 (Capa 3) del router de Acceso de Alianzanet , ubicado en el nodo Carolina de la empresa.

Su topología es similar a la mostrada para el enlace de PVM, la diferencia radica en la configuración lógica del enlace, ya que no existe una ruta simétrica desde el cliente hacia la red de acceso de Alianzanet, esto debido a que la dirección IP configurada para este enlace es privada y no pública.

Adicionalmente a esto, Alianzanet administra la red del cliente de manera remota, a través de un servidor configurado sobre GNU/Linux, mismo servidor que se halla listado como parte de los servidores Linux administrados por la empresa. Este servidor no se encuentra monitoreado en los actuales momentos.

Tabla 2.5 Enlace WISP EL Puyo

ULTIMA MILLA (CAPA FISICA)	Cobre
CARRIER	Andinadatos
ANCHO DE BANDA	1024 Mbps
COMPARTICIÓN	1:1
PUERTA DE ENLACE	192.168.61.1
CPE	CISCO SOHO 800
UBICACIÓN	EL PUYO

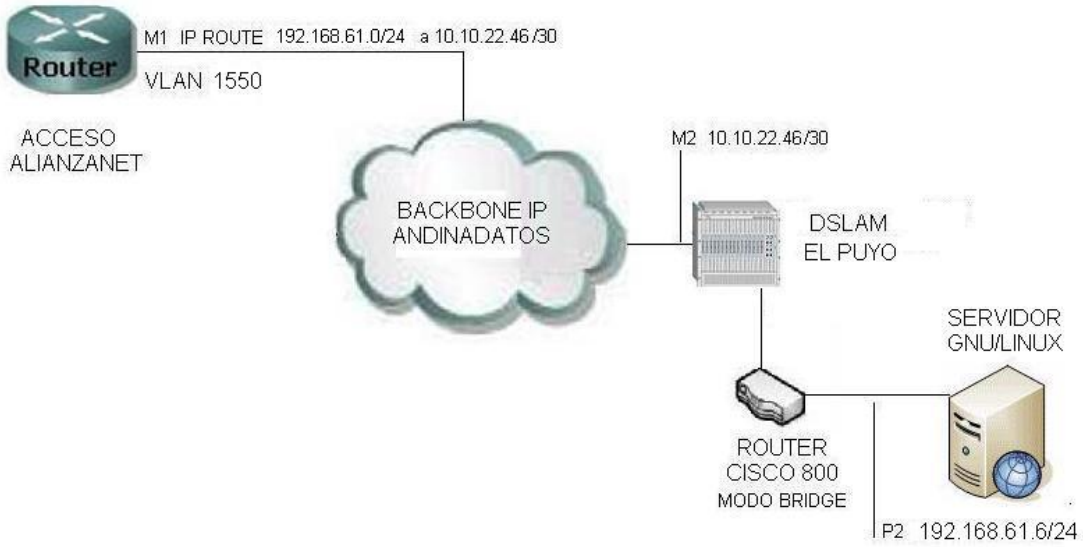


Figura. 2.6 Topología de Acceso WISP El Puyo

2.5.2.4 Centro Ferretero Cano Lastra. Alianzanet provee a este cliente de un enlace ADSL para el acceso en Tumbaco, y de un enlace de radio para sus oficinas en Puembo, además de administrar un Red Privada Virtual (VPN) entre estas dos oficinas.

Tabla 2.6 Enlace CL

ULTIMA MILLA (CAPA FISICA)	Cobre
CARRIER	Andinadatos
ANCHO DE BANDA	1024 Mbps
COMPARTICIÓN	1:2
PUERTA DE ENLACE	201.219.36.109
CPE	CISCO SOHO 800
UBICACIÓN	TUMBACO / PUEMBO

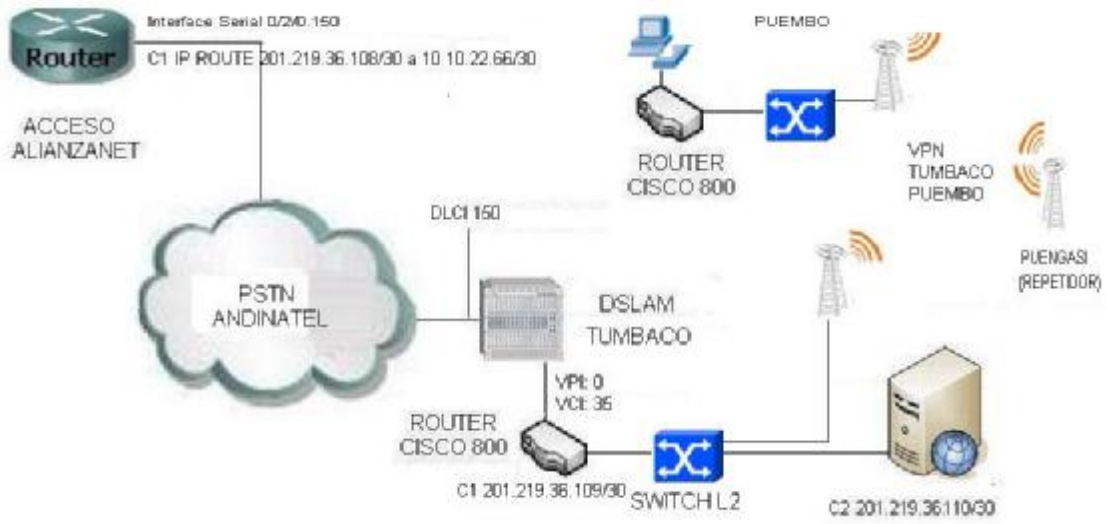


Figura. 2.7 Topología de Acceso CL

2.5.3 Conjuntos y Edificios

Alianzanet cuenta con los siguientes enlaces que cumplen con estas características:

- Edificio Zuko
- Edificio Kigman
- Edificio Banco de Guayaquil
- Edificio Torrenova
- Conjunto Altavista
- Conjunto El Alcazar
- Conjunto Puerta de Hierro
- Conjunto Conquistadores

2.5.3.1 Descripción. Alianzanet cuenta con un número moderado de enlaces, a través de los cuales se conectan más de un único usuario, este es el caso de los edificios y conjuntos habitacionales, dentro de los cuales, y dadas las condiciones que estos brindan, es factible instalar un enlace dedicado, y a través de una red de cableado estructurado, llevar el internet a todos y cada uno de los domicilios, sean estos casas contiguas o departamentos, dentro del edificio o conjunto habitacional

La importancia de monitorear estos enlaces, no solo estriba, al igual que en el caso de los enlaces corporativos, en el rubro que representa la facturación de los mismos para la empresa, sino el hecho de que todos y cada uno de los clientes del mencionado conjunto o edificio, dependen de un único enlace, por lo que, al presentarse inconvenientes en este, no solo se ve afectado un cliente, sino el conjunto entero.

Este grupo está conformado por enlaces con un moderado consumo de recursos dentro de la red, caracterizados por ciertos parámetros fundamentales:

- Anchos de banda superiores a los 512 Mbps en compartición 4:1.
- Un flujo de tráfico preferentemente durante las horas de la tarde y noche, estos enlaces se hallan instalados dentro de soluciones habitacionales preferentemente dedicadas a vivienda.
- Ultima Milla sustentada en enlaces de cobre, anclados a la red de Alianzanet por medio de un CPE estándar, que actúan simplemente como enlace, dejando la carga de la red, NAT y filtrado de direcciones MAC, a un ruteador configurado para estas tareas.
- Una red de cableado estructurado, cubriendo todos y cada uno de los puntos donde se hallan conectados los clientes, sobre topologías tipo anillo para los conjuntos y estrella para los edificios.

A diferencia de lo echo para los enlaces corporativos, se presentará a continuación las dos clases de topología que manejan este tipo de enlaces (Figuras 2.5 y Figura 2.6), tanto por el lado WAN de la red, como en el lado LAN de la misma, haciendo énfasis en la parte WAN del enlace, motivo de este proyecto de tesis.

Las Figuras 2.5 y 2.6 describen de manera esquemática la topología de red implementada tanto en los conjuntos habitacionales como en los edificios administrados por Alianzanet. Una ruta estática hacia dentro de la red es configurada en el router de acceso parte de la red de acceso de Alianzanet, esta ruta cumple con dos objetivos:

1. *Permitir el acceso*, vía interfaz web, a los ruteadores encargados de administrar y dar el acceso a los clientes, dentro de dichas soluciones habitacionales.
2. *Establecer un enlace directo* entre el router de acceso y la red LAN del conjunto, con el fin de configurar una lista de acceso (*Access-list*) para cargar el trabajo de la traducción de direcciones NAT (*Network Address Translation*), proceso que imprime un trabajo bastante pesado para un equipo estándar como el configurado en este tipo de enlaces.

2.5.3.2 Diagramas de red. A continuación se adjunta los correspondientes diagramas, en los dos casos no solo se describe el acceso WAN, sino se ilustra esquemáticamente el diagrama de la red LAN.

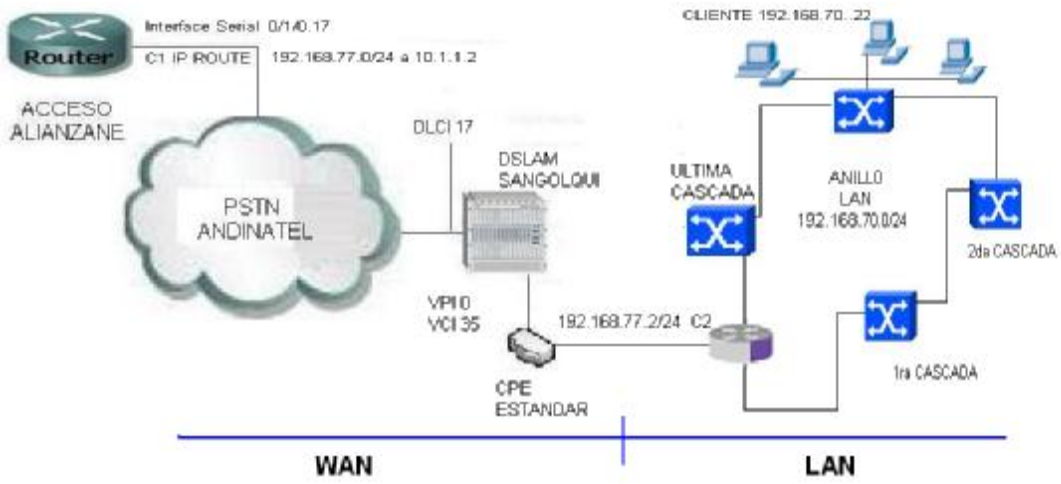


Figura. 2.8 Ejemplo de Topología LAN y WAN Conjunto El Alcázar

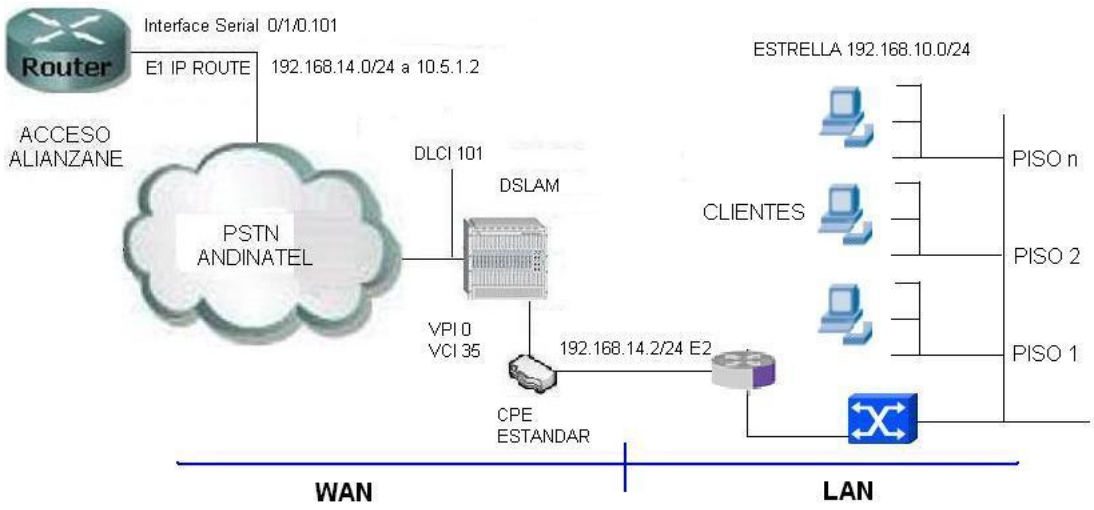


Figura. 2.9 Ejemplo de Topología LAN y WAN Edificio ZUKO

CAPITULO 3

IMPLEMENTACION DE LAS HERRAMIENTAS

3.1 INTRODUCCION

Desde los albores de las administración de redes y recursos compartidos, los administradores de redes de comunicaciones, tanto a nivel local en pequeñas y medianas empresas, como a nivel extendido, metropolitano, regional e internacional, se han visto en la necesidad de monitorizar, realizar un seguimiento del escenario administrado, de manera automática y eficaz, con el fin de atenuar o erradicar en su totalidad, problemas presentes en el estado del arte de los mismos, como lo son los cuellos de botella, protocolos y puertos no permitidos o restringidos, y por otro lado, monitorizar con el fin de planear el crecimiento o migración de la red, a nuevas y más amplias tecnologías.

Este reto del administrador de red se detalla en ciertos importantes puntos, presentados a continuación:

- Incremento de la velocidad, protocolos y tecnologías dentro de la red.
- La interconexión de diferentes tipos de equipos, sistemas y servicios, entrando en un tema de reserva de canal para determinado trafico específico.
- Los usuarios se encuentran en capacidad de administrar su propio PC, con cierto grado de independencia, lo cual aumenta el riesgo y la inseguridad de la red en general.
- La ardua labor que involucra dar seguimiento desde una perspectiva globalizada, a una red donde se ruedan subredes, VPN, VLAN, etc. Con restricciones especificas para cada segmento de red.

Existen un sinnúmero de herramientas disponibles en el campo de las telecomunicaciones, y específicamente en el ámbito de las redes basadas en conmutación de paquetes, para el monitoreo de redes tanto de tipo local o LAN como redes de área extendida y metropolitana WAN y MAN respectivamente.

La alternativa que en este caso presenta este trabajo de tesis, incluye un requisito indispensable, planteado como un objetivo personal; sea cual fuere la herramienta o herramientas escogidas para cumplir el objetivo general de este trabajo de tesis, dicha herramienta, debe ser desarrollada utilizando software de código abierto basado en GNU (*General Public License*).

3.2 Análisis de las Herramientas

De la amplia variedad de herramientas que ofrece la Fundación para el desarrollo de Software Libre FSF (*Free Software Foundation*), tres han sido las escogidas para entrar en el proceso de análisis y selección de la o las soluciones idóneas, para alcanzar el objetivo principal de este proyecto de tesis. Tomado en cuenta los reconocimientos y las recomendaciones publicadas por las diferentes entidades y grupos, alrededor del mundo, desarrolladores y usuarios, afiliados a la FSF, estas herramientas son:

- *Nagios de Nagios Enterprises*, software ampliamente modular e integral, para el monitoreo y administración de redes LAN, MAN, WAN, etc.

- *MRTG*, *The Multi Router Traffic Grapher*, software basado en el protocolo SNMP principalmente, para la visualización a través de gráficos, del consumo de ancho de banda presente en todas las interfaces del equipo al cual se esté apuntando.

- NTOP, *The network TOP*, herramienta basada en un sniffer de red, para el análisis estadístico y pormenorizado de los protocolos, hosts, consumo y comportamiento, presentes en la interfaz de red física sobre la cual se halla implementado.

3.2.1 Nagios

Nagios se constituye como una herramienta para el monitoreo de sistemas y redes de computadoras.

Nagios fue diseñado como una plataforma extremadamente solida para el monitoreo, organización y alerta de las diferentes redes y sistemas antes mencionados.

Nagios integra sobre esta pasarela, una variedad de poderosas herramientas, el aprovechamiento al máximo de estas herramientas y sistemas no solo involucra el entender como Nagios funciona, sino el comprender y analizar de manera detenida, cual es el trabajo que desempeña el sistema que se va a monitorear, esta relación es extremadamente importante, ya que Nagios como herramienta no es una fuente de conocimiento sobre la

complejidad del sistema a monitorear, sino que, se constituye en una herramienta casi indispensable, para entender dicha complejidad.

Figura. 3.1 Logo del Proyecto Nagios de *Nagios Enterprises*

3.2.1.1 Características del sistema. Algunas de las características con las que cuenta Nagios se enumeraran a continuación:

- Monitoreo de recursos de sistema en servidores de red.
- Carga del procesador.
- Consumo de recursos de disco.
- Uso de memoria de procesos RAM.
- Estado de servicios críticos (EXPLORER.EXE, SMTP, POP3, HTTP, SSH, DNS, SAMBA, etc.).
- Monitoreo bases de datos MySQL, Postgres, Oracle, SQL Server etc.
- Monitoreo de equipos de red activos, hosts, (Switch, Router, Hubs, CPE, NetWare, etc.).
- Monitoreo de Equipos compatibles con IP (Impresoras IP, Cámaras CCTV, Sensores de proximidad, temperatura, iluminación IP).
- Notificación y Alerta personalizadas, del estado de hosts, sistemas y servicios en caso de presentarse inconvenientes en los mismos, a través de diferentes sistemas de comunicación (E-mail, Pagers, SMS a teléfonos móviles, Alertas Sonoras, Gráficas o definidas por el usuario).
- Diseño de Plugins totalmente personalizables para adaptar el sistema acorde a nuestras necesidades.
- Habilidad para definir jerarquías y relaciones entre los diferentes hosts, sistemas y servicios de red.
- Detallado informe gráfico y textual, diario, semanal, mensual, etc., del comportamiento de los sistemas a monitorizarse.

- Integración y compatibilidad con otras herramientas de monitoreo para trabajar al servicio de Nagios.
- Publicación de mapas de red, alertas gráficas y configuración a través de su servidor WEB apache2 incluido, con validación de contraseñas y usuarios.

NAGIOS se vale de una amplia gama de herramientas para cumplir con las especificaciones de monitoreo del usuario, la información recopilada por tal o cual herramienta, entregada a NAGIOS, es procesada e interpretada por este, con el fin de tomar decisiones, ejecutando scripts, desarrollados por el usuario, para corregir determinado inconveniente en la red.

NAGIOS no está diseñado para realizar tareas específicas como muchos otros sistemas, a diferencia de estos, NAGIOS no se constituye como una simple herramienta, sino como un elaborado sistema de administración de red, todas los sistemas de monitoreo que se implementen sobre la red, pueden ser administrados por NAGIOS, toda la información que estos generen será almacenada por NAGIOS, para su posterior análisis y notificación al administrador de la red.

3.2.1.2 Requerimientos del sistema. En cuanto al *Hardware* cualquier equipo capaz de ejecutar una variante de Unix , sin necesidad de instalar un entorno gráfico:

Tabla 3.1 Requerimientos de Hardware implementación Nagios

REQUERIMIENTOS MINIMOS	RECOMENDADO
PC Torre Estándar AT	Servidor Torre o Rack
Intel CELERON-AMD Sempron 2.0 GHz	Intel Core2Quad 2.0 Ghz
512 MB RAM	1 GB RAM
5 GB de espacio libre en disco duro	10 GB de espacio libre en disco
NIC 10/100 BASE-T, dependiendo del entorno	NIC 100/1000 BASE-T

En cuanto al software el sistema operativo debe estar basado en una variante de Linux Kernel 2.6.x, se recomienda cualquiera de estas tres distribuciones:

- Fedora Core 7 al 11 ultimo *release*
- Ubuntu 7.10 Gutsy Gibbon al 9.04

- OpenSuse 10.03 al 11.1

Para los cuales no es necesario instalar el servidor gráfico XORG, lo cual ahorra recursos de memoria de procesos.

Nagios se encuentra bajo el amparo de GNU (*General Public License*) versión 2 publicada por la *Free Software Foundation*. Esto entrega al usuario de Nagios el PERMISO LEGAL DE COPIAR, DISTRIBUIR Y/O MODIFICAR NAGIOS BAJO CIERTAS CONDICIONES.

3.2.1.3 Porque usar Nagios. Existe una verdadera comunidad internacional de miembros, participando en la promoción, soporte y desarrollo de Nagios, aportando con:

- Plugins, aplicaciones adicionales y extensiones, que multiplican las capacidades de Nagios.
- Páginas Web fuentes de información, trucos, consejos y soporte técnico totalmente libre de recargos.
- Conferencias y Talleres para promover Nagios alrededor del mundo.

Nagios ha sido descargado de su sitio web oficial en más de 2 millones de ocasiones, ha llegado a convertirse en la solución industrial estándar, para el monitoreo de redes, sistemas y aplicaciones. La comunidad Nagios ha jugado un papel protagónico en el crecimiento de esta poderosa herramienta.

En conclusión, Nagios se constituye como una excelente desición, al momento de implementar un sistema de monitoreo, sus mayores fortalezas radican en:

Sistema de Código Abierto

- Robusto y Confiable
- Altamente configurable, desarrollado en Perl
- Modular
- Desarrollo y Evolución Constantes
- Una amplia comunidad en constante ampliación y desarrollo
- Compatible con cualquier sistema operativo basado en Unix

3.2.2 MRTG *Multi Router Traffic Grapher*

MRTG (Multi Router Traffic Grapher) se define como una aplicación para el manejo de redes, capaz de monitorear cualquier equipo de red remoto con soporte [31]SNMP (*Simple Network Management Protocol*) habilitado.

MRTG, como una herramienta basada en SNMP, envía solicitudes SNMP al equipo de red de acuerdo a un patrón de tiempo configurable.

MRTG fue originalmente diseñado para visualizar el consumo de ancho de banda, es decir, la carga de tráfico en un enlace de red. MRTG genera imágenes dinámicas en formato png representando el valor a lo largo del tiempo de la variable monitorizada. En la actualidad, MRTG puede adquirir información sobre cualquier [32]OID de SNMP para, basándose en esto, graficar el cambio de estos valores en el tiempo, en su versión mas reciente, puede implementarse para hacer un seguimiento del valor de cualquier variable a lo largo del tiempo, como el número de mensajes por minuto que envía o recibe un servidor SMTP, el número de usuarios simultáneos de un paquete de software con licencia, o el número de plazas libres de un aparcamiento, etc. MRTG puede recolectar información numérica, para proveer esta información a cualquier otra herramienta que así lo requiera.

Figura. 3.2 Logo del Proyecto MRTG

3.2.2.1 Características del sistema. MRTG posee un sinnúmero de beneficios entre los cuales los más relevantes se detallan a continuación.

- Seguimiento del valor de cualquier variable a lo largo del tiempo.
- Monitorea la carga de tráfico en enlaces de red.
- Monitoreo el ancho de banda consumido por un determinado protocolo.
- Trabaja especialmente con OID’s de SNMP.

31 SNMP: Protocolo simple para el manejo y administración de equipos en redes TCP/IP, se basa en el intercambio de mensajes con información de las diferentes variables parte del sistema cliente, del cual se quiere administrar.
32 OID: Identificador de Objeto, parte de la estructura de SNMP, provee de l información de identificación de las variables del sistema.

- Muestra de manera automática el consumo de las diferentes interfaces identificándolas por dirección IP por la descripción de dicha tarjeta.
- Plasma gráficos dinámicos diarios, semanales y mensuales, con un intervalo mínimo de 5 minutos entre cada muestra, en formato PNG, sus archivos LOG, en los cuales se recolecta la información de todas las interfaces, de manera periódica, basan su almacenamiento en un eficiente algoritmo de actualización, lo cual hace que estos archivos LOG, no aumenten de tamaño de manera desmesurada, consumiendo recursos en disco duro.
- Posee compatibilidad y soporte para *counters* SNMPv2c de 64bits.
- Publica las gráficas en formato HTML sobre cualquier servidor WEB preferentemente apache y apache2.

3.2.2.2 Requerimientos del sistema. En cuanto al *hardware* MRTG se caracteriza por ser un aplicativo bastante liviano, los recursos que consumo tanto en almacenamiento como en memoria de proceso son bastante bajos, podría decirse que prácticamente cualquier PC con requerimientos mínimos y una tarjeta de red está en condiciones de albergar a MRTG, en ese caso los requerimientos del hardware estarían supeditados a los necesarios para instalar la distribución de Linux.

Tabla 3.2 Requerimientos de Hardware implementación MRTG

REQUERIMIENTOS MINIMOS	RECOMENDADO
PC Torre Estándar AT	Servidor Torre o Rack
Intel CELERON-AMD Sempron 2.0 GHz	Intel Core2Quad 2.0 GHz
256 MB RAM	1 GB RAM
1 GB de espacio libre en disco duro	10 GB de espacio libre en disco
NIC 10/100 BASE-T, dependiendo del entorno	NIC 100/1000 BASE-T

Por el lado del *Software* el sistema operativo debe estar basado en una variante de Linux Kernel 2.6.x, esto tomando en cuenta uno de los objetivos principales del proyecto, MRTG puede ser implementado sobre sistemas basados en Win32, para el presente proyecto se recomienda cualquiera de estas tres distribuciones:

- Fedora Core 7 al 11 ultimo *release*

- Ubuntu 7.10 Gutsy Gibbon al 9.04
- OpenSuse 10.03 al 11.1

Para los cuales no es necesario instalar el servidor gráfico XORG, lo cual ahorra recursos de memoria de procesos. MRTG como todo sistema basado en código abierto, se encuentra bajo el amparo de GNU (*General Public License*) versión 2 publicada por la *Free Software Foundation*. Esto entrega al usuario de Nagios el PERMISO LEGAL DE COPIAR, DISTRIBUIR Y/O MODIFICAR NAGIOS BAJO CIERTAS CONDICIONES.

3.2.2.3 Porque usar MRTG. MRTG es una aplicación para el monitoreo de la variación de cualquier recurso en un sistema, en el dominio del tiempo, con un consumo de memoria, procesador y ancho de banda en el servidor bastante bajos, adicionalmente a esto:

- Es portable, trabaja con la mayoría de plataformas UNIX.
- Desarrollado en Perl, lo que lo hace 100% personalizable.
- Usa una implementación portable de SNMP sin necesidad de paquetes SNMP adicionales.
- Posee soporte para SNMPv2c
- Útil identificación de las interfaces por IP y descripción.
- Archivos LOG de tamaño constante
- Configuración automática a través de herramientas para implementación.
- Alto desempeño
- Interfaz WEB altamente configurable
- Desarrollo de la herramienta *RRDtool* core de MRTG para recolección de información numérica.

3.2.3 NTOP

NTOP es una poderosa herramienta específica, flexible y extensible, basada en código abierto, para medición y monitoreo de tráfico, con soporte para varias actividades relacionadas con el manejo, optimización e incluso planeamiento de capacidades y seguridades dentro de una red. El hecho de estar basado en código abierto, no implica que todo su código sea susceptible a modificación, esto debido a que los primeros

Desarrolladores fueron fuertemente influenciados por la arquitectura de [33]WEBBIN, conservando el núcleo de funcionamiento de NTOP, sobre ciertas aplicaciones fijas, es decir, no modificables.

3.2.3.1 Características del sistema. NTOP captura los paquetes que circulan dentro de la red ([34]*Sniffer*), ofreciendo un informe detallado sobre el resultado de tal captura.
Algunas de las tareas realizadas por NTOP son:

- Análisis y medición del trafico de la red
- Caracterización de los protocolos involucrados en el flujo generado por los host
- Qué hosts se hallan en la cima del consumo de tráfico ([35]*Top Talkers*, picos/storms, número de peticiones)
- Qué servidores, fuera de la red, contactan con mayor frecuencia los hosts.
- Que hosts del exterior han intentado, sea con o sin exito, utilizar servicios o recursos dentro de nuestra red.
- Captura de paquetes y demultiplexación, independiente del sistema operativo, (el mismo código debe correr sin cambios en diferentes las plataformas) o de la interfaz de red NIC usada para la captura de los paquetes.
- Servidor Web incluido para la visualización del tráfico, sin la necesidad del uso de clientes ad-hoc.

Figura. 3.3 Logo del Proyecto NTOP

3.2.3.2 Requerimientos del sistema. El sistema es extremadamente liviano, portable y poderoso, en contraposición con otras herramientas, demasiado simples (iptraf, netsniffer, etc.) o altamente consumidoras de recursos en el servidor, por lo que es susceptible a ser implementado en virtualmente cualquier ordenador con características mínimas de disco duro, memoria, procesador y tarjeta de red, dependiendo del entorno en donde se lo quiera implementar.

33 WEBBIN: Herramienta basada en código abierto para administración y provisión de servicios de red.
34 Sniffer: Herramienta para captura de tramas para redes que ruedan sobre TCP/IP.
35 *Top Talkers:* En redes de computadoras, se refiere al grupo de hosts con mayor cantidad de tráfico de protocolos dentro de la red.

Tabla 3.3 Requerimientos de Hardware implementación NTOP

REQUERIMIENTOS MINIMOS	RECOMENDADO
PC Torre Estándar AT	Servidor Torre o Rack
Intel CELERON-AMD Sempron 2.0 GHz	Intel Core2Quad 2.0 GHz
256 MB RAM	1 GB RAM
1 GB de espacio libre en disco duro	10 GB de espacio libre en disco
NIC 10/100 BASE-T, dependiendo del entorno	NIC 100/1000 BASE-T

Por el lado del *Software* el sistema operativo debe estar basado en una variante de Linux Kernel 2.6.x, esto tomando en cuenta uno de los objetivos principales del proyecto, NTOP puede ser implementado también sobre sistemas basados en Win32, para el presente proyecto se recomienda cualquiera de estas tres distribuciones de GNU/Linux:

- Fedora Core 7 al 11 ultimo *release*
- Ubuntu 7.10 Gutsy Gibbon al 9.04
- OpenSuse 10.03 al 11.1

Cabe recalcar que NTOP comparte la filosofía de UNIX; unir variadas y diferentes aplicaciones, para trabajar en conjunto al servicio de un kernel, es el kernel el llamado a manejar y administrar esta cooperación, con el fin de liberar la carga a la aplicación, para que esta concentre sus requerimientos de consumo (disco y procesador) en la tarea para la que fue diseñada, y no en la complejidad misma de la herramienta. Esto provee una modularidad inigualable a las herramientas basadas en código abierto, específicamente en el caso de NTOP, solo las aplicaciones y herramientas necesarias serán activadas por el usuario, de acuerdo a la tarea que desee implementar, sin desperdiciar ciclos de máquina en ejecutar tareas innecesarias.

3.2.3.3 Porque usar NTOP. Las bondades de NTOP son variadas, aquí se listan algunas de las más importantes a modo de resumen:

- Simple, eficiente, portable, poderoso.

- El objetivo de NTOP es desarrollar un kernel simple y eficiente capaz de manejar tareas generales vinculadas al monitoreo de red.
- Bajo consumo de recursos (memoria y CPU), pero capacidad para explotarlos de ser necesario.
- Habilidad para el manejo y monitoreo de red de manera remota, sin la necesidad de correr aplicaciones específicas para analizar la información.
- Capacidad para presentar los datos tanto en modo texto como vía web, de manera sencilla y fácil de interpretar.
- Susceptible a implementar herramientas adicionales desarrolladas por el usuario.

3.2.4 Análisis comparativo

A continuación, se detalla un cuadro comparativo sobre los aspectos más importantes de las herramientas analizadas anteriormente.

Tabla 3.4 Análisis Comparativo

ANALISIS COMPARATIVO SOBRE LAS HERRAMIENTAS DE MONITOREO			
CARACTERISTICAS	NAGIOS	MRTG	NTOP
Acceso vía web	V	V	V
Alertas personalizadas sobre problemas en la red	V	x	x
Compatibilidad SNMP	V	V	V
Administración autónoma de la red (toma de decisiones)	V	x	x
Historial del consumo de ancho de banda	V	V	V
Historial de Tráfico TCP/UDP	V	x	V
Implementación sobre paquetes Win32	V	V	V
Mapa personalizado del estado de la red	V	x	x
Monitoreo de sistemas no basados en TCP/IP	V	V	x
Modular	V	x	V
Monitoreo LAN	V	V	V
Monitoreo WAN	V	V	x

Tabla 3.5 Análisis Cualitativo

ANALISIS CUANTITATIVO DE LAS HERRAMIENTAS			
PARÁMETRO	GRADO		
Compatibilidad con otras herramientas de red	ALTO	MEDIO	BAJO
Dificultad para la implementación	ALTO	MEDIA	BAJO
Grado de Personalización	ALTO	ALTO	MEDIO
Estabilidad	ALTO	MEDIO	MEDIO
Historial General de la red	ALTO	BAJO	ALTO

Del análisis de las herramientas detallado anteriormente, existen parámetros con los que la herramienta seleccionada deberá contar, para cumplir con las expectativas de una red de servicios de internet, entre los cuales los más importantes son:

- Modularidad
- Escalabilidad
- Compatibilidad con otras herramientas
- Estabilidad
- Acceso y control remotos
- Notificación y Alerta del estado de la red en tiempo real
- Mapa Activo de la red
- Historial de la red
- Detalle minucioso del tráfico de la red.
- Alto nivel de personalización

No existe en la actualidad un sistema que realice todas las tareas que competen al monitoreo, de manera autónoma e independiente, si bien es cierto, unas herramientas mejor que otras, cumplen con ciertos parámetros de los antes mencionados, ninguna lo hace de manera total, por lo que la compatibilidad, modularidad y nivel de personalización, se convierten en factores preponderantes, ya que, al no contar con una herramienta que realice virtualmente todo el trabajo por nosotros, la oportunidad de combinar las herramientas en una sola, aparece como la opción más adecuada.

Con respecto al caso específico de los sistemas analizados anteriormente, MRTG y NTOP poseen características importantes al momento de monitorizar el consumo de ancho de banda y el tráfico, consumidos o transportados por la red, sin embargo, no cumplen con algunos de los aspectos fundamentales mencionados antes dentro de este capítulo, como son en este caso:

- modularidad
- escalabilidad
- Comportamiento autónomo (capacidad para la toma de decisiones)
- Estabilidad 100 % garantizada
- Alerta y notificación de fallos autónoma

Cabe recalcar que los sistemas mencionados realizan de manera excepcional el trabajo específico para el cual fueron diseñados, mas no se encargan de analizar y discriminar entre lo que está o no dentro de los parámetros normales de la red; es decir, si algo no anda bien en la red, tanto MRTG como NTOP entregarán la información sobre lo que esta

pasando en esos momentos dentro de la red, mas no discriminarán acerca de si estos valores son admitidos dentro de los cánones de una red sana o estable, dado que no existe un “criterio” de que “anda bien o no”, el administrador se ve en la necesidad de estar permanentemente revisando la información entregada por dichos sistemas, para después tomar decisiones sobre lo que se debe o no hacer frente a determinada situación. Adicionalmente a esto, parte de la la tarea de analizar la información recabada del estado de la red, es alertar al administrador de los problemas presentes a la brevedad posible, lo cual recae en un tema de alerta y notificación; tarea para la cual no ha sido desarrolladas las herramientas antes mencionadas.

Por el lado del sistema de monitoreo Nagios, este cumple con la mayor parte de los requerimientos necesarios en una herramienta de monitoreo:

- Eficaz
- Estable
- Personalizable
- Modular
- Autónoma
- Compatible

El análisis del presente trabajo de tesis no se centra en desarrollar un sistema de monitoreo de red, ya que existen ya sistemas con amplia experiencia en el campo del monitoreo y administración de redes de comunicaciones, el objetivo se centra en elegir e implementar el mejor sistema o sistemas, de los ya desarrollados, versátil, eficaz y probado, para acoplarlo a las necesidades y topologías de la red WAN de la empresa Alianzanet S.A., con el fin no sol de entregar una solución completa de monitoreo y gestión de los recursos de red presentes, sino partiendo de la información entregada por este sistema, entregar un elaborado análisis de las capacidades y necesidades de la red de la empresa.

Dado que las herramientas mencionadas anteriormente, de manera individual, no poseen las características necesarias para alcanzar todas las metas planteadas en este proyecto, el fusionar estas herramientas en una sola, o dicho de otra forma, encontrar aquella que pueda administrar y procesar la información entregada por cada una, cumpliría a cabalidad con el objetivo.

Dicho lo anterior, el sistema llamado a monitorizar la red de Alianzanet S.A. de punta a punta, administrando y procesando la información entregada por las otras dos herramientas, y tomando las decisiones adecuadas luego del respectivo análisis, previa configuración claro está es, de manera indiscutible, NAGIOS.

3.3 Instalación y puesta en marcha de las herramientas

3.3.1 Instalación GNU/Linux

GNU/Linux se denomina al núcleo, o llamado también Kernel, de un grupo de sistemas operativos basados en UNIX y amparados por la GNU GPL, licencia que promueve la libre utilización del software y defiende este uso libre de la apropiación por parte de cualquier entidad que así lo decidiera. Al llamarlo software libre, la Free Software Foundation lo define como software de código nativo abierto, libre de realizar cambios incluso a nivel binario, se refiere a cuatro libertades de los usuarios del software:

- La libertad de usar el programa, con cualquier propósito; procurando siempre encaminarse por el uso legal de los sistemas.
- La libertad de estudiar el funcionamiento del programa, y adaptarlo a las necesidades de cada sistema.
- La libertad de distribuir copias con el fin de aportar a la comunidad pública internacional.
- La libertad de mejorar el programa y hacer públicas las mejoras, lo cual es una ventaja para aquellos que se vinculan por primera vez al desarrollo e implementación de dicho software.

El software libre suele estar disponible gratuitamente, sin embargo no es obligatorio que sea así, por ende no hay que asociar software libre a “software gratuito” (denominado usualmente *freeware*), ya que, conservando su carácter de libre, puede ser distribuido comercialmente (“software comercial”). Análogamente, el “software gratis” o “gratuito” incluye en algunas ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa, cosa que no ofrecen los sistemas operativos tradicionales como Windows o Macintosh.

GNU Linux define todo su funcionamiento en código escrito y compilado sobre una variante de lenguaje de programación C, su compilador especial GCC interpreta las líneas de código del sistema sobre una arquitectura bastante diferente de los típicos sistemas micro núcleo o núcleo monolítico, a saber:

Los controladores de dispositivos y las extensiones del núcleo normalmente se ejecutan en un espacio privilegiado conocido como anillo 0.

Existe acceso irrestricto al hardware, por lo que explota al máximo el uso que podemos darle a los recursos de hardware del ordenador

Es modular, los controladores de dispositivos se pueden cargar y descargar como módulos sin afectar el desempeño del equipo.

Los controladores pueden ser detenidos momentáneamente por actividades más importantes jerarquizando el gasto de recursos de procesador, esta habilidad fue agregada para gestionar correctamente interrupciones de hardware, y para mejorar el soporte de multiprocesamiento Simétrico.

El núcleo o kernel de Linux puede correr sobre muchas arquitecturas de máquina virtual, tanto como host del sistema operativo o como cliente. La máquina virtual usualmente emula la familia de procesadores Intel x86 comportándose tal cual un ordenador físico.

Linux debe su soporte en un 100% al internet, descargando actualizaciones de software, servicios y sistemas, desarrollados de manera independiente, gratuita y de código abierto (llamado también LIBRE) por una amplia comunidad alrededor del mundo.

Existe una amplia variedad de herramientas de software desarrolladas específicamente para el manejo de redes de comunicaciones, sobre todo para aquellas que basan su funcionamiento en la conmutación de paquetes.

La independencia tecnológica, el bajo costo, las libertades para adaptarlo a las necesidades de cada caso y muchas veces, la posibilidad de contribuir con mejoras al software y así ayudar a otras personas e instituciones, hacen que Linux sea el sistema operativo por excelencia cuando de servidores y seguridad se trata, un servidor seguro garantiza un sistema de red estable, robusto y confiable.

Los servidores de red con Software Libre dominan el 65% del mercado, mientras que Windows posee actualmente un 25%. Según una encuesta realizada recientemente por IBM, el 83% de las empresas planean realizar trabajos basados en GNU/Linux durante 2009, mientras que sólo el 23% está planificando lo mismo en base a Windows.

En la actualidad existe un sin número de distribuciones basadas en el kernel básico de Linux, sin embargo existen distribuciones que por su historia y desarrollo, han contribuido en gran manera al desarrollo de GNU/Linux desde sus inicios en 1990, sirviendo de base para la amplia gama de distribuciones que actualmente existen dentro de la comunidad Linux, a saber:

- Red Hat (año de liberación versión 1, 1994)
- Fedora
- CentOS

- Debian (año de liberación versión 1, 1996)
- Ubuntu
- Slackware (año de liberación versión 1, 1993)
- OpenSuSe

Todas las distribuciones mencionadas tienen su historia y han sido implementadas en diferentes sistemas alrededor del mundo desde los inicios de GNU/Linux.

En el presente trabajo se optará por utilizar la distribución Ubuntu derivada de Debian, con las siguientes características:

Tabla 3.6 Distribución a utilizarse en el proyecto

Nombre de la Distribución	Ubuntu
Versión	8.04 Hardy Heron
Kernel de Linux	2.6.24.16 - Server
Año de Publicación	24 de abril del 2008

Usando el disco de Ubuntu 8.04 Hardy Heron, los pasos para la instalación del sistema se detallan a continuación:

1. Cambiar la secuencia de Arranque del servidor para poder arrancar el disco de Ubuntu.
2. Una vez realizado esto, el servidor arrancará desde el Disco desplegando la pantalla de instalación:

Figura. 3.4 Pantalla inicial de instalación de Linux

3. En este punto se tienen dos opciones:

• Probar Ubuntu sin alterar el equipo, lo cual nos da la posibilidad de probar el sistema en modo liveCD, e instalar Ubuntu usando un proceso gráfico de manera guiado.

• Instalar Ubuntu, una manera directa de instalar el sistema sin probar las bondades en modo liveCD.

Se escogió la primera opción, para de esta manera cargar el disco en modo LIVE e instalar el sistema usando el método guiado.

4. Escogida la primera opción y cargado el sistema, tendremos el escritorio de Ubuntu Hardy Heron, donde seleccionaremos el icono Instalar que se encuentra en el escritorio, en este punto tendremos la siguiente pantalla:

5.

Figura. 3.5 Linux selección de idioma

Escogemos español como el idioma de instalación.

6. Seleccionamos la zona del mundo donde nos encontramos, en este caso el mapa nos da la opción elegir Guayaquil-Ecuador.

