ESCUELA POLITECNICA NACIONAL

ESCUELA DE FORMACION TECNOLOGICA

Elaboración e Implementación de laboratorios didácticos para monitoreo del tráfico en la red, antes y después de segmentar en dominios de colisión y broadcast utilizando el open source CACTI.

PROYECTO PREVIO A LA OBTENCIÒN DEL TITULO DE TECNOLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

DÍAZ NARVÁEZ JEANETH VIVIVANA
TIPAN LEMA LUIS GUILLERMO

DIRECTOR: ING. DANIEL MANANGON
ING. CESAR GALLARDO
ING. EDGAR CHICAIZA

Quito, diciembre 2006

DECLARACION

Nosotros, Jeaneth Viviana Díaz Narváez Luis Guillermo Tipán, declaramos bajo juramento que el trabajo aquí descrito es de nuestra auditoria; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las transferencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de propiedad intelectual, por su Reglamento y por la normatividad institucional vigente.

_____	_____
Jeaneth Díaz	Luis Tipán

CERTIFICACION

Certifico que el presente trabajo fe desarrollado por Jeaneth Díaz y Luis Tipán, bajo mi supervisión.

_____

Daniel Manangón

DIRECTOR DE PROYECTO

INDICE

INDICE DE FIGURAS Y TABLAS

RESUMEN

El desarrollo, practica y documentado de esta investigación, surgió por la necesidad de crear laboratorios en una red prototipo con guías de estudio que permitan a los profesores utilizar como ayuda y a los estudiantes a entender y realizar con mayor facilidad las practicas de laboratorio.

A continuación se resume los capítulos que se han considerado necesarios para la realización de este proyecto:

CAPITULO 1. INTRODUCCIÓN:

Diseñar e implementar una red prototipo, utilizando la información necesaria para la implementación de los laboratorios didácticos

Configuración de los dispositivos que se va ha utilizar (Router, Switch, Estaciones de Trabajo) para el buen funcionamiento de la red.

Estudio, Implementación y Configuración del CACTI, servidor Proxy Squid

CAPITULO 2. ESTUDIO DE LA RED PROTOTIPO

Este capitulo se basa en el estudio de:

Redes LAN, Topología Bus, Diseño de una red Prototipo, Funcionamiento de la Red, Utilización del comando Ping, Modelos OSI y TCP/IP, Dominios de Colisión, Dominios de Broadcast, dispositivos utilizados como (Switch de capa 2, Router de capa 3 y sus utilidades), Definición y Características del Cacti y Proxy.

CAPITULO 3. ESTUDIO DE VLAN'S

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico, que tienen su propio dominio de broadcast, esto indica que solo los equipos que pertenecen a una VLAN determinada podrán compartir información.

CAPITULO 4. CONFIGURACIÓN E IMPLEMENTACIÓN DE LOS EQUIPOS.

Los equipos a ser utilizados en la ejecución de la práctica son:
Switch Catalyst 1900.
Router 2500 y 1600
Hosts (Estaciones de trabajo)

Los servidores levantados para la práctica son:
Servidor Cacti
Proxy Squid.

CAPITULO 5. CONCLUSIONES Y RECOMENDACIONES.

En conclusión la red creada con VLAN’s es mas segura que la de Topología Bus, pero al utilizar Routers segmentamos tanto dominios de Colisión como de Broadcast, por lo que es mas eficiente comparado con otro tipo de esquemas.
La utilización de switches, routers, evidencia la disminución de dominios de colisión y broadcast determinado a través de los sistemas de monitoreo Cacti y los instalados en el Proxy (iftop).

Se recomienda independizar el laboratorio para los estudiantes de la carrera de ASI de los equipos y configuraciones actualmente existentes, ya que de esta manera se podrán realizar laboratorios con mayor rapidez y determinar inconvenientes de red interna o externa.

CAPITULO I – INTRODUCCIÓN

1.1 ANTECEDENTES

El proyecto de elaboración e implementación de laboratorios didácticos para monitoreo del tráfico en la red, antes y después de segmentar en dominios de colisión y de broadcast utilizando el open source CACTI, surgió por la necesidad de crear laboratorios en una red prototipo con guías de estudio para los estudiantes.

1.2 OBJETIVOS DE LA INVESTIGACIÓN

1.2.1 OBJETIVO GENERAL

La elaboración de guías de estudio para los estudiantes permitirá a los profesores impartir clases referente a este tema, con la finalidad que los estudiantes puedan aplicarlo en sus prácticas correspondientes.

1.2.2 OBJETIVOS ESPECÍFICOS

- Diseño e implementación de una red prototipo.

    - Diseño de la red con segmentos de colisión mediante topología Bus.
    - Configurar segmentos de colisión y broadcast en la red con VLANs.
    - Configurar y gestionar dominios de colisión y broadcast en la red utilizando routers.

- Proveer la información necesaria para la implementación de los laboratorios didácticos

- Configuración de los dispositivos que se utilizaran (router, switch, estaciones de trabajo) para el buen funcionamiento de la red.

- Verificar que la red está actuando satisfactoriamente con las pruebas necesarias (ping, trace route, entre otras).

- Generar datos de prueba causando inundación en la red con cada uno de los diseños, para determinar mediante el análisis de mediciones el modelo más factible a usar y así que sea útil para los estudiantes.

- Estudiar e Implementar el CACTI.

- Configuración del CACTI

- Mediante el software CACTI se realizará consultas de los consumos: diario, semanal, mensual y anualmente. En la tabla diaria, todos los valores leídos serán intervalos hechos en un promedio de cinco minutos.

- Interpretación y análisis del tráfico en la red prototipo

- Recomendaciones a la red prototipo (topología bus, red con vlan's, routers de capa 3, switches de capa 2)

1.3 ALCANCE / METAS

Esta elaboración e implementación podrá ser usada en toda la comunidad Politécnica con el fin de ayudar con guías de laboratorio para quienes les interese realizar prácticas y también monitorear el tráfico en cada uno de los laboratorios que tienen las carreras de la Escuela Politécnica Nacional, con la ayuda de laboratorios con equipos óptimos para el diseño de las redes podremos implantar la mejor opción de red prototipo, y así los estudiantes no tengan problema al momento de utilizar y verificar la red (monitorear), con esto proporcionar una manera de espía, y telecontrol en el computador, de esta forma obtener los datos de los equipos existente en la red.

1.4 JUSTIFICACIÓN PRÁCTICA DEL PROYECTO

La Elaboración e Implementación de laboratorios didácticos, está enfocado a

mejorar y facilitar tanto a los estudiantes como a los profesores las prácticas de laboratorio mediante guías de estudio y documentación pertinente, con esto ampliar el campo de estudio en el ámbito de las redes prototipo y dotar de nuevas expectativas hacia la mejor manera de evitar estrés en la red mediante problemas de colisiones y de broadcast que tenemos hoy en día.

En estas guías de estudio podremos apreciar la importancia de las siguientes asignaturas dictadas en la ESFOT-ASI; así:

- Sistemas Operativos I y II

  Para la práctica se utilizo los conocimientos adquiridos del sistema operativo Linux, ya que el servidor proxy (Fedora Core 2) como el servidor cacti (Fedora Core 3), fueron levantados en este sistema operativo, además de la correcta configuración de los equipos en Windows para que la red tenga un correcto funcionamiento.

- Arquitectura I y II

  La identificación y función de los diferentes componentes de un PC, fueron aplicadas en el desarrollo de este trabajo, al tener que realizar las adecuaciones correspondientes a hardware y software, para de esta manera tener un PC con las características necesarias para la implementación del servidor proxy y cacti.

- Redes I y II

  El estudio fue basado en el modelo OSI y el modelo TCP/IP, especificando cada capa y sus aplicaciones con referencia a los diferentes dispositivos utilizados (router, switch, hub, cables, etc) y a sus configuraciones correspondientes a través del Hyperterminal (depende del dispositivo) para el funcionamiento de la red.

- Administración de Redes TCP/IP

  Se trabaja mediante consola aplicando comandos en Linux en forma local y remota (ssh en linux), conociendo una forma diferente de realizar las aplicaciones que generalmente se realizan en una interfaz grafica como lo

tiene windows (editor vi, transferencia de archivos, crear directorios, etc.). También se realiza la asignación de direcciones IP para los diferentes equipos que lo requieran para trabajar en la red.

- Tópicos Especiales

  Es fundamental para la realización de este proyecto la utilización de programación en PHP y la creación de una base de datos en MySql (para la creación de la interfaz en el servidor cacti), lo cual es utilizado para la implementación de la plataforma de monitoreo.

CAPITULO II – ESTUDIO DE RED PROTOTIPO

2.1 REDES LAN

2.1.1 LAN (LOCAL ÁREA NETWORK): REDES DE ÁREA LOCAL

Es un sistema de comunicación entre computadoras que permite compartir información, con la característica de que la distancia entre las computadoras debe ser pequeña, no superior a 3 Km. y distancia del PC al rack máximo 100m.

Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo. Se caracterizan por: tamaño restringido, tecnología de transmisión, por lo general broadcast **(**es decir, aquella en que a un sólo cable se conectan todas las máquinas**)**, alta velocidad y topología.

Son redes con velocidades entre 10 y 100 Mbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos.
Dentro de este tipo de red podemos nombrar a INTRANET, una red privada que utiliza herramientas tipo Internet, pero disponible solamente dentro de la organización.
Ej: IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring).[1]

[1] http://www.htmlweb.net/redes/topologia/topologia_11.html

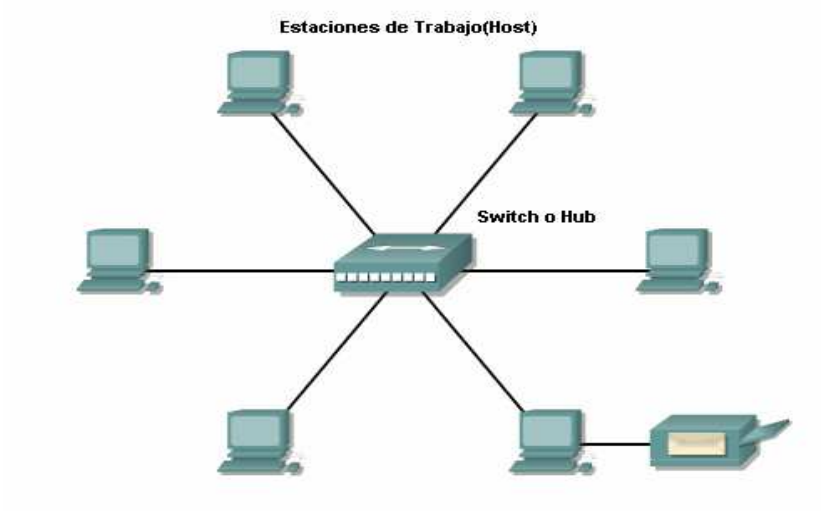


Fig. 1 - Redes LAN

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

2.1.2 REDES LAN MÁS COMUNES

Las topologías LAN más comunes son:

- Ethernet
- Token Ring
- FDDI

2.1.2.1 Ethernet

Topología de bus lógica y en estrella física, o en estrella extendida.

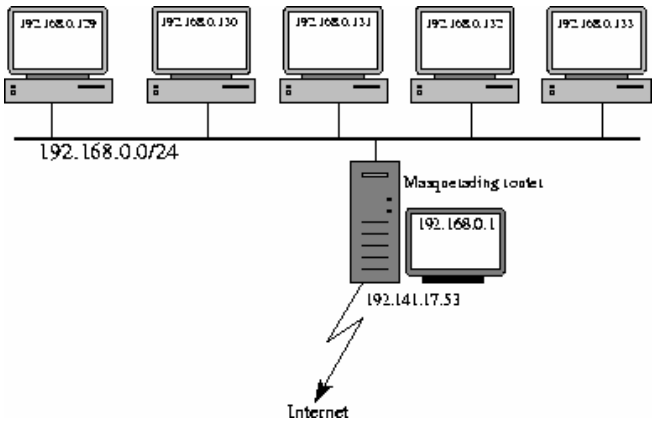


Fig. 2 - Red Ethernet

Fuete: http://www.linuxparatodos.net/linux/images/sv5755751.gif

2.1.2.2 Token Ring

Topología de anillo lógica y una topología física en estrella. Las redes Token Ring son redes de tipo determinista, al contrario de las redes Ethernet. En ellas, el acceso al medio está controlado, por lo que solamente puede transmitir datos una máquina por vez, implementándose este control por medio de un token de datos, que define qué máquina puede transmitir en cada instante. Token Ring e IEEE 802.5 son los principales ejemplos de redes de transmisión de tokens.

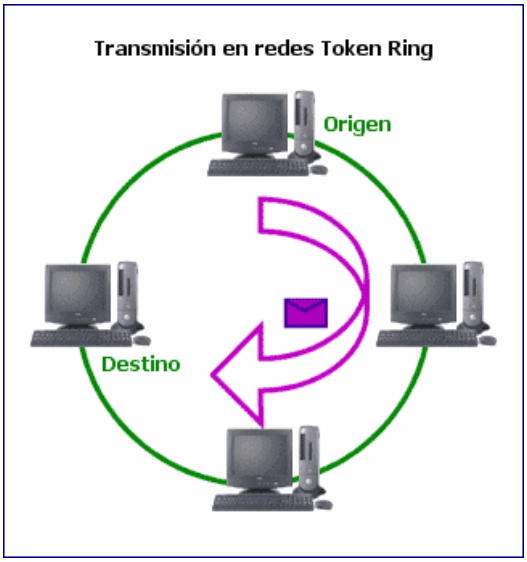


Fig. 3 - Token Ring

Fuente: http://www.htmlweb.net/redes/topologia/topologia_1.html

2.1.2.3 FDDI

Topología de anillo lógica y topología física de anillo doble. Las redes FDDI (Fiber Distributed Data Interface - Interfaz de Datos Distribuida por Fibra) surgieron a mediados de los años ochenta para dar soporte a las estaciones de trabajo de alta velocidad, que habían llevado las capacidades de las tecnologías Ethernet y Token Ring existentes hasta el límite de sus posibilidades.

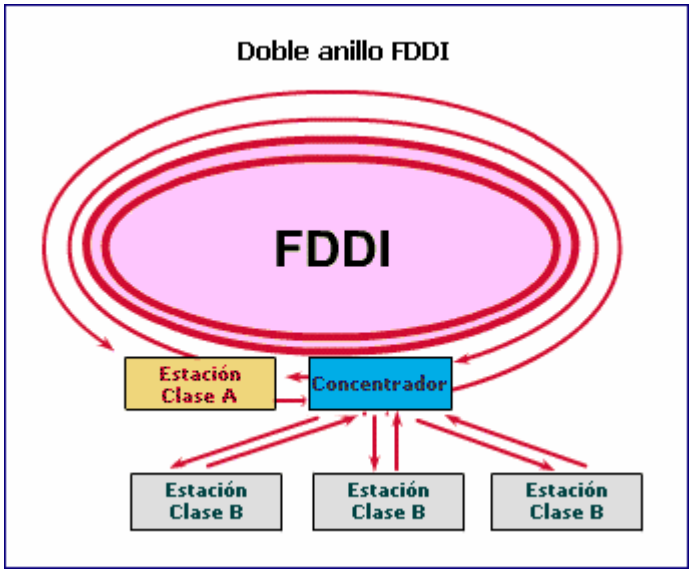


Fig. 4 - Red FDDI

Fuente: http://www.htmlweb.net/redes/topologia/topologia_1.html

2.1.3 VENTAJAS DE LAN

En una empresa suelen existir muchos ordenadores, los cuales necesitan de su propia impresora para imprimir informes, los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa, por lo que será necesario copiarlos en éste, pudiéndose producir desfases entre los datos de un usuario y los de otro, la ocupación de los recursos de almacenamiento en disco se multiplican (redundancia de datos), los ordenadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos (redundancia de software).

La solución a estos problemas se llama red de área local LAN (Local Area Network).

La red de área local nos va a permitir compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia de software) y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, un escáner, etc. (se elimina la redundancia de hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat.

Se permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y se permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos. Además una red de área local conlleva un importante ahorro, tanto de dinero, ya que no es preciso comprar muchos dispositivos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica compartida por varios ordenadores conectados en red; como de tiempo, ya que se logra una mejor gestión de la información y del trabajo.

2.1.4 CARACTERÍSTICAS DE LA LAN

- ✓ Tecnología broadcast (difusión) con el medio de transmisión compartido
- ✓ Cableado específico instalado normalmente a propósito
- ✓ Capacidad de transmisión comprendida entre 10 y 100 Mbps
- ✓ Extensión máxima no superior a 3 Km. (una FDDI puede llegar a 200 Km.)
- ✓ Uso de un medio de comunicación privado.
- ✓ La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos, cable par trenzado UTP y fibra óptica).
- ✓ La facilidad con que se pueden efectuar cambios en el hardware y el software.
- ✓ Gran variedad y número de dispositivos conectados.
- ✓ Posibilidad de conexión con otras redes.

2.1.5 REDES LAN ETHERNET

Ethernet es la tecnología de red LAN más usada, resultando idóneas para aquellos casos en los que se necesita una red local que deba transportar tráfico esporádico y ocasionalmente pesado a velocidades muy elevadas. Las redes Ethernet se implementan con una topología física de estrella y lógica de bus, y se caracterizan por su alto rendimiento a velocidades de 10 -100 Mbps.

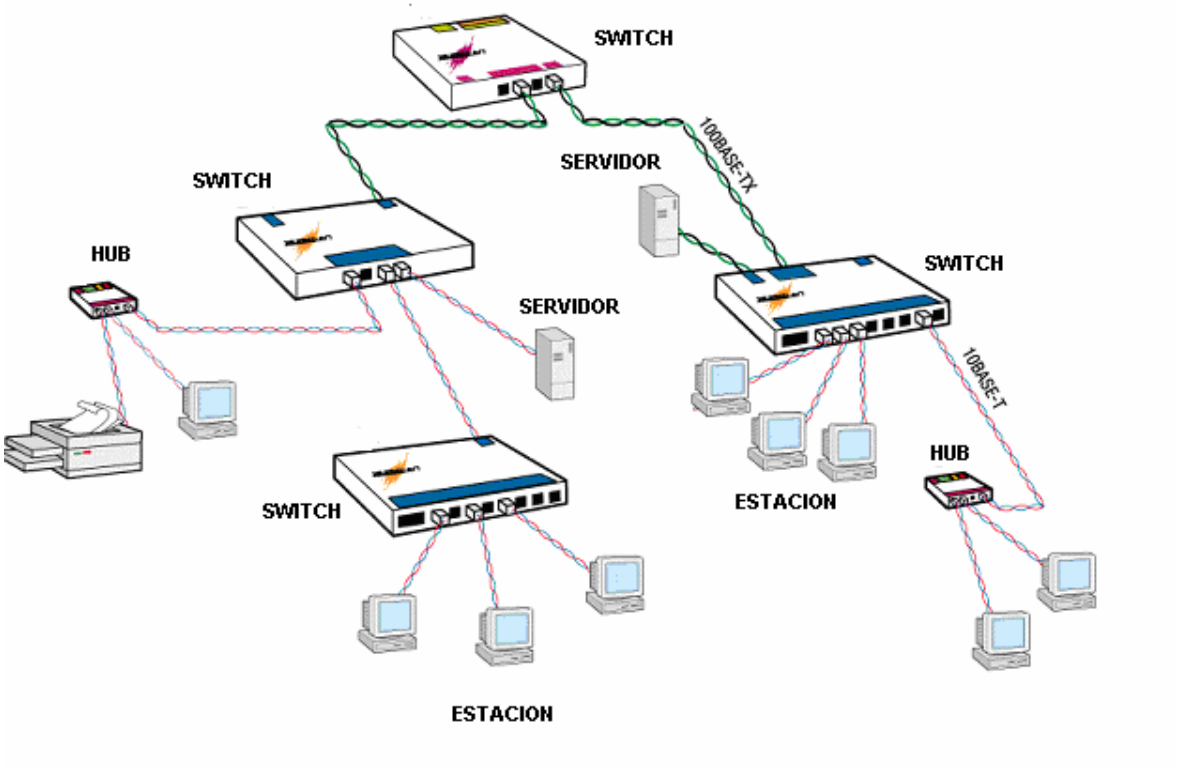


Fig. 5 - Red Lan Ethernet

Fuente: http://www.consulintel.es/Imagenes/Tutoriales/Lantronix/fe_net.gif

El origen de las redes Ethernet hay que buscarlo en la Universidad de Hawai, donde se desarrollo en los años setenta, con el Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones, CSMA/CD (Carrier Sense and Multiple Access with Collition Detection), utilizado actualmente por Ethernet. Este método surgió ante la necesidad de implementar en las islas Hawai un sistema de comunicaciones basado en la transmisión de datos por radio, que se llamó Aloha, y permite que todos los dispositivos puedan acceder al mismo medio, aunque sólo puede existir un único emisor en cada instante.

Con ello todos los sistemas pueden actuar como receptores de forma simultánea, pero la información debe ser transmitida por turnos.

Las redes Ethernet son de carácter no determinista, en la que las estaciones pueden transmitir datos en cualquier momento. Antes de enviarlos, escuchan el medio de transmisión para determinar si se encuentra en uso. Si lo está, entonces esperan. En caso contrario, las estaciones comienzan a transmitir. En caso de

que dos o más estaciones empiecen a transmitir tramas a la vez, se producirán encontronazos o choques entre tramas diferentes que quieren pasar por el mismo sitio a la vez. Este fenómeno se denomina colisión, y la porción de los medios de red donde se producen colisiones se denomina dominio de colisiones.
Existen dos especificaciones diferentes para un mismo tipo de red, Ethernet e IEEE 802.3. Ambas son redes de broadcast, lo que significa que cada máquina puede ver todas las tramas, aunque no sea el destino final de las mismas. Cada máquina examina cada trama que circula por la red para determinar si está destinada a ella. De ser así, la trama pasa a las capas superiores para su adecuado procesamiento. En caso contrario, la trama es ignorada.

Ethernet proporciona servicios correspondientes a las capas físicas y de enlace de datos del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física y la porción de acceso al canal de la capa de enlace de datos, pero no define ningún protocolo de Control de Enlace Lógico.

Ethernet es una tecnología de broadcast de medios compartidos. El método de acceso CSMA/CD que se usa en Ethernet ejecuta tres funciones:

1. Transmitir y recibir paquetes de datos.
2. Decodificar paquetes de datos y verificar que las direcciones sean válidas antes de transferirlos a las capas superiores del modelo OSI.
3. Detectar errores dentro de los paquetes de datos o en la red.

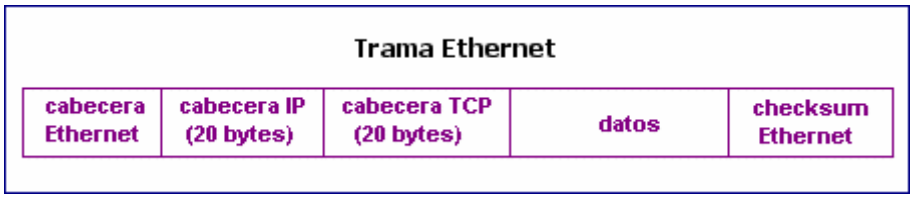
Tanto Ethernet como IEEE 802.3 se implementan a través de la tarjeta de red o por medio de circuitos en una placa dentro del host.

2.1.5.1 Formato de Trama Ethernet

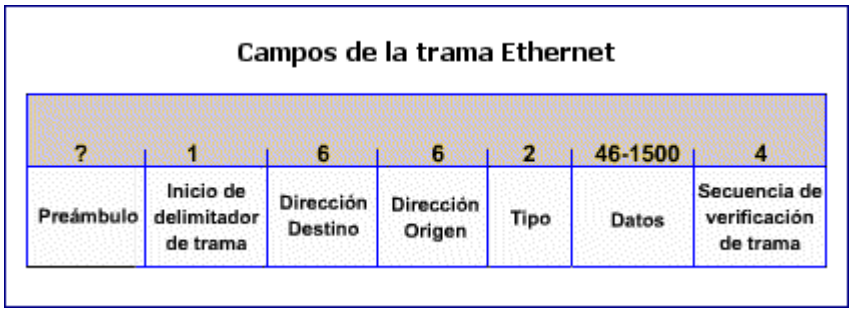
Según se ha visto, los datos generados en la capa de aplicación pasan a la capa de transporte, que los divide en segmentos, porciones de datos aptas para su transporte por red, y luego van descendiendo por las sucesivas capas hasta llegar a los medios físicos. Conforme los datos van bajando por la pila de capas, paso a paso cada protocolo les va añadiendo una serie de cabeceras y datos adicionales;

necesarios para poder ser enviados a su destino correctamente. El resultado final es una serie de unidades de información denominadas tramas, que son las que viajan de una estación a otra.

La forma final de la trama obtenida, en redes Ethernet, es la siguiente:



Y los principales campos que la forman son:



2.1.5.1.1 Preámbulo

Patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3. La trama Ethernet incluye un byte adicional que es el equivalente al campo Inicio de Trama (SOF) de la trama IEEE 802.3.

2.1.5.1.2 Inicio de delimitador de trama (Sof)

Byte delimitador de IEEE 802.3 que finaliza con dos bits 1 consecutivos, y que sirve para sincronizar las porciones de recepción de trama de todas las estaciones de la red. Este campo se especifica explícitamente en Ethernet.

2.1.5.1.3 Direcciones destino y origen

Incluye las direcciones físicas (MAC) únicas de la máquina que envía la trama y de la máquina destino. La dirección origen siempre es una dirección única, mientras que la de destino puede ser de broadcast única (trama enviada a una

sola máquina), de broadcast múltiple (trama enviada a un grupo) o de broadcast (trama enviada a todos los nodos).

2.1.5.1.4 Tipo (Ethernet)

Especifica el protocolo de capa superior que recibe los datos una vez que se ha completado el procesamiento Ethernet.

2.1.5.1.5 Longitud (IEEE 802.3)

Indica la cantidad de bytes de datos que sigue este campo.

2.1.5.1.6 Datos

Incluye los datos enviados en la trama. En la especificación IEEE 802.3, si los datos no son suficientes para completar una trama mínima de 64 bytes, se insertan bytes de relleno hasta completar ese tamaño (tamaño mínimo de trama). Por su parte, las especificaciones Ethernet versión 2 no especifican ningún relleno, Ethernet espera por lo menos 46 bytes de datos.

2.1.5.1.6 Secuencia de verificación de trama (FCS)

Contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de Ethernet y el checksum de verificación de la trama, comprueba que los datos correspondan a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese. El tamaño máximo de los paquetes en las redes Ethernet es de 1500 bytes.

2.1.6 TIPOS DE REDES ETHERNET

Existen por lo menos 18 variedades de Ethernet, relacionadas con el tipo de cableado empleado y con la velocidad de transmisión, como se puede apreciar en la tabla 2.1

Variedades de red Ethernet

Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m	Estrella	Bus
1000Base-T	UTP Cat 5	1000 Mbps	100 m	Estrella	Bus

Tabla 1 - Variedad de la Red Ethernet

Fuente: http:// www.pc-doctor.com.mx/.../temas/Redes.html

2.2 TOPOLOGIA BUS

Una Red en forma de Bus o Canal de difusión es un camino de comunicación bidireccional con puntos de terminación bien definidos. Cuando una estación trasmite, la señal se propaga a ambos lados del emisor hacia todas las estaciones conectadas al Bus hasta llegar a las terminaciones del mismo. Así, cuando una estación trasmite su mensaje alcanza a todas las estaciones, por esto el Bus recibe el nombre de canal de difusión.

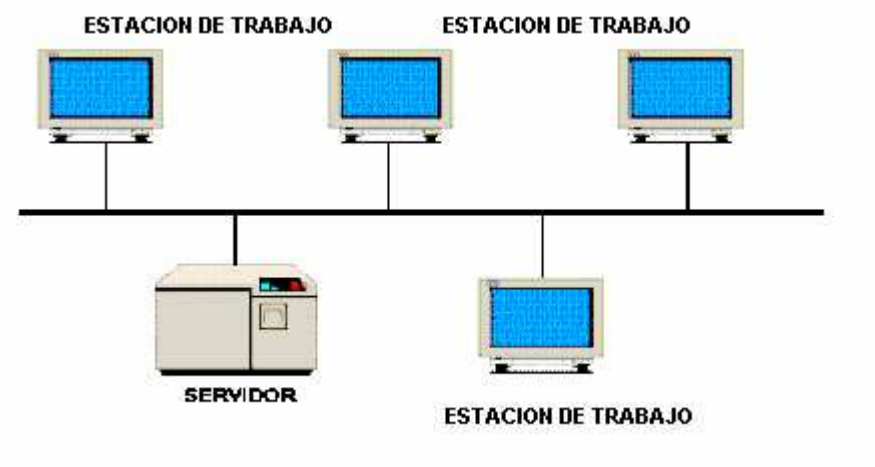


Fig. 6 - Topología Bus

Fuente: http://www2.canalaudiovisual.com/ezine/books/acREDES/2redes05.htm

Otra propiedad interesante es que el Bus actúa como medio pasivo y por lo tanto, en caso de extender la longitud de la red, el mensaje no debe ser regenerado por repetidores (los cuales deben ser muy fiables para mantener el funcionamiento de la red). En este tipo de topología cualquier ruptura en el cable impide la operación normal y es muy difícil de detectar. Por el contrario, el fallo de cualquier nodo no impide que la red siga funcionando normalmente, lo que permite añadir o quitar nodos a la red sin interrumpir su funcionamiento. Una variación de la topología en Bus es la de árbol, en la cual el Bus se extiende en más de una dirección facilitando el cableado central al que se le añaden varios cables complementarios. La técnica que se emplea para hacer llegar la señal a todos los nodos es utilizar dos frecuencias distintas para recibir y transmitir. Las características descritas para el Bus siguen siendo válidas para el árbol.

2.2.1 ELEMENTOS:

Servidor

Estación de Trabajo

Cable par Trenzado

Tarjeta de red NIC

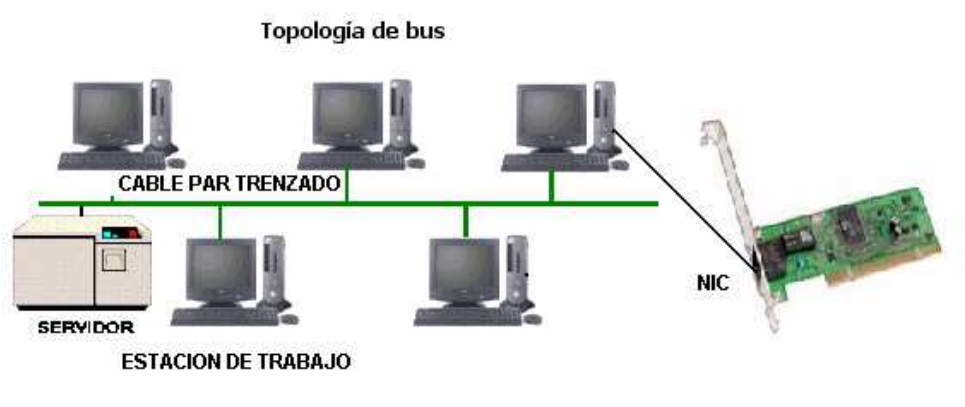


Fig. 7 - Elementos de la Topología Bus

Fuente: http://www2.canalaudiovisual.com/ezine/books/acREDES/2redes05.htm

2.2.2 CARACTERISTICAS

- Varias computadoras compartiendo un solo cable troncal.
- Sólo una computadora puede usar el cable a la vez.
- Si falla el troncal, falla toda la red.
- La instalación es simple y barata.

2.2.3 VENTAJAS DE LA TOPOLOGÍA DE BUS.

- Fácil de instalar y mantener.
- No existen elementos centrales de los que dependa toda la red, cuyo fallo dejaría in-operativas a todas las estaciones.

2.2.4 DESVENTAJAS DE LA TOPOLOGÍA DE BUS.

- Toda la red se caería si hubiera una ruptura en el cable principal.
- Se requiere terminadores. [2]

[2]http://www2.canalaudiovisual.com/ezine/books/acREDES/2redes05.htm

- No se debe utilizar como única solución en un gran edificio.

2.3 DISEÑO DE UNA RED PROTOTIPO

2.3.1 CONSTRUCCIÓN DE REDES EXITOSAS

Existen actividades a las que mucha gente llama más un arte que una ciencia, y aunque es una expresión un poco trillada, resulta bastante apropiada cuando se trata de diseñar una red. Quizá no sea una disciplina artística, sino una sabiduría casi instintiva que permite comprender la manera en que se mueve el tráfico en una red.

Casi todos los grandes fabricantes en el campo de redes, como Microsoft, Novell y Cisco, tienen algún tipo de programa de certificación para diseño de redes.

Generalmente, suelen durar alrededor de una semana y son ampliamente recomendables para quienes comienzan a familiarizarse en este campo. Sin embargo, las horas de práctica ayudan a desarrollar un instinto para redes.

El proceso de diseño de una red está dividido en cuatro etapas:

1. Determinar las necesidades

2. Diseñar la estructura de red (en papel)

3. Realizar pruebas o elaborar un prototipo de la red

4. Instalar la red, paso por paso. Realizar el primer paso y evaluarlo; realizar el segundo paso y evaluarlo, y así sucesivamente

Estos pasos son casi obvios cuando se reflexiona sobre ellos. Por desgracia, en el mundo real la gran mayoría de las redes se diseñan en el orden inverso. Primero se instala la red, después se estudia el diseño. Y finalmente se intenta definir qué hace falta para que la red funcione bien.

Determinar las necesidades puede ser el paso más difícil. Reemplazar una red ya existente puede ser mucho más sencillo. Si no se cuenta con una red que pueda servir como base, lo que se debe saber es qué necesita la compañía que haga la

red con exactitud. Seguramente habrá políticas de la empresa y discusiones territoriales. Aprender a convivir con ellas es normal.

Aunque no se pueda preguntar directamente, es necesario determinar las expectativas de los usuarios. Se determinará quiénes son los usuarios y cual requiere más recursos. Se debe tomar en cuenta que muchos usuarios que solicitan recursos y conexiones de alta velocidad, con frecuencia no los necesitan en realidad. Por lo general, los usuarios que podrían obtener los beneficios de una conexión dedicada con gran ancho de banda ni siquiera están conscientes de ello.

Una vez que se cuenta con la lista de aplicaciones de redes que soportará la red, es momento de averiguar el ancho de banda requerido para cada aplicación. Se establecerá contacto con el fabricante o con los programadores que hayan desarrollado las aplicaciones, para saber cuál es el ancho de banda de red necesario para un número determinado de usuarios. Esta información servirá como punto de referencia.

Asumir que los servicios centrales de redes requieren una conexión con gran ancho de banda, es un error común. Por ejemplo, DHCP (Dynamic Host Configuration Protocol) y DNS (Domain Name Services) son absolutamente esenciales para una red basada en TCP/IP; por lo general, una red no funcionará sin ellos. Pero éstas son en realidad aplicaciones de bajo ancho de banda, así que las consideraciones de diseño para ellas deben estar basadas principalmente en la confiabilidad y en la tolerancia a fallas que en el ancho de banda de la red.

Partiendo del caso de una red de gran eficiencia, asumiremos algún tipo de arquitectura con switches para la estructura de la red. Se determinará el ancho de banda necesario para soportar cada aplicación y para trabajar adecuadamente con el servidor. Para aplicaciones de uso extremo, se podrán utilizar tarjetas 100BASE-T o incluso gigabit ethernet.

Si se requiere más de 100-Mbps, pero sin llegar a velocidades de gigabit, se considerará conectar dos tarjetas juntas para equilibrar las cargas de trabajo. La mayoría de los sistemas operativos y switches actuales ya lo soportan.

Por lo general, el mejor lugar para conectarse a un servidor es en la estructura principal o main backbone, lo cual, por lo general le da a un servidor la mejor visibilidad posible. Pero si se sabe que la gran parte del tráfico será local, a un grupo específico de usuarios, se tomará en cuenta la posibilidad de colocar el servidor cerca del grupo al cual da servicio (por supuesto, nos referimos a una cercanía electrónica; no es necesario colocar el servidor físicamente en esa área). El lugar donde esté colocado el servidor tendrá una influencia decisiva sobre su eficiencia. Mientras menos puntos de procesamiento deban atravesar un paquete, más rápido llegará a su destino. Los servidores no especializados deberán estar localizados en un lugar central con respecto al backbone. Los servidores diseñados para dar servicio a un grupo pequeño de usuarios, tales como al departamento de contabilidad, se localizan mejor en el mismo segmento de la red que los usuarios.

En este punto será necesario establecer el esquema y las políticas para nombres y direcciones, además de ser el mejor momento para documentar todas las políticas de red, tales como contraseñas y otras cuestiones de seguridad. Muchas personas dejan la documentación hasta el último momento, pero si se deja para el final, por lo general nunca sale bien, ni a tiempo.

2.3.1.1 Gigabit Ethernet

Los estándares para Ethernet de 1000-Mbps o Gigabit Ethernet representan la transmisión a través de medios ópticos y de cobre. El estándar para 1000BASE-X, IEEE 802.3z, especifica una conexión full duplex de 1 Gbps en fibra óptica. El estándar para 1000BASE-T, IEEE 802.3ab, especifica el uso de cable de cobre balanceado de Categoría 5, o mejor.

Las 1000BASE-TX, 1000BASE-SX y 1000BASE-LX utilizan los mismos parámetros de temporización. Utilizan un tiempo de bit de 1 nanosegundo (0,000000001 segundos) o 1 mil millonésima parte de un segundo. La trama de Gigabit Ethernet presenta el mismo formato que se utiliza en Ethernet de 10 y 100-Mbps. Según su implementación, Gigabit Ethernet puede hacer uso de distintos procesos para convertir las tramas a bits en el cable.

2.3.2 ELABORACIÓN DE UNA RED PROTOTIPO

Ya se ha hablado sobre la dificultad de obtener los requerimientos precisos para aplicaciones de redes. Al elaborar primero un prototipo, antes de la instalación, es posible verificar las necesidades reales de los servidores de aplicaciones y evitar problemas posteriores. Las instalaciones de redes por lo general se hacen contra reloj y con muy poco tiempo de sobra, por lo que resulta difícil evaluar todas las aplicaciones de manera adecuada.

Sin embargo, la experiencia nos enseña que el tiempo que se invierte evaluando una aplicación antes de instalarla por completo ahorra tiempo a largo plazo.

