IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE:

"LICENCIADO EN INFORMÁTICA"

POR LA OPCION DE SEMINARIO DE TITULACION:

"INTERCONECTIVIDAD Y SEGMENTACION EN REDES DE ALTA VELOCIDAD"

VIGENCIA: DES/ESIME-CUL/5052005/17/09

DEBERA DESARROLLAR:

CRUZ JIMENEZ ALEXIS

NOMBRE DEL TEMA

"MONITOREO DE LA RED DE OPORTUNIDADES OAXACA**"**

CAPITULADO

I. INTRODUCCION A LAS REDES
II. SWITCHEO
III. TCP/IP
IV. SNMP
V. MONITOREO DE LA RED OPORTUNIDADES

Fecha: Noviembre de 2009

M. en C. RAYMUNDO SANTANA ALQUICIRA
Director del Seminario

ING. PEDRO AVILA BUSTAMANTE
Asesor

M. en C. LUIS CARLOS CASTRO MADRID
Jefe de la Carrera de Ingeniería en Computación

INSTITUTO POLITECNICO NACIONAL

CENTRO DE EDUCACCION CONTIUNA UNIDAD OAXACA

PROYECTO QUE PRESENTA:

CRUZ JIMENEZ ALEXIS

"MONITOREO DE LA RED DE OPORTUNIDADES OAXACA"

PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMATICA

POR LA OPCION DE SEMINARIO DE ITULACION:

INTERCONECTIVIDA Y SEGMENTACION EN REDES DE ALTA VELOCIDAD

OAXACA DE JUAREZ OAXACA, NOVIEMBRE DE 2009

DEDICATORIA

A mis Padres:

Que siempre me han dado todo su apoyo y cariño para seguir estudiando y poder culminar con esta etapa tan importante en la vida, en especial a mi madre que siempre ha querido ver a sus hijos con una carrera y ahora con este trabajo he podido hacer que ese sueño se cumpla.

A mis Hermanos:

A Roberto que siempre ha estado al pendiente de todos y nos ha dado todo su apoyo y cariño, pero lo más importante nos ha regalado un par de angelitos que han llenado de luz nuestras vidas y nos han hecho muy felices.

A Ángel a pesar de que todo el tiempo estamos en pleitos siempre ha estado con migo desde que empecé esta etapa de la vida que es la universidad y me ha dado su apoyo en todo momento y me ha acompañado en diferentes etapas de la vida que fueron importantes

A mis Sobrinos:

A mis sobrinos Alexis y Roberto que han llegado a nuestra familia y nos han enseñado lo maravilloso que es la vida, pero sobre todo nos han cambiado con el simple hecho de regalarnos una sonrisa.

INDICE

OBJETIVO.- Monitoreo de los switches de OPORTUNIDADES coordinación estatal Oaxaca

ALCANCE.- Monitoreo de la red local de la coordinación estatal Oaxaca en la detección de fallos.

PROBLEMÁTICA.- Hoy en día para la realización del trabajo en algunas áreas dentro de la coordinación estatal se requiere del uso de la red ya que se utilizan sistemas que se encuentran en la intranet y por lo tanto es primordial que la red se encuentre en buen estado y este operando siempre.

JUSTIFICACION.- Por causa de los diversos procesos de captura que se realizan en la empresa es necesario el monitoreo de la red ya que se improvisan centros de captura dentro de las instalaciones por lo cual causa fallos en la red y para evitar la perdida de tiempo es necesario implantar un método de automatización de notificación de fallos con el objetivo de evitar que se interrumpa el trabajo por perder la conexión a la red.

Capitulo I
Introducción a las Redes

1.1 HISTORIA DE LAS REDES

En 1957 los Estados Unidos crearon la Advaced Research Projects Agency (ARPA), como organismo afiliado al departamento de defensa para impulsar el desarrollo tecnológico.

Posteriormente a la creación del ARPA, Leonard Kleinrock, un investigador del MIT escribía el primer libro sobre tecnologías basadas en la transmisión por un mismo cable de más de una comunicación.

En 1965, la ARPA patrocino un programa que trataba de analizar las redes de comunicación usando computadoras. Mediante este programa, la máquina TX-2 en el laboratorio Licoln del MIT y la AN/FSQ-32 del System Development Corporation de Santa Mónica en California, se enlazaron directamente mediante una línea delicada de 1200 bits por segundo.

En 1967, La ARPA convoca una reunión en Ann Arbor (Michigan), donde se discuten por primera vez aspectos sobre la futura ARPANET.

En 1968 la ARPA no espera más y llama a empresas y universidades para que propusieran diseños, con el objetivo de construir la futura red. La universidad de California gana la propuesta para el diseño del centro de gestión de red y la empresa BBN (Bolt Beraneck and Newman Inc.) El concurso de adjudicación para el desarrollo de la tecnología de conmutación de paquetes mediante la implementación de la Interfaz Message Processors (IMP)

En 1969 se construye la primera red de computadoras de la historia. Denominada ARPANET, estaba compuesta por cuatro nodos situados en UCLA (Universidad de California en los Angeles), SRI (Stanford Research Institute), UCBS (Universidad de California de Santa Bárbara, Los Angeles) y la Universidad de UTA.

La primera comunicación entre dos computadoras se produce entre UCLA y Stanford el 20 de octubre de 1969. El autor de este envío fue Charles Kline (UCLA) En ese mismo año, La Universidad de Michigan crearía una red basada en conmutación de paquetes, con un protocolo llamado X.25, la misión de esta red era la de servir de guía de comunicación a los profesores y alumnos de dicha universidad. En ese mismo año se empiezan a editar los primeros RFC (Petición de comentarios) Los RFC son los documentos que normalizan el funcionamiento de las redes de computadoras basadas en TCP/IP y sus protocolos asociados.

En 1970 la ARPANET comienza a utilizar para sus comunicaciones un protocolo Host-to-host. Este protocolo se denominaba NCP y es el predecesor del actual TCP/IP que se utiliza en toda la Internet.

Ya en 1971 la ARPANET estaba compuesta por 15 nodos y 23 maquinas que se unían mediante conmutación de paquetes. En ese mismo año Ray Tomlinson realiza un programa de e-mail para distribuir mensajes a usuarios concretos a través de ARPANET.

En 1972 se elige el popular @ como tecla de puntuación para la separación del nombre del usuario y de la máquina donde estaba dicho usuario. Se realiza la primera demostración pública de la ARPANET con 40 computadoras. En esa misma demostración se realiza el primer chat.

En 1973 se produce la primera conexión internacional de la ARPANET. Dicha conexión se realiza con el colegio universitario de Londres (Inglaterra) En ese mismo año Bob Metcalfe expone sus primeras ideas para la implementación del protocolo Ethernet que es uno de los protocolos más importantes que se utiliza en las redes locales. A mediados de ese año se edita el RFC454 con especificaciones para la transferencia de archivos.

En 1974 Cerf y Kahn publican su artículo, un protocolo para interconexión de redes de paquetes, que especificaba con detalle el diseño del protocolo de control de transmisión (TCP)

En 1975, Se prueban los primeros enlaces vía satélite cruzando dos océanos (desde Hawai a Inglaterra) con las primeras pruebas de TCP de la mano de Stanford, UCLA y UCL. En ese mismo año se distribuyen las primera versiones del programa UUCP (Unís-to-Unix CoPy) del sistema operativo UNIX por parte de AT&T.

En 1982 es el año en que la DCA y la ARPA nombran a TCP e IP como el conjunto de protocolos TCP/IP de comunicación a través de la ARPANET.

El 1 de enero de 1983 se abandona la etapa de transición de NCP a TCP/IP pasando este último a ser el único protocolo de la ARPANET. Se comienza a unir redes y países ese mismo año como la CSNET, la MINET europea y se crearon nuevas redes como la EARN.

En 1985 se establecen responsabilidades para el control de los nombres de dominio y así el ISI (Información Sciences Institute) asume la responsabilidad de ser la raíz para la resolución de los nombres de dominio. El 15 de marzo se produce el primer registro de nombre de dominio (symbolics.com) a los que seguirían cmu.edu, purdue.edu, rice.edu, ucla.edu y .uk

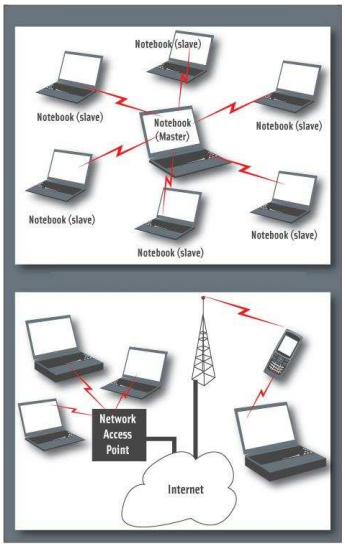
1.2 CLASIFICACION DE REDES

Podemos clasificar las redes en tres partes por alcance, por su modo de conexión y por su relación funcional

Redes por Alcance:

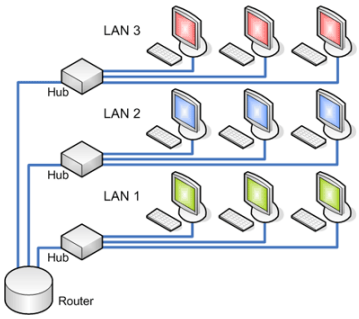
- **Red de área personal (*PAN*)**

Son redes de computadoras o dispositivos móviles que se conectan entre si y están cerca de alguna persona (ejemplo: los PDA o los Celulares).