Figura. 3.6 Linux selección zona horaria

7. Escogemos la distribución del teclado, es recomendable escoger la distribución de teclado usada por Macintosh, ya que nos da acceso a todo los caracteres espaciales del teclado:

Figura. 3.7 Linux distribución del teclado

8. A continuación se selecciona el tipo de particionado que va a realizar, la opción manual de particionado será la elegida con el fin de personalizar el particionado:

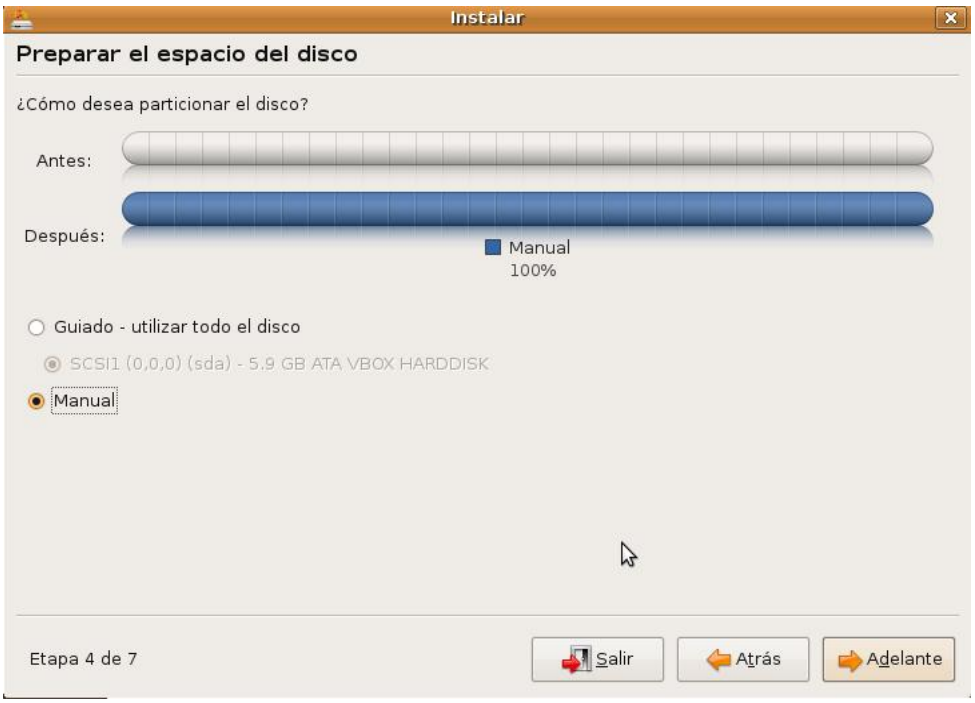


Figura. 3.8 Linux Selección de Particionado manual

9. En este punto el disco de instalación analiza el disco con la intervención del aplicativo *gparted*, con el fin de conocer el estado de la tabla de partición en caso de existir particiones anteriores:

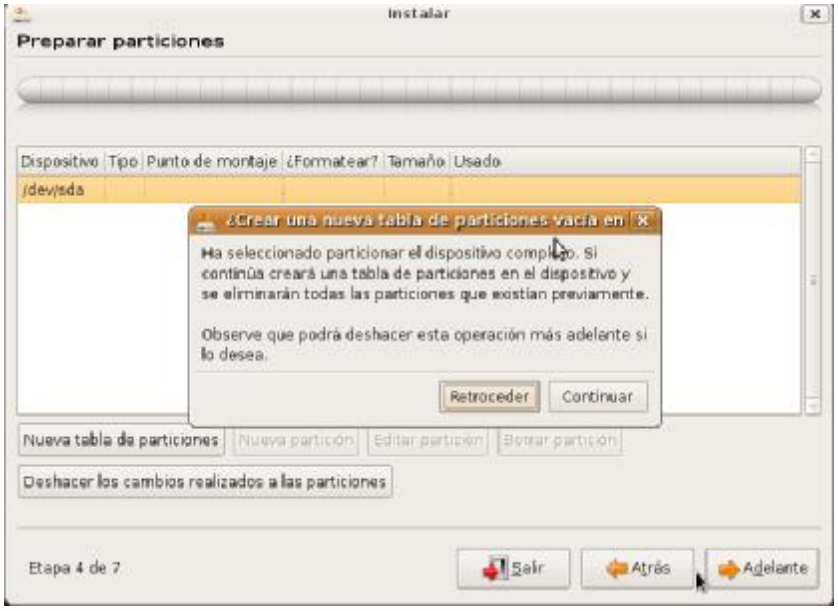


Figura. 3.9 Linux análisis de la tabla de particiones

9. Se procede a crear de manera arbitraria dos particiones fundamentales para el correcto funcionamiento del sistema Linux, como son:

- *Partición de Intercambio o SWAP*, esta representa la memoria virtual del sistema, a menudo se suele dimensionar esta en el doble de la memoria RAM disponible en el sistema, en este caso la partición swap ser de 512 MB (Figura 12.)
- *Partición principal*, esta alojara al fichero raíz o root representado por el símbolo / , puede tener la extensión que uno desee, en este caso la particin root del servidor de monitoreo tendrá una extensión de 10 GB (Figura. 13), cab recalcar que el sistema de ficheros que maneja Linux es del tipo ext3, un sistema de locación de espacio en disco diferente al manejado por Windows, sea NTFS o FAT32, este sistema de ficheros aloja los por clusters la información de manera ordenada y no randómica, haciendo más lento el almacenamiento, pero mucho más rápido el acceso sin opción a fragmentación de la información.
-

Figura. 3.10 Linux asignación de partición swap

Figura. 3.11 Linux asignación de partición root

10. Luego del particionado el disco queda como muestra la Figura 3.9:

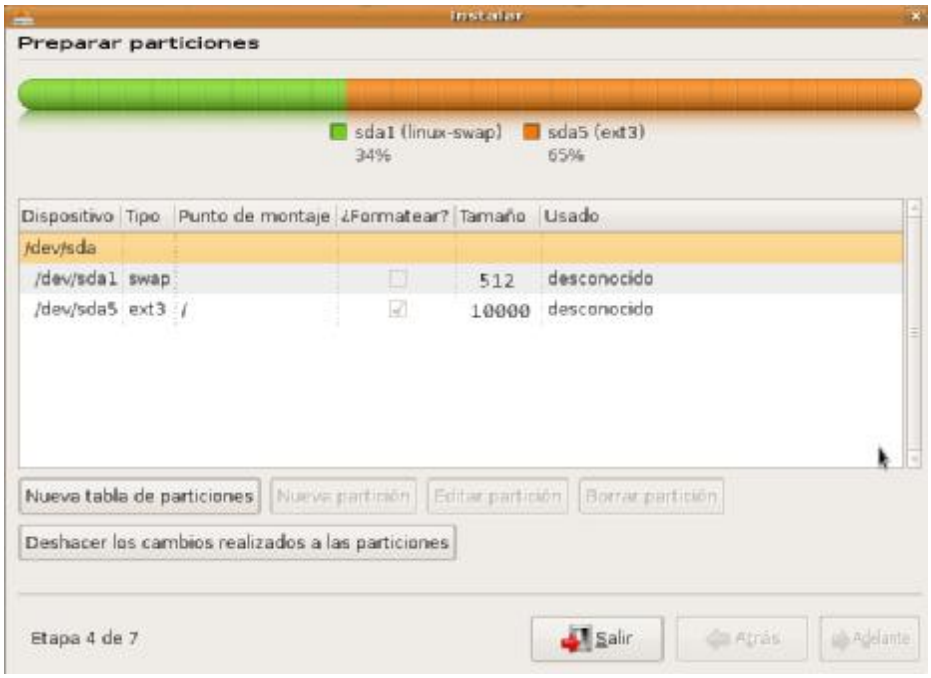


Figura. 3.12 Linux resumen del particionado

11. A continuación se debe asignar:

- Nombre de usuario, este será el encargado de administrar los recursos del servidor y, adicionalmente, se hallara en el mismo grupo de usuarios del usuario root y administrador del sistema.
- Contraseña, esta le pertenecerá solo al usuario *user*, se valdrá de esta además para realizar peticiones sudo, al usuario root del sistema, esto cuando se requiera configurar parámetros que afecten al sistema.
- Nombre del servidor, este corresponde al nombre que tendrá el equipo dentro de la red, este nombre lo identificara dentro de la granja de servidores

Figura. 3.13 Linux usuario y nombre del servidor

12. En la parte final de la instalación se detallara los parámetros asignados para el levantamiento del servidor (Figura. 3.11), para continuar finalmente con el proceso formal de instalación (Figura. 3.12).

Figura. 3.14 Linux resumen de la instalación

Figura. 3.15 Linux inicia la instalación

3.3.2 Instalación MRTG

3.3.2.1 Introducción. Como se había mencionado anteriormente, MRTG se basa en aprovechar las funciones brindadas por el protocolo SNMP, de manera específica, para medir el consumo de ancho de banda de determinada interface de red, sea dentro o fuera de la red donde se halla el servidor que aloja a MRTG.

Net SNMP es el nombre del equipamiento lógico, de uno de los sistemas desarrollados bajo código abierto, para implementar SNMP v1, SNMP v2c y SNMP v3 utilizando arquitecturas [36]IPv4 y/o [37]Ipv6. La librería Net SNMP contiene las funciones más comunes para construcción, recepción, decodificación y manipulación, de las peticiones y la respectiva información de respuesta, manejadas por SNMP.

El proyecto fue iniciado como un conjunto de herramientas SNMP por Steve Waldbusser en la CMU (*Carnegie Mellon University*), Pittsburgh, Pennsylvania, EE.UU., en 1992. Tras ser abandonado, fue retomado por Wes Hardaker en la UCDavis (*University of California, Davis*), renombrado como UCD-SNMP y mejorado para cubrir las necesidades del Departamento de Ingeniería Eléctrica de dicha institución. Tras dejar la universidad, Hardaker continuó el proyecto, cambiando el nombre de éste a Net-SNMP.

Cabe destacar que todo el código que se presente en este apartado se enmarcará con un recuadro para diferenciarlo del resto de la información, se esté líneas directo en el bash de Linux, o en dentro de los script parte de la configuración de los sistemas de monitoreo.

3.3.2.2 Instalación de Net – SNMP. Antes de instalar el paquete MRTG y configurar al servidor para que hable SNMP, debemos cerciorarnos de que el router al que vamos a monitorear, tenga configurada la misma clave o comunidad snmp, en caso de no existir esta configuración en el ruteador se procederá a hacerlo. Dentro de la configuración del ruteador, en modo consola, se ejecuta el siguiente comando:

```
show snmp group
```

el cual nos estragará la información deseada, sobre la o las comunidades *snmp* configuradas en el ruteador, en este caso el resultado es el mostrado en la Figura 3.12, a continuación:

36 IPv4: Protocolo internet versión 4, este acrónimo es identificado principalmente para designar redes con direcciones IP de 32 bits.
37 IPv6: Evolución del antes mencionado, el acrónimo es identificado principalmente para designar redes con direcciones IP de 128 bits

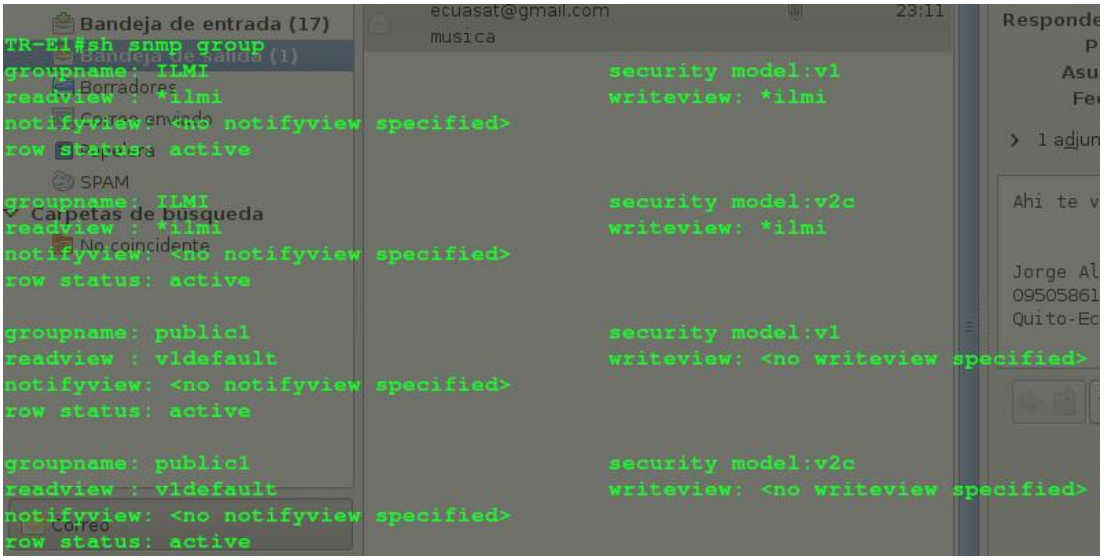


Figura. 3.16 Comunidad SNMP Router CISCO

El paquete Net SNMP necesita de ciertos requisitos, como cabeceras y librerias, para poder ser posteriormente instalado y configurado en GNU/Linux Ubuntu.

En este caso se listan los ficheros de configuración necesarios, instalados usando el gestor de paquetes *apt* de Ubuntu:

apt-get install libsnmp-base
apt-get install libsnmp5
apt-get install snmp and snmpd

- *libsnmp-base,* es una librería binaria base de SNMP, necesaria dado que contiene documentación para el manejo básico de Net SNMP, en este caso almacena información esencial sobre las MIB (*Management Information Base*), que consiste en una base de datos que alberga la información sobre los objetos, o parámetros, que pueden ser manejados o administrados, dentro de un dispositivo, con soporte para SNMP. Los objetos o variables, pueden ser configurados o leídos del dispositivo, sea de manera local o remota, para proveer información esencial sobre los dispositivos e interfaces, dentro de una red.
- *libsnmp5,* librería complementaria de libsnmp-base para la implementación de Net SNMP, en este caso es suficiente la versión 5 del paquete.

• *Snmpd, c*orrespondiente al *daemon* o demonio encargado de ejecutar las tareas SNMP programadas en el servidor, un daemon o demonio no es mas que un proceso ejecutable, que espera su llamada, no necesariamente por parte del usuario, para ejecutar un programa en modo *background*, es decir en segundo plano, sin la necesidad de que haya interacción con el usuario, en este caso el snmpd, no es más que el script ejecutable que se valdrá de todas las librerías antes mencionadas, para generar las peticiones y procesar las respuestas entregadas por SNMP.

Luego de instaladas las librerías mencionadas procedemos a instalar Net SNMP:

apt-get install Net-SNMP

Es importante mencionar que luego de instalados los ficheros antes mencionados, como toda utilidad en GNU Linux, se creará un fichero base de configuración, alojado en */etc/snmp/snmpd.conf*.

3.3.2.3 Configuración del fichero *snmpd.conf*. Se deben crear listas de control de acceso ACL correspondientes en el fichero /etc/snmp/snmpd.conf, las cuales servirán para definir que segmento de la red tendrá acceso hacia el servicio snmpd de la siguiente manera:

nano /etc/snmp/snmpd.conf

A una de estas listas se le otorgará permisos de lectura y escritura, esto con motivos de administración, mientras que se asignará permisos de solo lectura para aquel segmento de la red que solo tenga acceso a leer la información, mas no escribirla.

Por razones de seguridad solo la interfaz 127.0.0.1 o *local host* estará en el grupo de lectura escritura, es decir, solo el servidor que aloja a Net SNMP, a través de su NIC (Network Interface Card), tendrán la potestad de administrar el servicio.

Se otorgará permiso de acceso de solo lectura a una dirección de red en lista de control de acceso, con fines solo de visualización.

Considerando lo anterior, se agregarán y se comentaran las siguientes líneas en el fichero snmpd.conf:

```
Com2sec local 127.0.0.1/32 public1
Com2sec miredlocal 10.0.0.0/8 public1
```

La primera línea significa que habrá una lista de control de acceso denominada «local» y que corresponderá solo a 127.0.0.1/32, asignando public1 como clave de acceso. La segunda línea hace lo mismo pero define la red 10.0.0.0/8 con clave public1. Esto define el nombre de la comunidad SNMP que el servidor va a escuchar, esta comunidad se halla configurada en el ruteador de core de la red, ubicado en el nodo Carolina, dado que el servidor se halla dentro de la red MAN de Alianzanet, depende directamente del ruteador de core, mismo que maneja las rutas y subredes a través de las cuales los clientes tienen acceso al Internet.

El servidor se halla configurado dentro de una de las sub interfaces de la red, misma que se encuentra configurada de manera lógica dentro de una de las subredes alojadas en la red de acceso, basta configurar el servidor que hablará SNMP para que el grupo que escuche las peticiones, solo de lectura, sea el perteneciente a la red MAN de Alianzanet

3.3.2.4 Definición de grupos. Se crearon dos grupos: MyRWGroup y MyROGroup.

El primero es un grupo al que se asignarán más adelante permisos de lectura escritura, el segundo será un grupo al que posteriormente se asignarán permisos de solo lectura. Por cada grupo se asignan tres líneas que especifican el tipo de acceso que se permitirá en un momento dado a un grupo en particular. Es decir, MyRWGroup se asocia a local y MyROGroup a miredlocal, el código queda como sigue:

```
#Se asigna local al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
#Se asigna miredlocal al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal
```

Adicional a esto se debe especificar que permisos tendrán los dos grupos, MyROGroup y MyRWGroup, son de especial interés las últimas columnas:

```
## Group context sec.model sec.level prefix read write notif
Access MyROGroup “” any noauth exact all none none
Access MyRWGroup “” any noauth exact all all all
```

Se define además dos parámetros de carácter informativo para que cuando utilicen el servicio aplicaciones cliente, como MRTG, se incluya algo de información acerca de qué sistema se está accediendo.

```
Syslocation Servidor Linux ns1.alianzanet.ec
Syscontact Administrador (jorgealbertotapia@alianzanet.net)
```

A continuación se resume las líneas agregadas al fichero de configuración *snmp.conf*, los grupos permitidos a leer y escribir el servicio y la línea donde se especifica el acceso con el cliente snmp, en este caso MRTG.

```
# Listas de control de acceso (ACL)
## sec.name source community (alias clave de acceso)
com2sec local 127.0.0.1/32 public1
com2sec miredlocal 10.0.0.0/8 public1
#Se asigna ACL al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local
#Se asigna ACL al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal
# Establece permisos de lectura y escritura
## group context sec.model sec.level prefix read write notif
access MyROGroup “” any noauth exact all none none
access MyRWGroup “” any noauth exact all all all
# Información de Contacto del Sistema
```

```
syslocation Servidor Linux ns1.alianzanet.ec
syscontact Administrador (jorgealbertotapia@alianzanet.net)
```

Dado que las subredes de Alianzanet se hallan muy bien delimitadas en el grupo de lectura 10.0.0.0/8, no es necesario agregar nuevos grupos ni listas de acceso, sin embrago, de ser el caso el caso, el proceso es el detallado anteriormente, con los cambios del caso.

3.3.2.5 Administración del servicio. Como se ha dicho anteriormente, el sistema GNU/Linux trabaja con archivos ejecutables o demonios, quienes son los encargados de llamar al resto de archivos de configuración, con el fin de ejecutar determinada aplicación. Para ejecutar por primera vez el servicio snmpd, parar el servicio de necesitarse, o pal servicio dentro del fichero donde se almacenan todos los servicios ejecutables de GNU/Linux:

```
sudo /etc/init.d/snmpd
```

Seguido de la orden que se desea ejecutar, para iniciar el servicio, reiniciarlo de manera local o forzosa o pararlo en caso de necesitarlo, los comandos del bash de Linux se listan a continuación:

Tabla 3.7 Administración del servicio

COMANDO	FUNCION
Start	Inicia el demonio snmpd
Stop	Detiene snmpd
Restart	Reinicia snmpd
force-reload	Forza a recargar el servicio snmpd

Cabe recalcar que en Ubuntu el servicio snmpd luego de ser instalado y configurado, arranca automáticamente con el sistema operativo, sea que éste se haya apagado de manera intempestiva, planeada, o se haya reiniciado de ser el caso.

Luego de configurado en iniciado el servicio, se hace necesario comprobar el correcto funcionamiento del mismo, considerando, que sea signó como clave de acceso public1 en el router de acceso de la red, cuya configuración abarca las subredes contenidas en el rango

10.0.0.0/8, para probar si la configuración funciona, se ejecutó los siguiente comandos del bash de Linux, pertenecientes a las librerías de configuración de Net-SNMP , a fin de verificar que devuelvan la información acerca del sistema:

Snmpwalk -v 1 10.5.8.1 -c public1 system *Snmpwalk -v 1 10.5.8.1 –c public1 interfaces*

en este caso las MIB del [38]IOS de CISCO sobre el estado del sistema son entregadas mediante la primera línea, mientras que la segunda nos indica datos y características detalladas sobre las interfaces de red del dispositivo, en este caso el router de acceso de la red.

3.3.2.6 Configuración MRTG. Dado que la distribución de Linux a utilizarse es UBUNTU, existen varias formas de instalar el paquete MRTG, sin embargo la forma más segura es hacerlo a través del gestor de paquetes de Ubuntu apt, bajando e instalando el sistema de los repositorios oficiales de Ubuntu, utilizando el siguiente comando del bash de Linux:

Sudo apt-get install mrtg

Instalado el paquete, se debe acceder al sistema como el usuario root, debe respaldarse el fichero de configuración predeterminado de mrtg, el cual viene pre cargado en el directorio:

nano /etc/mrtg.cfg

con el fin de poder restaurarlo en el futuro si fuese necesario:

cp /etc/mrtg.cfg /home/mrtg/mrtg.cfg-OLD

Para generar el fichero de configuración para supervisar el rango de direcciones IP deseadas, dentro de la subred global de Alianzanet, es necesario ejecutar el siguiente comando que lleva en declaración la clave del sistema SNMP que deseamos monitorizar:

cfgmaker --global “workdir: /var/www/mrtg/” --global “Options[_]: \ bits,growright” --output /etc/mrtg.cfg --community=fibertel 201.219.0.70

38 IOS: Sistema operativo para equipos marca CISCO, está basado en UNIX para sistemas con bajas capacidades de procesamiento.

Donde:

- *Cfgmaker* = comando de configuración de mrtg
- *--global* = argumento de la función *cfgmaker*, que indica configuración global
- *Workdir:* = directorio de trabajo de mrtg, aquí se almacenaran los gráficos en formato PNG del consumo de las interface.

Cabe destacar que este directorio de trabajo podría estar alojado donde desee el administrador de MRTG, sin embargo en este caso se ha elegido el directorio */var/www*, con el objetivo de subir los gráficos generados por MRTG, al servidor web apache2, para la visualización de las graficas de manera remota vía protocolo HTML.
Las gráficas llevarán en su nombre la interfaz del router a la cual pertenecen y la dirección ip a través de la cual se está accediendo al equipo, por ejemplo:

201.219.1.210_se0_2_0.150.html

- Dirección IP del ruteador: 201.219.1.210, esta es la dirección IP de Border.
- Interface: Serial 0/2/0 subinterface 150, esta subinterface pertenece a la tercera troncal del router acceso.

- Options[_]: \bits,growrigth = que le indica al comando *cfgmaker* que las graficas del consumo de las interfaces serán generadas de izquierda a derecha.

- --output = le indica a cfgmaker que el fichero de salida, es decir, de donde va tomar la información será mrtg.cfg, es decir, el script que generará toda la información, el archivo fuente, será mrtg.cfg.

- --community = public1 10.5.8.1; esto le indica a cfgmaker que la clave de la comunidad SNMP que vamos a monitorear será public1, clave ya especificada, tanto en los ficheros de configuración de snmpd, como en el router CISCO 2801. La dirección ip 10.5.8.1, indica nada más que esa será la ip a través de la cual el servidor MRTG realizará las peticiones SNMP al router, cabe recalcar que esta ip se halla dentro del grupo MYROGROUP, en la subred 10.0.0.0/8.

3.3.2.7 Instalación servidor WEB A*pache*. Luego de generadas las gráficas de consumo por parte de MRTG, procederé a instalar y configurar el servidor web, con el fin de publicar las graficas dentro de un archivo de tipo HTML, para acceder a los resultados de manera remota, aprovechando la dirección IP pública configurada en el servidor MRTG. Cabe anotar que el servidor web *Apache* será necesario también para la implementación de los sistemas NAGIOS y NTOP.

La instalación del servidor web sigue un proceso bastante sencillo:
Lo instalamos vía apt:

apt-get install apache2

Luego del proceso de instalación es necesario configurar Apache2 para que reconozca el nombre del servidor, autenticado en los servidores DNS internacionales ([39]FQDN), para lo cual editaremos el archivo de configuración:

sudo nano /etc/apache2/httpd.conf

Se agrega al final del archivo el nombre del servidor, en este caso:

NameServer ns1.alianzanet.ec

El acceso se realizará a través del nombre del server MRTG o en su defecto usando la dirección IP de dicho server:

http://ns1.alianzanet.ec/mrtg.
Http://201.219.36.101/mrtg

Cabe recalcar en este punto que, si bien el sistema MRTG ya se hallaba implementado dentro de la empresa, este solo cubría el trafico generado por el nodo CAROLINA de Alianzanet, mas no existía un monitoreo para el nodo IÑAQUITO, los datos de comunidad snmp y dirección IP proporcionados en este capítulo, obedecen al sistema implementado para el monitoreo del nodo Iñaquito, se debe tomar muy en cuenta que el archivo de configuración snmpd.conf ha sido modificado para escuchar una sola comunidad snmp, esto debido a que el directorio de trabajo de MRTG así como su archivo de configuración general mrtg.cfg solo aceptan la escritura de un solo dispositivo SNMP.

39 FQDN: *Fully Qualified Domain Name*, es el "nombre completo" del servidor reconocido dentro de la zona respectiva en el DNS de la red. Este nombre representará la dirección IP del servidor

El software leerá el consumo de ancho de banda cada 5 minutos por defecto.

3.3.3 Instalación NTOP

La instalación se realiza mediante el gestor de paquetes apt de Ubuntu dentro del bash de Ubuntu:

Apt-get install ntop

Posterior a la instalación, y antes de proseguir con la configuración, es necesario definir la contraseña del usuario ntop, administrador del sistema, usnado el siguiente comando:

Sudo ntop –set-admin-password

este comando ordena al sistema el establecer una contraseña de administrador, sin esta contraseña, es imposible configurar NTOP para su correcto funcionamiento, ya que deben existir las garantías necesarias, en los que a seguridades respecta, para que el administrador haga uso de las herramientas de NTOP.

Se desplegará un mensaje como este:

NOTE: --set-admin-password requested no password. Did you forget the =? *Ntop startup - waiting for user response!* *Please enter the password for the admin user:*

En este punto ingresamos la contraseña de administración del sistema NTOP.

3.3.3.1 Configuración del servidor NTOP. Ntop tomara por defecto la interface [40]eth0, para analizar el tráfico que pasa por esta interface, en este caso, el servidor de monitoreo, objetivo de este proyecto, tiene destinada y conectada la interface eth1, dentro de la red de border de Alianzanet, por lo que es necesario editar el archivo de configuración de NTOP, donde estableceré la interface eth1 para el análisis, de la siguiente manera:

40 eth0: Primera interfaz reconocida por el sistema Linux, esta generalmente es la interfaz *Fast Ethernet* parte del chipset del servidor .

nano /var/lib/ntop/init.cfg

Dentro de este archivo se agregaran las siguientes líneas:

USER=”ntop” INTERFACES=”eth1”

El proveedor del canal de salida, en este caso Andinadatos, administra la VLAN de borde de Alianzanet, en el switch L3 a su cargo en el nodo Carolina, por lo que, en este caso, se tienen dos opciones:

1. Solicitar a Andinadatos la autorización y colaboración, para configurar en modo [41]*mirror*, un puerto del switch L3, donde se halla conectada la salida de Alianzanet, siendo este puerto imagen del enlace de borde, conectamos en este puerto el servidor de monitoreo que alojará a NTOP.
2. Conectar el servidor como enlace entre el router de border de Alianzanet, y la salida provista por Andinadatos, dando la posibilidad de implementar otras aplicaciones dentro del servidor como un Proxy transparente, *web caché, firewall*, etc.

En las Figuras 3.13 y 3.14 se ilustran las dos posibilidades:

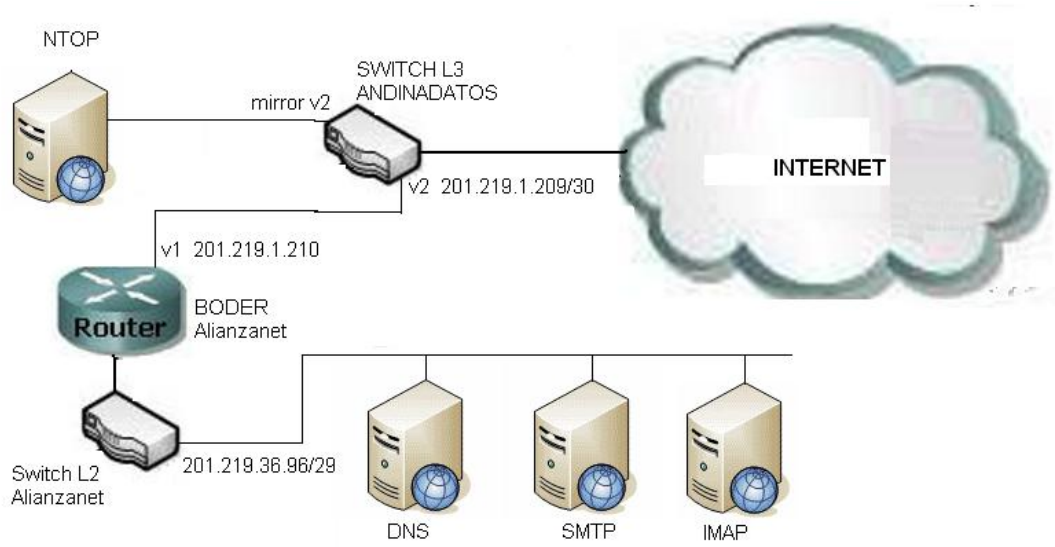


Figura. 3.17 Opción 1 NTOP

41 *mirror:* En redes el *port mirroring* constituye la configuración de determinado puerto, generalmente en un switch, con el fin de que se convierta en una imagen del trafico de un segundo puerto, designado a conveniencia.

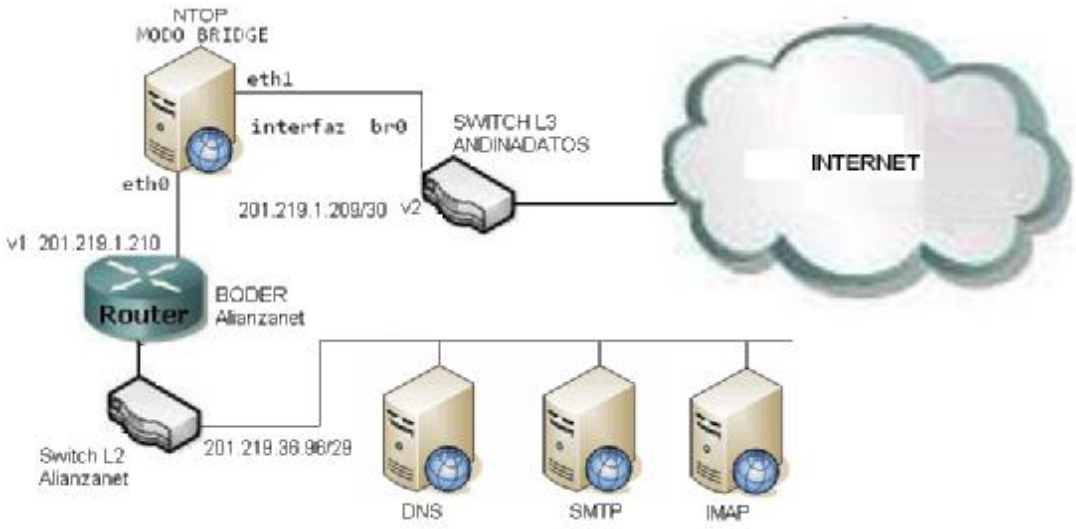


Figura. 3.18 Opción 2 NTOP

Luego de conversaciones mantenidas con el ejecutivo técnico, asignado por Andinadatos para Alianzanet, la opción 1 queda descartada, debido que no existe infraestructura en el switch que aloja, la VLAN de salida para Alianzanet, no existe un puerto libre, el cual se pueda configurar en modo mirror o SPAN (*Switch Port Analizer*).

Dado que se ha dado la apertura para colocar el servidor en el nodo Carolina, la opción 2, será la aplicada en este caso, se armara con dos tarjetas de red, al servidor que contiene el sniffer NTOP, fusionándolas en una interfaz virtual, denominada br0, misma que sea configurada con una IP publica dentro del rango que posee la empresa, esto con el fin de ingresar de manera remota al servidor y documentar los datos obtenidos por el sniffer. En la Tabla 3.8 se resume la configuración de esta solución.

Tabla. 3.8 Configuración del servidor NTOP

SERVICIO	INTERFAZ DE RED	MODO DE OPERACIÓN	TIPO	DIRECCION IP
NTOP	ETH0	BRIDGE	FISICA	N/D
	ETH1	BRIDGE	FISICA	N/D
	BR0	BRIDGE	LOGICA	200.50.234.78

Cabe recalcar que, en este caso, la interfaz que escuchara NTOP será cambiada por br0 dentro del fichero de configuración /var/ntop/init.cfg, ya que esta representa el puente entre las dos tarjetas físicas.

Para poder desplegar el mapa de tráfico de la red y demás información proveída por NTOP, es imprescindible instalar la herramienta complementaria *dot*, parte del paquete gráfico graphviz, paquete que se encuentra disponible usando apt:

Apt-get install graphviz

NTOP incluye un entorno gráfico HTML para consultar los resultados y administrar las diferentes tareas que es capaz de llevar a cabo.
Posterior a la instalación, NTOP configura el puerto 3000 del servidor por defecto, para el acceso a la interfaz, por la dirección http://201.219.36.100:3000.

3.3.4 Instalación Nagios

Para el correcto funcionamiento del sistema NAGIOS, es necesario instalar los siguientes paquetes básicos:

- *Apache2*, este paquete ya se encuentra instalado previamente como un requerimiento de MRTG.

- *El compilador GCC*, para lenguaje C y sus respectivos archivos binarios para desarrollo, la instalación de este paquete se obtiene con el comando

sudo apt-get install build-essential

Este paquete contiene una lista de librerías consideradas esenciales para compilar aplicativos Linux Ubuntu desarrollados en lenguaje *perl*, en este caso compilaremos el paquete completo de Nagios y sus aplicativos o Plugins.

- *Librerías para desarrollo GD*, la instalación de este paquete de librerías se obtiene usando el comando:

Sudo apt-get install lbgd2-xpm-dev

Esta librería aporta con soporte, para la plataforma gráfica e interactiva de Nagios basada en HTML, parte de la administración y configuración del sistema pueden hacerse via este acceso web.

Antes de instalar el paquete Nagios es necesario crear un usuario con los privilegios para administrar el sistema, esto crea a su vez, una cuenta dentro del servidor donde se almacenaran todos los archivos de configuración del sistema, el acceso a estos archivos lo tendrán solo el usuario root y el usuario Nagios, de la siguiente manera:

```
Sudo su
/usr/sbin/useradd -m nagios
Sudo passwd nagios
```

Las líneas de arriba ejecutan la orden de crear un usuarios extra llamado Nagios, asignándole la contraseña que elijamos para este.

Es necesario crear un grupo, al cual pertenecerán, tanto el usuario Nagios como el usuario por defecto de apache www-data, encargado de administrar la información a través de la interfaz HTML, al pretender al mismo grupo, facultará a Nagios, para ejecutar comandos externos, ordenes que serán ejecutadas de manera remota desde la interfaz web, los comandos ejecutados en el bash de Linux:

```
/usr/sbin/groupadd nagcmd
/usr/sbin/usermod -a -G nagcmd nagios
/usr/sbin/usermod -a -G nagcmd www-data
```

3.3.4.1 Descarga e instalación Nagios. NAGIOS se compone de dos paquetes principales:

- Código fuente Nagios
- Plugins o aplicativos Nagios

Por motivos de seguridad se creó un directorio dentro de / para almacenar ambos paquetes de código fuente, de la siguiente manera:

```
cd /
Sudo mkdir /descarga
cd /descarga
```

Dentro de este directorio se descargará el código fuente con la siguiente sentencia:

```
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.0.6.tar.gz
wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.13.tar.gz
```

Luego de esto se procede con la instalación del paquete, extrayendo el código fuente del mismo:

```
cd /descargas
tar xzf nagios-3.0.6.tar.gz
cd nagios-3.0.6
```

Dentro de este directorio, procedemos a rodar el script de configuración inicial de Nagios, pasando como argumento el grupo creado anteriormente con permisos para la ejecución de comandos externos:

```
./Configure—with-command-group=nagcmd
```

Luego de esto se compila el código fuente de NAGIOS, para posterior a esto instalar las diferentes instancias del sistema:

Archivos binarios	make install
Script de inicialización	make install-init
Archivos ejemplo de configuración	make install-config
Permisos para el directorio externo de comandos	make install-commandmode

Se instala adicionalmente la configuración web en el fichero de Apache2 *conf*.d, de la siguiente manera:

```
make install-webconf
```

Se crea una cuenta llamada *nagiosadmin*, con el fin de poder acceder a la interfaz Web de NAGIOS, la clave asignada en este punto será la utilizada para el acceso al sistema a través de Apache:

```
httpasswd2 -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Hay que tomar en cuenta que se crea un usuario y una contraseña Web, dentro de la cuenta de usuario Nagios, creada anteriormente, es decir, solo este usuario será admitido dentro del sistema vía interfaz web, absolutamente ningún otro.

Se reinicia el servicio de apache2 para que los cambios se ejecuten:

```
Service apache2 restart
```

Dentro del directorio donde se descargó el paquete de aplicativos:

```
cd /descargas
tar xzf nagios-plugins-1.4.13.tar.gz
cd nagios-plugins-1.4.13
```

Se ejecuta la herramienta de compilación sobre el paquete de aplicativos:

```
./configure—with-nagios-user=nagios—with-nagios-group=nagios
make
make install
```

Se procede a configurar Nagios para iniciar automáticamente cada vez que inicia el server:

```
ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

Esto le ordena al sistema que establezca un enlace, entre el script de inicialización del servicio Nagios (archivo ejecutable), y el directorio del server donde se listan las aplicaciones que se iniciarán con el sistema GNU/Linux, dando además a Nagios prioridad al inicio nivel S99.

El siguiente comando se ejecuta como un pre compilador del sistema, para detectar errores en el sistema, detallando el archivo de configuración que tiene el error y la línea errónea dentro del mismo:

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

De no existir errores después de la pre compilación, se inicia el servicio NAGIOS:

```
Service nagios start
```

Se ingresa al sistema a través de http://201.219.36.101/nagios/ se debe especificar el usuario y contraseña del administrador de Nagios, para lo cual se despliega la siguiente ventana de seguridad de apache2:

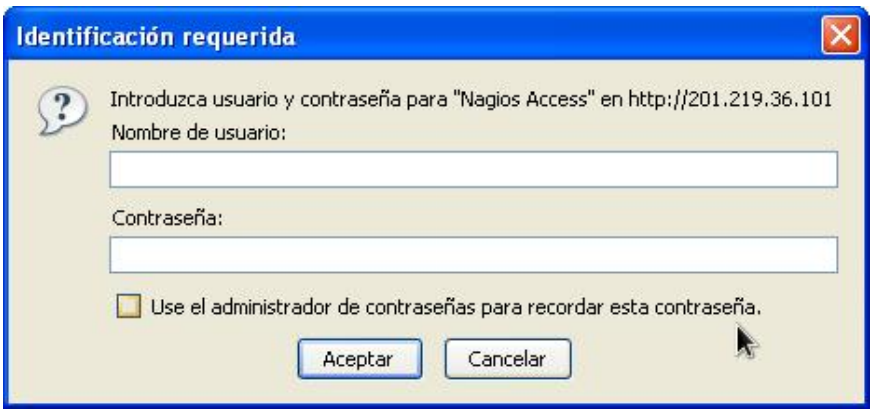


Figura. 3.19 Acceso Web Nagios Seguridad

En este punto se ingresan los datos del usuario *nagiosadmin* y la contraseña provista en apartados anteriores

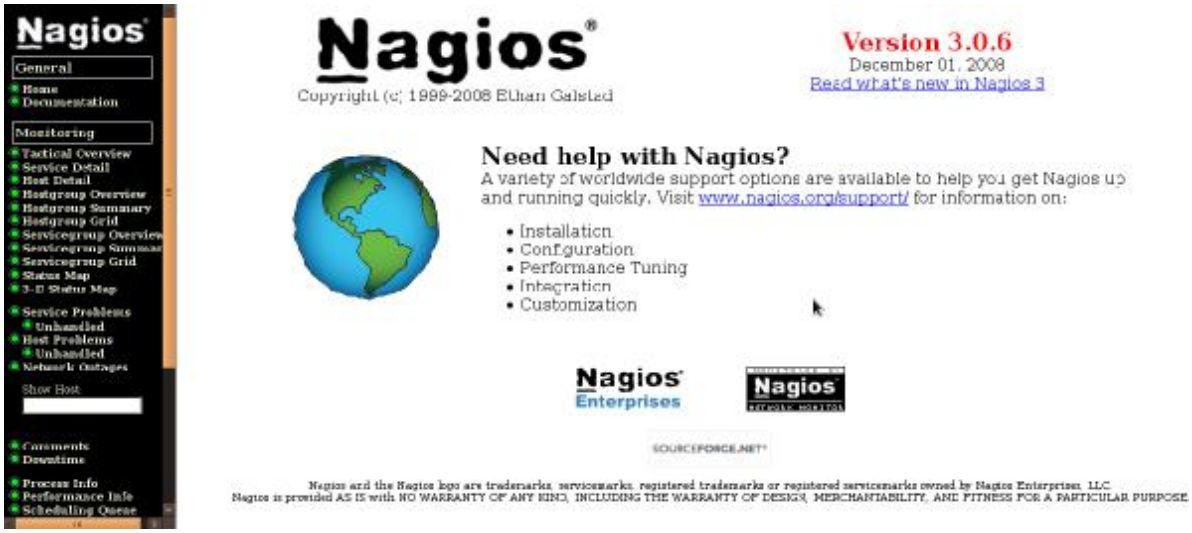


Figura. 3.20 Interfaz Web Nagios

3.3.4.2 Configuración Nagios. Antes de empezar con la configuración y declaración de los objetos, en Nagios es importante mencionar el papel que cumple el archivo de configuración principal.

Este archivo (*Main Configuration File*), otorga los permisos para la ejecución o inclusión de determinado archivo, aplicativo, recurso, contacto, host, etc. Dentro del sistema.
Contiene una especie de índice, donde el sistema discrimina que archivos serán aceptados el momento de poner en marcha el monitoreo, donde se ubican estos módulos para su posterior llamada, además de ciertas opciones como habilitar o deshabilitar servicios y notificaciones, en resumen, busca dentro de este, aquellos ficheros que serán tomados en cuenta, al momento de ejecutar todas estas tareas, tareas para las cuales el administrador a configurado el sistema.

Para editar este archivo hace falta tener en cuenta los siguientes puntos:

- Las líneas que empiezan con el carácter # son interpretadas como comentarios.