Durante la evaluación del prototipo, es conveniente utilizar un analizador de paquetes que pueda reportar el uso del ancho de banda y los errores, así como decodificar paquetes. Este es el mejor momento para ajustar el diseño de red que se obtuvo en la segunda etapa. En base a nuestra experiencia, es casi siempre necesario trabajar varias veces sobre el diseño de la red.

2.3.3 LA INSTALACIÓN PASO POR PASO

En el momento de la instalación de la red, se notará que enfatizamos el hecho de hacerlo paso por paso, deteniéndonos en cada punto para evaluar y verificar cada pieza de la red conforme se vaya instalando. Esto es porque resulta mucho más sencillo resolver problemas de la red cuando sólo existen un par de dispositivos, que podrían ser la causa del problema.

Con frecuencia se realizan instalaciones de toda la red y se trata de hacerla funcionar, toda a la vez. Esa no es una buena idea, siempre habrá problemas con cualquier red nueva. Sin embargo, al instalar y probar pieza por pieza, mientras se verifica el proceso de instalación paso por paso, se simplifica la solución de los problemas.

Se conservará la documentación actualizada y a la mano a lo largo de todo el proceso. Incluso cosas aparentemente triviales como numerar las plaquetas de pared en cada oficina, puede resultar invaluable cuando surjan problemas más adelante. Siempre será mejor que sobre documentación y no que falte.

2.4 FUNCIONAMIENTO DE LA RED

Las redes de ordenadores funcionan con una serie de componentes de uso común y que en mayor o menor medida aparece siempre en cualquier instalación.

2.4.1 SERVIDORES

Los servidores de ficheros conforman el corazón de la mayoría de las redes. Se trata de ordenadores con mucha memoria RAM, un enorme disco duro o varios y una rápida tarjeta de red. El sistema operativo de red se ejecuta sobre estos servidores así como las aplicaciones compartidas.

Fig. 8 - Servidor

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

Un servidor de impresión se encargará de controlar el trafico de red ya que este es el que accede a las demandas de las estaciones de trabajo y el que les proporcione los servicios que pidan las impresoras, ficheros, Internet, etc. Es preciso contar con un ordenador con capacidad de guardar información de forma muy rápida y de compartirla con la misma rapidez.

2.4.2 ESTACIONES DE TRABAJO

Son los ordenadores conectados al servidor. Las estaciones de trabajo no han de ser tan potentes como el servidor, simplemente necesita una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor.

Fig. 9 - Estación de Trabajo

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

Una estación de trabajo puede carecer de disquetera y de disco duro y trabajar directamente sobre el servidor. Prácticamente cualquier ordenador puede actuar como estación de trabajo.

2.4.3 TARJETA DE RED.

La tarjeta de red o NIC es la que conecta físicamente el ordenador a la red. Las tarjetas de red más populares son por supuesto las tarjetas Ethernet, existen también conectores Local Talk así como tarjetas token ring, tarjeta Ethernet con conectores RJ-45.

Fig. 10 - Tarjeta de Red

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

Los conectores LocalTalk se utilizan para ordenadores mac, conectándose al puerto paralelo. En comparación con Ethernet la velocidad es muy baja, de 230KB frente a los 10 o 100 MB de la primera.

Las tarjetas de Token Ring, son similares a las tarjetas Ethernet aunque el conector es diferente, por lo general es un DIM de nueve pines.

2.4.4 PUENTES O BRIDGES

Fig. 11 - Puente o Bridge

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

Los Bridges se utilizan para segmentar redes grandes en redes más pequeñas, destinadas a otra red pequeña diferente mientras que todo el tráfico interno seguirá en la misma red. Con esto se logra reducir el tráfico de la red.

2.4.5 EL MEDIO

Constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, par de cable, cable par trenzado (UTP) y la fibra óptica (cada vez en más uso esta última).

2.4.6 CONCENTRADORES DE CABLEADO

Una LAN en bus usa solamente tarjetas de red en las estaciones y cableado UTP para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.
Existen dos tipos de concentradores de cableado:

2.4.6.1 Concentradores Pasivos

Actúan como un simple concentrador cuya función principal consiste en interconectar toda la red.

2.4.6.2 Concentradores Activos

Además de su función básica de concentrador también amplifican y regeneran las señales recibidas antes de ser enviadas. Los concentradores pueden ser de capa 2 de acuerdo al modelo de referencia OSI (switch, bridges, etc.), o de capa 3 (switch, router).

Los concentradores de cableado tienen dos tipos de conexiones: para las estaciones y para unirse a otros concentradores y así aumentar el tamaño de la red. Los concentradores de cableado se clasifican dependiendo de la manera en que internamente realizan las conexiones y distribuyen los mensajes. A esta característica se le llama topología lógica.

2.4.7 DETERMINAR EL FUNCIONAMIENTO DE UNA RED

Esto incluye los procesos y procedimientos relacionados con el diagnóstico de fallas de hardware, software y sistemas de red de un computador

- Definir el problema
- Verificar factores de error
- Considerar las posibilidades
- Crear un plan de acción
- Implementar el plan
- Observar los resultados
- Documentar los resultados
- Revisar que todo funcione correctamente

2.4.8 PROBAR LA CONECTIVIDAD CON PING

Ping es un programa básico que verifica que una dirección IP particular existe y puede aceptar solicitudes. El acrónimo computacional ping es la sigla para Packet Internet or Inter-Network Groper. El nombre se ajustó para coincidir el término usado en la jerga de submarinos para el sonido de un pulso de sonar que retorna desde un objeto sumergido.

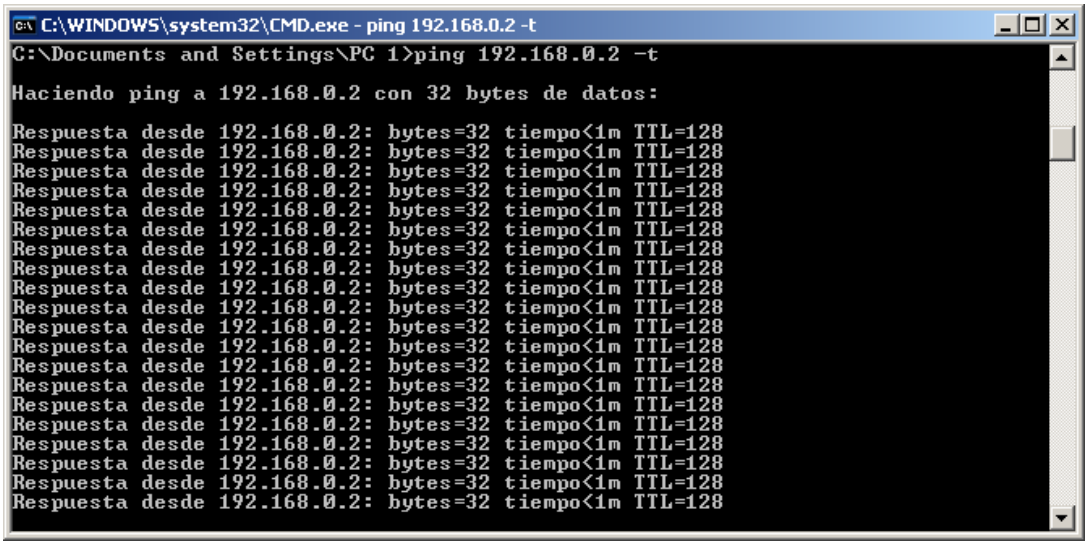


Fig. 12 - Conectividad con Ping

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

El comando **ping** funciona enviando paquetes IP especiales, llamados datagramas de petición de eco ICMP (Internet Control Message Protocol/Protocolo de mensajes de control de Internet) a un destino específico. Cada paquete que se envía es una petición de respuesta. La pantalla de respuesta de un ping contiene la proporción de éxito y el tiempo de ida y vuelta del envío hasta llegar a su destino. A partir de esta información, es posible determinar si existe conectividad a un destino. El comando **ping** se utiliza para probar la función de transmisión/recepción de la NIC, la configuración TCP/IP y la conectividad de red.

2.5 MODELO OSI, MODELO TCP/IP

La siguiente es una comparación de los modelos OSI y TCP/IP comparando sus similitudes y diferencias:

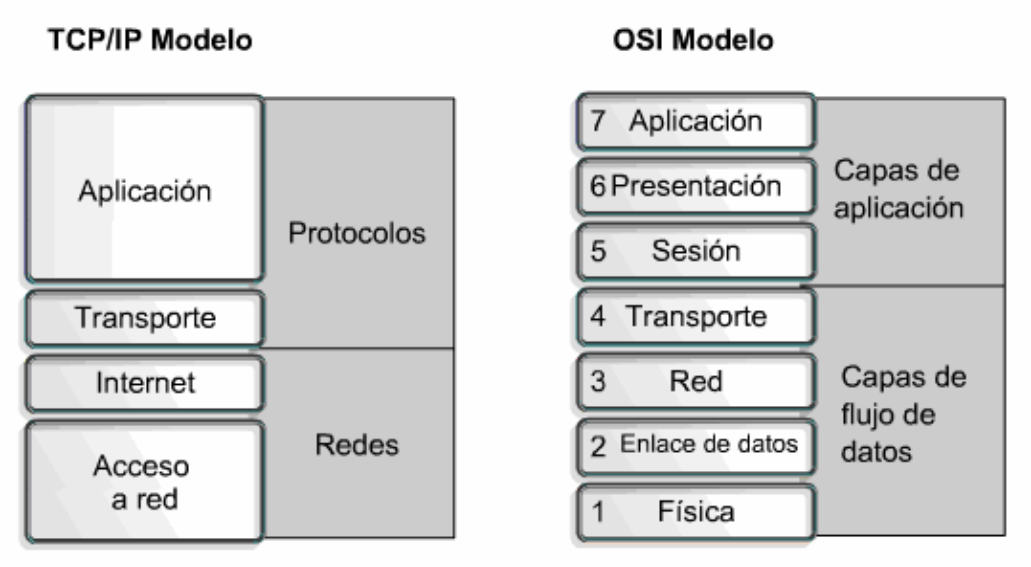


Fig. 13 - Modelo OSI – TCP/IP

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

Similitudes entre los modelos OSI y TCP/IP:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación por paquetes y no de conmutación por circuito.
- Los profesionales de networking deben conocer ambos modelos.

Diferencias entre los modelos OSI y TCP/IP:

- TCP/IP combina las capas de presentación y de sesión en una capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas

- La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.

La Internet se desarrolla de acuerdo con los estándares de los protocolos TCP/IP. El modelo TCP/IP gana credibilidad gracias a sus protocolos. A diferencia, en general, las redes no se construyen a base del protocolo OSI. El modelo OSI se utiliza como guía para comprender el proceso de comunicación.

2.6 DOMINIO DE COLISION

2.6.1 DETECCION DE COLISION

Los dispositivos de red detectan que se ha producido una colisión cuando aumenta la amplitud de la señal en los medios de networking.

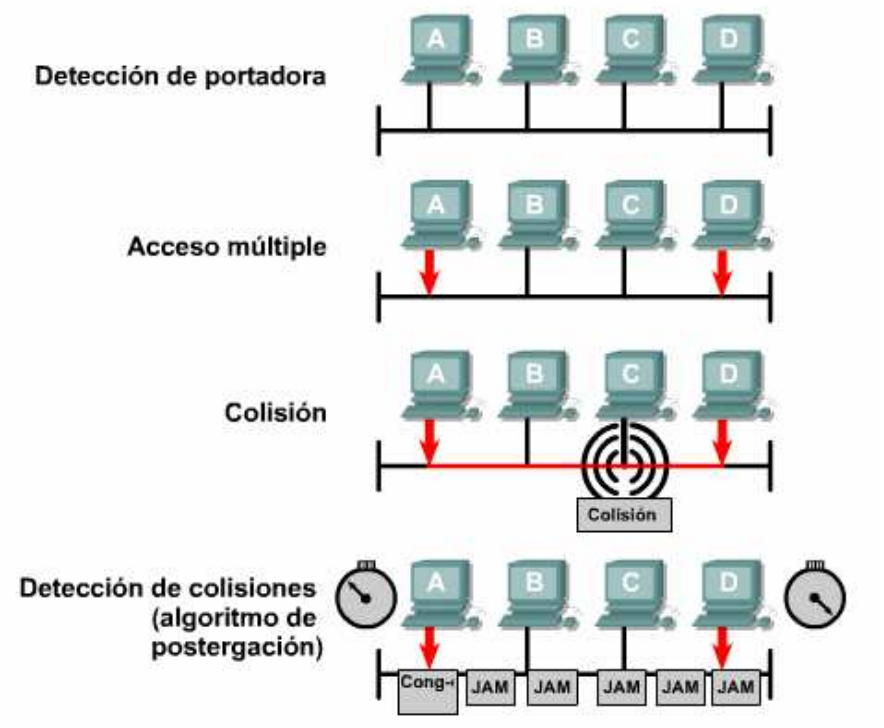


Fig. 14 - Detección de Colisión

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

Cuando se produce una colisión, cada nodo que se encuentra en transmisión continúa transmitiendo por poco tiempo a fin de asegurar que todos los dispositivos detecten la colisión. Una vez que todos los dispositivos la han

detectado, se invoca el **algoritmo de postergación** y la transmisión se interrumpe. Los nodos interrumpen la transmisión por un período determinado al azar, que es diferente para cada dispositivo (CSMA/CD).

Cuando caduca el período de retardo cada nodo puede intentar ganar acceso al medio de red. Los dispositivos involucrados en la colisión no tienen prioridad para transmitir datos.

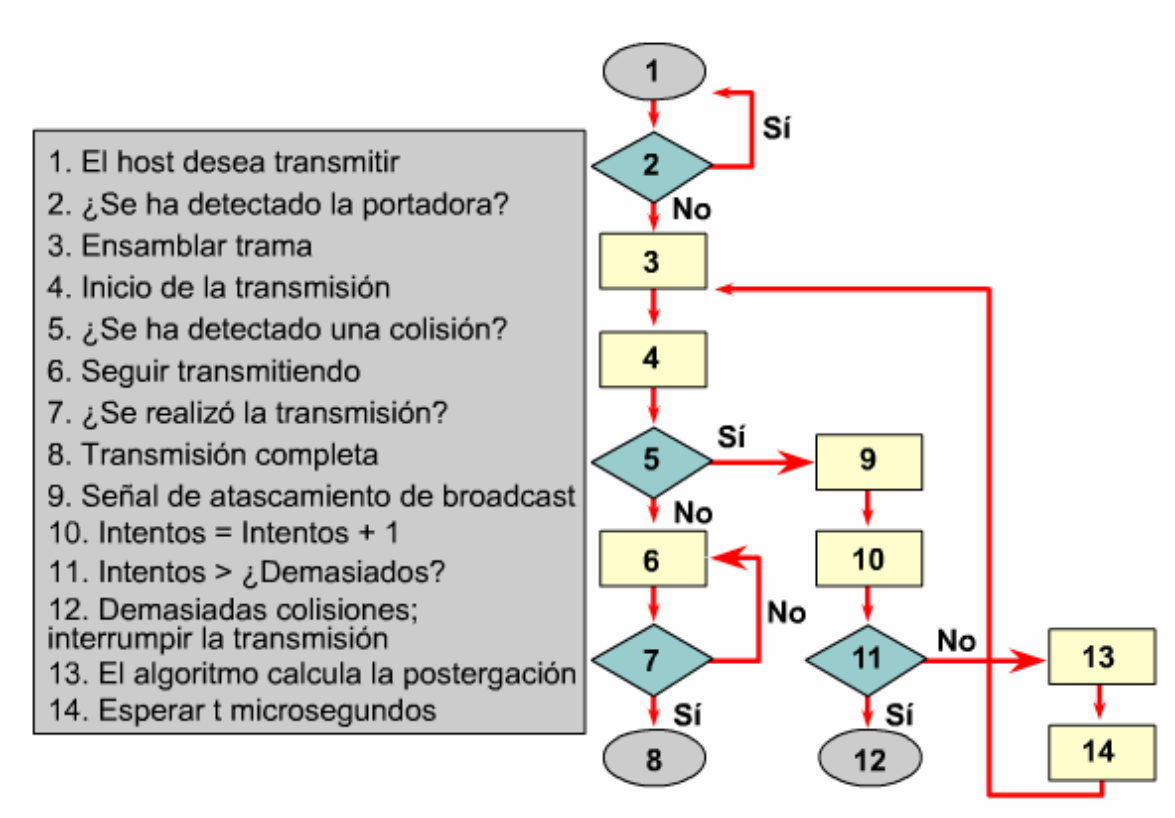


Fig. 15 - Algoritmo de Postergacion

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=ynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

2.6.2 COLISIÓN

Uno de los problemas que se puede producir, cuando dos bits se propagan al mismo tiempo en la misma red, es una colisión (Ver Fig. 17). En una red pequeña y de baja velocidad es posible implementar un sistema que permita que sólo dos computadores envíen mensajes, cada uno por turnos. Esto significa que ambas

pueden mandar mensajes, pero sólo podría haber un bit en el sistema. El problema es que en las grandes redes hay muchos computadores conectados, cada uno de los cuales desea comunicar miles de millones de bits por segundo. Recordar que los "bits" en realidad son paquetes que contienen información, datos, etc. Se pueden producir problemas graves como resultado del exceso de tráfico en la red.

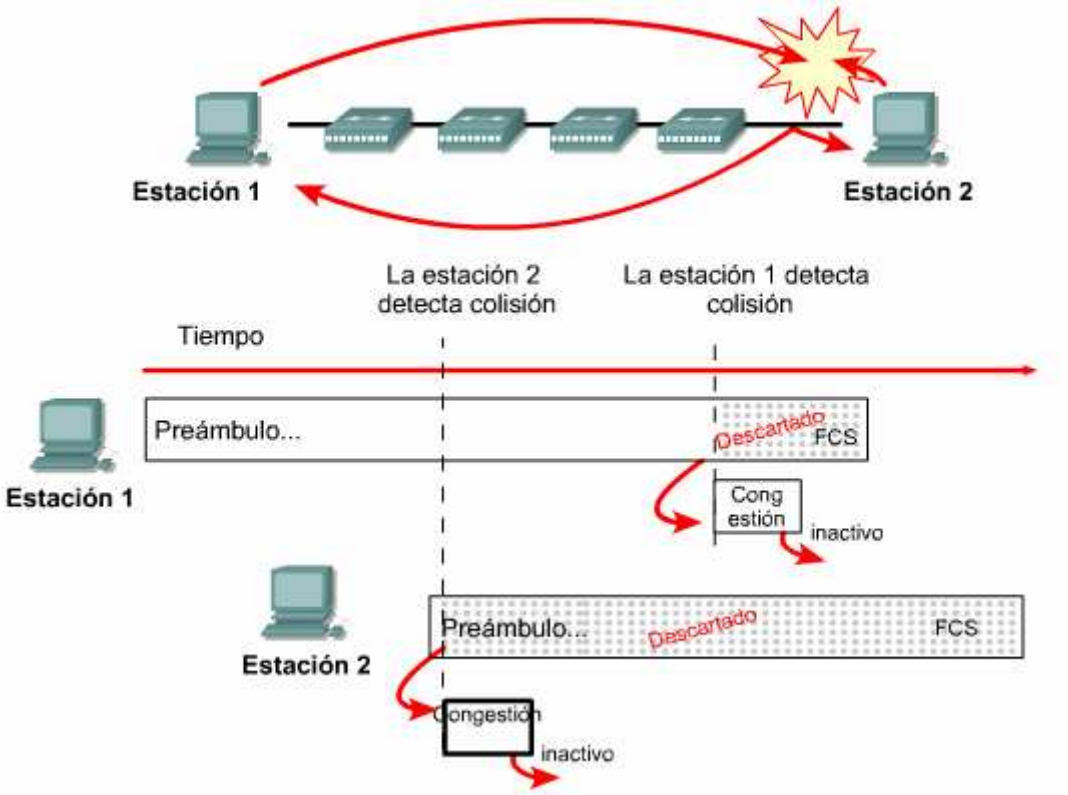


Fig. 16 - COLISIONES

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

El **preámbulo** indicado en la Fig. 17 en un patrón de unos y ceros que indica a las estaciones receptoras que una trama es Ethernet o IEEE 802.3.

El **FCS** (Secuencia de verificación de trama) de la Fig. 17 contiene un valor de verificación CRC (Control de Redundancia Cíclica) de 4 bytes, creado por el

dispositivo emisor y recalculado por el dispositivo receptor para verificar la existencia de tramas dañadas.

Cuando un paquete es recibido por el destinatario adecuado, les retira la cabecera de ethernet y el checksum de verificación de la trama, comprueba que los datos correspondan a un mensaje IP y entonces lo pasa a dicho protocolo para que lo procese.

Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes como, por ejemplo, los repetidores, puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo. Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos (Ver Fig. 17).

El área dentro de la red donde los paquetes se originan y colisionan, se denomina dominio de colisión, e incluye todos los entornos de medios compartidos.

Por ejemplo, un cable puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs. Todas estas interconexiones de la Capa 1 forman parte del dominio de colisión.

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

Al igual que lo que ocurre con dos automóviles, que no pueden ocupar el mismo espacio, o la misma carretera, al mismo tiempo, tampoco es posible que dos señales ocupen el mismo medio simultáneamente.

En general, se cree que las colisiones son malas ya que degradan el desempeño de la red. Sin embargo, una cantidad determinada de colisiones es una función natural de un entorno de medios compartidos (es decir, un dominio de colisión) ya

que una gran cantidad de computadores intentan comunicarse entre sí simultáneamente, usando el mismo cable.

Los repetidores regeneran y retemporizan los bits, pero no pueden filtrar el flujo de tráfico que pasa por ellos. Los datos (bits) que llegan a uno de los puertos del repetidor se envían a todos los demás puertos. El uso de repetidor extiende el dominio de colisión, por lo tanto, la red a ambos lados del repetidor es un dominio de colisión de mayor tamaño.

Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de networking que pueden dividir los dominios. Los puentes, switches y routers son ejemplos de este tipo de dispositivo de networking. Este proceso se denomina **segmentación de dominio de colisión**.

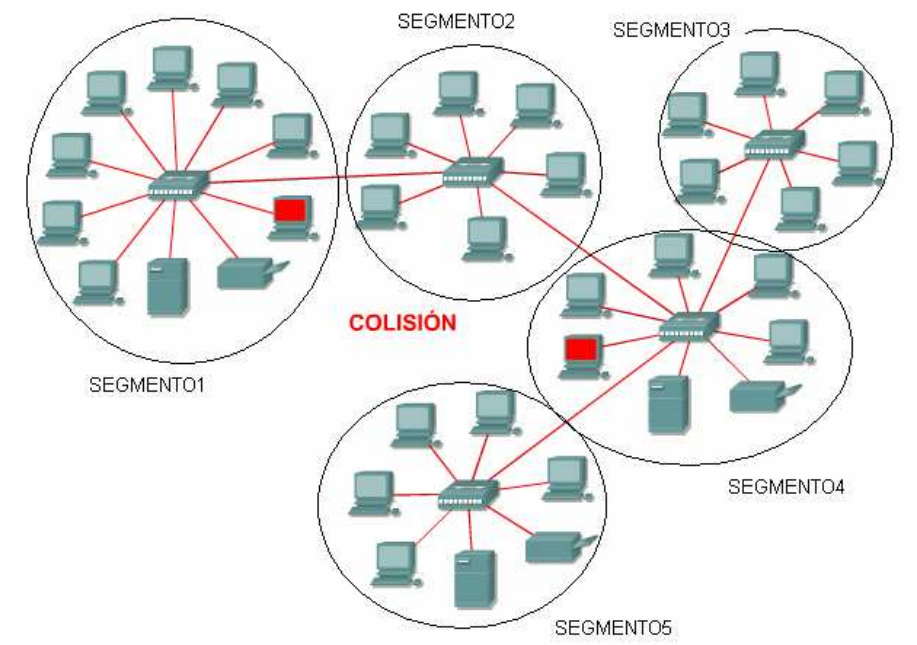


Fig. 17 - Dominios de Colisión

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=114961587167363,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación. El tráfico entre dispositivos en el mismo segmento no atraviesa el puente, y afecta otros segmentos. Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación.

La mejor solución para este problema es la utilización de switches para la correcta segmentación de una LAN. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los ordenadores conectados a ese segmento pero no a los ordenadores pertenecientes a otros dominios de colisión.

Todas las ramas de un hub forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del hub). Cada rama de un switch constituye un dominio de colisiones distinto (las colisiones no se retransmiten por los puertos del switch).

Este es el motivo por el cual la utilización de conmutadores reduce el número de colisiones y mejora la eficiencia de las redes. El ancho de banda disponible se reparte entre todos los ordenadores conectados a un mismo dominio de colisión.

Podemos indicar un número aproximado de 25-30 como medida máxima de ordenadores que se pueden conectar dentro de un mismo dominio de colisión. Sin embargo, este número dependerá en gran medida del tráfico de la red. En redes con mucho tráfico se debe tratar de reducir el número de ordenadores por dominio de colisión lo más posible mediante la creación de distintos dominios de colisión conectados por switches o mediante la creación de distintas subredes conectadas por routers. [21]

La tasa de colisión mide el porcentaje de paquetes que provocan colisiones. Algunas colisiones son inevitables, algo menos del 10% es frecuente en redes funcionando adecuadamente.

[21]http://www.saulo.net/pub/redes/a.html

Los Factores que Afectan a la Eficacia de la Red
▼Cantidad de tráfico
▼Número de nodos
▼Tamaño de los paquetes
▼Diámetro de la red

Tabla 2 - Factores que afectan la eficiencia de la red

Fuente: http://www.consulintel.es/html/Tutoriales/Lantronix/guia_et_p4.html

Midiendo la Eficacia de la Red
▼Promedio de picos de desvío de carga
▼Tasa de colisión
▼Tasa de utilización

Tabla 3 - Eficiencia De la Red

Fuente:http://www.consulintel.es/html/Tutoriales/Lantronix/guia_et_p4.html

2.7 DOMINIOS DE BROADCAST

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada estación de la red tenga acceso a los medios.

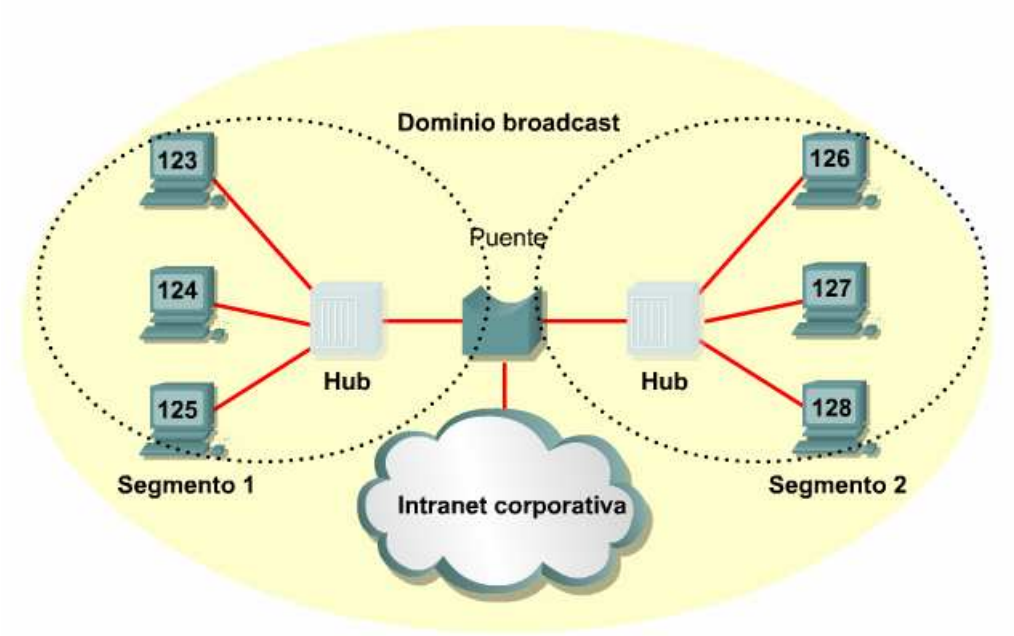


Fig. 18 - Dominios de Broadcast

Fuente: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada estación (host).

Pero los dispositivos de Capa 2 envían broadcast, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcast deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast.

En otras palabras, todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3. Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcast.

Los routers, en realidad, funcionan en las Capas 1, 2 y 3. Ellos, al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios. Ellos tienen un encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier otro dispositivo de Capa 2. Es la Capa 3 la que permite que el router segmente dominios de broadcast.

Para que un paquete sea enviado a través del router, el dispositivo de Capa 2 debe ya haberlo procesado y la información de la trama debe haber sido eliminada. El envío de Capa 3 se basa en la dirección IP destino y no en la dirección MAC. Para que un paquete pueda enviarse, debe contener una dirección IP que esté por afuera del alcance de las direcciones asignadas a la LAN, y el router debe tener un destino al cual enviar el paquete específico en su tabla de enrutamiento.

2.7.1 ROUTER

Un ruteador es un dispositivo de *propósito general* diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN.

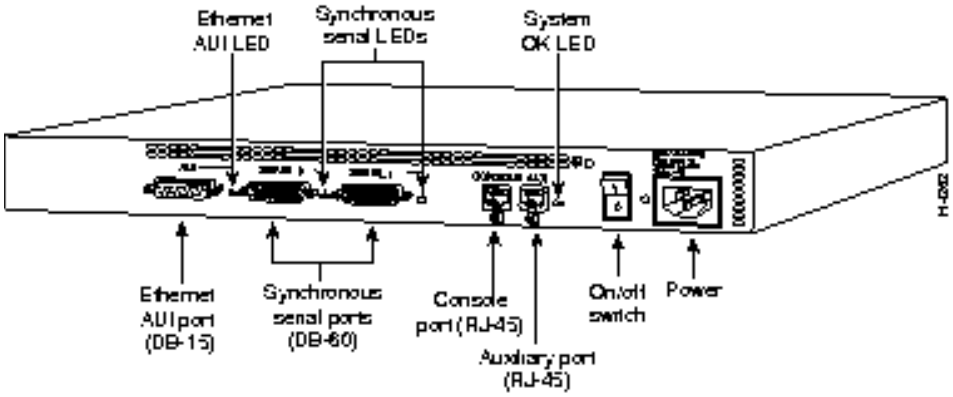


Fig. 19 - Router Modelo 2501

Fuente:http://www.cisco.com/en/US/products/hw/routers/ps233/products_installation_and_configuration_guide_chapter09186a008007c826.html

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch.

Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet.

Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes.

El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envió basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.
2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino.

Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retrazo y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames (tramas) por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

2.7.2 INTRODUCCIÓN AL FLUJO DE DATOS

El flujo de datos en un contexto de dominios de colisión y de broadcast se centra en la forma en que las tramas se propagan a través de la red. Se refiere al movimiento de datos a través de los dispositivos de Capa 1, 2 y 3 y a la manera en que los datos deben encapsularse para poder realizar esa travesía en forma efectiva. Recuerde que los datos se encapsulan en la capa de la red con una dirección de origen y destino IP, y en la capa de enlace de datos con una dirección MAC origen y destino. Una buena regla a seguir es que un dispositivo de Capa 1 (hub, conexiones, etc.) siempre envíe la trama, mientras que un dispositivo de Capa 2 (Switch, puentes) desee enviar la trama. En otras palabras, un dispositivo de Capa 2 siempre enviará la trama a menos que algo se lo impida.

Un dispositivo de Capa 3 (router, switch de capa 3) no enviará la trama a menos que se vea obligado a hacerlo. Usar esta regla ayudará a identificar la forma en que los datos fluyen a través de la red.

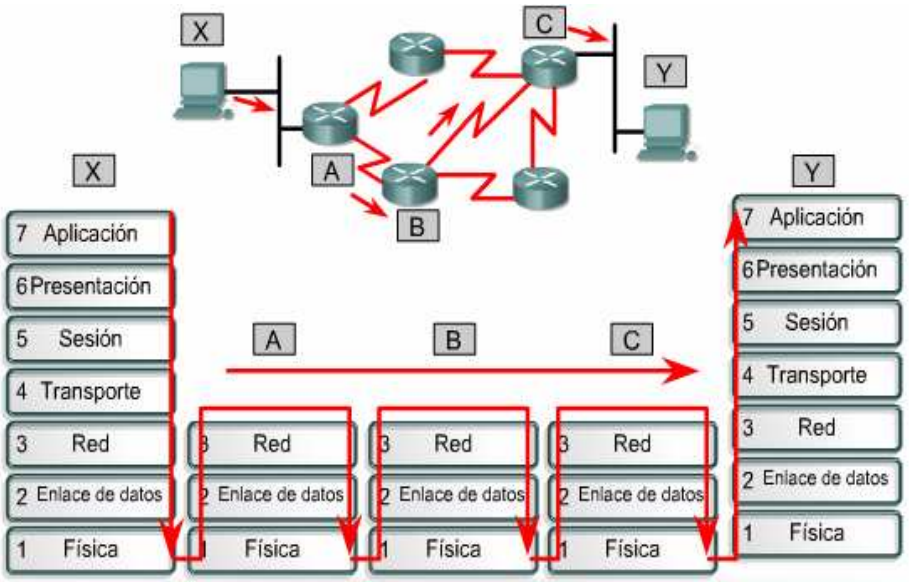


Fig. 20 - Flujo de Datos

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

Los dispositivos de Capa 1 no funcionan como filtros, entonces todo lo que reciben se transmite al segmento siguiente. La trama simplemente se regenera y retemporiza y así vuelve a su calidad de transmisión original. Cualquier segmento conectado por dispositivos de Capa 1 forma parte del mismo dominio, tanto de colisión como de broadcast. Los dispositivos de Capa 2 filtran tramas de datos basados en la dirección MAC destino.

La trama se envía si se dirige a un destino desconocido fuera del dominio de colisión. La trama también será enviada si se trata de un broadcast, multicast o unicast que se dirige fuera del dominio local de colisión.

La única vez en que la trama no se envía es cuando el dispositivo de Capa 2 encuentra que la estación (host) emisor y el receptor se encuentran en el mismo dominio de colisión. Un dispositivo de Capa 2, tal como un puente, crea varios dominios de colisión pero mantiene sólo un dominio de colisión.

Los dispositivos de Capa 3 filtran paquetes basados en la dirección IP destino. La única forma en que un paquete se enviará es si su dirección IP destino se encuentra fuera del dominio broadcast y si el router tiene una ubicación identificada para enviar el paquete. Un dispositivo de Capa 3 crea varios dominios de colisión y broadcast.

El flujo de datos en una red enrutada basada en IP, implica el movimiento de datos a través de dispositivos de administración de tráfico en las Capas 1, 2 y 3 del modelo OSI. La Capa 1 (hub) se utiliza en la transmisión por medios físicos, la Capa2 (switch. puente) para la administración de dominios de colisión, y la Capa 3 (router, switch de capa 3) para la administración de dominios de broadcast.

2.7.3 TRANSMIISION DE BROADCAST EN REDES ETHERNET

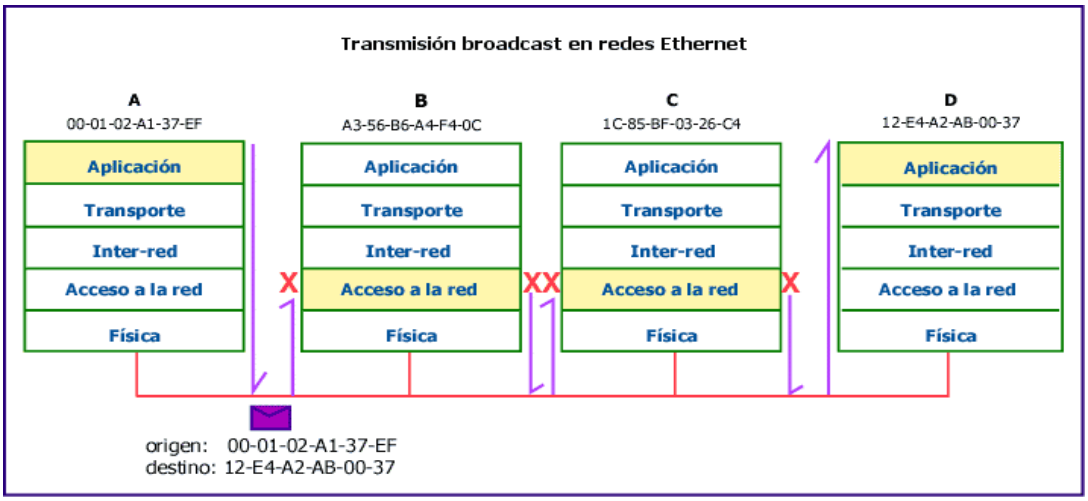


Fig. 21 Transmisión Broadcast

Fuente: http://www.htmlweb.net/redes/topologia/topologia_3.html

2.8 DEFINICION Y CARACTERISTICAS DE UN SWITCH DE CAPA 2

2.8.1 DEFINICIÓN

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a embotellamientos y anchos de banda pequeños.