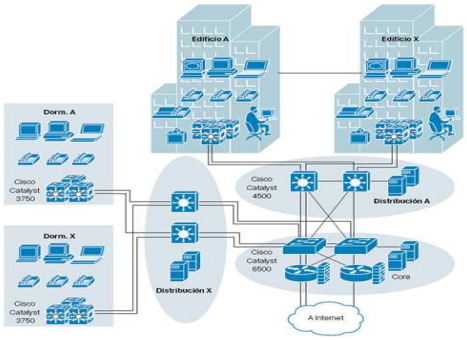
- **Red de área local (*LAN*)**

Una red Lan se limita a áreas pequeñas ya sea un cuarto o un edificio.



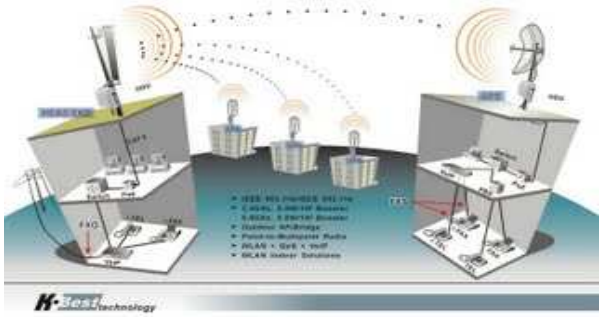
- **Red de área de campus (*CAN*)**

Son redes que surgen de la unión de dos o más LANs las cuales están delimitadas por un área específica (ejemplo: un campus universitario, un complejo industrial o una base militar).



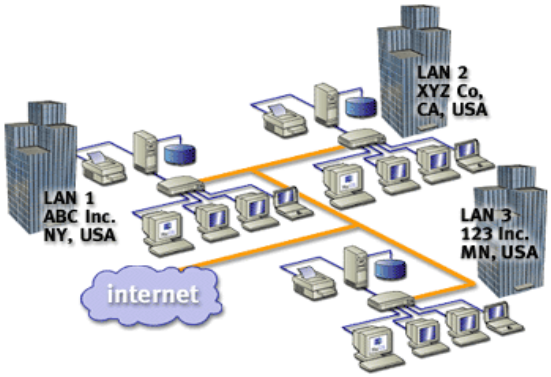
- **Red de área metropolitana (*MAN*)**

Es la red que une dos o mas redes locales pero su extensión no pasa mas aya de los límites de la ciudad o del área metropolitana.



- **Red de área amplia (*WAN*)**

Es una red de comunicación de datos que abarca un área geográfica mayor que las demás redes.



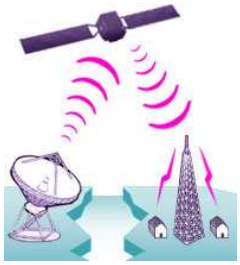
Redes por su modo de conexión:

- **Medios guiados**

Son aquellos en los que las ondas se transmiten por medio de encamino físico (ejemplo: cable coaxial, cable de par trenzado, fibra óptica, etc.).

- **Medios no guiados**

Son aquellos que no necesitan un medio físico para transmitir (ejemplo: radio, infrarrojos, microondas, láser y otras redes inalámbricas.



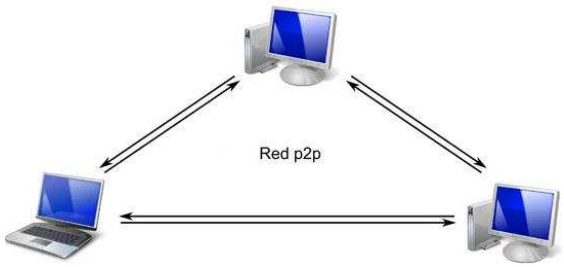
Redes por relación funcional:

- **Cliente-servidor.**

Son computadoras que realizan una petición (*cliente*) a otra computadora (*servidor*) que le da respuesta a dicha petición.

- **Igual-a-Igual (p2p).**

Es una red de computadoras que están enlazadas entre si o solo algunas de ellas pero estas no funcionan como clientes ni servidores.



1.3 TOPOLOGIAS DE RED

TOPOLOGIAS FISICAS

La topología o la forma en que se conecta la red, depende muchos aspectos como la distancia que hay entre las computadoras y la forma de comunicación entre ellas ya que nos determina la velocidad.

Una topología de rede es la forma en que se distribuyen los cables de la red para conectarse con el servidor y con cada una de las computadoras que comprenden la red.

La ubicación del cableado de la red nos puede determinar la posición de los equipos que van a integrarla dentro del área de trabajo, así como la facilidad en que se distribuirá el cableado y el corte de todo el sistema de la red.

Por las necesidades de las empresas de crecimiento una red debe de ser flexible en cuanto a sus futuras necesidades y en gran parte lo determina la topología implantada.

Dentro de las topologías podemos encontrar las siguientes:

Red de Bus:

Esta topología se caracteriza por tener un único canal de comunicación llamado bus, troncal o backbone, al cual se conectan los diferentes dispositivos. Así todos los dispositivos comparten el mismo canal para comunicarse entre ellos.

Red de Anillo:

En esta red cada estación de trabajo esta conectada a la siguiente y la última estación se encuentra conectada a la primera. Cada una tiene un receptor y un transmisor que realiza la función de repetidor, pasando la señal a la siguiente estación.

Red de Estrella:

Es una red en la cual los dispositivos están conectados directamente a un punto central y todas las comunicaciones se hacen a través de este punto.

1.4 TOPOLOGIAS LOGICAS

Broadcast:
Es una topología en donde cada Host envía sus datos hacia los demás Hosts de la red (*Ethernet*).

Transmisión de Token:

Controla el acceso a la red por medio de transmisión de Token electrónicos a cada Host de la red de manera secuencial (*Token Ring y FDDI*).

TIPOS DE TRANSMISION

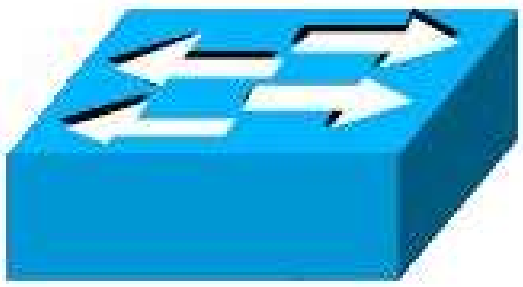
Por la direccionalidad de los datos:

Simplex (unidireccionales). - Un Equipo Terminal de Datos transmite y otro recibe (Streaming).

Half-Duplex (bidireccionales).- Sólo un equipo transmite a la vez. También se llama Semi-Duplex (Ej. una comunicación por equipos de radio, si los equipos no son full dúplex, uno no podría transmitir (hablar) si la otra persona está también transmitiendo (hablando) porque su equipo estaría recibiendo (escuchando) en ese momento).

Full-Duplex (bidireccionales).- Ambos pueden transmitir y recibir a la vez una misma información. (Ej. Videoconferencia).

Capitulo II
Switching



2.1 SWITCHES

Un **conmutador** o **switch** es un dispositivo digital de lógica de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC.

El switch escucha en todos sus puertos y construye tablas en las cuales mapéa direcciones MAC con el puerto através del cual se pueden alcanzar. De esta manera cuando un host envía un mensaje en un segmento de red que va destinado a otro segmento de red esté será leído por el switch y será enviado únicamente al segmento de red que corresponda limitando así al mínimo las colisiones de red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, uniéndolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejorando el rendimiento y la seguridad de las LANs.

Conmutación es la conexión que realizan los diferentes nodos que existen en distintos lugares para lograr un camino apropiado para conectar dos usuarios de una red de telecomunicaciones. Es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda.

Cuando un emisor necesita enviar un grupo de datos mayor que el tamaño fijado par aun paquete, éste los parte en paquetes y los envía uno a uno al receptor. Hay dos técnicas básicas para el envío de estos paquetes:

1. Técnica de Datagramas: Cada paquete se trata de forma independiente, es decir, el emisor enumera cada paquete, le añade información de control y lo envía hacia su destino.
2. Técnica de Circuitos Virtuales: Antes de enviar los paquetes de datos, el emisor envía un paquete de control que es de petición de llamada, este paquete se encarga de establecer un camino lógico de nodo en nodo por donde irán uno a uno todos los paquetes de datos. De esta forma se establece un camino virtual para todo el grupo de paquetes.

Un switch Ethernet brinda muchas ventajas como, permitir que varios usuarios se comuniquen en paralelo a través del uso de circuitos virtuales y segmentos de red dedicados en un entorno libre de colisiones. Esto aumenta al máximo el ancho de banda disponible en el medio compartido. Otra ventaja es al momento de desplazarse a un entorno de LAN conmutado es muy económico a que el hardware y el cableado se pueden volver a utilizar.

2.2 OPERACIONES DE LA CAPA 2 DE LOS SWITCHES

Los switches se consideran puentes multipuerto sin dominio de colisión debido a la micro segmentación. Los datos se intercambian a altas velocidades haciendo la conmutación de paquetes hacia su destino. Al leer la información de capa 2 de dirección MAC destino, los switches pueden realizar transferencias de datos a altas velocidades de forma similar a los puentes.

La conmutación Ethernet aumenta el ancho de banda disponible en una red. Esto se puede lograr creando segmentos de redes dedicadas, o conexiones punto a punto y conectando estos segmentos en una red virtual dentro del switch. Este circuito de red virtual existe solamente cuando dos nodos necesitan comunicarse. Esto se denomina circuito virtual ya que existe sólo cuando es necesario y se establece dentro del switch.

Aunque el switch reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch pertenecen al mismo dominio de bradcast. Por lo tanto, un broadcast emitido de un nodo lo percibirán todos los demás nodos conectados al switch.

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño.

De igual forma los puentes, los switches envían e inundan el tráfico basándose en las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz.