- Los nombres de las variables deben empezar en el inicio de la línea sin espacios en blanco.
- Los nombres de las variables son susceptibles al comando case de lenguaje C, las variables con nombres similares se diferencian si están con mayúscula o minúscula.
- El archivo de configuración por defecto se encuentra instalado en:

/usr/local/nagios/etc/nagios.cfg

En un principio será necesario tomar en cuenta los siguientes puntos, antes de empezar a rodar el monitoreo:

1. Habilitar todos aquellos ficheros de configuración que se utilizaran, para agregar hosts, contactos, servicios, etc., dado que se aprovechará los archivos que vienen por defecto incluidos en la instalación, hay que proceder a habilitarlos, para esto hay que cerciorarse de tener habilitadas las siguientes líneas dentro de nagios.cfg:

```
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
cfg_dir=/usr/local/nagios/etc/servers
cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

Estos cuatro ficheros habilitados, facultan al administrador el agregar respectivamente:

Contactos
Monitoreo del servidor local
Monitoreo de los servidores remotos
Monitoreo de los Routers y demás equipos activos dentro de la red

Conforme se agregue las diferentes estancias del monitoreo se agregaran archivos de configuración adicional, así como comandos, plantillas, funciones y scripts.

2. Habilitar las funciones de notificación, para que los contactos declarados dentro del fichero Contacts.cfg, puedan ser notificados al momento de producirse novedades dentro de la red.

Para esto se procede a editar la siguiente línea dentro de nagios.cfg:

enable_notifications=1

Esto determina el que se emitan notificaciones de host o servicios por parte del sistema en el siguiente reinicio del mismo.

Valores:

0 notificaciones deshabilitadas

1 notificaciones habilitadas

3. Siempre que se realicen cambios en la configuración de Nagios, en caso de que se editen los ficheros de configuración, los cambios no se llevaran a cabo si no se reinicia primero el servicio, y no se corrigen posibles errores en la manipulación y programación de los scripts.

Por esta razón, se hace necesario ejecutar las siguientes líneas en el bash de Linux:

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Esta línea ejecuta el depurador de perl para el fichero *nagios.cfg* el cual por obvias razones se halla conectado con el resto de archivos de configuración, por lo que, de existir algún error en la declaración de los objetos, este depurador arrojará el número de errores encontrados, así como la línea especifica y el archivo fuente del error.

Sudo service nagios restart

Este comando ejecutado en el bash de Linux reinicia el servicio de monitoreo, guardando los cambios realizados en los archivos de configuración y actualizando el entorno Web del CGI de Nagios. Si se agregaron nuevos servicios o host al sistema, o se cambio algún

parámetro de configuración de medición, el reiniciar el servicio es la única manera de ver reflejados estos cambios en el sistema.

A continuación se detalla la configuración de Nagios para monitorear en general tres elementos activos, en la red de Alianzanet:

- Servidores Linux
- Router de Core, Border y Acceso
- Clientes Corporativos (modems, servidores, ruteadores dentro de las redes de los mismos)

Como podemos ver Nagios se puede configurar para realizar varias tareas, para esto se deben editar los archivos de configuración de Nagios, y a su vez, crear algunos otros archivos, antes de empezar a monitorear.
A continuación la figura muestra un diagrama modular de la estructura de Nagios con respecto a sus archivos de configuración:

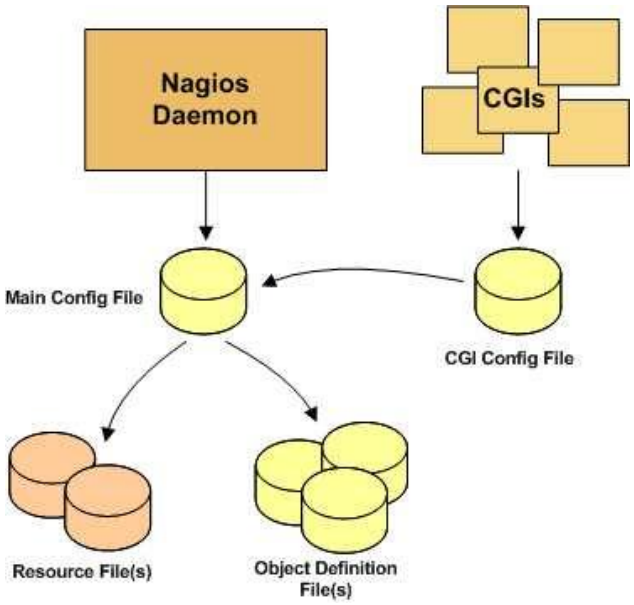


Figura. 3.21 Módulos de configuración Nagios

3.3.4.3 Configuración de *contacts.cfg.* En este objeto se definirán los contactos a los cuales se notificará, cuando algún elemento de la red se encuentra con problemas, este archivo se encuentra instalado por defecto en:

/usr/local/nagios/etc/objects/contacts.cfg

Por lo que se editará este archivo utilizando el editor de texto plano nano, de la siguiente manera:

Nano /usr/local/nagios/etc/objects/contacts.cfg

Agregando las siguientes líneas:

```
define contact{
        contact_name                    nagiosadmin             ; Short name of user
        use                             generic-contact         ; Inherit values from template
        alias                           Jorge Tapia             ; Full name of user
        contactgroups                   admins
        host_notifications_enabled      1
        service_notifications_enabled   1
        host_notification_options        d,u
        service_notification_options     c
        host_notification_period         24x7
        service_notification_period      24x7
        host_notification_commands      notify-host-by-email
        service_notification_commands   notify-service-by-email
        email                   jorgealbertotapia@gmail.com,95058616@im.movistar.com.ec
        }

define contact{
        contact_name                    Tecnico2                ; Short name of user
        use                             generic-contact         ; Inherit values from template
        alias                           Eduardo Moran           ; Full name of user
        host_notifications_enabled      1
        service_notifications_enabled   1
        host_notification_options        d
        service_notification_options     c
        host_notification_period         24x7
        service_notification_period      24x7
        host_notification_commands      notify-host-by-email
        contactgroups                   tecnicos
        service_notification_commands   notify-service-by-email
        email                           99938888@portafree.net,edumoran@msn.com
```

```
        }


define contact{
        contact_name                    Tecnico1            ; Short name of user
        use                             generic-contact     ; Inherit values from template
        alias                           Diego Puga          ; Full name of user
        host_notifications_enabled      0
        service_notifications_enabled   0
        host_notification_options       d
        service_notification_options    u,c
        host_notification_period        24x7
        service_notification_period     24x7
        host_notification_commands      notify-host-by-email
        contactgroups                   admins

define contact{
        contact_name                    Tecnico3            ; Short name of user
        use                             generic-contact     ; Inherit values from template
        alias                           Mauricio Poma       ; Full name of user
        host_notifications_enabled      1
        host_notification_options       d
        service_notifications_enabled   1
        host_notification_options       d,u,r
        service_notification_options    u,c
        host_notification_period        24x7
        service_notification_period     24x7
        host_notification_commands      notify-host-by-email,
        contactgroups                   tecnicos
        service_notification_commands   notify-service-by-email
        email                   maurod74@hotmail.com,096333345@alegropcs.net
        }
```

Estas líneas definen los usuarios a los cuales Nagios notificará de problemas en la red, de dos maneras:

1. Vía email
2. Vía SMS al teléfono celular del usuario

El sistema incluye dentro de su instalación inicial, la configuración de ***Exim4*** un aplicativo MTA (*Mail Transfer Agent*) para el envío de mensajes de correo electrónico, en este caso la llamada a la función de envio de correo electrónico incluye dentro de sus argumentos la dirección de correo del contacto, así como la información del estado del host o servicio monitoreado.

A continuación se detalla la función de cada línea en la definición:

define contact{

contact_name	Tecnico3

Define el nombre del contacto, este nombre será usado por el sistema para identificar al contacto, al momento de notificar determinada alarma se referirá a Tecnico 3 con todos los datos pasados por la defición del objeto, como direcciones de correo y sms, así como el resto de opciones de configuración las cuales se detallarán mas adelante.

use	generic-contact

Esta línea le dice al archivo de configuración principal, que al referirse al contacto Tecnico3, todas aquellas opciones que no se encuentren especificadas en la definición del objeto, se tomarán por defecto de una plantilla adjunta a los archivos de configuración por defecto de Nagios, cabe recalcar que estas opciones de configuración se heredan de este archivo llamado templates.cfg, las opciones de configuración especificadas en la declaración del objeto son tomadas por sobre las especificadas en el archivo templates.cfg

alias	Mauricio Poma

Este comando especifica el nombre competo del contacto, el cual se desplegará en los archivos LOG de Nagios, donde se lleva un registro de que notificaciones se han realizado con el nombre completo del contacto notificado.

host_notifications_enabled	1

Esta directiva puede tomar dos valores, a saber 1, que le indica al sistema a activación de las notificaciones para este contacto; 0, le indicará al sistema que las notificaciones la desactivación de dichas notificaciones.

host_notification_options	d

Este comando puede tomar varios argumentos:

Tabla. 3.9 Posibles estados del host

ESTADO	DETALLE
d	notifica al contacto cuando un host no responde o se encuentra en estado DOWN
u	notifica al contacto cuando un host es inalcanzable o se encuentra en estado UNREACHABLE
r	Notifica al contacto cuando un host se ha recuperado del estado DOWN y a pasado al estado UP.
f	Notifica al contacto cuando un host ha empezado a variar ose encuentra en un estado volátil, es decir, pasa de manera frecuente del estado UP a DOWN y viceversa, esto suele ocurrir cuando existe inestabilidad en el servicio o en la red.
s	Notifica al contacto cuando un host o servicio a pasado a un estado DOWN programado, esto en caso de mantenimiento o cambio de equipos.
N	Le dice al sistema que no notifique de ningún cambio en los equipos activos al contacto.

Para el ejemplo solo se notificará a este contacto cuando cualquier equipo activo se encuentre en estado DOWN, es decir completamente caído, cuando no se reciba respuesta del mismo.

service_notifications_enabled 1

Al igual que para los hosts o equipos activos, este comando le indica al sistema que las notificaciones por problemas en los servicios estarán habilitadas 1, o deshabilitadas 0.

service_notification_options u,c

De manera similar a las opciones de los hosts, este comando puede tomar diferentes valores:

w = Notifica al contacto cuando un servicio determinado se encuentra en estado WARNING, es decir se a superado el umbral configurado como aceptable para el servicio, por ejemplo cuando el porcentaje de paquetes perdidos es superior a 20%, el servicio entra en este estado de alerta.
u = notifica al contacto cuando determinado servicio se encuentra en estado desconocido o UNKNOWN, esto muestra un comportamiento errático en el servidor de monitoreo.

c = notifica al contacto cuando determinado servicio se encuentra en estado crítico o CRITICAL, cuando se ha superado el umbral crítico configurado para el servicio.

r = notifica al contacto cuando determinado servicio se a recuperado de un estado *Warning* o Down, y a pasado al estado OK.

f = notifica al contacto cuando determinado servicio ha pasado del estado Down al estado Up o viceversa, un número elevado de veces, volviéndose volátil.

n = indica al sistema que no envíe notificaciones de ningún tipo al contacto.

host_notification_period 24x7

Esta línea le dice al sistema que envíe notificaciones a este contacto las 24 horas del día los 7 días de la semana, sobre el estado de los hosts dentro de la red.

service_notification_period	24x7

De manera similar, el sistema enviará notificaciones a este las 24 horas del día los 7 días de la semana, sobre el estado de los servicios dentro de la red.

host_notification_commands	notify-host-by-email

Esta línea invoca al comando notify-host-by-email, declarado en el archivo de configuración commands.cfg, este archivo viene instalado por defecto, este comando envía una orden en modo texto para enviar un correo al contacto indicándole el estado de determinado host o servicio.

contactgroups	tecnicos

En este punto el objeto le dice al sistema que el contacto será parte de un grupo de contactos, declaración que se verá mas adelante, en este caso Tecnico3 será parte del grupo técnicos.

service_notification_commands	notify-service-by-email

De manera similar a los hosts, esta línea invoca al comando notify-service-by-mail, comando que enviará la orden al sistema de mandar un correo al contacto notificándole el estado de determinado servicio.

email	maurod74@hotmail.com,096333345@alegropcs.net

Esta línea establece la dirección de correo del contacto, dirección a la cual se remitirán las notificaciones, se pueden establecer varias direcciones para un mismo contacto, como direcciones de correo personal, empresarial e incluso, como en este caso, una dirección de correo asociada a un número de teléfono celular, con esto la operadora celular nos da la opción de recibir este correo a modo de mensaje de texto en el celular del contacto.

Adicional a todo esto, Nagios nos da la opción de agrupar diferentes grupos de contactos de acuerdo a la necesidad, es decir cuando algún elemento de la red se encuentre con problemas, estos objetos por separado, agrupan contactos para de esta manera darle una estructura modular al sistema, el sistema no tiene por qué listar todos los nombres de los contactos que se notificaran, con designar el grupo que será notificado en cada caso es suficiente, un usuario puede ser parte de dos o más grupos a la vez.

```
define contactgroup{
        contactgroup_name       admins
        alias                   IT Managers ALIANZANET
        members                 nagiosadmin,Tecnico1,jorge
        }

define contactgroup{
        contactgroup_name       tecnicos
        alias                   Tecnicos ALIANZANET
        members                 nagiosadmin,Tecnico1,Tecnico2,Tecnico3
        }
```

A continuación se detalla la función de cada línea en la definición:

define contactgroup {

```
contactgroup_name               tecnicos
```

Define el nombre del grupo de contactos, este nombre es arbitrario, el sistema utilizará este nombre como variable para referirse a todos los contactos parte de este.

```
alias                           Tecnicos ALIANZANET
```

Define un nombre largo del grupo de contactos, este nombre no será utilizado en los comandos de llamado de contactos, es simplemente un identificador en el LOG de Nagios para hacer la documentación de su actividad mucho mas comprensible al administrador o usuario.

```
members                 nagiosadmin,Tecnico1,Tecnico2, Tecnico3
```

Lista los contactos que serán parte de dicho grupo, separados por comas sin espacios, cuando el sistema haga una llamada de notificación a este grupo, la alerta será entregada a cada unos de los contactos definidos en members.

3.3.4.4 Monitoreo de los servidores locales. A continuación se detalla la configuración de los objetos y funciones, involucradas en el monitoreo de servicios privados, dentro de los servidores con sistema operativo GNU/Linux dentro de la red de Alianzanet, refiriéndose a servicios privados, como aquellos que tiene que ver con el sistema del servidor, con el estado de sus componentes, tanto lógicos como físicos, más no a servicios que pudieran denominarse públicos, de acceso compartido dentro de la red.

Se procederá a monitorizar:

1. Mensajes ICMP de tipo Echo, las respuestas al mensaje PING serán analizadas por el sistema.
2. Carga de procesamiento en el CPU, el sistema entregará datos reales de la carga de procesamiento del servidor expresado en porcentajes, y notificará a los contactos establecidos, en caso de que esta carga de trabajo del mismo, rebase los umbrales establecidos dentro de la declaración del comando check_local_load.
3. Uso de memoria RAM, el sistema notificará a los contactos establecidos, cuando el uso de recursos y espacio en memoria RAM rebase los valores establecidos en la declaración del comando, el sistema entregará en porcentaje, el consumo de memoria.
4. Consumo de la partición root, el sistema entregará informes sobre el consumo de la partición root (/) del servidor designado en porcentajes, es es una herramienta bastante útil ya que, como se ha indicado en capítulos anteriores, esta es la partición principal del sistema GNU/ Linux, en el caso de servidores tanto de correo IMAP como DNS, el disco duro se ve llenado con todo tipo de información, como son correos y almacén caché en cada caso, por lo que el sistema notificará en caso de que el consumo de esta partición se halle en valores críticos o fuera del rango designado por el comando.
5. Procesos en el servidor, este servicio reporta el número total de procesos ejecutándose en el servidor, al igual que el estado global de los mismos, se notificará a los contactos designados cuando este número de procesos exceda el establecido como umbral en la declaración del comando.

Cabe recalcar que el monitoreo del ping, es una herramienta bastante útil, y será configurada para todos y cada unos de los host o equipos dentro de la red de Alianzanet.
Los contactos designados son aquellos configurados dentro de los servicios y hosts, estos serán los únicos notificados al momento de presentarse problemas con determinado elemento de la red, si bien es cierto, sería un desperdicio de recursos, notificar de problemas en los servidores que corren sobre GNU/Linux, a personal no capacitado para resolver los inconvenientes que se presenten en los mismos.

Dentro de la instalación de los paquetes binarios y demás archivos de configuración de Nagios, se instalaron algunos archivos por defecto, uno de los cuales será utilizado para, dentro de este, levantar los servicios, hosts y grupos de hosts necesarios, para monitorear los servidores GNU/Linux levantados dentro de la red de Alianzanet.
Los servidores se clasificarán en dos grupos:

1. Local, servidor donde se hallan alojados los sistemas de monitoreo:

Nagios,
MRTG
NTOP

Este servidor es local para el sistema ya que es aquel que físicamente aloja a Nagios, entrando dentro de la red a través de la interface eth1 configurada con la IP 201.219.36.101, todos los componentes del servidor vienen a ser locales por esta razón.

2. Remoto, servidor dentro de la red de Alianzanet representado por una dirección IP y una interface dentro de la misma, estos servidores son remotos para el sistema Nagios no solo porque tienen configurada un dirección IP diferente a este, sino porque físicamente representan otro host dentro de la red.
Los servidores tanto locales como remotos con los que cuenta Alianzanet se detallan en la Tabla 3.10

Tabla. 3.10 Servidores Alianzanet

SERVIDOR	Local/remoto	Lógico /Físico	IP	S.O.	Observaciones
DNS PRIMARIO	Remoto	Físico	201.219.36.100	GNU/Linux	Anfitrión

Servidor de Nombres					
SendMail SMTP MRTG	Remoto	Lógico	201.219.36.98	GNU/Linux	Máquina Virtual VmWare
ZIMBRA IMAP	Remoto	Lógico	201.219.36.102	GNU/Linux	Máquina Virtual VmWare
Nagios MRTG NTOP OTRS DNS SECUNDARIO	Local	Lógico	201.219.36.101	GNU/Linux	Máquina Virtual VmWare
EMT	Remoto	Física	186.3.3.130	GNU/Linux	Servidor Empresa Metropolitana Quito Turismo
Puyo	Remoto	Físico	192.168.61.6	GNU/Linux	Servidor Cliente Corporativo ubicado en el Puyo

Luego de definido esto, la configuración del *servidor local* se detalla a continuación.

Para monitorear al servidor que aloja a Nagios junto con el resto de sistemas antes mencionados, se debe configurar el archivo donde se definirá el host y los servicios para el monitoreo.

La instalación del sistema Nagios arroja el archivo por defecto *local_host.cfg*, ubicado dentro de */usr/local/nagios /etc/objects/*, dentro de este fichero de configuración se incluye por defecto la declaración de un host, un servicio y un grupo, esto a modo de ejemplo con el fin de agilitar la introducción, por parte del administrador del sistema, al monitoreo de servidores basados en GNU/Linux, tanto remotos como locales.

Definición del host:

El archivo albergará el siguiente código para la declaración del host:

```
define host{
        use                     linux-server
        host_name               NAGIOS_101
        alias                   UBUNTU OTRS NAGIOS MRTG_ALIANZA 201.219.36.101
        address                 127.0.0.1
        hostgroups              LINUXSERVERS
        max_check_attempts      5       ; se chequea 10 veces antes de ser reportado
        notification_interval   5       ;se notificara a soporte cada 5 minutos
        notification_period     24x7    ;24 horas 7 dias a la semana
        contact_groups          admins
        notification_options    d,u
        first_notification_delay  0    ;se notificara de inmediato DOWN UNRECHABLE
        }
```

A continuación se detalla la función de cada línea en la definición:

define host{

use	linux-server

Define por herencia los parámetros establecidos en un archivo configurado por defecto, toda declaración no echa en la definición del host, se tomará del host por defecto linux-server, las líneas declaradas en el objeto tienen prioridad sobre las definidas en el archivo *templates.cfg* donde se encuentra declarado en host *linux-server.*

host_name	NAGIOS_101

Declara el nombre del objeto, en este caso del host NAGIOS_101, este será el nombre utilizado por el sistema para identificar al host al momento de monitorear su estado.

alias	UBUNTU OTRS NAGIOS MRTG_ALIANZA DNS 201.219.36.101

Es el nombre largo del host, el sistema no utilizará este nombre para referirse al host al momento de realizar su trabajo de monitoreo, sino como un registro para el archivo log de Nagios y detalles dentro de la interfaz web, el servidor se halla configurado en Ubuntu 8 y lleva en su sistema el software OTRS, NAGIOS, MRTG Y DNS.

address	201.219.36.101

Define la dirección IP del host, este dato es extremadamente importante ya que será a través de esta dirección, que el sistema determinará el estado del servidor, empezando por si se encuentra activo dentro de la red, y datos acerca del consumo de sus recursos privados: Disco Duro, Memoria RAM, procesador, mencionados anteriormente; así como de sus recursos públicos, los cuales se detallarán más adelante.

hostgroups	LINUXSERVERS

Agrupa a NAGIOS_101 dentro del grupo LINUXSERVERS, grupo de equipos al que pertenecerán todos los servidor es linux de Alianzanet, cuando el sistema se refiera al grupo LINUXSERVERS, se tomará en cuenta a todos los miembros del mismo para tal o cual tarea de revisión, esto le da bastante modularidad al sistema y una forma mas sencilla y ordenada de administrar el estado de dichos servidores.

max_check_attempts	5

Esta directiva establece el número de veces que se comprobará el estado del servicio antes de proceder a la notificación, en este caso se verificará 5 veces el estado del host, antes de ser reportado a los contactos pertinentes, este número es arbitrario.

notification_interval	5

Esta línea establece el intervalo entre una notificación y otra, para este caso, los contactos designados serán notificados con un intervalo de 5 minutos.

notification_period	24x7

Establece el intervalo de tiempo, durante el cual, se notificará a los contactos el estado del host, este es arbitrario, en caso de que se coordinen turnos de trabajo o se respeten descansos de fin de semana, para el servidor Nagios en cuestión, se notificará al grupo designado las 24 horas los 7 dias de la semana.

contact_groups	admins

El grupo de contactos que será notificado, es establecido por esta directiva, esto con el fin de que solo personal autorizado y capacitado, esté a cargo del estado de dicho host, adicionalmente esa directiva la da modularidad al sistema, y ahorra recursos de red, notificando solo a un grupo reducido, sin saturar el servicio de correos de salida SMTP, configurado específicamente para Nagios, dicha saturación pondría en riesgo la IP pública del servidor, corriendo el riesgo de ser listada en Listas Negras SMTP. Para el servidor de monitoreo Nagios, solo el grupo de contactos admins será notificado.

notification_options	d, u

Establece para que estado del host, se notificará al grupo de contactos configurado, esta directiva fue ya configurada anteriormente para los contactos (Tabla 8.), sin embargo en este caso, cada host puede ser configurado de distinta manera, para emitir notificaciones tomando en cuenta los diferentes estados que puede tomar el mismo.
Para el host Nagios en este caso, se notificará al grupo de contactos admins en caso de encontrarse en estado *Down o Unrechable* (Inalcanzable).

first_notification_delay	0

Esta directiva define el intervalo de espera, luego del cual, se notificará a los contactos pertinentes, el estado de dicho host, sujeto a la directiva anterior, es decir a los estados para los cuales se emitirán notificaciones. En este caso para el host Nagios, al detectarse los estados *Down o Unrechable*, se notificará al grupo de contactos admins, el valor 0, indica el hecho de que se notificará inmediatamente se detecten cualquiera de estos dos estados.

Luego de definidos los hosts, es necesario definir los servicios a monitorearse dentro del servidor local, para esto, se edita, de manera similar a la definición del host, el archivo de configuración *localhost.cfg*, agregando las siguientes líneas:

define service{	
use	local-service ; Name of service template to use
host_name	NAGIOS_101
service_description	PING

```
      check_command              check_ping!100.0,20%!500.0,60%
      }
define service{
      use                        local-service        ; Name of service template to use
      host_name                    NAGIOS_101
      service_description          Root Partition
      check_command                check_local_disk!10%!5%!/
      }
define service{
      use                          local-service        ; Name of service template to use
      host_name                    NAGIOS_101
      service_description          Total Processes
      check_command                check_local_procs!250!400!RSZDT
      }

define service{
      use                          local-service        ; Name of service template to use
      host_name                    NAGIOS_101
      service_description          Carga Actual del Servidor
      check_command                check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
      }

#Define el servicio para el monioreo del demonio SSHd.
define service{
      use                          local-service        ; Name of service template to use
      host_name                    NAGIOS_101
      service_description          SSH
      check_command                check_ssh
      }

#Define el servicio para el monioreo del demonio HTTPd
define service{
      use                          local-service        ; Name of service template to use
      host_name                    NAGIOS_101
      service_description          HTTP
      check_command                check_http
      }
```

A continuación se detalla la función de cada línea en la definición:

define service{

Define el objeto de tipo servicio, los servicios son funciones o tareas del host a ser monitoreado, es posible que entre en problemas un servicio mientras el host se halla aún operativo.

use	local_service

Define la herencia del servicio, este heredará los parámetros por defecto del servicio local_service definido en el archivo templates.cfg, toda linea en la definición presente tendrá prioridad sobre los parámetros heredados por defecto.

host_name	NAGIOS_101

Especifica el nombre del host para el cual se realizará la comprobación de dicho servicio, puede plantearse el mismo comando para monitorear varios hosts, sin embargo, para cada host se declarará un servicio, asociado directamente con este. Todos los servicios asociados a determinado host serán tomados como parte de este, si el host es inaccesible, sus servicios también los serán, y aparecerán en la interfaz de monitoreo, como
Estado del Servicio: Desconocido

service_description	HTTP

Describe al servicio, esto a modo de presentación, algo muy similar a lo que hace la línea alias en la declaración de los hosts. Esta descripción será adjuntada en las notificaciones configuradas para dicho servicio, al igual que se registrarán en el log de Nagios. En este caso, hace referencia al servicio HTTP configurado en dicho host o servidor (NAGIOS_101), service_description no entra en la llamada a las funciones de monitoreo.

check_command	check_http

Declara el comando correspondiente a dicho servicio, para comprobar el estado de este servicio, se ejecutará el comando, la información entregada por el mismo, será procesada por Nagios y presentada en la interfaz de monitoreo, a su vez, será almacenada en la variable *state* del servicio, para notificar a los contactos pertinentes.
En la figura 3.18 se detalla el proceso de Nagios para monitoreo, diagnostico y notificación de problemas en la red.

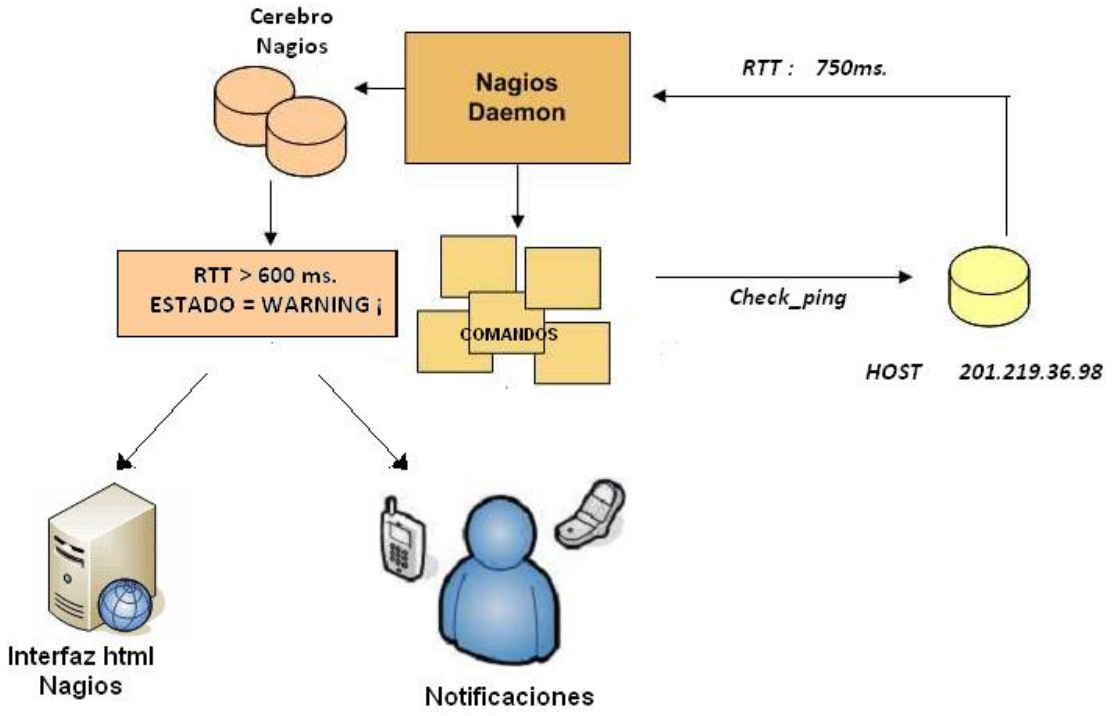


Figura. 3.22 Nagios proceso de notificación

Por el lado de los comandos utilizados, en el presente trabajo de tesis se detallarán en su momento cada uno de ellos, aplicados dependiendo la naturaleza del host, sea este un Ruteador, Servidor, Modem, Switch L3, etc.

En lo concerniente al servidor local, estos son los comandos utilizados para su monitoreo:

- ***check_ping***: Evalúa la respuesta al comando PING.

COMANDO check_ping!100.0,20%!500.0,60%

Analizando para esto las siguientes directivas:

- *RTA: Round Trip Time*, o tiempo de ida y vuelta del mensaje, este tiempo le dará al sistema, una medida de la saturación del enlace analizando el tiempo que le toma a este paquete, de baja prioridad TCP/IP, el salir del sistema y regresar al mismo, en caso de tener respuesta. Las notificaciones serán configuradas, para alertar a los contactos de tiempos altos o demasiado bajos, fuera de un umbral establecido. Este umbral es definido dentro de la declaración del comando, en el fichero commands.cfg.

- *Red de Destino Inaccesible (Destination Unrechable*), cuando el sistema recibe una respuesta de red inaccesible, notificará a los contactos pertinentes, de que existen problemas en la red a través de la cual, el equipo o host, obtiene el acceso.
- *Tiempo de Espera Agotado (Live Time Exceed),* cuando el sistema no reciba una respuesta dentro de un tiempo establecido, configurado dentro de la declaración del comando, Nagios notificará a los contactos establecidos el estado del host.los mensajes emitidos por el protocolo ICMP, detallado anteriormente.

Como se mencionó anteriormente, en este punto se establecen los umbrales para los cuales se analizará el estado de este servicio, la línea dentro del cuadro establece:

Umbral inferior:

RTT: 100 milisegundos, Packet Lose: 20%,

Umbral superior

RTT: 500 milisegundos, Packet Lose: 60%,

Se emitirá una notificación con el estado del servicio, cuando se registren tiempos de ida y vuelta fuera de este rango el estado del servicio pasará al estado *CRITICAL*.

- ***Check_host_alive***: Evalúa si el host se encuentra en línea con respecto a la red, si se encuentra en estado *UP*, de ser así, por medio de la interpretación de un sencillo algoritmo, el sistema evalúa si se ha llegado al 80% de paquetes perdidos, o en su defecto, se ha alcanzado un tiempo de respuesta, de ida y vuelta, de 5000 milisegundos, si el servicio cumple con cualquiera de estas dos directivas, el host para el cual evalúa el comando pasará al estado *DOWN*.

COMANDO check_ping!2000, 0,50%, !5000, 1% -p 20

El argumento -p 5 indica que no se puede sobrepasar los 5 mensajes PING con estas características.

- ***check_local_load***: Comprueba el consumo de procesador en el servidor local.

COMANDO check_local_load!5.0,4.0,3.0!10.0,6.0,4.0

El comando toma dos argumentos, 5.0, 4.0, 3,0 y 10.0,6.0,4.0, valores que establecen el limite superior e inferior para la carga de procesamiento, valores superiores al primer umbral entregarán el estado WARNING, valores superiores al segundo umbral entregarán el estado CRITICAL al servicio.

- ***check_local_disk:*** Comprueba el consumo de la partición root en le servidor local.

COMANDO check_local_disk!10%!5%!

El comando toma dos argumentos, 10% y 5%, valores que establecen el límite superior e inferior para el consumo de la partición root del sistema Linux, valores superiores a 10% entregará el estado *WARNING*, valores superiores a 5% entregarán el estado *CRITICAL* al servicio.

- ***check_local_procs:*** Comprueba el número de procesos que se hallan corriendo sobre el servidor Linux, cabe recalcar que cada servicio activo trabajando el servidor, es tomado como un proceso, cada proceso posee un número de identificación y un estado, dependiendo del estado en el que se encuentra el proceso.

COMANDO check_local_procs!250!400!RSZDT

Esto se halla detallado en la Tabla 3.11 a continuación:

Tabla. 3.11 Posibles estados de los procesos Linux

ESTADO DEL SERVICIO	DETALLE
d	Ininterrumpible, generalmente de Entrada o salida de datos.
r	ejecutándose o en cola para la ejecución
s	Dormido o esperando por un evento que culminará pronto, este estado permite al sistema detener el proceso si se lo desea, en caso de ser necesario, sin dañar el normal curso de funcionamiento.
t	Detenido, esto por un gestor de trabajo que necesito detener su funcionamiento por algún motivo.
z	Zombi, estado que indica ejecución del proceso pero en un estado autómata, es decir, iniciado por un tercer proceso de manera deliberada, dependiente de otro proceso, generalmente en estado r .

Los argumentos 250! y 400!, indican los umbrales superior e inferior del comando, si el número de procesos ejecutándose en el servidor superan los 250, el servicio entra en estado *WARNING*, si el número de procesos ejecutándose en el servidor superan los 400, el servicio entra en un estado *CRITICAL.*

- ***check_ssh***: Comprueba el estado del servicio ssh (*Secure Shell*) para acceso remoto, en el servidor local, se cerciora de que se puedan establecer conexiones a través del puerto configurado para conexiones entrantes de este tipo (22 por defecto).

COMANDO $USER1$/check_ssh $ARG1$ $HOSTADDRESS$

El comando le indica al sistema que el usuario $USER$ está solicitando dicha comprobación, en este caso el usuario principal del sistema Nagios , tomando como argumentos la dirección IP del host, y el puerto, comprobando que este se encuentre abierto.

- ***check_http:*** Comprueba el estado del servicio *http (Hyper Text Transfer Protocol*), para servicios web como *apache2*, en el servidor local, se cerciora de que se puedan establecer conexiones a través del puerto configurado para conexiones entrantes de este tipo (80 por defecto).

COMANDO $USER1$/check_http $ARG1$ $HOSTADDRESS$

El comando le indica al sistema que el usuario $USER$ está solicitando dicha comprobación, en este caso el usuario principal del sistema Nagios , tomando como argumentos la dirección IP del host, y el puerto, comprobando que este se encuentre abierto.

3.3.4.5 NRPE, monitoreo de los servidores remotos. Con el fin de monitorear los servidores remotos administrados por Alianzanet, se ha instalado y configurado una herramienta adicional al sistema Nagios, diseñada para trabajar en conjunto con este, esta herramienta será configurada no solo en el servidor de monitoreo principal, sino en los servidores remotos que funcionan bajo GNU/Linux.

La herramienta NRPE fue diseñada para permitir ejecutar los aplicativos de monitoreo de Nagios en máquinas remotas que funcionen bajo sistemas basados en GNU/Linux.

Las tareas de control realizadas en servidores locales, como verificación del consumo de memoria RAM, Disco duro y de los procesos que corren sobre el sistema, pueden ser verificados también en máquinas remotas, con la adecuada configuración del aplicativo NRPE.

Algo importante a tomar en cuenta es que las herramientas configuradas en el sistema Nagios, pueden ser utilizadas para monitorear servidores remotos, utilizando para esto la comunicación a través del protocolo *SSH (Secure-Shell Protocol)* sin la intervención de NRPE, sin embargo, el continuo uso de SSH y del puerto 22, recaen en una carga bastante alta tanto para el servidor de monitoreo como para el servidor remoto, carga que se traduce en un alto consumo de procesador como en un continuo uso del ancho de banda a través del cual acceden los dos servidores a la red WAN de Alianzanet.

A continuación se detalla un diagrama modular del sistema:

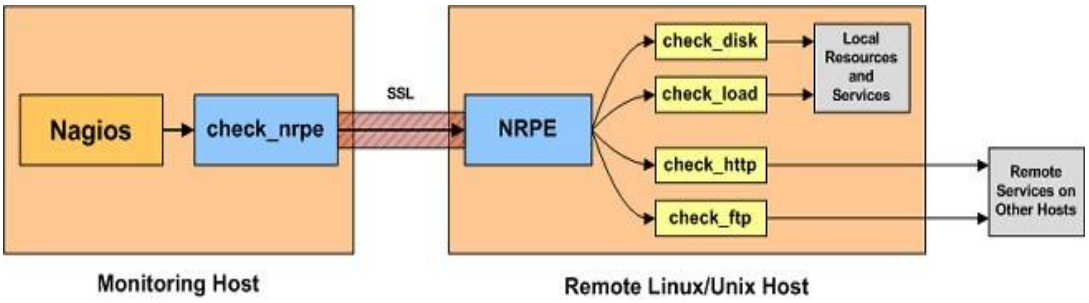


Figura. 3.23 Nagios y NRPE

Cuando Nagios necesite monitorear un recurso de servicio desde el servidor remoto Linux, seguirá el siguiente proceso:

- Nagios ejecutará el aplicativo check_nrpe, designando al sistema que servicio necesita ser comprobado.
- El aplicativo check_nrpe contacta al demonio NRPE configurado en el servidor remoto sobre una conexión protegida SSL.
- El demonio de NRPE comprueba el requerimiento del servidor de monitoreo sobre el estado del recurso solicitado.
- El resultado del chequeo realizado por el demonio NRPE es devuelto al aplicativo check_nrpe, este entrega la información al servidor Nagios para ser procesado.

La instalación de NRPE consta de dos partes:

- Instalación y configuración del Demonio NRPE en el equipo remoto
- Instalación y configuración del aplicativo en el servidor de Monitoreo
-

3.3.4.6 Instalación y configuración del Demonio NRPE en el equipo remoto. Se procederá a instalar el aplicativo *nagios_plugins* y la herramienta NRPE en el host remoto, siguiendo el siguiente proceso:

1. Creamos el usuario Nagios dentro del equipo remoto y le damos una contraseña:

```
sudo /usr/sbin/useradd nagios
sudo passwd nagios
```

2. Creamos un directorio donde descargar nagios_plugins e ingresamos dentro de este:

```
sudo mkdir /home/descargas
cd /home/descargas
```

3. Descargamos el fichero *nagios_plugins* junto con sus archivos binarios dentro del directorio */home/descargas*:

```
wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.6.tar.gz
```

4. Luego de descargado se lo descomprime dentro de */home/descargas*:

```
cd /home/descargas
tar -xvf nagios-plugins-1.4.6.tar.gz /home/descargas
```

5. Se Ingresa dentro del fichero /home/descargas/nagios-plugins-1.4.6 procediendo a la previa configuración del servidor, con el fin de garantizar las condiciones necesarias para instalar la herramienta *nagios_plugins*:

```
./configure
```

6. Luego de no haber obtenido errores en el proceso de pre configuración, compilamos la herramienta nagios_plugins y la instalamos dentro del sistema, el compilador arrojará un mensaje como este al final de la compilación:

i. —with-apt-get-command: /usr/bin/apt-get
ii. —with-ping6-command: /bin/ping6 -n -U -w %d -c %d %s
iii. —with-ping-command: /bin/ping -n -U -w %d -c %d %s
iv. —with-ipv6: yes
v. —with-mysql: not found
vi. —with-openssl: no
vii. —with-gnutls: no

viii. —with-perl: /usr/bin/perl
ix. —with-cgiurl: /nagios/cgi-bin
x. —with-trusted-path: /bin:/sbin:/usr/bin:/usr/sbin

Detalle:

i. Instalador de aplicaciones apt por defecto
ii. Comando tipo ping6 para Ipv6 OK
iii. Comando tipo ping para Ipv4 OK
iv. Compatibilidad con IPv6 OK
v. Base de datos mysql ausente
vi. Ecryptacion ssl ausente
vii. Servicio P2P gnuts ausente
viii. Interprete de comandos perl
ix. Control Grafic Interfaz OK
x. Ruta de confianza /usr/sbin

Esto nos dice entre otras cosas que no se ha detectado el paquete *OPENSSL*, paquete que instala los archivos binarios necesarios para codificar y decodificar datos sobre conexiones [42]TCP/IP utilizando algoritmos [43]SSL (*Security Sockets Layer*) en capa 6 (Presentación) del modelo OSI.

NRPE, de acuerdo a lo expuesto anteriormente, utiliza SSL dentro de la negociación o comunicación entre el servidor Nagios y el servidor remoto, por lo que es necesario instalar y configurar open-SSL en ambos servidores.
Luego de esto cambiamos los permisos y el propietario del fichero /usr/local/nagios al usuario Nagios creado anteriormente para que este pueda ejecutar NRPE y los aplicativos de nagios_plugins:

```
chown nagios.nagios /usr/local/nagios
chown -R nagios.nagios /usr/local/nagios/libexec
```

42 TCP/IP: Siglas que representan al Protocolo Internet en general.
43 SSL: Protocolo propuesto por Novell proporciona cifrado simétrico de datos que corren sobre TCP/IP en la capa 6 del modelo OSI

7. Se descarga el fichero de NRPE dentro de la carpeta creada anteriormente:

```
cd /home/user/descargas
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nrpe-2.8.tar.gz
```

8. Luego de descargado el código fuente este es desempaquetado previo esto a a compilación:

```
cd /home/user/descargas
tar xzf nrpe-2.8.tar.gz
cd nrpe-2.8
```

9. Dentro del fichero ya desempaquetado, se configuran el resto de dependencias del servidor, para que el sistema se cerciore de existen las condiciones necesarias para instalar NRPE :

```
./configure
```

10. La configuración de las dependencias de red del servidor arrojan el siguiente error:

```
Checking for SSL... configure: error: Cannot find ssl libraries
```

11. Haciendo referencia a la instalación de nagios_plugins, vista anteriormente, luego de instalado el aplicativo se obtuvo una alerta como esta:

```
--with-openssl: no
```

Lo cual explica el hecho de que, al pre configurar el servidor para la posterior puesta en marcha de NRPE, el sistema arroje este error, cabe recalcar que anteriormente se mencionó que NRPE (en el servidor remoto) y Nagios (en el servidor de monitoreo), codificarían la información a intercambiar, a través del algoritmo empleado por SSL.

12. Se procede a instalar los archivos binarios del paquete *Openssl*:

```
apt-get install libssl0.9.8
Apt-get install libssl-dev
```

Esto instala las librerías de SSL dentro de */usr/lib/libssl.so*.

13. Luego de lo cual se hace necesario proveer de un parámetro adicional al comando de configuración ./configure, de la siguiente manera:

```
./configure –with-ssl-lib=/usr/lib/libssl.so
```

Con esto el sistema ubica la librería necesaria dentro del directorio /usr/lib/ para codificar los mensajes de comunicación entre el servidor remoto y Nagios, esto completa la pre configuración.

14. Continua la instalación con la compilación e instalación de la herramienta:

```
make all
make install-plugin
make install-daemon
make install-daemon-config
```

15. Como último paso se enlaza al fichero de configuración de [44]*xinetd*, el demonio NRPE, de la siguiente manera:

```
/usr/bin/install -c -m 644 sample-config/nrpe.xinetd /etc/xinetd.d/nrpe
```

Es necesario enlazar o incluir al aplicativo de red NRPE dentro del servicio *xinetd*, para lo cual se edita el archivo de configuración del mismo *nano /etc/xinet.d/nrpe* la línea concerniente a la dirección IP del servidor que aloja al sistema de monitoreo principal Nagios, en este caso 201.219.36.101:

---

44 XINET: Servicio de red para sistemas UNIX, basado en su predecesor inet para gestionar interfaces, puertos, etc., *xnited* es el demonio de XINET.