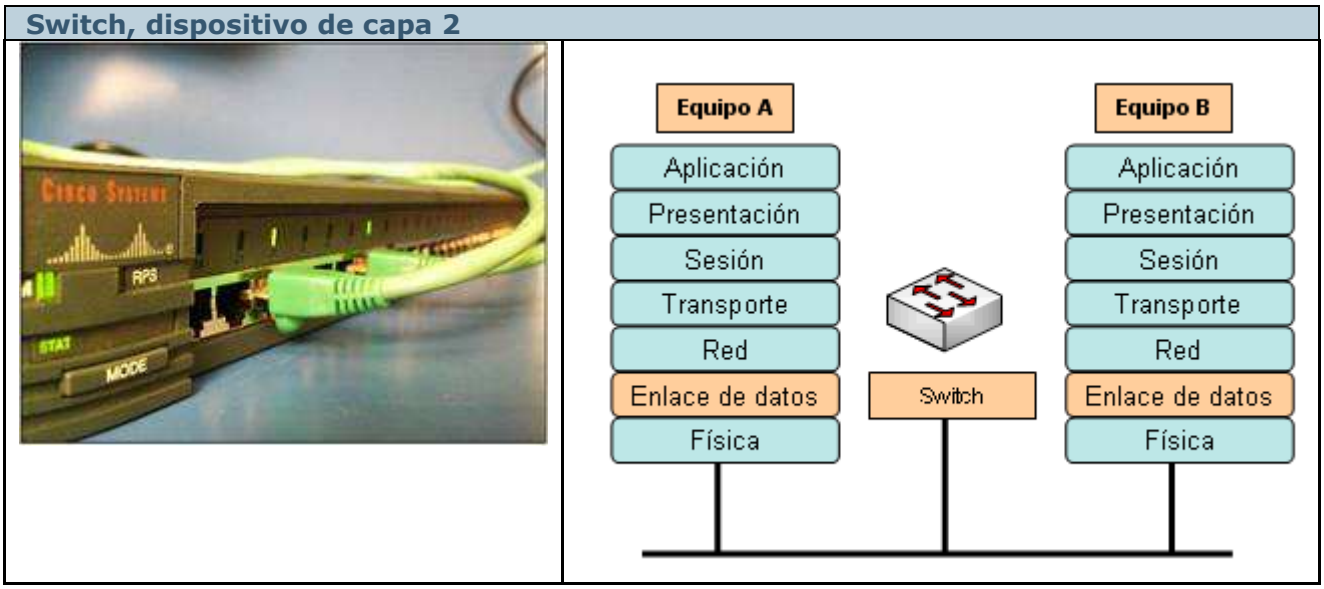


Fig. 22 – Switch de Capa 2

Fuente: http://www.adrformacion.com/cursos/wserver/leccion1/tutorial6.html

El switch puede agregar mayor ancho de banda debido a la segmentación de dominios de colisión que realiza, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

Opera en la capa 2 y actualmente existen switch de Capa 3, del modelo OSI y reenvía los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

2.8.2 DONDE USAR SWITCH DE CAPA 2

Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre cliente/servidor, pues los usuarios juzgan la red por la rapidez de obtener un prompt y la confiabilidad del servicio.
Hay diversos factores que involucran el incremento de ancho de banda en una LAN:

- ✓ El elevado incremento de nodos en la red.
- ✓ El continuo desarrollo de procesadores más rápidos y poderosos en estaciones de trabajo y servidores.
- ✓ La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones intensivas cliente/servidor.
- ✓ Cultivar la tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.

El tráfico de red es cada vez menos predecible. La antigua regla del 80/20 sostenía que el 80 por ciento del tráfico de la red se limitaba al grupo de trabajo y que sólo un 20 por ciento se dirigía a Internet. Sin embargo, con el uso cada vez mayor de sistemas para la empresa electrónica, la proporción actual se aproxima más al 50/50. Si la tendencia continúa, la relación podría llegar a invertirse al 20/80, lo que supone un aumento significativo del tráfico que atraviesa la red troncal. El aumento del ancho de banda de la red troncal de Internet también incrementa los requisitos que deben satisfacer las redes de los sitios de comercio electrónico.

Los switches resuelven los problemas de anchos de banda al segmentar un dominio de colisiones de una LAN, en pequeños dominios de colisiones.

2.8.3 SEGMENTANDO LANS CON SWITCH

Podemos definir una LAN como un dominio de colisiones, donde el switch está diseñado para segmentar estos dominios en dominios más pequeños. Puede ser ventajoso, pues reduce el número de estaciones a competir por el medio.

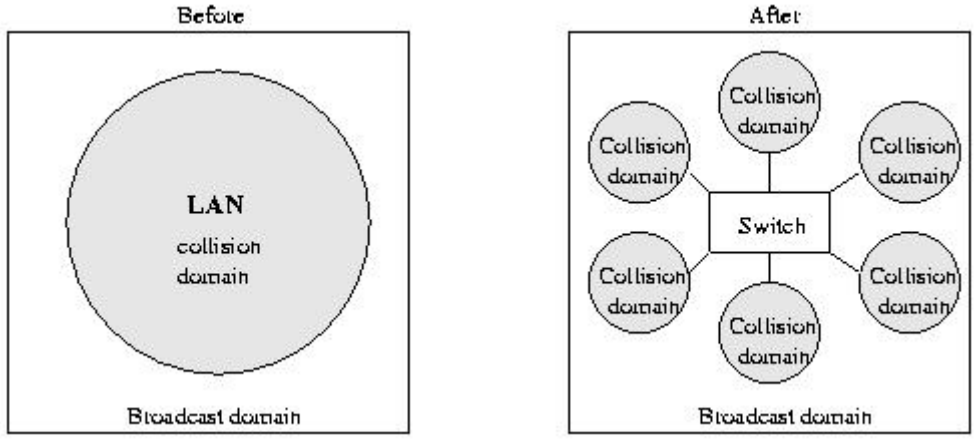


Fig. 23 - Segmentacion

Fuente: http://www.inaoep.mx/~moises/AGC/sw-rout.html#tecsw

Es importante notar que el tráfico originado por el broadcast en un dominio de colisiones, será reenviado a todos los demás dominios, asegurando que todas las estaciones en la red se puedan comunicar entre si.

2.8.4 ¿CÓMO SABE UN SWITCH LOS ORDENADORES QUE TIENE EN CADA RAMA?

Lo averigua de forma automática mediante aprendizaje. Los conmutadores contienen una tabla dinámica de direcciones físicas y números de puerto. Nada más enchufar el switch esta tabla se encuentra vacía. Un procesador analiza las tramas Ethernet entrantes y busca la dirección física de destino en su tabla. Si la encuentra, únicamente reenviará la trama por el puerto indicado.

Si por el contrario no la encuentra, no le quedará más remedio que actuar como un hub y difundirla por todas sus ramas.

Las tramas Ethernet contienen un campo con la dirección física de origen que puede ser utilizado por el switch para agregar una entrada a su tabla basándose en el número de puerto por el que ha recibido la trama. A medida que el tráfico se incrementa en la red, la tabla se va construyendo de forma dinámica. Para evitar que la información quede desactualizada (si se cambia un ordenador de sitio, por ejemplo) las entradas de la tabla desaparecerán cuando agoten su tiempo de vida (TTL), expresado en segundos.

2.8.5 SWITCHING

Esta palabra ha ido tomando distintas connotaciones a medida que se plantean nuevos esquemas para mejorar el rendimiento de las redes de área local (Torrent, 1998). Así, cuando hablamos de switch, podemos estarnos refiriendo a:

Fig. 24 – Switch de Capa 2 (Cisco Catalyst 2948G-GE-TX Switch)

Fuente: http://www.cisco.com/en/US/products/hw/switches/ps606/index.html

Fig. 25 – Switch de Capa 3 (Cisco Catalyst 2926G)

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

Fig. 26 – Switch de Capa 4 (Cisco Catalyst Blade Switch 3030)

Fuente: http://www.cisco.com/en/US/products/ps6764/index.html

2.8.5.1 Switch Capa 2

Este es el tipo de switch de red de área local (LAN) más básico, el cual opera en la capa 2 del modelo OSI. Su antecesor es el bridge, por ello, muchas veces al switch se le refiere como un bridge multipuerto, pero con un costo más bajo, con mayor rendimiento y mayor densidad por puerto.

El switch capa 2 hace sus decisiones de envío de datos en base a la dirección MAC destino contenida en cada frame (trama). Estos, al igual que los bridges, segmentan la red en dominios de colisión (Ver Fig25), proporcionando un mayor ancho de banda por cada estación.

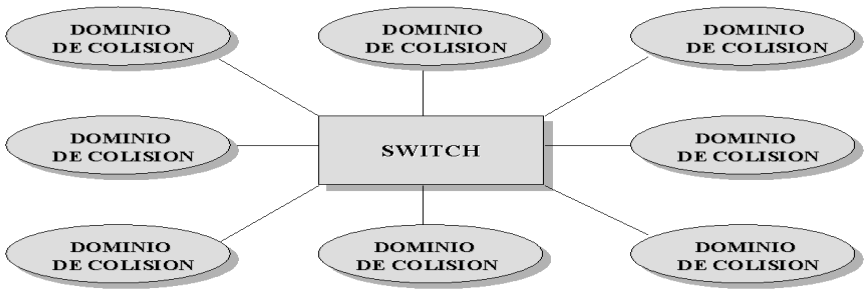


Fig. 27 - Dominios de colisión

Fuente: http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm

La configuración de los switches capa 2 y el soporte de múltiples protocolos es totalmente transparente a las estaciones terminales. Como igual es el soporte de las redes virtuales (VLAN´s), las cuales son una forma de segmentación que permite crear dominios de broadcast formando así grupos de trabajo independientes de la ubicación física.

El uso de procesadores especializados (ASIC: Application Specific Integrated Circuit) incrementaron la velocidad de conmutación de los switches, en comparación con los bridges, porque pueden enviar los datos a todos los puertos de forma casi simultánea.
Estos switches siguen, principalmente, dos esquemas de conmutación para envío de tráfico, los cuales son:

2.8.5.1.1 Cut-Trough

Comienzan el proceso de envío antes de que el frame sea completamente recibido. En estos switches la latencia es baja porque sólo basta con leer la dirección MAC destino para comenzar a transferir el frame. La desventaja de este esquema, es que los frames corruptos (corruptos, enanos, con errores, etc.) son también enviados.

2.7.5.1.2 Store-and-Forward

Lee y valida el paquete completo antes de iniciar el proceso de envío. Esto permite que el switch descarte paquetes corruptos y se puedan definir filtros de tráfico. La desventaja de este esquema es que la latencia se incrementa con el tamaño del paquete.

Algunos switches implementan otros esquemas (Fragment free) o esquemas híbridos en base a rendimiento y porcentaje de errores, pasando en un momento de modo Cut-trough al modo Store-and-forward y, viceversa.

2.8.6 RESUMEN DE CARACTERISTICAS

Router	Switch capa 2	Switch capa 3	Switch capa 4
• Entrega de tráfico en base a protocolo de capa 3. • Selección óptima de ruta. • Control de tráfico. • No pasa *broadcasts*. • Soporte de políticas de seguridad, filtros, administración de ancho de banda. • Mayor latencia y menor rendimiento en comparación con los *switches*.	• Equivalentes a los *bridges multipuertos*. • Baja latencia y alto rendimiento. • En redes muy grandes (*flat networks*), éstas son inundadas de "tormentas" de *broadcasts*, limitaciones de direcciones. • Tipos: *Cut-trough, store-and-forward, fragment-free*, híbridos. • Segmentar la red en dominios de colisión por puerto y dominios de *broadcasts* con la configuración de VLAN. • Entrega de tráfico en base a dirección MAC.	• Combinación de la funcionalidad de los *switches* capa 2 y de las características de los *routers*. • Alto rendimiento. • Tipos: PPL3 y CTL3. • Entrega tráfico basado en direcciones IP (cuando enruta la primera vez) y en direcciones MAC (cuando conmuta). • Por ahora, la mayoría sólo soporta IP (algunos también IPX) haciendo *bridging* de los restantes protocolos.	• Combinación de *switches* capa 3 con utilización de la información del encabezado de capa 4. • Se segmenta por "flujos" de aplicación pudiendo soportar administración de ancho de banda por "flujos" y aplicación de niveles de prioridades.

Fig. 28 - Cuadro Caracteristicas

Fuente: http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm

2.9 DEFINICIÓN Y CARACTERÍSTICAS DE UN ROUTER (CAPA 3)

2.9.1 DEFINICION

Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast, proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN.

Router, dispositivo de capa 3

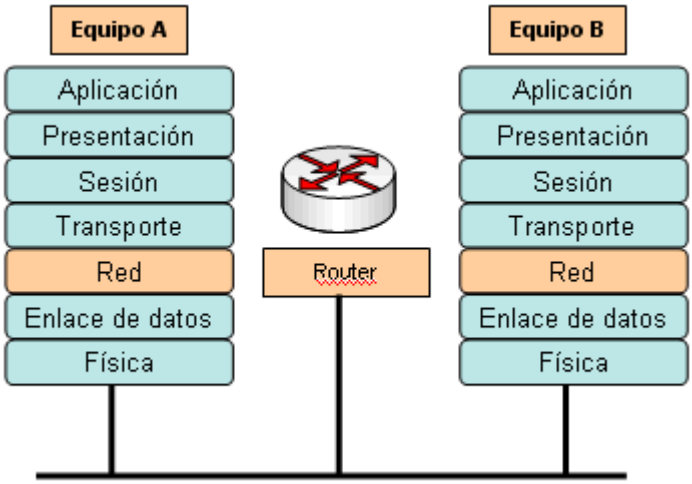


Fig. 29 – Router (Capa 3)

Fuente:http://www.adrformacion.com/cursos/wserver/leccion1/tutorial6.html

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet.

Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes.

El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envió basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.
2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de

transmisión, retrazo y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames (tramas) por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

2.9.2 DONDE USAR UN RUTEADOR

Las funciones primarias de un ruteador son:

- Segmentar la red dentro de dominios individuales de broadcast.
- Suministrar un envió inteligente de paquetes. Y
- Soportar rutas redundantes en la red.

Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los broadcast no pasara a través del ruteador. Otros importantes beneficios del ruteador son:

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs través del uso de Data Link Switching (DLSw).
- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, FastEthernet, Token Ring, FDDI y ATM.

2.9.3 ALGORITMO DE RUTEO

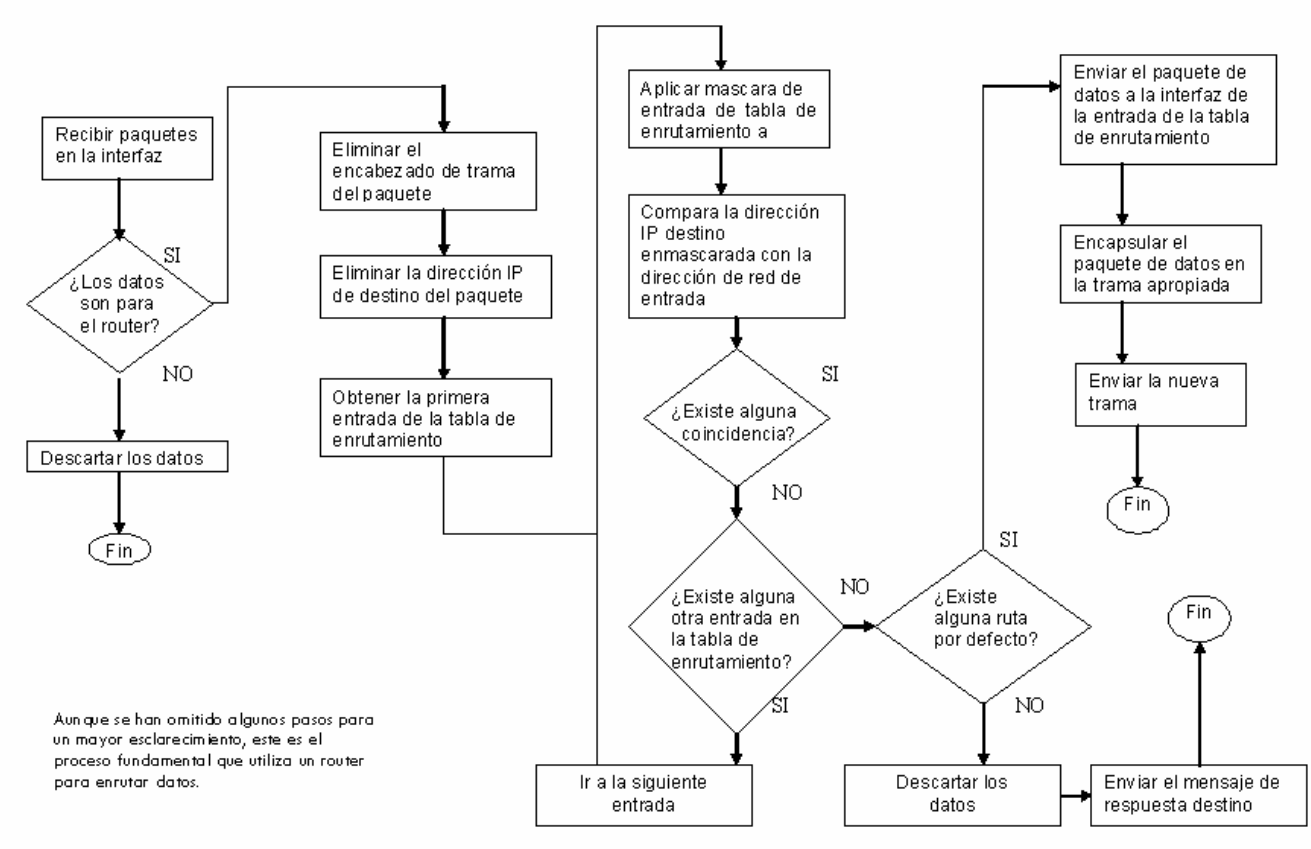


Fig. 30 Algoritmo de Ruteo

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615871673613,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet311072827537671,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/311072827537671/coursetoc.html

2.9.4 INTERFACES DE UN ROUTER

Fig. 31 – Interfaz del Router

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

Las conexiones de los routers a una red se denominan interfaces.

Un router puede disponer de las siguientes interfaces:

- Interfaces serie (serial) _ S0, S1,…

- Interfaces ethernet _ E0, E1,…
- Interfaces fast Ethernet _ F0, F1,…
- Puerto de consola (console)
- Puerto auxiliar (aux)
- Cada interfaz dispone de una dirección IP.

2.9.5 CARACTERISTICAS

- Interconecta redes
- Cada red tiene una dirección
- Cada estación tiene una dirección que permite saber a que red pertenece
- Cada conexión del router a una red se denomina interfaz
- Divide dominios de broadcast
- Filtra los broadcast
- Cada red tiene su propio dominio de broadcast
- Puede disponer de un sistema operativo propio para configurar las interfaces, protocolos de encaminamiento, etc.
- En cada subred, la dirección de la interfaz del router es la puerta de enlace para las estaciones pertenecientes a dicha subred.
- La puerta de enlace (default gateway) permite la comunicación con otras redes

2.10 DEFINICION Y CARACTERISTICAS DEL CACTI

2.10.1 DEFINICION

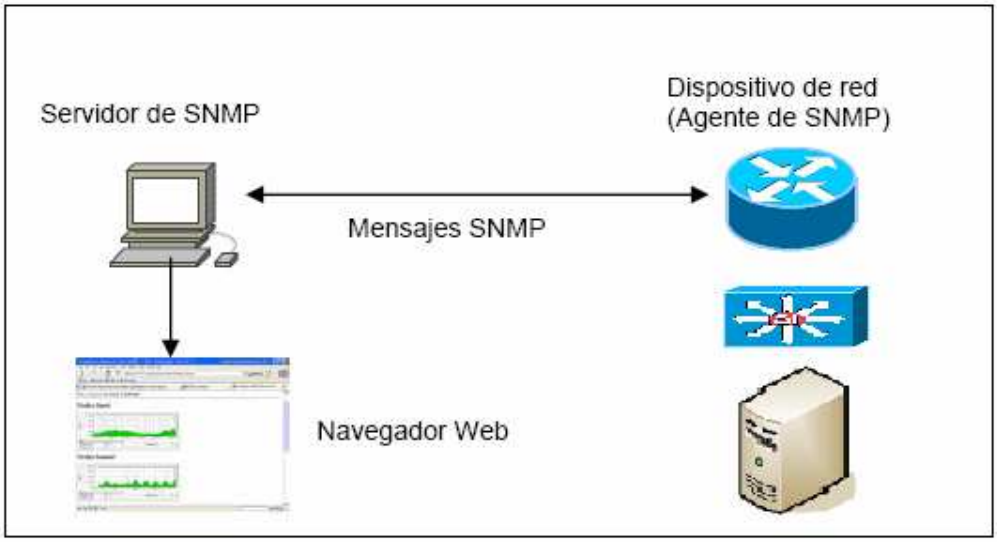


Fig. 35 -Topología de Monitoreo

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

Es una completa solución para el monitoreo de redes. Utiliza RRdtool (herramienta de la base de datos, diseñada para manejar datos en series de tiempo como: ancho de banda, temperatura, carga de la CPU, etc.) para almacenar la información de los dispositivos y aprovechar sus funcionalidades de graficación. Proporciona un esquema rápido de obtención de datos remotos, múltiples métodos de obtención de datos (SNMP, scripts), un manejo avanzado de templates, y características de administración de usuarios.
Además ofrece un servicio de alarmas mediante el manejo de umbrales. Todo ello en una sola consola de administración.

CACTI constituye un completo almacenamiento de toda la información necesaria para crear los gráficos y los agrupan en una base de datos de MySQL. Cacti tiene capacidades incorporadas del SNMP. Es capaz de la interrogación de todos los dispositivos SNMP en la red, y la adición de la información seleccionada ingresa a los gráficos. En su forma más simple, los cactos le darán la capacidad de agregar un gráfico para los aspectos mas comunes del usuario que supervisa (espacio de

disco, promedio de la carga, uso de la memoria, etc.) y la supervisión de la red (los octetos dentro y fuera de un interfaz).

El Cacti es un paquete libre y de la open-source de software diseñada a utilizar el SNMP para recopilar estadística de los dispositivos capaces del SNMP, incluyendo los dispositivos de Cisco y los interruptores, así como los servidores y los sitios de trabajo.

Es tan evidente que los cactos tienen gráficos, pero una función quizás misteriosa es plantillas del gráfico. Las plantillas permiten que agrupe juntos los gráficos que comparten algunas características comunes. Esto se utiliza normalmente para la simplificación del administrador, porque todos los cambios realizados a la plantilla afectarán todos los gráficos que utilice la plantilla definida. Así mismo, todos los permisos aplicados a una plantilla afectarán todos los gráficos que utilicen la plantilla.

Objetivos

- Analizar e implantar alternativas de monitoreo de Código Abierto (Open Source) para el establecimiento de un sistema de monitoreo global que incluya los servicios, aplicaciones y redes de la organización.
- Mejorar la disponibilidad, estabilidad y visibilidad en cuanto al uso de los recursos informáticos de la organización.

Retos

- Detectar las interrupciones en los sistemas y bajo rendimiento de la red.
- Detectar problemas de red antes de que estos impacten las actividades de los usuarios.
- Mejorar la capacidad de planeación y asignar/adquirir acertadamente los recursos necesarios.
- Dar solución rápida y efectiva a los problemas informáticos.

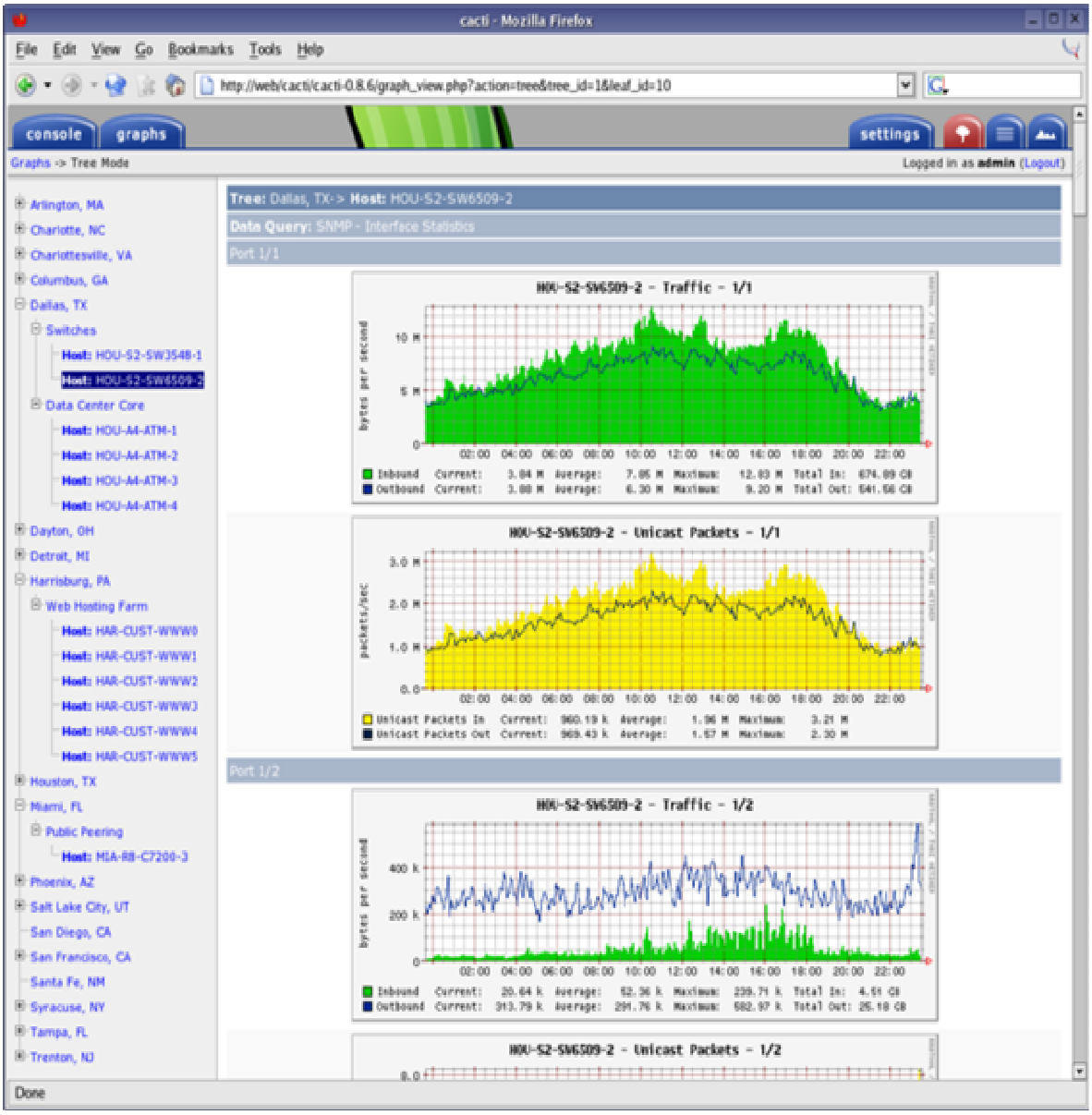


Fig. 36 - Cacti

Fuente:http://64.233.179.104/translate_c?hl=es&u=http://www.cacti.net/image.php%3Fimage_id%3D43&prev=/search%3Fq%3Dque%2Bes%2Bel%2Bsoftware%2Bcacti%26hl%3Des%26lr%3D%26sa%3DG

2.10.2 FUENTES DE DATOS

Las fuentes de datos pueden ser creadas y utilizan RRDTool “crean” y “ponen al día” las funciones. Cada fuente de datos se puede utilizar para recopilar datos locales o alejados y ponerlas en un gráfico.

Las ayudas RRD archivan con más de una fuente de datos y pueden utilizar un archivo de RRD almacenado donde quiera en el sistema de ficheros local.

Los ajustes redondos del archivo (RRA) se pueden modificar para requisitos particulares dando al usuario la capacidad de recopilar datos sobre timespans (duraciones, no estándar) mientras que las cantidades varían del almacén de datos.

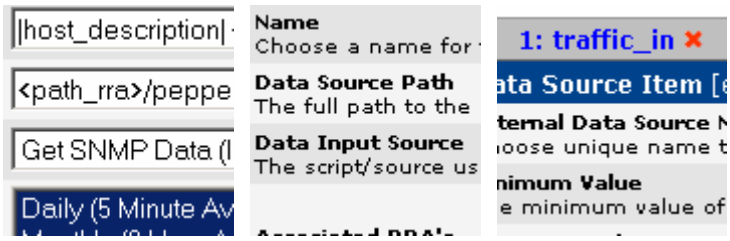


Fig. 37 - Fuentes de Datos

Fuente: www.cacti.com

2.10.3 GRÁFICOS

Una vez que se definan unas o más fuentes de datos, un gráfico de RRDTool se puede crear usando los datos. Los cactos permiten que cree casi cualquier gráfico imaginable de RRDTool usando todos los tipos del gráfico de RRDTool y funciones estándares de la consolidación. Un área de la selección de color y un acolchado automático del texto funcionan también, ayuda en la creación de los gráficos para hacer el proceso más fácil.

No sólo puede crear gráficos basados RRDTool en cactos, pero hay muchas maneras de exhibirlos. Junto con una “opinión estándar de la lista” y un “modo de la inspección previo”, que se asemeja al frontend 14all de RRDTool, hay una “opinión del árbol”, que permite que pongas gráficos sobre un árbol jerárquico para los propósitos de organización.

Fig. 38 – Gráficos

Fuente: www.cacti.com

2.10.4 EXIBICIÓN DEL GRÁFICO

La opinión del árbol permite que los usuarios creen “jerarquías del gráfico” y que pongan gráficos en el árbol. Esto es una manera fácil de manejar/organizar una gran cantidad de gráficos.

La opinión de la lista enumera el título de cada gráfico en una lista grande que llegue al usuario al gráfico real.
La opinión de la inspección previa exhibe todos los gráficos en un formato grande de la lista.

2.10.5 GERENCIA DEL USUARIO

Los administradores pueden crear a usuarios y asignar diversos niveles de permisos a los cactos.
Los permisos pueden ser por gráfico especificado para cada usuario, haciendo los cactos convenientes para las situaciones de la localización.
Cada usuario puede guardar sus propios ajustes del gráfico para las preferencias de la visión que varían.

2.10.6 PLANTILLAS

Las plantillas de la fuente de datos permiten a tipos comunes de la fuente de datos ser agrupadas en templating. Cada campo para una fuente de datos normal puede ser templated (plantilla) o especificó sobre una base de la fuente de datos.

Las plantillas del cliente son un grupo de las plantillas de la fuente del gráfico y de datos que permiten que defina tipos comunes del cliente. Sobre la creación de un cliente, adquirirá automáticamente las características de su plantilla.

2.10.7 REUNIÓN DE LOS DATOS

Contiene “un mecanismo de la entrada de datos” que permita que los usuarios definan las escrituras de encargo que se pueden utilizar para recopilar datos. Cada escritura puede contener las discusiones que se deben incorporar para cada fuente de datos creada usando la escritura (tal como un IP address).
Construido con la ayuda del SNMP que puede utilizar php-SNMP, ucd-SNMP, o red-SNMP.
Capacidad de recuperar datos usando el SNMP o una escritura con un índice. Un ejemplo de esto estaría poblando una lista con los interfaces del IP o las particiones montadas en un servidor. La integración con las plantillas del gráfico se puede definir para permitir una creación del gráfico del tecleo para los clientes.
PHP se proporciona para ejecutar las escrituras, para recuperar datos del SNMP, y para poner al día los archivos de RRD.

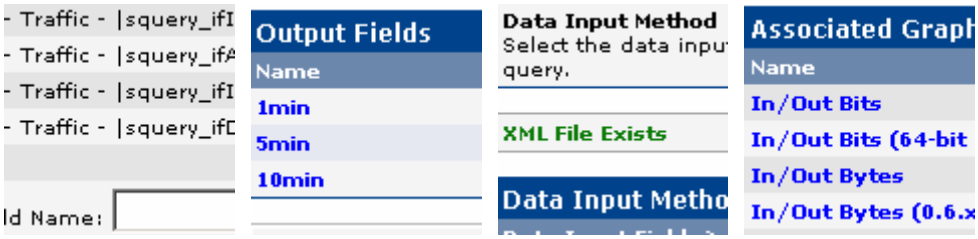


Fig. 39 – Reunión de Datos

Fuente: www.cacti.com

Las gráficas del cacti pueden mostrarse desde los últimos días, hasta los últimos dos años en un rango especificado. Esto servirá de respaldo para cualquier persona que sea el administrador en demostrar a través de las graficas que el consumo del AB (ancho de banda) para su salida al Internet o datos han sido las mejores, o que existieron inconvenientes. Además existe la posibilidad de que se grafique según el rango (desde que día) que se desee escoger.

Grafica del último día:

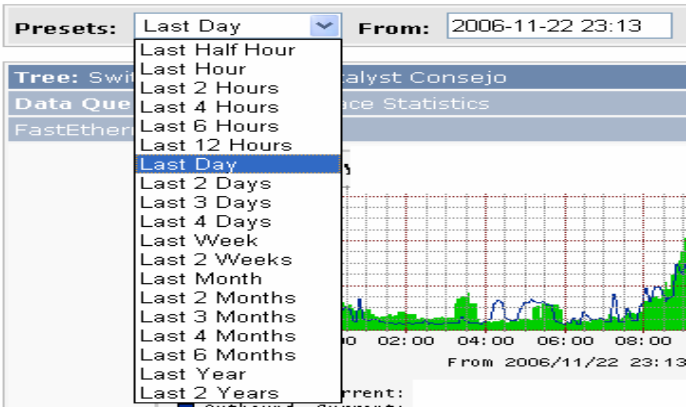


Fig. 40 – Grafica del Cacti (último día)

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

Grafica desde el rango (tiempo) escogido.

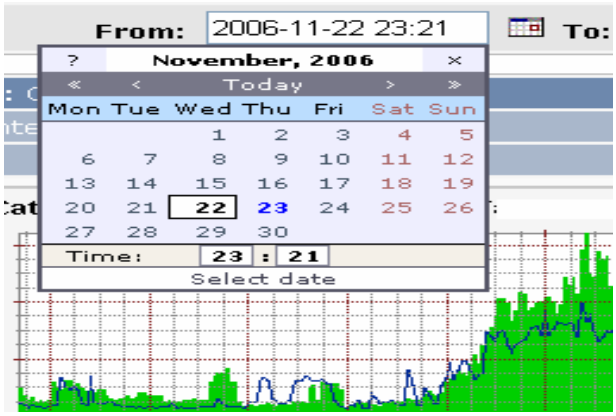


Fig. 41 – Grafica del Cacti

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

2.11 DEFINICION Y CARACTERISTICAS DEL PROXY- SQUID

2.11.1 DEFINICIÓN DE PROXY

2.11.1.1 ¿Qué es Servidor Intermediario (Proxy)?

El término en ingles Proxy tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de

Intermediario. Se suele traducir, en el sentido estricto, como delegado o apoderado (el que tiene el poder sobre otro).

Un Servidor Intermediario (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red.

2.11.1.2 Definición de Squid

Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo programática libre, está disponible el código fuente para quien así lo requiera.

NOTA ESPECIAL: Squid no debe ser utilizado como Servidor Intermediario (Proxy) para protocolos como SMTP, POP3, TELNET, SSH, IRC, etc. Si se requiere intermediar para cualquier protocolo distinto a HTTP, HTTPS, FTP, GOPHER y WAIS se requerirá implementar obligatoriamente un enmascaramiento de IP o NAT (Network Address Translation) o bien hacer uso de un servidor SOCKS como Dante.

2.11.2 CARACTERISTICAS DEL PROXY

2.11.2.1 Velocidad

Instalando un proxy en su red interna o equipo conseguirá acelerar la navegación ya que se recibirán más rápidamente las páginas que ya estén almacenadas en la caché por no tener que volver a recogerlas de Internet.

2.11.2.2 Control

En el caso de una red interna un proxy también permite controlar/monitorizar la actividad y las páginas visitadas por cada empleado.

2.11.2.3 Restricción

Con un proxy puede fácilmente impedir el acceso a ciertos contenidos que no están relacionados con la actividad de su empresa.

Además de las características mencionadas anteriormente, también se pueden citar las siguientes:

- Proporciona una capa extra de seguridad.
- Aísla a los usuarios de la intranet.
- Un Proxy actúa como un 'cache', es decir un almacenamiento dinámico de información con mayor acceso.
- Se realiza una vigilancia, control y acceso transparente para el usuario.

Entre las características para un administrador, podemos citar las siguientes:

- Podemos hacer usos de las características inherentes al SQUID para definir listas de control de acceso, tanto para usuarios, como para url's.

- Permite el control de acceso a diferentes sitios web. Podemos utilizar para este propósito al software GUARDIAN.

- Permite reportes detallados del uso de internet, usuarios, ancho de banda, horas de acceso, etc. Se puede utilizar para este propósito a SQUINT o SARG.

Si la petición ya ha sido realizada por otro cliente y este se conserva en 'cache'; dicha petición NO saldrá a internet; con el consiguiente ahorro de ancho de banda y rápido acceso, ya que la información se obtendrá del 'cache' del servidor. Y

consecuentemente si la petición es 'nueva', esta petición, si saldrá a la internet u otra red.

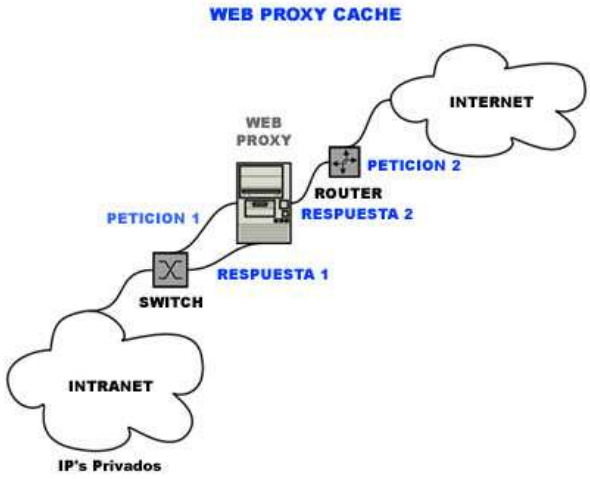


Fig. 40 – Proxy

Fuente: http://www.informatizate.net/articulos/proxy_buen_punto_20030822.html

El Uso de un Proxy es un mecanismo a tomar en consideración, para mejorar no solo la performance de la intranet; dadas las características antes mencionadas; sino también como un punto mas a favor de la seguridad de la empresa.

Dadas las muchas características de configuración de SQUID y el hecho de ser Software Libre; hacen de SQUID un software de muy buen desarrollo, soporte y calidad.

CAPITULO III – ESTUDIO DE VLANs

3.1 INTRODUCCIÓN

Las redes de área local virtuales (VLANs) han surgido de un conjunto de soluciones que los mayores distribuidores de equipamiento de redes de área local (LAN) habían propuesto para la conmutación de éstas. Aunque el entusiasmo del usuario final por la implementación de las VLANs todavía no se ha mostrado, la mayoría de las empresas han empezado a buscar fabricantes que propongan una buena estrategia para su VLAN, así como que éstas sean incorporadas sobre las redes existentes, añadiendo funciones de conmutación y un software de gestión avanzado.