2.3 SEGMENTACIÓN MEDIANTE SWITCHES DE UN DOMINIO DE COLISIÓN

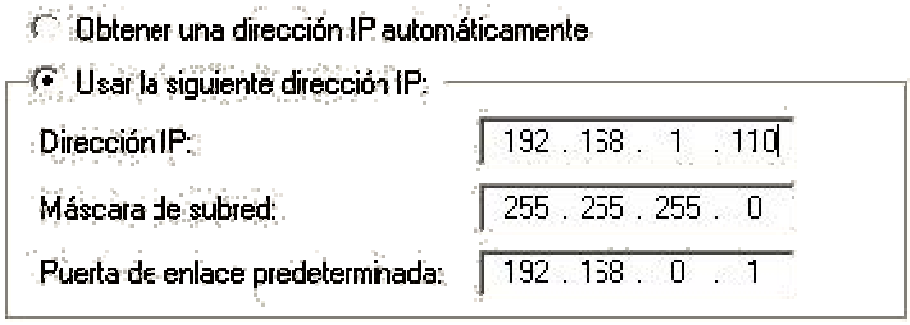
Una LAN que usa una topología Ethernet de conmutación crea una red que funciona como si sólo tuviera dos nodos, el nodo emisor el nodo receptor. Estos nodos comparten un ancho de banda que varia dependiendo de la velocidad de transmisión del switch ya puede ser a 10,100 o 1000 Mbps, lo que significa que prácticamente todo el ancho de banda está disponible para la transmisión de datos. Una LAN Ethernet conmutada permite que la topología LAN funcione más rápida y eficientemente que una LAN Ethernet estándar, ya que usa el ancho de banda de modo muy eficiente.

Podemos observar que aunque el 100% del ancho de banda puede estar disponible en las redes Ethernet tienen un mejor rendimiento cuando se mantiene por debajo del 30-40% de la capacidad total. Esta limitación se debe al método de acceso al medio de Ethernet (CSMA/CD). El uso de ancho de banda que supere el límite recomendado tiene como resultado un aumento en la cantidad de colisiones. El propósito e la conmutación de las redes de área local es aliviar las

insuficiencias de ancho de banda y los cuellos de botella de la red como, los que se producen entre un grupo de PC y un servidor de archivos remoto. Un switch es un puente multipuerto de alta velocidad que tiene un puerto para cada nodo, o segmento, la LAN. El switch divide la LAN en micro segmentos, creando dominios libres de colisiones a partir de un dominio de colisión de mayor tamaño.

La Ethernet conmutada se basa en la Ethernet estándar. Cada nodo está directamente conectado a uno de sus puertos, o a un segmento que está conectado a uno de los puertos del switch. Una computadora conectada directamente a un switch está en su propio dominio de colisión. Cuando una trama entra a un switch, se lee para obtener la dirección origen o destino. Luego, el switch determina cuál es la acción de conmutación que se llevar+a a cabo basándose en lo que sabe a partir de la información que ha leído en la trama. Si la dirección destino se encuentra ubicado en otro segmento, la trama se conmuta a su destino.

Capitulo III
TCP/IP



3.1 PROTOCOLOS TCP/IP Y EL MODELO OSI

TCP/IP es el estándar para las comunicaciones de Inter Network y funciona como el protocolo de transporte para Internet, permitiendo que millones de computadoras se comuniquen a nivel mundial.

La función de la pila o conjunto de protocolo **TCP/IP** es la transferencia de información desde un dispositivo de red a otro. Al hacer esto, se asemeja al modelo de referencia **OSI** en las capas inferiores y soporta todos los protocolos físicos y de enlace de datos.

Las capas que se ven afectadas por TCP/IP son la Capa 4 (transporte), Capa 3 (red) y Capa 7 (aplicación). Dentro de estas capas existen otros tipos de protocolos que tienen varios propósitos, todos relacionados con la transferencia de información.

TCP/IP permite la comunicación entre cualquier conjunto de redes interconectadas y sirve tanto para las comunicaciones LAN como para WAN. TCP/IP incluye también especificaciones para aplicaciones como correo electrónico, la conexión remota, la emulación de terminales y la transferencia de archivos.

3.2 SERVICIOS DE INTERNET A NIVEL DE APLICACIÓN

Desde el punto de vista de un usuario, una red de redes TCP/IP aparece como un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación. Utilizamos el término interoperabilidad para referirnos a la habilidad que tienen diversos sistemas de computación para cooperar en la resolución de problemas computacionales. Los programas de aplicación de Internet muestran un alto grado de interoperabilidad. Los servicios de aplicación de Internet más populares y difundidos incluyen:

- Correo electrónico. El correo electrónico permite que un usuario componga memorandos y los envíe a individuos o grupos. Otra parte de la aplicación de correo permite que un usuario lea los memorandos que ha recibido. Aunque existen muchos sistemas de correo electrónico, al utilizar TCP/IP se logra que la entrega sea más confiable debido a que no se basa en compradoras intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su máquina local, se habrá recibido de manera exitosa en el sitio de destino.

- Transferencia de archivos. Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado principalmente para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, el cual permite que lo usuarios envíen o

reciban archivos generalmente grandes de programas o de datos. Por ejemplo, al utilizar el programa de transferencia de archivos, se puede copiar de una máquina a otra una gran base de datos que contenga imágenes de satélite, un programa escrito en cualquier lenguaje de programación, o un diccionario del idioma inglés. El sistema proporciona una manera de verificar que los usuarios cuenten con autorización o, incluso, de impedir el acceso. Como el correo, la transferencia de archivos a través de una red de redes TCP/IP es confiable debido a que las dos máquinas comprendidas se comunican de manera directa, sin tener que confiar en máquinas intermedias para hacer copias del archivo a lo largo del camino.

- Acceso remoto. El acceso remoto permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva. El acceso remoto hace aparecer una ventana en la pantalla del usuario, la cual se conecta directamente con la máquina remota al enviar cada golpe de tecla desde el teclado del usuario a una máquina remota y muestra en la ventana del usuario cada carácter que la computadora remota lo genere. Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

Protocolos de diagnóstico de fallas

Ping (Packet Internet Groper) es una utilidad de diagnóstico que se utiliza para determinar si una computadora está conectada correctamente a los dispositivos o a Internet.

Traceroute es un programa que está disponible en varios sistemas y es similar a PING, excepto que suministra más información que PING. Este programa rastrea la ruta que toma un paquete hacia el destino y se utiliza para depurar problemas de enrutamiento.

Existen protocolos de Windows que son útiles y con los que debemos de familiarizarnos:

NBSTAT: utilitario para diagnosticar fallas de la resolución de nombres NetBios; se utiliza para visualizar y eliminar entradas del caché de nombres.

NETSTAT: utilidad que suministra información acerca de estadísticas TCP/IP; se puede usar para suministrar información del estado de las conexiones TCP/IP y resúmenes de ICMP, TCP y UDP.

IPCONFIG: utilitario para visualizar las configuraciones actuales de red para todos los adaptadores IP (nic) de un dispositivo; se puede usar para visualizar la dirección MAC, la IP y el Gateway.

3.3 PROTOCOLO TCP/IP Y LA CAPA DE TRANSPORTE

La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones. De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, etc. Además, el nombre de la aplicación puede variar de sistema en sistema. Es por ello que se ha implementado un sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se denominan puertos.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores). Estos dos protocolos son los siguientes:

- **TCP:** un protocolo orientado a conexión que brinda detección de errores; suministra control de flujo a través de ventanas deslizantes, y confiabilidad a través de los números de secuencia y acuses de recibo.
- **UDP:** un protocolo no orientado a conexión en el que la detección de errores es obsoleta; tiene la responsabilidad de transmitir mensajes, en esta capa no se suministra ninguna verificación de software para la entrega de segmentos.

3.4 PUERTOS TCP Y UDP

TCP y UDP utilizan números de puertos o sockets para enviar información a las capas superiores. Los números de puerto se utilizan para mantener un registro de las distintas conversaciones que atraviesan la red al mismo tiempo.

Los creadores del software de aplicación han acordado utilizar los números de puerto conocidos que se definen en la RFC1700. Por ejemplo, cualquier conversación destinada a una aplicación FTP utiliza el número de puerto 21 como estándar.

En lugar de las conversaciones que no involucran ninguna aplicación que tenga un número de puerto conocido, se les asignan números de puerto que se seleccionan de forma aleatoria dentro de un intervalo específico. Estos puertos se utilizan como direcciones origen y destino en el segmento TCP/UDP.

Algunos puertos son reservados, tanto en TCP como en UDP, aunque algunas aplicaciones no estén hechas para soportarlos. Los números de puerto tienen los siguientes intervalos asignados:

- Números inferiores a 255 corresponden a aplicaciones públicas.
- Los números entre 255-1023 se asignan a empresas para aplicaciones comerciales.
- Los números superiores a 1023 no están regulados.

Los sistemas finales utilizan números de puerto para seleccionar la aplicación adecuada. La computadora origen asigna dinámicamente los números d puerto origen, por lo general un número mayor de 1023.

3.5 MODELO OSI

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por Ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por Ej., cables, etc.), hasta otro programa de aplicación ubicado en otro host de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

El modelo se llama OSI (Interconexión de Sistemas Abiertos) de ISO por que tiene que ver con la conexión de sistemas abiertos, es decir sistemas que están abiertos a la comunicación con otros sistemas.

Los principios que se aplicaron para llegar a las siete capas que conforman el modelo OSI son las siguientes:

- Una capa se debe crear donde se necesite una abstracción diferente.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir con intención de definir protocolos estandarizados internacionalmente.

- Los límites de las capas se deben elegir a in de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficientemente grande para no tener que agrupas funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI.

Capa 7: La capa de aplicación.