```
only_from = 201.219.36.101
```

Es necesario adicionalmente especificarle al servidor remoto el puerto que será abierto para el monitoreo, editando para esto el fichero ***nano /etc/services*** y agregando las líneas:

```
nrpe            5666/tcp        # NRPE
```

Donde se especifica el puerto 5666 en capa de transporte TCP para el monitoreo a través de NRPE.

Con el fin de probar la configuración de NRPE, se echa mano de la herramienta NETSTAT (*Network Statistics*), que es una herramienta de ejecutada en línea de comandos, que muestra un listado de las conexiones activas del servidor, tanto entrantes como salientes, y los puertos utilizados para las mimas, esto se ejecuta de la siguiente manera en el bash de Linux:

```
netstat -at | grep nrpe
```

El comando | enlaza la orden de ***netstat*** a la orden grep nrpe, donde grep no es más que la línea de comandos para desplegar un tipo de información específica, en este caso, la orden le dice al sistema que liste las conexiones abiertas de salida que llevan en su nombre la etiqueta nrpe.

El resultado favorable a la prueba es:

```
tcp        0      0 *:nrpe                  :                 ESCUCHAR
```

Señalando el hecho de que el servicio de red NRPE se halla escuchando las conexiones entrantes.

Luego de instalado el demonio NRPE en el servidor a monitorearse, el sistema incluye ciertos comandos por defecto, los cuales pueden ser editados de acuerdo a las necesidades del sistema, estos comandos, de manera similar al monitoreo del servidor local, monitorean:

Tabla. 3.12 Comandos Básicos NRPE

COMANDO	DETALLE
check_users	número de usuarios locales y remotos registrados en ese momento en el servidor
check_load	Carga Total del servidor remoto
check_hda1	Consumo actual de la partición /root
check_total_procs	Procesos totales ejecutándose en el servidor remoto

Estos comandos serán editados de acuerdo al servidor, para este proyecto los discos duros de los servidores son de tipo *SATA* por lo que el sistema reconoce las particiones de los mismos con las siglas:

sdxn -> Sata Drive,
x = a, b, c (disco duro físico)
n = 1, 2, 3 (partición lógica)

Para comprobar la ubicación de la partición principal en el servidor, se ejecuta el comando *fdisk –l* el cual entregará la siguiente información:

Disposit		Comienzo	Fin	Bloques	Id	Sistema
/dev/sda1	*	1	1870	15020743+	83	Linux
/dev/sda2		1871	1958	706860	5	Extendida
/dev/sda5		1871	1958	706828+	82	Linux swap / Solaris

El listado indica claramente que la partición principal del sistema se halla alojada en *sda1*, por los que se procede a editar el comando para revisar el consumo del disco dentro del fichero *nano /usr/local/nagios/etc/nrpe.cfg* la línea de interés:

```
Command [check_sda1]=/usr/local/nagios/libexec/check_disk -w 20 -c 10 -p /dev/sda1
```

Los argumentos de -w y -c delimitan los umbrales dentro de los cuales:
-w 20 = *WARNING* 20% de espacio libre en la particion /
-c 10 = *CRITICAL* 10% de espacio libre en la particion /
Esto en lo que concierne a la configuración de la herramienta en el servidor remoto.

3.3.4.7 Instalación y configuración de NRPE en el servidor local. Se crea en primera instancia un fichero donde almacenar el código fuente que se va a descargar *mkdir /home/descargas,* luego de ubicarnos en el fichero *cd/home/descargas,* proceso va como sigue:

1. Descargamos el archivo:

```
wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nrpe-2.8.tar.gz
```

2. Descomprimimos el paquete nrpe-2.8.tar.gz e ingresamos al directorio:

```
cd /home/descargas
tar xzf nrpe-2.8.tar.gz
cd nrpe-2.8
```

3. Ejecutamos la orden de configuración de las dependencias del servidor y compilamos la herramienta:

```
./configure
Make all
```

4. Instalamos el aplicativo NRPE llamando al fichero ya compilado

```
Make install-plugin
```

Lugo de este sencillo proceso es necesario comprobar que el aplicativo *chekc_nrpe* instalado tenga comunicación con el demonio NRPE instalado en el servidor remoto, para esto se ejecuta el comando:

```
/usr/local/nagios/libexec/check_nrpe -H <dirección IP servidor remoto>
```

Este comando entregará la versión del demonio NRPE instalado en el servidor remoto, de estar correctamente instalado, por ejemplo:

```
/usr/local/nagios/libexec/check_nrpe -H 201.219.36.98
```

El resultado de dicho comando será NRPE v2.8.

Con el fin de aprovechar las bondades de NRPE, en el server Nagios definimos un comando dentro de los objetos del sistema con el fin de usar el aplicativo *check_nrpe*.
Para el presente sistema se definió el nuevo comando dentro del archivo de configuración *commands.cfg*, se procede a editarlo *nano /usr/local/nagios/etc/objects/commands.cfg*
Agregando la definición del objeto:

```
define command{
        command_name        check_nrpe
        command_line        $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
        }
```

Donde:

- *command_name:* Define la sintaxis del comando utilizado en este caso check_nrpe.
- *command_line:* Asigna la orden que se ejecutará al llamar al comando, las directivas señalan los siguientes parámetros:
- *$USER$/check_nrpe:* Toma el parámetro del usuario que llamará al comando es decir el usuario nagios.
- *-H $HOSTADDRESS$:* Indica la dirección IP del servidor a monitorear

- -c $ARG1$ -> indica el argumento que llevará la llamada, el cual puede ser cualquiera de los comandos propios de NRPE (check_load, check_disk, etc.).

Continuando con el proceso, de acuerdo con la Tabla 3.10 los servidores remotos que Alianzanet requiere monitorear son:

- Servidor DNS
- Servidor SMTP
- Servidor de correo IMAP Zimbra
- Servidor Cliente Corporativo El Puyo
- Servidor Cliente Corporativo EMQT

Anteriormente en la definición del servidor o host local se detallo cada una de las directivas parte de la declaración del host, el archivo donde se agregarán los servidores remotos será por conveniencia el fichero *local_host.cfg* con el fin de aprovechar la herencia en los objetos para cada servidor, *nano /usr/local/nagios/etc/objects/local_host.cfg* agregando las siguientes líneas:

```
define host {
    use                         linux-remoto        ; Name of host template to use
    host_name                   EMT_TELCONET
    alias                       UBUNTU8.04 EMQT OTRS DMZ INTERNET SAMBA
    address                     186.3.3.130
    hostgroups                  LINUXSERVERS
     max_check_attempts         5              ; se chequea 5 veces antes de ser reportado
     notification_interval      5                   ;se notificara a soporte cada 5 minutos
    parents                     CISCO800_TELCO
    notification_period         24x7                ;24 horas 7 dias a la semana
    contact_groups              admins
    notification_options        d,u
    first_notification_delay    0          ;se notificara de inmediato DOWN UNRECHABLE
      }

define host{
   use                          linux-remoto          ; Name of host template to use
   host_name                    SENDMAIL_98
   alias                        UBUNTU8.04  SMTP MRTGFIBERTEL 201.219.36.98
   address                      201.219.36.98
   hostgroups                   LINUXSERVERS
   max_check_attempts           5           ; se chequea 10 veces antes de ser reportado
   notification_interval        5                   ;se notificara a soporte cada 5 minutos
   notification_period          24x7                ;24 horas 7 dias a la semana
```

```
   contact_groups              admins
   notification_options        d,u
    first_notification_delay    0          ;se notificara de inmediato DOWN UNRECHABLE
      }

define host{
     use                    linux-remoto          ; Name of host template to use
     host_name              DNS_100
     alias                  UBUNTU8 SERVIDOR DE NOMBRES 201.219.36.100
     address                201.219.36.100
     hostgroups                    LINUXSERVERS
     max_check_attempts            5        ; se chequea 5 veces antes de ser reportado
     notification_interval         5        ;se notificara a soporte cada 5 minutos
     notification_period           24x7     ;24 horas 7 dias a la semana
     contact_groups                admins
     notification_options          d,u
      first_notification_delay      0     ;se notificara de inmediato DOWN UNRECHABLE
      }

define host{
      use                     linux-remoto          ; Name of host template to use
     host_name                SERVER_PUYO
     alias                    UBUNTU8 SERVIDOR CLIENTE EL PUYO 192.168.61.6
     address                  192.168.61.6
     hostgroups               LINUXSERVERS
     max_check_attempts       5        ; se chequea 10 veces antes de ser reportado
      notification_interval        5              ;se notificara a soporte cada 5 minutos
     notification_period       24x7             ;24 horas 7 dias a la semana
     contact_groups            admins
     notification_options       d,u
      first_notification_delay   0     ;se notificara de inmediato DOWN UNRECHABLE
     parents                     IP_METRO
      }

define host{
      use                     linux-remoto          ; Name of host template to use
     host_name                ZIMBRA_102
     alias                    UBUNTU8 SERVIDOR ZIMBRA 201.219.36.102
     address                  201.219.36.102
     hostgroups               LINUXSERVERS
     max_check_attempts       5       ; se chequea 10 veces antes de ser reportado
     notification_interval     5       ;se notificara a soporte cada 5 minutos
     notification_period       24x7             ;24 horas 7 dias a la semana
     contact_groups           admins
     notification_options      d,u
     first_notification_delay  0     ;se notificara de inmediato DOWN UNRECHABLE
     }
```

Como se puede apreciar en la declaración de los objetos las líneas son idénticas a la declaración de los hosts, excepto en ciertas líneas específicas, que se detallan a continuación:

- ***use linux-remoto*:** Esta línea declara que este host se apega a la configuración heredad de la plantilla linux-remoto , plantilla agregada para el monitoreo de los servidores remotos de Alianzanet en el fichero templates.cfg, esta plantilla consta como se muestra a continuación:

```
define host{
        name                    linux-remoto            ; Name of this template
        use                             generic-host        ; Inherit default values
        check_period                    24x7
        check_interval                  5
        retry_interval                  5
        max_check_attempts          5
        check_command               check-host-alive
        notification_period             24x7
        notification_interval           15
        notification_options            d
        contact_groups              admins, tecnicos
        first_notification_delay        0
        register                    0       ; DONT REGISTER THIS - ITS A TEMPLATE

        }
```

- ***parents CISCO800_TELCO:*** Esta línea define la dependencia del host en relación a otro dentro de la red de Alianzanet, en este caso existe en las líneas antes detalladas dos relaciones de dependencia como reza la Tabla 3.13.

Tabla. 3.13 Parent hosts Alianzanet

PARENT HOST	DIRECCION IP	CHILD HOST	DIRECCION IP
CISCO 2801	201.219.1.210	EL 90% DE LA RED	N/D
IP_METRO	10.10.22.46	SERVER_PUYO	192.168.61.6
CISCO800_TELCONET	186.3.3.129	EMT_TELCONET	186.3.3.130

Las relaciones parent_host – child_host definidas dentro del sistema Nagios, le dan modularidad y escalabilidad al mismo, el sistema guarda una lógica de como se halla estructurada la red.

Es lógico pensar que, dado que el parent_host se halla un salto antes que el child_host , en la relación a la ruta de red, si el parent_host es inaccesible, todos sus child_host también lo serán, esto hace que el sistema notifique a los contactos pertinentes, la caída del host principal, sin tener que notificar todos los host que dependen de este, con el fin de ser eficaz al momento de notificar, ahorrando los recursos que se emplearían al emitir alarmas de todos y cada uno de los host afectados.

Para la declaración de los servicios, se utilizará también el fichero *localhost.cfg*, agregando las siguientes líneas en el mismo:

```
define service{
        use                             generic-service         ; Name of service template to use
        host_name                       EMT_TELCONET
        service_description             PING
        check_command                   check_ping!300.0,20%!800.0,60%
        }
define service{
        use                             generic-service         ; Name of service template to use
        host_name                       SENDMAIL_98
        service_description             PING
        check_command                   check_ping!100.0,20%!500.0,60%
        }
define service{
        use                             generic-service         ; Name of service template to use
        host_name                       ZIMBRA_102
        service_description             PING
```

```
        check_command           check_ping!100.0,20%!500.0,60%
        }
define service{
        use                     generic-service         ; Name of service template to use
        host_name               DNS_100
        service_description      PING
        check_command           check_ping!100.0,20%!500.0,60%
        }
define service{
        use                       generic-service         ; Name of service template to use
        host_name               EMT_TELCONET
        check_command           check_nrpe!check_sda2
        service_description      Particion   root sda2
        }
define service{
        use                       generic-service         ; Name of service template to use
        host_name               SERVER_PUYO
        check_command           check_nrpe!check_sda3
        service_description      Particion root sda3
        }
define service{
        use                       generic-service         ; Name of service template to use
        host_name               SENDMAIL_98
        check_command           check_nrpe!check_sda1
        service_description      Particion root sda1
        }

define service{
        use                     generic-service         ; Name of service template to use
        host_name               ZIMBRA_102
        check_command           check_nrpe!check_sda1
        service_description      Particion root sad1
        }
define service{
        use                     generic-service         ; Name of service template to use
        host_name               DNS_100
        check_command           check_nrpe!check_sda2
        service_description      Particion root sda2
        }
define service{
        use                     generic-service         ; Name of service template to use
        host_name               EMT_TELCONET
        service_description      Total Processes
        check_command           check_local_procs!250!400!RSZDT
        }
define service{
        use                     generic-service
        host_name               SENDMAIL_98
        service_description      Procesos Totales
        check_command           check_nrpe!check_total_procs
```

```
        }
define service{
        use                     generic-service
        host_name               SERVER_PUYO
        service_description      Procesos Totales
        check_command           check_nrpe!check_total_procs
        }

define service{
        use                     generic-service
        host_name               ZIMBRA_102
        service_description      Procesos Totales
        check_command           check_nrpe!check_total_procs
        }
define service{
        use                     generic-service
        host_name               DNS_100
        service_description      Procesos Totales
        check_command           check_nrpe!check_total_procs
        }
define service{
        use                       generic-service       ; Name of service template to use
        host_name               EMT_TELCONET
        service_description      Carga Actual del Servidor
        check_command           check_nrpe!check_load
       }
define service{
        use                       generic-service       ; Name of service template to use
        host_name               ZIMBRA_102
        service_description      Carga Actual del Servidor
        check_command           check_nrpe!check_load
        }
define service{
        use                     generic-service       ; Name of service template to use
        host_name               DNS_100
        service_description      Carga Actual del Servidor
        check_command           check_nrpe!check_load
        }
define service{
        use                     generic-service       ; Name of service template to use
        host_name               SENDMAIL_98
        service_description      Carga Actual del Servidor
        check_command           check_nrpe!check_load
        }
define service{
       use                      generic-service       ; Name of service template to use
       host_name                SERVER_PUYO
       service_description      Carga Actual del Servidor
       check_command            check_nrpe!check_load
       }
```

3.3.4.8 Monitoreo de los enlaces, declaración de hosts. La empresa Alianzanet cuenta con más de 300 enlaces ADSL, de los cuales, el 10% son enlaces corporativos, enlaces que requieren mayor atención por parte del administrador de la red, debido en primera instancia, a los recursos que consumen estos enlaces dentro de la red, a su importancia dentro de la misma, y en segunda instancia, al valor que por estos factura la empresa, mismos atenuantes que contribuyen a que se les brinde un trato especial.

El otro 90% constituyen enlaces residenciales, enlaces que sin dejar de ser importantes, representan el consumo mayoritario de la red de Alianzanet, de este 90% se tomara un 20% a consideración, este lo integran conjuntos habitacionales y edificios, cuya red y acceso a internet los administra Alianzanet, el consumo de estos enlaces merece a su vez, como en el caso de los corporativos, un asiduo seguimiento, el presente apartado cubrirá el monitoreo tanto de los enlaces corporativos de Alianzanet como el de estos conjuntos y edificios. Adicional a esto en el capitulo anterior se dejo en claro que , por políticas de la empresa se tomará en cuenta para el monitoreo a través de la herramienta Nagios solo estos enlaces, mientras que se abordará el consumo generalizado del resto de enlaces como un consumo global, por troncal de acceso y por nodo.

A continuación se detalla la configuración de los objetos, funciones, comandos y sistemas independientes, involucrados en el monitoreo de dichos enlaces.

Dentro de los objetos instalados por defecto en la configuración de Nagios, se procederá a editar el archivo *switch.cfg*, ubicado en */usr/local/nagios/etc/objects/*, este archivo contiene un par de ejemplos de hosts, servicios y grupos declarados, esto con el fin de facilitar la introducción al manejo del sistema, cabe recalcar que en la configuración del archivo principal de Nagios, se habilitó el archivo de configuración *swich.cfg*, al igual que se ha hecho para el resto de ficheros. El monitoreo inicia agregando los siguientes hosts:

```
define host{
        use                     generic-switch
        host_name               CISCO800_TELCO      ;Nombre dentro del sistema
        display_name            GPUNTO CISCO800     ;nombre en la interfaz web
        address                 186.3.3.129         ;direccion IP del Host
        max_check_attempt       5                   ;5 chequeos antes de reportar
        hostgroups              corporativos        ;grupo de host asociados
        notification_interval   5                   ;se notifica cada 5 minutos
        notification_period     24x7                ;24 horas 7 dias a la semana
        contact_groups          admins,tecnicos     ;contactos a notificar
```

```
        notification_options            d,u         ;notifica DOWN UNRECHABLE
        first_notification_delay        0                   ;se notifica inmediatamente
        }
define host{
        use                             generic-switch
        host_name                       PEDROVICENTE        ;Nombre dentro del sistema
        display_name                    PEDRO VICENTE MALDONADO 1Mbps
        address                         201.219.36.89           ;dirección IP del equipo
        max_check_attempt               5                       ;5 comprob. antes de reportar
        hostgroups                      corporativos            ;grupo de host asociados
        parents                         CISCO2801, IPMETRO ;hosts parents
        notification_interval           5                       ;se notifica cada 5 minutos
        notification_period             24x7            ;24 horas 7 dias a la semana
        contact_groups                  admins, técnicos        ;contactos a notificar
        notification_options            d,u             ;notifica DOWN UNRECHABLE
        first_notification_delay        0               ;se notifica inmediatamente
        }

define host{
        use                             generic-switch
        host_name                       PUYO                ;nombre dentro del sistema
        display_name                    CORPORATIVO_EL PUYO
        address                         192.168.61.6        ;dirección IP del host
        max_check_attempt               5                   ;5 chequeos antes de reportar
        hostgroups                      corporativos        ;grupo de host asociados
        parents                         CISCO2801, IPMETRO
        notification_interval           5                   ; se notifica cada 5 minutos
        notification_period             24x7                ;24 horas 7 dias a la semana
        contact_groups                  admins, tecnicos    ;contactos a notificar
        notification_options            d,u                 ;notifica DOWN UNRECHABLE
        first_notification_delay        0                   ;se notifica inmediatamente
        }

define host{
        use                             generic-switch
        host_name                       CANOLASTRA          ; nombre dentro del sistema
        display_name                    CORPORATIVO_FERRETERIA CANO LASTRA
        address                         10.10.22.166        ;IP address of the switch
        max_check_attempt               5                   ;5 chequeos antes de reportar
        hostgroups                      corporativos        ;grupo de host asociados
        parents                         CISCO2801
        notification_interval           5                   ;se notifica cada 5 minutos
        notification_period             24x7                ;24 horas 7 dias a la semana
        contact_groups                  admins, técnicos    ;contactos a notificar
        notification_options            d,u             ;notifica DOWN UNRECHABLE
        first_notification_delay        0                   ;se notifica inmediatamente
        }
define host{
        use                             generic-switch      ;valor heredado de plantilla
        host_name                       CONQUISTADORES      ;nombre dentro del sistema
```

```
    address                 10.2.11.2                   ; direcciones IP del host
    hostgroups              conjuntos               ;grupo de host asociado
     max_check_attempts      5                       ;chequea 5 veces antes de reportado
    notification_period     24x7                    ;24 horas 7 dias a la semana
    notification_interval   10                      ;se notificara cada 10 minutos
  parents                   CISCO2801               ;host parent asociado
  contact_groups            admins, técnicos        ;grupo de contactos a notificar
  notification_options      d,u     ;se notifica estado DOWN UNRECHABLE
  first_notification_delay  0           ;se notifica inmediatamente el cambio de estado
  }
define host{
    use                     generic-switch          ;valores heredados de plantilla
    host_name               ALTAVISTA               ;nombre dentro del sistema
    address                 10.60.0.2               ;direcciones IP del host
    hostgroups              conjuntos               ;grupo de host asociado
    max_check_attempts      5                       ;chequea 5 veces antes de reportado
    notification_period     24x7                    ;24 horas 7 dias a la semana
    notification_interval   10                      ;se notificara cada 10 minutos
    parents                 CISCO2801               ;host parent asociado
    contact_groups          admins, técnicos        ;grupo de contactos a notificar
    notification_options    d,u,          ;se notifica estado DOWN UNRECHABLE
     first_notification_delay  0           ;se notifica inmediatamente el cambio de estado
     }

define host{
    use                     generic-switch          ;valor heredado de plantila
    host_name               PUERTAS                 ;nombre dentro del sistema
    display_name            EL LABRADOR CONJUNTO PUERTA DE HIERRO
    alias                   CONJUNTO PUERTA DE HIERRO
    address                 192.168.12.2            ;dirección IP del host
    hostgroups              conjuntos               ;grupo de host asociado
    max_check_attempts      5                       ; chequea 5 veces antes de reportado
    notification_period      24x7                   ; 24 horas 7 dias a la semana
    notification_interval    10                     ; se notificara cada 10 minutos
    parents                 CISCO2801               ; host parent asociado
    contact_groups          admins, técnicos        ; grupo de contactos a notificar
    notification_options     d,u          ;se notifica estado DOWN UNRECHABLE
    first_notification_delay  0           ;se notifica inmediatamente el cambio de estado
    }
define host{
    use                     generic-switch          ;Valor heredado de plantilla
    host_name               ALCAZAR1                ;Nombre dentro del sistema
    display_name            IPoA EL ALCAZAR
    address                 192.168.77.2            ;IP address of the switch
    hostgroups              conjuntos               ;grupo de host asociado
    max_check_attempts      5                       ;chequea 5 veces antes de reportado
    notification_period      24x7                    ;24 horas 7 dias a la semana
    notification_interval    10                      ;se notificara cada 10 minutos
    parents                  CISCO2801               ;host parent asociado
    contact_groups           admins, técnicos        ; grupo de contactos a notificar
```

```
        notification_options        d,u         ;se notifica estado DOWN UNRECHABLE
        first_notification_delay    0           ;se notifica inmediatamente el cambio de estado
        }
define host{
        use                         generic-switch              ; Valor heredado de plantilla
        host_name                   ALCAZAR2                    ; Nombre dentro del sistema
        display_name                VLAN 3969 EL ALCAZAR
        address                     10.55.0.10                  ;IP address of the switch
        hostgroups                  conjuntos                   ;grupo de host asociado
        max_check_attempts          5                           ;chequea 5 veces antes de reportado
        notification_period         24x7                        ;24 horas 7 dias a la semana
        notification_interval       10                          ;se notificara cada 10 minutos
        parents                     CISCO2801                   ;host parent asociado
        contact_groups              admins, técnicos            ; grupo de contactos a notificar
        notification_options        d,u         ;se notifica estado DOWN UNRECHABLE
        first_notification_delay    0           ;se notifica inmediatamente el cambio de estado
        }
define host{
        use                         generic-switch              ;valor heredado de plantilla
        host_name                   ZUKO                        ;nombre dentro del sistema
        address                     192.168.14.2                ;IP address of the switch
        hostgroups                  conjuntos                   ;grupo de host asociado
        max_check_attempts          5                           ;chequea 5 veces antes de reportado
        notification_period         24x7                        ;24 horas 7 dias a la semana
        notification_interval       10                          ;se notificara cada 10 minutos
        parents                     CISCO2801                   ;host parent asociado
        contact_groups              admins, técnicos            ; grupo de contactos a notificar
        notification_options        d,u         ;se notifica estado DOWN UNRECHABLE
        first_notification_delay    0           ;se notifica inmediatamente el cambio de estado
        }

define host{
        use                         generic-switch              ;valor heredado de plantilla
        host_name                   KIGMAN                      ;nombre dentro del sistema
        display_name                EDIFICIO KIGMAN TRANSTELCO
        address                     200.110.78.174              ;dirección IP del host
        hostgroups                  conjuntos                   ;grupo de host asociado
        max_check_attempts          5                           ;chequea 5 veces antes de reportado
        notification_period         24x7                        ;24 horas 7 dias a la semana
        notification_interval       10                          ;se notificara cada 10 minutos
        parents                     CISCO2801                   ;host parent asociado
        contact_groups              admins, técnicos            ; grupo de contactos a notificar
        notification_options        d,u         ;se notifica estado DOWN UNRECHABLE
        first_notification_delay    0           ;se notifica inmediatamente el cambio de estado
        }
define host{
        use                         generic-switch              ;valor heredado de plantilla
        host_name                   TORRENOVA                   ;nombre dentro del sistema
        display_name                EDIFICIO TORRENOVA TRANSTELCO
        address                     200.110.78.170              ;dirección IP del host
```

```
        hostgroups              conjuntos                   ;grupo de host asociado
        max_check_attempts      5                           ;chequea 5 veces antes de reportado
        notification_period     24x7                        ;24 horas 7 dias a la semana
        notification_interval   10                          ;se notificara cada 10 minutos
        parents                 CISCO2801                   ;host parent asociado
        contact_groups          admins, técnicos            ; grupo de contactos a notificar
        notification_options    d,u         ;se notifica estado DOWN UNRECHABLE
        first_notification_delay 0          ;se notifica inmediatamente el cambio de estado
        }
```

Los comandos utilizados en la declaración de estos hosts, son iguales a los utilizados en la declaración de los host servidores, mencionados anteriormente en el monitoreo de los servidores de Alianzanet.

Cabe recalcar que en este caso el *parent host* de los enlaces, excepto del enlace EMQT, es el router de acceso CISCO2801 parte de la red de acceso de Alianzanet. Para los enlaces fuera de la ciudad se adiciona el parent host IPMETRO, que es la tarjeta IP anexada a la red metro de Andinadatos donde el carrier configura la VLAN 1510 y la IP 10.10.22.46.

Para englobar a los hosts Corporativos, Conjuntos Habitacionales y edificios de Alianzanet, dentro del mencionado fichero *switch.cfg,* se declararan grupos de hosts de la siguiente manera:

- Corporativos
- Conjuntos
- Edificios

```
define hostgroup{
        hostgroup_name          corporativos        ; The name of the hostgroup
        alias                   Enlaces Corporativos dentro y fuera de la ciudad
        }

define hostgroup{
        hostgroup_name          edificios           ; nombre del hostgroup
        alias                   Edificios Alianzanet    ; Nombre en pantalla
        }
define hostgroup{
        hostgroup_name          conjuntos           ; nombre del hostgroup
        alias                   Conjutos Alianzanet     ; Nombre en pantalla
        }
```

Como se había mencionado en la declaración de los servidores, la declaración del hostgroups le da modularidad al sistema, permite al administrador organizar a los hosts al momento de monitorearlos, de esta manera es más sencilla y organizada su administración y visualización.

3.3.4.9 Monitoreo de los enlaces, declaración de los servicios. Los servicios involucrados en el monitoreo del grupo corporativos son los siguientes:

```
define service{
        use                     generic-service         ; heredado de plantilla
        host_name               CISCO800_TELCO      ;host asociado al servicio
        service_description     CONSUMO CISCO 870
        check_command           check_ping!200.0,20%!800.0,60%
        normal_check_interval   5       ;se chequea cada 5 minutos el servicio
        retry_check_interval    1       ;se chequea 2 veces antes de emitir alerta
        }

define service{
        use                     generic-service         ; heredado de plantilla
        host_name               CISCO800_TELCO      ; host asociado al servicio
        service_description     ESTADO DEL ROUTER PRINCIPAL EMQT
        check_command           check-host-alive        ; Comando para el monitoreo
        normal_check_interval   5       ;se chequea cada 5 minutos el servicio
        retry_check_interval    1       ;se chequea 2 veces antes de emitir alerta
        }

define service{
        use                     generic-service         ; heredado de plantilla
        host_name               PEDROVICENTE            ; host asociado al servicio
        service_description     ESTADO ENLACE PEDROVICENTE
        check_command           check-host-alive        ; comando para monitoreo
        normal_check_interval   5       ; se chequea cada 5 minutos el servicio
        retry_check_interval    1       ; se chequea 2 veces antes de emitir alerta
        }
define service{
        use                     generic-service         ; heredado de plantilla
        host_name               CANOLASTRA              ; host asociado al servicio
        service_description     ESTADO ENLACE CANOLASTRA
        check_command           check-host-alive    ;comando para monitoreo
        normal_check_interval   5       ;se chequea cada 5 minutos el servicio
        retry_check_interval    1       ;se chequea 2 veces antes de emitir alerta
        }

define service{
        use                     generic-service         ; heredado de plantilla
        host_name               PEDROVICENTE            ; host asociado al servicio
        service_description     CONSUMO PEDROVICENTE
        check_command           check_ping!200.0,20%!800.0,60%
        normal_check_interval   5       ; se chequea cada 5 minutos el servicio
        retry_check_interval    1       ; se chequea 2 veces antes de emitir alerta
        }
```

```
define service{
        use                     generic-service         ; heredado de plantilla
        host_name               PUYO                    ; host asociado al servicio
        service_description     CONSUMO EL PUYO         ;Descripcion del servicio
        check_command           check_ping!200.0,20%!800.0,60%   ;
        normal_check_interval   5       ; se chequea cada 5 minutos el servicio
        retry_check_interval    1       ; se chequea 2 veces antes de emitir alerta
        }
define service{
        use                     generic-service         ; heredado de plantilla
        host_name               CANOLASTRA              ; host asociado al servicio
        service_description     CONSUMO CANOLASTRA
        check_command           check_ping!200.0,20%!800.0,60%      ;
        normal_check_interval   5       ;se chequea cada 5 minutos el servicio
        retry_check_interval    1       ;se chequea 2 veces antes de emitir alerta
        }
define service{
        use                     generic-service         ;valor heredado de plantilla
        host_name               KIGMAN                  ;host asociado al servicio
        service_description     ESTADO ENLACE KIGMAN    ;nombre en pantalla
        check_command           check-host-alive        ;comando asociado a servicio
        normal_check_interval   5                       ;se chequea cada 5 minutos
        retry_check_interval    1                       ;se re chequea despues de 1 min
        }

define service{
        use                     generic-service         ;valor heredado de plantilla
        host_name               TORRENOVA               ;host asociado al servicio
        service_description     ESTADO EDIFICIO TORRENOVA   ;nombre en pantalla
        check_command           check-host-alive        ;comando asociado a servicio
        normal_check_interval   5                       ;se chequea cada 5 minutos
        retry_check_interval    1                       ;se re chequea despues de 1 min
        }

define service{
        use                     generic-service         ;valor heredado de plantilla
        host_name               BANCO_GUAYAQUIL         ;host asociado al servicio
        service_description     ESTADO BANCO DE GUAYAQUIL COLON   ;nombre en pantalla
        check_command           check-host-alive        ;comando asociado a servicio
        normal_check_interval   5                       ;se chequea cada 5 minutos
        retry_check_interval    1                       ;se re chequea despues de 1 min
        }

define service{
        use                     generic-service         ;valor heredado de plantilla
        host_name               ALCAZAR2                ;host asociado al servicio
        service_description     ESTADO DE VLAN ALCAZAR2         ;nombre en pantalla
        check_command           check-host-alive        ;comando asociado a servicio
```

```
        normal_check_interval     5                              ;se chequea cada 5 minutos
        retry_check_interval      1                              ;se re chequea despues de 1 min
        }

define service{
        use                       generic-service                ;valor heredado de plantilla
        host_name                 ZUKO                           ;host asociado al servicio
        service_description       CONSUMO EL ZUKO                ;nombre en panalla
        check_command             check-host-alive               ;comando asociado a servicio
        normal_check_interval     5                              ;se chequea cada 5 minutos
        retry_check_interval      1                              ;se re chequea despues de 1 min
        }

define service{
        use                       generic-service                ;valor heredado de plantilla
        host_name                 KIGMAN                         ;host asociado al servicio
        service_description       CONSUMO EDIFICIO KIGMAN        ;nombre en pantalla
        check_command             check-host-alive               ;comando asociado a servicio
        normal_check_interval     5                              ;se chequea cada 5 minutos
        retry_check_interval      1                              ;se re chequea despues de 1 min
        }

define service{
        use                       generic-service                ;valor heredado de plantilla
        host_name                 TORRENOVA                      ;host asociado al servicio
        service_description       CONSUMO TORRENOVA              ;nombre en pantalla
        check_command             check_ping!200.0,20%!900.0,40% ;comando asociado al servicio
        normal_check_interval     5                              ;se chequea cada 5 minutos
        retry_check_interval      1                              ;se re chequea despues de 1 min
        }

define service{
        use                       generic-service                ;valor heredado de plantilla
        host_name                 BANCO_GUAYAQUIL                ;host asociado al servicio
        service_description       CONSUMO BANCO DE GUAYAQUIL COLON ;nombre en pantalla
        check_command             check_ping!200.0,20%!900.0,40% ;comando asociado al servicio
        normal_check_interval     5                              ;se chequea cada 5 minutos
        retry_check_interval      1                              ;se re chequea despues de 1 min
        }

define service{
        use                       generic-service                ;valor heredado de plantila
        host_name                 PUERTAS
        service_description       CONSUMO PUERTAS                ;nombre en pantalla
        check_command             check_ping!200.0,20%!900.0,40% ;comando asociado al servicio
        normal_check_interval     5                              ;se chequea cada 5 minutos
        retry_check_interval      1                              ;se re chequea despues de 1 min
        }
```

```
define service{
        use                     generic-service                 ;valor heredado de plantilla
        host_name               ALTAVISTA                       ;host asociado al servicio
        service_description     CONSUMO ALTAVISTA               ; nombre en pantalla
        check_command           check_ping!200.0,20%!900.0,40%  ;comando asociado al servicio
        normal_check_interval 5                                 ;se chequea cada 5 minutos
        retry_check_interval    1                               ;se re chequea despues de 1 min
        }

define service{
        use                     generic-service                 ;valor heredado de plantilla
        host_name               CONQUISTADORES                  ;host asociado al servicio
        service_description     CONSUMO CONQUISTADORES          ;nombre en pantalla
        check_command           check_ping!200.0,20%!900.0,40% ;comando asociado al servicio
        normal_check_interval 5                                 ;se chequea cada 5 minutos
        retry_check_interval    1                               ;se re chequea despues de 1 min
        }


define service{
        use                     generic-service                 ;valor heredado de plantilla
        host_name               ALCAZAR1                        ;host asociado al servicio
        service_description     CONSUMO EL ALCAZAR1             ;nombre en pantalla
        check_command           check_ping!200.0,20%!900.0,40%  ;comando asociado al servicio
        normal_check_interval   5                               ;se chequea cada 5 minutos
        retry_check_interval    1                               ;se re chequea despues de 1 min
        }

define service{
        use                     generic-service                 ;valor heredado de plantilla
        host_name               ALCAZAR2                        ;host asociado al servicio
        service_description     CONSUMO ENLACE VLAN ALCAZAR2  ;nombre en pantalla
        check_command           check_ping!200.0,20%!900.0,40%  ;comando asociado al servicio
        normal_check_interval 5                                 ;se chequea cada 5 minutos
        retry_check_interval    1                               ;se re chequea despues de 1 min
        }
define serviceextinfo{
        host_name               CANOLASTRA
        service_description     CONSUMO CANOLASTRA
        notes_url               http://201.219.36.101/mrtg/201.219.1.210_se0_2_0.150.html
        icon_image              mrtg-m.png
        }
define serviceextinfo{
        host_name               ZUKO                            ;host asociado al servicio
        service_description     CONSUMO EL ZUKO                 ;nombre del servicio enlace al gráfico
        notes_url       http://201.219.36.101/mrtg/201.219.1.210_se0_1_1_0.180.html ;grafico MRTG
        icon_image              mrtg-m.png                      ;ícono alusivo al gráfico
        }

define serviceextinfo{
      host_name             CONQUISTADORES                  ;host asociado al servicio
      service_description   CONUSUMO CONQUISTADORES ;nombre del servicio enlace al grafico
      notes_url       http://201.219.36.101/mrtg/201.219.1.210_se0_1_0_0.135.html  ;grafico MRTG
      icon_image            mrtg-m.png                      ;ícono alusivo al gráfico
        }
```

```
define serviceextinfo{
      host_name               ALTAVISTA                          ;host asociado al servicio
      service_description     CONSUMO ALTAVISTA                  ;nombre del servicio enlace al gráfico
      notes_url          http://201.219.36.101/mrtg/201.219.1.210_se0_1_0_0.16.html  ;gráfico MRTG
      icon_image              mrtg-m.png                         ;ícono alusivo al gráfico
      }

define serviceextinfo{
      host_name               ZUKO                               ;host asociado al servicio
      service_description     CONSUMO EL ZUKO                    ;nombre del servicio enlace al gráfico
      notes_url          http://201.219.36.101/mrtg/201.219.1.210_se0_1_1_0.180.html  ;gráfico MRTG
      icon_image              mrtg-m.png                         ;ícono alusivo al gráfico
      }

define serviceextinfo{
      host_name               CONQUISTADORES                     ;host asociado al servicio
      service_description     CONUSUMO CONQUISTADORES ;nombre del servicio enlace al gráfico
      notes_url      http://201.219.36.101/mrtg/201.219.1.210_se0_1_0_0.135.html   ;gráfico MRTG
      icon_image              mrtg-m.png
      }

define serviceextinfo{
      host_name               ALTAVISTA                          ;host asociado al servicio
      service_description     CONSUMO ALTAVISTA                  ;nombre del servicio enlace al gráfico
      notes_url          http://201.219.36.101/mrtg/201.219.1.210_se0_1_0_0.16.html  ;gráfico MRTG
      icon_image              mrtg-m.png                         ;ícono alusivo al gráfico
      }
```

La declaración de los servicios, llamados a monitorear los hosts corporativos, sigue de igual manera que en la declaración del resto de servicios, detallados anteriormente para el monitoreo de los servidores, por lo tanto se describirá a continuación solo aquellos objetos que se han introducido específicamente para el monitoreo de estos enlaces.

- ***define serviceextinfo{***

Información extendida del servicio, su objetivo es crear un enlace dentro de la interfaz de visualización de Nagios, desde la línea donde se halla detallado el servicio, hacia virtualmente cualquier sitio o servidor dentro de la red de Alianzanet, en este caso, se ha asociado al servicio y al host, un enlace a las gráficas generadas por la herramienta MRTG, para que el administrador, pueda visualizar el grafico de consumo del enlace, de las últimas 12 horas.

Cabe recalcar que en este caso, para el proyecto desarrollado, la herramienta se halla instalada en el servidor de monitoreo, alojando a los dos sistemas dentro de si, tanto NAGIOS como MRTG.

- ***service_description*** ***CONSUMO CANOLASTRA***

Aquí se especifica el servicio para el cual estará disponible la información extra, es decir la gráfica de MRTG para el enlace en cuestión, el cliente corporativo CANOLASTRA.

- ***notes_url*** ***http://201.219.36.101/mrtg/201.219.1.210_se0_2_0.150.html***

Estas líneas le dicen al sistema, la ubicación exacta de la gráfica, dentro del directorio de apache2 en el fichero -> mrtg -> especificando el nombre de la gráfica que se presentará al dar click en el estado del servicio, en la interfaz de monitoreo html de Nagios.

- ***icon_image*** ***mrtg-m.png***

Selecciona del directorio iconos del sistema Nagios, la imagen o el ícono que representará el acceso a la gráfica, se ha escogido la letra G de MRTG, dejando en claro que la gráfica pertenece a este sistema.

Se hace importante anotar, que la gráfica generada por MRTG, podría, en teoría, ser tomada de cualquier servidor que contenga el sistema instalado y configurado, con una dirección IP, que sin ser pública, sea de libre acceso para el servidor que alberga a Nagios.

En la práctica esto no sucede, ya que, por motivos de seguridad, se definen dentro de los servidores estrictas políticas para el acceso remoto a los mismos, esto a directorios públicos específicos definidos por el administrador del sistema, en este caso, el fichero que alberga las gráficas de MRTG es:

/var/www/mrtg

Correspondiente a archivos de configuración del servidor web apache2, mismos que por obvias razones, están restringidos a todos los usuarios locales, excepto al administrador, mucho más, si se tratara de un usuario remoto no identificado.

En este punto estriba la ventaja de tener instalado y configurado el sistema MRTG en el mismo servidor que alberga al sistema Nagios, los dos sistemas no solo comparten un servidor físico, sino que el usuario nagios es parte del grupo de usuarios de root, con acceso a virtualmente “todo ” dentro del servidor, no se diga a las gráficas generadas por MRTG.

En este punto, es importante señalar un hecho particular, parte de la configuración de nagios, y es que, la plantilla utilizada como base, para declarar los hosts detallados en esta sección, al igual que para los hosts que se declararan más adelante, es la plantilla *generic-switch*, incluida en el fichero templates de nagios, esto no implica bajo ningún concepto, que se tratará a los routers como switch, ni mucho menos, en lo que concierne a la red, sino simplemente, se aprovecha la declaración de esta plantilla general, habilitada adicionalmente en el archivo principal nagios.cfg , el archivo es susceptible a renombrarse, o en su defecto, cabe la posibilidad de crear plantillas adicionales, para módems y routers, equipos encargados de los enlaces WAN, sin embargo los valores incluidos en estos, los mismos declarados para la plantilla *switch.cfg*, por lo que, se conservará el uso de esta plantilla. Adicionalmente a esto, se reitera el hecho de que, en la declaración de los host, los argumentos enunciados en los parámetros, tienen prioridad sobre aquellos incluidos en la plantilla.

3.3.4.10 Monitoreo de los Routers, declaración de los hosts. A continuación se detallarán los host y servicios creados para el monitoreo de estos elementos activos dentro de la red de Alianzanet.

Este grupo de hosts está conformado principalmente por tres equipos los cuales constituyen el core de la red de Alianzanet:

- CISCO 2801 (Nodo Carolina)
- CISCO 1800 (Nodo Iñaquito)
- CISCO 870 (EMQT)

En este punto es importante mencionar que la intervención del protocolo *SNMP* será fundamental para el control de estos equipos, no solo por la oportunidad que nos brindan estos equipos de monitorearlos usando esta poderosa herramienta, sino por la innumerable gama de información que nos ofrece *SNMP*, para conocer de principio a fin el estado de los servicios, recursos e interfaces, parte de estos elementos tan importantes dentro de la red de Alianzanet.

Adicionalmente a esto se ha incluido el monitoreo del router CISCO 870 parte esencial de la red de la EMQT, esto por dos razones:

- El acceso de este enlace al internet se lo realiza por medio de la red de Telconet, el cual es también empresa portadora, este enlace podría ser aprovechado por

Alianzanet para troncalizar su acceso y utilizarlos para brindar servicio a través del Backbone de Telconet.

- Es importante el monitoreo del consumo de este enlace, no solo tomando en cuenta que su facturación es la más alta dentro de la cartera de clientes corporativos de Alianzanet, sino que al conocer exactamente el promedio de consumo de este enlace, se puede conocer cuánto de este canal puro de 2Mbps se desperdicia, y cuanto se podría aprovechar para el acceso y troncalizado de enlaces sobre el backbone del carrier, en este caso Telconet.

Core, Acceso y Border de los nodos Carolina e Iñaquito, los routers CISCO 2801 y 1800 tienen a su cargo un elevado flujo de tráfico, por lo que se hace imprescindible el monitorear ciertos servicios fundamentales. Cabe recalcar que la instalación de los aplicativos *Net-snmp* y *Net-snmtp-utils*, necesarios para la puesta en marcha del sistema MRTG, serán de vital importancia para el uso del comando *check_snmp*, comando que hará la llamada a las diferentes instancias de SNMP dentro del sistema Nagios.

Detalle de los servicios:

Dentro de los objetos instalados por defecto en la configuración de Nagios, se procederá a editar el archivo *switch.cfg*, agregando los siguientes hosts:

```
define host{
        use                     generic-switch              ;valor heredado de plantilla
        host_name               CISCO800_TELCO      ;nombre dentro del sistema
        alias                   CISCO800 TELCONET  ;nombre en pantalla
        address                 186.3.3.129         ;direccion IP del host
        max_check_attempts      5                   ;se chequea 5 veces para reporte
        hostgroups              routers             ;grupo de host  asociado
        notification_interval   10                  ;se notifica cada 10 min
        notification_period     24x7                ;24 horas 7 dias
        contact_groups          admins,tecnicos     ;contactos a notificar
        notification_options    d,u                 ;se notifica DOWN  UNREACHABLE
        first_notification_delay  0                 ;se notifica inmediatamente
        }

define host{

        use                     generic-switch              ;valor heredado de pantilla
        host_name                 CISCO1800                 ;nombre dentro del sistema
        alias                   CISCO1800 FIBERTEL BORDER  ;nombre CGI
        address                 201.219.0.70                ;direccion IP del host
        max_check_attempts      5                   ;se chequea 5 veces para reporte
        hostgroups              routers             ;grupo de host  asociado
        notification_interval   10                  ;se notifica cada 10 min
        notification_period     24x7                ;24 horas 7 dias
        contact_groups          admins,tecnicos     ;contactos a notificar
        notification_options    d,u                 ;se notifica DOWN  UNREACHABLE
        first_notification_delay  0                 ;se notifica inmediatamente
        }
```