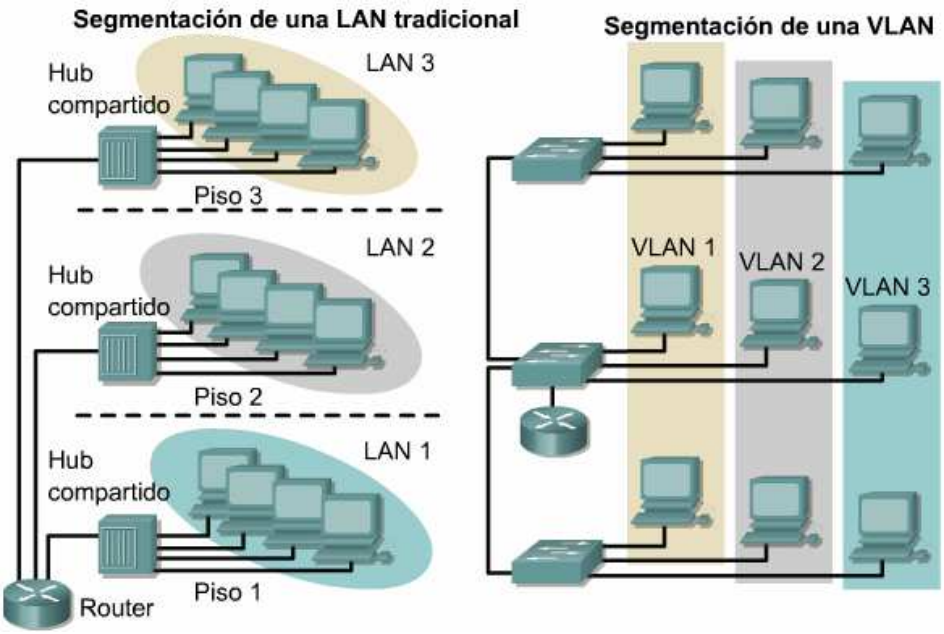


Fig. 41 - LAN Y VLAN

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

Una de las razones de que se centre la atención sobre las VLANs ha sido el rápido desarrollo de las LANs conmutadas, hecho que comenzó en 1994/1995.

Los modelos de red basados en la compartición de ancho de banda, presentes en las arquitecturas LAN de los primeros años noventa, carecen de la potencia suficiente como para proporcionar cada vez mayores anchos de banda que requieren las aplicaciones multimedia.

En la actualidad se necesitan nuevos modelos capaces de proporcionar la potencia suficiente no sólo para satisfacer la creciente necesidad de ancho de banda, sino también para soportar un número mayor de usuarios en la red.

En las LAN basadas en compartición de ancho de banda, los usuarios comparten un único canal de comunicaciones, de modo que todo el ancho de banda de la red se asigna al equipo emisor de información, quedando el resto de equipos en situación de espera. Para aumentar el ancho de banda disponible para cada usuario, se puede optar por la segmentación de sus segmentos y anillos. Ahora bien, estas técnicas no ofrecen buenas prestaciones, debido principalmente a las dificultades que aparecen para gestionar la red. Cada segmento suele contener por lo menos desde 30 usuarios.

La técnica idónea para proporcionar elevados anchos de banda es la conmutación. Mediante esta técnica, cada estación de trabajo y cada servidor poseen una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Las LANs basadas en compartición de ancho de banda se configuran mediante switches y routers. En una LAN conmutada, la función tradicional del *router* es el encaminamiento de la información en la red, pasa a ser realizada por el conmutador LAN, quedando aquél destinado a funciones relacionadas con la mejora de las prestaciones en lo que respecta a la gestión de la red. Con este nuevo papel del *router*, se pueden contener desde 100 usuarios. El decremento en los precios de conmutadores *Ethernet* y *Token Ring* ha sido uno de los principales empujes a que un buen número de empresas se inclinen por una LAN conmutada.

Sin embargo, el continuo despliegue de conmutadores, dividiendo la red en más y más segmentos (con menos y menos usuarios por segmento) no reduce la

necesidad de contenido de *broadcast,* información para gestionar la red. Las VLANs representan una solución alternativa a los *routers* con función de gestores de la red. Con la implementación de conmutadores (Switch) en unión con VLANs, cada segmento de la red puede contener como mínimo un usuario. Además, las VLANs pueden enrutar movimientos de las estaciones de trabajo hacia nuevas localizaciones, sin requerimiento de reconfigurar manualmente las direcciones IP.

3.1.1 ¿POR QUÉ NO TODAS LAS EMPRESAS SE HAN INCLINADO POR LAS VLANS?

Para la mayoría de organizaciones, los conmutadores (Switch) tienen todavía que ser implementados a una suficientemente mayor escala para necesitar VLANs. Esa situación cambiará pronto. Hay, de todos modos, otras razones para explicar la no tan agradable recepción que han tenido en el mercado de parte de los usuarios de red:

- Las VLANs han sido, y son aún soluciones a nivel de propietario de cada distribuidor. Como la industria de redes de información ha demostrado, las soluciones a nivel de propietario (privadas) son una oposición a las políticas de los sistemas abiertos que se han desarrollado en la migración a estaciones de trabajo locales y el modelo cliente servidor.

- Los clientes saben de los numerables costes asociados al cambio (adición y cambio de elementos, etc.) y se imaginan que las VLANs tienen sus propios costes administrativos fuertemente escondidos.

- Aunque muchos analistas han sugerido que las VLANs permiten el desarrollo de servidores centralizados, los clientes han de mirar hacia implementaciones de gran empresa y ver las dificultades en habilitar un acceso completo y de alta funcionalidad a los servidores centralizados.

3.2 DEFINICIÓN DE UNA VLAN

Una VLAN es una agrupación lógica de estaciones, servicios y dispositivos de red que no se limita a un segmento de LAN físico.

Las VLAN facilitan la administración de grupos lógicos de estaciones y servidores que se pueden comunicar como si estuviesen en el mismo segmento físico de LAN. También facilitan la administración de mudanzas, adiciones y cambios en los miembros de esos grupos.

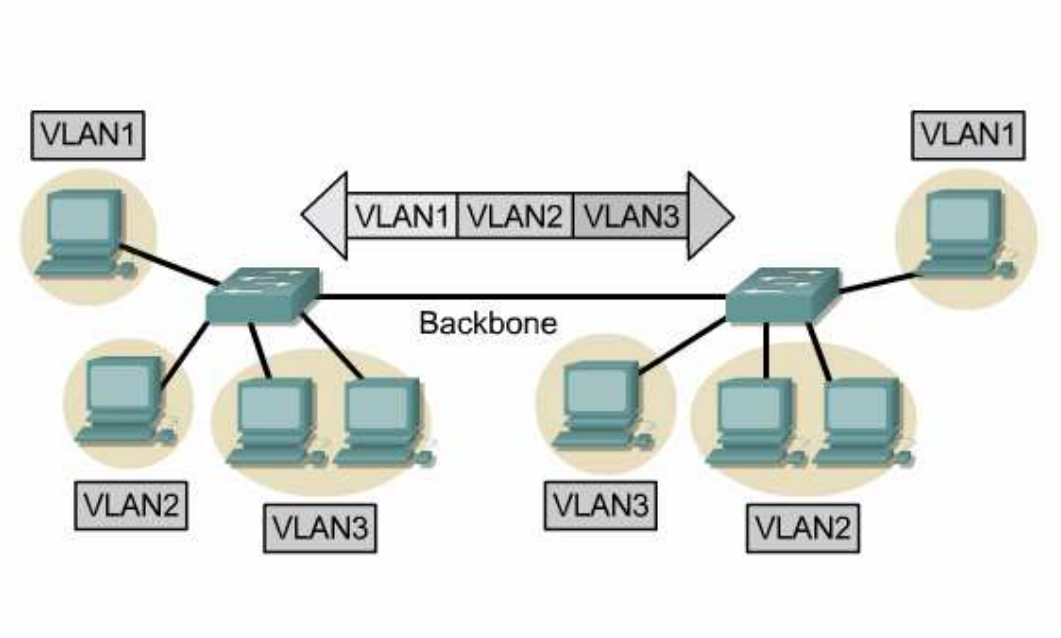


Fig. 42 – Vlans

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

Las VLAN segmentan de manera lógica las redes conmutadas según las funciones laborales, departamentos o equipos de proyectos, sin importar la ubicación física de los usuarios o las conexiones físicas a la red. Todas las estaciones de trabajo y servidores utilizados por un grupo de trabajo en particular comparten la misma VLAN, sin importar la conexión física o la ubicación.

La configuración o reconfiguración de las VLAN se logra mediante el software. Por lo tanto, la configuración de las VLAN no requiere que los equipos de red se trasladen o conecten físicamente.

Una estación de trabajo en un grupo de VLAN se limita a comunicarse con los servidores de archivo en el mismo grupo de VLAN. Las VLAN segmentan de forma lógica la red en diferentes dominios de broadcast, de manera tal que los paquetes sólo se conmutan entre puertos y se asignan a la misma VLAN. Las VLAN se componen de hosts o equipos de red conectados mediante un único dominio de puenteo. El dominio de puenteo se admite en diferentes equipos de red. Los switches de LAN operan protocolos de puenteo con un grupo de puente separado para cada VLAN.

Las VLAN se crean para brindar servicios de segmentación proporcionados tradicionalmente por routers físicos en las configuraciones de LAN. Las VLAN se ocupan de la escalabilidad, seguridad y gestión de red. Los routers en las topologías de VLAN proporcionan filtrado de broadcast, seguridad y gestión de flujo de tráfico. Los switches no puentean ningún tráfico entre VLAN, dado que esto viola la integridad del dominio de broadcast de las VLAN. El tráfico sólo debe enrutarse entre VLAN.

3.3 COMPONENTES DE LAS VLANS

Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

Con el switch, el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los “dominios de colisión” por cada uno de los puertos.
- Dedica el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los “dominios de broadcast”, en lugar de uno solo, se puede configurar el switch para que existan más “dominios”.

- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.
- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.
- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán “vernos” como una Red de Área Local independiente a las demás.

3.3.1 FUNCIONAMIENTO DE UNA VLAN

El funcionamiento e implementación de las VLANs está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q.

Con las VLANs se aísla el tráfico de colisiones y de broadcast, cada VLAN es independiente una de otra, pero todavía falta mencionar cómo es que se comunican entre sí, ya que muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLANs. Por ejemplo, los de sistemas con los de redes, o los de redes con finanzas, etc.

En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente.

Por la razón de que hay varias formas en que se puede definir una VLAN, se dividen éstas en tres tipos principales: basadas en puertos, basadas en MAC, VLANs de capa 3.

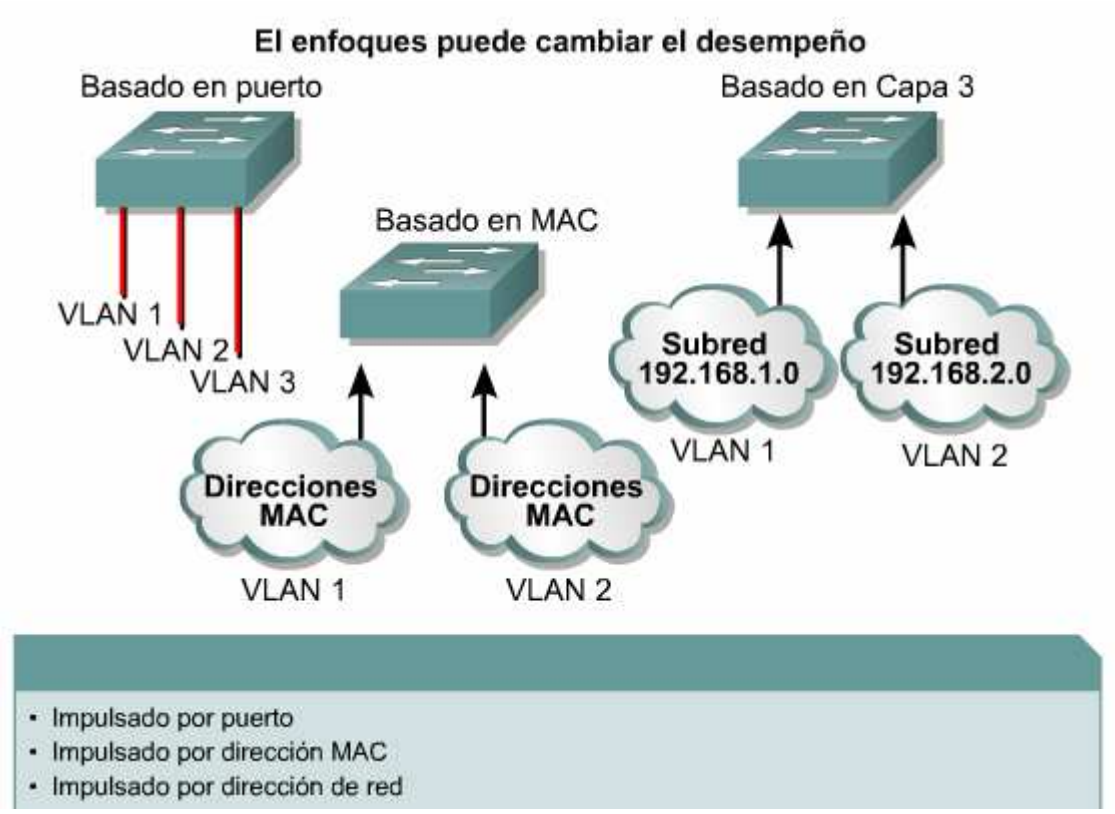


Fig. 43 - Tipos de Vlans

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

3.3.1.1 Vlans basadas en puertos

Según este esquema, la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores. La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.

Muchas de las primeras implementaciones de las VLANs definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1,2,3,7 y 8 sobre un

conmutador forman la VLAN A, mientras que los puertos 4,5 y 6 forman la VLAN B). Además, en la mayoría, las VLANs podían ser construidas sobre un único conmutador.

La segunda generación de implementaciones de VLANs basadas en puertos contempla la aparición de múltiples conmutadores (por ejemplo, los puertos 1 y 2 del conmutador 1 y los puertos 4,5,6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3,4,5,6,7 y 8 del conmutador 1 combinados con los puertos 1,2,3 y 8 del conmutador 2 configuran la VLAN B). Este esquema es el descrito por la figura 44 (Vlans basadas en puertos).

La agrupación por puertos es todavía el método más común de definir la pertenencia a una VLAN, y su configuración es bastante directa. El definir una red virtual completamente basada en puertos no permite a múltiples VLANs el incluir el mismo segmento físico (o conmutador).

De todos modos, la principal limitación de definir VLANs por puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro.

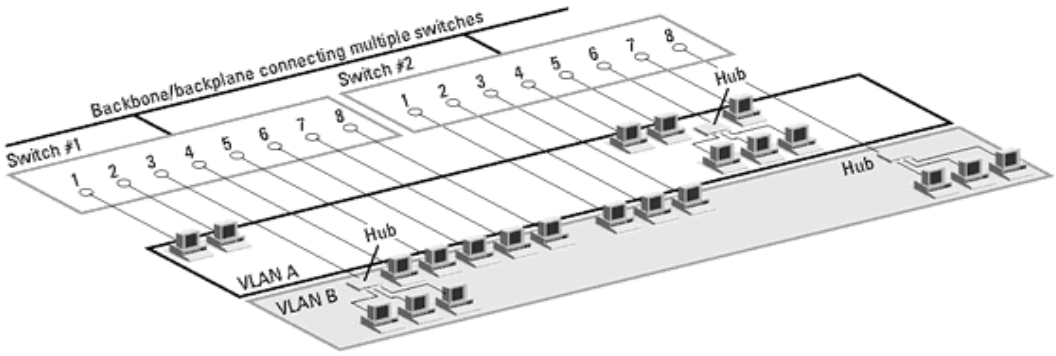


Fig. 44 - VLANs basadas en puertos

Fuente: http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link2

3.3.1.2 Vlans basadas en Mac

Constituye la segunda etapa de la estrategia de aproximación a la VLAN, y trata de superar las limitaciones la las VLANs basadas en puertos. Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC.

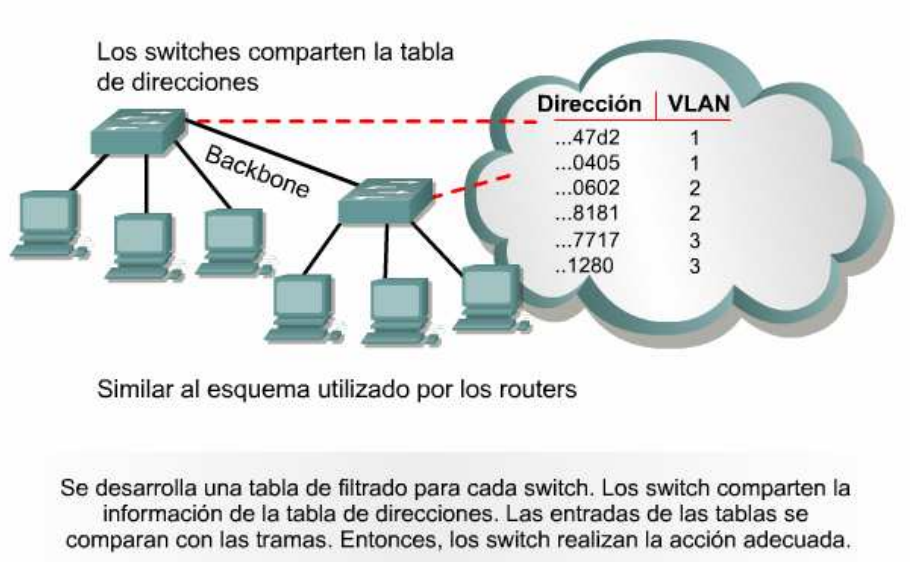


Fig. 45 - Vlans por Mac

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet-31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

Este tipo de implementación tiene varias ventajas y desventajas. Desde que las direcciones MAC (*media access control* - control de acceso al medio) se encuentran implementadas directamente sobre la tarjeta de interface de la red (NIC -*network interface card*), las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.

Entre los inconvenientes de las VLANs basadas en MAC está el requerimiento de que todos los usuarios deben inicialmente estar configurados para poder estar en al menos una VLAN.

Después de esa configuración manual inicial, el movimiento automático de usuarios es posible, dependiendo de la solución específica que el distribuidor haya dado. Sin embargo, la desventaja de tener que configurar inicialmente la red llega a ser clara en redes grandes, donde miles de usuarios deben ser asignados explícitamente a una VLAN particular. Algunos distribuidores han optado por realizar esta configuración inicial usando herramientas que crean VLANs basadas en el actual estado de la red, esto es, una VLAN basada en MAC es creada para cada subred.

Las VLANs basadas en MAC que son implementadas en entornos de medios compartidos se degradarán seriamente como miembros de diferentes VLANs coexistiendo en un mismo conmutador. Además, el principal método de compartición de información entre miembros de una VLAN mediante conmutadores en una red virtual basada en MAC también se degrada cuando se trata de una implementación a gran escala.

3.3.1.3 Vlans de capa 3

Las VLANs de capa 3 toman en cuenta el tipo de protocolo (si varios protocolos son soportados por la máquina) o direcciones de la capa de red, para determinar la pertenencia a una VLAN. Aunque estas VLANs están basadas en información de la capa 3, esto no constituye una función de encaminamiento y no debería ser confundido con el enrutamiento en la capa de red.

Realizada la distinción entre VLANs basadas en información de la capa 3 y el concepto de encaminamiento o *routing*, hay que apuntar que algunos distribuidores están incorporando varios conceptos de la capa 3 en sus conmutadores, habilitando funciones normalmente asociadas al enrutamiento.

Hay varias ventajas en definir VLANs de capa 3. En primer lugar, permite particionar por tipo de protocolo, lo que puede parecer atractivo para los administradores que están dedicados a una estrategia de VLAN basada en servicios o aplicaciones. En segundo lugar, los usuarios pueden físicamente mover sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación (este es un beneficio principalmente para los

usuarios de TCP/IP). Y en tercer lugar, definir una VLAN de capa 3 puede eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores.

Una de las desventajas de definir la VLAN de capa 3 (al contrario de lo que ocurría en las dos anteriores) es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas. Por esta razón, los conmutadores que usan información de la capa 3 para la definición de VLANs son generalmente más lentos que los que usan información de la capa 2. Esta diferencia no ocurre en todas las distintas implementaciones de cada distribuidor.

Las VLANs basadas en capa 3 son particularmente efectivas en el trato con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DEC*net* o *AppleTalk*, que no implican configuración manual. Además tienen la dificultad al tratar con protocolos no enrutables como NetBIOS (estaciones finales que soportan protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).

3.4 TIPOS DE VLANS

- Vlans Estática
- Vlans Dinâmica

3.4.1 VLAN ESTÁTICA

Las VLAN estáticas son puertos en un switch que se asignan estáticamente a una VLAN.

- Estos puertos mantienen sus configuraciones de VLAN asignadas hasta que se cambien.
- Aunque las VLAN estáticas requieren que el administrador haga los cambios, este tipo de red es segura, de fácil configuración y monitoreo.
- Las VLAN estáticas funcionan bien en las redes en las que el movimiento se encuentra controlado y administrado.

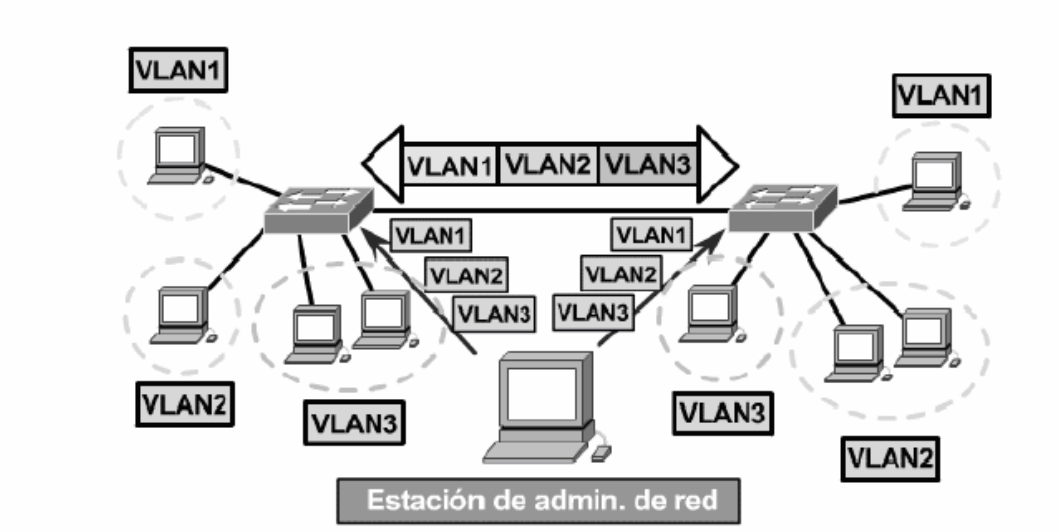


Fig. 46 - Vlan Estática

Fuente: http://www.eduangi.com/documentos/3_CCNA2.pdf

3.4.2 VLAN DINÁMICA

- Las VLAN dinámicas son puertos del switch que pueden determinar automáticamente sus tareas VLAN.
- Las VLAN dinámicas se basan en direcciones MAC, direccionamiento lógico o tipo de protocolo de los paquetes de datos

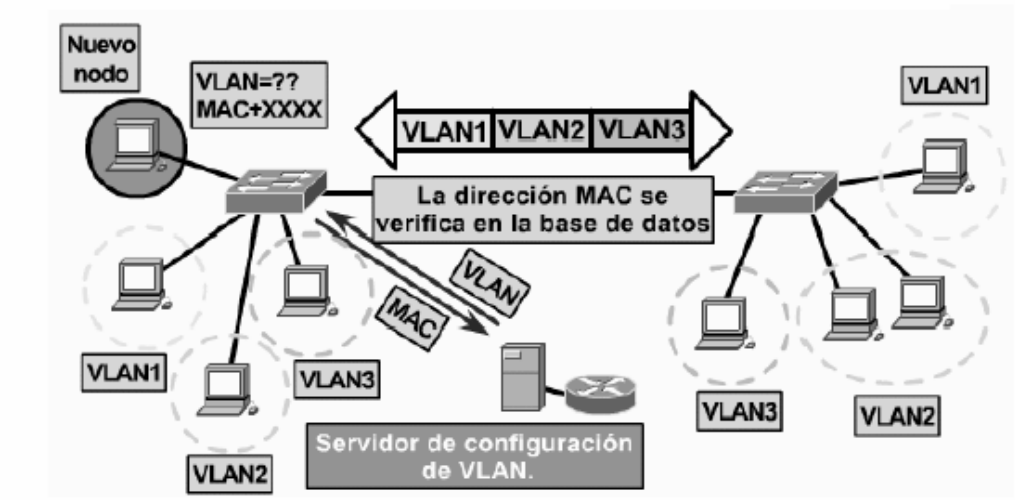


Fig. 47 - Vlan Dinámica

Fuente:http://www.eduangi.com/documentos/3_CCNA2.pdf

3.5 EL BENEFICIO DE IMPLEMENTAR UNA VLANS

- Reducción del coste de movimientos y cambios.
- Grupo de trabajo virtuales
- Seguridad

3.5.1 REDUCCIÓN DEL COSTE DE MOVIMIENTOS Y CAMBIOS.

La principal excusa para implementar una VLAN es la reducción en el coste de los cambios y movimientos de usuarios. Desde que estos costes son bastante sustanciales, este argumento es suficientemente obligatorio para la implementación de una VLAN.

Muchos fabricantes están prometiendo que la implementación de una VLAN resultará más conveniente a la hora de habilitar la administración de redes dinámicas, y que esto supondrá bastante ahorro. Esta promesa se puede aplicar con buenos resultados a redes IP, ya que, normalmente, cuando un usuario se mueve a una diferente subred, las direcciones IP han de ser actualizadas manualmente en la estación de trabajo.

Este proceso consume gran cantidad de tiempo que podría ser aprovechado para otras tareas, tales como producir nuevos servicios de red. Una VLAN elimina ese hecho, porque los miembros de una red virtual no están atados a una localización física en la red, permitiendo que las estaciones cambiadas de sitio conserven su dirección IP original.

Sin embargo, cualquier implementación de VLAN no reduce este coste. Una VLAN añade una nueva capa de conexión virtual que ha de ser administrada al mismo tiempo que la conexión física. Esto no quiere decir que no se puedan reducir los costes hablados anteriormente. Sólo que no hay que precipitarse a la hora de implementar una VLAN y es mejor estar bien seguro de que la solución no genera más trabajo de administración de red que el que se pueda ahorrar.

3.5.2 GRUPOS DE TRABAJO VIRTUALES

Uno de los objetivos más ambiciosos de una red virtual es el establecimiento del modelo de grupos de trabajo virtuales. El concepto es que, con una completa implementación de una VLAN a través de todo el entorno de red del campus, miembros del mismo departamento o sección puedan aparentar el compartir la misma red local, sin que la mayoría del tráfico de la red esté en el mismo dominio de *broadcast* de la VLAN. Alguien que se mueva a una nueva localización física pero que permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo.

Esto ofrece un entorno más dinámicamente organizado, permitiendo la tendencia hacia equipos con funciones cruzadas. La lógica del modelo virtual por grupos de trabajo va la siguiente forma: los equipos pueden estar conectados virtualmente a la misma LAN sin necesidad de mover físicamente a las personas para minimizar el tráfico a través de una red troncal colapsada. Además, estos grupos serán dinámicos: un equipo destinado a un proyecto puede ser configurado mientras dure ese proyecto, y ser eliminado cuando se complete, permitiendo a los usuarios retornar a sus mismas localizaciones físicas.

3.5.3 SEGURIDAD

El único tráfico de información en un segmento de un solo usuario será de la VLAN de ese usuario, por lo que sería imposible "escuchar" la información si no nos es permitida.

3.6 LOS RETOS DE LA MIGRACIÓN

El primer reto, y el más importante, será la limitación del presupuesto. Las empresas tienden a ajustar cada vez más sus presupuestos, por lo que antes de decidir ningún gasto es conveniente recordar cómo se distribuye: el 16% para bienes de equipo y el 84% para costes operativos. Dosificando sabiamente la inversión en productos que conduzcan a una red virtual, será posible reducir el tamaño del desagüe al que va a parar casi el 85% del presupuesto anual de redes.”Estadísticas realizadas por Cisco”

El segundo reto corresponde a la incorporación de los sistemas antiguos heredados. Si aún se tienen aplicaciones críticas funcionando en un *mainframe*, será necesaria una solución para integrar la red SNA en la nueva infraestructura. La migración progresiva hacia ATM y las redes virtuales conmutadas exige continuar dando soporte a las redes de acceso compartido existentes.

Lo primero es determinar las necesidades para seleccionar la tecnología que mejor se adapte a ellas. Después será preciso buscar una solución que soporte dicha tecnología. Antes de reemplazar la tecnología de acceso compartido con conmutadores ATM, hay que decidir si los usuarios necesitan realmente tales niveles de ancho de banda y calidad de servicio.

También habrá que tener en cuenta las aplicaciones que deberá soportar la infraestructura y las necesidades previstas para los próximos cinco años. Si el objetivo final a largo plazo es ATM, habrá que planificar cómo preparar la red existente para soportar dicha tecnología.

Si no se dispone de un sistema de gestión corporativa potente, distribuido y orientado a objetos, habrá que empezar a buscarlo. Aparte del beneficio inmediato que esto reportará (al reducir los tiempos de caída), será necesario para cualquier clase de red virtual, ya esté esta basada en paquetes o celdas.

3.7 VENTAJAS DE VLAN

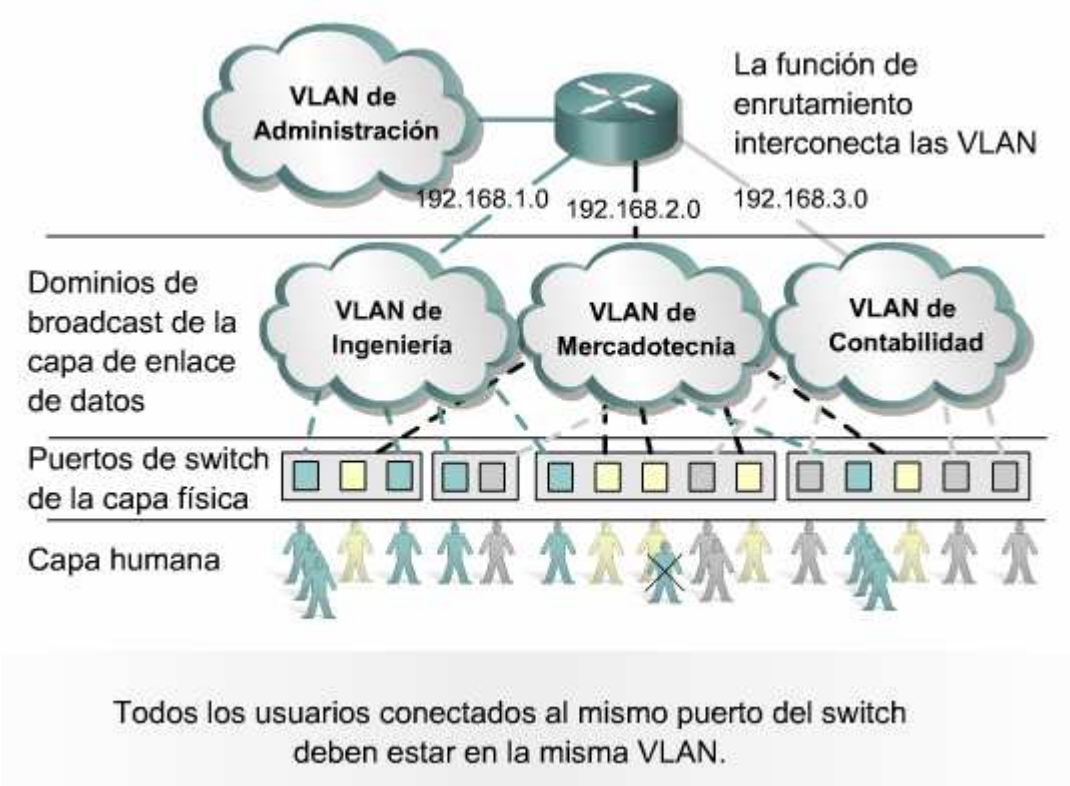


Fig. 48 - Ventajas de Vlan

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

Como hemos visto, hay varias ventajas a usar VLANs. Para resumir, las ventajas de la arquitectura de VLAN incluyen:

- Funcionamiento creciente
- Flexibilidad mejorada
- Independencia física de la topología
- Opciones crecientes de la seguridad

3.7.1 FUNCIONAMIENTO CRECIENTE

Las redes cambiadas por la naturaleza aumentarán los dispositivos compartidos excedente de los medios del funcionamiento en uso hoy, sobre todo reduciendo el tamaño de los dominios de la colisión. Agrupar a usuarios en redes lógicas también aumentará funcionamiento limitando tráfico de la difusión a los usuarios que realizan funciones similares o dentro de workgroups individuales. Además, menos tráfico necesitará ser encaminado.

3.7.2 FLEXIBILIDAD MEJORADA

VLANs proporciona una manera fácil, flexible, menos costosa de modificar a grupos lógicos en ambientes que cambian. VLANs hace redes grandes más manejables permitiendo la configuración centralizada de los dispositivos situados en localizaciones físicamente diversas.

3.7.3 INDEPENDENCIA FÍSICA DE LA TOPOLOGÍA

VLANs proporciona independencia de la topología física de la red permitiendo que los workgroups físicamente diversos sean conectados lógicamente dentro de un solo dominio de la difusión. Si la infraestructura física está ya en lugar, ahora se convierte en algo fácil agregar puertos en nuevas localizaciones a VLANs existente si un departamento se amplía o vuelve a poner. Estas asignaciones pueden ocurrir por adelantado del movimiento, y es entonces algo fácil mover los dispositivos con sus configuraciones existentes a partir de una localización a otra. Los viejos puertos se pueden entonces "desarmar" para el uso futuro, o reutilizar por el departamento para los nuevos usuarios en la VLAN.

3.7.4 OPCIONES CRECIENTES DE LA SEGURIDAD

VLANs tiene la capacidad de proporcionar la seguridad adicional no disponible en un ambiente compartido de la red de los medios. Por la naturaleza, una red cambiada entrega tramas solamente a los recipientes previstos, y a la difusión enmarca solamente a otros miembros del VLAN. Esto permite que el administrador de la red divida a usuarios en segmentos que requieren el acceso a la información sensible en VLANs separado del resto de la comunidad de usuario general sin importar la localización física. Además, la supervisión de un puerto

con un analizador del tráfico opinión solamente el tráfico asociado a ese puerto particular, haciendo la supervisión discreta de tráfico de la red más difícil.

Debe ser observado que la seguridad realzada que se menciona arriba no debe ser considerada una salvaguardia absoluta contra infracciones de la seguridad.

3.8 LIMITACIONES DE VLANs

Hay algunas limitaciones a usar VLANs, algo de ser más notable:

- Limitaciones de la difusión
- Limitaciones del dispositivo
- Apremios portuarios

3.8.1 LIMITACIONES DE LA DIFUSIÓN

Para manejar tráfico de la difusión en un ambiente de la atmósfera VLAN es necesario tener un servidor especial que sea una parte integrada de la infraestructura de la atmósfera. Este servidor tiene limitaciones en el número de las difusiones que pueden ser remitidas. Algunos protocolos de red que funcionarán dentro de VLANs individual, tal como IPX y Appletalk, hacen el uso extenso de tráfico de la difusión. Esto tiene el potencial de umbrales de afectación en los interruptores o los servidores de la difusión y puede requerir la consideración especial al determinar tamaño y la configuración de VLAN.

3.8.2 LIMITACIONES DEL DISPOSITIVO

El número de las direcciones de Ethernet que puede ser apoyado por cada dispositivo del borde es 500. Esto representa una distribución de cerca de 20 dispositivos por puerto de la red 21. Estos números son las limitaciones técnicas reales que podrían ser más a fondo reducido debido a los requisitos de funcionamiento de dispositivos unidos.

Estas limitaciones están sobre los niveles recomendados para el establecimiento de una red del alto rendimiento. De un punto de vista puro del funcionamiento, el dispositivo ideal del usuario final al cociente portuario de la red 21 sería un

dispositivo por puerto. Desde un punto de vista práctico, un solo puerto de la red 21 se podría compartir por un número de dispositivos que no requieren anchura de banda y no pertenecen al mismo VLAN. Un ejemplo de esto sería una computadora de escritorio, impresora, y una computadora de computadora portátil para un usuario individual.

3.8.3 TAREAS DE LA CONFIGURACIÓN DE VLAN

Utilice Menú virtual del LAN para realizar las tareas siguientes, que se describen:

- Tenga acceso al menú virtual del LAN
- Asigne un dominio de gerencia
- Defina un VLAN
- Puertos del interruptor del grupo a VLANs
- Configure los troncos (troncales)
- Configure VTP
- Configure VTP que pueda

CAPITULO IV – CONFIGURACIÓN E IMPLEMENTACIÓN DE LOS EQUIPOS

4.1 CASO 1 – DISEÑO DE LA RED MEDIANTE TOPOLOGÍA BUS Y CONFIGURACIÓN DE LAS ESTACIONES DE TRABAJO

4.1.1 PLANTEAMINETO DEL CASO

Para este diseño de red se plantea lo siguiente:
Establecer y documentar Requerimientos como:

- **Funcionalidad.-** Conectividad con velocidad razonable y confiabilidad entre usuario - usuario y usuario-aplicación.
- **Escalabilidad.-** Ampliaciones futuras sin realizar ningún cambio mayor al diseño global.
- **Adaptabilidad.-** Diseñada con visión hacia nuevas tecnologías.
- **Manejabilidad.-** Facilidad para monitoreo y manejo de la red.

Para maximizar la disponibilidad del ancho de banda y el rendimiento se deben considerar:

- La función y ubicación de los servidores.
- Administrar dominios de colision.
- Problemas con la segmentación.
- Administrar dominios de broadcast.

Entender los problemas que afecta el rendimiento de la red, como:

Velocidad efectiva (Throughput).

Tiempo de respuesta.

Acceso a los recursos.

4.1.2 OBJETIVOS

4.1.2.1 Objetivo General

Diseñar e Implementar la red propuesta con Topología Bus para el monitoreo del tráfico en la misma, utilizando el open source CACTI y el Proxy SQUID con la finalidad de acceder a Internet y así bajar archivos, imágenes, videos, etc., que nos permita visualizar en la gráfica del Cacti el

consumo del Ancho de Banda que se esta efectuando y así poder comparar con los otros diseños de prototipo de redes.

4.1.2.2 Objetivo Especifico

- Diseñar e implementar una red prototipo mediante Topología Bus.

- Proveer la información necesaria para la implementación del laboratorio didáctico.