La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Capa 6: La capa de presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa 5: La capa de sesión

Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Capa 4: La capa de transporte

La capa de transporte segmenta los datos originados en el host emisor y los reensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales.

Capa 3: La capa de red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

Capa 2: La capa de enlace de datos

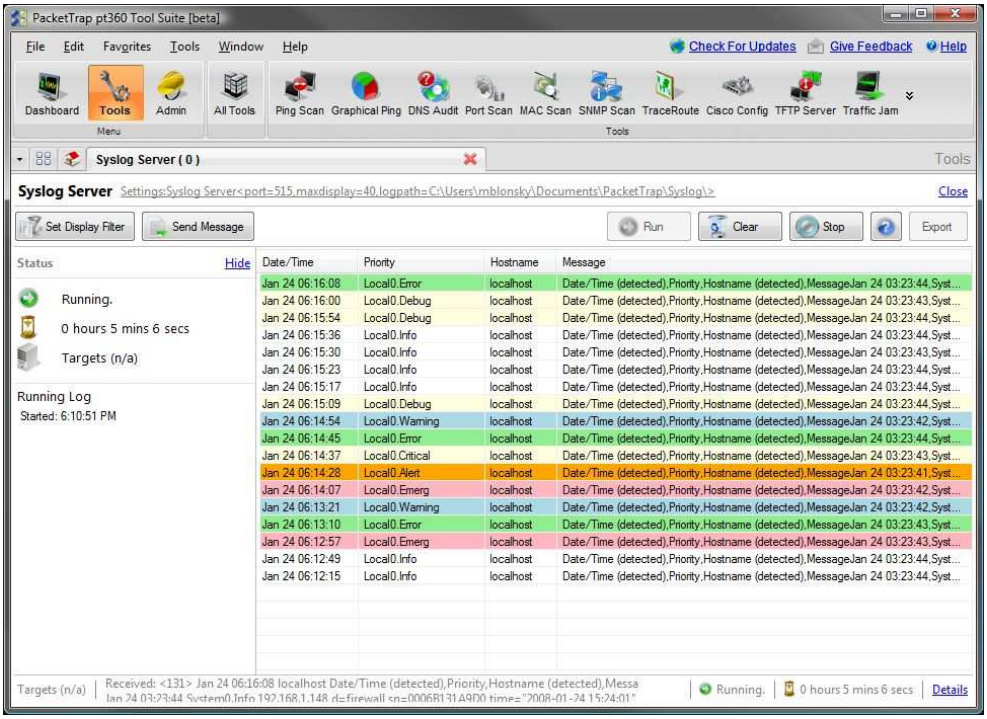
La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Capa 1: La capa física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física.

Capitulo IV

SNMP



4.1 SIMPLE NETWORK MANAGEMENT PROTOCOL

El **Protocolo Simple de Administración de Red** o **SNMP** es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

El sistema de administración de red se basa en dos elementos principales: un supervisor y agentes. El supervisor es el terminal que le permite al administrador de red realizar solicitudes de administración. Los agentes son entidades que se encuentran al nivel de cada interfaz. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos.

Los conmutadores, concentradores (hubs), routers y servidores son ejemplos de hardware que contienen objetos administrados. Estos objetos administrados pueden ser información de hardware, parámetros de configuración, estadísticas de rendimiento y demás elementos que estén directamente relacionados con el comportamiento en progreso del hardware en cuestión. Estos elementos se encuentran clasificados en algo similar a una base de datos denominada MIB ("Base de datos de información de administración"). SNMP permite el diálogo entre el supervisor y los agentes para recolectar los objetos requeridos en la MIB.

4.2 BASE DE INFORMACIÓN DE ADMINISTRACIÓN SNMP (MIB)

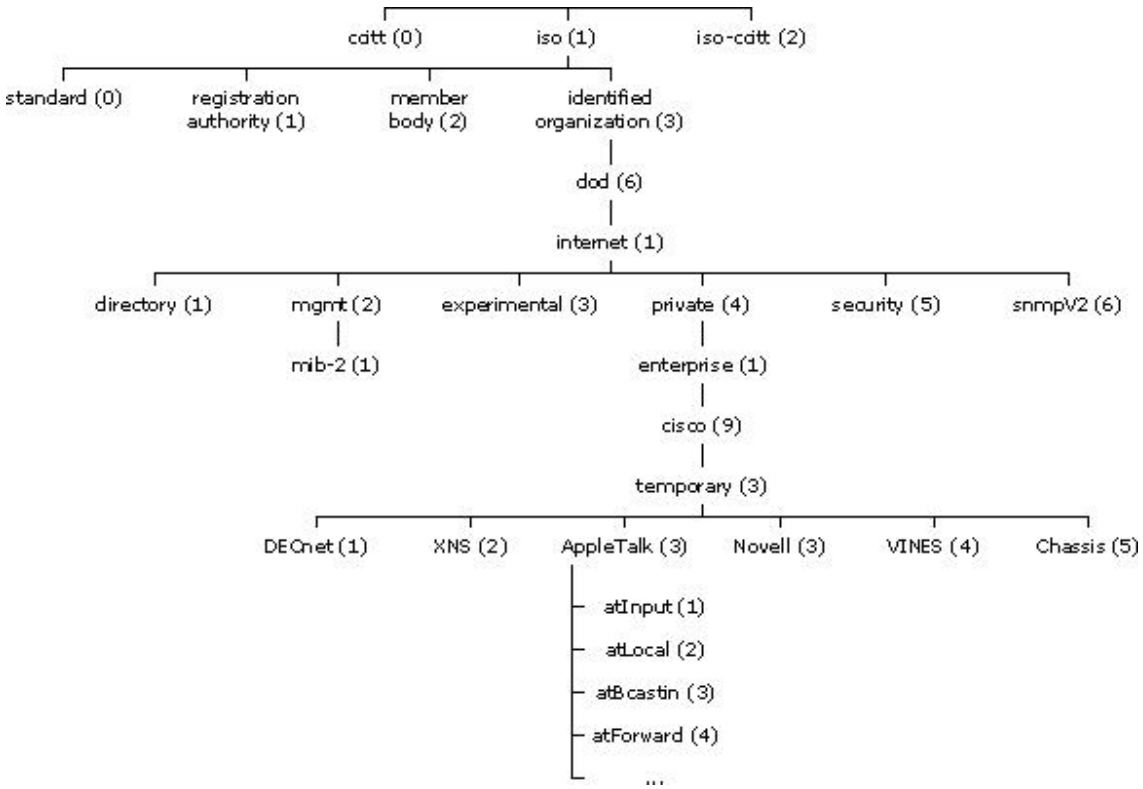
Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Las MIB’s son accedidas usando un protocolo de administración de red, como por ejemplo, SNMP.

Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un ejemplo de un objeto administrado es *atInput*, que es un objeto escalar que contiene una simple instancia de objeto, el valor entero que indica el número total de paquetes AppleTalk de entrada sobre una interfaz de un router.

Un identificador de objeto (*object ID*) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.



El árbol MIB ilustra las variadas jerarquías asignadas por las diferentes organizaciones

Los identificadores de los objetos ubicados en la parte superior del árbol pertenecen a diferentes organizaciones estándares, mientras los identificadores de los objetos ubicados en la parte inferior del árbol son colocados por las organizaciones asociadas.

Los vendedores pueden definir ramas privadas que incluyen los objetos administrados para sus propios productos. Las MIB's que no han sido estandarizadas típicamente están localizadas en la rama experimental.

El objeto administrado atInput podría ser identificado por el nombre de objeto *iso.identified-organization.dod.internet.private.enterprise.cisco.temporary.AppleTalk.atInput* o por el descriptor de objeto equivalente *1.3.6.1.4.1.9.3.3.1*.

El corazón del árbol MIB se encuentra compuesto de varios grupos de objetos, los cuales en su conjunto son llamados mib-2. Los grupos son los siguientes:

- System (1);
- Interfaces (2);
- AT (3);
- IP (4);
- ICMP (5);
- TCP (6);
- UDP (7);
- EGP (8);
- Transmission (10);
- SNMP (11).

Es importante destacar que la estructura de una MIB se describe mediante el estándar Notación Sintáctica Abstracta 1 (Abstract Syntax Notation One).

4.3 COMPONENTES Y COMANDOS BÁSICOS

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados.
- Agentes.
- Sistemas administradores de red (NMS's).

Un **dispositivo administrado** es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadoras o impresoras.

Un **agente** es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un **NMS** ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Los dispositivos administrados son supervisados y controlados usando cuatro comandos SNMP básicos: **lectura, escritura, notificación y operaciones transversales.**

El **comando de lectura** es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados.

El **comando de escritura** es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

El **comando de notificación** es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

Las **operaciones transversales** son usadas por el NMS para determinar qué variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ejemplo, una tabla de rutas.

4.4 MENSAJES SNMP

Para realizar las operaciones básicas de administración nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. La utilización de un mecanismo de este tipo asegura que las tareas de administración de red no afectarán al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP.

Los puertos comúnmente utilizados para SNMP son los siguientes:

Número	Descripción
161	SNMP
162	SNMP-trap

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

Versión Comunidad SNMP PDU

- Versión: Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1).
- Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private".
- SNMP PDU: Contenido de la unidad de datos del protocolo, el que depende de la operación que se ejecute.

Los mensajes GetRequest, GetNextRequest, SetRequest y GetResponse utilizan la siguiente estructura en el campo SNMP PDU:

Tipo Identificador Estado de error Índice de error Enlazado de variables

- Identificador: Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea.
- Estado e índice de error: Sólo se usan en los mensajes GetResponse (en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:
  - 0: No hay error.
  - 1: Demasiado grande.
  - 2: No existe esa variable.

  - 3: Valor incorrecto.
  - 4: El valor es de solo lectura.
  - 5: Error genérico.
- Enlazado de variables: Es una serie de nombres de variables con sus valores correspondientes (codificados en ASN.1).