```
define host{

        use                     generic-switch          ;valor heredado de plantilla
        host_name               CISCO2801       ;nombre dentro del sistema
        alias                   CISCO2801 ALIANZANET BORDER  ; nombre CGI
        address                 201.219.1.210           ; direccion IP del host
        max_check_attempts      5                       ; se chequea 5 veces para reporte
        hostgroups              routers                 ; grupo de host  asociado
        notification_interval   10                      ; se notifica cada 10 min
        notification_period     24x7                    ; 24 horas 7 dias
        contact_groups          admins,tecnicos         ; contactos a notificar
        notification_options    d,u                     ; se notifica DOWN  UNREACHABLE
        first_notification_delay  0                     ; se notifica inmediatamente
        }
```

La declaración de los objetos, en cuanto a formato y función, sigue como el resto de hosts, se puede notar para este caso, que el intervalo entre chequeos al host es mucho menor que para el resto de objetos, al igual que el número de veces que se chequea el host antes de cambiar de estado, esto debido a que , por obvias razones, estos equipos constituyen el CORE de la red, por lo que es necesario conocer, con la debida anticipación, en caso de existir fallas en los mismos.

Por otro lado, el monitoreo de estos equipos nos entrega importante información de la red en todos los sentidos, ya que son estos equipos los que sustentan el funcionamiento de las misma.

De manera similar a los host anteriores, se declara un grupo de host que reúna a los ruteadores administrados por Alianzanet, de la siguiente manera:

```
define hostgroup {
        hostgroup_name          routers   ; nombre del grupo de hosts dentro del sistema
        Alias                   Routers Alianzanet   ; nombre en pantalla
        }
```

3.3.4.11 Monitoreo de los Routers, declaración de los servicios. La declaración de los servicios se realizará dentro del archivo switch.cfg , como se detalla a continuación:

- *Tiempo de vida del sistema (System Up Time):* Este servicio se monitorea usando el protocolo SNMP, el router informa periódicamente al sistema Nagios el tiempo durante el cual se encuentra en estado UP, desde la última vez que se encontró un desperfecto.

- *Estado de las interfaces (Interface Oper Status):* Se monitoreará el estado de los enlaces, border, Vlan, etc., utilizando este útil comando de SNMP, con el fin de determinar si se encuentran habilitados o no dichos enlaces o interfaces.
- *Consumo de Memoria (Memory Load):* Esta herramienta nos entregará el consumo de memoria de procesador, Interfaces y RAM, de cada 5 minutos, se escogió a propósito este intervalo, ya que al enviar peticiones SNMP, desd el servidor hacia e ruteador se ve también afectado el consumo de memoria de proceso del mismo, por lo que un intervalo más largo entre cada consulta es ideal.
- *Carga del procesador (CPU Load):* El servidor enviará peticiones SNMP cada 5 minutos, con el fin de conocer la carga del procesador a ese instante, esta variable es fundamental, ya que en un estudio de sobre estimación de la red, la carga del CPU del router nos da una medida, de la factibilidad de ampliar la red, tomando en cuenta la carga promedio del equipo bajo las condiciones actuales.
- *Gráficos MRTG:* Adicional al estado y control de estos servicios, las herramientas instaladas en el servidor, tales como MRTG, serán muy útiles al momento de visualizar las variables controladas a través de SNMP, ya que, si bien es cierto, el tema del monitoreo en este caso recae en estos dos puntos de manera categórica, no solo visualizando el comportamiento de estas variables en los equipos activos, sino teniendo un control y notificación de cuando estas exceden los umbrales establecidos por el administrador del sistema.

En este punto se hace necesario recordar, lo visto en capítulos anteriores acerca de las bondades y la forma de funcionamiento del protocolo SNMP, más adelante se verá que, los datos involucrados en la comunicación, por parte de Net -SNMP en el servidor, y SNMP v1 en el router, se basarán en el transporte y traducción de las OID y MIB de CISCO, la interpretación de estas por parte del servidor será fundamental para el monitoreo.

Adicional a esto cabe recalcar que los comandos y las funciones con extensión .pl , fueron adaptados para poder funcionar dado las necesidades específicas del proyecto, para que el sistema Nagios pueda interactuar con las funciones check_snmp_load.pl y check_snmp_mem.pl , hubo a necesidad de cumplir dos pasos fundamentales:

1.- Agregar las funciones al directorio */usr/local/nagios/libexec/,* directorio donde se encuentran declarados los scripts, encargados de ejecutar los comandos de verificación de tipo check. Se debe especificar al sistema Linux, cual es el usuario propietario de estos scripts, y darles privilegios de ejecución, de la siguiente manera:

```
chowner nagios check_snmp_load.pl & check_snmp_mem.pl
chmod 644 check_snmp_load.pl & check_snmp_mem.pl
```

El índice del comando *change module (chmod) 664*, obedece a la notación del nivel de permisos que tienen los usuarios, en este caso el que nos interesa es el usuario propietario o Owner del script, que debe tener acceso de lectura y ejecución del script, esto simboliza el numero 6.

2.- Especificar dentro del archivo de recursos de Nagios, */usr/local/nagios/etc/resources.cfg*, la habilitación de estos dos scripts ejecutables, dejando establecido la ubicación de los mismos, y el usuario de nagios que ejecutará dichos comandos, agregando una línea en el archivo, de la siguiente manera:

```
$USER10$/usr/local/nagios/libexec/tesis
```

Este usuario será utilizado por los comandos declarados en commands.cfg para ejecutarlos con el permiso otorgado en el archivo de recursos.

Los servicios se declaran a continuación:

```
define service{

   use                          generic-service          ;valor heredado de plantilla
   host_name                    CISCO2801                ;nombre dentro del sistema
   service_description          CONSUMO BORDER ALIANZANET   ;nombre CGI
   check_command          check_ping!200.0,20%!800.0,60%      ;comado asociado al servicio
    normal_check_interval            5                    ;chequea el estado cada 5 minutos
   retry_check_interval              1                    ;se chequea 1 adicional antes de reportar
   }

define service{
   use                          generic-service              ;valor heredado de plantilla
   host_name                    CISCO2801
   service_description          Uptime
   check_command          check_snmp!-C public1 -o sysUpTime.0  ;comado asociado al sevicios
   normal_check_interval  5                    ;chequea el estado cada 5 minutos
   retry_check_interval              1                     ;se chequea 1 adicional antes de reportar
}

define service{
    use                          generic-service  ;valor heredado de plantilla
   host_name                    CISCO2801
   service_description          Consumo del procesador
   check_command          check_snmp_load_alianza!90,80,60!99,99,99!cisco!
    normal_check_interval          5              ;chequea el estado cada 5 minutos
    retry_check_interval           1              ;se chequea 1 adicional antes de reportar
}

define service{
      use                          generic-service ;valor heredado de plantilla
```

```
      host_name                CISCO2801
      service_description      Consumo de Memoria
      check_command            check_snmp_mem_alianza!90,80!98,98!-I!
      normal_check_interval    5          ;chequea el estado cada 5 minutos
      retry_check_interval     1          ;se chequea 1 adicional antes de reportar
}

define service{
   use                         generic-service        ;valor heredado de plantilla
   host_name                   CISCO1800              ;nombre dentro del sistema
   service_description         CONSUMO BORDER FIBERTEL  ;nombre CGI
   check_command         check_ping!200.0,20%!800.0,60%      ;comado asociado al servicio
    normal_check_interval      5                  ;chequea el estado cada 5 minutos
   retry_check_interval        1                  ;se chequea 1 adicional antes de reportar
}

define service{
  use                          generic-service          ;valor heredado de plantilla
  host_name                    CISCO1800
  service_description          Uptime
  check_command          check_snmp!-C fibertel -o sysUpTime.0  ;comado asociado al sevicios
   normal_check_interval       5                   ;chequea el estado cada 5 minutos
  retry_check_interval         1                   ;se chequea 1 adicional antes de reportar
}
define service{
    use                        generic-service  ;valor heredado de plantilla
   host_name                   CISCO1800
   service_description         Consumo del procesador
   check_command               check_snmp_load_fibertel!90,80,60!99,99,99!cisco!
    normal_check_interval      5          ;chequea el estado cada 5 minutos
    retry_check_interval       1          ;se chequea 1 adicional antes de reportar
}

define service{
       use                     generic-service ;valor heredado de plantilla
      host_name                CISCO1800
      service_description      Consumo de Memoria
      check_command            check_snmp_mem_fibertel!90,80!98,98!-I!
      normal_check_interval    5          ;chequea el estado cada 5 minutos
      retry_check_interval     1          ;se chequea 1 adicional antes de reportar
}
define service{
   use                         generic-service        ;valor heredado de plantilla
   host_name                   CISCO800_TELCO                ;nombre dentro del sistema
   service_description         CONSUMO ENLACE CCEE TELCONET   ;nombre CGI
   check_command         check_ping!200.0,20%!800.0,60%      ;comado asociado al servicio
    normal_check_interval      5                  ;chequea el estado cada 5 minutos
   retry_check_interval        1                  ;se chequea 1 adicional antes de reportar

}

define service{
   use                         generic-service          ;valor heredado de plantilla
   host_name                   CISCO800_TELCO
   service_description         Uptime
   check_command          check_snmp!-C CCEETELCO -o sysUpTime.0  ;comado asociado al sevicios
    normal_check_interval      5                   ;chequea el estado cada 5 minutos
   retry_check_interval        1                   ;se chequea 1 adicional antes de reportar
}
```

```
define service{
    use                         generic-service  ;valor heredado de plantilla
   host_name                    CISCO800_TELCO
   service_description          Consumo del procesador
   check_command                check_snmp_load_CCEE!90,80,60!99,99,99!cisco!
    normal_check_interval       5               ;chequea el estado cada 5 minutos
    retry_check_interval        1               ;se chequea 1 adicional antes de reportar
}

define service{

      use                       generic-service ;valor heredado de plantilla
     host_name                  CISCO800_TELCO
     service_description        Consumo de Memoria
     check_command              check_snmp_mem_CCEE!90,80!98,98!-I!
     normal_check_interval      5               ;chequea el estado cada 5 minutos
     retry_check_interval       1               ;se chequea 1 adicional antes de reportar
}

define service{
       use                      generic-service    ; Inherit values from a template
       host_name                CISCO2801
       service_description      BORDER CAROLINA
       check_command            check_mrtgtraf!/var/www/mrtg/201.219.1.210_fa0_1.log\
      !AVG!1000000,!4500000
          }
define service{
       use                      generic-service    ; Inherit values from a template
       host_name                CISCO2801
       service_description      BORDER IÑAQUITO
       check_command            check_mrtgtraf!USER1!@201.219.36.98:/var/www/mrtg/201.219.0.70_fa1_0.log!\
       password: futur07!AVG!1000000,!4000000
          }
```

Para la declaración de este grupo de hosts, se han adicionado ciertos objetos, no incluidos en apartados anteriores, que hacen minucioso el trabajo de notificación del sistema, por otro lado, se han agregado comandos elaborados específicamente para cumplir el objetivo de este proyecto, tomando en cuenta también la topología de la red.

```
normal_check_interval       5               ; chequea el estado cada 5 minutos
```

Designa el intervalo entre puntos de verificación del servicio, la plantilla *generic-service* incluye un tiempo nominal de 10 minutos, entre cada chequeo del estado del servicio, en ese caso se ha reducido a la mitad este tiempo con el fin de tener un monitoreo más agresivo del estado del servicio, esto debido a la importancia del mismo dentro de la red de CORE de Alianzanet.

La razón por la cual no se ha modificado el intervalo de verificación del resto de servicios, no solo estriba en el echo de que se les confiere un nivel de importancia MEDIO y BAJO

(Corporativos y Conjuntos), con respecto al consumo de recursos del servidor para su monitoreo, sino por el echo de que, a pesar de que el servidor en cuestión estuviera en capacidad de soportar, la carga de trabajo que implica, chequear todos los servicios cada 5 minutos, no es recomendable realizarlo de esta manera, ya que se hace improcedente desperdiciar tal volumen de recursos, pudiendo dar prioridad a otros servicios, como es el caso del los routers o servidores remotos, para los cuales (servidores remotos) se está utilizando un volumen generoso de recursos para ejecutar la herramienta NRPE.

retry_check_interval 1 ; se chequea 1 adicional antes de reportar

Establece el que se chequee el estado del servicio, una vez adicional, en caso de que se haya superado el número de peticiones de revisión nominales, se solicita que se verifique dos veces, antes del cambio de estado y la posterior notificación.
Esto le da un tratamiento preferencial al servicio, ya que, al contrario del resto de servicios, para los cuales se ejecuta una sola ronda de verificación cada 10 minutos, para los routers administrados por Alianzanet, dentro de una ronda de verificación, se chequea dos veces su estado.

check_mrtgtraf!/var/www/mrtg/201.219.1.210_fa0_1.log!AVG!1000000,!4500000

Este comando permite a Nagios, usar la información SNMP registrada en el fichero */var/mrtg/* dentro del cual se almacenan, no solo las gráficas generadas por MRTG, sino también los archivos *log* de MRTG, con esta información Nagios establece los umbrales sobre los cuales el consumo de determinada interfaz, en este caso la interfaz de border, se encuentra en estado *WARNING* o *CRITICAL*.
Umbral Inferior: 1000000 bps, 1Mpbs consumo demasiado bajo
Umbral Promedio: AVG, AVERAGE, promedio entre umbral inferior y superior
Umbral Superior: 4500000 bps, 4.5 Mbps consumo demasiado alto la interfaz entro en saturación.
Para el caso del router de core del nodo Iñaquito, se agregan parámetros adicionales como son:

USER1!@201.219.36.98:/var/www/201.219.0.70_fa1_0.log!\password:futur07

como se había indicado anteriormente, el sistema MRTG establece una sola clave de comunidad, para un solo host en particular, dado que el servidor que aloja a Nagios y MRTG (Nodo Carolina) es el mismo, para acceder al sistema MRTG (Nodo Iñaquito) es necesario ingresar en modo *usuario Nagios* al servidor remoto que lo aloja, cuya dirección IP es 201.219.36.98 y cuya clave para este usuario es futur07, hay que recordar que, de lo visto en apartados anteriores, todos los servidores remotos a monitorearse tienen creado el usuario Nagios, necesario para la instalación y funcionamiento de NRPE.

En cuanto a los comandos SNMP, la Figura 3.20 muestra la interacción entre el sistema Nagios, SNMP, y los equipos CISCO en cuestión, Nagios realiza el llamado al demonio Net-SNMP de Linux para que este a su vez, consulte al equipo CISCO, por el estado de estos servicios, vitales para el correcto funcionamiento de la red.

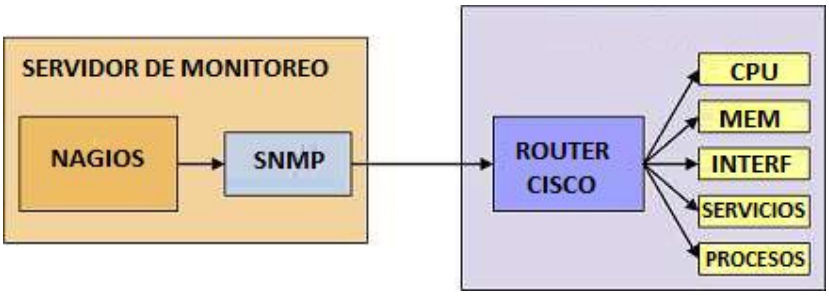


Figura. 3.24 Nagios SNMP

Los comandos utilizados para el monitoreo de los routers difieren de cierta manera de los comandos y servicios utilizados para el monitoreo del resto de enlaces y hosts, esto debido a las ventajas de las que nos provee *SNMP*, los scripts aplicados en el monitoreo de los routers CISCO fueron adaptados específicamente a las condiciones de la red de Alianzanet a la configuración misma del servidor Nagios, parte de este proyecto. A continuación se resume los detalles de estos comandos.

- ***Check snmp mem***. Este comando, como su declaración lo indica, solicita el consumo en porcentaje de memoria cada 5 minutos en el router, memoria de procesamiento, RAM y flash, en la fase de notificación, entrega al comando principal, declarado en commands.cfg, 4 argumentos, a saber:
  - Dirección IP del host

- Umbral de estado crítico (*CRITICAL*), el servicio pasará a estado crítico, cuando el consumo de memoria rebase, luego de las 5 comprobaciones de rigor, el 98% de su capacidad total, esto según estándares CISCO de desempeño.
- Umbral de estado de peligro (*WARNING*), el servicio pasará al estado warning, cuando supere el umbral, es decir el 80 % de consumo de memoria.
- Tipo de host, el script llamado a interactuar directamente con el ruteador, requiere este argumento para saber qué tipo de equipo esta monitoreando, con el fin de aplicar las normativas según el tipo de sistema, el argumento ' – I ' le indica a la función que el equipo es un elemento de red activo CISCO.

La sintaxis dentro de la declaración del servicio es como se vio en la líneas de código:

```
check_snmp_mem_alianza!90,80!98,98!-I!
```

La función *check_snmp_mem.pl* es llamada al ejecutarse el comando *check_snmp_mem_alianza*, el cual entrega los parámetros recogidos por el comando de notificación, más un valor adicional, el nombre de la comunidad snmp con la cual se comunicará la función *check_snmp_mem.pl* directamente, a continuación se detalla el comando:

```
Define command {
      Command name    check_snmp_load_alianza
       Command line        $USER1$/check_snmp_mem.pl -H $HOSTADDRESS$ -C public1 -w $ARG1$ -
c $ARG2$ -T $ARG3$
      }
```

Las letras en negrilla nos indican los argumentos pasados a la función, todos los parámetros son entregados por el comando declarado en el servicio, mas el dato adicional de la comunidad, el índice alianza al final del comando, se debe a que se ha creado tres comandos específicos, para los tres ruteadores administrados por Alianzanet, como se muestra a continuación:

Tabla. 3.13 Comunidades SNMP Alianzanet

ROUTER	COMANDO	COMUNIDAD	IP BORDER
CISCO 2801	check_snmp_mem_alianza	pulic1	201.219.1.210

CISCO 1800	check_snmp_mem_fibertel	Fibertel	201.219.0.70
CISCO 800	check_snmp_mem_CCEE	CCEETELCO	186.3.3.130

- ***Check snmp load.*** Este comando, como su declaración lo indica, solicita el consumo en porcentaje del procesador del router, para cada 5 segundos, 1 minuto y 5 minutos, en la fase de notificación, entrega al comando principal, declarado en commands.cfg, 4 argumentos, a saber:
  - DIRECCION IP DEL HOST
  - Umbral de estado crítico (CRITICAL), el servicio pasará a estado crítico, cuando el consumo de procesador rebase, luego de las 5 comprobaciones de rigor, el 99% de su capacidad total, esto según estándares CISCO de desempeño.
  - Umbral de estado de peligro (*WARNING*), el servicio pasará al estado *warning*, cuando supere el umbral, es decir el 98 %.
  - Tipo de host, el script llamado a interactuar directamente con el ruteador, requiere este argumento para saber qué tipo de equipo esta monitoreando, con el fin de aplicar las normativas según el tipo de sistema, el argumento 'cisco ' le indica a la función que el equipo es un elemento de red activo CISCO.

  La sintaxis dentro de la declaración del servicio es como se vio en la líneas de código:

```
check_snmp_load_alianza! 90,80,60!99,99,99!cisco!
```

La función *check_snmp_load.pl* la función es llamada al ejecutarse el comando *check_snmp_load_alianza*, el cual entrega los parámetros recogidos por el comando de notificación, más un valor adicional, el nombre de la comunidad snmp con la cual se comunicará la función check_snmp_load.pl directamente, a continuación se detalla el comando:

```
define command{
  command_name    check_snmp_load_alianza
  command_line       $USER1$/check_snmp_load.pl –H $HOSTADDRESS$ -C public1 -w $ARG1$ -c
$ARG2$ -T $ARG3$       }
```

Las letras en negrilla nos indican los argumentos pasados a la función.

- ***Check snmp Sysuptime.*** Este comando, consulta cada 5 minutos al router el tiempo de vida del sistema, es decir, desde la última ves que sufrió un corte en sus actividades, sea por mantenimiento, reload, o fallas de energía en el nodo, en la fase de notificación, entrega al comando principal, declarado en commands.cfg, 4 argumentos, a saber:
  - DIRECCION IP DEL HOST
  - Comunidad SNMP
  - OID de CISCO *sysUpTime* especifica el tiempo de vida, de la tabla de registro SNMP del router.
- La sintaxis dentro de la declaración del servicio es como se vio en la líneas de código:

```
check_snmp!-C public1 –o sysUpTime.0
```

Estos servicios SNMP se hallan declarados para cada unos de los routers administrados por Alianzanet.

CAPITULO 4

RECOPILACION DE LOS RESULTADOS

4.1 INTRODUCCION

Luego de instalados y configurados los sistemas se procede a recabar la información generada por estos sobre la base de la función para la cual fueron configurados.

Es importante en este punto mencionar que, si bien es cierto Nagios será el sistema directamente involucrado en el monitoreo del los diferentes equipos parte de la red WAN de Alianzanet S.A., este sistema, como se vio en el capitulo anterior, es un sistema autónomo, que aprovecha la información que puedan brindarle el resto de herramientas para, con esta información, discriminar sobre el estado de determinado host o servicio relacionado a dicho host.

Nagios administra al grupo de subsistemas de los que se vale, mas en si no genera ningún tipo de información, en cuanto al consumo de ancho de banda de la red en general, ni al tráfico de protocolos que circulan sobre la misma.

Es en este punto donde entran en acción las otras dos herramientas implementadas en el proyecto, hablamos de MRTG y NTOP, para entregar un historial del consumo de cada una de las interfaces, en cada router, en cada nodo, y a la vez, colaborar en la caracterización del trafico que rueda sobre la red WAN del ISP.

4.2 Consumo de ancho de banda nodo Carolina

Los datos se tomaran de un mes de consumo ininterrumpido, 4 semanas completas de tráfico 24/7, se procederá a documentar la información de cada nodo de manera independiente, y dentro del nodo, cada interfaz, tanto en acceso como la interfaz de border.

A continuación se detalla los componentes a medir dentro del Nodo Carolina:

ROUTER CISCO 2801

- Troncal 1 (Interface serial 0/1/0)
- Troncal 2 (Interface serial 0/1/1)
- Troncal 3 (Interface serial 0/2/0)
- Troncal IP (Interfase FastEthernet 0/0)
- Border (Interfase FastEthernet 0/1)

4.2.1 Primera Troncal

Configurada sobre la interface 0/1/0 del router de acceso, alberga a 49 clientes procedentes de todos los puntos de la cuidad con velocidades desde 128/64 Kbps hasta 512/256 Kbps.

A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.1 Ficha Técnica enlace Primera Troncal

ENLACE	Serial 0/1/0 TR1-E1
CAPACIDAD	2 Mbps (1 E1)
SUB-INTERFACES HIBRIDAS	49
TIPO DE INTERFACE	Frame-Relay (32)
UBICACIÓN TEMPORAL	Graficos Diario – Semanal - Mensual

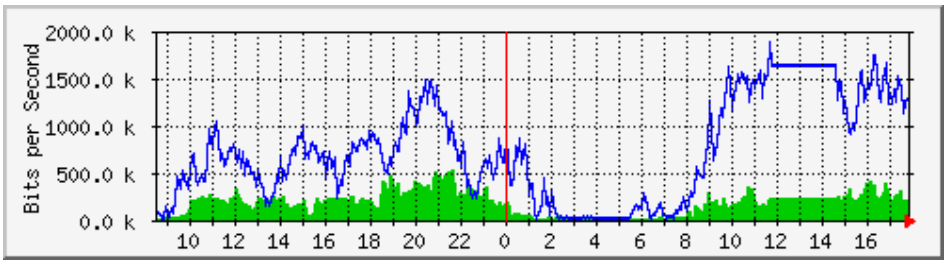


Figura. 4.1 TR-1 Carolina Grafico Diario

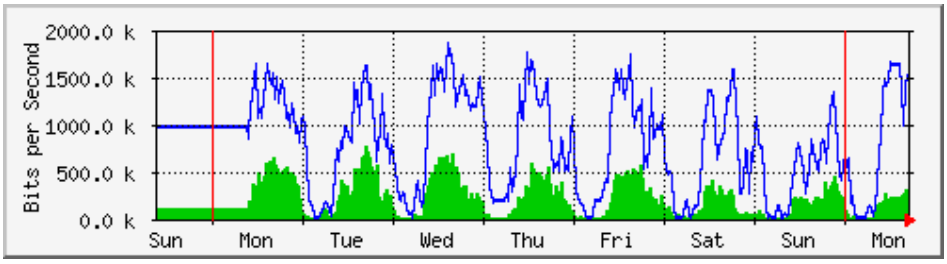


Figura. 4.2 TR-1 Carolina Grafico Semanal

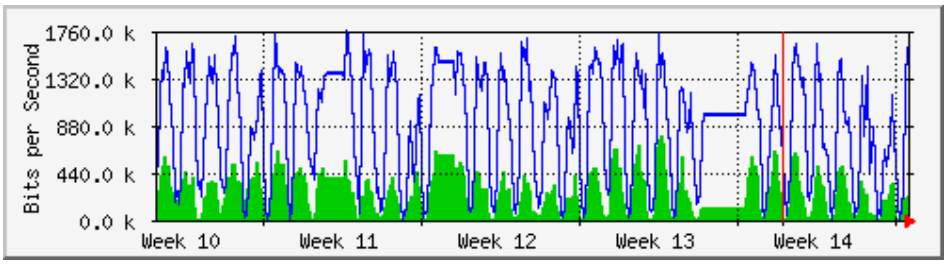


Figura. 4.3 TR-1 Carolina Grafico Mensual

A continuación en la Tabla 4.2 se muestra detalladamente el resumen de los resultados en forma numérica, tomando en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de este enlaces.

Tabla. 4.2 Consumo TR-1 Nodo Carolina

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	1760 Kbps	10:00 am. - 16:00 pm.	6 horas	85.90%
24 horas	2048 Kbps	MINIMO	256 Kbps	22pm, 2am – 6,8 am.	4 horas	13%
		PROMEDIO	1003 Kbps			
				DIA DE LA SEMANA		% CONSUMO SEMANAL
		MAX	1760 Kbps	Miercoles, Jueves, Viernes	3 dias	85.90%
7 dias	2048 Kbps		1650 Kbps	Lunes, Martes,Sabado	3 días	80.00%
			1400 Kbps	Domingo	1 días	68.35%
		PROMEDIO:	1661.42 Kbps			
				SEMANA		%CONSUMO MENSUAL
		MAX	1760 Kbps			
4 semanas (1 MES)	2048 Kbps	MINIMO	1100 Kbps	Todas		70.00%
		PROMEDIO	1430 Kbps			

En este caso la capacidad del canal E1 es de 2048 Kbps, la gráfica azul representa el consumo de bajada, mientras que la gráfica verde el consumo de subida.

El consumo máximo diario de esta interfaz es de 1760 Kbps, desde las 10:00 am hasta las 16:00 pm., con un ancho de banda libre de 288 Kbps, lo cual nos muestra que el enlace aún no alcanza su capacidad total, sin embargo, solo le queda un 14% libre antes de llegar al límite.

El consumo mínimo diario de este enlace de acceso se encuentra por horas, desde las 22:00 pm hasta las 2:00 am, y luego desde las 6:00 am a las 8:00 am, horas en las que se registran valles de 256 Kbps, el 12.5 % de su capacidad total. El resto del día se mantiene un consumo aleatorio y la escasez completa de consumo.

En cuanto al consumo semanal y mensual, se puede apreciar que los días de mayor consumo son los días de mitad de semana de miércoles a viernes con un consumo máximo promedio de 1661.4 Kbps, mientras que el resto de la semana se mantiene un consumo que oscila sobre y bajo los de 959.8 Kbps, excepto el día domingo, día en el que disminuye considerablemente, hasta llegar a los 258.3 Kbps como consumo mínimo.

Para el consumo mensual, este alcanza los 1760 Kbps como máximo, todas las semanas, 1100 Kbps como consumo mínimo, y un promedio de 1430 Kbps, desde que se encuentra funcionando el sistema de monitoreo.

4.2.2 Segunda Troncal

Configurada sobre la interface 0/1/1 del router de acceso, alberga a 51 clientes procedentes de todos los puntos de la cuidad con velocidades desde 128/64 Kbps hasta 1024/512 Kbps.

A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.3 Ficha Técnica enlace Segunda Troncal

ENLACE	Serial 0/1/1 TR2-E1
CAPACIDAD	2 Mbps (1 E1)
SUB-INTERFACES HIBRIDAS	51
TIPO DE INTERFACE	Frame Relay (32)
UBICACIÓN TEMPORAL	Graficos Diario – Semanal - Mensual

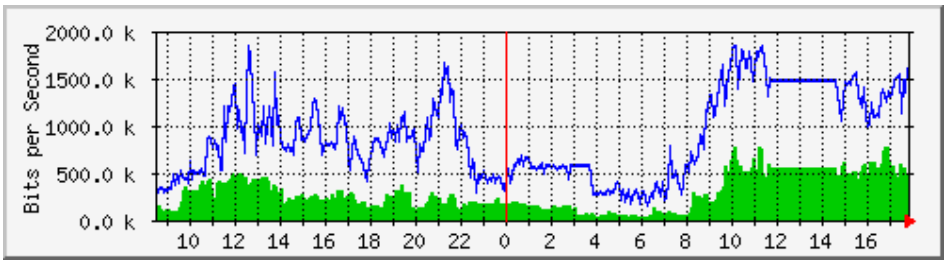


Figura. 4.4 TR-2 Carolina Grafico Diario

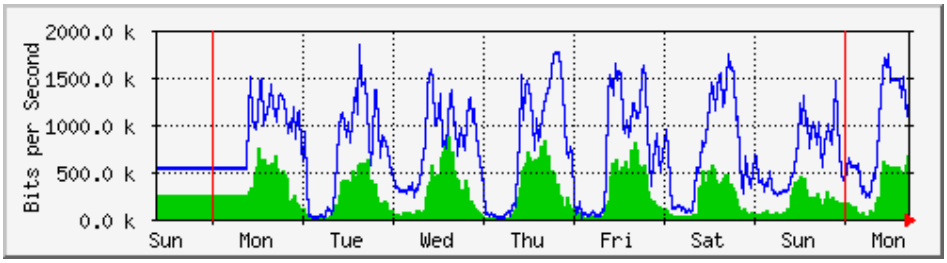


Figura. 4.5 TR-2 Carolina Grafico Semanal

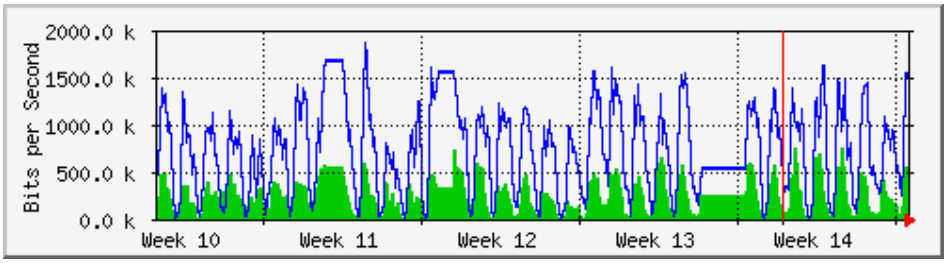


Figura. 4.6 TR-2 Carolina Grafico Mensual

La Tabla 4.4 resume los datos recabados del monitoreo de la segunda troncal de acceso, del nodo Carolina, se muestran detalladamente los resultados, tomado en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de este enlaces.

Tabla. 4.4 Consumo TR-2 Nodo Carolina

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	1816,6 Kbps	10:00 am. - 17:30 pm.	6 horas	85.90%
DIARIO	2048 Kbps	MINIMO	500 Kbps	22:30 pm. - 8:00 am.	6 horas	13%
		PROMEDIO	1158 Kbps			
				DIA DE LA SEMANA		% CONSUMO SEMANAL
		MAX	1900 Kbps	Mar,Jue,Sab	3 dias	92,77%
			1500 Kbps	Lun,Mie,Dom	3 dias	73,24%
			1650 Kbps	Vie	1 dia	80,56%
		TOTAL :	1692 Kbps			
SEMANAL	2048 Kbps					
		MINIMO	600 Kbps	Vie-Sab		30.00%
			250 Kbps	Lun-Mar		12.00%
			0 Kbps			0.00%
		TOTAL :	141.6 Kbps			
				SEMANA		%CONSUMO MENSUAL

En este caso la capacidad del canal E1 es de 2048 Kbps, la gráfica azul representa el consumo de bajada, mientras que la gráfica verde el consumo de subida.

El consumo máximo diario de esta interface es de 1816 Kbps, superior a la anterior TR-1, desde las 10:00 am hasta las 16:00 pm., lo cual nos muestra que el enlace aún no alcanza su capacidad total, sin embargo, solo le queda un 11,3% libre antes de llegar al límite, es decir 231 Kbps.

El consumo mínimo diario de este enlace de acceso se encuentra desde las 22:30 pm hasta las 8:00 am horas en las que se registran 500 Kbps, el 24,4 % de su capacidad total, el doble del enlace anterior con 12,4%.

En cuanto al consumo semanal y mensual, se puede apreciar que los días de mayor consumo son los días martes, jueves y viernes, con un consumo de 1900 Kbps, mientras que el resto de la semana se mantiene un consumo de 1500 Kbps, excepto el día viernes, día en el que se estabiliza considerablemente en 1650 Kbps, hasta llegar al mínimo en 141,6 Kbps.

En cuanto al consumo mensual, este alcanza los 1900 Kbps como máximo, todas las semanas, 1024 Kbps como consumo mínimo, y un promedio de 1462 Kbps, desde que se encuentra funcionando el sistema de monitoreo.

4.2.3 Tercera Troncal

Configurada sobre la interface 0/2/0 del router de acceso, alberga a 35 clientes procedentes de todos los puntos de la cuidad con velocidades desde 128/64 Kbps hasta 512/128 Kbps.

A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.5 Ficha Técnica enlace Tercera Troncal

ENLACE	Serial 0/2/0 TR3-T1
CAPACIDAD	1544.0 Kbps (1 T1)
SUB-INTERFACES HIBRIDAS	35
TIPO DE INTERFACE	Frame Relay (32)
UBICACIÓN TEMPORAL	Graficos Diario – Semanal - Mensual

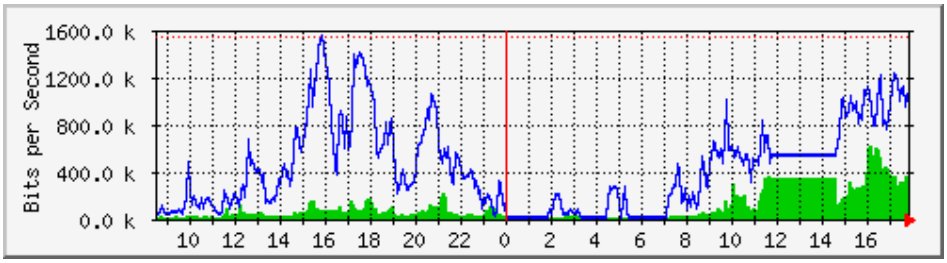


Figura. 4.7 TR-3 Carolina Grafico Diario

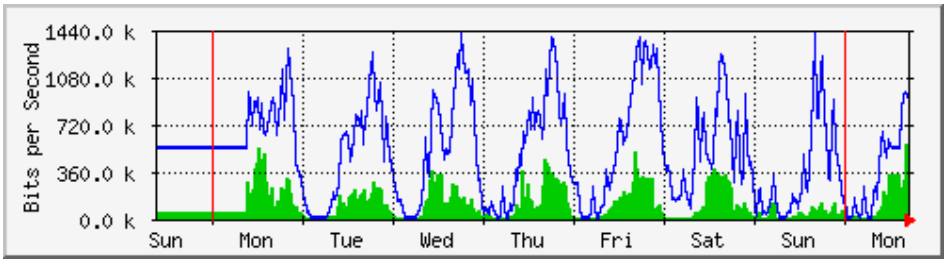


Figura. 4.8 TR-3 Carolina Grafico Semanal

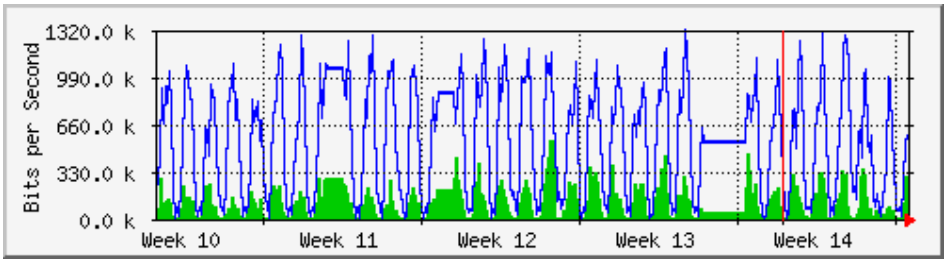


Figura. 4.9 TR-3 Carolina Grafico Mensual

A continuación en la Tabla 4.6 se muestran detalladamente los resultados para nodo Carolina en su *tercera troncal*, tomando en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de este enlace.

Tabla. 4.6 Consumo TR-3 nodo Carolina

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	1544 Kbps	15:30 - 16:30	1 hora	100.00%
DIARIO	1544 Kbps		1400 Kbps	16:30 – 17:30	1 hora	90.60%
		PROMEDIO	1472 Kbps			95.00%
		MINIMO	200 Kbps	23:00 pm. - 8:00 am.	9 horas	13%
				DIA DE LA SEMANA		% CONSUMO SEMANAL
		MAX	1440 Kbps	Mie-Vie, Dom	4 dias	28.50%
SEMANAL	1544 Kbps		1200 Kbps	Lun, Mar, Sab	3 días	77.72%
		PROMEDIO	1337 Kbps			86.60%
		MINIMO	360 Kbps	Entre días		23.31%
				SEMANA		%CONSUMO MENSUAL
		MAX	1320 Kbps			74.80%
MENSUAL	1544 Kbps	MINIMO	990 Kbps	Todas		
		PROMEDIO	1155 Kbps			

En este caso la capacidad del canal T1 es de 1544 Kbps, la gráfica azul representa el consumo de bajada, mientras que la gráfica verde el consumo de subida.

El consumo máximo diario de esta interface serial FR es de 1544 Kbps, con un ancho de banda libre de 0 Kbps, este consumo se hace presente solo durante las 16:00, disminuyendo al cambio de hora, y teniendo un repunte a 1400 Kbps, para las 17:00, esto es alarmante, en tanto en cuanto se alcanza el máximo del ancho de banda de la interfaz, sin embargo, se aprecia claramente que este tope máximo varía por el lapso de 1 hora desde las 15:30 hasta las 16:30, teniendo este pico esporádico a las 16:00.

Por el lado del consumo mínimo se observa un ancho de banda de 200Kbps, esto debido a que el resto del día el consumo de esta interfaz es casi nulo, debido al tipo de clientes que aloja.

En cuanto al consumo semanal y mensual, no existe ningún patrón definido de uso del enlace. Se puede hablar de un valor promedio de 880.5 Kbps.

Para el consumo mensual, este alcanza los 1320 Kbps como máximo, todas las semanas, 990 Kbps como consumo mínimo, y un promedio de 1155 Kbps, desde que se encuentra funcionando el sistema de monitoreo.

4.2.4 Troncal MPLS

Configurada sobre la interface FastEthernet 0/0 del router de acceso, alberga a 28 clientes procedentes de todos los puntos de la cuidad y del país, con velocidades desde 128/64 Kbps hasta 2 Mbps.

Este enlace constituye la única troncal IP de acceso para Alianzanet, se encuentra anclada a la red MPLS del backbone IP de Andinadatos, estos enlace se caracterizan por estar conectados a DSLAM IP propios de la red MPLS, siendo enlaces de tipo IP puros, y no híbridos como el resto de enlaces que albergan las otras tres troncales de Alianzanet, enlaces que aún ven su acceso sobre redes ATM-Frame Relay, sobra decir que MPLS es compatible, no solo con este tipo de tráfico, como se vió en capítulos anteriores, sino con todo tipo de trafico que se pueda etiquetar y transportar sobre IP.

A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.7 Ficha Técnica enlace Troncal IP

ENLACE	Troncal IP
CAPACIDAD	100 Mbps (802.3 Fast Ethernet)
SUB-INTERFACES IP	28
TIPO DE INTERFACE	EthernetCsmacd
UBICACIÓN TEMPORAL	Graficos Diario – Semanal – Mensual

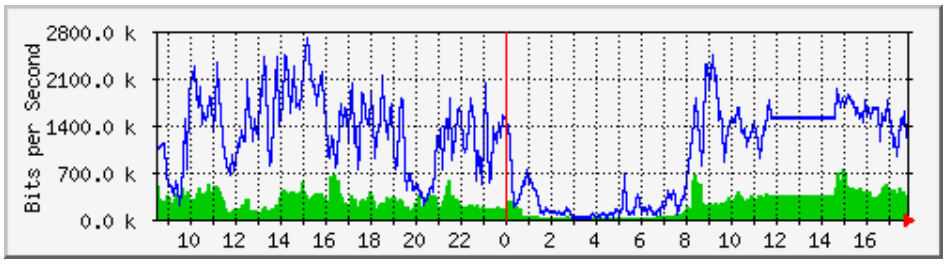


Figura. 4.10 TR-IP Carolina Grafico Diario

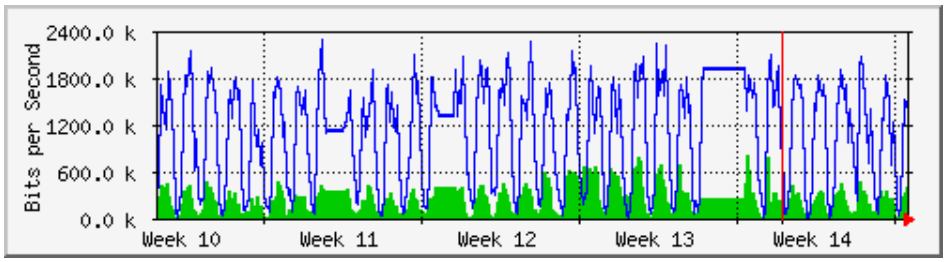


Figura. 4.11 TR-IP Carolina Grafico Semanal

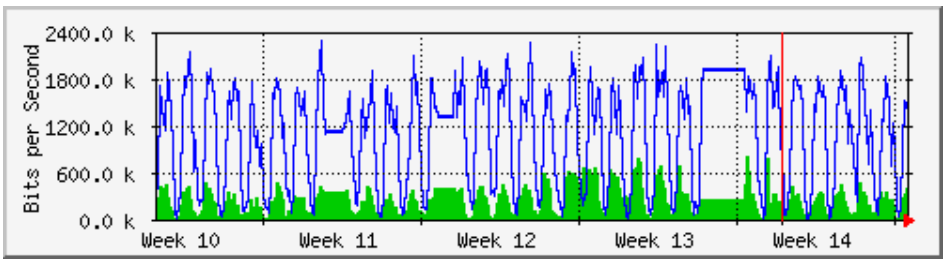


Figura. 4.12 TR-IP Carolina Grafico Mensual

A continuación en la Tabla 4.8 se muestran detalladamente los resultados para nodo Carolina en su *troncal MPLS*, tomando en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de este enlace.

Tabla. 4.8 Consumo TR-MPLS Nodo Carolina

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	2.3 Mbps	9:00 – 16:30	7 hora	2.30%
DIARIO	100 Mbps		2.1 Mbps	16:30 – 23:00	1 hora	2.10%
		TOTAL :	2.2 Mbps			2.20%
		MINIMO	700-0 Kbps	24:00 pm. - 7:00 am.	7 horas	1%
				DIA DE LA SEMANA		% CONSUMO SEMANAL
		MAX	2.3 Mbps	Lun, Mie – Vie	4 dias	2.30%
SEMANAL	100 Mbps		2.4 Mbps	Mar, Sab,Dom	3 días	2.40%
		TOTAL :	2.35 Mbps			2.35%
				SEMANA		%CONSUMO MENSUAL
		MAX	2350 Kbps			1.16%
MENSUAL	100 Mbps	MINIMO	1200 Kbps	Todas		
		PROMEDIO	1775 Kbps			

Esta troncal al igual que las anteriores alberga clientes para el acceso a la red de CORE de Alianzanet, sin embargo el sistema a través del cual, esta troncal se enlaza al backbone IP de Andinadatos es diferente, ya que es 100% IP.

En Capítulos anteriores se abordó el tema de la red MPLS, no solo teóricamente, sino la forma en que Alianzanet se conecta con esta, en este caso el enlace es un enlace 802.3 FastEthernet, con una capacidad de 100 Mbps, muy superior a los enlaces de acceso anteriormente mencionados. La presentación de la gráfica es la misma, el color azul representa el consumo de bajada, mientras que el verde el consumo de subida.

El consumo máximo diario de esta interface es de 2.3 Mbps, con un ancho de banda libre del 97.7%, desde las 9:00 hasta las 23:00, esto nos da la medida de que el canal se encuentra prácticamente libre.

El consumo de cierta manera se mantiene estable durante la mayoría del día, con un mínimo de 700 Kbps fuera de este rango, desde las 00:00 hasta las 7:00 am donde se replica el valor mencionado anteriormente.

En cuanto al consumo semanal y mensual, se puede apreciar que todos los días de la semana existe un consumo moderado de 2.35 Mbps en promedio, su consumo mínimo semanal es de 1.2 Mbps en promedio, existiendo una diferencia de casi el 50 % entre el valor máximo y el mínimo de consumo semanal y mensual, lo cual no sucede con el resto de interfaces.

4.2.5 Enlace Border

Configurado en la interface Fast Ethernet del router de Border, este enlace da el acceso internacional, a través de Andinadatos, a los clientes anclados al nodo Carolina en un numero de 136, con enlaces que van desde 128/64 Kbps a 1024/256 Kbps.

A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.9 Ficha Técnica enlace BORDER-CAROLINA

ENLACE	Border Carolina
CAPACIDAD	5.1 Mbps (2 E1 + 1 Mbps)
DIRECCION IP	201.219.1.210
TIPO DE I NTERFACE	EthernetCsmacd
UBICACIÓN TEMPORAL	Graficos Diario – Semanal – Mensual

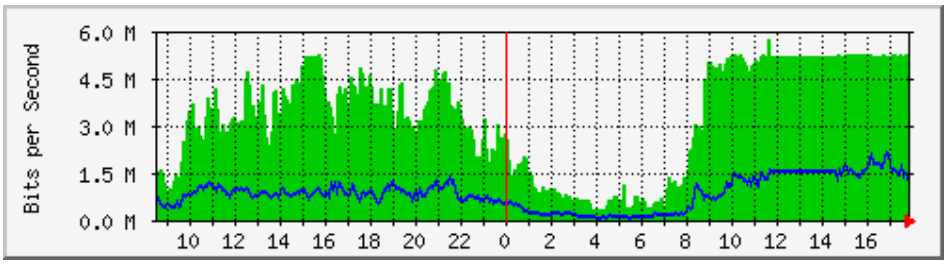


Figura. 4.13 Border Carolina Grafico Diario

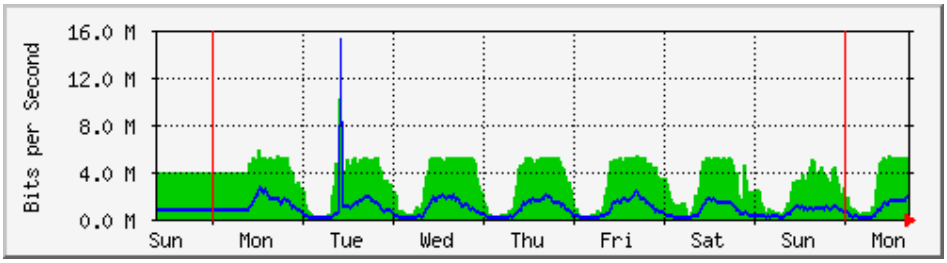


Figura. 4.14 Border Carolina Grafico Semanal

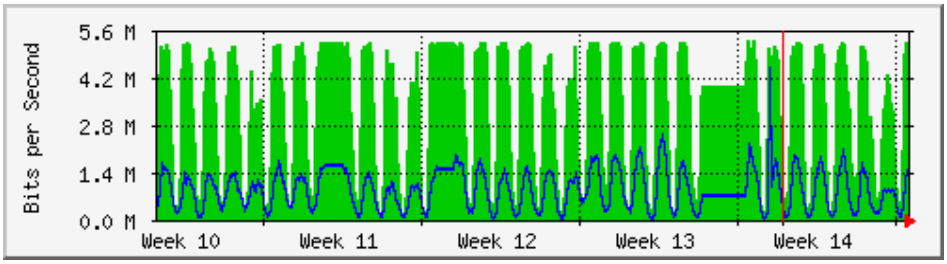


Figura. 4.15 Border Carolina Grafico Mensual

A continuación en la Tabla 4.10 se muestran detalladamente los resultados para el nodo Carolina en su interfaz de salida, tomado en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de estos enlaces.

Tabla. 4.10 Consumo Border Nodo Carolina

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	5120 Kbps	9:00 am. - 17:30 pm.	8 h. 30 m	100.00%
DIARIO	5.1 Mbps	MINIMO	1000 Kbps	3:00 am. - 7:00 am.	4 h.	19,53%
		PROMEDIO	3060 Kbps			
				DIA DE LA SEMANA		% CONSUMO SEMANAL
		MAX	5120 Kbps	Lunes – Sabado	6 dias	90.00%
SEMANAL	5.1 Mbps	MINIMO	4500 Kbps	domingo	1 dias	10.00%
		PROMEDIO	4810 Kbps			
				SEMANA		%CONSUMO MENSUAL
		MAX	5120 Kbps			
MENSUAL	**5.1 Mbps**	MINIMO	4500 Kbps	Todas		100.00%
		PROMEDIO	4810 Kbps			

En la Tabla 4.10 los resultados son claros, la capacidad del canal de salida es de 5120 Kbps, sin embargo este se halla saturado en horas laborables de 9:00 am a 17:30 pm, más adelante se analizará las inminentes repercusiones de esta saturación, sus causas, y sus posibles soluciones, previo a esto también se analizará que tipo de tráfico es el generado por los clientes de manera global, este es un paso indispensable para poder plantear una correcta planificación de la red WAN de Alianzanet.

En la Tabla 4.11 se observa un resumen del consumo de los circuitos anclados al nodo Carolina.

Tabla. 4.11 Resumen de Consumo Nodo Carolina

		CONSUMO			
ENLACE	CAPACIDAD	CONSUMO MAX	MINIMO	PROMEDIO	% CANAL LIBRE
TR-1	2048 Kbps	1760 Kbps	1100 Kbps	1430 Kbps	14.30%
TR-2	2048 Kbps	1900 Kbps	1024 Kbps	1462 Kbps	11.00%
TR-3	1544 Kbps	1320 Kbps	990 Kbps	1155 Kbps	25.00%
TR-MPLS	100 Mbps	2350 Kbps	1200 Kbps	1775 Kbps	97.70%
CONSUMO PROMEDIO TOTAL:				**5822 Kbps**	
BORDER	**5120 Kbps**	5120 Kbps	4500 Kbps	4810 Kbps	

Por el lado del consumo semanal y mensual, se puede apreciar que 6 días a la semana de Lunes a Sábado, el enlace de borde replica lo mencionado anteriormente, permaneciendo saturado en 5120 Kbps, con una disminución del consumo el día domingo máximo de 4500 Kbps.

Este comportamiento se hace más evidente en el gráfico mensual, las cuatro semanas que componen el mes presentan una meseta de consumo de 5.1 Mbps.

4.3 Consumo de ancho de banda Nodo Iñaquito

Los datos se tomaran de un mes de consumo ininterrumpido, 4 semanas completas de tráfico 24/7, se procederá a documentar la información de cada nodo de manera independiente, y dentro del nodo, cada interfaz, tanto en acceso como la interfaz de border.
A continuación se detalla los componentes a medir dentro del Nodo Iñaquito:

ROUTER CISCO 1800

- Border (Interfase FastEthernet 0/0)
- Troncal 1 (Interface serial 0/1/0)
- Troncal 2 (Interface serial 0/1/1)

4.3.1 Primera Troncal

Configurada sobre la interface 0/1/0 del router de acceso, alberga a 33 clientes procedentes de todos los puntos de la cuidad con velocidades desde 128/64 Kbps hasta 512/256 Kbps.
A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.12 Ficha Técnica enlace Primera Troncal

ENLACE	Serial 0/1/0 TR1
CAPACIDAD	1544 kbps (1 T1)
SUB-INTERFACES HIBRIDAS	33
TIPO DE INTERFACE	Frame-Relay (32)
UBICACIÓN TEMPORAL	Gráficos Diario – Semanal - Mensual

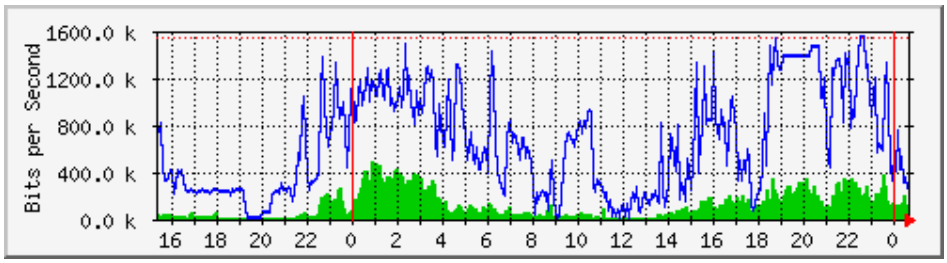


Figura. 4.16 TR-1 Nodo Iñaquito Grafico Diario

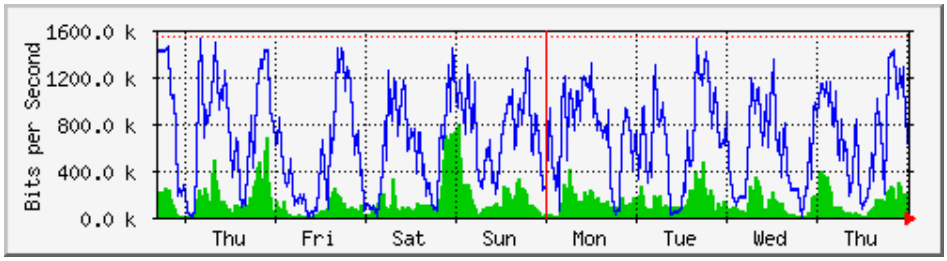


Figura. 4.17 TR-1 Nodo Iñaquito Grafico Semanal

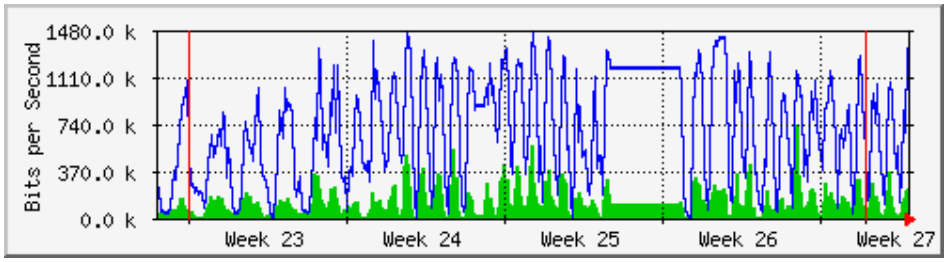


Figura. 4.18 TR-1 Nodo Iñaquito Grafico Mensual

A continuación en la Tabla 4.13 se muestran detalladamente los resultados para el nodo Iñaquito en su primera troncal, tomando en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de estos enlaces.

Tabla. 4.13 Consumo Primera Troncal Iñaquito

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	1544 Kbps	18:00 – 22:00	4 horas	100.00%
DIARIO	1544 Kbps	MINIMO	300 Kbps	16:00 - 18:00	9 horas	19%
		PROMEDIO	922 Kbps			59.71%
				DIAS	TOTAL	% semanal
		MAX	1472 Kbps	Mie, Jue, vie	3 dias	42.80%
SEMANAL	1544 Kbps	MINIMO	300 Kbps	Lun, Mar, Sab,Dom	4 días	47.20%
		PROMEDIO	886 Kbps			57.38%
				SEMANA		%CONSUMO MENSUAL
		MAX	1480 Kbps	Todas		66.32%
MENSUAL	1544 Kbps	MINIMO	570 Kbps			
		PROMEDIO	1024 Kbps			

Esta es la primera interfaz en la red de acceso del nodo Iñaquito, la capacidad del canal T1 es de 1544 Kbps, la gráfica azul representa el consumo de bajada, mientras que la gráfica verde el consumo de subida.

El consumo máximo diario de esta interface serial FR es de 1544 Kbps, sin embargo, este valor se registra por alrededor de 4 horas en la noche, lo cual difiere bastante con respecto a lo visto en circuitos anteriores como es el caso de la primera troncal en el nodo Carolina.

El consumo mínimo registrado para esta interfaz es de 300 Kbps, en este caso cabe el tomar en cuenta el consumo promedio diario del canal, en 922 Kbps que representa el 59 % de la capacidad total, con un holgado 41 % libre, a diferencia del antes mencionado enlace TR-1 del nodo Carolina con un escaso 14% libre.

Con respecto al tráfico semanal, este registra picos esporádicos de 1544 Kbps con un mínimo de 300 Kbps, dando un promedio de 886 Kbps, el consumo máximo se registra de miércoles a viernes, mientras que se mantiene un perfil bajo durante el resto de días de la semana.

Para el consumo mensual, este alcanza los 1480 Kbps como máximo, todas las semanas, 570 Kbps como consumo mínimo, y un promedio de 1024 Kbps, desde que se encuentra funcionando el sistema de monitoreo.

4.3.2 Segunda Troncal

Configurada sobre la interface 0/1/1 del router de acceso, alberga a 39 clientes procedentes de todos los puntos de la cuidad con velocidades desde 128/64 Kbps hasta 1024/512 Kbps.

A continuación se detalla la información técnica del enlace así como las gráficas de consumo del mismo.

Tabla. 4.14 Ficha Técnica enlace Segunda Troncal

ENLACE	Serial 0/1/1 TR2
CAPACIDAD	1541 Kbps (1 T1)
SUB-INTERFACES HIBRIDAS	39
TIPO DE INTERFACE	Frame Relay (32)
UBICACIÓN TEMPORAL	Graficos Diario – Semanal - Mensual

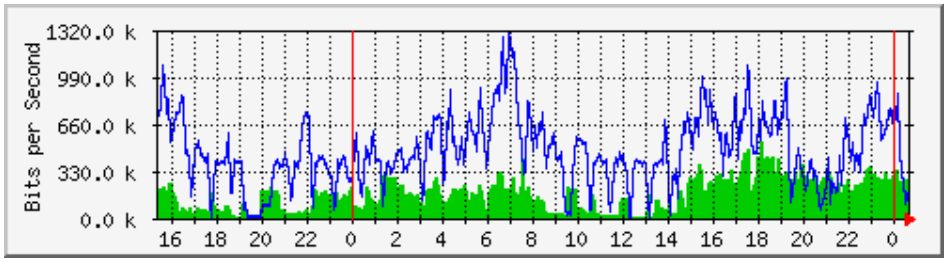


Figura. 4.19 TR-2 Nodo Iñaquito Grafico Diario

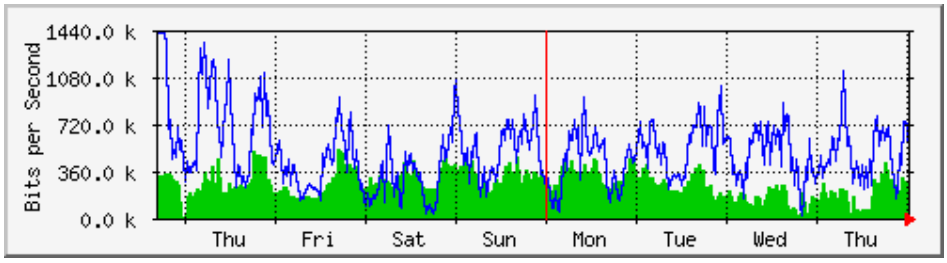


Figura. 4.20 TR-2 Nodo Iñaquito Grafico Semanal

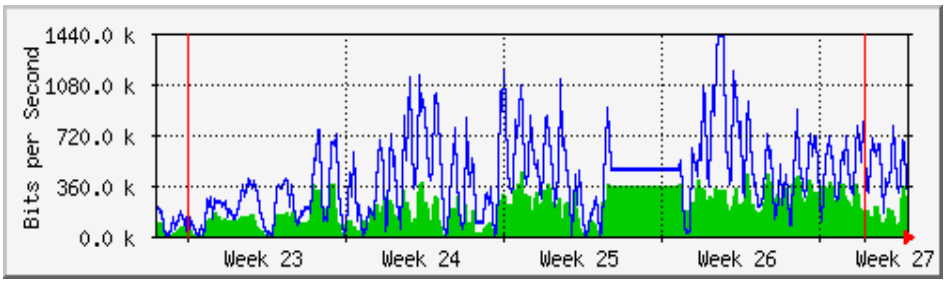


Figura. 4.21 TR-2 Nodo Iñaquito Grafico Mensual

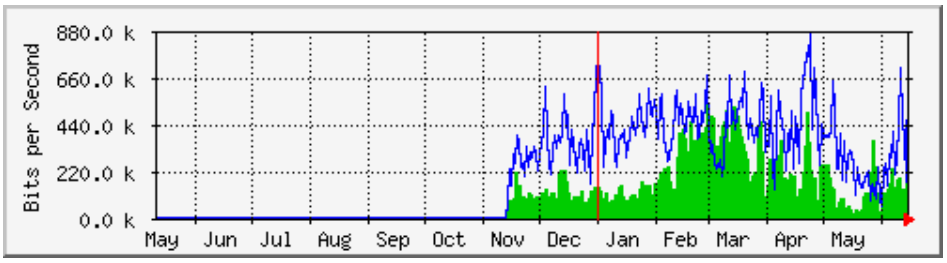


Figura. 4.22 TR-2 Nodo Iñaquito Grafico Anual

A continuación en la Tabla 4.15 se muestran detalladamente los resultados para el nodo Iñaquito en su segunda troncal, tomando en cuenta los datos entregados por la herramienta para el consumo diario, semanal, mensual y anual de estos enlaces.

Tabla. 4.15 Consumo Segunda Troncal Iñaquito

ENLACE	UBICACION TEMPORA	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL
TR-2	24 horas	1544 Kbps	MAX	1320 Kbps	7:00 – 8:00	1 hora
				1024 Kbps	15:30 – 16:30	1 hora
				900 Kbps	15:00 – 17:00	2horas
			PROMEDIO	1080 Kbps		
			MINIMO	400 Kbps	resto del día	
			PROMEDIO	886 Kbps		
					DIAS	TOTAL
			MAX	1080 Kbps	Mie, Jue, vie	3 dias
	7 dias	1544 Kbps	MINIMO	720 Kbps	Lun, Mar, Sab,Dom	4 días
			PROMEDIO	900 Kbps		
					SEMANA	
	4 semanas (1 MES)	1544 Kbps	PROMEDIO	1080 Kbps	mediados de Junio	
	Ultimos 6 meses	1544 Kbps	PROMEDIO	770 Kbps	Nov 2008 – Mayo 2009	

Esta es la segunda interfaz en la red de acceso del nodo Iñaquito, la capacidad del canal T1 es de 1544 Kbps, la gráfica azul representa el consumo de bajada, mientras que la gráfica verde el consumo de subida.

El consumo máximo diario de esta interface serial FR es de 1081 Kbps promedio, este valor es el resultado de picos de consumo de entre 1 y 3 horas, tanto en la mañana (7 - 8am) como en la tarde (15:00 – 19:00), representando un consumo del 70% del enlace, a estas horas específicas, con un consumo mínimo de 400 Kbps (25.9% de la capacidad

total), dando como resultado un promedio general de 740 Kbps, el 47.9% del total lo cual deja más del 50% del enlace libre durante el resto del día.

Con respecto al tráfico semanal, este registra picos esporádicos de 1080 Kbps con un mínimo de 400 Kbps, dando un promedio de 886 Kbps, el consumo máximo se registra de miércoles a viernes, mientras que se mantiene un perfil bajo durante el resto de días de la semana.

Para el consumo mensual, este alcanza los 1440 Kbps como máximo.

A partir del mes de mayo, se ha incluido el consumo de los 6 últimos meses (Tabla 4.16), por una razón importante, y es que, a diferencia de los enlaces de acceso anteriormente mencionados, este enlace muestra un consumo ascendente, como lo muestra la grafica a continuación:

Tabla. 4.16 Consumo Semestral TR-2 Nodo Iñaquito

CONSUMO Kbps	MES
330	1
550	2
660	3
880	4
1080	5

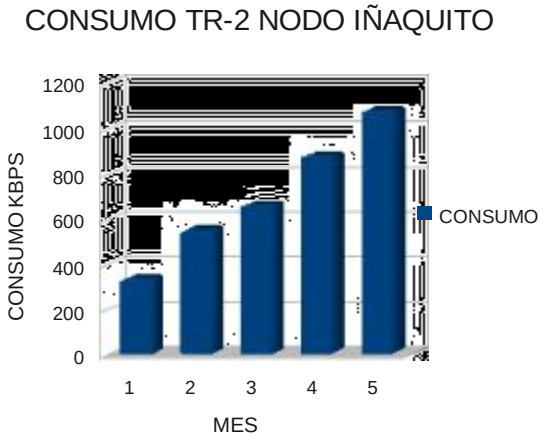


Figura. 4.23 TR-2 Nodo Iñaquito Consumo Ascendente

4.3.3 Enlace Border

Configurado en la interface Fast Ethernet 0/0 del router de Border, este enlace da el acceso internacional, a través de Andinadatos, a los clientes anclados al nodo Iñaquito en un numero de 87, con enlaces que van desde 128/64 Kbps a 1024/256 Kbps.

Tabla. 4.17 Ficha Técnica enlace BORDER-IÑAQUITO

ENLACE	Border Iñaquito
CAPACIDAD	4096 Kbps (2 E1 4096 Kbps)
DIRECCION IP	201.219.0.70
TIPO DE I NTERFACE	Ethernet Csmacd
UBICACIÓN TEMPORAL	Gráficos Diario – Semanal – Mensual

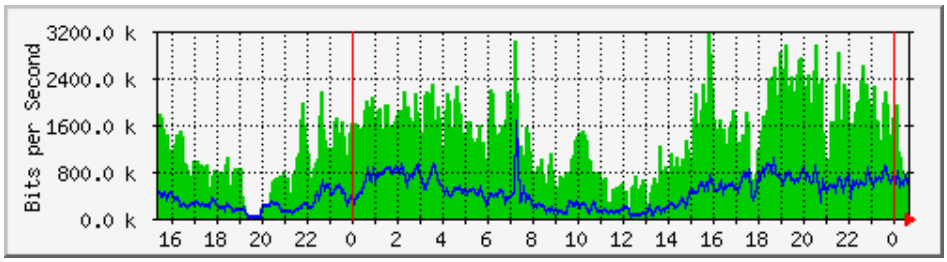


Figura. 4.24 Border Nodo Iñaquito Consumo Diario

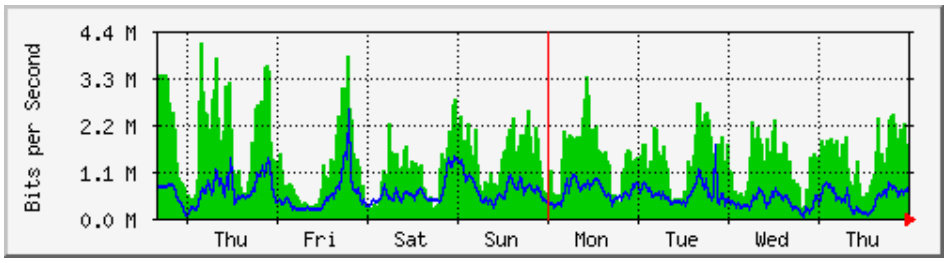


Figura. 4.25 Border Nodo Iñaquito Consumo Semanal

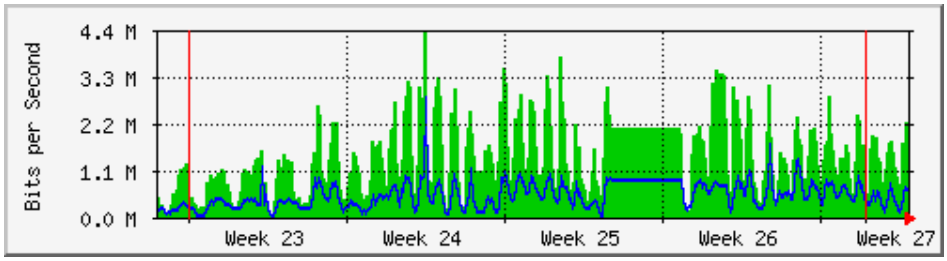


Figura. 4.26 Border Nodo Iñaquito Consumo Mensual

A continuación en la Tabla 4.18 se muestran detalladamente los resultados para el nodo Iñaquito en su interfaz de salida, tomado en cuenta los datos entregados por la herramienta para el consumo diario, semanal y mensual de estos enlaces.

Tabla. 4.18 Consumo Border Nodo Iñaquito

GRAFICO	CAPACIDAD	CONSUMO		HORA DEL DIA	TOTAL	% de consumo
		MAX	2650 Kbps	16:00 pm – 22:00 pm.	6 horas	64.70%
DIARIO	4096 Kbps	MINIMO	800 Kbps	8:00 am. - 14:00 pm.	6 horas	19,53%
		PROMEDIO	1725 Kbps			42.11%
				DIA DE LA SEMANA		% CONSUMO SEMANAL
SEMANAL	4096 Kbps	MAX	3500 Kbps	Lun,Mie,Jue,Vie,	4 dias	85.44%
		MINIMO	2300 Kbps	Mar, Sab, Dom	3 dias	56.15%
		PROMEDIO	2900 Kbps			70.80%
				SEMANA		%CONSUMO MENSUAL
		MAX	3300 Kbps	4		
MENSUAL	4096 Kbps	MINIMO	1300 Kbps	1 A 3		
		PROMEDIO	2300 Kbps			56.00%

La capacidad del canal de salida es de 4096 Kbps, el canal presenta un consumo del 64% como máximo en horas de la tarde, lo que deja un 36% de holgura con respecto a la capacidad total. Presenta un consumo mínimo del 19% en la mañana, esto corrobora lo documentado en las tablas 4.15 y 4.16, sobre el consumo de las interfaces de acceso del nodo Iñaquito, las cuales ven un mayor consumo en la tarde.

Tabla. 4.19 Resumen de Consumo Nodo Iñaquito

		CONSUMO			
ENLACE	CAPACIDAD	CONSUMO MAX	MINIMO	PROMEDIO	% CANAL LIBRE
TR-1	1544 Kbps	1480 Kbps	570 Kbps	1024 Kbps	33,77%
TR-2	1544 Kbps	1320 Kbps	900 Kbps	1110 Kbps	28,10%
CONSUMO PROMEDIO TOTAL:				2134 Kbps	
BORDER	4096 Kbps	3300 Kbps	1300 Kbps	2300 Kbps	44%

La tabla 4.19 recopila la información de las dos troncales de acceso conjuntamente con el enlace de border del nodo Iñaquito, se puede ver que no se ha alcanzado aún la saturación del canal registrando un 53 % del canal aún libre.

4.4 Caracterización de Trafico

NTOP se constituye como un sniffer de red, capaz de “escuchar” en la interfaz de red donde se le configure, todo el tráfico que circule a través de esta, el alcance de NTOP, no solo abarca la red a la que pertenece el dispositivo, sino que va mas allá, escuchando incluso el trafico de hosts remotos, que se encuentren relacionados a la red en cuestión, documentado su relación con la interfaz inmediata, del servidor que lo aloja.

A continuación se detalla los resultados obtenidos del segmento de red ubicado, en el canal de salida.