- Configurar las estaciones de trabajo que son las únicas que se necesitan configurar para el buen funcionamiento de la red y así realizar las pruebas de monitoreo.

- Verificar la interconexión de la red mediante los comandos (ping, trace route).

- Originar pruebas causando inundación en la red.

- Instalar y configurar el Servidor Proxy (véase Anexo 2) para acceso a Internet .

- Instalar y configurar el software CACTI (véase Anexo 1) que realizara la medición del consumo de Ancho de Banda que se esta produciendo en la red.
- Instalar y configurar el iftop que permite monitorear el consumo de Ancho de Banda en tiempo real (véase Anexo 2)

- Interpretar y analizar el tráfico en la red prototipo

4.1.3 DISEÑO DEL PROTOTIPO DE RED MEDIANTE TOPOLOGIA BUS

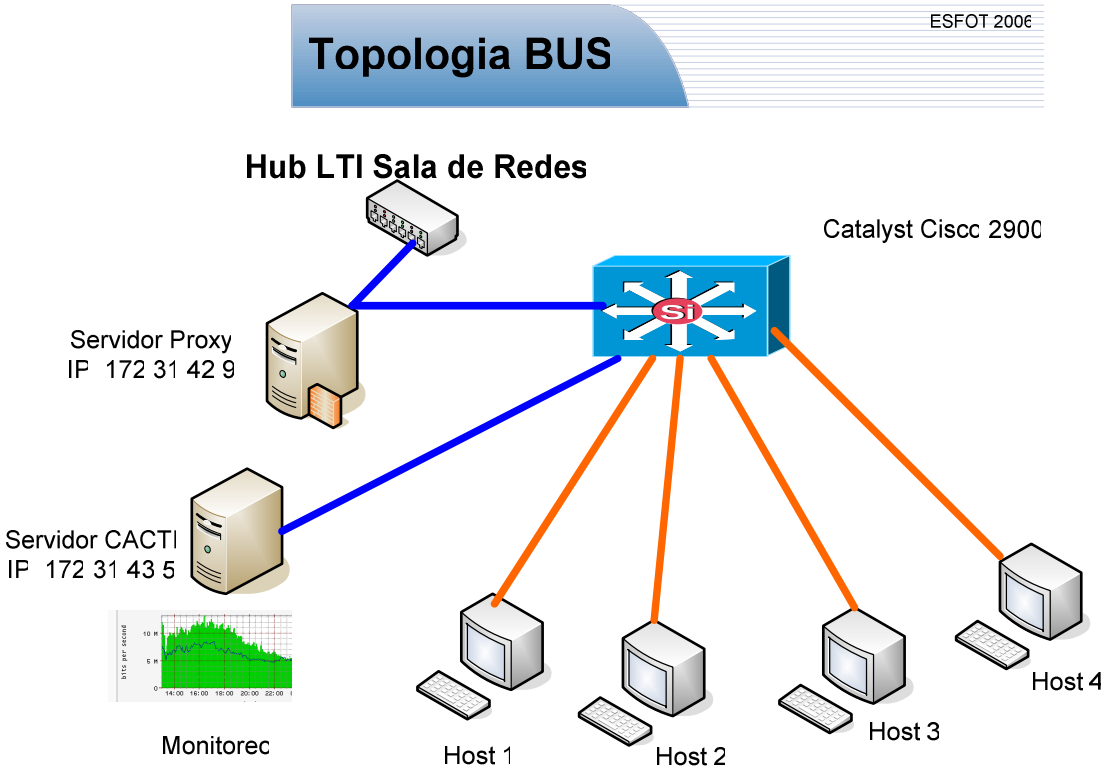


Fig. 49 – Grafica del Cacti

Fuente: Realizado por: Díaz Jeaneth – Tipán Luis

4.1.4 INTERCONEXIONES

La conexión entre dispositivos fue la siguiente:

- De las estaciones de trabajo al switch, cable directo.
- Del Hub al switch, cable directo.
- De los servidores al switch, cable directo.

4.1.5 CONFIGURACION DE LA RED

Una vez realizado el diseño de la red se procede a configurar las estaciones de la siguiente manera:

Dar click derecho en Mis sitios de red

Propiedades

Click derecho en Conexiones de Área Local

Propiedades

Protocolo Internet (TCP/IP)

Propiedades

Aparece la siguiente ventana en donde se configura la Dirección IP (Clase B), Mascara, y Puerta de Enlace, hacer esto en cada estación de trabajo sin repetir las direcciones.

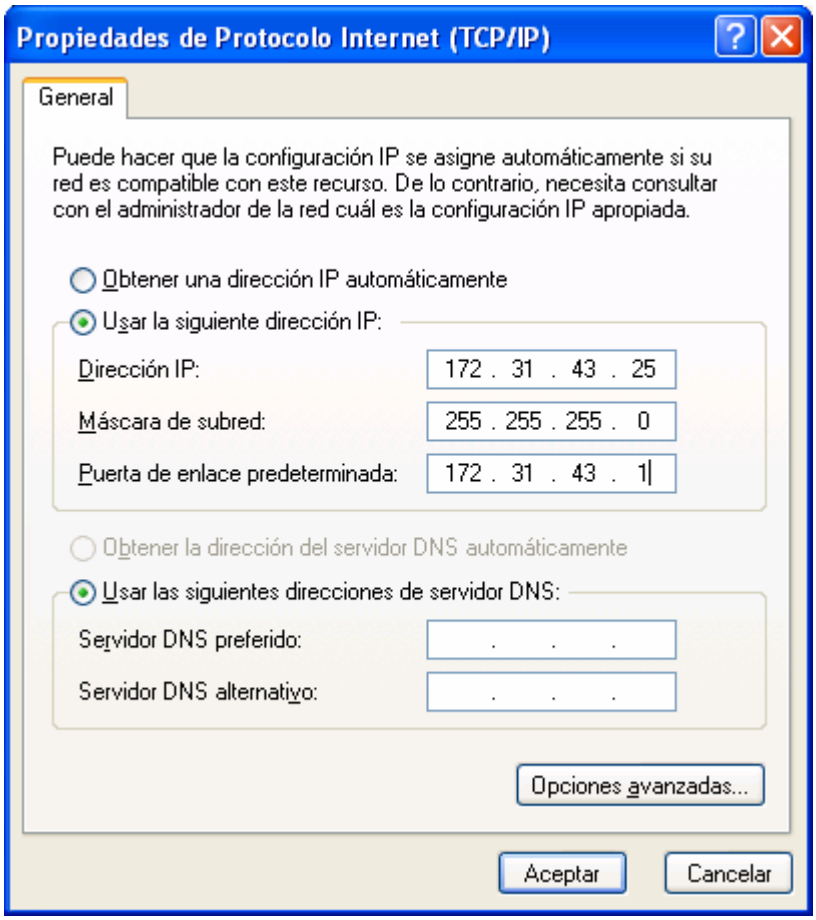


Fig. 50 – Propiedades de Protocolo (TCP/IP)

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

- Conectar la una interface del Proxy (eth0) al switch y la otra interface (eth0/1) al HUB que da acceso a la Polired.
- Abrir una ventana del explorador de Internet:

  Dar click en Herramientas

  Opciones de Internet

  Conexiones

  Configuraciones LAN

Aparece la siguiente ventana en donde se configura la dirección IP del Proxy que nos dará el acceso a Internet.

Realizar esta configuración a todas las estaciones existentes en la red.

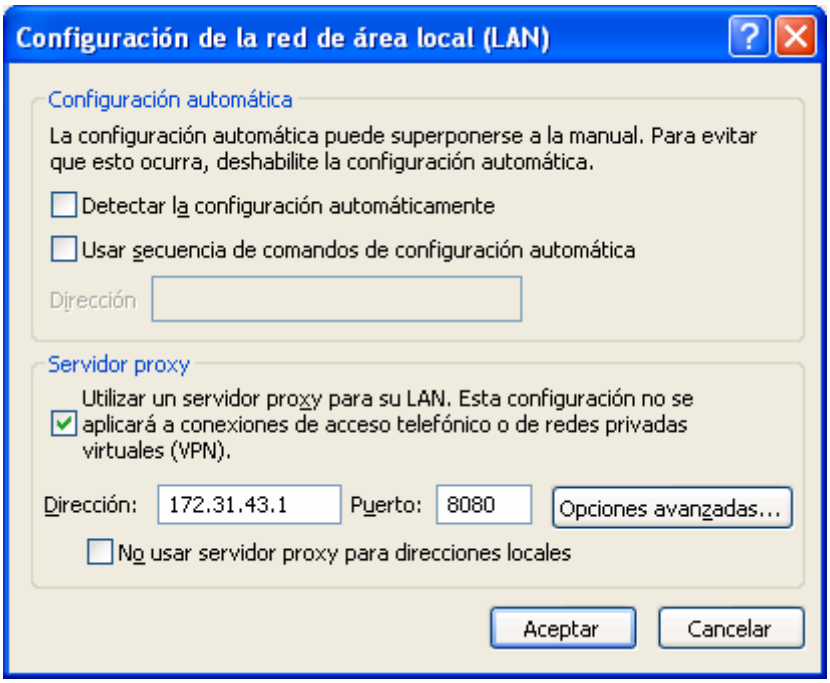


Fig. 51 – Configuración de la red de área local

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

4.1.6 PLAN DE PRUEBAS

El plan de prueba se debe realizar de la siguiente manera:

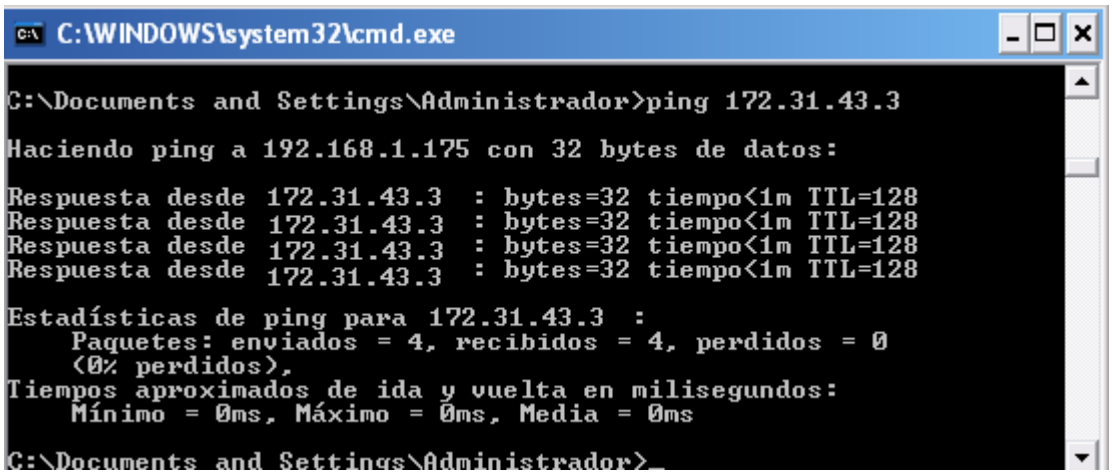


Fig. 52 – Prueba con comando Ping

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

- Dar un ping y esperar respuesta para saber que cada estación tiene conexión en la misma red. Ejemplo ping 172.31.43.3 (dependiendo de la red que se esté probando).
- Descargar toda clase de archivos como por ejemplo: software, videos, música, etc., que permitan inundar la red.
- En la interface gráfica del Cacti (**Fig. 36 – Cacti)** como se va incrementando el consumo que alcance cada estación, ya que nos mostrara cada interface del switch de capa 2 a la que ésta se conecta.
- En el Proxy con el comando iftop –i eth1 verificar en tiempo real lo que sucede con cada estación de trabajo.
- Análisis de la Grafica

4.2 CASO2 - CONFIGURACIÓN E IMPLEMENTACIÓN DEL SWITCH DE CAPA 2 PARA SEGMENTOS DE COLISIÓN EN LA RED CON VLANS

4.2.1 PLANTEAMINETO DEL CASO

En este caso se trata la segmentación de dominios de colisión (**Fig. 17 - Dominios de Colisión)** mediante configuración e implementación de VLAN's usando el Switch Cisco Catalyst 1900. La necesidad de segmentar en dominios de colisión (utilizando Switches de capa 2), se realiza con la finalidad de proporcionar mayor seguridad a la red y mediante VLAN's puedan tener comunicación entre ellas (estaciones de trabajo). Crear guías de estudio que permitan a los estudiantes aplicarlo en sus prácticas y evaluar cada caso.

4.2.2 OBJETIVOS

4.2.2.1 Objetivo General

Esta práctica pretende familiarizar al estudiante con la configuración y administración de una red local basada en conmutadores de capa 2 (switch) y redes locales virtuales (VLANs) (**ver Capitulo 3**). Aunque los detalles concretos de cómo se realizan estas tareas de configuración

dependen del equipo a utilizar. Los aspectos básicos son similares en todos los fabricantes.

La práctica simula una red local que abarca dos dispositivos identificados como: Monitoreo (Switch1) y Monitoreo2 (Switch2). En cada switch se dispone de un conjunto de estaciones de trabajo en la que se crean VLAN's, por ejemplo VLAN1, VLAN10, VLAN803, para cada dispositivo.

4.2.2.2 Objetivo Especifico

- Proveer la información necesaria para la implementación con VLAN's.
- Configurar segmentos de colisión en la red con VLANs.
- Configurar los dispositivos a utilizar (Switch de capa 2, estaciones de trabajo) para el correcto desempeño de la red.
- Comprobar que la red está operando satisfactoriamente con las pruebas necesarias (ping, trace route).
- Originar pruebas, causando inundación en la red mediante transferencia de archivos, imágenes, etc., por cada VLAN existente.
- Instalar y configurar el software CACTI (véase Anexo 1) que realizara la medición del consumo de Ancho de Banda que se esta produciendo en la red.
- Interpretación y análisis del tráfico en la red prototipo

4.2.3 DISEÑO DEL PROTOTIPO DE RED MEDIANTE SWITCH CON VLANS

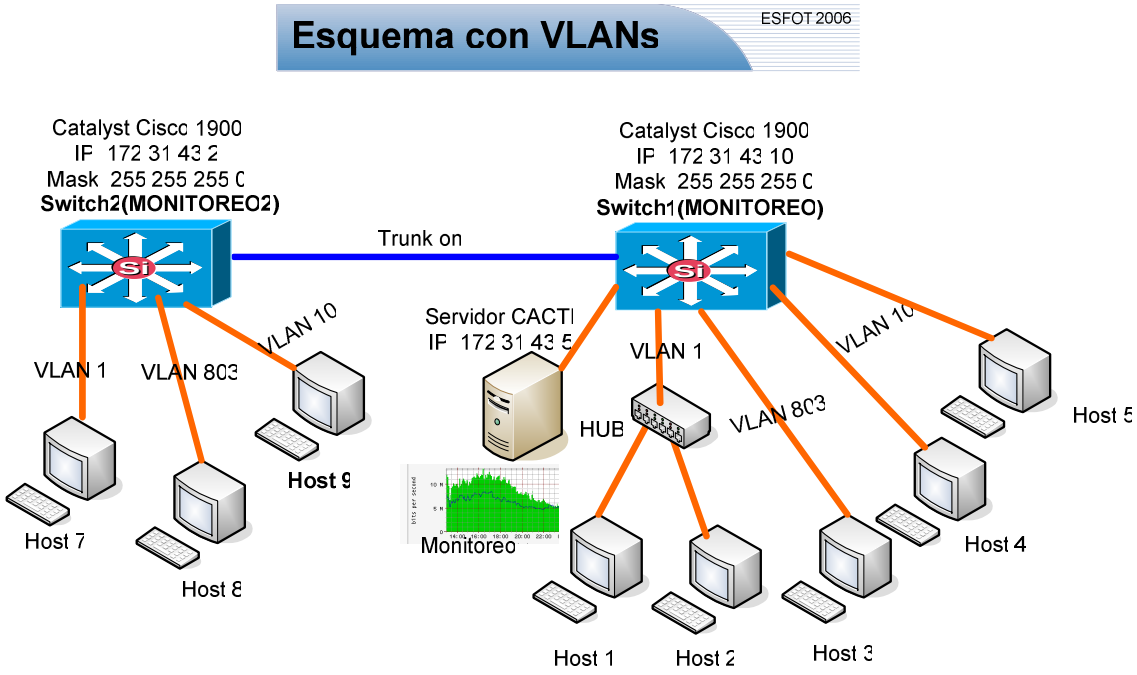


Fig. 53 – Diagrama de red con VLAN's

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

4.2.4 INTERCONEXIONES

La conexión entre los dispositivos fue la siguiente:

- De switch a switch, cable cruzado
- De las estaciones de trabajo al switch cable directo
- Del servidor CACTI al switch, cable directo
- Del switch al PC para conectarse a Hyperterminal, cable de consola

4.2.5 CONFIGURACION DE LA RED MEDIANTE VLAN's

Para este caso de estudio se ha utilizado, switch de capa 2 Catalyst 1900 como se muestra en la siguiente figura.

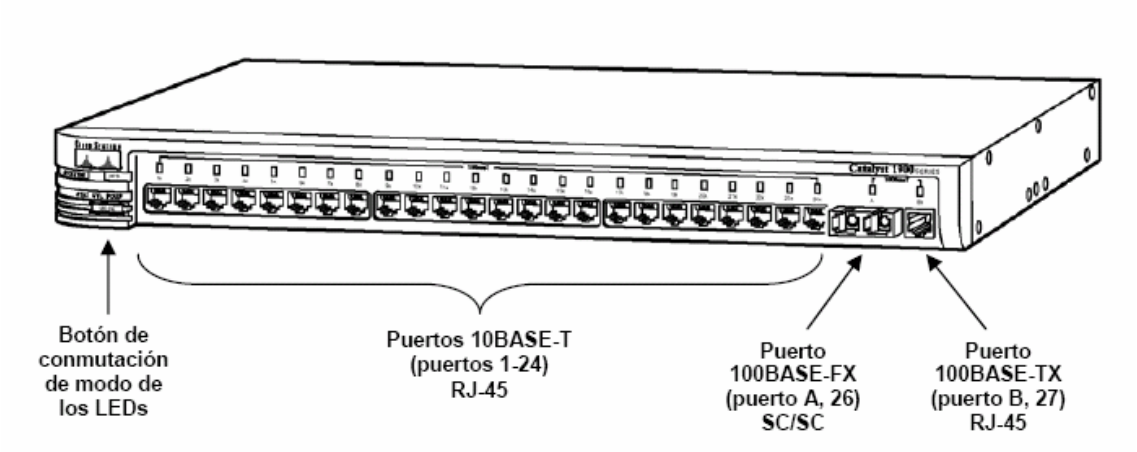


Fig. 54 – Switch Catalyst 1900

Fuente:Realizado por Díaz Jeaneth – Tipán Luis

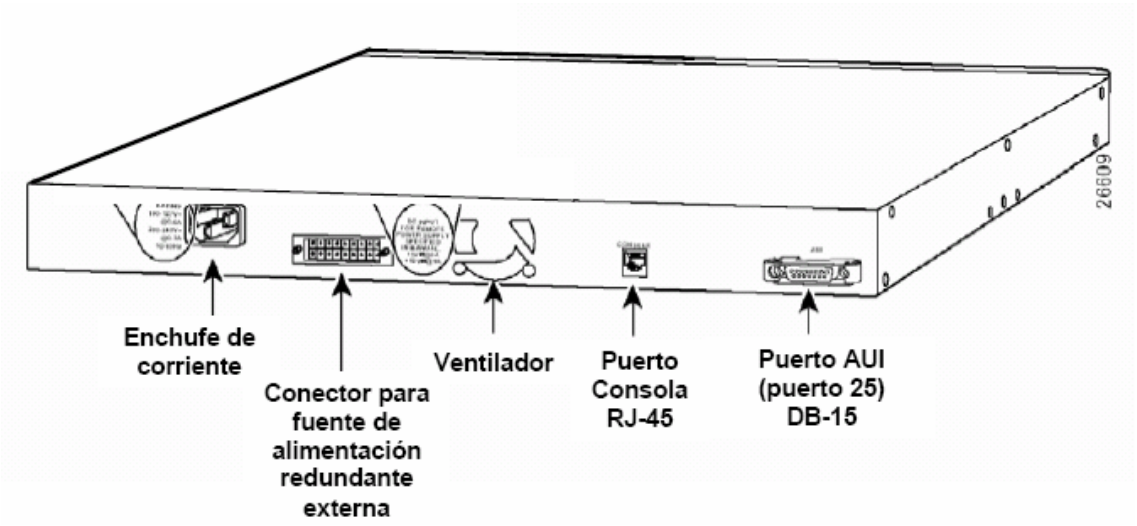


Fig. 55 – Switch Catalyst 1900 (parte tracera)

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

- Un PC conectado con un cable “rollover” (cable de consola) desde el puerto serial y configurado el programa HyperTerminal con las siguientes propiedades:

    - Ingresar a inicio
        - Programas
            - Comunicaciones
                - Hyperterminal

Ahí aparecen las siguientes ventanas las cuales se configuran como muestran las gráficas.

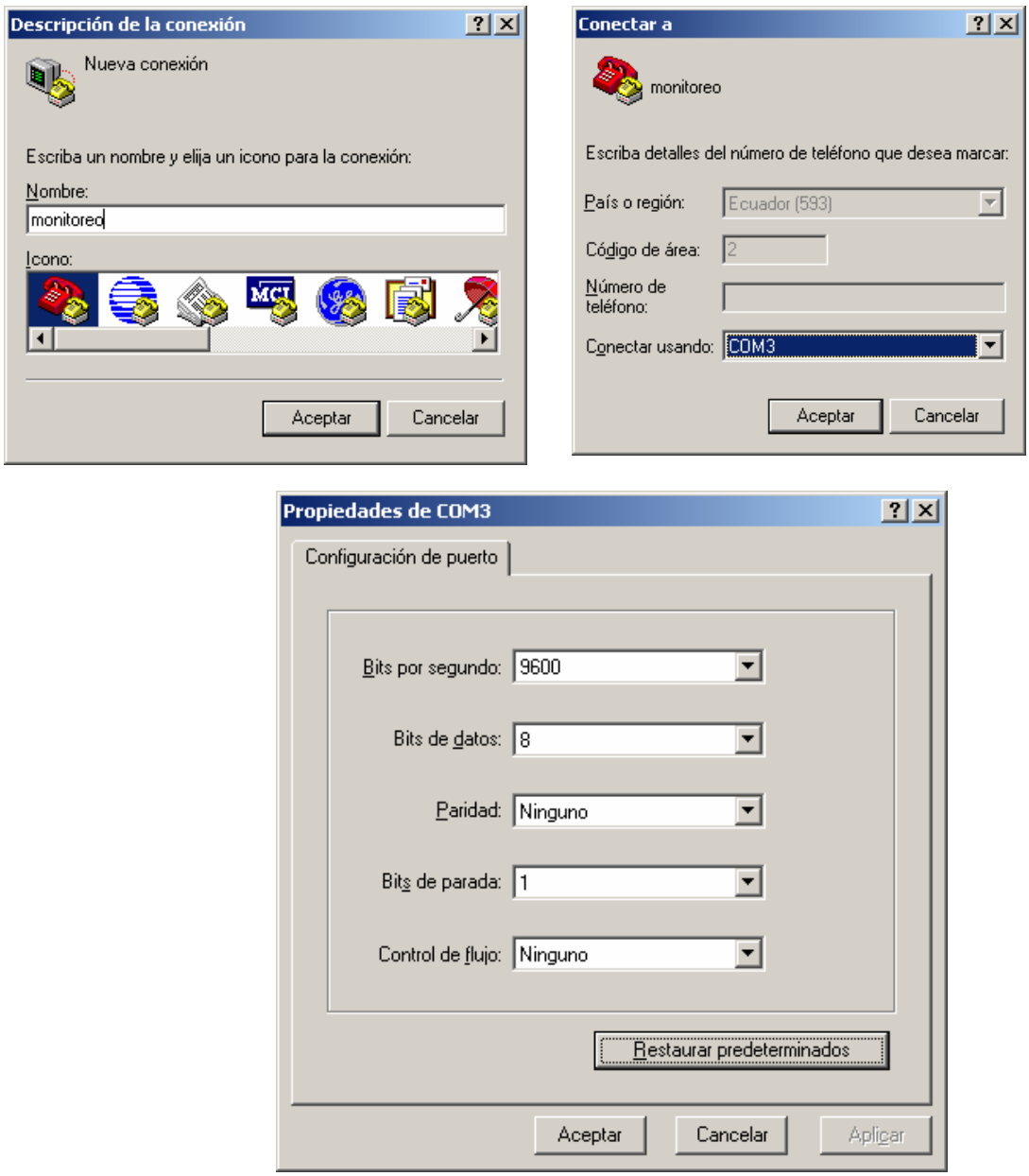


Fig. 56 – Conexión al Hyperterminal

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

- Al conectarse el switch se muestran los datos de hardware y sistema operativo.
- Entrar luego al modo de configuración del sistema para ingresar los parámetros de configuración inicial.

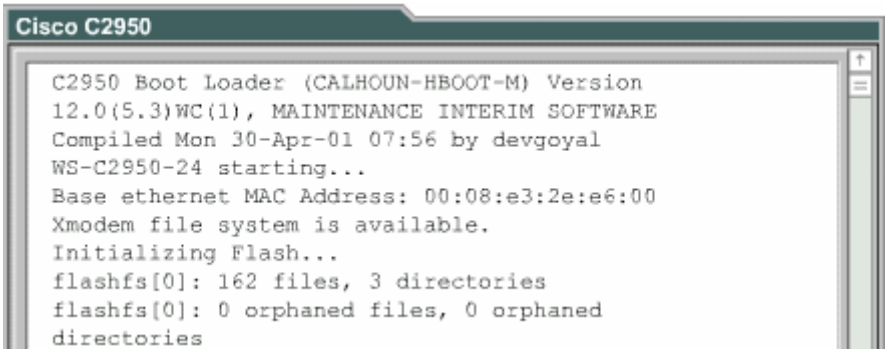


Fig. 57 – Datos del Switch

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

- La CLI (Ingreso a Línea de Comandos) de un switch es muy similar a la presentada por los routers que conocemos.
- La ayuda se invoca con "?"
- Igual que en los routers, la ayuda es sensible al contexto en que se puede obtener de:
  - Todos los comandos
  - Parte de un comando
  - Argumentos requeridos
  - etc.

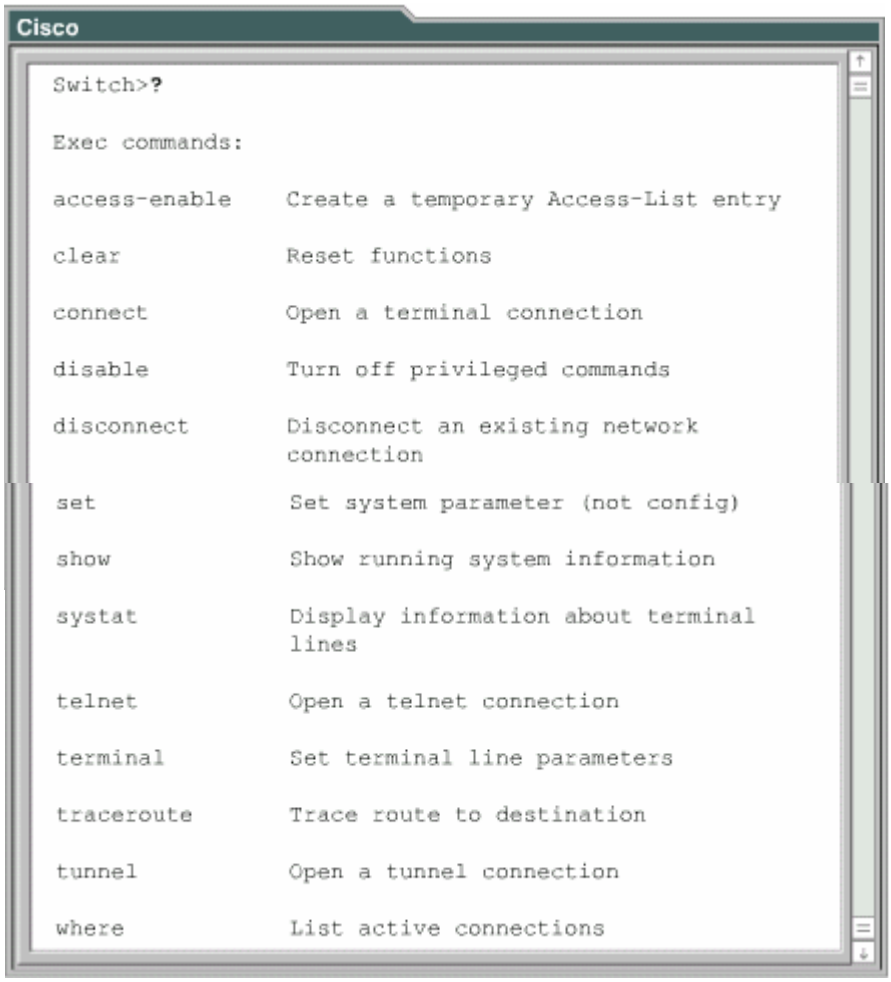


Fig. 58 – Datos del Switch

Fuente:http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1149615860671605,LMSID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=es,Version=1,RootID=knet31AYhFIol4BQhZCAUA,Engine=dynamic/CHAPID=null/RLOID=null/RIOID=null/knet/31AYhFIol4BQhZCAUA/coursetoc.html

- Antes de configurar un switch es necesario asegurarse que no exista una configuración previa (según sea el caso):
  - Borrar las VLANs definidas (delete flash:vlan.dat)
  - Borrar la configuración actual (erase startup-config)
  - Reiniciar el switch (reload)
- Se configura inicialmente el hostname (hostname *nombre*)
- Se determinan los passwords para todas las líneas (console, vty 0 4)
- Los puertos pueden reconfigurarse en velocidad o dirección de flujo (IP, MAC)

4.2.5.1 Administración de la tabla de direcciones MAC

- Los switches aprenden las direcciones MAC de los equipos conectados leyendo la dirección fuente de las tramas que reciben y crean una tabla MAC-puerto en su RAM.
- Por el número de posibles MAC y por que los equipos pueden moverse de puerto o apagarse, las entradas en la tabla son dinámicas, y si no se refrescan en 300 segundos, son eliminadas.
- Para ver el contenido de la tabla, se puede usar el comando:
  - **Show mac-address-table**
- Para limpiar la tabla manualmente, puede usarse el comando
  - **Clear mac-address-table**

4.2.5.2 Comandos para configuración el switch de capa 2 y VLAN's Estáticas

Aquí se muestra toda la configuración realizada en cada Switch.

4.2.5.2.1 Switch1 (MONITOREO)

1 user(s) now active on Management Console.

User Interface Menu

[M] Menus
[K] Command Line

Enter Selection: **k**

CLI session with the switch is open.
To end the CLI session, enter [Exit].

```
>ena
#config t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#hostname MONITOREO
MONITOREO(config)#enable password level 1 cisco
```

MONITOREO(config)#exit
MONITOREO#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.02
Copyright (c) Cisco Systems, Inc. 1993-1998
MONITOREO uptime is 0day(s) 00hour(s) 13minute(s) 34second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-30-80-86-15-40
MONITOREO#config t
Enter configuration commands, one per line. End with CNTL/Z.
MONITOREO(config)#ip add 172.31.43.10 255.255.255.0
MONITOREO(config)#exit
MONITOREO(config)#snmp-server community epn2006esfotasi
MONITOREO(config)#snmp-server contact guille_luigui@hotmail.com
MONITOREO(config)#snmp-server enable traps snmp
MONITOREO(config)#vlan 108 name ESTUDIANTES
MONITOREO(config)#vlan 10 name PROFESORES
MONITOREO(config)#exit
MONITOREO#config t
Enter configuration commands, one per line. End with CNTL/Z.
MONITOREO(config-if)#int e 0/4
MONITOREO(config-if)#vlan-membership static 803
MONITOREO(config-if)#int e 0/6
MONITOREO(config-if)#vlan-membership static 803
MONITOREO(config-if)#int e 0/8
MONITOREO(config-if)#vlan-membership static 803
MONITOREO(config-if)#int e 0/7
MONITOREO(config-if)#vlan-membership static 10
MONITOREO(config-if)#int e 0/9

```
MONITOREO(config-if)#vlan-membership static 10
MONITOREO(config-if)#int e 0/11
MONITOREO(config-if)#vlan-membership static 10
MONITOREO(config-if)#exit
MONITOREO(config)#int fastethernet 0/27
MONITOREO(config-if)#trunk on
MONITOREO(config)#^Z
MONITOREO#sh vlan
VLAN Name                                Status                 Ports
-------------------------------------
1 default                                Enabled                1-3,5,10-13,12-24
                                                                AUI, A, B
10 PROFESORES                            Enabled                7,9,11
803 ESTUDIANTES                          Enabled                4,6,8
1002                                     fddi-default Suspended
1003                                     token-ring-defau Suspended
1004                                     fddinet-default Suspended
1005                                     trnet-default Suspended
-------------------------------------
VLAN  Type    SAID    MTU   Parent  RingNo  BridgeNo Stp Trans1 Trans2
------------------------------------------------------------------------------
1     Ethernet 100001 1500    0       0       0      Unkn  1002  1003
10    Ethernet 100002 1500    0       1       1      Unkn  0     0
803   Ethernet 100003 1500    0       1       1      Unkn  0     0
1002  FDDI     101002 1500    0       0       0      Unkn  1     1003
1003  Token-Ring 101003 1500 1005    1       0      Unkn  1     1002
1004  FDDI-Net 101004 1500    0      0       1      IEEE  0     0
1005  Token-Ring-Net 101005 1500 0    0       1      IEEE  0     0
------------------------------------------------------------------------------
MONITOREO#?
  Exec commands:
  clear          Reset functions
  configure      Enter configuration mode
```

```
  copy            Copy configuration or firmware
  delete          Reset configuration
  disable         Turn off privileged commands
  enable          Turn on privileged commands
  exit            Exit from the EXEC
  help            Description of the interactive help system
  menu            Enter menu interface
  ping            Send echo messages
  reload          Halt and perform warm start
  session         Tunnel to module
  show            Show running system information
  terminal        Set terminal line parameters
  vlan-membership  VLAN membership configuration

MONITOREO#config t
Enter configuration commands, one per line.  End with CNTL/Z.
MONITOREO#show running-config
Building configuration...
Current configuration:
vlan 10 name "PROFESORES" sde 100010 state Operational mtu 1500
vlan 803 name "ESTUDIANTES" sde 100803 state Operational mtu 1500

hostname "MONITOREO"
ip address 172.31.43.10 255.255.255.0
snmp-server community "epn2006esfotasi" ro
snmp-server enable traps bsc
snmp-server contact "guille_luigui@hotmail.com"

enable password level 1 "CISCO"

interface Ethernet 0/1

interface Ethernet 0/2
```

```
interface Ethernet 0/3

interface Ethernet 0/4
  vlan-membership static 803

interface Ethernet 0/5

interface Ethernet 0/6
vlan-membership static 803

interface Ethernet 0/7
  vlan-membership static 10

interface Ethernet 0/8
  vlan-membership static 803

interface Ethernet 0/9
  vlan-membership static 10

interface Ethernet 0/10

interface Ethernet 0/11
  vlan-membership static 10

 interface Ethernet 0/12

interface Ethernet 0/13

interface Ethernet 0/14

interface Ethernet 0/15
interface Ethernet 0/16
```

interface Ethernet 0/17

interface Ethernet 0/18

interface Ethernet 0/19

interface Ethernet 0/20

interface Ethernet 0/21

interface Ethernet 0/22

interface Ethernet 0/23

interface Ethernet 0/24

interface Ethernet 0/25
interface FastEthernet 0/26

interface FastEthernet 0/27

trunk On

line console
end

4.2.5.2.2 Switch2 (MONITOREO2)

1 user(s) now active on Management Console.