GetRequest

A través de este mensaje el NMS solicita al agente retornar el valor de un objeto de interés mediante su nombre. En respuesta el agente envía una respuesta indicando el éxito o fracaso de la petición. Si la petición fue correcta, el mensaje resultante también contendrá el valor del objeto solicitado. Este mensaje puede ser usado para recoger un valor de un objeto, o varios valores de varios objetos, a través del uso de listas.

GetNextRequest

Este mensaje es usado para recorrer una tabla de objetos. Una vez que se ha usado un mensaje GetRequest para recoger el valor de un objeto, puede ser utilizado el mensaje GetNextRequest para repetir la operación con el siguiente objeto de la tabla. Siempre el resultado de la operación anterior será utilizado para la nueva consulta. De esta forma un NMS puede recorrer una tabla de longitud variable hasta que haya extraído toda la información para cada fila existente.

SetRequest

Este tipo de mensaje es utilizado por el NMS para solicitar a un agente modificar valores de objetos. Para realizar esta operación el NMS envía al agente una lista de nombres de objetos con sus correspondientes valores.

GetResponse

Este mensaje es usado por el agente para responder un mensaje GetRequest, GetNextRequest, o SetRequest. En el campo "Identificador de Request" lleva el mismo identificador que el "request" al que está respondiendo.

Trap

Un trap es generado por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente:

Tipo Enterprise	Dirección del agente	Tipo genérico de trap	Tipo específico de trap	Timestamp	Enlazado de variables

- Enterprise: Identificación del subsistema de gestión que ha emitido el trap.

- Dirección del agente: Dirección IP del agente que ha emitido el trap.
- Tipo genérico de trap:
  - Cold start (0): Indica que el agente ha sido inicializado o reinicializado.
  - Warm start (1): Indica que la configuración del agente ha cambiado.
  - Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva).
  - Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa).
  - Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad).
  - EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.
  - Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.
- Tipo específico de trap: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico.
- Timestamp: Indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap.
- Enlazado de variables: Se utiliza para proporcionar información adicional sobre la causa del mensaje.

GetBulkRequest

Este mensaje es usado por un NMS que utiliza la versión 2 ó 3 del protocolo SNMP típicamente cuando es requerida una larga transmisión de datos, tal como la recuperación de largas tablas. En este sentido es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla.

InformRequest

Un NMS que utiliza la versión 2 ó 3 del protocolo SNMP transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.

4.5 GESTIÓN A DISTANCIA

Ciertos fabricantes están desarrollando extensiones particulares para ciertas clases de productos y la gestión remota de dispositivos, conocidas como RMON (Remote MONitor), normas RFC 1757 (antes 1271) para Ethernet y RFC 1513 para Token Ring del IETF (Internet Engineering Task Force), que incluyen sobre unos 200 objetos clasificados en 9 grupos: Alarmas, Estadísticas, Historias, Filtros, Ordenadores, N Principales, Matriz de Tráfico, Captura de Paquetes y Sucesos. Con RMONv2 se decodifican paquetes a nivel 3 de OSI, lo que implica que el trafico puede monitorizarse a nivel de direcciones de red (puertos de los dispositivos) y aplicaciones específicas.

RMON define las funciones de supervisión de la red y los interfaces de comunicaciones entre la plataforma de gestión SNMP, los monitores remotos y los Agentes de supervisión que incorporan los dispositivos inteligentes.

- Alarmas: Informa de cambios en las características de la red, basado en valores umbrales para cualquier variable MIB de interés. Permite que los usuarios configuren una alarma para cualquier Objeto gestionado.

- Estadísticas: Mantiene utilización de bajo nivel y estadísticas de error.

- Historias: Analiza la tendencia, según instrucciones de los usuarios, basándose en la información que mantiene el grupo de estadísticas.

- Filtros: Incluye una memoria para paquetes entrantes y un número cualquiera de filtros definidos por el usuario, para la captura selectiva de información.

- Ordenadores: Una tabla estadística basada en las direcciones MAC, que incluye información sobre los datos transmitidos y recibidos en cada ordenador.

- Los N principales: Contiene solamente estadísticas ordenadas de los "N" ordenadores definidos por el usuario, con lo que se evita recibir información que no es de utilidad.

- Matriz de tráfico: Proporciona información de errores y utilización de la red, en forma de una matriz basada en pares de direcciones, para correlacionar las conversaciones en los nodos más activos.

- Captura de paquetes: Permite definir buffers para la captura de paquetes que cumplen las condiciones de filtrado.

- Sucesos: Registra tres tipos de sucesos basados en los umbrales definidos por el usuario: ascendente, descendente y acoplamiento de paquetes, pudiendo generar interrupciones para cada uno de ellos.

Capitulo V
Implementación De Monitoreo En Oportunidades Oaxaca

5.1 ESTADO ACTUAL

Oportunidades es un programa federal para el desarrollo humano de la población en pobreza extrema. Para lograrlo, brinda apoyos en educación, salud, nutrición e ingreso.

Es un programa interinstitucional en el que participan la Secretaría de Educación Pública, la Secretaría de Salud, el Instituto Mexicano del Seguro Social, la Secretaría de Desarrollo Social, y los gobiernos estatales y municipales.

Este programa se encuentra en un edificio de dos plantas en los cuales tenemos:

- Un Site con 1 router Cisco 2800 donde llega la señal de la coordinación nacional
- Dos switch Cisco Catalyst 2950T que reparten la señal a las diferentes áreas de trabajo
- El edificio cuenta con un total de 32 Host fijos.
- Existen 4 impresoras compartidas en la red

Estos equipos están conectados a una red local con un rango de IP´s 29.23.48.1/24 al 29.23.48.254/24

5.2 PLANTEAMIENTO DEL PROBLEMA

Por causa del los diferentes procesos que se realizan para la emisión de apoyos a las personas de escasos recursos es necesario montar centros de computo provisionales para la captura de los diferentes formatos que se han recibido de las diferentes áreas de operación los cuales contienen información con la cual se les va a otorgar apoyos correspondientes a sus necesidades.

Debido al montaje de estos centros de cómputo y por la necesidad de que los datos capturados se guardan directamente en el servidor de BD es primordial que la red se encuentre funcionando y en buen estado, como no se cuenta con el monitoreo de la red al momento de suceder un error es tardado en ocasiones en reestablecer el servicio ya que hay que revisar los cables de red, el hub o directamente desde el switch.

5.3 SOLUCIÓN

La opción factible que nos proporciona la administración de red, es el monitoreo de los switch´s ya que soportan mensajes SNMP (Simple Network Management Protocol), este tipo de monitoreo es manejado por medio de TRAPS los cuales son generados por el agente y recopilan la información de la red en los cuales nos indica que dispositivos están fallando.

5.4 IMPLANTACIÓN

CONFIGURACION DE SNMP EN EL SWITCH CALTALYS 2950T DE CISCO

El primer paso que hay q hacer es crear la VLAN en donde se va a crear la comunidad en donde vamos a agregar los host´s que integran la red y que van a ser monitoreados.

Ver Anexo 1

Posteriormente podemos ver que se ha creado nuestra VLAN con un *show vlan* el cual nos va a desplegar una lista de todas las VLAN configuradas con las que cuenta nuestro switch.

Ver Anexo 2

Seguimos con relacionar nuestra interfaz FastEthernet 0/2 con la VLAN que hemos creado.

Ver Anexo 3

Le asignamos una dirección IP a nuestra VLAN para poder administrar nuestro equipo de manera remota vía Telnet.

Ver Anexo 4

Una vez que ya nuestra VLAN tiene una dirección IP administrable, tenemos que configurar Telnet para poder ingresar desde otro equipo.

Ver Anexo 5

Una vez terminado de configurar Telnet tenemos que configurar la parte más importante que es ahora configurar el protocolo SNMP dentro de nuestro switch.

Ver Anexo 6

CONFIGURACION DE LOS HOSTS PARA PODER SER MONITOREADOS

Una vez terminado de hacer la configuración se tienen que configurar los equipos de cómputo que van a ser monitoreados por el SW para que estos puedan ser detectados.

Ingresamos al panel de control y entramos a Agregar o quitar Programas.

Ver Anexo 7

Dentro de agregar o quitar programas ingresamos en Agregar o quitar componentes de Windows

Ver Anexo 8

Activamos la opción de Herramientas de administración y supervisión

Ver Anexo 9

Aceptamos los cambios y esperamos a que termine de cargar la nueva configuración

Ver Anexo 10 y 11

MONITOREO DESDE LA ESTACION GESTORA

Iniciamos el Software de monitoreo instalado en la maquina que va a ser nuestro monitor, para este caso utilizáremos el PacketTrap PT360 de Cisco, ya que es compatible con el sistema operativo con el que trabajan los equipos de la organización.

Con este software podemos obtener las direcciones Mac de los equipos, podemos hacer un escaneo de las IP's, podemos conocer que puertos de los equipos están ocupados y cuales están libres, etc.

Con este software podemos observar de manera grafica cuando un Host esta fallando o cuando si esta activo, incluso podemos realizar de manera manual un escaneo para verificar que la red este bien y que no tenga errores

Ver Anexo 12

También podemos realizar un monitoreo por medio de las direcciones IP que estén activas o que tengan destinado un equipo.

Ver Anexo 13

Podemos observar los equipos que ya se encuentran configurados para poder ser administrados con SNMP lo cuales se pueden ver en la tabla.

Ver Anexo 14

CONCLUSIÓN

Podemos ver los resultados de la implantación del monitoreo de la red ya que al poder detectar a tiempo donde están surgiendo los problemas podemos solucionarlos mas rápido y así reestablecer el servicio de red y evitar que se pare el trabajo y la atención a las personas que van a la organización a solicitar algún movimiento relacionado con sus apoyos económicos.