Tabla. 4.20 Trafico de Paquetes Border Carolina

Paquetes	**Dropped (libpcap)**	36.3%	27,503,398
	Dropped (ntop)	0.0%	0
	Total Recibidos (ntop)		75,757,051
	Total Paquetes Procesados		75,757,051
	Unicast	98.9%	74,925,250
	Broadcast	1.1%	817,847
	Multicast	0.0%	13,954
	Tamaño Min		35 bytes
	Tamaño Promedio		377 bytes
	Tamaño Maximo		1,514 bytes
	Paquetes <= 64 bytes	32.0%	24,271,944
	64 < Size <= 128 bytes	29.6%	22,401,606
	128 < Size <= 256 bytes	8.2%	6,177,089
	256 < Size <= 512 bytes	3.6%	2,694,086
	512 < Size <= 1024 bytes	3.9%	2,978,519
	1024 < Size <= 1518 bytes	22.7%	17,233,807
	Paquetes > 1518 bytes	0.0%	0
	Paquetes mayores [> 1514]	0.0%	0
	Bad Packets (Checksum)	0.0%	216
Trafico	**Total**	30.8 GBytes [75,757,065 Pkts]	
	Trafico IP	30.7 GBytes [74,744,339 Pkts]	
	Trafico Fragmentado	2.2 GBytes [7.3%]	
	Trafico No IP	64.9 MBytes	

	TTL Promedio		80
	TTL <= 32	0.1%	39,964
	32 < TTL <= 64	26.7%	20,222,612
	64 < TTL <= 96	0.7%	507,657
	96 < TTL <= 128	45.0%	34,105,226
	128 < TTL <= 160	0.0%	393
	160 < TTL <= 192	0.0%	4,198
	192 < TTL <= 224	0.0%	301
	224 < TTL <= 256	6.6%	5,002,008

Figura. 4.27 Flujo de Tráfico Nodo Carolina

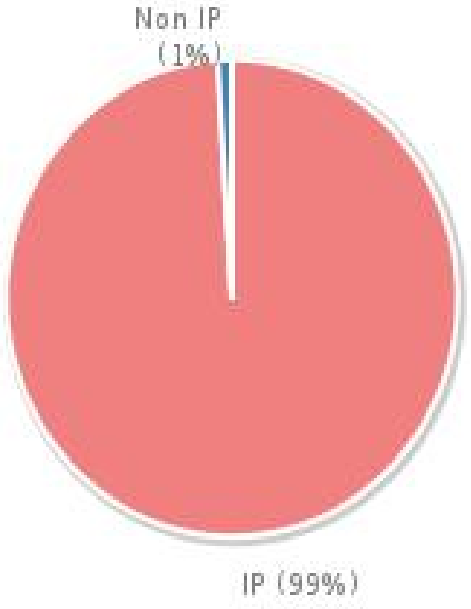


Figura. 4.28 Tráfico Global

El tráfico recogido por NTOP en la Tabla 4.20 corresponde al tráfico presente entre las 9:00 am y las 19:00 pm., de acuerdo a los resultados recogidos para el consumo de ancho de banda, es entre estas horas donde se registra los mayores volúmenes de consumo en lo que a ancho de banda respecta.

El número total de paquetes procesados asciende a 75.757.051, de los cuales el 98.9% es de flujo unicast, de un solo destinatario a otro en especifico, esto es comprensible tomando en cuenta que se esta viendo el trafico entre las dos tarjetas que conforman la configuración bridge de NTOP.

El 26.7% de los paquetes que circulan hacia afuera de la red, están por debajo de los 64 bytes, el 29.6% de 64 a 128 bytes y un 22.7% consta de paquetes grandes de entre 1024 y 1518 bytes, esto muestra un tráfico moderado y hasta cierto punto normal tomando en cuenta el tamaño del paquete promedio en 377 bytes y registrando un 0.03% apenas, en paquetes superiores a los 1518 bytes, este es el caso del paquete mas pesado registrado en 1,514 KBytes.

Un dato importante es que, a pesar de la presencia de trafico No-IP como es IPX y SPX, generalmente transportado a través de redes privadas virtuales VPN sobre la red de Alianzanet, se registran apenas 64.9 MB de 30.7 GB (74,744,339 de Paquetes) como trafico No-IP, lo cual no llega a saturar la red, como se vio en capítulos anteriores este tipo de trafico es generalmente usado en redes LAN ya que su rendimiento es mejor que el de

TCP/IP para este segmento de las red, pero es pobre en enlaces WAN, ya que genera demasiado trafico broadcast que satura la red, en este caso para la red de Border del nodo Carolina, el trafico broadcast presente es de 1.1% en el segmento donde se encuentra NTOP.

En cuanto al parámetro TTL de los paquetes este se encuentra entre 32 y 64 representando el 26.7%, y un 45% entre 96 y 128, valores nominales que nos muestran que la mayoría de destinos alcanzados por los paquetes generados por los clientes, están ubicados en un promedio de 86 saltos, como los muestra la Tabla 4.20.

4.4.1 Distribución Global de protocolos

Tabla. 4.21 Reporte de Tráfico

Protocol	Data	Percentage				
IP	30.7 GBytes	99.8%	TCP	22.0 GBytes	71.6%	
			UDP	3.7 GBytes	12.0%	
			ICMP	363.5 MBytes	1.2%	
			ICMPv6	72.1 KBytes	0%	
			IPSEC	506.4 MBytes	1.6%	
			IGMP	98.2 KBytes	0%	
			Other IP	55.7 MBytes	0%	
(R)ARP	40.2 MBytes	0%				
IPX	420.9 KBytes	0%				
IPv6	905.4 KBytes	0%				
STP	1.1 MBytes	0%				
Other	9.4 MBytes	0%				

En la Tabla 4.21 se puede observar que el 99.8% de los protocolos que corren sobre la red de border están dentro del grupo de protocolos IP, de los cuales, el 88.7% (30.7 GB) es de tipo TCP, es decir orientados a la conexión, mientras que el restante 21.3% son protocolos a nivel de datagramas UDP, ICMP, IGMP, IPSEC, etc.

El tráfico IPSEC equivalente al 1,6% representa un volumen de datos casi nulo, lo cual refleja el hecho de que no exista un elevado trafico de redes VPN activas, a través de este tipo de túneles IPSEC. Esto es importante ya que, como es conocido, este tipo de trafico es bastante pesado, lo cual exigiría un esfuerzo adicional, principalmente a las redes de Acceso y Core.

Por otro lado el 1.4% corresponde a protocolos No-IP entre los que, como se mencionaba anteriormente, están IPX, al igual que ARP, STP y un porcentaje inferior al 1% en el que

destaca un mínimo trafico de tipo IPv6, mismo que no es catalogado por NTOP, ni como IP tampoco como No-IP, dado que corresponde a la evolución de IPv4, manejando los paquetes de manera distinta, como se menciona en capítulos anteriores.

A continuación se encuentran documentados el consumo de tráfico para los más importantes protocolos que corren sobre la red de Border de Alianzanet, protocolos importantes tanto por su presencia en la red medida en Bytes, sino por su contribución a análisis, motivo de este proyecto de tesis.

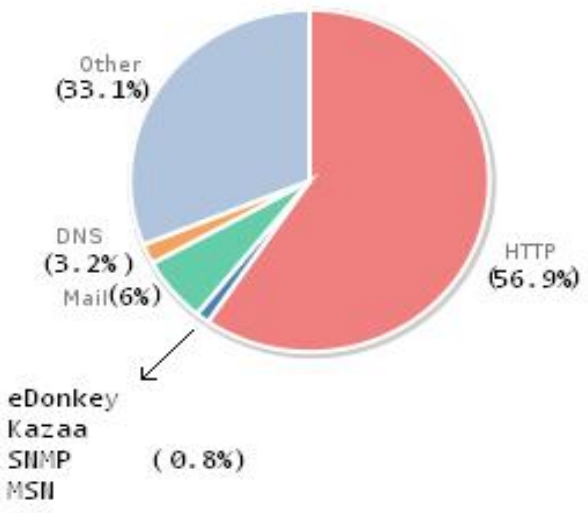
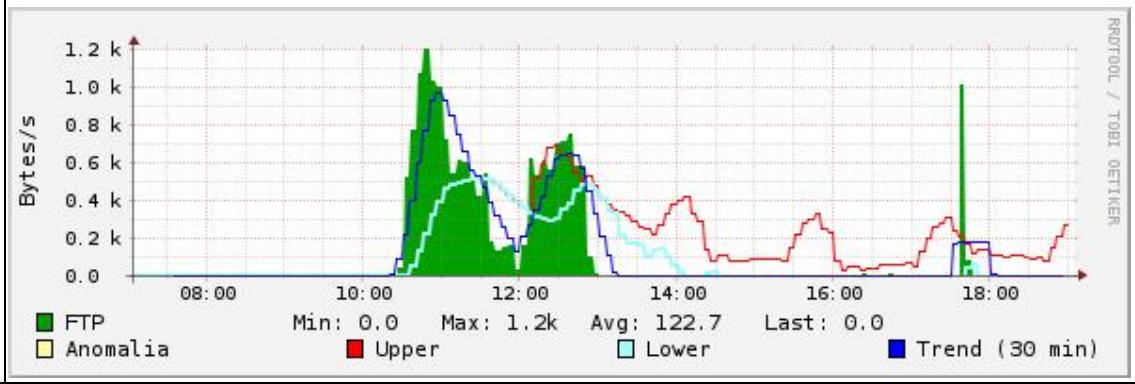
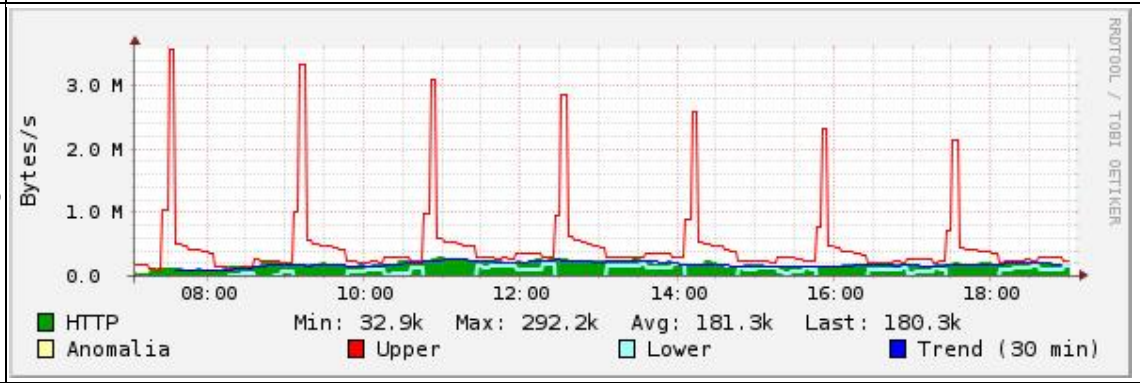
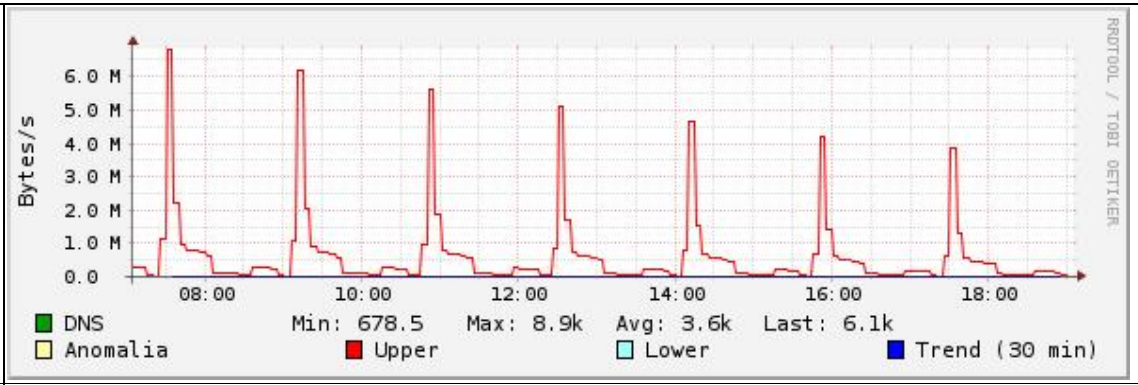
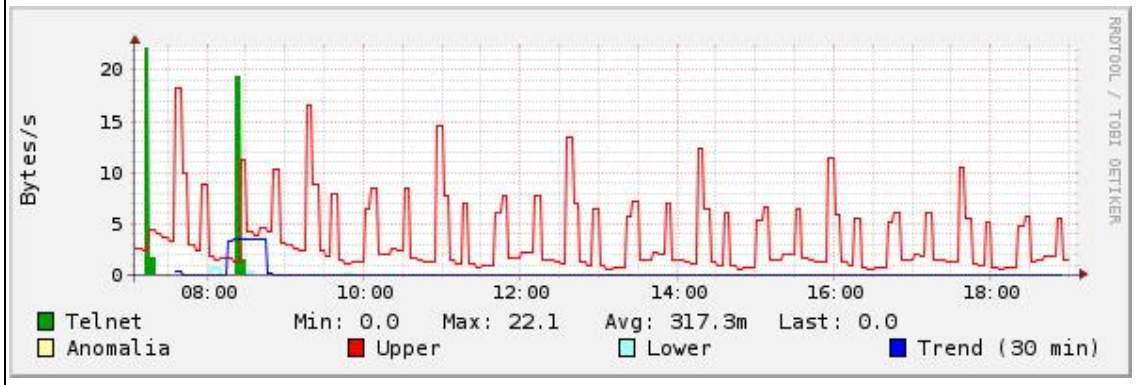


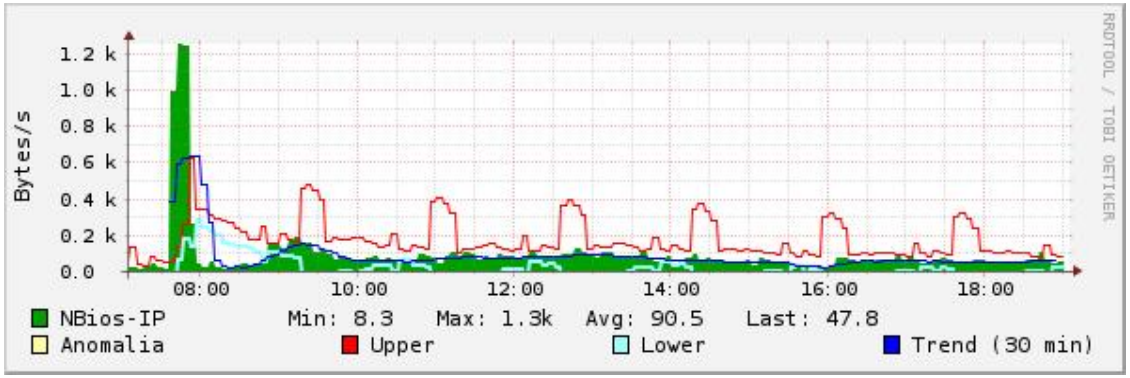
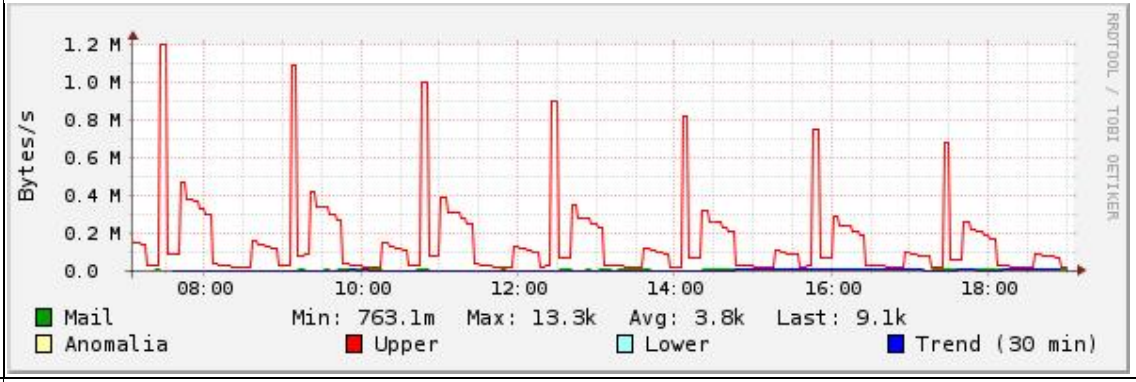
Figura. 4.29 Distribución de protocolos

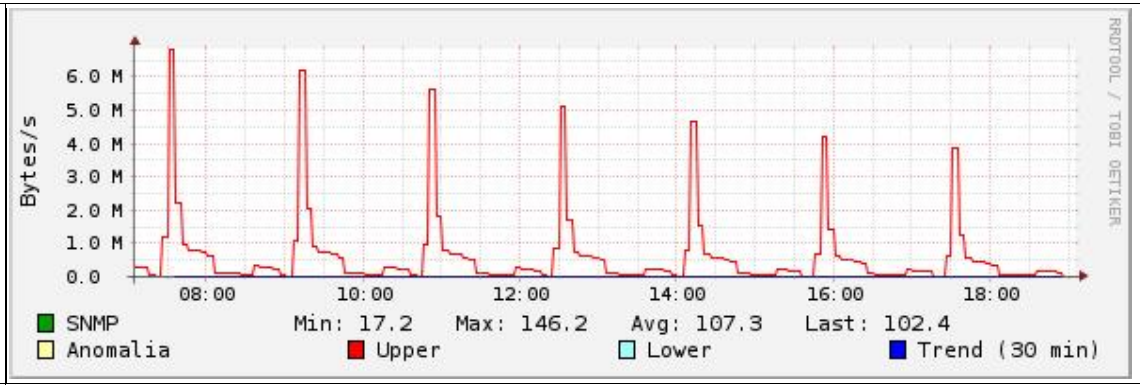
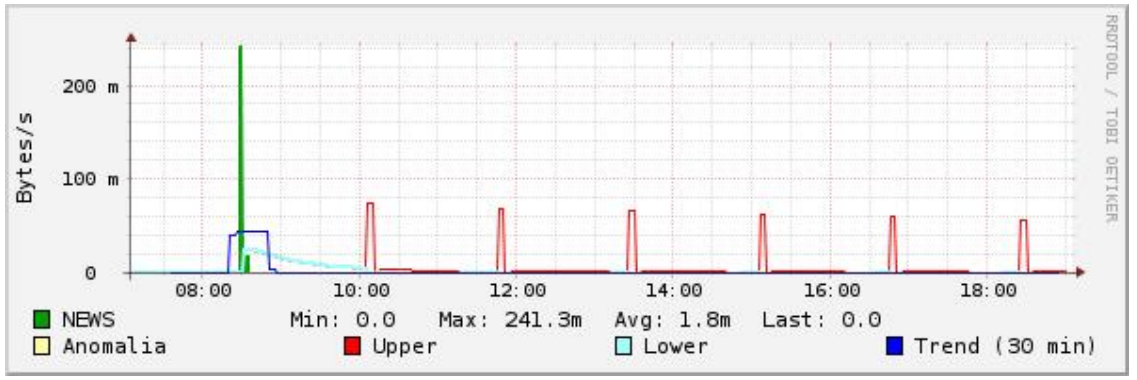
A continuación se dará revista de manera global al tráfico que circula por el border Carolina de Alianzanet, se listará a la vez los puertos abiertos en la red de border, en los últimos dos minutos de medición, esto por algoritmo propio del sistema NTOP.

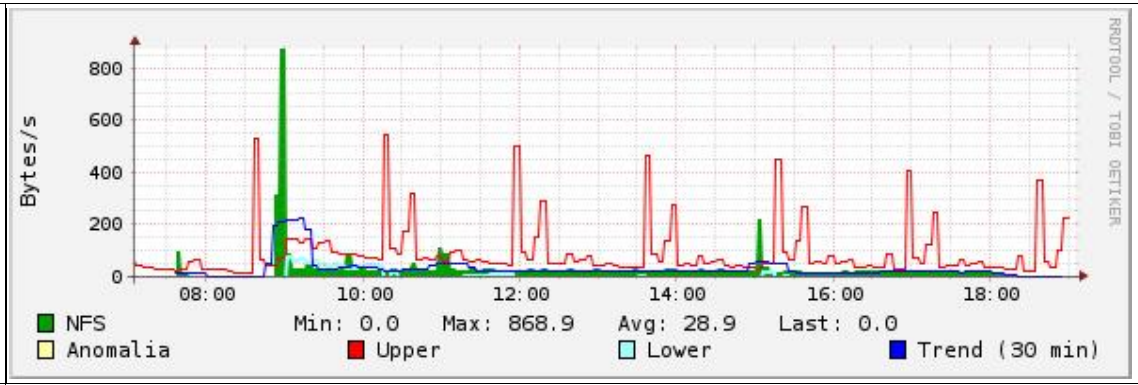
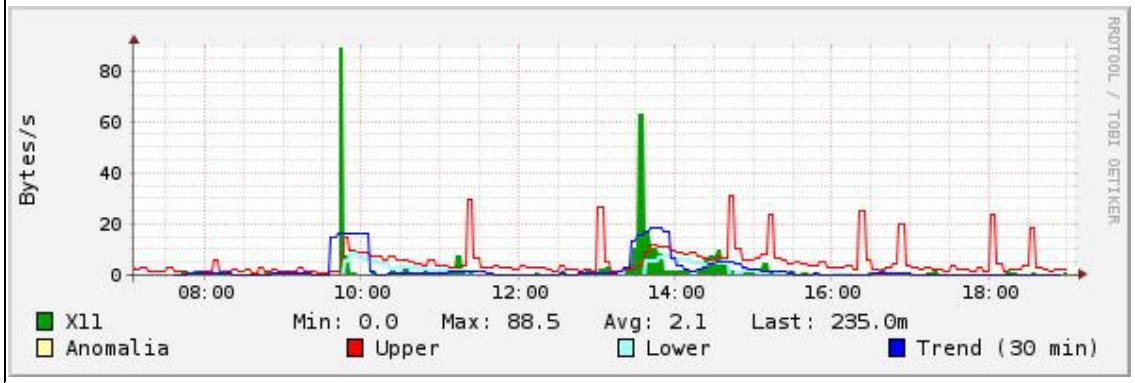
Tabla. 4.22 Trafico de Protocolos IP Acumulado

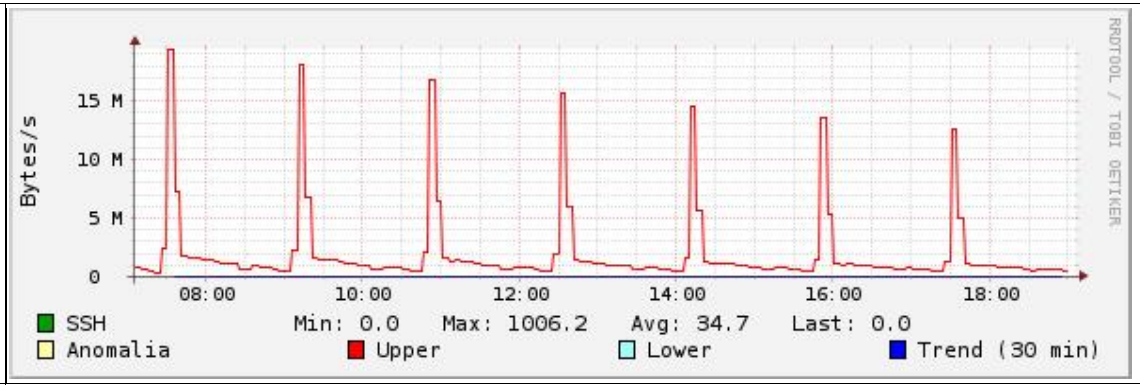
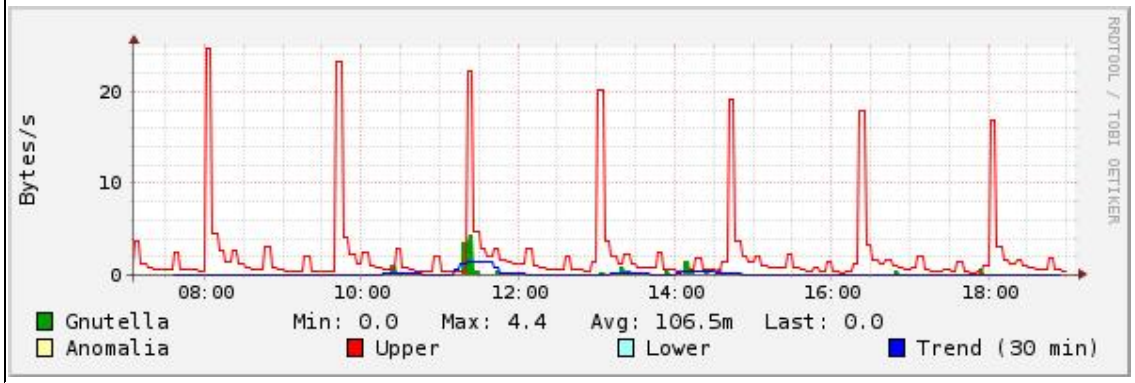
Protocolos TCP/UDP	Datos	Conexiones	Porcentaje Acumulado / Historico del Protolo	
FTP	5.1 MBytes	214	0%	
HTTP	17.2 GBytes	3,507	56.9%	

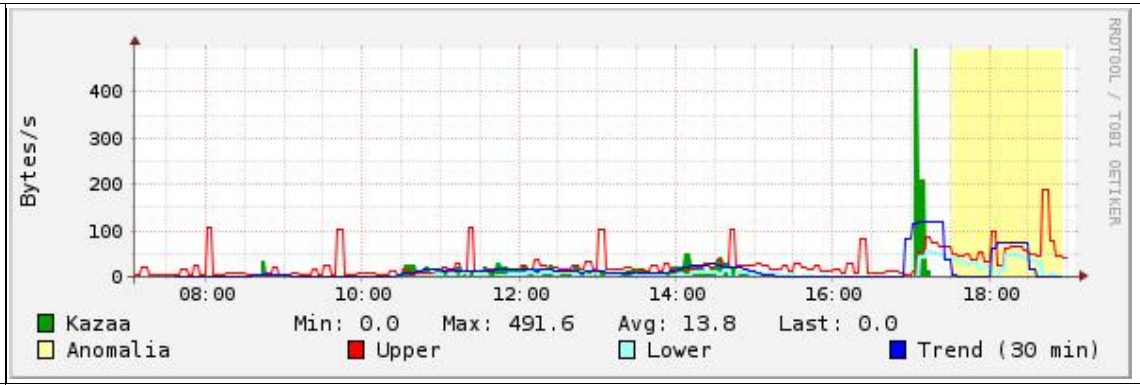
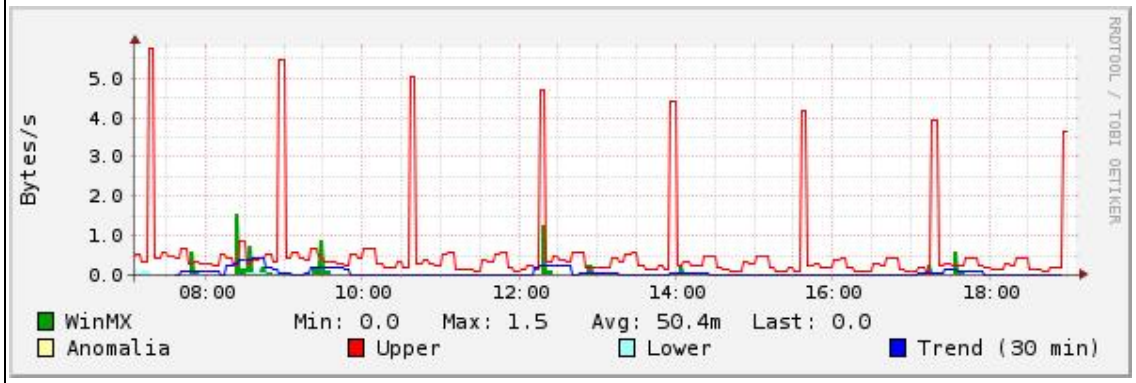
DNS	900.3 MBytes	2,807,618	3.2%	
Telnet	40.3 KBytes	83	0%	
NBios-IP	8.7 MBytes	37,395	0%	

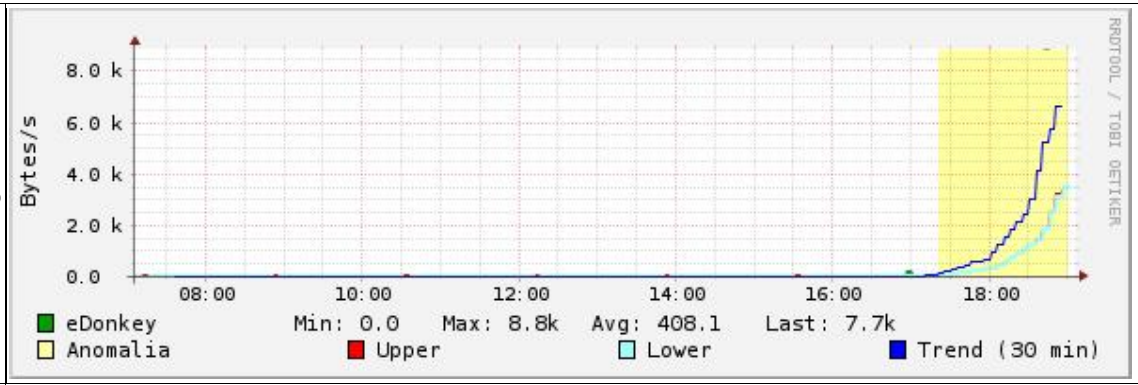
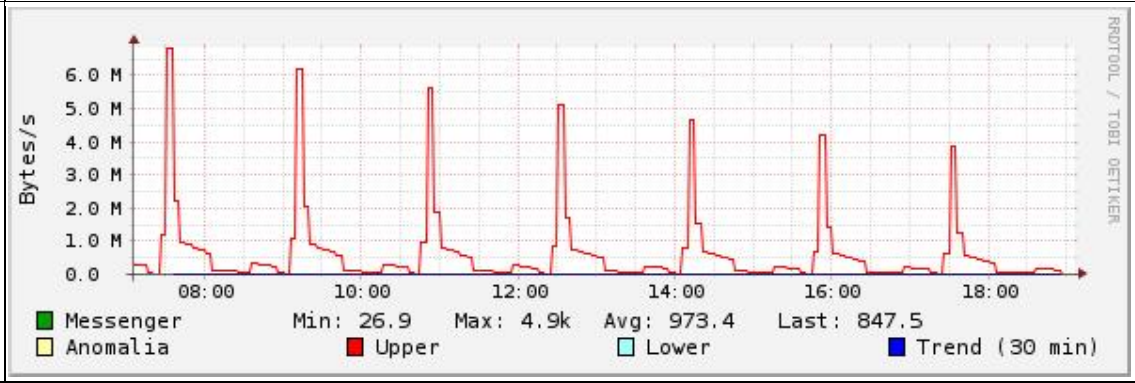
				
Mail	1,813.7 MBytes	155	6%	
SNMP	16.7 MBytes	181,796	0%	

				
NEWS	0.4 KBytes	1	0%	
NFS	2.8 MBytes	251	0%	

				
X11	128.5 KBytes	703	0%	
SSH	10.9 MBytes	4	0%	

				
Gnutella	73.6 KBytes	118	0%	
Kazaa	877.2 KBytes	324	0%	

				
WinMX	14.5 KBytes	55	0%	

eDonkey (servidor P2P)	17.7 MBytes	433	0%	
Messenger	86.5 MBytes	664	0%	
Other TCP/UDP-based Protocols	10.1 GBytes	8,173,389	33,1%	

5

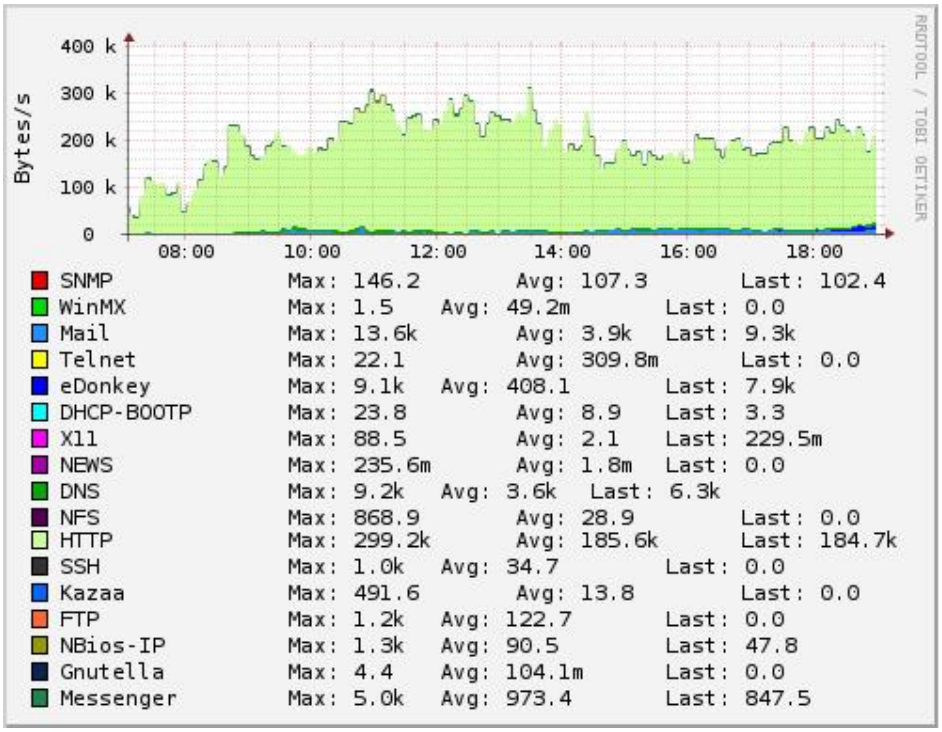


Figura. 4.29 Grafico Acumulado Distribución de protocolos

Tabla. 4.23 Resumen de Puertos por protocolo

TCP/UDP Port		Total	Sent	Rcvd
www	80	2.6 MBytes	2.4 MBytes	151.3 KBytes
1160	1160	453.0 KBytes	10.9 KBytes	442.1 KBytes
3227	3227	339.9 KBytes	9.1 KBytes	330.7 KBytes
smtp	25	300.1 KBytes	139.0 KBytes	161.2 KBytes
pop3	110	90.3 KBytes	87.2 KBytes	3.1 KBytes
62156	62156	289.4 KBytes	5.6 KBytes	283.9 KBytes
61488	61488	276.6 KBytes	6.3 KBytes	270.3 KBytes
62017	62017	177.8 KBytes	6.1 KBytes	171.7 KBytes
3954	3954	138.1 KBytes	3.8 KBytes	134.3 KBytes
49635	49635	134.1 KBytes	4.5 KBytes	129.6 KBytes

49218	49218	115.1 KBytes	4.2 KBytes	110.9 KBytes
49226	49226	114.1 KBytes	4.7 KBytes	109.4 KBytes
3952	3952	110.9 KBytes	3.2 KBytes	107.7 KBytes
4662	4662	104.8 KBytes	27.0 KBytes	77.8 KBytes
62567	62567	98.0 KBytes	3.4 KBytes	94.6 KBytes
9049	9049	98.0 KBytes	94.6 KBytes	3.4 KBytes
0	0	83.8 KBytes	83.3 KBytes	568
15970	15970	81.7 KBytes	79.4 KBytes	2.3 KBytes
11457	11457	81.7 KBytes	2.3 KBytes	79.4 KBytes
15969	15969	79.1 KBytes	77.0 KBytes	2.1 KBytes
39760	39760	76.4 KBytes	2.1 KBytes	74.3 KBytes
15972	15972	76.4 KBytes	74.3 KBytes	2.1 KBytes
4672	4672	76.0 KBytes	2.2 KBytes	73.9 KBytes
15923	15923	75.8 KBytes	73.7 KBytes	2.1 KBytes
58958	58958	70.8 KBytes	68.6 KBytes	2.2 KBytes
16005	16005	70.8 KBytes	2.2 KBytes	68.6 KBytes
55523	55523	52.8 KBytes	50.5 KBytes	2.4 KBytes
50878	50878	52.8 KBytes	2.4 KBytes	50.5 KBytes
49738	49738	51.3 KBytes	770	50.6 KBytes
13171	13171	51.3 KBytes	50.6 KBytes	770
2156	2156	49.3 KBytes	5.6 KBytes	43.7 KBytes
domain	53	48.1 KBytes	29.3 KBytes	18.8 KBytes
41879	41879	41.7 KBytes	385	41.4 KBytes

4.4.2 **Distribución de los principales protocolos TCP/UDP**

La tabla 4.20 resume el trafico de todos los protocolos y conexiones, que se establecen hacia la red de border de Alianzanet y hacia el internet, sin embargo, existen algunos protocolos que, por su mayor grado de presencia e importancia, son resumidos en las tablas 4.24 a la 4.30, de manera específica.

Antes de empezar con el análisis de la información recabada por NTOP, se hace necesario, describir cada uno de los ítems, que componen los gráficos y tablas, sobre los protocolos que ruedan sobre la red de Alianzanet.

Para entender los gráficos generados por NTOP, como primer punto, tenemos el hecho de que, la grafica que traduce el comportamiento del protocolo, la cual corresponde a:

Tabla. 4.24 Guía para interpretar los gráficos

OBJETO	DESCRIPCION
EJE X	Hora del día a la cual se capturo la información diagramada, a intervalos de dos horas entre cada valor en el eje, y dividido, cada intervalo, en subintervalos de 30 minutos.
EJE Y	Consumo en Kbps
COLOR VERDE	Trafico del Protocolo a través del tiempo
ROJO	Umbral superior de consumo
CELESTE	Umbral Inferior de Consumo
AMARLLO	Anomalia, comportamiento fuera de los umbrales registrados en determinado punto pasados los 30 minutos de mantener una tendencia.
AZUL	Tendencia sobre la cual se mantiene el consumo dl servicio, esta es establecida cada 30 minutos de mantenerse determinado comportamiento.

En cuanto a la tabla que acompaña cada una de las gráficas, resume los valores registrados por la herramienta, de la siguiente manera:

- **Protocolo:** Enuncia el nombre del protocolo razón de la tabla en cuestión, cabe recalcar, que en el caso especifico del correo electrónico y la mensajería instantánea, la herramienta resume el conjunto de protocolos que engloban dicho trafico como ***Correo*** **y** ***Messenger*** en cada caso, sin especificar los protocolos que intervienen de manera formal, como es el caso del correo electrónico, que dependiendo del sistema que se utilize intervienen IMAP, POP3, SMTP, TSL/SSL, etc, o en el segundo caso Windows Messenger el cual viene incluido con el SO Windows ,que engloba RVP (antiguo protocolo usado en las versiones anteriores a la 2003 de Exchange) y SIP/Simple, todos estos no son mencionados en este caso por NTOP.

- **Conexiones:** Documenta el número de conexiones TCP establecidas por cada protocolo de manera global, es decir, sin especificar que hosts dentro de red las han establecido. Se debe recordar que TCP es un protocolo orientado a la conexión, por lo que, dependiendo del protocolo, se realizaran infinidad de conexiones para establecer los diferentes servicios propios de TCP/IP.

- **Trafico:** Establece el trafico acumulativo del protocolo, desde el momento mismo en el que la herramienta, en este caso NTOP, se encuentra capturando los paquetes para el análisis, es decir, no representa el valor máximo o promedio, de trafico de determinado protocolo, para determinado punto de la grafica, sino recoge un valor acumulativo de todo el tráfico registrado por NTOP para ese protocolo.

- **Porcentaje:** En la Tabla 4.20 se había mencionado que el 71% del tráfico IP de Alianzanet, es de tipo TCP, orientado a la conexión, lo cual representa 22 GB de trafico total, los porcentajes designados en las tablas representan, la correspondiente cantidad de trafico por protocolo, por ejemplo, HTTP representa el 56.9% de estos 22 GB de trafico global TCP.

En la tabla 4.24 se resume las etiquetas necesarias para la interpretación de las graficas, este es el caso de:

4.4.2.1 Protocolo HTTP (*Hyper Text Transfer Protocol*). O protocolo de transmisión de Hyper Texto, su presencia en la red de acceso y border representa el 60**% del tráfico total**, es decir 22GB desde la **9am Hasta las 19pm**, a través del puerto 80, estandarizado para dicho servicio.

Tabla. 4.25 Protocolo HTTP

PROTOCOLO	Trafico	Conexiones	Porcentaje
HTTP	17.2 GBytes	3,507	56.9%

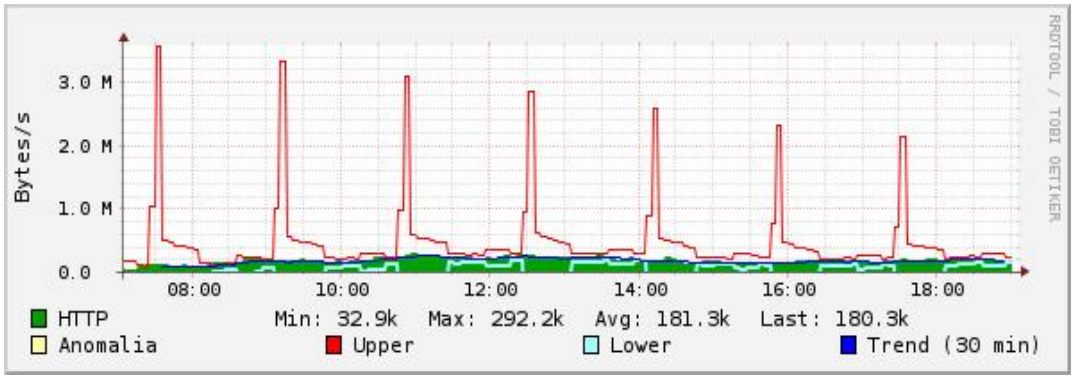


Figura. 4.30 Tráfico HTTP

4.4.2.2 Protocolo "MAIL "(SMTP, POP). Protocolos que sustentan el trafico de correo basado en cuentas de tipo POP3, este tipo de servidores de correo se constituye como el más difundido y utilizado por los usuarios de Alianzanet, esto se evidencia en el tráfico de entrada de correo, el cual se produce, de acuerdo a la Tabla 4.23 a través del puerto 25, sin presencia de puertos de entrad IMAP como son 143, 465, 993, 965, que son puertos estandarizados para el trafico de acceso a servidores IMAP.

La herramienta reporta un 6% del tráfico total IP de Alianzanet, como trafico de correo electrónico, 1813.7 MBytes, con apenas 155 conexiones establecidas durante este lapso del dia, algo a tomar en cuenta es que, el numero de correos enviados por determinado usuario o servidor, es independiente de las conexiones que se establezcan a través del puerto, es

decirm una conexión basta para enviar 1000 correos de 20 KB, lo cual nos da la cifra de 20 MB del trafico total, casi 1% del tráfico registrado en la Tabla 4.22.

Tabla. 4.26 Protocolos Correo

PROTOCOLO	Trafico	Conexiones	Porcentaje
Correo	1813.7 MBytes	155	6%

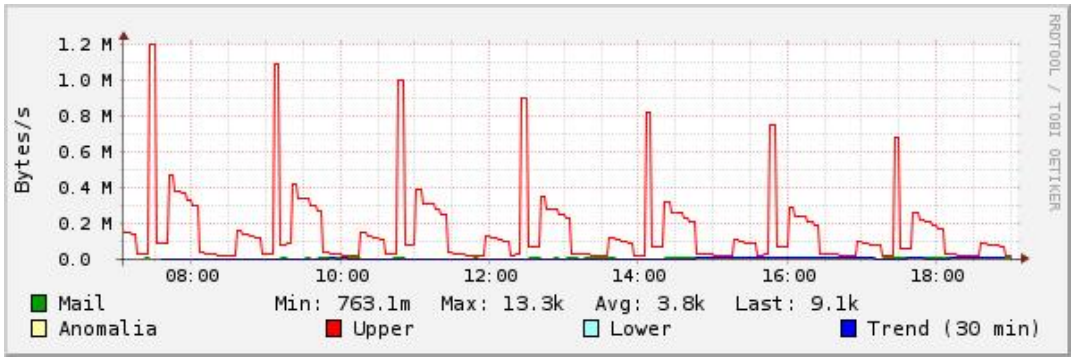


Figura. 4.31 Grafico de Correos

4.4.2.3 Protocolo DNS (Domain Name System). Este servicio es el encargado de transformar los dominios o nombres de internet en bits, lenguaje de máquina, y direcciones IP configuradas en los servidores web a nivel mundial.

El servicio registra un tráfico de 900.3 MB, que representa el 3.2 % del tráfico IP total, lo que se traduce en 2.807.658 conexiones durante el lapso de tiempo antes especificado, todas a través del puerto estandarizado a nivel general para el servicio DNS, el puerto 53, como lo muestra la tabla 4.23.

Tabla. 4.27 Protocolo DNS

PROTOCOLO	Trafico	Conexiones	Porcentaje
DNS	900.3 MBytes	2,807,618	3.2%

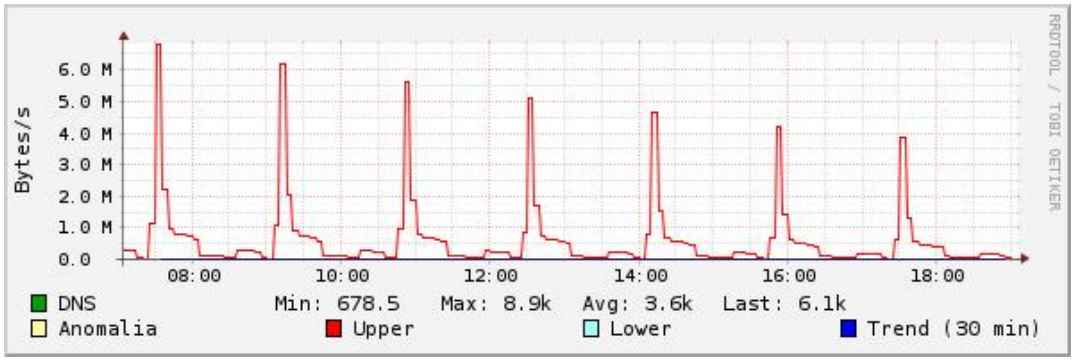


Figura. 4.32 Grafico DNS

4.4.2.4 Protocolo SNMP (Simple Network Management Protocol). Este servicio se encuentra ligado de manera directa, con el presente proyecto de tesis, ya que parte del monitoreo, específicamente aquel que involucra los routers de Alianzanet, se realiza utilizando la información que nos brinda este protocolo, la tabla 4.28 muestra un acumulado de 16.9 MB para este protocolo durante el lapso de tiempo establecido, que representa un 0.09% del tráfico total.

Tabla. 4.28 Protocolo SNMP

PROTOCOLO	Trafico	Conexiones	Porcentaje
SNMP	16.7 MB	182	0.09%

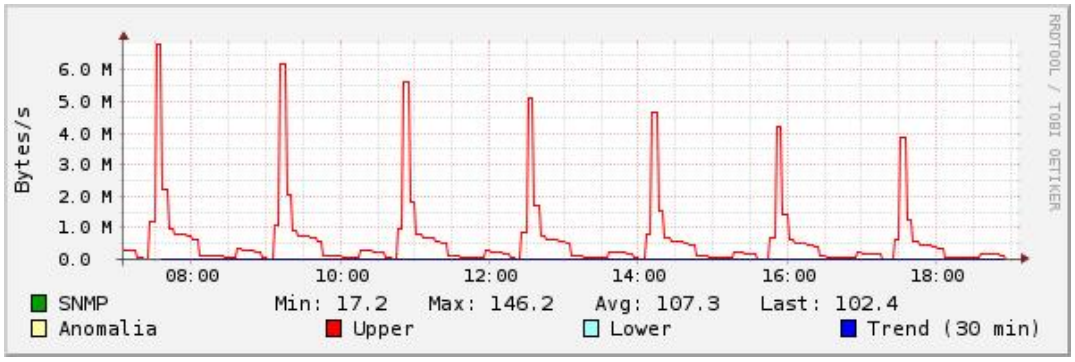


Figura. 4.33 Grafico SNMP

4.4.2.5 Protocols P2P (Pear to Pear Protocol). La tabla 4.29 muestra el trafico acumulado de los dos protocolos, que durante el lapso de tiempo establecido, registran en conjunto un 0.1% del tráfico total.

Por otro lado, se ha incluido el análisis de estos protocolos por una razón, y es que al borde de las 17:00 pm presentan una *anomalía* en su comportamiento, anomalía que es

perfectamente detectada por NTOP, en las figuras 4.29 y 4.30 claramente se observa dicho comportamiento.

Tabla. 4.29 Protocolos P2P

PROTOCOLO	Trafico	Conexiones	Porcentaje
P2P(Edonkey)	17.7 MB	433	0.1%
P2P (Kazaa)	877.2 KB	324	0%

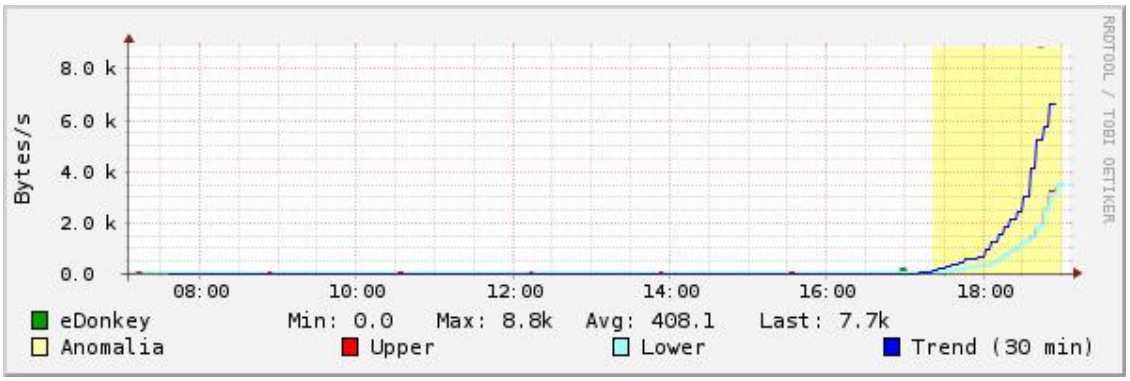


Figura. 4.34 Trafico P2P *Edonkey*

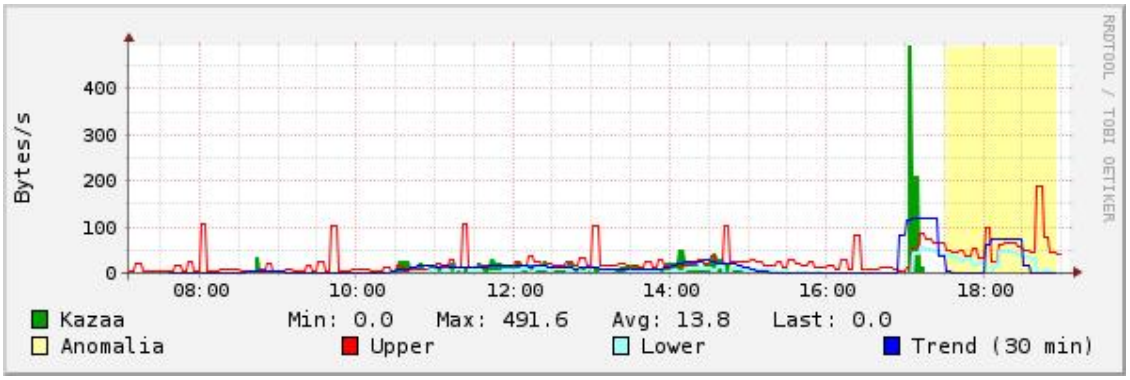


Figura. 4.35 Trafico P2P Kazaa

4.4.2.6 Otros Protocolos. Existe un 40 % de trafico no clasificado, perteneciente a la gama de protocolos TCP, como son RIP, FTP, WinMX, RDISC**,** OSPF, ARP, ICMP, IGMP, IPSEC, NBT, etc., este ultimo como un rezago de lo que fue NetBios como la antesala de TCP/IP para comunicación entre computadores, parte de una red. Este 40% representa un tráfico acumulado de 12GB de los 30 GB recogidos durante el periodo temporal establecido.

Tabla. 4.30 Otros Protocolos IP

PROTOCOLO	Trafico	Conexiones	Porcentaje
Otros	12.1 GBytes	8,173,389	40.1%

Por el lado de los puertos, en la tabla 4.24 se enlistan los puertos a través de los cuales se están estableciendo sesiones TCP/IP, NTOP recoge esta información, del ultimo minuto durante el cual se encuentra escuchando el trafico de Alianzanet, de lo cual se desprende el siguiente análisis.

De los 33 puertos abiertos en este último minuto, el 12% es decir 4 puertos, son puertos conocidos, designando como conocidos, aquellos puertos que se encuentran estandarizados para servicios como son:

- DNS puerto 53
- POP3 puerto 110
- SMTP puerto 25
- HTTP puerto 80

La tabla muestra claramente el tráfico de datos enviados y recibidos en ese momento, y es el puerto 80 aquel que, por obvias razones muestra la mayor cantidad de trafico con 2.6 MB en datos enviados y recibidos, en el último minuto de monitoreo.

CAPITULO 5

ANALISIS DE LOS RESULTADOS

5.1 INTRODUCCION

Más allá de una ciencia un arte, prácticamente reciente, el planeamiento o planificación de las capacidades de determinada red de datos WAN, involucra el balancear, las expectativas de desempeño de dicha red, por parte del usuario, contra la capacidad real de la misma.

Es conocido por todo aquel que se encuentra vinculado al medio, que un ancho de banda generoso en redes WAN, es sin duda costoso, viéndolo desde el estricto punto de vista financiero, muchas de las compañías que ven al accedo a redes WAN como uno de los pilares principales en su negocio, procuran controlar los costos, adquiriendo el mínimo ancho de banda, necesario para manejar su información a través de un circuito WAN.

Más aún es este el caso, de una compañía proveedora de servicios de internet (ISP), como lo es Alianzanet S.A., la cual maneja no solo 1, sino varios circuitos de acceso WAN, uno de los más importantes, el circuito o enlace de Border, vital para encaminar todo el trafico de sus clientes, hacia el internet.

Una adecuada planificación de las capacidades de la red, no solo faculta, en este caso al proveedor de internet, el brindar un servicio de calidad al cliente, sin disminuir el desempeño, sino que repercute directamente en la inversión y el costo de mantenimiento de dicha infraestructura tanto física como lógica, ahorrando a la empresa costos innecesarios.

Basado estudios y una amplia experiencia que data de principios del siglo XXI, el estudio, planificación y presupuesto de redes de área extendido WAN, se constituye como una actividad indispensable, para tomar una decisión al momento de requerir el aumento o disminución del ancho de banda de dicho circuitos.

Para esto, el poseer las herramientas adecuadas, permiten al adminstrador de la red, el tener una visión granular, tanto del consumo de ancho de ancho de banda, así como de los protocolos y el tipo de tráfico que circula por la red.
Luego de cumplir con los puntos anotados en el capitulo anterior:

-Análisis del consumo y congestión del ancho de banda
-Caracterización e identificación del tráfico de Alianzanet

El punto culminante de este proyecto deriva en una síntesis bastante objetiva de los problemas de la red de Alianzanet, y el planteamiento o la planificación de la solución.

5.2 Planificación de la capacidad

5.2.1 Nodo Carolina

Tabla. 5.1 Resumen de Consumo Nodo Carolina

		CONSUMO			
ENLACE	CAPACIDAD	CONSUMO MAX	MINIMO	PROMEDIO	% CANAL LIBRE
TR-1	2048 Kbps	1760 Kbps - 85,9%	1100 Kbps	1430 Kbps - 69,82%	14.30%
TR-2	2048 Kbps	1900 Kbps - 92,77%	1024 Kbps	1462 Kbps - 71,38%	7.30%
TR-3	1544 Kbps	1320 Kbps - 85,5%	990 Kbps	1155 Kbps - 74,8%	14.50%
TR-MPLS	100 Mbps	2350 Kbps - 2,35%	1200 Kbps	1775 Kbps -1,77%	97.70%
CONSUMO PROMEDIO TOTAL:				5822 Kbps	
BORDER	5120 Kbps	5120 Kbps	4500 Kbps	4810 Kbps	
			Saturación del Canal	700 Kbps	

La tabla 5.1 resume los resultados recogidos por la herramienta MRTG, para el consumo de ancho de banda de las interfaces.

La empresa CISCO, multinacional, productora y comercializadora de los equipos más difundidos en lo que a conectividad WAN se refiere, posee un bagaje interminable de estudios sobre

planificación de la capacidad de los circuitos WAN, en múltiples condiciones y sobre diferentes tipos de redes.

De acuerdo con *Cisco IT Global Engineering*, [45]"un circuito WAN que trabaja al 80% de su capacidad, es un circuito saturado, a la vez un enlace que promedia 60% de su capacidad durante el día, llegará a registrar picos del 90% de su capacidad durante ciertos periodos del día, lo cual reduce la productividad de la empresa y repercute sobre las actividades de negocios de las misma".

5.2.1.1 TR-1 2048 Kbps. Esta interface de acceso tiene una capacidad total de 2048 Kbps, de los cuales se alcanza su consumo máximo de 10am a 16pm el 85.9% del enlace, con un consumo promedio del 69.82%. Este consumo de preferencia durante las horas de la mañana y la tarde, se debe a que, a través de este enlace FR, se enlazan principalmente empresas, cuyo tráfico de datos se concentra durante las horas laborables del día.

Los resultados son claros y corroboran el criterio de CISCO mencionado anteriormente, el enlace promedia el 69.8%, lo cual se traduce en picos superiores al 85% a ciertas horas del día, esto constituye un enlace inminentemente saturado.

Adicional a esto, el circuito ATM/FrameRelay alberga a cerca de 49 clientes, lo cual produce, teniendo en cuenta los resultados, un "cuello de botella", termino establecido para enlaces, en este caso WAN, que alimentan a troncales de baja capacidad, la figura 5.1 ilustra claramente lo expuesto para este circuito.

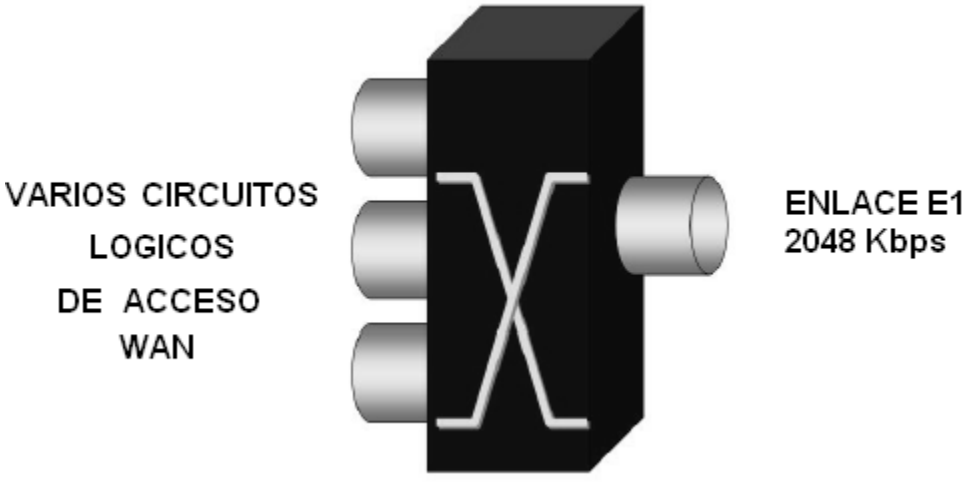


Figura. 5.1 Cuello de botella interfaces Carolina

5.2.1.2 TR-2 2048Kbps. Esta interface registra un consumo máximo del 92.77% equivalente a 1900 Kbps, superior al tráfico de TR-1, esto se explica debido no solo al mayor número de usuarios anclados a este enlace de acceso, sino al ancho de banda por cliente que se conecta a través de la PSTN de Andinatel, esta tendencia se registra de 10am a 17:30 pm. durante al menos 3 días a la semana.

Alrededor de 51 clientes, entre empresas y clientes residenciales, obtienen el acceso a través de este circuito, promediando un consumo del 86% con un ancho de banda libre de apenas el 11.3%, cayendo en saturación, replicando el comportamiento del circuito TR1, constituyéndose como el segundo punto de saturación dentro de la red de acceso de la empresa.

Cabe recalcar que este consumo de preferencia durante las horas de la mañana y la tarde, se deben a que, a través de este enlace FR, se enlazan principalmente empresas, cuyo tráfico de datos se concentra durante las horas laborables del día, sin embargo existe también anclados a este enlace, un número considerable de clientes residenciales, que hacen uso del ancho del banda en las horas de la noche.

5.2.1.3 TR-3 1544 Kbps. La tercera troncal TR3 registra un máximo de 1320 Kbps de 15:30 a 16:30, 1 hora, para replicar la tendencia luego a las 17:00, con picos de 1400 Kbps, este comportamiento es muy diferente al resto de interfaces analizadas anteriormente, y es que esta troncal, alberga en un 95 % a clientes residenciales, los cuales no utilizan el enlace en horas de la mañana, por obvias razones, ya que se encuentran fuera del domicilio, este repunte muestra a breves rasgos, simplemente que en ese momento alguno de los usuarios anclado a esta interfaz, se dispone a utilizar en exceso su canal de bajada, es claro que dicho usuario debe poseer, al menos un enlace de 512 Kbps de bajada, para haber causado dicho repunte.

El circuito promedia 1155 Kbps, el 74% del canal total, albergando a 35 clientes, algo menos saturado que el resto de troncales, pero dentro aún de los lineamientos establecidos, para el análisis de saturación de estos canales.

Este circuito TR3 se constituiría, ya como el tercer punto de saturación en la red de acceso de Alianzanet, esto nos deja ver entre otras cosas, que la empresa no tiene en este punto manera de seguir creciendo en infraestructura lógica, agregando mas circuitos lógicos, a las ya saturadas troncales ATM/Frame Relay analizadas hasta este punto, mas adelante en el análisis y planteamiento de la solución se debatirá el hecho de aumentar el ancho de banda de estos

circuitos, tomando en cuenta que constituyen tecnologías descontinuadas y con poco margen de re potenciación, cabe añadir al análisis un hecho relevante, la saturación de los 3 canales se replica por largo periodos del día, llegando a durar hasta 8 horas casi ininterrumpidas de saturación.

5.2.1.4 TR-4 MPLS 100 Mbps. La troncal IP de Alianzanet tiene un consumo máximo de 2.35 Mbps lo cual representa el 2.35% del ancho de banda total, promediando 1775 Kbps, un 1.7% muy por debajo del 65%, lineamiento establecido para el presente análisis

El canal esta 97% libre y por lo tanto sub-utilizado, esto desde el punto de vista del acceso, ya que el ancho de banda de este canal es controlado por Alianzanet, y no está supeditado al volumen de tráfico que entregue Andinadatos como enlace de acceso, en resumidas cuentas, se pueden utilizar los 100 Mbps íntegros para dar acceso a los clientes.

Si bien aún existen, dentro de la PSTN de Andinadatos, nodos e ingeniería ATM-Frame Relay, estos, tanto equipo activo (DSLAM) como Ingeniería (Ingeniería de tráfico), son soportados por MPLS, y la mayoría ya han sido migrados a MPLS puro.

Esto nos da una muestra de que, por el momento, esta es la única interfaz de acceso, a través de la cual podría tener crecimiento Alianzanet, sin embargo, más adelante se analizará la estrecha relación entre estos enlaces, su capacidad, y la capacidad del canal de salida y del equipo que se está utilizando como router de CORE de la red.

5.2.1.5 BORDER 5Mbps. El enlace de salida del nodo carolina, registra saturación de 9:00 am a 17:30 pm, período de tiempo considerado como de alto tráfico, debido a que a esta hora se encuentran laborando empresas con flujo ininterrumpible de datos de todo tipo, la línea horizontal en la gráfica de consumo nos deja ver que ya se ha superado la capacidad del canal de salida provisto por Andinadatos.

El circuito presenta un consumo máximo de 5120 Kbps, el 100% de la capacidad total, un mínimo de 4500 Kbps (88%) y un promedio superior al 90%, cifras alarmantes, que dejan en claro una cosa, la planificación de las capacidades de la red, se debe hacer de manera constante, para no llegar a sobrepasar los umbrales de consumo, el hecho de que la inversión en IT, por el lado del aumento de ancho de banda, este supeditada a la parte económica de la empresa, pierde validez, cuando la situación de la red, alcanza estos valores de sobre estimación y saturación.

Hablando netamente en cifras, la recopilación de los datos obtenidos de los gráficos de consumo, muestran claramente lo expuesto, el ancho de banda proveído por Andinadatos para Alianzanet **es superado en *700 Kbps,*** esto debido evidentemente a que el consumo de las **interfaces de acceso** en conjunto **es superior a lo contratado por la empresa.**

5.2.2 NODO IÑAQUITO

Tabla. 5.2 Resumen de Consumo Nodo Iñaquito

		CONSUMO			
ENLACE	CAPACIDAD	CONSUMO MAX	MINIMO	PROMEDIO	% CANAL LIBRE
TR-1	1544 Kbps	1480 Kbps-95%	570 Kbps	1024 Kbps - 66%	33.77%
TR-2	1544 Kbps	1320 Kbps-85%	900 Kbps	1080 Kbps - 69,9%	28.10%
CONSUMO PROMEDIO TOTAL:				2134 Kbps	
BORDER	4096 Kbps	3300 Kbps	1300 Kbps	2300 Kbps	44%
			Canal Libre	1796 Kbps	

La tabla 5.2 muestra el resumen de consumo en este nodo, partiendo de estos datos el análisis del consumo de estas interfaces se presenta a continuación.

5.2.2.1 TR-1 1544 Kbps. El circuito T1 presenta un consumo máximo de 1480Kbps, promediando 1024Kbps, el 66% del enlace, un 1% por encima del umbral establecido al principio del capítulo, este pico máximo esporádico, se registra de 18pm hasta las 22pm, apenas 4 horas durante el día, este horario fuera de la actividad laboral corrobora el tipo de clientes que aloja esta troncal y principalmente este nodo, clientes residenciales, con consumos bajos, y poco prolongados.

El consumo que promedia el circuito deja alrededor del 40% del enlace libre durante el resto del día, sin lugar a dudas, el consumo más bajo por hora y por interface de toda la red de acceso de Alianzanet.

5.2.2.2 TR-2 1544 Kbps. Este circuito registra un máximo de 1320 Kbps equivalente al 85% del ancho de banda total del circuito, y promedia 1080 Kbps (69.9%) , esto de 7 am. a 8 pm. y de 15 pm. a 16 pm. Esto muestra un enlace moderadamente saturado, con dos picos de 1 hora cada uno, se nota la clara diferencia que existe entre los circuitos de acceso de este nodo, y los del nodo carolina, saturados en porcentajes superiores al 85%, durante amplios lapsos de tiempo durante el día.

Tabla. 5.3 Consumo Semestral TR-2 Nodo Iñaquito

CONSUMO Kbps	MES
330	1
550	2
660	3
880	4
1080	5

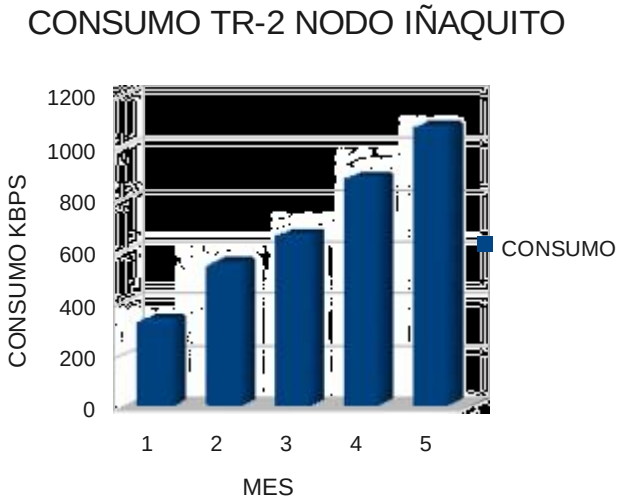


Figura 5.2 Trafico TR-2 Iñaquito ascendente

El análisis de los resultados muestra que, si bien es cierto, todas las interfaces han aumentado su consumo, durante el primer semestre del año 2009, el crecimiento de estas no ha sido exponencial, como es el caso del circuito TR-2 del nodo Iñaquito. La instalación de nuevos

enlaces se ha llevado de manera casi uniforme para todas las interfaces por igual, al igual que el aumento del ancho de banda de los circuitos lógicos anclados a cada una de ellas.

El comportamiento de esta troncal requiere un análisis individual, debido a su comportamiento, y es que la cartera de clientes alojados en este circuito no ha aumentado, sino que a disminuido, desde su ingreso a Alianzanet en Octubre del 2008 con 47 clientes, culminando el primer semestre del 2009 en 39 clientes.

Esto debido a que, los enlaces de esta troncal se han sometido en su mayoría, al proceso de UPGRADE de ancho de banda, proceso por el cual han pasado todos los enlaces de acceso de Alianzanet, pero que sin embargo se ha visto mas evidenciado en este enlace en específico.

De un consumo promedio de 330 Kbps, con enlaces de 128 Kbps limitados en 64 K, a in ancho de banda promedio de 1080 Kbps, un aumento del 327,7 % semestral, bastante lineal, y un aumento del 66.6% mensual, de continuar con este crecimiento, el enlace alcanzaría su tope, al final del mes de Julio del 2009, como lo muestra la figura 5.3.

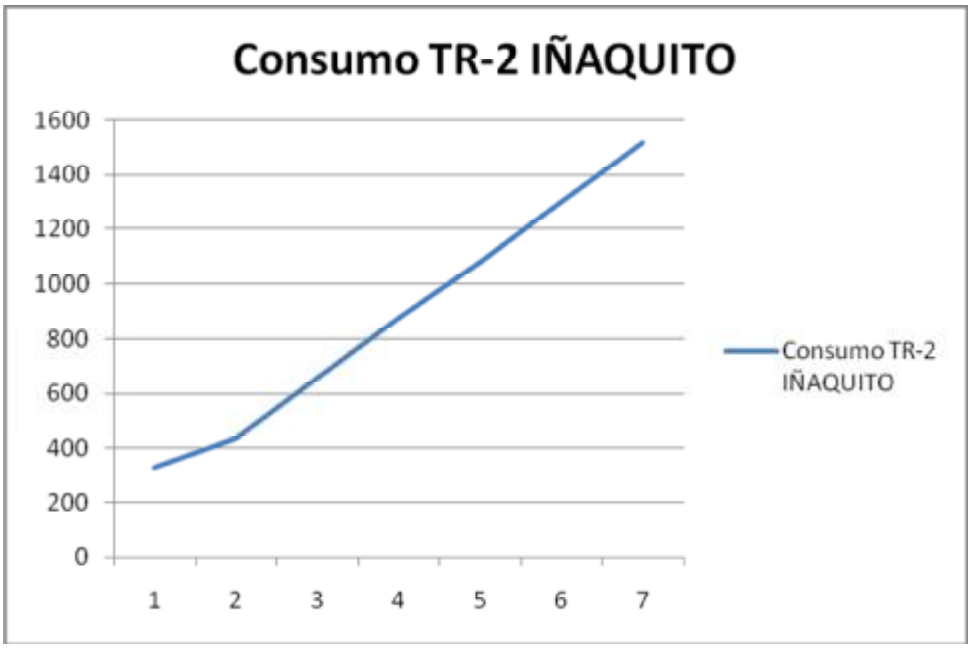


Figura. 5.3 Proyección del trafico en TR-2 Iñaquito

En el análisis de la solución se abordará este crecimiento y su la solución para no alcanzar la saturación del enlace, cabe mencionar que para este circuito, junto con el circuito TR-1 de este modo, se encuentran en vías de saturación, y aún existe una manera de prevenir su inminente

saturación y planificar la solución adecuada para no llegar a los extremos, como ha sucedido ya con las interfaces del nodo Carolina.

5.2.2.3 BORDER 4096 Kbps. El enlace de salida del nodo Iñaquito registra un consumo de 2621 Kbps máximo, la recopilación de los datos obtenidos de MRTG, muestran claramente lo expuesto en la tabla 34, el ancho de banda proveído por Andinadatos para Alianzanet es de ***4096 Kbps,*** sin embargo el consumo máximo se registra en 2300 Kbps, el 56% del canal total, dejando 1796 Kbps libres de saturación.

Por otro lado el circuito en mención presenta un consumo mínimo del 19% en la mañana, esto corrobora lo documentado en las tablas 4.13 y 4.15, sobre el consumo de las interfaces de acceso del nodo Iñaquito, las cuales ven un mayor consumo en la tarde.

Lo analizado para la segunda troncal de acceso este nodo, se ve claramente reflejado para el enlace de border, con un aumento generalizado del consumo de salida en el mes de junio del 2009, con relación a los 5 primeros meses, el aumento en TR-2 se refleja en el Border.

En general las dos interfaces de acceso tienen entre el 30 % y el 40 % de canal libre, apegados al criterio de CISCO para enlaces WAN basados en su tecnología, estos enlaces deberían mantener este registro, sin llegar a promediar el 65% de su consumo, como se ha visto ya para el nodo Carolina.

5.3 Caracterización de Tráfico

En este punto del análisis, la caracterización del tráfico implica la identificación, del tipo de datos que circula por este segmento de red, el segmento de border, en qué cantidad, y cómo influye al correcto funcionamiento de la misma.

La medición del tráfico en general, no hace lo suficiente para la correcta caracterización del tráfico de la red, esencialmente si el objetivo es tomar una decisión sobre el aumento de ancho de banda del canal.

El desconocimiento sobre el tipo de tráfico que circula por la red, hace imposible la tarea de implementar acciones, a nivel lógico (software) como físico (hardware), para solventar los problemas que presenta la red, a esto se suma, complicando la caracterización del tráfico, el echo de que muchas de las aplicaciones que usan los usuarios sobre el internet, se valen de puertos

dinámicos, estas aplicaciones se encuentran ya bastante difundidas, y representan, sobre la red de Alianzanet, el 40% del tráfico total de protocolos.

Es el caso por ejemplo, de aplicaciones que involucran transportar tráfico de audio y video sobre el internet, lo que implica el implementar políticas de calidad de servicio (QoS), sin la identificación del tráfico, es imposible establecer los lineamientos necesarios para aplicar el estándar mencionado, garantizando un alto rendimiento, con un consumo de ancho de banda menor al utilizado sin la intervención de QoS.

5.3.1 Protocolo Http

Presencia: 56.9 %
Puerto : 80

Esta cifra de tráfico http, la más alta registrada por la herramienta, es comprensible, ya que todos los sitios web en la actualidad brindan un portal, una interfaz para el usuario basada en este protocolo, estableciéndose **3000 conexiones** a través del puerto de comunicación estandarizado para http, puerto 80, cabe destacar el hecho de que, dichas conexiones son cerradas el momento en el que el usuario deja de acceder a determinado servidor web, esta conexión se establece una sola vez, mientras el usuario permanece conectado al servidor web, sea cual fuera el vinculo al que acceda, dentro del mismo servidor, excepto el momento en el que accede a servicios adicionales como son mail, PPP y por añadidura, antes del acceso, la consulta respectiva al servicio de nombre DNS.
Este casi 60% nos da la medida de que, si bien es cierto, el usuario utiliza el acceso al internet, en la mayoría de las ocasiones, para consultar determinado servidor web, un restante 40% del tráfico no es http, lo cual implica la intervención de otros servicios, conexiones y puertos, lo que pone una alerta al administrador de la red, sobre la identificación de está restante 40%, el cual podrá ser inofensivo o dañino, para el correcto desenvolvimiento del servicio.

5.3.2 Protocolos de Correo, entrante y saliente:

Presencia : 6%
Puertos : 25,110

La presencia de este tráfico durante el día deja en claro que el trafico de correo, a pesar de ser bastante liviano por naturaleza, puede representar una amenaza, dado que este 6% representa un tráfico de 2GB, a pesar de establecerse para esto, apenas 155 conexiones.
Este comportamiento pone en alerta al administrador de la red sobre posible correo masivo, la prueba clara de esto está en la tendencia a mantener trafico de correo por sobre los 30 minutos ininterrumpidos, registrado en la figura 48, en el periodo de las 15 a las 17 horas, es decir, 2 horas de trafico de correo con lapsos de 30 minutos sin interrupciones, evidenciando trafico spam momentáneo.

5.3.3 Protocolo DNS

Presencia : 3.2%
Puerto : 53

Este servicio, es uno de los más importantes para la correcta navegación de los usuarios, un inconveniente o el mal funcionamiento del servidor de nombres, recae en la completa y total anulación del acceso a internet, desde el punto de vista del usuario, en el caso de Alianzanet este se encuentra alojado en el nodo Carolina, bajo el FQDN (*Fully Qualified Domain Name*) ***ns.alianzanet.net.***
Un 3,2% de tráfico DNS es insignificante en cuanto a cifras, contrastando con las cifras del tráfico HTTP, el tema conexiones a puerto presenta un comportamiento apenas comprensible tomando en cuenta la forma que utiliza el servidor DNS para consultar por el nombre o ubicación de determinado servidor, el servidor DNS principal de Alianzanet, en este caso 201.219.36.100, debe establecer 3 conexiones diferentes a los servidores DNS principales a nivel mundial (*root,top,resolver)* para que el host que realizó la petición pueda acceder a la página de interés. Esto explica el elevado número de conexiones a través de este puerto, adicionalmente el servidor

de Alianzanet trabaja en la categoría de *resolver* dentro de la red de servidores de nombres a nivel mundial, por lo que también recibe peticiones del resto de servidores DNS a nivel internacional.

5.3.4 Protocolo SNMP

Presencia : 0.1%
Puerto : 161, 162

Un 0.09% a pesar de ser prácticamente insignificante, representa uno de los protocolos mas importantes para el monitoreo de Memoria, uso del CPU y consumo de trafico de los routers CISCO que cubren la red de Alianzanet, así como de sus interfaces.
Se establecen alrededor de 324 conexiones a través del puerto 161, equivalente a todas las consultas que realizan los sistemas de monitoreo, para el control, notificación y medición de los componentes de los equipos CISCO, como son:
- Consumo de ancho de Banda CACTI

- Estado de las interfaces UP&DOWN NAGIOS

- Estado de recursos de memoria, procesador, etc. NAGIOS

5.3.5 Protocolo P2P

Presencia : 0.09 %
Puerto : Asignación de puertos libres de manera Dinámica

Durante el período de tiempo establecido, el tráfico de este tipo de servicio, denominado P2P es insignificante, lo cual es alentador tomando en cuenta lo perjudiciales que pueden llegar a ser estos protocolos para el correcto funcionamiento de la red, principalmente porque transportan un nutrido trafico de Malware, Virus y Spyware, esto tomado del Capítulo correspondiente, donde se deja en claro la forma en la que este tráfico se esparce por la red.

A las 17pm, en las figuras 53 y 54, se registra una anomalía, la anomalía se constituye como un comportamiento inusual de determinado protocolo, y se presenta generalmente cuando el uso del protocolo sobre la red, sobrepasa los umbrales o la tendencia de comportamiento, que se ha

venido registrando por la herramienta NTOP, en este caso la tendencia en los dos casos es a la alta *(upper)* conforme avanzan las horas, de 0kB a 6KB en aumento, para el servidor Edonkey, y de 100 KB a al doble 200KB para el servicio tipo P2P Kazaa, aumentando tanto su umbral inferior, como el superior, esto nos da la medida de que estos protocolos son utilizados por los usuarios de la red de Alianzanet, con mayor frecuencia conforme avanzan las horas de la noche, con un punto de inflexión al borde de las 17 pm.

5.3.6 Otros Protocolos:

Presencia : 40.1%

Protocolos : Múltiples protocolos (P2P anónimos, MSN, skype, protocolos sustentados por 802.1p)

Como es conocido, existe un sin número de protocolos que recorren la red de un ISP, en su tráfico hacia las redes internacionales, en apartados anteriores se abordo aquellos protocolos que, por su importancia y presencia, merecen ser analizados a fondo.

En esta ocasión se pasará revista, como última instancia en este análisis de protocolos, aquellos protocolos que sin dejar de ser importantes, no representan información desequilibrante, para el posterior análisis final del estado de la red de Alianzanet. Mucho de este tráfico involucra a las instancias de ruteo, servicio de nombres, mensajes de handshake, sesiones activas punto a punto, en fin.

Engrosan la tabla puertos abiertos, que no se encuentran categorizados o estandarizados, puertos que podrían y de echo están abiertos, para permitir todo tipo de tráfico, incluso tráfico indeseado, estos 29 puertos son solo una muestra, de la cantidad de puertos que deben hallarse abiertos, a cada minuto, dentro de la red de Border de Alianzanet, tomando en cuenta no solo el hecho de que Alianzanet no cuenta con un sistema Firewall físico no tampoco lógico.

5.4 Problemas presentes en la red de Alianzanet

Alianzanet sufre de varios problemas, por diferentes motivos, entre los que figuran:

1. Numerosas interfaces lógicas, enlazadas a una sola interfaz física, que no abastece el trafico de las mismas, este es el caso de las troncales de acceso, tanto T1 como E1, produciéndose cuellos de botella por cada interface de acceso.

2. Interfaces lógicas que abarcan un ancho de banda que supera más del 80% de la capacidad total del enlace físico, y que a la vez promedian más del 65% del ancho de banda total.

3. Un trafico total desde la red de acceso hacia la red de border de 5822 Kbps, superando a lo contratado por Alianzanet para el enlace de salida, 2 E1 + 1024 Kbps, es decir, 5120 Kbps, produciendo congestión en la red de border debido a que el enlace de salida no satisface la demanda de la red de acceso.

4. A diferencia del nodo de Iñaquito, donde los niveles de saturación no han alcanzado valores críticos, para el nodo carolina el análisis de consumo de ancho de banda, y la caracterización del tráfico, iniciaron cuando la red ya estaba saturada, por lo que la decisión del aumento de ancho de banda es una decisión que se debe tomar de inmediato.

5. La red de Alianzanet, no cuenta con un dispositivo *Firewall* físico, colocado entre la red de Border y la red de Core, así mismo no se encuentran definidas ACLs (*Access List*) basadas en *IP Tables* (Tablas IP), las cuales podrían bloquear cierto tipo de trafico, ya que esto que aumentaría de manera desmedida el trabajo de dichos equipos, causando la inestabilidad de la red por cortes en el servicio, consecuencia del elevado consumo de memoria y procesador en los equipos. E resumen no se encuentran definidas políticas de seguridad como protección ante ataques provenientes del tráfico entrante y saliente, esto más que por una mala administración de la red, por un tema de presupuestos.

6. Las redes de acceso, core y border, se encuentran sustentadas por un único ruteador marca CISCO modelos 2801 y 1800 para cada nodo, mismos equipos que, a pesar de su gran versatilidad, y de la garantía que da la marca a sus productos, poseen una capacidad limitada, de 10 Mbps y 5.1 Mbps para trafico de salida, esto genera un

trabajo de NAT elevado, consumiendo demasiados recursos en procesador, esto de acuerdo a las hojas de especificaciones técnicas adjuntas al Anexo.

7. Alianzanet, como un ISP, más no como carrier, depende en el acceso directamente de Andinadatos, es decir, dado que la empresa carrier se encuentra implementando ya los primeros DSLAM MPLS de su red, reemplazando la Ingeniería basada en señalización 7 y ATM, la empresa se vería en la necesidad de analizar, que tan conveniente sería ampliar el ancho de banda de los circuitos ATM, dado que es una tecnología que se está reemplazando paulatinamente por MPSL.

8. El ISP mantiene dos redes, en acceso, core y border, para el manejo de sus clientes, en los nodos Carolina e Iñaquito, separados geográficamente, su administración y desempeño son totalmente independientes, y no existe interconexión, ni lógica ni física entre ellos, a la ves no existe un enlace de backup, en caso de existir problemas con alguna de las salidas internacionales que posee la empresa. Cabe recalcar

Los inconvenientes enunciados, implican serias repercusiones para la empresa, no solo en el aspecto técnico, con un bajo desempeño de la red en general, sino consecuencias a nivel económico y productivo, indiscutiblemente a nivel de los clientes, reduciendo la productividad, afectando negativamente la actividad de negocios y comercio, para las dos partes.
Es por eso que el análisis llevado a cabo en el presente proyecto de tesis, analiza desde el punto de vista individual, a cada una de las interfaces que componen la red de core de la empresa.

5.3 Ingeniería actual

En las figuras 5.1 y 5.2 se resume la topología actual de la red en los dos nodos de acceso.

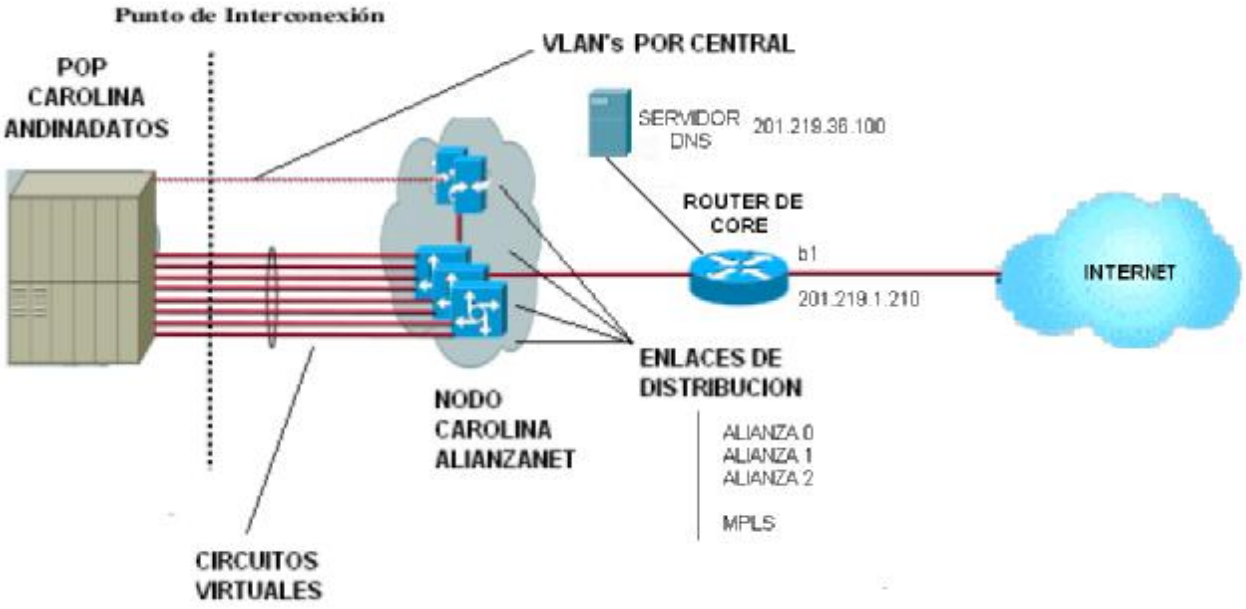


Figura. 5.4 Topología Actual Alianzanet nodo Carolina

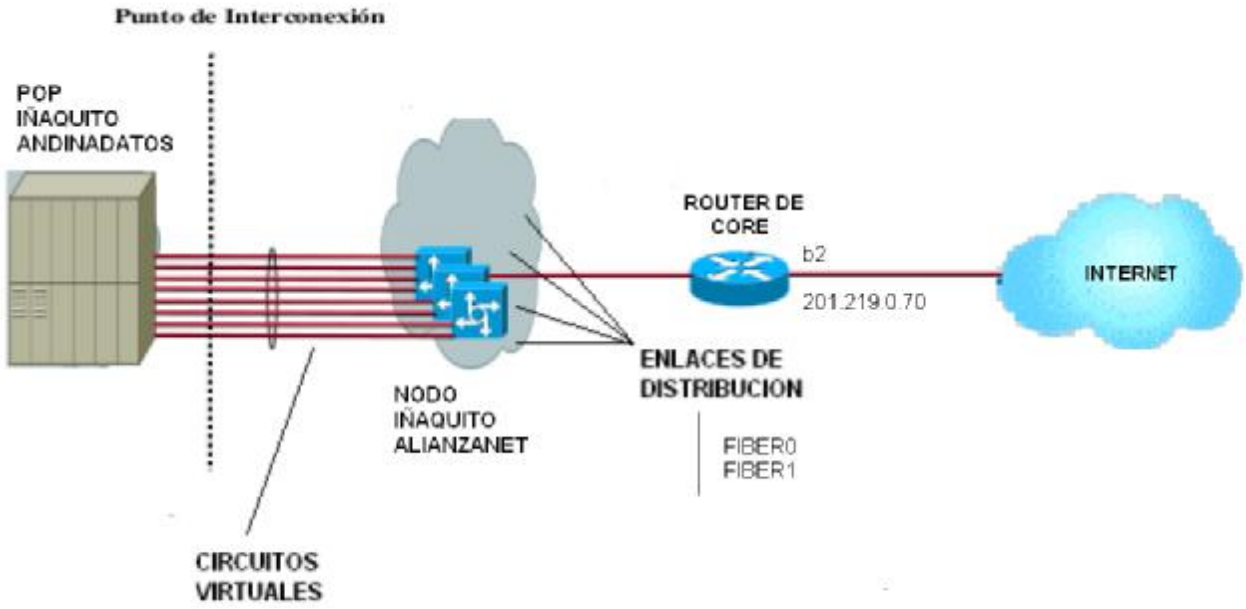


Figura. 5.5 Topología Actual Alianzanet nodo Iñaquito

En la tabla 5.1 se resume el estado actual de la red, un resumen de interfaces, anchos de banda y equipos activos dentro de la red de core de Alianzanet, en cada uno de sus nodos, antes de implementar la solución necesaria para solventar los inconvenientes de la misma.

Tabla. 5.3 Inventario Actual de la red

3NODO	SEGMENTO DE RED	EQUIPO	INTERFAZ	ANCHO DE BANDA	IP	DETALLE
CAROLINA	ACCESO	CISCO 2801	SE 0/1/0	2048 Kbps	N/A	E1 TRONCAL 1
			SE 0/1/1	2048 Kbps	N/A	E1 TRONCAL 2
			SE 0/2/0	1544 Kbps	N/A	T1 TRONCAL 3
			Fa 0/0	100 Mbps	N/A	IP MPLS
	BORDER	CISCO 2801	Fa 0/1	5120 Kbps	201.219.1.210	SALIDA INTERNACIONAL
	CORE	Servidor 0	Fa 0/3/0	100 Mbps	201.219.36.100	Servidor DNS
IÑAQUITO	ACCESO	CISCO 1800	SE 0/1/0	1544 Kbps	N/A	T1 TRONCAL 1
			SE 0/1/1	1544 Kbps	N/A	T1 TRONCAL 2
	BORDER	CISCO 1800	Fa 0/0	4096 Kbps	201.219.0.70	SALIDA INTERNACIONAL

5.4 Planteamiento de la solución

Luego de lo expuesto anteriormente, a continuación se presenta el planteamiento de la solución, a los problemas dentro de la red WAN de Alianzanet.

La planificación adecuada de la red WAN de Alianzanet, se realizara con el objetivo, no solo de prevenir problemas futuros de saturación, seguridad y uso eficiente de los recursos de la red, sino en este caso, la planificación se lleva acabo con el objetivo de resolver los inconvenientes ya presentes dentro de la topología y capacidad de la misma.

Para contrarrestar la saturación de los canales de acceso, principalmente los del nodo carolina, se debe solicitar dos enlaces E1 adicionales, bajo la Ing. ATM/Frame Relay, esto con el fin de cumplir dos objetivos:

1. Migrar usuarios principalmente con anchos de banda superiores a los 256 Kbps, a la nueva troncal, con el fin de descongestionear los enlaces de acceso ATM actuales.

Tabla. 5.4 Análisis de migración

NODO	ENLACE	TIPO	CAPACIDAD	% CANAL UTILIZADO	CANAL SOBRE EL 60%	CANAL A MIGRAR EN Kbps
				ACCESO		
CAROLINA	TR-1	SERIAL - E1	2048 Kbps	85,70%	25,70%	526,336
	TR-2	SERIAL - E1	2048 Kbps	92,70%	32,70%	669,696
	TR-3	SERIAL - T1	1544 Kbps	85,50%	25,50%	393,72
					TOTAL MIGRADO	1589,752 Kbps
IÑAQUITO	TR-1	SERIAL - T1	1544 Kbps	66,23%	6,23%	96,1912
	TR-2	SERIAL - T1	1544 Kbps	71,90%	11,90%	183,736
					TOTAL MIGRADO	277,926 Kbps
				BORDER		
CAROLINA	BORDER C	ETHERNET	5120 Kbps	100% - 5120 Kbps	40%	
IÑAQUITO	BORDER I	ETHERNET	4096 Kbps	56% - 2300 Kbps	0%	

Cabe destacar que estas últimas millas aun mantienen esta ingeniería de red, esto por políticas de andinatel, ya que la migración se esta haciendo de poco en poco principalmente para las centrales más grandes de andinatel como son:

-Quito Centro

-Mariscal

-Iñaquito

2. Dejar ancho de banda libre, tanto en las interfaces de acceso existentes como en la nueva, ya que si es el caso de crecer en puertos que se encuentran anclados a estas centrales, vendrían a ser configurados en estas interfaces seriales.

En la tabla 5.3 se muestra el estado en el que quedarían estos circuitos de acceso, las celdas con borde grueso representan el nuevo circuito serial solicitado a andinadatos.

Tabla. 5.5 Enlaces de acceso post migración

NODO	ENLACE	TIPO	CAPACIDAD	% CANAL LIBRE	CONSUMO POST MIGRACION
				ACCESO	
CAROLINA	TR-1	SERIAL - E1	2048 Kbps	40,00%	60% - 1228,8 Kbps
	TR-2	SERIAL - E1	2048 Kbps	40,00%	60% - 1228,8 Kbps
	TR-3	SERIAL - T1	1544 Kbps	40,00%	60% - 926,4 Kbps
IÑAQUITO	TR-1	SERIAL - T1	1544 Kbps	40,00%	60% - 926,4 Kbps
	TR-2	SERIAL - T1	1544 Kbps	40,00%	60% - 926,4 Kbps
AEPROVI	MIGRACIONES	SERIAL - 2E1	4096 Kbps	55%	45,5% - 1867,678 Kbps

Por el lado de la red de border, seria necesario solicitar un aumento de ancho de banda para el enlace de salida, con el fin de contrarrestar el consumo que se a migrado al nuevo enlace de acceso, en este caso tentativamente el enlace de border aumentaría en 2 E1, como lo muestra la tabla 5.6.

Tabla. 5.6 Enlaces de border post migración

			BORDER		
NODO	ENLACE	TIPO	CAPACIDAD	% CANAL LIBRE	CONSUMO POST MIGRACION
AEPROVI	BORDER 1	ETHERNET	7168 Kbps	40%	60% - 3072 Kbps
AEPROVI	BORDER 2	ETHERNET	6144 Kbps	51%	49,3% - 2022 Kbps

5.5 Ingeniería futura

El planteamiento de la solución se hará de la manera mas objetiva, tomando en cuenta el análisis exhaustivo del resultado realizado en el apartado anterior.

En estos momentos la red de core, border y acceso, de los dos nodos, se encuentra sustentada sobre 2 ruteadores de gama media, por lo que la solución, en primera instancia seria lograr la migración de los enlaces a un nodo central, desde donde se pueda administrar la red en su totalidad.

El cambio en la topología de la red es un paso esencial para lograr un desempeño óptimo de la misma, sin embargo hay que tomar en cuenta, que este cambio de topología se halla supeditado a factores externos, que recaen en el echo de que Alianzanet necesita, por el momento, un proveedor de ultima milla y salida internacional.

Luego de un análisis exhaustivo, se llega al acuerdo de:

-Desaparecer por completo el nodo Iñaquito y conservar el nodo Carolina para los enlaces de acceso Seriales, el nodo carolina se convertiría en un nodo meramente de acceso. Adicionalmente a esto, se mantendría el servidor DNS configurado en este nodo.

-Contratar un espacio en el Data Center de la Aeprovi (Asociación de Proveedores de Internet), en el cual se colocará la nueva infraestructura de la red, este cumpliría las siguientes funciones:

1. Acceso para la troncal MPLS de Alianzanet
2. Border principal, configurando las dos salidas de Alianzanet en este nodo
3. Border secundario, contratando un enlace con un segundo proveedor de salida internacional, con el fin de utilizarlo como backup y para el balanceo de carga.

Luego de la Caracterización del tráfico realizada, es claro que existe gran cantidad de puertos y tráfico no identificado, recorriendo la red de border de Alianzanet, por lo que solución para solventar estos inconvenientes se basa en dos puntos fundamentales:

1. La colocación y configuración de un servidor basado en Linux, mismo que podrá ser usado para configurar dos servicios principalmente:
   - Firewall
   - Proxy – Cache transparente
2. La colocación y configuración del servidor de monitoreo, punto clave de este proyecto de tesis con los sistemas:
   - Nagios
   - Ntop
   - MRTG

Estos servidores estarían alojados en el nuevo nodo de la empresa en el *Data Center* de la AEPROVI.

En la figura 5.7 se muestra la solución final apegada al lo sugerido en este capítulo.

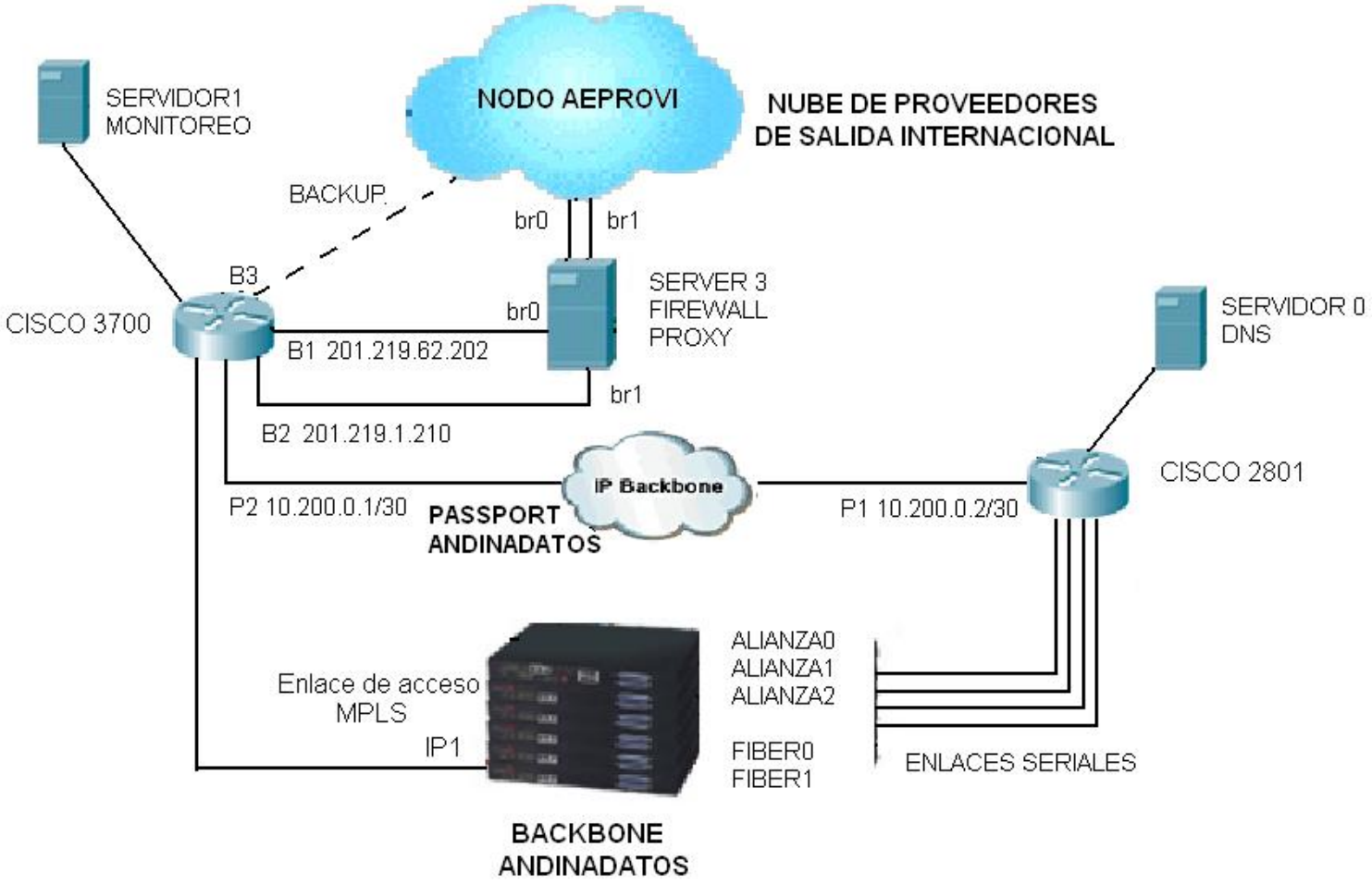


Figura. 5.6 Solución Final

Conclusiones y Recomendaciones

1. El monitoreo y planificación de redes WAN es una parte fundamental para la correcta administración de la red (Administración TI), esto se debe realizar de manera continua, oportuna y automática.

2. Las herramientas basadas en software libre ofrecen una amplia gama de aplicaciones en el sector de redes de comunicaciones, su desarrollo e implementación deben ser cada vez más frecuentes en nuestro país.

3. Una identificación adecuada y proactiva de las capacidades y debilidades de la red, faculta al administrador para tomar medidas preventivas y correctivas, ante posibles fallos de la misma, esta planificación y solución de los inconvenientes presentes y futuros se debe realizar sin escatimar costos de implementación.

Referencias Bibliográficas

Ali, M. Irfan, "Frame Relay in Public Networks" *IEEE Communications Magazine*, 1992.

Alles, Anthony, "ATM Internetworking" Cisco Systems Inc, 1995

Callon, R. et al. "A Framework for Multiprotocol Label Switching" IETF-MPLS, 1999.

Galstad, Ethan, "Nagios Version 3 Documentation", 2008.

Deri, Luca, "Effective Traffic Measurement Using ntop", Finsiel S.p.A., *IEEE Communications Magazine*, 2000.

Varios, "How Cisco IT Uses NetFlow to Improve Network Capacity Planning", *Cisco IT Case Study Network Capacity Planning*, 2007.

ANEXOS

A1. How Cisco IT Uses NetFlow to Improve Network Capacity Planning

A2. Effective Traffic Measurement Using ntop

A3. MPLS “Multiprotocol Label Switching”: Una Arquitectura de Backbone para la Internet del Siglo XXI

Fecha de Entrega: 26 de Octubre 2009

Sr. Jorge Alberto Tapia Cabrera
AUTOR

Ing. Gonzalo Olmedo, PhD.
COORDINADOR DE CARRERA