User Interface Menu

[M] Menus
[K] Command Line

```
Enter Selection:k

    CLI session with the switch is open.
    To end the CLI session, enter [Exit].
>ena
#config t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#hostname MONITOREO2

MONITOREO2(config)#enable password level 1 cisco
MONITOREO2(config)#exit
MONITOREO2#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V8.01.02
Copyright (c) Cisco Systems, Inc.  1993-1998
MONITOREO2 uptime is 0day(s) 00hour(s) 13minute(s) 34second(s)
cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-30-80-86-15-40
MONITOREO2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
MONITOREO2(config)#ip add 172.31.43.2 255.255.255.0
MONITOREO2(config)#exit
MONITOREO2(config)#snmp-server community epn2006esfotasi
MONITOREO2(config)#snmp-server contact guille_luigui@hotmail.com
MONITOREO2(config)#snmp-server enable traps snmp
MONITOREO2(config)#vlan 108 name ESTUDIANTES
MONITOREO2(config)#vlan 10 name PROFESORES
MONITOREO2(config)#exit
MONITOREO2#config t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
MONITOREO2(config-if)#int e 0/5
MONITOREO2(config-if)#vlan-membership static 803
MONITOREO2(config-if)#int e 0/14
MONITOREO2(config-if)#vlan-membership static 803
MONITOREO2(config-if)#int e 0/8
MONITOREO2(config-if)#vlan-membership static 10
MONITOREO2(config-if)#int e 0/15
MONITOREO2(config-if)#vlan-membership static 10
MONITOREO2(config-if)#exit
MONITOREO2(config)#int fastethernet 0/27
MONITOREO2(config-if)#trunk on
MONITOREO2(config)#^Z
MONITOREO2#sh vlan
VLAN Name                              Status                 Ports
-------------------------------------
1  default                             Enabled                1-7,9-13,16-24
                                                              AUI, A, B
10 PROFESORES                          Enabled                8,15
803 ESTUDIANTES                        Enabled                5,14
1002                                   fddi-default Suspended
1003                                   token-ring-defau Suspended
1004                                   fddinet-default Suspended
1005                                   trnet-default Suspended
-------------------------------------
VLAN  Type    SAID    MTU   Parent  RingNo  BridgeNo Stp Trans1 Trans2
------------------------------------------------------------------------
1     Ethernet 100001 1500    0       0       0      Unkn  1002  1003
10    Ethernet 100002 1500    0       1       1      Unkn  0     0
803   Ethernet 100003 1500    0       1       1      Unkn  0     0
1002  FDDI     101002 1500    0       0       0      Unkn  1     1003
1003  Token-Ring 101003 1500 1005    1       0      Unkn  1     1002
1004  FDDI-Net 101004 1500    0       0       1      IEEE  0     0
```

```
1005    Token-Ring-Net 101005 1500 0        0           1      IEEE     0      0
------------------------------------------------------------------------------
MONITOREO2#?
  Exec commands:
  clear             Reset functions
  configure         Enter configuration mode
  copy              Copy configuration or firmware
  delete            Reset configuration
  disable           Turn off privileged commands
  enable            Turn on privileged commands
  exit              Exit from the EXEC
  help              Description of the interactive help system
  menu              Enter menu interface
  ping              Send echo messages
  reload            Halt and perform warm start
  session           Tunnel to module
  show              Show running system information
  terminal          Set terminal line parameters
  vlan-membership   VLAN membership configuration

MONITOREO2#sh run
Building configuration...
Current configuration:
vlan 10 name "PROFESORES" sde 100010 state Operational mtu 1500
vlan 803 name "ESTUDIANTES" sde 100803 state Operational mtu 1500

hostname "MONITOREO2"
ip address 172.31.43.2 255.255.255.0
snmp-server community "epn2006esfotasi" ro
snmp-server enable traps bsc
snmp-server contact "guille_luigui@hotmail.com"

enable password level 1 "CISCO"
```

```
interface Ethernet 0/1

interface Ethernet 0/2

interface Ethernet 0/3

interface Ethernet 0/4

interface Ethernet 0/5
  vlan-membership static 803

interface Ethernet 0/6

interface Ethernet 0/7

interface Ethernet 0/8
  vlan-membership static 10

interface Ethernet 0/9

interface Ethernet 0/10

interface Ethernet 0/11

 interface Ethernet 0/12

interface Ethernet 0/13

interface Ethernet 0/14
  vlan-membership static 803

interface Ethernet 0/15
```

```
  vlan-membership static 10

interface Ethernet 0/16

interface Ethernet 0/17

interface Ethernet 0/18

interface Ethernet 0/19

interface Ethernet 0/20

interface Ethernet 0/21

interface Ethernet 0/22

interface Ethernet 0/23

interface Ethernet 0/24

interface Ethernet 0/25
interface FastEthernet 0/26

interface FastEthernet 0/27

  trunk On

line console
end
```

4.2.6 PLAN DE PRUEBAS

- Se procedió a verificar si existe comunicación entre Vlans mediante el comando Ping.
- Instalación de un Software libre llamado Messenger que no necesita conexión a Internet para comunicarse a todas las estaciones de trabajo.(en este caso de estudio no utilizaremos el Proxy por motivo de seguridad en la Vlans que no permite el acceso a Internet)
- Empezar a enviar información, archivos, imágenes, programas, etc.
- Verificar en la grafica del Cacti como se va incrementando el consumo en la red interna.

4.2.7 RECOMENDACIONES

- Un administrador debe documentar y mantener los archivos de configuración actuales de los equipos de red
- Se debe respaldar siempre en un servidor o un disco el archivo de configuración activo para cuando hayan problemas de que requieran volver a cargarlo en RAM. Es un archivo pequeño.
  - **Copy running-config tftp**
- Además debe respaldarse también el archivo de la imagen de IOS actual para igual propósito. Su tamaño es mucho mayor.
  - **Copy flash tftp**

4.3 CASO3 - CONFIGURACIÓN E IMPLEMENTACIÓN DEL ROUTER PARA GESTIONAR DOMINIOS DE COLISIÓN Y BROADCAST EN LA RED

4.3.1 PLANTEAMIENTO DEL CASO

La configuración e implementación del router para gestionar dominios de colisión y broadcast, se generó para mejorar la eficiencia de la red, disminuyendo colisiones y broadcast existentes en la red.

Elaborar guías de estudio para los estudiantes, con el propósito de ayudar a incrementar sus conocimientos en redes y facilitar el manejo de las configuraciones de: routers, switches, estaciones de trabajo y servidores.

4.3.2 OBJETIVOS

4.3.2.1 Objetivo General

El objetivo de ésta práctica es suministrar al alumno con guías de estudio que sean útiles para el manejo de la configuración y gestión de una red local basada en dispositivos como: switch y router. Aunque los detalles concretos de cómo se realizan estas tareas dependen del equipo utilizado, los aspectos básicos son similares en todos los fabricantes.

La práctica representa el establecimiento de una red local que abarca dos Routers denominados Router1 y Router2.

En cada Router se dispone de un switch, hub y un conjunto de estaciones de trabajo, además de los servidores CACTI y PROXY.

4.3.2.2 Objetivo Especifico

- Proveer la información necesaria para la creación de los laboratorios didácticos

- Configurar y gestionar dominios de colisión y broadcast en la red utilizando routers.

- Configurar los dispositivos ha utilizar (router, switch, estaciones de trabajo) para el correcto desempeño de la red.

- Verificar que la red esta actuando satisfactoriamente con las pruebas necesarias (ping, trace route).

- Instalar y configurar el Servidor Proxy (véase Anexo 2) para acceso a Internet .

- Instalar y configurar el software CACTI (véase Anexo 1) que realizara la medición del consumo de Ancho de Banda que se esta produciendo en la red.

- Instalar y configurar el iftop que permite monitorear el consumo de Ancho de Banda en tiempo real (véase Anexo 2)

- Originar pruebas, causando inundación en la red mediante transferencia y descargas de archivos, imágenes, etc.

- Interpretación y análisis del tráfico en la red prototipo

4.3.3 DISEÑO DEL PROTOTIPO DE RED UTILIZANDO ROUTERS

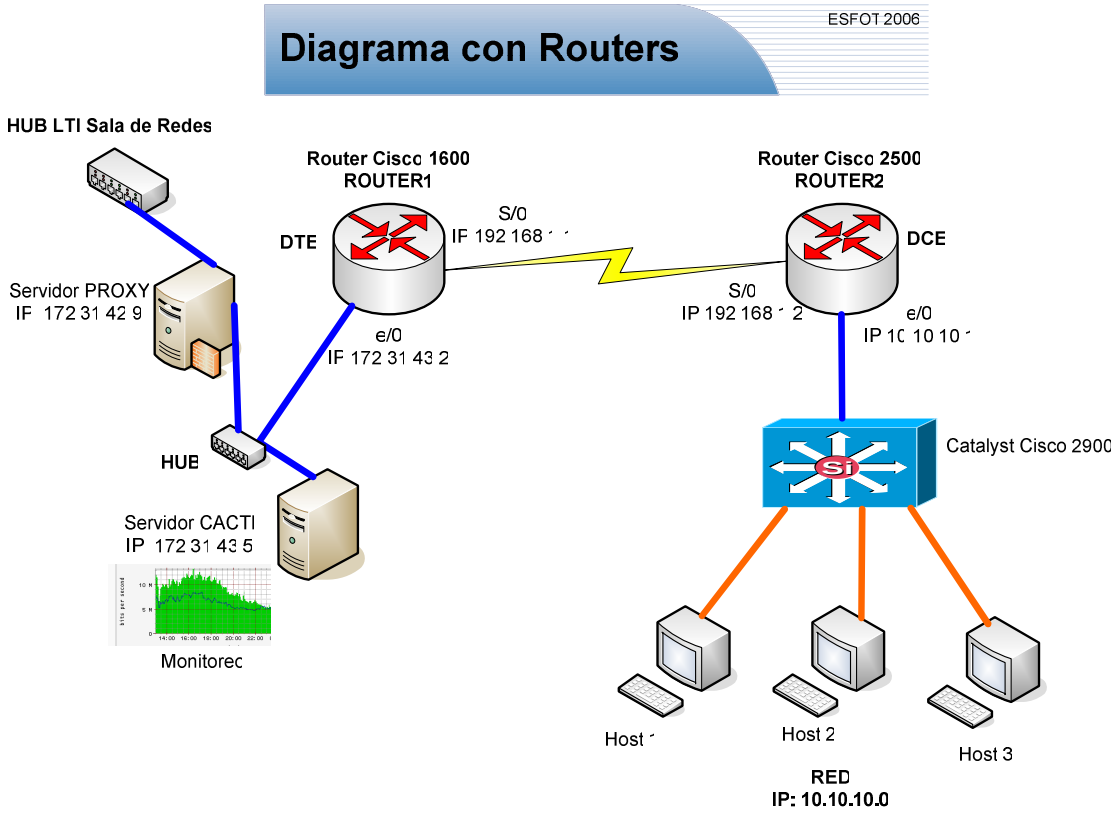


Fig. 59 – Diagrama con Routers

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

4.3.4 INTERCONECCIONES

- De Router a PC para administrar, cable de consola.
- De Router a Switch, cable directo.
- Del Switch a las estaciones de trabajo, cable directo.
- De Router a Hub, cable directo.
- De Switch a servidores, cable directo.
- De Hub a Servidores, cable directo.

4.3.5 CONFIGURACION DE LA RED CON ROUTERS

Una internetwork correctamente configurada brinda lo siguiente:

- Direccionamiento coherente de extremo a extremo
- Direcciones que representan topologías de red
- Selección de la mejor ruta
- Enrutamiento estático o dinámico.
- Conmutación.

Para conectar un PC a un router:

1. Configure el software de emulación (Hyperterminal) en el PC (**véase en caso 1**)para:
    - El puerto com adecuado
    - 9600 baudios
    - 8 bits de datos
    - Sin paridad
    - 1 bit de parada
    - Sin control de flujo
2. Conecte el conector RJ-45 del cable transpuesto al puerto de consola del router.
3. Conecte el otro extremo del cable transpuesto al adaptador RJ-45 a DB-9.

4. Conecte el adaptador DB-9 hembra al PC.

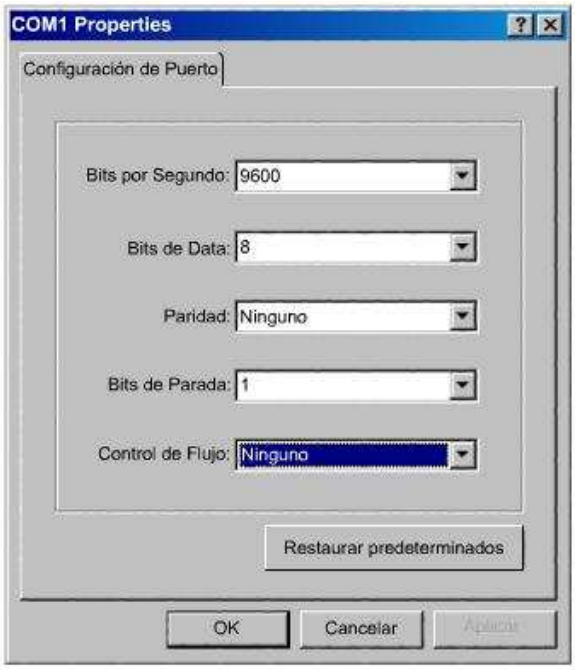


Fig. 60 – Propiedades para la conexión al Hyperterminal

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

Pasos para la configuración del Router

1. Primero debemos ingresar a:

   Router>**enable**
   Router#**config terminal**

2. Se debe asignar un nombre exclusivo al router, como la primera tarea de configuración. Esto se realiza en el modo de configuración global, mediante los siguientes comandos:

   Router(config)#**hostname EPN**
   EPN(config)#

3. Asignación de contraseñas.
   - Router(config)#**line console 0**
   - Router(config-line)#password cisco
   - Router(config-line)#**login**
   - Router(config)#**line vty 0 4**

- Router(config-line)#password cisco
- Router(config-line)#**login**
- Router(config)#**enable secret class**

Vty (terminales virtuales), para habilitar el acceso remoto de usuarios al router mediante Telnet.

4. A cada interfaz serial activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP. Configure la dirección de IP mediante los siguientes comandos:

   Router(config)#**interface serial 0/0**
   Router(config-if)#**ip address 192.168.1.1 255.255.255.0**
   Router(config-if)# **no shutdown**

   Si es DCE se configure asi:

   Router(config)#**interface serial 0/0**
   Router(config-if)#**ip add 192.168.1.2 255.255.255.0**
   Router(config-if)#**clock rate 56000**
   Router(config-if)#**no shutdown**

5. A cada interfaz Ethernet activa se le debe asignar una dirección de IP y la correspondiente máscara de subred, si se requiere que la interfaz enrute paquetes de IP.

   Router(config)#**interface ethernet 0**
   Router(config-if)#**ip address 192.168.16.1 255.255.255.0**
   Router(config-if)# **no shutdown**

6. Cuando se ha configurado siempre se debe guardar los cambios realizados mediante el siguiente comando.

   Router#**copy running-config startup-config**

7. Para poder usar nombres de host para comunicarse con otros dispositivos de IP, los dispositivos de red, como los routers, deben poder vincular los

nombres de host con las direcciones de IP. En este comando se debe incluir todas la ip que se encuentran alrededor del router.

Router(config)#**ip hosts EPN 192.168.16.2**

4.3.5.1 Comandos para configuración el Router de capa 3

4.3.5.1.1 Router Cisco 1600 (Router1)

```
Router>ena
Router#conf t
Router(config)#hostname ROUTER1
ROUTER1(config)#enable secret class
ROUTER1(config)#line console 0
ROUTER1(config)#password cisco
ROUTER1(config)#login
ROUTER1(config)#line vty 0 4
ROUTER1(config)#password cisco
ROUTER1(config)#login
ROUTER1(config)#int ethernet 0
ROUTER1(config-if)#ip add 172.31.43.2 255.255.255.0
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#int serial 0
ROUTER1(config-if)#ip add 192.168.1.1 255.255.255.0
ROUTER1(config-if)#no shutdown
ROUTER1(config-if)#exit
ROUTER1(config)#router rip
ROUTER1(config)#network 10.10.10.0
ROUTER1(config)#network 192.168.1.0
ROUTER1(config)#network 172.31.43.0
ROUTER1(config)#ip default-gateway 172.31.43.2
ROUTER1#copy run star
ROUTER1#show version
```

```
ROUTER1(config)#snmp-server community epn2006esfotasi
ROUTER1(config)#snmp-server contact jvividinar@hotmail.com
ROUTER1(config)#snmp-server enable traps snmp
ROUTER1(config)#snmp-server hosts 172.31.43.2 WORD
ROUTER1#sh run
Current configuration:
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname ROUTER1
enable secret 5 $1$0hKz$JqX37MTKRLOf/zuDTvoJg0

ip subnet-zero

interface Ethernet0
ip address 172.31.43.2 255.255.255.0
interface Serial0
ip address 192.168.1.1 255.255.255.0
no fair-queue

router rip
network 10.0.0.0
network 172.31.0.0
network 192.168.1.0

ip default-gateway 172.31.43.2
ip classless
ip route 172.31.0.0 255.255.0.0 172.31.43.0
no ip http server

snmp-server engineID local 00000009020000021660 82FC
snmp-server community epn2006esfotasi RO
```

```
snmp-server community WORD view v1default RO
snmp-server contact jvividinar@hotmail.com
snmp-server enable traps snmp
snmp-server host 172.31.43.2 WORD

line con 0
ip default-gateway 172.31.43.2
ip classless
ip route 172.31.0.0 255.255.0.0 172.31.43.0
no ip http server

snmp-server engineID local 00000009020000021660 82FC
snmp-server community epn2006esfotasi RO
snmp-server community WORD view v1default RO
snmp-server contact jvividinar@hotmail.com
snmp-server enable traps snmp
snmp-server host 172.31.43.2 WORD
line con 0
password cisco
login
transport input none
line vty 0 4
password cisco
login

end
```

4.3.5.1.2 Router Cisco 1600 (Router1)

```
Router>ena
Router#conf t
Router(config)#hostname ROUTER2
ROUTER2(config)#enable secret class
ROUTER2(config)#line console 0
```

ROUTER2(config)#password cisco
ROUTER2(config)#login
ROUTER2(config)#line vty 0 4
ROUTER2(config)#password cisco
ROUTER2(config)#login
ROUTER2(config)#int ethernet 0
ROUTER2(config-if)#ip add 10.10.10.1 255.255.255.0
ROUTER2(config-if)#no shutdown
ROUTER2(config-if)#exit
ROUTER2(config)#int serial 0
ROUTER2(config-if)#ip add 192.168.1.2 255.255.255.0
ROUTER2(config-if)#clock rate 56000
ROUTER2(config-if)#no shutdown
ROUTER2(config-if)#exit
ROUTER2(config)#router rip
ROUTER2(config)#network 10.10.10.0
ROUTER2(config)#network 192.168.1.0
ROUTER2(config)#network 172.31.43.0
ROUTER2#copy run star
ROUTER2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
ROUTER2#copy run star
ROUTER2#show version
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-I-L), Version 11.0(16), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Tue 24-Jun-97 12:20 by jaturner
Image text-base: 0x0301E644, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
ROM: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (f
c1)

```
ROUTER2 uptime is 0 minutes
System restarted by power-on
System image file is "flash:igs-i-l.110-16", booted via flash

cisco 2500 (68030) processor (revision D) with 8192K/2048K bytes of memory.
Processor board ID 03256116, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

ROUTER2#show run
ROUTER2#show running-config
Building configuration...
Current configuration:
version 11.0
service udp-small-servers
service tcp-small-servers

hostname ROUTER2

enable secret 5 $1$dJPb$PaE636tGXiXt1DXWqqXyW0

interface Ethernet0
 ip address 10.10.10.1 255.255.255.0

interface Serial0
 ip address 192.168.1.2 255.255.255.0
 no fair-queue
```

```
 clockrate 56000
interface Serial1
 no ip address
 shutdown

interface Serial1
 no ip address
 shutdown

router rip
 network 192.168.1.0
 network 172.31.0.0
 network 10.0.0.0

ip route 0.0.0.0 0.0.0.0 192.168.1.1

line con 0
 password cisco
 login
line aux 0
 transport input all
line vty 0 4
 password cisco
 login
end
```

4.3.6 PLAN DE PRUEBAS

- Se procedió a configurar las estaciones de trabajo con el rango de direcciones 10.10.10.0
- Probar conectividad mediante el comando ping desde el Router y Proxy a todas las direcciones de Clase A (10.10.10.0), Clase B (172.31.43.0), Clase C (192.168.1.0).

- Abrir una ventana del Internet Explorer y como se mencionó en la práctica del caso uno, configurar la dirección del Proxy para tener acceso a la Web.
- Descargar archivos, imágenes, videos, etc., que provoquen trafico en la red
- Instalar y configurar el Servidor Proxy (véase Anexo 2) para acceso a Internet.
- Instalar y configurar el software CACTI (véase Anexo 1) que realizará la medición del consumo de Ancho de Banda que se esta produciendo en la red.
- Instalar y configurar el iftop, que permite monitorear el consumo de Ancho de Banda en tiempo real (véase Anexo 2)

CAPITULO V – CONCLUSIONES Y RECOMENDACIONES GENERALES

5.1 CONCLUSIONES

El diseño cumplió con las expectativas para el cual se formuló el proyecto, de esta manera logrando el objetivo principal el cual era Elaborar e Implementar laboratorios didácticos para monitoreo del tráfico en la red, antes y después de segmentar en dominios de colisión y broadcast utilizando el open source CACTI, en forma rápida, fácil, y económica ya que se contó con los dispositivos que nos proporcionó el laboratorio del LTI, atendiendo a los estándares internacionales vigentes en cuanto a requerimientos en la interconexión de equipos en un ambiente de trabajo reducido y de esta manera obtener todas las potencialidades de una red Lan, sin dejar de lado los costos de los materiales ya que si estos no son comprendidos y llevados a la práctica; nuestra red quedara rápidamente fuera de uso; en síntesis lo básico es saber escoger un tipo de red según las características del lugar a instalar, elegir los protocolos a utilizar y elegir correctamente el sistema operativo de red.

La utilización de switches, routers, evidencia la disminución de dominios de colisión y broadcast determinado a través de los sistemas de monitoreo Cacti y los instalados en el Proxy Squid mediante el uso del (iftop).

Debido a la gran importancia que hoy tienen las redes de datos LAN/WAN en la productividad y eficiencia de las empresas, es indispensable contar con la Plataforma de Conectividad y Comunicaciones que nos asegure un acceso rápido a las Bases de Datos, mejore el desempeño de las aplicaciones y nos brinde seguridad en base a Sistemas de Respaldo y Plan de Contingencia ante catástrofes.

El crecimiento constante y la incorporación de nuevas tecnologías, gradualmente van complicando y muchas veces degradando la disponibilidad de la red. Por esta razón Cacti ofrece el servicio de “Análisis y Monitoreo de Redes”, orientado prevenir y a plantear soluciones concretas ante nuevos problemas o requerimientos y, de este modo asegurar la estabilidad, operabilidad y flexibilidad.

Este servicio está basado en tecnología de Análisis experto, que diagnostican automáticamente su red, proponiendo incluso soluciones.

Para brindar el mejor servicio en el control y mantención de la Red y ser un apoyo real en la incorporación de las soluciones tecnológicas, se propone un Plan de Asesoría basado en Análisis y Mediciones.

5.2 RECOMENDACIONES

Se recomienda independizar al laboratorio designado para los estudiantes de ASI de los equipos y configuraciones actualmente existentes, ya que de esta manera se podrán realizar laboratorios con mayor rapidez y determinar inconvenientes de red interna o externa.

A través de los manuales implementados en este trabajo los estudiantes podrán levantar (realizar), los servidores del proyecto presentado, de esta manera tenerlos en funcionamiento y obtener resultados para analizarlos, con lo cual el estudiante obtendrá una visión de lo que realmente se encuentra en las redes de grandes dimensiones.

Se recomienda en un futuro, para la realización de este tema, aumentar un Script en el Proxy Squid donde con pulsar un botón el administrador pueda bloquear el ingreso a los estudiantes o usuarios que provoquen elevado consumo en la red y así evitar tráfico en la misma, siendo otra forma de control en la red.

Para el caso de estudio 3 se recomienda el crear otro servidor Cacti para monitorear el consumo interno como lo externo de la red como se muestra en la figura siguiente:

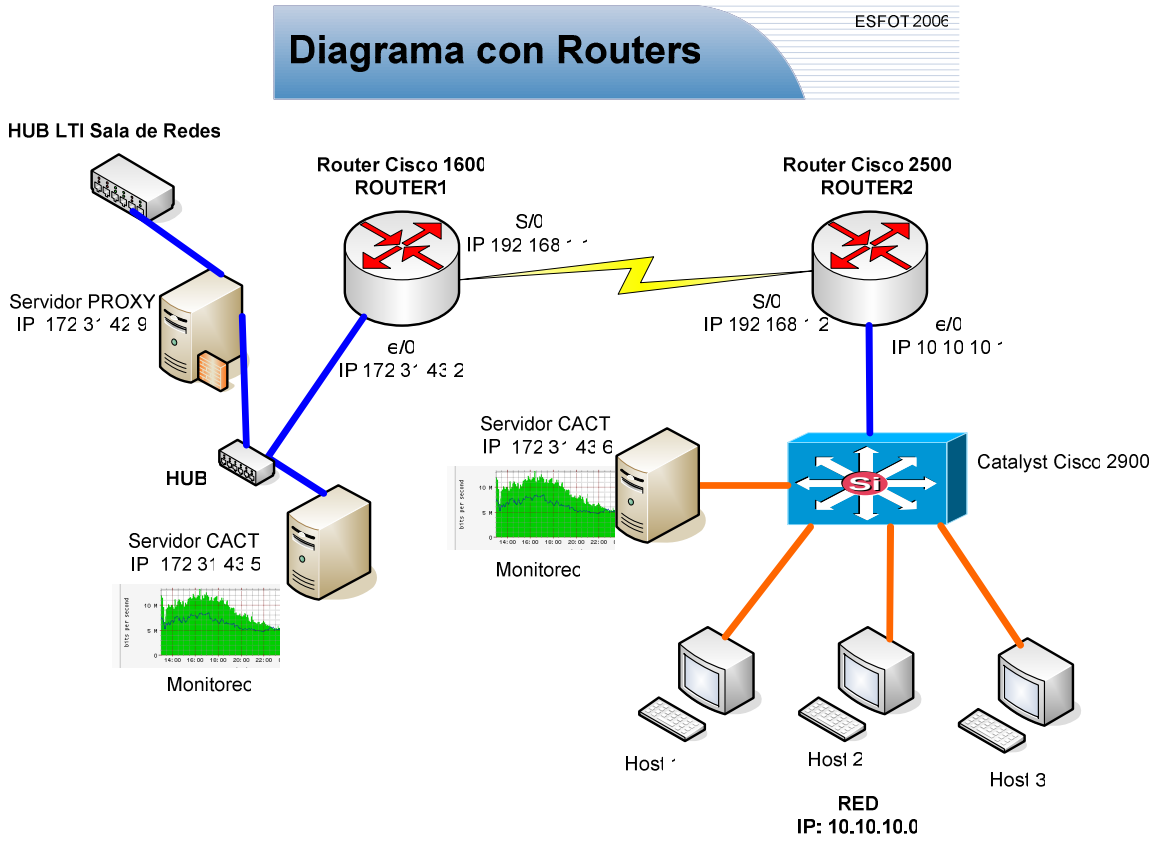


Fig. 61 – Recomendación para el Diagrama con Routers

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

BIBLIOGRAFIA

http://www.numaboa.com.br/informatica/internet/topoLan.php
http://www.geocities.com/TimesSquare/Chasm/7990/topologi.htm
http://www2.canalaudiovisual.com/ezine/books/acREDES/2redes05.htm
http://64.233.179.104/translate_c?hl=es&u=http://www.cacti.net/features.php&prev=/search%3Fq%3Dque%2Bes%2Bel%2Bsoftware%2Bcacti%26hl%3Des%26lr%3D%26sa%3DG
http://64.233.179.104/translate_c?hl=es&u=http://www.cacti.net/what_is_cacti.php&prev=/search%3Fq%3Dque%2Bes%2Bel%2Bsoftware%2Bcacti%26hl%3Des%26lr%3D%26sa%3DG
http://www.htmlweb.net/redes/topologia/topologia_3.html
http://www.netmedia.info/netmedia/articulos.php?id_sec=30&id_art=1294
http://www.monografias.com/trabajos7/swich/swich.shtml
http://www.inaoep.mx/~moises/AGC/sw-rout.html#tecsw
http://translate.google.com/translate?hl=es&sl=en&u=http://www.enterprisenetworkingplanet.com/netos/article.php/3605536&prev=/search%3Fq%3Dque%2Bes%2Bel%2Bsoftware%2Bcacti%26hl%3Des%26lr%3D%26sa%3DG
http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm
http://html.rincondelvago.com/redes_5.html
http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link7
http://www.faq-mac.com/mt/archives/003468.php
http://www.informatizate.net/articulos/proxy_buen_punto_20030822.html

GLOSARIO

Segmento.- Un segmento es un grupo de dispositivos tales como (PCs, servidores, etc) que están conectados entre sí.

Segmentar.- Segmentar es el proceso de separar ciertas partes de tráfico de la red, por razones de rendimiento, seguridad o fiabilidad. Se puede utilizar un switch o un router para separar los dispositivos de la red en segmentos.

Colisión.- Una colisión es cuando dos paquetes de datos están intentando usar el mismo medio de transmisión de manera simultanea es decir al mismo tiempo.

Gestionar.- Administrar o dirigir la red

Estrés del canal o inundación del canal.- Estado causado por el exceso de paquetes en la red

Tarjeta RDSI.- Tarjeta que permite la conexión a Internet a través de una línea RDSI, sustituiría al módem que conocemos, se instala en el interior del ordenador como cualquier otra tarjeta y el usuario realizará a través de ella la conexión a Internet. La velocidad de conexión que podremos alcanzar con una RDSI sería de 64 Kbps, si nuestro servidor nos permite utilizar los dos canales podremos alcanzar una velocidad de 128 Kbps.

Difusión.- Difusión a todas las computadoras de una red remota que se logra enviando una sola copia del paquete a la red remota y difundiéndolo al llegar. El TCP/IP maneja difusión dirigida.

Protocolo.- Conjunto de comandos que permite que dos computadoras se comuniquen entre si.

Comunicación bidireccional.- es aquélla en la cual puede ser enviada información tanto desde un trasmisor hacia un receptor como desde este último hacia el primero.

Datagramas.- Paquete sencillo enrutado en una red sin reconocimiento

Encapsulamiento.- Es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear. El encapsulado consiste pues en ocultar los detalles de implementación de un objeto, pero a la vez se provee una interfaz pública por medio de sus operaciones permitidas.

Decodificar.- El proceso de convertir las palabras escritas en palabras habladas

Servidores Centralizados.- El uso de servidores centralizados ofrecen al usuario una alternativa mucho mejor tanto para compartir como para proteger sus documentos.

Dominio de puenteo.- Se desarrolló para aliviar los problemas de rendimiento que surgieron con el aumento de las colisiones

Conmutación.- Cómo se conmuta una trama a su puerto de destino es una compensación entre la latencia y la confiabilidad.

Lan Conmutadas.- A los bridges multipuerto de alta velocidad se les llama switches LAN, ya que gracias al redireccionamiento inteligente que realizan mediante sus tablas de direcciones actúan conmutando frames entre sus múltiples puertas. Aquellas LANs basadas en switches se las suele llamar LAN conmutadas.

Trama.- Conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado. Desde uno de los componentes de equipo de red, los cuadros pueden ser unidestinados (enviados a un solo dispositivo), multidestinados (enviados a dispositivos múltiples) o difundidos (enviados a todos los dispositivos)

Broadcast.- (o en castellano "difusiones") , se producen cuando una fuente envía datos a todos los dispositivos de una red.

Unicast.- Comunicación establecida entre un solo emisor y un solo receptor en una red.

Multicast.- Es la comunicación de un sólo emisor y varios receptores dentro de una red

Ancho de banda.- Término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso y mayor tráfico o cantidad de personas.

Prompt.- indicador de modo usuario, que permite a este realizar peticiones de servicios al intérprete de órdenes. Este se sustituye actualmente por sistemas de ventanas.

Nodo.- Una red conectada a Internet, con identidad propia a través de una dirección IP de red y generalmente un nombre de dominio.
Ordenador o conjunto de ordenadores que reciben la llamada del usuario y la dirigen hacia el servicio solicitado allá donde se encuentre.

TTL.- Es el tiempo de vida de un paquete en la red. Con este campo, acotamos la permanencia del paquete en la red. Mide el número de saltos que ha dado el paquete, es decir, el número de sistemas intermedios que ha atravesado.

Time To Live (TTL): tiempo de vida en segundos que le queda al paquete. Cada router debe al menos decrementar este tiempo en 1. En la práctica siempre se hace eso, y por lo tanto no tiene mucho que ver con tiempo, sino con número de saltos. Sirve para descartar paquetes en loop.

Latencia.- lapso necesario para que un paquete de información viaje desde la fuente hasta su destino. La latencia y el ancho de banda, juntos, definen la capacidad y la velocidad de una red.

Tabla de Ruteo.- Es la tabla donde se almacenan los caminos disponibles para realizar el proceso de ruteo.

Redes jerárquicas.- Red con varios niveles de comunicación representados por sus nodos correspondientes. La información de origen recorre los nodos en nivel ascendente y luego en orden descendente hasta su nodo destino.

Red troncal.- Backbone. Red principal o troncal, llamada también la espina dorsal de Internet ; Medio de transmisión al que se conectan otras redes de menor velocidad. Es denominada la espina dorsal de Internet.

SNA.- SNA (Standard Network Architecture), es el protocolo de red utilizado por IBM para conectividad con sus hosts o mainframes —grandes ordenadores y servidores muy robustos que soportan millones de transacciones que por lo general son utilizados en bancos

ATM.- Modo de transmisión asíncrona (Asynchronous Transmision Mode). Un protocolo de comunicaciones definido para comunicaciones de datos a alta velocidad.

VTP.- (Virtual Terminal Protocol) : Protocolo de control de transmisiones para la red Internet relativo a terminales.

Conmutación (switching).- este termino es generalmente usado para describir la transferencia de datos de un puerto de entrada hacia uno de salida en una maquina , en la cual la selección del puerto de salida se basa en la información de tipo capa 2.

ANEXOS

ANEXO 1 – INSTALACION Y CONFIGURACION DEL CACTI

1.1 TABLA DE CONTENIDO

1.2 CONFIGURACIÓN DEL SISTEMA OPERATIVO

1.2.1 DISTRIBUCIÓN DE PARTICIONES PARA UN DISCO DE 80 GB:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	2.0G	465M	1.4G	25%	/
/dev/sda2	99M	17M	77M	18%	/boot
/dev/sda3	981M	18M	914M	2%	/home
/dev/sda4	29G	195M	27G	1%	/monitor
/dev/sda5	688M	17M	636M	3%	/opt
/dev/sda6	688M	17M	636M	3%	/tmp
/dev/sda7	15G	6.7G	7.1G	49%	/usr
/dev/sda8	2.0G	37M	1.8G	2%	/usr/local
/dev/sda9	7.7G	1.7G	5.7G	24%	/var
/dev/sda10	9.7G	60M	9.1G	1%	/var/lib/mysql

Fig. 62 – Tabla de particiones en el disco

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

Dar click derecho en la pantalla y abrir un Terminal e ingresar a las siguientes ubicaciones:

1.2.2 vi etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=172.31.42.255
IPADDR=172.31.42.9
NETMASK=255.255.255.0
NETWORK=172.31.42.0
ONBOOT=yes
TYPE=Ethernet
```

1.2.3 vi /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=epn.edu.ec
GATEWAY=172.31.42.1
```

1.2.4 vi /etc/hosts

```
127.0.0.1           epn.edu.ec cacti localhost.localdomain localhost
172.16.1.3          epn.edu.ec cacti localhost.localdomain localhost
```

1.2.5 vi /etc/hosts.allow

```
sshd : 172.31.42.158 172.41.43.2
httpd : ALL
```

1.2.6 vi /etc/hosts.deny

```
ALL : ALL
```

1.2.7 Servicios a tiempo de inicio en **cd /etc/rc.d/rc3.d** y listamos con el comando **ll**

```
/etc/rc.d/rc3.d/S10network -> ../init.d/network
/etc/rc.d/rc3.d/S12syslog -> ../init.d/syslog
/etc/rc.d/rc3.d/S28autofs -> ../init.d/autofs
/etc/rc.d/rc3.d/S44acpid -> ../init.d/acpid
/etc/rc.d/rc3.d/K50snmpd -> ../init.d/snmpd
/etc/rc.d/rc3.d/S55sshd -> ../init.d/sshd
/etc/rc.d/rc3.d/S56xinetd -> ../init.d/xinetd
/etc/rc.d/rc3.d/S64mysqld -> ../init.d/mysqld
/etc/rc.d/rc3.d/S85gpm -> ../init.d/gpm
/etc/rc.d/rc3.d/S85httpd -> ../init.d/httpd
/etc/rc.d/rc3.d/S90crond -> ../init.d/crond
/etc/rc.d/rc3.d/S99local -> ../rc.local
```

En caso de no encontrar estos servicios es recomendable bajarse de Internet y ejecutarlos para evitar cualquier inconveniente.

1.3 DESCARGA DE PAQUETES Y ARCHIVOS NECESARIOS

1.3.1 Nos ubicamos en cd /usr/local/src/ y creamos los siguientes directorios:

```
[root@cacti ~]# cd /usr/local/src/
[root@cacti src]# mkdir CACTI_RPMS
[root@cacti src]# mkdir CACTI_TELCO_IMAGES
[root@cacti src]# ll
total 8
drwxr-xr-x  2 root root 4096 oct 31 13:50 CACTI_RPMS
drwxr-xr-x  2 root root 4096 oct 31 14:12 CACTI_TELCO_IMAGES
```

1.3.2 En el directorio CACTI_RPMS descargamos los paquetes rpm necesarios.

```
[root@cacti src]# cd CACTI_RPMS/
[root@cacti CACTI_RPMS]# ll
total 1632
-rw-r--r--  1 root root 1084862 nov  7  2005 cacti-0.8.6f.fc3.i386.rpm
-rw-r--r--  1 root root   44269 nov  7  2005 cacti-cactid-0.8.6e-1.1.fc3.rf.i386.rpm
-rw-r--r--  1 root root  371764 nov  7  2005 rrdtool-1.0.50-1.1.fc3.rf.i386.rpm
-rw-r--r--  1 root root  152249 nov  7  2005 rrdtool-devel-1.0.50-1.1.fc3.rf.i386.rpm
```

1.3.3 En el directorio CACTI_TELCO_IMAGES descargamos las imágenes que utilizaremos en la interfase Web:

```
[root@cacti src]# cd CACTI_TELCO_IMAGES/
[root@cacti CACTI_TELCO_IMAGES]# ll
total 52
-rw-r--r--  1 root root 14515 oct 23 16:21 auth_deny_epn.GIF
-rw-r--r--  1 root root 22458 oct 23 16:21 auth_login_epn1.GIF
-rw-r--r--  1 root root  3842 oct 23 16:22 cacti_backdrop2_epn.GIF
-rw-r--r--  1 root root  3997 oct 23 16:23 cacti_backdrop_epn1.GIF
-rw-r--r--  1 root root  3488 oct 31 14:01 cacti_logo_epn.GIF
```

1.4 INSTALACIÓN Y CONFIGURACIÓN DE CACTI

1.4.1 Instalación de paquetes: nos ubicamos en cd /usr/local/src/CACTI_RPMS/ y ejecutamos los rpms.

```
[root@cacti ~]# cd /usr/local/src/CACTI_RPMS/
[root@cacti CACTI_RPMS]# rpm -hiv rrdtool-1.0.50-1.1.fc3.rf.i386.rpm
[root@cacti CACTI_RPMS]# rpm -hiv rrdtool-devel-1.0.50-1.1.fc3.rf.i386.rpm
[root@cacti CACTI_RPMS]# rpm -hiv cacti-0.8.6f.fc3.i386.rpm
```

1.4.2 Se creo un file system para almacenar los registros del CACTI, diferente al que viene por defecto en la instalación, razón por la cual es necesario reubicar el

directorio cacti que se encuentra en cd /var/www/html/ en la partición /monitor y crear el enlace respectivo para conservar la ruta original:

```
[root@cacti ~]# cd /var/www/html/
[root@cacti html]# cp -rf cacti/ /monitor
[root@cacti html]# rm -rf cacti/
[root@cacti html]# ln -sf /monitor/cacti/ cacti
[[root@cacti html]# ll
total 0
lrwxrwxrwx  1 root root 15 oct 31 17:21 cacti -> /monitor/cacti/
[[root@cacti html]# cd /monitor/
[root@cacti monitor]# ll
total 20
drwxr-xr-x  11 root root  4096 oct 31 20:28 cacti
drwx------   2 root root 16384 nov 20  2003 lost+found
```

1.4.3 Asignar los permisos correspondientes para los directorios cd /monitor/cacti/rra y /monitor/log de manera que el usuario de sistema cactiuser pueda escribir en ellos, ya que con este usuario se va a ejecutar el programa.

```
[root@cacti ~]# cd /monitor/cacti/
[root@cacti cacti]# chown -R cactiuser rra/ log/
```

1.4.4 Editar el archivo vi /monitor/cacti/include/config.php y cambiar usuario y password que se utilizarán para conectarse a la base de datos, según el siguiente ejemplo:

```
[root@cacti ~]# vi /monitor/cacti/include/config.php
```

```
/* make sure these values refect your actual database/host/user/password */
$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "cactiuser";
$database_password = "mydejavu";
```

1.4.5 Crear la base de datos cacti con MySQL:

```
[root@cacti ~]# chkconfig --level 543 mysqld on
[root@cacti ~]# service mysqld restart
[root@cacti ~]#  cd /monitor/cacti/
[root@cacti ~]# mysqladmin --user=root create cacti
[root@cacti ~]# mysql cacti < cacti.sql
```

1.4.6 Configurar el usuario y clave para el acceso a la base de datos cacti según el user y password especificado en vi /monitor/cacti/include/config.php (paso 3.4):

```
[root@cacti ~]# mysql --user=root mysql
```

```
mysql> GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'mydejavu';
mysql> flush privileges;
mysql> quit
```

1.5 PERSONALIZACIÓN DE LA INTERFASE WEB

1.5.1 Copiar las imágenes de /usr/local/src/CACTI_TELCO_IMAGES/ a /monitor/cacti/images

```
[root@cacti ~]# cd /monitor/cacti/images/
[root@cacti images]# cp /usr/local/src/CACTI_TELCO_IMAGES/* ./
```

1.5.2 Reemplazar las imágenes de logotipos creando enlaces simbólicos como se muestra a continuación:

```
[root@cacti images]# ln -sf auth_login_epn1.GIF auth_login.gif
[root@cacti images]# ln -sf cacti_backdrop_epn1.GIF cacti_backdrop.gif
[root@cacti images]# ln -sf cacti_backdrop2_epn.GIF cacti_backdrop2.gif
[root@cacti images]# [root@cacti images]# ln -sf cacti_logo_epn.GIF cacti_logo.gif
```

1.5.3 Modificar el título de la página de login cambiando *<title>Login to Cacti</title>* que viene por defecto a *<title>Login to MONITOREO LTI</title>* en el archivo /monitor/cacti/auth_login.php

```
[root@cacti ~]# vi /monitor/cacti/auth_login.php
```

```
<html>
<head>
	<title>Login to MONITOREO LTI</title>
	<STYLE TYPE="text/css">
```

1.5.4 Modificar el título de página del archivo /monitor/cacti/include/auth.php cambiando *<title>Cacti</title>* que viene por defecto a *<title>MONITOREO LTI</title>*

```
[root@cacti ~]# vi /monitor/cacti/include/auth.php
```

```
    <html>
<head>
      <title>MONITOREO LTI</title>
      <link href="include/main.css" rel="stylesheet">
</style>
</head>
```

1.5.5 Modificar el título de página del archivo /monitor/cacti/include/top_header.php cambiando *<title>Cacti</title> que viene* por defecto a *<title>EPN :: MONITOREO LTI</title>*

```
[root@cacti ~]# vi /monitor/cacti/include/top_header.php
```

```
<html>
<head>
      <title>EPN :: MONITOREO LTI</title>
      <link href="include/main.css" rel="stylesheet">
      <script type="text/javascript" src="include/layout.js"></script>
</style>
</head>
```

1.5.6 Modificar el título de página del archivo /monitor/cacti/include/top_graph_header.php cambiando *<title>Cacti</title>* que viene por defecto a *<title>EPN :: MONITOREO LTI</title>*

```
[root@cacti ~]# vi /monitor/cacti/include/top_graph_header.php
```

```
<html>
<head>
      <title>EPN :: MONITOREO LTI</title>
      <?php if (isset($_SESSION["custom"])) {
            if ($_SESSION["custom"]) {
```

1.5.7 Modificar el contenido del archivo [root@cacti ~]# vi /monitor/cacti/about.php según lo siguiente

```
<?php
/*
 +-------------------------------------------------------------------------+
 | Copyright (C) 2004 Ian Berry                                            |
 |                                                                         |
 | This program is free software; you can redistribute it and/or           |
 | modify it under the terms of the GNU General Public License             |
 | as published by the Free Software Foundation; either version 2          |
 | of the License, or (at your option) any later version.                  |
 |                                                                         |
 | This program is distributed in the hope that it will be useful,         |
 | but WITHOUT ANY WARRANTY; without even the implied warranty of          |
 | MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the           |
 | GNU General Public License for more details.                            |
 +-------------------------------------------------------------------------+
 | cacti: a php-based graphing solution                                    |
 +-------------------------------------------------------------------------+
 | Most of this code has been designed, written and is maintained by       |
 | Ian Berry. See about.php for specific developer credit. Any questions   |
 | or comments regarding this code should be directed to:                  |
 | - iberry@raxnet.net                                                     |
 +-------------------------------------------------------------------------+
 | - raXnet - http://www.raxnet.net/
*/

include("./include/auth.php");
include("./include/top_header.php");

html_start_box("<strong>About Cacti</strong>", "98%", $colors["header"], "3", "center", "");
?>

<tr>
	<td bgcolor="#<?php print $colors["header_panel"];?>" colspan="2">
		<strong><font color="#<?php print $colors["header_text"];?>">Version <?php print
$config["cacti_version"];?></font></strong>
	</td>
</tr>
<tr>
	<td valign="top" bgcolor="#<?php print $colors["light"];?>" class="textArea">
		<a href="http://www.cacti.net/"><img align="right" src="images/cacti_about_logo.gif" border="0"
alt="raXnet"></a>


		<p> </p>
                        Cacti is designed to be a complete graphing solution based on the RRDTool's framework.
Its goal is to make a
		network administrator's job easier by taking care of all the necessary details necessary to create
		meaningful graphs.

		<p>Please see the <a href="http://www.cacti.net/">official Cacti website</a> for information, support, and
updates.</p>

		<p><strong>Current Cacti Developers</strong><br>
		<ul type="disc">
			<li><strong>Ian Berry</strong> (raX) is original creator of Cacti which was first released to the world in
```

```
2001. He remained the sole
                developer for over two years, writing code, supporting users, and keeping the project
active. Today, Ian continues
                to actively develop Cacti, focusing on backend components such as templates, data
queries, and graph management.</li>
                <li><strong>Larry Adams</strong> (TheWitness) joined the Cacti team in June of 2004
right before the major 0.8.6 release. He helped bring the new poller architecture to
life by providing ideas, writing code, and managing an active group of beta testers. Larry continues
to focus on the poller as well as RRDTool integration and SNMP in a Windows environment.</li>
<li><strong>Tony Roman</strong> (rony) joined the Cacti team in October of 2004 offering years of
programming and system administration experience to the project. He is contributing
a great deal to the upcoming 0.9 release of Cacti by providing many usability and
documentation changes in addition to revamping Cacti's user management component.</li>
            </ul>
            </p>

            <p><strong>Thanks</a></strong><br>
<ul type="disc">                <li>A very special thanks to <a href="http://ee-
staff.ethz.ch/~oetiker/"><strong>Tobi Oetiker</strong></a>, the creator of <a
href="http://www.mrtg.org/">RRDTool</a> and the very popular
                <a href="http://www.mrtg.org">MRTG</a>.</li>                <li><strong>Brady
Alleman</strong>, creator of NetMRG and <a
href="http://www.thtech.net">Treehouse Technologies</a> for questions and ideas. Just
as a note, NetMRG is a complete Network Monitoring solution also written in PHP/MySQL. His
product also makes use of RRDTool's graphing capabilities, I encourage you to check it out.</li>
<li><strong>Andy Blyler</strong>, for ideas, code, and that much needed overall support
                during really lengthy coding sessions.</li>                <li><strong>The users of
Cacti</strong>! Especially anyone who has taken the time to create a bug report, or otherwise
help me fix a Cacti-related problem. Also to anyone who has purchased an item from my amazon.com
                wishlist or donated money to the project.</li>
            </ul>
            </p>
              <p><strong>License</strong><br>

              <p>Cacti is licensed under the GNU GPL:</p>
              <p><tt>This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public Licenseas published by the Free Software
Foundation; either version 2
of the License, or (at your option) any later version.</tt></p>

<p><tt>This program is distributed in the hope that it will be useful,but WITHOUT ANY WARRANTY;
without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.</tt></p>
            <p><strong>Cacti Variables</a></strong><span style="font-family: monospace; font-size:
10px;"><br
            <strong>Operating System:</strong> <?php print $config["cacti_server_os"];?><br>
<strong>PHP SNMP Support:</strong> <?php print $config["php_snmp_support"] ? "yes" : "no";?><br>
              </span></p>
      </td>
</tr>


&amp;nbsp;</p><hr width="85%">
&amp;nbsp;</p><p align="center"><a href="http://www.epn.edu.ec" title="Ir a www.epn.edu.ec"><img
src="http://www.epn.edu.ec/espanol/imagenes/cactiLogo_275x60.gif" border="0" alt="ESFOT"></a></p>
<p align="center"><strong>Implementado el 31 de Octubre del 2006<br>
Tesis Guillermo - Viviana<br>
ESFOT</strong></p>
```

```
<p> </p>
</td>
</tr>

<?php
        html_end_box();
include("./include/bottom_footer.php");
?>
```

1.6 CONFIGURACIÓN DE APACHE

1.6.1 Editar el archivo de configuración de Apache ubicado en /etc/httpd/conf/httpd.conf y configurar los parámetros que se muestran a continuación:

```
[root@cacti ~]# vi /etc/httpd/conf/httpd.conf
```

```
ServerAdmin guille_luigi@hotmail.com
```

```
DocumentRoot "/var/www/html/cacti"
```

```
ServerName 172.16.1.3:80
```

```
<Directory "/var/www/html/cacti">
```

1.6.2 Configurar el servicio httpd para que arranque a tiempo de inicio y reiniciar el Apache:

```
[root@cacti ~]#  chkconfig --level 543 httpd on
[root@cacti ~]# service httpd restart
```

1.7 CONFIGURACIÓN DE CACTI DESDE LA INTERFASE WEB

1.7.1 Acceder vía browser al cacti, utilizando la dirección IP 172.31.42.9

Fig. 63 – Ingreso a la interface CACTI

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.2 Inmediatamente cargará la página de guía de instalación del cacti, procederemos a dar click en link **Next>>** ubicado en la parte inferior derecha del recuadro.

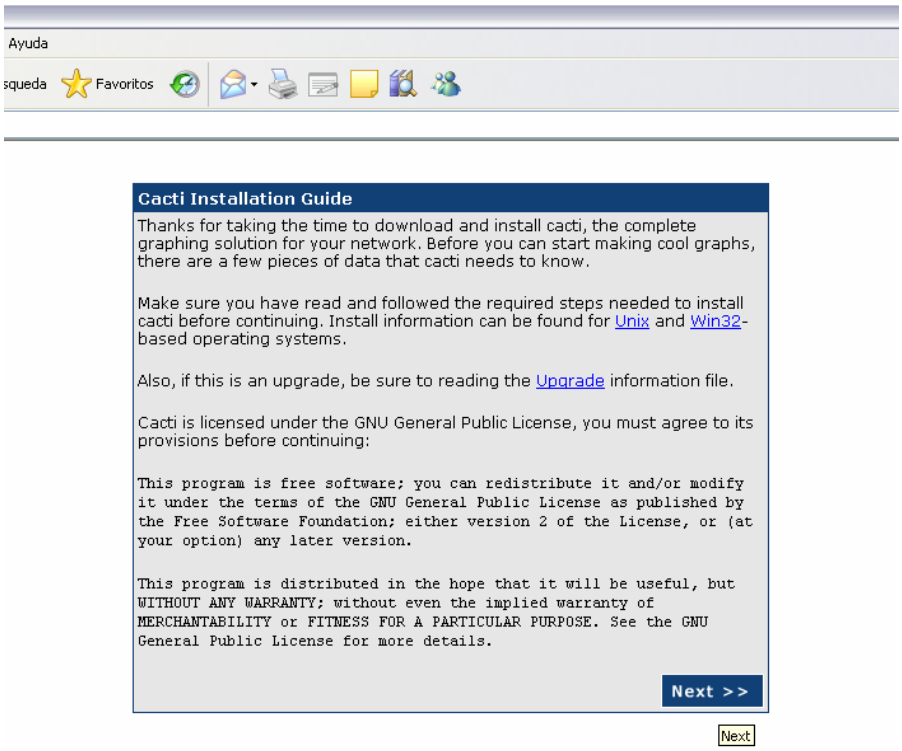


Fig. 64 – Ventana con guía de instalación

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.3 Seleccionar la opción *New Install* en la persiana del cuadro de diálogo *Cacti Installation Guide* y a continuación damos click en link **Next>>** ubicado en la parte inferior derecha del recuadro.

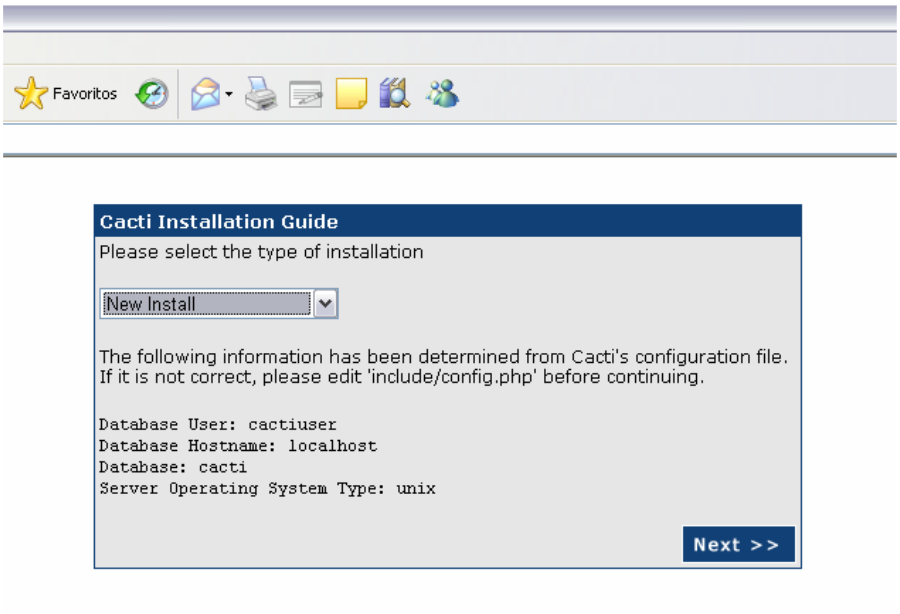


Fig. 65 – Tipo de instalación

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.4 En el siguiente recuadro confirmamos que las rutas de los ejecutables correspondientes a los programas utilizados por el cacti, sean las correctas y a continuación damos click en link **Finish** ubicado en la parte inferior derecha del recuadro.

Fig. 66 – Confirmación de rutas

Fuente:Realizado por Díaz Jeaneth – Tipán Luis

1.7.5 A continuación aparecerá el cuadro de diálogo de acceso al sistema, al cual ingresaremos con el user admin y password cactiesfot

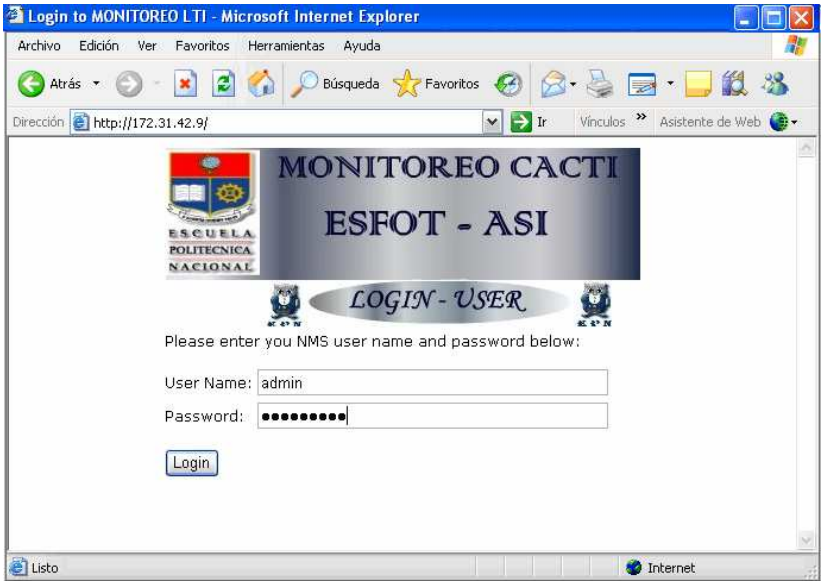


Fig. 67 – Ingreso del Administrador

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.6 Inmediatamente después de haber ingresado con el user y password admin, el sistema nos solicitará cambiar la clave para el usuario admin.

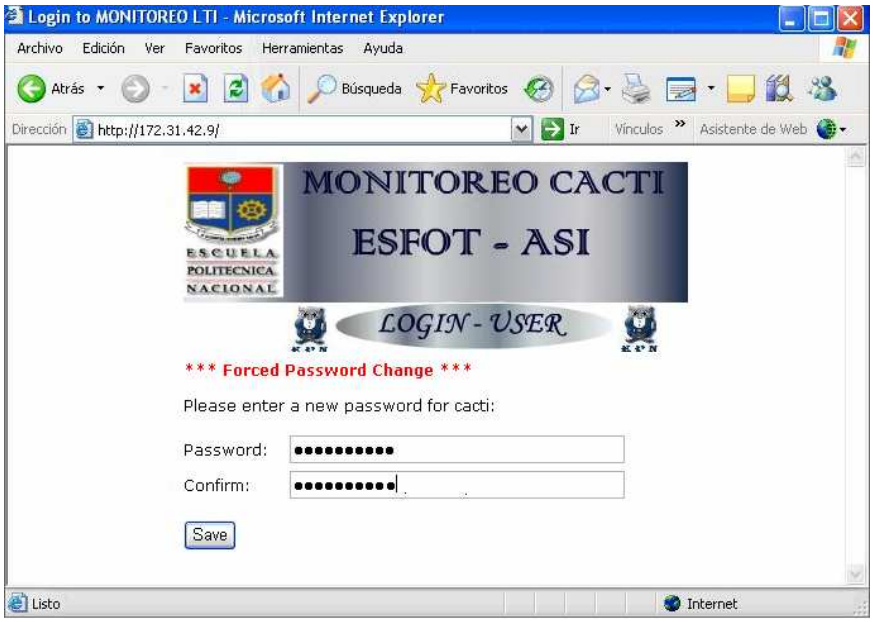


Fig. 68 – Cambio de Password

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.8 A continuación aparecerá la consola de administrado del cacti

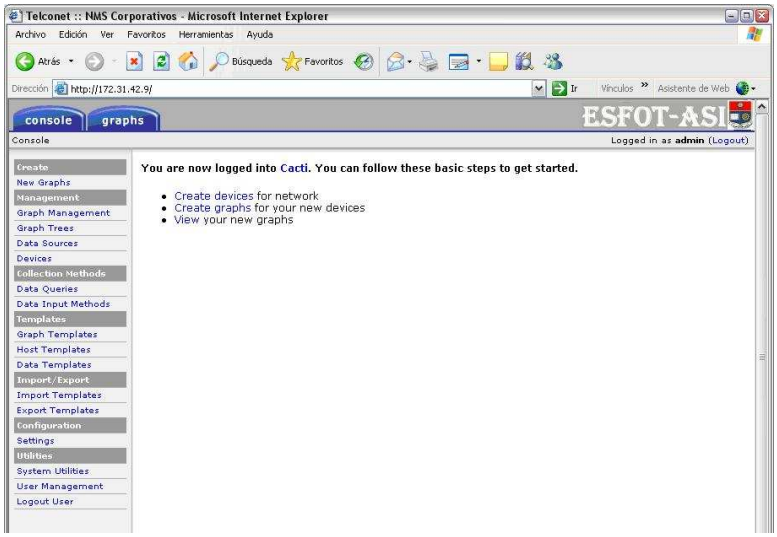


Fig. 69 – Diagrama consola de Administracion

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.9 Seleccionamos la opción *Settings* en la parte inferior del menú izquierdo y en la pestaña *General*, sección *SNMP Defaults*, seleccionamos la version1 de SNMP, agregamos la comunidad SNMP y damos click en el botón **SAVE** ubicado en la parte inferior derecha de la página.

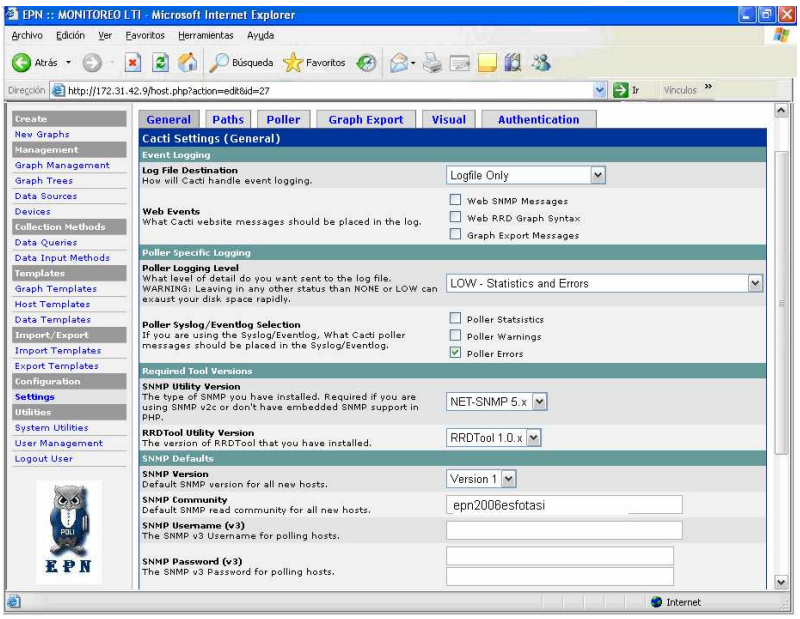


Fig. 70 – Opción settings

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.7.10 Seleccionamos la pestaña *Poller*, en la sección *Poller Execution Parameters*, configuramos los siguientes valores:

- *Maximum Concurrent Poller Processes* = **60**
- *Script and Script Server Timeout Value* = **25**

En la sección *Poller Host Availability Settings* configuramos los siguientes valores:

- *Downed Host Detection* = **SNMP - Reliable**
- *Ping Type* = **UDP Ping**
- *Ping Timeout Value* = **400**
- *Ping Retry Count* = **1**

Finalmente damos click en el botón **SAVE** ubicado en la parte inferior derecha de la página.

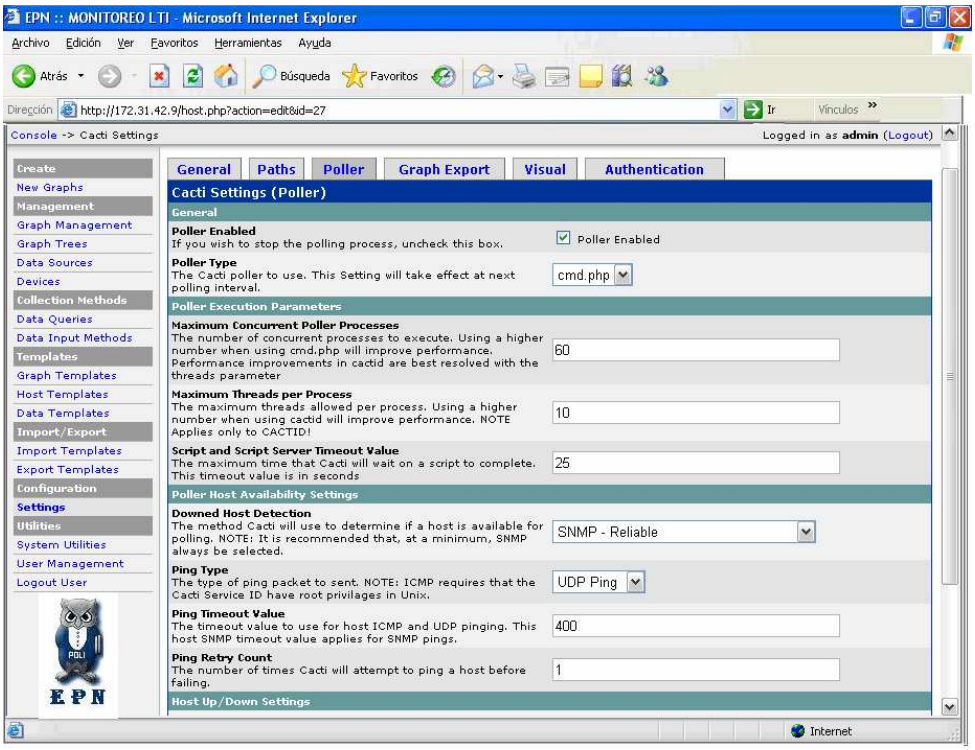


Fig. 71 – Configuracion

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.8 PUESTA EN MARCHA DEL SERVICIO

1.8.1 Comprobar que se haya creado la entrada correspondiente en el croad para ejecutar cacti de forma programada, esto lo hacemos revisando el archivo cacto ubicado en /etc/cron.d/ cuyo contenido debe ser similar al siguiente ejemplo donde se especifica el usuario con que se va a ejecutar el programa y la ruta del poller:

```
[root@cacti ~]# cat /etc/cron.d/cacti
*/5 * * * *     cactiuser       php /var/www/html/cacti/poller.php > /dev/null 2>&1
```

1.8.2 Configurar crond para que arranque a tiempo de inicio y reiniciar el servicio

```
[root@cacti ~]# chkconfig --level 543 crond on
[root@cacti ~]# service crond restart
```

1.8.3 Ejecución del cacti en forma manual:

Para ejecutar manualmente cacti, debemos hacerlo como usuario cactiuser y no como root ya que esto cambiaría los permisos de los archivos ubicados en /monitor/cacti/rra y /monitor/cacti/log de manera que el usuario cactiuser ya no tendrá permisos para escribir en ellos, provocando que el cacti deje de graficar.

Una vez logueados como usuario cactiuser ejecutamos el comando **php poller.php**

```
[root@cacti ~]#  su - cactiuser
[cactiuser@nmscorp ~]$ php poller.php
OK u:0.06 s:0.10 r:7.42
OK u:0.06 s:0.10 r:7.42
OK u:0.06 s:0.10 r:7.42
OK u:0.06 s:0.10 r:7.42
OK u:0.06 s:0.10 r:7.42
OK u:0.06 s:0.10 r:7.42
OK u:0.06 s:0.10 r:7.42
Content-type: text/html
X-Powered-By: PHP/4.3.11

09/27/2005 12:07:25 PM - SYSTEM STATS: Time: 11.9537 s, Method: cmd.php, Processes: 60,
Threads: N/A, Hosts: 186, Hosts/Process: 4, Data Sources 2158, RRDs Processed 1624
```

1.9 ADMINISTRACIÓN DE HOSTS/DEVICES EN CACTI

Entre las opciones que ofrece Cacti para la administración de dispositivos, podemos citar la siguientes para nuestro uso:

- Agregar hosts con platillas de consultas snmp predefinidas, en base al tipo de dispositivo que se desea agregar.
- Agregar hosts con platillas de consultas snmp predefinidas, en base al tipo de dispositivo que se desea agregar.
- Crear usuarios y asignarle permisos para visualizar o modificar uno o varios Hosts/Devices.
- Habilitar o deshabilitar dentro del poller Hosts/Devices previamente creados.
- Realizar modificaciones en la literatura contenida en los gráficos generados.

1.9.1 Agregar nuevos hosts/devices

1.9.1.1 Desde la consola Web del user admin damos clic en el link *Create devices*

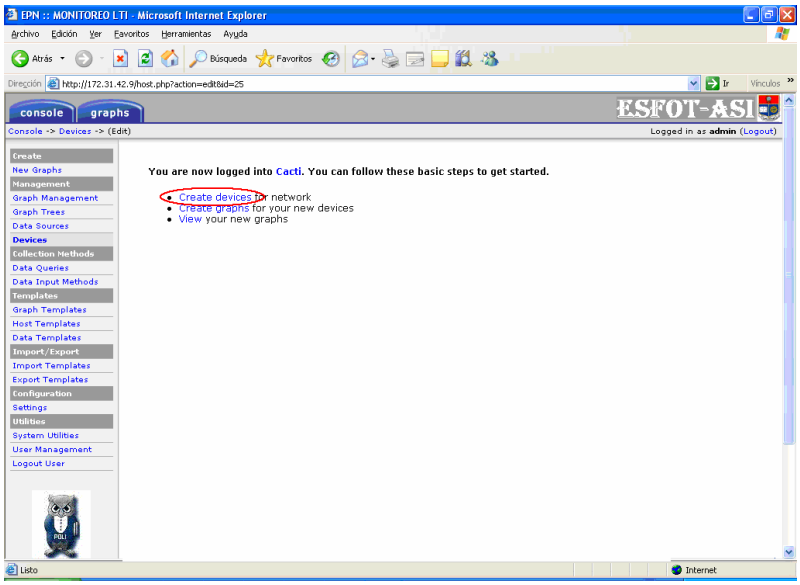


Fig. 72 – Gráfica Creando dispisitivo

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.9.1.2 A continuación cargará una pantalla con el listado de hosts/devices creados, por defecto (default) encontraremos agregado a local host (127.0.0.1). Hacemos click en el link Add ubicado en la parte superior derecha del cuadro.

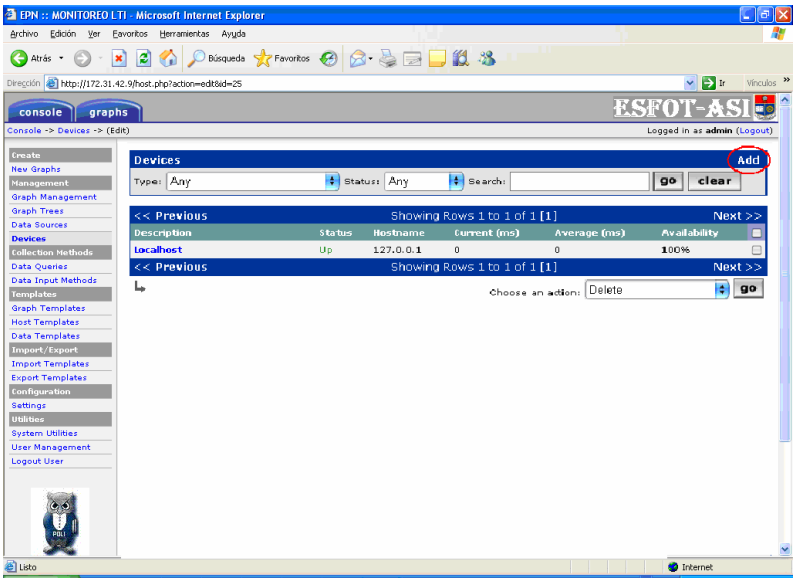


Fig. 73 – Gráfica de acerca de Add

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.9.1.3 Seguidamente nos cargará el formulario para ingresar los datos del dispositivo que se quiere agregar:

Description: Agregamos una descripción para el nuevo dispositivo (puede ser el mismo hostname).

Hostname: Agregamos el nombre del dispositivo según la referencia DNS (También soporta dirección IP en el caso de no haber referencia DNS).

Host Template: Aquí podemos seleccionar la opción *ucd/net SNMP Host* en caso de que el dispositivo a agregar sea un sistema UNIX/LINUX ó la opción *Cisco Router* en el caso de tratarse de un dispositivo Cisco como switch o router.

SNMP Community: En el caso de no tener configurada la comunidad SNMP de forma predeterminada, debemos agregarla en este campo.

SNMP Versión: En el caso de no tener configurado el cacti para que utilice SNMP versión 2 de forma predeterminada, debemos especificarlo seleccionado la opción correspondiente en este campo en nuestro caso utilizamos la versión 1.

Después de haber llenado el formulario con los datos del dispositivo que queremos agregar, hacemos clic en el botón **create** ubicado en la parte inferior derecha del formulario.

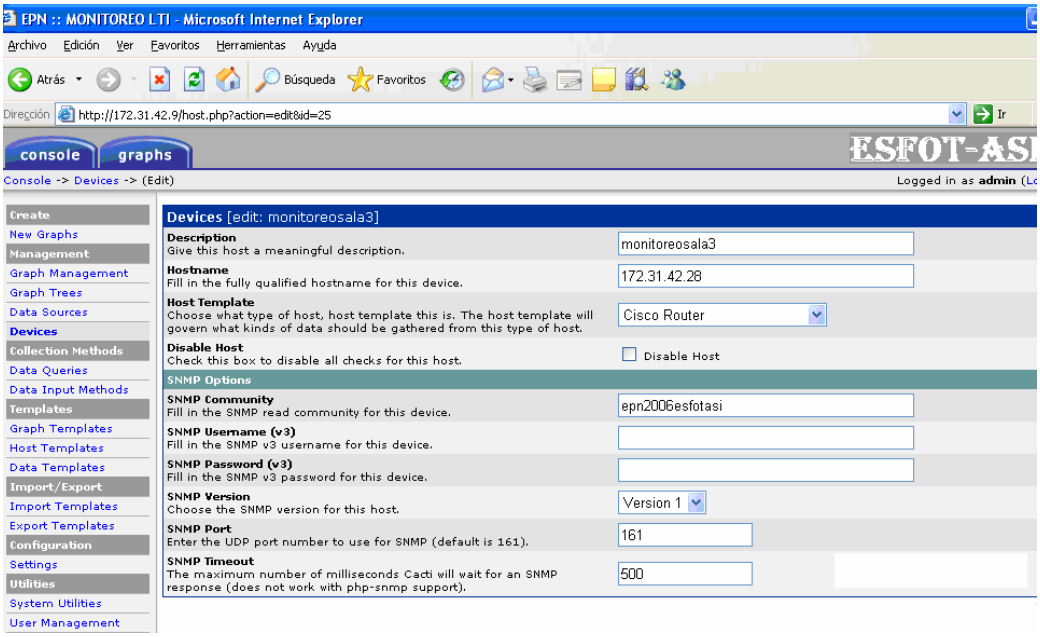


Fig. 74 – Propiedades de al crear un dispositivo

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.9.1.4 Inmediatamente después de haber creado el dispositivo, si la lectura SNMP fue correcta deberán aparecen los siguientes mensajes:

a) En la parte superior del formulario, la información correspondiente al Sistema Operativo, Uptime y Hostname del dispositivo agregado.

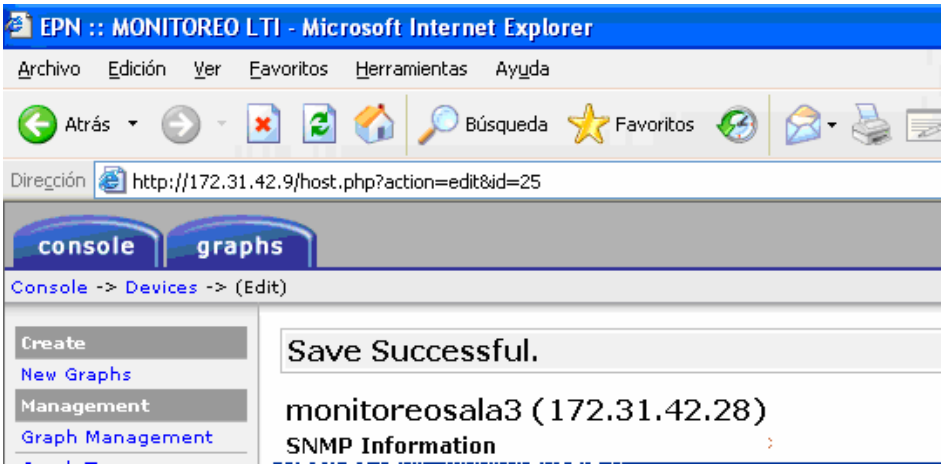


Fig. 75 – Gráfica acerca de aprobación

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

b) En la parte inferior del formulario, en la sección *Associated Data Queries* la columna *Status* correspondiente al campo *SNMP - Interface Statistics* deberá contener valores superiores a cero para *Ítems* y *Rows*.

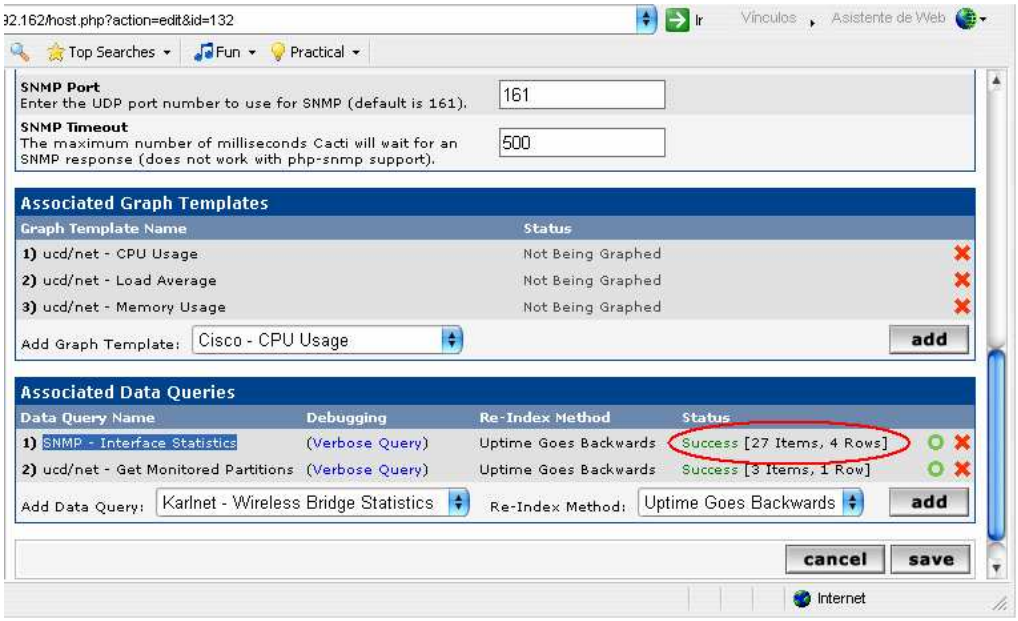


Fig. 76 – Gráfica formulario

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

c) Después de verificar si tubo éxito la lectura SNMP, hacemos clic en el link *Create Grapas for this Host* para pasar al formulario de selección de gráficos.

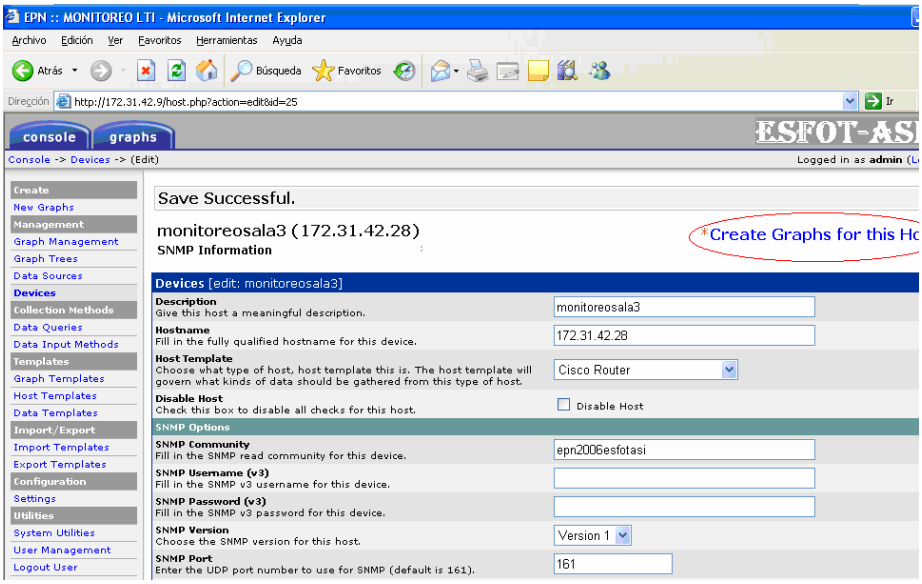


Fig. 77 – Creación de Gráficas

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.9.1.5 Seleccionamos las interfaces que desamos monitorear en el dispositivo creado, así como los items de *CPU Usage*, *Load Average* y *Memory Usage* en el caso de dispositivos Linux y en el caso de dispositivos Cisco, el item *CPU Usage*. Después de seleccionar los ítems que deseamos graficar hacemos click en el boton **create** ubicado en la parte inferior derecha del formulario.

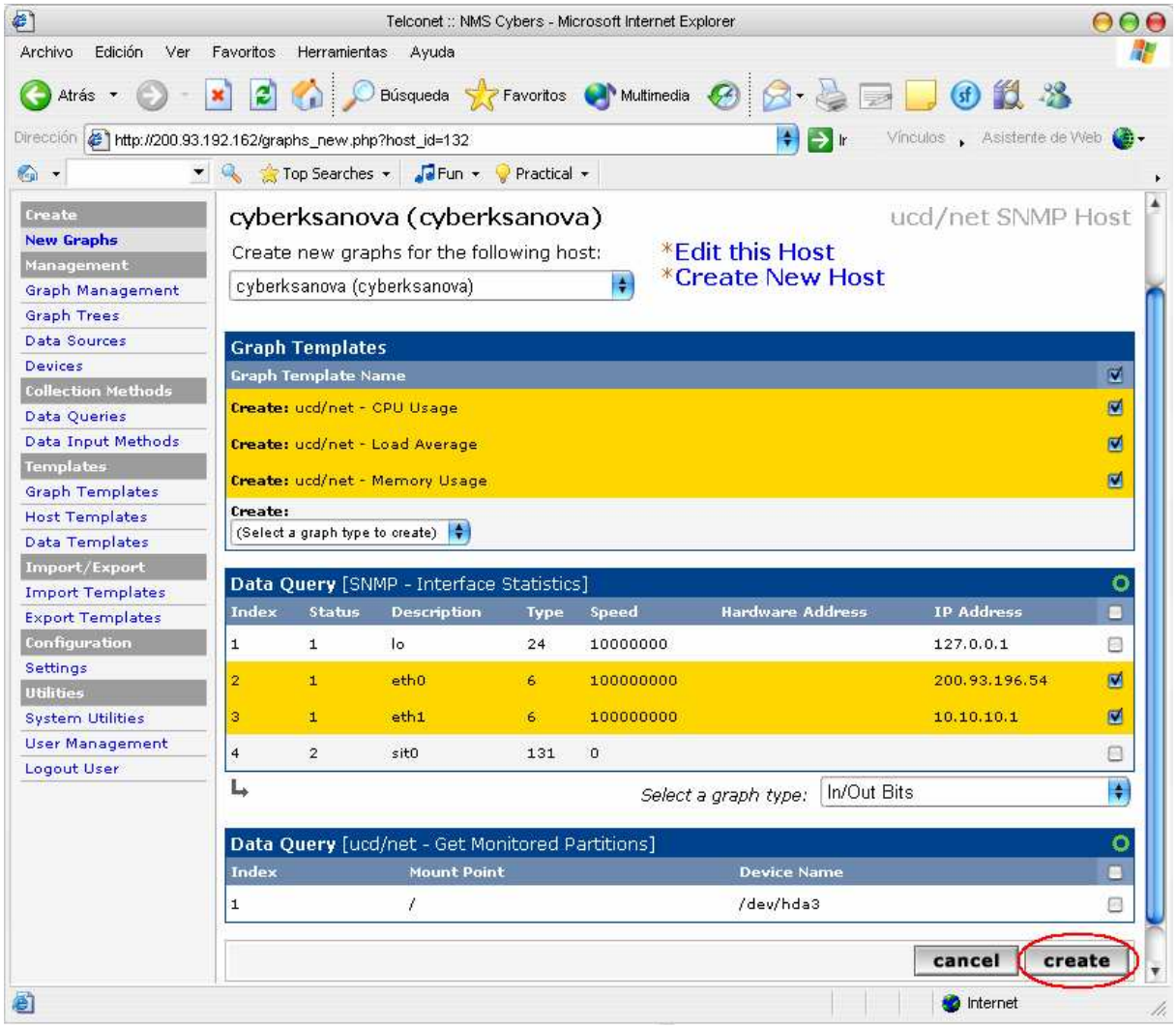


Fig. 78– Activación de interfaces

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.9.1.6 Seguidamente deberá aparecer en la parte superior del cuadro una serie de mensajes indicado que se crearon las gráficas correspondientes a cada uno de los items seleccionados, y en la sección de los items, veremos sombreados aquellos a los que ya se les ha generado gráfica.

1.10 CONFIGURAR EL ÁRBOL GRÁFICO (GRAPH TREES)

Con la finalidad de clasificar los dispositivos a monitorear, en nuestro caso por diseño, seguiremos los siguientes pasos:

1.10.1 Borrar el árbol predeterminado

1.10.1.1 Desde la consola Web del user admin seleccionamos la opción *Graph Trees* y a continuación borramos el *Default Tree* haciendo click en la X de color roja situada del lado derecho del mismo.

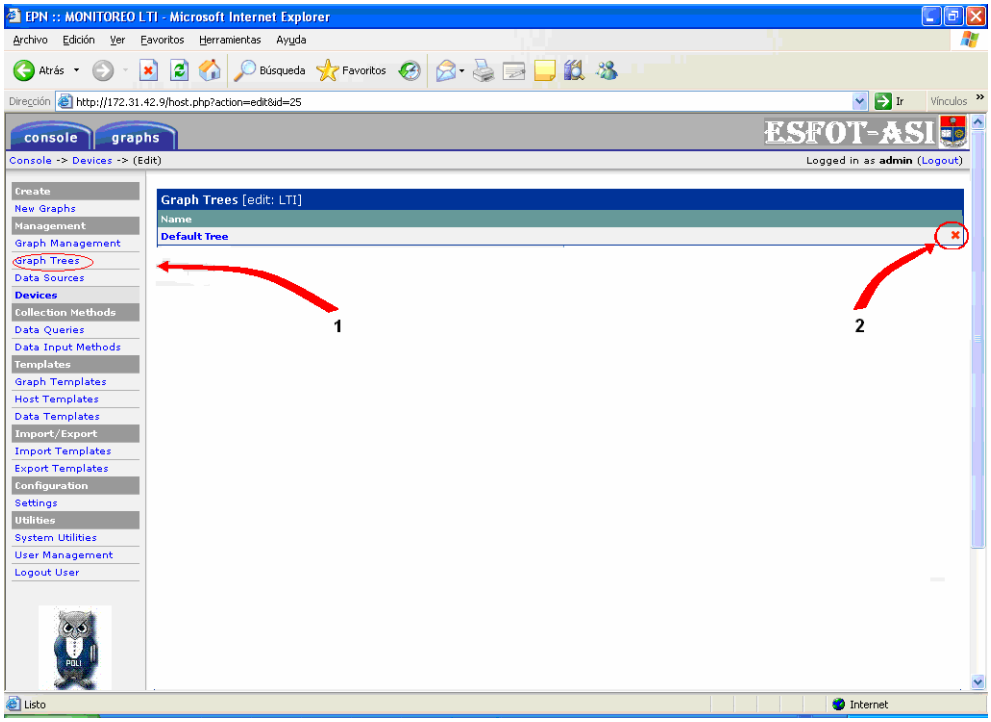


Fig. 79– Delete default tree

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.10.1.2 Hacemos click en el botón **delete** que se muestra en el siguiente gráfico:

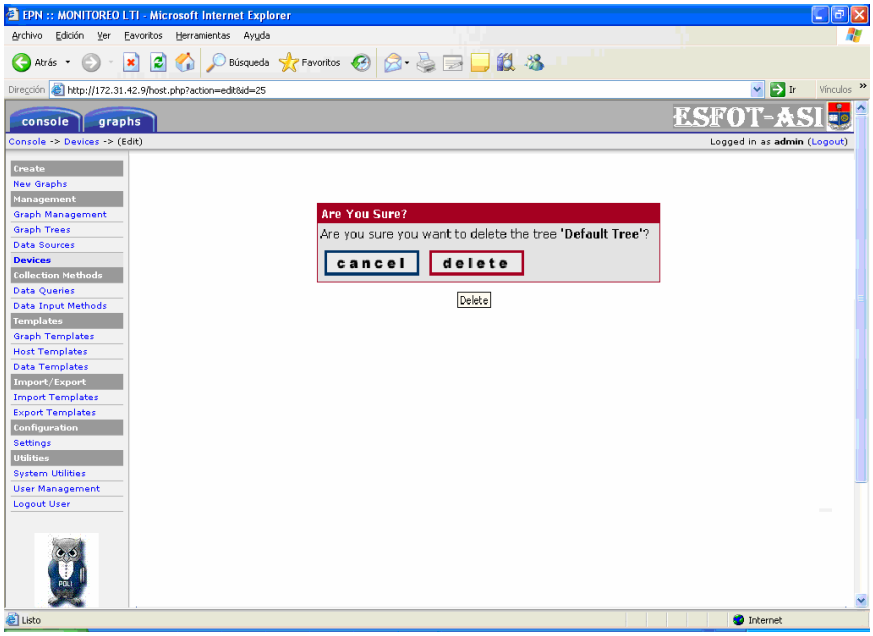


Fig. 80– Gráfica Delete

Fuente:Realizado por Díaz Jeaneth – Tipán Luis

1.10.1.3 Crear los árboles necesarios, en nuestro caso por cada diseño donde tenemos presencia:

1.10.1.4 Después de haber borrado el *Defaul Tree* en el listado de árboles deberá aparecer vacío, procederemos a dar clic en el link **Add** ubicado en el extremo derecho del título *Graph Trees* en la parte superior del cuadro.

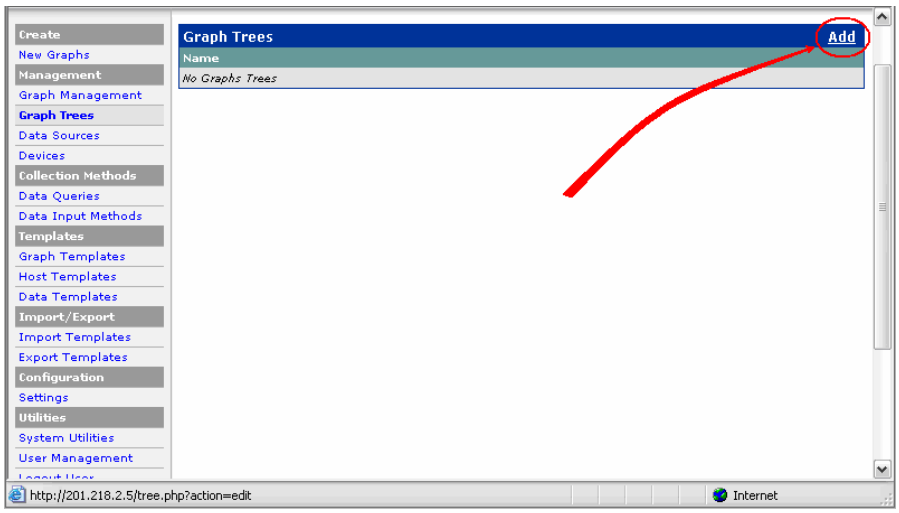


Fig. 81– Añadir tree (árbol)

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.10.1.5 Ingresamos el nombre que vamos a definir para el árbol, en el campo name y en el campo *Sorting Type* seleccionamos la opción *Alphabetic Ordering*, y damos click en el botón **create**

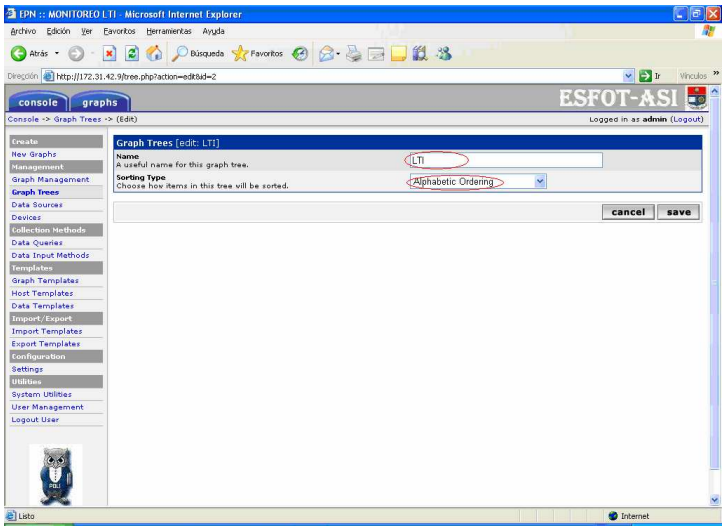


Fig. 82– Nombre de árbol

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.10.2 AGREGANDO HEADERS AL ÁRBOL:

1.10.2.1 Seleccionamos la opción *Graph Trees* de la sección *Management* en la parte superior del menú derecho en la consola del administrador de cacti.

Luego en el cuadro *Graph Trees* hacemos clic en el nombre del árbol sobre el cual vamos a trabajar.

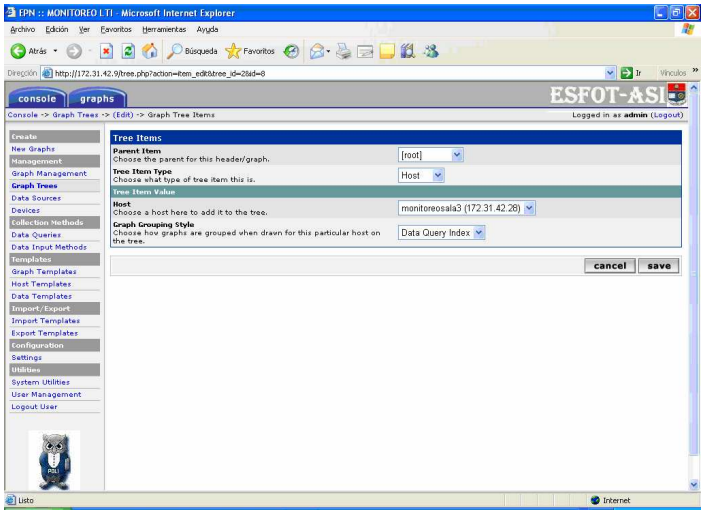


Fig. 83– Agregando Headers al árbol

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.10.2.2 Seleccionamos la opción *Graph Trees* de la sección *Management* en la parte superior del menú derecho en la consola del administrador de cacti.

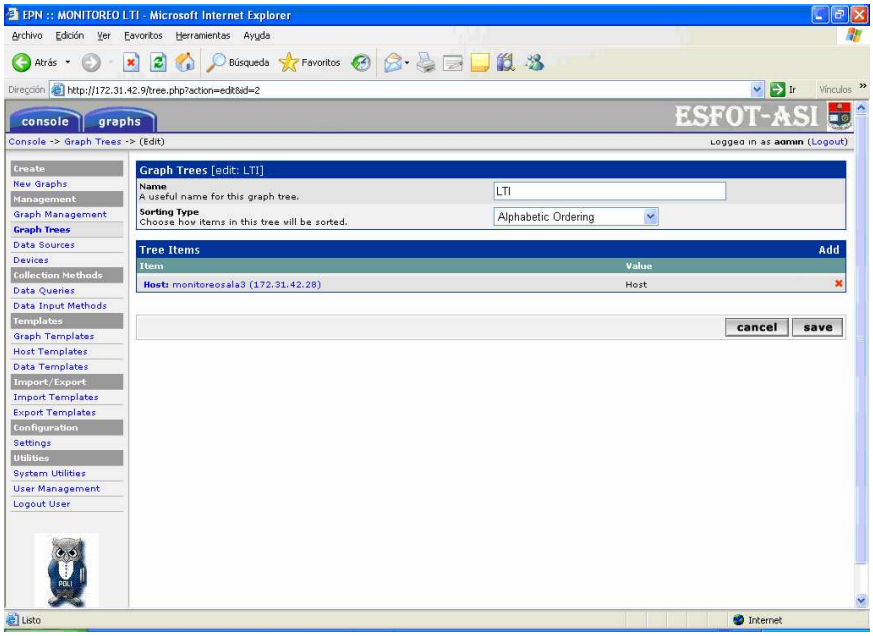


Fig. 84– Opción ordenar alfabéticamente

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.10.2.3 En el cuadro *Tree Items* seleccionamos la opcción *Header* en el campo *Tree Item Type* y digitamos en nombre para el Header o Titular en el campo Title. Seguidamente damos click en el botón **create** ubicado en la parte inferior derecha del cuadro.

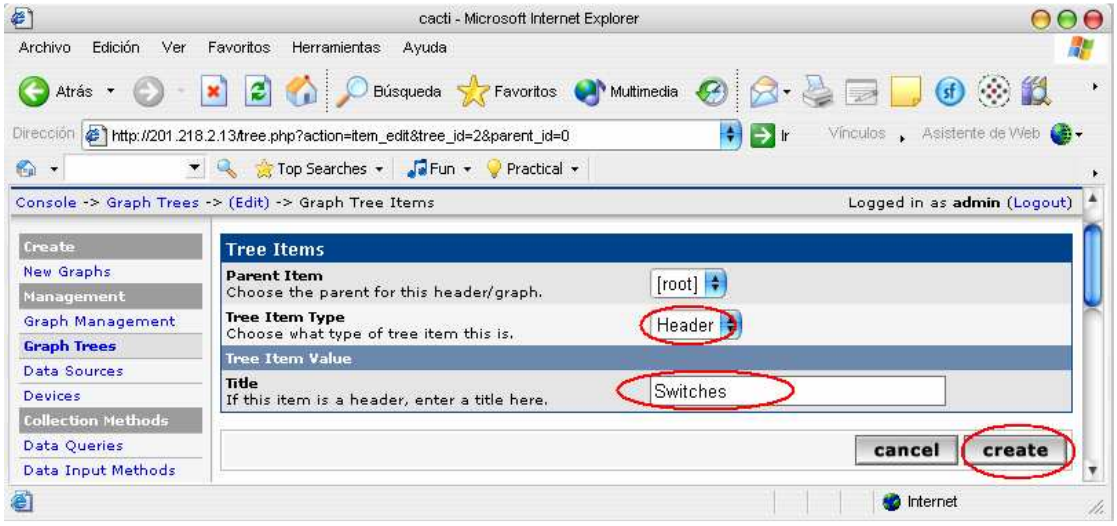


Fig. 85– Agregando nombre de dispositivo al árbol

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.10.2.4 Después de esto aparecerá el mensaje Save Successful en la parte superior de cuadro de edición del árbol sobre el cual estamos trabajando, y en la sección Tree Ítems/Item veremos tanto los hosts agregados como el nuevo header o titular.

Finalmente damos click en el botón save ubicado en la parte inferior derecha de cuadro.

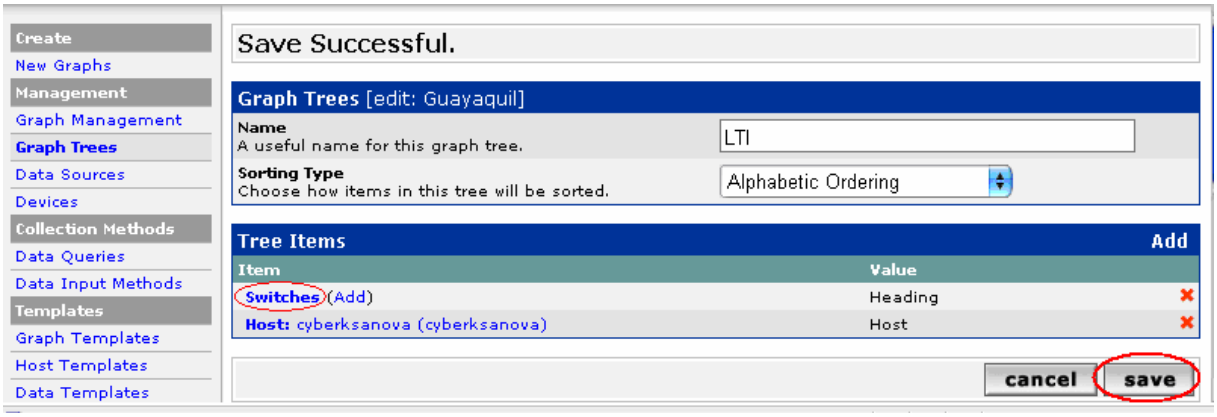


Fig. 86– Guardar creación de dispositivo en el árbol

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.11 TIPOS DE CONSULTAS GRÁFICAS

1.11.1 Periódos de tiempo predefinidos:

De la lista desplegable *Presets:* puede seleccionar los siguientes periódos:

- **Last Half Hour** La última media hora
- **Last Hour** La última hora
- **Last 2 Hours** Las últimas 2 horas
- **Last 4 Hours** Las últimas 4 horas
- **Last 6 Hours** Las últimas 6 horas
- **Last 12 Hours** Las ultimas 12 horas
- **Last Day** El último día
- **Last 2 Days** Los 2 últimos días
- **Last 3 Days** Los 3 últimos días
- **Last 4 Days** Los 4 últimos días

- **Last Week** La última semana
- **Last 2 Weeks** Las 2 últimas semanas
- **Last Month** El último mes
- **Last 2 Months** Los 2 últimos meses
- **Last 3 Months** Los 3 últimos meses
- **Last 4 Months** Los 4 últimos meses
- **Last 6 Months** Los 6 últimos meses
- **Last Year** El último año
- **Last 2 Years** Los 2 últimos años

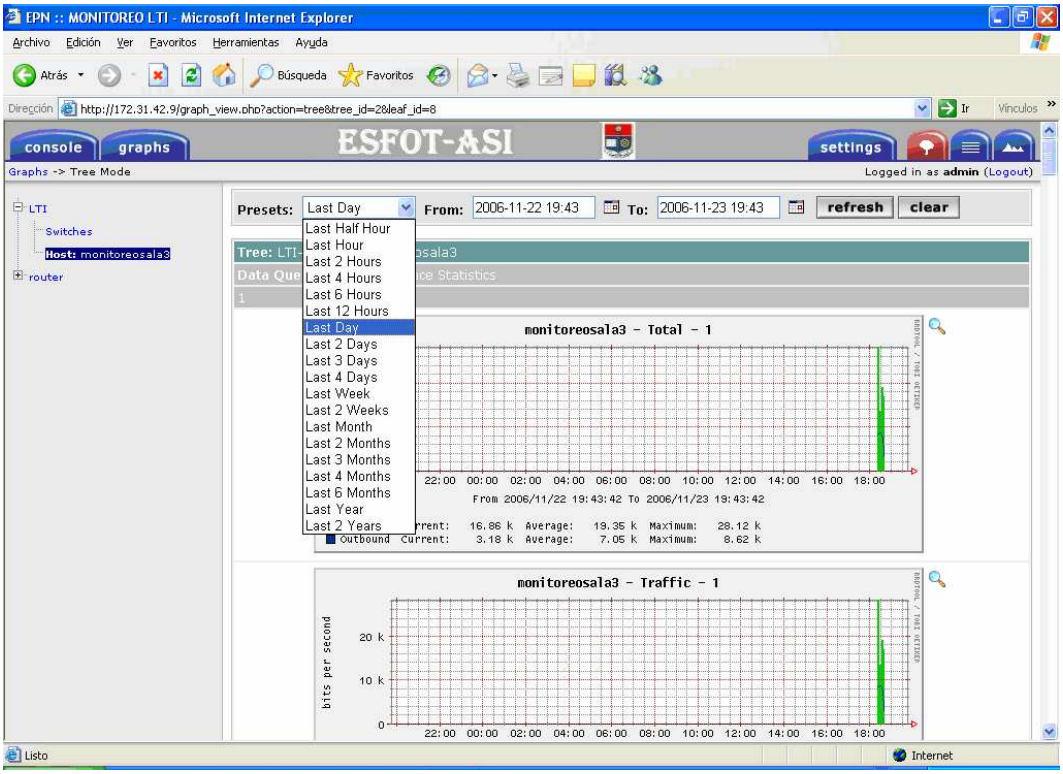


Fig. 87– Gráfica por día, mes año

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.11.2 Periódos de tiempo específicos:

Para seleccionar la fecha de inicio hacemos click en el icono en forma de calendario, que se encuentra ubicado despues de campo que contiene la fecha correspondiente a la opcion ***From:***

Se abrirá un calendario, en el cual podremos seleccionar mes y día.

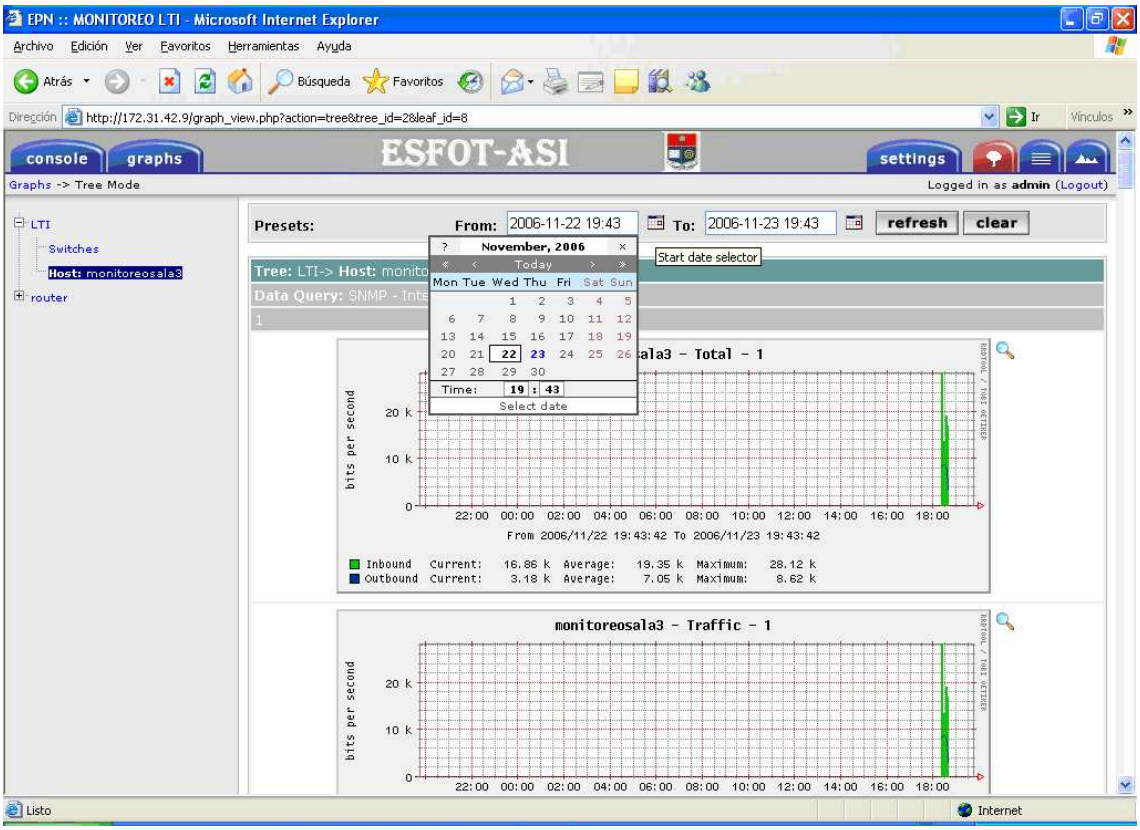


Fig. 88– Gráfica por fecha desde

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

Para seleccionar hasta que fecha se desea la grafica damos click en el icono en forma de calendario, que se encuentra ubicado despues de campo que contiene la fecha correspondiente a la opcion ***to:***

Se abrirá un calendario, en el cual podremos seleccionar mes y día.

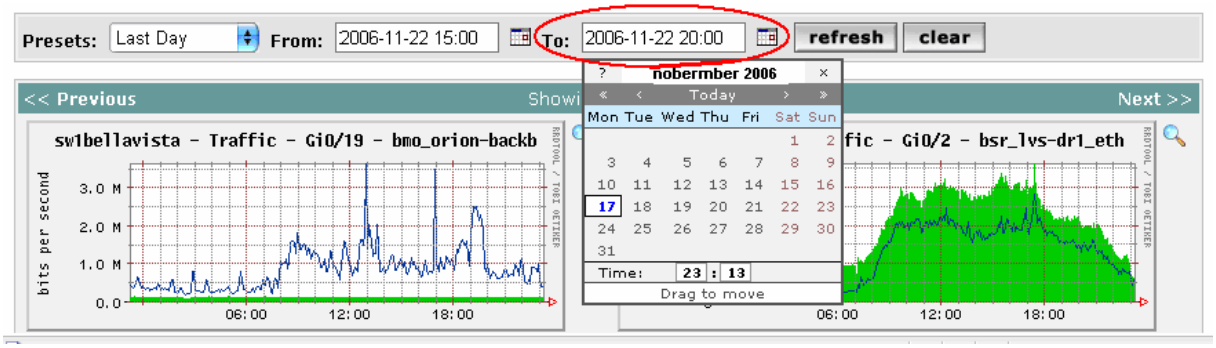


Fig. 89– Gráfica por fecha hasta

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

1.12 PROBLEMAS PARA CAPTURAR LOS NOMBRES O DESCRIPCIONES DE INTERFACES

Los templates del cacti no estan configurados para utilizar la variables que captura la descripción del puerto de un switch y en algunos dispositivos tampoco logra capturar el nombre de la interface. Ej

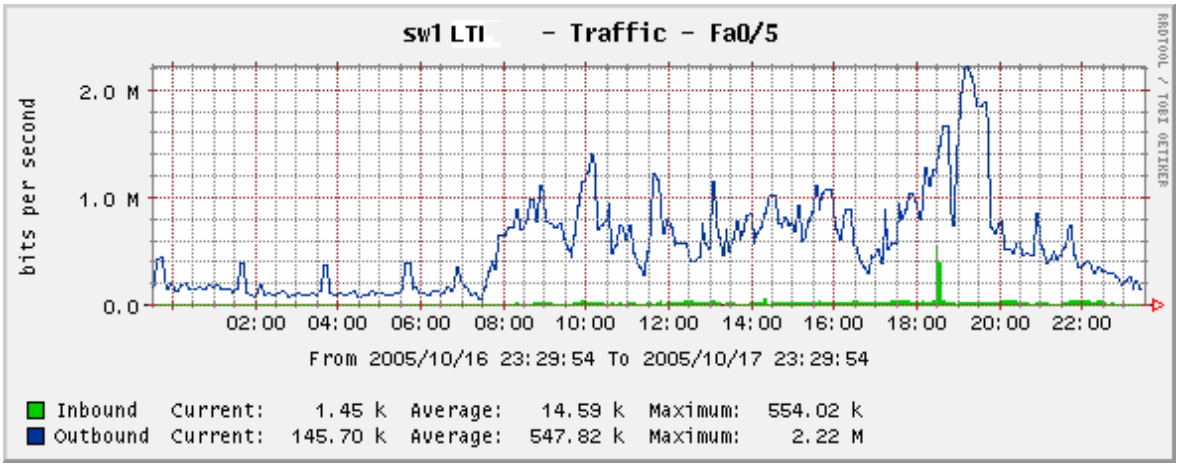


Fig. 90– Gráfica medición de ancho de banda

Fuente: Realizado por Díaz Jeaneth – Tipán Luis

REFERENCIAS

http://www.cacti.net/

http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

ANEXO 2 - INSTALACION Y CONFIGURACION DEL PROXY

1.1 CONFIGURACION DEL SQUID

Instalación a través de yum.

yum –y install squid

yum -y update kernel iptables

Antes de continuar.

Evite dejar espacios vacíos en lugares indebidos. El siguiente es un ejemplo de cómo no se debe habilitar un parámetro.

Mal

```
# Opción incorrectamente habilitada
  http_port 3128
```

Bien

```
# Opción correctamente habilitada
http_port 3128
```

Squid utiliza el puerto 8080 o 3128 y su fichero de configuración localizado en /etc/squid/squid.conf, y podrá trabajar sobre éste utilizando su editor de texto simple preferido. Existen un gran número de parámetros, de los cuales recomendamos configurar los siguientes:

- Parámetro http_port:

  # Default: http_port 3128

  http_port 3128

  http_port 8080

- Parámetro cache_mem.

  El parámetro cache_mem establece la cantidad ideal de memoria .

Si se posee un servidor con al menos 128 MB de RAM, establezca 16 MB como valor para este parámetro:

cache_mem 16 MB

Parámetro cache_dir:

Este parámetro se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. Para entender esto un poco mejor, responda a esta pregunta: ¿Cuanto desea almacenar de Internet en el disco duro? De modo predefinido Squid utilizará un caché de 100 MB, de modo tal que encontrará la siguiente línea:

cache_dir ufs /var/spool/squid 100 16 256

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda.

Los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno. No modifique esto números, no hay necesidad de hacerlo.

Controles de acceso

Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid. Procedamos a entender como definir unas y otras.

Listas de control de acceso.

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

acl [nombre de la lista] src [lo que compone a la lista]

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.1.n con máscara de sub-red 255.255.255.0, podemos utilizar lo siguiente:

acl miredlocal src 192.168.1.0/255.255.255.0

También puede definirse una Lista de Control de Acceso especificando un fichero localizado en cualquier parte del disco duro, y la cual contiene una lista de direcciones IP. Ejemplo:

acl permitidos src "/etc/squid/permitidos"

El fichero /etc/squid/permitidos contendría algo como siguiente:

192.168.1.1
192.168.1.2
192.168.1.3

Reglas de Control de Acceso

Estas definen si se permite o no el acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

http_access [deny o allow] [lista de control de acceso]

En el siguiente ejemplo consideramos una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada permitidos:

http_access allow permitidos

También pueden definirse reglas valiéndose de la expresión !, la cual significa no. Pueden definirse, por ejemplo, dos listas de control de acceso, una denominada lista1 y otra denominada lista2, en la misma regla de control de acceso, en donde se asigna una expresión a una de estas. La siguiente establece que se permite el acceso a Squid a lo que comprenda lista1 excepto aquello que comprenda lista2:

```
http_access allow lista1 !lista2
```

Listas de Control de Acceso: definición de una red local completa

```
# # Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl todalared src 192.168.1.0/255.255.255.0
```

A continuación procedemos a aplicar la regla de control de acceso:

```
http_access allow localhost
http_access allow todalared
http_access deny all
```

Caché con aceleración

En la sección HTTPD-ACCELERATOR OPTIONS deben habilitarse los siguientes parámetros:

```
httpd_accel_host virtual
httpd_accel_port 0
httpd_accel_with_proxy on
```

Iniciando, reiniciando y añadiendo el servicio al arranque del sistema.
Una vez terminada la configuración, ejecute el siguiente mandato para iniciar por primera vez Squid:

```
service squid start
```

Si desea que Squid inicie de manera automática la próxima vez que inicie el sistema, utilice lo siguiente:

chkconfig squid on

Depuración de errores

Cualquier error al inicio de Squid solo significa que hubo errores de sintaxis, errores de dedo o bien se están citando incorrectamente las rutas hacia los ficheros de las Listas de Control de Acceso.

Cuando se trata de errores graves que no permiten iniciar el servicio, puede examinarse el contenido de el fichero /var/log/squid/squid.out con el mandato less, more o cualquier otro visor de texto:

less /var/log/squid/squid.out

Re-direccionamiento de peticiones a través de iptables

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to- port 8080

Lo anterior, que requiere un guión de cortafuegos funcional en un sistema con dos interfaces de red, hace que cualquier petición hacia el puerto 80 (servicio HTTP) hecha desde la red local hacia el exterior, se re-direccionará hacia el puerto 8080 del servidor

Restricciones por Extensiones

Debemos definir una *Lista de Control de Acceso* que a su vez defina al fichero */etc/squid/listaextensiones*. Esta lista la denominaremos como *"listaextensiones"*. De modo tal, la línea correspondiente quedaría del siguiente modo:

acl listaextensiones urlpath_regex "/etc/squid/listaextensiones“

Habiendo hecho lo anterior, deberemos tener en la sección de *Listas de Control de Acceso* algo como lo siguiente:

```
# # Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl redlocal src 192.168.1.0/255.255.255.0
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

A continuación especificaremos modificaremos una *Regla de Control de Acceso* existente agregando con un símbolo de *!* que se denegará el acceso a la *Lista de Control de Acceso* denominada *listaextensiones*:

```
http_access allow redlocal !listaextensiones
```