UNIVERSIDAD INDUSTRIAL DE SANTANDER

ANÁLISIS DE LA GESTIÓN DE LOS DISPOSITIVOS ADMINISTRABLES EN LA RED DE DATOS INSTITUCIONAL

PAOLA FERNANDA GUZMÁN CASTILLO

FACULTAD DE INGENIERÍAS FISICOMECÁNICAS

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES

BUCARAMANGA

2005

ANÁLISIS DE LA GESTIÓN DE LOS DISPOSITIVOS ADMINISTRABLES EN LA RED DE DATOS INSTITUCIONAL

PAOLA FERNANDA GUZMÁN CASTILLO

Trabajo de investigación presentado como requisito
Para optar al título de MAGÍSTER EN INGENIERÍA

Director
Ph.D. OSCAR GUALDRON GONZALEZ

FACULTAD DE INGENIERÍAS FISICOMECÁNICAS
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES
BUCARAMANGA
2005

Es mejor arrepentirse de lo que se hace
y no de lo que se deja de hacer…

AGRADECIMIENTOS

A Dios por darme las herramientas para poder llevar a cabo este trabajo. A todas y cada una de las personas que me acompañaron y aconsejaron durante esta etapa, especialmente a mis compañeros del Grupo de Investigación en Conectividad y Procesado de Señal. A mi director por su orientación, paciencia y confianza. A mi familia por su apoyo incondicional.

TABLA DE CONTENIDO

LISTA DE FIGURAS

TITULO: ANÁLISIS DE LA GESTIÓN DE LOS DISPOSITIVOS ADMINSITRABLES DENTRO DE LA RED DE DATOS INSTITUCIONAL*

AUTOR: GUZMAN CASTILLO, PAOLA FERNANDA**

PALABRAS CLAVE: Fallas de red, Gestión de Red, Base de Información de Gestión MIB, Detección de fallas, Clasificación de Fallas, Tormenta Broadcast, Congestión.

DESCRIPCIÓN

El trabajo desarrollado comprende dos etapas: la primera estuvo orientada a determinar las características principales de la red de datos de la universidad, incluyendo un inventario detallado del hardware de la red y los servicios ofrecidos con ellos. Una vez evaluadas diferentes opciones, se seleccionó una herramienta de gestión de red que según los requisitos técnicos y las limitaciones de presupuesto consideradas, satisface de manera apropiada las necesidades identificadas. Las características principales de la herramienta seleccionada junto con una configuración sugerida para la red de datos de la universidad se han incluido en una guía escrita que forma parte de este trabajo.

En la segunda parte, aceptando la hipótesis de que las fallas de red pueden ser clasificadas a partir de los datos contenidos en la Base de Información de Gestión (MIB) de los dispositivos asociados a ella, se desarrolló una metodología para la identificación y clasificación de algunas de las fallas de red más comunes en redes de área local que utilizan Ethernet como tecnología de red. La metodología planteada detecta cambios repentinos o patrones inusuales en los datos de la MIB de los dispositivos administrables que forman parte del segmento analizado y los asocia con algún tipo de falla específico. El trabajo se restringió al análisis de dos de las fallas más frecuentes en redes de datos: congestión y tormenta de Broadcast. Dado el gran número de variables disponibles en la estructura de la MIB, fue requerido un análisis teórico que permitió establecer un reducido grupo de ellas y su asociación con cada una de las fallas analizadas. Los valores de las variables MIB seleccionadas fueron registrados tomando como escenario un segmento de red Ethernet operando bajo condiciones normales y condiciones de falla. Finalmente, una red neuronal de clasificación fue exitosamente entrenada usando los datos registrados.

---

*Trabajo de Investigación
**Facultad de Ingenierías Fisicomecánicas
Maestría en Ingeniería Área Electrónica
Director: Gualdrón González, Oscar

TITLE: EVALUATION OF THE MANAGEABLE DEVICES OF THE DATA NETWORK AT UNIVERSIDAD INDUSTRIAL DE SANTANDER[†]

AUTHOR: GUZMÁN CASTILLO, PAOLA FERNANDA**

KEYWORDS: Network Fault, Network Management, Management Information Base (MIB), Fault Detection, Fault Classification, Broadcast Storm, Congestion

DESCRIPTION

This work has been done in two stages. The first one was aimed to determine the main features of the data network of the university, including a detailed inventory of the network hardware as well as the services offered with them. An appropriated network management tool was selected among several ones evaluated according to the technical requirements and budget constraints. The main features of the selected tool with a suggested configuration for the data network of the university have been included in a guide written as part of this work.

In the second stage, accepting that network failures can be classified from the data contained in the Management Information Base (MIB) of the devices associated to it as hypothesis, a methodology to identify and classify some common failures in local area networks using Ethernet technology was developed. The methodology detects sudden changes or unusual patterns in the MIB data of the managed devices belonging to the segment under analysis and associates them with some type of failure. The work was restricted to analyze two of the most frequent failures in a data network: Congestion and broadcast storm. Given the huge number of variables available in the MIB structure, a theoretical analysis was required to establish a reduced set of them that could be associated with each type of failure. The values of the selected MIB variables were registered under normal and failure conditions in an Ethernet segment. Finally, a neural network classifier was successfully trained using these data.

---

*Trabajo de Investigación
**Facultad de Ingenierías Fisicomecánicas
Maestría en Ingeniería Área Electrónica
Director: Gualdrón González, Oscar

INTRODUCCIÓN

Durante la última década, se ha observado una significativa ampliación en los servicios ofrecidos por las redes de comunicaciones a sus usuarios. La creciente demanda por parte de los usuarios ha marcado la pauta en la evolución de las grandes redes.

La tendencia actual es hacia redes de mayor tamaño y por tanto mayor complejidad. Debido a esto y a la gran dependencia que de ellas tienen las organizaciones en la actualidad, ya que permiten la integración de aplicaciones, servicios e información de todo tipo para sus usuarios; se ha originado un gran interés en la gestión de los recursos de red y el incremento de su disponibilidad. Las actividades de gestión se han convertido en un factor crítico en la medida que la confiabilidad de la red es un requisito básico para hacer un uso eficiente de los recursos y ofrecer una calidad del servicio adecuada.

La gestión de redes busca garantizar un adecuado nivel de servicio por medio de la planificación, organización, supervisión y control de los dispositivos de red. Los objetivos principales de la gestión de red son incrementar la disponibilidad y el rendimiento de los elementos del sistema, así como su efectividad.

La Universidad Industrial de Santander no ha sido ajena a la necesidad de contar con una red de datos en permanente evolución, que le permita ofrecer unas condiciones básicas de acceso, con lo cual se favorece el desarrollo investigativo y el mejoramiento de la actividad docente, no sólo a nivel de la institución sino también para su entorno. Por esta razón, en los últimos años se ha notado un crecimiento significativo de la infraestructura física de la red institucional, evidenciada con la puesta en marcha de nuevas salas de cómputo, la instalación de nuevos servicios y la adquisición de equipos de tecnología reciente.

En el caso particular de la Universidad Industrial de Santander, el desarrollo de la mayor parte de las actividades propias de la institución, se encuentra soportado por diferentes sistemas de información incluidos el sistema financiero, el sistema académico y otros servicios de base de datos entre otros, los cuales son utilizados en los diferentes campus y algunas sedes a través de la red de datos institucional. De allí la importancia que se debe prestar a las tareas de mantenimiento, supervisión y gestión en general de dicho recurso.

Es importante resaltar que en la mayoría de los casos el bajo desempeño de una red no se relaciona de manera única con la infraestructura de la misma, y por tanto de nada sirve realizar grandes inversiones en adquisición de equipos o mejoramiento de accesos a proveedores de servicio, si la falla principal radica en una estrategia de gestión de red inadecuada.

Teniendo en cuenta las anteriores consideraciones surgió la idea de realizar el presente trabajo de investigación cuyo objetivo central era hacer un análisis detallado de la gestión de la red de datos Institucional, el cual se espera sirva como punto de partida para el desarrollo futuro de un esquema de gestión acorde a las necesidades de la red. Al hablar de gestión de redes se debe tener presente la magnitud del problema- Como se describirá en el primer capitulo, según el modelo OSI (Open Systems Interconection) se pueden diferenciar cinco áreas funcionales de la gestión en las que se hace una recopilación de las distintas tareas implícitas en esta actividad.

Dentro de las actividades de gestión de redes, la gestión de fallas tiene una alta prioridad, ya que una falla simple puede propagarse a través de la red y causar pérdidas considerables. Debido a la innegable importancia que tiene desde el punto de vista tanto del administrador como del usuario el poder controlar este tipo de situaciones, la gestión de fallas se ha convertido en el eje central de este trabajo.

Para la realización del trabajo se ha definido una serie de etapas que será descrita de la siguiente manera a lo largo del presente documento: en el primer capitulo se presenta una recopilación de los conceptos teóricos tenidos en cuenta para la realización del trabajo. La

concepción del esquema de gestión debe desarrollarse de manera particular para cada red y requiere un conocimiento profundo y detallado de la misma, por tal razón como punto de partida se realizó un reconocimiento general de la red, con el fin de identificar las principales características de los dispositivos que la conforman, así como los servicios ofrecidos; los resultados de esta etapa han sido consignados en el segundo capitulo del documento.

Al hablar de los elementos necesarios para realizar la tarea de gestión se debe resaltar la importancia que tiene para el éxito de esta actividad, el personal encargado o recurso humano disponible, sin embargo también se hace evidente la necesidad de contar con una herramienta de gestión acorde a las necesidades de la red. En el tercer capitulo se describen el procedimiento y criterios tenidos en cuenta para la selección de la herramienta de gestión que se considera se ajusta mejor a los requerimientos de la red de datos Institucional.

Teniendo en cuenta que el eje central del trabajo estaba orientado al área de gestión de fallas, y siendo conscientes de la dificultad que en algunos caso esta actividad representa para los operadores humanos se desarrolló una metodología para la detección y clasificación de distintos tipos de fallas en un segmentos Ethernet,[3] tecnología utilizada en la red de datos de la Universidad Industrial de Santander.

[3] Nombre comercial de la tecnología que implementa el Carrier Sense Multiple Access with Collision Detection (CSMA/CD) estandarizado por la norma IEEE 802.3. Se usará el nombre comercial por simplicidad a lo largo del documento.

1. ESTADO DEL ARTE Y MARCO TEÓRICO

Los modelos de gestión de red evolucionan a la par con el desarrollo de las tecnologías que permiten el crecimiento de las redes mismas.

El término **Gestión de red** involucra básicamente dos aspectos: la administración de los dispositivos de red como lo son los hubs, switches, enrutadores, etc, y la administración de los enlaces que los interconectan. Sin embargo antes de empezar a hablar de gestión de red es importante revisar algunos conceptos de redes haciendo énfasis en los que caracterizan la red de datos de la Universidad Industrial de Santander, referente clave de la investigación.

1.1 Redes de Área Local

Una Red de Área Local se puede definir como un tipo de red privada que permite la interconexión entre un conjunto de terminales o equipos informáticos, por lo general computadores personales, para transmitir datos a gran velocidad en un entorno geográfico restringido.

Según el comité IEEE 802 (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos):

> "Una Red de Área Local se distingue de otros tipos de redes de datos en que las comunicaciones están normalmente restringidas a un área geográfica de tamaño limitado, como un edificio de oficinas o un campus, y en que puede depender de un canal físico de comunicaciones con una velocidad binaria media/alta y con una tasa de errores reducida".

El concepto de red de área local responde fundamentalmente a la necesidad de compartir recursos, tales como cableado interno, periféricos en una amplia variedad y, particularmente, para permitir que diferentes usuarios puedan compartir recursos entre sí.

Las propiedades básicas que caracterizan una red de área local son las siguientes:

- Permite la interconexión de dispositivos heterogéneos.
- Contribuye al incremento de la velocidad de transferencia de datos (Decenas de Mbps).
- Su empleo está restringido a zonas geográficas poco extensas, tales como departamentos de una empresa, edificios de oficinas, campus universitarios, etc., con a lo sumo unos pocos kilómetros de longitud total.
- Los medios de comunicación, así como los diferentes componentes del sistema, suelen ser privados.
- Se caracteriza por la facilidad de instalación y flexibilidad de reubicación de equipos y terminales, así como por el costo relativamente reducido de los componentes que utiliza.

La necesidad de compartir recursos es una de las razones principales para la instalación de una red en una organización, ya que estas facilitan el acceso a los mismos por parte de los usuarios permitiendo una utilización más eficiente y económica entre otros de:

- Módems y líneas de comunicaciones
- Discos y unidades de almacenamiento masivo
- Impresoras
- Aplicaciones e Información

Existen varias tecnologías de capa de enlace de datos disponibles para redes LAN. Entre éstas se encuentran Ethernet, Token Ring, Token Bus y FDDI (Fiber Distributed Data Interface) principalmente. La red de datos de la Universidad Industrial de Santander, al igual que la gran mayoría de las redes que han sido instaladas recientemente, utiliza Ethernet[26], debido a que dicha tecnología proporciona características superiores en aspectos como escalabilidad, administrabilidad, confiabilidad y capacidad; además, satisface requerimientos

como ancho de banda elevado, costos moderados, y calidad de servicio, aspectos que las demás tecnologías no han logrado desarrollar al mismo nivel.

Ethernet ha logrado posicionarse como la primera solución para Redes de Área Local. Algunas características que le han permitido afianzarse son el uso de tramas de longitud variable entre 64 y 1518 bytes y además el incremento considerable de su velocidad de operación desde su inicio a 10Mbps hasta alcanzar tasas de transmisión de 10 Gbps; éstas y otras características han ubicado a Ethernet como la solución más utilizada, llegando a tener más del 80% del dominio del mercado.

Para la evaluación del desempeño de una red de datos, al igual que para el planteamiento de un esquema de gestión de red, es necesario conocer sus condiciones físicas, lo cual requiere la observación y análisis de varios aspectos. El estudio de los aspectos físicos de la red permite dimensionar su capacidad real, es decir, establecer el número total de usuarios, número de segmentos, dispositivos de red asociados, estado de los enlaces, cumplimiento de normativas, etc., que son elementos básicos para desarrollar una adecuada gestión de red.

1.2 Estructura Física

La topología física empleada en la red de datos de la UIS corresponde a una estrella jerárquica. Una topología en estrella es un conjunto de enlaces punto a punto originados de un nodo central; los enlaces aparecen como radios saliendo del nodo, así como los rayos salen de una estrella. Este tipo de topología tiene varias ventajas:

- El nodo central facilita las tareas de administración para mover, adicionar y cambiar equipos.
- Los puntos de cableado central proveen una rápida gestión de problemas.
- Los enlaces punto a punto independientes evitan problemas que un enlace pudiese causar a los demás.
- Los equipos del nodo central pueden permitir una rápida migración a nuevos tecnologías.

- Ofrece capacidad de seguridad física, porque en caso de falla en algún segmento, éste se puede aislar fácilmente. Una topología en estrella también tiene mayores ventajas para realizar tareas de instalación y mantenimiento, ya que, se puede determinar cuál equipo está conectado a cada extremo. En la Figura 1 se muestra la estructura básica de una topología estrella.

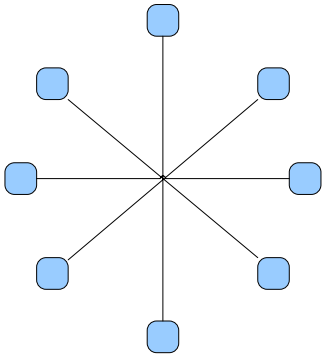


Figura 1. Topología Estrella

Debido a diversas razones como el crecimiento elevado y rápido de la red de datos de la Universidad no se ha dado lugar a la actualización y planeación rigurosa de dicha expansión.

1.3 Dispositivos Asociados

Hoy en día las redes combinan diferentes tipos de dispositivos entre los que encuentran hubs, bridges (puentes), swicthes (capa 2 o capa 3) y enrutadores. Algunos de ellos como los switches y los enrutadores permiten ser administrados y configurados para que tomen decisiones cuando reciben un paquete.

De alguna forma u otra se podría considerar que, excepto los hubs, estos dispositivos tienen un atributo en común: son conmutadores. Cada dispositivo recibe tráfico en un puerto y decide si debe ser enviado a un puerto de otro dispositivo. La diferencia radica en la velocidad y la información que utiliza para tomar esta decisión.

Cuando hablamos de gestión de red nos referimos a la gestión de los dispositivos de red específicamente, por eso es importante tener un conocimiento preciso y detallado de las

características principales presentes en estos dispositivos e identificar cuales son administrables remotamente.

1.3.1. Hubs o Repetidores

Un hub[3] es un dispositivo que permite construir multisegmentos en los sistemas Ethernet y se usa fundamentalmente para conectar nodos en una LAN. Un hub puede ser el centro de una estrella lo cual simplifica el cableado y cambio de conexiones.

Se puede decir que un hub Ethernet es un repetidor multipuerto, ya que el tráfico enviado por una estación es enviado a todos los demás puertos del dispositivo. Los hubs desempeñan funciones básicas que no varían para ninguno de los sistemas de 10, 100 y 1000 Mbps, entre las que se pueden nombrar las siguientes: Alertar sobre colisiones a todos los segmentos; cuando un hub detecta una colisión envía una señal *jam*, la cual asegurará que en los demás segmentos se detecte la colisión y se detengan las transmisiones. Restaurar la amplitud y simetría de la señal. Adicionalmente la mayoría de los hubs cuentan con LEDs que indican ciertos aspectos de la actividad de la red, tales como, segmentos que se encuentren transmitiendo o recibiendo datos, segmentos en los que ocurran colisiones y segmentos aislados por causa de una falla.

Los hubs han sido ampliamente utilizados para construir y extender sistemas Ethernet; sin embargo, en los últimos años se han visto desplazados porque los diseños actuales involucran principalmente switches, los cuales tienen otras características y capacidades más atractivas para los diseñadores de redes de datos, como lo es manejar un dominio de colisión único por cada puerto, lo cual reduce el número de colisiones dentro del segmento y por tanto mejora el desempeño.

En términos de administración de una red, los hubs son dispositivos de acceso compartido, por lo tanto el número de estaciones conectadas o el nivel de tráfico generado por cada una de ellas pueden en algún momento llegar a degradar el desempeño de la red.

1.3.2. Switches o conmutadores

Los switches[3,12] son dispositivos de alta capacidad. A diferencia de los hubs en ellos no se debe competir por el acceso al medio, cada nodo tiene asignados sus propios recursos independientemente del número de estaciones conectadas o el tráfico generado por ellas. Son dispositivos que permiten enlazar segmentos Ethernet que operan a distintas velocidades y controlar el flujo y tráfico a través de un sistema. Los switches mejoran la confiabilidad de los sistemas Ethernet y pueden incrementar ampliamente el ancho de banda habilitado.

Los switches son diseñados de tal forma que su modo de operación sea transparente a las estaciones y/o equipos de trabajo en la red; es decir, que puedan enlazar segmentos de una red LAN sin necesidad de realizar ningún cambio en las estaciones. La capacidad de un switch puede ser identificada teniendo en cuenta el número de puertos, la velocidad de transmisión (fps), las opciones de administración y el número de direcciones MAC (Medium Access Control) que puede almacenar, entre otros.

1.3.2.1 Características avanzadas de los switches

Las más representativas son:

Administración. Los switches pueden tener un software de administración que permite recolectar y visualizar estadísticas sobre errores y actividad de la red. El acceso a este software puede hacerse directamente por puertos de consola o en forma remota utilizando una conexión a través de algún protocolo.

Filtros. Los filtros le permiten al administrador de una red especificar el filtrado de tramas basado en ciertos parámetros, como dirección de las tramas, tipo del campo, etc, con el fin de controlar el flujo de tráfico en la red. El número de filtros que soporta un switch varía ampliamente dependiendo del fabricante. Es importante tener en cuenta que los filtros a pesar de permitir una mejor administración de la red son muy complejos de configurar y pueden causar algunas fallas o disminuir el desempeño de la misma. Por esta razón el administrador de red debe conocer ampliamente las características del filtro y su forma de implementación.

1.3.2.2 LAN Virtuales (VLANs)

La configuración de VLANs es una de las características adicionales que pueden ofrecer los switches, para agrupar el flujo de tráfico dentro de éstos. En términos generales las VLANs tienen dos características bastante interesantes desde el punto de vista del administrador, la primera es limitar los dominios de broadcast en el ámbito de un segmento de red y la segunda, que permiten la interconexión de estaciones ubicadas en distintos segmentos de red físicos como si se encontraran dentro de la misma LAN.

Las VLANs en un switch se pueden configurar de distintas formas, por agrupación directa de puertos, agrupación por direcciones IP (Internet Protocol) y agrupación por direcciones MAC entre otras, pero en cualquiera de los casos existe una separación de dominios de broadcast, lográndose una contención y regulación del tráfico que circula por los puertos del switch.

1.3.3. Enrutadores o routers

El Enrutador es el componente de hardware básico para interconectar redes heterogéneas. Físicamente, los enrutadores[12] semejan puentes (un enrutador es un computador de propósito especial dedicado a interconectar redes). Como los puentes, los enrutadores tienen procesador y memoria convencionales así como interfaces de E/S para todas las redes que se conectan. Las conexiones del enrutador no están limitadas a ciertas tecnologías de red. Un enrutador puede interconectar LANs, LANs con WANs o WANs. Además, cuando un enrutador interconecta dos redes de la misma categoría general, estas no necesariamente deben usar la misma tecnología.

1.3.4. Servidores

El servidor es un computador o dispositivo que se encarga de la administración de los recursos de red. Por ejemplo un servidor de archivos es un computador y dispositivo dedicado al almacenamiento de archivos. Cualquier usuario dentro de la red puede cargar o descargar archivos desde el servidor. Un servidor de impresión es un computador que administra una o más impresoras y un servidor de red es un computador que administra el tráfico dentro de la red. Un servidor de base de datos es un sistema de cómputo que procesa peticiones de base de datos provenientes de diferentes usuarios. Los servidores son

usualmente equipos dedicados, esto significa que no realizan otras tareas distintas a sus tareas como servidor.

1.4 Conceptos de Gestión de Red

La ISO (International Organization for Standardization) define la gestión de red como:
"El conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red"

La gestión de redes comprende las herramientas necesarias para realizar las siguientes funciones:

Monitorización de la red

Se suele realizar de dos formas: mediante una estación de gestión o estación de trabajo que recibe mensajes de los dispositivos de la red (switches, enrutadores o routers, servidores, etc.) o mediante una estación que interroga regularmente el estado de los dispositivos.

Control de los dispositivos de la red

Se realiza enviando comandos por la red desde la estación de gestión hasta los dispositivos de la red para cambiar su configuración.

Los sistemas de gestión deben poder crecer a medida que crecen las necesidades de los usuarios, de forma que se puedan proteger las inversiones realizadas. Un entorno integrado de gestión consiste en una combinación de recursos humanos, organizativos y tecnológicos. La gestión de redes es una estrategia a largo plazo que puede afectar a todo el personal de una organización.

Además de la gestión operativa (atender usuarios, resolver fallas en el menor tiempo posible, monitorizar, etc.) existen otros aspectos involucrados que permiten definir el análisis y la optimización de la red:

- La descripción funcional de tareas que serán objeto de la gestión.
- La especificación de procedimientos que faciliten la atención de eventos de interés.

- La adquisición de medios técnicos.
- La adaptación de los recursos humanos disponibles.

1.4.1. Componentes de un sistema de gestión

Los procedimientos de gestión de redes se basan en el modelo **Gestor-Agente**, que puede operar de dos formas. La forma directa consiste en un proceso de gestión centralizado en el cual una entidad llamada gestor obtiene la información de gestión interrogando a cada uno de los dispositivos administrables.

El otro esquema consiste en una gestión distribuida en la cual los agentes presentes en cada dispositivo pueden comportarse también como gestores y recopilar información de otros dispositivos presentes en el mismo nodo de red y hacer un único reporte al gestor principal, ahorrando de esta manera recursos y tiempo en el proceso de gestión.

La gestión de un entorno de telecomunicaciones es una aplicación de procesamiento de información, en la cual intervienen elementos fundamentales como son el gestor, el agente, el protocolo de gestión, y la base de información de gestión MIB (Management Information Base), los cuales interactúan entre sí como se muestra en la Figura 2.

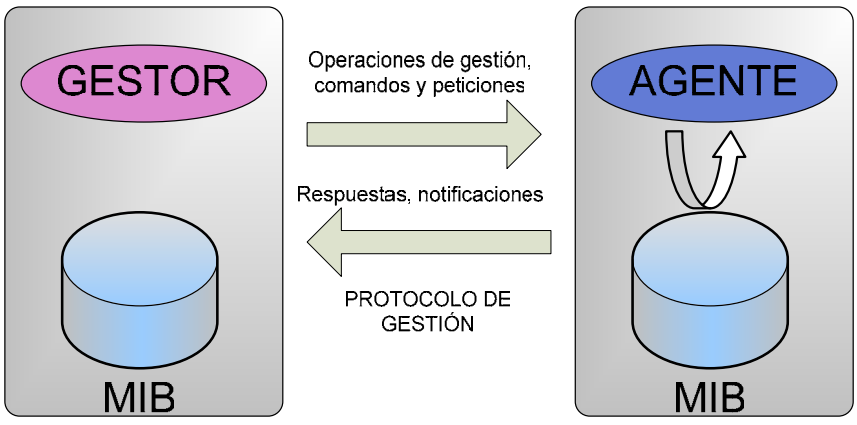


Figura 2. Modelo Gestor-Agente

1.4.1.1 Estación de gestión o gestor

El gestor es la componente de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas. Este se implementa en una estación de gestión en la cual se debe disponer de la MIB del dispositivo en gestión y una interfaz de usuario.

A continuación se hace una descripción de los componentes de la estación de gestión o gestor:

- *Interfaz de usuario:* Es la interfaz entre el usuario y el sistema que puede ser basada en caracteres o gráfica.
- *Base de datos:* Mantiene cualquier información de la red (descripciones de diferentes parámetros, configuración de contadores, entre otros), almacenando el histórico de eventos y permitiendo la realización de seguimientos.
- *Programa monitor:* Supervisa las condiciones actuales y permite programar la inspección futura. Visualiza las alarmas activadas por los agentes y realiza actualizaciones mediante sondeos regulares.
- *Protocolo de gestión:* Controla las operaciones de gestión entre el gestor y el agente.

1.4.1.2 Agente

El agente tiene la función de responder a las directivas enviadas por el gestor y lo realiza obteniendo información de la MIB para manipular los objetos involucrados en la operación. El agente se encuentra ubicado en el dispositivo de telecomunicaciones gestionado.

1.4.1.3 Protocolo de Gestión

El protocolo es el conjunto de especificaciones y convenciones que gobiernan la interacción de procesos y elementos dentro de un sistema de gestión. En la actualidad SNMP (Simple Network Management Protocol), que forma parte del modelo de gestión de Internet, y CMIP (Common Management Information protocol), su equivalente en el modelo de gestión OSI, son los protocolos predominantes.

1.4.1.4 MIB

La MIB contiene información sobre los objetos a gestionar. El concepto de objeto es diferente al empleado en la programación orientada a objetos y se asemeja más a una estructura de datos compleja. Cada recurso de la red se representa mediante un objeto. La MIB se encuentra ubicada en el dispositivo gestionado, y una referencia de ésta es necesaria en el gestor. Las operaciones de monitorización consultan el valor de los objetos y las operaciones de control modifican el valor de los objetos.

La MIB, es una colección de información organizada jerárquicamente, que se accede mediante la utilización de protocolos de gestión de red como SNMP. La MIB contiene toda la información relacionada con el estado y con la configuración de los elementos de red.

La MIB tiene 126 áreas de información sobre el estado del dispositivo, el desempeño, sus conexiones y su configuración. A través de la MIB se tiene acceso a la información de gestión, contenida en la memoria interna de cada dispositivo administrable. La estación de gestión (gestor) consulta la MIB de cada dispositivo a través del software agente instalado en cada uno de ellos.

La información almacenada en la MIB y que se encuentra disponible para su monitorización, puede ser clasificada como sigue[11]:

Estática: Es la información que caracteriza o describe la configuración actual y los elementos presentes, tal como el número e identificación de los puertos en un router. Esta configuración varía con muy poca frecuencia.

Dinámica: Ésta información cambia frecuentemente por estar relacionada con los eventos en la red, tal como el cambio de estado de un dispositivo o un enlace.

Estadística: Es información que puede ser obtenida de la información dinámica, tal como el número de paquetes descartados por unidad de tiempo.

Cada una de las variables que conforma la MIB es identificada con el OID (Object Identifier) 1.3.6.1.2.1 dentro del árbol de OIDs establecido por la ASN.1 (Abstract Syntax Notation One), estándar internacional que describe la estructura para el intercambio de datos entre sistemas de comunicación[9].

Los OIDs corresponden a una secuencia de enteros separados por puntos decimales, que establecen niveles numéricos que permiten establecer el camino hacia cualquier objeto dentro del árbol partiendo de la raíz. Por ejemplo a la variable etherStatsPkts, que permite conocer el número total de paquetes recibidos (incluyendo paquetes de broadcast y multicast), le corresponde el OID 1.3.6.1.2.1.16.1.1.1.5 (iso.org.dod.internet.mgmt.mib-2.rmon.statistics. etherStatsTable.etherStatsEntry.EtherStatsPkts).

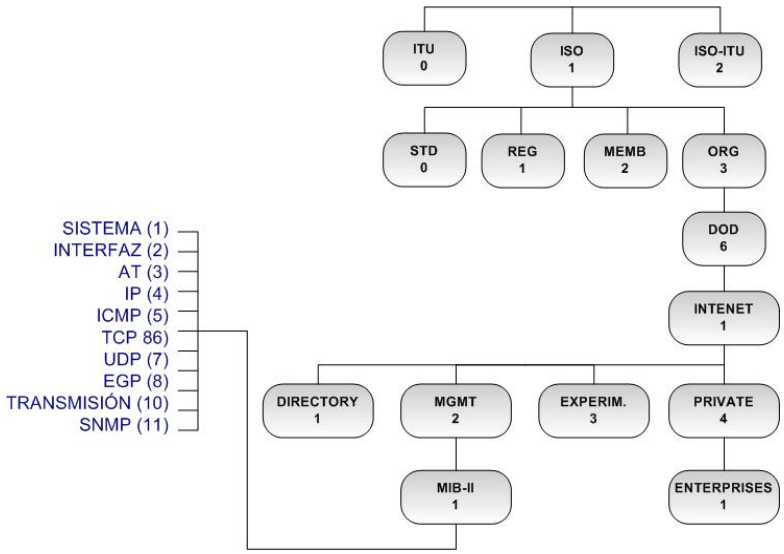


Figura 3. ASN.1 Árbol jerárquico de OIDs

Al final de cada rama se encuentran los campos de datos. Un campo de datos puede ser un único valor o una tabla completa con diferentes valores. La MIB consiste en una colección de objetos organizados en grupos. Cada objeto almacena valores que representan los diferentes recursos administrados.

Con el fin de centrar la atención en la información relacionada con la gestión de dispositivos, dentro del árbol jerárquico de identificadores de objetos, se deben ubicar básicamente los

nodos relacionados con la información de SNMP como lo es nodo de internet y sus ramificaciones hasta llegar a la MIB y sus variables.

Iniciando en la raíz del árbol, se encuentran tres nodos en el primer nivel: iso, ccitt y joint-iso-ccitt. Descendiendo por la rama del nodo iso, se encuentra una subdivisión para su uso por otras organizaciones (org), una de las cuales es el departamento de defensa de los Estados Unidos (dod). El RFC (Request For Coments) 1155 por su parte hace la suposición que una subdivisión de dicho nodo (dod), puede ser asignada para su administración por el IAB (Internet Architecture Board). Así, el nodo internet tiene el identificador de objeto 1.3.6.1. Todos los objetos de interés para SNMP derivan del nodo internet, y por tanto tienen el prefijo 1.3.6.1 en sus identificadores de objeto.

El RFC 1155 define 4 nodos por debajo del nodo internet: directory (1), mgmt (2), experimental (3), private (4). La subdivisión naciente en el nodo mgmt contiene las definiciones de las bases de información de gestión que han sido aprobadas por el IAB. Hasta el momento, han sido desarrolladas dos versiones de la MIB, MIB-1 y MIB-2. La MIB-2 es una extensión de la primera, sin embargo las dos son identificadas por el mismo OID, ya que solo una de ellas puede estar presente en cada configuración.

MIB-1 (RFC 1156) se utilizó a principios de 1988 y tiene 114 entradas en la tabla, las cuales están divididas en grupos. Para que un dispositivo administrable pueda ser compatible con MIB-1, debe manejar grupos que son aplicables a ésta. Por ejemplo, una impresora administrada no tiene que aplicar todas las entradas que traten con el Protocolo para Gateway Exterior (Exterior Gateway Protocol EGP), el cual generalmente lo aplican solamente los enrutadores y los dispositivos similares.

MIB-2 (RFC 1213) es una ampliación a MIB- 1 aprobada en 1990; está conformada por 171 entradas que están divididas en diez grupos. Las adiciones amplían algunas de las entradas de los grupos básicos de MIB-1 y agregan tres nuevos grupos. Al igual que con MIB-1, un dispositivo SNMP que pretenda ser compatible con MIB-2 debe adaptar todos esos grupos que son aplicables a ese tipo de dispositivo.

La MIB en su configuración estándar mantiene 171 variables distribuidas en los siguientes grupos[4]:

- **System (1).** Contiene objetos que describen alguna información básica sobre el agente SNMP, o el dispositivo de red en el que el software agente está siendo ejecutado.

- **Interface (2).** Ofrece información de configuración y estadísticas de desempeño de las interfaces de red. Esta información es aplicable a todo tipo de interfaz.

- **At (Address Translation) (3).** Este grupo era obligatorio para todos los sistemas pero fue descontinuado por la MIB-II. Cada grupo de protocolo de red contiene sus propias tablas de traducción de direcciones.

- **IP (4).** Mantiene información importante relacionada con la operación del protocolo IP en el nodo de red.

- **ICMP (Internet Control Message Protocol) (5).** Provee estadísticas sobre Mensajes ICMP, y es útil para administración de desempeño. Básicamente tiene contadores sobre diferentes tipos y condiciones de mensajes ICMP**.**

- **TCP (Transmission Control Protocol) (6).** Provee algoritmos, parámetros y estadísticas sobre el protocolo TCP. Supervisa segmentos enviados y recibidos, cantidad actual y acumulada de conexiones abiertas, estadísticas de errores, etc.

- **UDP (User Datagram Protocol) (7).** Provee estadísticas de tráfico y detalles sobre datagramas UDP y puntos extremos.

- **EGP (Exterior Gateway Protocol) (8).** Provee estadísticas de tráfico y detalles sobre mensajes EGP generados, recibidos y no enviados y condiciones de vecinos EGP.

---

[4] Ver figura 3

- **Dot3 (Transmisión) (9).** Contiene objetos relacionados con el medio de transmisión especifico para cada interfaz del sistema. Reservado para MIBs específicas de un medio físico.

- **SNMP (10).** Provee estadísticas de tráfico y operaciones del protocolo SNMP.

- **RMON (Remote MONitoring) (16).** Este grupo de objetos no hace parte de los grupos estándar iniciales. RMON es una especificación de monitorización estándar que permite a varios monitores de la red y sistemas de gestión, intercambiar datos de monitorización de red

1.4.2. Arquitecturas de gestión de red

En este apartado se describen las tres principales arquitecturas de gestión de red:

- Modelo OSI
- Modelo TMN[11] (Telecommunication Management Network)
- Modelo Internet (SNMP)

1.4.2.1 Modelo OSI

La ISO ha contribuido en el desarrollo de la mayoría de las funciones de los sistemas de gestión de red y ha definido cinco áreas: gestión del desarrollo de la red, gestión de la configuración, gestión de parámetros de utilización, gestión de fallas y gestión de seguridad de la red, cada una de las cuales se encarga de monitorizar parámetros específicos entre los que se pueden mencionar rendimiento, tiempos de respuesta al usuario, configuración de dispositivos, utilización de enlaces y alarmas, para asegurar la óptima operación de los recursos que conforman la red.

Gestión de Configuración

Esta área se relaciona con la configuración de los dispositivos de la red, para lo cual la estación de gestión debe tener la capacidad de leer o modificar los parámetros asociados a cada elemento gestionado. La gestión de configuración se refiere tanto al nivel físico como al nivel lógico. Debe permitir conocer en cada momento la topología de la red y ofrecer capacidad de auto detectar nuevos dispositivos.

Gestión de Rendimiento

Esta área de la gestión busca entregar información en forma ordenada para determinar la carga del sistema y de la red bajo condiciones naturales y artificiales, que junto con estadísticas obtenidas de la misma permiten desarrollar actividades de planeación de configuración. En ella se incluyen todas las funciones necesarias para evaluar el comportamiento de los objetos gestionados y de la red, incluidos los medios de transmisión. Con base en los resultados se determina la carga real de tráfico (throughput), la disponibilidad y el tiempo de respuesta, y se puede prever la congestión de determinados nodos o rutas con el fin de anticipar eventos futuros que puedan afectar el servicio ofrecido a los usuarios.

Indicadores de rendimiento

Una condición básica para la administración de una red de telecomunicaciones es la capacidad para medir el desempeño de la red, o monitorización del desempeño. No es posible administrar y controlar un sistema de telecomunicaciones sin monitorizar su desempeño. Una de las dificultades más frecuentes para el administrador de la red radica en la selección y uso de los indicadores apropiados que miden el desempeño de la red. Entre los problemas que surgen se encuentran los siguientes:

- Hay demasiados indicadores en uso
- Algunos indicadores no se encuentran asociados con situaciones específicas.
- Algunos indicadores son introducidos y soportados sólo por algunos proveedores
- Algunos indicadores son medidos con exactitud pero incorrectamente interpretados
- Algunas veces el cálculo de indicadores toma demasiado tiempo, y los resultados finales difícilmente pueden ser usados para controlar el ambiente de operación.

Los indicadores que puede usar el administrador de la red se agrupan en dos categorías[4] :

Medidas orientadas al servicio

- Disponibilidad
- Tiempo de respuesta
- Exactitud

Medidas orientadas a la eficiencia

- Throughput[5]
- Utilización

Estos indicadores serán descritos con detalle en el siguiente capitulo.

Gestión de Contabilidad

Se ocupa de actividades de recolección de información de contabilidad, funciones relativas a la administración de los recursos de la red y el cargo que por su uso se debe efectuar a los usuarios. Permite distribuir los costos, generando las facturas para las diferentes dependencias de la organización cuando hay lugar a ello.

Gestión de fallas

Esta área se ocupa de la generación de notificaciones específicas de error para facilitar la detección, aislamiento y corrección de los incidentes que se generen en la red, controlando cualquier funcionamiento que se salga de los márgenes de tolerancia fijados por el administrador. Lo normal es que al producirse una falla se genere una alarma que indique la causa y el lugar del mismo, alertando al personal encargado de la gestión, que actuará en consecuencia. Debido a la importancia que tiene esta área de la gestión sobre el trabajo realizado, se profundizara sobre ella más adelante en la sección 2.5.

Gestión de la Seguridad

Uno de los aspectos más críticos en la gestión de una red corporativa, esencial para mantener la integridad y confidencialidad de los datos y protegerla de la intrusión por terceros, es la seguridad. Con la adopción de Internet como medio de comunicación global y la implantación de su tecnología en las empresas para la creación de Intranets, el aislamiento entre el entorno corporativo y el mundo exterior se ha de conseguir mediante la utilización de firewalls y claves de acceso, que han de estar integrados en el sistema de gestión de red. La gestión de seguridad no se limita a los mecanismos de seguridad (protocolos, mecanismos de cifrado, etc.) sino a toda la política de seguridad que debe implantarse como administración de contraseñas, responsabilidades de los usuarios o seguridad de acceso físico.

[5] Throughput es la tasa a la cual los datos útiles pueden ser enviados sobre el canal.

1.4.2.2 Modelo Internet (SNMP)

El primer estándar para administración de red especificado es el SNMP es un protocolo de capa de aplicación que facilita el intercambio de información de gestión entre los dispositivos de red. Forma parte de la pila de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol) y es el empleado por la gran mayoría de herramientas de gestión.

El esquema de gestión basado en SNMP presenta tres componentes básicos: los elementos de red o dispositivos administrables, los agentes y el sistema de gestión de red NMS (Network Management System).

Un dispositivo administrable es un nodo de red que contiene un agente SNMP. Los dispositivos administrables recopilan y almacenan información de gestión y la ponen a disposición de la estación o sistema de gestión haciendo uso para esto del protocolo SNMP. Los dispositivos administrables, algunas veces llamados elementos de red, pueden ser enrutadores, switches, puentes, hubs, hosts o impresoras, entre otros.

Un agente es un módulo de la herramienta de gestión de red que reside en cada uno de los dispositivos administrables. Un agente tiene un conocimiento local de la información de gestión y traslada esta información a un formato compatible con SNMP.
Un NMS ejecuta aplicaciones que permiten monitorizar y controlar los dispositivos administrables. Las estaciones de gestión son normalmente estaciones de trabajo que visualizan gráficamente los factores más relevantes sobre los elementos que están siendo monitorizados como estado de los enlaces o volumen de tráfico a través de los enlaces a lo largo de determinados periodos de tiempo.

La comunicación de gestión se puede dar en doble vía: el gestor interroga al agente por un valor específico o el agente le reporta al gestor cuando algo imprevisto sucede. Por otro lado el gestor está habilitado para modificar y leer variables del agente.

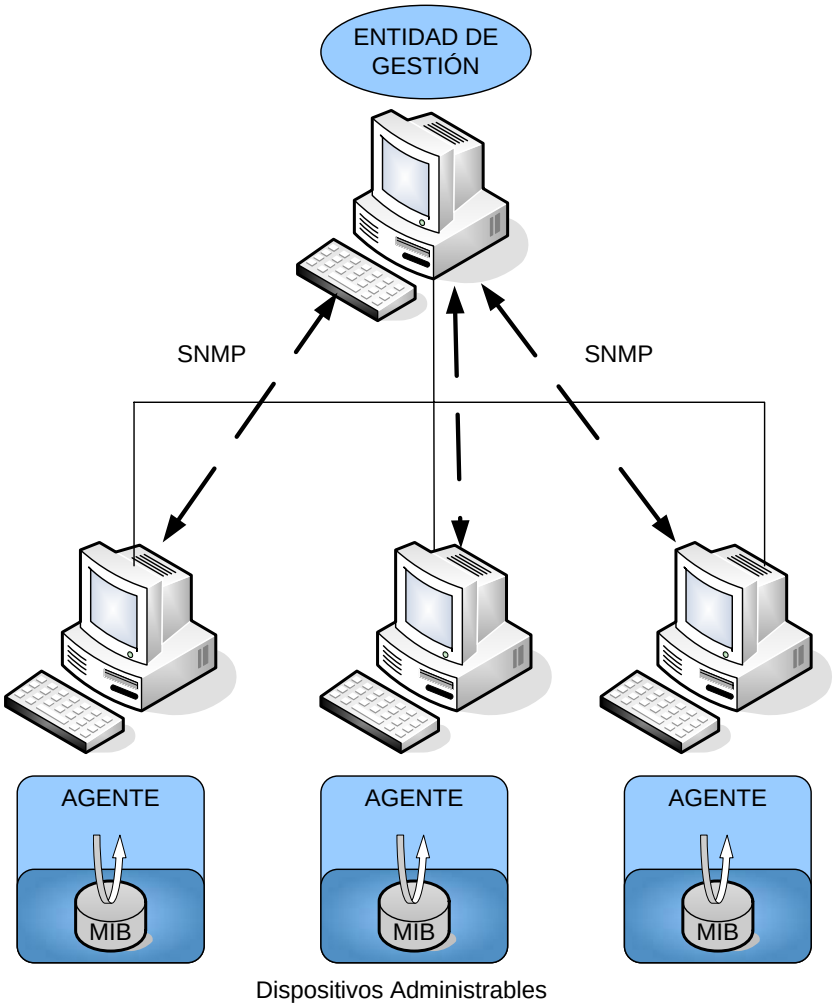


Figura 4. Componentes del esquema de gestión de red basado en SNMP

SNMP se basa en el modelo gestor / agente e involucra la estación de gestión, el agente de gestión, el protocolo de gestión y la base de información para la gestión En síntesis, SNMP es utilizado para la intercomunicación entre la estación de gestión y el agente de cada dispositivo, los cuáles son los encargados directos de mantener y mejorar el desempeño de la red enviando mensajes a los distintos dispositivos asociados a la red y modificando estructuras lógicas y parámetros necesarios para una correcta administración.

SNMP define cinco tipos de mensajes que son intercambiados entre el gestor y el agente.

1. Obtener el valor de una o más variables : `get-request`

2. Obtener la siguiente variable después de una o más variables especificadas : `get-next-request`
3. Fijar el valor de una o más variables: `set-request`
4. Retornar el valor de una o más variables: `get-response`. Este es el mensaje enviado por el agente al gestor en respuesta a los operadores `get-request`, `get-next-request`, y `set-request`.
5. Notificar al gestor cuando algo imprevisto sucede en el agente: `trap`.

Los tres primeros mensajes son enviados por el gestor hacia el agente, y los últimos dos los envía el agente hacia el gestor.

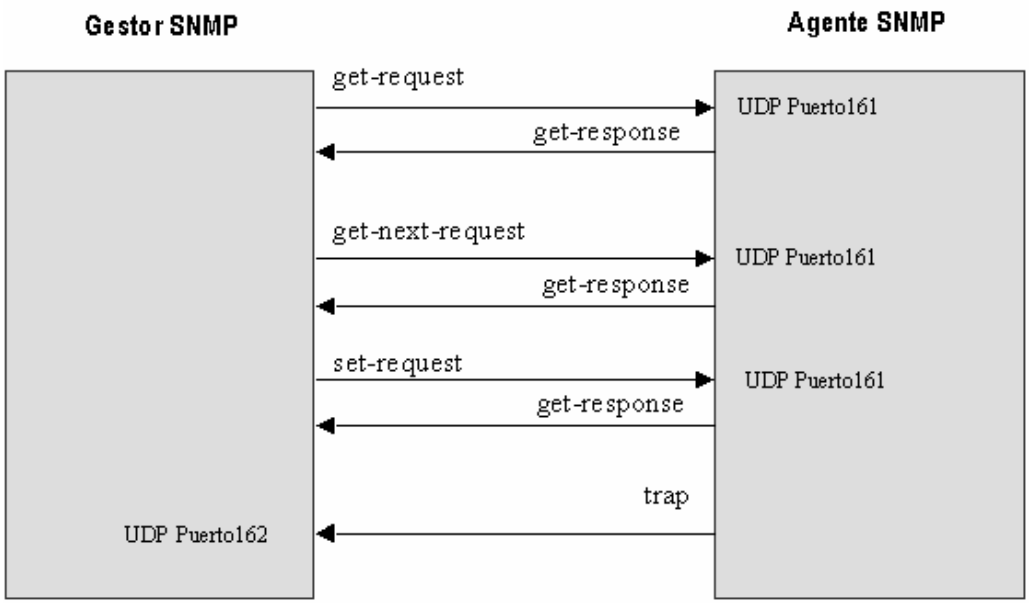


Figura 5. Resumen de los operadores SNMP

El gestor envía las peticiones empleando UDP sobre el puerto 161 mientras el agente envía los traps al puerto 162. De esta manera un mismo sistema puede fácilmente desempeñarse como gestor y como agente.

1.5 Gestión De Fallas

Como ya se mencionó anteriormente el centro de este trabajo es el área de gestión de fallas. La gestión de fallas es muy importante si tenemos en cuenta que en algunos casos los

proveedores de servicios de red pueden perder clientes si ellos no están en capacidad de prestar un servicio eficiente.

En una red que use tecnología Ethernet, un tipo de falla bastante común es la pérdida temporal o extendida de ancho de banda, denominada falla suave por algunos autores. Aunque las causas de este tipo de fallas varían, desde el punto de vista de los usuarios de la red, las fallas suaves son percibidas como una notable degradación del desempeño o un comportamiento anómalo.

En el proceso de localizar y corregir problemas en la red los pasos básicos son:

- Identificar (pasiva o activamente) un comportamiento anormal de la red
- Aislar el problema; minimizar su impacto en el resto de la red.
- Tratar de reproducirlo para poder analizarlo
- Corregir el problema

La gestión de fallas debe ser preferentemente proactiva, es decir, se debe tratar de identificar tempranamente una condición potencial de falla antes de que ésta se manifieste. La gestión activa se refiere a mecanismos de sondeo que solicitan información de los dispositivos. Debe haber un compromiso entre la precisión de la información adquirida y la cantidad de tráfico inyectado.

1.5.1. Fallas de red

En una red que usa tecnología Ethernet las fallas pueden ser congregadas en dos grandes áreas como son las fallas físicas o de estado y las fallas de desempeño. En general las fallas físicas se relacionan con la disponibilidad de conexión o al funcionamiento de los dispositivos en el segmento de red, mientras que las de desempeño se orientan generalmente a la administración del ancho de banda.

1.5.1.1 Definición de falla

En la definición de una falla de red pueden presentarse varios criterios y opiniones, sobre todo en las LAN de tecnología Ethernet. Una definición general dice que las fallas de red son aquellas condiciones bajo las cuales el servicio entregado se desvía del servicio especificado o esperado.

La gran mayoría de autores definen dos grandes tipos de fallas en una red de tecnología Ethernet: fallas severas y fallas leves[17].