Tanto así como podemos administrar los equipos si llega a surgir algún error o el usuario detecte algo que no se encuentre dentro de lo normal podemos ahorrar tiempo para la revisión del equipo ya que no seria necesario ir físicamente hasta el lugar del usuario para revisar su computadora lo podemos hacer de manera remota, ya que si no se puede resolver de manera remota entonces si ya se procederá en ir a ver que es lo que esta pasando.

ANEXOS

```
Oportunidades>enable
Oportunidades#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
Oportunidades(config)#vlan 2
Oportunidades(config-vlan)#name oposystem
Oportunidades(config-vlan)#exit
Oportunidades(config)#
```

Anexo 1

```
Oportunidades#sh vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
2    oposystem                           active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
 --More--
```

Anexo 2

```
Oportunidades#configure terminal
Enter configuration commands, one per line.     End with CNTL/Z.
Oportunidades(config)#int fa 0/2
Oportunidades(config-if)#switchport mode access
Oportunidades(config-if)#switchport acces vlan 2
Oportunidades(config-if)#
```

Anexo 3

```
%LINK-5-CHANGED: Interface Vlan2,  changed state to up
Oportunidades(config-if)#ip address 29.23.48.1 255.255.255.0
Oportunidades(config-if)#exit
Oportunidades(config)#
```

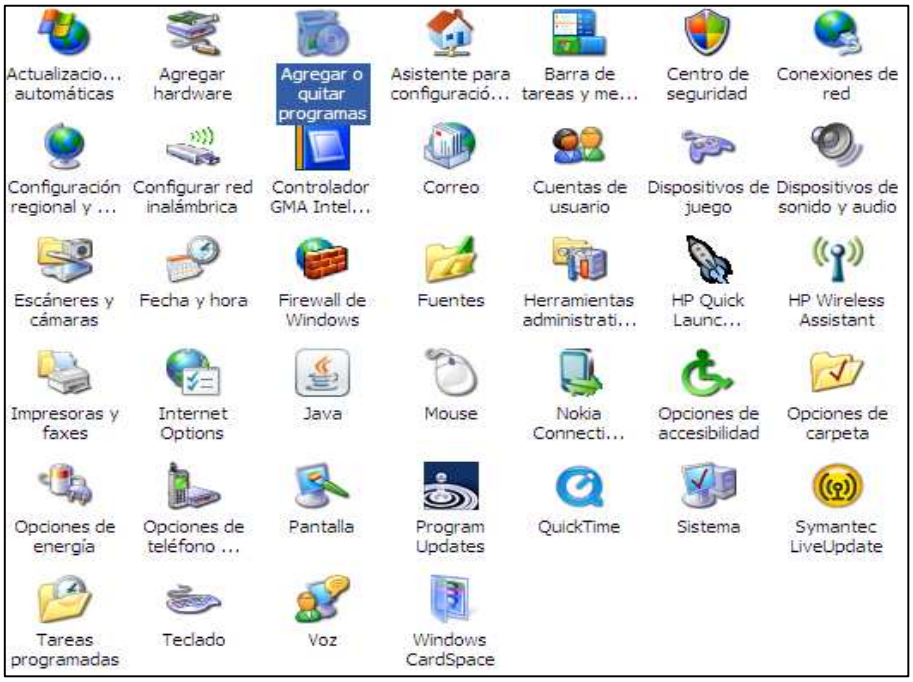
Anexo 4

```
Oportunidades#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Oportunidades(config)#line vty 0 4
Oportunidades(config-line)#login
% Login disabled on line 1, until 'password' is set
% Login disabled on line 2, until 'password' is set
% Login disabled on line 3, until 'password' is set
% Login disabled on line 4, until 'password' is set
% Login disabled on line 5, until 'password' is set
Oportunidades(config-line)#password CEO20
Oportunidades(config-line)#exit
Oportunidades(config)#exit
Oportunidades#
```

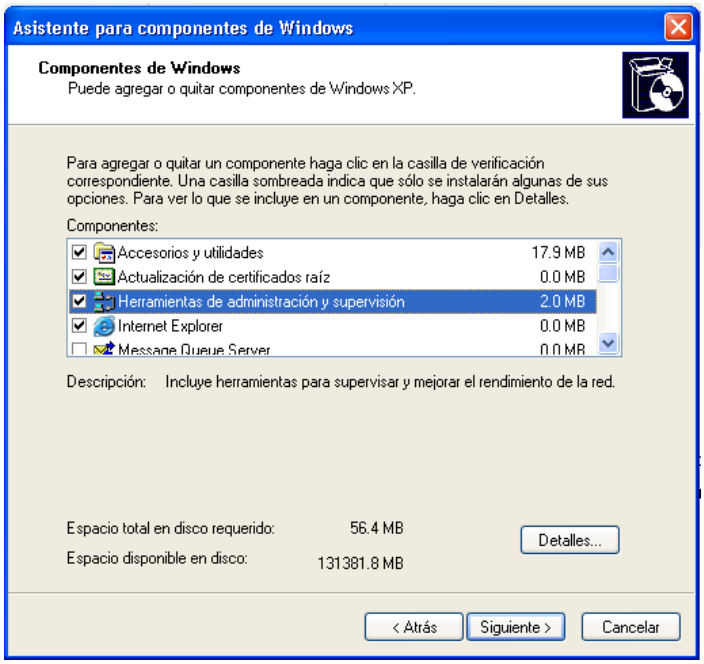
Anexo 5

```
Oportunidades(config)#snmp-server community public
Oportunidades(config)#exit
Oportunidades#
%SYS-5-CONFIG_I: Configured from console by console
Oportunidades#
```

