Instituto Tecnológico de Costa Rica

Escuela de Ingeniería en Electrónica

Red de Gestión Interna para equipos de la RAI, IMAP´s y Equipos conmutados por medio de ADSL para el Instituto Costarricense de Electricidad

Informe de Proyecto de Graduación para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura

Paolo Abarca Colato

Cartago, Enero 2009

INSTITUTO TECNOLOGICO DE COSTA RICA

ESCUELA DE INGENIERIA ELECTRONICA

PROYECTO DE GRADUACIÓN

TRIBUNAL EVALUADOR

Proyecto de Graduación defendido ante el presente Tribunal Evaluador como requisito para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura, del Instituto Tecnológico de Costa Rica.

Miembros del Tribunal

Ing. William Marín Moreno

Profesor asesor

Ing. Eduardo Interiano Salguero

Profesor lector

Los miembros de este Tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por la Escuela de Ingeniería Electrónica

Cartago, 27 de enero de 2009

Declaro que el presente Proyecto de Graduación ha sido realizado enteramente por mi persona, utilizando y aplicando literatura referente al tema e introduciendo conocimientos propios.

En los casos en que he utilizado bibliografía, he procedido a indicar las fuentes mediante las respectivas citas bibliográficas.

En consecuencia, asumo la responsabilidad total por el trabajo de graduación realizado y por el contenido del correspondiente informe final.

Cartago, 27 de enero de 2009

Paolo Abarca Colato

Cédula: 1 – 1179 - 0271

Resumen

En la actualidad, debido a los constantes avances tecnológicos, las empresas buscan la manera de mantenerse actualizadas para brindar un mejor servicio.

En el área de telecomunicaciones del ICE esto no es la excepción, ya que tiempo atrás, era necesario la presencia física de los técnicos en las diferentes centrales para solucionar los distintos problemas que surgían, pero esto ya es cosa del pasado dado que remotamente se pueden solucionar muchas de las averías que surgen.

Con todo cambio de tecnología, surgen nuevas formas de realizar las labores, sin embargo, muchas veces no se toma en cuenta factores que en un futuro pueden llegar a ocasionar algún tipo de problemática.

El Instituto Costarricense de Electricidad brinda a sus empleados la posibilidad de realizar algunas de sus tareas de manera remota, con lo cual se le facilita a cada uno de los técnicos que laboran turnos nocturnos un puerto de conexión, de ésta manera, ellos pueden trabajar desde sus hogares sin importar donde se presente la avería siempre y cuando cuenten con una conexión a internet, sin embargo, dependiendo del problema, se deben de trasladar al lugar de la avería.

A pesar de ser una buena opción para realizar las labores de manera más eficiente, también le está generando una seria problemática a la institución, ya que el ICE está dejando de recibir ingresos por cada uno de los puertos de conexión que se les asigna a los empleados.

El objetivo principal del proyecto es la eliminación de los puertos que utilizan en la actualidad los técnicos, esto con el fin de que la institución reciba ingresos por el alquiler de los mismos.

Para poder dar solución a esta problemática se implementará una red privada de gestión, con la cual se tendrá acceso a los distintos equipos que se utilizan para gestionar cuando ocurre una avería, así como también tendrá acceso a Internet para poder realizar consultas.

Palabras claves: tareas remotas, puerto de conexión, red privada de gestión, Internet.

Summary

At present, due to the constant technological advances, businesses seek ways to keep updated to provide better service.

In ICE`s telecommunications area this is not the exception, since long ago, it was necessary to the physical presence of technicians at the different plants to solve the various problems that arose, but this is already a thing of the past as it can be remotely solve many of the failures that arise.

With any change in technology, new ways of performing the work, however, often do not take into account factors in the future could lead to some kind of problem.

The Instituto Costarricense de Electricidad provides its employees the opportunity to perform some of their tasks remotely, so you get to each of the technicians who work night shifts a connection port, that way, they can work from their homes no matter where this is the fault long as they have with an internet connection, however, depending on the problem, we must move to the place.

Despite being a good option to make the work more efficiently, it also is creating a serious problem for the institution, since the ICE is failing to get paid for each port connecting to them to employees.

The project's main objective is the elimination of the ports used by the technicians at present, that in order for the institution receives income from the rental of its.

To be able to solve this problem will implement a private network management, with which it will have access to various computers used to manage when a fault occurs, and you will have access to the Internet to conduct consultations.

Keywords: remote tasks, connection port, private network management, Internet

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

Capítulo 1 : Introducción

1.1 Problema existente e importancia de su solución

Debido a los avances tecnológicos, en el área de Telecomunicaciones es posible solucionar algunos problemas de manera remota, tales como problemas de enrutamiento, interfaces apagadas, quejas de los clientes debido a que no pueden navegar algunos sitios, etc.

Para poder realizar dichas tareas remotamente, el Instituto Costarricense de Electricidad, más específicamente el área de Telecomunicaciones de la institución, le brinda a cada uno de los técnicos que realizan labores de guardia un puerto de conexión para su vivienda, los cuales debido al faltante actual existente, los puertos que se les brindó a los técnicos, están reduciendo el ingreso económico que podría estar recibiendo el ICE.

En la actualidad la institución está dejando de recibir ingresos de hasta $300144 anuales únicamente en el gran área metropolitana debido a los 148 técnicos que cuentan con un puerto de conexión comercial. Si se incluyen las localidades fuera de la gran área metropolitana los ingresos que se dejan de recibir aumentan de manera considerable.

Como se puede observar, las pérdidas que está ocasionando el uso de los puertos comerciales por parte de los técnicos es muy alta, de ahí la importancia de buscar una manera en que los técnicos sigan realizando sus labores remotas sin necesidad de utilizar los puertos comerciales y sin disminuir la calidad del servicio que ellos brindan.

1.2 Solución seleccionada

El principal objetivo que la empresa requiere para la solución del problema planteado anteriormente, es la eliminación total del uso de los puertos comerciales asignados a los técnicos.

La solución a esta problemática es crear una red dedicada a la gestión por medio remoto, de ésta manera se puede crear una red privada exclusiva para la utilización por parte de los técnicos. Con el diseño de una red de gestión privada, se puede eliminar el uso completo de los puertos comerciales por parte del personal técnico, de igual forma, podrán seguir realizando las labores en forma remota más eficazmente debido a que el nuevo enlace será exclusivo para tales tareas.

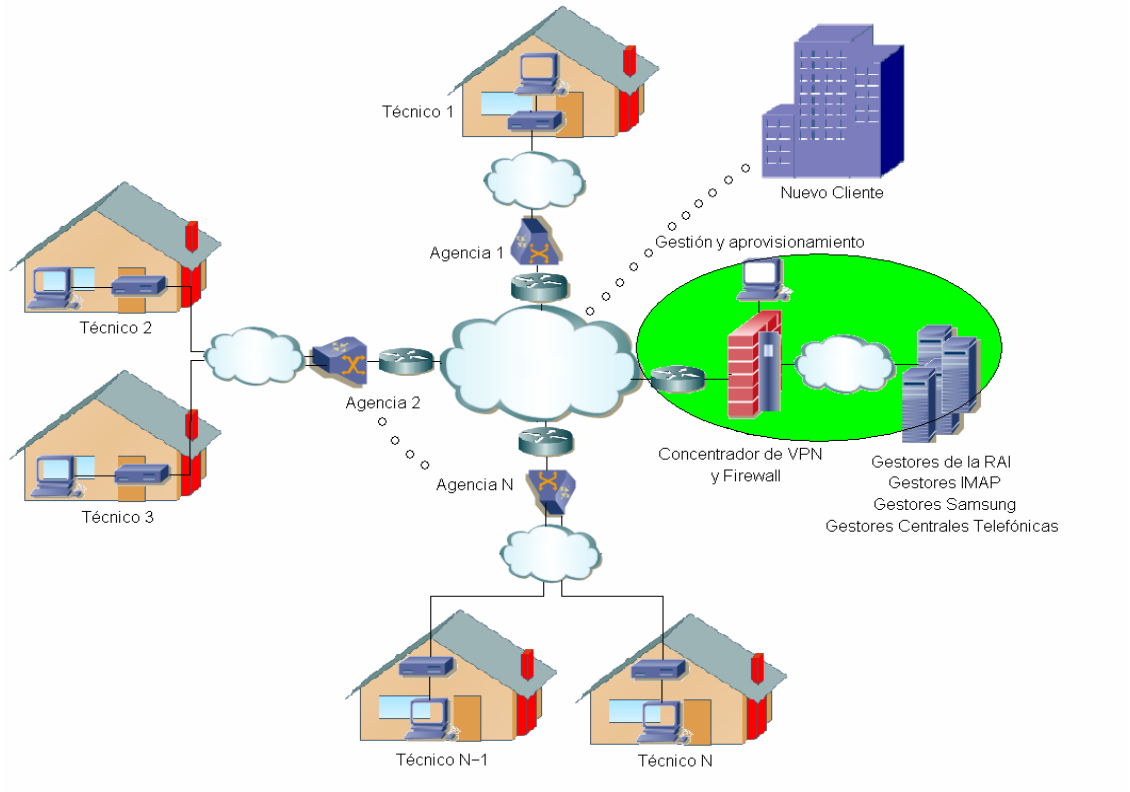


Figura 1.1 Diagrama de la red privada de gestión

La figura 1.1 muestra un esquema de la red privada de gestión, donde el óvalo verde indica la central de San Pedro en la que se implementará el equipo de gestión de la red, el cual tendrá control sobre el funcionamiento de los equipos localizados en las otras centrales. También en este mismo nodo, se encontrará el equipo firewall para darle seguridad a la red, aparte de los equipos necesarios a los que se debe de tener acceso para realizar las labores remotas.

Además, cada una de las centrales contará con un equipo DSLAM por el cual cada uno de los técnicos tendrá acceso a la red de gestión, de esta manera quedarán disponibles los puertos que en la actualidad utilizan y podrán ser comercializados.

La tabla 1.1 muestra las localidades en las que se implementará dicha solución., como primera central aparece San Pedro dado que es el centro de la red ya que es el punto de gestión de los demás nodos.

Tabla 1.1 Centrales de implementación de la red de gestión

	Central		**Central**
1	San Pedro	12	Oeste
2	Desamparados	13	Rincón Grande de Pavas
3	Aserrí	14	Curridabat
4	San Rafael Abajo Desamparados	15	Tres Ríos
5	San Antonio de Desamparados	16	Cartago
6	Coronado	17	Taras
7	El Alto de Guadalupe	18	Paraíso
8	Norte	19	Heredia
9	Sur	20	San Joaquín de Flores
10	Hatillo	21	Santo Domingo
11	Escazú	22	Alajuela

Capítulo 2 : Meta y objetivos

2.1 Meta

Eliminar el uso de todos los puertos comerciales utilizados por los técnicos en la gran área metropolitana para que la institución pueda recibir ingresos por su alquiler.

2.2 Objetivo General

Diseñar e implementar una red privada de gestión que permita la conectividad entre las distintas centrales de la Institución en la gran área metropolitana.

2.3 Objetivos específicos

- Diseñar la topología LAN para las centrales de la gran área metropolitana que se desean interconectar.
- Implementar la topología LAN en las centrales.
- Diseñar la topología WAN que permita conectar las distintas LAN.

Capítulo 3 : Marco teórico

3.1 Descripción del sistema o proceso a mejorar

En la actualidad, para que los técnicos puedan realizar las tareas remotas, deben de contar con un puerto de conexión comercial, debido a que necesitan acceso a la red mientras se encuentran en sus labores de guardia, ya que se encargan de verificar que los enlaces que tienen a su cargo se encuentren funcionando. En el momento en que ocurre alguna falla, se procede a la revisión para detectar el problema.

También es posible que algún cliente contacte al técnico y le reporte algún fallo en su conexión por medio de los reportes que se generan en el día, ya que muchas veces es necesario trasladarse hasta el lugar de la falla por lo que no todos los reportes pueden ser atendidos en el día y exista la necesidad de solucionarlos después desde el hogar, dado que dependiendo del problema que se presente, el mismo se pueda solucionar de manera remota. Siempre es necesario que el técnico cuente con conexión a la red para poder solucionar las averías reportadas remotamente.

3.2 Principios relacionados con la solución del problema

Conectividad [6]

Para que éste proyecto tenga validez, un punto muy importante es que exista conectividad entre los distintos nodos al punto principal en este caso la central de San Pedro. La conectividad se define como: “Capacidad de dos elementos hardware o software para trabajar conjuntamente y transmitirse datos e información en un entorno informático heterogéneo”. De acuerdo a la definición, si no existe pérdida de información en la conexión se obtiene la conectividad deseada, la cual es importante para la comunicación entre los equipos.

Red privada virtual (VPN) [7]

Una red privada virtual es: “Tecnología de redes que permite la extensión de una red de área local sobre una red pública o no controlada (como Internet). Por ejemplo, crear una red entre distintas computadoras utilizando como infraestructura a Internet. Evidentemente debe haber mecanismos de protección de los datos que se manejan”.

Las VPN permitirán la conexión entre las distintas centrales y la central de San Pedro. Se debe de realizar una VPN de capa 3 entre cada uno de los sitios y el punto central.

Equipo de Seguridad [8 - 9]

Para mantener la seguridad de la red se instalará un firewall el cuál se puede observar en la figura 3.1. Este dispositivo cumple la función de proteger la red contra intrusos, previniendo el acceso a usuarios no autorizados, así como evita el tráfico de información no autorizada. Además brindan protección segura contra ataques, hackers, virus, asegurando la integridad de los datos. Resumiendo, entre los principales beneficios que brindan estos equipos están:

- Protección de los servidores de la red de ataques de otros servidores en Internet.
- Administración de los accesos por medio de Internet a la red privada.
- Permite un punto de control de la seguridad.
- Brinda salida a Internet a los usuarios de la red privada.

Figura 3.1 Firewall

El dispositivo firewall a utilizar en la red tiene la opción de configurar el filtrado de contenido que se desee, permitiendo el paso o denegado el paso de la información dependiendo de cuál sea el caso.

Equipo de Gestión

Para llevar un control de lo que sucede en la red es necesario algún mecanismo desde el cual se pueda observar el comportamiento de la misma, para este fin se utiliza un servidor con un software de administración, el cual indica cuales puertos de los diferentes equipos DSLAM se encuentran encendidos y cuales apagados, además de poder observar el ancho de banda que maneja cada uno de ellos entre otras características.

Si por algún motivo ocurre una avería en alguno de los equipos administrados por el servidor, se puede detectar cuál puerto del equipo sufre la falla para poder corregirla, por lo que todos los equipos que tengan acceso al servidor pueden ser administrados desde el mismo.

Equipos DSLAM [10]

DSLAM son las siglas en inglés de Digital Subscriber Line Access Multiplexer (Multiplexor digital de acceso a la línea de abonado). Este dispositivo es un multiplexor localizado en la central telefónica que proporciona a los abonados acceso a los servicios DSL sobre cable de par trenzado de cobre, separando la voz y los datos de las líneas de abonado.

Estos equipos DSLAM trabajan bajo un nuevo protocolo de internet sobre ADSL basado en IP por lo que son llamados IP-DSLAM. La figura 3.2 muestra un IP-DSLAM. Este tipo de DSLAM ofrece una serie de ventajas sobre la tecnología tradicional basada en ATM ya que aumentan la eficiencia, la velocidad y mejora la gestión. Otras de las características que estos equipos poseen son la reducción de la complejidad de conversión de formato de datos, aparte de solucionar problemas de congestión de tráfico de alta velocidad y proporcionan un buen mecanismo para aplicaciones de video.

Figura 3.2 DSLAM-IP

La conexión en las centrales telefónicas del DSLAM se muestra en la figura 3.3, el repartidor principal representa la regleta que se utiliza para brindar conectividad entre el DSLAM y los usuarios, también se muestra la manera en la que el par telefónico de la central llega a cada uno de los usuarios, mostrando que en cada uno de los puntos de conexión debe de existir un splitter el cuál se encargará de dividir la señal para el teléfono y de la del CPE.

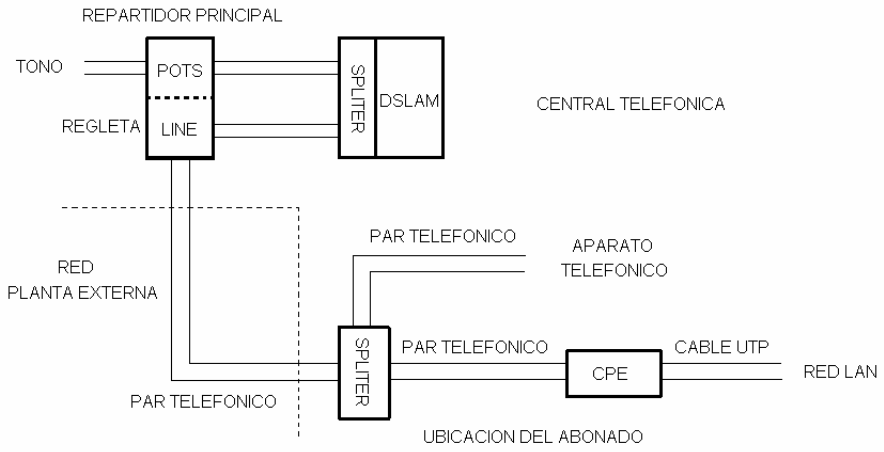


Figura 3.3 Diagrama de conexión del DSLAM en la central telefónica

Equipos de conmutación y enrutamiento

La conmutación de la red está dada por un switch, estos dispositivos operan en la capa de enlace de datos del modelo OSI. La función principal de este elemento es la de tomar decisiones inteligentes sobre si pasar señales al siguiente segmento de la red o no.

Los switches aprenden las direcciones MAC para realizar la comunicación, de ésta manera construyen tablas de envío y determinan el destino de los datos que envían, además permiten que muchos usuarios se comuniquen en paralelo mediante la utilización de circuitos virtuales y segmentos de red dedicados en un entorno virtual libre de colisiones, lo que permite un máximo ancho de banda disponible en un medio compartido.

El enrutamiento en la red la realizan los enrutadores los cuales operan en la capa 3 del modelo OSI, tomando decisiones basadas en direcciones de red (direcciones IP) utilizando una o más métricas. Los enrutadores envían paquetes desde una red a otra basándose en la información de la capa de red, construyen tablas de enrutamiento e intercambian información de la red con otros enrutadores. Las funciones principales son:

- Seleccionar las mejores rutas para los paquetes entrantes.

- La conmutación de paquetes a la interfaz saliente correcta.

Equipos de usuario final

En este caso los equipos de usuario final son el CPE (customer premises equipment) o equipo local del cliente y la computadora. La figura 3.4 muestra un CPE, el cual es utilizado para encaminar o terminar una comunicación. Como se señaló en la figura 3.3, una de las salidas del splitter se conecta al CPE, la que permite la conexión de la computadora a la red.

El CPE posee dos direcciones IP para poder funcionar de manera adecuada, una de ellas es una dirección WAN, la que permite la conectividad al equipo que se encuentra en la central telefónica y la dirección LAN, la cual generalmente es asignada por DHCP. La conexión de la computadora al CPE puede darse por medio de una interfaz Ethernet o por medio inalámbrico.

Figura 3.4 CPE

Capítulo 4 : Procedimiento metodológico

4.1 Obtención y análisis de información

Una vez que se aclaró el problema por el cual está pasando la institución, se procede a analizar el estado en el cuál se encuentra para posteriormente darle solución.

En los últimos tiempos, ha existido una alta demanda para la obtención del servicio de Internet ADSL por parte del ICE, cabe destacar que el incremento de esta demanda no se debe únicamente a personas o instituciones ajenas al ICE que buscan obtener éste servicio, sino que también debido a las facilidades que brinda en la actualidad una conexión a Internet, muchas personas pueden realizar sus labores desde el hogar, sin ser la excepción las personas que brindan turnos de guardia en el ICE.

Debido a éste motivo, los trabajadores en el ICE han adquirido éste servicio para poder realizar sus labores de guardia sin ningún problema, situación que ha provocado la disminución de la cantidad de puertos que la institución puede comercializar, ya que no se puede dejar a un empleado sin el uso de este puerto debido a que no se le sería posible realizar sus labores desde el hogar.

4.2 Evaluación de las alternativas y síntesis de una solución

Por el tipo de proyecto a realizar, las alternativas que se presentaron para la solución del problema son muy similares. Para iniciar el planteo de la posible solución, se realizaron consultas y entrevistas a distintas personas que laboran en este medio y de acuerdo a sus opiniones se coincidía en que la mejor solución es la implementación de una red de gestión privada.

La única diferencia entre las distintas soluciones consistía en la manera de realizar el direccionamiento de la red, ya que de acuerdo a la información recopilada se obtuvo tres maneras distintas de realizarlo, por lo que se estudiaron las diferentes alternativas y se decidió realizar pruebas de acuerdo al funcionamiento del equipo para descartar las distintas opciones que se manejan.

De acuerdo a los resultados obtenidos en estas pruebas se selecciona la manera con la que se atacará el problema para darle solución.

4.3 Implementación de la solución

Una vez que se encuentra clara la problemática por la que está pasando la institución, el primer punto que se debe de definir para iniciar con la implementación de la solución es el direccionamiento que se va a utilizar.

Como ya se mencionó con anterioridad, éste es uno de los puntos más delicados para el diseño de la solución debido a que se debe de tomar en cuenta la funcionalidad de los equipos a utilizar, por lo que el direccionamiento sufrió una evolución ya que pasó por las tres etapas mencionadas anteriormente debido a la funcionalidad del equipo y más importante aún, debido a las necesidades de la empresa.

Para diseñar el direccionamiento de la topología a utilizar, se debe de conocer cuántas centrales van a estar conformando la red, aparte de esa información, se debe de conocer cuántos equipos van a estar conectados en cada una de las centrales.

Con el direccionamiento asignado, se procede a realizar la configuración de los equipos, la cual puede realizarse en la central de San Pedro y una vez que se cuenta con el equipo configurado, inicia la implementación de los mismos en las distintas centrales. En cada una de las centrales, se debe de buscar la posición que le fue asignada al equipo.

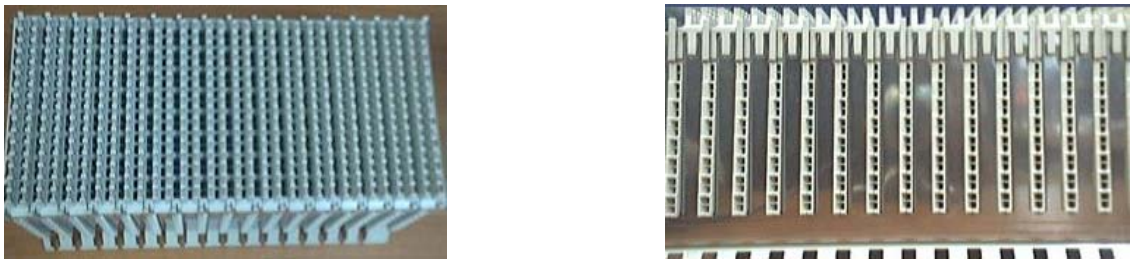
Cada una de las centrales a excepción de San Pedro contará con un equipo DSLAM conectado a un switch, en este caso perteneciente a los equipos de la Red Avanzada de Internet más conocido como la RAI, el cual a su vez se encuentra directamente conectado a la nube de la RAI, topología que permite la conectividad entre las diferentes localidades, además es necesaria la implementación de una VPN de capa 3 entre los equipos de la RAI en cada uno de los nodos y San Pedro para que exista conectividad entre ellos debido a que el tráfico fluye por internet en una red privada.

En San Pedro se va a contar con un equipo firewall el cuál aparte de brindar seguridad y filtrado de contenido, también será el encargado de permitir a los técnicos salir a Internet.

También en cada uno de los demás sitios se va a contar con una regleta para realizar la conexión entre el equipo DSLAM y la central, después se debe de realizar un pase para tener conexión con los clientes, en este caso los técnicos.

Cuando el equipo DSLAM se encuentre ubicado en la posición asignada, se debe de realizar el cableado del equipo, dependiendo de la central en la que se encuentre, será necesaria la implementación de uno o dos cables UTP para realizar la conexión entre este equipo y el switch de la RAI. Aparte del cable UTP, se debe de cablear el DSLAM a la regleta localizada en el distribuidor principal como se explicó anteriormente.

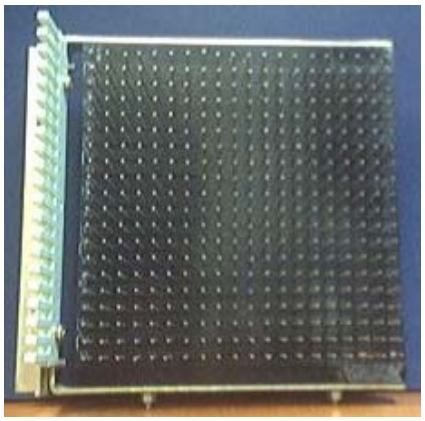
En este punto ocurrió un problema debido a que el tipo de regleta que se iba a utilizar en un inicio tuvo que sustituirse por otro tipo, lo anterior debido a que en un futuro el primer tipo de regleta podría generar averías por la forma en la que se cablea. La figura 4.1 muestra este tipo de regleta, la figura 4.1 (a) muestra una vista superior mientras que la (b) una vista lateral. Esta regleta permite su conectividad a presión, método que no es muy seguro para este tipo de conexión ya que por quedar el cableado por fuera y ser a presión, mientras se está realizando algún trabajo cabe la posibilidad de desconectar un cable sin darse cuenta lo que generaría averías en la red.



(a) (b)

Figura 4.1 Primer regleta a utilizar

Para evitar problemas por este tipo de conexión, se sustituyó esa regleta por otra, la cual utiliza el método de enrollar el cable. La figura 4.2 muestra este otro tipo de regletas. Como en este caso el cable se enrolla se evita averías por falsos contactos o porque el cable se suelte después del transcurso del tiempo, así como también es más difícil que por un error se jale el cable se desprenda como puede ocurrir con la primer regleta.



(a)

(b)

Figura 4.2 Regleta para enrollar

La figura 4.3 indica la manera en la que se debe de enrollar el cable a la regleta, dicha figura muestra la posición por colores de los cables en la regleta de manera abreviada por lo que en la tabla 4.1 se indican dichas abreviaturas. La mitad de los pares de uno de los cables corresponden a las filas 0 y 1, mientras que la otra mitad la conforman las filas 10 y 11. Como se puede observar, existen otros dos pares de filas, lo que corresponde a otro cable, ya que en algunas centrales se necesita conectar dos cables a la regleta.

	A	B	C	D	E	F	G	H	J	K	L	M	N	P	R	S	T	U	V	W
0	AZ	BC AZ	NA	BC NA	VE	BC VE	MA	BC MA	GR	BC GR	AZ	R AZ	NA	R NA	VE	R VE	MA	R MA	GR	R GR
1	AZ	NE AZ	NA	NE NA	VE	NE VE														
2																				
3	AZ	BC AZ	NA	BC NA	VE	BC VE	MA	BC MA	GR	BC GR	AZ	R AZ	NA	R NA	VE	R VE	MA	R MA	GR	R GR
4	AZ	NE AZ	NA	NE NA	VE	NE VE														
5																				
6																				
7																				
8																				
9																				
10	MA	NE MA	GR	NE GR	AZ	AM AZ	NA	AM NA	VE	AM VE	MA	AM MA	GR	AM GR	AZ	VL AZ	NA	VL NA	VE	VL VE
11	MA	VL MA	GR	VL GR																
12																				
13	MA	NE MA	GR	NE GR	AZ	AM AZ	NA	AM NA	VE	AM VE	MA	AM MA	GR	AM GR	AZ	VL AZ	NA	VL NA	VE	VL VE
14	MA	VL MA	GR	VL GR																
15																				
16																				
17																				
18																				
19																				

Figura 4.3 Código de colores del alambrado del equipo a la regleta

La figura 4.4 muestra como queda ubicado los pares del cable del DSLAM, ya que la mitad van a la parte de la central y la otra mitad hacia los usuarios. Los PE indican los puertos de entrada de la central telefónica (POT), mientras que los PT indican los puertos terminales los cuales se conectan al DSLAM (LINE).

	A	B	C	D	E	F	G	H	J	K	L	M	N	P	R	S	T	U	V	W
0	PE1		PE2		PE3		PE4		PE5		PE6		PE7		PE8		PE9		PE10	
1	PE 11		PE12		13															
2																				
3	PE 1		PE 2		PE 3		PE 4		PE 5		PE 6		PE 7		PE 8		PE 9		PE 10	
4	PE 11		PE 12		13															
5																				
6																				
7																				
8																				
9																				
10	PT 1		PT 2		PT 3		PT 4		PT 5		PT 6		PT 7		PT 8		PT 9		PT 10	
11	PT 11		PT 12																	
12																				
13	PT1		PT2		PT3		PT4		PT5		PT6		PT7		PT8		PT9		PT10	
14	PT11		PT12																	
15																				
16																				
17																				
18																				
19																				

Figura 4.4 Distribución de los puertos a la central y al equipo

Tabla 4.1 Abreviaturas utilizadas en la figura 4.5

AZ	Azul	NE AZ	Negro – Azul
BC AZ	Blanco - Azul	NE NA	Negro – Naranja
NA	Naranja	NE VE	Negro – Verde
BC NA	Blanco - Naranja	NE MA	Negro – Marrón
VE	Verde	NE GR	Negro – Gris
BC VE	Blanco - Verde	AM AZ	Amarillo – Azul
MA	Marrón	AM NA	Amarillo – Naranja
BC MA	Blanco - Marrón	AM VE	Amarillo – Verde
GR	Gris	AM MA	Amarillo – Marrón
BC GR	Blanco - Gris	AM GR	Amarillo – Gris
R AZ	Rojo - Azul	VL AZ	Violeta – Azul
R NA	Rojo - Naranja	VL NA	Violeta – Naranja
R VE	Rojo - Verde	VL VE	Violeta – Verde
R MA	Rojo - Marrón	VL MA	Violeta – Marrón
R GR	Rojo - Gris	VL GR	Violeta - Gris

A continuación se debe de realizar la VPN de capa 3 comentada anteriormente, esto con el fin de que exista conectividad entre la central en la que se encuentre y la central de San Pedro.

Una vez que todo el equipo se encuentre cableado, se realizarán las pruebas de funcionamiento por medio del protocolo ICMP, las cuales indicarán si la implementación de los sitios se realizó de manera correcta.

4.4 Reevaluación y rediseño

El diseño de la red de gestión privada tiene una cualidad muy relevante, la cuál es la escalabilidad que posee. Esta característica es muy importante debido a la rapidez con la que en la actualidad crecen las redes de gestión de este tipo, ya que facilita las tareas que se deben de realizar y aumentan la eficiencia con la que se solucionan las averías.

Como la red posee esta habilidad, si se desea en un futuro agregar más equipo, se puede realizar de forma sencilla ya que se cuenta con direcciones disponibles para hacerlo.

Aparte de la posibilidad de expansión en las centrales instaladas, también la red puede crecer hacia otras centrales, lo anterior se puede realizar por medio de VPNs de capa 3 que brindan conectividad a otras localidades y se cuentan con subredes para realizar el direccionamiento.

Capítulo 5 : Descripción detallada de la solución

5.1 Análisis de soluciones y selección final

Como ya se había mencionado, por la naturaleza de este tipo de proyecto, las soluciones son muy similares entre sí, la gran diferencia entre ellas la marca el direccionamiento a utilizar, por lo que se tienen las siguientes posibles soluciones:

1) Tener todos los equipos en una sola red, lo cual formaría una MAN.

2) Implementar los equipos DSLAM en una red y los CPE en otra red distinta por sitio.

3) Cada una de las centrales tendrá una subred para el DSLAM y los CPEs.

En la primera opción, tanto los equipos DSLAM, los CPEs y las interfaces de los switches y enrutadores a utilizar de todas las centrales se encontraría en una misma red. Esta opción de direccionamiento no es factible debido a que no es posible realizar las VPNs de capa 3 que se utilizan para interconectar las diferentes centrales con la de San Pedro, lo anterior se debe a que como las interfaces de los enrutadores se encuentran en la misma red, ocurre un traslape en cuanto al direccionamiento por lo que el enrutador no sabe cómo realizar el enrutamiento.

Para la segunda posible solución se desea implementar dos redes distintas en cada sitio, una que abarque a los equipos DSLAM y los puertos de los switches y de los routers y otra que abarque a los CPEs, de esta forma se soluciona el problema mencionado anteriormente con respecto a la implementación de las VPN de capa 3, ya que cada sitio al tener una red distinta no existirá ningún traslape, así el enrutamiento se puede llevar a cabo sin ningún problema.

Ahora surge un nuevo problema el cual se debe a la implementación de una red para el equipo DSLAM y las diferentes interfaces de los switches y enrutadores y otra red para los CPEs. Esta problemática se da debido a que los DSLAM y los CPE no son equipos capaces de enrutar por lo que no es posible pasar de una red a otra, con lo que no es posible establecer comunicación entre estos equipos.

Para la tercera y última posible solución se han tomado en cuenta los distintos problemas que se han presentado en las dos soluciones anteriores. Para esta solución, se implementará una red distinta en cada una de las centrales y en los casos en los que se encuentran dos tarjetas instaladas en el DSLAM, cada una tendrá una red diferente, de esta manera se mantiene el funcionamiento de las VPN de capa 3 necesarias para la conectividad entre las centrales, además con todos los equipos dentro de la misma red la conectividad entre los mismos se soluciona, el cual era un problema que se presentaba en las dos soluciones anteriores.

De esta manera, los dos problemas que se habían presentado anteriormente cuentan con una solución, por lo tanto, esta última opción es la seleccionada.

5.2 Descripción del software

Diseño de la topología LAN y WAN

El primer punto a conocer para poder diseñar el direccionamiento de la topología LAN y WAN a utilizar es conocer cuántas centrales van a estar conformando la red, aparte de esa información, se debe de conocer cuántos equipos van a estar conectados en cada una de las centrales.

Una vez teniendo claro estas necesidades, se procede a realizar el direccionamiento. Se utilizará una red con máscara 255.255.255.0 por cada una de las centrales, esto con el propósito de contar con direcciones ip de reserva para una posible expansión ya que se cuenta con 254 direcciones utilizables las cuales no se utilizarán por completo. La tabla 5.1 muestra un ejemplo del direccionamiento utilizado. La primera dirección utilizable de cada una de las redes será asignada para el direccionamiento WAN, mientras que las demás serán utilizadas para la LAN.

Tabla 5.1 Redes utilizadas en las centrales

Central	Red utilizada
San Pedro	192.170.1.0
Desamparados	192.170.2.0
San Gabriel	192.170.3.0
Aserrí	192.170.4.0
San Rafael Abajo Desamparados	192.170.5.0
Higuito	192.170.6.0
San Antonio de Desamparados	192.170.7.0
Coronado	192.170.8.0
El Alto de Guadalupe	192.170.9.0
Norte	192.170.10.0
Sur	192.170.11.0
Hatillo	192.170.12.0
Escazú	192.170.13.0
Oeste	192.170.14.0
Rincón Grande de Pavas	192.170.15.0
Curridabat	192.170.16.0
Tres Ríos	192.170.17.0
Cartago	192.170.18.0
Taras	192.170.19.0
Heredia	192.170.20.0
Santo Domingo	192.170.21.0
Alajuela	192.170.22.0

La figura 5.1 indica el esquema de cómo será la implementación entre cada una de las centrales y la central principal, en este caso San Pedro. Como ya fue mencionado, la primera dirección ip utilizable será asignada para el diseño de la WAN la cuál será programada en el enrutador de cada una de las centrales y la segunda dirección utilizable se utilizará en el DSLAM, lo que permitirá mayor orden en la topología.

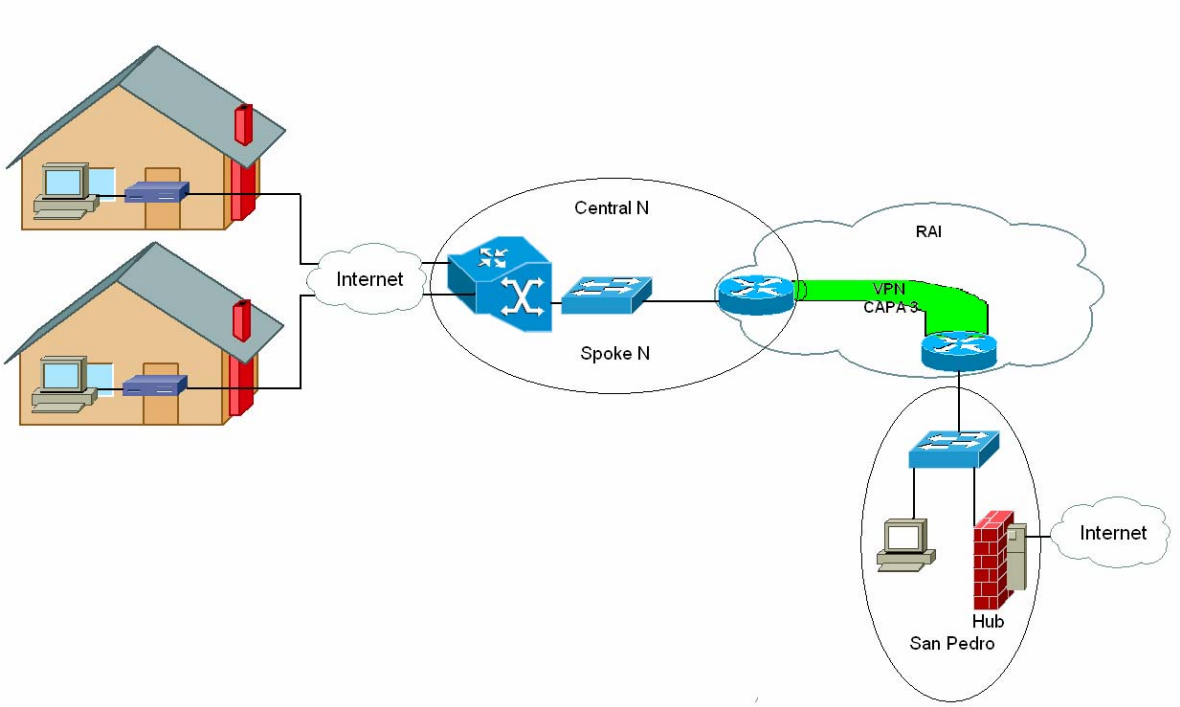


Figura 5.1 Diagrama de conexión entre una central y la central de San Pedro

También como se puede observar en la figura 5.1, cada una de las centrales contará con un equipo DSLAM conectado a un switch que se encuentra configurado como acceso, este dispositivo pertenece a los equipos de la Red Avanzada de Internet más conocido como la RAI, el cual a su vez se encuentra directamente conectado a la nube de la RAI, topología que permite la conectividad entre las diferentes localidades.

La figura 5.1 también muestra la necesidad de la implementación de una VPN de capa 3 entre cada uno de los nodos y San Pedro para que exista conectividad entre cada uno de ellos, debido a que el tráfico fluye por internet en una red privada, lo cual da paso al desarrollo de la WAN con el direccionamiento ya mencionado.

En San Pedro se va a contar con un equipo Firewall el cuál aparte de brindar seguridad y filtrado de contenido, también será el encargado de permitir a los técnicos salir a Internet.

Configuración de las VPN [3 - 5]

Para la implementación de la WAN es necesaria la elaboración de las VPN de capa 3. Para la realización de las VPN se utiliza un software de Cisco llamado IPS Center. La creación de las VPNs de capa 3 son necesarias para permitir la conectividad entre los distintos puntos, ya que por ser una red privada que viaja por la Internet no se pueden ver los equipos localizados en una central con respecto a otra. La figura 5.2 muestra la interfaz principal de este software.

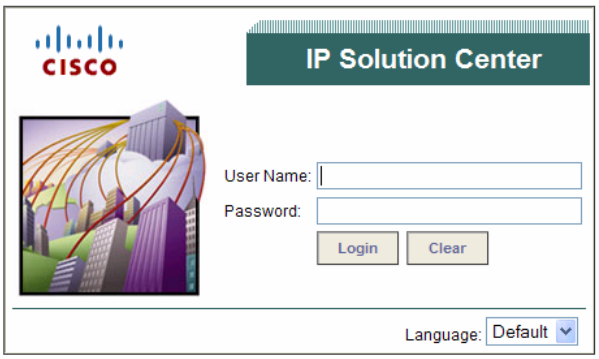


Figura 5.2 Interfaz de ingreso al IP Solution Center

En esta pantalla debe de ingresar el usuario y la contraseña para poder ingresar al software, el cual tiene una licencia. Una vez que se ingresa, se da inicio a la configuración de la VPN.

La figura 5.3 muestra la pantalla de inicio de configuración de la VPN, el primer paso para comenzar con la configuración de la VPN es seleccionar el sitio principal, el cuál va a ser llamado “Hub” y todos los sitios que se interconecten a éste serán llamados “Spokes”. También se debe de seleccionar la interface del router a la que se encuentra conectado el equipo de la central y agregarle una descripción a la VPN para poderla identificar posteriormente si se desea hacer algún cambio.

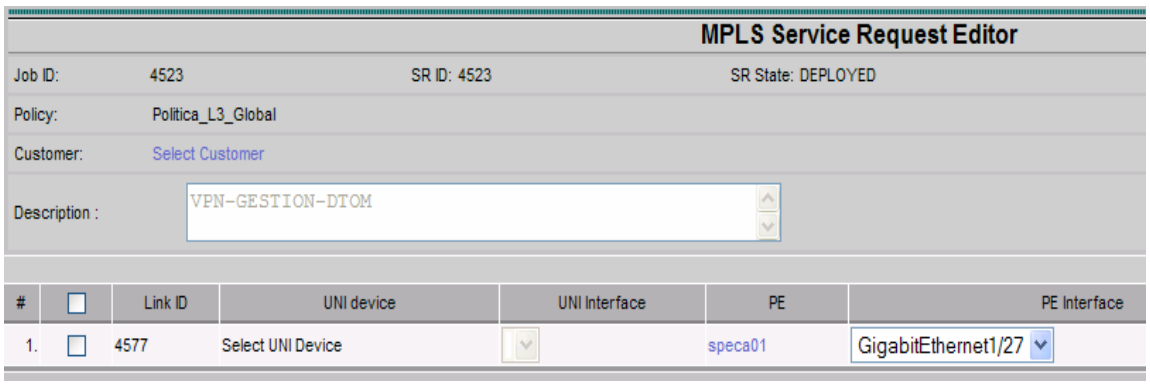


Figura 5.3 Interfaz de selección del puerto del enrutador.

La figura 5.4 muestra el siguiente paso para la creación de la VPN el cual es seleccionar la sub-interface del router Spoke a la que está conectado el equipo. También se le puede agregar una descripción a la interface para identificar la función que desempeña, se debe de seleccionar el tipo de encapsulación a utilizar, la cual para efectos nuestros es la DOT1Q que es un estándar de la IEEE soportado por los equipos Cisco, además es recomendada por Cisco cuando se trabaja con VLANs. Por último se debe de colocar un identificador de la VLAN.

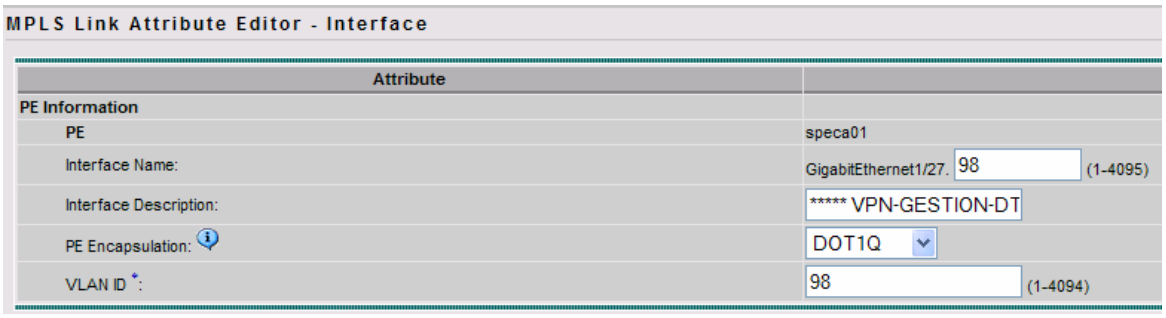


Figura 5.4 Interfaz de configuración del puerto del enrutador.

La figura 5.5 muestra la selección el esquema IP a utilizar, en este caso se trabaja con IP versión 4. Después se debe de configurar la dirección IP y la máscara de red que tendrá la sub-interface. Este direccionamiento es el diseñado para la WAN de la topología.

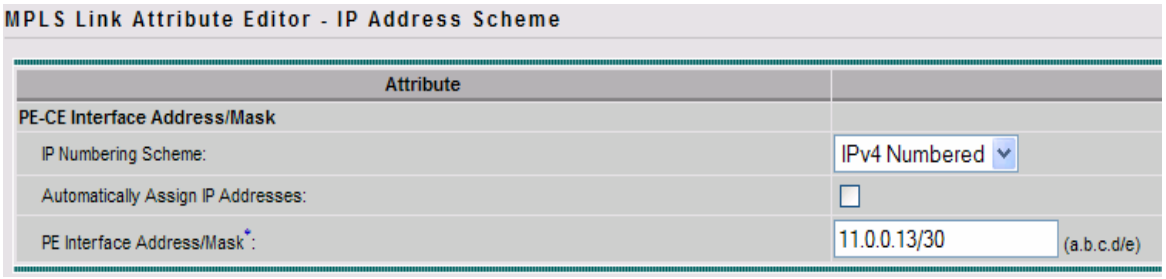


Figura 5.5 Interfaz de configuración del direccionamiento

El siguiente paso se puede observar en la figura 5.6. En este punto se da la creación de la VPN, en la pantalla se muestra el nombre que se le dio a la VPN para realizar la confirmación de la misma antes de su creación, así como también se indica si fue configurada como Hub o como Spoke.

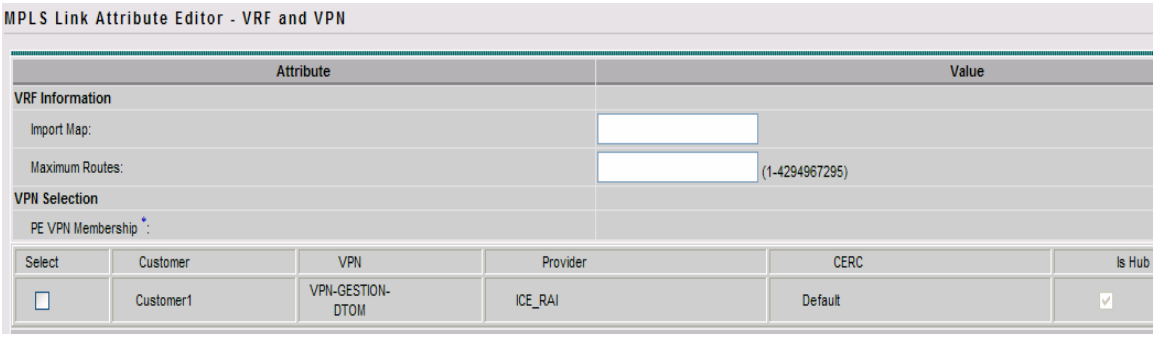


Figura 5.6 Interfaz de creación de la VPN

De esta manera la VPN ya está configurada, la información que se despliega al final de su configuración se muestra en la figura 5.7, la cual confirma la información que se estuvo configurando en los pasos anteriores, es un resumen de la configuración del enlace.

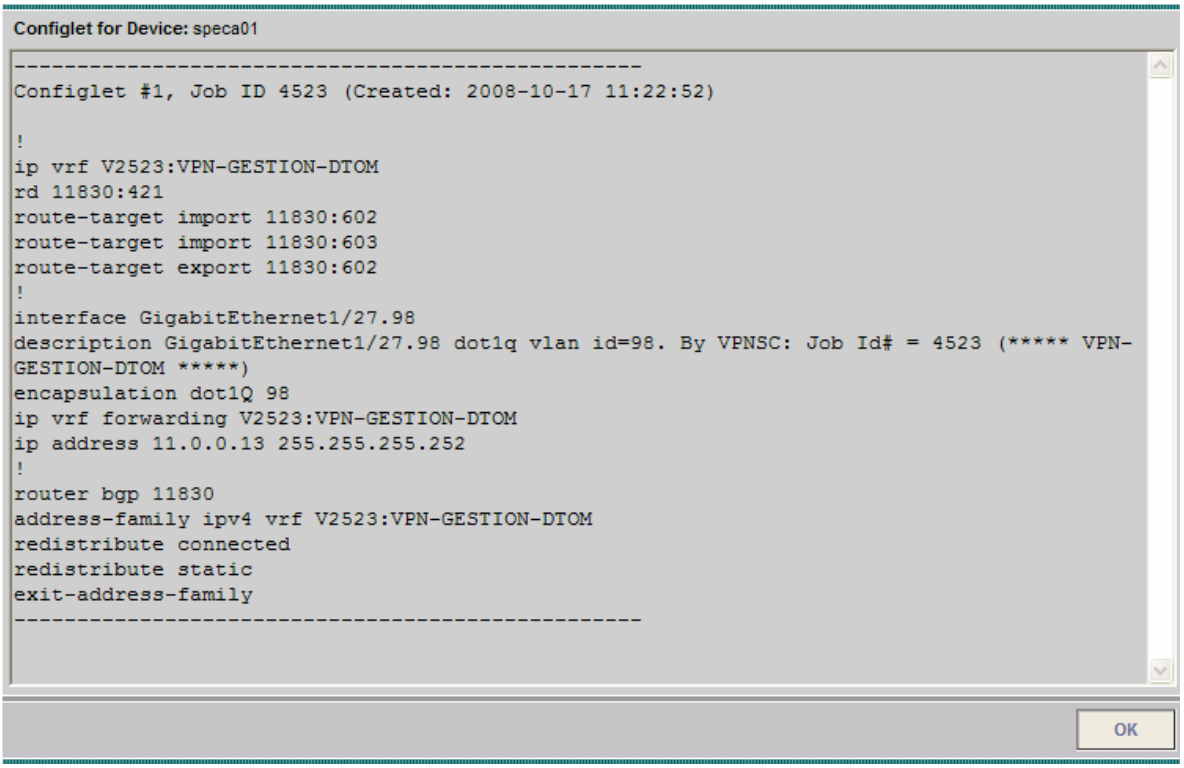


Figura 5.7 Interfaz de confirmación de los parámetros configurados

Las VPN creadas utilizan el protocolo MPLS (Multiprotocol Label Switching *o* Conmutación Multi-Protocolar mediante Etiquetas) el cual es un mecanismo de transporte de datos estándar creado por la IETF (Internet Engineering Task Force, o Grupo de Trabajo en Ingeniería de Internet) y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP. Funciona anexando un encabezado a cada paquete el cual contiene una o más etiquetas, al conjunto de etiquetas se le llama pila.

Capítulo 6 : Análisis de Resultados

6.1 Resultados

Antes de iniciar con el desarrollo del proyecto no existía ningún tipo de conexión entre los diferentes equipos a utilizar en las centrales. La figura 6.1 muestra el cambio producido en la medición realizada en un inicio. Como se puede observar, la disponibilidad de la red es de un 0%, con lo que no es posible establecer conexión entre los equipos, luego pasa a un 100% con lo que existe conectividad.

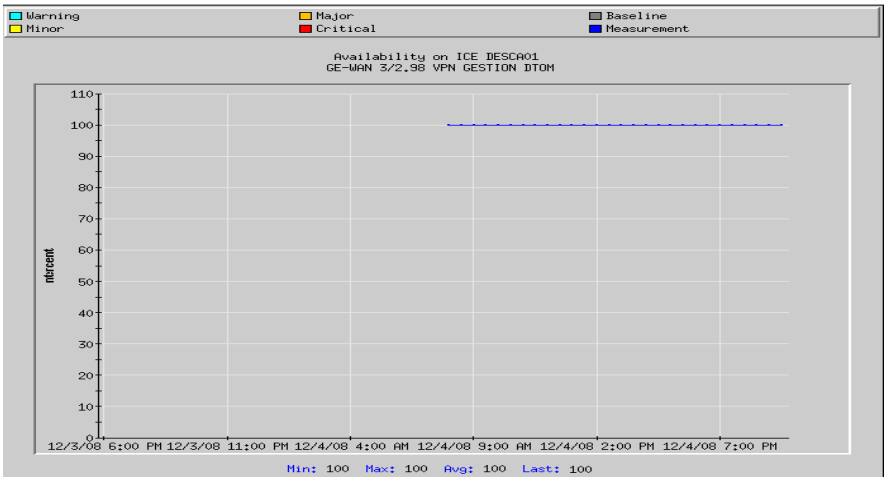


Figura 6.1 Cambio de estado con la implementación de la red

Una vez que se realizó la implementación de los equipos en las distintas centrales y fueron creadas las VPNs para permitir la conectividad entre los distintos puntos fue posible establecer la conectividad entre ellos. La figura 6.2 muestra la disponibilidad de la conexión del firewall localizado en San Pedro en la red de gestión privada. Esta gráfica muestra en tiempo real lo que sucedió durante las pruebas mientras se generaba tráfico, la figura 6.3 también muestra la disponibilidad del mismo enlace, sin embargo, el tiempo de muestreo es mayor, ya que se realizó la medición del enlace desde que se produjo tráfico hasta el día siguiente, el cuál a pesar de no generar tráfico durante esas horas, sigue disponible en un 100%.

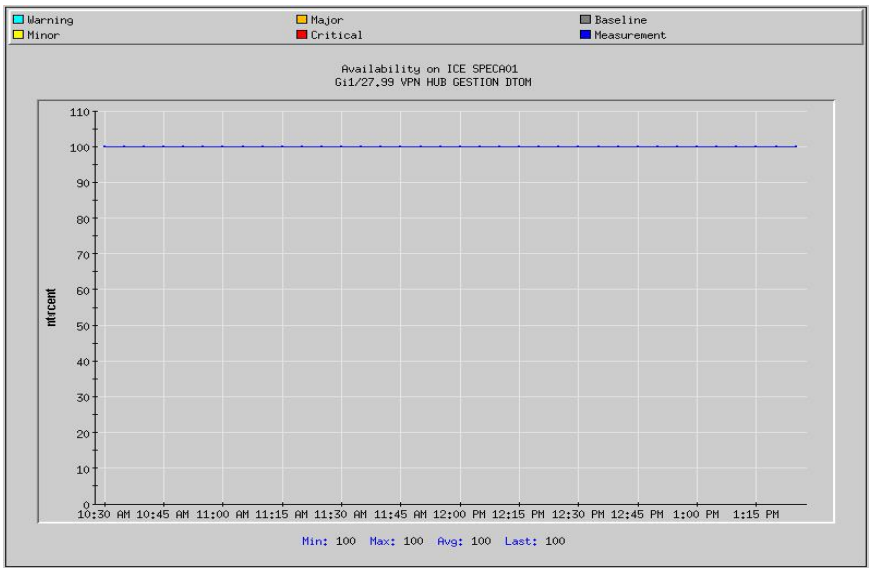


Figura 6.2 Disponibilidad de la conexión del Firewall

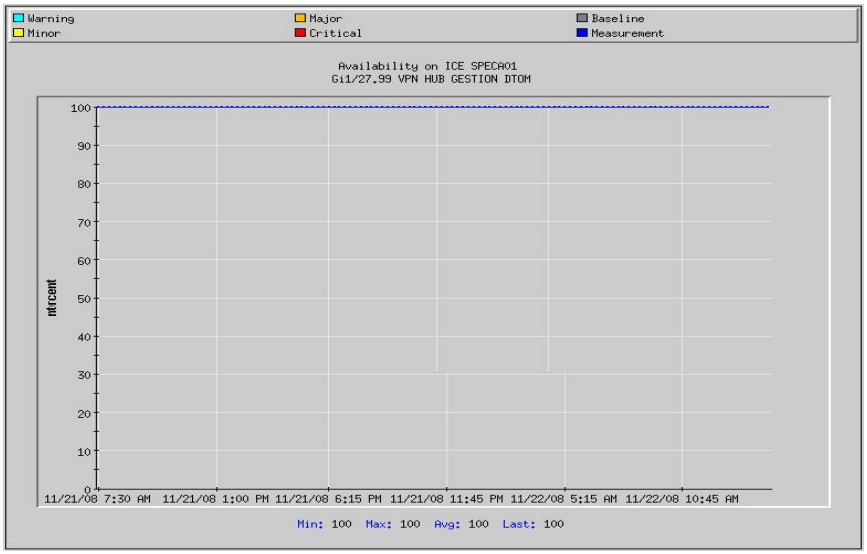


Figura 6.3 Disponibilidad de la conexión del Firewall

Durante las pruebas se generaba un bit rate de entrada y de salida en cada uno de los dispositivos, por lo que en el caso del firewall dichas mediciones se muestran en las figuras 6.4 y 6.5 respectivamente. El bit rate de entrada corresponde a la información que recibe el dispositivo por el enlace, mientras que el bit rate de salida corresponde a la información que el dispositivo envía por el mismo enlace. Como se puede observar, la gráfica del bit rate de salida posee una serie de transferencias de información antes del pico máximo, lo que se debe a que como el firewall es el encargado de proveer salida a internet a los dispositivos, dependiendo de la cantidad de personas que están tratando de acceder a internet y de las tareas realizadas se presentará una salida de información por parte del firewall, lo que indica que en esos momentos, el firewall estuvo distribuyendo información.

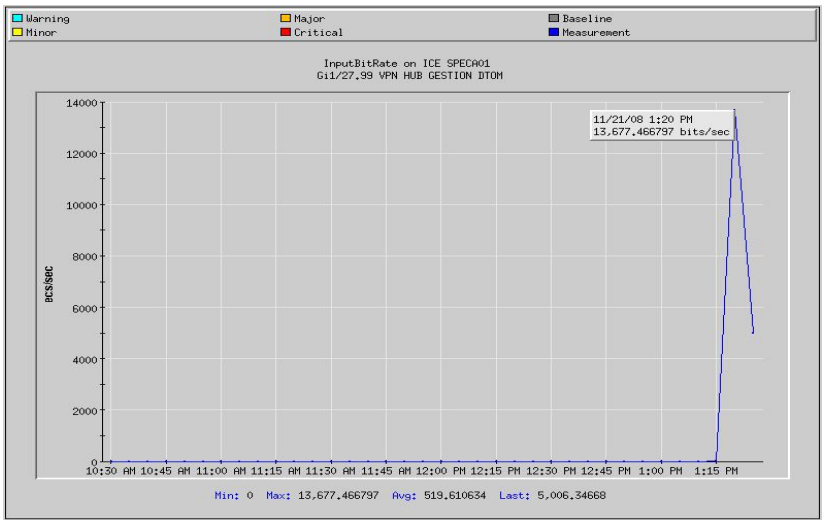


Figura 6.4 Bit rate de entrada de la conexión del Firewall

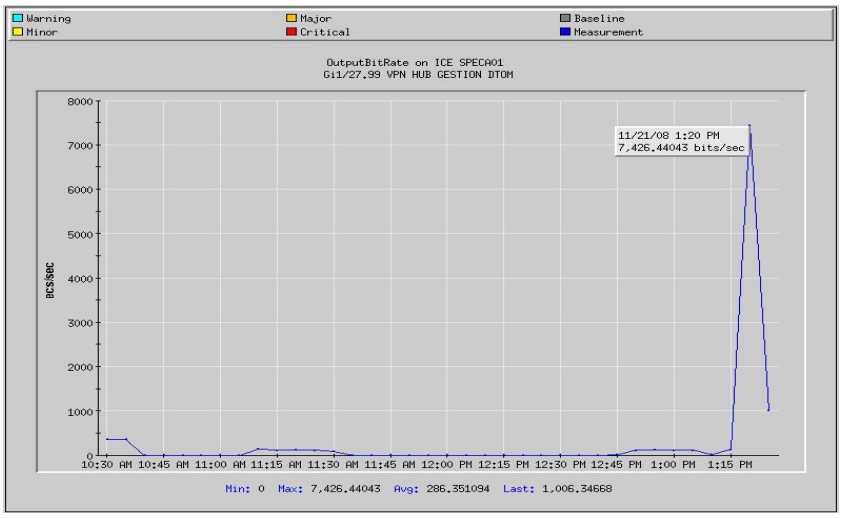


Figura 6.5 Bit rate de salida de la conexión del Firewall

El FireHunter es capaz de realizar una sola gráfica en la que se muestra ambos bit rate sumados, dicha medición puede observarse en la figura 6.6. Esta gráfica es útil para resumir en un solo diagrama la cantidad de información que está pasando por un enlace.

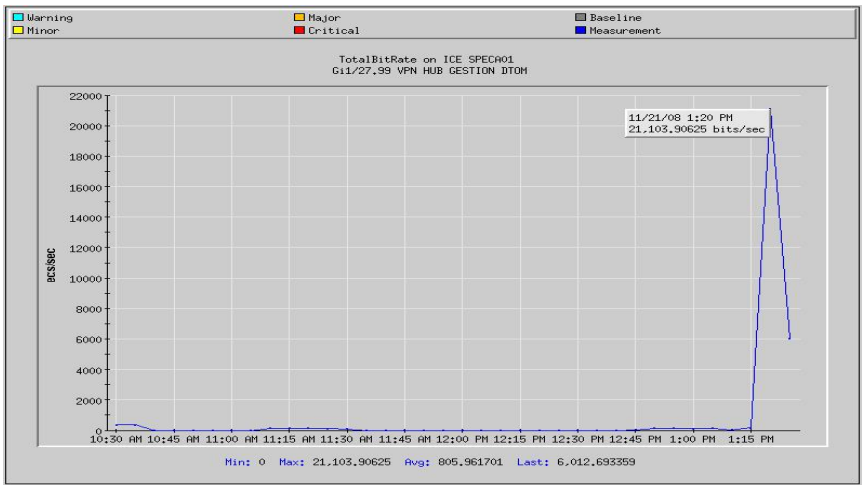


Figura 6.6 Total de bit rate de la conexión del Firewall

Otro elemento importante instalado en San Pedro es el servidor. La figura 6.7 indica la disponibilidad del enlace del servidor durante el periodo de pruebas, o sea, mientras se estaba generando tráfico. Como se puede observar, la disponibilidad del enlace siempre se mantuvo en un 100% mientras se realizaban las pruebas.

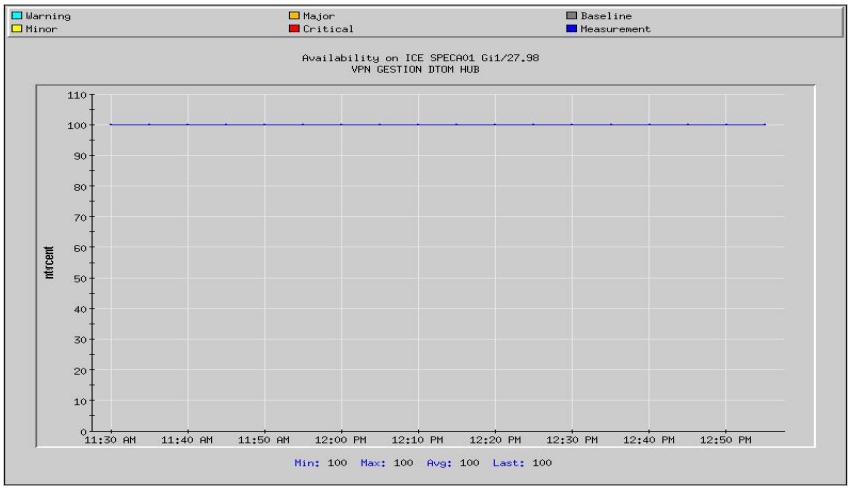


Figura 6.7 Disponibilidad de la conexión del Servidor

La figura 6.8 muestra la disponibilidad del enlace del servidor en un tiempo mayor, ya que la medición se realizó hasta el día siguiente demostrando que el enlace seguía disponible en un 100% a pesar de no generarse tráfico, lo que demuestra que existe conectividad entre ambos sitios a pesar de no existir paso de información por la red.

Figura 6.8 Disponibilidad de la conexión del Servidor

Las figuras 6.9 y 6.10 muestran el bit rate de entrada y de salida respectivamente mientras se realizaban las pruebas de conectividad generando tráfico. Como se puede observar, en este caso existe un mayor tráfico entrante que saliente, lo que se debe principalmente a que el servidor debe de recibir información del estado de los enlaces de los distintos sitios.

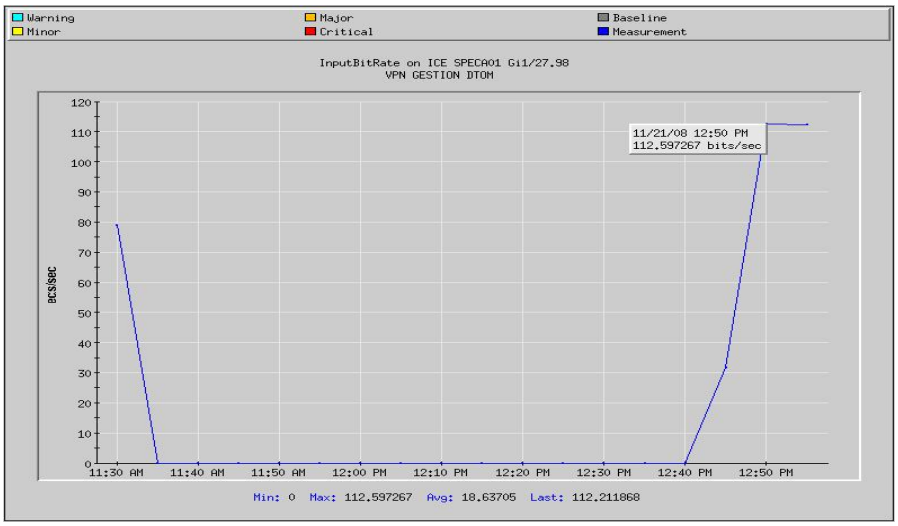


Figura 6.9 Bit rate de entrada de la conexión del Servidor

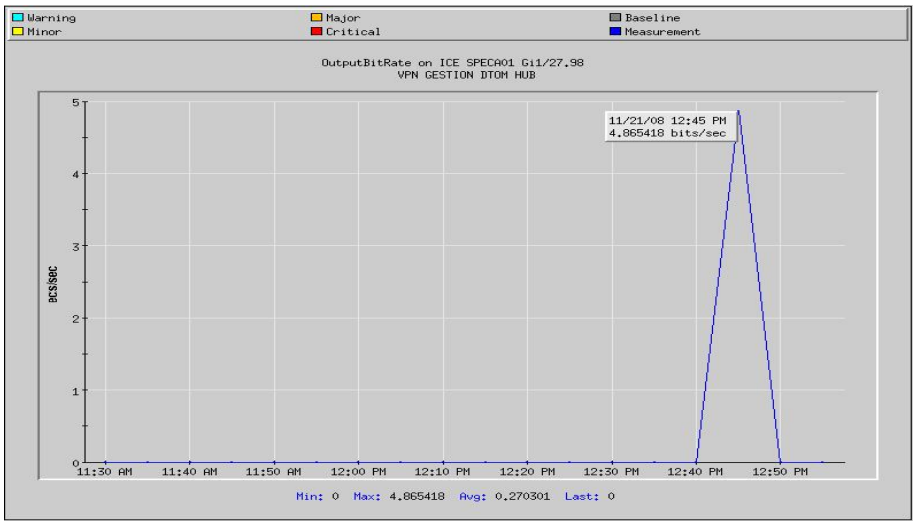


Figura 6.10 Bit rate de salida de la conexión del Servidor

La figura 6.11 muestra la suma del bit rate de entrada y de salida, el cual se utiliza para conocer la cantidad de tráfico total que pasa por este enlace.

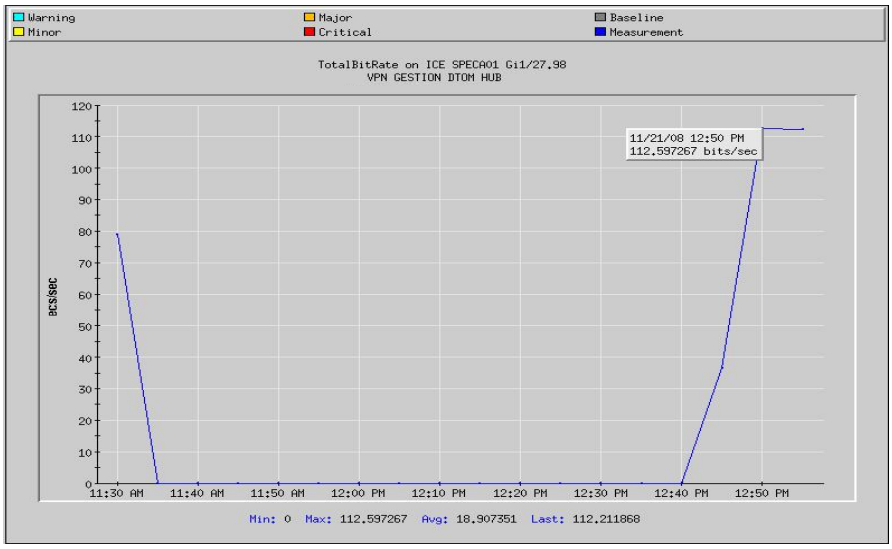


Figura 6.11 Total del bit rate de la conexión del Servidor

Con las mediciones finalizadas en San Pedro, se procedió a realizar mediciones en las centrales para demostrar la conectividad de las mismas con el nodo principal. La figura 6.12 muestra la disponibilidad del enlace entre la central de San Pedro y Desamparados la cuál es de un 100% lo que garantiza la conectividad entre ambos puntos.

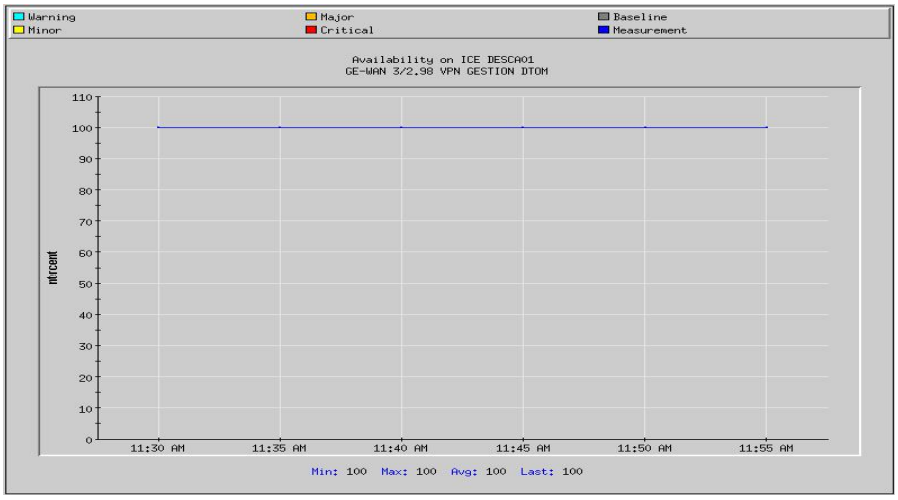


Figura 6.12 Disponibilidad de la conexión en la central de Desamparados

También se realizó una medición de disponibilidad del enlace en un tiempo mayor, la cual incluye un periodo en el que no existió tráfico por el enlace, sin embargo el mismo se encontró disponible en un 100%, dicha medición se puede observar en la figura 6.13.

Figura 6.13 Disponibilidad de la conexión en la central de Desamparados

En la central de Desamparados también se realizó mediciones de tráfico. La figura 6.14 muestra el bit rate de entrada mientras que la figura 6.15 muestra el bit rate de salida. Como se puede observar, el bit rate de entrada se mantuvo descendiendo una vez que alcanzó un valor máximo, esto se debió a que en el momento en que se recopiló la información para realizar las gráficas, ya existía tráfico en el enlace debido a que ya se estaba navegando por internet, motivo por el cual solo fue posible presentar los momentos finales de las pruebas realizadas y se estaba generando una menor cantidad de tráfico. De igual forma ocurrió con el bit rate de salida, el cuál descendió en un punto a cero debido a que dejó de enviar información y solamente estaba recibiendo, sin embargo, este punto es muy pequeño ya que siempre se encuentra intercambiando información con el nodo central.

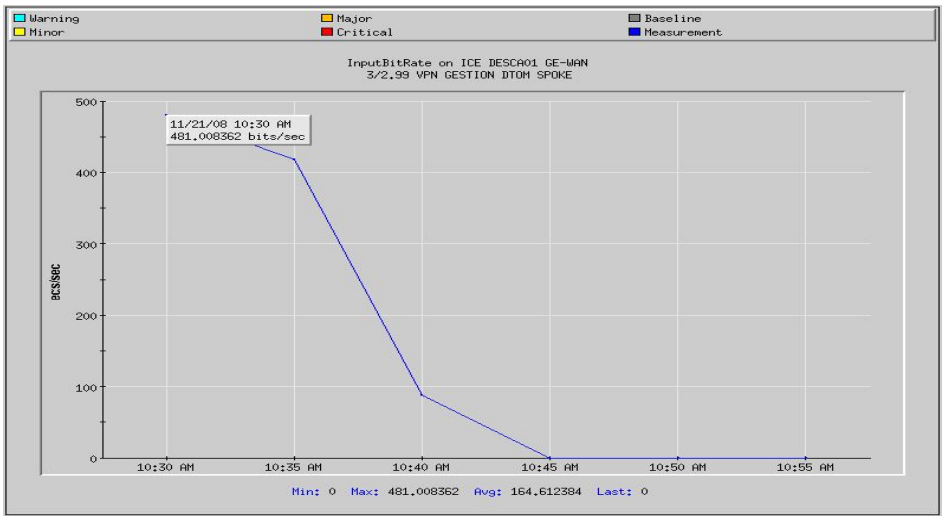


Figura 6.14 Bit rate de entrada de la conexión en la central de Desamparados

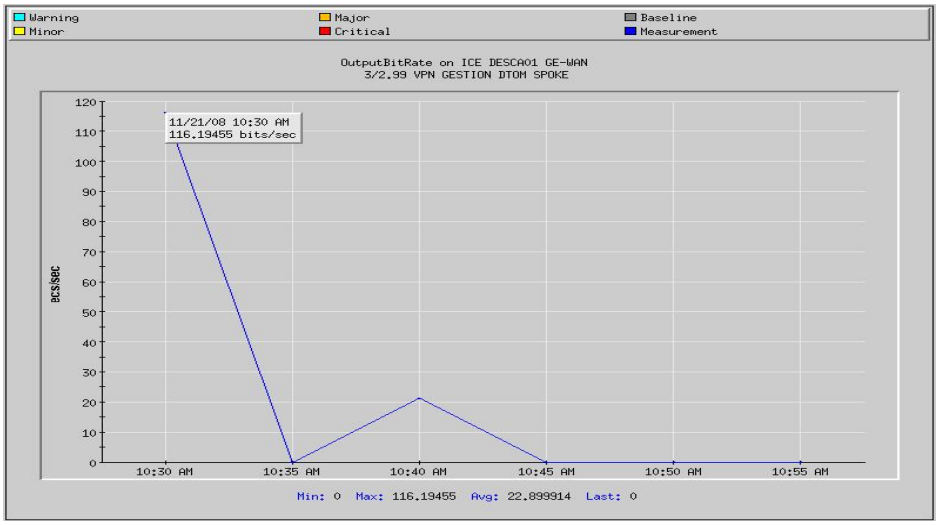


Figura 6.15 Bit rate de salida de la conexión en la central de Desamparados

La figura 6.16 muestra el tráfico total por este enlace, el cuál como en los casos anteriores es la suma del bit rate de entrada con el de salida. Esta información es útil para analizar la cantidad de tráfico que pasa por esta conexión.

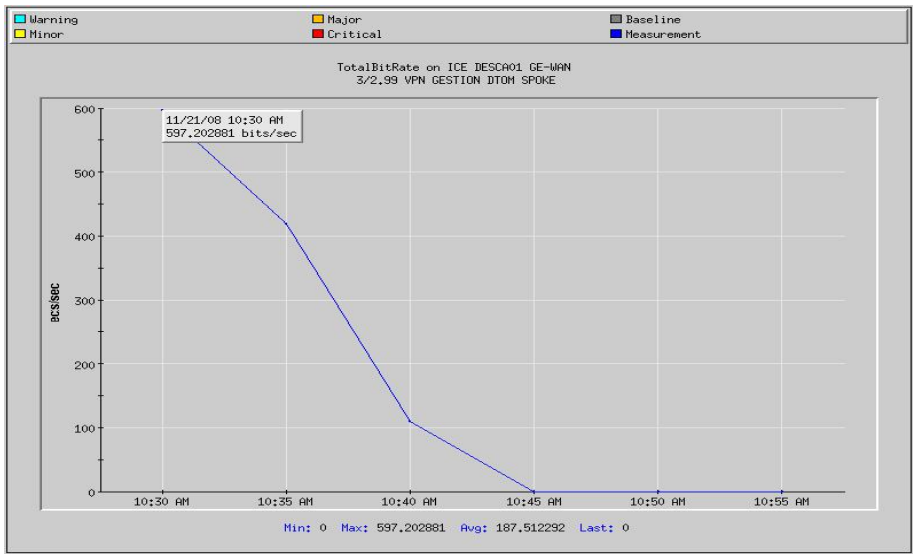


Figura 6.16 Total del bit rate de la conexión en la central de Desamparados

A continuación, la figura 6.17 muestra la disponibilidad del enlace entre San Pedro y Coronado. Como se puede observar, la gráfica muestra un 100% de conexión, con lo que se asegura la conectividad entre ambas centrales.

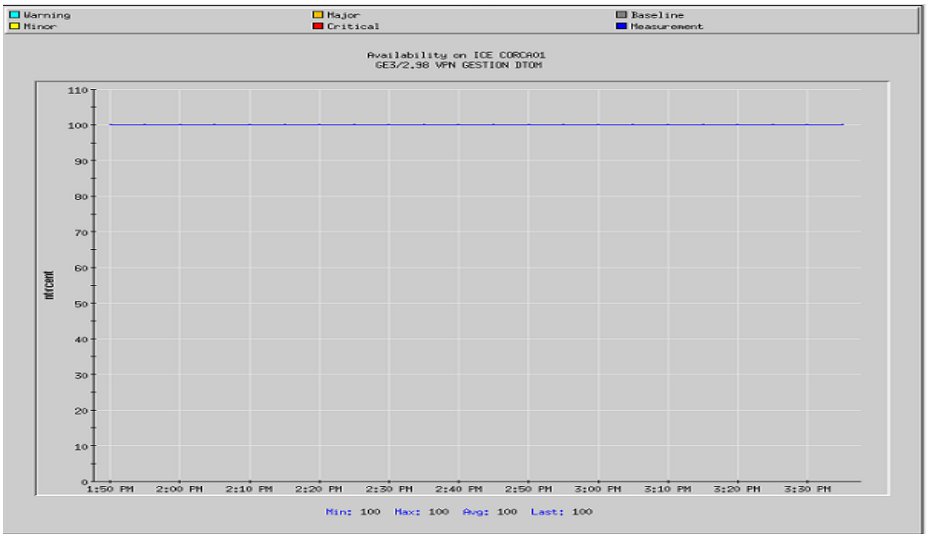


Figura 6.17 Disponibilidad de la conexión en la central de Coronado

En esta central también se realizaron pruebas de navegación de la red, la figura 6.18 y la figura 6.19 muestran el bit rate de entrada y de salida respectivamente. Como se puede observar ambas gráficas son muy similares dado que en esta central se estuvo intercambiando bastante información con el servidor para realizar pruebas de acceso por parte del mismo, así como también existió intercambio de paquetes con terceros lo que produjo bastante tráfico entrante y saliente.

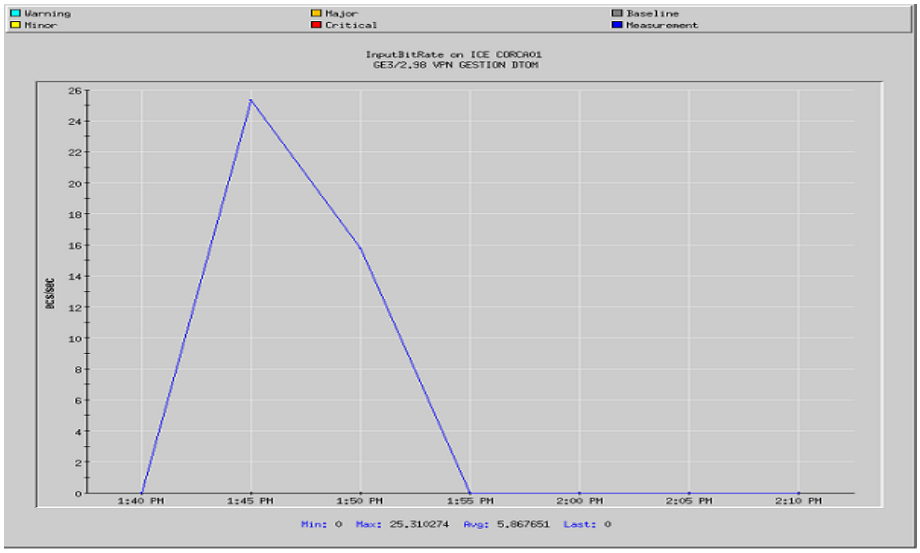


Figura 6.18 Input bit rate de la conexión en la central de Coronado

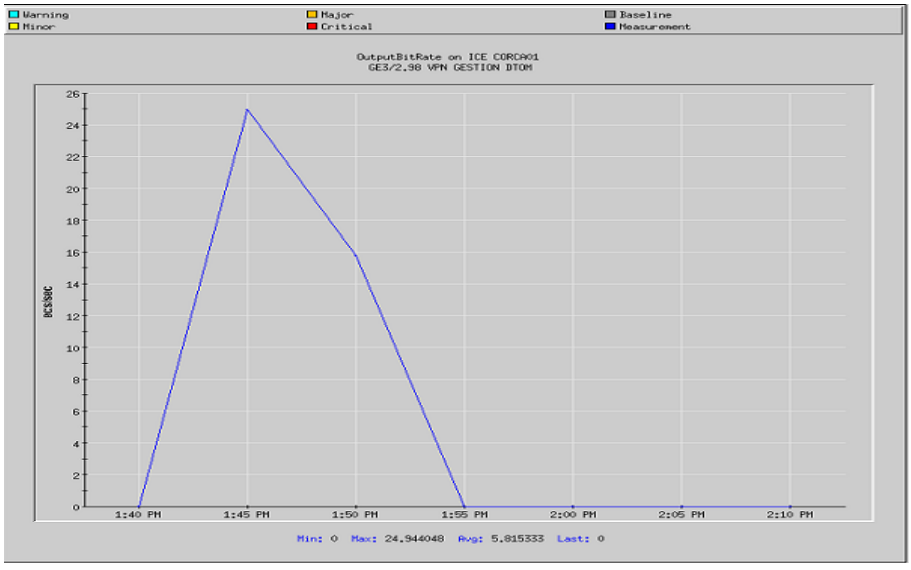


Figura 6.19 Output bit rate de la conexión en la central de Coronado

La figura 6.20 muestra el bit rate total del enlace, el cual tiene casi la misma forma de los bits rates por separado debido a la semejanza entre ellos con la diferencia de magnitud por ser una suma.

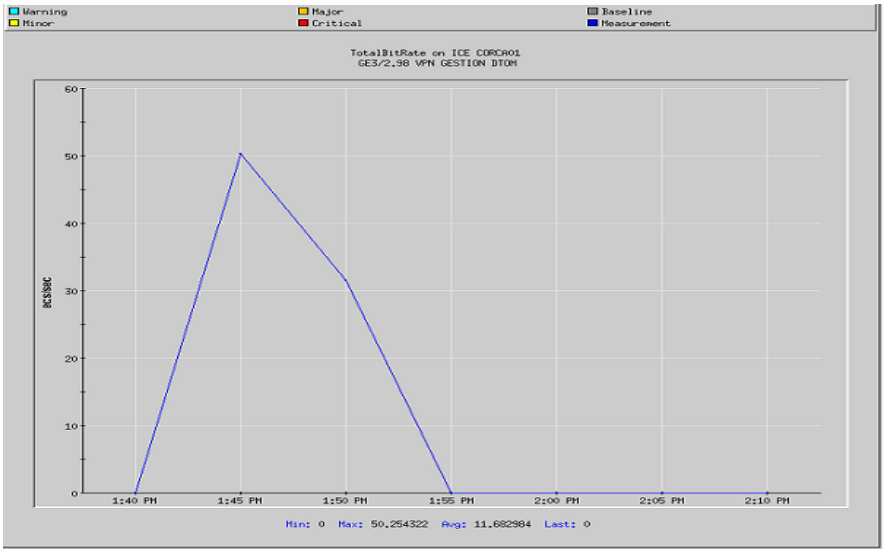


Figura 6.20 Total del bit rate de la conexión en la central de Coronado

La figura 6.21 muestra la medición de disponibilidad realizada en la central del Sur, la cual presenta un 100% lo que permite la conectividad entre los dos nodos sin ningún problema.

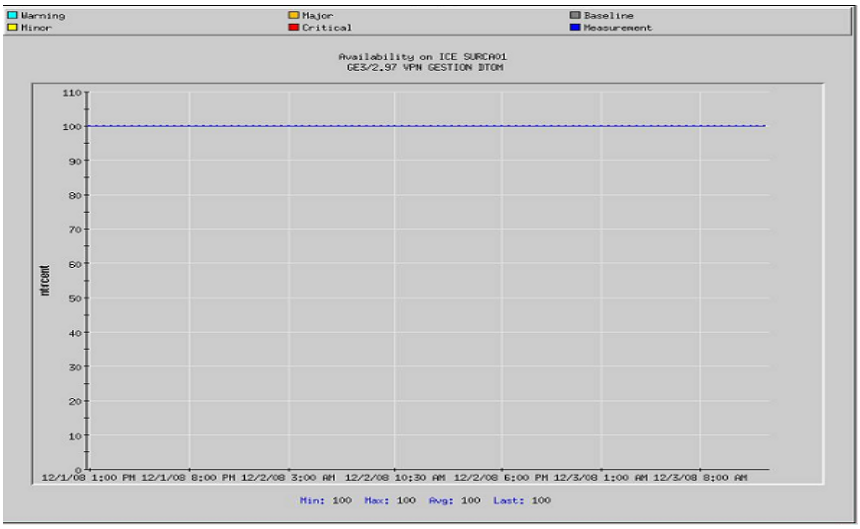


Figura 6.21 Disponibilidad de la conexión en la central de Sur

Como en las otras centrales, en el Sur también se realizaron mediciones de tráfico de entrada y de salida, dichas mediciones se pueden observar en las figuras 6.22 y 6.23. Las figuras indican que en esta zona existió un mayor flujo de entrada que de salida, sin embargo, el tráfico de salida siempre conservó la tendencia en un inicio a aumentar y una vez que alcanzó el punto máximo conservó la tendencia a disminuir.

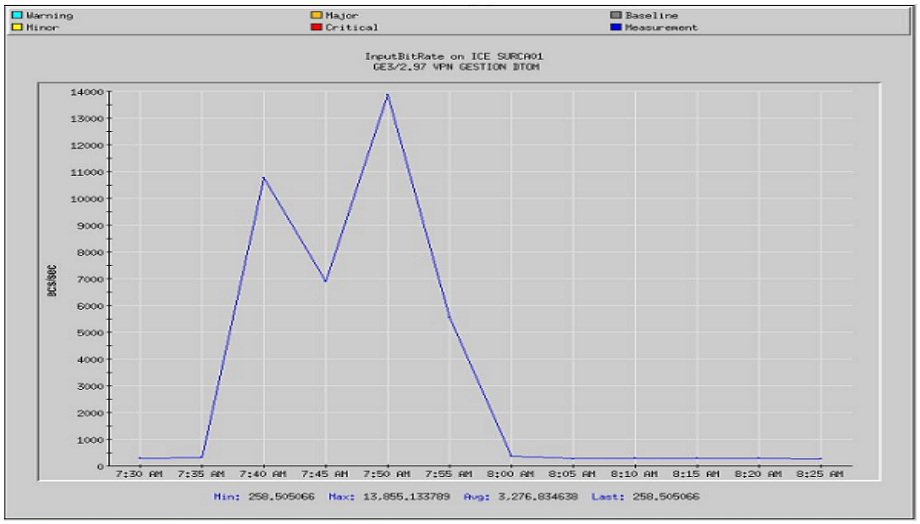


Figura 6.22 Input bit rate de la conexión en la central de Sur

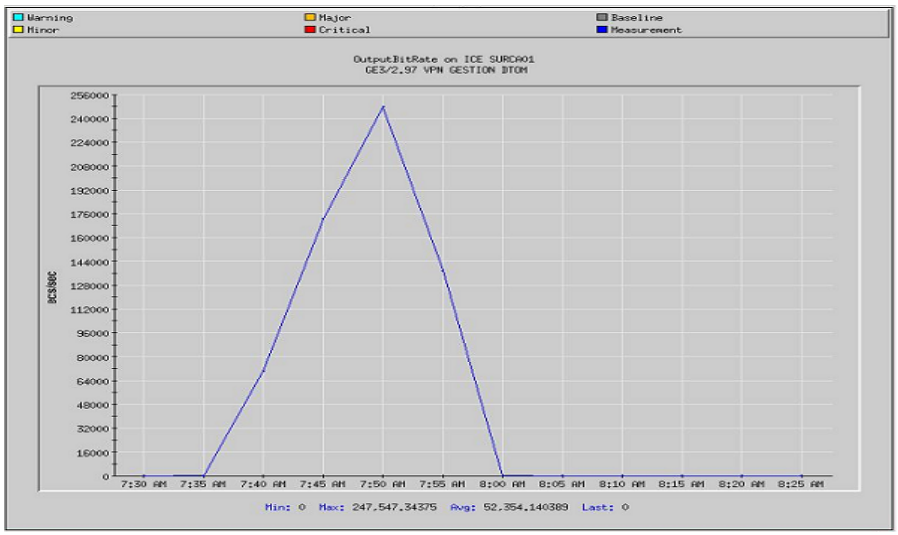


Figura 6.23 Output bit rate de la conexión en la central de Sur

La figura 6.24 representa la suma del tráfico de entrada con el de salida. Como se puede observar, la forma de la gráfica conserva la forma del diagrama del tráfico de salida debido a que éste conserva la tendencia ya sea a crecer o disminuir, a pesar que el gráfico de bit rate de entrada no tiene la misma tendencia, lo que produce en la suma de ambos es un crecimiento un poco más lento.

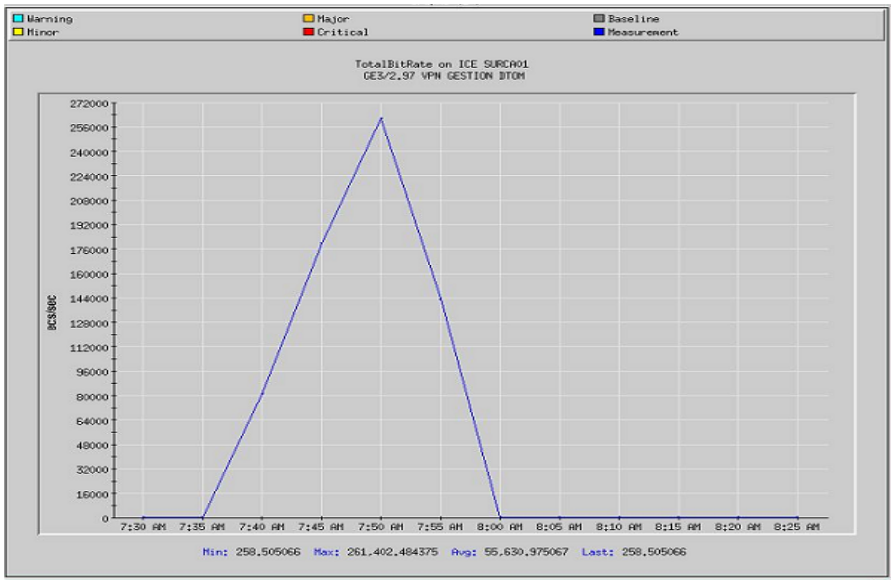


Figura 6.24 Output bit rate de la conexión en la central de Sur

La figura 6.25 muestra la disponibilidad del enlace entre las centrales de San Pedro y Norte la cual se localiza en Tibás. Como se puede observar la conectividad se encuentra en un 100% lo que permite la conexión entre ambos nodos sin problemas.

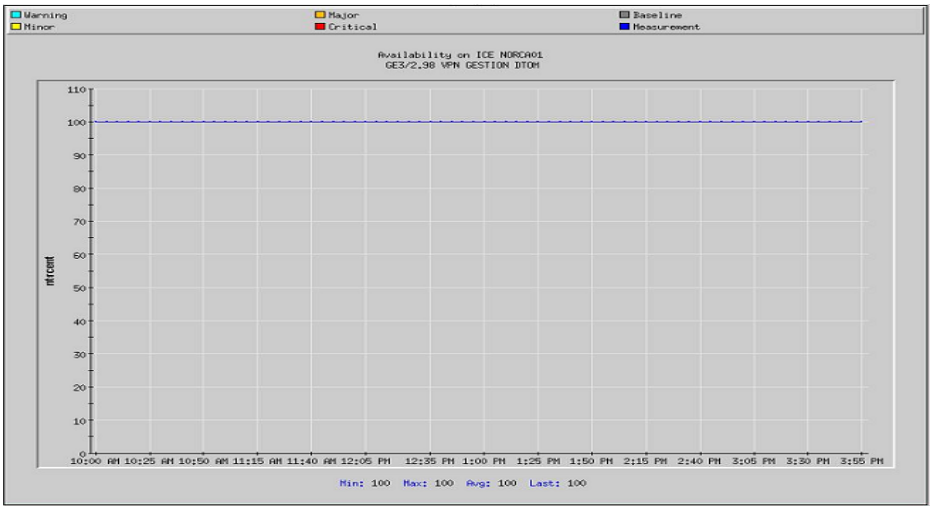


Figura 6.25 Disponibilidad de la conexión en la central de Norte

La figura 6.26 muestra el tráfico de entrada en esta central. En la gráfica se puede observar un pico que sobresale, el cuál es el momento en el que se produjo mayor tráfico de entrada por el enlace, mientras que en el resto del tiempo existió tráfico pero en menor cantidad.

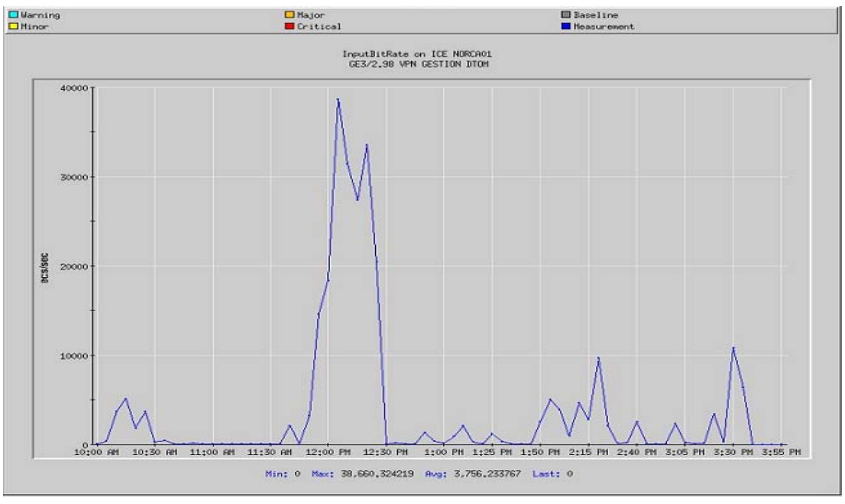


Figura 6.26 Input bit rate de la conexión en la central de Norte

La figura 6.27 muestra el tráfico de salida de la conexión. Como en el caso anterior, también existe un pico que sobresale el cuál es el momento en el cuál existió la mayor cantidad de tráfico de salida fluyendo por el enlace.

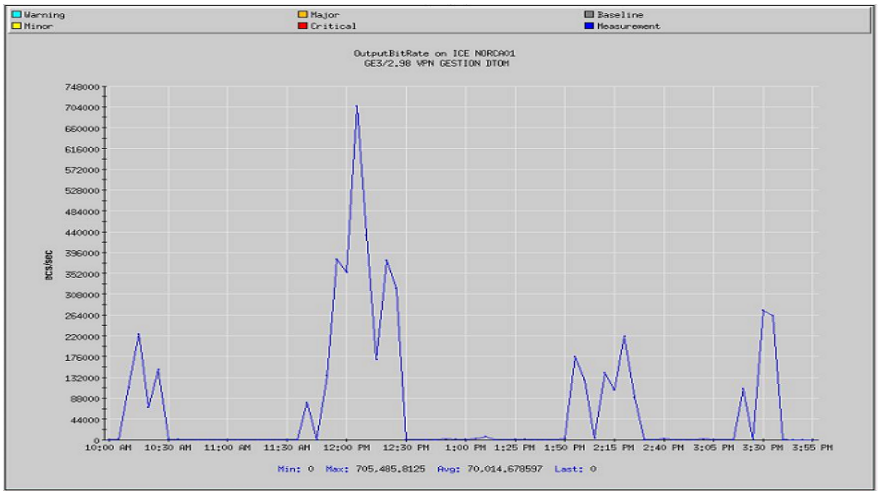


Figura 6.27 Output bit rate de la conexión en la central de Norte

La figura 6.28 representa la suma del tráfico entrante y saliente, como se puede observar existió bastante intercambio de información en esta central, aparte de que por ser una de las centrales con más personal conectado, las pruebas realizadas tomaron más tiempo que en las otras.

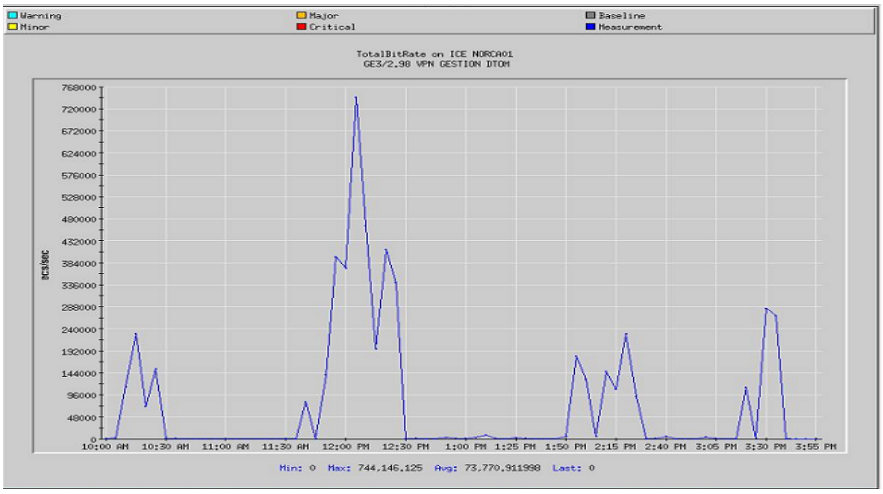


Figura 6.28 Total del bit rate de la conexión en la central de Norte

La figura 6.29 representa la conectividad en la central del Oeste, la que como se puede observar se encuentra a un 100%, lo cual nuevamente asegura la conectividad entre ambos nodos.

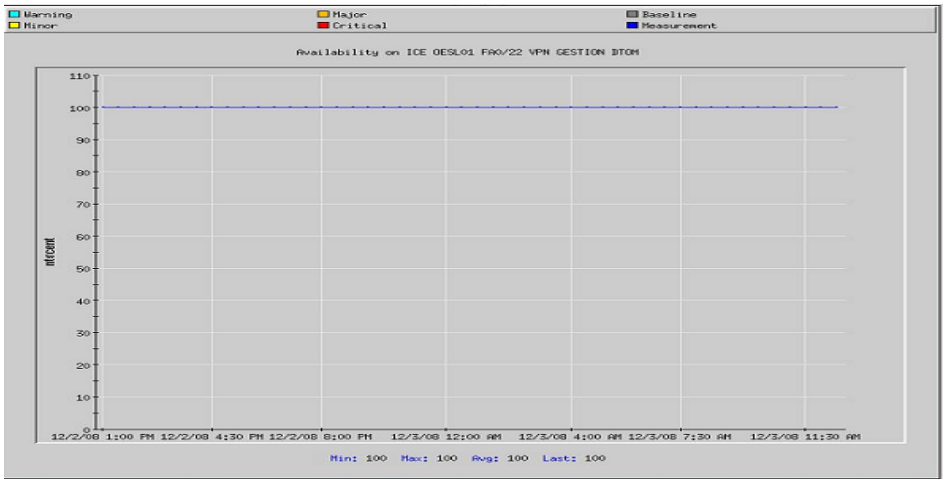


Figura 6.29 Disponibilidad de la conexión en la central de Oeste

Las figuras 6.30 y 6.31 representan el tráfico entrante y saliente del enlace. En esta central también existió mucho intercambio de información con terceros y con el nodo de San Pedro, por lo que como se puede observar en ambas figuras son muy similares.

Figura 6.30 Input bit rate de la conexión en la central de Oeste

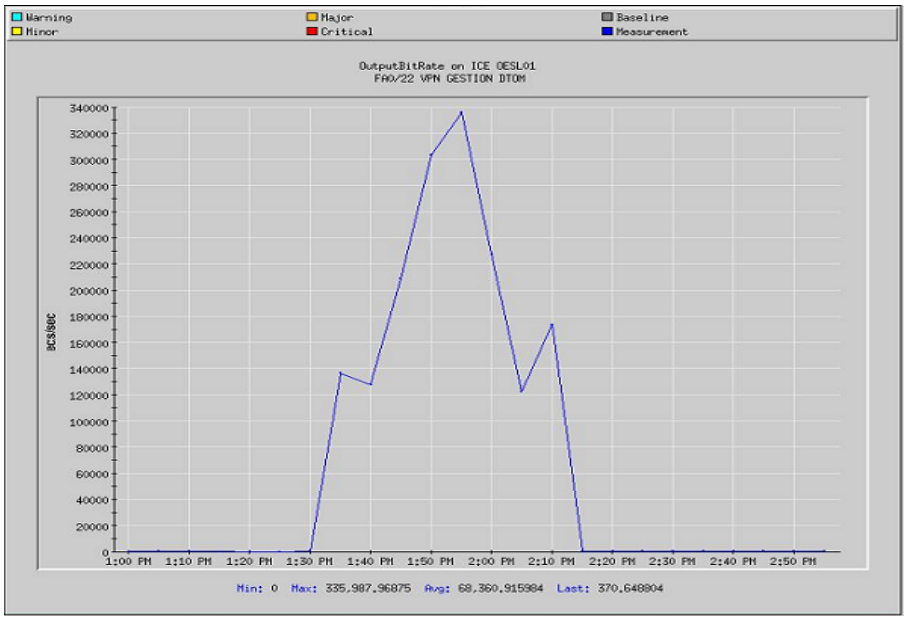


Figura 6.31 Output bit rate de la conexión en la central de Oeste

La figura 6.32 representa la suma total del tráfico de entrada y salida del enlace, el cual como se puede observar conserva casi la misma forma de ambas pero con diferente magnitud debido a que cada una por separada tenía formas muy similares con magnitudes distintas.

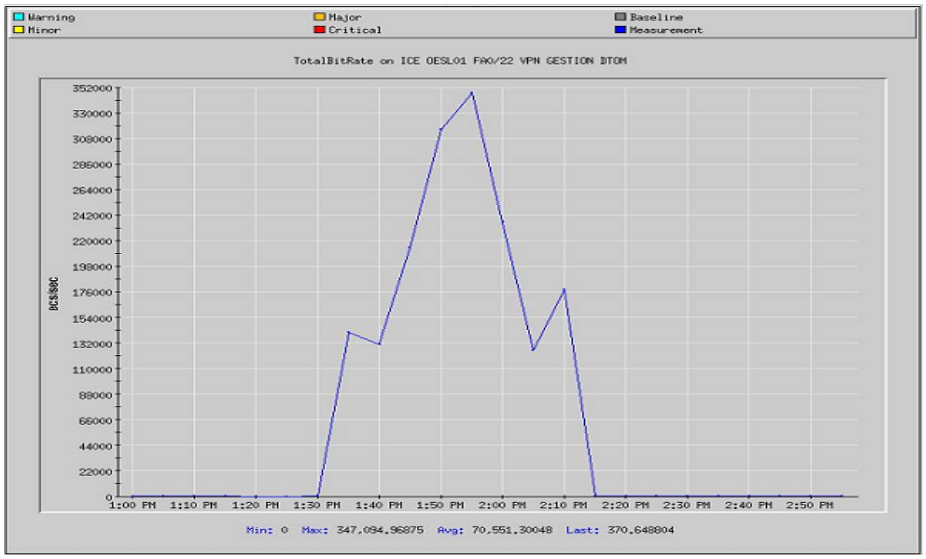


Figura 6.32 Total del bit rate de la conexión en la central de Oeste

Capítulo 7 : Conclusiones y recomendaciones

7.1 Conclusiones

1) El direccionamiento depende de los requerimientos de cantidad de equipo que tenga la red.

2) Para que existan dos redes distintas en una misma LAN debe de existir por lo menos un dispositivo capaz de realizar enrutamiento.

3) Las VPN de capa 3 permiten la conectividad entre dos puntos distantes.

4) Las VPN proporcionan un camino seguro para la transmisión de datos.

5) La máxima transferencia de datos la limita el dispositivo con menor ancho de banda.

6) La conexión del puerto del DSLAM a la regleta tiene un orden específico que se debe de seguir.

7) Los IP-DSLAM son dispositivos de conmutación, puede verse como un switch de capa 2.

8) El Firewall es un dispositivo que brinda seguridad a la red.

9) La traducción de direcciones de la red (NAT) la realiza el Firewall.

10) Por medio de esta red de gestión es posible la implementación del teletrabajo.

7.2 Recomendaciones

1) Siempre que se realiza un direccionamiento es importante tener en cuenta una posible expansión.

2) El diseño de esta red brinda acceso a Internet por medio de un puerto del Firewall, sin embargo, para no saturarlo, se podría dar acceso por medio de uno o dos puertos más.

3) Crear un enlace redundante en la central de San Pedro para evitar una posible pérdida de conexión, debido a que se cuenta únicamente con un medio de salida a las demás centrales.

4) Por ser una red de gestión, se debe de mantener en mantenimiento preventivo, lo cual evitará que en un futuro que los técnicos no puedan realizar sus labores.

17. Bibliografía

[1] Cisco Systems, Inc. Academia de Networking de Cisco Systems: Guía del primer año. 3 ed. Pearson Educación.

[2] Cisco Systems, Inc. Academia de Networking de Cisco Systems: Guía del segundo año. 3 ed. Pearson Educación.

[3] Cisco Systems, Inc. Centro de Soluciones IP: Volúmen 1.

[4] Cisco Systems, Inc. Centro de Soluciones IP: Volúmen 2. 3

[5] Cisco Systems, Inc. Centro de Soluciones IP: Guía de Laboratorio.

[6] Definiciones tecnológicas. Sitio WEB [en línea].
< http://www.mastermagazine.info/termino/4394.php > [Consulta: Setiembre 2008].

[7] Definiciones tecnológicas. Sitio WEB [en línea].
< http://www.alegsa.com.ar/Dic/red%20privada%20virtual.php > [Consulta: Setiembre 2008].

[8] Firewall. Sitio WEB [en línea].
< http://www.monografias.com/trabajos14/firewalls/firewalls.shtml > [Consulta: Setiembre 2008].

[9] Firewall. Sitio WEB [en línea].
< http://es.kioskea.net/contents/protect/firewall.php3 > [Consulta: Setiembre 2008].

[10] DSLAM. Sitio WEB [en línea].
< http://es.wikipedia.org/wiki/DSLAM > [Consulta: Setiembre 2008].

[11] ZyXEL. Zywall 1050 datasheet [en línea].
< http://www.us.zyxel.com/web/index.php > [Consulta: octubre 2008]

[12] ZyXEL. DSLAM IES 1000 datasheet [en línea].
< http://www.us.zyxel.com/web/index.php > [Consulta: octubre 2008]

[13] ZyXEL. CPE datasheet [en línea].
< http://www.us.zyxel.com/web/index.php > [Consulta: octubre 2008]

18. Anexos

Manual de usuario

Firewall

Figura 18.1 Zywall 1050

1) Para configurar el equipo es necesario ingresar la dirección 192.168.1.1 en el navegador, el equipo cuenta con una contraseña predeterminada para su configuración.

2) Configurar la dirección IP de la tarjeta de red de la computadora, para que sea parte de la dirección de acceso por defecto que trae el equipo.

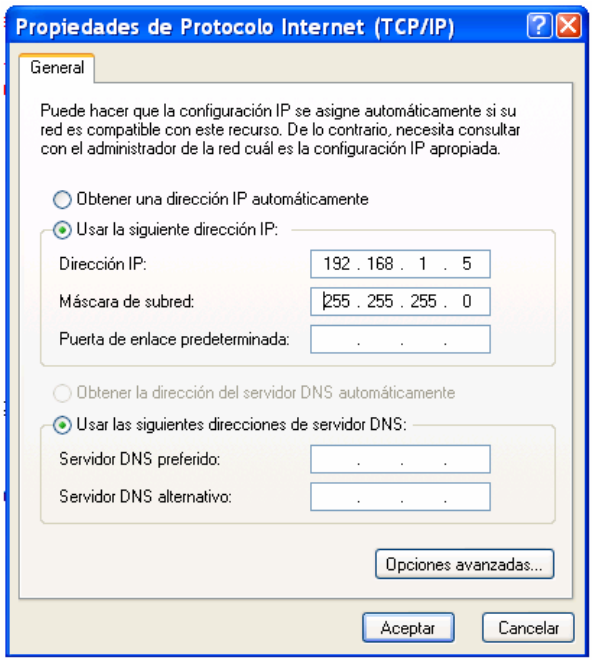


Figura 18.2 Interfaz de configuración de la dirección IP en la computadora

3) Una vez que se ingrese a esta dirección se le solicita autentificarse para lo cual, este equipo trae como usuario admin y como password 1234 por defecto.

Figura 18.3 Interfaz de ingreso al equipo

4) Una vez que ingrese, se despliega una pantalla indicando que se cambie la contraseña que trae el equipo por defecto.

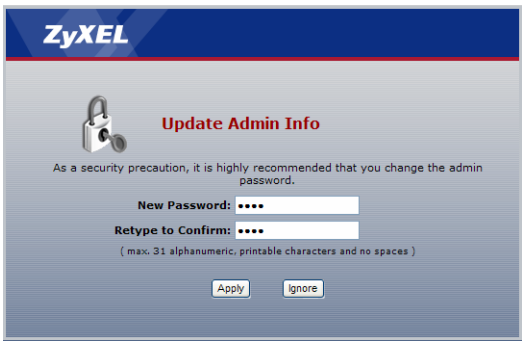


Figura 18.4 Interfaz de cambio de contraseña

5) Con el cambio de contraseña realizado, la pantalla presenta el status del Firewall, la cual nos muestra información de cómo se encuentra el dispositivo en ese momento. Se puede observar información del Firewall, recursos del sistema, el estado de las interfaces entre otros.

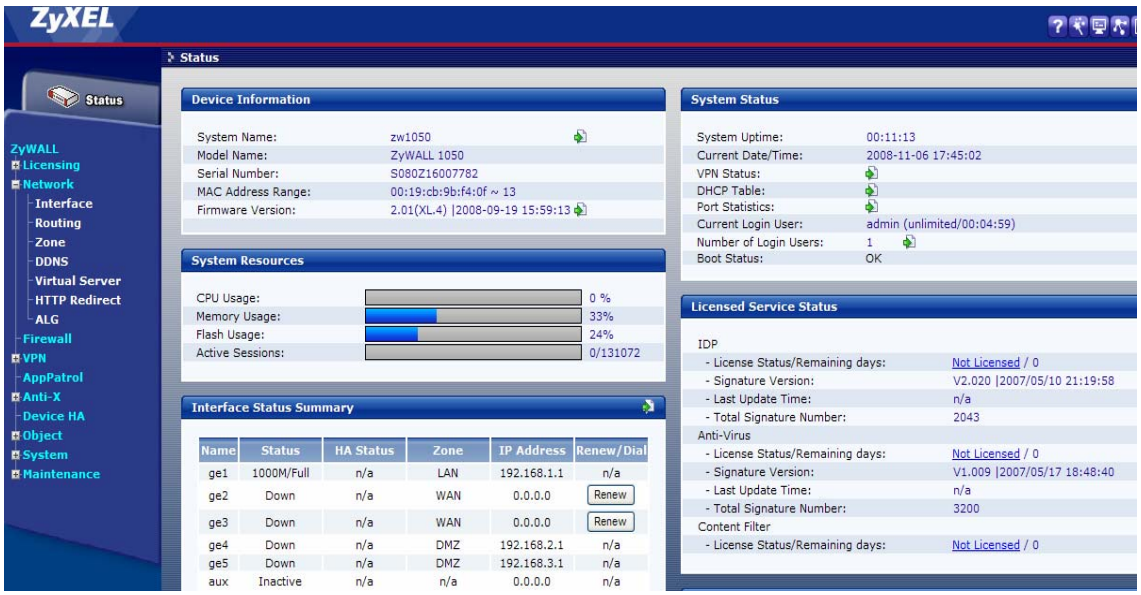


Figura 18.5 Status del Zywall 1050

6) Para realizar la configuración de las interfaces, se debe ingresar en Interface que se localiza en el menú Network. En primera instancia, se muestra datos técnicos de las interfaces.

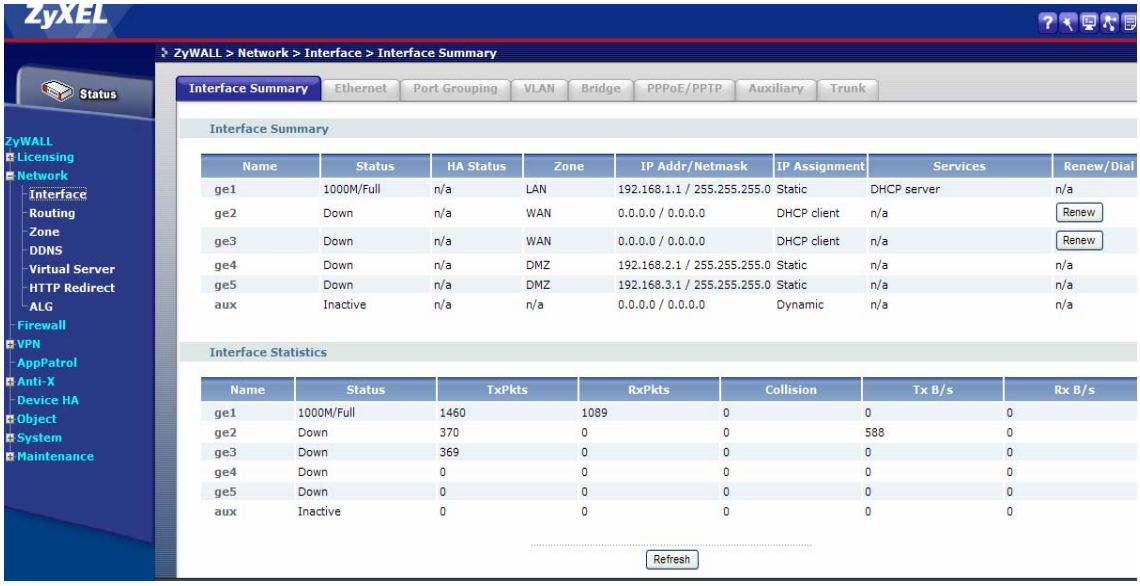


Figura 18.6 Interfaz del menú Network

7) Ahora para realizar la configuración de la interfaz, se debe de ingresar en la pestaña Ethernet.

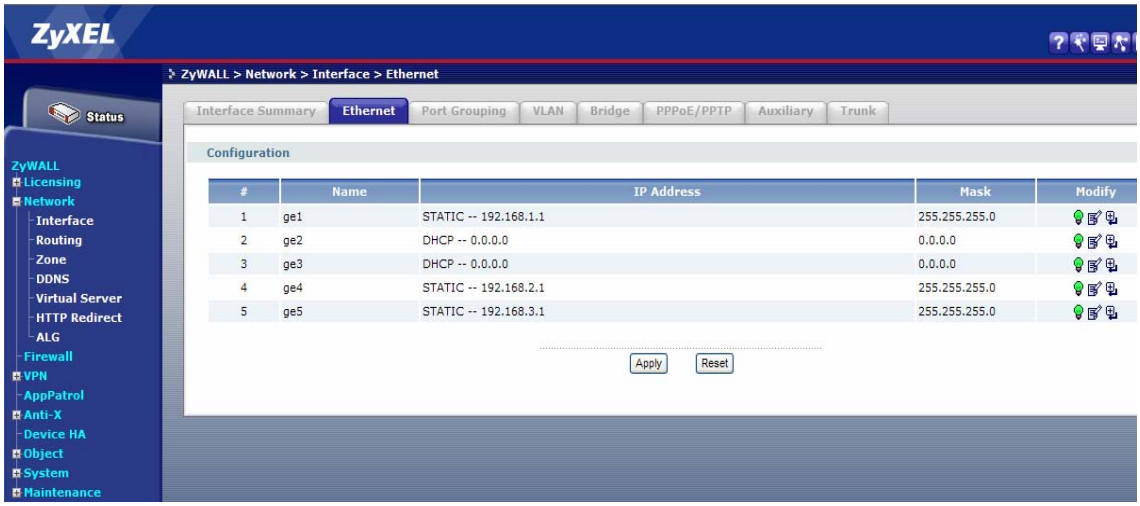


Figura 18.7 Interfaz del menú Ethernet

8) Una vez posicionado en esta pantalla, se hace click sobre la opción de modificar de la interface que se desea utilizar, en este caso se configurará la interfaz 1 correspondiente a un puerto LAN. Se le pueda dar una pequeña descripción a la interfaz si se quiere. Se debe de configurar la dirección ip del equipo, así como la máscara y la puerta de enlace.

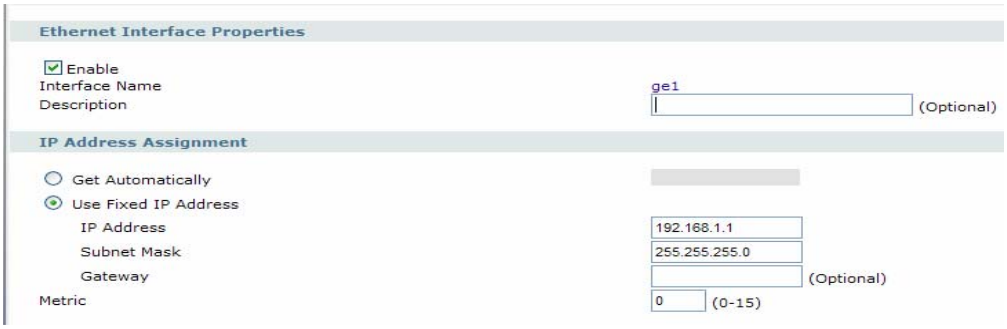


Figura 18.8 Interfaz de configuración del puerto LAN

9) Para configurar la interfaz WAN se siguen los mismos pasos de configuración de la interfaz LAN, para tener salida a internet se requiere una dirección ip pública. También se debe de configurar los DNS, los cuales no se configuran para la LAN.

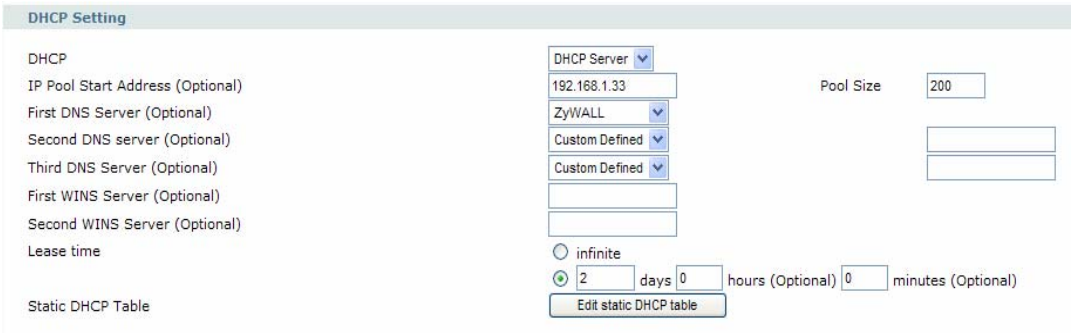


Figura 18.9 Interfaz de configuración del puerto WAN

10) Una vez que se ha configurado la dirección ip, la máscara de subred, la puerta de enlace y los DNS, se debe de crear un objeto dirección, de lo contrario no se puede tener acceso a internet todavía. Para crear éste objeto, se debe de ingresar en Address en el menú de Object y después en añadir.

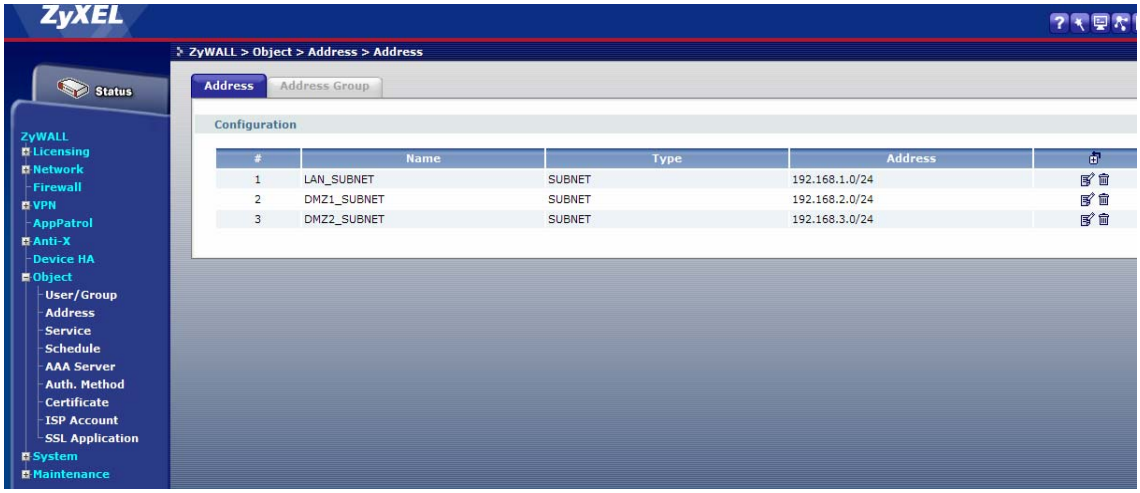


Figura 18.10 Interfaz del submenú Address del menú Object

11) La interface para la creación del objeto es la siguiente:

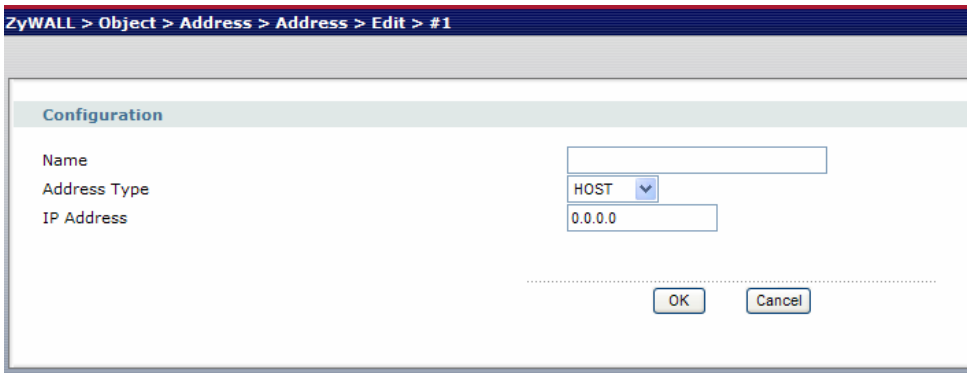


Figura 18.11 Interface para la creación del objeto

12) Una vez que ha sido creada el objeto dirección, se debe de agrupar con el que trae el equipo por defecto. Lo anterior se realiza en la pestaña Address Group.

Figura 18.12 Interface para la agrupación de objetos

13) Con el grupo creado se procede a realizar el enrutamiento que va a utilizar el Firewall para brindar salida a la red. Se selecciona Routing en el menú Network.

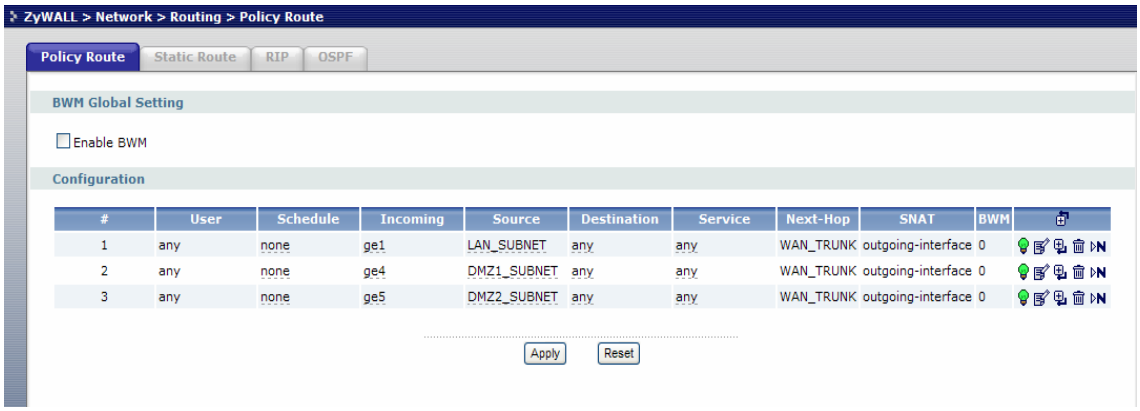


Figura 18.13 Interface del submenú Routing del menú Network

14) Una vez dentro del submenú de Routing, en la pestaña de Policy Route, se debe de seleccionar la opción de modificar y en Criteria cambiar el Source Address que tiene el equipo por el grupo que fue creado.

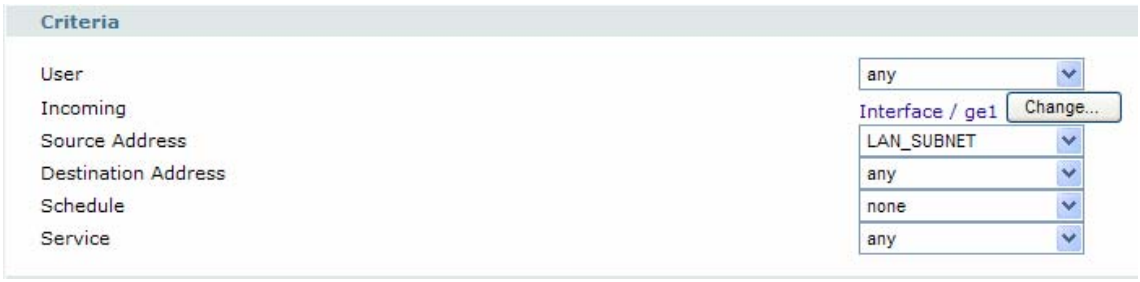


Figura 18.14 Interface paras seleccionar las políticas de enrutamiento

MiniDslam

Figura 18.15 Módulo del DSLAM IP

1) Para configurar el equipo es necesario ingresar la dirección 192.168.1.1 en el navegador, el equipo cuenta con una contraseña predeterminada para su configuración.

2) Configurar la dirección IP de la tarjeta de red de la computadora, para que sea parte de la dirección de acceso por defecto que trae el equipo.

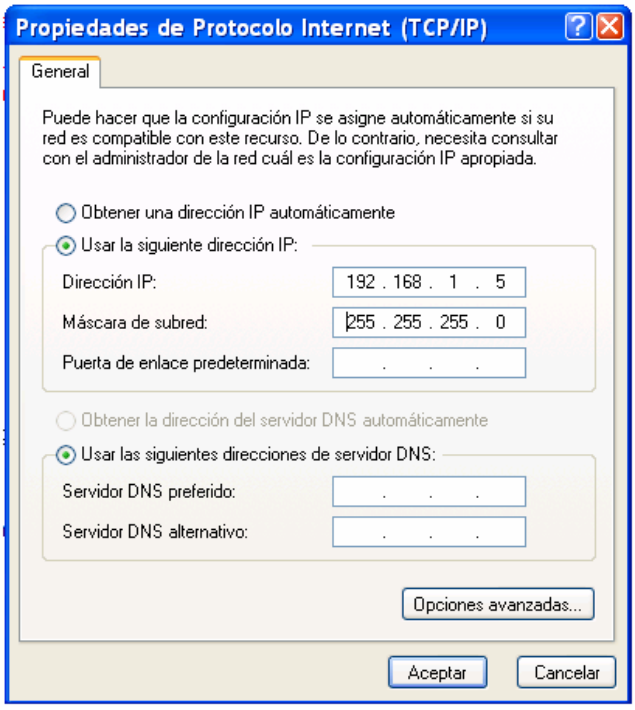


Figura 18.16 Interfaz de configuración de la dirección IP en la computadora

3) Una vez que se ingrese a esta dirección se le solicita autentificarse para lo cual, este equipo trae como usuario admin y como password 1234 por defecto.

Figura 18.17 Interfaz de ingreso al equipo

4) Una vez autentificado la pantalla inicial que se mostrará es la siguiente:

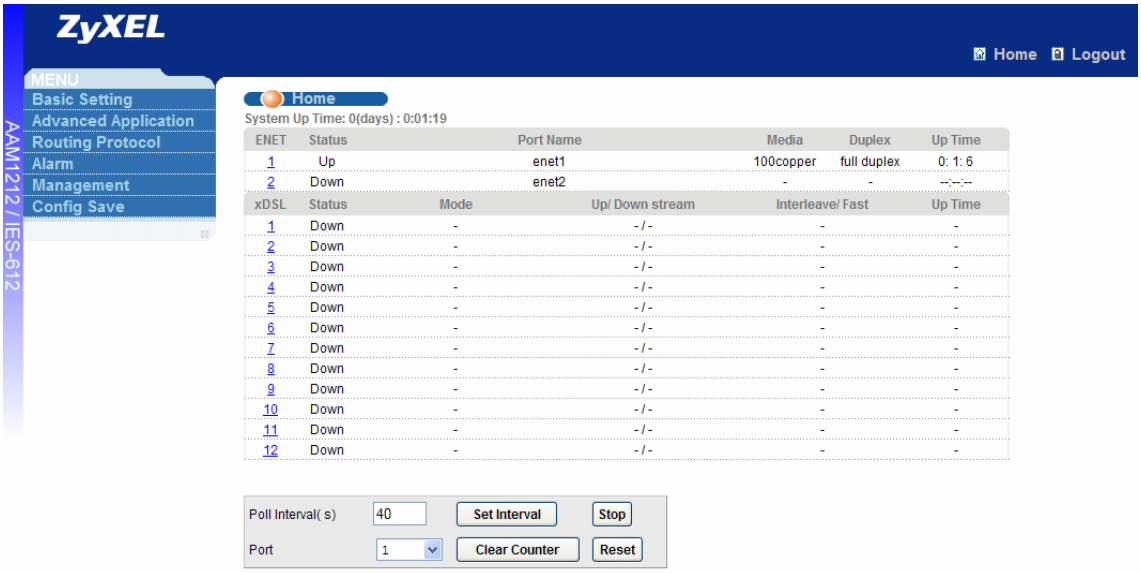


Figura 18.18 Interfaz de inicio del DSLAM

5) Como primer punto para la configuración del equipo, se debe de actualizar el firmware del mismo y posteriormente el ROM. Para actualizar el firmware se debe de ingresar a Management en el menú principal, después en el submenú se debe de seleccionar Maintenance, para lo cual aparece en la pantalla principal varias opciones de las cuáles se debe de seleccionar la opción Firmware Upgrade.

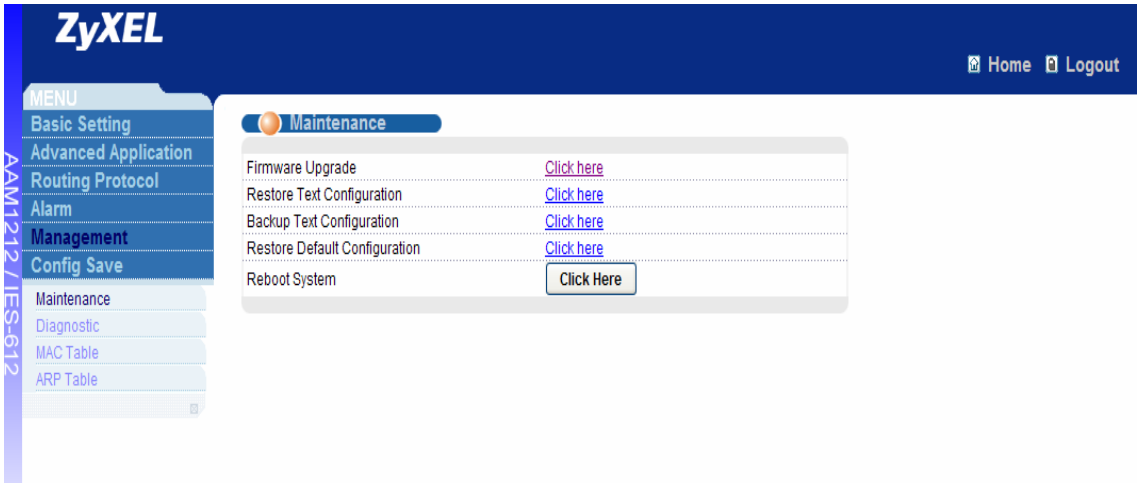


Figura 18.19 Interfaz de mantenimiento del DSLAM

6) Una vez seleccionada esta opción, se abre una nueva pantalla en la cual se debe de buscar el archivo de actualización con extensión .bin y una vez localizado se debe de hacer click en Upgrade.

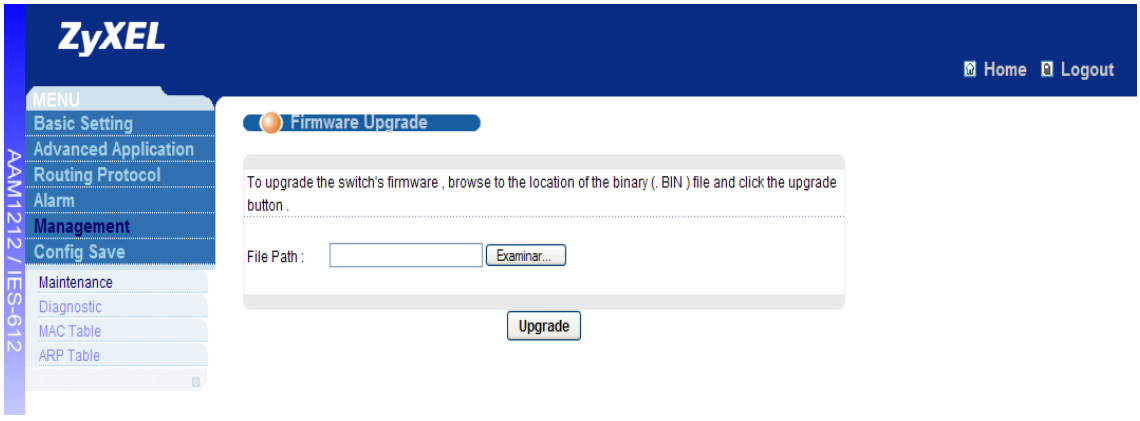


Figura 18.20 Interfaz de actualización del firmaware del DSLAM

7) Con la actualización del Firmware realizada, se procede a realizar la actualización de la ROM por medio de consola. Para realizar esta configuración se debe de utilizar algún programa como el hyperterminal para realizarla. Se le debe de asignar un nombre a la conexión:

Figura 18.21 Interfaz de conexión al hyperterminal

8) Una vez asignado el nombre, se debe de seleccionar el puerto serie por el cual se realizará la conexión, en este caso se realizará por el COM1.

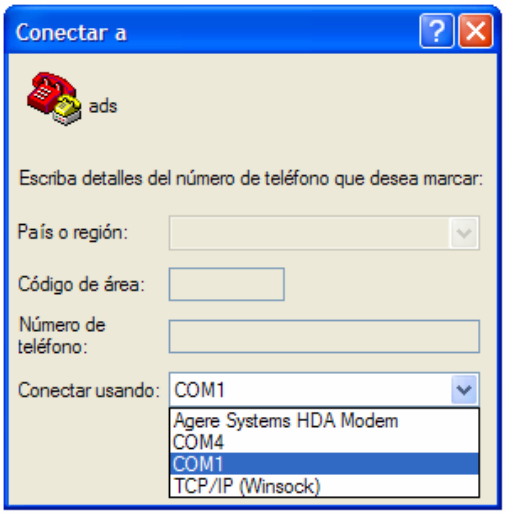


Figura 18.22 Interfaz de selección de puerto de comunicación del hyperterminal

9) Con el puerto seleccionado se debe de realizar la configuración de los parámetros para realizar la comunicación como se muestra a continuación:

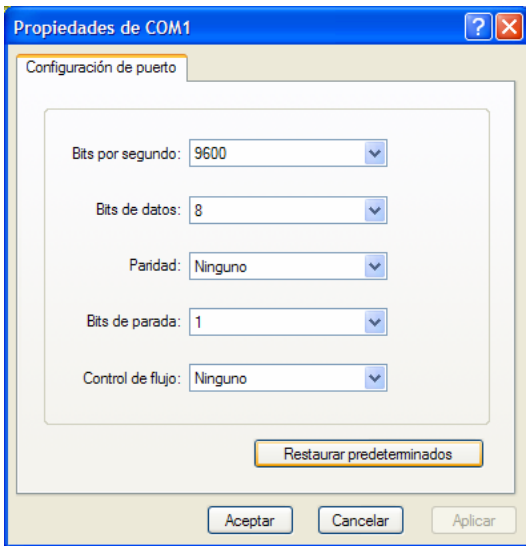


Figura 18.23 Interfaz de configuración del hyperterminal

10) De esta manera se cuenta con comunicación entre el miniDSLAM y la computadora, por lo tanto puede dar inicio al proceso de actualización de la ROM. Como primer paso digite el comando ras>sys reboot con lo cual se reiniciará el equipo.

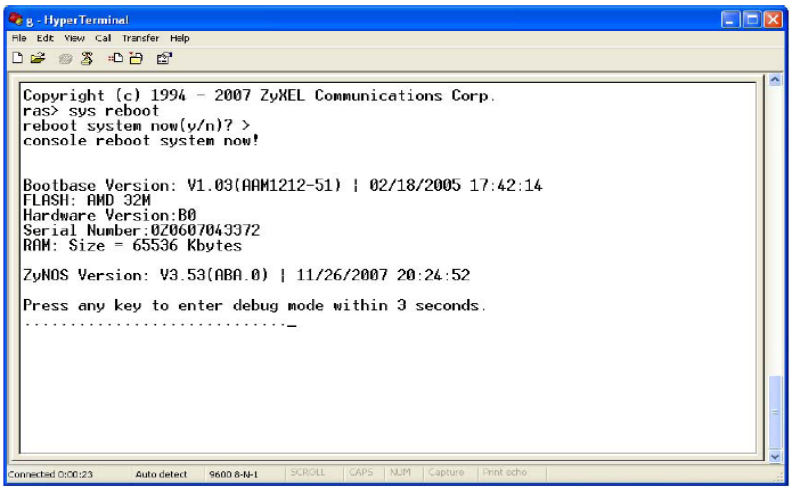


Figura 18.24 Reinicio del equipo

11) Una vez que aparece el mensaje “Press any key to enter debug mode within 3 seconds”, presione cualquier tecla para ingresar al modo de depuración. El modo de depuración no muestra ningún prompt.

12) Una vez que se encuentra en el modo de depuración, digite el comando atba5 para cambiar la velocidad de la consola a 115200 bps.

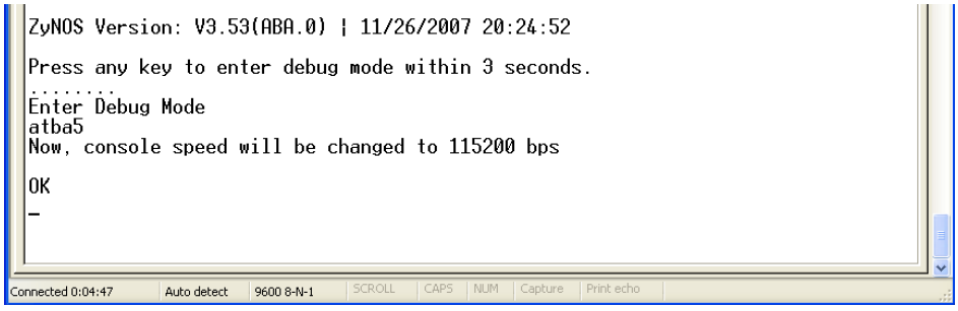


Figura 18.25 Comando para cambiar velocidad del equipo

13) Después desconecte la consola en el menú Call ó Llamada y seleccione la opción Disconnect o Desconectar.

14) Luego en Archivo>Propiedades, se debe de seleccionar configurar y variar la velocidad de 9600 bps a 115200 bps.

15) Se debe de reanudar la consola en el menú Call o Llamada y seleccione Llamada.

16) Ahora se debe de ingresar el comando atlc y presionar “Enter”, para la carga del archivo de configuración.

17) A continuación ingrese al menú de Transfer o Transferir. Se debe de seleccionar la opción Send File o Enviar Archivo. Seleccione el botón de búsqueda para indicar la ruta del archivo, en este caso el archivo que debe cargar es el que tiene la extensión .rom.

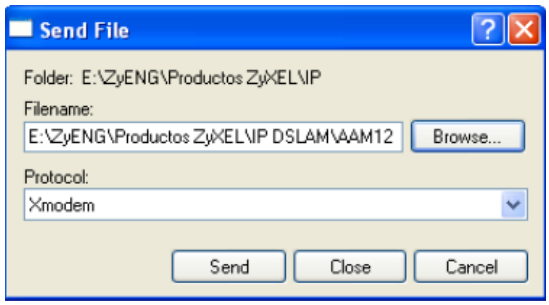


Figura 18.26 Selección del archivo para cargar y el protocolo a utilizar

18) El protocolo que se debe de seleccionar es el XMODEM para que la transmisión sea más rápida y segura.

19) Una vez finalizada la carga del archivo de configuración es necesario apagar y volver a encender el equipo.

20) Una vez reiniciado el equipo, se debe de ingresar al mismo de igual manera que al inicio. En el menú principal seleccione la opción Basic Setting.

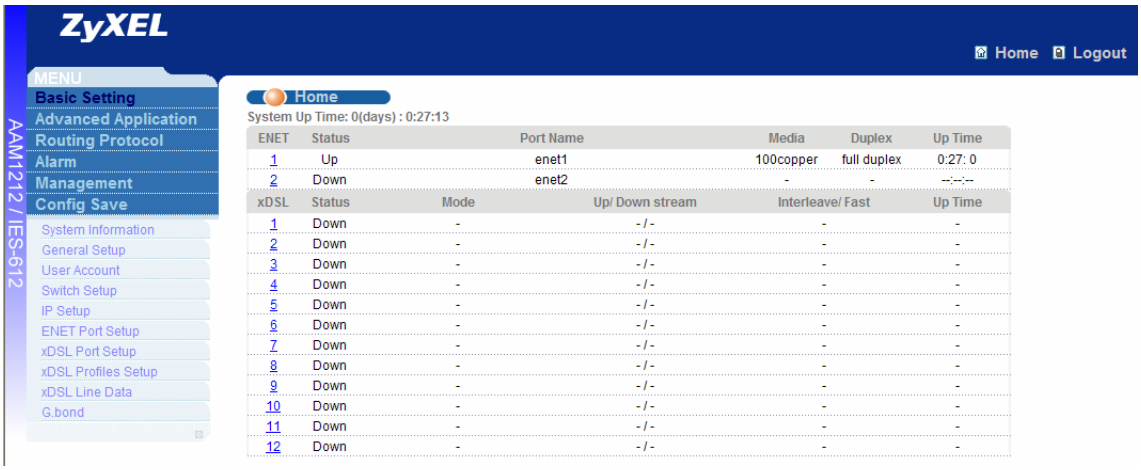


Figura 18.27 Menú de Basic Setting

21) Con esta selección se abre un submenú en el cuál se debe de seleccionar la opción IP Setup para configurar la dirección ip, la máscara y el default gateway que utilizará el equipo.

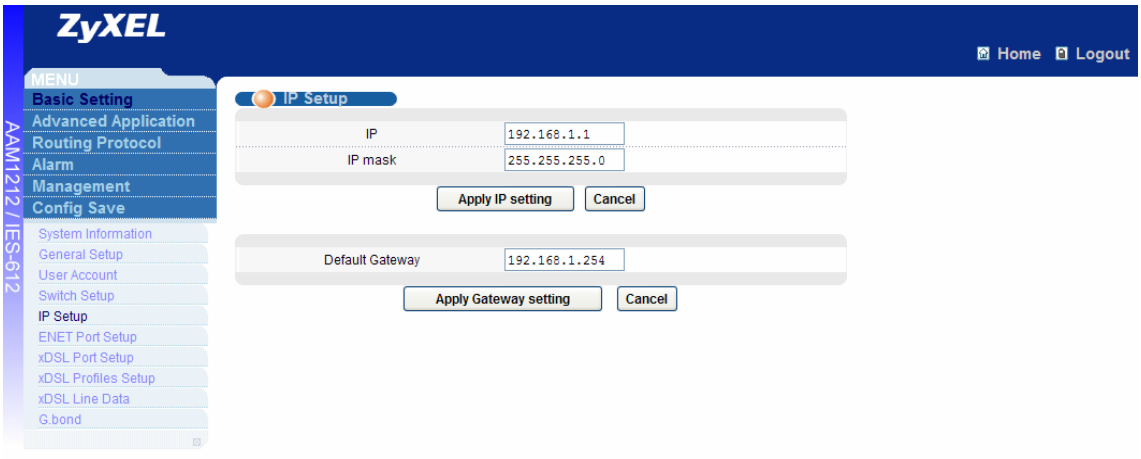


Figura 18. 28 Interfaz de configuración del direccionamiento

22) En el mismo submenú, seleccione la opción User Account para configurar las contraseñas de las personas que tendrán acceso al equipo, así como el grado del privilegio que tendrán las mismas.

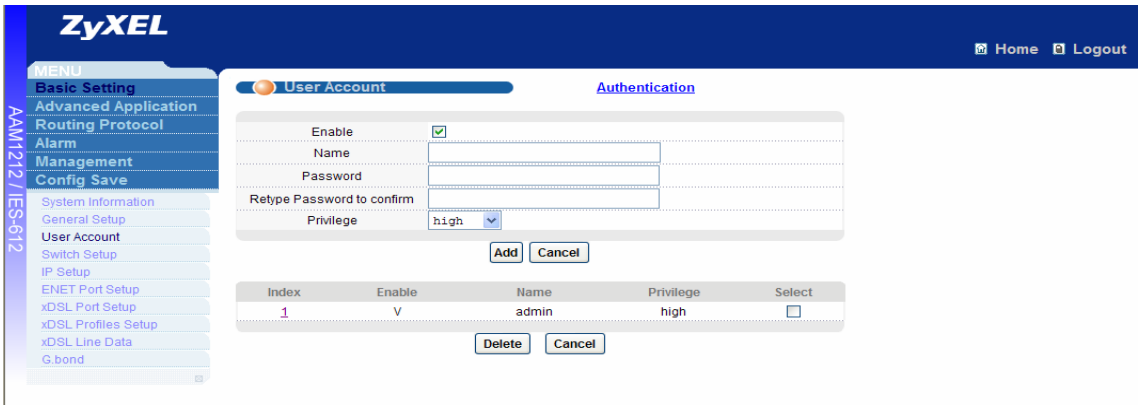


Figura 18.29 Interfaz de configuración de los usuarios

23) A continuación en el menú principal seleccione la opción Advance Application.

24) En el submenú seleccione la opción Access Control.

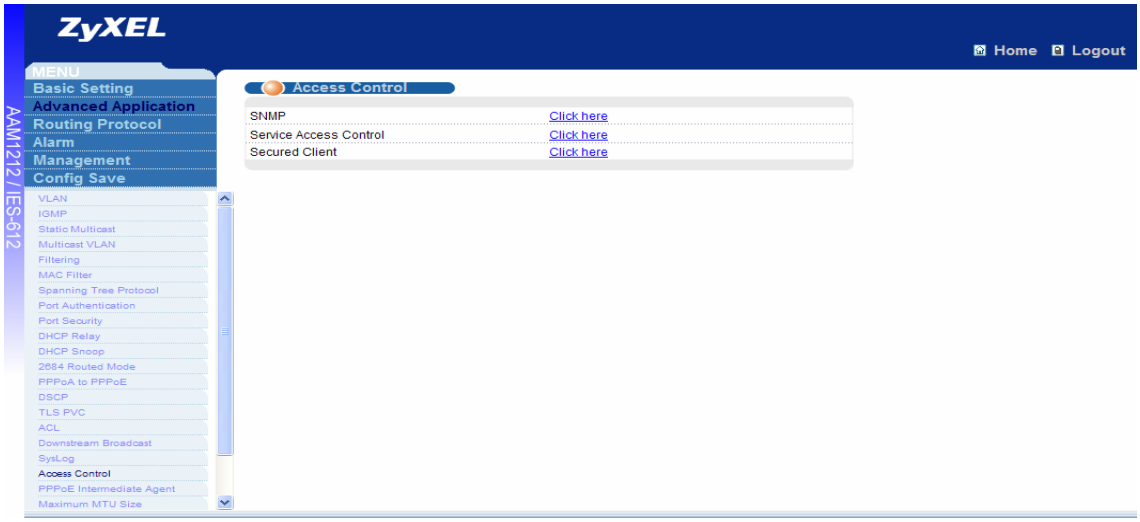


Figura 18.30 Interfaz de control de acceso

25) Ahora en la pantalla principal seleccione la opción SNMP. En Trap Destination 1 configure la dirección ip del server que realizará la gestión del equipo configurado.

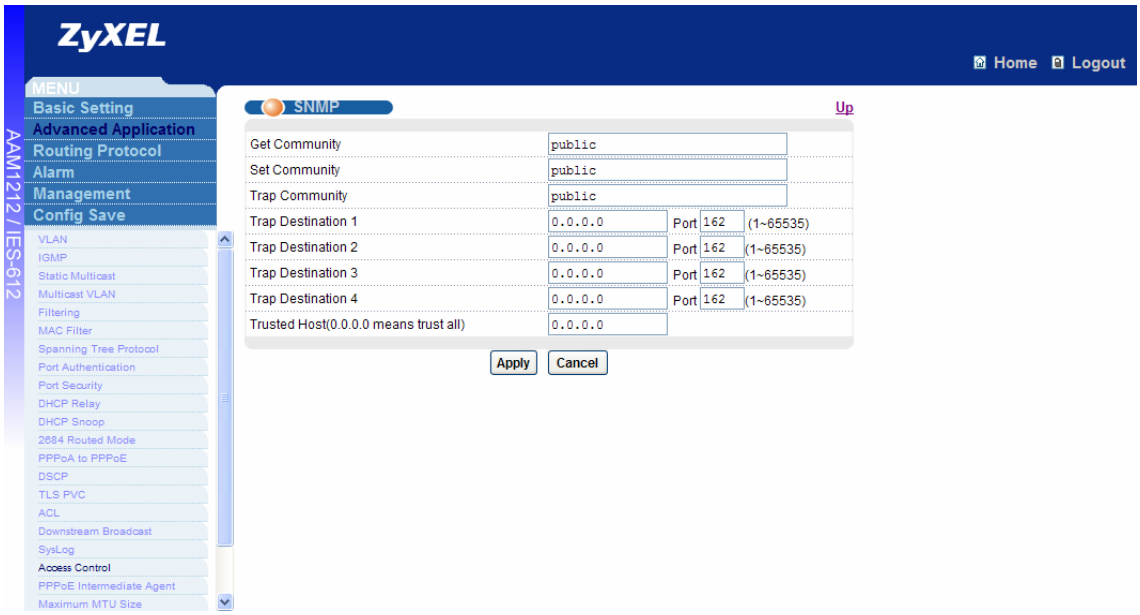


Figura 18.31 Interfaz para la configuración de la conexión con el server

26) Una vez configurado todos los parámetros anteriores guarde la configuración en el menú principal en la opción Config Save.

27) Nuevamente se abre un submenú en el cuál se encuentra la única opción Save.

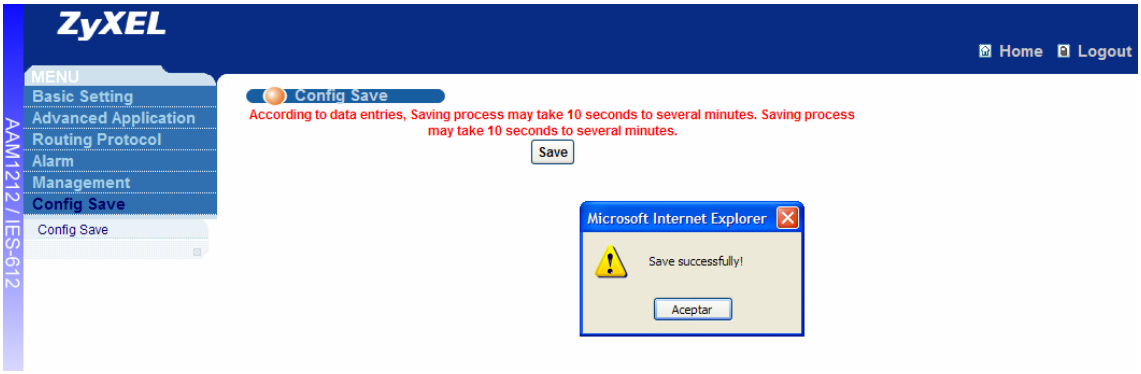


Figura 18.32 Interfaz de salvar configuración

28) Para finalizar se debe de aceptar la confirmación que se mostrará en la pantalla.

CPE

Figura 18.33 CPE

1) Primero presione el botón de Reset del CPE durante 30 segundos y luego continúe con los siguientes pasos.

2) Conectar el cable de red a cualquiera de los puertos LAN del 2 al 4 CPE.

3) Configurar la dirección IP de la tarjeta de red de la computadora, para que sea parte de la dirección de acceso por defecto que trae el equipo.

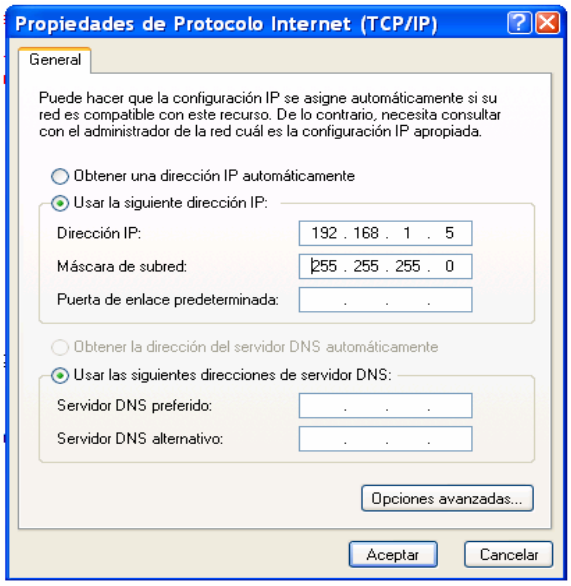


Figura 18.34 Interfaz de configuración de la dirección IP en la computadora

4) Para configurar el equipo es necesario ingresar la dirección 192.168.1.1 en el navegador, el equipo cuenta con una contraseña predeterminada para su configuración la cual es 1234**.** Después se debe de dar click en el botón Login.

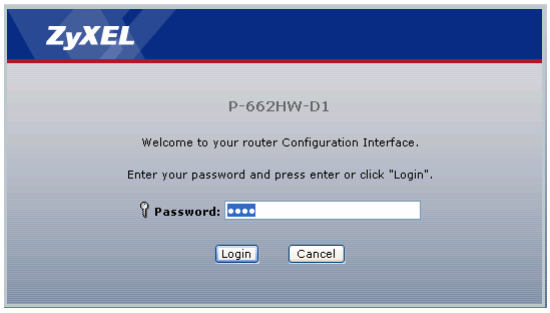


Figura 18.35 Interfaz de ingreso al equipo

5) Se cambia la contraseña que el equipo trae por defecto por la contraseña que se le dará al equipo y se le da click sobre Apply. Este paso se efectuará cada vez que al equipo se le aplique el reset únicamente.

Figura 18.36 Interfaz de cambio de contraseña del equipo

6) Luego se muestra una pantalla donde nos preguntan si queremos cambiar el certificado de fabrica en este caso hacemos un click en Ignore

Figura 18.37 Interfaz de reemplazo del certificado del equipo

7) A continuación se muestra el menú para iniciar con la configuración del equipo. Se selecciona la opción Go to Advance Setup.

Figura 18.38 Interfaz de selección para el ingreso al equipo

8) Se muestra el status del cpe una vez que se selecciono la configuración avanzada.

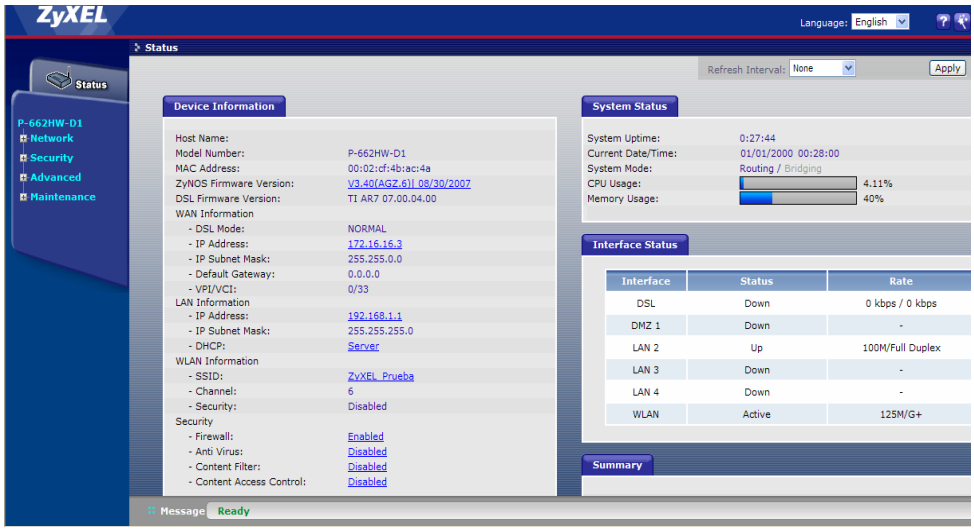


Figura 18.39 Interfaz del estado del equipo

9) En el menú Network, se selecciona la opción WAN del submenú. La configuración del apartado general se muestra a continuación:

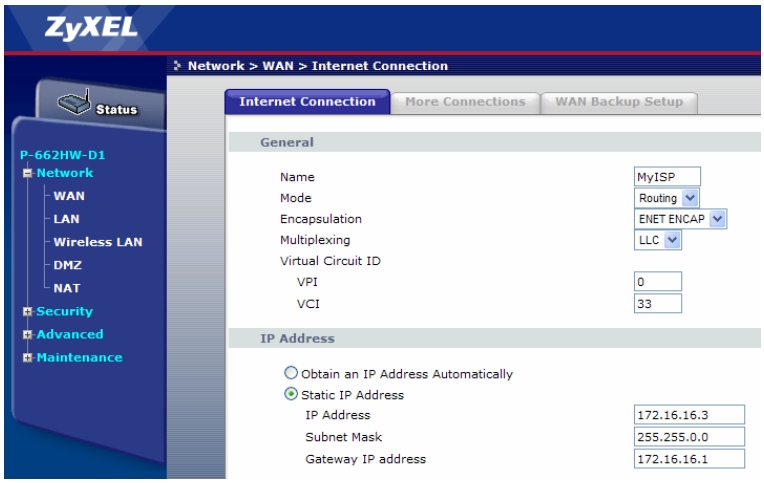


Figura 18.40 Interfaz de configuracción de la WAN del equipo

10) Para finalizar se debe de configurar estos requerimientos, en el apartado de IP Address se debe de seleccionar la opción Static IP Address y configurar la dirección ip, la máscara de subred y la puerta de enlace del equipo.