Fallas Severas: Se caracterizan por la inhabilidad para entregar paquetes. Las causas posibles para una falla de este tipo son: falla de energía, un cable cortado o la falla de un equipo de red principal (Ej. un enrutador). Este tipo de fallas son las más desastrosas ya que el funcionamiento de la red se reduce a cero. La detección de estas fallas es sencilla ya que se detecta rápidamente por los usuarios o los administradores de red.

Fallas Leves: Se caracterizan por una pérdida parcial de ancho de banda. Las fallas suaves no están definidas de una forma estricta, pero la literatura generalmente las caracteriza por la degradación de desempeño o pérdida de ancho de banda de red. Las principales causas de las fallas suaves son: uso inapropiado de la red, la congestión temporal que causa retraso de transmisión, las fallas de hardware en una estación y las fallas de protocolos de nivel superior, entre otras.

Tanto las fallas suaves como las duras pueden ser asociadas con los parámetros estándar de medida desempeño como son la latencia, la tasa throughput y la confiabilidad.

1.5.1.2 Parámetros de desempeño

Algunos de los parámetros de desempeño más importantes para monitorizar en una red con tecnología Ethernet son:

- Load (carga): porcentaje del ancho de banda de red usado para la transmisión de datos.
- Packet Count (cuenta de paquetes): número de paquetes de datos por minuto que se propagan por la red.

- Collision Count (cuenta de colisiones): número de colisiones entre paquetes por minuto que ocurren en la red.
- Small Packets (paquetes pequeños): proporción de paquetes que son menores de 128 bytes.
- Large Packets (paquetes grandes): proporción de paquetes que son mayores a 1024 bytes.
- Broadcasts (difusiones): número de paquetes de difusión (broadcast) por minuto en la red.
- Source Addresses (direcciones de origen): brinda información sobre:
  - Incremento sorpresivo de la actividad de un nodo
  - Permite detectar la aparición de direcciones nuevas o ilegales
  - Caída en la actividad de la estación asociada a una dirección particular

- Destination Addresses (direcciones de destino): brinda información sobre:
  - Incremento sorpresivo de la actividad
  - Direcciones nuevas o ilegales
  - Caída en la actividad de la dirección

1.5.1.3 Tipos de fallas

Los tipos de falla más comunes en redes de tecnología Ethernet son:

- **Tormenta Broadcast (Broadcast storm).** Esta falla es causada por el envío repetitivo de mensajes de difusión (broadcast) usualmente con el fin de solicitar información o servicios. Además de perturbar el desempeño de todas las estaciones (ya que deben capturar el paquete broadcast), el desempeño de red se perturbará debido a la inundación de respuestas a la difusión (broadcast).

- **Congestión de red.** Esta falla ocurre cuando un incremento en la carga de red resulta en una disminución en la capacidad de trabajo útil de la misma. Cuando se dice que hay congestión de red, se habla de un estado en el que la demanda de tráfico es alta pero con una tasa de throughput muy pequeña, con altos niveles de pérdida de paquetes y retardos.

La congestión tiene varias causas; puede originarse en la retransmisión innecesaria de paquetes, o en los paquetes no entregados, que son transportados a través de la red, pero se descartan antes de llegar a su destino final, produciendo un gran desperdicio de ancho de banda.

Las aplicaciones se convierten en una de las principales responsables de este tipo de falla. Un mal comportamiento de los paquetes, peticiones erróneas que bloquean los recursos del sistema, aplicaciones que no manejan de forma adecuada las peticiones de los clientes o temporizadores mal establecidos, pueden originar este tipo de condiciones de falla.

También es común que se presente congestión cuando grandes incrementos en la carga ofrecida son correspondidos solamente con pequeños incrementos en el throughput de la red o incluso por una reducción del throughput existente; esta situación se presenta cuando múltiples puertos de entrada compiten por el mismo puerto de salida y saturan su ancho de banda. Si la red está congestionada, la utilización es usualmente muy alta y los paquetes son descartados debido a que la memoria intermedia del dispositivo (buffer) está saturada y las tasas de colisión son elevadas.

El problema fundamental que genera esta falla es que todos los recursos de red están limitados, incluyendo el tiempo de procesamiento del dispositivo de red (Ej. Router, Switch) y el throughput de cada enlace. Los usuarios pueden sobrecargar fácilmente ciertos recursos de red (de manera similar a un ataque de negación de servicio), inutilizando a la red a menos que se tomen las medidas necesarias para evitar esta situación.

En el esquema de protocolos TCP/IP generalmente se vigilan los errores, pérdidas o retardos de paquetes. La congestión es un aspecto muy importante, ya que es la causa de toda la pérdida de paquetes en redes conmutadas.

Adicionalmente existen otras condiciones o fallas asociadas con la generación de congestión en redes de tecnología Ethernet: la paginación de la red y el nodo murmurante.

- **Network Paging (Paginación de la red).** Se presenta al paginar o trasladar archivos o procesos muy grandes a través de la red. Produce un consumo de ancho de banda excesivo que afecta el desempeño general de la red.

- **Babbling Node (Nodo Murmurante).** Es una estación que transmite repetidamente paquetes aleatorios en la red. Esta falla es característica de una tarjeta de red defectuosa o una mala implementación de protocolo.

- **Stalled bridge (Puente Atascado).** Esta falla ocurre cuando un Bridge o Router entra en estado inactivo (down) o detiene el reenvío de paquetes en una u otra dirección. Esta falla resulta en pérdida de conexiones y de este modo reduce la actividad en todas las secciones de la red que se relacionan con el dispositivo. En este tipo de falla también se incluye la pérdida de otros componentes de red o redes desconectadas.

- **Runt flood (Inundación de Fragmentos, enanos).** Esta falla ocurre cuando una estación envía paquetes con longitud inferior al límite de 64 bytes definido por el protocolo Ethernet. La transmisión de paquetes fragmentados resulta en la pérdida de ancho de banda de red.

- **Jabbering node (Inundación de Gigantes).** Esta falla ocurre cuando una estación envía paquetes que son mayores al límite de 1518 bytes definido por el protocolo Ethernet. La transmisión de paquetes de gran tamaño resulta en una pérdida extrema de ancho de banda.

- **Fallas de hardware.** Son problemas específicos relacionados con el medio de transporte. Existen muchos tipos de fallas de hardware que pueden ocurrir en una red de tecnología Ethernet entre los que se incluyen conectores defectuosos o problemas eléctricos.

Las fallas de Hardware no son detectadas fácilmente usando los parámetros de desempeño monitorizados usualmente. Estas fallas se manifiestan generalmente en otros parámetros, como son: el espaciamiento ínter-paquetes, paquetes de error, etc.

En general la incidencia de estas fallas es muy reducida en las redes de tecnología Ethernet bien configuradas. Los problemas de Hardware y también otras fallas como los Runts y Jabbers se pueden apreciar principalmente como anomalías evidentes en gráficas de paquetes versus carga y paquetes versus colisiones.

2. SELECCIÓN Y CONFIGURACIÓN DE LA HERRAMIENTA DE GESTIÓN

Los parámetros de desempeño de una red han sido ampliamente estudiados durante años. Como resultado se han producido cientos de reportes teóricos que muestran la forma en que el tráfico de una red se ve afectado por la carga de la misma. Desafortunadamente para los administradores, en la mayoría de los casos las ecuaciones y teorías planteadas no son suficientes para resolver los problemas reales que se pueden presentar cada día en la red. Por tal razón, se requieren herramientas de gestión que permitan monitorizar y analizar el comportamiento de la red, con el fin de identificar las posibles causas de los problemas de desempeño que la pueden afectar.

2.1 Criterios de selección de la Herramienta de Gestión

Uno de los objetivos fundamentales de la gestión es mejorar el desempeño de la red, por lo tanto es muy importante tener claro qué se entiende por desempeño de una red y cómo se puede medir. La frase más odiada por los administradores de red es “la red está lenta hoy”. Qué es exactamente una red “lenta”? Quién determina cuando una red es lenta y cómo lo puede hacer? estas son algunas de las preguntas que pueden surgir al hablar de desempeño de red.

La situación sería más simple si existiera una respuesta estándar para cada una de estas preguntas, junto con un procedimiento único para resolver los problemas de una red lenta. Por ahora tendremos en cuenta que para gestionar una red adecuadamente se requiere un conjunto de actividades, reglas y procedimientos preventivos y correctivos que juntos reciben el nombre de sistema integrado de gestión.

Un sistema integrado de gestión está compuesto por cuatro elementos fundamentales que son el desarrollo tecnológico, el recurso humano, los procedimientos de trabajo y las herramientas de gestión. Cada uno de ellos juega un papel fundamental dentro de la tarea de gestión. A grandes rasgos, el desarrollo tecnológico hace referencia al tipo de dispositivos presentes en la red y al diseño de la red en general; al hablar de recurso humano se hace referencia al personal encargado de la gestión de la red, las condiciones y conocimientos requeridos para esto, las actividades asignadas y el número de personas a cargo de cada actividad; los procedimientos de trabajo son el conjunto de pasos, tareas y directrices que se deben tener en cuenta para lograr una gestión de red eficiente, estos procedimientos se deben enfocar hacia una gestión de red preventiva más que correctiva.

El último elemento presente en un sistema integrado de gestión, es la herramienta de gestión. Hay una gran variedad de herramientas disponibles en el mercado; el objetivo es encontrar la que mejor se ajuste a las necesidades de cada red en particular; por ejemplo, las herramientas de gestión de red orientadas a las medidas de desempeño pueden ayudar al administrador a determinar el estado de la red, e identificar las áreas que pueden ser mejoradas con el fin de lograr un desempeño superior.

Uno de los objetivos de este trabajo era realizar la evaluación y selección de una herramienta de gestión que se ajuste a las necesidades específicas de la red de la Universidad Industrial de Santander.

Para garantizar que la selección de la herramienta de gestión sea acertada, se deben considerar diversos aspectos durante la etapa de evaluación de la misma. A continuación se mencionan los criterios tenidos en cuenta durante esta etapa de selección.

Como criterio básico de la gestión de red tenemos que se deben conocer muy bien las condiciones de operación esperadas de la red, así como la descripción de los dispositivos asociados a ella. La funcionalidad de algunas herramientas de gestión suele estar ligada a su uso con dispositivos de ciertos fabricantes únicamente, por ello es bastante útil conocer el tipo de dispositivos con los que se cuenta y buscar una herramienta que los soporte ampliamente. Otro criterio importante es definir con claridad los parámetros o condiciones de

desempeño que se desean monitorizar y controlar, así como la información que se desea recibir como producto de estas tareas y el formato en el que se esperan los datos. En general, se deben definir claramente las tareas a realizar mediante el uso de la herramienta.

En el caso particular de la red de datos de la Universidad Industrial de Santander, las necesidades no difieren significativamente de las de la gran mayoría de las redes de este tipo; sin embargo existían algunos criterios o preferencias adicionales que marcaron la diferencia al realizar la selección definitiva.

En resumen, el proceso de selección se desarrolló como sigue:

1. Partiendo de la escasa documentación disponible de la red y con base en la información suministrada por el administrador, se hizo una rápida identificación del tipo de dispositivos presentes dentro de la red, teniendo en cuenta factores relacionados con los fabricantes y las opciones de administración ofrecidas por cada uno.
2. Analizando la misión de la organización en este caso la Universidad Industrial de Santander, se buscó identificar las condiciones de desempeño esperadas en la red, teniendo en cuenta el tipo de procedimientos y servicios de red empleados como resultado de la actividad académica, investigativa, administrativa y financiera que se debe desarrollar dentro de la universidad.
3. Se plantearon las tareas de gestión mínimas que se debían desarrollar con el fin de verificar y controlar que el desempeño obtenido fuera el esperado. A partir de estas tareas se hizo una selección previa de tres herramientas que a nivel general cumplían con los requisitos establecidos.
4. Una vez seleccionadas las herramientas a evaluar se dio inicio a este proceso. A partir de las versiones demo de cada una de las herramientas, se probaron y analizaron sus opciones y se hizo una comparación cualitativa entre ellas. Estos resultados se reflejan en la matriz de comparación presentada más adelante.

2.1.1. Criterio Económico

El administrador de una red, no sólo es el responsable de la instalación y el mantenimiento de los enlaces y dispositivos dentro de la red tales como hubs, switches, routers y firewalls entre otros, debe también asegurar que todos juntos trabajen eficientemente dentro de la red. Por supuesto, todo esto debe ser hecho dentro de los límites de un presupuesto, que por lo general es menor que lo que realmente se necesita para cumplir el trabajo. Por esto el factor costo a la hora de seleccionar los elementos empleados para cumplir con las tareas de gestión no es el único criterio pero no deja de ser un elemento de gran importancia.

El costo de una herramienta debe ser acorde con las prestaciones ofrecidas. Es evidente que también intervienen factores comerciales relacionados con la solidez de la empresa que la produce, el soporte técnico disponible o el tiempo que lleva el producto en el mercado entre otros. Todos estos aspectos se deben tener en cuenta al momento de realizar una elección de este tipo, siempre buscando el mejor compromiso entre calidad, respaldo y costo.

2.1.2. Criterio Técnico

2.1.2.1 Desempeño de la Red

El desempeño de una red es frecuentemente difícil de medir. Un alto desempeño para una aplicación puede resultar bastante bajo para otra. En ocasiones si los problemas son detectados oportunamente pueden ser resueltos simplemente con la reubicación o reconfiguración de algunos cuantos elementos sin necesidad de hacer inversiones en nuevo equipo.

Existe una gran cantidad de parámetros que pueden ser asociados al desempeño de la red y existen herramientas especializadas que permiten su medición; lo ideal es definir en cada caso particular cuáles son los parámetros de mayor importancia y seleccionar una herramienta que permita medir el mayor número posible de ellos.

La mayoría de las herramientas utilizan una combinación de los siguientes elementos para medir el desempeño de la red:

- Disponibilidad
- Tiempo de Respuesta
- Porcentaje de Utilización de la Red
- Tasa de Throughput de la Red
- Ancho de Banda

- **Disponibilidad**

Una manera simple de medir el desempeño de la red es determinando si se encuentra operativa. Una forma simple para probar la disponibilidad de la red es mediante la utilización del comando Ping. Usando Ping se pueden enviar mensajes ICMP desde una estación origen a estaciones remotas ubicadas en diversos segmentos de red para así verificar la operatividad de la red en protocolos de capa 1, 2 y 3[6].

- **Tiempo de Respuesta**

Desde el punto de vista del cliente la disponibilidad no es el único parámetro de desempeño que cuenta, puesto que a él no solo le importa si puede o no acceder al servidor sino el tiempo que tiene que esperar cada vez que hace una petición. Para obtener una idea más acertada del desempeño de la red, se toma una medida del tiempo que le toma a un paquete atravesarla. El tiempo que tarda un paquete en viajar entre un punto y otro dentro de la red, es denominado tiempo de respuesta. Dependiendo de la aplicación hay circunstancias en las que un tiempo de respuesta elevado resulta inadmisible. La gran mayoría de las herramientas utilizan el envío de mensajes de echo para calcular el tiempo de ida y vuelta desde un punto a otro (Ping Test), otro procedimiento que puede resultar útil es medir la carga dentro de las estaciones (CPU Load).

Factores que inciden en el tiempo de respuesta:

[6] Una respuesta inadecuada de ping indica la existencia de problemas en las capas física, de enlace de datos o de interred.

Existen diversos factores que pueden tener incidencia en el tiempo de respuesta entre un cliente y un servidor. Algunos de estos factores pueden ser controlados por el administrador de la red pero otros están fuera de su control. Los siguientes son algunos de los factores que pueden contribuir con un tiempo de respuesta de red lento.

- Segmentos de red sobrecargados
- Fallas de cableado
- Tormentas de Broadcast
- Falla en los dispositivos de Red
- Estaciones sobrecargadas

- **Utilización de la Red**

Un factor fundamental en el desempeño de una red es la utilización de cada segmento de red presente en el camino entre dos puntos finales. La utilización de la red representa el porcentaje de tiempo que la red está en uso sobre un periodo de tiempo dado. Para calcular la utilización de la red se toma el número de bytes que han entrado y salido de la interfaz y se dividen en la capacidad total de la interfaz en un periodo dado. Para conocer el número de bits que han atravesado la interfaz este valor debe ser multiplicado por ocho.

- **Tasa de Throughput**

La tasa de Throughput de una red es similar en concepto a la utilización. La tasa de throughput de la red se define como la tasa a la cual los datos utilizables pueden ser enviados sobre un enlace[7]. Determinar la tasa de throughput le permite al administrador de la red identificar posibles cuellos de botella que disminuyen el desempeño de un enlace entre dos estaciones. Es importante tener en cuenta, que el ancho de banda teórico se ve reducido por el uso de encabezados, sincronismos y otros aspectos, por tal razón el throughput es siempre menor al ancho de banda teórico ofrecido por la tecnología empleada. En ocasiones de nada sirve que las estaciones cliente y servidor estén conectadas a dispositivos de red de alta velocidad si estos dispositivos van a estar conectados a través de un grupo de dispositivos en algunos casos de baja velocidad. En la Figura 6 se muestra un ejemplo de esto.

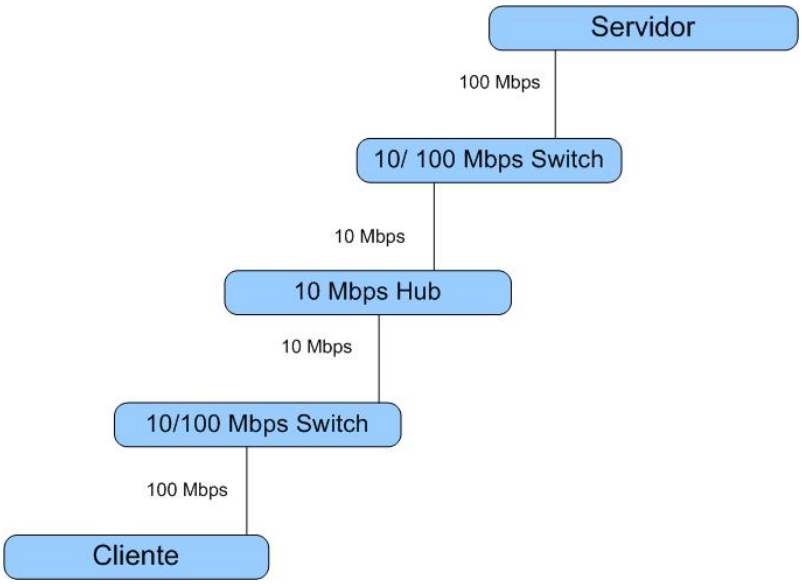


Figura 6. Cuellos de botella en un enlace

En la figura se observa que el enlace de menor ancho de banda impone un límite superior al throughput entre cliente y servidor en este caso 10 Mbps.

- **Ancho de banda**

El ancho de banda determina la tasa a la cual la información puede ser enviada por un canal de transmisión dado. Usualmente es medido en bps e indica la cantidad de información que puede ser enviada por un canal en un tiempo determinado. Por tal razón la capacidad de ancho de banda entre dos punto en la red es una medida clave del desempeño de la misma.

Teniendo en cuenta que uno de los objetivos de esta tesis era seleccionar una herramienta de gestión que se ajustara a las necesidades de la red de la Universidad, como punto de partida se identificaron algunas tareas claves que se esperaba fueran realizadas con dicha herramienta:

2.1.2.2 Tareas a realizar

La identificación de estas tareas se realizó partiendo de los conceptos generales de la gestión, teniendo en cuenta los parámetros de desempeño mencionados en la sección anterior y los intereses específicos del administrador de la red.

Las tareas identificadas son:

Administración de direcciones IP

La asignación y control del uso de las direcciones IP dentro de una red, es uno de los principales problemas a los que se enfrenta un administrador. Cuando el tamaño de la red es considerablemente grande, el garantizar que todas las estaciones que diariamente están conectadas a la red han sido oficialmente reportadas ante la entidad encargada es algo difícil de hacer. Por tal razón la necesidad de contar con una herramienta que permita de manera continua verificar cuántas y cuáles direcciones están en uso dentro de la red es más que evidente.

Descubrimiento de red

La documentación de la red es una tarea de gran importancia que requiere un gran esfuerzo, tanto para su elaboración como para su mantenimiento. Del grado de actualización de esta información y del conocimiento que se tenga sobre los dispositivos presentes en la red depende en buena parte el éxito de su administración. Se debe buscar una herramienta que ofrezca al administrador la posibilidad de conocer de manera remota el número y las características de los dispositivos presentes dentro de su red.

Gestión de desempeño

Como se mencionó anteriormente el rendimiento de la red se encuentra asociado a distintos parámetros que deben ser controlados con el fin de garantizar que el desempeño de la red es el apropiado. Las actividades básicas a realizar son: administración del ancho de banda, medición de los tiempos de respuesta, control del porcentaje de utilización y tasas de errores.

Monitorización y reporte de eventos

La herramienta de gestión debe permitir al administrador llevar un control sobre el estado de los dispositivos activos asociados a la red. Además debe ofrecer la opción de enviar reportes cuando una situación específica se presente.

2.2 Evaluación y selección de la herramienta de Gestión

2.2.1. Preselección

Teniendo como criterios de selección los aspectos mencionados en la sección anterior, se realizó una búsqueda en Internet y en distintas revistas enspecializadas en el tema con el fin de conocer las opciones disponibles. Se debe resaltar que existe en el mercado un gran surtido de herramientas asociadas con las tareas de gestión de red; el inconveniente principal es que la gran mayoría de ellas se centran en una actividad específica sin tener en cuenta las demás. En la Tabla 1 se mencionan algunas de las herramientas que fueron analizadas.

Tabla 1. Herramientas de gestión tenidas en cuenta para la selección

Nombre de la Herramienta	Software	Hardware	Fabricante	Gratuita o comercial
Network Inspector	SI	SI	FLUKE Networks	Comercial
Network View	SI	NO	NetworkView	Comercial
NetPerf	SI	NO	Hewlett-Packard	Gratuita
NetMon	SI	SI	Nullsoft	Comercial
SolarWinds Tools set	SI	NO	SolarWinds	Comercial
Network Monitor	SI	NO	ObjectPlanet	Comercial
LANsurveyor	SI	NO	NEON Software	Comercial

En este caso particular, se buscaba seleccionar una herramienta para suplir una combinación de necesidades, por tal razón a pesar de que al inicio de esta etapa se contaba con un buen número de alternativas, rápidamente al aplicar los criterios establecidos anteriormente este abanico de posibilidades se fue reduciendo significativamente.

Al finalizar esta etapa y cumpliendo con el objetivo propuesto se contó con dos herramientas que hasta el momento cumplían con los requisitos establecidos. En este punto se inicia una evaluación más detallada de las opciones ofrecidas por cada una de ellas.

2.2.2. Evaluación

Las dos herramientas seleccionadas en la etapa anterior fueron: Network View Version 3.1 y SolarWinds Network Management Toolset version 5.5. A continuación se presenta una descripción general de cada una de ellas.

2.2.2.1 Network View

Se trata de una herramienta compacta que permite realizar tareas de descubrimiento y administración empleando como plataforma el sistema operativo Windows.

Requerimientos

- Windows 2000 Professional, Server o Advanced Server, Windows XP Home o Professional, Windows Server 2003 estándar o empresarial.
- Windows NT 4.0 Server o Workstation con SP6. El servicio de Microsoft SNMP y el de WMICore 1.5 deben ser instalados también.
- Resolución 1024x768 o superior
- Windows 95, 98, ME No son soportados

Características principales

- Descubrimiento de rutas y nodos TCP/IP usando DNS, SNMP, Ports, NetBIOS y WMI (Discovery)
- Permite obtener las direcciones MAC y los nombres de los fabricantes de las tarjetas de red (NIC[7])
- Monitorización de nodos de red y reporte de eventos
- Documentación con mapas impresos y reportes
- MIB Browser y Port Scanner

2.2.2.2 SolarWinds Network Management Toolset

Se trata de un grupo de 45 herramientas que incluye opciones para la gestión de configuración, la administración del ancho de banda, la monitorización del desempeño de

[7] NIC : Network Interface Card

red, la administración de direcciones, el descubrimiento de elementos de red y la gestión de fallas. Las herramientas se encuentran clasificadas en cinco grupos. Existen diferentes ediciones o versiones del producto. Después de analizar sus prestaciones y teniendo en cuenta los criterios de selección se optó por la versión para ingenieros de esta herramienta (SolarWinds Engineers Edition)

Requerimientos

Sistema Operativo	Windows 95 / 98 / NT / 2000 / Millennium Las herramientas de SolarWinds presentan un mejor desempeño sobre Windows NT y 2000.
CPU	Pentium II 500 MHz o superior (recomendado)
Memoria	64 MB RAM (128 MB o superior (recomendado))
Espacio en Disco	Al menos 200 MB
Conexión de red	Tarjeta de Red o MODEM
Internet Explorer	Algunas herramientas SolarWinds usan Internet Explorer 5.0, por tal razón este debe estar instalado.

Características Principales

- Descubrimiento de Red (IP Network Browser)
- Monitorización de fallas (Network Monitor)
- Gestión del desempeño (Network Performance Monitor)
- MIB Browser
- Monitorización del Ancho de banda (Bandwidth Monitor)
- Seguridad (Security Check)
- Herramientas de Gestión de enrutadores Cisco.

La Base de datos del MIB Browser contiene más de 220,000 OIDs compilados a partir de miles de bases de información de gestión (MIB) entre estándar y propietarias.

Teniendo en cuenta que a nivel general las dos herramientas brindan características similares, se hizo necesario profundizar un poco en cada una de ellas y revisar los servicios adicionales que ofrecen. A partir de las versiones demo de cada una de las herramientas se realizó una evaluación más detallada de sus opciones con el fin de tener claros criterios de selección. Los resultados de esta evaluación se presentan en la siguiente matriz de comparación donde se registraron los aspectos analizados.

Tabla 2. Matriz de comparación Herramientas de Gestión

Matriz de Comparación	SolarWinds	NetworkView
CPU Load	✓	
Calculadora IP	✓	
Medidor de ancho de banda	✓	
Auditoria DNS	✓	✓
Ping	✓	✓
Administrador de direcciones IP	✓	
Descubrimiento de Red	✓	✓
Descubrimiento de direcciones MAC	✓	✓
MIB Browser	✓	✓
Monitorización de Red (SNMP)	✓	
Monitorización de Red (ICMP)	✓	✓
Proxy Ping	✓	
Router CPU Load	✓	
Seguridad	✓	
SNMP Grafico	✓	
Barrido SNMP	✓	
Generación de listas de Subredes	✓	

Mapeo de puertos de un switch	✔	
Escaneo de puertos[8]		✔
Trace Route	✔	✔
Actualización de MIBs	✔	✔
Wake-On-Lan	✔	
Generador de Tráfico	✔	
Totales	**22**	**9**

A partir de los resultados presentados en la tabla anterior, se pueden comparar cuantitativamente las dos herramientas. De allí se observa que el grupo de herramientas ofrecido por SolarWinds tiene mayores prestaciones y un número significativo de servicios adicionales respecto a Network View. Teniendo en cuenta que las dos herramientas satisfacen los requerimientos básicos, que la diferencia de precio no es significativa y se ajusta al presupuesto y que las prestaciones adicionales de SolarWinds son superiores, se recomendó la adquisición de ésta última como herramienta de gestión para la red de datos institucional.

2.2.3. Descripción General de la Herramienta de Gestión SolarWinds Engineers Edition

En esta sección se presentará una revisión general de las principales opciones ofrecidas por la herramienta seleccionada; en el anexo A se presenta una Guía de Usuario que fue elaborada como parte de este trabajo, donde se describe la función de cada herramienta. Teniendo en cuenta que el centro de este trabajo está orientado al área de gestión de fallas, se profundizará en aquellas herramientas y procedimientos que deben ser usados en labores de monitorización y reporte de eventos.

2.2.3.1 Herramientas de descubrimiento de Red (Network Discovety Tools)

Las herramientas disponibles en este grupo cuentan con una de las más rápidas y robustas ingenierías de desarrollo en materia de descubrimiento de dispositivos de red. Estas

[8] Disponible en la versión 7 de SolarWinds

herramientas tienen la capacidad de descubrir y documentar un único dispositivo o una red completa. IP Network Browser y Network Sonar son las herramientas de descubrimiento más populares. Cuenta además con una herramienta de auto descubrimiento de puertos tanto en switches capa 2 como capa 3 (Switch Port Mapper). Otras herramientas de descubrimiento incluidas en SolarWinds Engineer Edition son: MAC Address Discovery que proporciona una lista de las direcciones MAC de todas las estaciones conectadas a un switch. Subnet List a partir de la información contenida en la tabla de rutas de un enrutador dentro de la red, entrega una lista de las distintas subredes asociadas a la misma. SNMP Sweep realiza un barrido de un rango de direcciones e indica cuales de ellas se encuentran en uso y DNS Audit permite escanear un rango determinado de direcciones IP en busca de errores en la resolución de direcciones IP a partir de los nombres de dominio o viceversa.

2.2.3.2 Herramientas de diagnostico (Ping Tools)

Dentro del grupo de herramientas de Solarwinds Engineers Edition se incluyen varias utilidades que contribuyen con la administración diaria de la red. Algunas de las herramientas incluidas son: Ping, es una herramienta que permite crear un registro de los tiempos de respuesta de una estación a partir del envío de peticiones simples del comando ping; Ping Sweep es una herramienta que permite escanear un rango de direcciones IP y mostrar cuales direcciones dentro de ese rango están en uso y cuales no; Enhanced Ping permite monitorizar continuamente un cierto número de servidores, enrutadores, PCs, etc, y mostrar los tiempos de respuesta en tiempo real. Trace Route permite rápidamente trazar una ruta desde la estación actual hacia cualquier dispositivo en la red y Proxy Ping que realiza un Ping Test desde un enrutador cisco remoto hasta cualquier otro dispositivo SNMP.

2.2.3.3 Herramientas de seguridad (Security Tools)

SolarWinds ofrece un grupo de avanzadas herramientas de seguridad que permiten entre otras actividades probar la seguridad de los dispositivos de red empleando utilidades como SNMP Brute Force Attack que puede determinar remotamente la secuencia de caracteres de una comunidad SNMP de solo lectura o de lectura/escritura, probando todas las posibles combinaciones de letras y números, y Dictionary Attack que le permite al administrador saber si la secuencia de caracteres elegida como comunidad SNMP es segura. Remote

TCP Reset visualiza todas las sesiones activas sobre un dispositivo remoto y Password Decryption intenta descifrar el password de acceso a los enrutadores Cisco.

2.2.3.4 Herramientas de Administración de direcciones IP (IP Address Management Tools)

Dentro del grupo de herramientas ofrecido por SolarWinds se incluye un amplio surtido de utilidades que facilitan la administración de direcciones IP dentro de una red. SolarWinds facilita la documentación del espacio de direcciones de una red. Dentro de las utilidades incluidas se encuentran: IP Address Management permite saber cuales direcciones se encuentran en uso, cuales disponibles o reservadas. DHCP Scope Monitor permite la monitorización sobre los servidores DHCP del rango de direcciones disponible para ser asignadas además del porcentaje de aprovechamiento de las mismas. Advanced Subnet Calculator útil para tareas de diseño permite cálculos de direcciones IP y mascaras de red. DNS / WhoIs Resolver proporciona información relacionada con el mapeo de nombres de dominio a direcciones IP y viceversa, además de alguna información relacionada con la red del host y el servidor DNS encargado de ese dominio. DNS Audit permite escanear un rango de direcciones para saber cuales se encuentran en uso.

2.2.3.5 Herramientas Misceláneas (Miscelaneus Tools)

Un par de herramientas incluidas dentro de SolarWinds Engineer's Edition Toolset no se pueden clasificar dentro de ninguna categoría específica y han sido llamadas misceláneas. Se trata de un servidor TFTP útil para la actualización o instalación del IOS a nivel de dispositivos de red y un potente generador de tráfico llamado WAN Killer.

2.2.3.6 Herramientas para revisión de la MIB (MIB Browser Tools)

Además del vasto surtido de herramientas para la gestión básica de la red, SolarWinds incluye un poderoso MIB Browser con más de 220,000 OIDs previamente compilados. Con ayuda de esta herramienta se pueden enviar peticiones a dispositivos de red remotos y obtener su configuración a través del protocolo SNMP. Con ayuda de la herramienta MIB Walk se puede hacer un recorrido por cada uno de los nodos dentro del árbol de la MIB. La herramienta Update System MIBs permite modificar remotamente los valores de la MIB de un dispositivo remoto.

2.2.3.7 Gestión del desempeño de Red (Network Performance Management Tools)

El tamaño de la red o el número de dispositivos que se pueden monitorizar con una herramienta de gestión es en algunos casos una limitante, este grupo de herramientas de gestión del desempeño disponible en SolarWinds, permite controlar el desempeño de la red sin importar el tamaño de la misma. La herramienta Network Performance Monitor puede monitorizar y enviar reportes de aspectos relacionados con disponibilidad, utilización del ancho de banda, carga de un procesador, utilización de la memoria o espacio en un disco. Permite el envío de reportes o alarmas cuando un umbral de desempeño es alcanzado. Dentro de este grupo también se incluye la herramienta SNMP Graph, la cual permite monitorizar cualquier dispositivo de red administrable siempre y cuando tenga habilitado el protocolo SNMP. También cuenta con una herramienta de monitoreo en tiempo real (Network Monitor) con la cual se pueden manejar estadísticas para varios switches y enrutadores simultáneamente. Por último la utilidad CPU gauge muestra el desempeño del procesador para un switch, servidor o enrutador.

2.2.3.8 Herramientas de Monitorización de fallas (Monitoring Tools)

El monitor de red es una aplicación de administración altamente interactiva que permite la monitorización continua de los dispositivos de red y el envío de alarmas cuando una condición anómala se presenta.

2.3 Gestión de fallas con SolarWinds Engineers Edition Toolset

Como ya se mencionó anteriormente, uno de los objetivos de este trabajo de investigación era la configuración o puesta en marcha de las opciones disponibles dentro de la herramienta seleccionada. La atención se centra en la configuración de las herramientas de gestión de fallas y gestión de desempeño disponibles en SolarWinds.

2.3.1. Network Performance Monitor (Monitorización del desempeño de la Red)

Es una herramienta que permite monitorizar el tráfico y la utilización, de cientos de interfaces en el mismo instante. Permite la notificación en tiempo real vía e-mail o beeper cuando una condición de alarma es detectada. Estas condiciones de alarma pueden estar relacionadas

con el cambio de estado de un enrutador, fallas en un servidor, interfaces deshabilitadas o fuera de servicio, etc.

Network Performance Monitor puede monitorizar y recolectar estadísticas de tráfico de cualquier dispositivo que soporte SNMP. La latencia y el número de paquetes perdidos por un dispositivo pueden ser monitorizados aún cuando este no soporte SNMP. Además, permite la monitorización del ancho de banda lo cual facilita la ubicación de los cuellos de botella dentro de la red. Permite la configuración de alarmas asociadas con más de 150 condiciones de la red. Algunas de las condiciones que pueden ser asociadas a una alarma son errores en las interfaces, errores recibidos o transmitidos por hora, por día o por meses por una determinada interfaz, tamaño promedio de paquete recibido o transmitido, bits recibidos por segundo, estado de una interfaz entre otras.

2.3.1.1 Configuración de la herramienta

En la barra de herramientas de SolarWinds se debe seleccionar el grupo correspondiente a Network Performance Management, una vez allí seleccione la utilidad Network Perfomance Monitor. Debe aparecer una ventana como la que se muestra en la Figura 7.

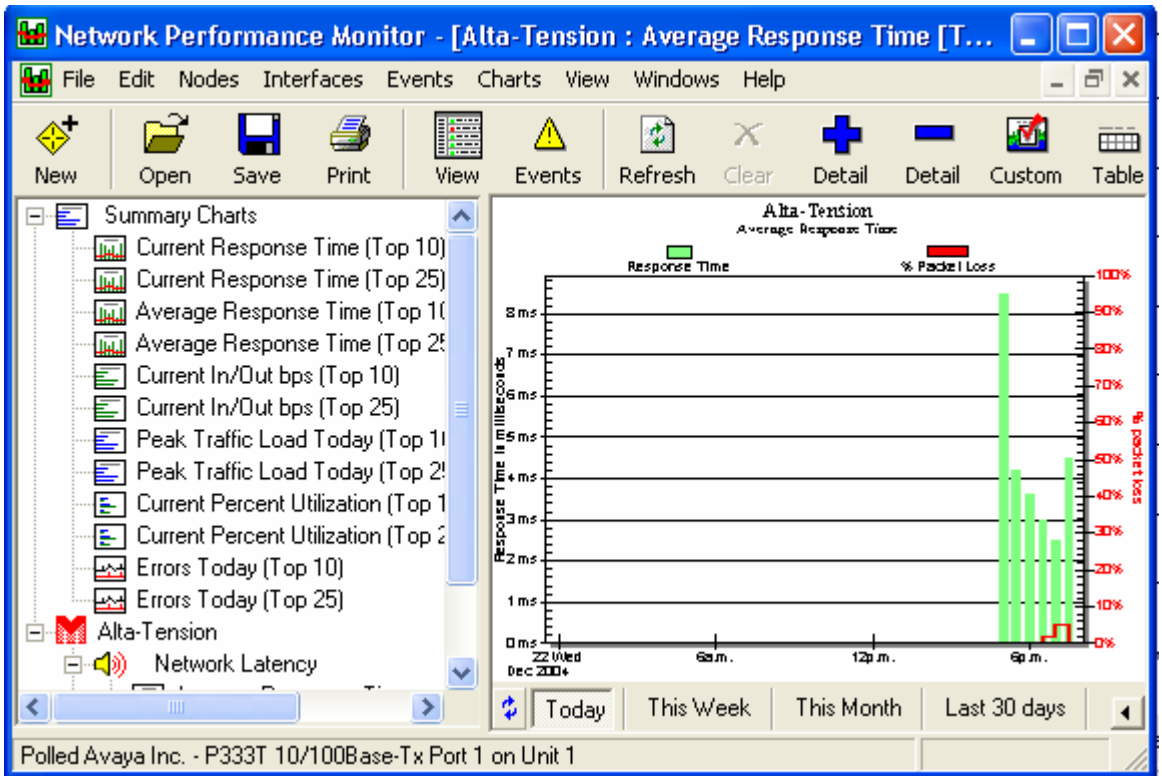


Figura 7. Network Performance Monitor

Para iniciar la configuración simplemente seleccione el icono **"New"** en la barra de tareas o selecciones la opción **"Add Interface"** en el menú de **"Interfaces".**

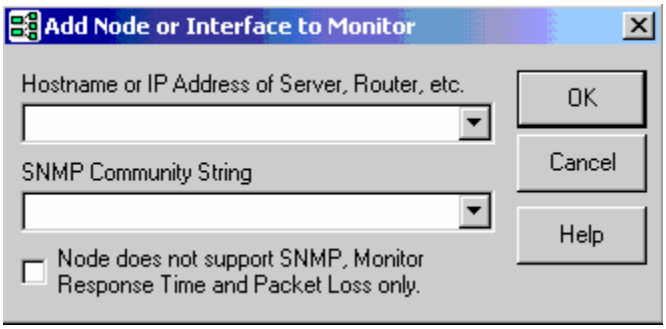


Figura 8. Adición de Nodos

Network Performance Monitor usa el protocolo SNMP para la recolección de estadísticas. Si se desea monitorizar las interfaces o tomar estadísticas de un dispositivo de red, se debe suministrar la comunidad SNMP del dispositivo. Si solamente se quiere monitorizar el tiempo de respuesta o el número de paquetes perdidos, esta información no es necesaria.

Una vez se realiza la adición del nodo, Network Performance Monitor realiza un descubrimiento de las interfaces del dispositivo como se muestra en la siguiente figura.

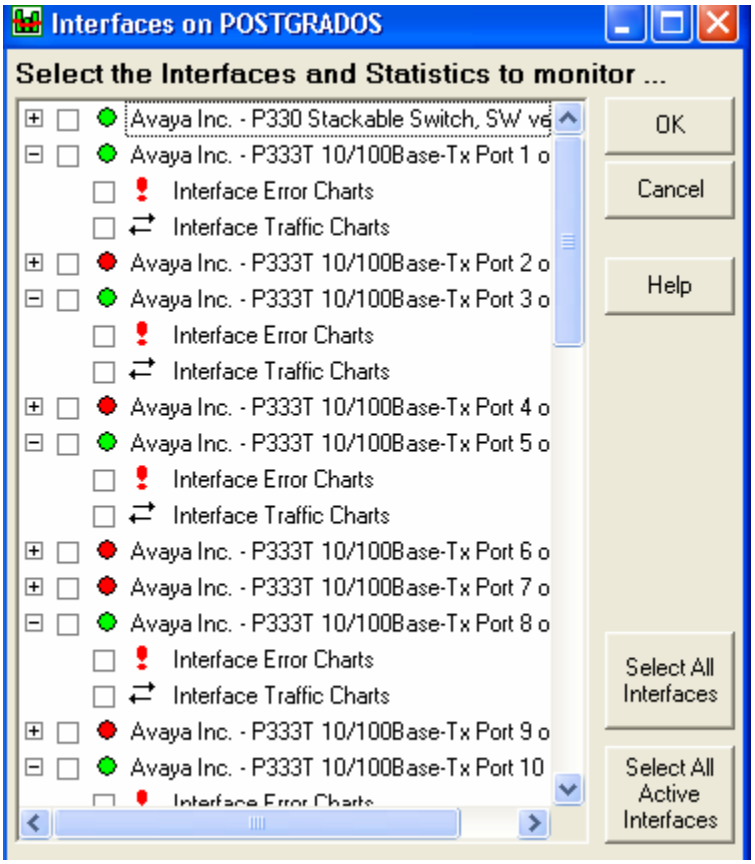


Figura 9. Listado de interfaces del dispositivo adicionado

Simplemente se deben seleccionar las interfaces y los aspectos de la interfaz que se desean monitorizar, como por ejemplo, las características de tráfico de la interfaz **"Interface Traffic Charts"** o los errores **"Interface Error Charts".** Si no se seleccionan estos valores solo se monitoriza el estado de la interfaz pero no se obtienen estadísticas.

2.3.1.1.1 Configuración de opciones

Al seleccionar la opción **"Network Performance Monitor Settings"** en el menú archivo se despliega el cuadro de diálogo presentado en la Figura 10. Dentro de las opciones a configurar se encuentran: tamaño y características de la base de datos, opciones de

sondeo como: intervalos de muestreo de interfaces y recolección de estadísticas; opciones para la presentación de los datos (tipo de letra, color entre otros); opciones de ICMP y SNMP; umbrales de alarmas e iconos desplegados cuando se presenta cada una de ellas.

- **Database (Base de Datos)**
    - **Nightly Database Maintenance**

Network Performance Monitor realiza un mantenimiento de las estadísticas recolectadas. Las estadísticas con resumidas en estadísticas por hora y estas a su vez en estadísticas por día. La hora para hacer este mantenimiento puede ser cualquier hora durante el día, procurando que sea la hora de menos tráfico pero no es requisito fundamental.

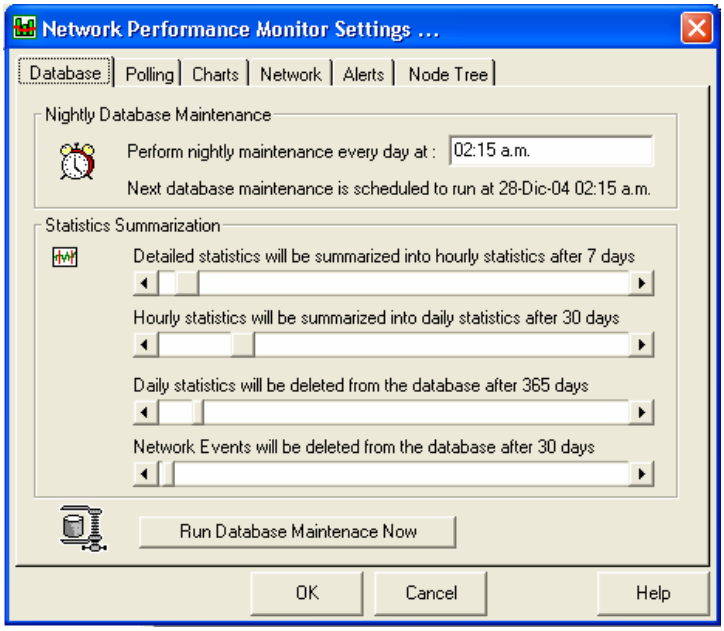


Figura 10. Configuración de opciones de base de datos

- **Statistical Summarization (Resumen de estadisticas)**

Esta opción permite definir el tiempo que los datos van a ser almacenados y el período en días en el que se debe realizar el resumen de estadísticas.

- **Polling (Sondeo)**

Esta opción permite definir el intervalo de sondeo que va a ser empleado con cada objeto monitorizado. Se debe procurar que este intervalo no sea demasiado alto como para que se pierda información o no se pueda reaccionar rápidamente ante un evento, pero a la vez se debe tener cuidado de no generar demasiado tráfico con esta actividad.

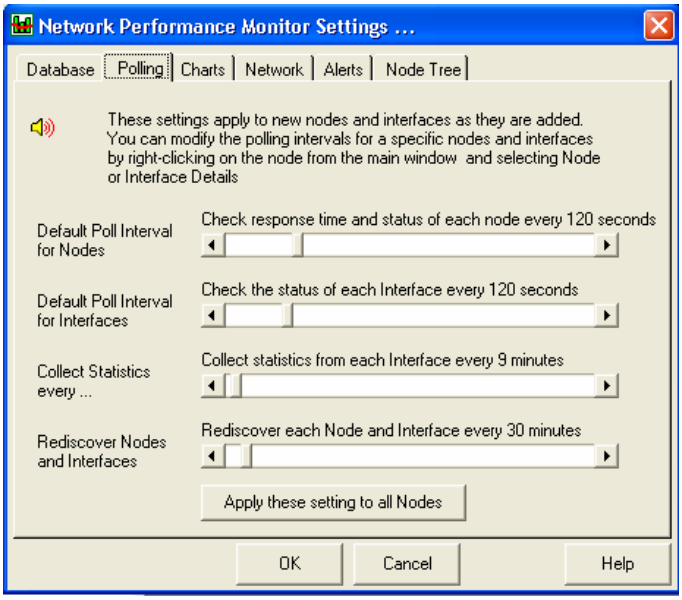


Figura 11. Configuración de opciones de sondeo

- **Network (Opciones de Red)**

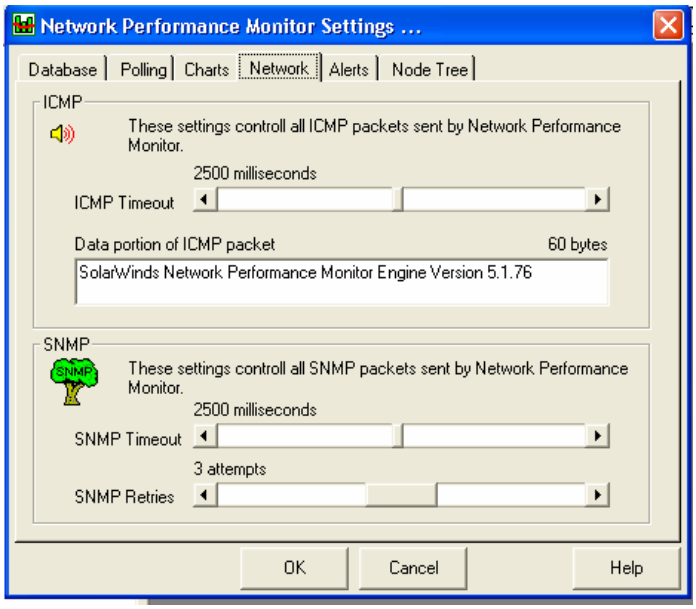


Figura 12. Configuración de opciones ICMP y SNMP

En este punto se definen las opciones de operación asociadas a los protocolos ICMP y SNMP. Tales opciones son el timeout o tiempo que se debe esperar por una respuesta, el número de intentos que se debe hacer y en el caso del protocolo ICMP el tamaño del paquete.

- **Alerts (alarmas)**

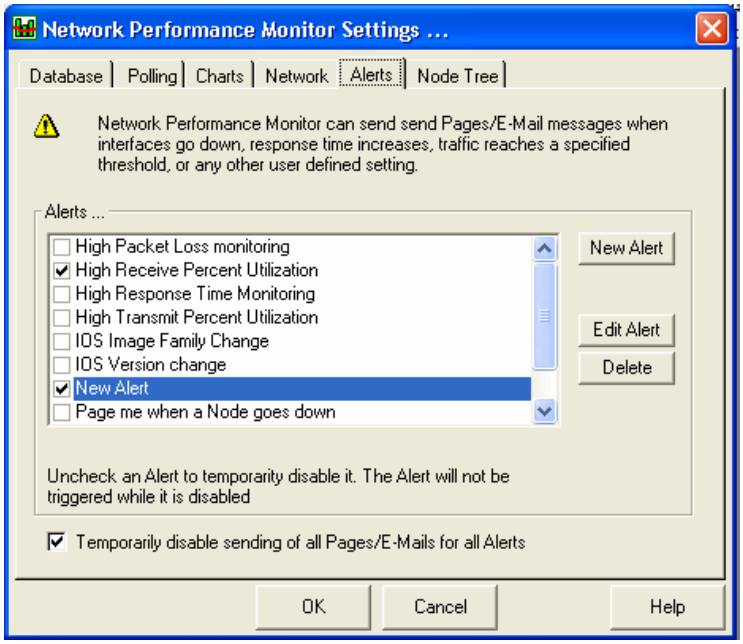


Figura 13. Configuración de alarmas

Una vez configuradas las alarmas, Network Performance Monitor puede enviar mensajes de correo electrónico reportando cualquier evento relacionado con distintas condiciones de la red (tiempo de respuesta, estado de las interfaces, porcentaje de utilización, umbrales de tráfico, etc.).

La tabla de alarmas le permite al usuario habilitar las alarmas predefinidas o crear unas nuevas. Para habilitar una alarma ya existente, simplemente hay que seleccionar la casilla a la izquierda.

Las alarmas predefinidas pueden ser modificadas seleccionándola y hacienda clic en el botón **"Edit Alert".**

- **Creación de alarmas de red**

Para crear o editar Alarmas, se debe seleccionar "**Network Performance Monitor Settings**" desde el menú "**File**". En la pestaña "**Alert**" se pueden crear nuevas o editar alarmas ya existentes.

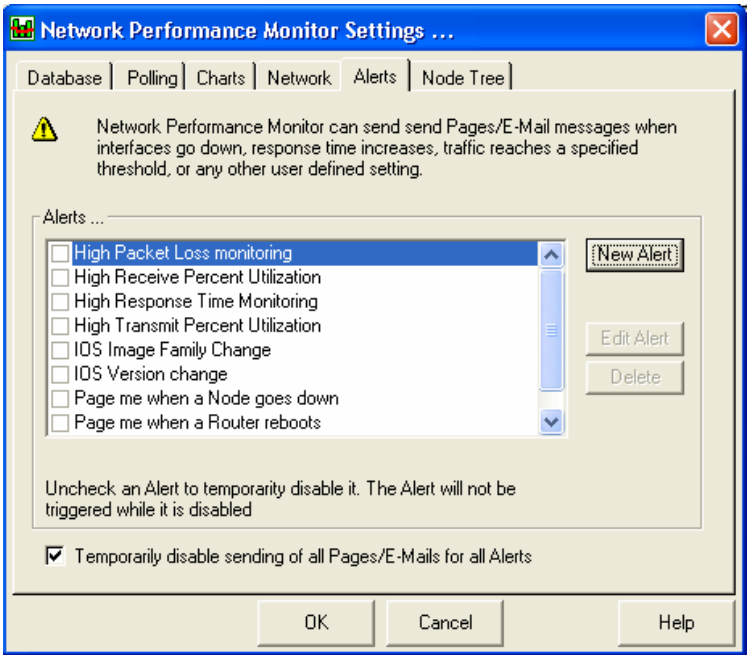


Figura 14. Creación y edición de alarmas

Las alarmas son condiciones definidas por los usuarios ante las cuales se debe enviar un mensaje de correo electrónico o un reporte mediante una Pagina Web cuando se presenta algún evento especial en la operación de la red. Una alarma puede ser creada para activarse cuando se presente un problema de latencia, un alto porcentaje de utilización sobre una interfaz, un cambio en el estado de una interfaz, una tasa de errores anormal entre otras condiciones asociadas al estado de la red.

Al hacer clic sobre las opciones **"Edit Alert"** o **"New Alert"** se presentará el cuadro de diálogo asociado con los detalles de la alarma.

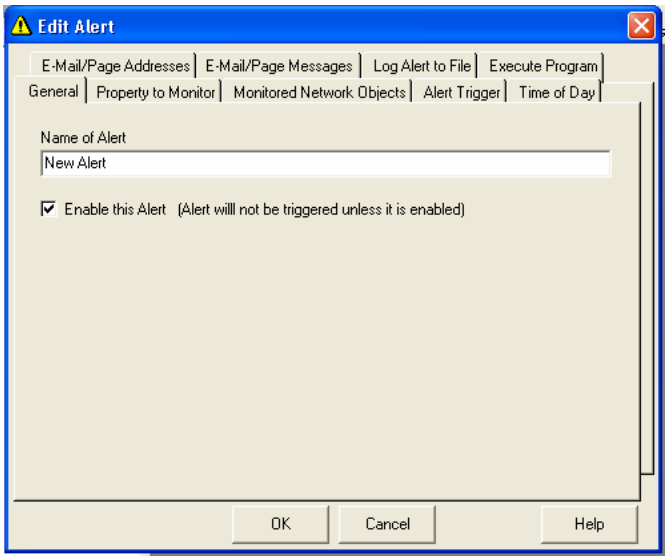


Figura 15. Definición de alarmas

General: En esta opción se define el nombre de la alarma y se habilita. La alarma no se activará si la casilla **"Enable"** no está seleccionada.

Property to monitor (Condiciones a Monitorizar): Esta pestaña permite seleccionar la condición que se desea monitorizar con la alarma. Sólo se puede asociar una condición a cada alarma. Si se desea monitorizar múltiples condiciones, se debe crear una alarma para cada una.

Para visualizar la descripción de cada condición solo es necesario seleccionarla.

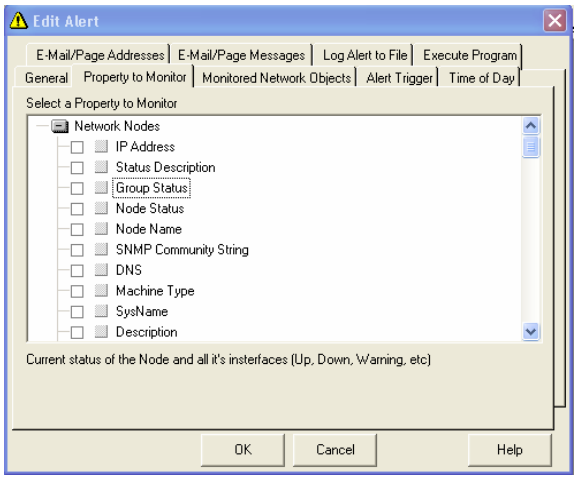


Figura 16. Condiciones a Monitorizar

Monitored Network Object (Objetos de Red Monitorizados): El usuario puede seleccionar uno o más dispositivos de red a los cuales se les puede aplicar la alarma.

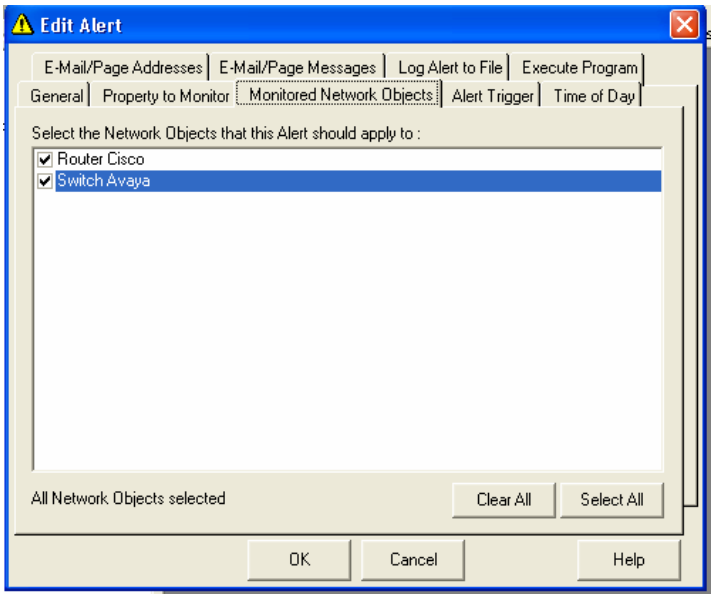


Figura 17. Objetos de red Monitorizados

Alert Trigger (Activación de Alarmas): las opciones de activación de la alarma pueden cambiar dependiendo de la condición que se quiera monitorizar. Se deben ajustar las características de disparo y restauración (reset) de la alarma.

Se puede enviar un mensaje de restauración cuando la condición de desactivación es encontrada. Dicho mensaje sólo puede ser enviado si la alarma ya fue disparada.

También se puede configurar la herramienta para que no envíe mensajes de reset, desactivando la opción mensajes de reset de la pestaña "**E-Mail/Page Messages**".

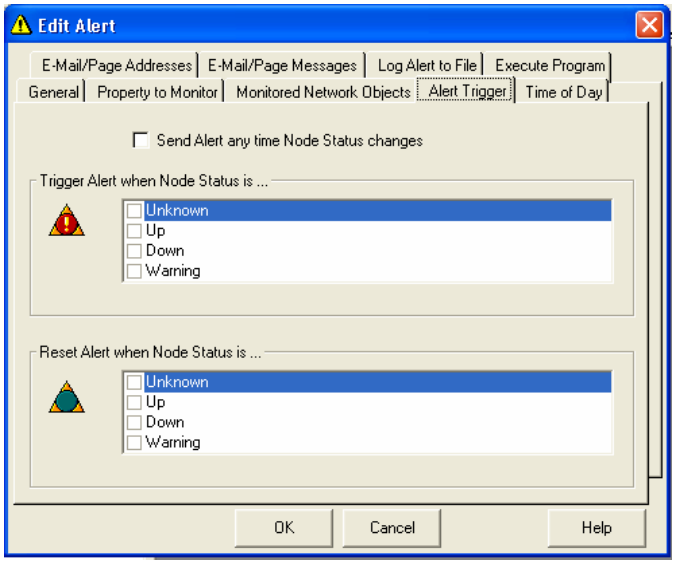


Figura 18. Disparo de alarmas

Time of Day (Hora de envío de alarmas): Network Performance Monitor puede ser configurada para que envíe alarmas solo durante ciertas horas.

Por ejemplo: se puede crear una alarma que monitorice el estado de las interfaces sobre un grupo de servidores Web los sábados y los domingos. Cuando una de las interfaces salga de operación (down), Network Performance Monitor enviará un mensaje de correo o un mensaje a un beeper. Marcando la pestaña **"Time of Day"** el usuario puede especificar el día la semana y la hora en las que la alarma debe ser activada.

Sugerencia: Para enviar las alarmas a una persona durante el día y a otra persona diferente durante la noche o los fines de semana, simplemente hay que crear dos alarmas con diferentes **“Time of Day”.**

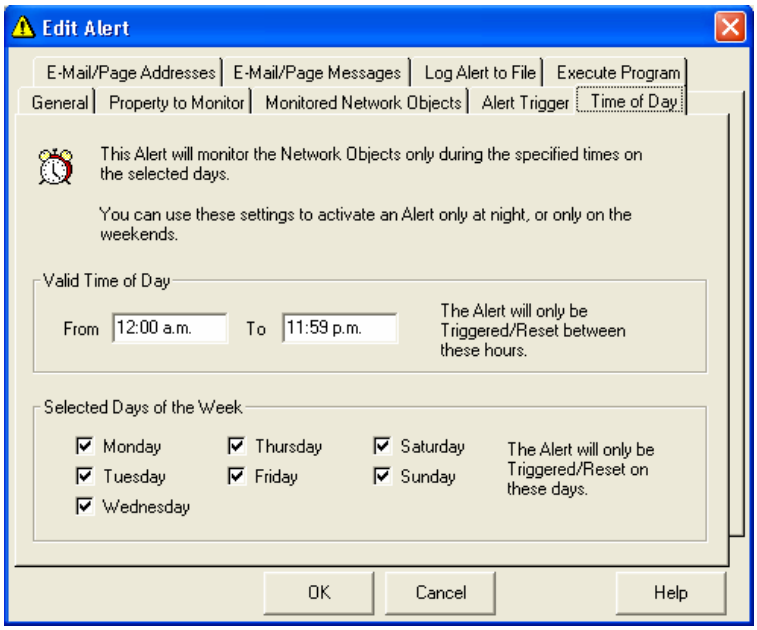


Figura 19. Hora de envío de alarmas

Pager / E-Mail Addresses (Direcciones de correo electrónico)

Aquí es donde se especifican las direcciones de correo a donde se deben enviar las alarmas. Se pueden ingresar múltiples direcciones de correo simplemente separándolas con coma o punto y coma.

Para crear alarmas que no sólo dejen el registro en la ventana de detalles de eventos, sin enviar ningún reporte por correo, simplemente se deja este espacio en blanco.

From E-Mail Account (Cuenta de Correo origen)

Todos los mensajes de correo o beepers generados por Network Performance Monitor tendrán esta cuenta de correo como dirección de respuesta.

SMTP Gateway

Se debe especificar la dirección o el nombre de dominio del servidor SMTP, para que los mensajes de alarma puedan ser generados.

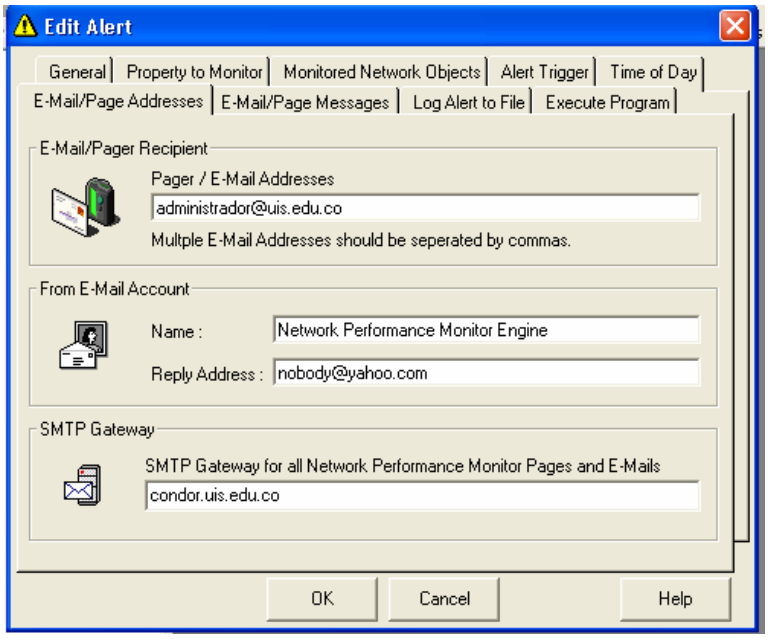


Figura 20. Configuración de direcciones

Solución de problemas: Si se tienen problemas para enviar los mensajes, el primer paso es probar la conexión con el servidor SMTP, esto se puede hacer manualmente corriendo el programa "E-Mail-Notification.exe". Este programa esta instalado en el Directorio SolarWinds (normalmente C:\ProgramFiles\SolarWinds\Common). Al ejecutar el programa aparece una ventana como la que se muestra a continuación.

Figura 21. Prueba de conexión servidor SMTP

Se debe indicar la dirección IP de servidor, indicar el número de intentos de conexión que se deben realizar, y ofrece las opciones de registro de fallas de conexión y visualización del estado del servidor siempre que se esté enviando un mensaje.

Log Alert to a File (Registrar alarmas en un archivo)

Esta característica permite registrar las alarmas en un archivo de texto para su posterior revisión y análisis.

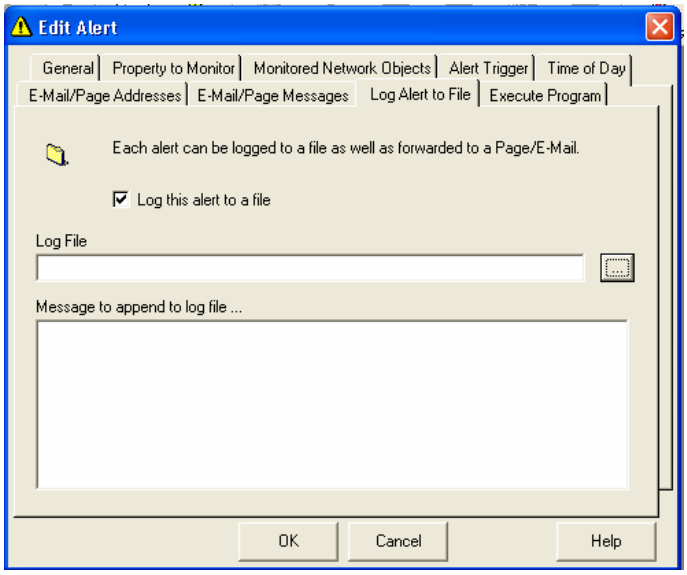


Figura 22. Registro de alarmas en un archivo de Texto

2.3.2. Network Monitor (Monitor de Red)

El monitor de Red de SolarWinds permite monitorizar cientos de dispositivos y tomar registros de tiempos de respuesta y porcentaje de paquetes perdidos. Esta herramienta también puede ser configurada para enviar un mensaje de correo electrónico cuando un dispositivo deje de responder.

Si se necesita monitorizar el volumen de tráfico en una interfaz o los porcentajes de errores, esta herramienta no es la indicada. En tal caso se debe usar la herramienta Network Performance Monitor descrita en el numeral anterior.

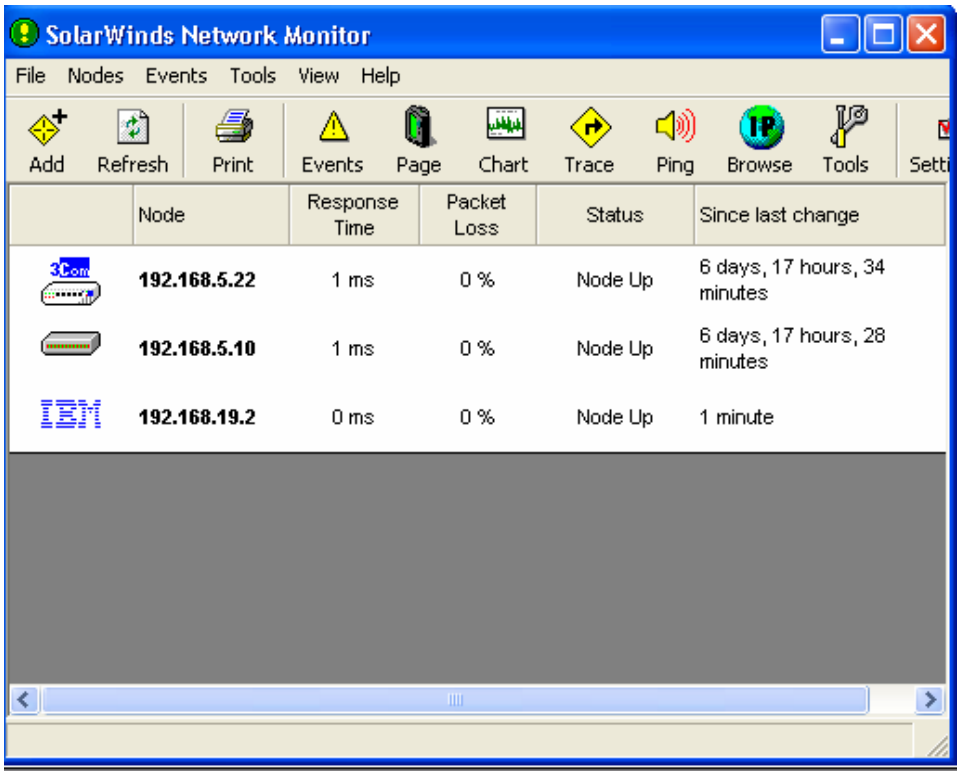


Figura 23. Network Monitor

Haciendo clic en el botón **"Add"** de la barra de tareas se ingresan los dispositivos a monitorizar; también es posible importar una lista de dispositivos.

2.3.2.1 Opciones de configuración de la herramienta

Network Monitor Settings

Al seleccionar **"Settings ..."** del menú **"File"** desde la ventana principal de la herramienta se presenta el cuadro de dialogo de Network Monitor Settings el cual presenta las siguientes alternativas en diferentes pestañas.

Event Notification (Notificación de eventos)

En esta pestaña se deben definir tres aspectos en particular, el primero es indicar la dirección o direcciones de correo o números de beeper a donde serán enviados los reportes.

En segundo lugar se deben suministrar las especificaciones de la cuenta origen del mensaje y por último se especifica el tipo de eventos que se desea reportar.

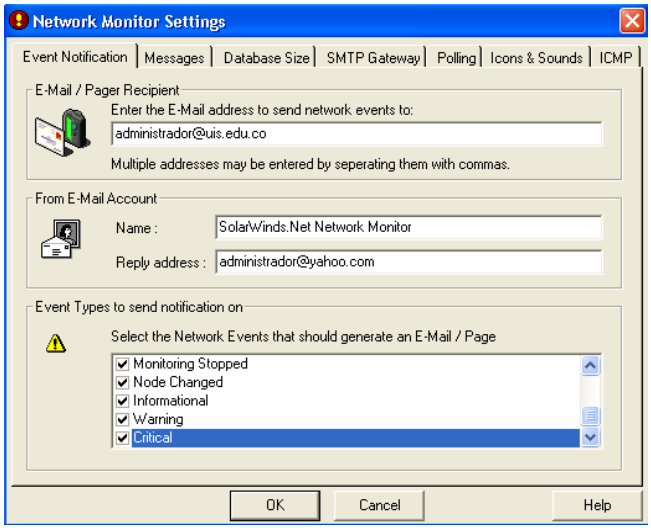


Figura 24. Notificación de eventos

Messages (Mensajes)

Personalización de mensajes

Network Monitor le permite al usuario personalizar los mensajes a enviar dependiendo de la condición que se quiera reportar.

Database Size

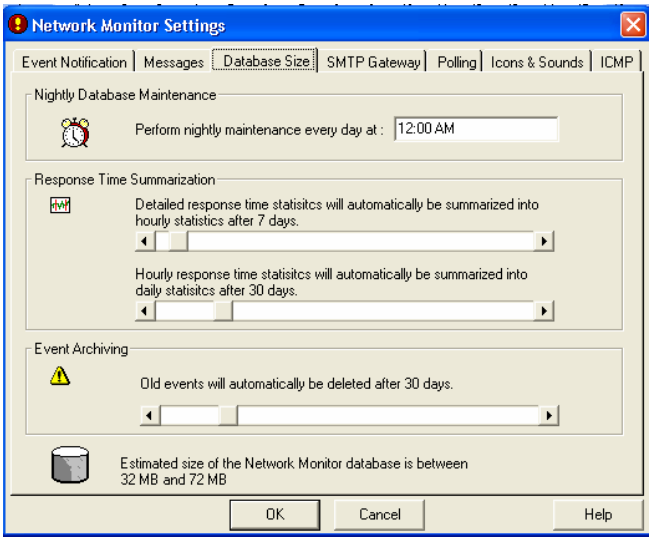


Figura 25. Opciones de base de datos

La configuración de las opciones para el mantenimiento de la base de datos es un punto fundamental. Durante el mantenimiento de la base de datos Network Monitor realiza las siguientes actividades:

- Resume los resultados obtenidos con relación a los tiempos de respuesta y paquetes perdidos y los organiza en estadísticas por hora o por día.
- Resume las estadísticas horarias en estadísticas diarias.
- Elimina eventos antiguos
- Elimina la información que no se esta usando.

Se deben definir aspectos como la hora a la que se debe realizar este mantenimiento, cada cuando se debe hacer el resumen de las estadísticas o cuanto tiempo se almacena un registro antes de eliminarlo.

SMTP Gateway

Para que Network Monitor pueda generar los mensajes de reporte de eventos, debe tener configurado un servidor SMTP. Se debe indicar la dirección IP o el nombre de dominio del servidor y el número de intentos que se deben hacer para el envío de un mensaje. En caso de tener problemas se debe hacer la prueba de conexión con el servidor como se indicó en la sección anterior.

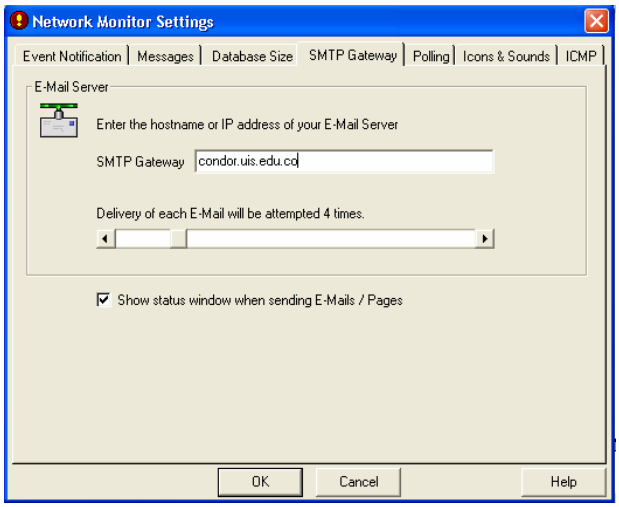


Figura 26. SMTP Gateway

Polling (Sondeo)

El intervalo de sondeo especifica con que frecuencia Network Monitor debe tomar el tiempo de respuesta y las estadísticas de paquetes perdidos de cada nodo.

Icons & Sounds

Permite seleccionar los iconos que van a ser asociados a cada nodo y los sonidos que serán emitidos cada vez que se presente un evento en un nodo.

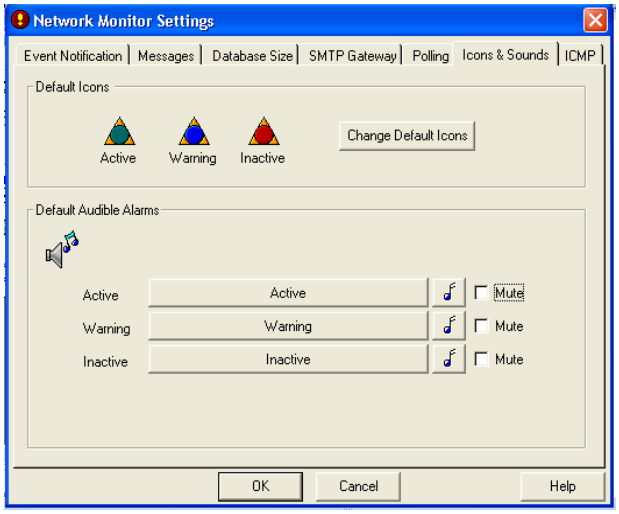


Figura 27. Iconos y sonidos

ICMP

Se define el tiempo de vida y el tamaño de cada paquete ICMP**.**

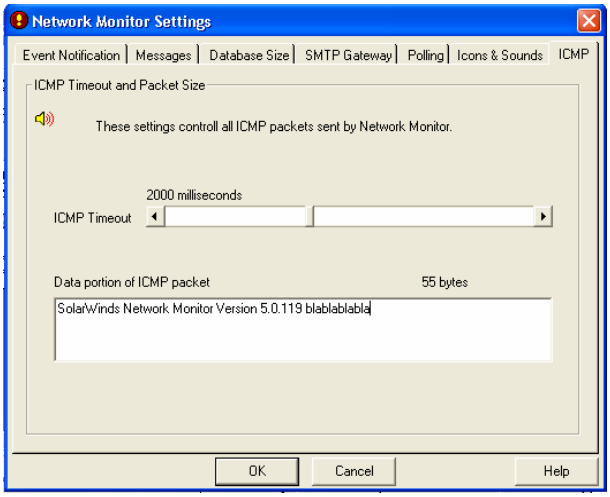


Figura 28. ICMP

Adición manual de un evento al registro de eventos

La ventana de detalles de los eventos muestra los eventos activos actualmente. Tan pronto como un nuevo evento aparece, se agrega a la ventana de eventos. Cuando un evento es eliminado, automáticamente se remueve de la ventana de eventos. Para visualizar la ventana de detalles de los eventos seleccione "**Event Details ...**" del menu "**Events**".

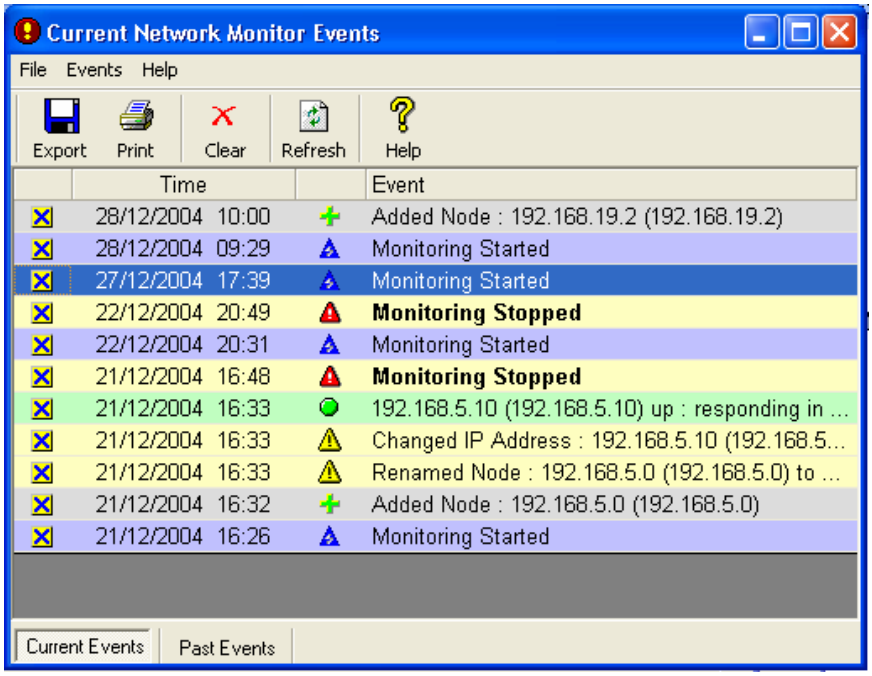


Figura 29. Ventana de Eventos

Para agregar un nuevo evento se usa el menú **"Events"** de la ventana anterior y se selecciona la opción **"Manually Add/ Send Event..."**

2.3.3. Watch It !

Watch It es un monitor de red. Puede monitorizar servidores, enrutadores y switches, entre otros y notificarle al administrador cuando el tiempo de respuesta se está degradando o cuando un dispositivo sale de servicio. Se emplean alarmas sonoras para indicar cuando un dispositivo está descartando paquetes, no responde o se activa de nuevo.

Watch It visualiza una fila de luces a lo largo del borde derecho de la pantalla.

Cuando el puntero del mouse se ubica sobre la fila de luces aparece la ventana de Watch It.

Figura 30. Watch It

El tiempo de respuesta de cada dispositivo es monitorizado constantemente. Cuando el tiempo de respuesta se empieza a incrementar o el dispositivo empieza a descartar paquetes, la luz junto al dispositivo se torna amarilla. Cuando el dispositivo no responde la luz se torna roja.

Para agregar un nuevo dispositivo solo se debe proporcionar la dirección IP o el nombre de dominio.

2.4 Configuración sugerida de la herramienta de gestión para la red de datos institucional.

Según las necesidades detectadas y el análisis hecho de la red de datos institucional, se propusieron unos lineamientos básicos para la configuración de la herramienta. Dentro de los aspectos fundamentales de la configuración sugerida se presta especial atención a las opciones relacionadas con la administración de direcciones IP y monitorización y reporte de eventos relacionados con los principales elementos de hardware de la red.

En primera instancia se recomienda el uso de Watch It para la monitorización y control de estado y tiempo de respuesta de servidores. Los servidores que según la importancia de los servicios ofrecidos se considera deben ser monitorizados son: el servidor de correo, servidor DNS y Exchanger (MX) (condor.uis.edu.co dirección IP 192.168.19.2), el servidor web (dodo.uis.edu.co dirección IP 192.168.19.15), el servidor de biblioteca (pelicano.uis.edu.co

dirección IP 192.168.19.6) y los servidores que soportan el sistema académico y el sistema financiero de la universidad.

Por otra parte se sugiere la configuración de alarmas que mediante el establecimiento de umbrales permitan controlar el porcentaje de utilización de las interfaces de los edificios donde se encuentra un mayor número de servidores, como lo son el edificio de administración, el laboratorio de posgrados, el edificio de biblioteca y el laboratorio de pesados.

Por último se recomienda la configuración de alarmas que reporten el cambio de estado de las interfaces asociadas a cada uno de los enrutadores que forman parte de la conexión a Internet y las conexiones entre las distintas sedes o campus de la WAN UIS.

3. DOCUMENTACIÓN DE LA RED

Al abordar la gestión, uno de los aspectos claves consiste en saber cuales datos se pueden extraer de la red y sobre todo cuales de ellos aportan información realmente útil que contribuya con la realización de la tarea de gestión.

La documentación de la red es un paso fundamental en el proceso de gestión. No se puede medir el desempeño y prestar atención a las fallas de manera eficiente si no se tiene un previo conocimiento de dónde se encuentra cada dispositivo y cómo está conectado.

No importa que tan sofisticadas sean las herramientas empleadas, las medidas hechas y las alertas generadas: No significan nada si no se tiene un previo conocimiento de cómo opera la red normalmente.

Idealmente, una gestión de red efectiva inicia con un buen diseño de red. Desafortunadamente, la mayoría de la gente no puede darse ese lujo, como en el caso de la red institucional, ya que la demanda inmediata de nuevos servicios y el rápido crecimiento del número de usuarios, implica un incremento significativo del número de dispositivos asociados a la red en un tiempo muy corto. Esta situación afecta significativamente la realización de un diseño adecuado y la debida documentación.

La teoría existente sobre gestión de redes indica que el éxito en la realización de la misma depende del buen conocimiento que se tenga de la red y su funcionamiento, por tal razón, con el fin de implementar una gestión de red efectiva se comenzó por conocer y documentar la red en su configuración actual (2004). Este inventario incluye una documentación de la composición tanto física como lógica de la red y sus componentes.

En este capitulo se describe el procedimiento seguido para descubrir como están conectados los distintos servidores, dispositivos de red y usuarios dentro de la red. Se hace un inventario del número de subredes existentes dentro de la red institucional, el número de servidores junto con la información detallada asociada a cada uno de ellos como: dirección IP, dirección MAC, servicios instalados, sistema operativo entre otros; descripción de los diferentes dispositivos activos presentes dentro de la red así como su interconexión.

También se presenta un diagrama y una descripción de la interconexión existente entre cada una de las sedes de la Universidad con el campus principal, dispositivos involucrados y características de cada enlace.

3.1 Examen preliminar

Como primer paso para la realización del Análisis de la tarea de gestión dentro de la red de datos institucional, se realizó un examen de la red. El propósito de este proceso era valorar con precisión y documentar el estado actual de la red, sus componentes, el personal involucrado y los procedimientos usados.

En cuanto a estos dos últimos elementos, se puede decir que debido a diversos factores entre ellos el escaso personal a cargo de la administración de la red, y la manera un poco repentina en la que se ha dado el crecimiento de la misma; en la actualidad dentro de la gestión de la red de datos institucional, no se cuenta con procedimientos establecidos para la atención y distribución de las diferentes tareas. Por tal razón, la documentación obtenida como producto de esta etapa del trabajo, se centra en las conexiones, características físicas y configuración lógica de la red y los elementos asociados a ella.

Sin la realización de dicho examen, no queda alternativa distinta a confiar en la memoria de las personas, o remitirse a mapas y bases de datos probablemente desactualizadas. Por tal razón antes de dar inicio a cualquier actividad de gestión vale la pena tomarse el tiempo para la realización de esta valoración.

Por falta de un conocimiento apropiado de las conexiones físicas y la localización exacta de los elementos de red, en ocasiones puede tomar un largo tiempo aislar un problema de red y se tiene una alta probabilidad de cometer errores introduciendo fallas dentro de la red, al realizar desplazamientos, agregar o cambiar dispositivos.

Para la realización de esta actividad se hizo uso de distintas herramientas de auto-discovery y mapeo disponibles en el mercado algunas de ellas en versión de prueba o demo. Aunque estas herramientas son bastante potentes en algunas ocasiones y para tener una mayor certeza, se debe contrastar la información obtenida de ellas; para esto, el trabajo estuvo soportado en la información suministrada por el personal encargado de la gestión de la red.

Cuando el rendimiento en una porción de la red empieza a bajar o se torna inestable, el primer paso es encontrar y aislar tan rápido como sea posible la fuente del problema. En ocasiones y dependiendo del tamaño y complejidad de la red, esta no es una tarea fácil; la meta es lograr que la red continúe operando y reducir el área afectada tanto como sea posible. En una red bien documentada, el administrador sabe cuales aplicaciones, dispositivos y comunidad de usuarios se verán afectados al presentarse un problema específico, y puede de manera proactiva hacer las notificaciones necesarias.

3.2 Importancia de la documentación

A menos de que se sea lo suficientemente afortunado como para seguir la creación y el crecimiento de la red desde su inicio, o se tenga la oportunidad de contar con un organigrama detallado del crecimiento de la misma, una de las opciones más probables es que se deba trabajar sobre una red que ha sido sometida a diversos cambios y actualizaciones, sin que dichos cambios hayan sido documentados.

Dependiendo de la actividad central de la organización y de su dependencia de la red para la realización de esta actividad, en algunos casos una falla de red puede significar pérdidas millonarias, que se incrementan con el tiempo que tarde la resolución del problema. Por ello cualquier procedimiento que pueda contribuir con la disminución de este tiempo de respuesta debe ser realizada de manera anticipada.

Uno de los principales inconvenientes relacionados con la documentación es el mantenimiento de la misma; esta es una tarea continua que debe ir a la par con el crecimiento y operación de la red. Cualquier modificación en la topología de la red, debe ser reportada y actualizada oportunamente, ya que así como una buena documentación contribuye significativamente con la efectividad al momento de atender una falla, una documentación inadecuada o desactualizada pude ser una fuente más de error.

3.3 Descripción general de la topología de la red de datos de la Universidad Industrial de Santander

Alrededor del año 1989 la red institucional funcionaba con un Dragon Switch como elemento central que incluía 8 puertos Ethernet, no se contaba con switches departamentales, el número de usuarios era mucho menor y algunos servicios como el correo electrónico eran ofrecidos a un reducido porcentaje de miembros de la comunidad universitaria.

Actualmente se cuenta con un Switch-Router central modelo Cajun P880 marca Lucent Technologies[9], de características muy superiores al Dragon switch mencionado anteriormente, que tiene instalados 34 puertos de fibra óptica con velocidades de 100 Mbps y 1000 Mbps; este dispositivo se encarga del enrutamiento entre las distintas subredes que forman parte de la red institucional.

En la actualidad se cuenta con 79 subredes, las cuales han sido asignadas a ciertas dependencias y en algunos casos a edificios. Debido a que el número de subredes (segmentos lógicos) es superior al número de segmentos físicos (edificios), es bastante común que en un mismo edificio se encuentran estaciones asociadas a distintas subredes. Este esquema de conexión es posible gracias a la opción de configuración de VLANs que tienen los switches disponibles dentro de la red.

[9] Lucent Technologies, filial de AT&T, hoy día se conoce como Avaya. Ver Anexo D

En el caso particular de la red de datos de la Universidad Industrial de Santander, se ha definido una VLAN por cada subred. Por ejemplo a la subred con dirección IP 192.168.45.0 le ha sido asociada la VLAN 45, a la subred con dirección IP 192.168.84.0 la VLAN 84 y así sucesivamente.

Dentro de las ventajas ofrecidas por el uso de VLANs se encuentra la capacidad de aislar el tráfico broadcast. A pesar de que un grupo de estaciones se encuentren conectadas al mismo switch o pertenezcan al mismo segmento físico, pueden pertenecer a distintas subredes y por tanto a diferentes VLANs, por tal razón el tráfico broadcast dirigido a una determinada subred solo será recibido por las estaciones asociadas a la VLAN correspondiente. .

Para la concentración a nivel de cada segmento de la red, se hace uso de 30 switches departamentales distribuidos a lo largo de los distintos segmentos de la red.

El ancho de banda contratado para acceso a Internet ha sido incrementado de 64 Kbps (1989) a un enlace que en la actualidad se encuentra en 8 Mbps (2004), contratados 4 Mbps con Colombia Telecomunicaciones y 4 Mbps con ETB. En los diagramas presentados más adelante se ofrecen más detalles sobre estos enlaces, así como de la interconexión a nivel del Switch-Router central Cajun P880.

La demanda de servicios por parte de los usuarios ha hecho que se incremente el número de estaciones que operan como servidores dentro de la red, así como el número de usuarios atendidos por cada uno de ellos y los servicios prestados. En la actualidad podemos hablar de un número aproximado de 45 estaciones que hacen las veces de servidor, cada uno de ellos con distintos tipos de servicios instalados. A diferencia de las condiciones manejadas años atrás, actualmente un alto porcentaje de la comunidad universitaria recibe el servicio de correo electrónico, dispone de un área de almacenamiento para sus archivos personales en alguno de los servidores y tiene la posibilidad de administrar su propio portal web o página personal entre muchos otros beneficios.

3.3.1. Interconexión del Switch-Router central Cajun P880

Como se mencionó anteriormente el principal dispositivo de interconexión presente a nivel del backbone de la red es el Switch-Router o Switch IP Cajun P880 de la marca Lucent Technologies, cuenta con 20 puertos para fibra operando a 100 Mbps (Fast Ethernet FX) y 14 puertos para fibra operando a 1000 Mbps (Gigabit Ethernet SX o LX[10]). La asignación de un puerto de 100 Mbps o 1000 Mbps depende del volumen de tráfico manejado por el segmento. El P880 está construido sobre un chasis central que permite incluir dos fuentes de alimentación y ofrece 9 ranuras para conectar tarjetas sobre las cuales se incluyen los puertos de servicio. En el caso de la UIS, no se ha adquirido la fuente de alimentación de respaldo y las ranuras se encuentran asignadas de la siguiente forma:

Tabla 3. Asignación de ranuras dentro del Cajun P880

Ranura/Módulo	Descripción
1	Módulo supervisor
2	Módulo supervisor
3	10 puertos 100FX
4	10 puertos 100FX
5	4 puertos 1000SX
6	4 puertos 1000FX
7	4 puertos 1000FX
8	Libre
9	4 puertos 1000FX

Como puede observarse el número total de interfaces físicas (puertos) es inferior al número de subredes que se desean interconectar, por tal razón el enrutamiento se hace mediante la

[10] SX y LX se refieren la longitud de onda utilizada en la fibra: short en el caso de 850 nm y long en el caso de 1310 nm

definición de interfaces lógicas; estas interfaces hacen las veces de gateway o puerta de enlace para cada una de las subredes.

A continuación se presenta el diagrama de interconexión del dispositivo de conmutación central con cada uno de los switches departamentales instalados en los diversos edificios dentro del campus de la universidad sede Cra 27, las sedes Bucarica, Guatiguará y el campus de la Facultad de Salud.

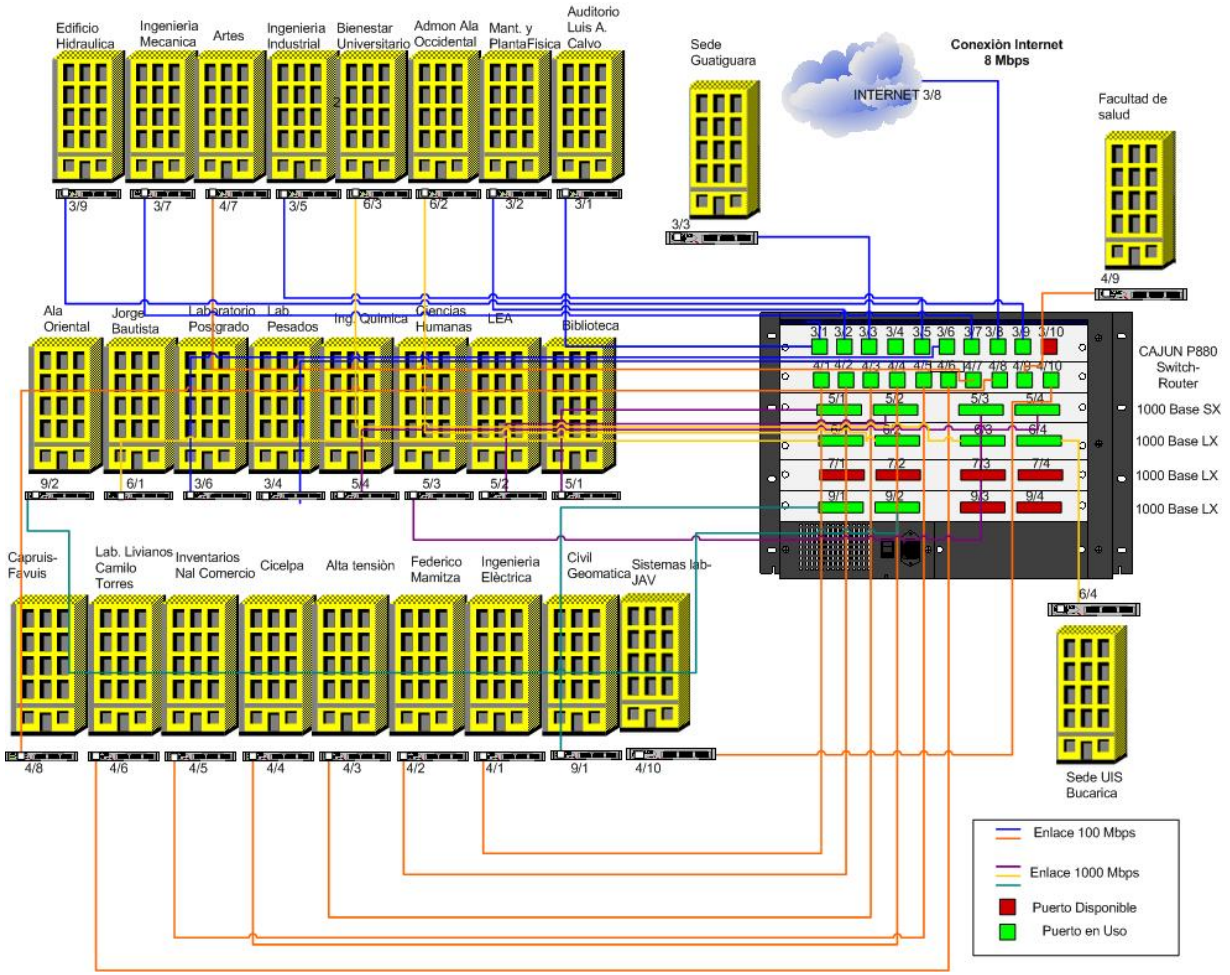


Figura 31. Cajun P880 Diagrama de Conexiones

En el diagrama se observa la distribución de puertos dentro del Cajun P880, como se puede ver en la actualidad el puerto número 10 del módulo 3 (3/10) se encuentra disponible, al igual que los cuatro puertos del módulo 7 y los puertos 3 y cuatro del módulo 9 (9/3, 9/4).

Tabla 4. Interconexión puertos Switch-Router central Cajun P880

Módulo/Puerto	Tipo de Interfaz	Dependencia
3/1	Fast Ethernet 100 Mbps	Auditorio Luis A. Calvo
3/2	Fast Ethernet 100 Mbps	Mantenimiento y Planta Física
3/3	Fast Ethernet 100 Mbps	Sede UIS Guatiguará
3/4	Fast Ethernet 100 Mbps	Laboratorio Pesados
3/5	Fast Ethernet 100 Mbps	Ingeniería Industrial
3/6	Fast Ethernet 100 Mbps	Laboratorio de Posgrado
3/7	Fast Ethernet 100 Mbps	Ingeniería Mecánica
3/8	Fast Ethernet 100 Mbps	Conexión a Internet
3/9	Fast Ethernet 100 Mbps	Edificio Hidráulica
3/10	Fast Ethernet 100 Mbps	Disponible
4/1	Fast Ethernet 100 Mbps	Ingeniería Eléctrica
4/2	Fast Ethernet 100 Mbps	Federico Mamitza
4/3	Fast Ethernet 100 Mbps	Alta Tensión
4/4	Fast Ethernet 100 Mbps	Cicelpa
4/5	Fast Ethernet 100 Mbps	Inventarios Nacional de Comercio
4/6	Fast Ethernet 100 Mbps	Laboratorio Livianos Camilo Torres
4/7	Fast Ethernet 100 Mbps	Edificio de Artes
4/8	Fast Ethernet 100 Mbps	Capruis-Favuis
4/9	Fast Ethernet 100 Mbps	Facultad de Salud
4/10	Fast Ethernet 100 Mbps	Sistemas Laboratorio JAV
5/1	Gigabit Ethernet 1000Mbps	Edificio Biblioteca

5/2	Gigabit Ethernet 1000Mbps	Edificio LEA (Luis Eduardo Arias)
5/3	Gigabit Ethernet 1000Mbps	Ciencias Humanas
5/4	Gigabit Ethernet 1000Mbps	Ingeniería Química
6/1	Gigabit Ethernet 1000Mbps	Edificio Jorge Bautista
6/2	Gigabit Ethernet 1000Mbps	Administración Ala Occidental
6/3	Gigabit Ethernet 1000Mbps	Bienestar Universitario
6/4	Gigabit Ethernet 1000Mbps	Sede UIS Bucarica
7/1	Gigabit Ethernet 1000Mbps	Disponible
7/2	Gigabit Ethernet 1000Mbps	Disponible
7/3	Gigabit Ethernet 1000Mbps	Disponible
7/4	Gigabit Ethernet 1000Mbps	Disponible
9/1	Gigabit Ethernet 1000Mbps	Ingeniería Civil Geomática
9/2	Gigabit Ethernet 1000Mbps	Administración Ala Oriental
9/3	Gigabit Ethernet 1000Mbps	Disponible
9/4	Gigabit Ethernet 1000Mbps	Disponible

3.3.2. Inventario Lógico de Subredes y administración de direcciones[11]

El objetivo de esta etapa era tener un inventario del número de subredes que conforman la red de datos de la Universidad, el número de estaciones asociadas a cada uno y las direcciones IP asignadas.

La WAN de la Universidad esta conformada por 72 subredes, cada una de las cuales se encuentra asociada a una dependencia, departamento o escuela específica como por ejemplo: la subred de Biblioteca, la subred de Ingeniería Industrial entre otras. La Universidad Industrial de Santander cuenta con distintos campus como lo son: sede Málaga, sede Barbosa, sede Socorro, sede Barranca, sede Guatiguara, UIS sede Bucarica y la

[11] Ver tabla de subredes en la base de datos

Facultad de Salud. La red de computadores que presta servicio en cada una de ellas a pesar de encontrarse en ubicaciones tan distantes, se comporta como una subred dentro de la WAN institucional.

Para la definición de estas subredes y para la identificación en general de todas las estaciones que forman parte de la red institucional se emplea el rango de las direcciones IP privadas clase C comprendido entre 192.168.0.0 hasta la 192.168.255.0. Este esquema gracias al cual se puede asignar todo el rango de direcciones de una red clase C (254 direcciones disponibles) a algunas dependencias donde probablemente el número de estaciones no corresponde ni al 5% de este valor, sólo se puede dar gracias a que el uso de estas direcciones no es regulado y no se debe pagar por ellas.

El procedimiento empleado para la realización de este inventario fue el siguiente: empleando la herramienta Subnet List disponible dentro de SolarWinds, se obtuvo una lista de las subredes que conforman la red, mediante una revisión de la tabla de rutas del switch-router central (Cajun P880). Una vez se obtuvo la lista de subredes el siguiente objetivo era saber cuales de las direcciones disponibles dentro de cada una de las subredes estaban siendo usadas. Para esto se dispone dentro de SolarWinds de un gran número de herramientas entre las que se encuentran: Ping Sweep, IP Network Browser, SNMP Sweep e IP Address Management. Cada una de ellas realiza un barrido del rango de direcciones indicado o de todo el rango de direcciones de una red y permite conocer cuales de dichas direcciones están siendo utilizadas.

Sin embargo de todas las herramientas anteriormente mencionadas, IP Address Management es la que permite llevar un mejor control de las direcciones que se están usando dentro de la red, cuáles se encuentran disponibles y cuáles se quieren reservar. La herramienta debe ser configurada ingresando una entrada para cada una de las redes o subredes que se quieran administrar, se debe suministrar únicamente la dirección IP y la máscara de red. Esta información es almacenada en una base de datos creada por la herramienta, y puede ser usada cada vez que se quiera repetir el escaneo.

Durante el desarrollo de esta actividad se hizo evidente la complejidad implícita en mantener actualizada la documentación de la red; en el caso particular de la administración de direcciones IP, es un proceso continuo ya que constantemente pueden estar entrando y saliendo estaciones de la red.

La función principal de las herramientas de administración de direcciones como esta es mantener un control de las direcciones que son usadas dentro de la red y procurar que no sean otras distintas a las que han sido asignadas por el administrador: Sin embargo en el caso de la red institucional no se conocía esta información hasta ahora se intentaba descubrir que direcciones se encontraban en uso independientemente de que cuenten con autorización o no. Actualmente se estudia la posibilidad de administrar direcciones usando DHCP con lo cual este problema se aliviaría de manera importante.[12]

En el caso de la red institucional, la definición de nuevas subredes, la conexión de nuevos equipos y la salida de otros ha sido un punto clave durante el último año, por tal razón se dice que los datos entregados se toman como una aproximación y no como un valor exacto.

Los resultados de esta etapa así como los relacionados con el inventario de hardware (Switches, servidores) serán presentados en una base de datos que permite que esta información siga siendo actualizada. A partir de la dirección IP de la subred el usuario podrá conocer la dependencia a la que corresponde, la máscara y qué direcciones del rango disponible se encuentran actualmente en uso.

3.3.2.1 Características Generales

El número de estaciones que se encuentran actualmente conectadas a la WAN de la Universidad es del orden de 1512, 44 de las cuales corresponden a estaciones con servidores instalados oficialmente.

[12] Trabajo de grado de Ingeniería Electrónica desarrollado por Jose Miguel Aguilera y Angélica María Anaya sobre la implantación del Dynamic Host Configuration Protocol en la red institucional.

La dirección IP definida para la puerta de enlace de cada una de las redes, corresponde como regla general a la primera dirección del rango (192.168.x.1), a excepción de la subred 192.168.37.0 correspondiente al Ala Oriental del Edificio de Administración cuya puerta de enlace es la dirección IP 192.168.37.251.

La subred que cuenta con mayor número de estaciones asociadas es la correspondiente a la facultad de salud cuya dirección IP es 192.168.30.0 y cuenta con un total aproximado de 120 estaciones lo cual corresponde a un porcentaje de uso del rango de direcciones del 47,24%. En segundo lugar se encuentran subredes como la del laboratorio de Posgrados 192.168.41.0 y la del Edificio de Petróleos 192.168.44.0 las cuales cuentan con 78 y 74 estaciones respectivamente y sus porcentajes de uso son de 30,71% y 29,13%.

En general se puede decir que la mayoría de subredes presentes dentro de la red están sobredimensionadas y el porcentaje de direcciones en uso es bastante bajo. Hablamos de un porcentaje promedio de uso de direcciones por subred de 10,44%.

En la tabla 5 se presenta la información relacionada con la direcciones IP, mascara, número de estaciones y porcentaje de uso por subred.

Tabla 5. Listado de Subredes Universidad Industrial de Santander[13]

Identificación Subred	Subred IP	Mascara	Uso	Disponibles	Porcentaje de Uso (%)
Avaya (switches)	192.168.5.0	255.255.255.0	36	218	14,17
Guatiguará	192.168.6.0	255.255.255.0	48	206	18,90
router (Conexión Internet)	192.168.9.0	255.255.255.248	2	4	33,33
Biblioteca	192.168.18.0	255.255.255.0	41	213	16,14
Servidores	192.168.19.0	255.255.255.0	21	233	8,27
Ciencias Humanas	192.168.20.0	255.255.255.0	50	204	19,69
Educación	192.168.21.0	255.255.255.0	11	243	4,33
LEA	192.168.22.0	255.255.255.0	22	232	8,66
Biblioteca Base de	192.168.23.0.	255.255.255.0	37	217	14,57

[13] Ver anexo B tabla de subredes

datos					
Lab. Pesados	192.168.24.0	255.255.255.0	41	213	16,14
Lab. Livianos	192.168.27.0	255.255.255.0	52	202	20,47
Fisica1	192.168.28.0	255.255.255.0	10	244	3,94
Fisica2	192.168.29.0	255.255.255.0	4	250	1,57
Salud Admon.	192.168.30.0	255.255.255.0	120	134	47,24
Cicelpa	192.168.31.0	255.255.255.0	23	231	9,06
Artes	192.168.32.0	255.255.255.0	4	250	1,57
Capruis	192.168.33.0	255.255.255.0	12	242	4,72
Diseño Industrial	192.168.34.0	255.255.255.0	38	216	14,96
Bienestar	192.168.35.0	255.255.255.0	25	229	9,84
Luis A. Calvo	192.168.36.0	255.255.255.0	5	249	1,97
Ala Oriental	192.168.37.0	255.255.255.0	33	221	12,99
Ala Occidental	192.168.38.0	255.255.255.0	58	196	22,83
Ing. Química	192.168.39.0	255.255.255.0	30	224	11,81
Ing. Industrial	192.168.40.0	255.255.255.0	32	222	12,60
Postgrados	192.168.41.0	255.255.255.0	78	176	30,71
Planta Física	192.168.42.0	255.255.255.0	17	237	6,69
Mecánica	192.168.43.0	255.255.255.0	21	203	8,27
Petróleos	192.168.44.0	255.255.255.0	74	180	29,13
Alta tensión	192.168.45.0	255.255.255.0	39	215	15,35
Eléctrica	192.168.46.0	255.255.255.0	31	223	12,20
MorfoPatología	192.168.47.0	255.255.255.0	1	253	0,39
HURV	192.168.48.0	255.255.255.0	1	253	0,39
Sala Conferencias	192.168.49.0	255.255.255.0	1	253	0,39
INSED	192.168.50.1	255.255.255.0	61	193	24,02
Favuis	192.168.51.0	255.255.255.0	1	253	0,39
Bucarica	192.168.54.0	255.255.255.0	20	234	7,87
Financiero Tesorería	192.168.58.0	255.255.255.0	21	233	8,27
Admisiones	192.168.59.0	255.255.255.0	14	240	5,51
LEA salas2-3-5	192.168.61.0	255.255.255.0	58	196	22,83
LEA salas4-6	192.168.62.0	255.255.255.0	38	216	14,96
Alta Tensión Lab. Elec.	192.168.71.0	255.255.255.0	18	236	7,09
Hidráulica	192.168.72.0	255.255.255.0	3	251	1,18
CITI	192.168.73.0	255.255.255.0	10	244	3,94
CNBiling	192.168.74.0	255.255.255.0	3	251	1,18

Nodo PML	192.168.75.0	255.255.255.0	10	244	3,94
FUNDEUIS	192.168.76.0	255.255.255.0	8	246	3,15
DSI	192.168.80.0	255.255.255.0	8	246	3,15
Planeación Rectoría	192.168.81.0	255.255.255.0	18	236	7,09
Sistemas1	192.168.84.0	255.255.255.0	24	230	9,45
Civil Geomática	192.168.85.0	255.255.255.0	56	198	22,05
Civil Geomática2	192.168.86.0	255.255.255.0	1	253	0,39
Civil Geomática3	192.168.87.0	255.255.255.0	1	253	0,39
Petróleos Sala CPIP	192.168.88.0	255.255.255.0	15	239	5,91
Publicaciones	192.168.89.0	255.255.255.0	14	240	5,51
Asesorías	192.168.92.0	255.255.255.0	7	247	2,76
Incubadora Empresas	192.168.93.0	255.255.255.0	1	253	0,39
CIDLIS	192.168.94.0	255.255.255.0	16	238	6,30
TELEUIS	192.168.96.0	255.255.255.0	3	251	1,18
Recursos Humanos	192.168.97.0	255.255.255.0	14	240	5,51
Sede Socorro 1	192.168.99.0	255.255.255.224	0	30	0,00
Sede Socorro 2	192.168.99.32	255.255.255.224	13	17	43,33
Sede Socorro 4	192.168.99.96	255.255.255.224	11	19	36,67
Sede Socorro 5	192.168.99.128	255.255.255.224	5	25	16,67
Sede Socorro 6	192.168.99.160	255.255.255.224	1	29	3,33
Sede Barranca	192.168.100.0	255.255.255.0	25	229	9,84
Sede Málaga	192.168.101.0	255.255.255.0	12	242	4,72
Sede Barbosa	192.168.102.0	255.255.255.0	4	250	1,57
Fisioterapia1	192.168.105.0	255.255.255.0	4	250	1,57
Nutrición	192.168.106.0	255.255.255.0	1	253	0,39
Instituto Lenguas	192.168.107.0	255.255.255.0	13	241	5,12

3.3.3. Inventario de hardware (switches, servidores, routers)

La gestión de redes tiene como objetivo fundamental la supervisión y control de los dispositivos de red, buscando garantizar su máximo aprovechamiento. De allí que el primer paso para poner en marcha cualquier modelo de gestión requiere conocer cuáles son esos dispositivos.

Haciendo uso de la herramienta IP Network Browser se escanearon los distintos segmentos de la red, lo cual permitió localizar los principales dispositivos administrables asociados a ella. Al igual que en el caso de las subredes, se han creado dos tablas que permiten manejar la información asociada a cada uno de estos dispositivos, una tabla que contiene la información relacionada con los servidores y la otra todos los aspectos asociados a los distintos elementos presentes en el backbone de la red como switches y enrutadores.

3.3.3.1 Características Generales

Como ya se mencionó anteriormente la topología física de la red corresponde a una estrella donde el nodo central es el Switch-Router central Cajun P880, del cual se desprende una conexión a través de un enlace de fibra óptica multimodo a cada uno de los segmentos físicos de la red. Para la concentración en cada segmento se dispone de un switch departamental y varios hubs en muchos casos.

En total podemos hablar de 30 switches departamentales distribuidos de la siguiente manera: 24 están ubicados en los distintos edificios del campus universitario de la carrera 27, uno en la sede UIS Bucarica, cuatro en la Facultad de Salud y uno más en la sede UIS Guatiguará. Cada switch cumple con las siguientes características: Cajun P330 Stackable Switch, SW versión 3.5.23 de la marca Avaya, 24 puertos 10/100 Base-TX y uno o dos puertos de fibra óptica correspondiente al uplink de interconexión con el Cajun P880[14].

La tabla asociada a los switches proporciona información relacionada con:

- Dirección IP
- Dependencia o edificio
- Dirección Física (MAC)
- Subredes Lógicas Asociadas
- Localización
- Aspectos generales del dispositivo (información de puertos por ejemplo)

[14] Ver Anexo D hoja de datos de los dispositivos

Para realizar el escaneo de servidores se siguió un procedimiento similar. Debido a que no todos se encuentran dentro de la misma subred lógica se tuvieron que escanear y analizar cada una de las subredes individualmente con el fin de identificar cuáles de las estaciones presentes podían ser servidores. Como política interna para identificar la gran mayoría de los servidores dentro de la red de datos institucional se emplean nombres de aves. Por tal razón la identificación se hizo a partir de los nombres de dominio y alguna información suministrada por el administrador de la red relacionada con la configuración interna del servidor DNS.

Con la Herramienta IP Network Browser solo se pudo identificar la dirección IP y el nombre de dominio de las estaciones; en algunos casos dependiendo de la configuración SNMP del dispositivo y de si la MIB es o no soportada por la herramienta se pudo obtener otro tipo de información como, dirección física, sistema operativo, servicios instalados, entre otros. En otros casos fue necesario hacer uso de herramientas de escaneo de puertos que permitieron hacer esta identificación de servicios; para definir el dispositivo y puerto de conexión de cada servidor se empleó la herramienta Switch Port Mapper, también disponible en SolarWinds, y se hizo una revisión detallada de los puertos de cada uno de los switches departamentales. La herramienta reporta la dirección IP, nombre de dominio y dirección física de la estación o estaciones conectadas a cada puerto.

La tabla relacionada con los servidores contiene la siguiente información:

- Nombre de Dominio
- Dirección IP Privada (válida dentro de la WAN)
- Dirección IP Pública
- Dirección Física (MAC)
- Sistema Operativo
- Ubicación
- Descripción General
- Servicios Instalados

En términos generales se puede decir que dentro de la red de datos de la Universidad Industrial de Santander hay aproximadamente 44 servidores públicos, y que los servicios

más comunes son la transferencia de archivos (FTP[15]), servicio de páginas Web (HTTP[16]), Telnet y correo electrónico.

Además de los switches departamentales y el Switch-Router Central, existen otros dispositivos administrables que forman parte de la red de datos institucional y sin los cuales no sería posible la interconexión entre las distintas sedes ni la conexión externa a Internet. Al hacer un inventario de estos dispositivos se encontraron:

2 Enrutadores Cisco 1721
3 Enrutadores Cisco 2501
1 Enrutador Cisco 2522
1 Enrutador Cisco 3620

La información adicional relacionada con su conexión dentro de la red y sus características generales, se presenta en la tabla de dispositivos activos y gráficamente mediante los diagramas de interconexión entre sedes y Enlace a Internet presentados más adelante.

3.3.4. Interconexión entre sedes

La WAN de la Universidad Industrial de Santander está conformada por tres sedes que se encuentran en Bucaramanga (Sede Principal Cra 27, Sede Bucarica, Sede Facultad de Salud), una sede ubicada en Piedecuesta, y cuatro sedes más ubicadas en el Socorro, Málaga, Barranca y Barbosa respectivamente. El esquema de interconexión entre ellas varía dependiendo básicamente de la distancia; más adelante se presenta un diagrama y una explicación de cada uno de estos esquemas.

Es importante resaltar que a pesar encontrarse en distintas ubicaciones físicas e independientemente de su esquema de interconexión cada una de estas sedes se ve como si fuera un edificio más dentro del campus de la Universidad y forman parte de la misma WAN.

---

[15] File Transfer Protocol: Protocolo de transferencia de archivos

[16] HyperText Transfer Protcol: Protocolo de transferencia de hipertexto

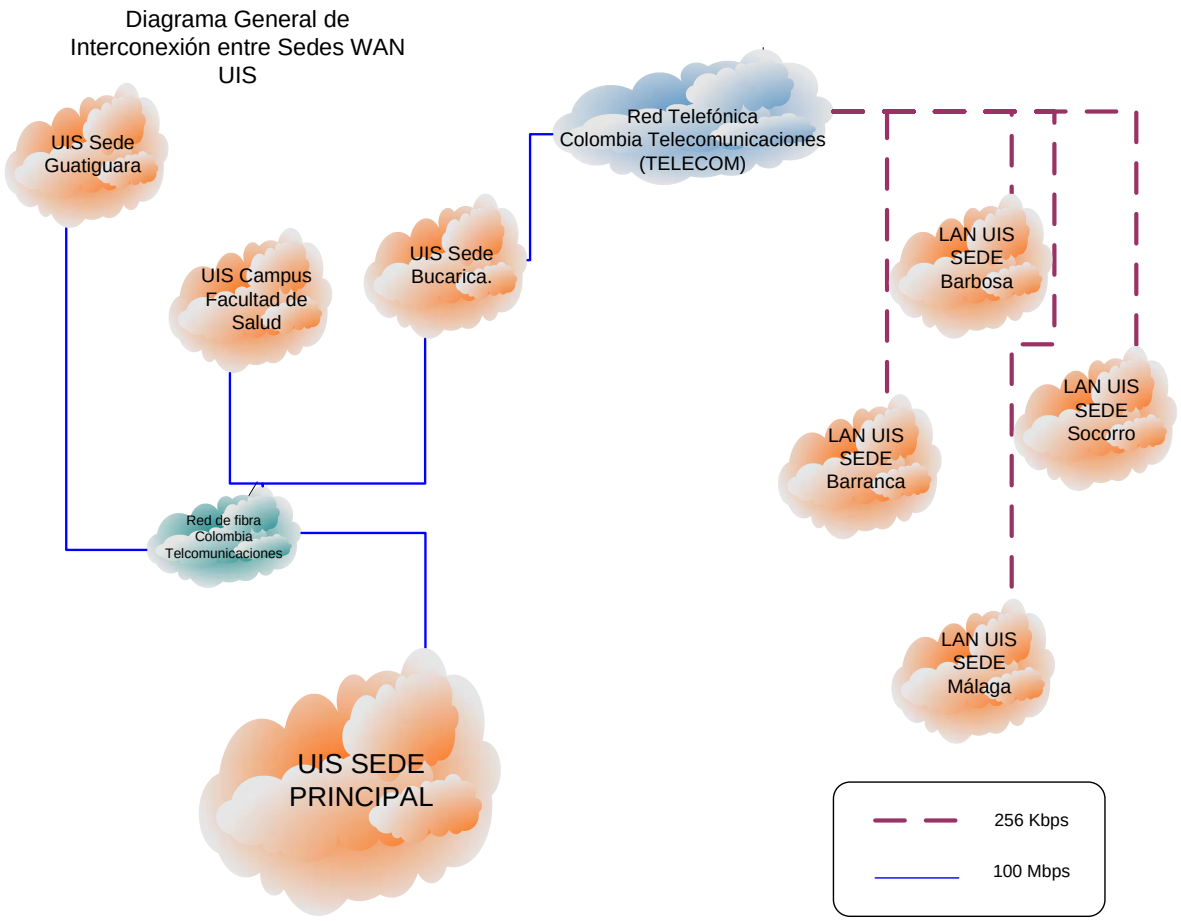


Figura 32. Diagrama de Interconexión WAN UIS

Para la conexión entre la sede Principal y la sede Bucarica al igual que con el campus de la Facultad de Salud, se utiliza la red de fibra de Colombia Telecomunicaciones; en el caso del la sede Bucarica se utiliza un enlace de fibra monomodo de 1Gbps; para la conexión con la Facultad de Salud se utiliza un enlace Fast Ethenet con fibra multimodo.

3.3.4.1 Conexión Sede UIS Guatiguará

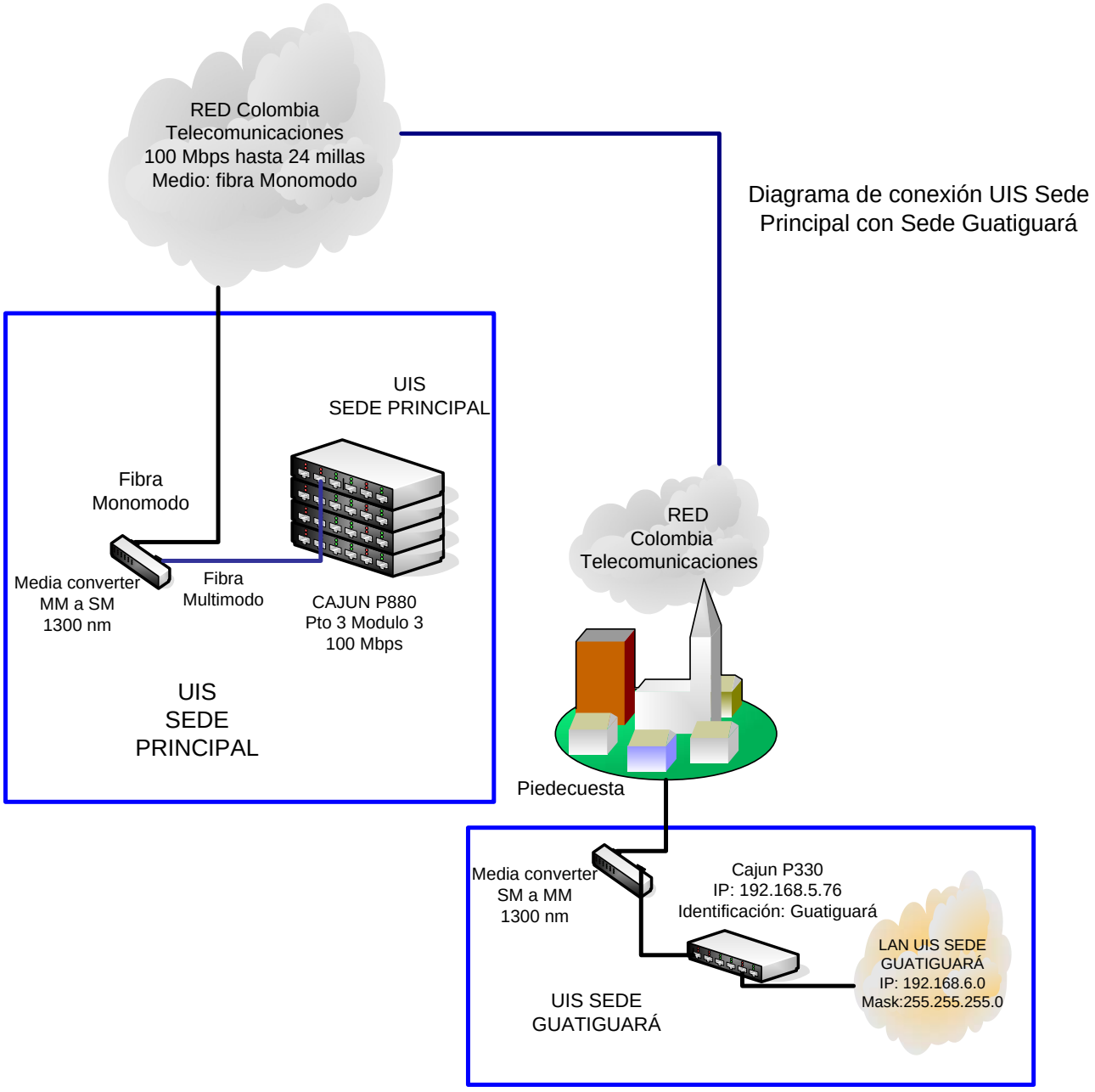


Figura 33. Interconexión de red UIS sede Principal- Sede UIS Guatiguará

En la figura 33 se presenta de forma detallada la interconexión de red entre el campus principal de la Universidad y la sede Guatiguará ubicada en el municipio de Piedecuesta.

La conexión inicia en el puerto Fast Ethernet 3 del módulo 3 del Switch-Router central Cajun P880, al cual se conecta un patch cord de fibra multimodo que llega a un convertidor de medios para obtener una salida por fibra monomodo a través de la cual se entra a la red de fibra de Colombia Telecomunicaciones (100Mbps), hasta llegar a Piedecuesta. En la sede Guatiguará se emplea nuevamente un convertidor de medios, en este caso de monomodo a multimodo, cuya salida se conecta al módulo de fibra del Switch departamental Cajun P330 cuya dirección IP es 192.168.5.76.

3.3.4.2 Conexión Sede UIS Barranca

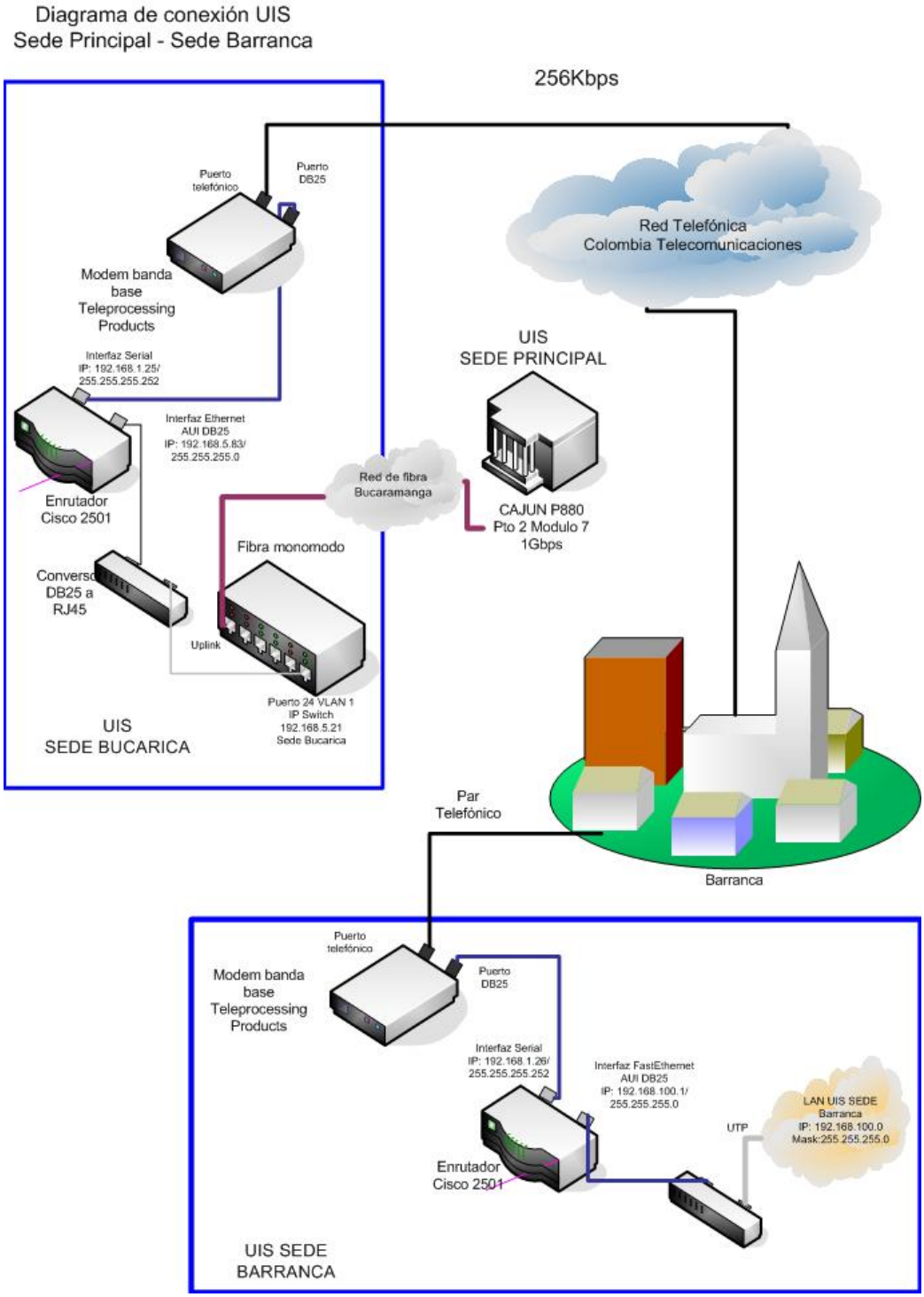


Figura 34. Interconexión de red UIS sede Principal- Sede UIS Barranca

La conexión entre la sede principal de la Universidad y la sede UIS Barranca se hace a través de la conexión con la sede Bucarica. Del puerto de servicio 24 del switch Cajón P330 con dirección IP 192.168.5.21 (Bucarica), se llega a la interfaz Ethernet AUI de un enrutador Cisco 2501 ubicado allí mismo, para lo cual se debe utilizar un conversor RJ45 a DB25.

Saliendo por la interfaz serial del enrutador se llega a un MODEM ADTRAM 654 que ajusta la señal para que pueda ser transmitida por Red Telefónica hasta llegar a la oficina de Colombia Telecomunicaciones ubicada en el municipio de Barranca, desde donde por par aislado de cobre se llega a un MODEM ADTRAM 654 ubicado dentro de la sede de la Universidad. Este último a su vez se conecta al puerto serial de un enrutador Cisco 2501 que se encarga de la interconexión con la subred Barranca cuya dirección IP es 192.168.100.0/24.

3.3.4.3 Conexión sede UIS Socorro

El esquema de interconexión con la Sede Socorro al igual que con las sedes de Málaga y Barbosa, es bastante similar al anterior, en este caso saliendo de un puerto de Switch Cajun P330 ubicado en la sede Bucarica (puerto 12), se llega a la interfaz Ethernet AUI de un enrutador Cisco 2522 que cuenta con ocho interfaces seriales de las cuales la Serial 0 es usada para la conexión con la sede Socorro y las Seriales 3 y 7 para la conexión con la sedes Barbosa y Málaga respectivamente.

La conexión nuevamente se realiza a través de la Red Telefónica de Colombia Telecomunicaciones hasta llegar a una oficina ubicada en los respectivos municipios. Desde allí nuevamente por par aislado de cobre se llega a las instalaciones de cada una de las sedes, se pasa por un MODEM banda base que hace la conversión a un puerto DB25 para la conexión con un enrutador Cisco 2501 en el caso de la conexión con la sede Socorro y enrutadores Cisco 1721 para Málaga y Barbosa.

Una vez dentro de cada una de las sedes a través de la interfaz Ethernet del enrutador se establece la conexión con la subred respectiva.

Detalle diagrama de interconexión UIS Sede Principal - Sede Socorro

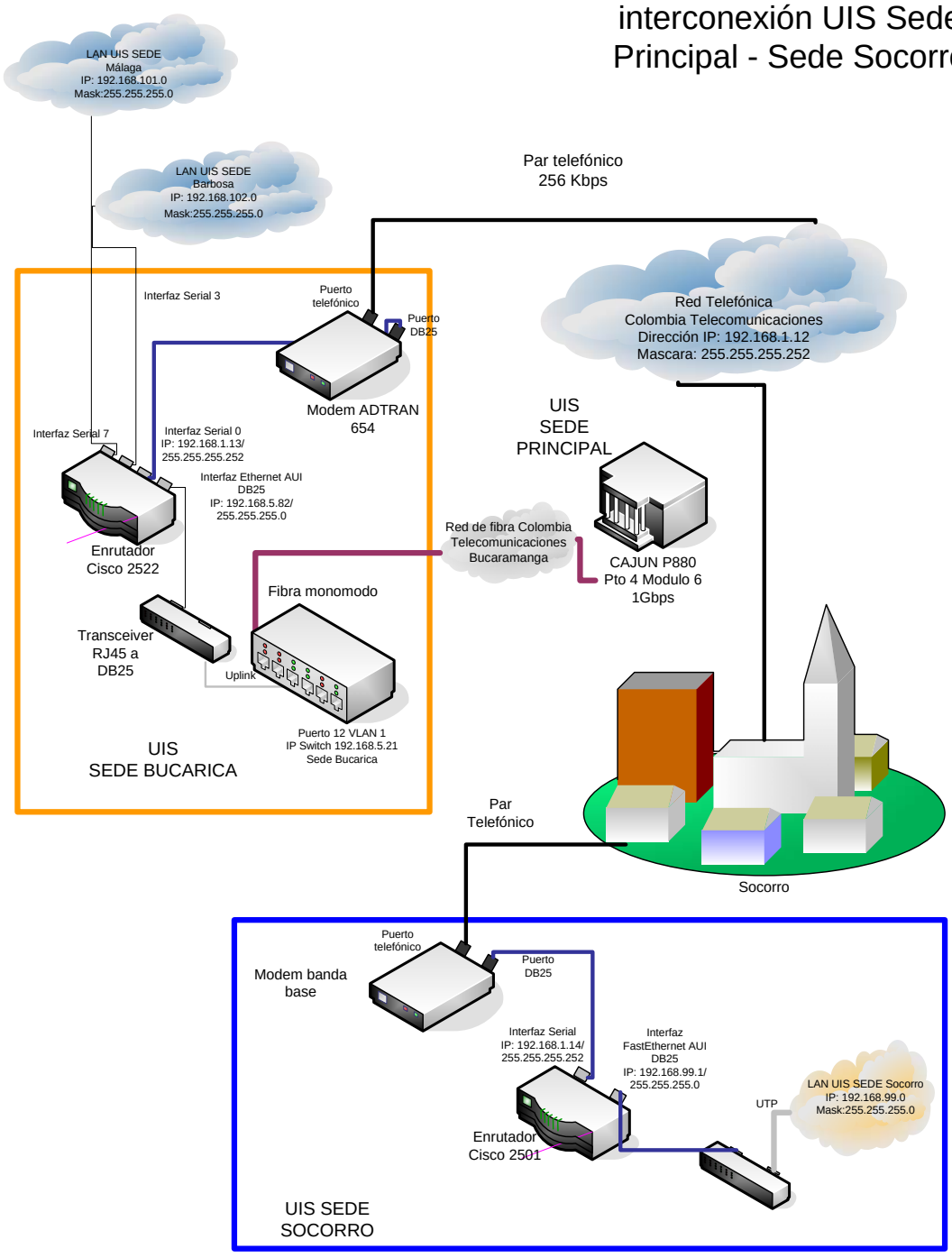


Figura 35. Interconexión de red UIS sede Principal- Sede UIS Socorro

3.3.4.4 Conexión sede UIS Málaga

Es importante resaltar que este esquema de interconexión al igual que el de la sede Barbosa forman parte de las últimas modificaciones realizadas a la estructura de la red que entraron en funcionamiento a partir de diciembre de 2004

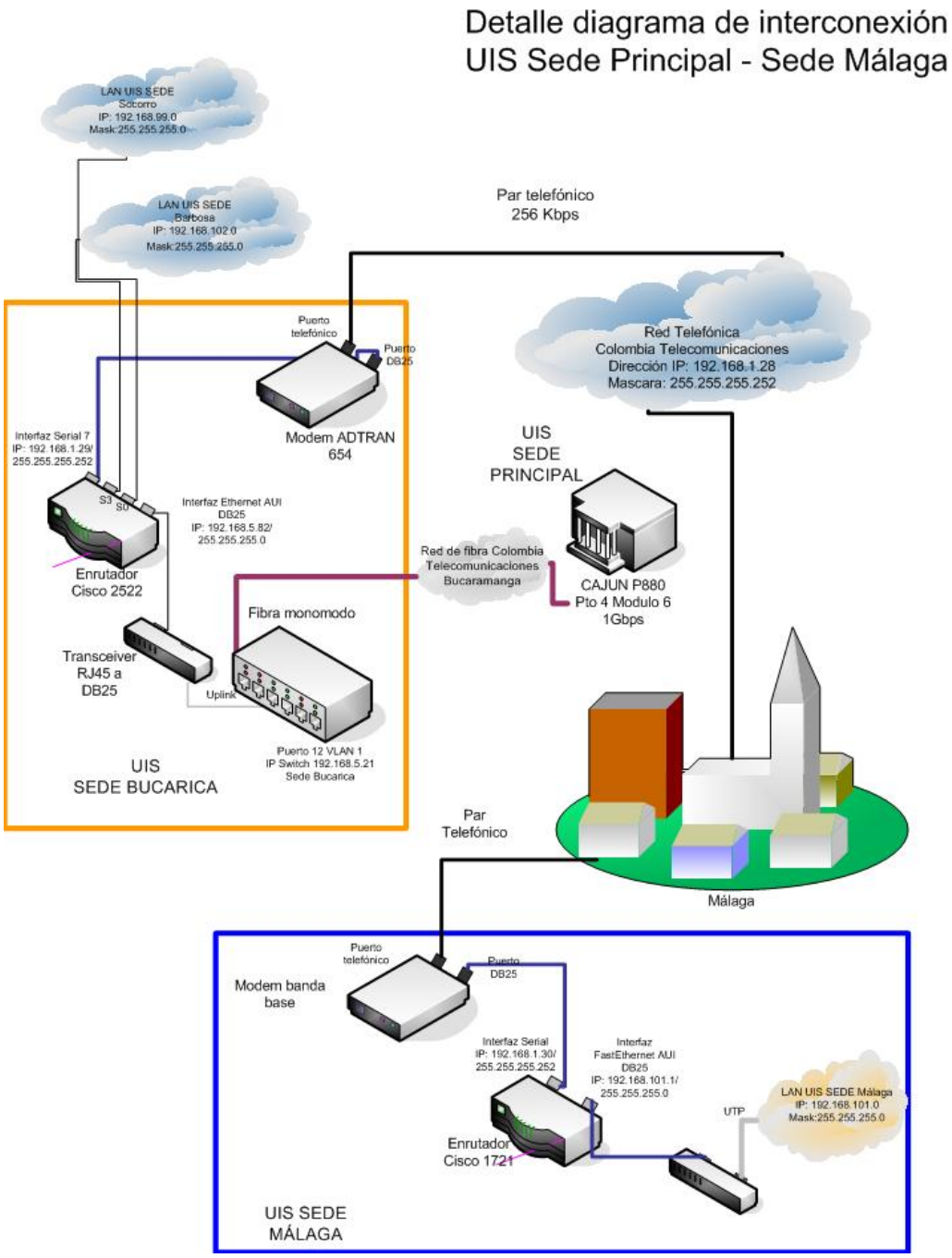


Figura 36. Interconexión de red UIS sede Principal- Sede UIS Málaga

3.3.4.5 Conexión Sede UIS Barbosa

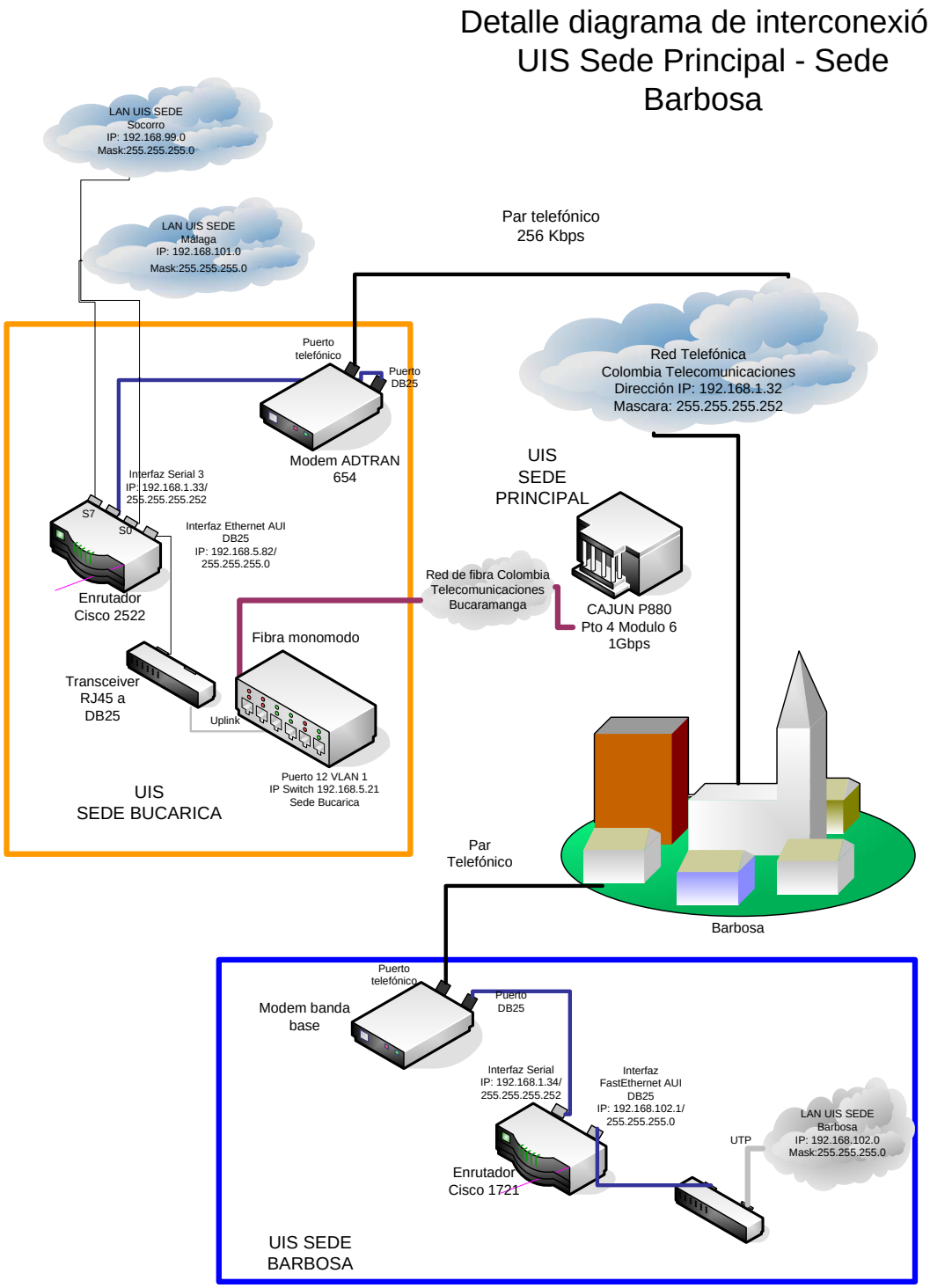


Figura 37. Interconexión de red UIS sede Principal- Sede UIS Barbosa

3.3.5. Descripción Enlace Conexión a Internet

En la Figura 38 se presenta el diagrama actual de conexión a Internet de la Red de datos de la Universidad Industrial de Santander. En los últimos dos meses, al igual que en los esquemas de conexión entre sedes, se han presentado cambios significativos en este enlace. Para el mes de septiembre de 2004 la Universidad contaba con un enlace de 4Mbps soportados equitativamente por los proveedores Colombia Telecomunicaciones (Telecom) y Telefónica. A partir del mes de noviembre de 2004 este enlace se ha reemplazado por uno de 8Mbps donde se ha pasado de un enlace de 2Mbps a uno de 4Mbps con la empresa Colombia Telecomunicaciones y se ha sustituido el servicio ofrecido por Telefónica con un enlace de 4Mbps contratado con la empresa ETB.

El principal cambio en el enlace a parte de la ampliación del ancho de banda, radica en la instalación de un enrutador Cisco 3640 propiedad de ETB que soporta BGP[17]. Este enrutador se encuentra dentro de las instalaciones de la Universidad Sede principal y se encarga del enrutamiento entre la red Institucional que a partir de este momento adquiere la connotación de un Sistema Autónomo[18] en Internet.

Partiendo del puerto 8 módulo 3 del Switch-Router Cajun P880, se sale por una fibra multimodo (100Mbps) hasta llegar a un convertidor de medios 100 Base FX (MM) a 100 Base TX; a través de un cable UTP se establece una conexión con el Firewall Cisco Pix 515, encargado de la seguridad dentro de la red. El siguiente paso es la Interfaz Fast Ethernet 0/0 de el enrutador BGP Cisco 3640; este dispositivo es el punto de unión entre los enlaces ofrecidos por los dos proveedores y la LAN UIS.

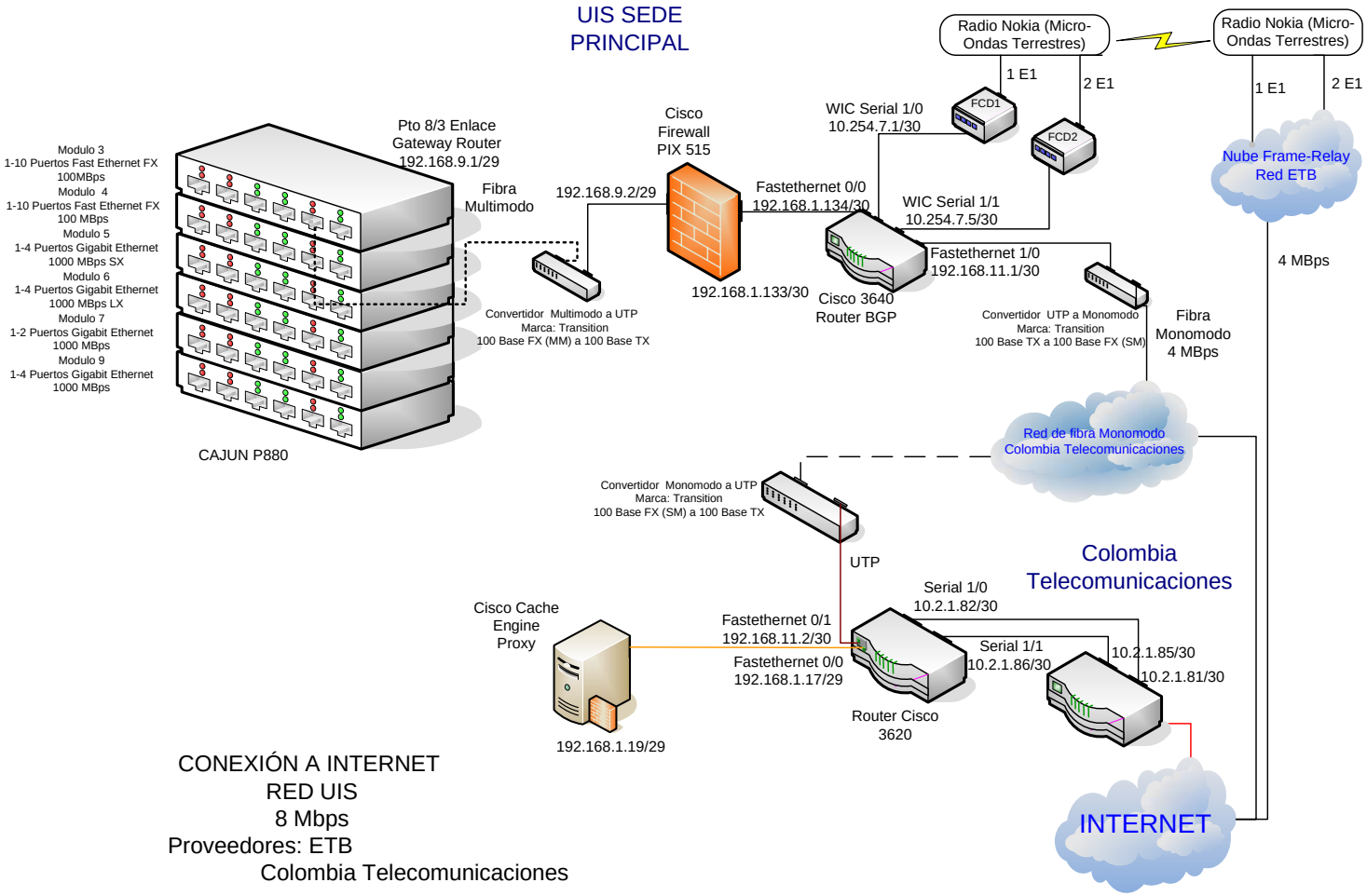
Es importante tener en cuenta que de este punto en adelante los elementos empleados son propiedad del proveedor y por tanto su configuración o sustitución no son responsabilidad del

[17] Border Gateway Protocol

[18] por Sistema Autónomo (SA) se entiende una zona de la red con políticas internas de enrutamiento propias que se comunica con otros SA mediante protocolos de pasarela externa, BGP típicamente. Cada SA se identifica con un número único asignado por autoridades de Internet.

administrador de la WAN institucional. Sin embargo dentro del enlace ofrecido por Colombia Telecomunicaciones se encuentran dos elementos que son propiedad de la UIS?; se trata del Proxy Cisco Cache Engine y un enrutador Cisco 3620 que para facilitar el esquema de conexión física han sido ubicados dentro de las instalaciones del proveedor.

Como se observa en el diagrama, el servicio prestado por ETB está basado en una solución de última milla inalámbrica (Micro Ondas Terrestres), mientras que el enlace Telecom esta basado en el servicio prestado por su red de Fibra Óptica Monomodo.



CONEXIÓN A INTERNET
RED UIS
8 Mbps
Proveedores: ETB
Colombia Telecomunicaciones

Figura 38. Conexión a Internet Red LAN Universidad Industrial de Santander

4. METODOLOGÍA PARA LA IDENTIFICACIÓN DE CONDICIONES DE FALLA EN REDES ETHERNET

El crecimiento acelerado de las redes y en especial de las LAN, ha originado un gran interés en la gestión de los recursos de red y el incremento de su disponibilidad. El uso eficiente de los recursos y la calidad del servicio ofrecido dependen de la confiabilidad que ofrece la red. Por lo tanto la detección, identificación y corrección de fallas de red es una tarea básica dentro de la administración de la red.

Actualmente existen diversas técnicas disponibles para la detección de fallas de desempeño. El estudio propuesto busca plantear y probar una metodología general que permita identificar posibles condiciones de falla propias de un segmento de red tipo Ethernet.

Partiendo de la hipótesis de que las fallas presentes dentro de una red pueden ser clasificadas usando la información contenida en las variables de la MIB de los dispositivos asociados a ella, se propone desarrollar una metodología que permita realizar la clasificación e identificación de distintos tipos de falla a partir de la detección de cambios o valores inusuales en los datos de la MIB.

La organización del presente capítulo es como sigue: en primer lugar se discuten los criterios tenidos en cuenta para la identificación y selección de las condiciones de falla empleadas como base de estudio, así como el proceso de identificación y selección de las variables MIB asociadas a las fallas seleccionadas. Una vez conocidas las condiciones de operación de las fallas elegidas y establecida una relación entre estas y las variables de la MIB, se describe la técnica utilizada para la generación de fallas en el numeral 4.2. Por último se aborda el proceso propuesto para la clasificación de las fallas.

4.1 Selección de fallas y asociación con variables MIB

El objetivo de esta etapa es la identificación y selección de las fallas a clasificar. En esta sección se describirá el proceso y los criterios de selección de las fallas de red Ethernet típicas utilizadas durante este estudio. Además se expondrá la asociación de tales fallas con un conjunto de variables MIB con base en la afinidad entre las características de las fallas y la información almacenada en tales variables. El objetivo es establecer una base conceptual que permita identificar los posibles estados de falla

propios de una red a partir de la información obtenida de los dispositivos administrables asociados a ella.

En la literatura relacionada con este tema, se presentan con frecuencia procedimientos de selección de variables basados en la experiencia de los investigadores y administradores de las redes bajo estudio[17]. Debido a que el propósito de este trabajo es crear la base para la realización de una metodología general, este tipo de criterios no se ajusta a los objetivos perseguidos.

El análisis de grandes volúmenes de datos para reducirlos a sólo aquellos eventos anómalos que sean indicativos de problemas en la red es el objetivo principal en los trabajos relacionados con este tema. Habitualmente se busca identificar los parámetros de desempeño que son afectados por una falla o anomalía específica para luego seleccionar las variables que brindan información detallada sobre estos parámetros.

Para la identificación y selección del tipo de fallas a clasificar se tuvieron en cuenta criterios básicos usados en medidas de desempeño y las características generales de la red bajo estudio; se realizó un reconocimiento de los servicios, aplicaciones y procedimientos empleados normalmente por los usuarios, así como del tipo de red y los dispositivos presentes en ella con el fin de identificar las condiciones que se deseaban controlar. Es de gran importancia tener en cuenta que cada red tiene sus particularidades y por lo tanto las condiciones de desempeño así como la calidad del servicio esperado, varían en cada una de manera independiente.

4.1.1. Criterios de selección de fallas

Los problemas en una red tipo Ethernet se afrontan siguiendo la premisa de que las fallas de red se manifiestan a través de degradaciones del desempeño que hacen que el servicio entregado se desvíe del servicio especificado o esperado. El método más usado para notar estas degradaciones es la detección de anomalías, donde una anomalía es definida como “un desempeño estadísticamente inusual”[17]. A partir de esta definición se pueden orientar los esfuerzos para la descripción de fallas, hacia el análisis de las condiciones anómalas que las caracterizan.

Como parte fundamental de esta etapa se realizó un estudio de los tipos de fallas más comunes en redes tipo Ethernet. Algunas de las fallas analizadas fueron: Tormenta

Broadcast (Broadcast Storm), Congestión de red o Problemas de Congestión (Network Congestion), Puente Atascado (Stalled Bridge), Inundación de Fragmentos (Runt Flood), Inundación de Gigantes (Jabbering Flood), todas ellas descritas en el capítulo 1.

Entre este conjunto tan amplio, es preciso seleccionar un número mínimo de fallas representativas que puedan ser descritas de manera simple a partir de la información almacenada en las variables de la MIB, de forma tal que puedan identificarse los estados de falla mediante la monitorización de un grupo de variables asociadas a cada uno de ellos

Como se mencionó anteriormente, es importante resaltar que dependiendo de las características particulares de la red se debe realizar la selección de las condiciones a controlar. Como la idea del trabajo es plantear una metodología general, por tal razón además de algunos criterios de selección expuestos más adelante, se eligieron las fallas que se considera pueden tener una alta incidencia y afectar en general cualquier red.

Como criterios para la selección de las fallas se tuvieron en cuenta los siguientes:

- Frecuencia de ocurrencia de la falla (las fallas de inundación de fragmentos e inundación de enanos manejan un bajo nivel de ocurrencia, razón por la cual fueron descartadas).
- La selección de fallas está limitada por los parámetros de desempeño soportados y reportados por el sistema de monitorización disponible.
- Las fallas seleccionadas deben representar un amplio rango de problemas en la red, como el mal uso de de los servicios originado en los protocolos de alto nivel, problemas de implementación de protocolos, tráfico excesivo, saturación de la capacidad de la red, etc.

Para la selección se realizó un análisis de las características y propiedades de cada una de las fallas anteriormente mencionadas, se aplicaron los criterios establecidos y considerando la incidencia que cada una de ellas tendría sobre el tipo de red bajo estudio (segmento Ethernet) así como las evidentes similitudes existentes entre algunas de ellas, se tuvo preferencia por aquellas tuvieran un carácter más general. Como resultado de este proceso se seleccionaron la Congestión de red y la Tormenta de Broadcast.

Tormenta Broadcast (Broadcast Storm): Esta falla es causada por el envío repetitivo de mensajes broadcast, usualmente en busca de información o servicios. Además de perturbar el desempeño individual de las estaciones, también se ve afectado el rendimiento general de la red debido a la inundación de respuestas a la difusión (broadcast).

Congestión de Red (Network Congestion): Un incremento en la carga de red resulta en una disminución en la capacidad de trabajo útil de la misma. Si la red esta congestionada, la utilización es usualmente muy alta, y el número de paquetes descartados se incrementa.

4.1.2. Criterios de selección de variables MIB

A partir del análisis de las características de las fallas seleccionadas, se realizó una revisión detallada de la definición asociada a cada una de las variables contenidas dentro de la MIB del dispositivo; esta revisión se efectuó sobre las variables que se encuentran contenidas en los diez grupos principales de la MIB estándar además de las variables del grupo RMON. Se seleccionaron de manera tentativa aquellas variables que teóricamente podrían aportar información para la identificación de las condiciones o síntomas asociados a las fallas seleccionadas en la etapa anterior.

Mantener el número de variables en un nivel reducido es fundamental porque garantiza que el nivel de tráfico generado por la monitorización de los dispositivos no va a ser considerable y además simplifica el procesamiento de datos necesario en el proceso de detección y clasificación. Al hacer la revisión teórica de cada una de las variables contenidas dentro de los grupos principales de la MIB se notó que un gran número de dichas variables son redundantes o presentan una correlación directa.

Existen dos procedimientos clave, muy usados para la selección adecuada de las variables[22]:

- El primero, consiste en usar el conocimiento y experiencia sobre la falla, sus causas y manifestaciones.
- El segundo, consiste en comparar el comportamiento de cada variable durante una falla contra el comportamiento durante la operación normal.

Teniendo en cuenta las ventajas y desventajas que ofrece cada uno de ellos, para la realización de esta etapa se empleó híbrido de los dos procedimientos. En primer

lugar, haciendo uso del primer procedimiento, a partir del análisis y la descripción de cada una de las variables de la MIB estándar así como de la definición teórica y las características de cada una de las fallas se estableció una primera asociación Falla-Variables MIB.

El segundo procedimiento, se emplea como método de comprobación; partiendo de la asociación teórica previa se realizaron pruebas de monitorización para analizar el comportamiento de las variables MIB seleccionados frente a la presencia de la falla y se seleccionaron los que presentaban mayor variabilidad.

Los criterios tenidos en cuenta para la selección inicial de las variables son:

- Relación entre la definición estándar de la variable y las causas o consecuencias de la falla, que aporten información crítica para la gestión, especialmente la asociada con el estado y desempeño de la red.
- Con el fin de mantener el carácter general del trabajo, se tomaron variables que hacen parte de los grupos estándar de la MIB, ya que en ocasiones los grupos privados, son limitados a los dispositivos y los fabricantes.
- El protocolo SNMP (Simple Network Management Protocol) en sus distintas versiones soporta varias clases o sintaxis de objetos usados para representar información diferente. Se seleccionaron las variables que manejan las siguientes sintaxis: INTEGER, COUNTER, GAUGE y TIME TICKS, ya que ofrecen un formato adecuado que permite presentar y manejar la información de una forma directa y simple para la monitorización y su posterior análisis. Variables del tipo Octect String, Object Identifier, entre otras, presentan grandes dificultades a la hora de obtener información cualitativa a partir de ellas.
- Elegir los objetos que proporcionen la información de la forma más general posible para descartar aquellos que la repitan de manera total o parcial y así evitar la redundancia de información entre variables.

4.1.2.1 Procedimiento de Selección de Variables

Después de fijar los criterios base, hay que tener en cuenta que este proceso de selección está orientado a la búsqueda de las variables MIB que permitan obtener información clave sobre los síntomas que preceden y describen la presencia de las fallas seleccionadas en un segmento de red específico.

Ya que las fallas seleccionadas, Congestión y Tormenta Broadcast, están relacionadas con variaciones en los niveles de tráfico dentro de la red, las variables que se eligieron

son aquellas que almacenan información sobre aumentos exagerados en los niveles de tráfico, número de paquetes recibidos y transmitidos, y transmisión excesiva de paquetes de difusión respectivamente.

Dentro de los grupos estándar de la MIB existen gran cantidad de variables que pueden ser fácilmente asociadas a los escenarios de estas fallas, por tal razón el análisis de las definiciones de cada una de ellas se hizo de forma estricta, con el fin de escoger sólo aquellas variables que aportaran información significativa sobre las fallas y para evitar la redundancia de información.

Una vez realizada la primera revisión teórica a partir de la descripción de cada una de las variables se obtuvieron alrededor de 70. Después de un análisis exhaustivo de sus propiedades y teniendo en cuenta que las variables con información relevante asociada a las fallas bajo estudio son las pertenecientes a los grupos representativos de protocolos de capas superiores y los asociados con las interfaces de red, se puede afirmar que entre estos grupos los mas importantes son: Interfaces, IP, ICMP, SNMP y RMON; siguiendo esta premisa se llego a la preselección de variables que permitió reducir el grupo inicial a 30 variables como se ilustra en las siguientes tablas.

Tabla 6. Grupo inicial de variables de la MIB asociadas a la falla Tormenta Broadcast

TORMENTA BROADCAST		
NOMBRE	**OID**	**DESCRIPCIÓN**
IfInNUcastPkts	1.3.6.1.2.1.2.2.1.12	Muestra el número de paquetes entregados por esta subcapa a una superior, los cuales fueron direccionados a una dirección Broadcast o multicast en esta subcapa.
IfOutNUcastPkts	1.3.6.1.2.1.2.2.1.18	Muestra el número total de paquetes que los protocolos de capas altas solicitaron para ser transmitidos y que fueron direccionados a una dirección broadcast o multicast en esta subcapa; incluyendo aquellos que fueron descartados o no

		enviados.
EtherStats BroadcastPkts	1.3.6.1.2.1.16.1.1.1.6	Muestra el número total de paquetes bien formados recibidos que fueron dirigidos a la dirección broadcast. No se incluyen los paquetes multicast.
Rip2GlobalQueries	1.3.6.1.2.1.23.1.2	Indica el número de respuestas enviadas a consultas RIP desde otros sistemas.

Tabla 7. Grupo inicial de variables de la MIB asociadas a la falla de Congestión

CONGESTIÓN		
NOMBRE	**OID**	**DESCRIPCIÓN**
IfInOctets	1.3.6.1.2.1.2.2.1.10	Muestra el número total de octetos recibidos en la interfaz, incluyendo caracteres de trama (frame).
IfInUcastPkts	1.3.6.1.2.1.2.2.1.11	Muestra el número de paquetes entregados por esta subcapa a una superior, los cuales no fueron direccionados a una dirección Broadcast ni multicast en esta subcapa.
IfInDiscards	1.3.6.1.2.1.2.2.1.13	Muestra el número de paquetes entrantes que fueron elegidos para ser descartados aunque no se hayan detectado errores, para evitar que sean entregados a un protocolo de capa superior. Una posible razón para descartar tales paquetes es la liberación de espacio en los buffer.
IfInErrors	1.3.6.1.2.1.2.2.1.14	Para interfaces orientadas a paquetes, muestra el número de paquetes de entrada que contienen errores, evitando su entrega a protocolos de capa superior. Para interfaces orientadas a caracteres o de longitud fija, muestra el número de unidades de transmisión de entrada que contienen errores,

		evitando su entrega a protocolos de capa superior.
IfOutOctets	1.3.6.1.2.1.2.2.1.16	Muestra el número total de octetos transmitidos fuera de la interfaz incluyendo caracteres de tramas.
IfOutUcastPkts	1.3.6.1.2.1.2.2.1.17	Muestra el número total de paquetes que los protocolos de capas altas solicitaron para ser transmitidos y que no fueron direccionados a una dirección broadcast o multicast en esta subcapa; incluyendo aquellos que fueron descartados o no enviados.
IfOutDiscards	1.3.6.1.2.1.2.2.1.19	Muestra el número de paquetes de salida que fueron elegidos para ser descartados aunque no se hayan detectado errores, para evitar que sean transmitidos. Una posible razón para descartar tales paquetes es la liberación de espacio en los buffer.
IfOutQLen	1.3.6.1.2.1.2.2.1.21	Muestra la longitud de la cola de paquetes de salida (en paquetes).
IpInReceives	1.3.6.1.2.1.4.3	Indica el número total de datagramas de entrada recibidos desde las interfaces, incluyendo aquellos recibidos con errores.
IpForwDatagrams	1.3.6.1.2.1.4.6	Indica el número de datagramas de entrada para los que esta entidad no fue su destino IP final, como resultado de esto se hizo el intento de encontrar una ruta para reenviarlos a su destino final. En entidades que no actúan como routers IP, este contador incluirá solo aquellos paquetes que fueron enrutados desde el origen a través de esta entidad, y el procesamiento de la opción de enrutamiento desde el origen fue exitoso.
IpInDiscards	1.3.6.1.2.1.4.8	Indica el número de datagramas IP de entrada para los que no hubo problemas al prevenir su procesamiento constante, pero que fueron descartados Este contador no incluye ningún datagrama descartado mientras espera su reensamble.

IpInDelivers	1.3.6.1.2.1.4.9	Indica el número total de datagramas de entrada entregados satisfactoriamente a los protocolos IP de usuario (incluyendo ICMP).
IpOutRequest	1.3.6.1.2.1.4.10	Indica el número total de datagramas cuyos protocolos IP de usuario local (incluyendo ICMP) suplieron las peticiones de IP para transmisión. Este contador no incluye ninguna datagrama contado en ipForwDatagrams.
IpOutDiscards	1.3.6.1.2.1.4.11	Indica el número de datagramas de entrada para los que no hubo problemas al prevenir su transmisión a su destino, pero que fueron descartados (por falta de espacio en los buffer).
IpFragCreates	1.3.6.1.2.1.4.19	Indica el número de fragmentos de datagramas IP que han sido generados como resultado de la fragmentación en esta entidad.
IpRoutingDiscards	1.3.6.1.2.1.4.23	Muestra el número de entradas de enrutamiento que fueron escogidas para ser descartadas aun siendo validas. Una razón para descartar tales entradas podría ser para liberar espacio en los buffer para otras entradas de enrutamiento.
IcmpInSrc Quenchs	1.3.6.1.2.1.5.6	Indica el número de mensajes ICMP de fuente desconectada recibidos
IcmpOutSrc Quenchs	1.3.6.1.2.1.5.19	Indica el número de mensajes ICMP de fuente desconectada enviados.
TcpInSegs	1.3.6.1.2.1.6.10	Indica el número total de segmentos recibidos, incluyendo aquellos recibidos con errores. Esta cuenta incluye los segmentos recibidos en las conexiones establecidas actualmente.
SnmpInPkts	1.3.6.1.2.1.11.1	Muestra el número total de mensajes entregados a una entidad SNMP desde el servicio de transporte.
SnmpOutPkts	1.3.6.1.2.1.11.2	Muestra el número total de mensajes SNMP que fueron aprobados desde una entidad de protocolo SNMP hasta el servicio de transporte.
SnmpInTraps	1.3.6.1.2.1.11.19	Muestra el número total de PDUs Traps SNMP que han sido aceptadas y procesadas por la

		entidad de protocolo SNMP.
SnmpOutTraps	1.3.6.1.2.1.11.29	Muestra el número total de PDUs Traps SNMP que han sido generadas por la entidad de protocolo SNMP.
EtherStatsOctets	1.3.6.1.2.1.16.1.1.1.4	Muestra el número total de octetos de datos (incluyendo aquellos en paquetes defectuosos) recibidos en la red (excluyendo los bits de entramado pero incluyendo octetos FCS). Esta variable puede ser usada como un estimado razonable de la utilización de Ethernet.
EtherStatsPkts	1.3.6.1.2.1.16.1.1.1.5	Muestra el número total de paquetes (incluyendo los paquetes defectuosos, paquetes de broadcast, y paquetes multicast) recibidos.
EtherStats Collisions	1.3.6.1.2.1.16.1.1.1.13	Indica el número total de colisiones mejor estimado (más preciso) en este segmento Ethernet. El valor retornado dependerá de la localización del sondeo RMON.

4.2 Generación de fallas

Una vez identificadas las fallas que se deseaban detectar y seleccionadas las variables de la MIB asociadas a cada una de ellas, se procede con la etapa de generación de fallas. Esta etapa tiene dos objetivos fundamentales. El primero es la simulación de los posibles escenarios de falla representativos de cada una de las condiciones seleccionadas en la etapa anterior, mientras el segundo es el registro de los datos necesarios para la etapa de clasificación.

Teniendo en cuenta que se trataba de un primer trabajo sobre el tema y considerando la complejidad que añadía al problema la inestabilidad del tráfico dentro de una red real, durante la etapa de generación de fallas se mantuvo un ambiente controlado. Las pruebas se realizaron a nivel de laboratorio simulando las condiciones de operación de un segmento típico de red Ethernet real. La ventaja ofrecida por el trabajo a nivel de laboratorio fue que permitía conocer el momento exacto en el que se presentaba cada falla y se podían variar aspectos relacionados con la duración, la periodicidad y los valores pico alcanzados, entre otros.

Existen diferentes aspectos que se deben tener en cuenta para la definición de las condiciones precisas de simulación. Un punto clave en esta etapa es la selección de las herramientas a utilizar tanto para la generación de las fallas como para la monitorización de las variables de la MIB. Se evaluaron diferentes opciones y se empleó una matriz de comparación que contenía los criterios de selección establecidos de acuerdo con las necesidades.

4.2.1. Evaluación y Selección de la Herramienta de monitorización

Un Monitor de Tráfico para Redes de Computadores es un instrumento que entrega datos acerca de la red en la cual está conectado. Estos datos pueden ser entregados en diversas formas, dependiendo del fin con el cual el monitor es diseñado.

Para este trabajo, la herramienta de monitorización debe soportar el protocolo SNMP para que proporcione la información almacenada en las variables de la MIB.

Para la selección del software se tienen en cuenta los siguientes criterios:

- La herramienta software debe contener en su base de datos, como mínimo los grupos estándar de la MIB mencionados en el capítulo 2.

- Debe permitir establecer la frecuencia de sondeo de las variables, interrogar distintas variables simultáneamente, visualizar el sondeo de manera gráfica y además tener la capacidad de almacenar los datos para su posterior manipulación y análisis.

- Se deben tener en cuenta aquellas herramientas adicionales que el software seleccionado ofrezca y que puedan ayudar al administrador de la red.

- Se prefieren las herramientas con un entorno gráfico agradable y de fácil manejo para el usuario.

Teniendo en cuenta estos criterios y después de analizar otras herramientas como Network View, SolarWinds y ManageEngine OpUtils, se decidió seleccionar SOLARWINDS como la herramienta para llevar a cabo la monitorización de las variables, por su agradable presentación y facilidad de configuración para la monitorización y el registro de los datos; además permite fácilmente acceder a

cualquier herramienta complementaria a través de enlaces en la mayoría de sus aplicaciones.

Con esto se valida la selección documentada en el capítulo 3, al elegir esta herramienta como la más apropiada para la realización de las tareas de gestión dentro de la red de la Universidad.

 **SOLARWINDS Engineer´s Edition 5.5**. Junio 2003. Corporación Solarwinds.

Este aplicativo está conformado por varias herramientas dedicadas a la administración, la monitorización y al reconocimiento de la red.

Dentro de sus 9 herramientas, aquellas que brindan información sobre las variables de la MIB y que pueden servir para la monitorización de estas son: el MIB BROWSER y el PERFORMANCE MONITORING.

- **MIB browser**. Incluye un navegador completo de la MIB, llamado de igual forma. Permite explorar el árbol, requerir la información de cualquier OID y modificar remotamente sus valores.

La base de datos de la MIB de SolarWinds contiene más de 1.000 módulos MIB y más de 100.000 OIDs públicos y privados (de fabricante).

Solarwinds incluye otras herramientas que realizan funciones basadas en el protocolo SNMP tales como: MIB Walk, el cual genera una tabla de todas las MIB y OIDs soportadas en un dispositivo específico, Update System MIB, y MIB Viewer.

- **Performance monitoring.** Consta de un conjunto de herramientas que permiten monitorizar el desempeño de dispositivos mediante cálculos basados en información estadística suministrada por las variables de la MIB; en la mayoría de opciones de esta herramienta la información de las variables es transparente para el usuario.

Dentro de este grupo, la herramienta SNMP-Graph permite monitorizar las variables MIB en tiempo real; muestra gráficamente datos de cualquier variable simplemente seleccionando el dispositivo y el OID deseado.

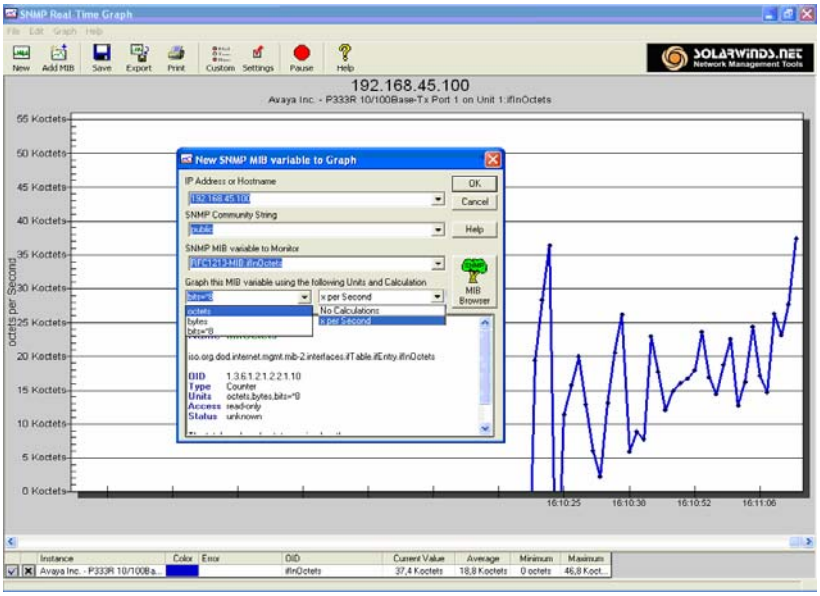


Figura 39. Herramienta gráfica de SOLARWINDS SNMP-Graph.

4.2.2. Evaluación y Selección de la herramienta de Generación de tráfico

El éxito de esta etapa está relacionado en buena parte con la capacidad que tenga la herramienta seleccionada para generar el tráfico característico del las fallas analizadas, siendo este el primer criterio tenido en cuenta para la selección de dicha herramienta. Además de este, se tuvieron en cuenta los siguientes criterios:

1. La capacidad de generar diferentes patrones de tráfico y la posibilidad de modificar parámetros como la carga total a generar, el tamaño y distancia entre paquetes, los tiempos de conexión y los puertos para cada una de ellas.

2. La herramienta debe ofrecer la opción guardar los datos del proceso de generación en formatos que luego puedan ser visualizados fácilmente para su posterior análisis.

3. Se prefirieron herramientas con un entorno gráfico agradable y de fácil manejo para el usuario.

Después de evaluar las anteriores características en las herramientas, se seleccionaron aquellas que funcionan en plataformas Windows XP, ya que esto brinda mayor compatibilidad con todas las aplicaciones con las que se cuenta en el laboratorio y con las herramientas de monitorización seleccionadas.

Al terminar este proceso de selección se determinó utilizar las siguientes herramientas asociadas a cada escenario de falla.

4.2.2.1 Herramientas software seleccionadas para la falla de congestión.

- **Wan killer.** Este programa hace parte del paquete "Miscellaneous" de SolarWinds Professional Edition Ver 5.0.

Es una herramienta de generación de tráfico, que permite definir el porcentaje de ancho de banda del canal a ocupar con el tráfico generado; también permite ajustar el tamaño del paquete generado. Para su utilización se debe seleccionar el protocolo de transporte (TCP o UDP) y el número del puerto destino.

- **Lan Traffic V2.** LanTraffic V2 es un herramienta software para pruebas que permite generación de tráfico UDP y TCP en una red IP. Puede ser configurado con un gran número de parámetros diferentes y soporta múltiples conexiones TCP simultáneas. Esta herramienta está compuesta de dos partes: el emisor y el receptor; gracias a ello es posible medir el RTT (Round Trip Time) en cada conexión parámetro esencial para evaluar el desempeño de una red IP. Se utilizó una versión demo para las pruebas.

- **TFGen V1.0.** Este software permite generar tráfico en la red de área local (LAN); está diseñado para trabajar bajo redes TCP/IP únicamente. Utiliza el protocolo de transporte UDP por lo que requiere al menos un nodo IP de destino. Tiene la capacidad de generar tráfico Multicast y puede generar tráfico con patrones específicos. Esta herramienta es gratuita (freeware).

4.2.2.2 Herramientas software seleccionadas para la falla de tormenta de broadcast.

- **TFGen V1.0.** Como se describió anteriormente, esta herramienta permite dirigir el tráfico generado a direcciones IP multicast y así configurarse para generar broadcast IP a todas las estaciones conectadas al segmento bajo estudio.

- **Formas complementarias de generación.** Otra forma de generar tráfico broadcast, pero de tipo ARP es utilizar aquellas herramientas que realicen funciones de reconocimiento de la red.

Dentro del grupo de herramientas DISCOVERY NETWORK de SolarWinds existen varias opciones para el descubrimiento de la red, que indirectamente se pueden utilizar para la generación de tráfico broadcast ARP, al ejecutar cualquiera de estas herramientas tales como: **IP Network Browser, Ping Sweep, SNMP Sweep** y **MAC Address Discovery.**

Estas herramientas funcionan realizando un barrido en la subred que ocasiona la consulta de cada dirección IP, determinando cuales son las estaciones que están conectadas, y sus respectivos nombres de dominio o direcciones MAC; además informa si estas estaciones soportan el protocolo SNMP.

Para realizar estas tareas la aplicación produce una gran cantidad de tráfico broadcast que podemos aprovechar para generar este tipo falla.

En la tabla 8 se presenta una comparación de las características más sobresalientes que resumen las utilidades y las limitaciones de las diferentes herramientas de generación analizadas.

Tabla 8. Matriz de Comparación Software de Generación de tráfico

CARACTERISTICAS		WAN KILLER	TFGEN V1.0	LANTRAFFIC V2
TIPO DE PAQUETE		UDP,TCP	UDP,TCP	UDP,TCP
DEFINICION DE PUERTO DE SALIDA		SI	SI	SI
DEFINICION DE PUERTO DE ENTRADA				SI
DEFINICION DE ANCHO DE BANDA		SI	SI	SI
DEFINICION DE TAMAÑO DE PAQUETES	CONSTANTE	SI, % DE ANCHO DE BANDA	SI, % DE ANCHO DE BANDA	SI
	ALEATORIO			SI
	ALTERNADO			SI
	INCREM/DECREM			SI
PATRON DE TRAFICO	CONSTANTE	SI, % DE ANCHO DE BANDA	SI, % DE ANCHO DE BANDA	SI
	LEY MATEMATICA			SI
	ARCHIVO			SI
	ALEATORIO		SI	SI
	PERIODICO		SI	SI
RETARDO INTER-PAQUETE	CONSTANTE	SI	SI	SI
	ALEATORIO			SI
	ALTERNADO			SI
	INCREM/DECREM			SI
MODO DE RECEPCION		ECHO		ECHO, ABSORBER
MULTIPLES CONEXIONES (IP DESTINOS)				SI
ESTADISTICAS Y PARAMETROS DE TRAFICO (THROUGHTPUT, DATOS, ERRORES).				SI

4.2.3. Escenarios de falla

En el desarrollo de las pruebas asociadas a esta etapa se pueden diferenciar dos grandes actividades, la monitorización de las variables de la MIB y la generación de tráfico que permita implementar los escenarios de falla previamente seleccionados.

Teniendo en cuenta que se trataba de un primer trabajo sobre el tema y considerando la complejidad que se añadía al problema por la inestabilidad del tráfico dentro de la red, durante la etapa de generación de fallas se eligió un segmento de red Ethernet pequeño, 10 estaciones en promedio y un volumen de trafico relativamente estable. La ventaja ofrecida por el trabajo a nivel de laboratorio fue que permitía conocer el momento exacto en el que se presentaba cada falla.

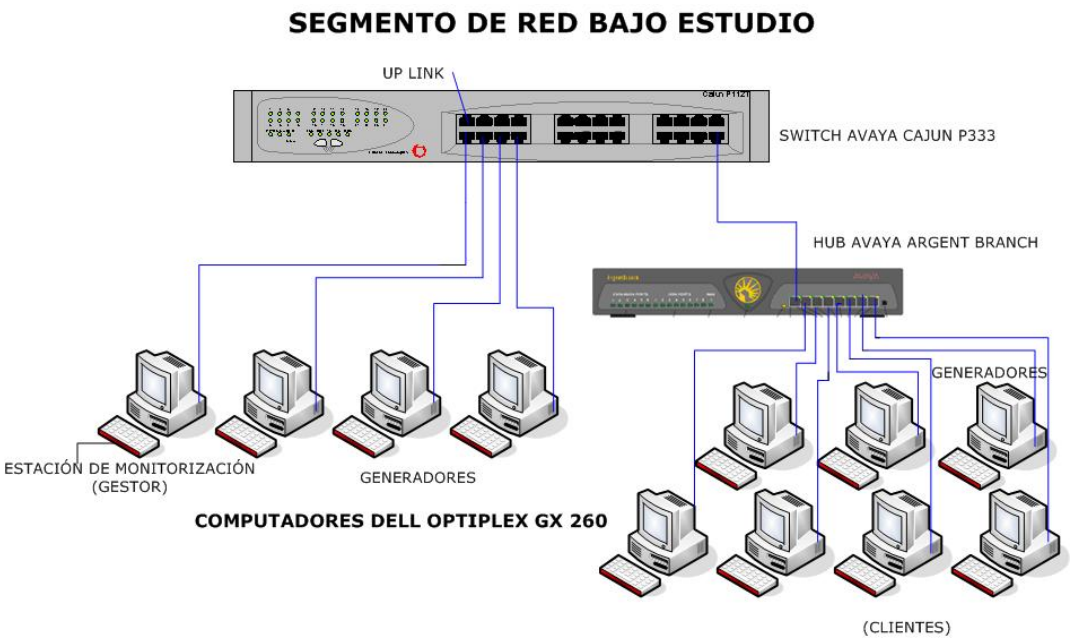


Figura 40. Configuración empleada durante la etapa de simulación

Como se mencionó anteriormente debido a las ventajas ofrecidas por cada una de las herramientas de generación de tráfico analizadas, se decidió emplear una combinación de ellas. Estos aplicativos fueron instalados en cuatro estaciones que hicieron las veces de generadores dentro del esquema de simulación. Dos de ellas se encontraban fuera del segmento y dos dentro. Se dispuso una estación única de monitorización en la cual se instaló el software de monitorización de variables SNMP ofrecido por SolarWinds.

Para desarrollar las pruebas se definieron dos condiciones. Una condición normal que se relacionó con el tráfico presente durante la operación normal del segmento, es decir cuando los usuarios habituales de la sala se encontraban realizando las actividades relacionadas con sus respectivos trabajos y una condición anómala que se presentaba en el momento que se activaban los generadores de tráfico.

Se realizaron diferentes pruebas y tomas de datos variando la duración, en nivel y la frecuencia de aparición de cada una de las fallas, se monitorizaron las variables previamente asociadas a cada condición y algunas otras ya eliminadas con el fin de descartar errores en la selección y perdida de información. En esta etapa se corroboró visualmente que las variables elegidas realmente reflejaban los cambios esperados.

4.2.3.1 Principales aspectos relacionados con la monitorización

Uno de los factores que se debe tener en cuenta y que debe ser definido como paso previo a la realización de las pruebas es la frecuencia de sondeo de los dispositivos. Este valor generalmente está limitado[25] por la capacidad de almacenamiento del equipo que realiza el sondeo y por el impacto que este proceso genere sobre la red.

Al seleccionar esta frecuencia de sondeo autores como Stallings[9] recomiendan intervalos muy cortos con el fin de detectar y responder adecuadamente a las fallas que se presenten en la red. Sin embargo obtener esta información a partir de los dispositivos administrables con una frecuencia muy alta puede convertirse en un problema debido al incremento de tráfico y al consumo de recursos del dispositivo por parte de las operaciones de sondeo SNMP[13].

En el caso particular de la detección de fallas se debe tener presente que de acuerdo con el intervalo de muestreo empleado, se debe definir la duración de la condición de falla para que pueda ser detectada, lo cual condiciona un poco el uso de intervalos de muestreo muy largos.

Ya que no existe un consenso sobre este aspecto en la literatura existente y teniendo en cuenta las limitaciones mencionadas, el tiempo promedio de sondeo en una red de tamaño mediano esta alrededor de los 15 minutos[28]; siguiendo estos lineamientos y teniendo en cuenta las condiciones del segmento de red bajo estudio, se decidió realizar el sondeo de los dispositivos administrables que hacen parte de la prueba con frecuencias de 2, 5 y 10 minutos para obtener un volumen de información suficiente sobre el comportamiento de las variables MIB seleccionadas. De esta forma se asegura la adquisición de datos que permitan establecer un nivel de detección adecuado.

Una vez definida la frecuencia de sondeo se deben establecer el número y tipo de campañas de tomas de datos que se efectuarán y bajo qué condiciones, con el fin de limitar la información adquirida mediante el proceso de sondeo, sólo a aquella que resulte útil para cumplir los objetivos del trabajo.

Muchos autores recomiendan realizar una monitorización previa del segmento de red bajo condiciones normales de operación, con el fin de tener un conjunto de datos de referencia que podrían ser útiles al momento de analizar el comportamiento estadístico de las variables MIB, pero la naturaleza dinámica del tráfico en las redes de datos,

conduce a que su desempeño sea variante en el tiempo[17]. Esto nos indica que la utilización de una red varía con la hora del día, el día de la semana y la temporada del año, y de esta manera cualquier sistema o herramienta que quiera efectuar una detección de condiciones de falla adecuadamente debe tener en cuenta la naturaleza variante de las condiciones de red y estar en capacidad de adaptarse a estos cambios.

Buscando la adaptación a estas condiciones se decidió realizar la monitorización teniendo en cuenta las frecuencias de sondeo definidas, en el horario laboral, para apreciar la incidencia de las condiciones de falla creadas, y tener una visión clara de cómo se reflejan estos cambios en las variables de la MIB.

4.2.3.2 Generación de tráfico

Para cumplir con el objetivo de implementar los escenarios de falla seleccionados la segunda actividad a definir es la generación de tráfico.

Esta actividad consiste en la inyección de tráfico en el segmento de red bajo estudio haciendo uso de las herramientas software seleccionadas. El objetivo es recrear las condiciones específicas que según la teoría caracterizan cada una de las fallas seleccionadas y observar su efecto sobre las variables MIB estudiadas.

Para la realización de esta tarea y con el fin de emular con precisión las condiciones particulares de cada falla, las herramientas de generación deben ser configuradas teniendo en cuenta los siguientes parámetros: patrón de tráfico, tamaño de paquete, volumen de tráfico generado y tiempo que dura la generación.

- **Patrón de tráfico.** Teniendo en cuenta las condiciones del segmento de red de la prueba y las características de las fallas seleccionadas, se decidió que los patrones de generación más indicados son tráfico continuo y constante, y tráfico continuo y aleatorio, ya que de esta forma se pueden generar los niveles de tráfico que dan origen a la congestión del segmento de red y al volumen de paquetes de difusión suficiente para crear una tormenta de broadcast.

- **Tamaño de paquete.** Este parámetro puede ser utilizado para regular la cantidad de tráfico generado; a menor tamaño el volumen de paquetes generados será mayor. Esta característica es especialmente útil al momento de generar la falla de congestión, ya que cada uno de estos paquetes origina un paquete de respuesta y el procesamiento de cada una de estas peticiones, produce un alto consumo de los

recursos de los dispositivos de red, así como la ocupación de los enlaces por la gran cantidad de paquetes que se encuentran circulando en el segmento.

Teniendo en cuenta estas situaciones y siguiendo los tamaños de paquete establecidos en el estándar de Ethernet[19] se eligieron tamaños de paquete en rangos que están entre 180 y 500 bytes como tamaño pequeño; y cercanos a 1518 como tamaño grande.

- **Volumen de tráfico generado.** Su importancia radica en que las fallas seleccionadas para este estudio están directamente relacionadas con la cantidad de tráfico presente en el segmento de red y en como se afecta el desempeño de los dispositivos que hacen parte de éste. Como se puede advertir el volumen a generar está relacionado directamente con los dos parámetros anteriores y por lo tanto deben ser establecidos en conjunto y teniendo en cuenta las características del segmento de red en particular. Las herramientas de generación disponibles permiten establecer el volumen de tráfico a generar como un porcentaje de la capacidad teórica de los enlaces que hacen parte del segmento de red; de esta manera se puede definir un porcentaje de utilización que implique una condición anómala.

- **Duración de la generación.** Del tiempo que dure la generación dependerán los efectos que se produzcan en el desempeño del segmento de red y que conllevan al surgimiento de las fallas. Además, el interés no radica sólo en crear la falla sino en sostenerla el suficiente tiempo para que se vea reflejada en el comportamiento de las variables de la MIB.

Para que la falla pueda visualizarse en un número suficiente de muestras del proceso de monitorización y teniendo en cuenta las frecuencias de sondeo elegidas de 2, 5 y 10 minutos se decidió establecer como duración de la sesión de generación de tráfico un tiempo promedio de 15 minutos.

Teniendo en cuenta que el desempeño y consumo de recursos por parte del sistema de clasificación depende del número de variables seleccionadas, la premisa era que el número de variables asociadas a cada falla fuera mínimo. Como otra opción de filtrado que permitía reducir este número, se aplicaron criterios particulares definidos por las

[19] El tamaño de paquete del estándar Ethernet está entre 64 y 1518 bytes.

limitaciones o características de los dispositivos hardware y herramientas de software seleccionadas para la monitorización de variables MIB.

Con la ayuda de la herramienta MIB Walk de Solarwinds se pudo determinar cuáles variables de la MIB eran soportadas por el dispositivo administrable asociado al segmento, en este caso un Switch Cajun P333R marca Lucent Technologies; los resultados obtenidos con dicha herramienta muestran que existen algunas variables seleccionadas previamente que no son soportadas por el dispositivo; por ello se hizo necesario realizar un ajuste al grupo de variables seleccionadas inicialmente.

Se realizaron distintas pruebas preliminares donde se monitorizaban las variables preseleccionadas y se buscaba analizar su comportamiento ante la presencia inducida de las fallas. De esta manera se descartaron algunas otras que no presentaban una variabilidad significativa. Una vez realizado este proceso y teniendo en cuenta los criterios anteriores se obtuvo un número bastante razonable de variables por cada falla como se muestra en las tablas 9 y 10

Tabla 9. Variables Asociadas a la Falla Tormenta Broadcast

Nombre	OID
IfInNUcastPkts	1.3.6.1.2.1.2.2.1.12
IfOutNUcastPkts	1.3.6.1.2.1.2.2.1.18

Tabla 10. Variables Asociadas a la Falla Congestión de Red

Nombre	OID
IfInUcastPkts	1.3.6.1.2.1.2.2.1.11
IfOutUcastPkts	1.3.6.1.2.1.2.2.1.17
EtherStatsOctets	1.3.6.1.2.1.16.1.1.1.4
IfInOctets	1.3.6.1.2.1.2.2.1.10
IfOutOctets	1.3.6.1.2.1.2.2.1.16

Entre el conjunto de variables planteados inicialmente existen tres que no aportan información específica sobre el comportamiento del tráfico en la red, pero son

variables que indican la presencia de fallas y son muy útiles para complementar la información suministrada por las variables que se seleccionaron.

De esta forma se tendrá en cuenta el comportamiento de estas variables como una referencia para las pruebas a realizarse. Estas variables auxiliares se muestran en la siguiente tabla.

Tabla 11. Variables de la MIB auxiliares

Nombre	OID
IfInDiscards	1.3.6.1.2.1.2.2.1.13
IfInErrors	1.3.6.1.2.1.2.2.1.14
EtherStatsCollisions	1.3.6.1.2.1.16.1.1.1.13

4.3 Detección y clasificación de fallas

Como resultado de las campañas de monitorización realizadas durante la etapa de generación de fallas se obtuvieron los datos que fueron usados para la clasificación. En total se dispuso de 941 muestras que corresponden a aproximadamente 32 horas de monitorización, estas medidas fueron hechas durante las horas laborales a lo largo de 4 días empleando una frecuencia de sondeo de 2 minutos. El segmento monitorizado corresponde al Laboratorio de Redes de la escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones, empleada para la realización de las actividades del grupo de investigación en Conectividad y Procesado de Señal, por tanto el tráfico registrado corresponde al tráfico generado por sesiones HTTP, transferencia de archivos desde y hacia distintos servidores dentro y fuera de la universidad, consultas a servidores de correo y transferencias internas entre las estaciones de la sala entre otras.

Empleando el esquema propuesto para la generación de las fallas se realizaron diversas pruebas de generación de las cuales de obtuvieron los siguientes datos.

Tabla 12. Datos obtenidos de la etapa de generación

Tipo de falla	Número de muestras
Tormenta Broadcast	27
Congestión Entrante	147

Congestión Saliente	155
Datos condición normal	672
Total datos	941

En la Figura 41 se muestra un ejemplo del comportamiento de las variables de la MIB frente a la generación de una falla de tormenta de broadcast. Bajo condiciones normales de operación las dos variables asociadas a la falla (ifOutNuncastPkts , ifInNUcastPkts) se mantienen en un valor cercano a cero, en presencia del generador de tráfico broadcast se ve como estos valores se alteran significativamente. Las zonas correspondientes a la presencia de falla se han encerrado en el recuadro rojo. Una situación similar sucede con la falla de congestión.

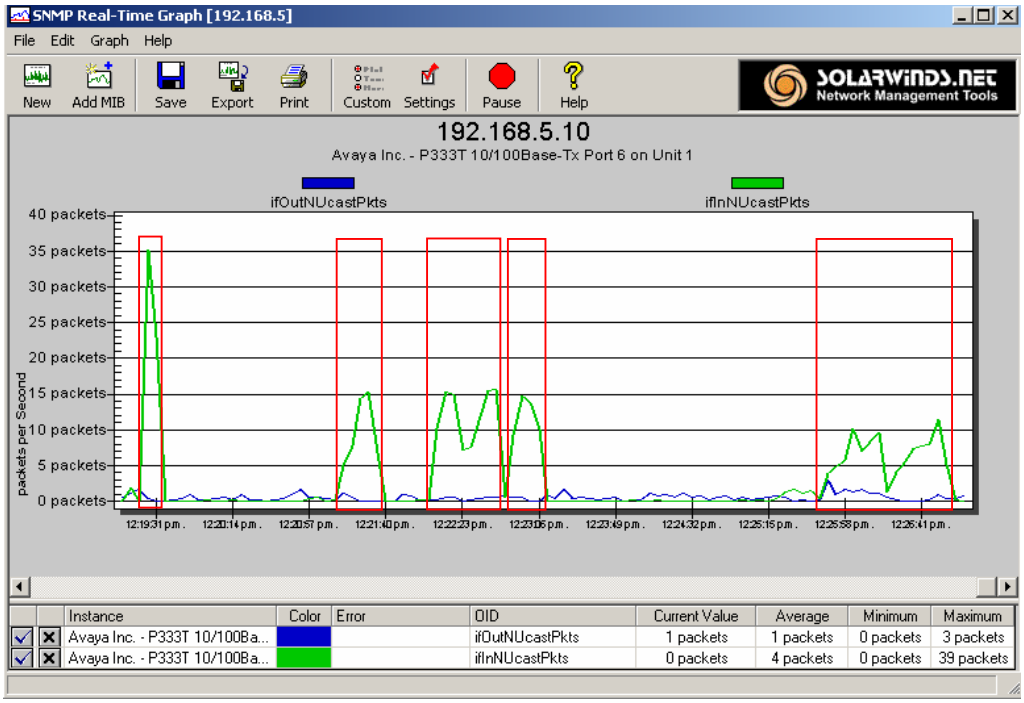


Figura 41. Ejemplo falla tormenta de Broadcast

Debido a que en ocasiones no sólo es importante detectar si se está presentando un incremento en el nivel de tráfico, sino que puede ser bastante útil determinar la fuente de esa sobrecarga, como un primer paso se decidió dividir la falla de congestión en dos grupos: congestión entrante y congestión saliente. Para la congestión entrante, el tráfico asociado fue generado desde las estaciones que se encontraban fuera del segmento, para la congestión saliente se asume el caso contrario, la definición de entrante o saliente se ha dado desde el punto de vista del segmento, es decir si el tráfico entra o sale del segmento. Si se mira desde el punto de vista del dispositivo, la

relación es inversa ya que el tráfico que entra al segmento, sale de la interfaz del dispositivo lo cual lo convierte en tráfico o paquetes salientes y lo mismo sucede con el tráfico saliente del segmento, es aquel que entra a la interfaz por lo tanto se asocia con paquetes entrantes.

Si se analizan los resultados presentados en la tabla 12 se observa que la suma del total de los datos obtenidos con cada una de las condiciones de falla no coincide con el total de datos de falla presentado, esto se debe a que existen instantes en los que se pueden presentar dos o los tres tipos de falla de forma simultánea.

Uno de los elementos cruciales en la gestión de fallas de red es la velocidad con la que se detecta, ubica e identifica el tipo de falla. La gran mayoría de las soluciones propuestas para este fin incluyen el uso de técnicas de inteligencia artificial. En este caso particular teniendo en cuenta las ventajas que ofrece el uso de redes neuronales en el análisis de grandes volúmenes de datos, se ha decidido hacer uso de esta técnica para el desarrollo del sistema de clasificación de fallas.

Con el fin de dar una mejor estructura al sistema, la etapa de clasificación ha sido dividida en dos subetapas, la primera corresponde a la detección de la condición anómala mediante la identificación de una alteración en el nivel de las variables asociadas, y la segunda a la clasificación y asociación de la condición detectada con un tipo de falla específico.

4.3.1. Detección de anomalías

Como paso previo a la asociación de una condición específica con una falla en particular, se ha implementado una etapa de detección. Como se muestra en la figura 42 se trata de un sistema basado en redes Neuronales donde al emplear como entradas el vector de variables MIB asociadas a las diferentes fallas, y dependiendo de los valores de las mismas, el sistema podrá identificar si se presenta una condición de anomalía o una condición normal.

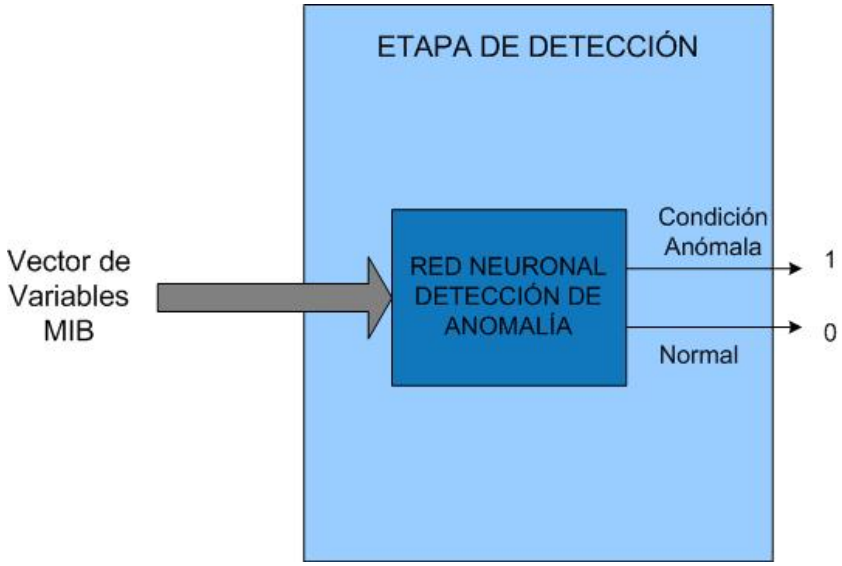


Figura 42. Sistema de Detección de Anomalías

En términos generales la estructura de la red empleada es como sigue: el vector de entrada está conformado por los valores normalizados de las dos variables de la MIB asociadas a la falla de tormenta de Broadcast y las cinco variables asociadas a la falla de congestión, para un total de 7 variables en el vector de entrada. El número de capas ocultas y las neuronas asociadas a cada una de ellas es un aspecto de diseño que no tiene una única respuesta. Para este caso particular este número fue definido mediante prueba y error. Después de varias sesiones de entrenamiento, los mejores resultados se obtuvieron al emplear una capa intermedia con 10 neuronas. Se observó durante el entrenamiento que a medida que el número de capas intermedias se incrementa, puede mejorar el desempeño de la red sin embargo esto implica una mayor duración del entrenamiento.

Se tiene una sola salida y dos posibles valores, un valor mayor o igual a cero punto cinco (0,5) se redondea a 1 y es indicio de que hay una condición anómala, mientras un valor inferior a cero punto cinco (0,5) se redondea a un 0 e indica una condición normal.

4.3.2. Clasificación de fallas

Una vez superada la etapa de detección y teniendo la ventaja de conocer el momento preciso en el que se presenta una condición anómala, gracias al procedimiento de generación de fallos utilizado, se procede a su clasificación. A cada una de las fallas le ha sido asociado un grupo de variables específico. El objetivo es que a partir de la

información aportada por dichas variables el sistema pueda identificar el tipo de falla que se está presentando.

En esta etapa se han explorado fundamentalmente dos esquemas:

Primer esquema

En este primer esquema se empleó una única red que tiene como entradas las siete variables de la MIB asociadas a las fallas bajo estudio y tres neuronas en la capa de salida. Cada una de las salidas puede tomar un valor entre cero y uno; se tiene un comparador gracias al cual si el valor de salida es superior a 0,5 se considera que se está presentando la falla. En la Figura 43 se muestra el esquema empleado.

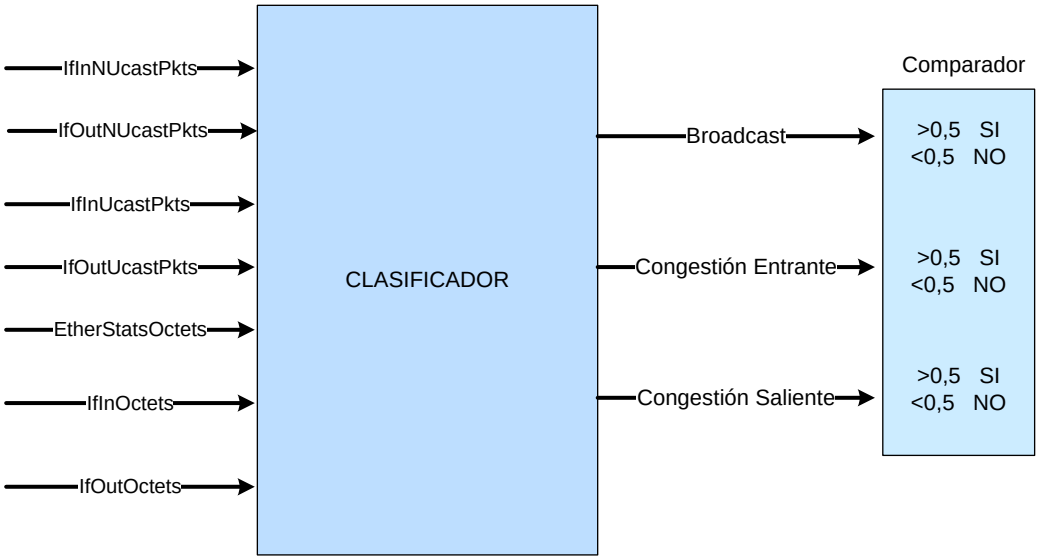


Figura 43. Primer Esquema de clasificación

Segundo esquema

Con el fin de segmentar y simplificar un poco el problema, en este segundo esquema se entrenó una red para cada tipo de falla en este caso una red para la falla Tormenta Broadcast y una para la falla Congestión de Red.

En el caso de la falla Tormenta de Broadcast la red tendrá las mismas siete entradas del esquema anterior y una sola salida, donde nuevamente un valor superior a cero punto cinco (0,5) indica que la condición está asociada a la falla.

Para la falla de congestión de Red como se mencionó anteriormente se hizo una discriminación adicional dependiendo del sentido del tráfico. Para su identificación se

ha empleado una red con dos salidas de dos niveles cada una, un valor mayor que cero punto cinco (0,5) en la salida correspondiente a congestión saliente indica que este es el tipo de falla presente, lo mismo sucede con el caso de la congestión entrante al segmento; si las dos salidas reportan un valor superior a cero punto cinco (0,5) indica que la congestión se esta dando en los dos sentidos; finalmente si los dos valores son cercanos a cero se concluye que la anomalía detectada en la etapa anterior no está asociada a la falla de congestión.

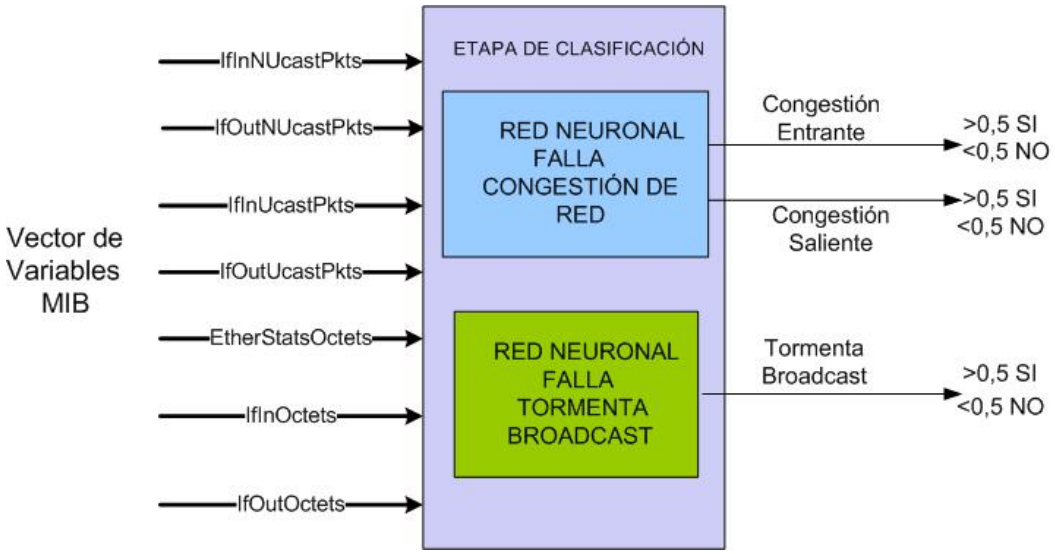


Figura 44. Segundo esquema de clasificación

Con el fin de garantizar que la estructura seleccionada fuera la mejor se realizaron diferentes modificaciones en la arquitectura de la red para cada uno de los esquemas planteados, variando básicamente el número de capas intermedias y el número de neuronas asociadas a cada una de ellas. Los resultados cuantitativos de estas pruebas son presentados más adelante.

4.3.3. Descripción de la Red Neuronal

Las variables de entrada y salida de la red pueden ser binarias o continuas. En este caso particular como parte del preprocesamiento de los datos todas las entradas han sido normalizadas con valores entre cero y uno y por tratarse de una tarea de clasificación se han tomado salidas binarias. La arquitectura empleada es perceptrón multicapa o MLP (Multilayer Perceptron) que ofrece la ventaja de manejar los dos tipos

de variables y el algoritmo de aprendizaje empleado es el denominado backpropagation (retropropagación) o BP.

En un proceso de entrenamiento uno de los factores a tener en cuenta es el error de aprendizaje o la meta de error. Este valor se suele calcular como el error cuadrático medio (MSE) entre los valores de respuesta deseados y aquellos proporcionados por la red sobre el conjunto total de patrones de aprendizaje.

La meta de error es calculada como la sumatoria de la diferencia máxima al cuadrado entre los resultados obtenidos y los resultados esperados y se promedia sobre todas las salidas y todos los patrones de entrada para el aprendizaje.

$$MSE = \frac{1}{NQ}\sum_{n,q=1}^{N,Q}\left(T_n^q - Y_n^q\right)^2$$

Donde T_n^q y Y_n^q representan los valores deseados y obtenidos respectivamente de la n-sima salida de la red cuando se presenta el patron q-simo en la entrada.

Como la red neuronal corresponde a un clasificador se puede aceptar una diferencia máxima (difmax) de cero punto cinco (0,5) entre el valor deseado y el obtenido en una de las salidas cuando se presenta un patrón. A partir de este concepto se pueden establecer dos cotas para la meta de error, la primera de ellas más exigente y la segunda naturalmente más laxa.

La primera corresponde a

$$MSE = \frac{dif\ \max^2}{NQ}$$

Esta condición corresponde a un caso bastante ideal y exigente en el cual todos los patrones de entrada utilizados en el aprendizaje son correctamente clasificados y además todas las salidas obtenidas corresponden exactamente con las salidas esperadas excepto una. Sin embargo gracias al criterio establecido según el cual los valores en el intervalo [0-0,49] se asocian a condición normal y los valores entre [0,5 y 1] con condición de fallo, si la diferencia máxima entre ellas es cero punto cinco (0,5) la salida que no corresponde exactamente con el valor deseado sigue siendo correctamente clasificada.

La situación más flexible es tomada cuando todos los datos de salida quedan en el límite de aceptación, es decir todos los valores que se esperarían en uno se

encuentran en un valor ligeramente superior a 0,5 y los valores esperados en cero toman un valor ligeramente inferior a 0,5. A pesar de la gran diferencia entre los valores deseados y los obtenidos, el resultado de la clasificación sigue siendo correcto para todas las salidas y todos los patrones de entrada. Bajo estas condiciones se tiene que

$$MSE = difmax^2$$

Se buscó que los conjuntos de datos de entrenamiento validación y prueba fueran estadísticamente equivalentes para lo cual se aleatorios el orden en el que se presentan los datos de entrada antes de cada entrenamiento.

Otro de los aspectos fundamentales en las redes neuronales es su capacidad de generalizar a partir de ejemplos. Por generalización se entiende la capacidad de la red de dar una respuesta correcta ante patrones que no han sido empleados durante su entrenamiento.

Del total de 941 datos obtenidos durante las campañas de monitorización realizadas durante la etapa de generación de fallas, se tomó un 60% de ellos para el entrenamiento de la red neuronal, un 20% para la etapa de prueba y el 20% restante para la etapa de validación.

El grupo de datos de prueba se usa para comprobar la eficiencia real o error de generalización de la red. Si la red es entrenada con un error de aprendizaje muy pequeño la capacidad de generalización de la misma se puede degradar. Tras una fase inicial el error de aprendizaje tiende a disminuir monótonamente, mientras que el error de generalización a partir de cierto punto comienza a incrementarse, lo que indica una degradación progresiva del aprendizaje.

Al principio la red se ajusta progresivamente al conjunto de entrenamiento, sin embargo, si en un momento dado la red se ajusta demasiado a las particularidades de los datos empleados para el entrenamiento, el proceso de aprendizaje se convierte en un proceso de memorización y es lo que se conoce como un sobreaprendizaje.

La idea es entrenar la red hasta un punto óptimo donde el error de generalización sea mínimo. El procedimiento consiste en entrenar y validar a la vez para detenerse en el

momento indicado. Por estas razones se debe hacer la distribución de los datos entre entrenamiento, validación y prueba.

4.3.4. Resultados

Como se mencionó anteriormente se realizaron varias sesiones de entrenamiento tanto para la etapa de detección como de clasificación. A continuación se presentan los mejores resultados obtenidos en las dos etapas. Se hicieron pruebas variando el número de capas ocultas y las neuronas en cada una de ellas.

4.3.4.1 Resultados Detección de anomalías

Tabla13. Resultados Etapa de detección

Capas ocultas/Neuronas	**Número de aciertos**			**Número de Errores**			**Porcentaje de desempeño**		
	Ent.	Val.	Test.	Ent.	Val.	Test	Ent.	Val.	Test
1/5	559	188	189	5	0	0	99.1%	100%	100%
1/10	561	187	188	3	1	1	99.4%	99.4%	99.4%
2/5	560	187	188	4	1	1	99.2%	99.4%	99.4%
2/10	559	188	189	5	0	0	99.1%	100%	100%

En la siguiente figura se muestran los resultados obtenidos para el mejor de los casos que según las pruebas realizadas se logra al emplear una capa oculta de cinco neuronas. A pesar de que todas las pruebas produjeron resultados satisfactorios, se toma esta alternativa como la mejor debido a que el uso de más capas intermedias implica un mayor procesamiento y un incremento del tiempo de entrenamiento.

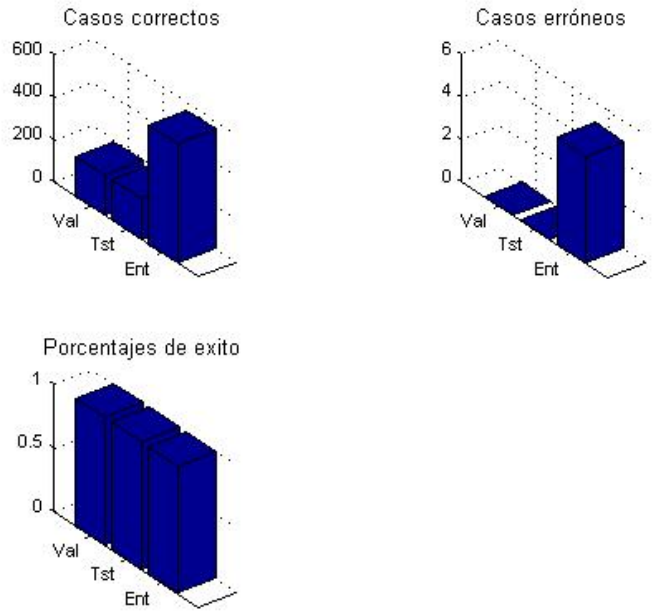


Figura 45. Resultados Entrenamiento Red de Detección de anomalías

4.3.4.2 Resultados sistema de clasificación de fallas

Como se mencionó anteriormente para la clasificación de las fallas se probaron dos esquemas, en el primero de ellos se entrenó una red neuronal para la totalidad de las fallas bajo estudio (Tormenta de Broadcast, Congestión Entrante y Congestión Saliente). A pesar de que los resultados obtenidos son bastante buenos, con el fin de descartar la posibilidad de mejorar el desempeño el sistema se probó un segundo esquema donde se entrenó una red para la tormenta de Broadcast y otra para la falla de congestión. Los resultados obtenidos se presentan a continuación.

En esta etapa, solo se trabaja con los datos que en la etapa de detección han sido asociados a una condición de anomalía, por esta razón se ha reducido el número de datos de entrenamiento de novecientos cuarenta y uno (941) a doscientos sesenta y nueve (269). Los datos restantes corresponden a condiciones de operación normal.

Primer esquema

La arquitectura de la red empleada corresponde a un perceptron multicapa con siete neuronas en la capa de entrada, dos capas ocultas de 15 neuronas cada una y tres neuronas en la capa de salida. Como se muestra en la tabla 14, se empleó un total de 161 datos para la etapa de entrenamiento, 55 para validación y 53 para la etapa de

prueba. En este caso solo se presenta una configuración ya que se considera que los resultados

Tabla 14. Red única para clasificación de fallas

Falla	Número de aciertos			Número de Errores			Porcentaje de desempeño		
	Ent.	Val.	Test.	Ent.	Val.	Test	Ent.	Val.	Test
Tormenta Broadcast	161	55	53	0	0	0	100%	100%	100%
Congestión Entrante	158	54	50	3	0	3	98.14%	100%	94.34%
Congestión Saliente	160	54	50	1	1	3	99.38%	98.18%	94.34%

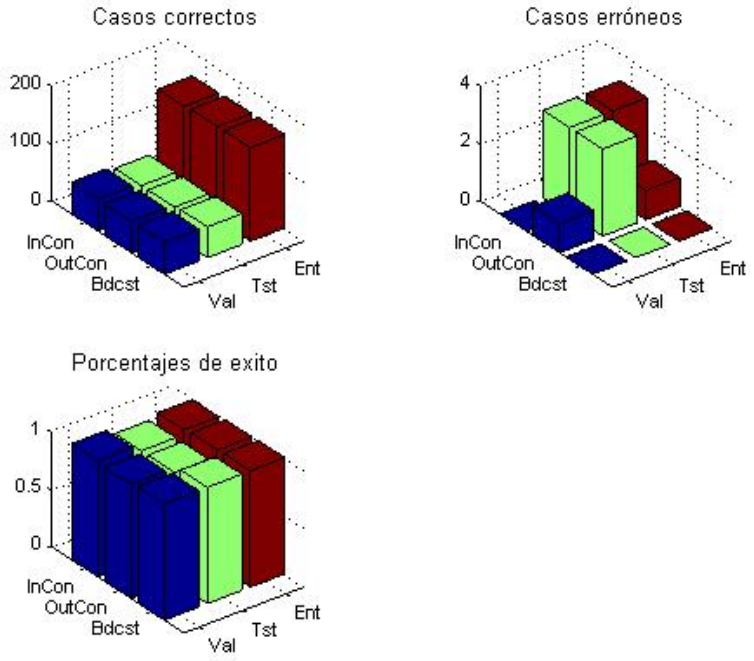


Figura 46. Resultados Red Única para Clasificación

Segundo esquema

En esta etapa se entrenaron dos redes, una para la falla de tormenta Broadcast y otra para la falla de congestión, la cual como ya se ha mencionado se encuentra dividida en congestión entrante y congestión saliente. Los resultados se presentan por tipo de falla. La red empleada para la falla de tormenta Broadcast tiene una salida que puede tomar dos valores para indicar si la falla detectada corresponde con la de tormenta de

broadcast o no. Por su parte, para la falla de congestión se empleó un red con dos salidas un valor superior a cero punto cinco (0,5) en la primera salida indica que la falla detectada corresponde con la de congestión entrante y de igual manera un valor superior a cero punto cinco (0,5) en la segunda salida indica que la falla se ha clasificado como de congestión saliente del segmento.

Tabla 15. Tormenta de Broadcast

Capas ocultas/Neuronas	**Número de aciertos**			**Número de Errores**			**Porcentaje de desempeño**		
	Ent.	Val.	Test.	Ent.	Val.	Test	Ent.	Val.	Test
1/5	159	55	53	2	0	0	98.7%	100%	100%
1/10	160	54	52	1	1	1	99.3%	98.18%	98.11%
2/5	160	54	52	1	1	1	99.38%	98.18%	98.11%
2/10	159	54	52	2	1	1	99.38%	98.18%	96.23%

Tabla 16. Congestión Entrante

Capas ocultas/Neuronas	**Número de aciertos**			**Número de Errores**			**Porcentaje de desempeño**		
	Ent.	Val.	Test.	Ent.	Val.	Test	Ent.	Val.	Test
1/5	158	54	52	3	1	1	98.14%	98.18%	98.11%
1/10	157	54	52	4	1	1	97.52%	98.18%	98.11%
2/5	158	54	52	3	1	1	98.14%	98.18%	98.11%
2/10	157	55	51	4	0	2	97.52%	100%	96.23%

Tabla 15. Congestión Saliente

Capas ocultas/Neuronas	**Número de aciertos**			**Número de Errores**			**Porcentaje de desempeño**		
	Ent.	Val.	Test.	Ent.	Val.	Test	Ent.	Val.	Test
1/5	161	55	53	0	0	0	100%	100%	100%
1/10	161	55	53	0	0	0	100%	100%	100%
2/5	161	55	53	0	0	0	100%	100%	100%
2/10	160	55	53	1	0	0	99.38%	100%	100%

4.3.4.3 Discusión de resultados

En las tablas anteriores se presentan los resultados del sistema propuesto tanto para la etapa de detección como para la etapa de clasificación.

Se debe resaltar que los resultados obtenidos con los dos esquemas son altamente satisfactorios para un sistema de clasificación. Como criterio para detener el

entrenamiento se tomo el porcentaje de efectividad logrado con los datos de prueba ya que a diferencia de los datos de entrenamiento y validación, estos corresponden a aquellos datos que nunca han sido vistos por la red, es decir miden el desempeño del sistema ante nuevas entradas. Como se observa en las tablas de resultados, en todos los casos la meta se cumplió y los porcentajes de desempeño se encuentran cercanos al 100%.

La casilla de porcentaje de desempeño presente en las tablas de resultados, corresponde al porcentaje dado por el número de aciertos con relación al número total de datos en cada uno de los casos. Este es el parámetro tenido en cuenta para determinar cual es la mejor configuración. Las configuraciones empleadas difieren simplemente en el número de capas ocultas y el número de neuronas en cada una de ellas.

Haciendo un análisis cuantitativo de dichos resultados se puede concluir que: para la etapa de detección los mejores resultados se obtienen al emplear una capa oculta con cinco neuronas y el porcentaje de desempeño tomando como referencia los datos de prueba es 100%.

Para la etapa de clasificación como se mencionó anteriormente se plantearon dos esquemas. Un primer esquema donde se empleó una única red para la clasificación de la falla tormenta de broadcast y congestión en sus dos versiones. En este caso se presentaron los resultados obtenidos para la mejor configuración lograda al emplear dos capas ocultas de quince neuronas cada una y se obtuvo un porcentaje de desempeño de 100% para la falla de tormenta de broadcast y un 94,34% en la clasificación de congestión entrante y congestión saliente nuevamente tomando como referencia los datos de prueba.

En el segundo esquema se planteó el uso de dos redes de clasificación una por cada tipo de falla. Se han presentado resultados para distintas configuraciones donde nuevamente se varían el número de capas ocultas y neuronas asociadas. En este caso los mejores resultados fueron obtenidos para la falla tormenta de broadcast al emplear una capa oculta de cinco neuronas en este caso hablamos de un porcentaje de desempeño del 100% para los datos de prueba. Para la red asociada a falla de congestión teniendo en cuenta los porcentajes de desempeño tanto al clasificar congestión entrante como congestión saliente, al igual que en el caso anterior los mejores resultados se lograron al usar una capa intermedia de cinco neuronas. En

este caso hablamos de un porcentaje de desempeño de 98.11% y 100% para congestión entrante y saliente respectivamente.

En conclusión a pesar de que los resultados obtenidos con los dos esquemas son muy buenos, y que en términos del tiempo requerido para el entrenamiento no se presentan diferencias significativas, cuantitativamente se puede ver claramente que el segundo esquema resulta favorable, es decir que el sistema se desempeña mejor al emplear una red para cada tipo de falla.

5. RESULTADOS OBTENIDOS

A continuación se presentan los productos obtenidos como resultados directos o indirectos del presente trabajo.

- La selección de una herramienta de gestión de red que suple las necesidades de gestión detectadas dentro de la red de datos institucional. Algunas de las tareas identificadas fueron administración de direcciones IP, monitorización de ancho de banda, monitorización de eventos y control del tiempo de respuesta entre otros.

- Una descripción detallada de la herramienta de gestión seleccionada y el procedimiento que se debe seguir para su configuración. Se presenta una configuración sugerida de la herramienta para las necesidades específicas de la Red de datos de la Universidad Industrial de Santander, centrando la atención en las opciones ofrecidas para la detección y reporte de condiciones de falla.

- Una descripción general asociada a la topología y estructura tanto física como lógica de la red, un listado de subredes y un inventario aproximado de las estaciones conectadas a cada una de ellas que incluye ubicación, dirección IP y dirección MAC.

- Una base de datos con el inventario del hardware de la red donde se presentan las principales características de los elementos activos que la conforman, incluyendo switches, servidores y enrutadores.

- Diagramas correspondientes a la conexión de la red de datos de la sede principal con las distintas sedes municipales (Pamplona, Málaga, Socorro, Barranca), y las sedes ubicadas dentro del área metropolitana (Bucarica, Guatigurará), además de la Facultad de Salud. Un diagrama actualizado y

detallado de la conexión a Internet y de la interconexión del Switch-Router Cajun P880 con cada uno de los segmentos de la red.

- Una metodología para la detección y clasificación de fallas de red a partir de la información obtenida de los dispositivos asociados a la misma. Se han seleccionado dos tipos de falla los cuales según los criterios analizados encierran buena parte de los problemas de desempeño presentes en un segmento de red. Las fallas analizadas fueron tormenta de broadcast y congestión; esta última se analizó como congestión entrante y congestión saliente del segmento de red.

A partir del trabajo desarrollado y de los resultados obtenidos se consideran pertinentes las siguientes observaciones

- En el caso particular de la red de datos de la Universidad Industrial de Santander, el equipo encargado de la gestión de la red no cuenta con el número adecuado de personas, aspecto que origina una buena parte de las deficiencias encontradas.

- Al seleccionar una herramienta de gestión al igual que cualquier elemento de software o hardware de red, se debe tener claro conocimiento de las características ofrecidas por cada una de las opciones disponibles. La decisión se debe tomar a partir de los criterios de selección generados a partir de la identificación de necesidades y siempre dejando un margen de crecimiento, es decir pensando en la actualización futura o posibles cambios que pueda tener la red.

- Para que el nivel de tráfico generado por la gestión se mantenga en un nivel razonable, así como para que el volumen de datos a procesar no sea muy elevado se debe buscar que el grupo de variables que caracteriza la falla sea mínimo sin descartar información que pueda ser necesaria para una correcta clasificación.

- El sistema empleado en la etapa de detección debe estar enfocado a no dejar pasar ningún comportamiento anómalo en el estado de las variables, sin importar que se incurra en falsas detecciones ya que estas pueden ser corregidas hasta cierto punto en la etapa de clasificación. La falsa aceptación

(detección de falla cuando no existe) es menos grave que un falso rechazo (clasificar como normal una condición de falla).

- Tanto el sistema empleado en la detección como en la clasificación, pueden variar dependiendo del tipo de falla y condiciones establecidas. Por tal razón el objetivo de este trabajo se centra en la metodología que se debe seguir para selección de las fallas de interés según el caso y la asociación con las variables MIB, además de describir los procedimientos y los criterios que se deben tener en cuenta para la validación de la misma.

Adicionalmente parte de los resultados obtenidos en este trabajo de investigación fueron presentados, en el evento internacional CONCAPAN XXIV organizado por el IEEE el cual se llevó a cabo durante los días 10, 11, 12 de Noviembre de 2004 en San José de Costa Rica. Se realizó una presentación oral del trabajo y el documento se encuentra registrado en las memorias del evento. En la actualidad se está preparando un artículo para enviarlo a una revista internacional especializada.

Se participó en la codirección de un proyecto de pregrado próximo a concluir, realizado por dos estudiantes de la Escuela de Ingenierías Eléctrica, Electrónica y Telecomunicaciones. Dicho trabajo está relacionado con el área de detección de fallas por lo tanto se enmarca en el dominio de investigación de esta tesis.

6. CONCLUSIONES

Al finalizar este trabajo de investigación y una vez satisfechos los objetivos propuestos en el plan de trabajo, se puede concluir lo siguiente:

Se contribuyó de manera importante al mejoramiento de la red de datos institucional en aspectos relacionados con la documentación de la misma y la configuración de una herramienta de gestión que se ajusta a las necesidades detectadas dentro de la red. Adicionalmente se propuso una metodología general para la detección automática de dos tipos de falla en un segmento de red tipo Ethernet que mostró ser de una excelente efectividad en las pruebas realizadas. Dicha metodología puede ser adaptada para otros tipos de falla con los criterios propuestos para la selección de las variables de la MIB correspondientes y usando el modelo propuesto que en la primera etapa detecta y luego clasifica la falla.

Según los resultados obtenidos con la metodología propuesta, se prueba la validez de usar las variables de la MIB de los dispositivos asociados a un segmento de red para la identificación de fallas o condiciones anormales de funcionamiento. Se puede decir que la definición teórica de las variables de la MIB es un punto de partida valido para realizar su asociación con las distintas fallas de red. A partir de dichas definiciones se puede establecer una relación entre estas variables y los parámetros de desempeño de la red, los cuales a su vez reflejan los efectos de una falla sobre la red.

Además de la definición teórica de las variables, características de los dispositivos tales como el nivel de operación, versión empleada del protocolo de gestión y opciones de configuración son aspectos que se deben tener en cuenta para la selección de las variables MIB, en algunos casos cuando se presentan problemas de selección debido a las similitud en las definiciones de algunas variables estos aspectos resultan un criterio clave que permite que algunas de ellas sean descartadas.

El éxito de los resultados obtenidos sustenta la validez de la metodología presentada y por otro lado se ratifica la solidez del trabajo realizado si se tiene en cuenta que la literatura revisada no llega al punto de estimar porcentajes de efectividad de las técnicas propuestas.

Recomendaciones:

La gestión de red es un tema bastante extenso, dentro del cual la gestión de fallas es solo una de sus áreas funcionales y aún así resulta bastante amplia. Este es el primer trabajo de maestría que se culmina en el área especifica de gestión de fallas aplicado a la red institucional por tanto se recomienda dar continuidad a la investigación probando otros escenarios y tipos de falla y empleando la metodología propuesta hacer su asociación con las variables de la MIB.

En el caso particular de la red de datos de la Universidad Industrial de Santander, el siguiente paso, puede ser emplear como fuente de información el Switch-Router central Cajun P880, específicamente el puerto asociado a uno de los edificios dentro del campus. De esta manera el segmento bajo estudio y el tráfico analizado no será solo el asociado a un limitado número de estaciones sino el correspondiente a todo un edificio.

Como una alternativa que complementa el sistema de detección de fallas propuesto se recomienda el uso de mensajes de tipo Trap, mediante los cuales los dispositivos gestionados pueden realizar el reporte de eventos a la estación de gestión, existen diversas herramientas que permiten la recepción y administración de dichos mensajes.

7. BIBLIOGRAFÍA

Libros

[1]. BLUM, Richard. NETWORK PERFORMANCE OPEN SOURCE TOOLKIT, Wiley Publishing, Inc. 2003 ISBN: 0-471-43301-2. Este libro describe una gran variedad de pruebas de desempeño de redes en función de las herramientas software más conocidas para estas labores.

[2]. BREKNE, Tønnes; CLEMETSEN, Marius; HEEGAARD, Poul; INGVALDSEN, Tone; VIKEN, Brynjar. STATE OF THE ART IN PERFORMANCE MONITORING AND MEASUREMENTS, Telenor R&D R 15/2002 ISBN 82-423-0530.5. Este libro ofrece una introducción a las medidas de desempeño de redes IP, y describe los conceptos y métodos en uso actualmente para el estudio del desempeño de redes, sus actores y herramientas.

[3]. BREYER, Robert y RILEY, Sean. Switched, Fast and Gigabit Ethernet, Third Edition, United States of America, MacMillan Technical Publishing, 1999.

[4]. DELLA MAGIORA Paul; ELLIOT, Christopher. PERFORMANCE AND FAULT MANAGEMENT, Cisco press 2000 ISBN: 1-57870-180-5. Este Libro es una referencia en las áreas de medidas de desempeño de redes y gestión de fallas.

[5]. DUBUISSON, Olivier. ASN.1 COMMUNICATION BETWEEN HETEROGENEOUS SYSTEMS, OSS Nokalva, 2000 ISBN: 0-12-6333361-0. Este libro presenta la teoría sobre la notación de sintaxis abstracta 1

[6]. HAYKIN, Simon. NEURAL NETWORKS. Segunda Edición . Prentice Hall, Upper Saddle River. NJ 1999. Este libro proporciona los conceptos generales y específicos de las redes neuronales artificiales.

[7]. SPURGEON, Charles. ETHERNET: THE DEFINITIVE GUIDE, O'Reilly & Associates, 2000. ISBN 1-56592-660-9. Tomado como libro de consulta referente a conceptos de Ethernet, en especial el capítulo 19 que trata sobre el desempeño de redes.

[8]. STALLINGS William. COMUNICACIONES Y REDES DE COMPUTADORES, Sexta Edición, Pearson Educación S.A.: 2000. Libro de estudios general sobre redes, con descripción de protocolos y sistemas de referencia.

[9]. STALLINGS William. SNMP, SNMPV2, SNMPV3, AND RMON1 AND 2, Addison-Wesley, ISBN: 0201485346 1999. Libro de estudios especifico sobre el protocolo SNMP en sus diferentes versiones y su aplicación a la gestión de redes.

[10]. STEVENS W.R. TCP/IP ILLUSTRATED, Vol. 1: THE PROTOCOLS, Addison-Wesley 1994. Libro de consulta sobre los protocolos de redes en especial el protocolo SNMP.

[11]. SUBRAMANIAN M. NETWORK MANAGEMENT- PRINCIPLES AND PRACTICE, Addison-Wesley, 2000 ISBN: 0201357429. Este libro profundiza en el área de gestión de redes y es de importancia especial el capítulo 13, donde se trata la gestión de fallas.

[12]. TANENBAUN Andrew S. REDES DE COMPUTADORAS, Tercera Edición, Prentice Hall Hispanoamericana S.A., 1997. Libro de consulta sobre información general de redes de computadoras, presenta un capitulo dedicado al desempeño de redes.

Artículos

[13]. BREITBART, Yuri; CHAN, Chee-Yong; GAROFALAKIS, Minos; RASTOGI, Rajeev; SILBERSCHATZ, Avi. "Efficiently Monitoring Bandwidth and Latency in IP Networks", Information Sciences Research Center, Bell Laboratories 2000. Este documento plantea diversos métodos para realizar de manera eficiente procesos de monitoreo de parámetros de desempeño en redes basadas en IP.

[14]. CABRERA, J; LEWIS, L; QIN, X; LEE, W; PRASANTH, R; RAVICHANDRAN, B; MEHRA, R. “Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables a Feasibility Study”, IEEE 2001. Este documento muestra una propuesta de metodología para la utilización de sistemas de gestión de red (NMS) para la detección temprana de ataques distribuidos de negación de servicio.

[15]. CHAO, C.S; YANG D.L; LIU A.C. “An Automated Fault Diagnosis System Using Hierarchical Reasoning and Alarm Correlation”, Feng Chia University, Taiwán 2000. En este documento se presenta el desarrollo de un sistema práctico para el diagnostico de fallas de red.

[16]. DUARTE , Elías Procópio; DOS SANTOS, Aldri L. “Network Fault Management Based on SNMP Agent Groups”, IEEE 2001. En este documento se presenta una estructura novedosa para la monitorización de objetos de gestión SNMP en una red de área local, se describe la creación e implementación de una herramienta para la gestión de fallas de red en una LAN.

[17]. FEATHER, Frank; SIEWIOREK, Dan; MAXION, Roy. “Fault Detection in an Ethernet Network Using Anomaly Signature Matching”, SIGCOMM 1993. Se presenta un método para la detección automática de problemas en una red de área local Ethernet, para lo cual se hace una investigación profunda sobre los tipos de condiciones de falla que afectan a esta clase de redes.

[18]. HOOD, Cynthia S; JI, Chuanyi. Intelligent Agents For Proactive Fault Detection, IEEE Internet Computing, March -April 1998. En este documento se presenta la creación de una herramienta de detección de fallas, basada en agentes inteligentes.

[19]. HIGBIE, Carrie. “Congestion-Can standards provide relief?”, The Siemon Company 2004. Este documento presenta conceptos y definiciones sobre el estado de congestión en una red.

[20]. THOTTAN, M; JI, Chuanyi. “Adaptive Thresholding for Proactive Network Problem Detection”, Rensselaer Polytechnic Institute 1999. Este documento presenta un estudio encaminado a detectar problemas de red potenciales a través de mediciones del tráfico de red, utilizando como referencia a las variables de la MIB.

[21]. THOTTAN, M; JI, Chuanyi. “Anomaly Detection in IP Networks”, IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL 51, NO. 8, AUGUST 2003. Este documento presenta conceptos sobre las anomalías más frecuentes en redes Ethernet y las formas de detectarlas.

[22]. THOTTAN, M. “MIB Variable Based Fault Classification: The Next Step Towards Proactive Management”, Bell Labs 2001. Se presenta un estudio en el que se plantea una clasificación de fallas de red, utilizando para ello la información contenida en las variables MIB.

[23]. THOTTAN, M; JI, Chuanyi. “Proactive Anomaly Detection Using Distributed Intelligent Agents”, IEEE Network September/ October 0890-8044/ 1998. Este documento presenta un procedimiento para la detección proactiva de fallas de red mediante la aplicación de agentes inteligentes.

[24]. THOTTAN, M; JI, Chuanyi. “Properties of Network Faults”, Bell Labs 2001. Este documento presenta una descripción de las fallas de red más comunes y sus características.

[25]. THOTTAN, M; JI, Chuanyi. “Statistical Detection of Enterprise Network Problems”, Rensselaer Polytechnic Institute 1999. Este documento presenta un procedimiento para la detección de problemas de red basándose en métodos estadísticos.

Trabajos de grado

[26]. CHAVEZ, C, CONTRERAS, J y RUEDA, D, “Evaluación del desempeño de la red de datos Institucional en los edificios de Ingeniería Eléctrica, Laboratorio de alta tensión y Laboratorio de pesados”. Tesis de grado, Universidad Industrial de Santander, 2002.

[27]. MARABOLI ROSSELOTT, Marcelo. “Monitor de Tráfico Ethernet Netgraph” Memoria de grado, Universidad Técnica Federico Santa María de chile, Departamento de Electrónica Noviembre 1997. Trabajo de investigación a nivel de

pregrado relacionado con el área de gestión de redes haciendo un énfasis especial en el estudio de herramientas de monitorización y sus propiedades.

[28]. SAYENKO, Oleksandr. “Policy Based Model for Monitoring SNMP Resources”, Master’s Thesis Work, University of Jyväskylä, Finland, Department of Mathematical Information Technologies 8/8/2002. Trabajo de investigación a nivel de maestría relacionado con el área de gestión y monitorización de redes.

Otras fuentes

[29]. CISCO SYSTEMS. INTERNETWORKING TECHNOLOGY HANDBOOK, Capítulos 6, 55, 56 2004. Disponible en Internet: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/. Este documento presenta información general sobre gestión de redes, protocolo SNMP, monitoreo remoto RMON, etc.

[30]. LAN TRAFFIC V2–USER GUIDE, ZTI 1998-2003. All rights reserved. France Telecom licensed product. www.zti-telecom.com. Esta fuente presenta el manual de usuario del software LAN Traffic.

[31]. RFC´S 1156, 1158, 1212, 1213, 1271, 1724, 1757, 2914. En esta serie de notas sobre el Internet, se presentan documentos que contienen proposiciones, comentarios y los estándares relacionados a la tecnología del Internet, específicamente sobre SNMP, la MIB y la Gestión de Redes propuesta por el IETF.

[32]. WAN KILLER OVERVIEW. Wan Killer Network traffic generator Help. Copyright 1995-2002. www.solarwinds.net. Esta fuente presenta el archivo de ayuda de la herramienta de generación Wan Killer que hace parte del paquete Solarwinds.

[33]. YUMOTO, K. “What's TFGEN”. Copyright 1996. www.st.rim.or.jp/~yumo/index.html. Esta fuente presenta el manual de usuario para el software TFGEN.

ANEXO A. Descripción básica de la herramienta de gestión de red Solarwinds Engineer's Edition

Herramientas de Gestión de Red

El presente manual proporciona una descripción general de cada una de las herramientas disponibles dentro del grupo de herramientas para la gestión de red ofrecido por la versión 5.5 de la edición para ingenieros de SolarWinds. Las herramientas aquí presentadas contribuyen significativamente con la realización de muchas de las tareas básicas de gestión, tales como:

Descubrimiento de la Red
Monitorización de Fallas
Monitorización de Desempeño
Administración de direcciones IP
Seguridad de Red
Exploración de la MIB
Diagnóstico de Red
Seguimiento de variables SNMP en tiempo real, entre otros.

Información general sobre la herramienta de gestión SolarWinds Engineer´s Edition

La herramienta seleccionada o forma parte de un grupo de herramientas para la gestión de red, desarrolladas y comercializadas por SolarWinds.net. Dentro de la variedad de opciones se encuentran herramientas para la administración, monitorización y descubrimiento de la red. Dentro de la gama de productos de SolarWinds se encuentran cinco productos o versiones diferentes del producto, después de realizar un análisis detallado de las prestaciones ofrecidas por cada una de ellas se seleccionó la edición para ingenieros (Engineer´s Edition).

Requerimientos mínimos del sistema para la instalación

Sistema Operativo	Windows 95 / 98 / NT / 2000 / Millennium Las herramientas de SolarWinds presentan un mejor desempeño sobre Windows NT y 2000.
CPU	Pentium II 500 MHz o superior (recomendado)
Memoria	64 MB RAM (128 MB o superior (recomendado))
Espacio en Disco	Al menos 200 MB
Conexión de red	Tarjeta de Red o modem
Internet Explorer	Algunas herramientas SolarWinds usan Internet Explorer 5.0, por tal razón este debe estar instalado.
Tarjeta de sonido	Recomendado, pero no es requisito.

AL hacer clic sobre el icono que representa la herramienta, se despliega una barra como la que se presenta a continuación en la que se encuentran los diferentes grupos de herramientas ofrecidos por SolarWinds, esta distribución de las herramientas esta hecha pensando en las distintas tareas requeridas por el administrador. A continuación se muestran de manera resumida algunos de los grupos de herramientas ofrecidos por SolarWinds.

Herramientas para el descubrimiento de elementos de una red (Network Discovery Tools)

IP Network Browser: Es una herramienta interactiva que permite descubrir los dispositivos dentro de una red. El IP Network Browser puede escanear una subred y mostrar detalles relacionados con los dispositivos que se encuentran dentro de ella. Se puede usar la IP de un dispositivo específico, una subred o un rango de direcciones. Dependiendo del tipo de dispositivos encontrados y de si poseen un agente SNMP, brinda información relacionada con los mismos. Ej. Información de puertos en switches, servicios instalados en servidores, etc.

Además desde allí se pueden activar algunas otras opciones como seleccionar un elemento y realizarle un ping, iniciar una sesión de Telnet, obtener su configuración si se trata de un dispositivo cisco o realizar un traceo de la ruta hasta el.

Ping Sweep: esta herramienta permite escanear un rango de direcciones IP y mostrar cuales direcciones dentro de ese rango están en uso y cuales no. Ping Sweep además puede obtener el nombre de dominio para cada una de las direcciones IP que están en uso.

Subnet List: Esta herramienta le permite de manera rápida determinar la cobertura de una red y descubrir todas las subredes dentro de la misma.

SNMP Sweep: Esta herramienta puede ser configurada para escanear un rango de direcciones IP y muestra cuáles de esas direcciones están en uso. El SNMP Sweep también muestra el nombre de dominio asociado a esa dirección, el nombre del sistema, la localización, a quien se debe contactar para cualquier aspecto relacionado con el dispositivo, la ultima vez que fue reiniciado, la descripción del sistema, versión del sistema operativo.

Network Sonar: Se trata de una herramienta de alto desempeño útil en el

descubrimiento de una red. Network Sonar puede construir una base de datos con la estructura y la lista de los dispositivos sobre una red TCP/IP.
El proceso puede ser detenido en cualquier momento y cuando se inicie nuevamente retomará en el punto que había dejado. El proceso consiste en definir un enrutador origen a partir del cual se pueda obtener las subredes conectadas, una vez hecho esto se procede a la búsqueda se seleccionan las redes sobre las que se quiere obtener información, tal como número de nodos por subred, tipos de dispositivos conectados, el número de subredes por cada red, rutas, esta información puede ser presentada como estadísticas en tablas o como diagramas de porcentaje.

DNS audit. (Auditor DNS): Esta herramienta permite escanear un rango determinado de direcciones IP en busca de errores en la resolución de direcciones IP a partir de los nombres de dominio o viceversa, además sirve como herramienta de control y supervisión del uso de los mismos.

Switch Port Mapper: Permite descubrir remotamente los dispositivos conectados a los puertos de cada switch/hub. Este puede descubrir la dirección MAC, la dirección IP y el nombre de host de cada uno de los dispositivos conectados, además de los detalles sobre cada puerto. El mapeo de puertos es hecho mediante una correlación de la información de puertos/MAC/interfaces dentro del switch o hub. La relación MAC/IP es tomada de un router o servidor que debe estar directamente a la misma subred que el switch o hub. Se debe suministrar la dirección IP del switch a analizar su comunidad SNMP y la dirección IP del enrutador. La información proporcionada sobre las interfaces se puede modificar seleccionando settings en el menú file. Únicamente se pueden mapear hubs y switches que soporten BRIDGE-MIB.

MAC Address Recovery: Dirige un proceso de búsqueda en la subred local y crea una tabla de resolución de direcciones MAC a direcciones IP. Su área de acción esta limitada a la subred física a la cual está conectada, se esta desarrollando una nueva versión para el descubrimiento y la correlación entre direcciones físicas y direcciones IP es subredes remotas. Presenta una tabla donde se encuentra la dirección IP, el nombre de dominio de la estación y su dirección MAC, además de algunos datos relacionados con el fabricante de la tarjeta.

Cisco Tools

Un buen número de herramientas dentro de SolarWinds han sido desarrolladas especialmente para dispositivos Cisco Router/Switches

Config Editor / Viewer: Con esta herramienta se puede extraer rápidamente la configuración actual del dispositivo (running config) y archivarla para tomarla como referencia en el futuro. Cisco Config se presenta en un formato bastante sencillo. Config Viewer esta también habilitado para descifrar passwords y comparar cambios entre enrutadores o archivos históricos de configuración.

Download Config: Descargar un archivo de configuración desde un enrutador Cisco hacia un PC.

Upload Config: Permite cargar o actualizar una nueva configuración a un enrutador Cisco o cambiar algún parámetro de configuración usando SNMP. Uno de los usos más frecuentes es resetear un password de acceso desconocido.

Running Vs Startup Configs: Esta herramienta es usada para comparar la memoria de operación con la memoria de inicio Running and Startup (en NVRAM) de un enrutador Cisco. Si alguna persona ha cambiado la configuración del enrutador pero no a salvado los cambios a la memoria no volátil, entonces pueden existir diferencias entre las dos configuraciones.

Router Password Decrypt: La herramienta permite descifrar contraseñas de tipo 7 de Cisco. Los passwords tipo 7 son comúnmente usados para terminales y conexiones habilitadas sobre switches y enrutadores Cisco. Se debe tener el password cifrado para poderlo descifrar. La secuencia de caracteres cifrados es tomada normalmente de la configuración impresa del Cisco o descargando la configuración directamente del enrutador o switch. Se requiere la dirección IP del dispositivo y la comunidad SNMP de lectura/escritura.

Proxy Ping esta herramienta ofrece la posibilidad de iniciar remotamente un Ping

Test desde un enrutador cisco remoto, los resultados son calculados con base en las PINGs enviados directamente desde el enrutador seleccionado hasta

otro dispositivo remoto. Se debe conocer la dirección IP y la comunidad SNMP del enrutador que se va a usar como Proxy y se proporciona la dirección IP del dispositivo destino.

Advanced CPU Load: Se trata de una herramienta que monitoriza y grafica la carga de varios enrutadores Cisco o Servidores Windows en tiempo real.

CPU Gauge: Muestra en tiempo real la carga para enrutadores Cisco o Servidores Windows.

Router CPU Load: Muestra la carga CPU en tiempo real de un Enrutador Cisco en una gráfica de barras. La carga de uno o varios enrutadores puede ser visualizada al mismo tiempo. Puede además mostrar una alarma si el administrador le ha definido un umbral y éste ha sido sobrepasado.

IP Network Browser: Es una herramienta interactiva que permite descubrir los dispositivos dentro de una red. El IP Network Browser puede escanear una subred y mostrar detalles relacionados con los dispositivos que se encuentran dentro de ella. Se puede usar la IP de un dispositivo específico, una subred o un rango de direcciones. Dependiendo del tipo de dispositivos encontrados y de si poseen un agente SNMP, brinda información relacionada con los mismos. Ej. Información de puertos en switches, servicios instalados en servidores, etc.

Security Check: se trata de una herramienta que permite examinar la seguridad de un router o switch catalyst de Cisco intentando entrar al dispositivo e indicando si el IOS puede ser actualizado. La herramienta intenta determinar la comunidad SNMP read-only y read-write. Una vez se conoce la comunidad SNMP read-write, se puede descargar la configuración del dispositivo y modificarla. Router Security Check solo puede irrumpir en dispositivos donde se detecta un alto nivel de vulnerabilidad.

Herramientas del grupo Ping (Ping Tools)

Ping Indica el promedio del tiempo de respuesta, el número de paquetes perdidos al igual que el tiempo de respuesta actual indicando la hora de cada petición. El tamaño del paquete, el retardo entre PINGs, el timeout del mensaje ICMP y el tiempo de vida (TTL) pueden ser modificados. SolarWInds PING puede exportar los resultados en formato de texto o RTF o imprimir reportes.

Trace Route SolarWinds TraceRoute no solo le muestra el

camino que el tráfico de red sigue para ir desde su PC hasta el servidor o dispositivo destino, este además visualiza selecta información SNMP sobre los dispositivos encontrados por el camino. Esta es una poderosa herramienta para la traza de rutas. Información relacionada con el tiempo de respuesta y paquetes perdidos es desplegada no solo como un número sino como una barra grafica.

Una vez la ruta es aprendida, el trace route de SolarWinds puede recordarla junto con los detalles sobre ella. Una vez las rutas son recordadas TraceRoute. Puesto que se recuerdan las rutas, TraceRoute puede mostrarle la ruta y el dispositivo que falla siempre que una parte de la red esta abajo.

Cada salto en el camino seleccionado es trazado y procesado concurrentemente esto hace que TraceRoute sea una herramienta muy rápida. Realizando los ajustes (“Settings”) necesarios se puede obtener información adicional como System OID, Community String, Location y mucho más.

Proxy Ping esta herramienta ofrece la posibilidad de iniciar remotamente un Ping Test desde un enrutador cisco remoto, los resultados son calculados con base en las PINGs enviados directamente desde el enrutador seleccionado hasta otro dispositivo remoto. Se debe conocer la dirección IP y la comunidad SNMP del enrutador que se va a usar como Proxy y se proporciona la dirección IP del dispositivo destino.

Ping Sweep: esta herramienta permite escanear un rango de direcciones IP y mostrar cuales direcciones dentro de ese rango están en uso y cuales no. Ping Sweep además puede obtener el nombre de dominio para cada una de las direcciones IP que están en uso.

Enhanced Ping Esta herramienta permite monitorizar continuamente un cierto número de servidores, enrutadores, PCs, etc. Y mostrar los tiempos de respuesta en tiempo real. Al igual que en la herramienta ping el tamaño del paquete, el retardo entre PINGs, el timeout del mensaje ICMP y el tiempo de vida (TTL) pueden ser modificados.

Herramientas para la Administración de direcciones IP (IP Address Management)

La administración de las direcciones IP es una tarea bastante compleja, el rápido incremento en el número de nodos que conforman la red de muchas organizaciones hace que se dificulte aun más su realización.

El administrador de la red además de ser el encargado de realizar el diseño, distribución y asignación de direcciones para las redes y subredes que forman parte de su compañía debe controlar el uso y garantizar el buen desempeño de la red. El objetivo es el siguiente: el administrador debe ser la única persona habilitada para autorizar el uso de una dirección IP específica siempre que se quiera agregar un elemento a la red, de esta manera se puede mantener un registro de cada una de las direcciones que están siendo empleadas dentro de la LAN de la organización. Con base en esta premisa el administrador puede, haciendo uso de una herramienta como la que se muestra a continuación, controlar y supervisar que las direcciones IP empleadas por cada una de las estaciones, correspondan con el diseño y los rangos disponibles, además de que cuente con la debida autorización.

De igual manera resulta importante el poder llevar un control similar pero orientado a la asignación y uso de nombre de dominio; este control se puede realizar con un procedimiento similar al anterior.

El grupo de herramientas ofrecido para la administración de direcciones IP fue desarrollado pensando en que fuera rápido y fácil de usar.

Advanced Subnet Calculador (Calculadora avanzada de subred): es una herramienta que puede asistir al administrador en la realización del diseño de las distintas subredes, permite el cálculo rápido de rangos de direcciones, máscaras de subred, direcciones de broadcast etc. Esta aplicación ofrece la posibilidad de trabajar con direcciones Full Class o con direcciones sin clase CIDR (Classless Inter Domain Routing).

Address Details

Desde esta ventana, usted puede a partir de una dirección IP particular o el nombre de dominio de una estación, obtener la

información complementaria (nombre de dominio o IP), además podrá visualizar la dirección en los diferentes formatos (decimal, hexadecimal y binario), tendrá a su disposición información relacionada con el tipo de dirección y la máscara de subred. Adicionalmente le será proporcionada alguna información relacionada con la organización propietaria de la dirección, en caso tal de que se trate de una IP pública.

IP address management (Administrador de direcciones IP): es una herramienta que permite monitorizar de manera automática las direcciones IP dentro de una determinada subred o subredes y realizar reportes relacionados con su uso. Se proporciona la dirección y la mascara de subred. Entrega información relacionada con el Nombre de dominio de la estación, el tipo de dispositivo, tiempo de respuesta entre otros. Permite ir almacenando la lista de las subredes escaneadas para que cada vez que se inicialice la herramienta se pueda acceder fácilmente a la información relacionada con cada una de ellas.

DNS & Who Is Resolver: Proporciona información relacionada con el mapeo de nombres de dominio a direcciones IP y viceversa, además de alguna información relacionada con la red del host y el servidor DNS encargado de ese dominio. Rango de direcciones asignado, entre otros.

Ping Sweep: esta herramienta permite escanear un rango de direcciones IP y mostrar cuales direcciones dentro de ese rango están en uso y cuales no. Ping Sweep además puede obtener el nombre de dominio para cada una de las direcciones IP que están en uso.

DNS audit. (Auditor DNS): Esta herramienta permite escanear un rango determinado de direcciones IP en busca de errores en la resolución de direcciones IP a partir de los nombres de dominio o viceversa, además sirve como herramienta de control y supervisión del uso de los mismos. Los resultados pueden ser exportados en un archivo de texto plano, en formato HTML en un documento de excel, o permite copiar los datos simplemente.

DHCP Scope Monitor (Monitor de Alcance DHCP): El monitor de alcance de DHCP (Dynamic Host Configuration Protocol), protocolo que permite la asignación dinámica de direcciones IP dentro de una red, permite la monitorización sobre los servidores DHCP del rango de direcciones disponible para ser asignadas además del porcentaje de aprovechamiento de las mismas.

Herramientas para la Gestión del Desempeño de la red (Performance Management)

Como parte de las tareas de gestión se debe controlar el uso y garantizar el buen desempeño de la red. Por tal razón se debe hacer una constante monitorización de los dispositivos de la red, así como el análisis de las variables que éstos reportan, de tal forma que se pueda corregir o incluso prevenir una posible falla.

Dentro del grupo de herramientas provisto por SolarWInds se encuentran varias opciones que proveen la habilidad de monitorizar cualquier cosa sobre el tráfico desde un simple puerto hasta el tiempo de respuesta y la disponibilidad de cualquier servidor en la red. Algunas de las herramientas descritas a continuación ofrecen reporte grafico.

Network Performance Monitor (Monitorización del funcionamiento de la Red): es una herramienta que permite monitorizar el tráfico y la utilización de cientos de interfaces. En tiempo real le notificará vía e-mail o enviando un beeper cuando una condición de alerta es detectada, tal como reinicio de enrutadores, fallas en el servidor, interfaces deshabilitadas o fuera de servicio, etc.

SNMP Graph (Reporte gráfico de SNMP): Monitoriza y grafica las estadísticas de cualquier OID dentro de la MIB de un dispositivo que responde a SNMP. Esta herramienta puede monitorizar varios elementos al mismo tiempo y graficar su comportamiento en la misma pantalla.

Bandwith Gauges: Muestra un juego de ventanas que le permiten monitorizar, en tiempo real la transmisión y recepción de tráfico por cualquier interfaz o puerto de un dispositivo. También tiene la capacidad de crear grupos específicos de dispositivos con los mismos parámetros para ser revisados posteriormente.

Bandwith Monitor (Monitorización del Ancho de Banda): es un monitor en tiempo real de tráfico y ancho de banda. Se puede seleccionar un número de dispositivos (varios cientos de interfaces pueden requerir un computador con una

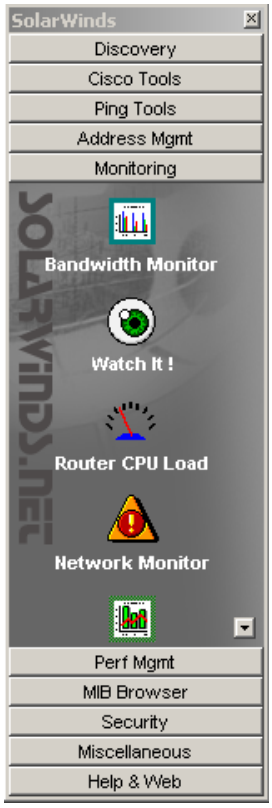
buena memoria RAM) para monitorizar concurrentemente. Los dispositivos no debe estar en la misma red el único requisito es que respondan las peticiones SNMP.
El monitor de ancho de banda es ideal para monitorizar la utilización del ancho de banda ofrecido por el proveedor de servicios. Esta herramienta también es útil aislando cuellos de botella dentro de la red. La herramienta se puede personalizar y permite ajustar entre otros factores el umbral en el cual un nodo pasa de estado normal a advertencia y peligro. Los resultados pueden ser graficados o exportados para revisiones posteriores.

Advanced CPU Load: Se trata de una herramienta que monitoriza y grafica la carga de varios enrutadores Cisco o Servidores Windows en tiempo real.

CPU Gauge: Muestra en tiempo real la carga para enrutadores Cisco o Servidores Windows.

Router CPU Load: Muestra la carga CPU en tiempo real de un enrutador Cisco en una gráfica de barras. La carga de uno o varios enrutadores puede ser visualizada al mismo tiempo. Puede además mostrar una alarma si el administrador le ha definido un umbral y éste ha sido sobrepasado.

Herramientas del grupo Monitoring



Bandwith Monitor (Monitorización del Ancho de Banda): es un monitor de tráfico y ancho de banda en tiempo real. El usuario puede seleccionar cualquier número de dispositivos. Los dispositivos no necesitan estar dentro de la misma red, el único requisito es que respondan peticiones del protocolo SNMP.

Es una herramienta que le permite monitorizar la utilización del ancho de banda y contrastar con lo ofrecido por el proveedor de servicios. Permite la identificación de cuellos de botella dentro de la red. Permite la definición de alarmas mediante la definición de umbrales o porcentajes de utilización limite.

Watch It es un monitor de red. Permite monitorizar servidores, enrutadores, sitios web, etc, y permite notificar cuando el tiempo de respuesta se esta degradando o cuando un dispositivo ha dejado de estar disponible. Se pueden configurar distintos sonidos que se activan para indicar que un dispositivo esta perdiendo paquetes, que ha dejado de responder o que esta activo de nuevo.

Router CPU Load: Muestra la carga CPU en tiempo real de un Enrutador Cisco en una gráfica de barras. La carga de uno o varios enrutadores puede ser visualizada al mismo tiempo. Puede además mostrar una alarma si el administrador le ha definido un umbral y éste ha sido sobrepasado.

Network Monitor puede monitorizar cientos de dispositivos y obtener datos relacionados con tiempos de respuesta y paquetes perdidos. Network Monitor puede reportar cuando un dispositivo deja de responder mediante el envío de un beeper o un E-Mail.

Network Performance Monitor (Monitorización del desempeño de la Red): es una herramienta que permite monitorizar el tráfico y la utilización de cientos de interfaces. En tiempo real le notificará vía correo electrónico o enviando un beeper cuando una condición de alerta es detectada, tal como reinicio de enrutadores, fallas en el servidor, interfaces deshabilitadas o fuera de servicio, etc.

Enhanced Ping Esta herramienta permite monitorizar continuamente un cierto número de servidores, enrutadores, PCs, etc. Y mostrar los tiempos de respuesta en tiempo real. Al igual que en la herramienta ping el tamaño del paquete, el retardo entre PINGs, el timeout del mensaje ICMP y el tiempo de vida (TTL) pueden ser modificados.

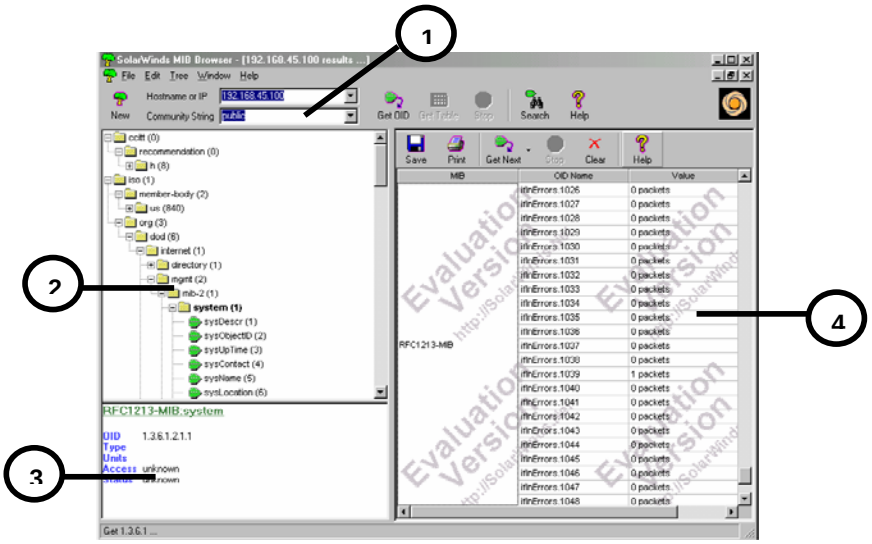
SysLog Server es una herramienta que escucha constantemente en espera de mensajes Syslog entrantes sobre el puerto UDP 514 y decodifica los mensajes recibidos con propósitos de registro.

Los mensajes Syslog fueron originalmente usados por sistemas UNIX para mantener registros de aplicaciones, red y sistemas operativos. Actualmente un gran número de dispositivos de red pueden ser configurados para generar mensajes Syslog. La herramienta permite recibir los mensajes, almacenarlos en una base de datos y enviar mensajes Syslog.

Herramientas del grupo MIB Browser

MIB Browser: Permite hacer un recorrido por el árbol jerárquico de la MIB, Según el grupo seleccionado, permite visualizar las tablas o los distintos valores asociados a cada una de las variables, proporcionando el OID apropiado obtener los valores para una variable en particular y muchas otras funciones. La base de datos de MIBs ofrecida por SolarWinds contiene un poco más de 1,000 MIBs y 100,000 OIDs entre públicos y privados.

MIB Browser



Campo destinado a la identificación del dispositivo que se quiere analizar (IP o nombre de dominio) y la comunidad (public o private).

En esta zona se despliega la estructura de la MIB del dispositivo y siguiendo el camino correcto se pueden localizar las distintas variables. Es necesario que antes de iniciar la inspección de la MIB de un determinado dispositivo, se seleccione el nodo del que se quiere partir (por lo general nodo Internet para obtener toda la información)

En esta sección de la ventana, se muestra la descripción de la variable seleccionada. OID, Tipo de variable (counter, gauge, INTEGER, etc), unidades en las que se presenta (octetos, packets, etc), acceso entre otros.

Tabla que contiene la información de cada una de las variables interrogadas.

Update System MIB Es una herramienta que permite de manera remota cambiar o  actualizar parámetros de identificación del dispositivo tales como System Name, Location, y Contact. Update System MIB solicita la dirección IP o el nombre del host junto con el SNMP read-write community string para hacer los cambios.

SNMP Graph (Reporte gráfico de SNMP): Monitoriza y grafica las estadísticas de cualquier OID de una MIB que responde a SNMP. Esta herramienta puede monitorizar varios elementos al mismo tiempo y graficar su comportamiento en la misma pantalla.

MIB Walk: esta herramienta como su nombre lo dice, recorre el árbol SNMP de un dispositivo y a partir de la base de datos de MIBs proporcionada por Solarwinds , genera una tabla que contiene todas las MIBs y OIDs soportados por el dispositivo.

MIB Viewer: Usa la amplia base de datos de MIBs de Solarwinds, para desplegar un OID específico o una tabla. Este proporciona los mismos resultados del MIB Browser pero es un método rápido de recuperar MIBs frecuentemente usadas.

Herramientas de Seguridad (Security)

Security Check: se trata de una herramienta que permite examinar la seguridad de un router o switch catalyst de Cisco intentando entrar al dispositivo e indicando si el IOS puede ser actualizado. La herramienta intenta determinar la comunidad SNMP read-only y read-write. Una vez se conoce la comunidad SNMP read-write, se puede descargar la configuración del dispositivo y modificarla. Router Security Check solo puede irrumpir en dispositivos donde se detecta un alto nivel de vulnerabilidad.

Router Password Decrypt: La herramienta permite descifrar contraseñas de tipo 7 de Cisco. Los passwords tipo 7 son comúnmente usados para terminales y conexiones habilitadas sobre switches y enrutadores Cisco. Se debe tener el password cifrado para poderlo descifrar. La secuencia de caracteres cifrados es tomada normalmente de la configuración impresa del Cisco o descargando la configuración directamente del enrutador o switch. Se requiere la dirección IP del dispositivo y la comunidad SNMP de lectura/escritura.

Remote TCP Session Reset: permite visualizar remotamente todas las sesiones activas, sobre un servidor, enrutador, servidor de acceso, etc. Permite resetear una sesión remotamente.

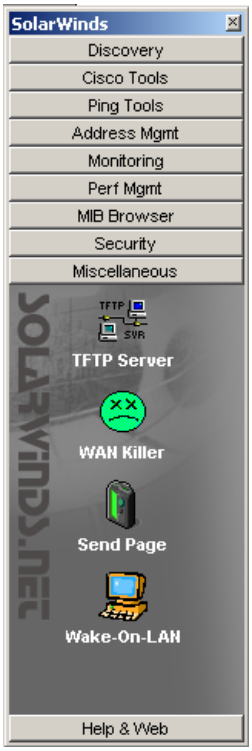
SNMP Brute Force Attack: El ataque SNMP de fuerza bruta puede determinar remotamente la secuencia de caracteres de una comunidad SNMP de solo lectura o de lectura/escritura, probando todas las posibles combinaciones de letras y números. La herramienta puede ser personalizada para que solo intente con ciertos caracteres o secuencias de cierta longitud. La velocidad del ataque también puede ser personalizada.

SNMP Dictionary Attack: Esta herramienta ha sido desarrollada para compañías que quieran estar seguras de que la secuencia de caracteres elegida como comunidad SNMP es segura. Esta herramienta no solo ataca agresivamente la red, le permite al usuario importar sus propios diccionarios en el

modulo de ataque. La herramienta cuenta con una gran variedad de diccionarios precargados, comúnmente usados por la comunidad de hackers, así como un editor de diccionarios que le permite realizar modificaciones o combinaciones de ellos.

Edit Dictionaries: Se usa junto con la herramienta para ataque de diccionario de SNMP, es la aplicación que permite editar los diccionarios disponibles en la herramienta y hacer modificaciones o combinaciones de ellos, además permite importar o exportar otros diccionarios ya existentes.

Herramientas Misceláneas (Miscellaneus Tools)



TFTP server: Servidor TFTP que le permite transmitir y recibir archivos con una probabilidad de error muy baja. Este servidor ofrece avanzadas características de seguridad. Soporta múltiples conexiones simultáneas a diferencia de la gran mayoría. Dentro de las características de seguridad ofrecidas permite que este sea configurado para transmitir o recibir o para los dos procesos, además permite evitar el acceso de determinadas direcciones IP al servidor. Se puede configurar el servidor para que después de un tiempo especificado de inactividad se apague automáticamente. El servidor puede guardar un registro en un documento de texto de todas las peticiones recibidas

WAN killer: Generador de tráfico WAN, con solo proporcionar el ancho de banda del enlace y la carga necesitada WAN killer puede generar tráfico randomico. El tamaño de los paquetes puede ser ajustado.

Target Hostname or IP Address: Servidor, enrutador o dispositivo remote. Esta es la dirección IP a la que será enviado el tráfico.

Port: puerto remoto al que será enviado el tráfico. Este puede ser seleccionado de la lista o puede ser agregado.

Si se usa el puerto 7 (echo), el tráfico recibido por el dispositivo destino es enviado de regreso al WAN killer por lo tanto la carga será generada en los dos sentidos. Si por el contrario se emplea el puerto 9 (discard), este descartara todos los paquetes que reciba de esta manera la carga se hará en un solo sentido.

Packet Size: tamaño en bytes de los paquetes enviados, porcentaje del ancho de banda que se quiere ocupar.

Circuit Bandwidth: tamaño del circuito o enlace WAN en Kbps (miles de bits por segundo).

Send E-mail / page: esta herramienta es una buena alternativa que permite

enviar de manera rápida y fácil un mensaje de correo o un beeper. Antes de enviar el correo se debe especificar un gateway de correo, se proporciona el nombre de dominio a la IP del gateway y se prueba la conexión con el haciendo click en test gateway. Send page usa SMTP puerto 25 para enviar los mensajes de correo al gateway.

Remote Wake-On-LAN: esta herramienta puede transmitir un paquete "mágico" hacia un determinado dispositivo o servidor y encenderlo remotamente, asumiendo que la tarjeta de red o la mother board han sido configuradas para soportar Wake-On-LAN. Configuración de la BIOS, habilitar la tarjeta de red para activar el dispositivo.

ANEXO B. Inventario Red UIS

En este anexo se presentan las tablas de datos obtenidos como producto de la etapa de documentación de red. Se presenta una tabla con la información relacionada con los servidores externos dentro de la red, al decir externos se hace referencia a que los servicios ofrecidos por estas estaciones pueden ser accedidos desde fuera de las instalaciones de la Universidad. Una segunda tabla que presenta los servicios instalados en cada una de dichas estaciones.

En el caso de los switches se proporciona la información relacionada con la ubicación del dispositivo, la dirección IP, dirección de hardware, así como la información de las subredes asociadas a el mediante la definición de VLANs.

Se presenta además un listado de las distintas subredes que forman parte de la red institucional y el número y listado de direcciones IP en uso dentro de cada una de ellas.

Toda esta información puede ser modificada y revisada mediante el uso de la base de datos desarrollada para tal fin.

Inventario Servidores Universidad Industrial de Santander						
Dirección IP externa	**Dirección IP**	**Nombre de dominio**	**Dirección MAC**	**Sistema operativo**	**Información adicional**	**Ubicación**
200.21.228.6	192.168.19.2	condor.uis.edu.co	0800.690D.A490	Red Hat Linux release 9 (shrike)	Servidor Correo, DNS, MX	Puerto : 1/21 Switch: AdminAlaOriental (192.168.5.71)
200.21.228.15	192.168.19.6	pelicano.uis.edu.co	0800.6905.6A64	Silicon Graphics	Servidor Biblioteca	Puerto: 1/6 Switch: AdminAlaOriental (192.168.5.71)
200.21.228.7	192.168.19.7	tucan.uis.edu.co	0800.690A.3FE8	Silicon Graphics	Cromatografia	Puerto: 1/21 Switch : Posgrados (192.168.5.12)
200.21.228.8	192.168.19.8	copeton.uis.edu.co	0050.8B788C95	Linux Slackware 7	Servidor escuela de Matemáticas	Puerto: 1/21 Switch: Lab. Livianos (192.168.5.17)
200.21.228.12	192.168.19.12	cormoran.uis.edu.co	00C0.9F2B.E042	Linux Red Hat	Ing. Sistemas servidor web	Puerto : 1/16 Switch : Lab. Pesados (192.168.5.6)
200.21.228.11	192.168.19.15	dodo.uis.edu.co	0800.20C3.F56C	Sun Microsystem	Servidor Web	Puerto : 1/8 Switch: AdminAlaOriental (192.168.5.71)

200.21.228.22	192.168.19.17	dsi01.uis.edu.co	0000.E23D.45C1	Windows 98-SE	PC Ing. BPM	Puerto: 1/3 Switch: AdminAlaOriental (192.168.5.71)
200.21.228.18	192.168.19.18	quetzal.uis.edu.co	0000.21C7.6CFB	Linux Mandrake	Servidor Ing. Eléctrica	Puerto: 1/13 Switch: Lab. Pesados (192.168.5.6)
200.21.227.23	192.168.19.23	gavilan.uis.edu.co	0040.9D20.06DC	Windows	Servidor Facultad de Salud	Puerto: 1/21 Switch : Aud. L.G. Salud (192.168.5.31)
200.21.228.32	192.168.19.32	albatros.uis.edu.co	00B0.D0EA.6035	Linux Mandrake release 8.0 (Traktopel)	Servidor Web, Correo Ing. Civil	Puerto: 1/17 Switch: Geomática (192.168.5.60)
200.21.228.33	192.168.19.33	garza .uis.edu.co	0800.690B.5BD5	Silicon Graphics	No Disponible	Puerto : 1/12 Switch: Geomática (192.168.5.60)
200.21.228.39	192.168.19.39	gorrion.uis.edu.co	0050.BF0A.96B2	Linux Mandrake	Servidor Escuela de Quimica	Puerto: 1/22 Switch: Posgrados (192.168.5.12)
200.21.228.51	192.168.19.51	carpintero.uis.edu.co	0008.74A8.39C1	Windows NT	Servidor Esc. Ing. Industrial	Puerto: 1/21 Switch: Ing. Industrial (192.168.5.9)
200.21.228.10	192.168.19.52	tux.uis.edu.co	00C0.9F0A.874A	Linux Red Hat release 9 (shrike)	Facultad de Ciencias DIF	Puerto: 1/3 Switch: Posgrados (192.168.5.12)

200.21.228.54	192.168.19.54	pinguino.uis.edu.co	0002.B3E7.4C5B	Linux Red Hat release 9 (shrike)	Servidor Grupo CPS Ing. Eléctrica	Puerto : 1/20 Switch: Ing. Electrica (192.168.5.10)
200.21.228.56	192.168.19.56	garceta.uis.edu.co	0060.97CF.B0A1	Windows 2000	Servidor Mecánica	Puerto 1/6 Switch: Lab. Pesados (192.168.5.6)
200.21.228.57	192.168.19.57	condorito.uis.edu.co	00E0.7D75.6FD2	Linux Red Hat	Servidor Geomatica	Puerto 1/13 Switch: Geomática (192.168.5.60)
200.21.228.59	192.168.19.59	pinzon.uis.edu.co	00E0.7D8C.9502	Linux Mandrake	Servidor Grupo Halley	Puerto 1/24 Switch: Posgrados (192.168.5.12)
200.21.228.36	192.168.19.62	guacharo.uis.edu.co	0050.0466.54EE	Linux	Servidor Escuela de Química	Puerto 1/23 Switch: Posgrados (192.168.5.12)
200.21.228.38	192.168.19.63	kiwi.uis.edu.co	0800.690B.5BD3	Silicon Graphics	No disponible	Puerto 1/4 Switch: Geomática (192.168.5.60)
200.21.228.3	192.168.19.70	tyrano.uis.edu.co	0800.6905.A030	Silicon Graphics	Servidor DNS alternativo	Puerto 1/11 Switch: AdminAlaOriental (192.168.5.71)

200.21.228.70	192.168.37.24	crai.uis.edu.co	000D.606B.3C2E	No disponible	Servidor Proyecto CRAI	Puerto: 1/18 (Hub) Switch: AdminAlaOriental (192.168.5.71)
200.21.228.76	192.168.37.27	alcatraz.uis.edu.co	000F.1F68.17AB	Linux	Servidor DELL Evaluzación Docente DSI	Puerto: 1/18 (Hub) Switch: AdminAlaOriental (192.168.5.71)
200.21.228.5	192.168.37.163	colibrí.uis.edu.co	00C0.9F1A.3BF4	Windows 2000	Servidor Acceso LIBRUIS via web	Puerto: 1/18 (Hub) Switch: AdminAlaOriental (192.168.5.71)
No disponible	192.168.37.66	hades.uis.edu.co	0006.5B5C.E28A	Windows XP	No disponible	Puerto: 1/18 (Hub) Switch: AdminAlaOriental (192.168.5.71)
200.21.228.47	192.168.37.160	perdiz.uis.edu.co	0090.276A.F01E	Windows 2000	Servidor Temporal Intranet	Puerto: 1/17 Switch: AdminAlaOriental (192.168.5.71)
200.21.228.34	192.168.37.166	halcon.uis.edu.co	000B.DB8F.E0E8	UNIX	Servidor Web UIS pruebas	Puerto: 1/4 Switch: AdminAlaOriental (192.168.5.71)
No disponible	192.168.37.161	aguila.uis.edu.co	0050.8BE9.7EA7	IRIX 6.2-6.5	No disponible	Puerto: 1/22 Switch: AdminAlaOriental (192.168.5.71)

200.21.228.17	192.168.37.164	alpha.uis.edu.co	000B.CD03.80EE	UNIX	Servidor Desarrollo Unired	Puerto: 1/9 Switch: AdminAlaOriental (192.168.5.71)
200.21.228.35	192.168.31.96	serceiam.uis.edu.co	0006.5BC7.1E7F	Windows	Servidor Web CEIAM	Puerto: 1/16 Switch: Cicelpa (192.168.5.8)
200.21.228.27	192.168.24.62	clarinero.uis.edu.co	0800.690A.B04A	IRIX	Servidor Web Especialización Geomatica	Puerto: 1/19 Switch: Geomática (192.168.5.60)
200.21.228.55	192.168.24.70	oca.uis.edu.co	0050.8BEC.43C6	Windows 2000 server	Ingenieria Civil Servidor de mapas http	Puerto: 1/120 Switch: Geomática (192.168.5.60)
200.21.228.53	192.168.94.53	milano.uis.edu.co	0800.20A2.E2FB	Linux Red Hat	CIDLIS Servidor Web	Puerto: 1/8 Switch: Bucarica (192.168.5.21)
200.21.228.37	192.168.94.52	flamingo.uis.edu.co	0800.20A7.2776	Linux Red Hat	CIDLIS Servidor Web	Puerto: 1/8 Switch: Bucarica (192.168.5.21)
200.21.228.60	192.168.50.70	Insed.uis.edu.co	0050.8BE7.6026	Linux Mandrake	Servidor Web INSED, Correo, FTP	Puerto: 1/21 Switch: Ciencias Humanas (192.168.5.11)
200.21.228.20	192.168.20.68	ced19.uis.edu.co	No disponible	Linux	Servidor CEDEUIS	Puerto: 1/13 Switch: AdminAlaOriental (192.168.5.71)

200.21.228.21	192.168.20.74.	ced25.uis.edu.co	0006.5BF1.8635	No disponible	Servidor web Grupo GENTE	Puerto: 1/12 Switch: AdminAlaOriental (192.168.5.71)
200.21.228.23	192.168.6.56	ctr02.uis.edu.co	00C0.9F23.64A4	Windows NT	Servidor FTP CINTROP guatiguara	Puerto: 1/X Switch: Guatguara (192.168.5.76)
200.21.228.24	192.168.6.11	cic02.uis.edu.co	0090.27C2.2310	Windows NT	Servidor Web Corrosión Guatiguara	Puerto: 1/X Switch: Guatguara (192.168.5.76)
200.21.228.41	192.168.45.77	ele97.uis.edu.co	0009.6BCF.C3EC	Linux	Servidor Grupo GISEL	Puerto: 1/14 Switch: Alta Tensión (192.168.5.22)
200.21.228.71	192.168.88.29	default-yax8n3n.uis.edu.do	0090.27C2.2310	No disponible	Servidor Web Sala de Informatica CPIP	Puerto: 1/14 Switch:Edificio J. Bautista (192.168.5.16)
200.21.228.52	192.168.50.56	insed49.uis.edu.co	0008.020A.042E	Windows	PC pruebas videoconferencia con Webcam	Puerto: 1/1 Switch: Ciencias Humanas (192.168.5.11)
200.21.228.49	192.168.50.139	aulainsed.uis.edu.co	000B.DB8F.708F	No disponible	Aula Virtual INSED web, correo, Ftp, ssh	Puerto: 1/1 Switch: Ciencias Humanas (192.168.5.11)
200.21.228.19	192.168.37.131	estp03.uis.edu.co	000B.DB8F.E31F	No disponible	Sist inf Banco de programas y Proy. Planeación	Puerto: 1/10 Switch: AdminAlaOriental (192.168.5.71)

Inventario Switches Universidad Industrial de Santander					
Dirección IP	**Identificación**	**Dirección MAC**	**Generalidades**	**Subredes Asociadas**	**Localización**
192.168.5.3	**DiseñoIndustrial**	00400D8A3CC4	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.34.0 (Diseño Industrial)	Edificio Federico Mamitza
192.168.5.4	**MantenPlantaF**	00400D8A3CAB	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.42.0 (Planta Física)	Mantenimiento y Planta Fisica
192.168.5.5	**bien-univ**	00400D8A3FEC	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.35.0 (Bienestar)	Bienestar Universitario
192.168.5.6	**Lab Pesados**	00400D8A3C2E	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.24.0 (Lab. Pesados) 192.168.46.0 (Eléctrica) 192.168.84.0 (Sistemas1) 192.168.19.0 (Servidores) 192.168.43.0 (Mecánica) 192.168.94.0 (CIDLIS) 192.168.65.0 (Sistemas Lab. JAV)	Ed. Laboratorio de pesados
192.168.5.7	**lab-lea**	00400D8A4014	24 puertos 10/100Base-Tx+ 1 1000Base-Sx uplink	192.168.22.0 (LEA) 192.168.61.0 (LEA Salas 2-3-5) 192.168.62.0 (LEA Salas 4-6) 192.168.19.0 (Servidores)	Laboratorio LEA
192.168.5.8	**cicelpa**	00400D8A3CA2	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.31.0 (Cicelpa)	Cicelpa
192.168.5.9	**ing-ind**	00400D8A3B15	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.40.0 (Ing. Industrial) 192.168.19.0 (Servidores)	Edificio Ing. Industrial
192.168.5.10	**ing-electrica**	00400D8A401C	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.46.0 (Eléctrica) 192.168.19.0 (Servidores)	Edificio Eléctica Nueva Secretaría

192.168.5.11	**ciencias-hum.**	00400D8A3B15	24 puertos 10/100Base-Tx+ 1 1000Base-Sx uplink	192.168.50.0 (INSED) 192.168.20.0 (Ciencias Humanas) 192.168.19.0 (Servidores) 192.168.107.0 (Inst. Lenguas) 192.168.21.0 (Educación) 192.168.89.0 (Publicaciones)	Ciencias humanas
192.168.5.12	**POSTGRADOS**	00400D8A3CF4	24 puertos 10/100Base-Tx+ 1 1000Base-Lx uplink	192.168.41.0 (Posgrados) 192.168.19.0 (Servidores)	Edificio Lab. Posgrados Oficina 300
192.168.5.13	**biblioteca**	00400D8A4071	24 puertos 10/100Base-Tx+ 1 1000Base-Sx uplink	192.168.18.0 (Biblioteca) 192.168.23.0 (BaseDatos)	Edificio Biblioteca
192.168.5.14	**esc-art**	00400D8A3CEC	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.32.0 (Artes) 192.168.50.0 (Insed)	Escuela de artes
192.168.5.15	**ing-quimica**	00400D8A2174	24 puertos 10/100Base-Tx+ 1 1000Base-Sx uplink	192.168.44.0 (Petroleos) 192.168.19.0 (Servidores)	Edificio Ingeniería Química
192.168.5.16	**jbautista**	00400D8AEA53	24 puertos 10/100Base-Tx+ 1 1000Base-Lx uplink	192.168.44.0 (Petroleos) 192.168.88.0 (Petroleos CPIP) 192.168.19.0 (Servidores)	Edificio Jorge Bautista
192.168.5.17	**lab-livian**	00400D8A3CCE	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.27.0 (Lab. Livianos) 192.168.28.0 (Fisica1) 192.168.29.0 (Fisica2) 192.168.19.0 (Servidores)	Laboratorio de Livianos
192.168.5.18	**ing-mec**	00400D8A3EEA	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.43.0 (Mecánica)	Edificio Ingeniería Mecánica
192.168.5.19	**LuisACalvo**	00400DC03940	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.36.0 (LuisACalvo)	Auditorio Luis A. Calvo
192.168.5.20	**Liquidaciones**	00400D8A3FA8	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.36.0 (Luis A. Calvo) 192.168.38.0 (Ala Occidental) 192.168.42.0 (Planta Fisica)	Antigua Nacional de comercio

192.168.5.21	**bucarica**	00400D8A3BD7	24 puertos 10/100Base-Tx+ 1 1000Base-Lx uplink	192.168.54.0 (Bucarica) 192.168.75.0 (NodoPML) 192.168.94.0 (CIDLIS) 192.168.76.0 (Fundeuis) 192.168.92.0 (Asesorias) 192.168.73.0 (CITI) 192.168.96.0 (Teleuis) 192.168.93.0 (Incubadora Empresas)	Sede UIS-bucarica
192.168.5.22	**altatension**	00400D8A3D1F	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.45.0 (AltaTensión) 192.168.71.0 (AltaTensión Lab. Elect)	Edificio Eléctrica antigua Primer Piso
192.168.5.28	**centralfs**	00400D8A3CFC	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.30.0 (Salud Admon) 192.168.19.0 (Servidores)	Central facultad de salud
192.168.5.29	**HURGV-UIS**	00400D8ABE43	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.30.0 (Salud Admon)	Hospital URGV piso 5
192.168.5.30	**paramed**	00400D8A3FC0	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.30.0 (Salud Admon)	Paramédicas
192.168.5.31	**auditLCGalanSalud**	00400D8A406E	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.30.0 (Salud Admon) 192.168.19.0 (Servidores) 192.168.105.0 (Fisioterapia1) 192.168.106.0 (Nutrición)	Auditorio Luis Carlos Galán Sarmiento
192.168.5.60	**geomatica**	00400DC006BA	24 puertos 10/100Base-Tx+ 1 1000Base-Lx uplink	192.168.85.0 (Civil Geomatica) 192.168.87.0 (Civil Geomatica3) 192.168.24.0 (Lab. Pesados) 192.168.19.0 (Servidores)	Ed. Lab de Pesados Ing. Civil. Primer piso
192.168.5.71	**AdminAlaOriental**	00400DC03969	24 puertos 10/100Base-Tx+2 1000Base-Lx uplink	192.168.19.0 (Servidores) 192.168.37.0 (Ala Oriental) 192.168.20.0 (Ciencias Humanas) 192.168.38.0 (Ala Occidental) 192.168.81.0 (Planeación) 192.168.80.0 (DSI)	Edificio Administración Ala Oriental

192.168.5.73	**AdminAlaOccidental**	00400DC08756	24 puertos 10/100Base-Tx+ 1 1000Base-Lx uplink	192.168.38.0 (Ala Occidental) 192.168.59.0 (Admisiones) 192.168.58.0 (Financiero Tesorería) 192.168.97.0 (Recursos Humanos) 192.168.22.0 (LEA)	Edificio de Administración Ala Occidental
192.168.5.76	**Guatiguara**	00400DC0B542	24 puertos 10/100Base-Tx+ 2 100Base-F uplink	192.168.6.0	Rack 1 Guatiguara

Listado de subredes					
Identificación Subred	**Subred IP**	**Mascara**	**Direcciones en USO**	**Uso**	**Disponibles**
Avaya (switches)	192.168.5.0	255.255.255.0	192.168.5.1 192.168.5.3 192.168.5.4 192.168.5.5 192.168.5.6 192.168.5.7 192.168.5.8 192.168.5.9 192.168.5.10 192.168.5.11 192.168.5.12 192.168.5.13 192.168.5.14 192.168.5.15 192.168.5.16 192.168.5.17 192.168.5.18 192.168.5.19 192.168.5.20 192.168.5.21 192.168.5.22 192.168.5.28 192.168.5.29	36	218

			192.168.5.30 192.168.5.31 192.168.5.41 192.168.5.60 192.168.5.71 192.168.5.73 192.168.5.76 192.168.5.81 192.168.5.82 192.168.5.83 192.168.5.105 192.168.5.187		
Guatiguara	192.168.6.0	255.255.255.0	192.168.6.1 192.168.6.4 192.168.6.9 192.168.6.11 192.168.6.17 192.168.6.20 192.168.6.21 192.168.6.22 192.168.6.24 192.168.6.26 192.168.6.27 192.168.6.28 192.168.6.29 192.168.6.31	48	206

			192.168.6.32 192.168.6.56 192.168.6.64 192.168.6.66 192.168.6.68 192.168.6.70 192.168.6.72 192.168.6.75 192.168.6.84 192.168.6.85 192.168.6.86 192.168.6.91 192.168.6.102 192.168.6.104 192.168.6.106 192.168.6.110 192.168.6.111 192.168.6.141 192.168.6.142 192.168.6.144 192.168.6.171 192.168.6.182 192.168.6.200 192.168.6.202 192.168.6.203 192.168.6.204 192.168.6.205		

			192.168.6.207 192.168.6.208 192.168.6.209 192.168.6.211 192.168.6.214 192.168.6.220 192.168.6.232		
router (telecom)	192.168.9.0	255.255.255.248	192.168.9.1 192.168.9.2		
Biblioteca	192.168.18.0	255.255.255.0	192.168.18.1 192.168.18.11 192.168.18.12 192.168.18.13 192.168.18.15 192.168.18.17 192.168.18.18 192.168.18.20 192.168.18.21 192.168.18.22 192.168.18.23 192.168.18.24 192.168.18.25 192.168.18.26 192.168.18.27 192.168.18.28 192.168.18.29	41	213

			192.168.18.30 192.168.18.31 192.168.18.32 192.168.18.33 192.168.18.34 192.168.18.35 192.168.18.36 192.168.18.37 192.168.18.39 192.168.18.40 192.168.18.41 192.168.18.42 192.168.18.43 192.168.18.44 192.168.18.46 192.168.18.47 192.168.18.48 192.168.18.50 192.168.18.51 192.168.18.130 192.168.18.131 192.168.18.154 192.168.18.190		
Servidores	192.168.19.0	255.255.255.0	192.168.19.1 192.168.19.2 192.168.19.6	21	233

			192.168.19.7 192.168.19.8 192.168.19.12 192.168.19.15 192.168.19.17 192.168.19.18 192.168.19.32 192.168.19.33 192.168.19.39 192.168.19.51 192.168.19.52 192.168.19.54 192.168.19.56 192.168.19.57 192.168.19.62 192.168.19.63 192.168.19.70		
Ciencias Humanas	192.168.20.0	255.255.255.0	192.168.20.1 192.168.20.5 192.168.20.7 192.168.20.9 192.168.20.11 192.168.20.13 192.168.20.14 192.168.20.15 192.168.20.35	50	204

			192.168.20.36 192.168.20.43 192.168.20.50 192.168.20.55 192.168.20.58 192.168.20.59 192.168.20.62 192.168.20.64 192.168.20.65 192.168.20.69 192.168.20.70 192.168.20.73 192.168.20.74 192.168.20.75 192.168.20.132 192.168.20.133 192.168.20.142 192.168.20.143 192.168.20.149 192.168.20.150 192.168.20.155 192.168.20.158 192.168.20.165 192.168.20.174 192.168.20.175 192.168.20.183 192.168.20.191		

			192.168.20.212 192.168.20.213 192.168.20.227 192.168.20.228 192.168.20.240 192.168.20.241 192.168.20.242 192.168.20.244 192.168.20.245 192.168.20.246 192.168.20.247		
Educación	192.168.21.0	255.255.255.0	192.168.21.1 192.168.21.11 192.168.21.12 192.168.21.13 192.168.21.14 192.168.21.16 192.168.21.17 192.168.21.26 192.168.21.27 192.168.21.28 192.168.21.37	11	243
LEA	192.168.22.0	255.255.255.0	192.168.22.1 192.168.22.12 192.168.22.13 192.168.22.14	22	232

			192.168.22.15 192.168.22.16 192.168.22.17 192.168.22.18 192.168.22.19 192.168.22.85 192.168.22.87 192.168.22.92 192.168.22.93 192.168.22.110 192.168.22.120 192.168.22.121 192.168.22.122 192.168.22.126 192.168.22.160 192.168.22.161		
BiblioteBase de datos	192.168.23.0.	255.255.255.0	192.168.23.1 192.168.23.11 192.168.23.12 192.168.23.13 192.168.23.14 192.168.23.16 192.168.23.17 192.168.23.18 192.168.23.19 192.168.23.20	37	217

			192.168.23.22 192.168.23.23 192.168.23.24 192.168.23.25 192.168.23.27 192.168.23.28 192.168.23.29 192.168.23.30 192.168.23.31 192.168.23.32 192.168.23.33 192.168.23.34 192.168.23.35 192.168.23.36 192.168.23.37 192.168.23.38 192.168.23.39 192.168.23.40 192.168.23.41 192.168.23.42 192.168.23.43 192.168.23.44 192.168.23.46 192.168.23.47 192.168.23.50 192.168.23.51 192.168.23.55		

Lab. Pesados	192.168.24.0	255.255.255.0	192.168.24.1 192.168.24.11 192.168.24.26 192.168.24.27 192.168.24.29 192.168.24.30 192.168.24.33 192.168.24.40 192.168.24.59 192.168.24.62 192.168.24.65 192.168.24.70 192.168.24.73 192.168.24.85 192.168.24.102 192.168.24.105 192.168.24.106 192.168.24.120 192.168.24.121 192.168.24.122 192.168.24.123 192.168.24.125 192.168.24.126 192.168.24.127 192.168.24.129 192.168.24.130 192.168.24.134	41	213

			192.168.24.144 192.168.24.145 192.168.24.146 192.168.24.147 192.168.24.148 192.168.24.150 192.168.24.189 192.168.24.244		
Lab. Livianos	192.168.27.0	255.255.255.0	192.168.27.1 192.168.27.3 192.168.27.15 192.168.27.19 192.168.27.20 192.168.27.28 192.168.27.45 192.168.27.48 192.168.27.52 192.168.27.54 192.168.27.55 192.168.27.65 192.168.27.68 192.168.27.69 192.168.27.70 192.168.27.83 192.168.27.86 192.168.27.87	52	202

			192.168.27.101 192.168.27.106 192.168.27.109 192.168.27.110 192.168.27.165 192.168.27.166 192.168.27.176 192.168.27.179 192.168.27.181 192.168.27.182 192.168.27.183 192.168.27.184 192.168.27.185 192.168.27.186 192.168.27.187 192.168.27.188 192.168.27.189 192.168.27.190 192.168.27.192 192.168.27.193 192.168.27.194 192.168.27.195 192.168.27.199 192.168.27.200 192.168.27.250		
Fisica1	192.168.28.0	255.255.255.0	192.168.28.1	10	244

			192.168.28.11 192.168.28.13 192.168.28.15 192.168.28.16 192.168.28.17 192.168.28.20 192.168.28.21 192.168.28.24		
Fisica2	192.168.29.0	255.255.255.0	192.168.29.1 192.168.29.13 192.168.29.14	4	250
Salud Admon.	192.168.30.0	255.255.255.0	192.168.30.1 192.168.30.5 192.168.30.6 192.168.30.7 192.168.30.8 192.168.30.9 192.168.30.10 192.168.30.11 192.168.30.12 192.168.30.13 192.168.30.14 192.168.30.20 192.168.30.27 192.168.30.31 192.168.30.38	120	134

			192.168.30.40 192.168.30.43 192.168.30.45 192.168.30.47 192.168.30.48 192.168.30.49 192.168.30.51 192.168.30.56 192.168.30.58 192.168.30.59 192.168.30.60 192.168.30.63 192.168.30.64 192.168.30.65 192.168.30.66 192.168.30.67 192.168.30.69 192.168.30.74 192.168.30.77 192.168.30.81 192.168.30.82 192.168.30.83 192.168.30.84 192.168.30.85 192.168.30.86 192.168.30.87 192.168.30.88		

			192.168.30.89 192.168.30.90 192.168.30.91 192.168.30.92 192.168.30.95 192.168.30.96 192.168.30.98 192.168.30.100 192.168.30.102 192.168.30.103 192.168.30.108 192.168.30.111 192.168.30.114 192.168.30.116 192.168.30.121 192.168.30.126 192.168.30.127 192.168.30.128 192.168.30.132 192.168.30.133 192.168.30.134 192.168.30.135 192.168.30.136 192.168.30.138 192.168.30.141 192.168.30.143 192.168.30.150		

			192.168.30.151 192.168.30.152 192.168.30.162 192.168.30.163 192.168.30.165 192.168.30.168 192.168.30.169 192.168.30.170 192.168.30.178 192.168.30.181 192.168.30.184 192.168.30.186 192.168.30.191 192.168.30.192 192.168.30.194 192.168.30.197 192.168.30.198 192.168.30.202 192.168.30.203 192.168.30.206 192.168.30.214 192.168.30.217 192.168.30.220 192.168.30.224 192.168.30.225 192.168.30.226 192.168.30.230		

			192.168.30.241 192.168.30.248 192.168.30.249 192.168.30.250 192.168.30.252 192.168.30.254		
Cicelpa	192.168.31.0	255.255.255.0	192.168.31.1 192.168.31.11 192.168.31.12 192.168.31.28 192.168.31.31 192.168.31.34 192.168.31.42 192.168.31.43 192.168.31.48 192.168.31.50 192.168.31.52 192.168.31.90 192.168.31.93 192.168.31.94 192.168.31.95 192.168.31.96 192.168.31.98 192.168.31.100 192.168.31.101 192.168.31.102	23	231

			192.168.31.104		
Artes	192.168.32.0	255.255.255.0	192.168.32.1 192.168.32.11 192.168.32.13 192.168.32.14	4	250
Capruis	192.168.33.0	255.255.255.0	192.168.33.1 192.168.33.18 192.168.33.19 192.168.33.20 192.168.33.21 192.168.33.23 192.168.33.25 192.168.33.26 192.168.33.27 192.168.33.30 192.168.33.254	12	242
Diseño Industrial	192.168.34.0	255.255.255.0	192.168.34.1 192.168.34.11 192.168.34.13 192.168.34.15 192.168.34.16 192.168.34.18 192.168.34.19 192.168.34.20 192.168.34.21 192.168.34.22	38	216

			192.168.34.23 192.168.34.24 192.168.34.25 192.168.34.26 192.168.34.27 192.168.34.28 192.168.34.29 192.168.34.32 192.168.34.34 192.168.34.35 192.168.34.36 192.168.34.37 192.168.34.38 192.168.34.39 192.168.34.47 192.168.34.54 192.168.34.60 192.168.34.92 192.168.34.99 192.168.34.103 192.168.34.190 192.168.34.199		
Bienestar	192.168.35.0	255.255.255.0	192.168.35.1 192.168.35.11 192.168.35.12 192.168.35.13	25	229

			192.168.35.14 192.168.35.15 192.168.35.16 192.168.35.17 192.168.35.18 192.168.35.19 192.168.35.21 192.168.35.22 192.168.35.23 192.168.35.24 192.168.35.25 192.168.35.27 192.168.35.28 192.168.35.29 192.168.35.30 192.168.35.34 192.168.35.35 192.168.35.37 192.168.35.38 192.168.35.61 192.168.35.62		
Luis A. Calvo	192.168.36.0	255.255.255.0	192.168.36.1 192.168.36.6 192.168.36.7 192.168.36.8 192.168.36.10	5	249

Ala Oriental	192.168.37.0	255.255.255.0	192.168.37.13 192.168.37.21 192.168.37.22 192.168.37.24 192.168.37.27 192.168.37.40 192.168.37.41 192.168.37.43 192.168.37.44 192.168.37.45 192.168.37.48 192.168.37.49 192.168.37.57 192.168.37.59 192.168.37.60 192.168.37.61 192.168.37.62 192.168.37.65 192.168.37.66 192.168.37.67 192.168.37.68 192.168.37.69 192.168.37.96 192.168.37.131 192.168.37.160 192.168.37.161 192.168.37.163	33	221

			192.168.37.164 192.168.37.166 192.168.37.215 192.168.37.251		
Ala Occidental	192.168.38.0	255.255.255.0	192.168.38.1 192.168.38.11 192.168.38.12 192.168.38.15 192.168.38.21 192.168.38.22 192.168.38.23 192.168.38.24 192.168.38.25 192.168.38.26 192.168.38.27 192.168.38.29 192.168.38.30 192.168.38.31 192.168.38.48 192.168.38.51 192.168.38.53 192.168.38.54 192.168.38.61 192.168.38.63 192.168.38.64 192.168.38.66	58	196

			192.168.38.68 192.168.38.77 192.168.38.82 192.168.38.84 192.168.38.85 192.168.38.87 192.168.38.92 192.168.38.93 192.168.38.94 192.168.38.107 192.168.38.109 192.168.38.110 192.168.38.113 192.168.38.116 192.168.38.117 192.168.38.118 192.168.38.123 192.168.38.126 192.168.38.128 192.168.38.129 192.168.38.130 192.168.38.131 192.168.38.132 192.168.38.133 192.168.38.135 192.168.38.136 192.168.38.137		

			192.168.38.138 192.168.38.144 192.168.38.160 192.168.38.168 192.168.38.180 192.168.38.181		
Ing. Química	192.168.39.0	255.255.255.0	192.168.39.1 192.168.39.13 192.168.39.14 192.168.39.17 192.168.39.21 192.168.39.24 192.168.39.28 192.168.39.30 192.168.39.44 192.168.39.49 192.168.39.50 192.168.39.61 192.168.39.70 192.168.39.71 192.168.39.85 192.168.39.87 192.168.39.92 192.168.39.110 192.168.39.113 192.168.39.117	30	224

			192.168.39.121 192.168.39.124 192.168.39.125 192.168.39.126 192.168.39.127 192.168.39.130 192.168.39.148 192.168.39.153 192.168.39.156 192.168.39.163		
Ing. Industrial	192.168.40.0	255.255.255.0	192.168.40.1 192.168.40.12 192.168.40.14 192.168.40.15 192.168.40.18 192.168.40.19 192.168.40.20 192.168.40.22 192.168.40.24 192.168.40.27 192.168.40.29 192.168.40.31 192.168.40.34 192.168.40.35 192.168.40.36 192.168.40.44	32	222

			192.168.40.45 192.168.40.48 192.168.40.66 192.168.40.77 192.168.40.79 192.168.40.80 192.168.40.81 192.168.40.85 192.168.40.86 192.168.40.127		
Postgrados	192.168.41.0	255.255.255.0	192.168.41.1 192.168.41.21 192.168.41.31 192.168.41.32 192.168.41.35 192.168.41.40 192.168.41.42 192.168.41.44 192.168.41.45 192.168.41.51 192.168.41.52 192.168.41.53 192.168.41.54 192.168.41.55 192.168.41.75 192.168.41.76	78	176

			192.168.41.81 192.168.41.82 192.168.41.86 192.168.41.87 192.168.41.88 192.168.41.90 192.168.41.93 192.168.41.94 192.168.41.97 192.168.41.100 192.168.41.102 192.168.41.103 192.168.41.104 192.168.41.107 192.168.41.110 192.168.41.111 192.168.41.112 192.168.41.113 192.168.41.116 192.168.41.124 192.168.41.128 192.168.41.145 192.168.41.146 192.168.41.147 192.168.41.148 192.168.41.149 192.168.41.150		

			192.168.41.151 192.168.41.152 192.168.41.153 192.168.41.154 192.168.41.160 192.168.41.162 192.168.41.164 192.168.41.172 192.168.41.191 192.168.41.192 192.168.41.201 192.168.41.202 192.168.41.203 192.168.41.204 192.168.41.205 192.168.41.230 192.168.41.235 192.168.41.236 192.168.41.248 192.168.41.249 192.168.41.250 192.168.41.251 192.168.41.253 192.168.41.254		
Planta Física	192.168.42.0	255.255.255.0	192.168.42.1 192.168.42.8	17	237

			192.168.42.14 192.168.42.18 192.168.42.20 192.168.42.22 192.168.42.28 192.168.42.41 192.168.42.52 192.168.42.54 192.168.42.55 192.168.42.56 192.168.42.57 192.168.42.61 192.168.42.63		
Mecánica	192.168.43.0	255.255.255.0	192.168.43.1 192.168.43.14 192.168.43.16 192.168.43.21 192.168.43.22 192.168.43.23 192.168.43.24 192.168.43.26 192.168.43.27 192.168.43.28 192.168.43.29 192.168.43.30 192.168.43.34	21	203

			192.168.43.35 192.168.43.36 192.168.43.39 192.168.43.40 192.168.43.41 192.168.43.43 192.168.43.44 192.168.43.46 192.168.43.47 192.168.43.50 192.168.43.51 192.168.43.52 192.168.43.53 192.168.43.54 192.168.43.55 192.168.43.56 192.168.43.57 192.168.43.58 192.168.43.59 192.168.43.60 192.168.43.61 192.168.43.62 192.168.43.67 192.168.43.68 192.168.43.69 192.168.43.70 192.168.43.74		

			192.168.43.78 192.168.43.79 192.168.43.80 192.168.43.81 192.168.43.83 192.168.43.87 192.168.43.89 192.168.43.90		
Petróleos	192.168.44.0	255.255.255.0	192.168.44.1 192.168.44.5 192.168.44.12 192.168.44.14 192.168.44.15 192.168.44.16 192.168.44.20 192.168.44.31 192.168.44.33 192.168.44.36 192.168.44.40 192.168.44.41 192.168.44.50 192.168.44.52 192.168.44.53 192.168.44.54 192.168.44.55 192.168.44.62	74	180

			192.168.44.65 192.168.44.69 192.168.44.71 192.168.44.75 192.168.44.83 192.168.44.87 192.168.44.89 192.168.44.91 192.168.44.93 192.168.44.96 192.168.44.100 192.168.44.101 192.168.44.102 192.168.44.104 192.168.44.107 192.168.44.109 192.168.44.110 192.168.44.111 192.168.44.112 192.168.44.113 192.168.44.114 192.168.44.115 192.168.44.116 192.168.44.121 192.168.44.125 192.168.44.126 192.168.44.127		

			192.168.44.128 192.168.44.129 192.168.44.130 192.168.44.131 192.168.44.132 192.168.44.133 192.168.44.134 192.168.44.135 192.168.44.136 192.168.44.137 192.168.44.138 192.168.44.142 192.168.44.149 192.168.44.151 192.168.44.153 192.168.44.169 192.168.44.178 192.168.44.198 192.168.44.205 192.168.44.211 192.168.44.215 192.168.44.240 192.168.44.241 192.168.44.244		
Alta tensión	192.168.45.0	255.255.255.0	192.168.45.1 192.168.45.20	39	215

			192.168.45.32 192.168.45.33 192.168.45.34 192.168.45.35 192.168.45.36 192.168.45.37 192.168.45.38 192.168.45.39 192.168.45.40 192.168.45.41 192.168.45.42 192.168.45.45 192.168.45.53 192.168.45.54 192.168.45.55 192.168.45.56 192.168.45.57 192.168.45.59 192.168.45.61 192.168.45.65 192.168.45.68 192.168.45.69 192.168.45.70 192.168.45.71 192.168.45.73 192.168.45.75 192.168.45.76		

			192.168.45.77 192.168.45.112 192.168.45.115 192.168.45.120		
Eléctrica	192.168.46.0	255.255.255.0	192.168.46.1 192.168.46.11 192.168.46.12 192.168.46.19 192.168.46.23 192.168.46.24 192.168.46.29 192.168.46.30 192.168.46.31 192.168.46.32 192.168.46.37 192.168.46.39 192.168.46.40 192.168.46.42 192.168.46.45 192.168.46.47 192.168.46.51 192.168.46.57 192.168.46.62 192.168.46.64 192.168.46.65 192.168.46.66	31	223

			192.168.46.68 192.168.46.69 192.168.46.145 192.168.46.150 192.168.46.176 192.168.46.251		
MorfoPatología	192.168.47.0	255.255.255.0	192.168.47.1	1	253
HURV	192.168.48.0	255.255.255.0	192.168.48.1	1	253
Sala Conferencias	192.168.49.0	255.255.255.0	192.168.49.1	1	253
INSED	192.168.50.1	255.255.255.0	192.168.50.1 192.168.50.10 192.168.50.12 192.168.50.14 192.168.50.15 192.168.50.18 192.168.50.19 192.168.50.20 192.168.50.21 192.168.50.22 192.168.50.23 192.168.50.24 192.168.50.27 192.168.50.28 192.168.50.30 192.168.50.31 192.168.50.32	61	193

			192.168.50.35 192.168.50.37 192.168.50.38 192.168.50.41 192.168.50.44 192.168.50.45 192.168.50.47 192.168.50.49 192.168.50.50 192.168.50.52 192.168.50.56 192.168.50.57 192.168.50.70 192.168.50.71 192.168.50.72 192.168.50.73 192.168.50.74 192.168.50.75 192.168.50.76 192.168.50.77 192.168.50.78 192.168.50.81 192.168.50.82 192.168.50.83 192.168.50.84 192.168.50.85 192.168.50.87		

			192.168.50.88 192.168.50.89 192.168.50.90 192.168.50.91 192.168.50.93 192.168.50.94 192.168.50.95 192.168.50.97 192.168.50.98 192.168.50.100 192.168.50.101 192.168.50.120 192.168.50.122 192.168.50.139 192.168.50.200		
Favuis	192.168.51.0	255.255.255.0	192.168.51.1	1	253
Bucarica	192.168.54.0	255.255.255.0	192.168.54.1 192.168.54.12 192.168.54.13 192.168.54.18 192.168.54.25 192.168.54.26 192.168.54.28 192.168.54.35 192.168.54.62 192.168.54.65	20	234

			192.168.54.82 192.168.54.83 192.168.54.84 192.168.54.215 192.168.54.217 192.168.54.233 192.168.54.242 192.168.54.243 192.168.54.244		
Financiero Tesorería	192.168.58.0	255.255.255.0	192.168.58.1 192.168.58.11 192.168.58.12 192.168.58.13 192.168.58.14 192.168.58.15 192.168.58.17 192.168.58.19 192.168.58.20 192.168.58.22 192.168.58.23 192.168.58.25 192.168.58.26 192.168.58.29 192.168.58.32 192.168.58.33 192.168.58.34	21	233

			192.168.58.35 192.168.58.37 192.168.58.55		
Admisiones	192.168.59.0	255.255.255.0	192.168.59.1 192.168.59.11 192.168.59.13 192.168.59.14 192.168.59.15 192.168.59.17 192.168.59.18 192.168.59.19 192.168.59.20 192.168.59.21 192.168.59.22 192.168.59.23 192.168.59.24 192.168.59.26	14	240
LEA salas2-3-5	192.168.61.0	255.255.255.0	192.168.61.1 192.168.61.11 192.168.61.12 192.168.61.13 192.168.61.14 192.168.61.15 192.168.61.16 192.168.61.17 192.168.61.18	58	196

			192.168.61.19 192.168.61.20 192.168.61.22 192.168.61.23 192.168.61.24 192.168.61.25 192.168.61.26 192.168.61.27 192.168.61.28 192.168.61.29 192.168.61.30 192.168.61.31 192.168.61.32 192.168.61.33 192.168.61.34 192.168.61.35 192.168.61.36 192.168.61.37 192.168.61.38 192.168.61.39 192.168.61.40 192.168.61.41 192.168.61.42 192.168.61.43 192.168.61.44 192.168.61.45 192.168.61.46		

			192.168.61.47 192.168.61.48 192.168.61.49 192.168.61.50 192.168.61.51 192.168.61.52 192.168.61.53 192.168.61.54 192.168.61.55 192.168.61.56 192.168.61.57 192.168.61.58 192.168.61.59 192.168.61.60 192.168.61.61 192.168.61.62 192.168.61.63 192.168.61.64 192.168.61.65 192.168.61.66 192.168.61.67 192.168.61.68		
LEA salas4-6	192.168.62.0	255.255.255.0	192.168.62.1 192.168.62.31 192.168.62.32 192.168.62.33	38	216

			192.168.62.34 192.168.62.35 192.168.62.36 192.168.62.37 192.168.62.38 192.168.62.39 192.168.62.40 192.168.62.41 192.168.62.42 192.168.62.43 192.168.62.44 192.168.62.45 192.168.62.46 192.168.62.47 192.168.62.48 192.168.62.53 192.168.62.54 192.168.62.55 192.168.62.56 192.168.62.57 192.168.62.58 192.168.62.59 192.168.62.60 192.168.62.61 192.168.62.62 192.168.62.63 192.168.62.64		

			192.168.62.65 192.168.62.66 192.168.62.67 192.168.62.68 192.168.62.69 192.168.62.70 192.168.62.71		
Alta Tensión Lab. Elec.	192.168.71.0	255.255.255.0	192.168.71.1 192.168.71.11 192.168.71.12 192.168.71.13 192.168.71.14 192.168.71.15 192.168.71.16 192.168.71.17 192.168.71.18 192.168.71.19 192.168.71.20 192.168.71.21 192.168.71.22 192.168.71.23 192.168.71.24 192.168.71.28 192.168.71.29	18	236
Hidraulica	192.168.72.0	255.255.255.0	192.168.72.1 192.168.72.17	3	251

			192.168.72.18		
CITI	192.168.73.0	255.255.255.0	192.168.73.1 192.168.73.11 192.168.73.12 192.168.73.13 192.168.73.14 192.168.73.15 192.168.73.16 192.168.73.17 192.168.73.18 192.168.73.19	10	244
CNBiling	192.168.74.0	255.255.255.0	192.168.74.1 192.168.74.14 192.168.74.15	3	251
Nodo PML	192.168.75.0	255.255.255.0	192.168.75.1 192.168.75.11 192.168.75.12 192.168.75.13 192.168.75.14 192.168.75.15 192.168.75.18 192.168.75.19 192.168.75.20 192.168.75.21	10	244
FUNDEUIS	192.168.76.0	255.255.255.0	192.168.76.1 192.168.76.11	8	246

			192.168.76.12 192.168.76.13 192.168.76.14 192.168.76.15 192.168.76.100 192.168.76.112		
DSI	192.168.80.0	255.255.255.0	192.168.80.1 192.168.80.11 192.168.80.12 192.168.80.16 192.168.80.19 192.168.80.21 192.168.80.23 192.168.80.25	8	246
Planeación Rectoria	192.168.81.0	255.255.255.0	192.168.81.1 192.168.81.11 192.168.81.12 192.168.81.13 192.168.81.14 192.168.81.15 192.168.81.17 192.168.81.18 192.168.81.20 192.168.81.21 192.168.81.22 192.168.81.25	18	236

			192.168.81.27 192.168.81.28 192.168.81.42 192.168.81.51 192.168.81.70 192.168.81.71		
Sistemas1	192.168.84.0	255.255.255.0	192.168.84.1 192.168.84.12 192.168.84.13 192.168.84.14 192.168.84.15 192.168.84.16 192.168.84.19 192.168.84.20 192.168.84.21 192.168.84.22 192.168.84.23 192.168.84.25 192.168.84.26 192.168.84.27 192.168.84.28 192.168.84.29 192.168.84.30 192.168.84.49 192.168.84.58 192.168.84.66	24	230

			192.168.84.68 192.168.84.70 192.168.84.215		
Civil Geomatica	192.168.85.0	255.255.255.0	192.168.85.1 192.168.85.14 192.168.85.27 192.168.85.28 192.168.85.29 192.168.85.42 192.168.85.51 192.168.85.53 192.168.85.58 192.168.85.61 192.168.85.103 192.168.85.105 192.168.85.106 192.168.85.108 192.168.85.109 192.168.85.110 192.168.85.111 192.168.85.112 192.168.85.118 192.168.85.120 192.168.85.200 192.168.85.201 192.168.85.202	56	198

			192.168.85.203 192.168.85.204 192.168.85.205 192.168.85.206 192.168.85.207 192.168.85.208 192.168.85.209 192.168.85.210 192.168.85.211 192.168.85.212 192.168.85.213 192.168.85.214 192.168.85.216 192.168.85.217 192.168.85.218 192.168.85.220 192.168.85.250		
Civil Geomatica2	192.168.86.0	255.255.255.0	192.168.86.1	1	253
Civil Geomatica3	192.168.87.0	255.255.255.0	192.168.87.1	1	253
Petroleos Sala CPIP	192.168.88.0	255.255.255.0	192.168.88.1 192.168.88.2 192.168.88.3 192.168.88.4 192.168.88.5 192.168.88.6 192.168.88.7	15	239

			192.168.88.8 192.168.88.13 192.168.88.29 192.168.88.30 192.168.88.31 192.168.88.32 192.168.88.34 192.168.88.35		
Publicaciones	192.168.89.0	255.255.255.0	192.168.89.1 192.168.89.13 192.168.89.14 192.168.89.15 192.168.89.16 192.168.89.18 192.168.89.19 192.168.89.20 192.168.89.21 192.168.89.22 192.168.89.23 192.168.89.24 192.168.89.26 192.168.89.27	14	240
Asesorias	192.168.92.0	255.255.255.0	192.168.92.1 192.168.92.15 192.168.92.18 192.168.92.19	7	247

			192.168.92.31 192.168.92.70 192.168.92.242		
Incubadora Empresas	192.168.93.0	255.255.255.0	192.168.93.1	1	253
CIDLIS	192.168.94.0	255.255.255.0	192.168.94.1 192.168.94.2 192.168.94.52 192.168.94.53 192.168.94.103 192.168.94.105 192.168.94.109 192.168.94.110 192.168.94.112 192.168.94.160 192.168.94.161 192.168.94.162 192.168.94.165 192.168.94.166 192.168.94.169 192.168.94.195	16	238
TELEUIS	192.168.96.0	255.255.255.0	192.168.96.1 192.168.96.12 192.168.96.13	3	251
Recursos Humanos	192.168.97.0	255.255.255.0	192.168.97.1 192.168.97.12 192.168.97.14	14	240

			192.168.97.15 192.168.97.16 192.168.97.17 192.168.97.18 192.168.97.20 192.168.97.21 192.168.97.22 192.168.97.24 192.168.97.25 192.168.97.26 192.168.97.78		
Sede Socorro 1	192.168.99.0	255.255.255.224	192.168.99.1		
Sede Socorro 2	192.168.99.32	255.255.255.224	192.168.99.34 192.168.99.35 192.168.99.36 192.168.99.37 192.168.99.38 192.168.99.39 192.168.99.40 192.168.99.41 192.168.99.43 192.168.99.44 192.168.99.45 192.168.99.46 192.168.99.51	13	17
Sede Socorro 4	192.168.99.96	255.255.255.224	192.168.99.98	11	19

			192.168.99.100 192.168.99.102 192.168.99.103 192.168.99.104 192.168.99.105 192.168.99.106 192.168.99.107 192.168.99.109 192.168.99.110 192.168.99.111		
Sede Socorro 5	192.168.99.128	255.255.255.224	192.168.99.129 192.168.99.130 192.168.99.140 192.168.99.149 192.168.99.150	5	25
Sede Socorro 6	192.168.99.160	255.255.255.224	192.168.99.181	1	29
Sede Barranca	192.168.100.0	255.255.255.0	192.168.100.1 192.168.100.66 192.168.100.68 192.168.100.69 192.168.100.70 192.168.100.71 192.168.100.72 192.168.100.74 192.168.100.75 192.168.100.76	25	229

			192.168.100.77 192.168.100.78 192.168.100.79 192.168.100.130 192.168.100.160 192.168.100.162 192.168.100.168 192.168.100.169 192.168.100.170 192.168.100.175 192.168.100.176		
Sede Malaga	192.168.101.0	255.255.255.0	192.168.101.1 192.168.101.12 192.168.101.14 192.168.101.32 192.168.101.33 192.168.101.37 192.168.101.39	12	242
Sede Barbosa	192.168.102.0	255.255.255.0	192.168.102.1 192.168.102.10 192.168.102.11 192.168.102.13	4	250
Fisioterapia1	192.168.105.0	255.255.255.0	192.168.105.1 192.168.105.12 192.168.105.13 192.168.105.14	4	250

Nutrición	192.168.106.0	255.255.255.0	192.168.106.1	1	253
Instituto Lenguas	192.168.107.0	255.255.255.0	192.168.107.1 192.168.107.12 192.168.107.13 192.168.107.17 192.168.107.18 192.168.107.21 192.168.107.22 192.168.107.23 192.168.107.25 192.168.107.26 192.168.107.28 192.168.107.38 192.168.107.41	13	241

ANEXO C. Tablas de Variables MIB.

A continuación se presentan las tablas de variables de la MIB seleccionadas inicialmente para su estudio y clasificación, teniendo en cuenta su posible asociación a las fallas bajo estudio. Este conjunto de variables hacen parte de los grupos estándar de la MIB II.

System (1.3.6.1.2.1.1)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
sysUpTime	1.3.6.1.2.1.1.3	TimeTicks		Indica la cantidad de tiempo desde que el sistema fue reiniciado por última vez en centésimas de segundo.

Interfaces (1.3.6.1.2.1.2)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
ifNumber	1.3.6.1.2.1.2.1	Integer32		Registra el número total de interfaces de red, independientemente de su estado actual.
ifDescr	1.3.6.1.2.1.2.2.1.2	Octet String	DisplayString	Muestra información textual acerca de la interfaz. Debe incluir el nombre del fabricante, del producto y la versión del hardware y el software de la interfaz.
ifType	1.3.6.1.2.1.2.2.1.3	Integer32	1-161	Muestra el tipo de interfaz; valores adicionales de esta variable son asignados por la IANA.
ifAdminStatus	1.3.6.1.2.1.2.2.1.7	Integer32	up 1	Muestra el estado deseado de

			down 2 testing 3	la interfaz. El estado de prueba (3) indica que no pueden pasar paquetes operacionales. Cuando un sistema gestionado inicializa, todas las interfases arrancan con este objeto en el estado bajo (2). Como resultado de una acción de gestión explicita o por información de configuración almacenada por el sistema gestionado, el objeto es cambiado a los estados activo (1) o prueba (3).
ifOperStatus	1.3.6.1.2.1.2.2.1.8	Integer32	up 1 down 2 testing 3 unknown 4 dormant 5 notPresent 6 lowerLayer Down 7	Muestra el estado operacional actual de la interfaz. El estado prueba (3) indica que no pueden ser pasados paquetes operacionales. Si ifAdminStatus esta bajo (2) entonces este objeto debe estar bajo. Si ifAdminStatus es cambiado a activo entonces este objeto debe cambiar a arriba(1), Si la interfaz esta lista para transmitir y recibir tráfico de la red; si la interfaz esta esperando por acciones externas (como una línea serial esperando por una conexión entrante) debe cambiar al estado durmiendo (5); debe permanecer en el estado bajo (2) si y solo si existe una falla que la previene de cambiar al estado arriba (1); debe permanecer en estado No presente (6) si la interfaz tiene componentes, generalmente de hardware inactivos
IfInOctets	1.3.6.1.2.1.2.2.1.10	Counter32		Muestra el número total de

				objetos recibidos en la interfaz, incluyendo caracteres de trama.
IfInUcastPkts	1.3.6.1.2.1.2.2.1.11	Counter32		Muestra el número de paquetes entregados por esta subcapa a una superior, los cuales no fueron direccionados a una dirección Broadcast ni multicast en esta subcapa.
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12	Counter32		Muestra el número de paquetes entregados por esta subcapa a una superior, los cuales fueron direccionados a una dirección Broadcast o multicast en esta subcapa.
ifInErrors	1.3.6.1.2.1.2.2.1.14	Counter32		Para interfaces orientadas a paquetes, muestra el número de paquetes de entrada que contienen errores, evitando su entrega a protocolos de capa superior. Para interfaces orientadas a caracteres o de longitud fija, muestra el número de unidades de transmisión de entrada que contienen errores, evitando su entrega a protocolos de capa superior.
IfInUnknown Protos	1.3.6.1.2.1.2.2.1.15	Counter32		Para interfaces orientadas a paquetes, muestra el número de paquetes recibidos por la interfaz que fueron descartados debido a un protocolo desconocido o no soportado. Para interfaces orientadas a caracteres o de longitud fija que soporten protocolos multiplexados, muestra el número de unidades de transmisión recibidas a través de la interfaz que fueron descartadas debido a un protocolo desconocido o no soportado. Para cualquier interfaz que no soporte protocolos multiplexados este contador será siempre 0.
ifOutOctets	1.3.6.1.2.1.2.2.1.16	Counter32		Muestra el número total de octetos transmitidos fuera de la interfaz incluyendo caracteres de tramas.

Ip (1.3.6.1.2.1.4)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
IpInReceives	1.3.6.1.2.1.4.3	Counter32		Indica el número total de datagramas de entrada recibidos desde las interfaces, incluyendo aquellos recibidos con errores.
IpInHdrErrors	1.3.6.1.2.1.4.4	Counter32		Indica el número de datagramas de entrada descartados debido a errores en sus cabeceras IP, incluyendo malas sumas de comprobación, números de versión incongruentes, otros errores de formato, exceso del time to live, errores descubiertos en el procesamiento de sus opciones IP, etc.
IpInAddrErrors	1.3.6.1.2.1.4.5	Counter32	DisplayString	Indica el número de datagramas de entrada descartados debido a que las direcciones IP en los campos de destino de sus cabeceras IP no son direcciones validas para ser recibidas en esta entidad. Este conteo incluye direcciones invalidas (0.0.0.0) y direcciones de clases no soportadas (clase E). Para entidades que no son routers IP y por eso no reenvían datagramas, este contador incluye datagramas descartados debido a que la dirección de destino no es una dirección local.
IpForwDatagrams	1.3.6.1.2.1.4.6	Counter32		Indica el número de datagramas de entrada para los que esta entidad no fue su destino IP final, como

				resultado de esto se hizo el intento de encontrar una ruta para reenviarlos a su destino final. En entidades que no actúan como routers IP, este contador incluirá solo aquellos paquetes que fueron enrutados desde la fuente a través de esta entidad, y el procesamiento de la opción de enrutamiento desde la fuente fue exitoso.
IpInUnknown Protos	1.3.6.1.2.1.4.7	Counter32		Indica el número de datagramas direccionados localmente recibidos satisfactoriamente pero descartados debido a un protocolo desconocido o no soportado
IpInDiscards	1.3.6.1.2.1.4.8	Counter32		Indica el número de datagramas IP de entrada para los que no hubo problemas al prevenir su procesamiento constante, pero que fueron descartados (por falta de espacio en los buffer). Este contador no incluye ningún datagrama descartado mientras espera su reensamble. Si el ancho de banda de la interfaz es mayor que el máximo valor para este objeto (4,294,967,295), luego se debe utilizar el objeto ifHighspeed para reportar la velocidad de esta interfaz, para una subcapa a la cual no se aplique el concepto de ancho de banda este valor podría ser cero.

IpInDelivers	1.3.6.1.2.1.4.9	Counter32		Indica el número total de datagramas de entrada entregados satisfactoriamente a los protocolos IP de usuario (incluyendo ICMP).
IpOutRequests	1.3.6.1.2.1.4.10	Counter32		Indica el número total de datagramas cuyos protocolos IP de usuarios locales (incluyendo ICMP) suplieron las peticiones de IP para transmisión. Este contador no incluye ningún datagrama contado en ipForwDatagrams.
IpOutDiscards	1.3.6.1.2.1.4.11	Counter32		Indica el número de datagramas de entrada para los que no hubo problemas al prevenir su transmisión a su destino, pero que fueron descartados (por falta de espacio en los buffer). Este contador podría incluir datagramas contados en ipForwDatagrams si cualquiera de esos paquetes cumple este (estricto) criterio de descarte.
IpOutNoRoutes	1.3.6.1.2.1.4.12	Counter32		Indica el número de datagramas IP descartados debido a que no se encontró ruta para transmitirlos a su destino. Este contador incluye cualquier paquete contado en ipForwDatagrams que cumpla este criterio de no ruta. Esto también incluye cualquier datagrama cuyo Host no pueda ser enrutado debido a que sus routers por defecto están fuera de línea.

IpReasmReqds	1.3.6.1.2.1.4.14	Counter32		Indica el número de fragmentos IP recibidos en esta entidad que necesitan ser reensamblados.
IpReasmFails	1.3.6.1.2.1.4.16	Counter32		Indica el número de fallas detectadas por el algoritmo de reensamble IP (por cualquier razón: Tiempo agotado, errores, etc.). No es necesaria una cuenta de fragmentos IP descartados desde que algunos algoritmos (en especial el algoritmo RFC 815) pueden perder la pista del número de fragmentos debido a la combinación de ellos a medida que son recibidos.
IpFragCreates	1.3.6.1.2.1.4.19	Counter32		Indica el número de fragmentos de datagramas IP que han sido generados como resultado de la fragmentación en esta entidad.
IpRouteType	1.3.6.1.2.1.4.21.1.8	Integer32	other 1 invalid 2 direct 3 indirect 4	Muestra el tipo de ruta. Los valores directo (3) e indirecto (4) se refieren a la noción de enrutamiento directo e indirecto en la arquitectura IP. Fijar este objeto con el valor inválido (2) tiene el efecto de invalidar la entrada correspondiente en la variable ipRouteTable. Así efectivamente se desvincula el destino identificado con dicha entrada de la ruta identificada con dicha entrada. Esta es una implementación específica tan importante como que el agente remueva una entrada inválida de la tabla. De acuerdo a esto las estaciones de gestión deben ser preparadas para recibir información tabulada desde los agentes que corresponden a entradas que no están en uso actualmente. La interpretación adecuada de tales entradas requiere el examen de la variable ipRouteType apropiado.
IpRouting Discards	1.3.6.1.2.1.4.23	Counter32		Muestra el número de entradas de enrutamiento que fueron escogidas para ser descartadas aun siendo validas. Una razón para descartar tales entradas podría ser para liberar espacio en los buffer para

				otras entradas de enrutamiento.
ipCidrRoute Status	1.3.6.1.2.1.4.24.4.1.16	Integer32	active 1 notInService 2 notReady 3 createAndGo 4 createAnd Wait 5 destroy 6	Indica la variable de estado de la fila, usada de acuerdo a las normas de instalación y eliminación de filas.

Icmp (1.3.6.1.2.1.5)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
icmpInMsgs	1.3.6.1.2.1.5.1	Counter32		Indica el número total de mensajes ICMP que fueron recibidos por esta entidad. Este contador incluye todos los valores contados en la variable icmpInErrors.
icmpInEchos	1.3.6.1.2.1.5.8	Counter32		Indica él número de mensajes ICMP de eco (petición) recibidos.
icmpInEchoReps	1.3.6.1.2.1.5.9	Counter32		Indica el número de mensajes ICMP de respuesta de ecos recibidos.

TCP (1.3.6.1.2.1.6)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
tcpActiveOpens	1.3.6.1.2.1.6.5	Counter32		Indica el número de veces que las conexiones TCP han hecho una transición directa al estado SYN-SENT a partir del estado CLOSED (cerrado).
tcpPassiveOpens	1.3.6.1.2.1.6.6	Counter32		Indica el número de veces que las conexiones TCP han hecho una transición directa al estado SYN-RCVD a partir del estado LISTEN.

tcpCurrEstab	1.3.6.1.2.1.6.9	Unsigned32		Indica el número de conexiones TCP para las cuales el estado actual es ESTABLISHED o CLOSE-WAIT.
tcpInSegs	1.3.6.1.2.1.6.10	Counter32		Indica el número total de segmentos recibidos, incluyendo aquellos recibidos en error. Esta cuenta incluye los segmentos recibidos en las conexiones actuales
tcpInErrs	1.3.6.1.2.1.6.14	Counter32		Indica el número total de segmentos recibidos en error (malas sumas de verificación TCP, etc.)

UDP (1.3.6.1.2.1.7)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
UdpInDatagrams	1.3.6.1.2.1.7.1	Counter32		Indica el número total de datagramas UDP entregados a usuarios UDP.
UdpOutDatagrams	1.3.6.1.2.1.7.4	Counter32		Indica el número total de datagramas UDP enviados desde esta entidad.

Transmission (1.3.6.1.2.1.10)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
dot3Stats SingleCollision Frames	1.3.6.1.2.1.10.7.2.1.4	Counter32		Muestra una cuenta de las tramas transmitidas satisfactoriamente sobre una interfaz en particular para la cual la transmisión es frenada exactamente por una sola colisión. Una trama que es

				contada por una instancia de esta variable, también es contada por la instancia correspondiente de las variables ifOutUcastPkts, ifOutMulticastPkts, o ifOutBroadcastPkts; y no es contada por la instancia correspondiente de la variable dot3StatsMultipleCollisionFrames. Este contador no se incrementa cuando la interfaz esta operando en modo full-duplex
dot3Stats MultipleCollision Frames	1.3.6.1.2.1.10.7.2.1.5	Counter32		Muestra una cuenta de las tramas transmitidas satisfactoriamente sobre una interfaz en particular para la cual la transmisión es frenada por más de una colisión. Una trama que es contada por una instancia de esta variable, también es contada por la instancia correspondiente de las variables ifOutUcastPkts, ifOutMulticastPkts, o ifOutBroadcastPkts; y no es contada por la instancia correspondiente de la variable dot3StatsSingleCollisionFrames. Este contador no se incrementa cuando la interfaz esta operando en modo full-duplex.
dot3Stats SQETestErrors	1.3.6.1.2.1.10.7.2.1.6	Counter32		Muestra una cuenta de las veces que el mensaje SQE TEST ERROR es generado por la subcapa PLS (physical layer signaling) para una interfaz en particular. El SQE TEST ERROR es fijado de acuerdo a las reglas de verificación del mecanismo de detección SQE (signal quality

				error) en la función de detección de portadora PLS como se describe en IEEE Std. 802.3, 1998 Edición, sección 7.2.4.6. Este contador no se incrementa en interfaces que operan a velocidades mayores a 10Mb/s, o en interfaces que están operando en modo full-duplex.
dot3Stats Deferred Transmissions	1.3.6.1.2.1.10.7.2.1.7	Counter32		Muestra una cuenta de tramas para las cuales el primer intento de transmisión sobre una interfaz en particular es retrasado debido a que el medio esta ocupado. La cuenta representada por una instancia de esta variable no incluye tramas implicadas en colisiones. Este contador no se incrementa cuando la interfaz esta operando en modo full-duplex.
dot3Stats LateCollisions	1.3.6.1.2.1.10.7.2.1.8	Counter32		Muestra el número de veces que una colisión es detectada en una interfaz en particular después que pase un slotTime en la transmisión de un paquete. Una colisión (posterior) incluida en una cuenta representada por una instancia de esta variable también es considerada como una colisión (genérica) para propósito de otras estadísticas asociadas con colisiones. Este contador no se incrementa cuando la interfaz esta operando en modo full-duplex.
dot3Stats Excessive Collisions	1.3.6.1.2.1.10.7.2.1.9	Counter32		Muestra una cuenta de tramas para las cuales la transmisión sobre una interfaz en particular falla debido a colisiones

				excesivas. Este contador no se incrementa cuando la interfaz esta operando en modo full-duplex. Las discontinuidades en el valor de este contador pueden ocurrir durante la reinicialización del sistema de gestión, y otras veces como es indicado en el valor de la variable ifCounterDiscontinuityTime.
dot3Stats InternalMac TransmitErrors	1.3.6.1.2.1.10.7.2.1.10	Counter32		Muestra una cuenta de tramas para las cuales la transmisión sobre una interfaz en particular falla debido a un error transmitido de forma interna en la subcapa MAC. Una trama solo es contada por una instancia de esta variable si no es contada por la correspondiente instancia de las variables dot3StatsLateCollisions,dot3StatsExcessiveCollisions o dot3StatsCarrierSenseErrors. El significado exacto de la cuenta representada por una instancia de esta variable es de implementación específica. En particular, una instancia de esta variable puede representar una cuenta de errores de transmisión en una interfaz en particular que no fue contada de otra manera.
dot3Stats CarrierSense Errors	1.3.6.1.2.1.10.7.2.1.11	Counter32		Indica el número de veces que la condición de detección de portadora se perdió o nunca se estableció cuando se intento transmitir una trama sobre una interfaz en particular. La cuenta representada por una instancia de esta variable se incrementa al menos una vez

				por cada intento de transmisión, aun si la condición de detección de portadora fluctúa durante un intento de transmisión. Este contador no se incrementa cuando la interfaz esta operando en modo full-duplex.
dot3Stats Frame TooLongs	1.3.6.1.2.1.10.7.2.1.13	Counter32		Muestra una cuenta de tramas recibidas en una interfaz en particular que exceden el máximo tamaño permitido de trama. La cuenta representada por una instancia de esta variable se incrementa cuando la trama TooLong status es retornada por el servicio MAC a el LLC (u otro usuario MAC). Las tramas recibidas para las cuales se obtienen múltiples condiciones de error, de acuerdo a las convenciones de IEEE 802.3 Layer Management, son contadas exclusivamente de acuerdo al estatus de error presentado al LLC (logical link control).
dot3Stats Internal MacReceive Errors	1.3.6.1.2.1.10.7.2.1.16	Counter32		Muestra una cuenta de tramas para las cuales la recepción en una interfaz en particular falla debido a un error de interno de subcapa MAC recibido. Una trama solo es contada por una instancia de esta variable si no es contada por la instancia correspondiente de cualquiera de las variables: dot3StatsFrameTooLongs, dot3StatsAlignmentErrors, dot3StatsFCSErrors. El significado preciso de la cuenta representada por una instancia de esta variable es de implementación específica.

				En particular, una instancia de esta variable puede representar una cuenta de errores recibidos en una interfaz en particular que de otra manera no son contados.

SNMP (1.3.6.1.2.1.11)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
SnmpInPkts	1.3.6.1.2.1.11.1	Counter32		Muestra el número total de mensajes entregados a una entidad SNMP desde el servicio de transporte.
SnmpOutPkts	1.3.6.1.2.1.11.2	Counter32		Muestra el número total de mensajes SNMP que fueron aprobados desde una entidad de protocolo SNMP hasta el servicio de transporte.

RMON (1.3.6.1.2.1.16)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
EtherStats DropEvents	1.3.6.1.2.1.16.1.1.1.3	Counter32		Muestra el número total de eventos en los cuales los paquetes fueron suprimidos por el sondeo debido a falta de recursos. Este número no es necesariamente el número de paquetes suprimidos; solo es el número de veces que esta condición ha sido detectada.
EtherStats Octets	1.3.6.1.2.1.16.1.1.1.4	Counter32		Muestra el número total de octetos de datos (incluyendo aquellos en paquetes malos)

				recibidos en la red (excluyendo los bits de entramado pero incluyendo octetos FCS). Esta variable puede ser usada como un estimado razonable de la utilización de Ethernet. Si se desea una precisión mayor, las variables etherStatsPkts y etherStatsOctets deben ser muestreadas antes y después de un intervalo común.
EtherStats Pkts	1.3.6.1.2.1.16.1.1.1.5	Counter32		Muestra el número total de paquetes (incluyendo los paquetes malos, paquetes de broadcast, y paquetes multicast) recibidos.
EtherStats BroadcastPkts	1.3.6.1.2.1.16.1.1.1.6	Counter32		Muestra el número total de paquetes válidos recibidos que fueron dirigidos a la dirección broadcast. No se incluyen los paquetes multicast.
EtherStats MulticastPkts	1.3.6.1.2.1.16.1.1.1.7	Counter32		Muestra el número total de paquetes validos recibidos que fueron dirigidos a una dirección multicast. Este número no incluye paquetes dirigidos a la dirección broadcast.
EtherStats CRC AlignErrors	1.3.6.1.2.1.16.1.1.1.8	Counter32		Muestra el número total de paquetes recibidos que tuvieron una longitud (excluyendo bits de entramado, pero incluyendo octetos FCS) entre 64 y 1518 octetos, pero tuvieron o una mala secuencia de chequeo de trama (FCS) con un número integral de octetos (FCS error) o una mala FCS con un número no integral de octetos (Alignment Error).
EtherStats	1.3.6.1.2.1.16.1.1.1.9	Counter32		Muestra el número total de

UndersizePkts				paquetes recibidos que eran de menos de 64 octetos de longitud (excluyendo bits de entramado, pero incluyendo octetos FCS) y estaban bien formados.
EtherStats OversizePkts	1.3.6.1.2.1.16.1.1.1.10	Counter32		Muestra el número total de paquetes recibidos que eran mayores a 1518 octetos (excluyendo bits de entramado, pero incluyendo octetos FCS) y estaban bien formados.
EtherStats Fragments	1.3.6.1.2.1.16.1.1.1.11	Counter32		Muestra el número total de paquetes recibidos que eran de menos de 64 octetos de longitud (excluyendo bits de entramado, pero incluyendo octetos FCS) y tenían o una más secuencias de chequeo de trama (FCS) con un número integral de octetos (error FCS) o una mala FCS con un número de octetos no integral (Alignment Error). Es enteramente normal para la variable etherStatsFragments el incrementarse. Esto se debe a que cuenta tanto runts(los cuales son acontecimientos normales debido a las colisiones) como golpes de ruido.
EtherStats Jabbers	1.3.6.1.2.1.16.1.1.1.12	Counter32		Muestra el número total de paquetes recibidos que eran de más de 1518 octetos de longitud (excluyendo bits de entramado, pero incluyendo octetos FCS) y tenían o una más secuencias de chequeo de trama (FCS) con un número integral de octetos (error FCS) o una mala FCS con un

				número de octetos no integral (Alignment Error). Observe que esta definición del jabber es diferente que la definición en IEEE-802.3 sección 8.2.1.5 (10BASE5) y sección 10.3.1.4 (10BASE2). Estos documentos definen el jabber como la condición donde cualquier paquete excede 20 ms. El rango permitido para detectar el jabber esta entre 20 ms y 150 ms.
EtherStats Collisions	1.3.6.1.2.1.16.1.1.1.13	Counter32		Indica el número total de colisiones mejor estimado (más preciso) en este segmento Ethernet. El valor retornado dependerá de la localización del sondeo RMON. Un sondeo localizado juega un rol mucho menor cuando se considera el 10BASE-T. 14.2.1.4 (10BASE-T) of IEEE standard 802.3 que define una colisión como la presencia simultanea de señales sobre los circuitos DO (data output) y RD (received data) (trasmisión y recepción en el mismo tiempo).
EtherStats Dropped Frames	1.3.6.1.2.1.16.1.4.1.1	Counter32		Muestra el número total de tramas que fueron recibidas por la sonda y por lo tanto no se contabilizó para entrar en *StatsDropEvents, pero para la cual la sonda escogió no contar para esta entrada por cualquier razón. Con frecuencia, este evento ocurre cuando la sonda no cuenta con algunos recursos y decide liberar la carga desde este grupo. Esta cuenta no incluye paquetes que no fueron

				contados debido a que tenían errores de capa MAC. A diferencia del contador dropEvent, este número, es el número exacto de tramas omitidas (dropped).
EtherHistory DropEvents	1.3.6.1.2.1.16.2.2.1.4	Counter32		Muestra el número total de eventos en los que los paquetes fueron suprimidos por la sonda debido a una falta de recursos durante este intervalo de muestreo. Este número no es necesariamente el número de paquetes suprimidos, solo es el número de veces que esta condición ha sido detectada.
EtherHistory Octets	1.3.6.1.2.1.16.2.2.1.5	Counter32		Muestra el número total de octetos de datos (incluyendo aquellos en paquetes defectuosos) recibidos en la red (excluyendo los bits de entramado pero incluyendo los octetos FCS).
EtherHistory Pkts	1.3.6.1.2.1.16.2.2.1.6	Counter32		Muestra el número de paquetes (incluyendo los defectuosos) recibidos durante este intervalo de muestreo.
EtherHistory Broadcast Pkts	1.3.6.1.2.1.16.2.2.1.7	Counter32		Muestra el número de paquetes buenos recibidos durante este intervalo de muestreo que fueron dirigidos a la dirección de broadcast
EtherHistory MulticastPkts	1.3.6.1.2.1.16.2.2.1.8	Counter32		Muestra el número de paquetes buenos recibidos durante este intervalo de muestreo que fueron dirigidas a una dirección multicast. Este número no incluye paquetes direccionados a la dirección de broadcast.
EtherHistory CRCAlign	1.3.6.1.2.1.16.2.2.1.9	Counter32		Muestra el número de paquetes recibidos durante

Errors				este intervalo de muestreo que tenían una longitud (excluyendo los bits de entramado pero incluyendo los octetos FCS) entre 64 y 1518 octetos, pero que tenían o una mala FCS con un número integral de octetos (error FCS) o una mala FCS con un número no integral de octetos (error de alineación).
EtherHistory UndersizePkts	1.3.6.1.2.1.16.2.2.1.10	Counter32		Muestra el número de paquetes recibidos durante este intervalo de muestreo que tenían menos de 64 octetos de longitud (excluyendo los bits de entramado pero incluyendo los octetos FCS) y estaban de lo contrario bien formados.
EtherHistory OversizePkts	1.3.6.1.2.1.16.2.2.1.11	Counter32		Muestra el número de paquetes recibidos durante este intervalo de muestreo que tenían más de 1518 octetos de longitud (excluyendo los bits de entramado pero incluyendo los octetos FCS) pero estaban de lo contrario bien formados.
EtherHistory Fragments	1.3.6.1.2.1.16.2.2.1.12	Counter32		Muestra el número de paquetes recibidos durante este intervalo de muestreo que tenían menos de 64 octetos de longitud (excluyendo los bits de entramado pero incluyendo los octetos FCS) que tenían una mala FCS con un número integral de octetos(error FCS) o una mala FCS con un número no integral de octetos (error de alineación). Es totalmente normal para la variable etherHistoryFragments el incrementarse. Esto se debe a que cuenta ambos enanos

				(runts) los cuales son acontecimientos normales debido a las colisiones y a los golpes de ruido.
EtherHistory Collisions	1.3.6.1.2.1.16.2.2.1.14	Counter32		Muestra la mejor estimación del número total de colisiones en este segmento Ethernet durante este intervalo de muestreo. El valor retornado dependerá de la ubicación de la sonda RMON. Así una sonda ubicada en un puerto de repetidor puede grabar mas colisiones que las que una sonda conectada a una estación en el mismo segmento podría. La ubicación de la sonda juega un papel mucho más pequeño cuando se considera los documentos que definen una colisión como la presencia simultanea de señales en los circuitos DO y RD (transmitiendo y recibiendo al mismo tiempo). Una estación 10BASE-T solo puede detectar colisiones cuando esta transmitiendo. Por lo tanto las sondas ubicadas en una estación y un repetidor, deben reportar el mismo número de colisiones.
EtherHistory Utilization	1.3.6.1.2.1.16.2.2.1.15	Integer32		Muestra el mejor estimado de la utilización media de la capa física en esta interfaz durante este intervalo de muestreo, en porcentaje.
HistoryControl Dropped Frames	1.3.6.1.2.1.16.2.5.1.1	Counter32		Muestra el número total de tramas que fueron recibidas por la sonda y por esa razón no fueron contadas para las StatsDropEvents, pero para las cuales la sonda eligió no contar para esta entrada por

				cualquier razón. Con frecuencia este evento ocurre cuando la sonda no cuenta con algunos recursos y decide deshacerse de la carga para esta colección. Esta cuenta no incluye paquetes que no fueron contados debido a que tenían errores de capa MAC. A diferencia del contador dropEvents counter, este número es el número exacto de tramas suprimidas.
AlarmRising Threshold	1.3.6.1.2.1.16.3.1.1.7	Integer32		Indica un umbral para la estadística muestreada. Cuando el valor muestreado actual es mayor o igual a este umbral, y el valor en el último intervalo de muestreo era menos que este umbral, un solo evento será generado. Un solo evento también será generado si la primera muestra después de que esta entrada llegue a ser válida es mayor o igual a este umbral y al alarmStartupAlarm asociado es igual a risingAlarm(1) o a risingOrFallingAlarm(3). Después de que se genere un evento de subida, otro evento así no será generado hasta que el valor muestreado caiga por debajo de este umbral y alcance el alarmFallingThreshold. Este objeto no puede ser modificado si el objeto asociado del alarmStatus es igual a valid (1).

AlarmFalling Threshold	1.3.6.1.2.1.16.3.1.1.8	Integer32		Indica un umbral para la estadística muestreada. Cuando el valor muestreado actual es mayor o igual a este umbral, y el valor en el último intervalo de muestreo era menos que este umbral, un solo evento será generado. Un solo evento también será generado si la primera muestra después de que esta entrada llegue a ser válida es mayor o igual a este umbral y al alarmStartupAlarm asociado es igual a risingAlarm(1) o a risingOrFallingAlarm(3). Después de que se genere un evento de subida, otro evento así no será generado hasta que el valor muestreado caiga por debajo de este umbral y alcance el alarmFallingThreshold. Esta variable no puede ser modificada si la variable asociado del alarmStatus es igual a valid (1).

RIP2 (1.3.6.1.2.1.23)

NOMBRE	OID	SINTAXIS	ENUMERACIÓN	DESCRIPCIÓN
rip2GlobalQueries	1.3.6.1.2.1.23.1.2	Counter32		Indica el número de respuestas enviadas a consultas RIP desde otros sistemas.