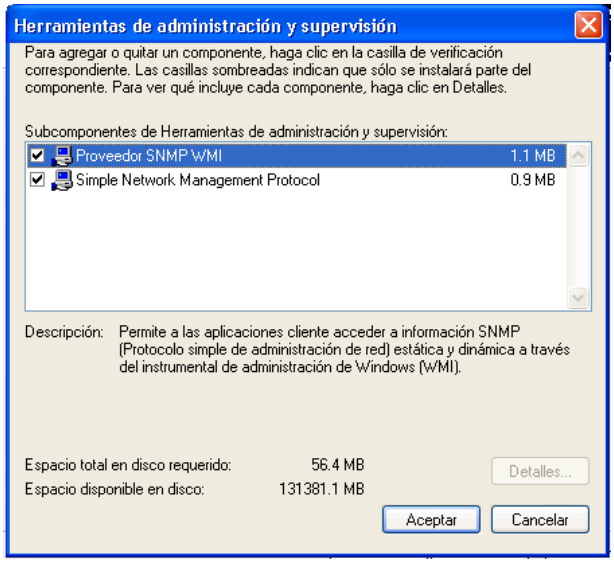
Anexo 6



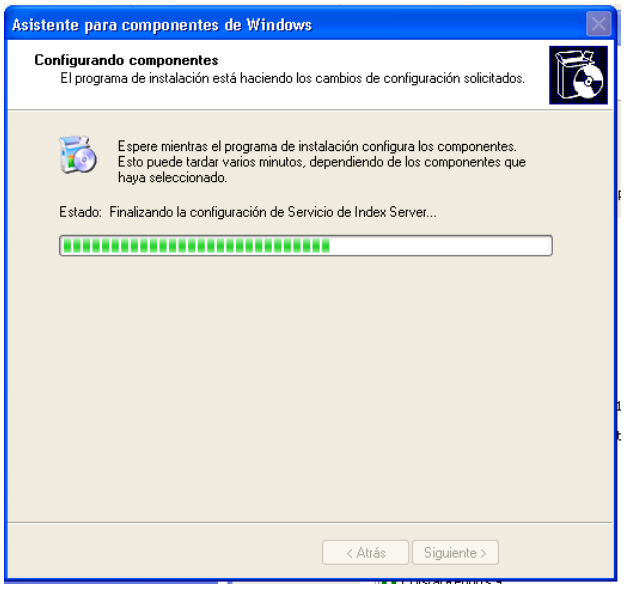
Anexo 7



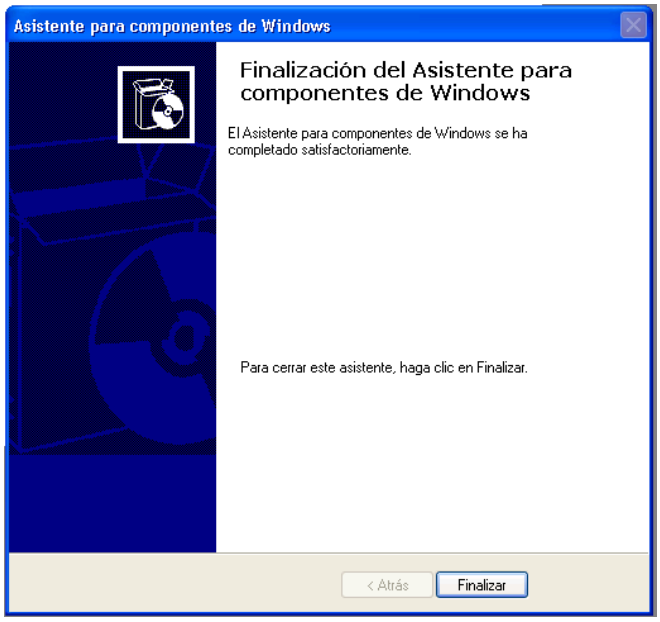
Anexo 8



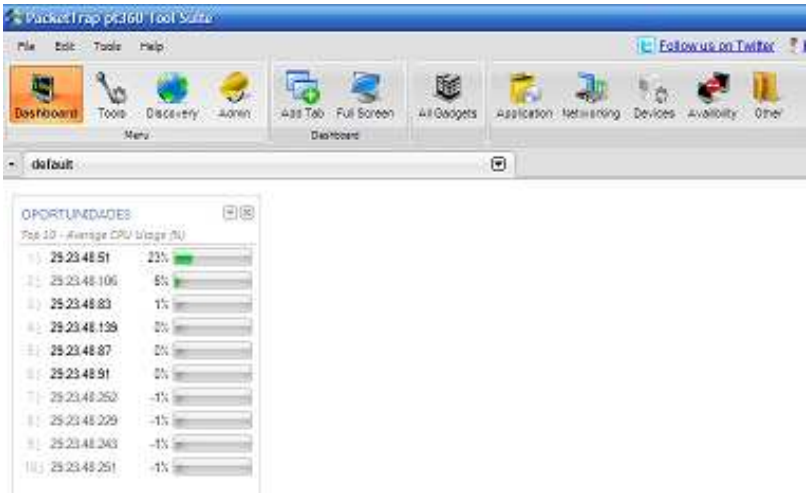
Anexo 9



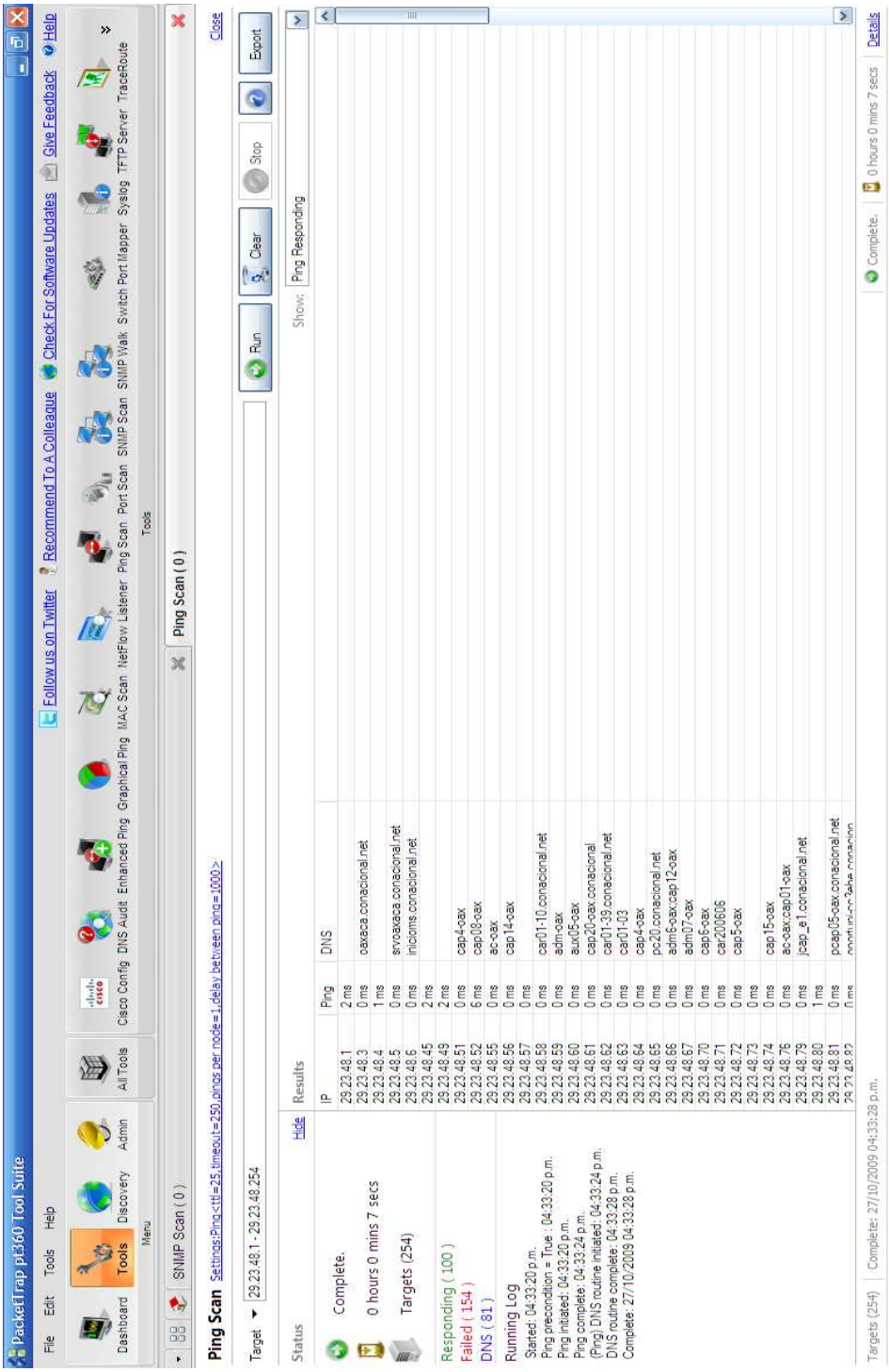
Anexo 10



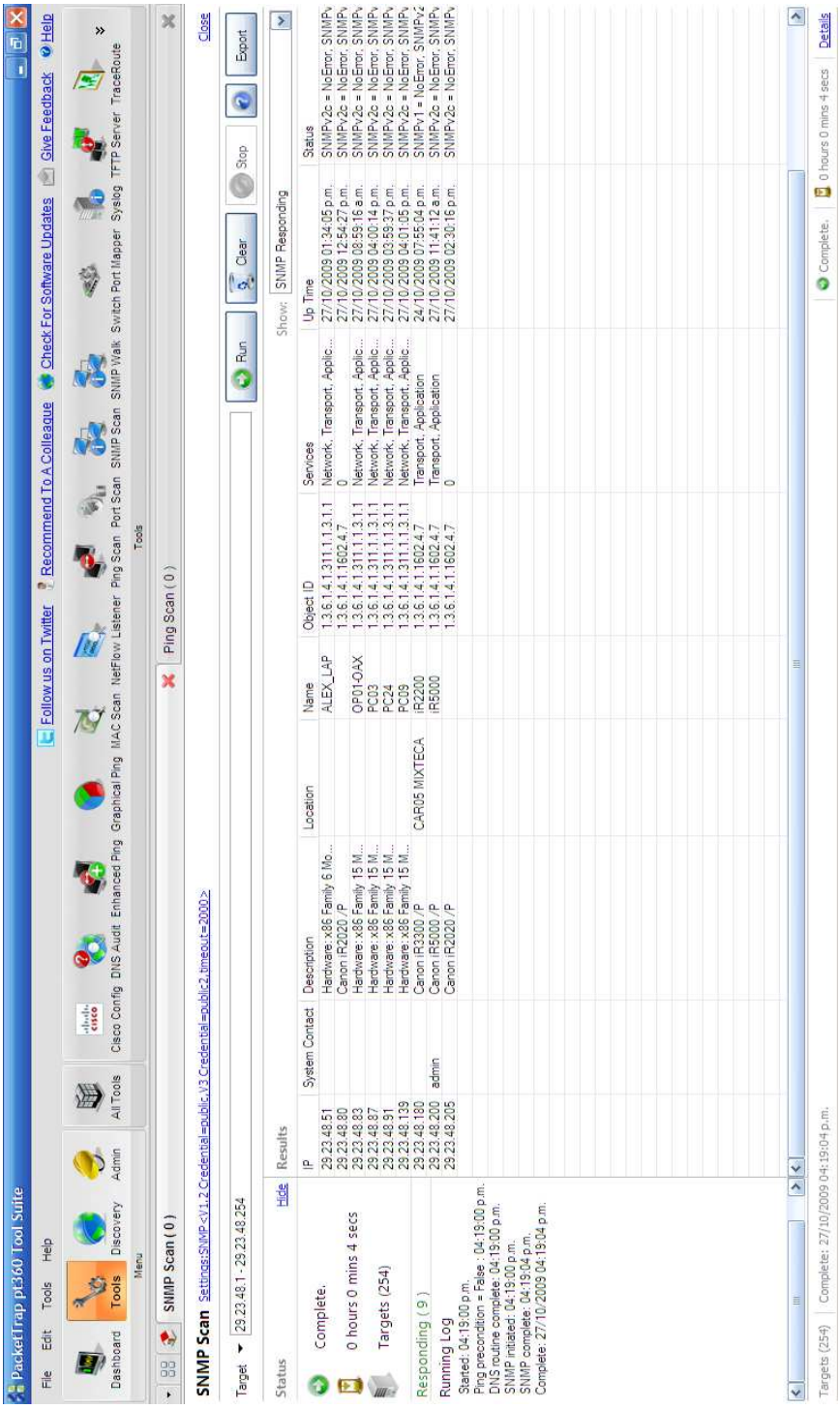
Anexo 11


PacketTrap pt360 Tool Suite
File
Edit
Tools
Help
Follow us on Twitter
Dashboard
Tools
Discovery
Admin
Add Tab
Full Screen
All Gadgets
Application
Networking
Devices
Availability
Other
Menu
Dashboard
default
OPORTUNIDADES
Top 10 - Average CPU Usage (%)
1) 25.23.48.51 23%
2) 25.23.48.106 5%
3) 25.23.48.83 1%
4) 25.23.48.139 0%
5) 25.23.48.87 0%
6) 25.23.48.91 0%
7) 25.23.48.252 -1%
8) 25.23.48.229 -1%
9) 25.23.48.243 -1%
10) 25.23.48.251 -1%

