ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESTUDIO DE UN SISTEMA DE GESTIÓN DE REDES USANDO EL PROTOCOLO SNMP"

TESIS DE POSTGRADO

Previa a la obtención del Título de:

MAGÍSTER EN TELECOMUNICACIONES

Presentado por:

Ing. Juan Pablo García Baquerizo

GUAYAQUIL – ECUADOR

AÑO

2013

A G R A D E C I M I E N T O S

Quiero agradecer a DIOS, al ESPÍRITU SANTO, a mi esposa María Elena, a todos los que han confiado en mí, a mis maestros y al Ing. César Yépez, por su dirección y apoyo en esta Tesis.

Juan Pablo García Baquerizo

D E D I C A T O R I A

A Dios, a mis padres, Rosa Amelia y Miguel, por su amor y dedicación, a mi hijo, Juan Pablo, a mi esposa, María Elena, por su apoyo incondicional.

Juan Pablo García Baquerizo

TRIBUNAL DE SUSTENTACIÓN

_____

ING. CÉSAR YÉPEZ FLORES
DIRECTOR DE TESIS

_____

ING. PATRICIA CHAVEZ BURBANO
VOCAL TRIBUNAL DE GRADUACIÓN

_____

DR. BORIS VINTIMILLA
SUBDECANO DE LA FIEC

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

(Reglamento 4256 TITULO IV Capítulo II Art. 18 literal c)

Ing. Juan Pablo García Baquerizo

RESUMEN

El presente estudio muestra los beneficios que el Protocolo de Administración Simple de Redes (SNMP) proporciona a un “Sistema de Gestión de Redes”, implementado en una institución para el control de un centro de cómputo, conmutadores, enrutadores, enlaces y otras funciones como la gestión de impresión, climatización, etc. El Sistema de Gestión se complementa con el uso de herramientas de monitoreo y con acciones de mensajería generados por las alarmas configuradas en los agentes.

Se presenta el análisis del uso del protocolo en algunas aplicaciones de la Junta de Beneficencia de Guayaquil, y en función de los resultados obtenidos se establece la importancia de tener una herramienta de control para la operación y monitoreo de los centros de cómputo y del hardware relacionado, así como determinar las ventajas de estas implementaciones. El sistema obtiene logs de eventos, que permiten realizar el análisis de los datos obtenidos a través de los agentes y visualizar la información en la consola del administrador con gráficos en línea, que facilitan la lectura de las variables de interés y la revisión del comportamiento de los dispositivos que integran las soluciones de IT.

Se espera que el análisis oportuno de los eventos, junto con el estudio de las variables que alteran el funcionamiento normal, permita la reducción de los incidentes, del tiempo de respuesta y de la solución; e incremente la disponibilidad de los servicios dentro de la institución. Además se presenta, una política general para el “Sistema de Gestión de Redes”, junto a conclusiones y recomendaciones del análisis realizado, proporcionando una base para estudios posteriores.

Este trabajo busca documentar, con ejemplos, el uso de la tecnología que soporta el protocolo SNMP como solución eficaz en la gestión y en el control de redes y motivar al personal de TI en la aplicación de políticas de control y monitoreo, sin incrementar sus costos, mejorando los tiempos de respuesta.

ÍNDICE GENERAL

CAPÍTULO 3
RED DE DATOS

CAPÍTULO 4
DISEÑO DE LA SOLUCIÓN

CAPÍTULO 5
ANALISIS DE RESULTADOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

TABLA DE ABREVIATURAS

AA: Aire Acondicionado

AC: Corriente Alterna

AP: Punto de acceso

ASN: Notación de Sintaxis Abstracta

BD: Base de Datos

BTU: Unidad térmica Británica

CPU: Unidad de Procesamiento Central

DoS: Denegación de Servicio

DSP: Procesamiento de señales digitales

FTP: Protocolo de transferencia de archivos

GE: General Electric

HMI: Interfaz Hombre Máquina

HP: Hewlett Packard

HTML: Lenguaje de Marcado de Hipertexto

HTTP: Protocolo de Transferencia de Hipertexto

IETF: Grupo de Tareas de Ingeniería de Internet

IP: Protocolo de Internet

ISO: Organización Internacional para la Normalización

JBG: Junta de Beneficencia de Guayaquil

LAN: Red de Área Local

MAC: Control de acceso al medio

MAN: Red de Area Metropolitana

MB: Mega Byte

MIB: Base de Información de Administración

MTBF: Tiempo medio entre fallas

NGN: Redes de nueva generación

NMS: Sistema Administrador de Red

NOC: Centro de operación de la red

N-QAM: Modulación de amplitud en cuadratura

OID: Identificador de Objeto

OFDM: Multiplexación por División de Frecuencia Ortogonal

OSPF: Protocolo de la ruta abierta más corta

PDU: Unidad de datos de protocolo

PoE: Energia sobre ethernet

PRTG: Graficador de trafico de enrutadores Paessler

QPSK: Modulación por movimiento de fase en cuadratura

RF: Radio Frecuencia

RFC: Petición De Comentarios

RIP: Protocolo de Información de enrutamiento

ROM: Memoria de Lectura

RRD: Base de Datos Round Robin

SAN: Red de Almacenamiento

SCADA: Supervisión, control y adquisición de datos

SGMP: Protocolo de Monitoreo de Puerta de Enlace Simple

SLA: Acuerdo de nivel de Servicio

SNMP: Protocolo Simple de Administración de Red

SMN: Sistema de Administración de red

SQL: Lenguaje de consulta estructurado

TCP: Protocolo de Control de Transmisión

TI: Tecnología de la información

UDP: Protocolo de Datagrama de Usuario

UPS: Unidad de Sistema de Potencia

Vin: Voltaje de entrada

VLAN: Redes Locales virtuales

VoIP: Voz sobre IP

Vout: Voltaje de salida

W: Vatios

WAN: Red de Área Extensa

WWW: Red Infórmatica Mundial

XML: Lenguaje de marcas extensible

INTRODUCCIÓN

En muchos casos la plataforma de TI instalada no es administrada y opera sin los debidos controles, ocasionado inconvenientes en los procesos e interrupciones de servicio, que en la mayoría de los casos produce pérdidas económicas y caída de los negocios. Pero ello, no sucede por que no existan las herramientas para evitarlo, sino porque se desconoce su correcto uso.

Por eso se busca analizar las diversas opciones para el registro, supervisión y control de eventos e incidentes basados en el protocolo SNMP, con la ayuda de aplicaciones gráficas que facilitan la lectura y observación de los datos en la red. A su vez toda la información recopilada y analizada sirve para el establecimiento de políticas de control que permitan mantener la disponibilidad de los servicios de comunicación.

CAPÍTULO 1

DESCRIPCIÓN DEL PROBLEMA

Los servicios de TI, en los que se basan las operaciones de las empresas, se realizan en muchos casos sin la adecuada administración y control que aseguren el buen funcionamiento y la estabilidad de los procesos del negocio. Por eso se hace un estudio de los antecedentes, objetivos y modelo propuesto para la administración de un Sistema de Control de Redes.

1.1 Antecedentes

La importancia de mantener la disponibilidad de los servicios, de asegurar el acceso a los datos y de garantizar la integridad de los mismos, implica el establecimiento de políticas y procesos que aseguren la adecuada operación de las redes. La protección de los datos y de los equipos que los contienen es una de las preocupaciones de toda organización y sobre todo del personal de

TI (Tecnología de la Información), más aún en lo que se refiere a la información almacenada en los servidores de los centros de cómputo.

Para mantener la confiabilidad de la red y la disponibilidad de los servicios se establecen controles y políticas de mantenimiento que el área de gestión de la operación administra, lo que de por si permitiría evitar pérdidas y daños. Entre algunos procesos importantes encontramos el control de los UPS, enlaces entre dependencias, enrutadores, conmutadores, etc., para lo cual se debe implementar un sistema eficiente y confiable. Para ello se puede aprovechar los mecanismos de control, gestión y estadísticas del protocolo SNMP, que la mayoría de los equipos disponen, y que permiten estudiar el comportamiento de las redes y los parámetros de los equipos conectados a la red, para establecer medidas de prevención de fallas así como procesos de operación.

1.2 Justificación

Se pretende realizar un estudio de los beneficios que proporciona el protocolo SNMP para la gestión y el control de la operación de

una Red de Datos, ya que en nuestro medio no se conocen estudios que confirmen las ventajas de la implementación de dicho protocolo, además, el desarrollo de plataformas de servicio con esta tecnología aún no ha sido explotada por las todas las empresas.

Según información facilitada por la empresa Celco, solo el 20% de las empresas en el Ecuador, manejan en algunas de sus oficinas a nivel nacional un servicio de control de redes por SNMP. En la tabla I se puede observar el porcentaje de empresas que por sector comercial usan el protocolo SNMP.

Tabla I Porcentaje de empresas que usan SNMP

Sector comercial	Porcentaje en su sector
Banca	80%
TV	25%
Tecnología	70%
Educación	0%
Sin fines de lucro	60%
Municipios	2%
Comercial	35%
Gobierno	25%

Para nuestro análisis consideramos como fundamentales: los enlaces de comunicación y la administración del centro de cómputo, ya que muchas empresas pierden dinero y tiempo al no

tener herramientas de monitoreo operando en el control de sus centros de cómputo, donde la calidad del servicio dado se mide por el mayor porcentaje de disponibilidad y por el menor tiempo de parada, como se puede apreciar en la tabla II.

Tabla II Disponibilidad de un Centro de Cómputo

Tier	% de Disponibilidad	% Parada	Tiempo de parada en un año
Tier 1	99.671	0.329	28.82 horas
Tier 2	99.741	0.251	22.68 horas
Tier 3	99.982	0.018	1.57 horas
Tier 4	99.995	0.005	52.56 minutos

La caída de la red debido a una falla de energía eléctrica, un daño en un UPS, un enrutador, etc., puede incrementar los tiempos de parada y como consecuencia disminuir la disponibilidad de los servicios, que para empresas que ofrecen un sistema 24*7 resulta crítico.

1.3 Objetivos

1.3.1 Objetivo General

Estudiar los beneficios que se obtienen en la Gestión de la Operación de una Red de Datos a través del protocolo SNMP.

1.3.2 Objetivos específicos

1. Analizar los procesos de control en una Red de Datos usando el protocolo SNMP.

2. Estudiar los beneficios que se obtienen en la Gestión de la Operación de una Red de Datos a través del uso de software basado en protocolo SNMP. (Cacti, Scada, PRTG, etc.).

3. Medir las variables que se presentan y que deben someterse al control de la Gestión de la Operación.

4. Análisis de la eficacia de la implementación del protocolo SNMP para la gestión de la operación de la Red.

5. Establecer políticas de control a partir de los estudios de los beneficios del protocolo SNMP que mejoren la gestión de operación de la red.

1.4 Planteamiento del problema

La pérdida de los servicios de red se puede medir en función del tiempo que toma la recuperación del negocio y las pérdidas económicas que se generan, las cuales ocasionan un efecto dómino al afectar a los clientes de empresas de servicio crítico. Esto puede traer consigo sanciones para las empresas que ofrecen servicio de telefonía móvil e internet, así como problemas en las transacciones que se realizan en línea o en el respaldo de cualquier tipo de información de una sede de negocios a su matriz. Por ello es importante medir las variables que tienen relación con el buen funcionamiento de la red y monitorear cada dispositivo que permita la comunicación, sobretodo aquellos equipos considerados críticos en el negocio. Esto permitirá la implementación de políticas de control y de contingencia dentro de las organizaciones.

Para administrar dichos procesos de control es necesario utilizar un sistema de gestión de redes a través del uso de software basado en algún protocolo de comunicación, como por ejemplo Cacti, Scada, PRTG, etc., que usan el estándar SNMP para administrar de manera sencilla y segura la red.

1.5 Modelo propuesto para la solución

El control y monitoreo de los sistemas de red se hace usando el protocolo SNMP, se utilizan agentes instalados en la máquinas administradas, que recaban toda información especificada en el estándar SNMP, que luego es concentrada en el centro de administración y presentada en un ambiente Web.

Se realiza el estudio de casos (revisión de incidentes en detalle) y el análisis de resultados obtenidos de las lecturas de los log, en las gráficas de los distintos parámetros y en las tablas de datos, lo que permite establecer planes y políticas de contingencia para mejorar la Gestión de la Operación de la Red de Datos.

Se analizan algunas aplicaciones de software relacionados con el control de los parámetros que son de interés del gestor de operaciones y se comparan sistemas que manejen el protocolo SNMP contra sistemas que no lo poseen para establecer con mayor claridad sus beneficios.

CAPÍTULO 2

PROTOCOLO SNMP

Es un protocolo de la capa de aplicación, utilizado para la gestión de redes, que permite monitorear y controlar los dispositivos en la red. Se basa en paquetes UDP, protocolo de la capa de transporte, basado en IP, compatible con SNMP. UDP es un protocolo sin conexión que no garantiza la entrega del paquete. Se puede apreciar la arquitectura en la figura 2.1

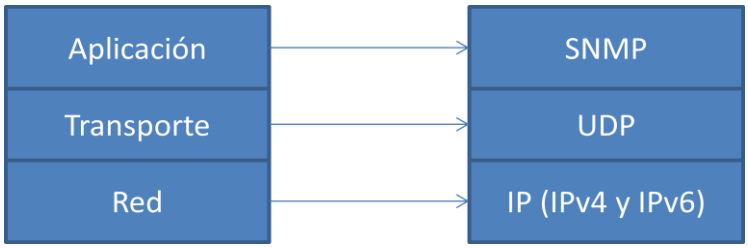


Figura 2.1 Ubicación en la pila de protocolos

SNMP está basado en el modelo agente/administrador, que consiste de un agente, un administrador y una base de datos de la administración de la información (MIB), objetos gestionados y protocolos de red [1]. El

administrador provee la interfaz entre el gestor humano y el sistema, el agente proporciona la interfaz entre el administrador y el equipo físico que se está gestionando, ambos utilizan la base MIB para obtener la información.

2.1 Versiones

SNMP es una extensión del protocolo SGMP, que era el estándar recomendado para Internet. Actualmente existen tres versiones del protocolo:

2.1.1 SNMPv1 RFC1157 (1990)

Constituye la primera definición e implementación del protocolo SNMP, descrito en las RFC 1155, 1157 y 1212 del IETF. Su diseño se presenta como una solución temporal para los problemas de comunicación de los años 80, cuando los sistemas de control eran propietarios y dependían de cada fabricante, complicando el control de las redes heterogéneas y encareciendo los costos debido a que el mercado era restringido. En la figura 2.2 se puede observar la plataforma de trabajo de SNMPv1.

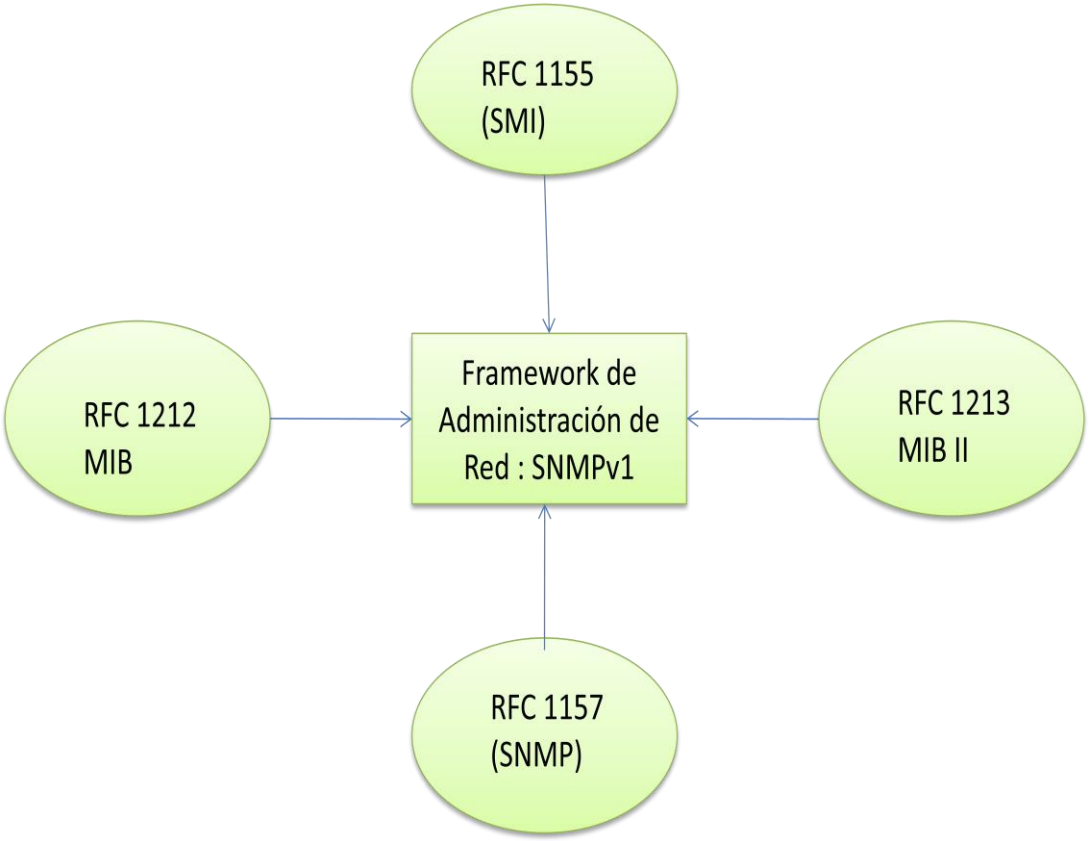


Figura 2.2 Protocolo SNMP, Referencia http://www.gsic.uva.es

2.1.2 SNMPv2

Aparece en 1993, se lo define en las RFC 1441-1452, puede leer SNMPv1, introduce mejoras de seguridad, mayor detalle en la definición de variables, operaciones con grandes volúmenes o GetBulk, comunicación entre administradores a través de Inform, mejora en las Adquisiciones y en la Monitorización de datos.

2.1.3 SNMPv3

Aparece en 1997, se lo describe en las RFC 1902-1908 y 2271-2275, presenta mejoras en las características de seguridad como privacidad, autenticación y autentificación. Además usa lenguajes orientados a objetos.

No se trata de que SNMPv3 reemplace a SNMPv1 y/o SNMPv2, sino que definiendo las capacidades adicionales arriba mencionadas sea utilizada en unión de SNMPv2 (preferiblemente) o SNMPv1.

2.2 Componentes básicos de SNMP

Los componentes básicos son: agentes, administradores y la base de información de administración. Ver figura 2.3

Agentes: Es el software que facilita el acceso a la información, provee la información referente a los problemas y realiza actualizaciones.

Administradores: El equipo administrador, a través del software se encarga de enviar y recibir los mensajes SNMP.

Base de información de administración: La MIB es la base que contiene la información del estado del sistema, las estadísticas de rendimiento y los parámetros de configuración.

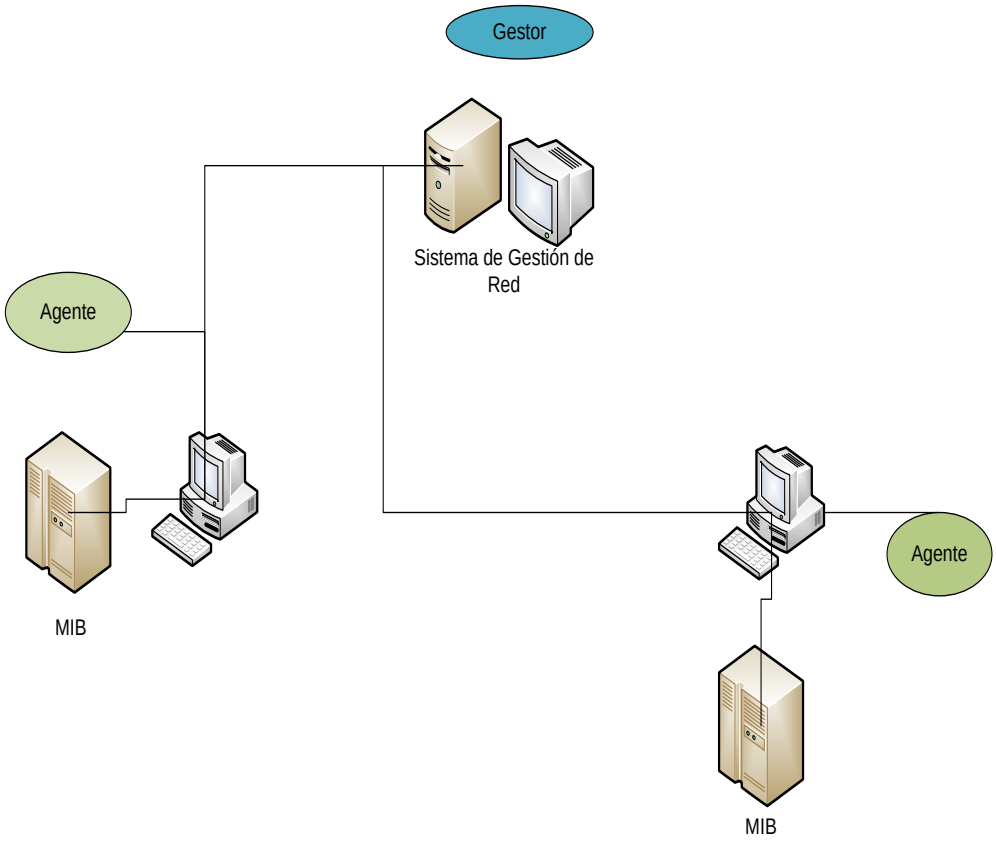


Figura 2.3 Componentes SNMP

2.3 Base de información de administración (MIB)

Es una base de información gestionada, a través de la cual se obtienen los identificadores de objetos OID, dados por la IETF para las aplicaciones SNMP.

El MIB está escrito en notación ASN.1. (Las siglas corresponden a Abstract Syntax Notation 1). Es una notación estándar mantenida por la ISO (Organización Internacional para la Normalización) que proporciona el modelo formal para la definición de los objetos y las tablas de los objetos en el MIB [2].

La ASN.1. reúne las siguientes características: Es legible, está específicamente diseñado para la comunicación entre disímiles sistemas informáticos, así que es el mismo para todas las máquinas. Es extensible, por lo que se puede utilizar para describir casi cualquier cosa y una vez que un término se define en ASN.1, puede ser utilizado para definir otros términos.

Los elementos definidos en el MIB pueden ser muy amplios (por ejemplo, los objetos creados por empresas privadas) o pueden ser muy específicos (como un mensaje de captura especial generado por un punto específico de alarma en una RTU).

2.3.1 Identificador de Objetos (OID)

Un OID es una secuencia de números enteros que identifica de forma única un objeto administrado, mediante la definición de una ruta de acceso a ese objeto a través de una estructura de árbol llamado el árbol OID o un árbol de inscripción. Cuando un agente SNMP necesita acceder a un objeto específico administrado, atraviesa el árbol OID para encontrarlo.

Los OID identifican los objetos de datos que son parte de un Mensaje SNMP. Cuando el dispositivo SNMP envía una trampa o un GetResponse, transmite una serie de OID, junto con sus valores actuales. Ver ejemplo en el Anexo 1.

En la figura 2.4 se puede observar, que al compilar los archivos MIB en el administrador SNMP, se proporcionan no sólo los OID definidos por el equipo de los proveedores, sino también las OID para entidades públicas: iso, org, dod, internet, y así sucesivamente.

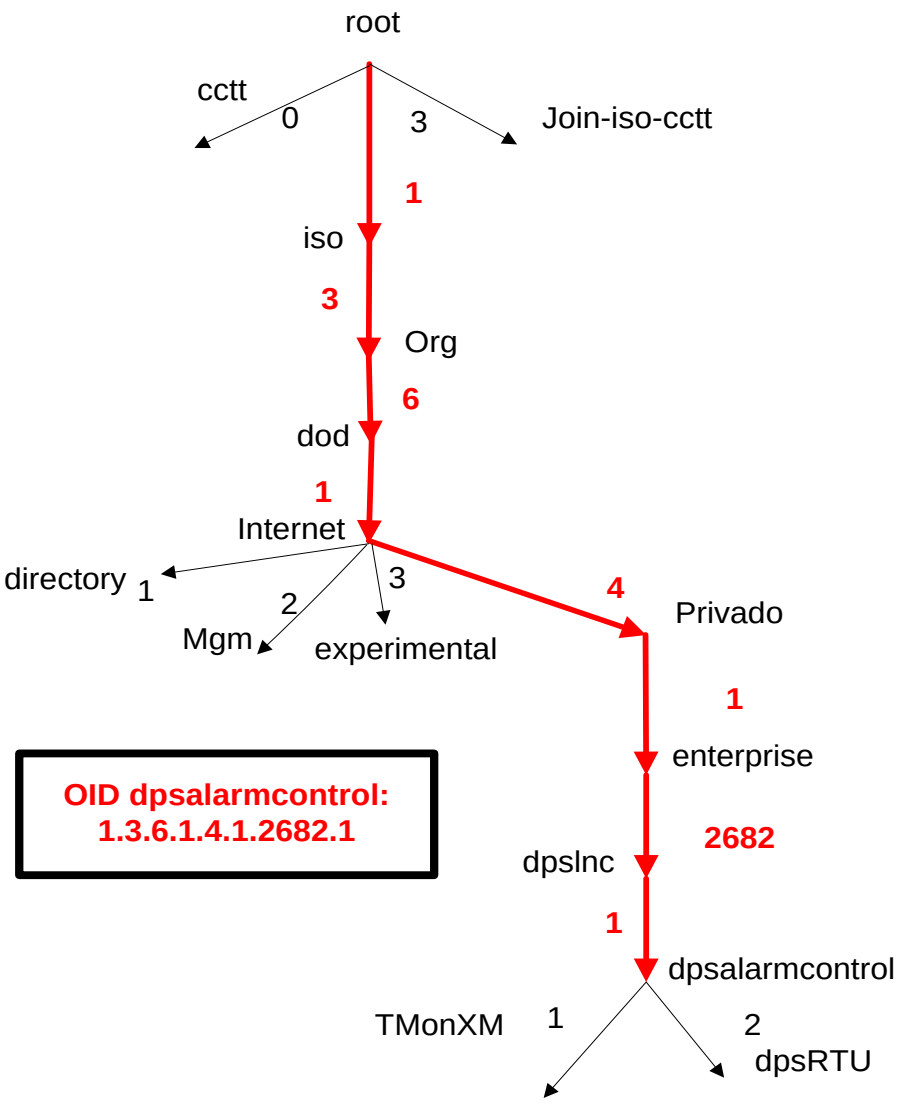


Figura 2.4 Ejemplo de árbol de inscripción. Tutorial MIB DPSTelecom

Los primeros números identifican el dominio de la organización que emitió el OID, seguido por números que identifican los objetos dentro del dominio. De forma similar,

cada OID comienza en el nivel de raíz del dominio y cada vez se vuelve más específico. El último término de un OID, es el elemento más específico. He aquí un ejemplo: 1.3.6.1.4.1.2681.1.2.102:

1 (ISO), la Organización Internacional de Normalización

3 (org): Una organización ISO reconocida.

6 (dod): EE.UU. Departamento de Defensa, la agencia originalmente responsable de la Internet.

1 (Internet): Internet OID.

4 (privado): Las organizaciones privadas.

1 (empresas): Las empresas comerciales.

2682 (dpsInc): DPS Telecom.

1 (dpsAlarmControl): DPS alarma y dispositivos de control.

2 (dpsRTU): unidad de telemetría DPS a distancia.

102 (dpsRTUsumPClr), una trampa generada cuando todos los puntos de alarma en una RTU son claros.

2.3.2 Identificación de un objeto MIB

De acuerdo a la Corporación Oracle [3], las palabras usadas principalmente en la identificación de un objeto son tres: Sintaxis, acceso y descripción.

Sintaxis: Define la estructura de datos abstracta que corresponde al tipo objeto.

Acceso: Define si el valor del objeto solo puede ser recuperado pero no modificado (solo lectura) o si también puede ser modificado (lectura-escritura).

Descripción: Contiene una definición textual del tipo de objeto.

En las figuras 2.5 y 2.6 se observan ejemplos de MIBS de Radios Motorola:

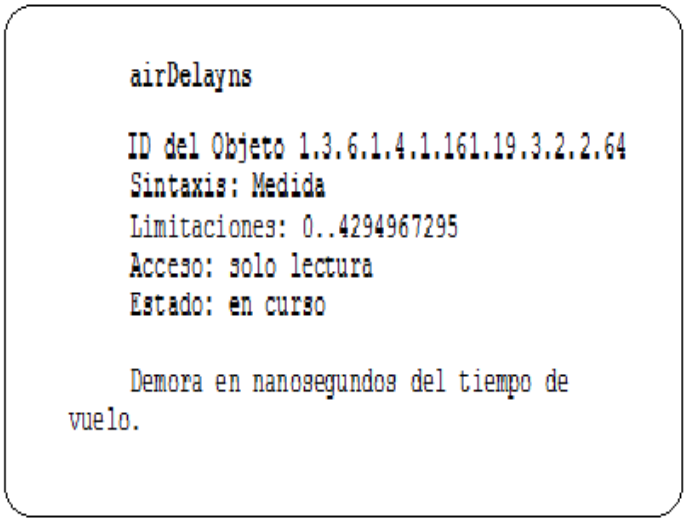


Figura 2.5. MIB Airdelayns Motorola

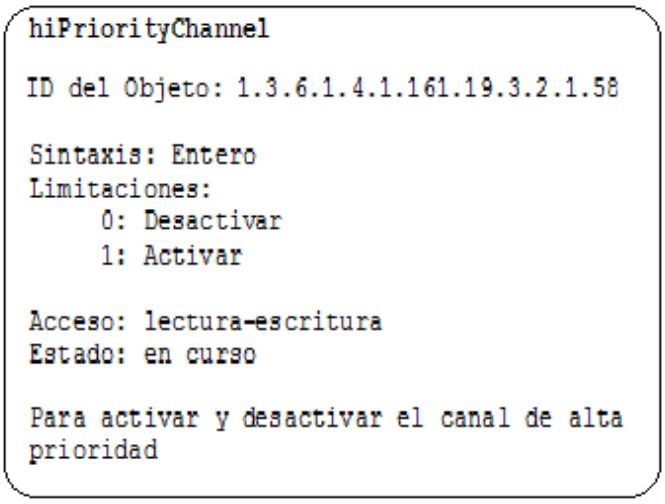


Figura 2.6 MIB Hipriority channel Motorola

2.4 Mensajes Básicos

SNMP utiliza los siguientes mensajes básicos: Get, Get-next, Get Bulk Request, GetResponse, Set, Set next Request, Walk, Trap e Inform Request.

Get: Solicita uno o más atributos de un objeto al agente.

Get-next: Es una petición por un valor en el siguiente objeto en la MIB. Se obtienen los valores sucesivos en la Rama MIB.

Get Bulk Request (en snmp v2): Solicita un conjunto amplio de atributos en vez de solicitar uno a uno

GetResponse: Indica el intercambio ejecutado o por qué no se lo ha podido hacer.

Set: Permite a la estación de gestión alterar el valor de los objetos en el agente.

Set next request: Se actualiza el atributo siguiente de un objeto

Walk: Realiza una serie completa de getnexts automáticamente y se detiene cuando devuelve resultados que no están en el rango del OID especificado originalmente. Ver ejemplo en el Anexo 2

Trap: Permite a un agente notificar a la estación de gestión los eventos significativos, las fallas, como por ejemplo pérdida de la comunicación, caída de un servicio, voltajes fuera de rango, etc.

Inform Request (en Snmp v2): Describe la base local de información de gestión MIB para intercambiar información entre los nodos de administración.

2.4.1 Funcionamiento del proceso

El gestor envía un Get o GetNext para leer una o más variables y el agente responde con la información solicitada. Si se requiere cambiar un valor, el gestor envía un set de cambios que el agente gestiona y confirma que se pueden realizar. Cuando ocurre un evento específico el agente envía un TRAP, el agente comprueba cada MIB para identificar si el objeto es gestionado y será cambiado. En la figura 2.7 se puede apreciar parte del proceso.

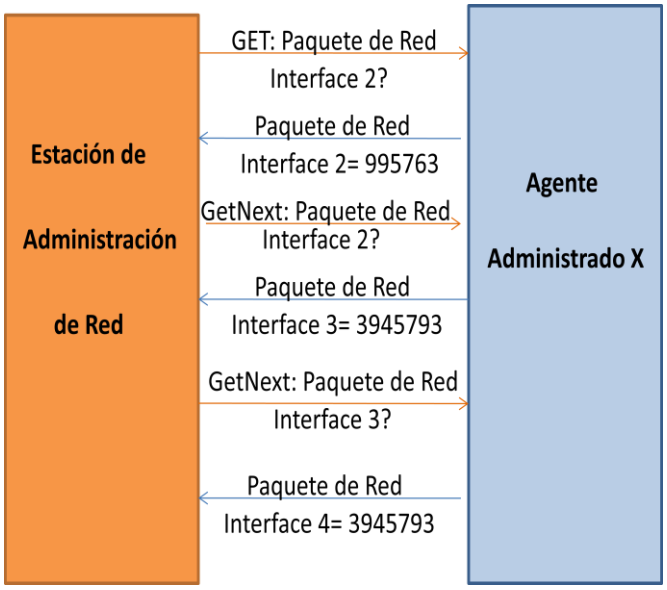


Figura 2.7 Ejemplo de mensajes SNMP. Refencia: Seguridad de la Información [7]

2.5 Tipos de paquetes y estructuras

Las comunidades SNMP están formadas por un agente SNMP y un conjunto de entidades de aplicación SNMP (gestores), las cuales a su vez están conformadas por los elementos de red y las estaciones de gestión que interactúan entre si a través del protocolo SNMP.

SNMP usa un conjunto de reglas, conocidos como esquemas de autenticación para determinar si un mensaje entrante es una petición legítima de un usuario autorizado, o una petición accidental o malintencionada de un usuario no autorizado. Este proceso evita que usuarios que no están autorizados obtengan información o realicen cambios en los parámetros operativos del enrutador. Por lo tanto, el protocolo de autenticación permite que, el agente y el gestor SNMP, ignoren y descarten peticiones de usuarios no autorizados.

La autenticación es muy simple, ya que se define un grupo de nombres de comunidad permitidos para cada elemento de la red, a los cuáles se les asocia: Las direcciones de los gestores de los

que aceptarán peticiones y a los que mandarán alarmas (traps), las variables a las que el nombre de comunidad tiene acceso y el tipo de acceso a las mismas. Cada paquete SNMP recibido por el enrutador será validado o descartado según cumpla o no las restricciones impuestas por el esquema de autenticación. Es decir que, la variable accedida, su tipo de acceso y la dirección IP del origen del paquete SNMP deben ser asociados al nombre de comunidad del paquete SNMP [4].

Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad SNMP y una PDU. Estos datagramas no necesitan ser mayores que 484 bytes, pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores.

La figura 2.8 muestra el formato del paquete. Cada variable de enlace contiene un identificador, un tipo y un valor (si es un conjunto o GetResponse). El agente comprueba cada identificador contra su MIB para determinar si el objeto está gestionado. El

director utiliza su MIB para mostrar el nombre legible de la variable y en ocasiones interpretar su valor [5].

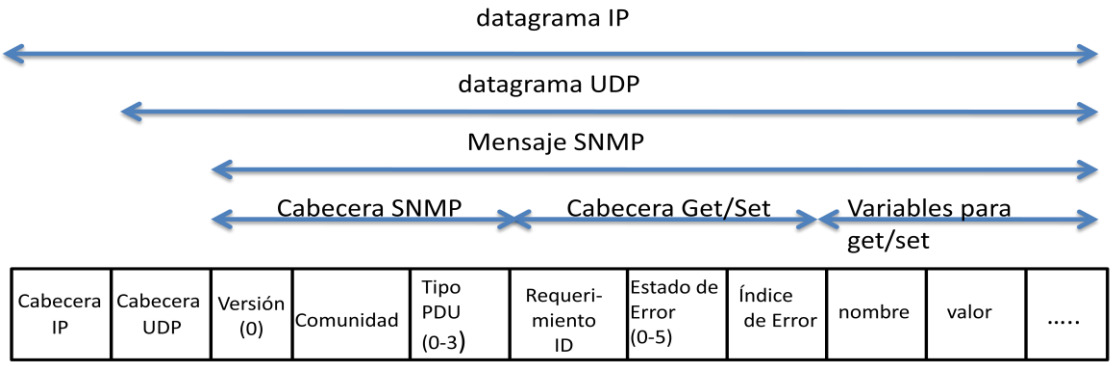


Figura 2.8 Estructura de un paquete SNMP. DPS Telecom, Tutorial SNMP

Una PDU genérica incluye los siguientes datos [6]: ID del requerimiento, Estado del Error, Índice de Errorer y VarBindList.

• ID de requerimiento: Número entero que muestra el orden de emisión de cada datagrama. Con este parámetro también se pueden identificar datagramas duplicados en servicios de datagramas poco fiables.

• Estado de Error: Número entero para indicar si ha existido un error y de que tipo es. Los valores que toma se encuentran en la tabla III.

Tabla III: Tipos de errores que se presentan

Nombre	Número	Función
noError	0	No existe error
tooBig	1	Demasiado grande
noSuchName	2	Sin nombre
badValue	3	Valor Erroneo
readOnly	4	Solo lectura
genErr	5	Error generado

• Índice de Errores: Entero que en caso de presentarse un error proporciona la variable que ha generado ese error.

• VarBindList: Es una lista de nombres de variables con su valor asociado. A veces los PDU quedan definidos sólo con los nombres, pero aún así deben llevar valores asociados. Para estos casos se prefiere definir un valor NULL.

2.5.1 GetRequest-PDU y GetNextRequest-PDU

Son PDU's utilizados para que la entidad destino proporcione los valores de ciertas variables. En el caso de GetRequest-PDU las variables solicitadas se encuentran en la lista VarBindList y en el caso de GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos

de los nombres de las variables de la lista. Por lo que, GetNextRequest-PDU es útil para elaborar tablas de información sobre un MIB. Estas PDU's siempre esperan como respuesta una GetResponse-PDU.

2.5.2 SetRequest-PDU

Solicita a la entidad destino relacionar a cada objeto reflejado en la lista VarBindList con el valor que tiene asignado en dicha lista. Es similar a GetRequest-PDU, salvo por el identificador de PDU. También espera como respuesta una GetResponse-PDU.

2.5.3 GetResponse-PDU

Se genera sólo como respuesta a GetRequest-PDU, GetNextRequest-PDU o SetRequest-PDU. Posee la información solicitada por la entidad destino o una indicación de error.

Las reglas que sigue una entidad de protocolo cuando recibe una GetRequest-PDU, una SetRequest-PDU o una GetNextRequest-PDU, son [6]:

1. Si un nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de GetNextRequest PDU) no coincide con el de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje una GetResponse-PDU idéntica a la recibida, pero con el campo Estado de error con el valor 2 (noSuchName), y con el campo Índice de Errores identificando el nombre del objeto en la lista recibida que ha originado el error.

2. Si se recibe un SetRequest-PDU y el valor de alguna variable de la lista presentada no es del tipo correcto o está fuera del rango, la entidad envía al remitente un GetResponse-PDU idéntica a la recibida, pero con el Estado de Error en el valor 3 (badValue) y el campo Índice de Errores indicando el objeto de la lista que ha generado el error.

3. Si el tamaño de la PDU que se recibió excediera una determinada limitación, la entidad enviará al remitente un

GetResponse-PDU idéntica a la recibida, pero con el campo Estado de Error con el valor 1 (tooBig).

4. Si el valor de un objeto de la lista no pudiera ser obtenido (o alterado, según sea el caso) por un motivo no contemplado en las reglas anteriores, la entidad envía al remitente un GetResponse-PDU idéntica a la recibida, pero con el campo Estado de Error con valor 5 (genErr), y el campo Índice de Errores mostrando el objeto de la lista que ha originado el error.

   Si estas reglas no fueran aplicadas, la entidad enviará al remitente un GetResponse-PDU con las siguientes características:

   - Respuesta a un GetResponse-PDU: Presentará la lista varBindList recibida, con la respectiva asignación del valor correspondiente a cada nombre de objeto.

   - Respuesta a un GetNextResponse-PDU: Proporcionará una lista varBindList con todos los

sucesores lexicográficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "get". Junto a cada nombre, aparecerá su correspondiente valor.

- Respuesta a un SetResponse-PDU: será igual a esta, pero antes la entidad asignará a cada variable mencionada en la lista varBindList su correspondiente valor. Esta asignación se considera simultánea para todas las variables de la lista.

  En cualquiera de estos casos el valor del campo Estado de Error es 0 (noError), igual que el del Índice de Errores. El valor del campo ID del requerimiento es el mismo que el de la PDU recibida.

2.5.4 Trap-PDU

Son generados por el agente que opera en un dispositivo monitoreado, estos mensajes no son solicitados por la consola del administrador y se clasifican según su prioridad (Muy importante, urgente,...), indicando una excepción o

trampa. Estas notificaciones se producen cuando el agente SNMP detecta un cambio de parámetros en las variables MIB.

Los datos que incluye una Trap-PDU son los siguientes: Enterprise, agent-addr, generic-trap, specific trap, time-stamp y variable-bindings.

• Enterprise: tipo de objeto que ha generado la trampa.

• Agent-addr: dirección del objeto que ha generado la trampa.

• Generic-trap: entero que indica el tipo de trampa. Los tipos estándar de trampas mostrados en la Tabla IV [7] y en la figura 2.9, indican los siguientes eventos y valores:

Tabla IV: Trampas estándar

Nombre	Número	Descripción del Evento
Coldstart	0	Agente reiniciado
Warmstart	1	Cambio en la configuración del agente
Linkdown	2	Interfaz de comunicación fuera de servicio (inactiva)
Linkup	3	Interfaz de comunicación en servicio (activa)
Authenticationfailure	4	El agente ha recibido una solicitud de un NMS no autorizado
EGPNeighbortLoss	5	Un equipo cercano a enrutadores que usan el protocolo EGP está fuera de servicio
Enterprise	6	Nuevas traps configuradas por el administrador de la red

• specific-trap: entero con un código específico.

• time-stamp: tiempo desde la última inicialización de la entidad de red y la generación de la trampa.

• variable-bindings: lista tipo varBindList con información de posible interés.

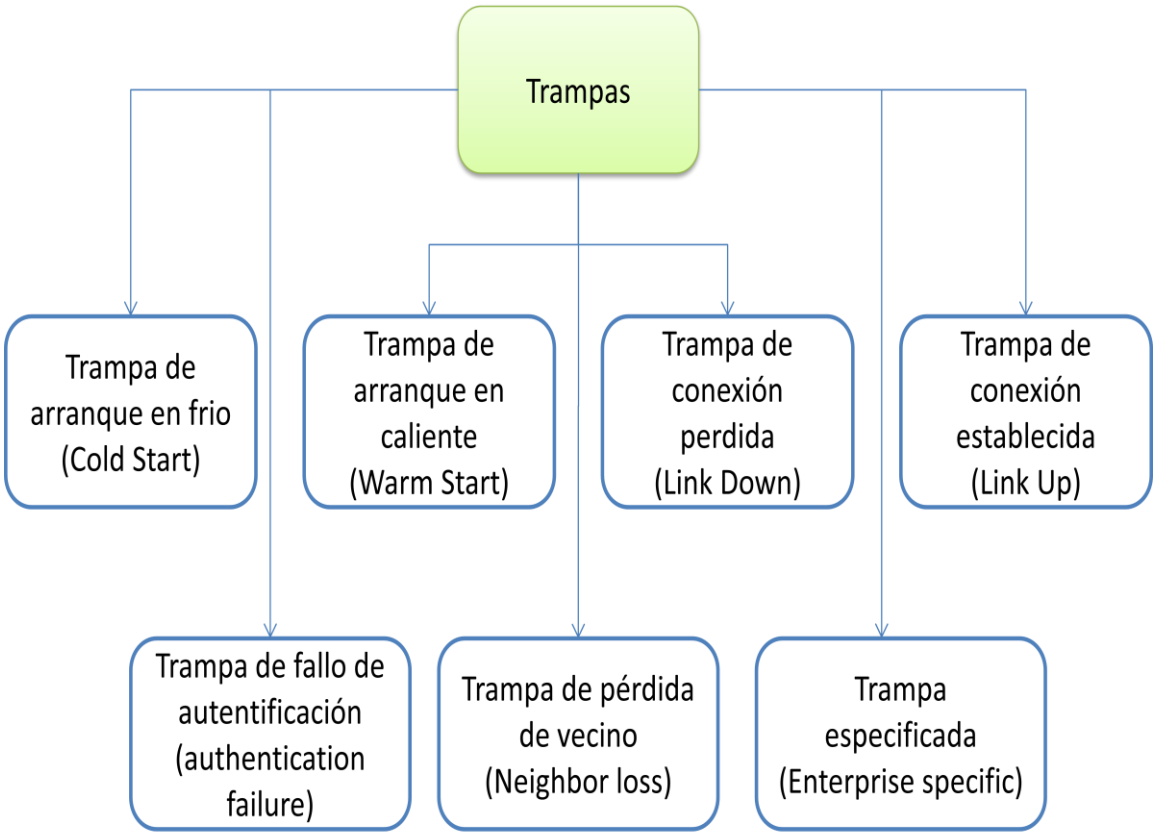


Figura 2.9 Diagrama de Trampas

2.6 Ventajas de SNMP

De acuerdo al tutorial de SNMP [8], existen siete ventajas en el uso de dicho protocolo:

1. Notificaciones de alarmas detalladas que permiten al personal de soporte tomar acciones de inmediato. Incluyen: Lugar, fecha/hora, usuario, evento o incidente y su gravedad. Ver figura 2.10.

2. Notificación inmediata del cambio de estado, incluyendo nuevas alarmas, los cambios se aprecian en la información recibida. Ver figura 2.11.

3. Lista actualizada de las alarmas vigentes. Ver figuras 2.12 y 2.13.

4. Ventanas de mensajes que muestran instrucciones específicas para la toma de una acción apropiada. Los operadores del sistema sabrán que acción tomar y a quien llamar.

5. Localizador y notificaciones por correo electrónico. Ver figura 2.14.

6. Las alarmas y los controles derivados se correlacionan, combinan datos de múltiples entradas y equipos de control de sitios remotos. Ver figura 2.15.

7. Fácil de usar con una interfaz WEB que proporciona acceso rápido a las configuraciones, alarmas de los técnicos, ya sea en portátiles o celulares. Ver figuras 2.16 y 2.17.

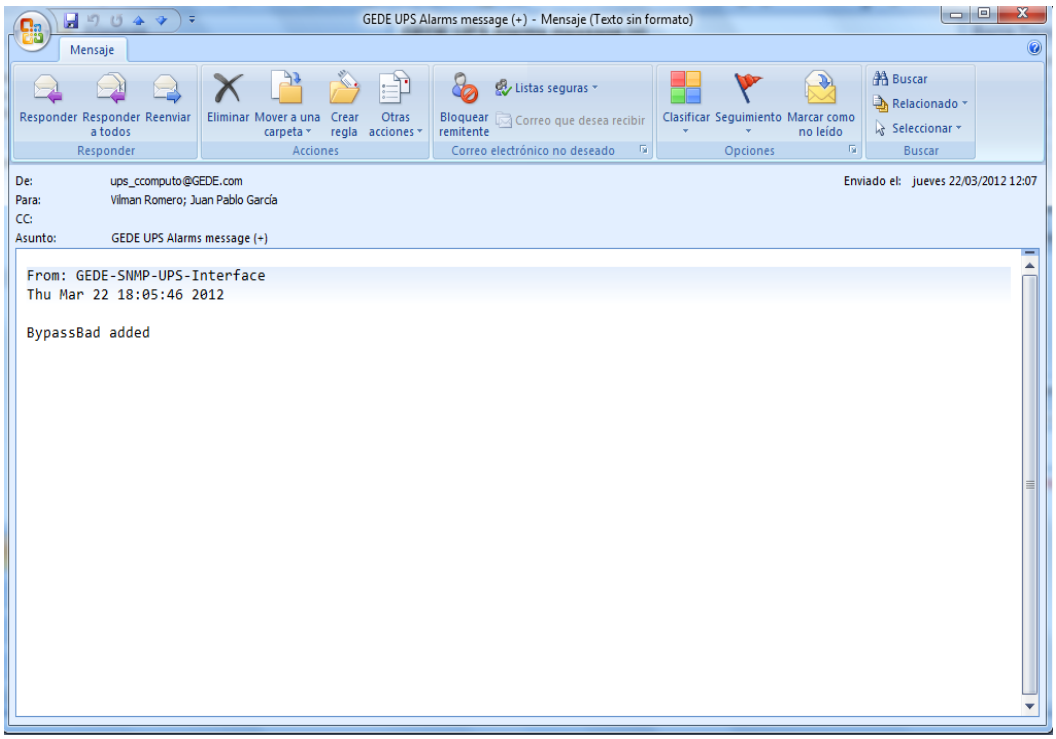


Figura 2.10 Ejemplo de notificación del agente SNMP al personal técnico responsable del mantenimiento del UPS

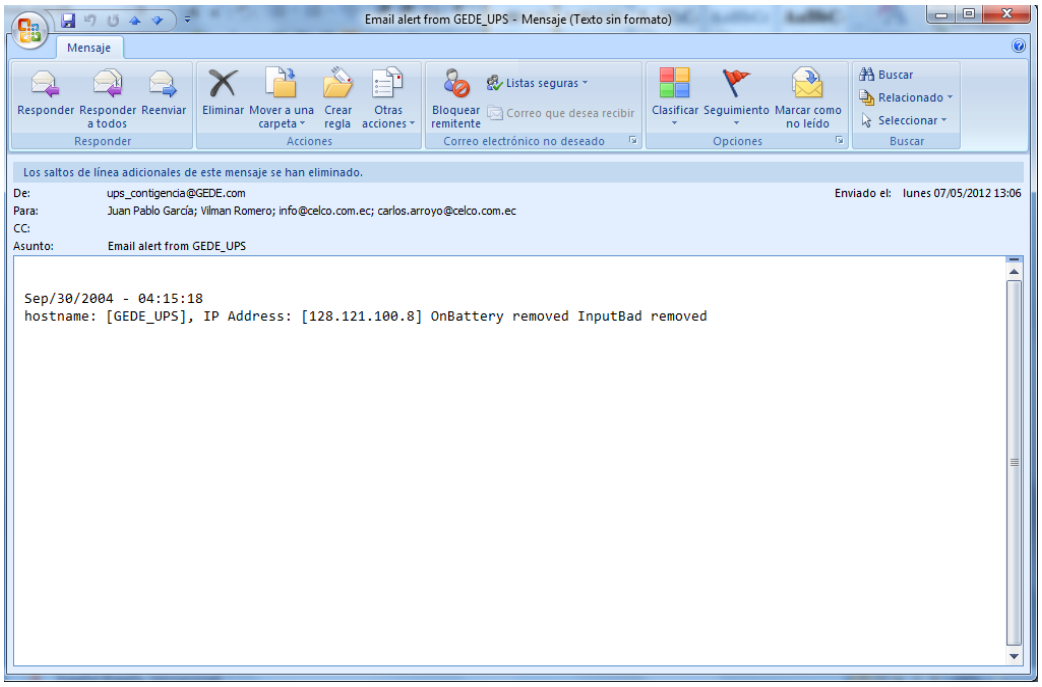


Figura 2.11 Mensaje con el cambio de estado presentado por el UPS GE.

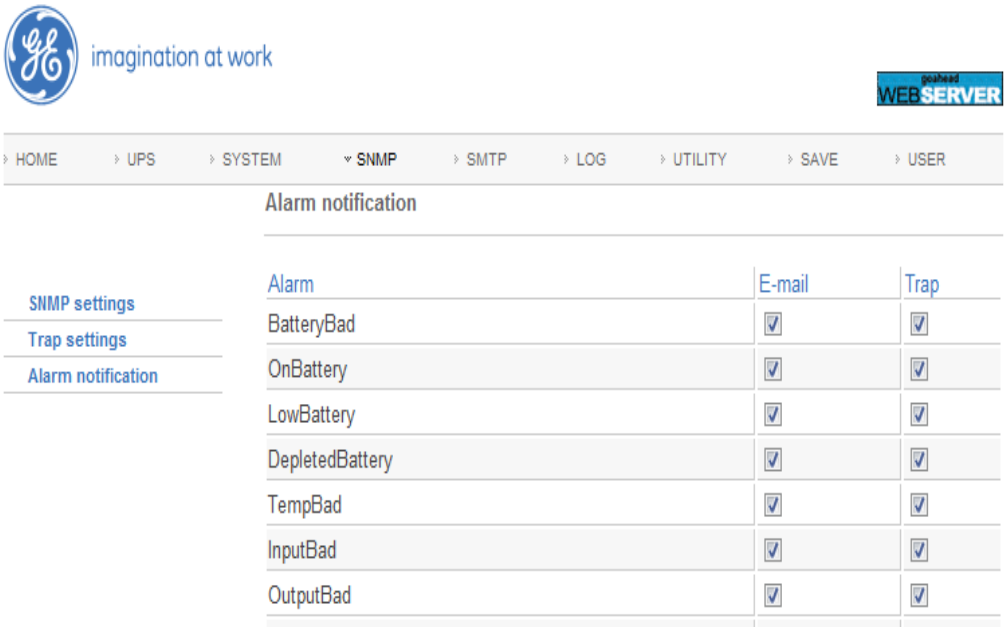


Figura 2.12 Tipos de alarma habilitadas para la mensajería del UPS GE

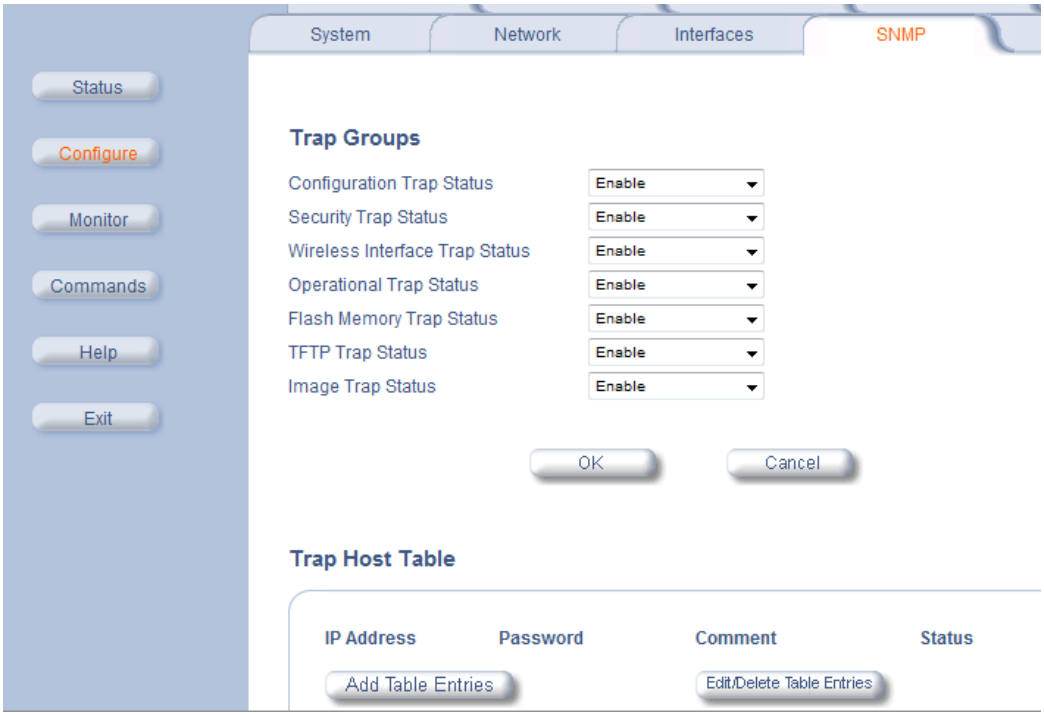


Figura 2.13 Configuración de los Traps de las Radios Tsunami

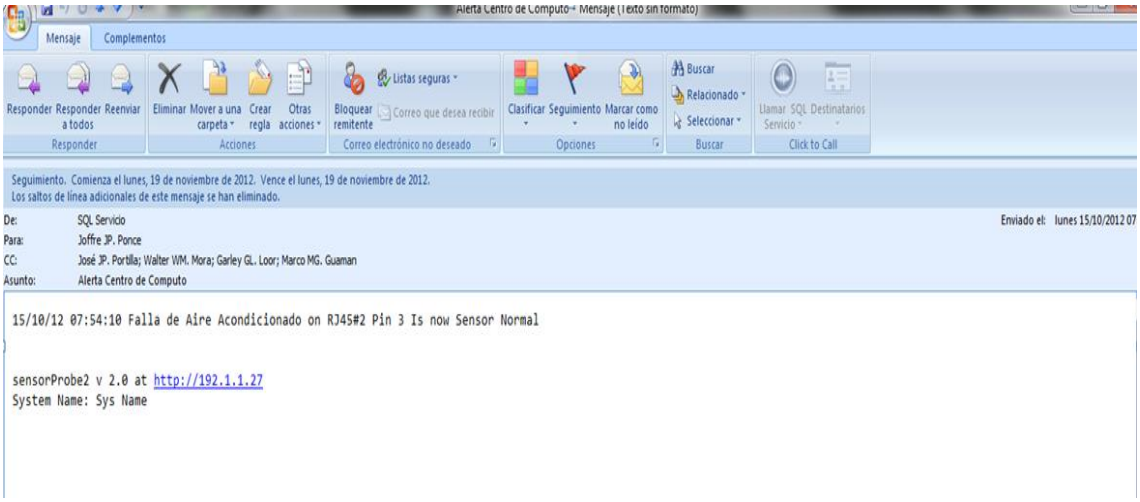


Figura 2.14 ejemplo de notificación de alarma del AA Liebert

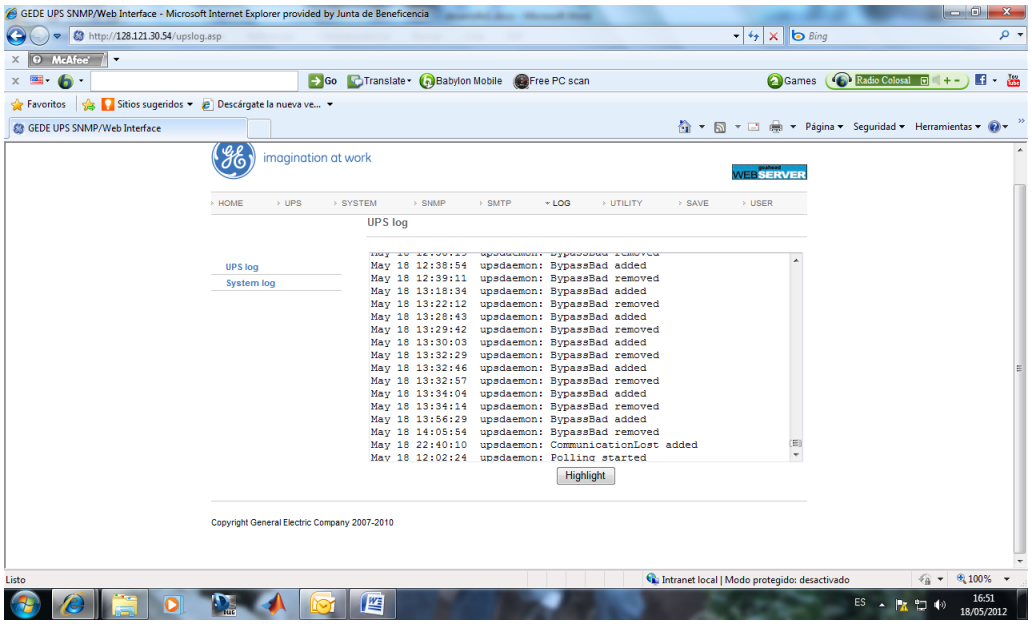


Figura 2.15 Lista de logs del UPS GE

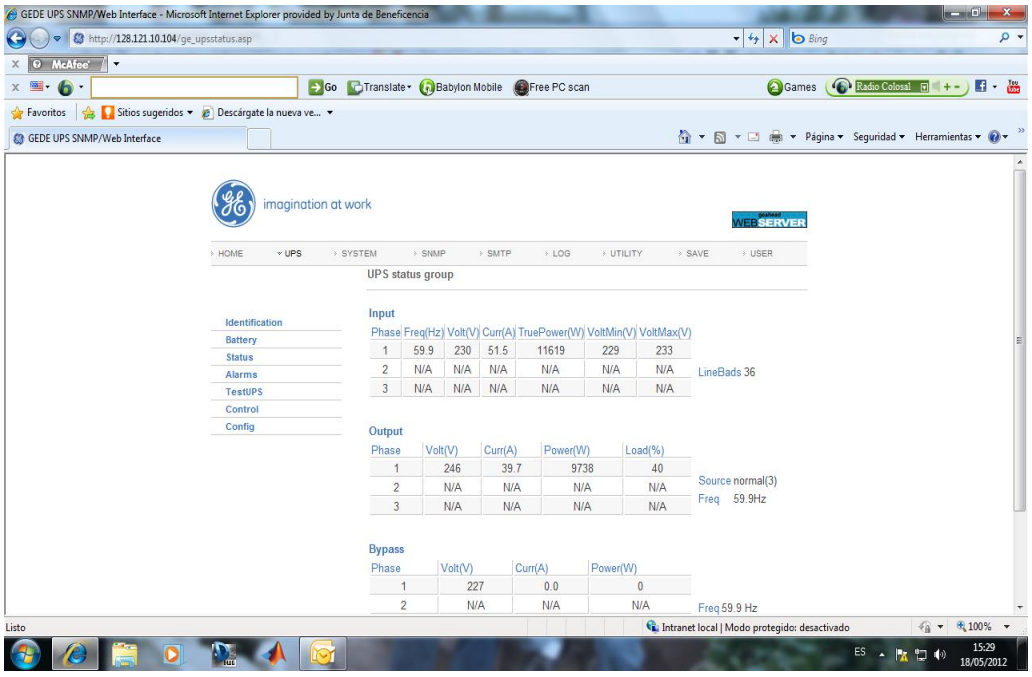


Figura 2.16 Interfaz WEB del UPS GE donde se aprecia los valores de entrada, salida y bypas

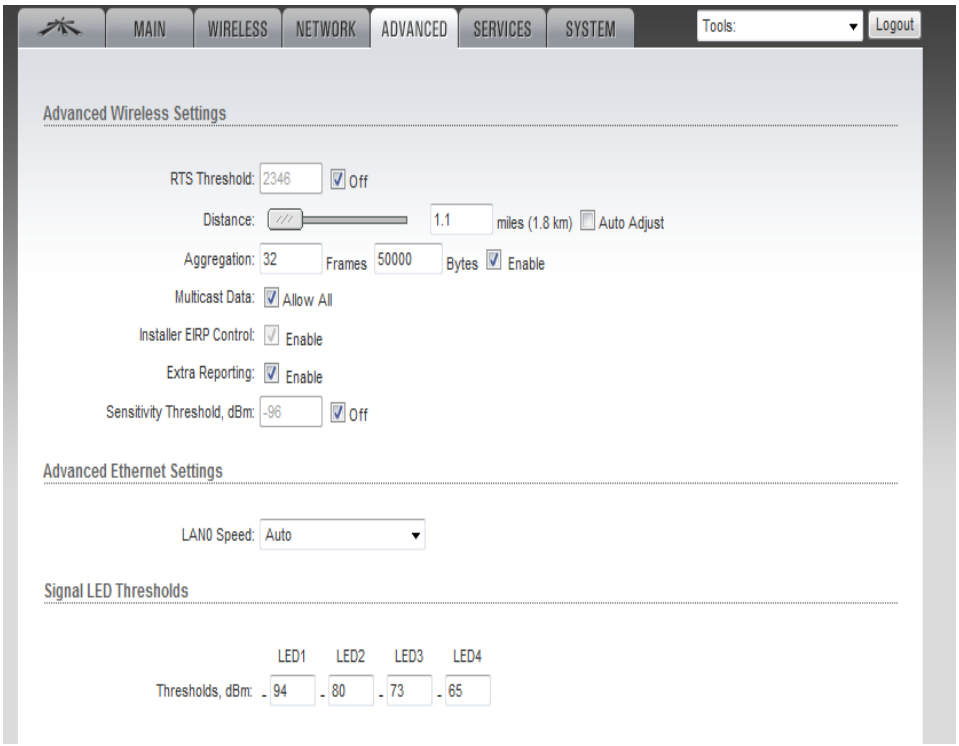


Figura 2.17 Interfaz WEB de las radios Rocket M5 donde se aprecia la configuración avanzada

CAPÍTULO 3

RED DE DATOS

El análisis de la red de datos de una institución, permite obtener información valiosa para el control de los servicios que se ofrecen a los usuarios internos y externos. Por ello es importante procurar un buen diseño e implementación de la red, del centro de cómputo y de los sistemas relacionados, a fin de asegurar la disponibilidad y confiabilidad de los servicios de TI.

3.1 Definición

Una red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios, para ello se requiere de un emisor,

un mensaje, un medio y un receptor. De esta forma podemos encontrar redes satelitales, redes de comunicaciones móviles, redes NGN, de banda ancha, etc.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Ver figura 3.1.

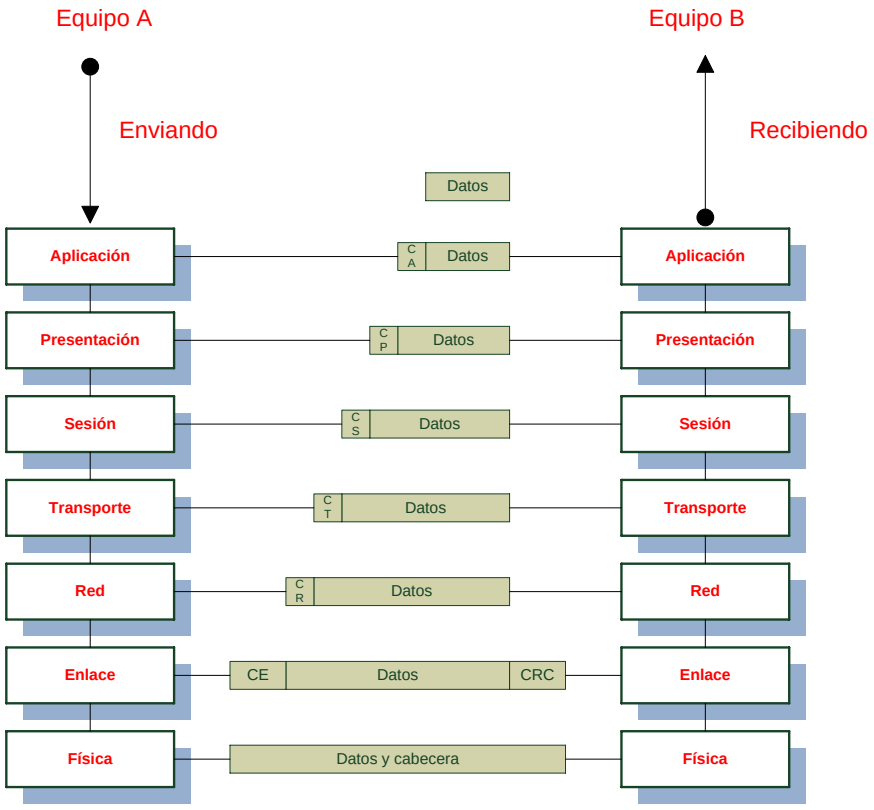


Figura 3.1 Modelo OSI. Referencia: Material Redes de Datos MET

1) Nivel Físico: se ocupa de la transmisión de bits primarios a lo largo del canal físico de comunicación. El servicio proporcionado transfiere secuencias de bits, incluso en un canal no libre de errores, de un punto a otro de la red. Ejemplos de protocolos de nivel 1 son todos los diferentes métodos de modulación y codificación de la información, tales como las modulaciones N-QAM (Modulación de amplitud en cuadratura), QPSK (Quadri-Fase Shift Keying), OFDM (Orthogonal Frequency Division Multiplexing), etc.

2) Nivel de Enlace: partiendo del servicio de transmisión de bits dado por la capa Física, la tarea del Nivel de Enlace es proveer un control de errores al Nivel superior. Además de detectar y corregir errores, fragmenta y ordena en paquetes los datos enviados.

3) Nivel de red: gestiona todas las operaciones de encaminamiento de paquetes a través de las redes que conectan los procesos de comunicación, y por lo tanto las reglas de determinación de los diversos caminos y la distribución de las tablas de encaminamiento entre nodos.

4) Nivel de Transporte: Acepta datos de la capa de sesión, la divide en unidades más pequeñas si es necesario (paquetes) y los pasa a la capa de red, asegurándose de que estas unidades vienen normalmente del destino correcto. Incluso en redes con alta tasa de error, o que sufren de alta tasa de pérdida de paquetes, un protocolo de capa 4 es capaz de asegurar una conexión fiable entre los dos terminales.

5) Nivel de Sesión: Permite a los usuarios de diferentes sistemas establecer sesiones de comunicación entre ellos, lo que facilita, por ejemplo, controlar y sincronizar el diálogo. Las sesiones pueden ajustar el tráfico, simultáneamente en ambas direcciones o sólo en una dirección.

6) Nivel de Presentación: se encarga del formato de presentación de las aplicaciones, realizando conversión de caracteres, códigos y algunas funciones de seguridad (cifrado).

7) Nivel de Aplicación: se denomina también ***"nivel de usuario"*** porque proporciona la interfaz de acceso para la utilización de los servicios de alto nivel. Contiene programas de aplicación utilizados directamente por el usuario. Ejemplos de aplicaciones son un

cliente de correo electrónico, un navegador web, un programa de videoconferencia, y así sucesivamente**.** Como un ejemplo de protocolo de comunicación entre las aplicaciones, se puede mencionar el Hyper Text Transfer Protocol (HTTP), comúnmente utilizado en la navegación de la World Wide Web (WWW) para la comunicación entre el navegador y el servidor web.

3.1.1 Topología de Red

Es la configuración entre las estaciones y las conexiones entre ellas, ya sea en bus, estrella, anillo, etc. Ver figura 3.2.

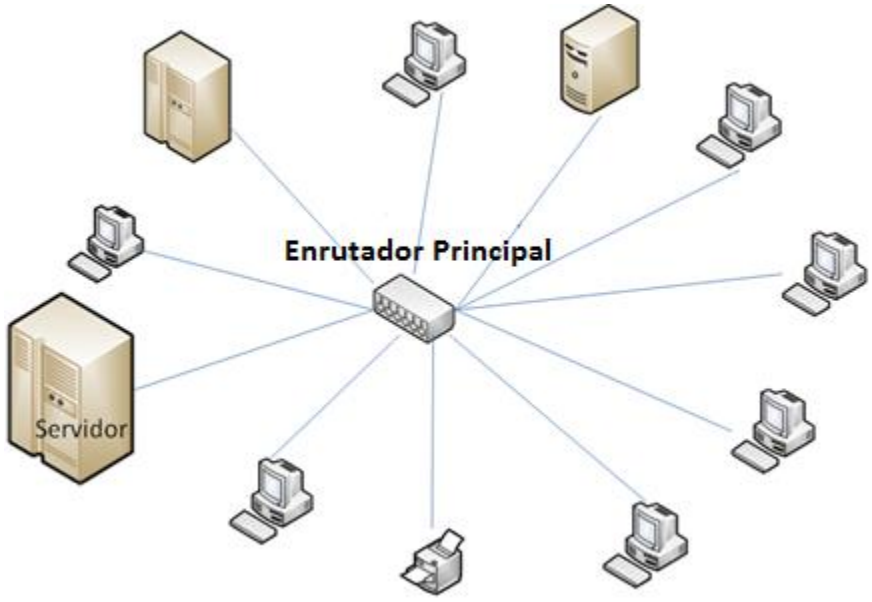


Figura 3.2 Topología Estrella

3.1.2 Tipos de Redes

Según el territorio que abarca la red se clasifica en: Red de área local, de área extensa y de área metropolitana.

La Red de Área Local (LAN, *Local Area Network*), se refiere a una red comprendida en un área geográfica limitada, como un edificio de oficinas, un hospital, etc. Se caracteriza por un canal físico con velocidad media/alta y con una tasa de errores reducida [9].

La Red de Área Extensa (WAN, *Wide Area Network*), es la red que ofrece servicios de comunicación entre zonas geográficamente distantes. Es utilizada, por ejemplo para conectar una oficina matriz con sus sucursales.

La Red de Area Metropolitana (MAN, Metropolitan Area Network), se caracteriza por presentar velocidades que van desde los 2Mbps hasta los 155Mbps (banda ancha), dando cobertura a áreas geográficas extensas, con servicios que integran la transmisión de datos, voz y vídeo, sobre medios

de transmisión guiados como fibra óptica y par trenzado de cobre.

3.2 Áreas y dispositivos de interés

Las áreas y dispositivos de interés a ser gestionadas a través del protocolo SNMP son:

1. Centros de Cómputo
2. Enlaces y Troncales
3. Conmutadores y Enrutadores
4. Otros controles
    a. Conexiones Inalámbricas
    b. Sistema de Refrigeración y Humedad
    c. Gestión de Impresión

3.2.1 Centros de Cómputo

Un centro de cómputo, muchas veces es considerado como una entidad dentro de las organizaciones, cuyo objetivo principal es proveer a las empresas la información tecnológica requerida para atender sus servicios y mantener la competitividad, asegurar la disponibilidad de la

información y apoyar la labor administrativa para hacerla más segura y fluida. El centro de cómputo administra, custodia y procesa los datos con los que opera la compañía. Todas las actividades de los demás departamentos se basan en la información que les proporciona dicho centro, por lo que casi no se escatima en mantenerlo con la tecnología de punta necesaria, ni del personal humano requerido, ya que muchas veces se requieren operadores las 24 horas del día. Puede a llegar a absorber la mayor parte del presupuesto y manejar los datos críticos de la empresa y de terceros [10].

Por ello se requiere implementar procesos de control de los dispositivos de red y del hardware instalado en el centro de cómputo. Dichos procesos son manejados por el Gestor de Operaciones y apoyados por la Dirección de TI. En la figura 3.3 se puede apreciar la distribución interna del centro de cómputo. Algunos procesos dependerán de la clasificación del centro de cómputo que operemos, según sea Tier I, Tier II, Tier III o Tier IV.

Figura 3.3 Centro de Cómputo
http://administracionderededed.blogspot.com

“Pitt Turner, Jhon Seader y Kenneth Brill, desarrollaron para el Uptime Institute, Inc. un enfoque de clasificación por niveles, llamado clasificación TIER, que consiste en especificar la funcionalidad del sitio de infraestructura y plantear la necesidad de una norma común de evaluación comparativa [11]”.

La clasificación por niveles implica algunas definiciones. Un centro de cómputo que puede mantenerse ante la presencia de un imprevisto, debido a una de falla en la infraestructura sin afectar la carga crítica de la institución se considera que es tolerante a fallos. Un sitio que es capaz de

realizar las actividades planeadas, como mantenimientos e instalaciones planificadas, sin necesidad de apagar la carga crítica se considera fácil de mantener al mismo tiempo. Todo esto considerando que un centro de datos típico se compone de por lo menos 20 sistemas principales, mecánicos, eléctricos, de climatización, de protección contra incendios, la seguridad (Control de acceso y cámaras) y otros sistemas, cada uno de los cuáles se puede dividir en subsistemas y componentes adicionales, los cuales deben cumplir con las dos premisas mencionadas anteriormente, ser tolerante a fallos y / o de fácil mantenimiento al mismo tiempo [12]. La Tabla V muestra la clasificación del Uptime Institute, que se detalla a continuación:

El Tier I se compone de un único sistema de alimentación de energía y de distribución de refrigeración, no tiene componentes redundantes, proporcionando 99,671% de disponibilidad, se lo considera como un centro de datos básico. Es susceptible a la interrupción de las actividades. Tiene una distribución de energia y sistema de refrigeración,

pero puede o no tener un piso falso, un UPS, o un generador de motor. La infraestructura debe parar por completo una vez al año para realizar el mantenimiento preventivo y reparación. Errores de funcionamiento o fallas espontáneas de componentes de la infraestructura del sitio causarán interrupciones del centro de datos.

En cambio, el Tier II se compone de un único sistema de alimentación de energía y de distribución de refrigeración, con componentes redundantes, que lo hacen menos susceptible, proporcionando 99,741% de disponibilidad. Tienen un suelo elevado, UPS y generadores, pero presentan una sola vía de distribución. El mantenimiento de los tableros de alimentación principal y otras partes de la infraestructura del sitio requerirán del apagado de los equipos del centro de cómputo.

En el Tier III, existen múltiples vías de alimentación de energía activa y caminos de distribución de refrigeración, pero sólo uno activo, tiene componentes redundantes, y es fácil de mantener simultáneamente, proporcionando

99,982% de disponibilidad. Las actividades previstas son realizadas sin interrumpir el funcionamiento de los servidores. Se incluye el mantenimiento preventivo y programable, la reparación y sustitución de componentes, adición o eliminación de componentes, pruebas de componentes y sistemas, y más.

Tabla V. Comparación de clasificación Tier. Uptime Institute

	Tier I	Tier II	Tier III	Tier IV
Tipo de Edificación	Interna	Interna	Independiente	Independiente
Personal	Ninguno	1 turno	1 + 1 turno	24 *7
Carga critica usable	100% N	100% N	90% N	90%N
Watts por pie cuadrado inicial	20-30	40-50	40-60	50-80
Watts por pie cuadrado final	20-30	40-50	100-150	150 +
Refrigeración ininterrumpida	no	no	quizas	si
Relación piso elevado/Espacio	20%	30%	80-90%	100% +
Altura piso elevado	12"	18"	30-36"	30-36"
Voltaje	208-480	208-480	12-15Kv	12-15Kv
Puntos de Falla	Muchos+Error Humano	Muchos+Error Humano	Algunos+Error Humano	Ninguno+Error Humano
Anual Downtime	28,8 horas	22 horas	1,6 horas	0,4 horas
Disponibilidad	99,671%	99,749%	99,982%	99,995%
Primer año de implementación	1965	1970	1985	1995

Pero las actividades no planificadas, como errores en la operación o fallas espontáneas de los componentes de la infraestructura seguirán ocasionando una interrupción en el

centro de datos. Se considera que la carga crítica en el sistema no supera el 90% del total.

Finalmente, el Tier IV se compone de múltiples vías de alimentación de energía activa y caminos de distribución de refrigeración, tiene componentes redundantes y es tolerante a fallos, proporcionando 99,995% de disponibilidad. Requiere rutas de distribución simultáneas y activas, para proveer tolerancia a fallos, lo que significa tener dos sistemas de UPS separados, en los que cada uno tiene redundancia N+1, para sostenerse frente a una falla crítica imprevista. La carga crítica en el sistema no supera el 90% del total. En la figura 3.4 se puede apreciar la caída del servicio anual según la clasificación Tier.

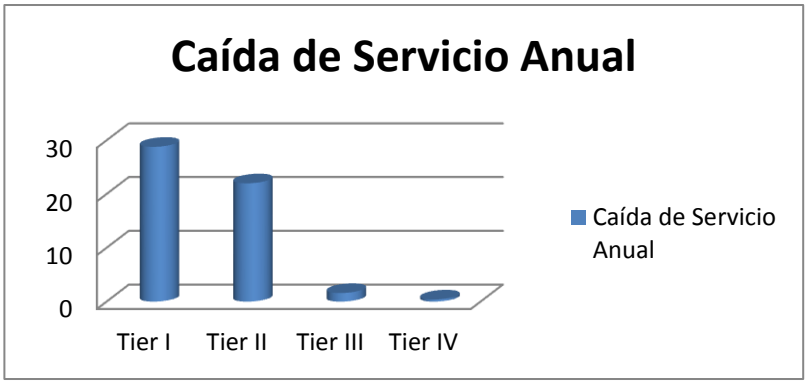


Figura 3.4 Caídas de Servicio Anuales

3.2.2 Enlaces y troncales

El enlace de datos se refiere al conjunto de equipos electrónicos, que consisten de un transmisor, un receptor y un circuito de telecomunicaciones para la interconexión. Las configuraciones básicas son:

Simplex: todas las comunicaciones se realizan en una única dirección

Semiduplex: las comunicaciones se realizan en ambas direcciones, pero no al mismo tiempo.

Duplex: las comunicaciones se realizan en ambas direcciones simultáneamente.

Un enlace punto a punto, es un enlace troncal, que comunica a dos dispositivos de red, con la finalidad de transportar más de una VLAN. El enlace troncal de VLAN, extiende las VLAN a través de toda la red [13].

La caída de un enlace interrumpiría las labores normales de la empresa durante el tiempo en que se lo pueda recuperar o mientras se activa un recurso redundante, por

ello es importante como parte del proceso de control de las comunicaciones que el Gestor de Operaciones realice una verificación permanente de la calidad del enlace, para garantizar el flujo de datos de manera continua.

Además deberá encargarse de gestionar y supervisar los mantenimientos del sistema que convengan a fin de mantenerlo operativo.

3.2.3 Conmutadores y Enrutadores

Una red funciona mediante la conexión de ordenadores y periféricos, a través de equipos tales como: Enrutador y conmutador. Estos dispositivos permiten a los equipos que están conectados en la red comunicarse entre si, así como con otras redes. Ver figura 3.5

El conmutador es un dispositivo analógico de interconexión de redes de computadoras que opera en la capa de enlace de datos, del modelo OSI. Se lo utiliza con el propósito de conectar múltiples redes entre sí dentro de un edificio o

campus para que funcionen como una sola red, mejorando el rendimiento y la seguridad de la misma [14]. Estos se clasifican en: administrados y no administrados:

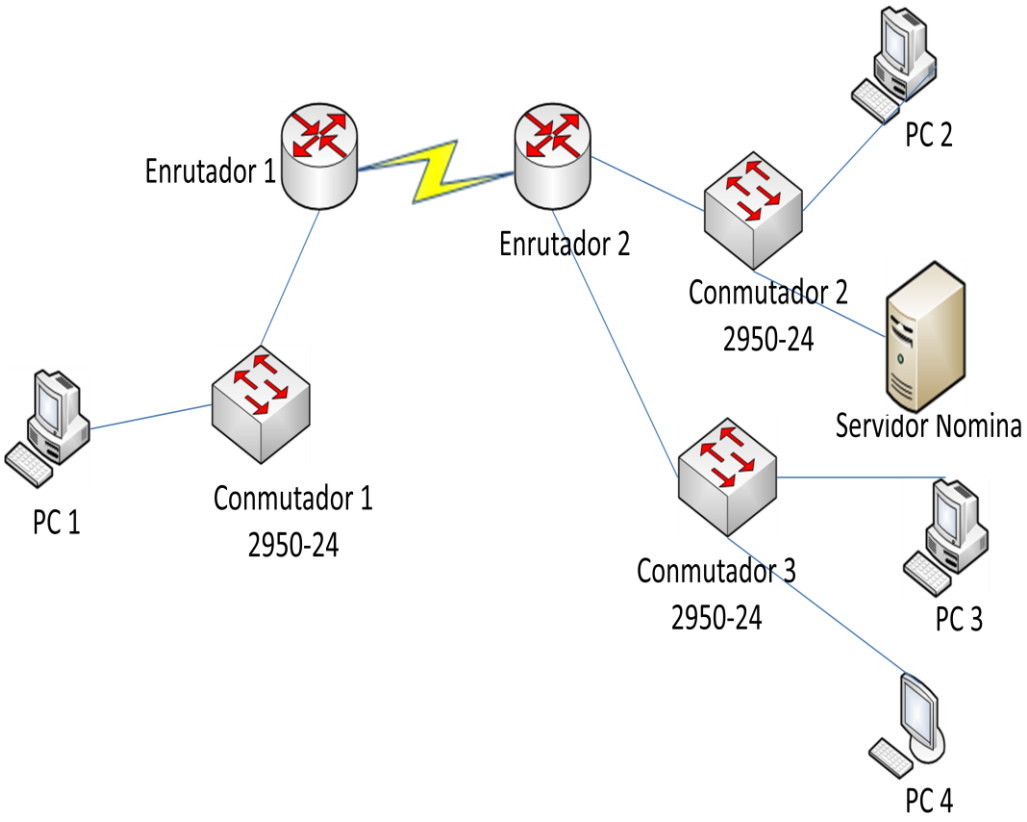


Figura 3.5 Red administrada con enrutadores y conmutadores.

- Los no administrados funcionan automáticamente y no permiten cambios. Los equipos de redes pequeñas usan este tipo de dispositivos.

- Los administrados pueden ser programados. Esto permite una gran flexibilidad ya que el conmutador puede configurarse y monitorizarse local o remotamente, permitiendo el control del tráfico transmitido en la red [15]. En la figura 3.6 se observa una configuración de conmutadores.

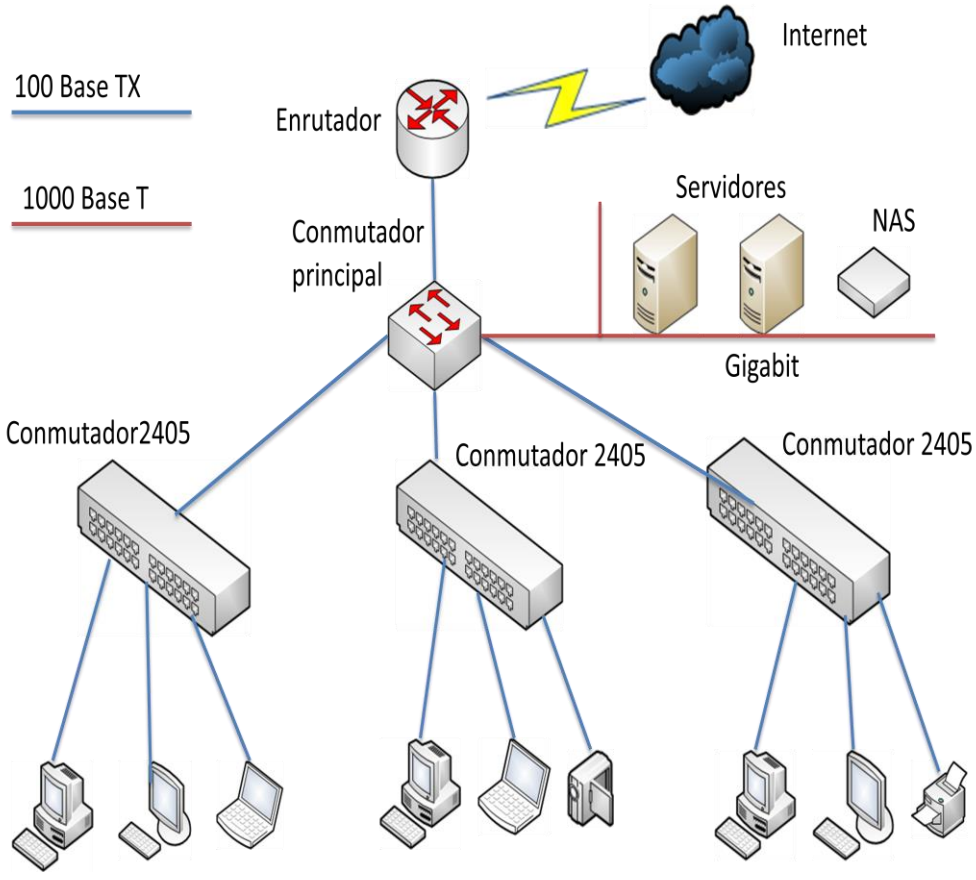


Figura 3.6 Conmutadores administrables

También se los puede clasificar en conmutadores de capa 2, capa 3 y capa 4:

Los Conmutadores de Capa 2, funcionan como puentes multi-puertos. Su propósito principal es dividir la Red LAN en múltiples dominios de colisión.

Los dispositivos de capa 3 incorporan funciones de enrutamiento, determinan el camino basado en informaciones de la capa de red, validan la integridad del cableado por suma de verificación y soportan los protocolos de enrutamiento tradicionales (RIP, OSPF, etc).

Finalmente, los conmutadores de capa 4, incorporan a las funcionalidades del conmutador la habilidad de implementar políticas y filtros a partir de informaciones de capa 4 o superiores, como puertos TCP/UDP, SNMP, FTP, etc.

Por otra parte, la función del enrutador es interconectar las redes, permitiendo asegurar el enrutamiento de paquetes entre redes o encontrar la ruta que debe seguir el paquete

de datos. Para escoger las rutas se utilizan las tablas de enrutamiento, que son mapas de las direcciones que pueden seguirse para llegar al destino [16]. En la figura 3.7 se puede observar una red con enrutadores.

Existen dos tipos de protocolos de enrutamiento principales: Vector Distancia y Estado de Enlace.

En el de Vector Distancia, los enrutadores generan una tabla de enrutamiento que se encarga de calcular el "valor" (métrica) de cada ruta y luego la envían a los enrutadores cercanos para que tengan los datos actualizados. Para cada solicitud de conexión el enrutador elige la ruta menos costosa.

En cambio, en los de estado de enlace, los enrutadores escuchan permanentemente la red para identificar los distintos dispositivos que la rodean y así calcular la ruta más corta a cada enrutador. La tabla de enrutamiento es elaborada mediante el algoritmo de Dijkstra.

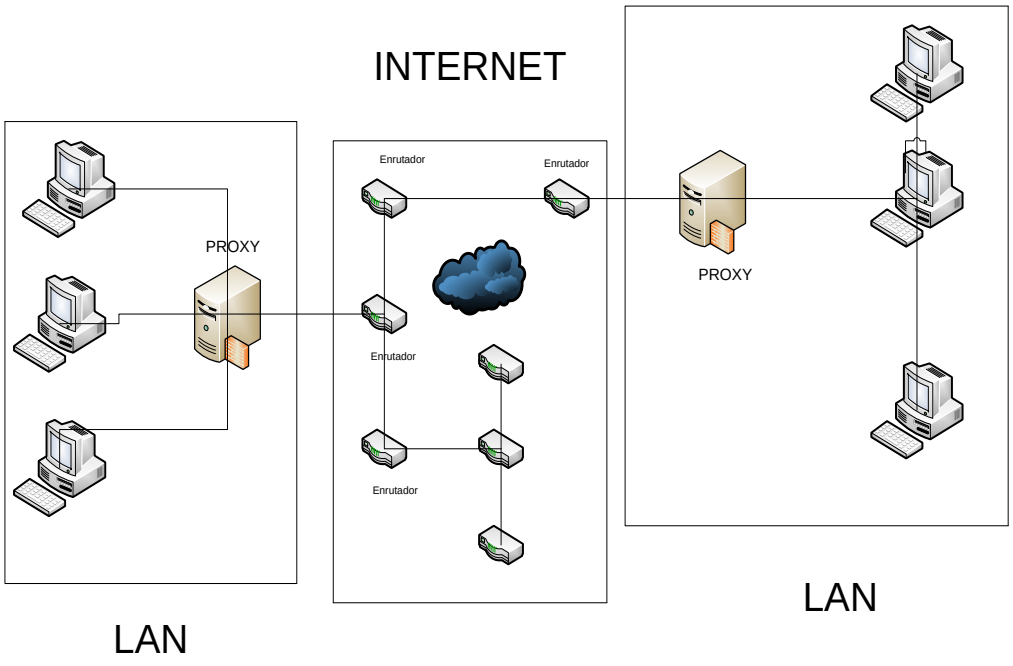


Figura 3.7 Red de Enrutadores

3.2.4 Otros controles

Existen otros parámetros que merecen la atención del gestor de operaciones, como las conexiones inalámbricas, los sistemas de refrigeración y humedad, y la gestión de la impresión.

3.2.4.1 Conexiones Inalámbricas

Para ello se emplea un Enrutador inalámbrico, cuya característica es permitir la conexión de dispositivos inalámbricos a las redes en las que el

enrutador se encuentra conectado mediante conexiones por cable (generalmente Ethernet).

3.2.4.2 Sistema de Refrigeración

El sistema de refrigeración y humedad del centro de cómputo esta proporcionado por un aire acondicionado Liebert de 69000 BTU. El aire frío circula por debajo del piso falso y sube a través de las rejillas perforadas distribuidas equitativamente en el centro de datos, permitiendo la adecuada climatización del área.

3.2.4.3 Gestión de impresión

A fin de optimizar los recursos en el proceso de impresión de la institución se contrato un servicio de outsourcing, el cual tiene entre sus funciones realizar la gestión de impresión y llevar un sistema de auditoría para controlar el consumo de papel y toners, así como asegurar la disponibilidad del servicio. Para ello se utiliza un software propietario de la empresa HP que permite visualizar los consumos y los estados de

las impresoras. La aplicación trabaja con el protocolo SNMP.

3.3 Políticas de seguridad

La seguridad y funcionalidad de una red está determinada por las medidas que se adopten en lo referente a la seguridad para el sitio.

De acuerdo a la RFC-2196 de la IETF [17]*: "Una política de seguridad es un enunciado formal de las reglas que los usuarios que acceden a los recursos de la red de una organización deben cumplir"*

La política de seguridad pretende como objetivos principales alcanzar los siguientes aspectos [18]:

- Que los usuarios de la red comprendan sus obligaciones en la protección de los recursos de la red.
- Instruir sobre los mecanismos necesarios para que estos requerimientos sean logrados.

- Suministar una guía de implementación, configuración y control de los sistemas de la red para conseguir el cumplimiento de la política.

Al implementar la política de seguridad se pretende asegurar la disponibilidad del servicio a través del cumplimiento de cuatro procesos fundamentales: La política de autenticación, la política de privacidad, la política de acceso y la política de administración de la red.

La política de autenticación busca la confiabilidad con el uso de contraseñas o mecanismos de firmas digitales, para ello establece normas para la autenticación remota.

Mientras que en la política de privacidad se definen los alcances en lo referente a la privacidad de las funciones de monitoreo, al registro de actividades y al acceso a recursos de la red.

En cambio, la política de acceso se encarga de establecer claramente los derechos de acceso y los privilegios de los usuarios en la red, para evitar pérdidas o exposición de la información a

través del uso de guías preestablecidas para los usuarios en lo referente a conexiones externas, comunicación de datos, conexión de dispositivos a la red, etc.

La política de administración de la red y un sistema de IT, se refiere a la aplicación de las tecnologías por parte de los responsables de la administración interna y externa.

Los servicios de las empresas tienden a cambiar en pro de mejorar los resultados con la implementación de nuevas tecnologías, por lo que la política de seguridad debe ser revisada de manera periódica para que se ajuste a las necesidades reales de la seguridad de la institución. Como parte de la implementación de las políticas, se hace un análisis de todos los riesgos posibles, considerando la identificación de los objetos que son claves dentro de la operación del servicio de TI e identificando las posibles amenazas a ellos.

Es importante identificar lo que tiene que ser protegido, es decir, aquello que siendo vital para la disponibilidad del servicio, se pueda ver afectado por un problema de seguridad. Por ejemplo:

1. Hardware: AS400, Cuchillas, Servidores, Unidades de procesamiento, terminales, impresoras, SAN, enrutadores, etc.

2. Software: Programas fuentes, utilidades, sistemas operativos, etc.

3. Datos: archivos en línea, bases de datos, datos siendo trasmitidos por algún medio, etc.

Las amenazas que se analizan, son aquellas que afectan los objetivos claves para mantener el servicio disponible. Pueden ser catalogados según el potencial de pérdida calculado. Las amenazas están relacionadas con el servicio a ofrecer, sin embargo existen amenazas típicas que deben ser revisadas en la Gestión de la Operación de TI:

1. La posibilidad del acceso no autorizado a recursos y/o información.
2. La exposición no autorizada de información.

3. Los ataques de Rechazo del servicio (DoS – Denial of Service).

3.4 Gestión de la operación de la red

El objetivo principal de la Gestión de la Operación de la red, es el mantenimiento de la infraestructura de TI y mantener la disponibilidad de los servicios de la red. Se puede dividir en dos subunidades [19]: Control de operaciones y Gestión de instalaciones

3.4.1 Control de operaciones

Su función es la monitorización y supervisión de los servicios, para ello se recomienda contar con un NOC (centro de operación de la red), cuyas actividades principales son:

- La gestión de consolas: Es la organización de los procesos de monitorización, incluyendo su evaluación.
- Programación de tareas: Procesa los trabajos habituales de TI.
- Back-up: Ordena las actividades relacionadas al respaldo de los datos.

Las tareas de Gestión se apoyan en diversas herramientas para la ejecución de operaciones de control y vigilancia de los dispositivos de la red, las que incluyen análisis gráficos,

alertas, reportes y alarmas. La estructura utilizada por las herramientas es la de “gestor-agente” [20]:

Gestores: Interactuan con los operadores y realizan acciones para cumplir con las tareas planificadas dentro del control de la red

Agentes: Son invocados por el gestor de la red.

El proceso que se ejecuta es el intercambio de información entre los nodos gestores y los gestionados, lo que se muestra en la figura 3.8. Los agentes almacenan en los nodos que se gestionan la información de su estado y las características de operación del recurso. El gestor solicita al agente, por medio de un protocolo de red, la ejecución de operaciones con los datos de gestión, con los cuáles se podrá conocer el estado del recurso.

Al presentarse una situación fuera de lo normal, los agentes sin ser llamados por el gestor, envían los denominados eventos o notificaciones (trap) al gestor, que son recibidos por un operador para su atención correspondiente.

Figura 3.8 Gestion de la Operación de la Red

Dentro de los protocolos de gestión de red, se destaca el SNMP, usado en redes empresariales debido a su facilidad de uso y soporte universal de hardware.

3.4.2 Gestión de instalaciones

Es la responsable del mantenimiento de los equipos de la red y del centro de datos, además de la supervisión de los equipos de alimentación eléctrica y de climatización.

La gestión de la operación de la red se relaciona con el tamaño de la misma y con su complejidad, puede ser administrada por una sola persona que se encargue de

supervisar los enlaces de la red desde un computador o tan compleja como la operación de un grupo de 20 operadores que verifican todo el día como opera la red.

3.5 Controles y variables

A continuación se detalla el análisis que se hizó de algunas de las variables fundamentales, consideradas dentro del Sistema de Gestión de la Red, para mantener la disponibilidad de los servicios ofrecidos en las dependencias de la Junta de Beneficencia de Guayaquil. Los gráficos mostrados corresponden a lecturas tomadas de una aplicación propia del hardware o a un software especializado en el control de variables bajo el protocolo SNMP.

3.5.1 Control de energía

El suministro de energía para los servidores debe ser permanente, de lo contrario se afectaría la disponibilidad de los servicios, por lo que el operador realiza un control de los valores de voltaje de entrada y salida del centro de cómputo. También se necesita administrar los valores de

carga (W) y el porcentaje del mismo, para evitar una sobrecarga en los UPS.

En la figura 3.9 se observan los valores correspondientes a las variables de voltaje, corriente, frecuencia y potencia presentes en el Centro de Cómputo de la Oficina Central, que es soportado por un sistema de UPS en paralelo con una capacidad de 30Kva.

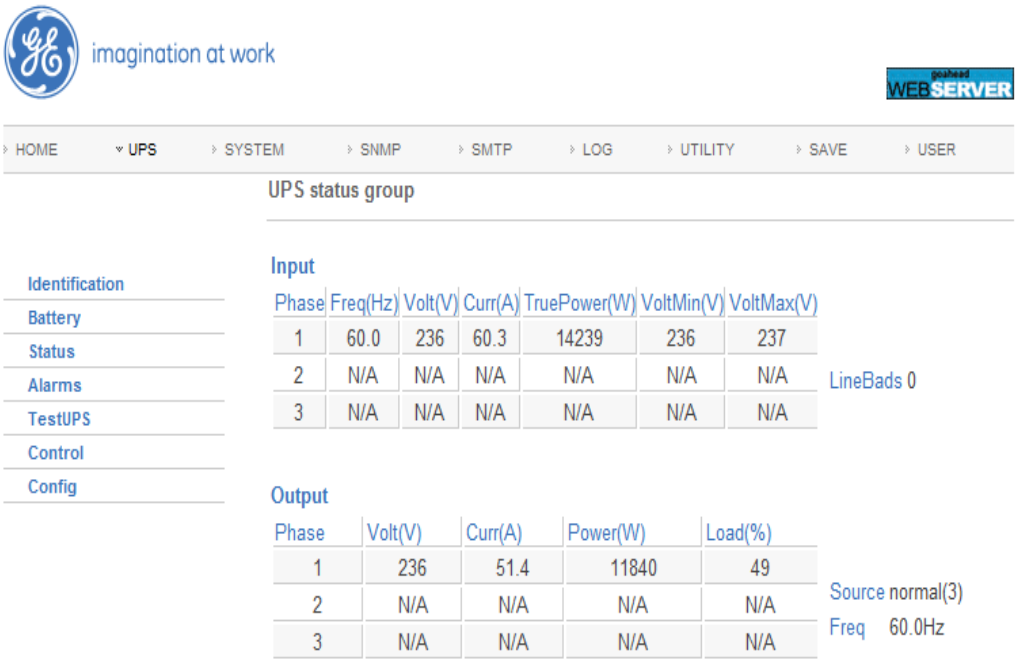


Figura 3.9 Status de UPS Centro de Cómputo Oficina Central

Al momento de la lectura se puede apreciar un voltaje de entrada de 236v y una corriente de 60.3 A, protegiendo una carga de 14Kva. La salida del UPS muestra 236v, 51,4 A y una carga del 49%.

En la figura 3.10 se observan los valores correspondientes a las variables de voltaje, corriente, frecuencia y potencia presentes en el Centro de Cómputo del Hospital Luis Vernaza, que es soportado por un sistema de UPS con una capacidad de 10Kva.

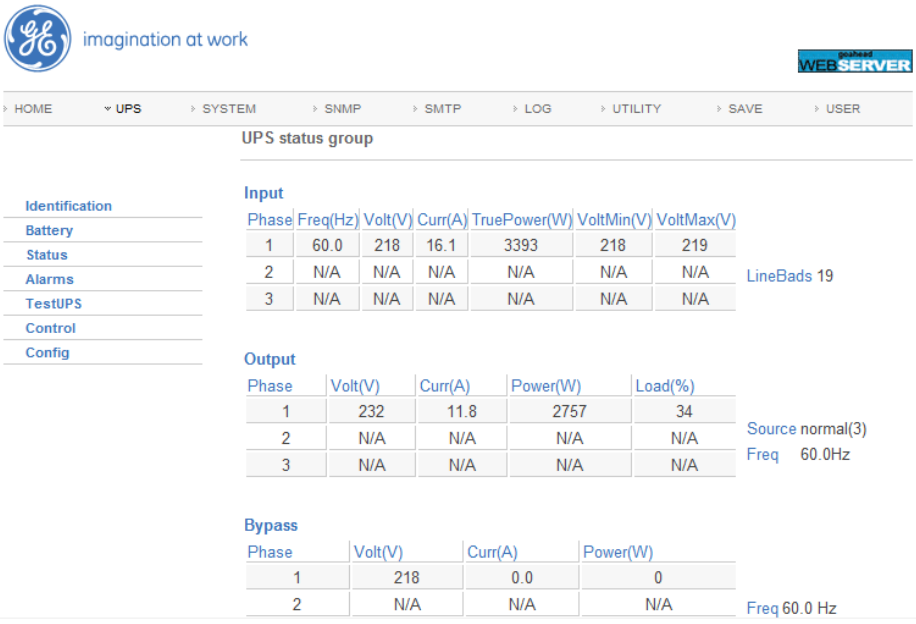


Figura 3.10 Status Centro de Cómputo Hospital Luis Vernaza

Al momento de la lectura se puede apreciar un voltaje de entrada de 218v y una corriente de 16.1 A, protegiendo una carga de 3.39Kva. La salida del UPS muestra 232v, 11,8 A y una carga del 34%.

En la figura 3.11 se observan los valores correspondientes a las variables de voltaje, corriente, frecuencia y potencia presentes en el Centro de Cómputo del Instituto de Neurociencias, que es soportado por un sistema de UPS con una capacidad de 10Kva.

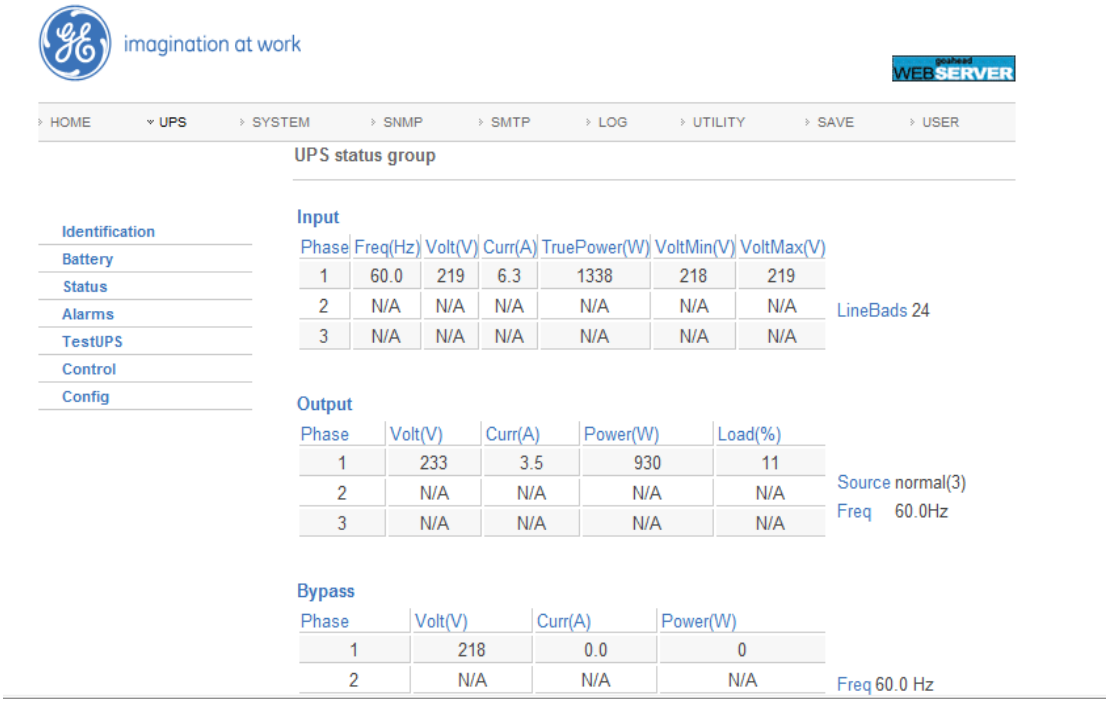


Figura 3.11 Status UPS centro de Computo Instituto de Neurociencias

Al momento de la lectura se puede apreciar un voltaje de entrada de 219v y una corriente de 6.3 A, protegiendo una carga de 1.34Kva. La salida del UPS muestra 233v, 3,5 A y una carga del 11%. En la figura 3.12 se muestran algunos de los Traps que maneja el sistema de control de energía a través de la tarjeta SNMP instalada en el UPS GE. Estas alarmas son enviadas vía mail al personal de soporte de la empresa para su revisión, tal como lo muestra la figura 3.13, donde se notifica al personal técnico sobre un incidente ocurrido con la energía de entrada y que motiva que el UPS active el funcionamiento de las baterías.

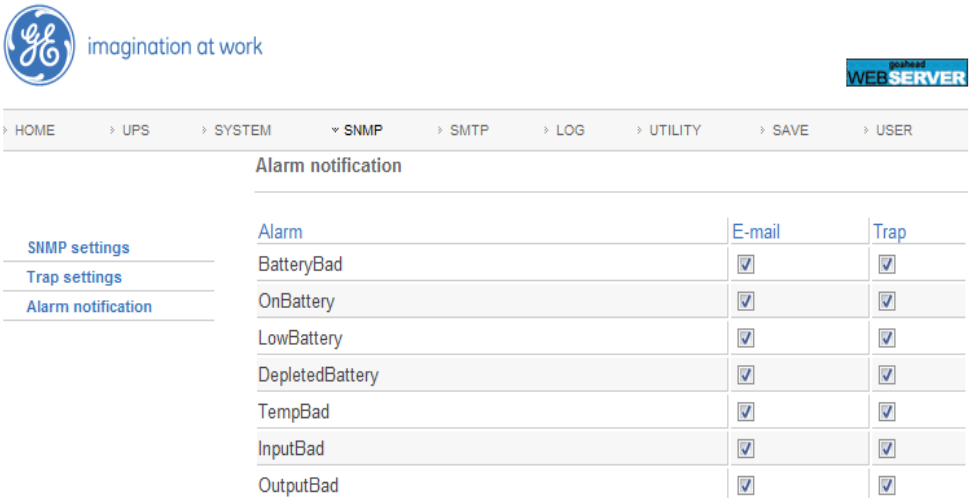


Figura 3.12. Traps activados de UPS GE

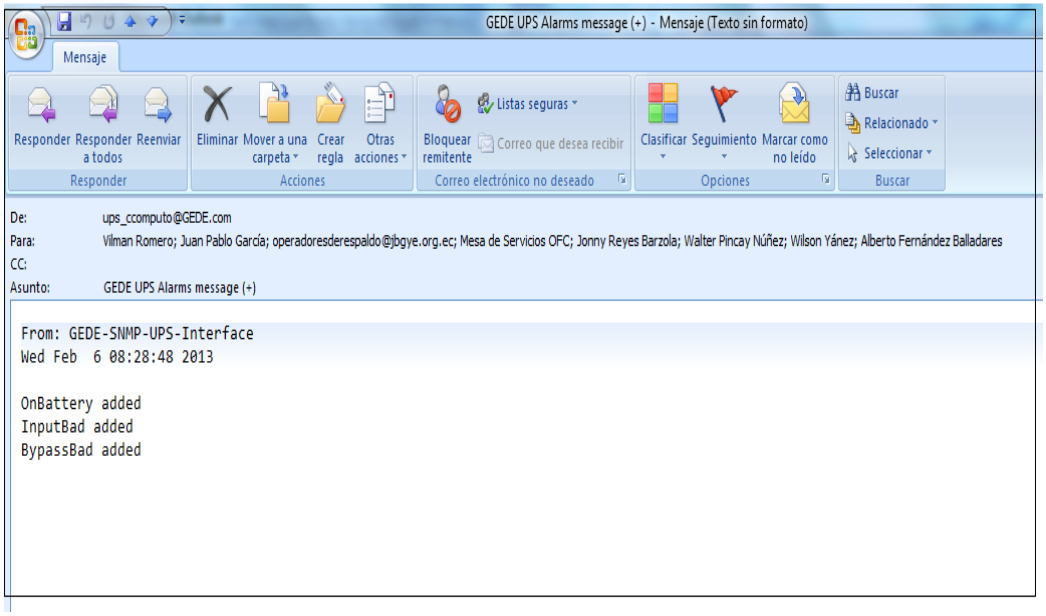


Figura 3.13 Mensaje del UPS

3.5.2 Control de Conmutadores y Enrutadores

Los Comutadores utilizados en las redes LAN de cada una de las dependencias y los enrutadores que las enlazan son monitoreados constantemente para garantizar que el servicio de comunicación este disponible las 24 horas del día. La falla de uno de estos dispositivos puede ocasionar el colapso de algún área operativa crítica de los hospitales, debido a la alta tasa de usuarios por día, que en algunos casos sobrepasa las mil personas. Por ello la importancia de la implementación de un Sistema de Control de la Red.

En las figuras (3.14 y 3.15) se aprecia el consumo del CPU del enrutador de oficina central en dos fechas distintas, con picos de 22% y mínimos de 3%

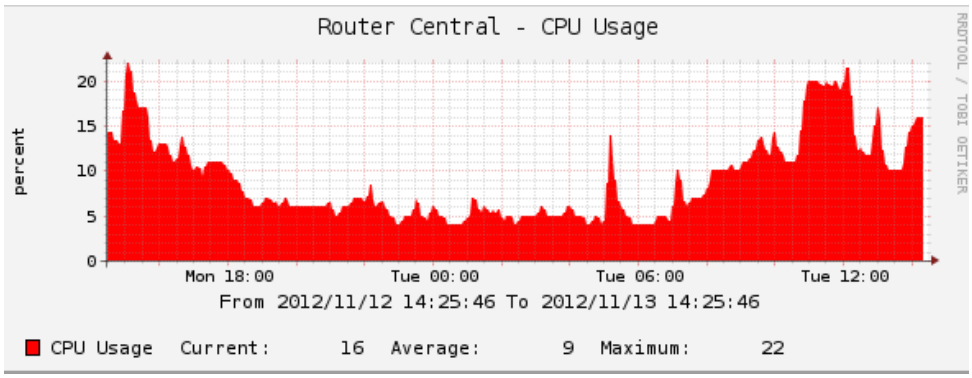


Figura 3.14 Gráficos de uso del CPU (%) en Oficina Central

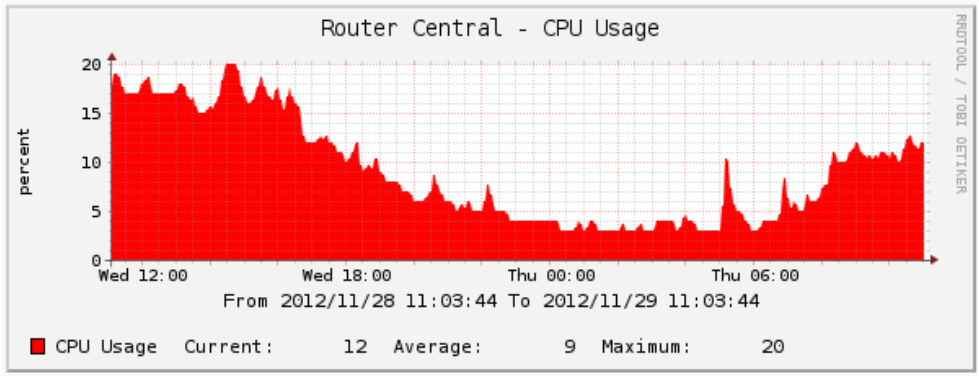


Figura 3.15 Gráficos de uso del CPU (%) en Oficina Central

Se observa en las figuras (3.16 y 3.17) el uso del ancho de banda de la red LAN de la Oficina Central de la JBG, con un máximo de 35.71 MB y 33.27MB en las dos muestras presentadas sobre 100MB posibles.

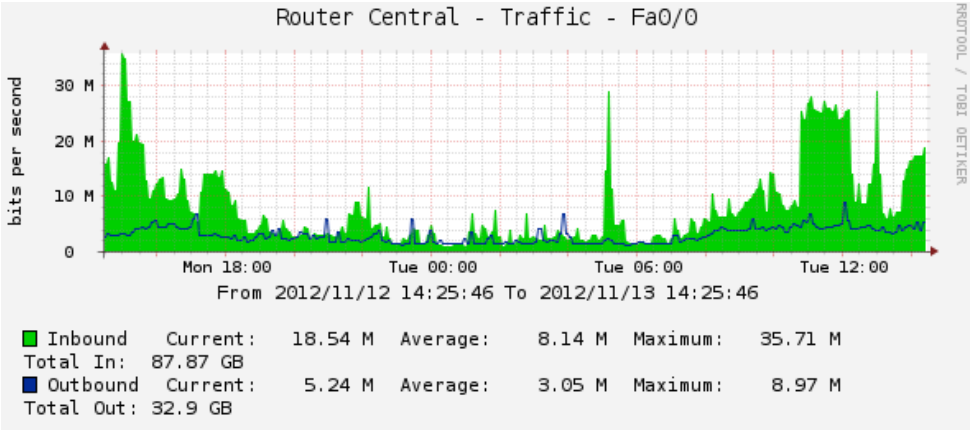


Figura 3.16 Gráfico de Ancho de banda de la LAN de Oficina Central

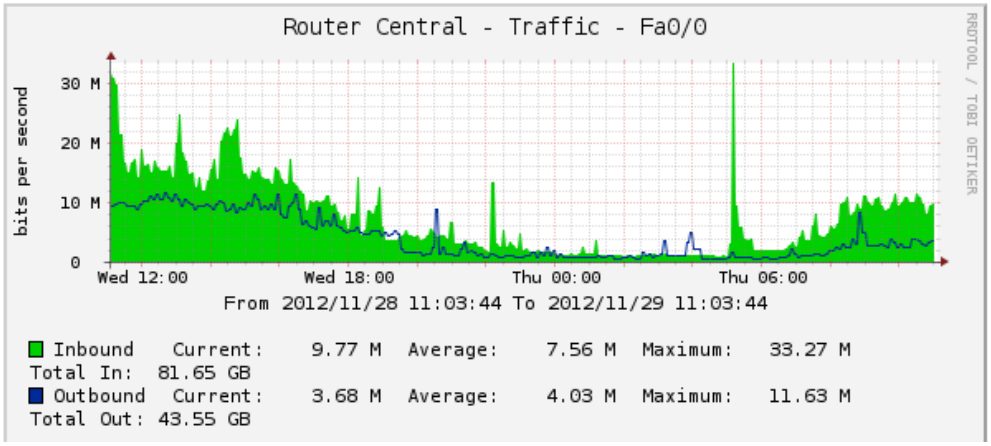


Figura 3.17 Gráfico de Ancho de banda de la LAN de Oficina Central

En la figura 3.18 se aprecia el consumo de ancho de banda entre la Oficina Central de la Junta de Beneficencia de Guayaquil y el Hospital Luis Vernaza, con un máximo de 14.11 MB en una conexión punto a punto de 20MB.

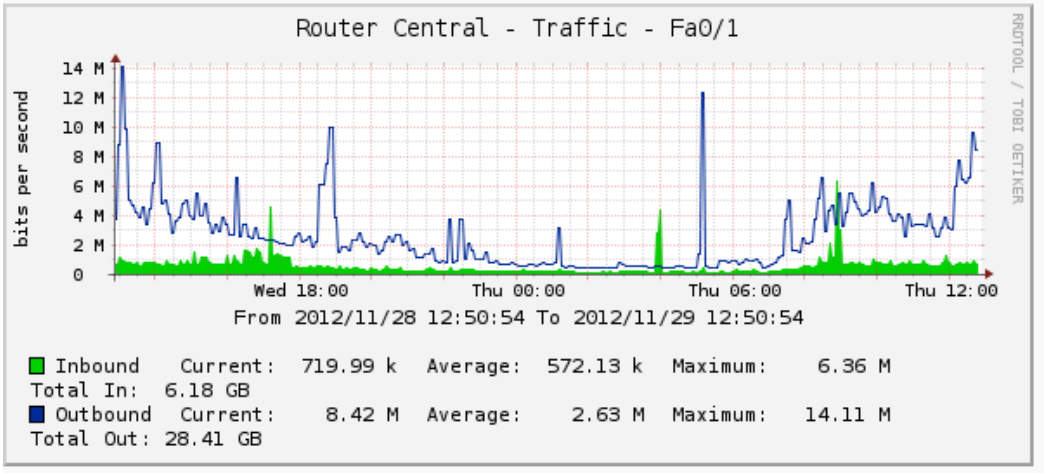


Figura 3.18. Gráfico de ancho de banda entre Oficina Central y Hospital Luis Vernaza

Se observa en las figuras (3.19 y 3.20) el uso del ancho de banda entre la Oficina Central de la Junta de Beneficencia de Guayaquil y el Hospital Roberto Gilbert, con un máximo de 26.36MB y 12.93MB en las dos muestras presentadas sobre 50MB posibles.

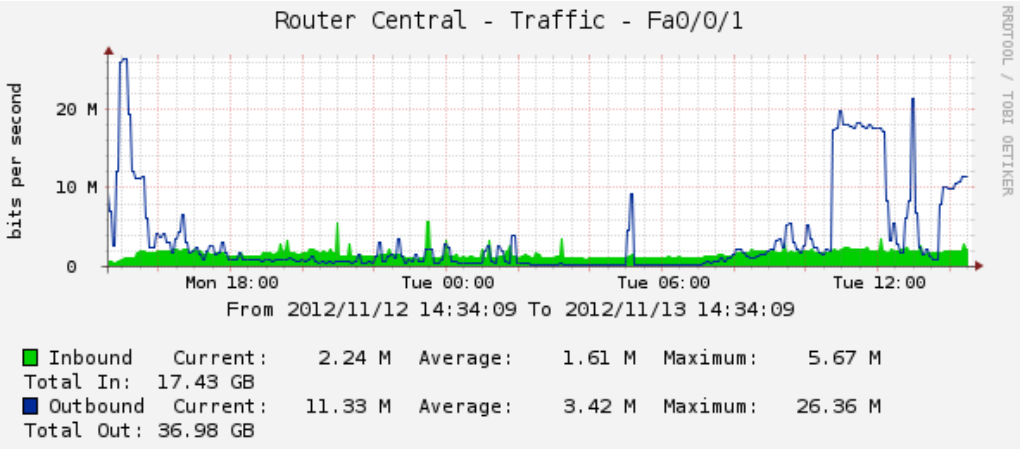


Figura 3.19. Gráfico de ancho de banda entre Oficina Central y Hospital Roberto Gilbert

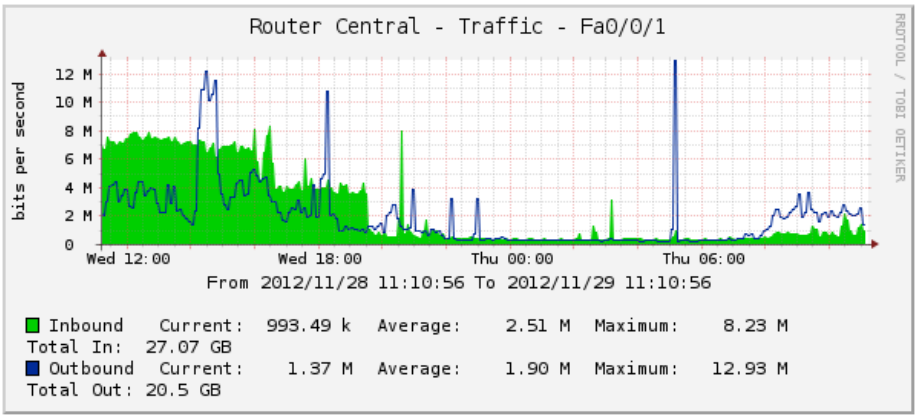


Figura 3.20. Gráfico de ancho de banda entre Oficina Central y Hospital Roberto Gilbert

Se observa en las figuras (3.21 y 3.22) el uso del ancho de banda entre la Oficina Central de la Junta de Beneficencia de Guayaquil y la Lotería Nacional, con un máximo de 6.88 MB y 5.7MB en las dos muestras presentadas sobre 10MB posibles.

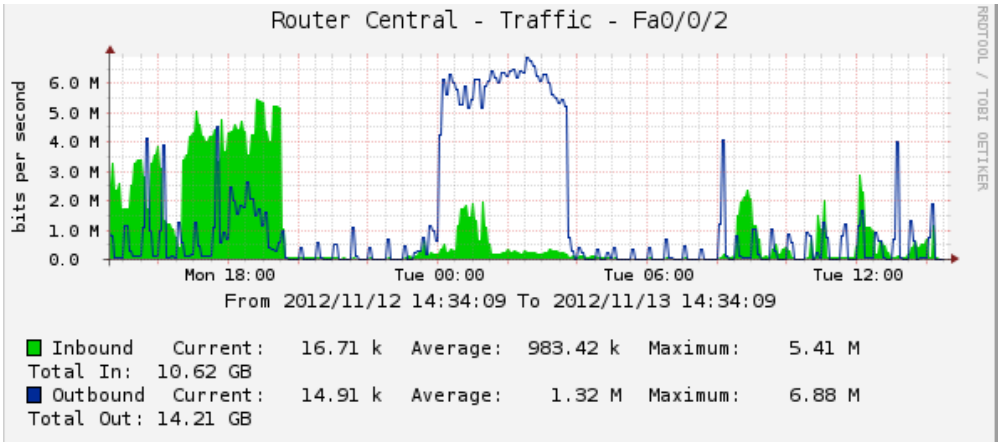


Figura 3.21. Gráfico de ancho de banda entre Oficina Central y Loteria Nacional

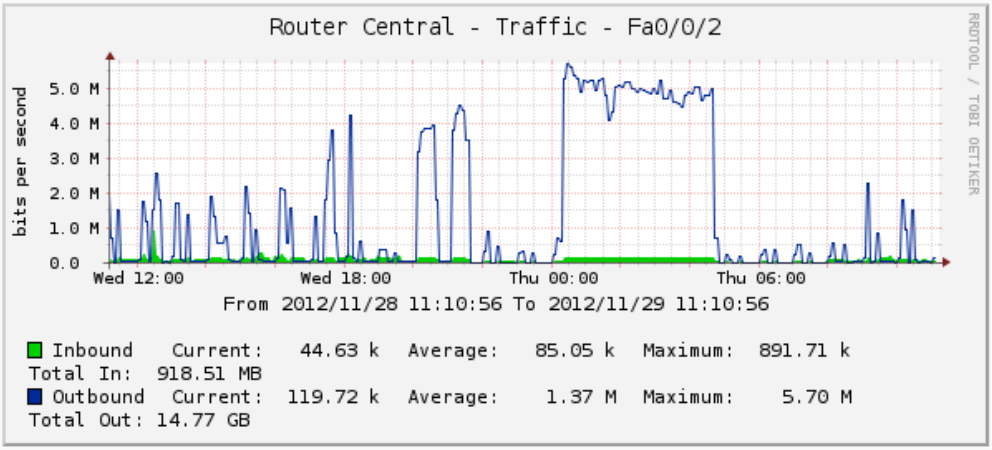


Figura 3.22. Gráfico de ancho de banda entre Oficina Central y Loteria Nacional

Se observa en las figuras (3.23 y 3.24) la comunicación entre la Oficina Central y la Maternidad, con un máximo de 8.63 MB y 9.3MB en las dos muestras presentadas sobre 10MB posibles.

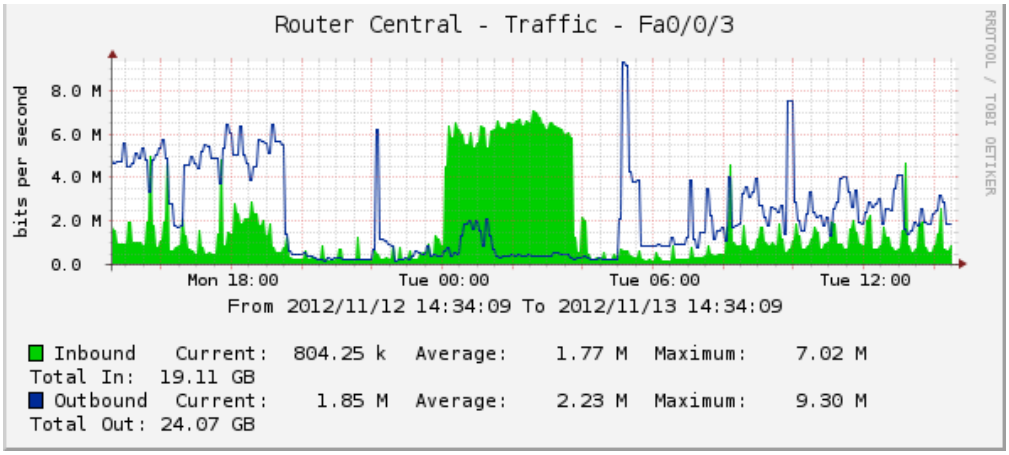


Figura 3.23. Gráfico de ancho de banda entre Oficina Central y la Maternidad

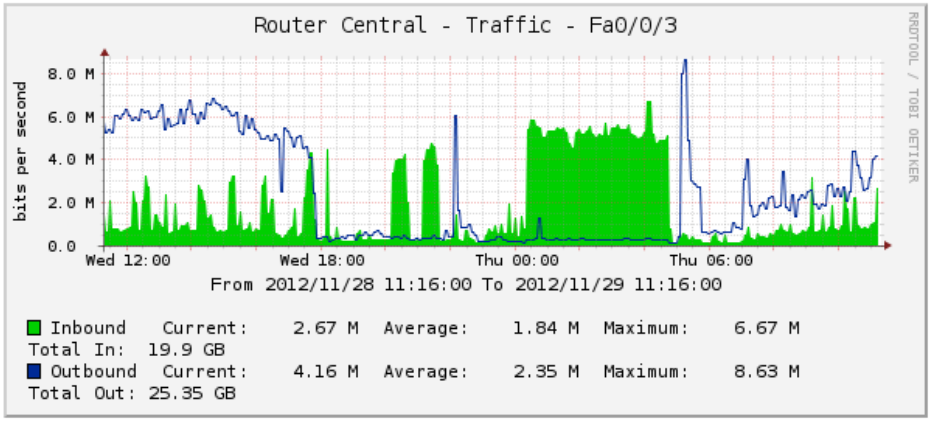


Figura 3.24 Gráfico de ancho de banda entre Oficina Central y la Maternidad

Se observa en la figura 3.25 la comunicación entre el Hospital Luis Vernaza y la Oficina Central, con un máximo de 14.14 MB sobre 20MB posibles.

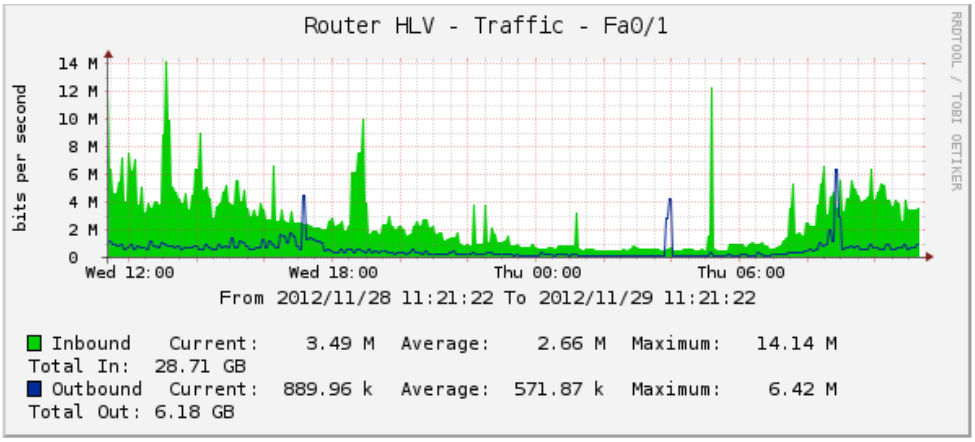


Figura 3.25 Gráfico de ancho de banda entre Hospital Luis Vernaza y la Oficina Central

Se observa en la figura 3.26 la comunicación entre el Conmutador Dlink (LAN) y el enrutador de la Oficina Central de la Junta de Beneficencia de Guayaquil, con un máximo de 34.79 MB de datos sobre 100MB posibles.

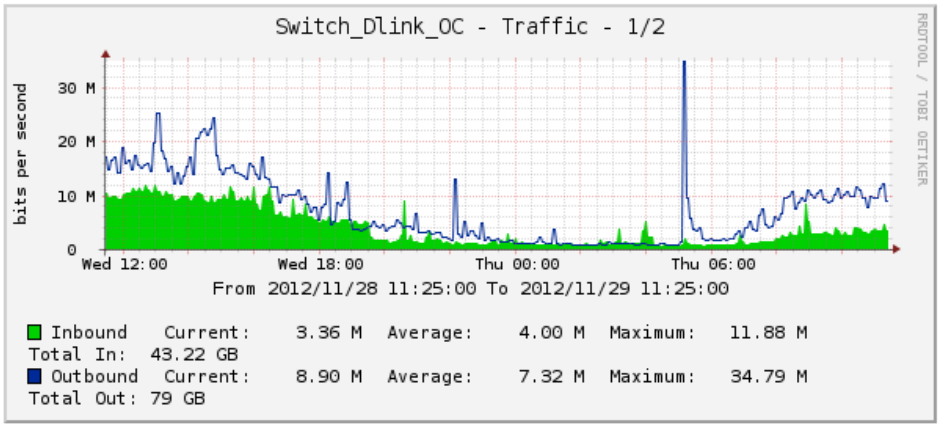


Figura 3.26 Tráfico de la LAN en Oficina Central

En la figura 3.27 se observa la comunicación entre el Conmutador Dlink(LAN) y el AS400 (BD) en la Oficina Central de la Junta de Beneficencia de Guayaquil, con un máximo de 27.39 MB de datos sobre 100MB posibles.

En la figura 3.28 se muestra el gráfico del Ancho de Banda del conmutador principal del Hospital Roberto Gilbert, con un máximo de 13.56 MB de datos sobre 100MB posibles.

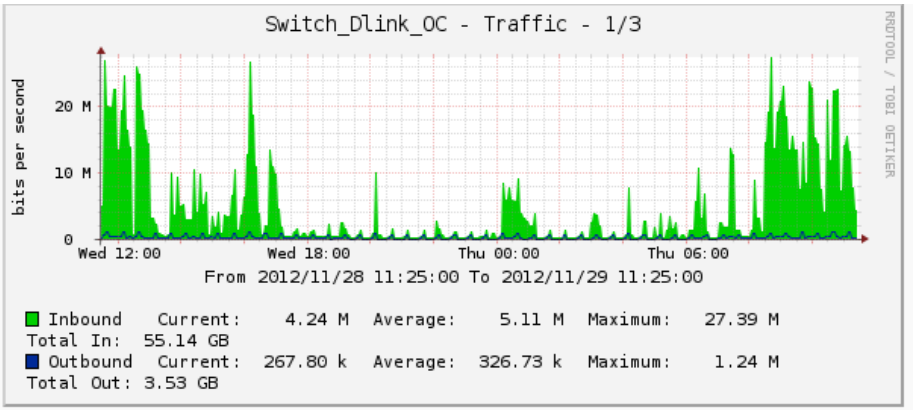


Figura 3.27. Tráfico de datos hacia el AS400 en Oficina Central

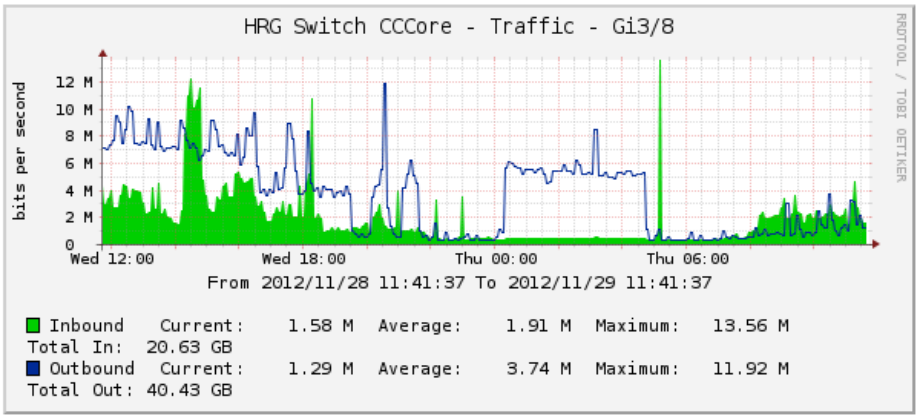


Figura 3.28. Tráfico de datos en el Switch principal del Hospital Roberto Gilbert

3.5.3 Control de enlaces

Los enlaces entre las dependencias requieren de un control permanente dentro del Sistema de Gestión de la Red, debido a la importancia del servicio que proveen.

Aquí se evaluó el consumo del ancho de banda en cada uno de los sitios de la institución, analizando las radios y los enrutadores que están en operación permanente.

Las figuras 3.29 y 3.30 corresponden al servicio de Internet con Movistar, con un tráfico de 3.56 MB y 12. 61 MB en la LAN de 14MB posibles.

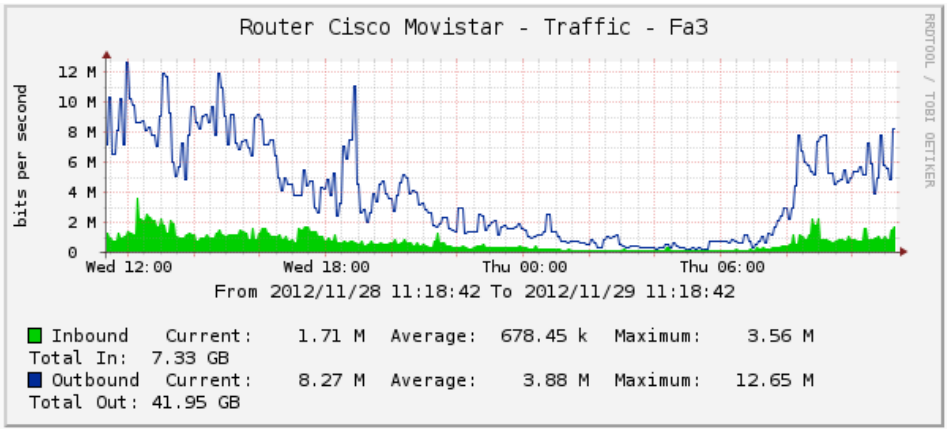


Figura 3.29. Tráfico de Internet

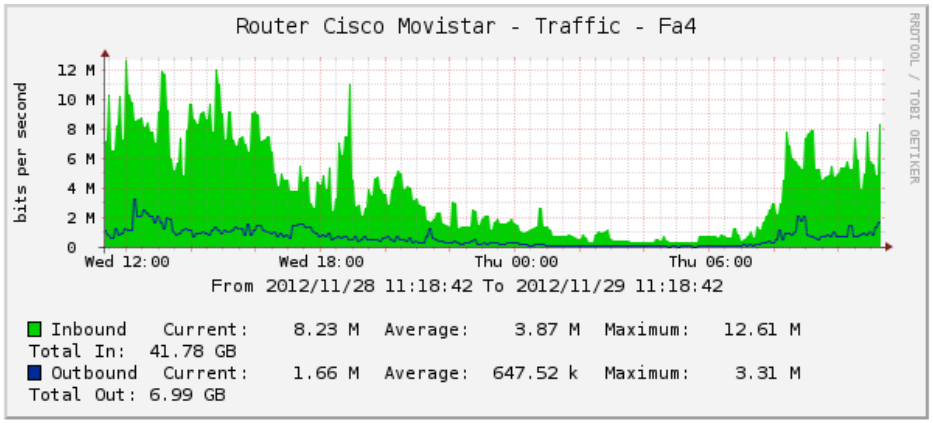


Figura 3.30 Tráfico de Internet

En la figura 3.31 se observa el Jitter y la latencia del enlace entre la Oficina Central y el Hospital Luis Vernaza.

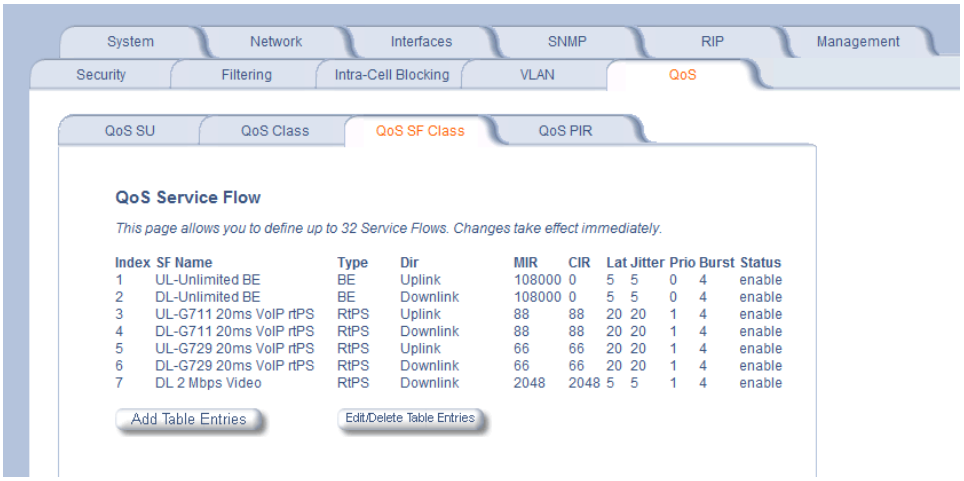


Figura 3.31 Jitter y Latencia entre Oficina Central y el Hospital Luis Vernaza

En la figura 3.32 se observa la comunicación entre La Oficina Central y la Maternidad, con un ancho de banda de entrada de 8.57MB y de 6.66MB de salida. La latencia del enlace se muestra en la figura 3.33.

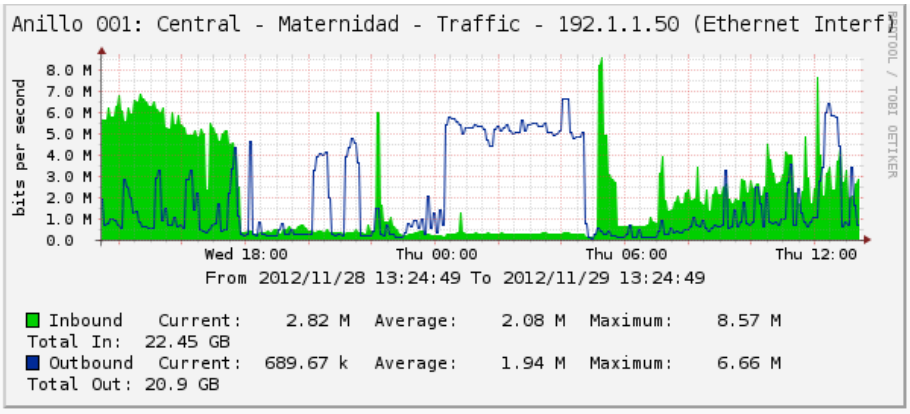


Figura 3.32 Consumo de ancho de banda entre Oficina Central y la Maternidad

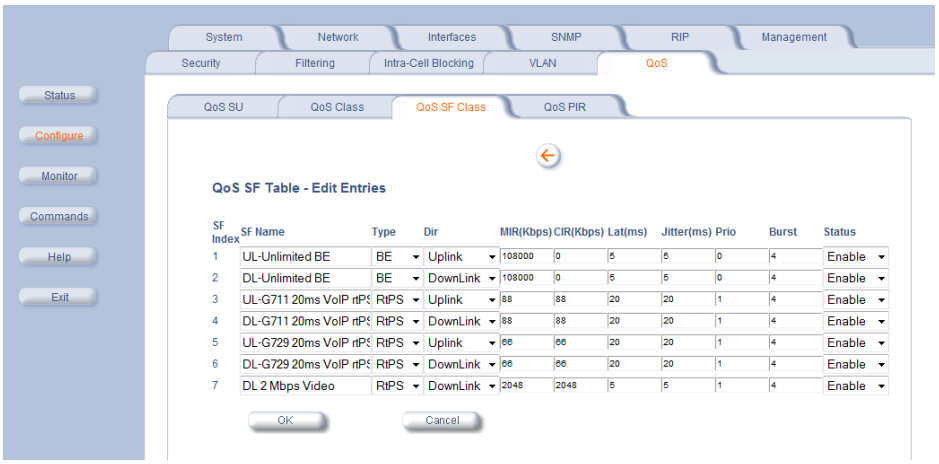


Figura 3.33. Jitter y Latencia en el radio entre Oficina Central y la Maternidad

En la figura 3.34 se observa el enlace entre la Maternidad y el punto de atención en Mapasingue. Con un ancho de banda de entrada de 5.18 MB y de 5.73 MB en la salida de 10MB posibles en conexión tipo anillo.

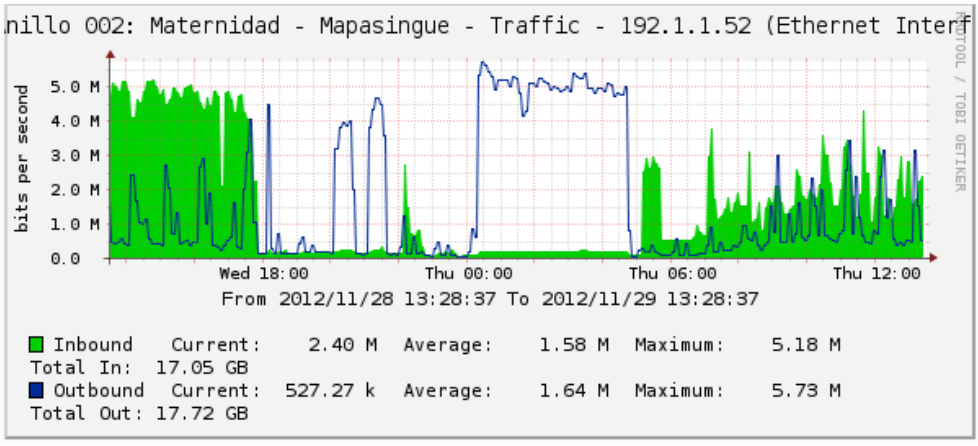


Figura 3.34 Ancho de banda del enlace entre Maternidad y Mapasingue

En la figura 3.35 se observa el enlace entre el punto de atención en Mapasingue y el Instituto de Neurociencias. Con un ancho de banda de entrada de 5.13 MB y de 5.72 MB en la salida de 10MB posibles en conexión tipo anillo.

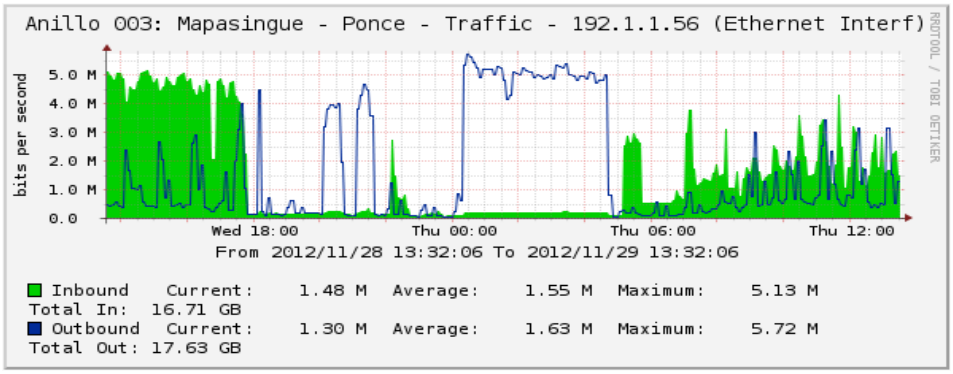


Figura 3.35 Consumo de ancho de banda del enlace entre Mapasingue e INC

En la figura 3.36 se muestra la comunicación entre el Instituto de Neurociencias y el Hospital Roberto Gilbert. Con un ancho de banda de entrada de 3.57 MB y de 5.69 MB en la salida de 10MB posibles en conexión tipo anillo.

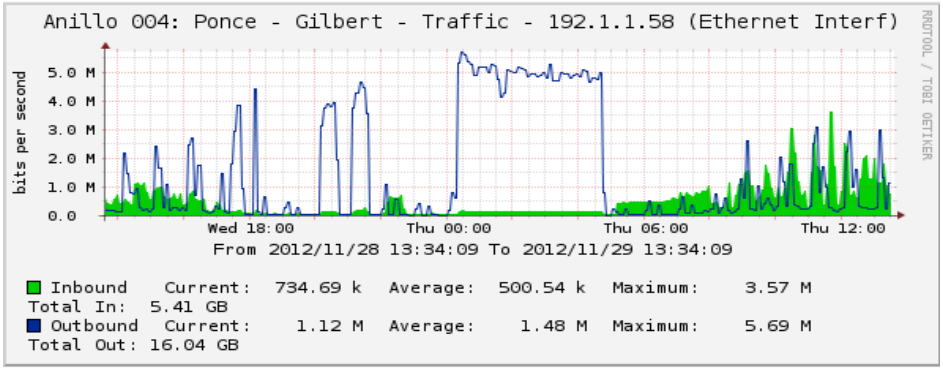


Figura 3.36 Consumo de ancho de banda del enlace entre el Instituto de Neurociencias y el Hospital Roberto Gilbert

Abajo, en la figura 3.37, se observa el Jitter y la Latencia del enlace entre el Instituto de Neurociencias y el Hospital Roberto Gilbert.

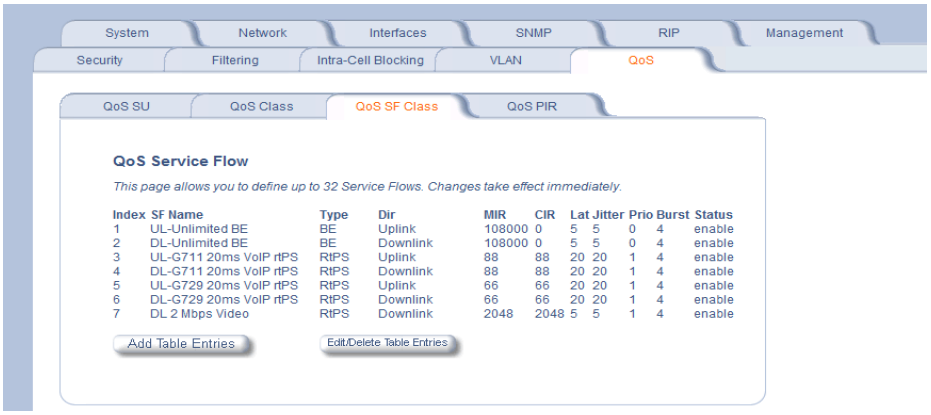


Figura 3.37. Jitter y Latencia en el radio entre el Instituto de Neurociencias y el Hospital Roberto Gilbert

En la figura 3.38 se observa el enlace entre el Instituto de Neurociencias y la Unidad Educativa Santistevan, con un ancho de banda de entrada de 0.5 MB y de 2.83 MB en la salida de 10MB posibles en conexión tipo anillo.

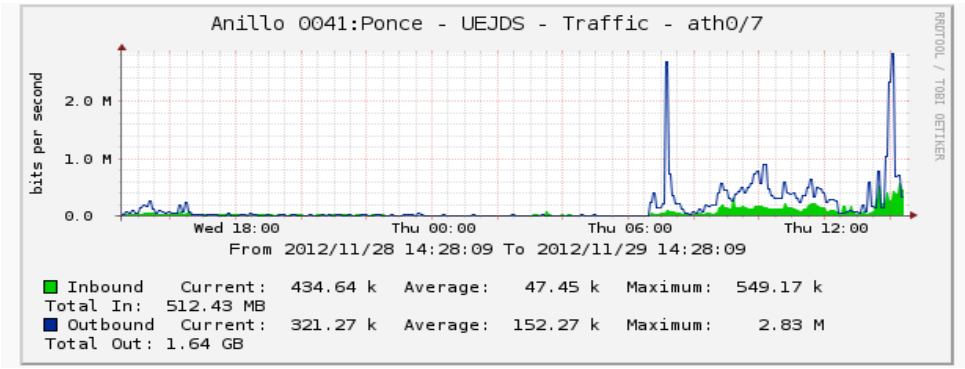


Figura 3.38 Consumo de ancho de banda del enlace entre el Instituto de Neurociencias y la Unidad Educativa José Domingo Santistevan.

En la figura 3.39 se observa el enlace entre el Hospital Roberto Gilbert y el Cementerio General. Con un ancho de banda de entrada de 5.23 MB y de 8.25 MB en la salida de 10MB posibles en conexión tipo anillo.

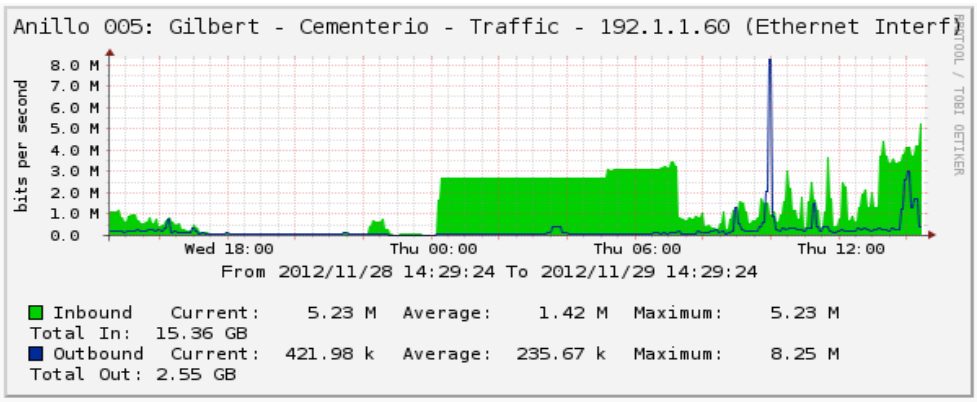


Figura 3.39. Gráfica de consumo de ancho de banda de enlace Hospital Roberto Gilbert-Cementerio General

En la figura 3.40 se observa el enlace entre el Cementerio General y el Comisariato de la Junta de Beneficencia de Guayaquil. Con un ancho de banda de entrada de 5.77 MB y de 8.13 MB en la salida de 10MB posibles.

En la figura 3.41 se aprecia el enlace entre el Comisariato de la Junta de Beneficencia de Guayaquil y el Hospital Luis Vernaza. Con un ancho de banda de entrada de 5.15 MB y

de 8.07 MB en la salida de 10MB posibles en conexión tipo anillo.

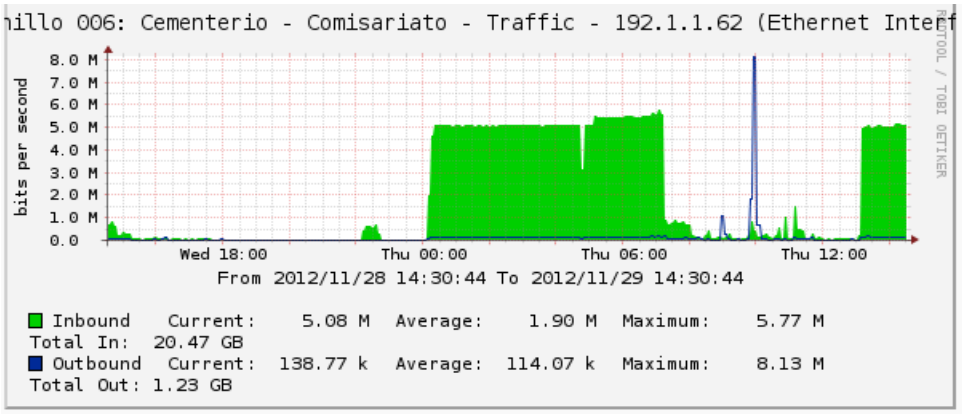


Figura 3.40. Consumo de ancho de banda entre el Cementerio General y el Comisariato de la Junta de Beneficencia de Guayaquil

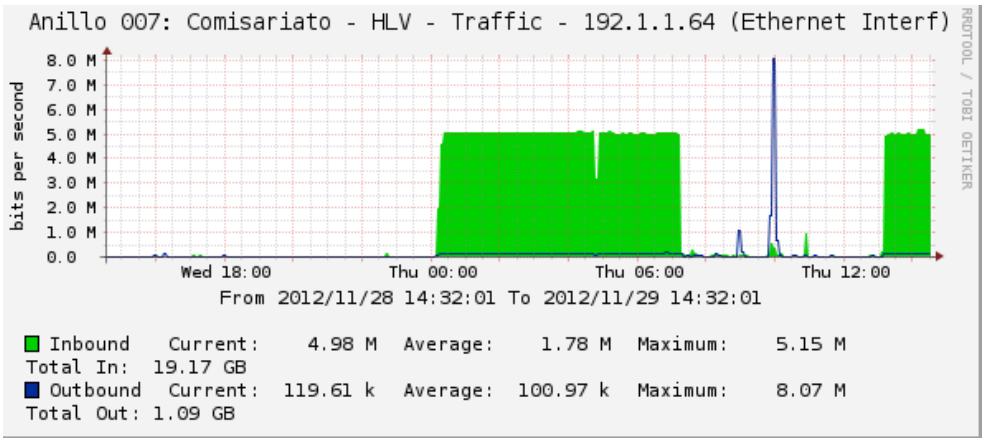


Figura 3.41. Consumo de ancho de banda entre el Comisariato y el Hospital Luis Vernaza

En la figura 3.42 se observa el enlace entre el Hospital Luis Vernaza y la Oficina Central. Con un ancho de banda de

entrada de 0.5 MB y de 0.45 MB en la salida de 10MB posibles en conexión tipo anillo.

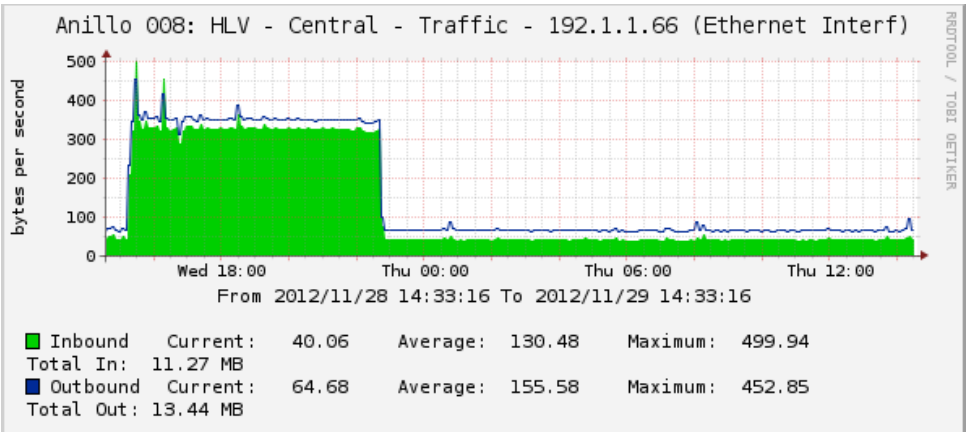


Figura 3.42. Consumo de ancho de banda entre el Hospital Luis Vernaza y la Oficina Central

En la figura 3.43 se aprecia el ancho de banda de la conexión entre la Oficina Central y el Hospital Luis Vernaza, con una salida de 12.49MB y una entrada de 7.72MB de 20MB posibles.

En la figura 3.44 se aprecia el ancho de banda de la conexión entre el Hospital Luis Vernaza y la Oficina Central, con una salida de 7.72MB y una entrada de 12.47MB de 20MB posibles.

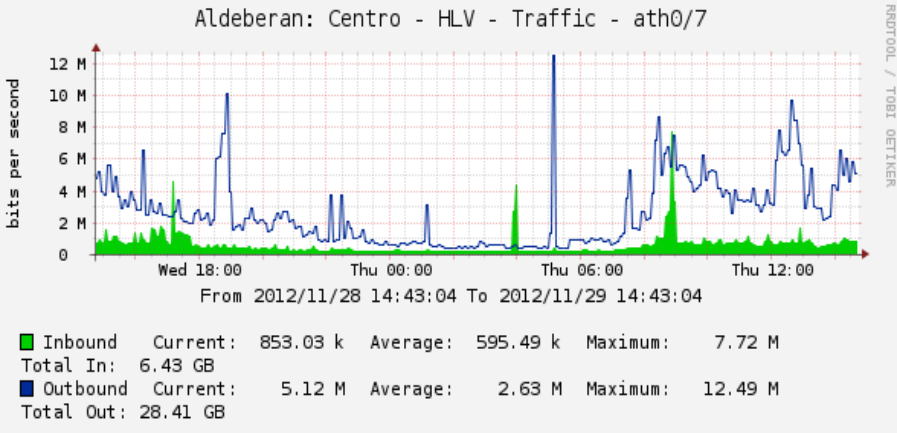


Figura 3.43. Consumo de ancho de banda entre la Oficina Central y el Hospital Luis Vernaza

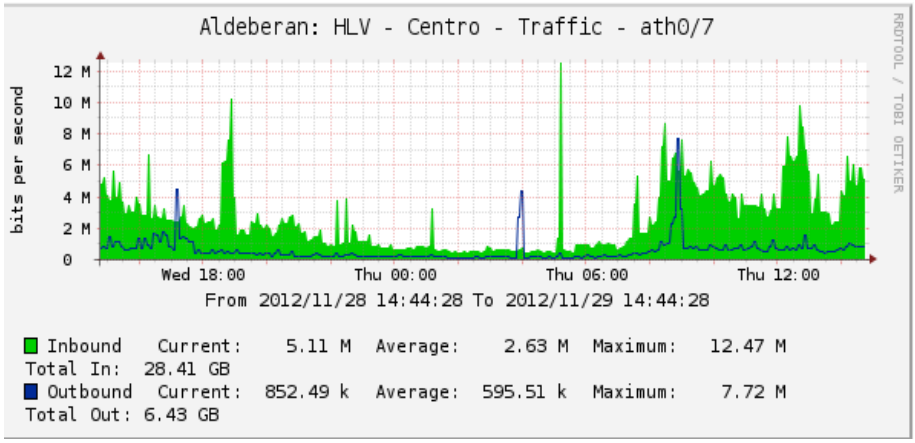


Figura 3.44. Consumo de ancho de banda entre el Hospital Luis Vernaza y la Oficina Central

En la figura 3.45 se observa el ancho de banda del enlace entre el Hospital Roberto Gilbert y la Consulta Kennedy, con una salida de 8.07MB y una entrada de 2.72MB de 20MB posibles.

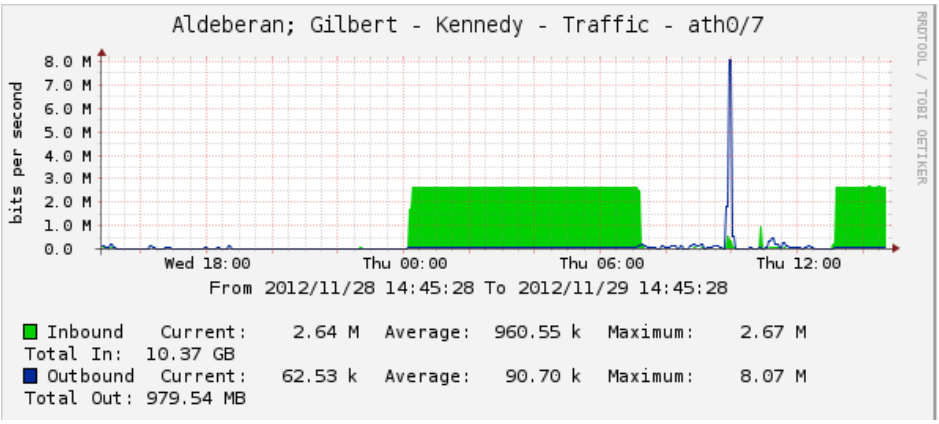


Figura 3.45. Consumo de ancho de banda entre el Hospital Roberto Gilbert y la Consulta Kennedy

En la figura 3.46 se aprecia el ancho de banda del enlace entre la Consulta Kennedy y el Hospital Roberto Gilbert, con una salida de 2.66MB y una entrada de 8.11MB de 20MB posibles.

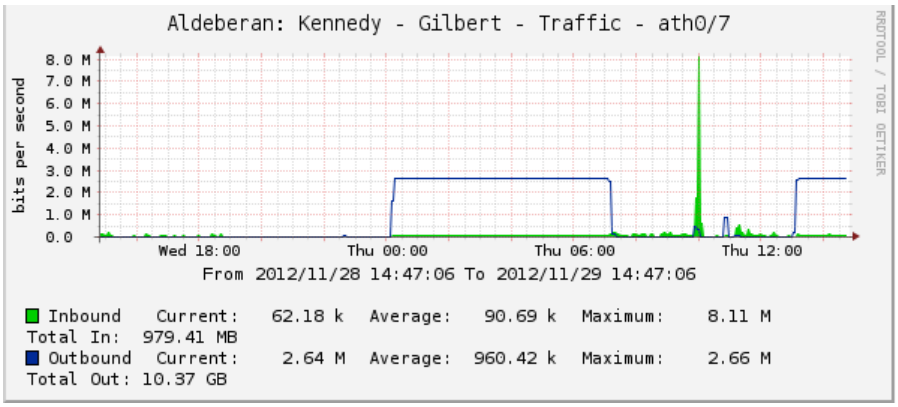


Figura 3.46. Consumo de ancho de banda entre la Consulta Kennedy y el Hospital Roberto Gilbert

En la figura 3.47 se observa la configuración del radio Rocket que establece la comunicación entre Oficina Central y el Hospital Roberto Gilbert, observándose el nivel de frecuencia, ancho del canal, distancia entre los locales, etc.

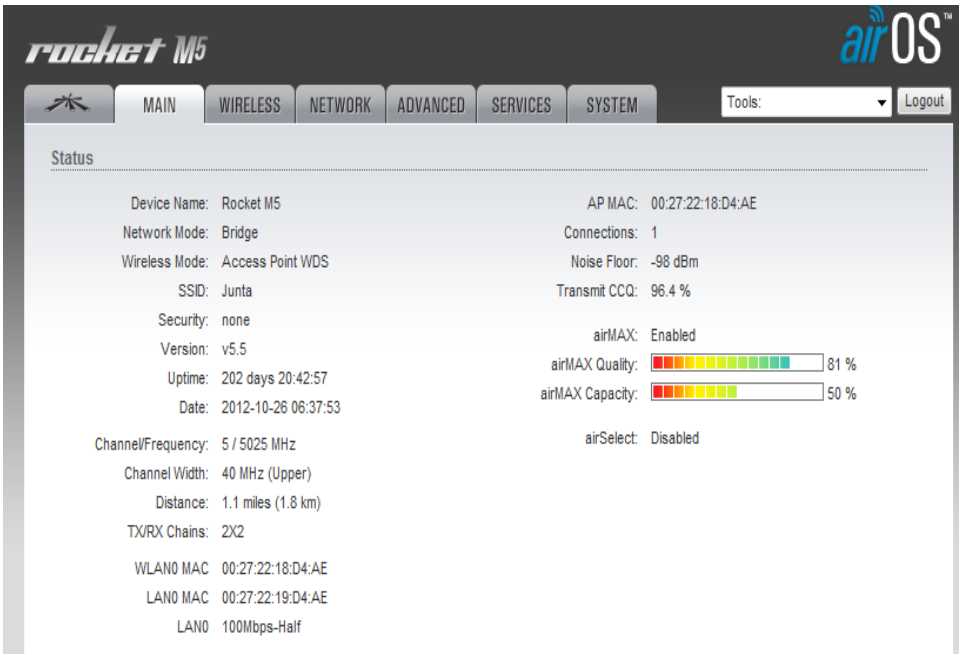


Figura 3.47. Configuración de radio rockect de Oficina Central

Abajo, en la figura 3.48 se aprecia el volumen de información del mismo radio, observándose la señal de transmisión y de recepción. La figura 3.49 muestra en cambio las interfaces de dicha radio.

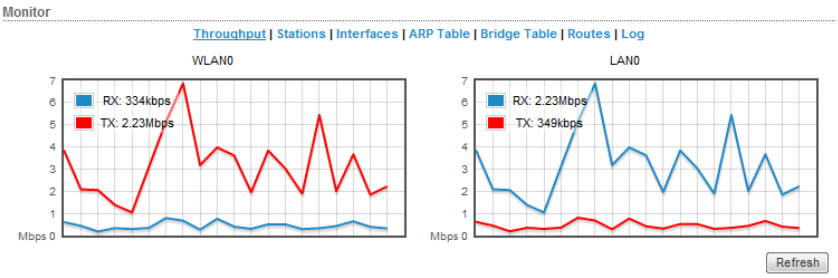


Figura 3.48 Volumen de información transmitida de radio rockect de Oficina Central

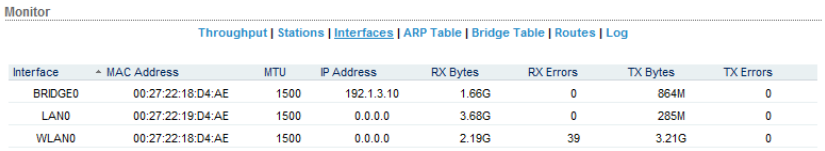


Figura 3.49. Interfaces del radio de Oficina Central

La figura 3.50 muestra la configuración del agente SNMP y del Web Server de Oficina Central en la radio Rocket correspondiente.

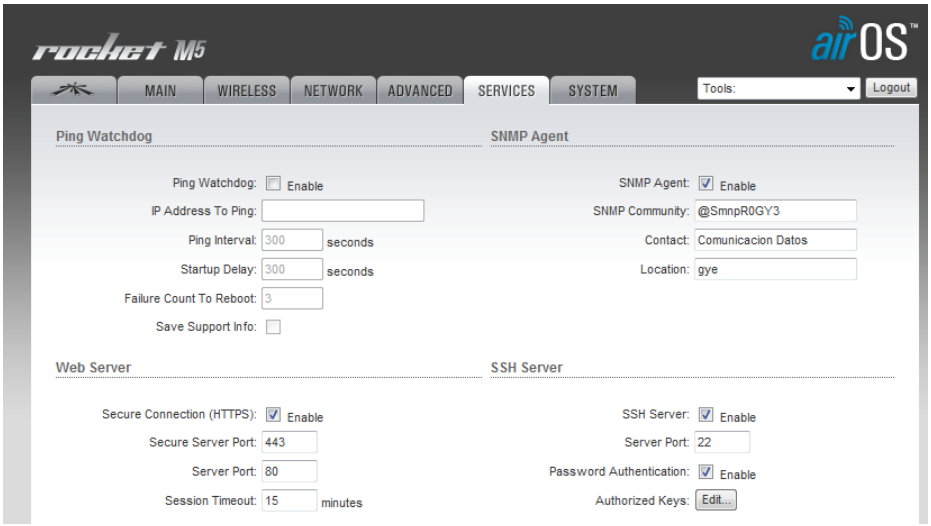


Figura 3.50 Configuración del agente SNMP y Web Server de Oficina Central

En la figura 3.51 se observa la configuración del radio que establece la comunicación entre el Hospital Roberto Gilbert y la Oficina Central, observándose el nivel de frecuencia, ancho del canal, distancia entre los locales, etc. Abajo, en la figura 3.52 se observa el volumen de información transmitida y recibida por la radio.

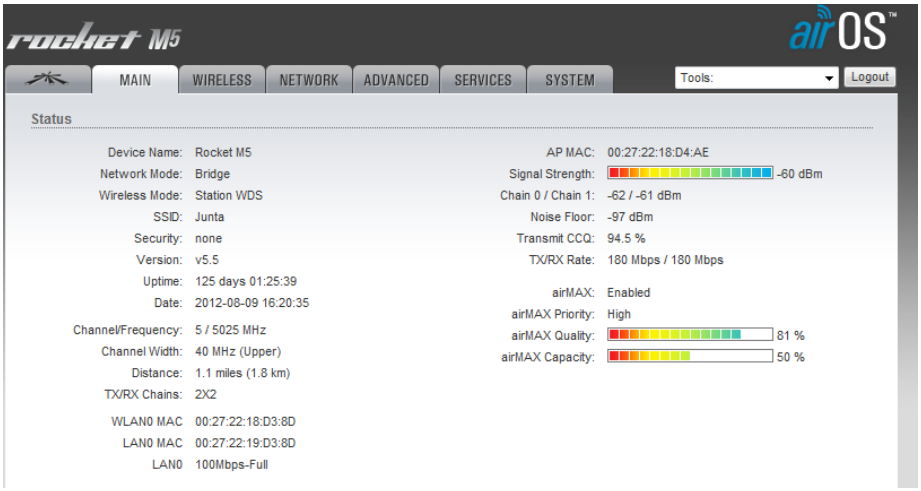


Figura 3.51 Configuración de radio rocket del Hospital Roberto Gilbert

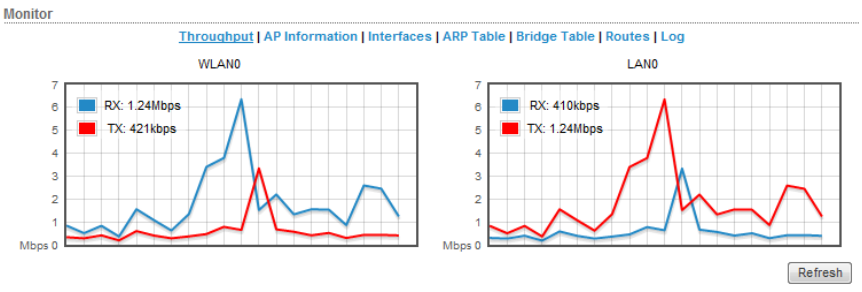


Figura 3.52 Volumen de informacion transmitida por la de radio rocket del Hospital Roberto Gilbert

La figura 3.53 muestra la configuración de la radio del Hospital Roberto Gilbert, mientras que en la figura 3.54 se observa la configuración del radio Rocket que establece la comunicación entre el Instituto de Neurociencias y el Colegio Santistevan, observándose el nivel de frecuencia, ancho del canal, distancia entre los locales, etc. Abajo, en la figura 3.55 se observa el volumen de información transmitida del mismo radio.

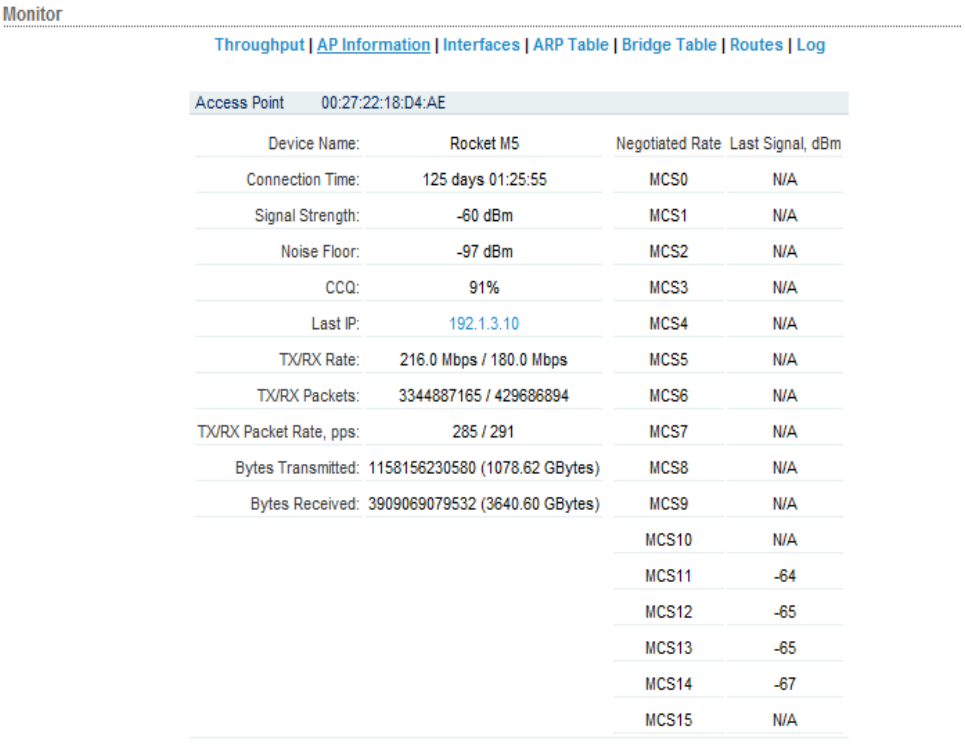


Figura 3.53. Configuración de Radio Rocket del Hospital Roberto Gilbert.

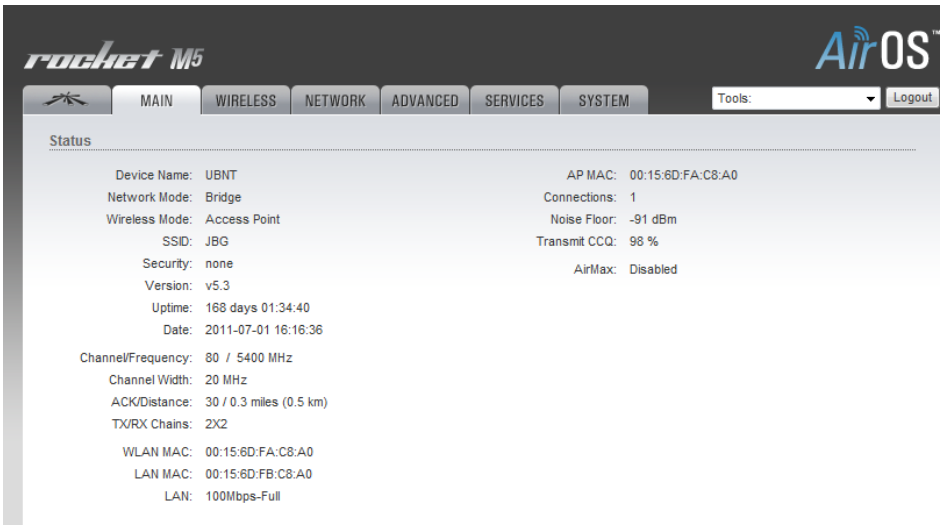


Figura 3.54. Configuración de radio Rocket Instituto de Neurociencias

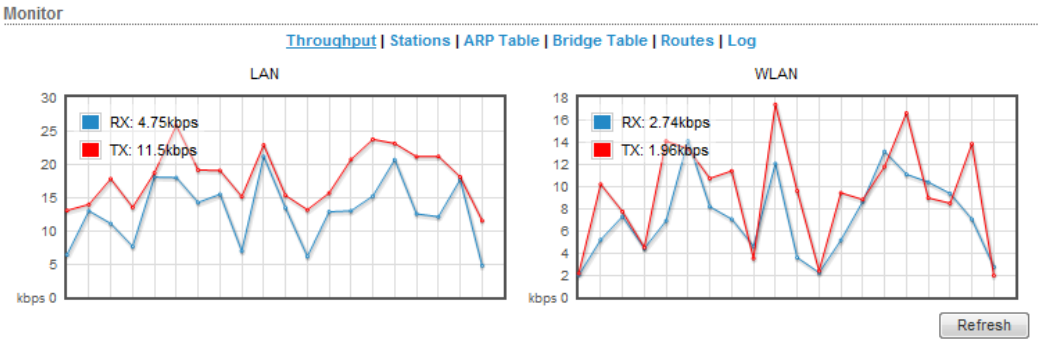


Figura 3.55 Volumen de información transmitida de la radio rocket del Instituto de Neurociencias

La figura 3.56 muestra el cuadro con la configuración de la estación MAC del radio Rocket que establece la comunicación entre el Instituto de Neurociencias y el Colegio Santistevan. En la figura 3.57 se observa la configuración del radio Rocket que establece la

comunicación entre el Colegio Santistevan y el Instituto de Neurociencias, observándose el nivel de frecuencia, ancho del canal, distancia entre los locales, etc. Abajo, en la figura 3.58 se aprecia el volumen de la información transmitida y recibida por el radio. Además la figura 3.59 muestra la configuración de la radio del Instituto Santistevan.

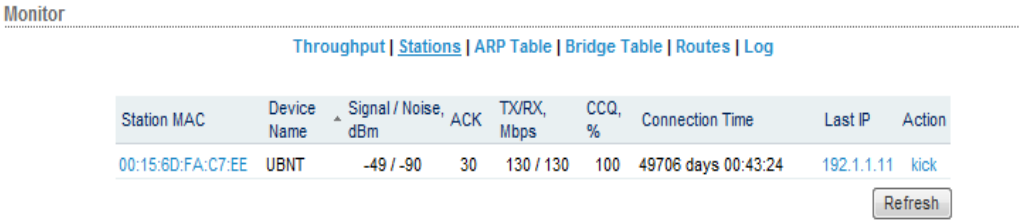


Figura 3.56. Configuración MAC del radio del Instituto de Neurociencias

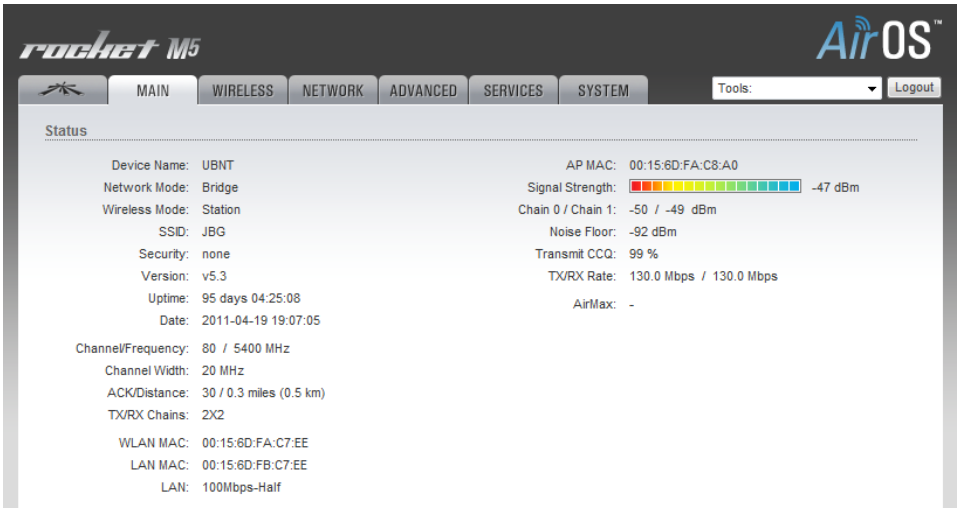


Figura 3.57. Configuración de radio Rocket Colegio Santistevan

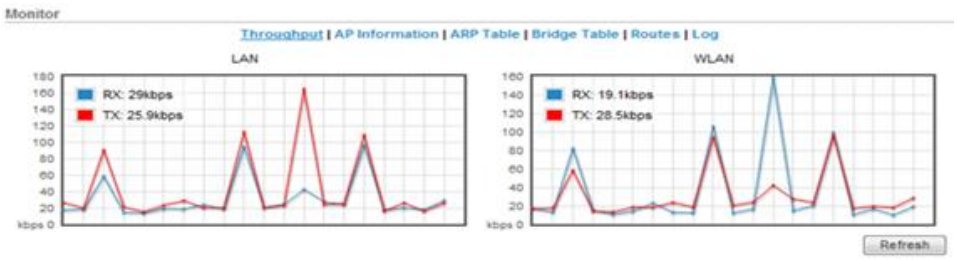


Figura 3.58 Volumen de información transmitida por la radio Rocket del Colegio Santistevan

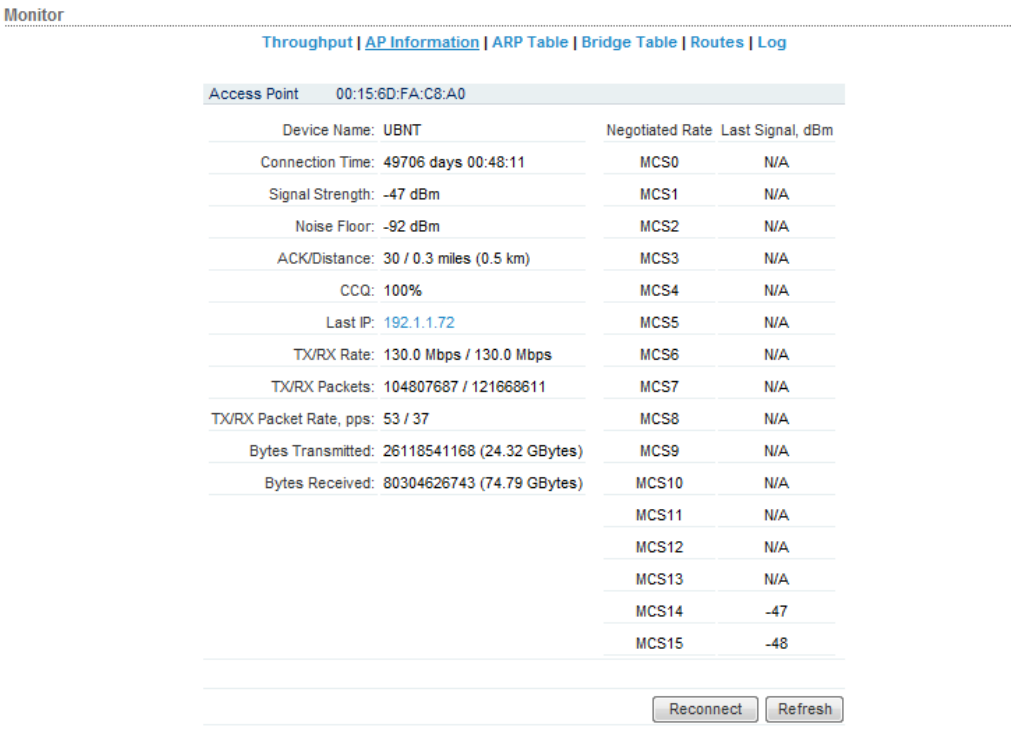


Figura 3.59. Configuración de Radio Rocket del Instituto Santistevan

3.5.4 Control de llamadas de VoIP

El sistema de Voz sobre IP aun no ha sido instalado en su totalidad en las dependencias de la Junta de Beneficencia,

sin embargo existe un proyecto que incluye a todos los hospitales y que se encuentra en su primera fase de implementación, para cubrir las llamadas a una central unificada de Help Desk. Dicho proyecto incluirá el control y registro de las llamadas, por lo que también pasará a formar parte del Sistema de Gestión de Redes. En la figura 3.60 se observa el registro de una llamada de VoIP.

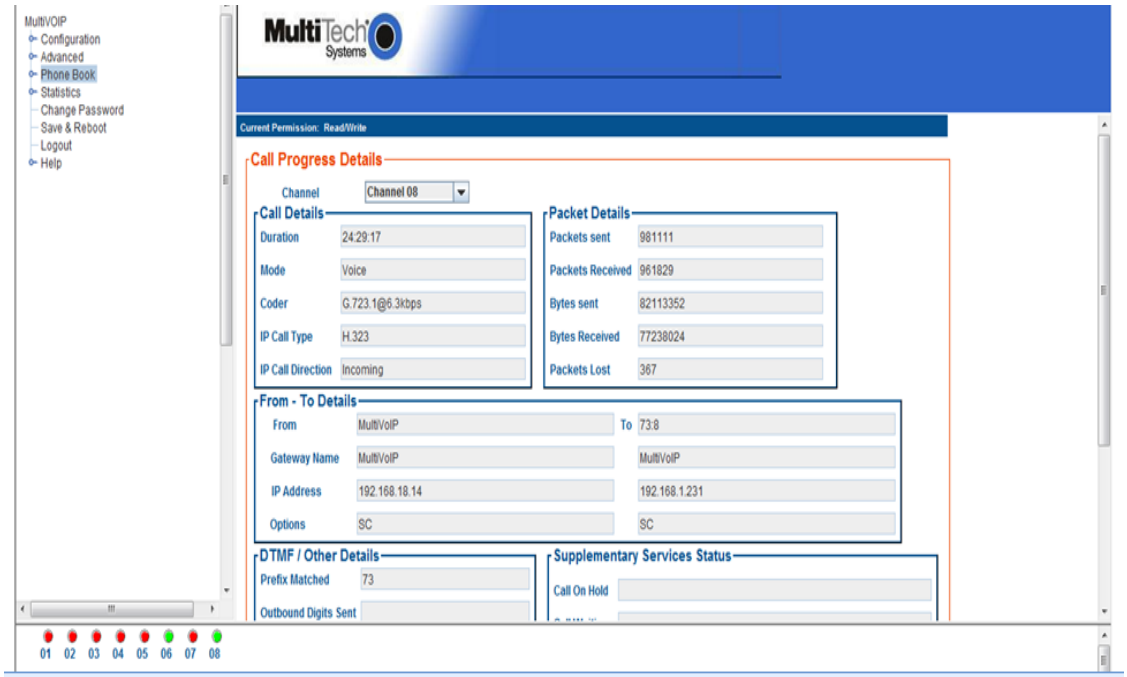


Figura 3.60. Detalle de llamada VoIP en Lotería Nacional

3.5.5 Otros controles adicionales

Otras de las aplicaciones que se controlan con el Sistema de Gestión de la Red, es la red Inalámbrica dentro de los Hospitales de la Junta de Beneficencia, que se ha constituido en un factor importante para la conexión de los equipos portátiles de los médicos extranjeros y de los visitantes en áreas no restringidas, así como para el uso de aplicaciones hospitalarias puntuales. A continuación se puede apreciar en las figuras 3.61, 3.62 y 3.63 el tráfico generado en el Hospital Roberto Gilbert.

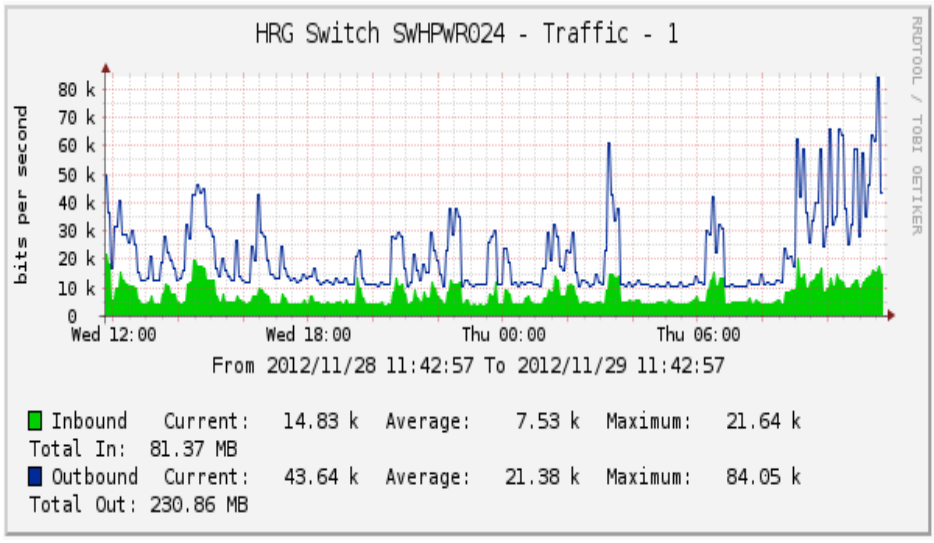


Figura 3.61 Tráfico generado en el AP conectado al puerto 1 del Conmutador

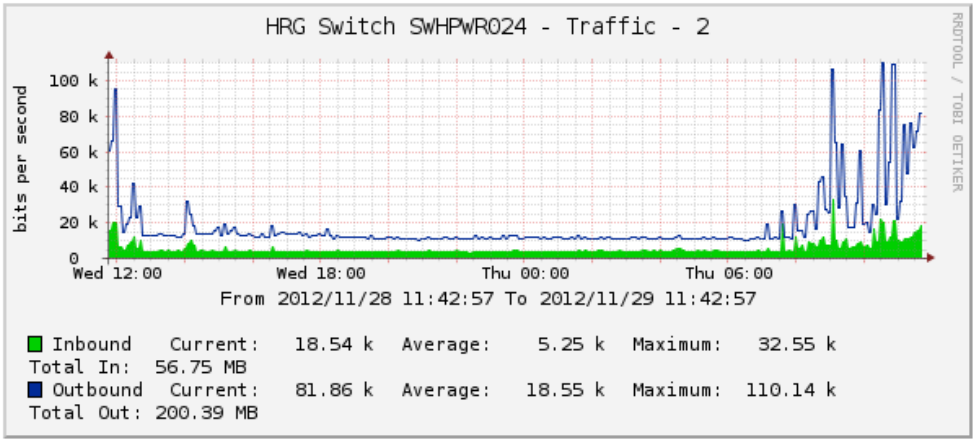


Figura 3.62 Tráfico generado en el AP conectado al puerto 2 del Conmutador

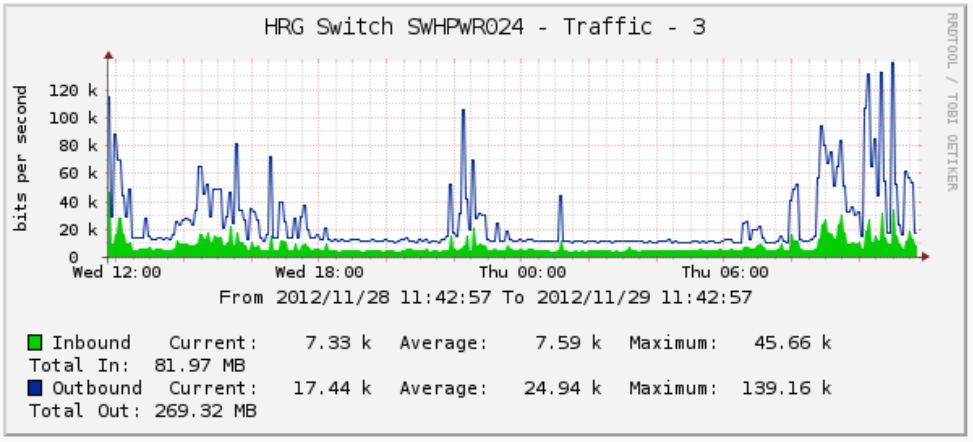


Figura 3.63 Tráfico generado en el AP conectado al puerto 3 del Conmutador

El control de la temperatura y la humedad del centro de cómputo deben ser parte del Sistema de Gestión de Redes a fin de mantener la climatización adecuada de los Servidores principales, para evitar el sobrecalentamiento

de los procesadores y otros componentes de los equipos. En la figura 3.64 se presenta la descripción de los valores de temperatura y humedad sensados en el AA del centro de cómputo, donde se muestra un incidente con el conector de red.

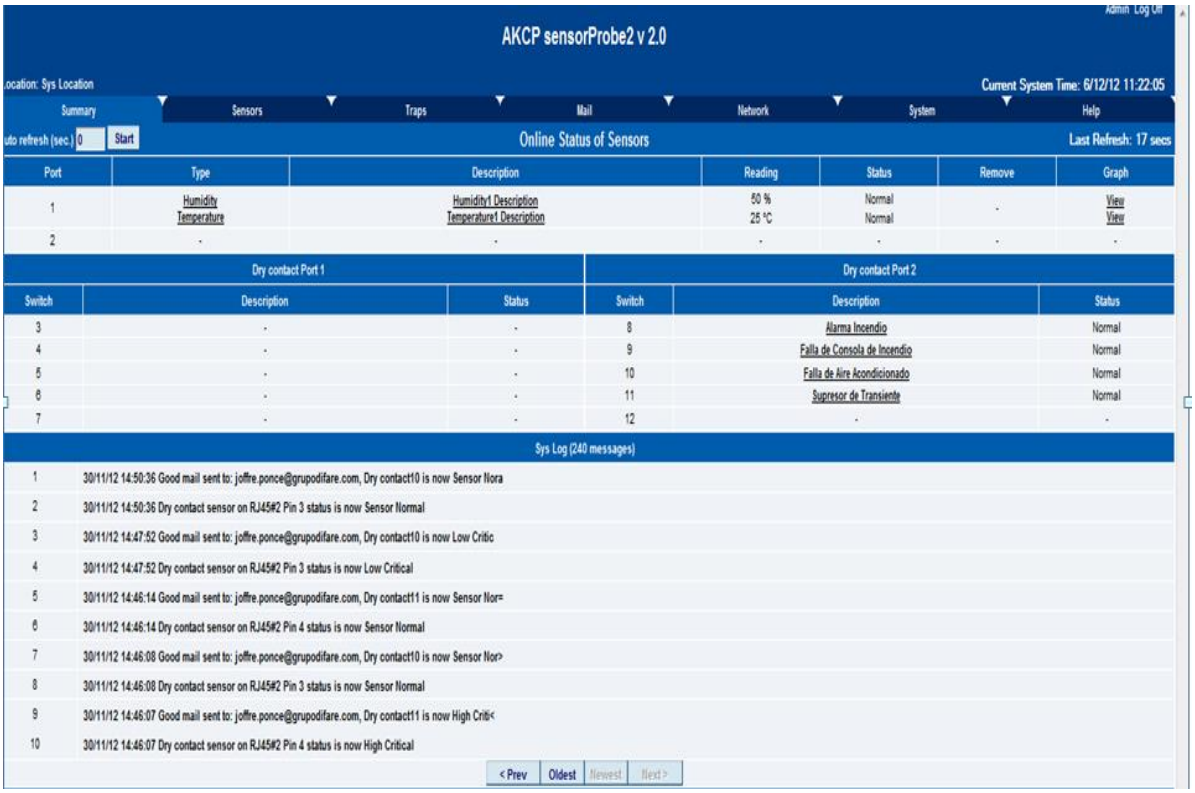


Figura 3.64 Incidente en AA Liebert

Las figuras 3.65 y 3.66 muestran los parámetros de los valores de temperatura y humedad configurados en el AA del centro de cómputo.

Figura 3.65 configuración de temperatura del AA Liebert

Figura 3.66 configuración de humedad del AA Liebert

La administración del servicio de impresión es uno de los aspectos que se puede incluir en el sistema de Gestión de Redes vía SNMP, tal como lo muestran las siguientes pantallas, donde se administra tanto el consumo de papel como de los toners. Además se pueden visualizar

advertencias e incidentes que se producen en los equipos y tomar las medidas pertinentes para atender o solucionar el requerimiento o incidente presentado. Se puede observar en la figura 3.67 el administrador de impresión, donde la impresora Láser M4555 MFP presenta una advertencia, debido a que la cubierta está abierta y la bandeja 3 está vacía.

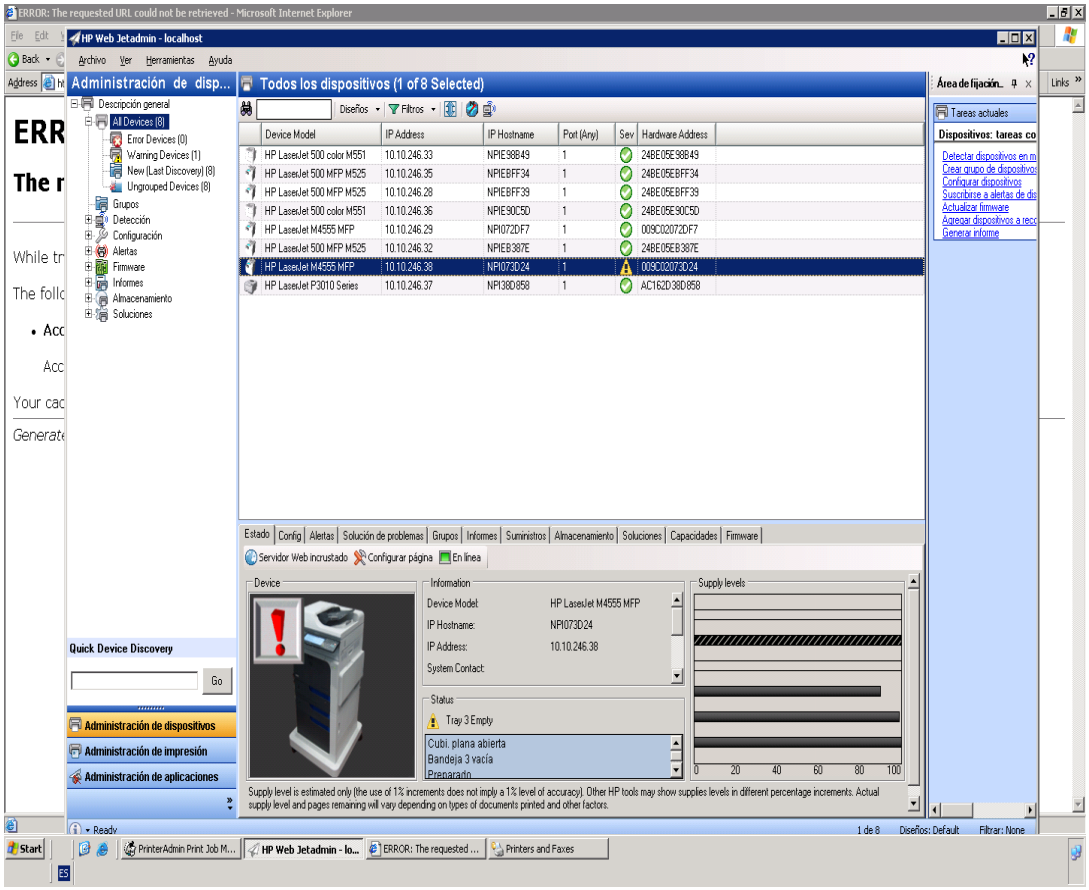


Figura 3.67 Administración de Impresoras HP

En la figura 3.68 se puede observar que una de las impresoras Láser M4555 MFP presenta una advertencia, debido a un cartucho de tinta negro bajo.

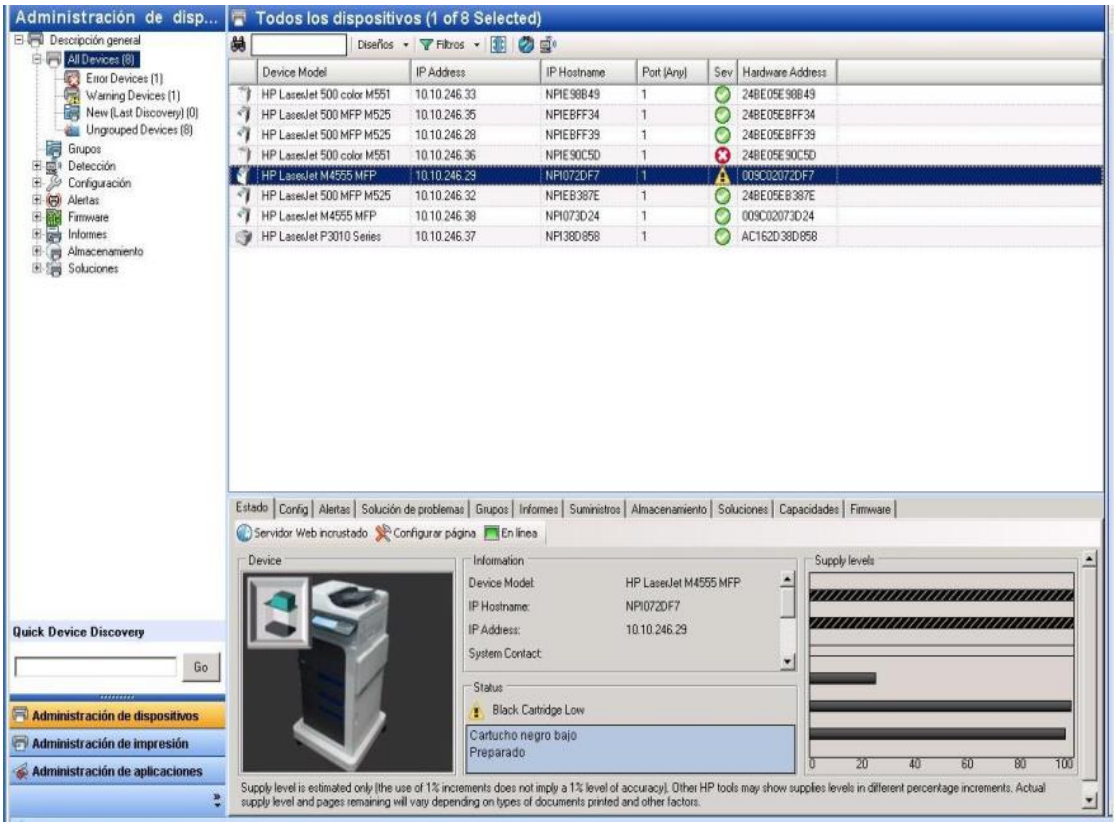


Figura 3.68 Administración de Impresoras HP

En la figura 3.69, en cambio, se puede apreciar en el administrador de impresión que una de las impresoras Láser M551 presenta un error de comunicación.

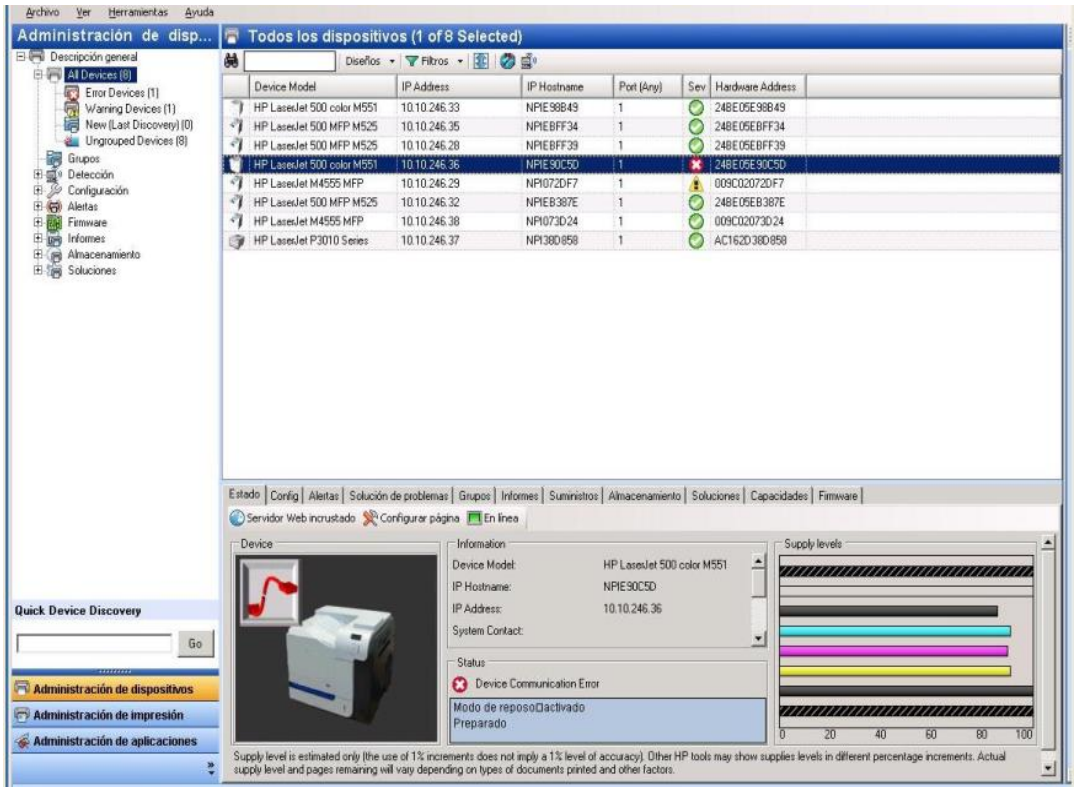


Figura 3.69 Administración de Impresoras HP

CAPÍTULO 4

DISEÑO DE LA SOLUCIÓN

La solución se diseñó e implementó con varios dispositivos de hardware, los que en unión del software adecuado, permiten la lectura de datos que los agentes facilitan para el control de los parámetros de TI.

4.1 Dispositivos de control SNMP

Los dispositivos de hardware (agentes) que permitieron la lectura de datos de control a través del protocolo SNMP utilizados en el Sistema de Gestión de la Red de la Junta de Beneficencia son: Tarjetas SNMP para UPS General Electric de 10Kva, Conmutador Cisco Catalyst 2960, Conmutador Cisco 3750, Enrutador Cisco 2911, Radio Ubiquiti Rocket M5 y Tarjetas SNMP para Aire Acondicionado Liebert, entre otros.

4.1.1 Tarjeta SNMP para UPS

La interfaz SNMP / Web de GE, presenta la información sobre el UPS de dos maneras [21]: Agente SNMP y Servidor Web.

Agente SNMP: La información que provee el protocolo SNMP cumple con el estándar UPS-MIB, definido en el RFC1628, permitiendo uno o más SMN para monitorear, administrar y controlar el UPS. El proceso de gestión de GE, que se observa en la figura 4.1, incluye el uso de un software de monitoreo remoto, para determinar el estado del UPS, garantizar la desconexión segura y ordenada cuando se requiera.

Servidor Web: Para monitorear y controlar el UPS se puede utilizar el formato HTML en cualquier navegador de internet, desde cualquier estación de trabajo y desde cualquier punto geográfico. En la figura 4.2 podemos apreciar la tarjeta SNMP GE utilizada para la comunicación de los UPS de 10Kva.

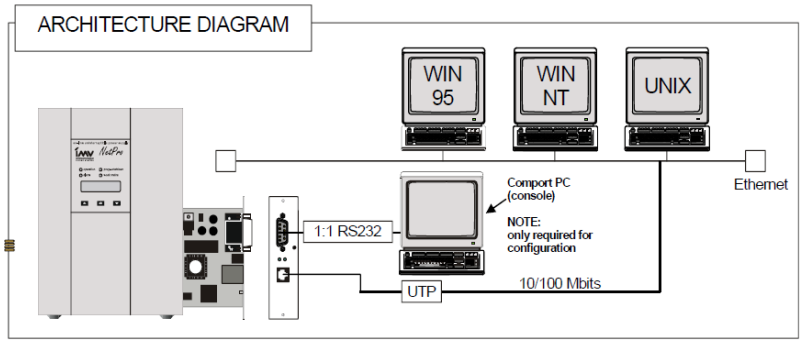


Figura 4.1 Diagrama de comunicación Sistema de Gestión de UPS, Manual de tarjeta SNMP GE [21]

Figura 4.2. Tarjeta SNMP GE, Manual de tarjeta SNMP GE [21]

En la figura 4.3 se observan los puertos y leds de la tarjeta SNMP utilizada:

1) Led Verde: Define 4 modos de funcionamiento:

a. Encendido y estable: Tarjeta alimentada, pero no hay ninguna comunicación con el UPS.

b. Parpadeo lento (1/seg.): Tarjeta alimentada y con comunicación con el UPS.

c. Parpadeo rápido (6/sec.): Tarjeta actualizando la ROM, no se debe resetear o desconectar la tarjeta en este momento.

d. Al iniciarse la tarjeta en modo de restauración, el LED correspondiente está intermitente.

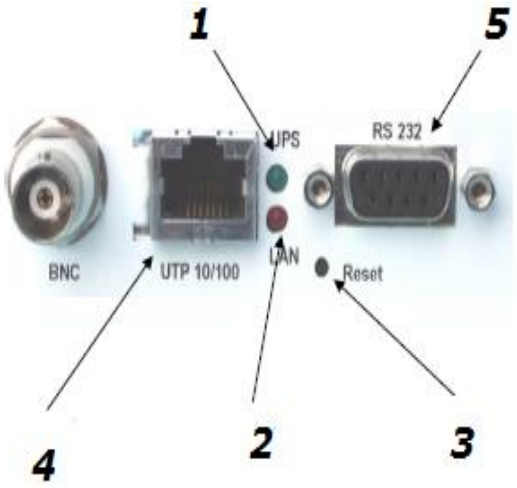


Figura 4.3. Puertos de la Tarjeta SNMP GE, Manual de tarjeta SNMP GE [21]

2) Led rojo: Cuando existe transmisión y recepción de los paquetes en la red LAN.

3) Reset: Para un reset de la tarjeta.

4) Puerto RJ45: Para comunicarse a 10 o 100 Mbits según el estándar 10BaseT o 100Base TX.

5) Puerto RS232: Para configurar la tarjeta.

4.1.2 CONMUTADOR CISCO 2960

Los conmutadores de Cisco Catalyst Serie 2960 ofrecen la opción de administración vía SNMP y presentan un amplio número de características, entre las que se incluyen [22]: Instalación de una única red que cubra las necesidades de comunicación, gracias al soporte para comunicaciones de datos, inalámbricas y voz. Capacidad de Power over Ethernet, que permite implementar nuevas funcionalidades, como voz y tecnología inalámbrica, ahorrando el uso de un nuevo cableado. Conexiones de tipo Fast Ethernet (transferencia de datos de 100 Mbps) o Gigabit Ethernet (transferencia de datos de 1000 Mbps), dependiendo de las necesidades de rendimiento. Diversos modelos de configuración, permitiendo conectar computadores, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red. Configuración de LANs virtuales, para que los empleados se conecten a través de funciones de organización, equipos de proyecto o aplicaciones.

Además presenta seguridad integrada**,** monitorización de red y solución de problemas de conectividad mejoradas, actualizaciones de software sin gastos adicionales y garantía de hardware de por vida. En la figura 4.4 se observa el conmutador Cisco 2960.

Figura 4.4 Conmutador Cisco 2960, Cisco, Brochure Cisco catalyst 2960

4.1.3 Conmutador Cisco 3750

Los conmutadores de la serie Cisco Catalyst 3750, son empleados especialmente en organizaciones medianas y en sucursales de empresas de gran tamaño. Utiliza la tecnología StackWise™, mejorando la eficacia de las redes LAN, combinando su facilidad de uso y la máxima resistencia en conmutadores apilables [23].

La arquitectura de apilamiento de Cisco StackWise proporciona a los conmutadores apilables un alto nivel de

resistencia, automatización, seguridad avanzada integrada, calidad de servicio, disponibilidad y rendimiento. Mediante la tecnología Cisco StackWise, las organizaciones pueden crear una sola unidad de conmutación de 32 Gbps con hasta nueve conmutadores de la serie Cisco Catalyst 3750. Pueden utilizarse los conmutadores de 24 y 48 puertos de 10/100/1000 Mbps con PoE para garantizar la máxima productividad y la protección de la inversión, y a la vez pueden implementarse nuevas aplicaciones como telefonía IP, acceso inalámbrico, vigilancia por video, sistemas de administración de edificios y puntos remotos de información con video. En la figura 4.5 se puede observar un conmutador Cisco 3750.

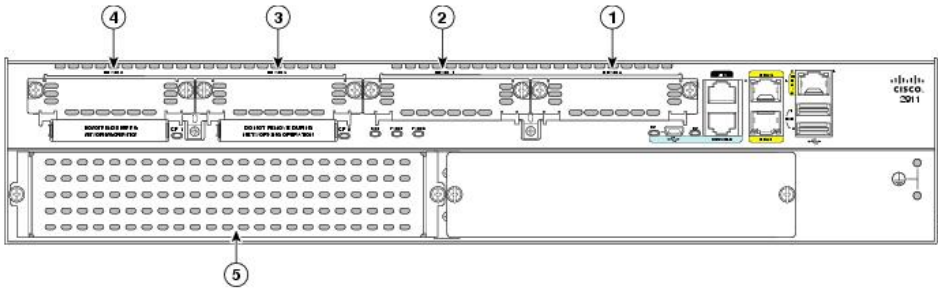
Figura 4.5 Conmutador Cisco 3750. Brochure Cisco Catalyst 3750

4.1.4 Enrutador Cisco 2911

La serie de Enrutadores Cisco 2911, son equipos con protocolo de conexión remota SNMP, que proporcionan

datos de alta seguridad, voz, video y servicio de aplicación. Las características claves incluyen [24]: 3 puertos Ethernet 10/100/1000 integrados, una ranura para el módulo de servicio, ranuras mejoradas de alta velocidad para interfaz WAN, 2 ranuras para el procesador de señales digitales (DSP), una ranura de Servicio Interno para el módulo de servicios de aplicaciones.

Posee distribución de energía integrada mejorada, a través de los módulos de soporte 802.3af Power over Ethernet (PoE) y Cisco PoE, también presenta un sistema de seguridad con gestión de la identidad, mediante la autenticación, autorización y la infraestructura de clave pública, además tiene soporte optimizado para voz y video, con normas certificadas para los servicios del navegador VoiceXML. En las figuras 4.6 y 4.7 se aprecian las interfaces del enrutador 2911 y las tarjetas Ethernet de 4 y 8 puertos, utilizados en la operación de control de la red.



1	EHWIC 0	4	EHWIC 3
2	EHWIC 1	5	Service module slot (SM)
3	EHWIC 2		

Figura 4.6. Interface Card Slot en los Enrutadores Cisco 2911. Catalogo Cisco http://www.cisco.coml

Figura 4.7. Cisco Gigabit Ethernet EHWICs de 4 y 8 puertos, Tomado de página Cisco, http://www.cisco.com

4.1.5 Radio Ubiquiti Rocket M5

Es un radio de alta potencia, MIMO 2x2, muy lineal, con el funcionamiento del receptor mejorada. Cuenta con un rendimiento increíble (50Km) y con una velocidad de avance de 150Mbps. El dispositivo fue diseñado específicamente para el aire libre en sistema punto a punto y aplicaciones

Airmax [25]. En la figura 4.8 se puede observar el modelo de la radio Ubiquiti.

Las características técnicas principales son: Posee un procesador “Atheros” MIPS 24KC, 400MHz, memoria de 64MB SDRAM con 8MB Flash, Interfaz de red: 10/100 BASE-TX (Cat. 5, RJ-45), tamaño: 16cm x 8cm x 3cm, consumo máximo: 6.5 watts, energía pasiva a través de Ethernet, temperatura de operación a la intemperie: -30°C a 75°C y fuente pasiva de potencia sobre la red de datos para 110-240VAC, 24VDC, 1A y alimentación tipo americano.

Figura 4.8. Radios Ubiquiti Rocket M5. Catálogo Ubiquiti Rocket M5

4.1.6. Tarjeta SNMP para Aire Acondicionado

Para controlar la temperatura y humedad del AA Liebert, se requiere la instalación de la tarjeta SNMP, "Web Liebert OC de Emerson Network Power", que permite manejar un amplio rango de parámetros de funcionamiento, alarmas, notificaciones, transfiriendo los datos medidos por la red [26]. Ver figura 4.9.

Figura 4.9. Tarjeta SNMP para AA Liebert. Tomado de Emerson, http://www.emersonnetworkpower.com/

4.2 Software basado en SNMP

Para administrar los equipos se requiere del software adecuado para el registro, graficación y levantamiento de datos las 24 horas del día, en algunos casos es propietario del Hardware (UPS GE), y en otros casos es una combinación de software propietario y una aplicación de uso libre. Si se requiere centralizar el monitoreo, mediante el uso de software especializado, los costos dependerán

del número de sensores o agentes requeridos. La inversión podría llegar a $20000 según sea el caso.

Los usados en el Sistema de Control de la Junta de Beneficencia son: Software UPS GE (propietario), Software AA Liebert (propietario), Software de VoIP (propietario), Software de radios Tsunami y Rocket (propietario) y Cacti (software libre). Todos ellos implementados sin costo. Sin embargo, existen otras aplicaciones que pueden ser consideradas, como, SCADA, PRTG y Nagios.

4.2.1 Software UPS GE

La configuración y los eventos de los UPS GE están disponibles en formato HTML, lenguaje básico de la comunicación por internet. Además cada navegador de Internet estándar se puede utilizar para monitorear y controlar el UPS usando HTML desde cualquier punto de la red o incluso desde cualquier parte del mundo.

Es un sistema básico y sencillo que permite configurar las trampas, los correos del personal técnico, y registrar eventos en el log, además de poder visualizar los valores de voltaje, corriente y temperatura de las baterías y del

sistema de entrada/salida del UPS. Los valores de carga también son proporcionados para mantenerse en el umbral máximo.

4.2.2 Software AA Liebert

Es una aplicación amigable que permite configurar los parámetros básicos del AA como temperatura y humedad, así como las direcciones de soporte que deben recibir las alarmas o los cambios de estado. Asi mismo realiza el registro de los logs de eventos que ocurren.

4.2.3 Software VoIP

Los logs de VoIP, son presentados de una forma básica, incluyendo los registros de las llamadas en el protocolo SIP, con detalles de inicio de llamada, direcciones IP del solicitante y solicitado, nombre del usuario, etc.

4.2.4 Software Radios Tsunami y Rocket

Ambos equipos de comunicación presentan un entorno Web amigable con información básica: En el Rocket, se puede determinar los niveles de frecuencia, ancho de banda, distancia entre puntos, valor de ruido (dB), gráfico

de la señal de transmisión y recepción, relación señal/ruido, MAC Adress, IP Adress, Rx errors, etc. En el caso de las radios Tsunami, se puede observar los niveles de frecuencia, ancho de banda, valores de Jitter, latencia, burst, MIR y CIR, registro de logs, etc.

4.2.5 Software CACTI

CACTI, permite representar en forma gráfica los datos guardados en una base de datos, llamada RRD, tales como temperatura, voltaje, número de impresiones, uso de la conexion a internet, etc [27].

Las plantillas de CACTI presentan gráficas avanzadas, a través de una interfaz fácil de usar y con herramientas para la gestión de los usuarios, en redes del tamaño de una LAN, hasta redes más complejas. Todo esto es procesado a través de un sensor, que se encarga de tomar los datos que se almacenan en una base de datos SQL.

CACTI, define una fuente de datos estableciendo la forma del almacenamiento de los datos y la infomación que se requiere, la misma que se mantiene en intervalos de 5

minutos. Una vez hecha la definición de la base, se puede crear el gráfico esperado usando los distintos tipos de gráficos estándar de RRD y las opciones de consolidación.

Una de las funcionalidades de esta herramienta de gestión, es la capacidad de añadir nuevos usuarios y otorgarles derechos a ciertas áreas de operación dentro de CACTI. Por lo tanto el nivel de gestión puede varios entre los múltiples usuarios, habrá quienes visualicen la informacion gráfica unicamente y otros que podrán incluso modificarla.

4.2.6 SCADA

"Es sinónimo de control de supervisión y adquisición de datos, cualquier aplicación que obtiene los datos acerca de un sistema con el fin de controlar lo que hace el sistema es una aplicación SCADA" [28]. Una aplicación SCADA tiene dos elementos:

- El proceso: Sistema-Máquina que se va a supervisar, como por ejemplo, un sistema eléctrico, una red, un sistema de semáforos, o cualquier otro elemento.

- Una red de dispositivos inteligentes que interactúan con el sistema-máquina, a través de sensores y controles de salidas, para tener la capacidad de medición y control de ciertos elementos del primer sistema.

Con SCADA podemos gestionar todo tipo de equipos. Su aplicación típica es la regularización y automatización de los procesos de la industria cuando se tiene que controlar sistemas con un alto número de controles sensibles y demasiado ágiles para el control del hombre. En la figura 4.10 se muestra un diagrama referente a los usos, que alrededor del mundo se controlan con SCADA y en la figura 4.11 se pueden apreciar las principales funciones de SCADA, como la adquisición, presentación y control de los datos, y el control de las operaciones.

SCADA monitorea sistemas complejos, por lo que para la adquisición de datos supervisa cientos o miles de sensores, tanto de entrada al sistema (voltaje de entrada a UPS) como de salida (presión de valvula de liberación de agua en un depósito).

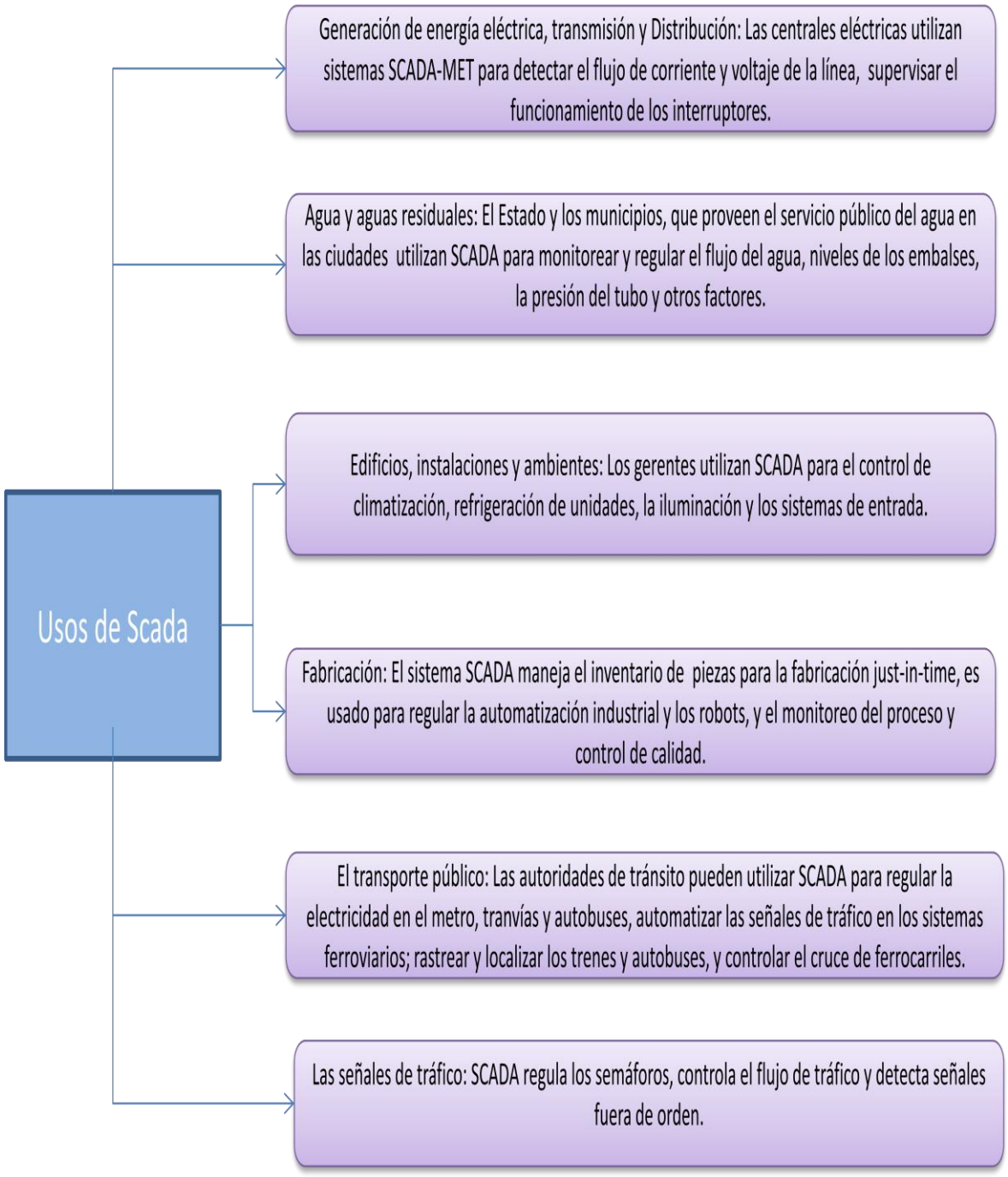


Figura 4.10 Usos del sistema SCADA.

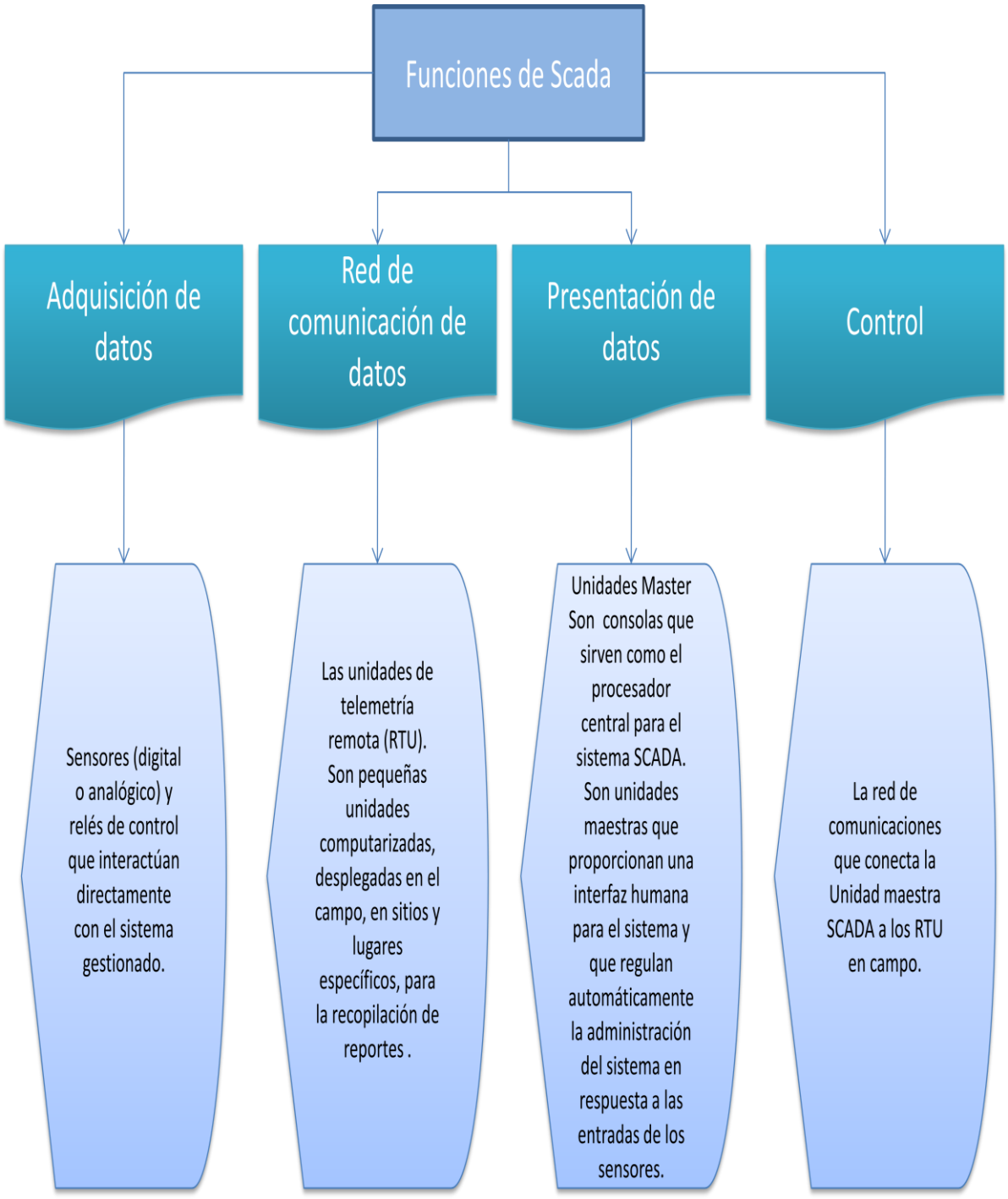


Figura 4.11. Funciones de SCADA

Como SCADA controla varios sistemas desde una operadora central, necesita usar la red de comunicaciones para que los sensores envíen los datos que recolectan. Por razones de seguridad, se recomienda que se trabaje en una red LAN/WAN cerrada, para que no haya exposición de datos a la Internet.

Los datos son presentados a los operadores humanos en una estación maestra, HMI, en la que supervisa todos los sensores y alertas instalados, de tal forma que pueda informar en el momento en que se active una alarma, es decir cuando una operación se sale de su funcionamiento normal. Se puede así obtener una visión global del sistema gestionado, con registros de informes y tendencias históricas desde la consola master.

4.2.7 Software PRTG

PRTG Network Monitor es una aplicación cuya función principal es la monitorización del tráfico de la red, analizando el flujo de datos que circula por ella. Administra la conexión de los distintos dispositivos SNMP, como

enrutadores, conmutadores, cortafuegos, impresoras y otros [29]. La aplicación se ejecuta de manera local, a través de una interfaz gráfica para el control de los eventos, obteniéndose gráficos de barras e informes detallados de los datos estadísticos en tiempo real. Las principales funcionalidades del PRTG se detallan en la figura 4.12.

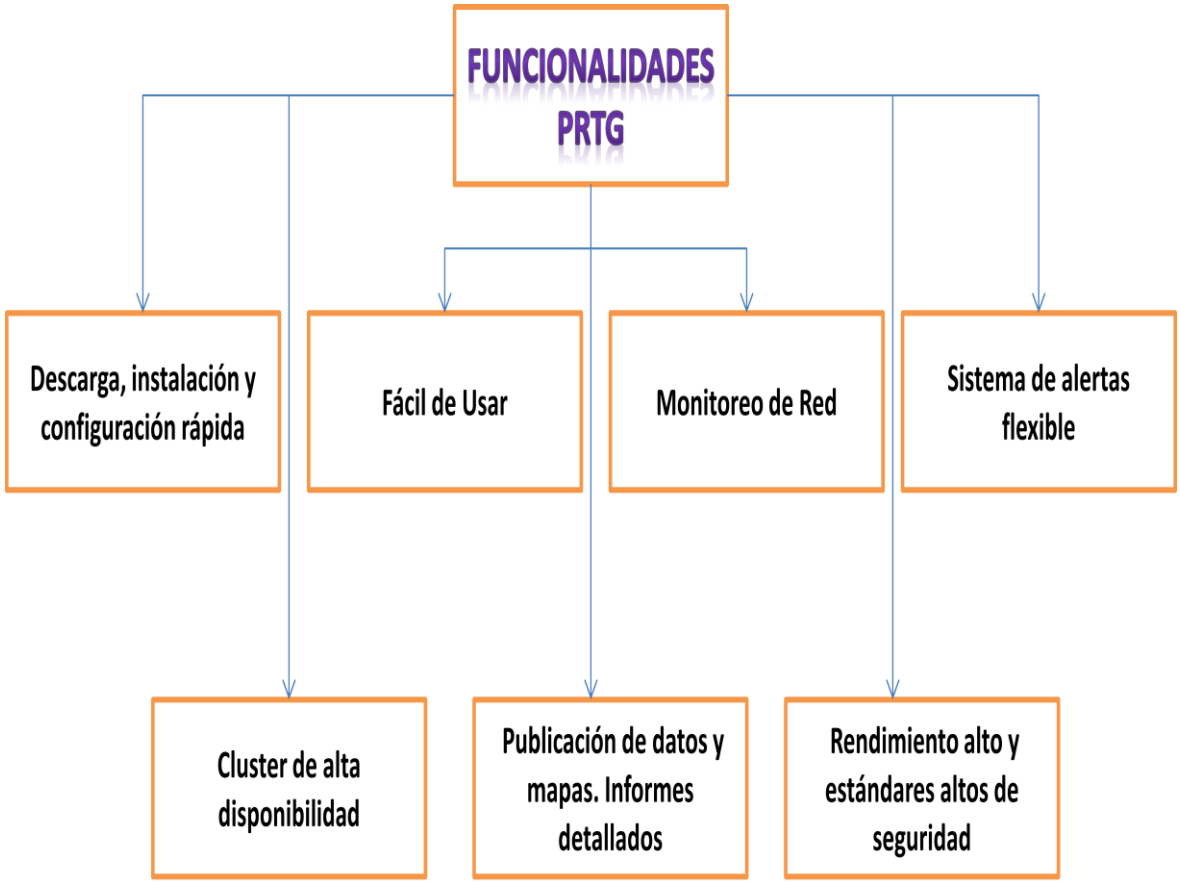


Figura 4.12 Funcionalidades de PRTG

4.2.8 Software NAGIOS

Es un sistema de código abierto, utilizado también en la monitorización de equipos y servicios informáticos, entre sus características están [30]: Facilidad de crecimiento y versatilidad para vigilar cualquier parámetro de interés de un sistema, envío de alertas al detectar un mal funcionamiento en el sistema, y cuando se recupera, flexibilidad en la configuración de la monitorización de la infraestructura de IT, según lo requiera el administrador.

Reacciona automáticamente a los problemas. Posee un sistema de notificaciones, adaptable a las tecnologías web 2.0 y presenta definición de alertas, para que no sean excesivas.

Cuenta con un sistema de dependencia, tanto de hardware como de software. Esto significa que si un equipo de enrutamiento sufre un daño, todos los sistemas conectados a él dejarán de funcionar. Las tareas que se pueden ejecutar con Nagios se resumen en la figura 4.13.

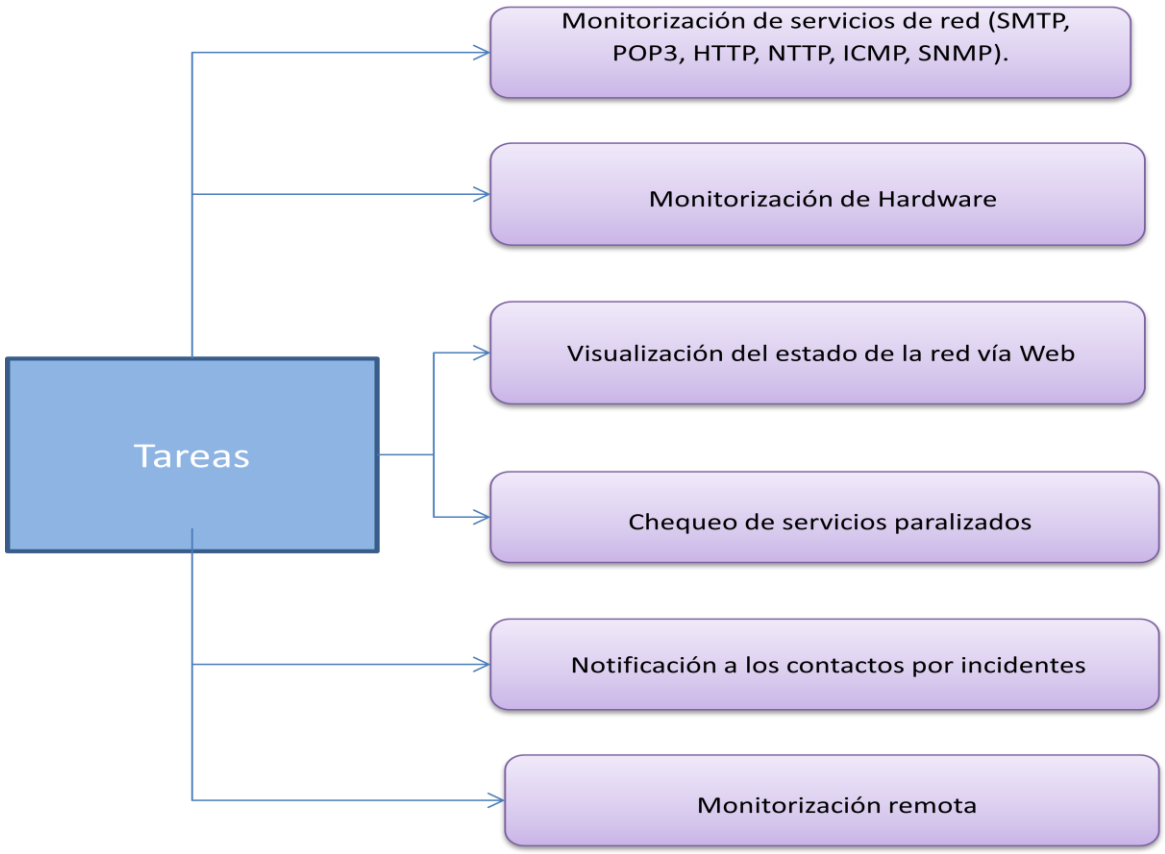


Figura 4.13. Tareas de Nagios

4.3 Topología de la Red

Existen dos configuraciones que enlazan a las dependencias de la Junta de Beneficencia de Guayaquil, para asegurar la disponibilidad del servicio: Configuración en anillo, para todas las dependencias y configuración punto a punto para la operación crítica.

Las redes internas (LAN) están conectadas en estrella, con cuartos de distribución de cableado y su centro de cómputo respectivo. En su mayoría con cable de cobre categoría 6A para equipos de cómputo y 5e para la red de impresoras. Existen conexiones de Fibra, para el enlace entre los centros de cableado y el centro de cómputo.

4.3.1Configuración en Anillo

La configuración en anillo enlaza a todas las dependencias de la Junta de Beneficencia, empleándose radios ubiquiti y tsunami, los mismos que se conectan a la LAN a través de los enrutadores Cisco 2911. El servicio provee la conectividad de las distintas áreas y permite el acceso a las bases de datos y sistemas de almacenamiento que están preestablecidas para el respaldo de los datos. La conectividad es verificada las 24 horas del día por el operador, para asegurar la disponibilidad de los servicios de la red, controlar la calidad del servicio y verificar el consumo del ancho de banda. En la figura 4.14 se observa el diagrama de la configuración de la red que une a todas las dependencias en conexión tipo anillo.

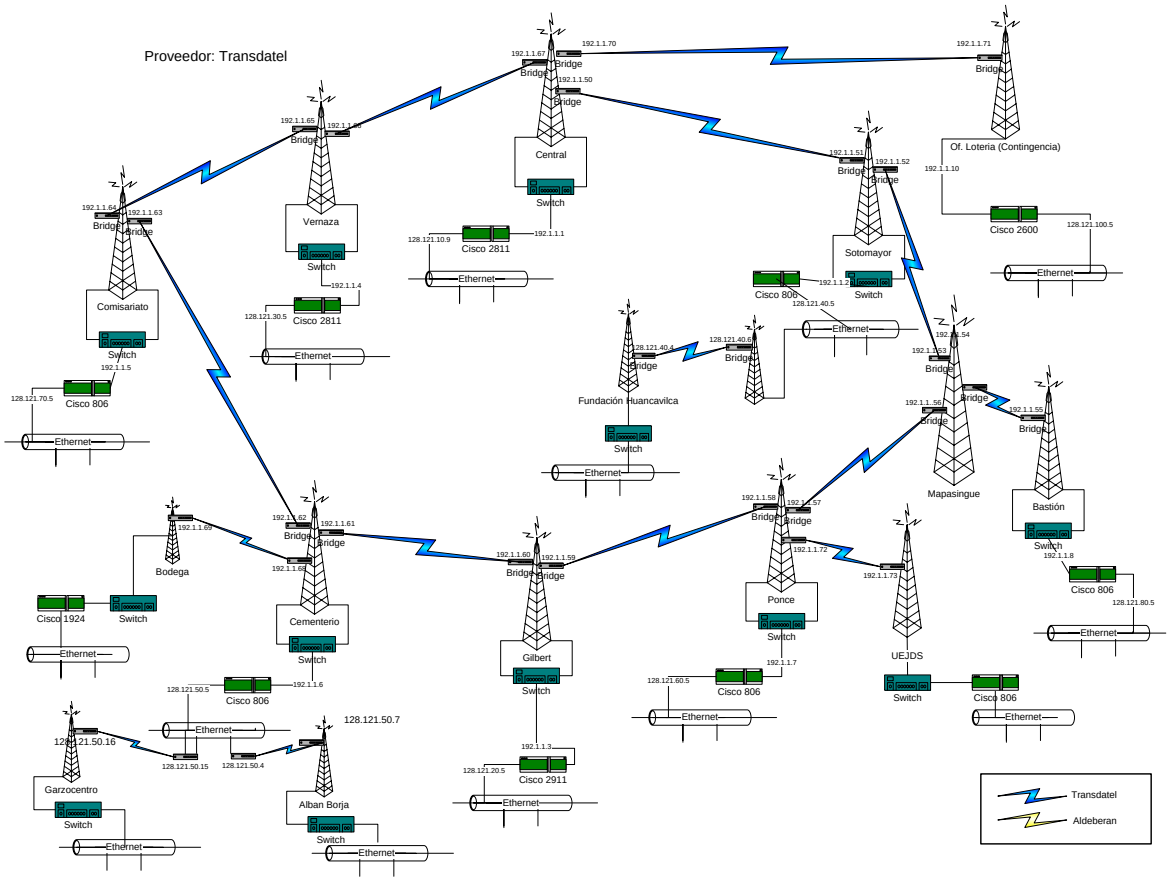


Figura 4.14 Diagrama de la configuración de la red entre las dependencias de la Junta de Beneficencia en conexión anillo.

En la figura 4.15 se puede observar el diagrama de conexiones de conmutadores de la oficina central. El Dlink 3026 cumple la función de conmutador principal, a el se conectan el resto de conmutadores que dan servicio a la red LAN y el AS400 que administra la base de datos institucional.

En los conmutadores Cisco 2960 se conectan los servidores que administran los diferentes servicios, incluidos los equipos Blade. El resto de conmutadores reciben las conexiones de todos los centros de datos del edificio y los puntos del área de sistemas.

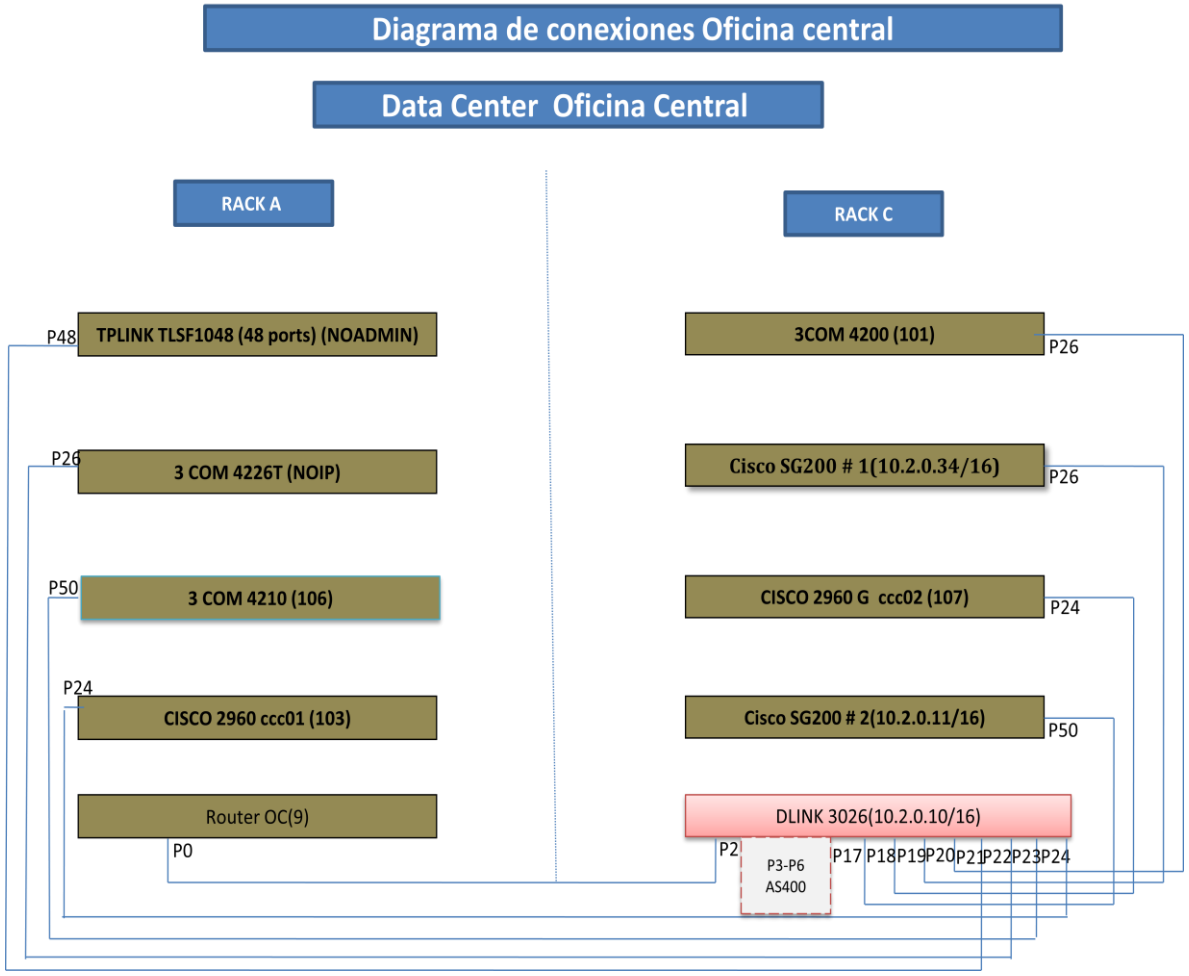


Figura 4.15 Diagrama de conexiones de conmutadores de la oficina central

4.3.2 Configuración punto a punto

En la figura 4.16 se observan las conexiones punto a punto entre la oficina central y los Hospitales Luis Vernaza y Roberto Gilbert.

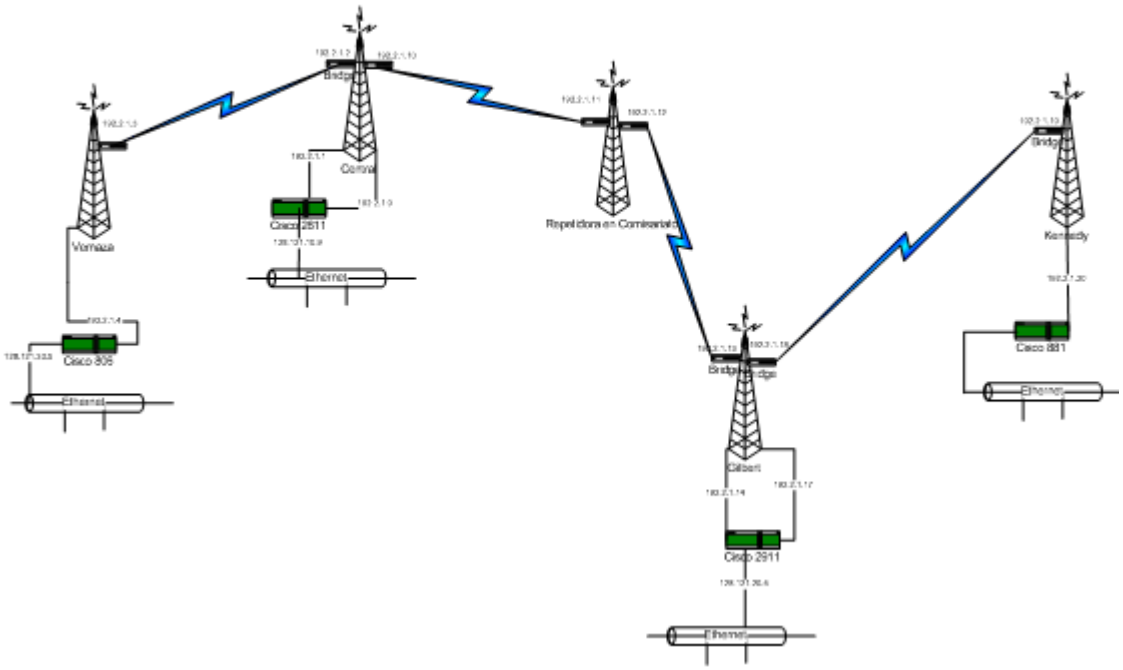


Figura 4.16 Diagrama de la configuración de la red entre las dependencias de la Junta de Beneficencia en conexión punto a punto.

4.4 Parámetros de control

Los parámetros de control medidos y estudiados en la Junta de Beneficencia son:

Voltaje: Valores de Vin y Vout de los centros de cómputo

Potencia: Carga de los centros de cómputo

Amperaje: Valores de corriente en el centro de cómputo

Ancho de Banda: Valores pico de transferencia de datos (Mb/s) y consumo del ancho de banda.

Temperatura: Valores de temperatura en el Centro de cómputo

Humedad: Registro de humedad en el Centro de cómputo

Nivel de RF: Valor de nivel de la señal recibida por el radio receptor.

Jitter: Valores de jitter admitidos en el enlace, indicador del nivel de interferencia permitido.

4.5 Eventos, incidentes y notificaciones

Un evento es cualquier suceso detectable, que tiene cierta relevancia para la Gestión de la Infraestructura y para la entrega de servicios de TI, estos pueden ser alertas o notificaciones creadas por los mismos servicios de TI o por las herramientas de monitoreo que pueden ser activas o pasivas. Las categorías de Eventos son: Informativos, precauciones y excepciones.

1. Informativos: Son los que reflejan operaciones normales

2. Precauciones: Representan operaciones inusuales y,
3. Excepción: Son operaciones anormales.

Los mecanismos de alerta se deben definir con las herramientas usadas para filtrar, correlacionar y escalar los eventos, a su vez se pueden establecer umbrales o niveles de desempeño. En cambio un incidente es una interrupción no planeada de un servicio de TI, la reducción de la calidad del mismo o la falla de un ítem de configuración que aún no ha impactado en la entrega de un servicio.

Dentro de la Gestión de Operación, el objetivo principal de la Gestión de Incidentes es la restauración de la operación normal del servicio, lo más rápido posible, para así minimizar el impacto adverso en las operaciones del negocio, asegurando de esta forma que se mantengan los niveles de calidad y disponibilidad del servicio.

Se define a la operación normal del servicio como la operación del servicio dentro de los límites establecidos por los SLA. Las métricas principales de la Gestión de Incidentes son:

1. El número total de incidentes
2. Número y porcentaje de incidentes críticos
3. Porcentaje de incidentes gestionados en los tiempos de respuesta acordados (SLA)
4. Porcentaje de incidentes cerrados por la mesa de servicios
5. Los incidentes atendidos por hora del día.

Finalmente, la notificación es la recepción de avisos debido a eventos o incidentes presentados y detectados por los agentes. Ver figura 4.17.

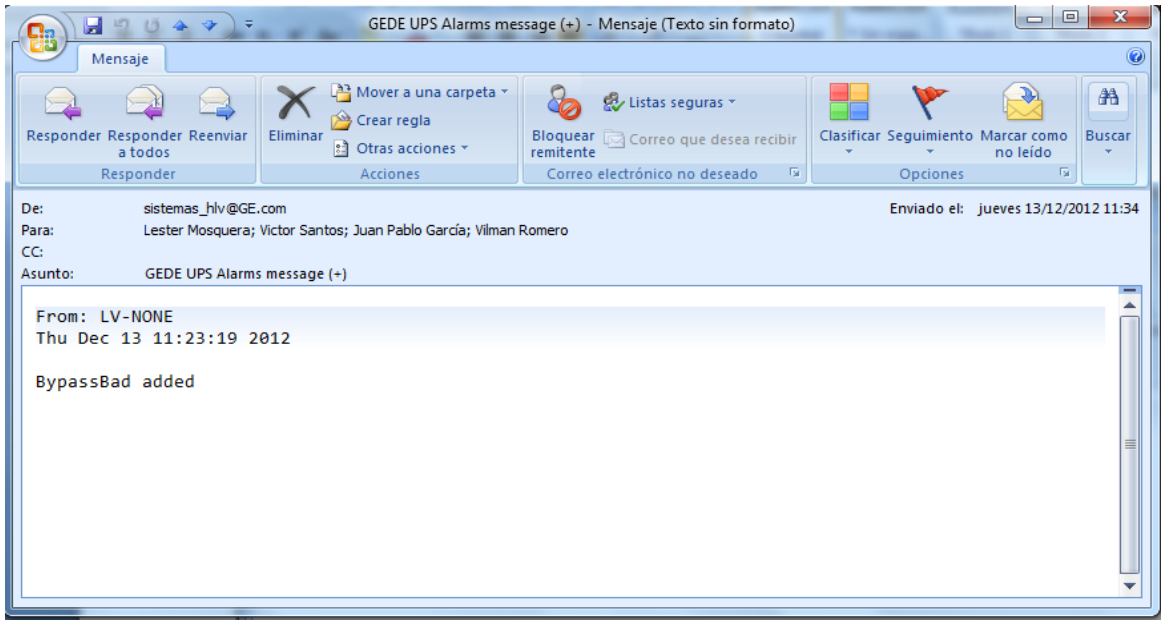


Figura 4.17 Notificación de alarma, recibida por personal técnico de la Junta de Beneficencia

CAPÍTULO 5

ANÁLISIS DE LOS RESULTADOS

Se presentan eventos e incidentes ocurridos en la plataforma de trabajo de TI de la Junta de Beneficencia de Guayaquil, que son controlados en la Gestión de la Operación y que permiten a la mesa de servicio y al personal técnico atender los sucesos bajo la política interna, en función de los procesos de servicios establecidos y de acuerdo a los SLA internos.

5.1 Lectura y análisis de los log por dispositivo

Por medio de las herramientas de software se registraron logs de eventos e incidentes, los que se analizaron para establecer procesos de atención y evaluar políticas de acción y contingencia, a fin de mantener el servicio disponible las 24 horas del día, los 365 días del año.

5.1.1 Eventos

A continuación se presentan algunos eventos registrados por los agentes, dentro del proceso de control de la Gestión de la Operación:

En la figura 5.1 se presenta el log de eventos de la radio que comunica la Oficina Central con el Hospital Enrique Sotomayor donde se aprecian dos caídas de señal.

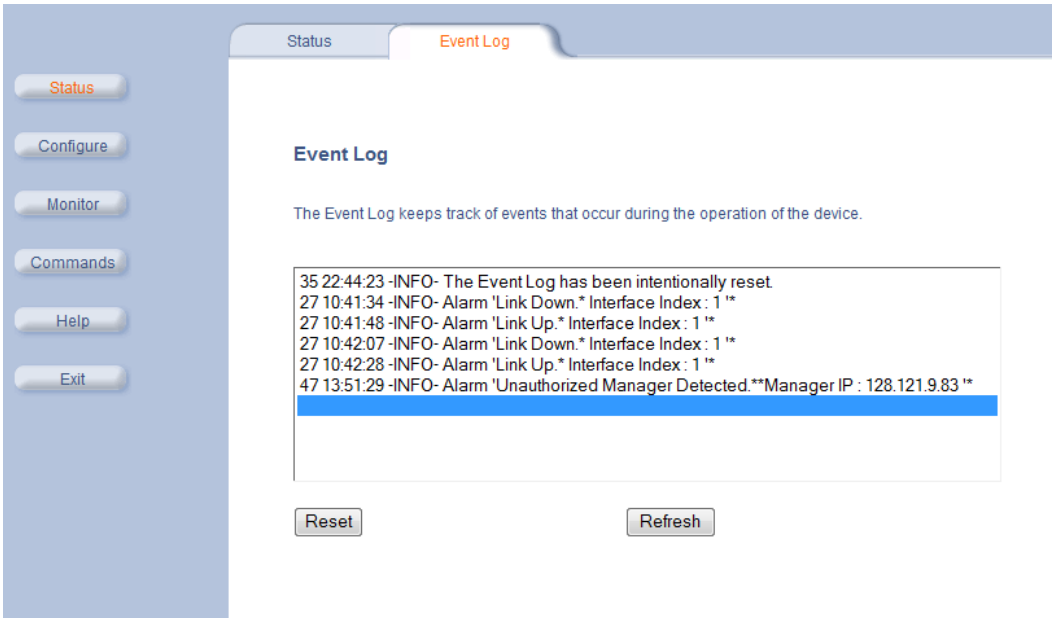


Figura 5.1. Detalle de eventos presentados en el enlace entre la Oficina Central y la Maternidad.

En la figura 5.2 se aprecia el reinicio y configuración del radio que comunica al Instituto de Neurociencias con el Hospital Roberto Gilbert, mientras que en la figura 5.3 se

observa la alarma “Cold Started”, es decir el reinicio del equipo, y la configuración del radio que comunica al dispensario satélite de la Maternidad con el Hospital Enrique Sotomayor.

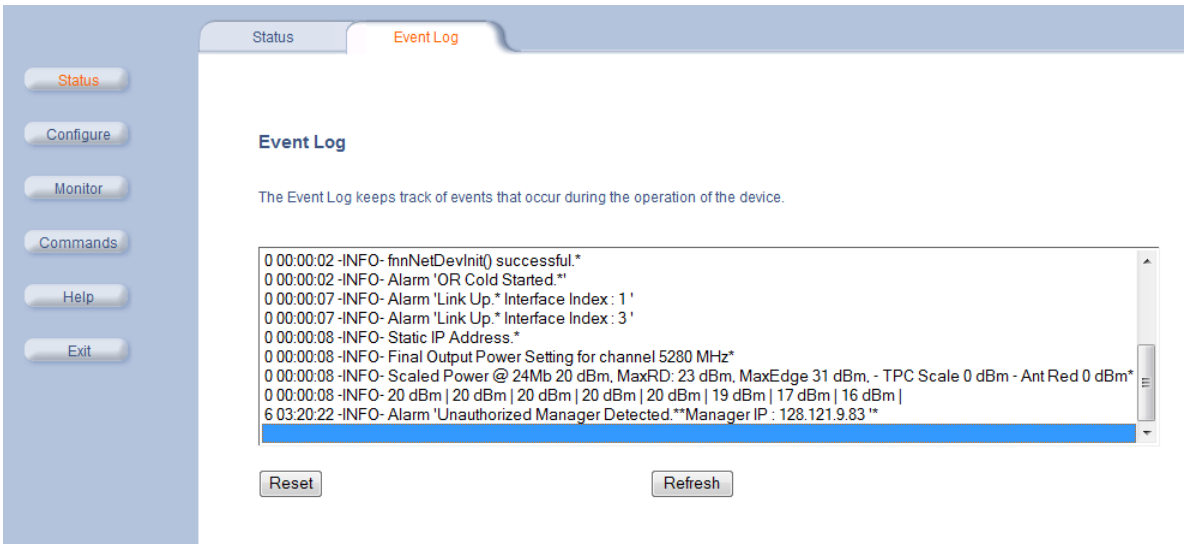


Figura 5.2 Registro de logs entre el Instituto de Neurociencias y el Hospital Roberto Gilbert

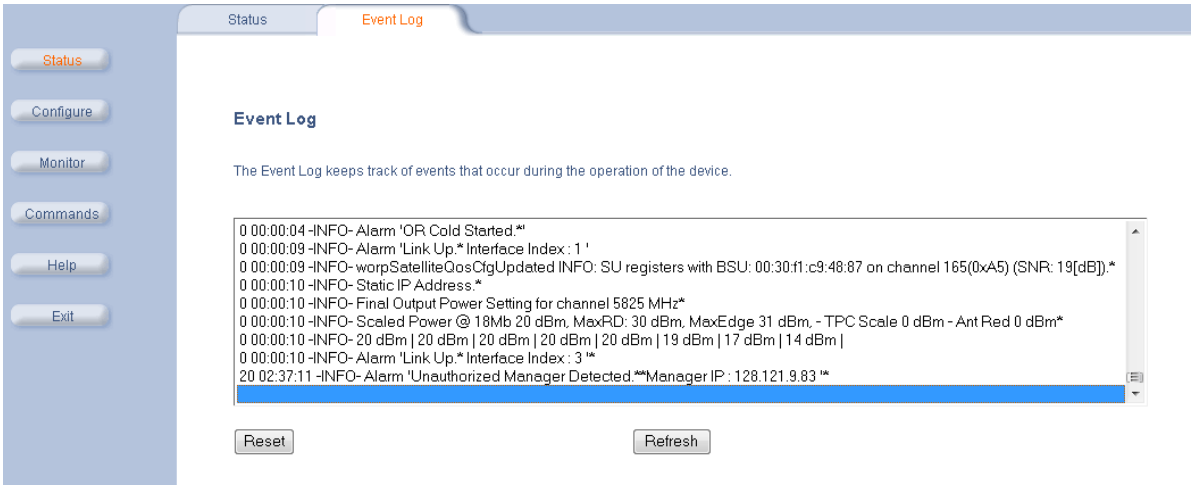


Figura 5.3 Alarma “Cold Started”y configuración de la radio del dispensario de la Maternidad

En la figura 5.4, se aprecia un evento en el que el UPS sensó la caída de energía de la calle, el proceso es:

1) El UPS se colocó a modo de Baterias. Se registró un voltaje de entrada no adecuado y la conexión de bypass no disponible. Por lo tanto la alimentación de energía para los servidores y equipos del Centro de Cómputo fue a través de las baterías de los UPS, en este caso por un tiempo de 10 minutos.

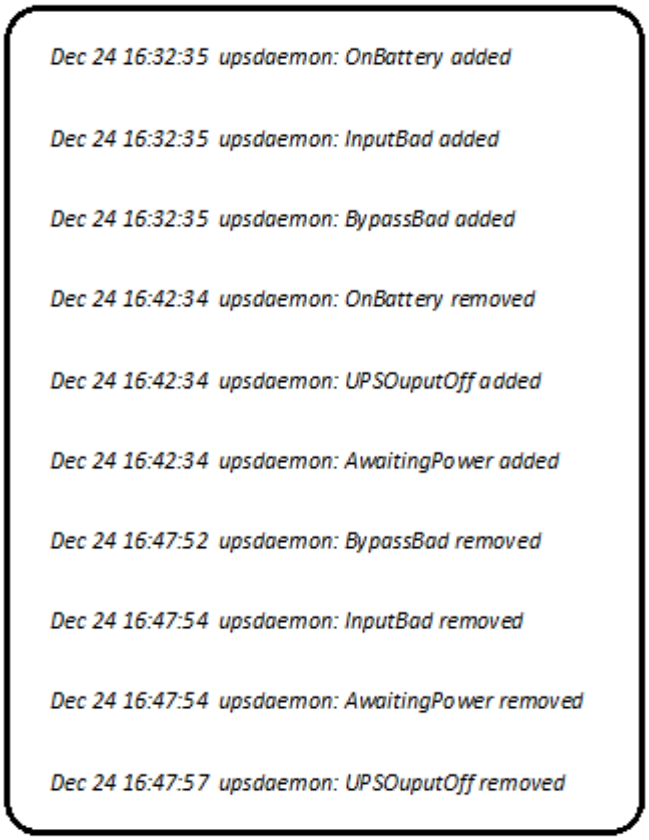


Figura 5.4 Logs de UPS GE de Oficina Central

2) Se retiró el modo de Baterías porque se sensó el ingreso de voltaje (generador que ingresa con retraso). Al mismo tiempo, el UPS indicó que la salida de voltaje estaba en Off y que estaba esperando energía de alguna fuente.

3) Luego de 5 minutos el UPS sensó el ingreso de energía de la calle y retiró la opción Bypass no disponible.

4) Se retiró la alarma de voltaje erróneo, la alarma de espera de voltaje y la alarma de salida de voltaje Off. Luego de ello el sistema siguió operando normalmente.

En la figura 5.5, en cambio, se observa una alerta suscitada por una variación significativa en los valores de carga del centro de cómputo, que de acuerdo a lo que registró el UPS es del 21%.

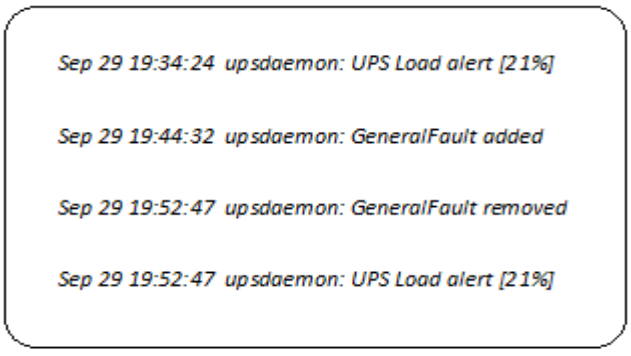


Figura 5.5 Logs de UPS GE oficina central

En los siguientes logs, se aprecian eventos de todos los enrutadores de la Junta de Beneficencia de Guayaquil, donde se encontraron en servicio 59 equipos. Los eventos se pueden resumir de la siguiente manera:

Lectura de datos de 59 equipos (Enrutadores y Conmutadores), indicando el número de fuentes (puertos) y dispositivos que procesan la información, además del tiempo de procesamiento. Advertencia de tabla vacía, debido a que no se pudo obtener información de 21 enrutadores. Ver figura 5.6.

```
12/13/2012 03:01:41 PM - SYSTEM STATS: Time:39.0043 Method:cmd.php
Processes:5 Threads:N/A Hosts:59 HostsPerProcess:12 DataSources:989
RRDsProcessed:465

12/13/2012 03:00:35 PM - SYSTEM STATS: Time:34.2892 Method:cmd.php
Processes:5 Threads:N/A Hosts:59 HostsPerProcess:12 DataSources:989
RRDsProcessed:465

12/13/2012 03:00:01 PM - POLLER: Poller[0] WARNING: Poller Output
Table not Empty. Issues Found: 21, Data Sources:
traffic_out(DS[87]), traffic_in(DS[88]), traffic_in(DS[90]),
traffic_out(DS[90]), traffic_in(DS[91]), traffic_out(DS[91]),
traffic_in(DS[92]), traffic_out(DS[92]), traffic_in(DS[93]),
traffic_out(DS[93]), traffic_in(DS[94]), traffic_out(DS[94]),
traffic_in(DS[95]), traffic_out(DS[95]), traffic_in(DS[105]),
traffic_out(DS[105]), traffic_in(DS[106]), traffic_out(DS[106]),
traffic_in(DS[107]), traffic_out(DS[107]), traffic_in(DS[108]),
Additional Issues Remain. Only showing first 20
```

Figura 5.6. Logs de los Routers de la Red de la Junta de Beneficencia.

Los siguientes eventos se produjeron en el enrutador 32 del Hospital Roberto Gilbert, ya que se cambió su configuración, ver figura 5.7, además en la figura 5.8 se registraron 2 equipos de los que no se encontró información (87 y 88).

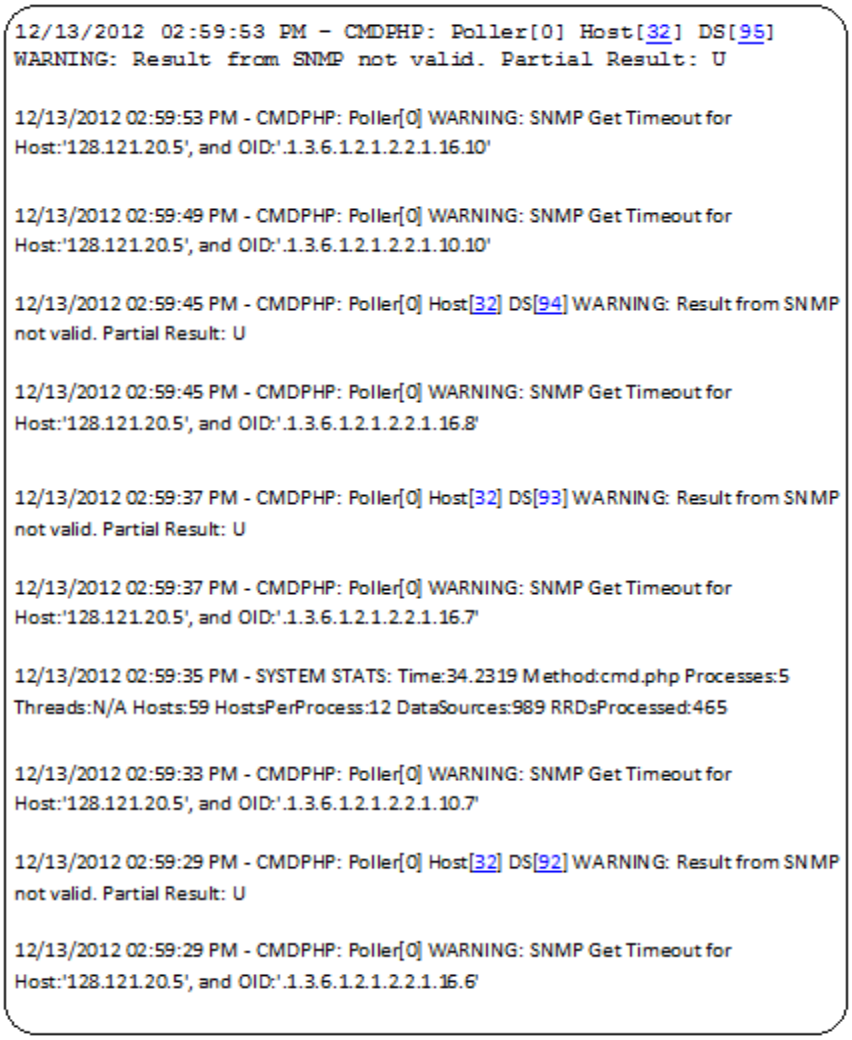


Figura 5.7. Logs correspondiente a los Routers de la Red de la Junta de Beneficencia.

Además en la figura 5.8 se observa que el proceso se repitió, registrándose 60 equipos, al sumarse el enrutador 32 configurado recientemente

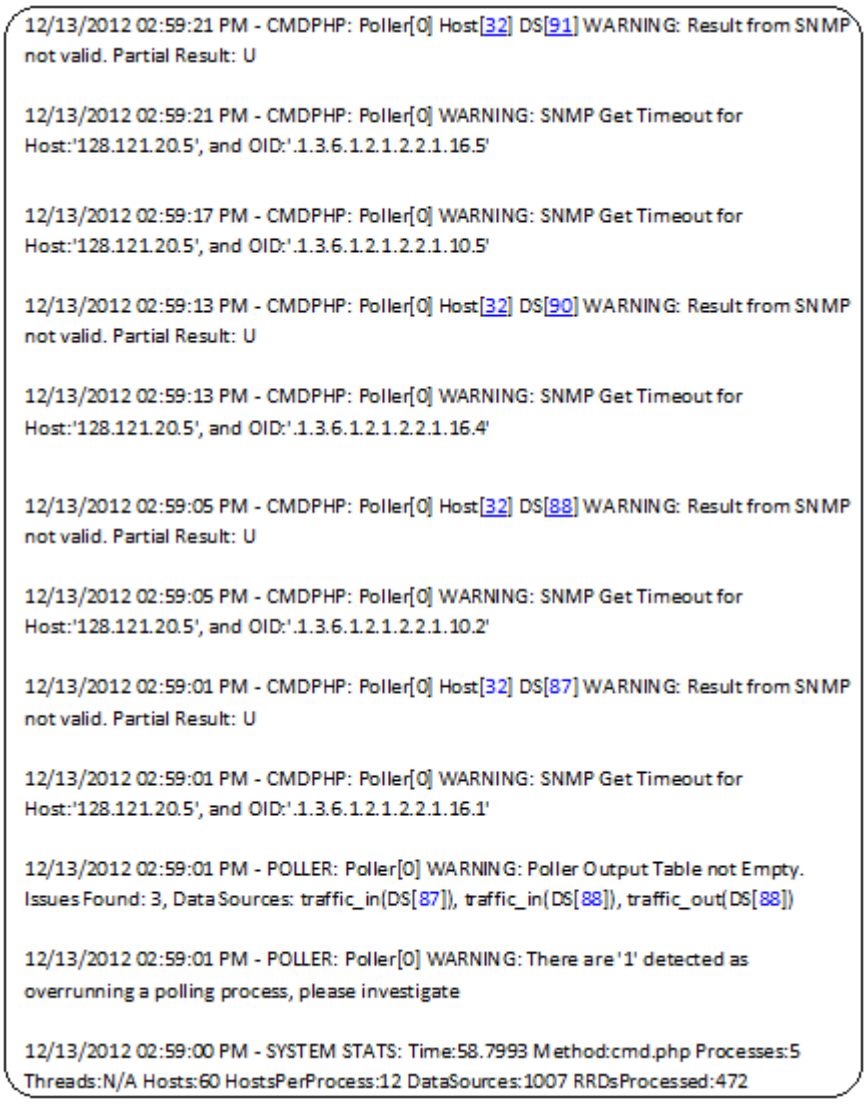


Figura 5.8. Logs correspondiente a los Routers de la Red de la Junta de Beneficencia

El siguiente log, mostrado en la figura 5.9, presenta el proceso de llamada de Voz sobre IP, utilizando el protocolo SIP. Allí se puede apreciar una llamada entre los usuarios 10.17.16.98 y 10.17.9.152. Además en la figura 5.10 se ilustra la señalización de la misma llamada.

```
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TCP
192.1.3.4:5060;branch=z9hG4bK614b5ccfa02d5
From: "Katty Ratto"
<sip:43731390@192.1.3.4>;tag=12757211~8ba61023-ef85-44e0-
9c86-a0a9377591d1-25155464
To: <sip:0997299972@192.167.254.1>;tag=45A3DDC8-6B3
Date: Fri, 07 Dec 2012 16:52:52 GMT
Call-ID: 88d24f80-c211ee4-5c4505-40301c0@192.1.3.4
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE,
REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID:
<sip:0997299972@192.167.254.1>;party=called;screen=no;pri
vacy=off
Contact:
<sip:0997299972@192.167.254.1:5060;transport=tcp>
Content-Length: 250
5070119: Dec  7 11:53:13.781:
//345589/88D24F800000/SIP/Msg/ccsipDisplayMsg:

Sent:
ACK sip:0997299972@10.17.9.152:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.17.16.98:5060;branch=z9hG4bK2D22A23B5
From: "Katty Ratto"
<sip:43731390@10.17.16.98>;tag=45A3CB3C-65A
To: <sip:0997299972@10.17.9.152>;tag=tz6z67e7-CC-45
Date: Fri, 07 Dec 2012 16:52:54 GMT
```

Figura 5.9 Logs de VoIP

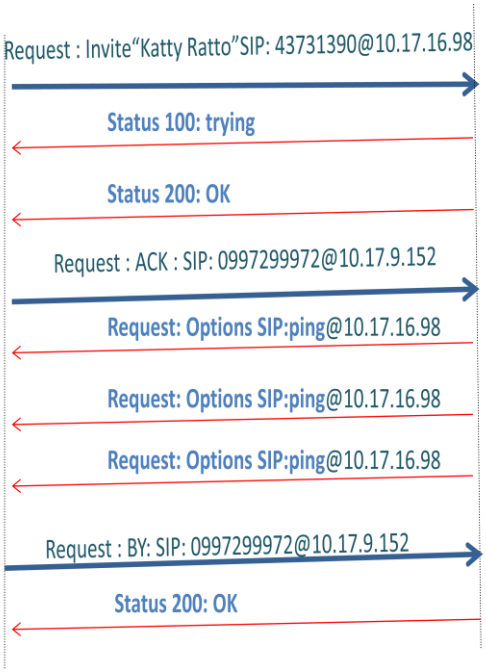


Figura 5.10 Señalización de VoIP

5.1.2 Incidentes

A continuación se analizan algunos incidentes registrados durante el proceso de control de la operación de TI:

5.1.2.1 Incidente: Caída señal Radios Tsunami

En los Log que se muestran en la figura 5.11 se puede apreciar la caída de la señal entre la oficina central de la Junta de Beneficencia y el Hospital Luis Vernaza, produciendo la no disponibilidad de los servicios para los usuarios del Hospital y el consiguiente retraso en las actividades normales.

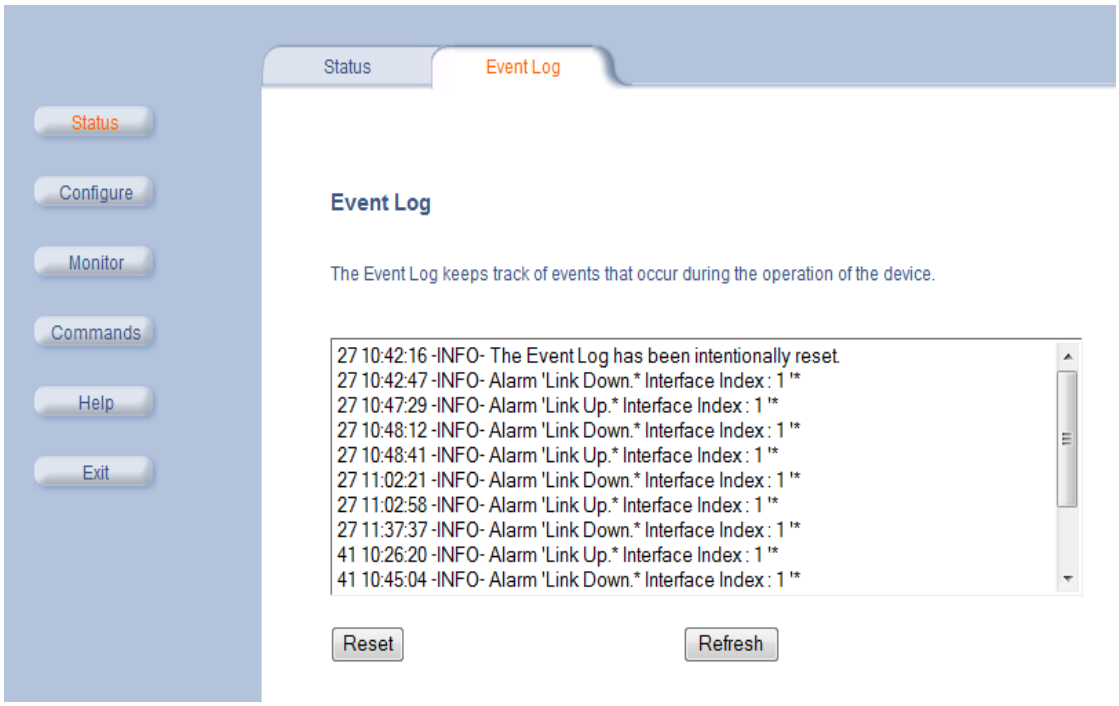


Figura 5.11 Logs de Radio Tsunami

Consecuentemente se levantó el proceso de atención para solucionar el inconveniente a través de la mesa de servicio y la asistencia del proveedor respectivo.

5.1.2.2 Incidente: Comunicación AA Liebert

En la figura 5.12 se aprecian fallas en los pines 3 y 4 del conector RJ45 que conecta el AA a la red, por lo que personal de soporte debió verificar el estado del conector para proceder a su cambio o al del cable si es necesario.

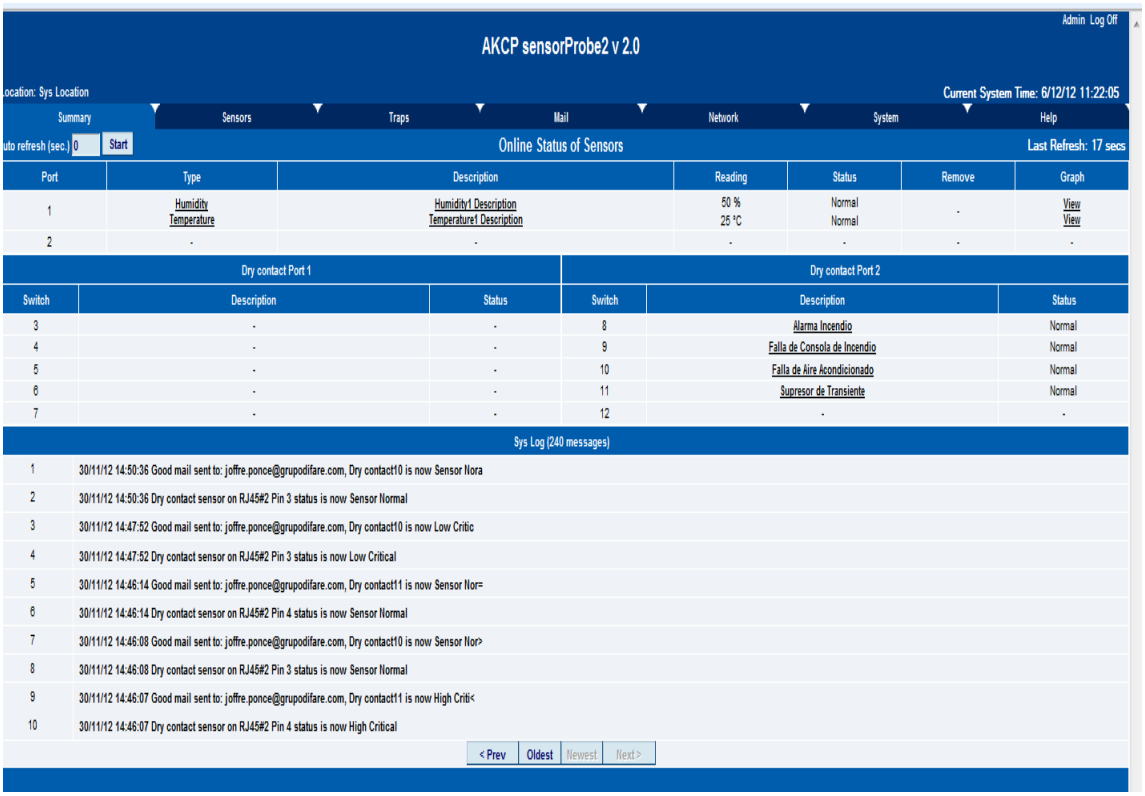


Figura 5.12 Incidente de comunicación en AA. Liebert

5.1.2.3 Incidente: Saturación del Ancho de Banda del servicio de Internet.

En las figuras 5.13 y 5.14 se observa la saturación del ancho de banda del servicio de Internet de la oficina central. En el primer caso el consumo llegó a 13.14MB entre las 14H00 y las 19H00 de 14MB posibles y en el segundo caso se alcanzaron valores de hasta 15.61MB entre las 11H35 y las 12H05. En ambas ocasiones la saturación del

ancho de banda produjo lentitud del servicio para el resto de los usuarios de la institución, por lo que personal de seguridad lógica realizó un análisis del consumo por usuario para determinar quien colapsó el servicio.

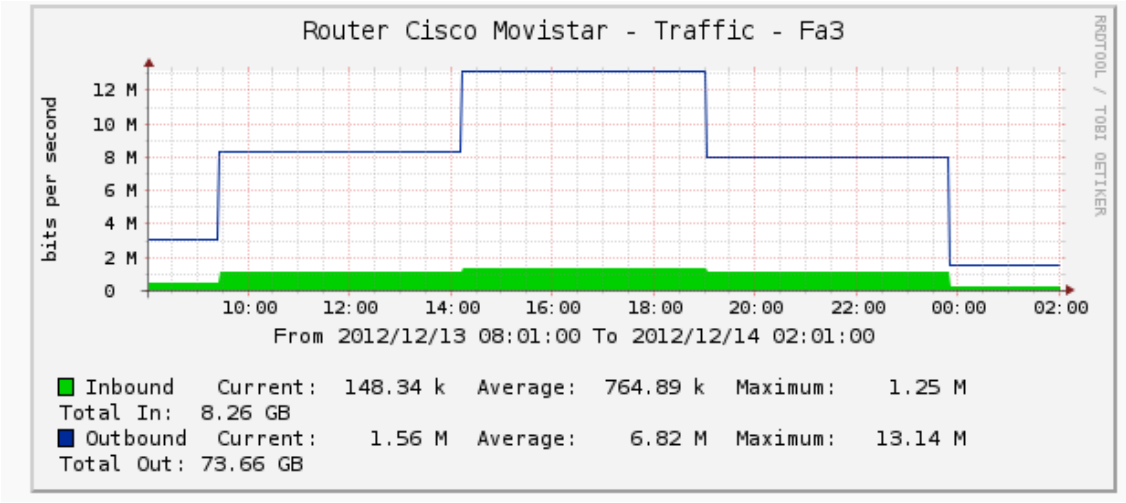


Figura 5.13 Saturación del enlace de Internet de 14h00 a 19h00.

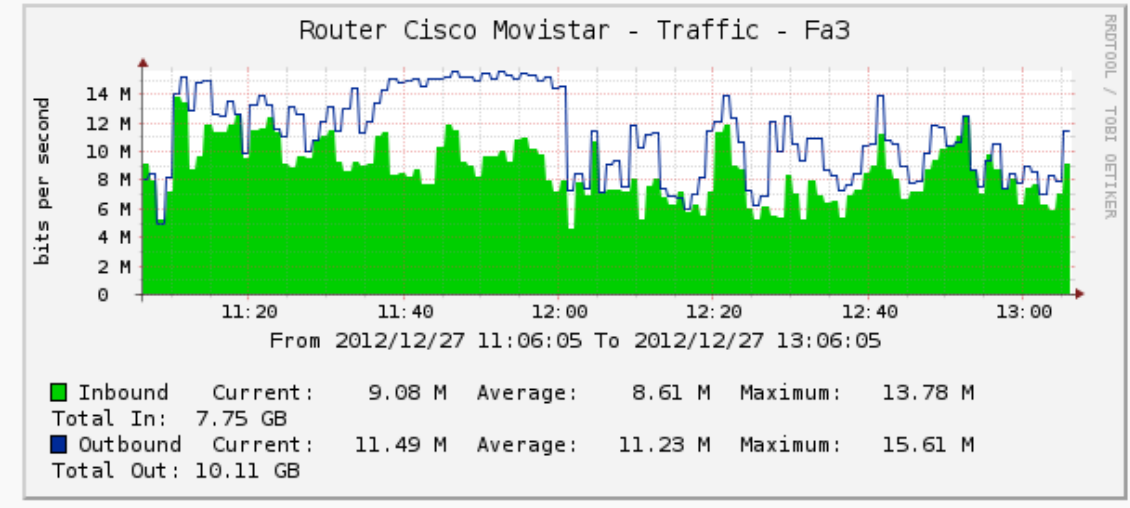


Figura 5.14 Saturación del enlace de Internet de 11h35 a 12h05**.**

5.1.2.4 Incidente: UPS Hospital Luis Vernaza

Se puede apreciar en la figura 5.15 el log del UPS del centro de cómputo del Hospital Luis Vernaza, donde se registraron una serie de aparentes cortes de energía, que se repitieron desde el mes de enero hasta julio del 2012, varias veces al día, la mayoría en las noches y madrugadas.

```
Jan 13 12:39:44  upsdaemon: OnBattery added
Jan 13 12:39:44  upsdaemon: InputBad added
Jan 13 13:10:09  upsdaemon: BypassBad added
Jan 13 13:41:03  upsdaemon: BypassBad removed
Feb 11 17:01:20  upsdaemon: OnBattery added
Feb 11 17:01:20  upsdaemon: InputBad added
Feb 11 17:01:20  upsdaemon: BypassBad added
Feb 11 17:01:33  upsdaemon: InputBad removed
Feb 11 17:01:36  upsdaemon: OnBattery removed
Mar 10 20:21:11  upsdaemon: OnBattery added
Mar 10 20:21:11  upsdaemon: InputBad added
Mar 10 20:21:11  upsdaemon: BypassBad added
Mar 10 20:21:18  upsdaemon: InputBad removed
Mar 10 20:21:19  upsdaemon: OnBattery removed
Mar 10 20:21:20  upsdaemon: BypassBad removed
Apr 14 00:02:54  upsdaemon: OnBattery added
Apr 14 00:02:54  upsdaemon: InputBad added
Apr 14 00:02:54  upsdaemon: BypassBad added
Apr 14 00:39:28  upsdaemon: InputBad removed
Apr 14 00:39:30  upsdaemon: OnBattery removed
Apr 14 00:39:33  upsdaemon: BypassBad removed
May  4 08:01:35  upsdaemon: BypassBad added
May  4 08:01:59  upsdaemon: BypassBad removed
May 14 00:17:29  upsdaemon: BypassBad added
May 14 00:18:39  upsdaemon: BypassBad removed
May 26 00:00:44  upsdaemon: BypassBad added
May 26 00:01:04  upsdaemon: BypassBad removed
Jun  6 02:13:33  upsdaemon: BypassBad added
Jun  6 02:17:45  upsdaemon: BypassBad removed
Jun 26 00:04:59  upsdaemon: BypassBad added
Jun 26 00:08:20  upsdaemon: BypassBad removed
Jul 14 01:34:53  upsdaemon: BypassBad added
Jul 14 01:36:39  upsdaemon: BypassBad removed
Jul 27 01:27:28  upsdaemon: BypassBad added
Jul 27 01:58:48  upsdaemon: BypassBad removed
```

Figura 5.15 Log de UPS Hospital Luis Vernaza

El personal de soporte del Hospital Luis Vernaza reportó que no se presentaron apagones, por lo que se solicitó al proveedor del equipo revisar la causa de los mensajes.

Para definir el motivo por el cual los UPS emiten muchas alarmas de bypass no disponible, el proveedor colocó un analizador de energía en el panel de entrada de voltaje del centro de cómputo durante 24 horas. Ver figura 5.16.

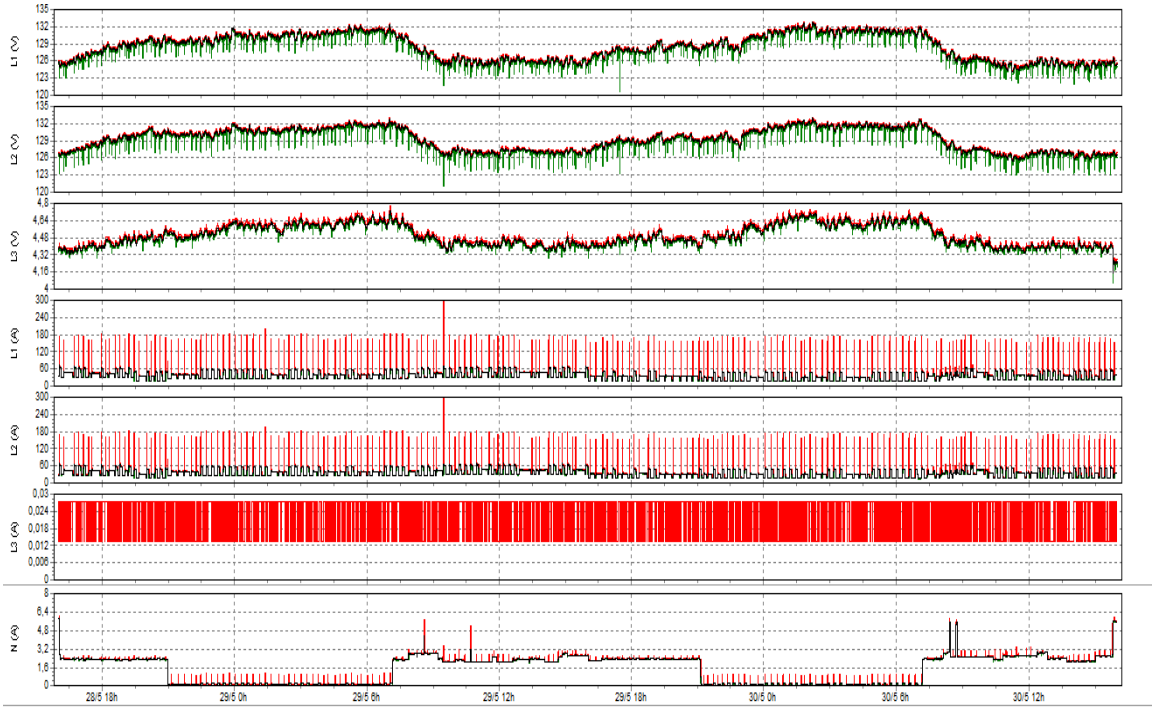


Figura 5.16 Lectura de Voltajes de entrada de UPS GE 10Kva en Hospital Luis Vernaza

La información que se obtuvó, mostrada en la figura 5.16, indicó que el voltaje entre línea y neutro varió entre 120V y 133V, es decir que entre línea y línea variaba entre 208 y 230V. El voltaje llegó a su máximo valor en horas de la madrugada, entre las 00H00 y las 06H00, en cambio entre las 09H00 y las 18H00 el voltaje disminuía.

El rango de voltaje de entrada (AC), depende de la carga protegida, según los porcentajes que se detallan:

Hasta 100% de carga 162-285V

Hasta 50% de carga 146-285V

Hasta 20% de carga 133-285V

Fuera de este rango el ups trabajaría en modo batería, además se debe considerar que los límites de voltaje con el cual el ups se mantiene con el bypass habilitado es:

-15%, +10% del nominal.

Pero la configuración del voltaje de entrada del UPS era 208/120V, considerando los rangos de trabajo sin que se deshabilite el bypass 177/102 y 228/131, por lo que en las noches el voltaje (133) excedía el límite máximo de trabajo (131) sin que se deshabilite el bypass.

Para minimizar la alarma de bypass no disponible, se procedió a configurar físicamente en la parte posterior del UPS la entrada a 240V y a través del display a 220V (entrada) y salida a 230V, de esta manera se calibró el rango del bypass dentro de los límites. Una vez que se realizó la configuración del UPS no se han vuelto a presentar más alarmas repetitivas y el incidente quedó solucionado.

5.1.2.5 Incidente: UPS de Oficina Central

El voltaje de entrada de los equipos AS400 y Blades S de IBM en el centro de cómputo de la oficina central, es suministrado por un sistema en paralelo de tres (3) UPS´S, los mismos que reciben

alimentación de un sistema monofásico a 240 voltios. Ver figura 5.17

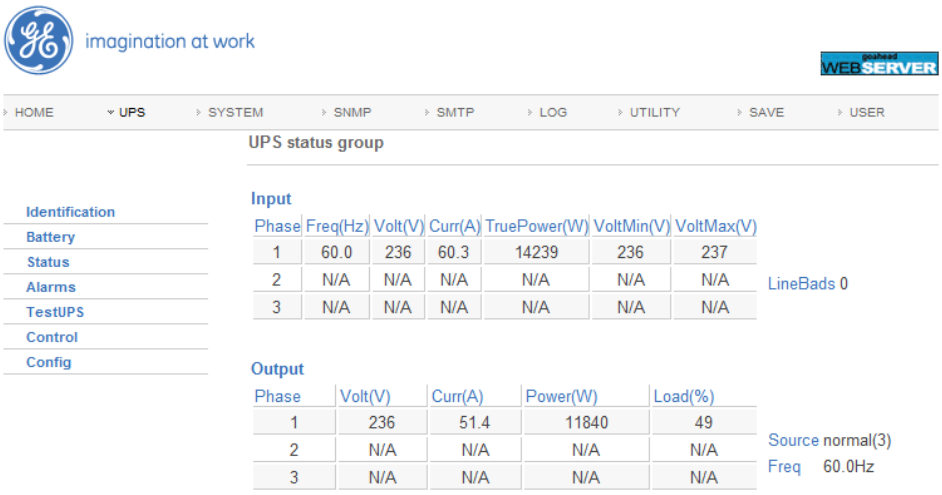


Figura 5.17 Voltajes de entrada y salida del UPS GE del Centro de Cómputo principal

Sin embargo, se detectó que durante el día el voltaje de entrada llegaba a valores superiores a los 241 v, por lo que se debían tomar las medidas para asegurar que el voltaje de salida sea máximo de 240v durante todo el día, debido a que los equipos servidores deben funcionar en un rango entre 220 y 240 voltios. Para ello se realizó un estudio con un analizador de energía, calibrado para tomar muestras cada minuto, obteniéndose los siguientes datos y gráficos:

La figura 5.18, muestra valores que variaban entre fases, con variaciones que iban de los 240V a los 260V. La regulación CONELEC 004/01 establece aceptable un +/- 10% de regulación de voltaje, por lo que, se puede tomar como aceptables estos valores. La gráfica anterior también permitió visualizar que el voltaje era alto en las noches y a primeras horas de la mañana, si el pico máximo mostrado era superado podía poner en riesgo a los equipos conectados al servicio público.

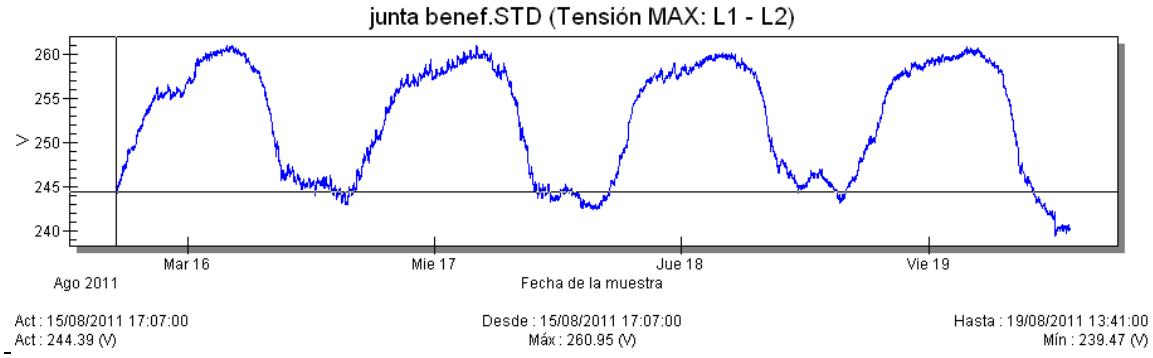


Figura 5.18 Voltajes de entrada máximos y mínimos.

En la figura 5.19 se muestra el consumo de corriente, con un valor promedio de 50 amperios por fase, equivalente a 12KVA por fase. Además la gráfica también muestra que el miércoles 16 de agosto hubo

un pico alto de consumo, pudo ser por el arranque de algún servidor o por la conexión de un equipo no autorizado.

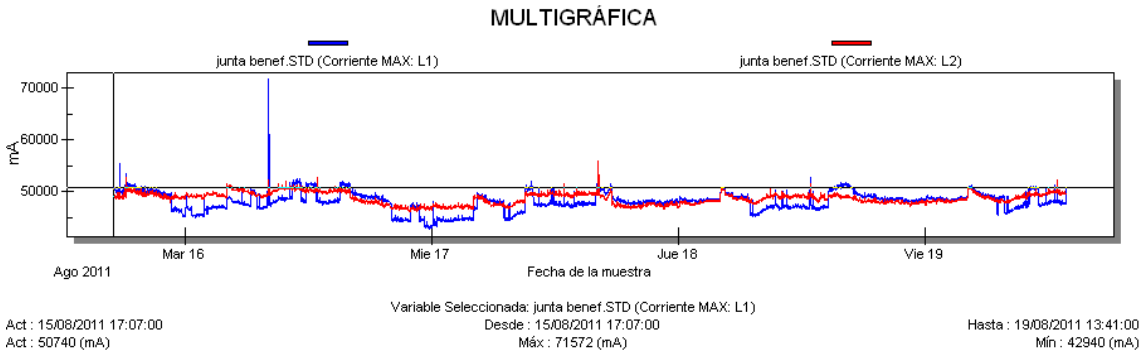


Figura 5.19. Consumos de corriente máximo y mínimos.

Según los resultados que se obtuvieron, se debía modificar el tap del transformador, para proceder a calibrar la salida del sistema del UPS a 220 voltios, ya que, cuando la carga del sector bajaba, la entrada de voltaje en el centro de cómputo subía a 260v, lo que provocaba que a su vez la entrada de voltaje de los servidores fuese superior a los 240v, lo cual dañaba la circuitería de los equipos y producía fallas en los sistemas de arreglo de discos. Una vez que se calibró el tap y que se realizó la configuración del UPS se obtuvieron voltajes inferiores a los 240v y el

sistema permaneció correctamente protegido, resolviéndose el incidente presentado. Ver figura 5.20.

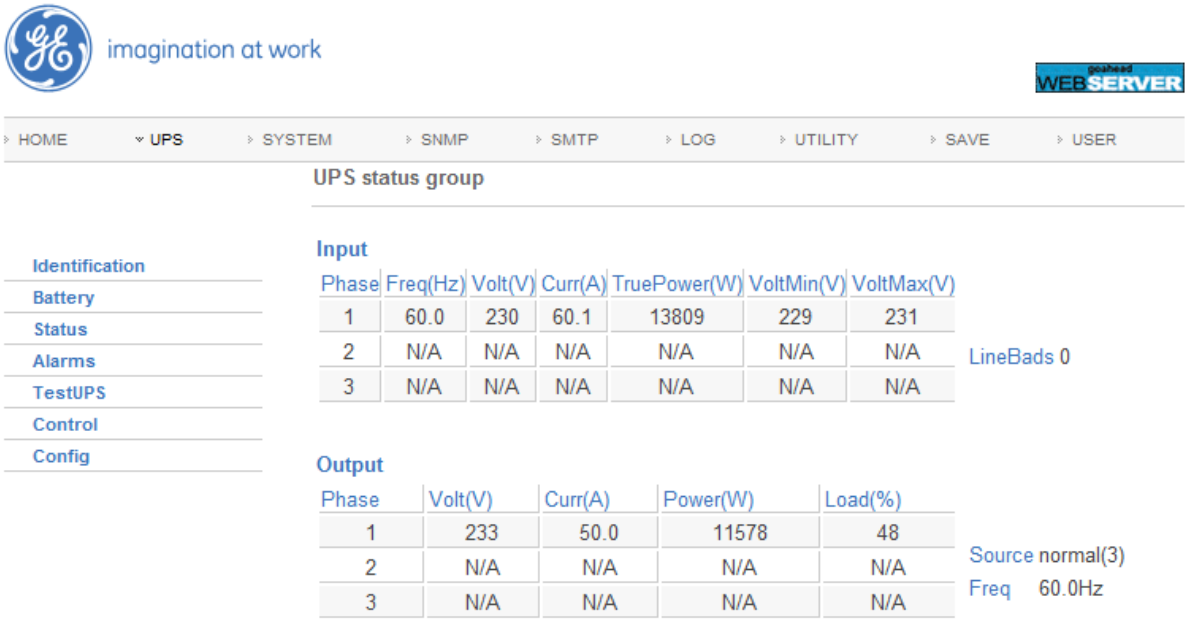


Figura 5.20. Voltajes de entrada y salida corregidos del UPS GE del Centro de Cómputo principal

5.2 Análisis de los parámetros de interés en la Operación de la Red

El Sistema de Gestión de control incluye en su totalidad:

a) Los voltajes de alimentación de los equipos servidores de todas las dependencias de la Junta de Beneficencia, que deben

mantenerse en el rango de 220v a 240v para energizar a los servidores.

b) La corriente de los Centros de Cómputo, que debe mantenerse en forma proporcional al crecimiento de la carga.

c) El consumo del ancho de banda de todos los enlaces, que de acuerdo a las gráficas analizadas, se mantiene dentro de los parámetros máximos (revisar gráficas de consumo), presentándose pequeños picos motivados por el incremento del proceso de facturación en algunas de las dependencias y el uso de la base de datos en forma simultánea. Sin embargo hubo un registro de un alto consumo de internet, lo que produjo la saturación del enlace dedicado.

d) La potencia, para no sobrepasar el valor máximo soportado de carga por cada sistema de UPS.

e) La temperatura del AA, la misma que se encuentra dentro de los parámetros adecuados para mantener la climatización en el Centro de Cómputo, incluso la humedad permanece en el rango permitido.

f) Nivel de RF: Valores de nivel de la señal recibida por el radio receptor.

g) Los valores de jitter admitidos para mantener la disponibilidad del enlace.

5.3 Cuadros de resultados

A continuación se presentan tablas con el resumen de resultados del análisis de eventos e incidentes.

5.3.1 Eventos

En la tabla VI se describen algunos de los eventos que se presentaron durante la Gestion de la Operación, como servicio de batería añadida en los sistemas de UPS, Incremento de temperatura en UPS o AA, Sobrecarga en los UPS y la caída de la señal entre la oficina central y la maternidad.

En la tabla se plantea la causa que originó el evento, su importancia sobre la operación y disponibilidad del servicio, la posible afectación y las acciones a seguir por el personal de control para disminuir los eventos repetitivos.

Tabla VI. Registro de eventos presentados

Tipos de Eventos	Elemento afectado	Importancia del Evento	Observación	Posible afectación	Acción
Batería añadida	UPS	Precaución	Caída de Voltaje	Al Sistema de Servidores. Suspensión de Servicios.	Seguimiento a Voltajes Revisar Voltajes de entrada de la calle Revisar la disponibilidad del Generador Revisar Baterías disponibles Revisar sistema de alimentación Plan Mantenimiento General de UPS
Aumento de Temperatura	UPS/AA	Alta	Daño en Ventilador	Al Sistema de Servidores. Suspensión de Servicios.	Mantenimiento interno Cambio de partes requeridas. Mejora en climatización general.
Sobrecarga	UPS	Alta	Carga por encima de umbral	Apagado de UPS Pérdida de redundancia Caída de servidores	Análisis de carga Apagado de equipos no críticos Cambio de la capacidad de Sistema de UPS
Caída de señal	Radio	Alta	Avería en radio Daño en fibra	Pérdida de la comunicación entre dependencias No disponibilidad de los servicios Daño en radio o fibra	Mantenimiento de equipo de radio, conectores y cables Levantamiento de servicio redundante

5.3.2 Incidentes

En la tabla VII, se describen algunos de los incidentes suscitados durante la Gestion de la Operación, como la caída del enlace o la saturación del servicio de Internet, caídas de la red LAN, falla de comunicación de la tarjeta de red del AA y sobrevoltaje a la entrada de los centros de cómputo.

En la tabla se plantea la causa que originó el incidente, su importancia sobre la operación y disponibilidad del servicio, la posible afectación y las acciones a seguir por el personal de TI. Se hace énfasis en el uso de sistemas de contingencia para la comunicación entre dependencias, en el mantenimiento continuo, en la revisión de los sistemas de alimentación en todos los centros de cómputo, en la mejora en los sistemas de protección, el mantenimiento de los sistemas de transformadores, en la certificación de los puntos de datos y en el establecimiento de políticas de control del uso de los servicios de la red y del manejo de la seguridad a través de claves por usuario.

Tabla VII. Registro de incidentes presentados

Tipos de Incidentes	Elemento afectado	Importancia del Incidente	Observación	Posible afectación	Acción
Caída de enlace	Radio Antena Router Fibra	Alta	Daño en radio, enlace, Antena o router	No disponibilidad de servicios Pérdida Económica	Uso de Sistema de contingencia: Anillo o Punto-Punto Mantenimiento Cambio de partes requeridas
Saturación servicio Internet	Servicio Internet	Alta	Demanda excesiva de algún usuario	Lentitud del servicio para todos los usuarios	Revisión de uso del servicio por usuario Políticas de uso y seguridad de la red Manejo de claves para servicios de mayor demanda en Internet
Pérdida de comunicación con AA	AA	Alta	Falla en conector de red o tarjeta interna	Pérdida de control en los valores de temperatura y humedad del centro de cómputo	Revisión de conector de red y de tarjeta interna. Certificación de punto
Sobre voltaje	Servidor AS400 Blades UPS	Alta	Pico de Voltaje Falla en el sistema de protección	UPS Servidores Equipos en general	Revisión y calibración de voltajes de entrada Mantenimiento Transformadores Sistema de UPS redundantes Mejora sistema de protección Alimentación redundante

5.4 Comparación de sistemas de control: con y sin protocolo SNMP

En la tabla VIII, se hace una comparación entre un sistema gestionado con el protocolo SNMP y uno no gestionado.

Tabla VIII. Comparación de Sistemas Gestionados con y sin protocolo SNMP

Eventos e Incidentes	Posibles afectaciones	Con Sistema de Gestión SNMP	Sin sistema de Gestión SNMP
Batería añadida Incremento de Temperatura Sobrecarga Caída de enlace Caída LAN Daño en AA Sobre voltaje	Falla en segmento de red Suspensión de Servicios Apagado de UPS Perdida de redundancia No disponibilidad de servicios Pérdida Económica	Análisis de Logs permanente Revisión de eventos y solución a los mismos Revisión de Incidentes/Alarmas Se toman medidas de contingencia rápidamente según los SLA contemplados en la mesa de servicio	No hay percepción de eventos Falta de visibilidad del problema Retraso en la toma de acciones Pérdida de clientes Pérdida económica Mayor tiempo de caída de servicios

En un sistema de control de red vía SNMP se obtiene información de inmediato, en línea, lo que permite tomar medidas correctivas o

preventivas y disminuir el tiempo de interrupción de los servicios, aumentando la disponibilidad de los mismos.

En cambio, en un sistema sin gestión SNMP, no se pueden tomar medidas correctivas en corto tiempo, ya que no se tiene una visión clara del problema y se requerirá de mayor tiempo de análisis para plantear una solución.

5.5 Políticas a implementar

A fin de que el Sistema de Gestión de Redes tenga los resultados esperados se establecen las siguientes políticas que deben ser implementadas por el Gestor de Operaciones:

1. **Instalación y configuración de los agentes**: Una vez que se haya instalado el hardware respectivo, se procederá a la configuración de los agentes por parte del proveedor, bajo los requerimientos del área de operaciones de la empresa.

2. **Configuración del administrador del servicio**: En forma simultánea a la configuración del agente se configurará el administrador o los administradores designados.

3. **Control y administración de la consola:** La operación de control y administración de la consola se la hará 24x7 en el site central e incluirá:

    a. **Revisión de logs:** Cada agente proporciona los logs respectivos que deben ser revisados diariamente para determinar si hay comportamientos fuera de lo normal. Es mejor si se utiliza un correlacionador de logs.

    b. **Registro de traps o alarmas**: Los traps o alarmas deben ser configurados y gestionados por el área de operación. Existirá una variedad de alarmas disponibles para cada agente, que podrán ser audibles, vistas por consola o recibidas en un mail.

4. **Atención a incidentes:** Para la atención a incidentes reportados por el operador o recibidos vía mail desde el correo del agente, se procederá de acuerdo a la política interna de cada dependencia y en relación con los SLA establecidos a nivel interno o con el proveedor, procurando que el MTBF sea lo menor posible.

5. **Levantamiento de información:** Tanto para el caso de elaboración de reportes semanales o para el establecimiento del número de eventos e incidentes presentados, se realizará el levantamiento de información respectivo y se elaborará una estadística para evaluar el proceso de Gestión de Redes implementado.

CONCLUSIONES

A través de la experiencia práctica, adquirida en la toma de muestras gráficas de las variables de operación, podemos concluir:

1. El proceso de control de la Red, implementado sobre el protocolo SNMP, permite agilizar la atención de los posibles incidentes, debido al monitoreo permanente y a la funcionalidad de las alarmas, que permiten notificaciones en línea y ejecuciones de planes de contingencia o prevención en un corto plazo, tal como se lo analiza en la tabla VIII.

2. La Gestión de Operación de la Red se ve mejorada con el uso de las herramientas de software basados en SNMP, siendo estas amigables y de fácil uso, ya que permiten la configuración de los parámetros a medir y de las alarmas que se recibirán en caso de presentarse valores distintos a los configurados, según se comprueba en el capítulo 5.

3. El agente facilita información valiosa sobre las variables de interés en el proceso de Gestión de la Operación de la Red, según se observa en los

gráficos de la sección 3.5 y de acuerdo al análisis presentado en la sección 5.2

.

4. En el caso de la Junta de Beneficencia, de acuerdo al análisis de los logs realizado en el capítulo 5, el uso de las herramientas de control, basadas en el protocolo SNMP, ha sido eficaz al momento de informar y validar incidentes o eventos.

5. El Sistema de Gestión de Impresión implementado permite administrar y controlar el uso de los consumibles en forma adecuada, a través del uso del software de administración y de la aplicación de políticas implementadas para su fín a nivel institucional, según se puede observar en la sección 3.5.5.

6. Un Sistema de Gestión de Redes basado en el protocolo SNMP es efectivo y permite mejorar el servicio a los usuarios, ya que facilita el control de los servicios y posibilita la toma de medidas preventivas y correctivas en corto tiempo, según se lo analiza en la tabla VIII

7. El estudio realizado, permite confirmar la viabilidad de la administración de una red a través del protocolo SNMP, por su eficacia en el control y gestión de la operación, por su facilidad de configuración, por la amplitud

de la información receptada y por los costos bajos al usar software propietario.

RECOMENDACIONES

Luego de haber realizado el análisis de la importancia de un Sistema de Gestión de Redes se recomienda:

1. Verificar que el hardware adquirido permita habilitar el control de datos vía protocolo SNMP.

2. Establecer políticas de contingencia y control, para el buen manejo de la red y así mantener el servicio disponible las 24 horas del día.

3. Mantener la Gestión de la Operación en forma permanente, a través de políticas establecidas dentro del diseño del servicio.

4. Aprovechar al máximo las herramientas brindadas por el software de control, y no limitarse a solo usarlo en las configuraciones iniciales.

5. Implementar la red de comunicaciones debidamente, bajo las normas internacionales, a fin de asegurar la disponibilidad de la misma para el proceso de control de la red.

6. Calificar debidamente al personal de operaciones en el uso de las herramientas y políticas de Gestión.

ANEXO 1

OID Radios Junta

Se detallan los OID de las radios utilizadas en la Junta de Beneficencia y que han sido capturados a través del software CACTI.

Data Query Debug Information + Running data query [1].

+ Found type = '3' [SNMP Query].

+ Found data query XML file at '/srv/www/htdocs/cacti/resource/snmp_queries/interface.xml'

+ XML file parsed ok.

+ Executing SNMP get for num of indexes @ '.1.3.6.1.2.1.2.1.0' Index Count: 7

+ Executing SNMP walk for list of indexes @ '.1.3.6.1.2.1.2.2.1.1' Index Count: 7

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.1' value: '1'

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.2' value: '2'

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.3' value: '3'

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.4' value: '4'

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.5' value: '5'

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.6' value: '6'

+ Index found at OID: '1.3.6.1.2.1.2.2.1.1.7' value: '7'

+ Located input field 'ifIndex' [walk]

+ Executing SNMP walk for data @ '.1.3.6.1.2.1.2.2.1.1'

+ Found item [ifIndex='1'] index: 1 [from value]

+ Found item [ifIndex='2'] index: 2 [from value]

+ Found item [ifIndex='3'] index: 3 [from value]

+ Found item [ifIndex='4'] index: 4 [from value]

+ Found item [ifIndex='5'] index: 5 [from value]

+ Found item [ifIndex='6'] index: 6 [from value]

+ Found item [ifIndex='7'] index: 7 [from value]
+ Located input field 'ifOperStatus' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.2.2.1.8'
+ Found item [ifOperStatus='Up'] index: 1 [from value]
+ Found item [ifOperStatus='Down'] index: 2 [from value]
+ Found item [ifOperStatus='Up'] index: 3 [from value]
+ Found item [ifOperStatus='Down'] index: 4 [from value]
+ Found item [ifOperStatus='Up'] index: 5 [from value]
+ Found item [ifOperStatus='Up'] index: 6 [from value]
+ Found item [ifOperStatus='Up'] index: 7 [from value]
+ Located input field 'ifDescr' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.2.2.1.2'
+ Found item [ifDescr='lo'] index: 1 [from value]
+ Found item [ifDescr='gre0'] index: 2 [from value]
+ Found item [ifDescr='eth0'] index: 3 [from value]
+ Found item [ifDescr='eth1'] index: 4 [from value]
+ Found item [ifDescr='br0'] index: 5 [from value]
+ Found item [ifDescr='wifi0'] index: 6 [from value]
+ Found item [ifDescr='ath0'] index: 7 [from value]
+ Located input field 'ifName' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.31.1.1.1.1'
+ Located input field 'ifAlias' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.31.1.1.1.18'
+ Located input field 'ifType' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.2.2.1.3'
+ Found item [ifType='softwareLoopback(24)'] index: 1 [from value]

+ Found item [ifType='other(1)'] index: 2 [from value]
+ Found item [ifType='ethernetCsmacd(6)'] index: 3 [from value]
+ Found item [ifType='ethernetCsmacd(6)'] index: 4 [from value]
+ Found item [ifType='ethernetCsmacd(6)'] index: 5 [from value]
+ Found item [ifType='ethernetCsmacd(6)'] index: 6 [from value]
+ Found item [ifType='ethernetCsmacd(6)'] index: 7 [from value]
+ Located input field 'ifSpeed' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.2.2.1.5'
+ Found item [ifSpeed='0'] index: 1 [from value]
+ Found item [ifSpeed='0'] index: 2 [from value]
+ Found item [ifSpeed='100000000'] index: 3 [from value]
+ Found item [ifSpeed='0'] index: 4 [from value]
+ Found item [ifSpeed='0'] index: 5 [from value]
+ Found item [ifSpeed='0'] index: 6 [from value]
+ Found item [ifSpeed='300000000'] index: 7 [from value]
+ Located input field 'ifHwAddr' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.2.2.1.6'
+ Found item [ifHwAddr=''] index: 1 [from value]
+ Found item [ifHwAddr=''] index: 2 [from value]
+ Found item [ifHwAddr='00:27:22:09:38:0C'] index: 3 [from value]
+ Found item [ifHwAddr='02:27:22:09:38:0C'] index: 4 [from value]
+ Found item [ifHwAddr='00:27:22:08:38:0C'] index: 5 [from value]
+ Found item [ifHwAddr='00:27:22:08:38:0C'] index: 6 [from value]
+ Found item [ifHwAddr='00:27:22:08:38:0C'] index: 7 [from value]
+ Located input field 'ifIP' [walk]
+ Executing SNMP walk for data @ '.1.3.6.1.2.1.4.20.1.2'

ANEXO 2

Se muestra la ejecución de la orden Walk, la que realiza una serie completa de getnexts automáticamente y se detiene cuando devuelve resultados que no están en el rango del OID especificado originalmente. Por ejemplo, si quisiéramos obtener toda la información almacenada en el grupo system del MIB de una máquina podríamos hacerlo utilizando esta órden:

```
# snmpwalk -v 2c -c public localhost system
SNMPv2-MIB::sysDescr.0 = STRING: Linux mago.aut.uah.es 2.6.0-test11 #27
Tue
Dec 16 11:39:03 CET 2003 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
SNMPv2-MIB::sysUpTime.0 = Timeticks: (120246) 0:20:02.46
SNMPv2-MIB::sysContact.0 = STRING: Root (configure
/etc/snmp/snmp.local.conf)
SNMPv2-MIB::sysName.0 = STRING: mago.aut.uah.es
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (4) 0:00:00.04
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-
MIB::snmpFrameworkMIBCompliance
```

SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module to describe generic objects
for network interface sub-layers
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing IP and ICMP
implementations
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.7 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.9 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (0) 0:00:00.00

SNMPv2-MIB::sysORUpTime.5 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (4) 0:00:00.04
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (4) 0:00:00.04
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (4) 0:00:00.04

ANEXO 3

Autorización de uso de información.

JUNTA DE BENEFICENCIA DE GUAYAQUIL
Dirección de Informática
Vélez 109 Conmutador 2324-060 Casilla 789
Guayaquil – Ecuador
ervierav@loteria.com.ec

Septiembre 10 de 2012

Señor Doctor
Boris Ramos
Director de la Maestría en Telecomunicaciones
Facultad de Ingeniería Eléctrica y Telecomunicaciones
ESPOL

De mis consideraciones:

Por medio de la presente, le saludo y le informo que el Ingeniero Juan Pablo García Baquerizo, con cédula de identidad 0910857283, ha sido autorizado para registrar información relacionada con la Gestión de Operación de la Red, basada en el protocolo SNMP, incluyendo imágenes y gráficos relacionados con el control de datos de los centros de cómputo, red de comunicación y gestión de impresión de la Junta de Beneficencia de Guayaquil, así como la mención de eventos e incidentes de TI atendidos, con fines estrictamente académicos, como material de su trabajo de Tesis para la obtención de su titulo de Máster en Telecomunicaciones.

Atentamente

Erwin Rivera Villamar
Director de Informática

Copia a: Ing. César Yépez Director de Tesis

BIBLIOGRAFÍA

[1] Marshall DenHartog, Tutorial SNMP: The Fast Track Introduction to SNMP Alarm Monitoring, DPS Telecom, Julio 2010, página 4.

[2] Marshall DenHartog, Demystifiyng the SNMP MIB: “How to Read and Understand the SNMP MIB”, DPS Telecom, febrero 2008, página 4.

[3] Oracle corporation, What Is an SNMP-Compliant MIB, http://docs.oracle.com/cd/E13161_01/tuxedo/docs10gr3/snmpmref/1tmib.html, 2008

[4] Rteldat, Introducción a SNMP, http://www.it.uc3m.es/~teldat/Cbra/castellano/protocolos/Dm512v840_Agente_SNMP.PDF, página 3, diciembre 2012.

[5] Marshall DenHartog, Tutorial SNMP: The Fast Track Introduction to SNMP Alarm Monitoring, DPS Telecom, Julio 2010, página 5.

[6] Figueroa Arias, Tesis: Herramientas de Gestión basada en Web, http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Arias_Figueroa.pdf, pagina 15, diciembre 2012

[7] Murillo Sujel, Seguridad de la información, http://h18000.www1.hp.com/products/quickspecs/10757_div/10757_div.HTML, septiembre 2011.

[8] Marshall DenHartog,Tutorial SNMP: The Fast Track Introduction to SNMP Alarm Monitoring, DPS Telecom, Julio 2010, página 10.

[9] Hinojosa Víctor, Madruñero Luis, Ortega Luis, Tesis: Sistema de Gestión de Red, repositorio.utn.edu.ec/bitstream/123456789/577/1/TesisFinal.doc, página 5, diciembre 2012.

[10] Cervantes Rosalba, Manual de administración de centros de cómputo, http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/Adm%C3%B3n%20de%20Centros%20de%20Computo%20%20%20R.C.M/UNIDAD%20I.pdf, página 2, diciembre 2012.

[11] Turner W. Pitt IV, P.E., Seader Jhon H. (Hank), P.E. and Brill Kenneth G. White Paper: Tier Classifications, Uptime Institute, www.uptimeinstitute.org, octubre 2012

[12] Turner W. Pitt IV, P.E., Seader Jhon H. (Hank), P.E. and Brill Kenneth G. White Paper: Tier Classifications, Uptime Institute, www.uptimeinstitute.org, octubre 2012

[13] Gomez Emmanuel, Presentación: Enlace Troncal http://www.slideshare.net/gomez012/enlace-troncal, diciembre 2012

[14] Quinodoz Carolina, Blog de Informática, Función de un Switch, http://profecarolinaquinodoz.com/principal/?tag=funcion-de-un-switch, mayo 2009.

[15] Cisco, Lo que necesita saber sobre Routing y Switching, http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/routing_switching_primer.html, diciembre 2012.

[16] Kioskea, Router, http://es.kioskea.net/contents/lan/routeurs.php3, diciembre 2012

[17] Fraser Ed. RFC 2196, Site Security Handbook, 2.1.1 Definition of a Security Policy, página 7, diciembre 2012

[18] Textos científicos, Política de Seguridad, http://www.textoscientíficos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/2006, diciembre 2012.

[19] Osiatis, gestión de Operaciones, http://itilv3.osiatis.es/operación_servicios_TI/gestión_operaciones_ti/funciones_gestión_operaciones.php, diciembre 2012

[20] Millan Ramon, Gestión de Red, Arquitectura de gestión de red http://www.ramonmillan.com/tutoriales/gestiónred.php, diciembre 2012

[21] General Electric, manual de operación tarjeta SNMP, páginas 4 y 5, octubre 2012.

[22] Cisco, Brochure Cisco catalyst 2960, http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/catalyst_2960_series_switches/index.html, diciembre 2012

[23] Cisco, Brochure Cisco catalyst 3750, http://www.cisco.com/en/US/products/hw/switches/ps5023/index.html, diciembre 2012.

[24] Cisco, Brochure Router 2911, http://www.cisco.com/en/US/products/ps10540/index.html, diciembre 2012

[25] Ubiquit, Ubiquiti Networks, Catálogo de radio rocket M5, http://dl.ubnt.com/datasheets/rocketm/rm_ds_web.pdf, diciembre 2012.

[26] Emerson, Tarjeta de Interfaz Liebert, http://www.emersonnetworkpower.com/es-CALA/Products/Monitoring/ForLargeDataCenter/AdvancedMonitoring/Pages/LiebertOpenCommsWebcardInterfaceCard.aspx., diciembre 2012.

[27] Cacti, about cacti, http://www.cacti.net/, octubre 2012

[28] Berry Bob, Scada Tutorial, DPS Telecom, página 3

[29] Paessler, PRTG Network Monitor, http://www.es.paessler.com/prtg/features, octubre 2012.

[30] Innovative Businness Solutions Coral, Nagios,http://ibs.ec/site/productos/nagios.html, diciembre 2012.