Anexo 12


PacketTrap pt360 Tool Suite
File Edit Tools Help
Follow us on Twitter
Recommend To A Colleague
Check For Software Updates
Give Feedback
Help
Dashboard
Tools
Discovery
Admin
Menu
All Tools
Cisco Config
DNS Audit
Enhanced Ping
Graphical Ping
MAC Scan
NetFlow Listener
Ping Scan
Port Scan
SNMP Scan
SNMP Walk
Switch Port Mapper
Syslog
TFTP Server
TraceRoute
Tools
SNMP Scan (0)
Ping Scan (0)
Ping Scan
Settings:Ping:<ttl=25,timeout=250,pings per node=1,delay between pings=1000>
Close
Target
29.23.48.1 - 29.23.48.254
Run
Clear
Stop
Export
Status
Hide
Results
Show:
Ping Responding
Complete.
0 hours 0 mins 7 secs
Targets (254)
Responding (100)
Failed (154)
DNS (81)
Running Log
Started: 04:33:20 p.m.
Ping precondition = True : 04:33:20 p.m.
Ping initiated: 04:33:20 p.m.
Ping complete: 04:33:24 p.m.
(Ping) DNS routine initiated: 04:33:24 p.m.
DNS routine complete: 04:33:28 p.m.
Complete: 27/10/2009 04:33:28 p.m.
IP
Ping
DNS
29.23.48.1 2 ms
29.23.48.3 0 ms oaxaca.conacional.net
29.23.48.4 1 ms
29.23.48.5 0 ms srvoaxaca.conacional.net
29.23.48.6 0 ms inicioms.conacional.net
29.23.48.45 2 ms
29.23.48.49 2 ms
29.23.48.51 0 ms cap4-oax
29.23.48.52 6 ms cap08-oax
29.23.48.55 0 ms ac-oax
29.23.48.56 0 ms cap14-oax
29.23.48.57 0 ms
29.23.48.58 0 ms car01-10.conacional.net
29.23.48.59 0 ms adm-oax
29.23.48.60 0 ms aux05-oax
29.23.48.61 0 ms cap20-oax.conacional
29.23.48.62 0 ms car01-39.conacional.net
29.23.48.63 0 ms car01-03
29.23.48.64 0 ms cap4-oax
29.23.48.65 0 ms pc20.conacional.net
29.23.48.66 0 ms adm6-oax;cap12-oax
29.23.48.67 0 ms adm07-oax
29.23.48.70 0 ms cap6-oax
29.23.48.71 0 ms car200606
29.23.48.72 0 ms cap5-oax
29.23.48.73 0 ms
29.23.48.74 0 ms cap15-oax
29.23.48.76 0 ms ac-oax;cap01-oax
29.23.48.79 0 ms jcap_e1.conacional.net
29.23.48.80 1 ms
29.23.48.81 0 ms pcap05-oax.conacional.net
Targets (254)
Complete: 27/10/2009 04:33:28 p.m.
Complete.
0 hours 0 mins 7 secs
Details

Anexo 13


PacketTrap pt360 Tool Suite
File Edit Tools Help
Follow us on Twitter
Recommend To A Colleague
Check For Software Updates
Give Feedback
Help
Dashboard
Tools
Discovery
Admin
All Tools
Cisco Config
DNS Audit
Enhanced Ping
Graphical Ping
MAC Scan
NetFlow Listener
Ping Scan
Port Scan
SNMP Scan
SNMP Walk
Switch Port Mapper
Syslog
TFTP Server
TraceRoute
Menu
Tools
SNMP Scan (0)
Ping Scan (0)
SNMP Scan
Settings:SNMP-v1,2 Credential=public,v3 Credential=public2,timeout=2000>
Close
Target
29.23.48.1 - 29.23.48.254
Run
Clear
Stop
Export
Status
Hide
Results
Show:
SNMP Responding
Complete.
0 hours 0 mins 4 secs
Targets (254)
Responding (9)
Running Log
Started: 04:19:00 p.m.
Ping precondition = False : 04:19:00 p.m.
DNS routine complete: 04:19:00 p.m.
SNMP initiated: 04:19:00 p.m.
SNMP complete: 04:19:04 p.m.
Complete: 27/10/2009 04:19:04 p.m.
IP
System Contact
Description
Location
Name
Object ID
Services
Up Time
Status
29.23.48.51
29.23.48.80
29.23.48.83
29.23.48.87
29.23.48.91
29.23.48.139
29.23.48.180
29.23.48.200
29.23.48.205
admin
Hardware: x86 Family 6 Mo...
Canon iR2020 /P
Hardware: x86 Family 15 M...
Hardware: x86 Family 15 M...
Hardware: x86 Family 15 M...
Hardware: x86 Family 15 M...
Canon iR3300 /P
Canon iR5000 /P
Canon iR2020 /P
CAR05 MIXTECA
ALEX_LAP
OPD1-OAX
PC03
PC24
PC09
iR2200
iR5000
1.3.6.1.4.1.311.1.1.3.1.1
1.3.6.1.4.1.1602.4.7
Network, Transport, Applic...
Transport, Application
0
27/10/2009 01:34:05 p.m.
27/10/2009 12:54:27 p.m.
27/10/2009 08:59:16 a.m.
27/10/2009 04:00:14 p.m.
27/10/2009 03:59:37 p.m.
27/10/2009 04:01:05 p.m.
24/10/2009 07:55:04 p.m.
27/10/2009 11:41:12 a.m.
27/10/2009 02:30:16 p.m.
SNMPv2c = NoError, SNMPv
SNMPv1 = NoError, SNMPv
Targets (254)
Complete: 27/10/2009 04:19:04 p.m.
Complete.
0 hours 0 mins 4 secs
Details

Anexo 14

GLOSARIO

CSMA/CD: siglas que corresponden a Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

DNS: El sistema de nombre de dominio (en inglés Domain Name System, DNS) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

FTP: File Transfer Protocol - Protocolo de Transferencia de Archivos, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

GATEWAY: (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

HUB: concentrador. Es un dispositivo que se utiliza típicamente en topología en estrella como punto central de una red, donde por ende confluyen todos los enlaces de los diferentes dispositivos de la misma.

ICMP: Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IP: el número que identifica a cada dispositivo dentro de una red con protocolo IP; Un protocolo usado para la comunicación de datos a través de una red.

IPX: El protocolo intercambio de paquetes entre redes (IPX, Internetwork Packet Exchange) se usa en redes Novell NetWare.

ISO: La Organización Internacional para la Estandarización, cuyo nombre en inglés es International Organization for Standardization, nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

MAC: Media Access Control (Control de acceso al medio). Identificador hexadecimal de 48 bits que corresponde de manera única a cualquier interfaz o dispositivo de red (routers, switch, tarjetas de red). Esto equivale a 2^48 direcciones posibles, cuya nomenclatura es XX:XX:XX:XX:XX:XX.

MIB: Base de Información Gestionada (Management Information Base) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones. Es parte de la gestión de red definida en el modelo OSI. Define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutadores y conmutadores) en la red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o gauge), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

NIC. (Network Interface Card) o tarjeta de red. Conectada a un slot libre de la computadora, es la encargada de gestionar las comunicaciones. Es, en definitiva, la que proporciona la conexión física entre la computadora y el cable.

OSI: Open Source Initiative es una organización dedicada a la promoción del código abierto. Fue fundada en febrero de 1998 por Bruce Perens y Eric S. Raymond.

PING: Es una utilidad que comprueba el estado de la conexión con uno o varios equipos remotos por medio de los paquetes de solicitud de eco y de respuesta de eco (ambos definidos en el protocolo de red ICMP) para determinar si un sistema IP específico es accesible en una red. Es útil para diagnosticar los errores en redes o enrutadores IP.

RAM: La memoria de acceso aleatorio (random-access memory) es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados. Es el área de trabajo para la mayor parte del software de un computador.

TCP: Transmission Control Protocol (Protocolo de control de transmisión). Protocolo encargado de la transferencia de paquetes, libre de errores con servicio de puertos, pudiendo recuperar paquetes perdidos o desordenados producidos por el protocolo IP.

TCP/IP: Es un conjunto de protocolos que permiten la transmisión de información en redes. Consiste en cuarto capas, capa de aplicación, capa de transporte, capa de Internet y capa de acceso a la red.

TRAP: Mensaje enviado por un agente SNMP a un NMS, consola, o terminal, para indicar la ocurrencia de un evento significativo, como una condición definida específicamente, o un umbral que ha sido alcanzado.

UDP: *User Datagram Protocol* (Protocolo de datagrama de usuario). Es un protocolo sencillo que ofrece servicio de puertos y que se usa para aplicaciones de red que se ejecuten dentro de una subred, ya que no es fiable (ya que no se verifica si los paquetes han llegado a su destino como ocurre con el TCP).

VPN: *Virtual Private NetworkK* (Red privada virtual). Es una tecnología de red que permite la extensión de una LAN sobre una WAN. Se usa principalmente para conexiones seguras remotas al puesto de trabajo desde cualquier lugar del mundo (VPN de acceso remoto) o la conexión entre dos oficinas o sucursales de cualquier empresa (VPN punto a punto).

VLAN: *Virtual LAN* (Red de área local virtual). Red local que podemos crear sin importarnos cómo o dónde estén ubicadas las máquinas. Las comunicaciones entre VLANs requieren de un router o de un switch gestionable. Permiten dividir una red local en varias redes virtuales. Las define es estándar IEEE 802.1Q.

BIBLIOGRAFÍA

- CCNA 2.1.2 CISCO SISTEMS.
- http://www.coit.es/publicac/publbit/bit102/quees.htm
- http://cavalcanti.blip.tv/
- http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html
- http://www.packettrap.com/product/pt360/links/EnablingSNMPOnWindowsXP.html
- http://www.packettrap.com/support/
- http://www.normes-internet.com/normes.php?rfc=rfc1700&lang=es
- http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a05.shtml
- http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol