INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

SEMINARIO DE TITULACIÓN
"SEGURIDAD DE LA INFORMACIÓN"

TESINA

MONITOREO DEL DESEMPEÑO DE LA RED: "IMPLEMENTACIÓN DE IP SLA´S BASADAS EN ICMP EN UN ENLACE WAN"

Que presentan para obtener el Título de
Ingeniero en Comunicaciones y Electrónica

ARROYO MENDOZA RUBÉN
DEL ANGEL AQUINO EDUARDO
SALAS PLIEGO LUIS ANSELMO

Asesor:

Dr. ANTONIO CASTAÑEDA SOLÍS

VIGENCIA: DES/ESIME-CUL-2008/23/3/10

México, D.F., MAYO 2011

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

POR LA OPCIÓN DE TITULACIÓN SEMINARIO EN SEGURIDAD DE LA INFORMACIÓN

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

DEBERÁN DESARROLLAR:

ARROYO MENDOZA RUBEN
DEL ANGEL AQUINO EDUARDO
SALAS PLIEGO LUIS ANSELMO

"IMPLEMENTACIÓN DE IP SLA´S BASADAS EN ICMP EN UN ENLACE WAN"

INTRODUCCIÓN

LOS ALTOS COSTOS EN EL ALQUILER DEL ANCHO DE BANDA, GENERAN LA NECESIDAD DE GARANTIZAR LOS ACUERDOS DE NIVELES DE SERVICIO DE LOS PROVEEDORES, A TRAVÉS DE LAS HERRAMIENTAS DE MONITOREO BASADAS EN PAQUETES DE MENSAJES DE CONTROL DE INTERNET, SE PUEDE APROVECHAR AL MÁXIMO EL RENDIMIENTO DE LA RED EN UN ENLACE DE ÁREA AMPLIA. ESTE PROYECTO PROPONE LA APLICACIÓN DE LA HERRAMIENTA CACTI, QUE DETERMINA INDICADORES DE LA RED COMO LATENCIA, JITTER, PÉRDIDA DE PAQUETES Y OTRAS ESTADÍSTICAS. AL OBTENER LOS PARÁMETROS QUE SE DESEEN MONITOREAR CON LA HERRAMIENTA PROPUESTA, SE PUEDEN COMPARAR LOS ACUERDOS DE NIVEL DE SERVICIO PARA ESTABLECER Y SABER SI SE CUMPLEN DICHOS ACUERDOS CON LO CONTRATADO CON LOS DIFERENTES PROVEEDORES DE SERVICIOS DE ANCHO DE BANDA.

CAPITULADO

México D.F., Mayo de 2011

VIGENCIA: DES/ESIME-CUL-2008/23/3/10

DR. GABRIEL SÁNCHEZ PÉREZ
Coordinador del Seminario

DR. ANTONIO CASTAÑEDA SOLIS
Asesor

M. EN C. LUIS CARLOS CASTRO MADRID
Jefe de la carrera de I.C.

ÍNDICE

íNDICE DE FIGURAS

ÍNDICE DE TABLAS

Objetivo General

- Implementar un servicio de monitoreo de red el cual permita verificar el cumplimiento de los SLA.

Objetivos Particulares

- Establecer los parámetros técnicos de uso eficiente del Ancho de Banda en un enlace WAN.

- Seleccionar el Software que permita medir los parámetros de desempeño establecidos.

Planteamiento del problema

Los altos costos en el alquiler del ancho de banda, generan la necesidad de garantizar los acuerdos de niveles de servicio de los proveedores, a través de las herramientas de monitoreo basadas en paquetes de mensajes de control de internet, con acuerdos de niveles de servicio (IP SLA), esto para poder lograr que se cumplan los acuerdos que una empresa este interesada en contratar, y al mismo tiempo, que le permita aprovechar al máximo el rendimiento de la red en un enlace de área amplia. Por lo tanto, es necesario dar a conocer como se conforman dichos acuerdos de nivel de servicio, para demostrar la operación en tiempo real del monitoreo de la red. Se establecerán los parámetros y herramientas que permitan realizar dicho evento y se darán a conocer, los procesos que se deben ejecutar, así como los resultados de dicha operación, que garanticen el rendimiento de la red en un enlace de área amplia.

Justificación

Se utilizara la herramienta ***IP SLA***, que permite monitorear los acuerdos de nivel de servicio para aplicaciones y determinados indicadores de la red. Estos datos generados por IP SLA pueden ser monitoreados mediante mensajes de control de internet o directamente desde la interfaz del sistema operativo del equipo. Es por eso, que con esta herramienta se puede recopilar información del rendimiento de la red como: tiempo de respuesta, latencia, jitter, pérdida de paquetes y otras estadísticas de la red para garantizar un óptimo manejo y administración de la misma, por lo tanto, con estas herramientas los administradores deben de estar preparados para poder medir el rendimiento de la red de forma predecible, continua y confiable, y también monitorear proactivamente el estado a través de una herramienta llamada ***CACTI*** que se menciona en capítulos posteriores.

INTRODUCCIÓN

La necesidad de monitorear los componentes de una red lleva a asegurar la disponibilidad de los servicios de la red, así como la información almacenada, ya que se debe conocer en todo momento el estado de los equipos de telecomunicaciones para asegurar el correcto funcionamiento de la misma.

Se debe considerar el monitoreo de la red como una actividad importante, ya que el monitorear una red proporciona en todo momento la seguridad de detectar problemas que se pueden presentar en el flujo de datos, y no solamente para poder darles métodos de soluciones sino también para conocer cómo se comporta y saber si lo hace de manera adecuada.

La medición de la calidad del servicio, es necesaria mediante una herramienta de monitoreo en una red de área amplia (***WAN***), para así, poder analizar el tráfico en la red y poder dar más cobertura de ancho de banda a aquellos servicios que son más utilizados, mejorando la calidad del servicio prestado a los usuarios finales de la red. Los sistemas de calidad de servicio medidos con un sistema de monitoreo en las redes de datos que actualmente están aplicados a nivel mundial, no deben ser ajenos para aquellas empresas que quieran mejorar la calidad de servicio que prestan a los usuarios finales de una red de área amplia. Uno de los factores que disminuyen la velocidad de transmisión de datos en una red pueden ser los espías, ya que ocupan una pequeña porción del ancho de banda ocasionando deterioros en la red, impidiendo mantener una calidad prestada en el servicio.

Administrar la asignación del ancho de banda puede ser algo complejo. Contratar un uso de ancho de banda que sea mayor de lo que en realidad se usa, significa que la compañía está pagando por un ancho de banda que en realidad no necesita, y contratar un servicio de ancho de banda que esté por debajo del nivel de uso, puede resultar en congestión y mal desempeño de la red. El monitoreo de la red WAN se torna entonces, muy importante. Los administradores de redes necesitan optimizar la calidad del servicio balanceando la tasa de transferencia, velocidad media de transmisión, datos y el tiempo de respuesta.

Con la herramienta de monitoreo CACTI, se puede visualizar la red WAN entera ya que emite alertas en mensajes de control de Internet, cuando un enlace deja de funcionar. Esta herramienta evita tiempo de inactividad identificando previamente el mal funcionamiento de los dispositivos de la red, con la ayuda del monitoreo a través de CACTI, se crean alarmas con respecto a las fallas posibles que se puedan presentar en la transmisión de los datos.

CACTI permite generar reportes, proporcionando la información detallada de la disponibilidad de todas las interfaces. Ya que se pueden utilizar estos reportes para asegurar que los acuerdos de niveles de servicio establecidos se cumplan.

El desempeño óptimo de la red es crítico para tener un buen desempeño de la red WAN. Cuando la red experimenta congestión, CACTI le ayuda a resolver problemas rápidamente proporcionándole acceso al estado de algunas variables importantes en el desempeño como:

- Uso del CPU.
- Uso de Memoria.
- Errores.
- Voltaje, Temperatura etc.
- Estadísticas del Buffer (Aciertos, fallas y errores).

CAPITULO I: ELEMENTOS DE GESTIÓN DE RED.

La gestión de red es una combinación de tareas para controlar, informar y monitorear las entidades que conforman una red en tiempo real, esto permite que la red funcione correctamente. Estas tareas pueden estar repartidas por diferentes puntos de la red, lo cual hace que diferentes acciones, se repitan para concentrar datos y determinar una acción cada vez que sucede un evento nuevo.

1.1 Objetivos de la Gestión de Redes

Los objetivos de la gestión de una red son:

- Hacer un uso eficiente de la red al utilizar mejor los recursos disponibles, como por ejemplo el ancho de banda.
- Detectar fallos y corregirlos a la brevedad posible.
- Monitoreo del rendimiento, detección de cuellos de botella, optimización de los sistemas.
- Controlar cambios y actualizaciones en la red, de modo que ocasionen pocas interrupciones posibles, en cuanto el servicio a los usuarios.
- Hacer un seguimiento de la red entorno a la utilización de los recursos, presentación de credenciales y permisos que se tengan establecidos dentro de un sistema.

- Saber el rendimiento del sistema, como por ejemplo la utilización del procesador, de la capacidad de almacenamiento, aplicación y los tiempos de espera.
- Establecer un control de la red y de acceso al sistema.

Por lo tanto, gestionar una red, es garantizar un nivel de servicios en las entidades de un sistema al máximo tiempo posible, haciendo mínima la perdida que origina una detención o funcionamiento incorrecto del sistema. [1]

1.2 Paradigma Gestor-Agente

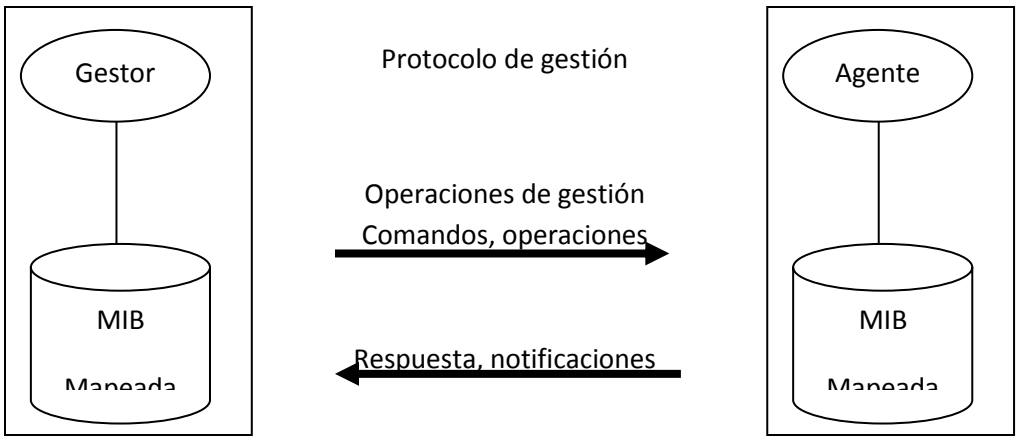
Al gestionar una red, se deben de integrar todos los elementos, esto permite teóricamente la interconexión de los recursos de telecomunicaciones y poder evitar la diferencia entre datos de gestión, métodos y protocolos de comunicación, con funcionalidad similar, así mismo se logra que la persona o personas encargadas de la administración de la red, conozcan todos los sistemas que van a utilizar perfectamente.

Los elementos de un sistema de gestión son, el gestor, el agente, el protocolo de gestión y la base de información de gestión (***MIB***). Los gestores son los elementos del sistema de administración que emite las operaciones que reciben y replican información. El agente tiene la función de responder a las directivas enviadas por el gestor. El MIB es el conjunto de objetos gestionados que representan a los recursos de la red que permiten algún tipo de gestión en una forma abstracta. El protocolo es el conjunto de especificaciones que dirigen los procesos y elementos de un sistema de gestión.

La base del funcionamiento de los sistemas de apoyo a la gestión, se basa en el intercambio de información de gestión entre nodos gestores y nodos gestionados, y es a esto que se le llama paradigma gestor – agente.

Como se puede ver en la figura 1.1, el gestor pide al agente a través del protocolo de gestión de red que realice diversas operaciones para poder conocer el estado del recurso y poder influir en el comportamiento, los agentes mantienen en cada nodo gestionado información sobre el estado y las características del funcionamiento de un determinado recurso de la red, cuando en el agente se produce alguna falla, sin necesidad de notificarle al gestor emiten notificaciones que son enviadas al gestor para que el sistema de gestión pueda actuar inmediatamente.

Figura 1.1 Paradigma Gestor – Agente.



1.3 Monitoreo

El monitoreo de una red se encarga de observar y analizar el estado de los componentes de la red, decide que información se recoge del sistema, como accede y que se hace con ella. La finalidad de recabar información de la red es con el fin de detectar anomalías y conocer el comportamiento de los recursos gestionados. Para llevar a cabo esta tarea es necesario:

- Definir la información de gestión que se administra.
- Acceso a la información que se desea monitorear.
- Diseño de políticas de monitoreo.
- Proceso de la información que se monitorea.

Existen diferentes protocolos para la gestión de red, de los cuales destaca ***SNMP*** (Protocolo Simple de Administración de la Red) que pertenece al protocolo ***TCP/IP***. Otro protocolo estándar es el ***ICMP*** (Protocolo de Mensajes de Control de Internet) de la ***ISO*** (International Organization for Standardization), que está presente en la mayoría de los servicios de telecomunicación para la gestión de redes. [2]

1.4 FCAPS

FCAPS, es una herramienta de gestión de redes de telecomunicaciones. Las letras F, C, A, P y S significan fallas, configuración, contabilidad, rendimiento y seguridad, que son necesarias para manejar diversas categorías, dentro de las tareas del modelo ISO de gestión de red. En algunos casos, el término de contabilidad se sustituye con el de Administración.

1.4.1 Gestión de Fallas (Management Fault)

En la gestión de fallas, un fallo representa una condición para que una entidad de una red, no pueda cumplir con el servicio que debe de ofrecer. La gestión de fallas, se encarga de detectar, aislar y corregir una operación anormal, debe de estar preparado para reunir una determinada porción de la red, para aislar y reparar el problema que surja en cualquier instante.

El subsistema de administración proporciona rápidamente la capacidad de copia de seguridad, prueba, y restaurar los componentes de red y sistemas. Por lo tanto es necesario implementar mecanismos para la detección de fallos, como por ejemplo alarmas u otro tipo de notificaciones al sistema.

Existen diversos problemas relacionados con la gestión de fallas, como por ejemplo: fallas no observables, fallas inciertas, donde la información de la falla, no es verdadera en cuanto al origen, puede darse el caso de una detección de fallas múltiples por una sola causa o el caso de detección de fallas por múltiples causas al aislar una o varias fallas.

La gestión de fallas tiene las siguientes tareas a realizar:

- Determinación de los síntomas del problema.
- Aislamiento del fallo.
- Resolución del fallo.
- Comprobación de la validez de la solución de la red.
- Almacenamiento de la detección y resolución del problema.

Existen diferentes tecnologías que tratan de evitar las fallas de conectividad de una red como por ejemplo: el *ping* que realiza un sondeo periódico del recurso mediante el protocolo ICMP, permite también establecer el tiempo de respuesta, para el aislamiento de fallas, se puede utilizar el comando ***traceroute***, que permite ver la ruta que siguen los paquetes hacia un nodo y que está basado en el parámetro *Time To Live* de IP.

1.4.2 Gestión de Configuración (Management Configuration)

La gestión de la configuración de la red, se encarga de las funciones orientadas a administrar de forma ordenada, los cambios que se pueden producir en la red. Se encarga de entregar información confiable y actualizada sobre la infraestructura de las redes, esta información no solo incluye información sobre elementos de configuración de la infraestructura (***CIs***), sino como estos elementos de configuración se relacionan unos con otros.

La gestión de configuración tiene 3 tareas fundamentales: recolección automatizada de datos sobre el inventario y estado de la red, tales como, versiones de software y hardware de los distintos componentes, cambio en la configuración de los recursos y almacenamiento de los datos de configuración.

La gestión de configuración, comprueba si los cambios en la infraestructura se han registrado de manera correcta, incluyendo la relación entre CIs y monitorear el estado de los componentes para garantizar un correcto uso de los mismos. Al implementar una gestión solida de la configuración, se puede proporcionar información sobre los siguientes temas:

- **Política del producto:**
  - ¿Qué componentes están en uso, versión, y por cuánto tiempo se han tenido?
  - ¿Qué componentes se pueden eliminar y cuáles necesitan actualizarse?
  - ¿Cuánto costara reemplazar ciertos componentes?
  - ¿Qué licencias se tiene? ¿Son correctas?
  - ¿Qué contratos de mantenimiento deben ser revisados?
  - ¿Hasta qué punto está estandarizada nuestra infraestructura?

- **Corrección de la información y evaluación de impactos:**
  - ¿Qué componentes se necesitan para un procedimiento de recuperación ante un desastre?
  - ¿El plan de recuperación ante un desastre, seguirá siendo eficaz si se cambian las configuraciones?
  - ¿A qué red está conectado el equipo?
  - ¿Qué componentes son responsables de los errores conocidos?

- **Provisión de los servicios y fijación de precios:**
  - ¿Cuáles son las configuraciones de componentes esenciales para ciertos servicios?
  - ¿Qué componentes se usan en cada lugar y quiénes los utilizan?
  - ¿Cuáles son los componentes que pueden ordenar los usuarios y a cuáles se les da soporte?

1.4.3 Administración de Usuarios, Recursos y Bitácoras (Management Account)

La gestión de contabilidad, también denominada administración de usuarios, recursos y bitácoras realiza estadísticas sobre la utilización de los recursos de la red para realizar ajustes, administra los nombres de los usuarios, direcciones, incluyendo servicios relacionados con directorios y permisos para el uso de los diferentes recursos de la red. La gestión de contabilidad recopila el uso de los recursos o de servicios basados en el monitoreo y la medición, asigna cuentas, mantiene bitácoras de contabilidad, monitorea las cuotas asignadas, mantiene estadísticas de uso, y finalmente, define políticas de contabilidad y tarifas, que permiten generar facturas y cargos a los usuarios.

Si varios proveedores están involucrados en la prestación de los servicios, las reglas de conciliación también pertenecen a la administración de contabilidad. Este proceso puede realizarse por un procedimiento de repartir ingresos, mediante una tarifa plana o un precio para cierta unidad de tráfico.

Los parámetros utilizados para calcular los costos incluye la cantidad de paquetes o bytes transmitidos, duración de la conexión, ancho de banda y la calidad de servicio (***QoS***) de la conexión, localización de los participantes en la comunicación, conversión de costos para servicios de Gateway (puertas de enlace), uso de recursos en los servidores, y uso de

productos de software (control de licencias). Además de los costos variables también se tienen en cuenta los costos fijos (espacio de oficina, costo del mantenimiento, depreciación de muebles y equipos, etc.). Las tareas más importantes de la gestión de contabilidad son:

- Mecanismos que informen de la actividad de cada usuario.
- Contadores que entreguen información sobre el uso de la red.
- Aplicaciones que procesen los datos recogidos, con posibilidad de definir algoritmos de asignación de costes personalizados.

1.4.4 Gestión de rendimiento (Management Performance)

La gestión de rendimiento, se utiliza para identificar problemas potenciales antes de que se conviertan en servicios que afectan a las fallas. Se puede revisar la información histórica y analizar los datos actuales para determinar las tendencias y predecir los acontecimientos. El objetivo principal es utilizar de manera óptima, todos los recursos de comunicación y el incremento de la capacidad para satisfacer las tareas que realiza a diario el usuario.

Para mejorar el rendimiento de la red se requiere conocer lo que se necesita ser mejorado. Para eso los usuarios son una buena fuente de información acerca de esas necesidades. Medir de manera eficaz el rendimiento aislado de cada uno de los distintos componentes de la red no es difícil, aunque lo difícil es establecer el rendimiento de la red cuando se combinan todos los componentes. La modificación de algún componente de la red no asegura inmediatamente un mayor rendimiento de la misma.

La gestión de rendimiento se basa en cuatro tareas:

- Recolección de datos o variables indicadoras de rendimiento, tales como la tasa promedio de éxito de la entrega de mensajes en la red (***throughput***), los tiempos de respuesta o latencia, la utilización de la línea, etc.
- Análisis de los datos, para determinar los niveles normales de rendimiento.
- Establecimiento de umbrales, como indicadores que fijan los niveles mínimos de rendimiento que pueden ser tolerados.
- Determinación de un sistema de proceso periódico de los datos de prestación de los distintos equipos, para el estudio continúo.

1.4.5 Gestión de Seguridad (Management Security)

La gestión de seguridad, establece y mantiene los criterios de acceso a los recursos de la red. Los recursos de la red, incluyen la gestión de datos y aplicaciones, de modo que el subsistema de seguridad también pueden crear y modificar los niveles de permiso para las personas que acceden al sistema de gestión de red. Este subsistema también realiza particiones de la red, según sea necesario, para la operación de la red corporativa.

La gestión de seguridad, se puede considerar como la triple A: acceso, autenticación y autorización. Por ejemplo, puede acceder a la red de un banco con su tarjeta, después tendrá que autentificar con el PIN individual, y sólo entonces se le autoriza a obtener fondos de la cuenta, asumiendo que dispone de fondos suficientes.

A menudo, incluye la seguridad física y electrónica de acceso a un centro de datos. El mismo sistema que gestiona PIN, se puede utilizar

también para mantener un registro de códigos de la puerta o tarjetas para el control de quién y cuándo entra.

Desde una perspectiva de la gestión de la red, dos aspectos de seguridad deben ser considerados en la gestión de la comunicación de información, entre el dispositivo gestionado y la gestión del dispositivo: autenticación y cifrado. La gestión de la red de información y los comandos entre los que fluye una gestión y un elemento o dispositivo administrado, tendrán que validar el remitente (es decir, la parte de autenticación) y mantener en secreto la información real (es decir, la parte de cifrado). Por ejemplo, sería una grave violación de seguridad si un intruso puede obtener información sobre cómo extraer y manipular tablas de enrutamiento. El intruso, podría encargar el router para cambiar la ruta de mesa y todos los paquetes a una estación específica.

Entre las funciones realizadas por los sistemas de gestión de seguridad, están:

- Identificación de recursos sensibles en la red, tales como ficheros o dispositivos de comunicaciones.
- Determinación de las relaciones entre los recursos sensibles de la red y los grupos de usuarios.
- Monitoreo de los puntos de acceso a los recursos sensibles de red.
- Almacenamiento de los intentos de acceso no autorizados a estos recursos, para poder realizar un análisis.

La parte de control, dentro de la gestión de redes, es la encargada de modificar parámetros, e invocar acciones en los recursos gestionados. Las tareas de control, aportan potencia a los sistemas de gestión, permiten en todo momento y de forma remota, determinar diferentes características del comportamiento de la red. Las funciones de control, están agrupadas en

diferentes funciones, la ISO realizó una clasificación de las tareas de gestión en cinco áreas: gestión de fallos, gestión de contabilidad, gestión de configuración, gestión de desempeño y gestión de seguridad (FCAPS). Estas gestiones se encuentran en la norma 7498-4 o el equivalente CCITT X.700. [3]

1.5 SLA (Service Level Agreement)

Un acuerdo de nivel de servicio (SLA), es un contrato entre una empresa y los clientes, sobre los diferentes niveles de un servicio, en función de una serie de parámetros que proporciona una empresa, esto implica que el servicio prestado haga mejor las funciones bajo determinadas condiciones y con un buen nivel de calidad, todo esto, con el fin de garantizar el compromiso que se tiene con el cliente y verificando un buen nivel de servicio.

El SLA, incluye información sobre el cliente, como nombre, descripción y dominios asociados; uno o más objetivos de nivel de servicio para detectar vulnerabilidades o tendencias hacia violaciones del SLA; crear varios niveles de servicios internos y externos ayuda a tener una completa visión de los servicios que se proporcionan al cliente.

El SLA debe de cumplir varios puntos como:

- Tipo de servicio a brindar.
- Soporte a clientes y asistencia técnica.
- Seguridad en los datos.
- Tiempo de respuesta.
- Garantía del sistema.
- Conectividad.
- Disponibilidad del sistema.

Para tener una buena calidad de los servicios prestados, al establecer los acuerdos de nivel de servicio, se deberá tener:

- **Horario de soporte:**
  Es el tiempo, en el cual a través de cualquier medio, se puede reportar un accidente o hacer una petición de soporte.
- **Tiempo máximo de respuesta:**
  Es el tiempo máximo, que el administrador tarda en responder cualquier petición de reporte o un incidente.
- **Mantenimiento y actualización de versiones:**
  Garantizar que siempre se tendrá la última versión de software para mejorar la funcionalidad, seguridad y corrección de cualquier problema que aparezca continuamente.
- **Respaldo de datos:**
  Guardar una copia de de datos y archivos, de forma que puedan ser recuperados posteriormente en caso de alguna falla, inconsistencia o perdida.

Existen a veces varios errores, a la hora de implementar los servicios a un cliente, como definir niveles de servicios inalcanzables, regulación excesiva, el que exista algún error a la hora de definir las prioridades, complejidad técnica, que haya irrelevancia, es decir, si una SLA no tiene algún efecto sobre el cliente, el objetivo no tiene sentido. [4]

CAPITULO II: ELEMENTOS TÉCNICOS PARA LA ADMINISTRACIÓN DE REDES.

2.1 TCP/IP

TCP/IP, es la base de Internet, y sirve para comunicar todo tipo de dispositivos, como las computadoras que utilizan diferentes sistemas operativos y las computadoras centrales sobre redes de área local (***LAN***) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972, por el departamento de defensa de los Estados Unidos, ejecutándolo como un medio de comunicación, para los diferentes organismos del país en una red de área extensa del departamento de defensa.

Existen varios protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra ***HTTP*** (Protocolo de Transferencia de Hipertexto), que es el que se utiliza para acceder a las páginas web, además de otros como el ***ARP*** (Protocolo de Resolución de Direcciones) para la resolución de direcciones, el ***FTP*** (Protocolo de Transferencia de Archivos) para transferencia de archivos, el ***SMTP*** (Protocolo Simple de Transferencia de Correo), el ***POP*** (Protocolo de la Oficina de Correo) para correo electrónico, ***TELNET*** para acceder a equipos remotos, entre otros más.

TCP/IP, está compuesto por cuatro capas, cada capa se encarga de determinados aspectos de la comunicación, y al mismo tiempo brinda un servicio específico a la capa superior. Estas capas son:

- Aplicación
- Transporte
- Internet
- Acceso a Red

Algunas de las capas del modelo TCP/IP, poseen el mismo nombre que las capas del modelo OSI. Por lo tanto, es necesario no confundir las funciones de las capas de los dos modelos, ya que desempeñan diferentes funciones en cada modelo.

2.1.1 Capa de Aplicación

La capa de aplicación del modelo TCP/IP, maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP, combina todas las aplicaciones en una sola capa, y asegura que estos datos estén correctamente empaquetados, antes de que pasen a la capa siguiente. TCP/IP, incluye las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, y las especificaciones para aplicaciones comunes. TCP/IP, cuenta con protocolos que soportan la transferencia de archivos, e-mail, y conexión remota, además de los siguientes:

- **FTP (Protocolo de Transferencia de Archivos):**
  Es un servicio confiable, orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.

- **TFTP (Protocolo de Transferencia de Archivos Trivial):**
  Es un servicio no orientado a conexión, que utiliza el protocolo de datagrama de usuario (UDP). Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.

- **NFS (Sistema de Archivos de Red):**
  Es un conjunto de protocolos para un sistema de archivos distribuido, desarrollado por Sun Microsystems que permite acceso a los archivos de un dispositivo de almacenamiento remoto, por ejemplo, un disco rígido a través de una red.

- **SMTP (Protocolo Simple de Transferencia de Correo):**
  Administra la transmisión de correo electrónico, a través de las redes informáticas. No admite la transmisión de datos, que no sea en forma de texto simple.

- **TELNET (TELecommunication NETwork):**
  Telnet, tiene la capacidad de acceder de forma remota a otra computadora. Permite que el usuario se conecte a un host de Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.

- **SNMP (Protocolo Simple de Administración de Red):**
  Es un protocolo, que provee una manera de monitorear y controlar los dispositivos de red, y de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.

- **DNS (Sistema de Nombre de Dominios):**
  Es un sistema que se utiliza en Internet, para convertir los nombres de los dominios y de losnodos de red publicados abiertamente en direcciones IP.

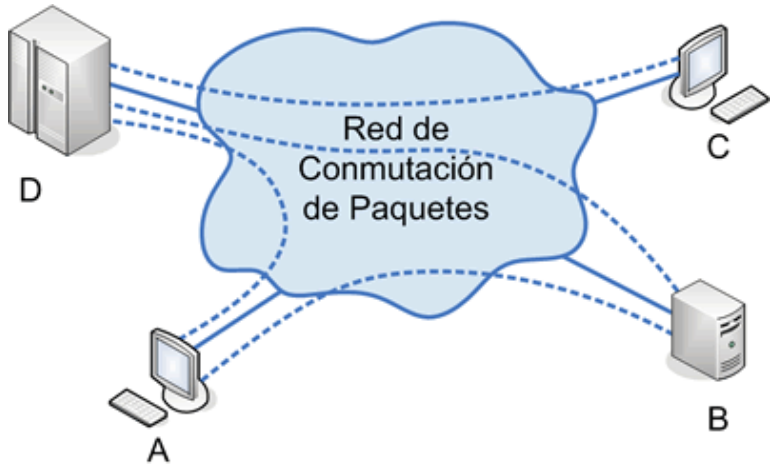
2.1.2 Capa de Transporte

La capa de transporte, proporciona servicios de transporte desde el host origen, hacia el host destino. En esta capa se forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. Los protocolos de transporte, segmentan y reensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos.

La corriente de datos de la capa de transporte, brinda transporte de extremo a extremo. La capa de transporte, envía los paquetes de datos desde la fuente transmisora, hacia el destino receptor a través de la nube de internet. Las características del protocolo TCP son, el establecimiento de operaciones de punta a punta, el control de flujo proporcionado por ventanas deslizantes y la confiabilidad proporcionada por los números de secuencia y los acuses de recibo. El control de punta a punta, que se proporciona con las ventanas deslizantes, la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando se utiliza TCP.

Como se muestra en la figura 2.1, la capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts, e incluye los siguientes servicios: segmentación de los datos de capa superior y envío de los segmentos desde un dispositivo de extremo a extremo.

Figura 2.1 Servicios de la capa de transporte



Internet es una nube, ya que los paquetes pueden tomar múltiples rutas para llegar al destino, generalmente los saltos entre routers, se representan con una nube que representa las distintas posibles rutas, debido a que nunca se sabe que ruta toman los paquetes. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. La nube maneja los aspectos tales como, la determinación de la mejor ruta, balanceo de cargas, etc.

2.1.3 Capa de Internet

La capa de Internet, tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa, es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes, ocurren en esta capa.

Protocolos Que Operan en la Capa de Internet:

- **IP** proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.
- **ICMP**, suministra capacidades de control y envío de mensajes.

- **ARP**, determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.
- ***RARP***, Protocolo de resolución inversa de direcciones, determina las direcciones IP cuando se conoce la dirección MAC.

IP es un protocolo poco confiable. Esto no significa que IP no enviará correctamente los datos a través de la red. Llamar a IP significa que no realiza la verificación y la corrección de los errores. De esta función se encarga TCP, es decir el protocolo de la capa superior, ya sea desde las capas de transporte o aplicación.

Las principales funciones del protocolo IP son: definir un paquete y un esquema de direccionamiento, transferir los datos entre la capa Internet y las capas de acceso de red y enrutar los paquetes hacia los hosts remotos.

2.1.4 Capa de Acceso de Red

La capa de acceso de red, maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red, define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión. Los estándares del protocolo de los módem, tales como el Protocolo Internet de Enlace Serial (***SLIP***) y el Protocolo de Punta a Punta (***PPP***) brindan acceso a la red a través de una conexión por módem.

Las funciones de esta capa son: la asignación de direcciones IP a las direcciones físicas, el encapsulamiento de los paquetes IP en tramas. Basándose en el tipo de hardware y la interfaz de la red, la capa de acceso de red definirá la conexión con los medios físicos de la misma.

El funcionamiento de TCP/IP, se basa en dividir la información en trozos o paquetes, que viajan de manera independiente hasta el destino, donde conforme van llegando se ensamblan de nuevo para dar lugar al contenido original, durante este proceso proporciona a cada uno de ellos una cabecera que contiene diversa información, como el orden en que deben unirse posteriormente. Otro dato importante que se incluye, es la denominada suma de comprobación, que coincide con el número total de datos que contiene el paquete. Esta suma sirve para averiguar en el punto de destino si se ha producido alguna pérdida de información. Estas funciones las realizan los protocolos TCP/IP: El Protocolo de Control de Transmisión (TCP) se encarga de fragmentar y unir los paquetes y el Protocolo de Internet (IP) hace llegar los fragmentos de información al destino correcto.

A medida que se encapsulan, los paquetes son enviados mediante routers, que deciden en cada momento cuál es el camino más adecuado para llegar al destino. Dado que la carga de internet varía constantemente, los paquetes pueden ser enviados por distintas rutas, llegando en ese caso en desorden. Con la llegada de paquetes al destino, se activa de nuevo el protocolo TCP, que realiza una nueva suma de comprobación y la compara con la suma original. Si alguna de ellas no coincide se solicita de nuevo el envío del paquete desde el origen. Por fin, cuando se ha comprobado la validez de todos los paquetes, TCP los une formado el mensaje inicial.

TCP/IP, está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que *NetBEUI* ó *IPX/SPX*; además es algo más lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápido en redes con un volumen de tráfico grande donde hay que enrutar un gran número de tramas.

TCP/IP se utiliza en muchos routers y conexiones a mainframe ó a computadoras UNIX, así como también en redes pequeñas ó domésticas y en teléfonos móviles. [7]

2.2 ICMP

El Protocolo de Mensajes de Control de Internet (ICMP), es un protocolo de Internet que se centra en el control de los mensajes y la presentación de informes de errores. ICMP, está configurado para proporcionar estas funciones como mediador entre un servidor y una puerta de enlace. La presencia de ICMP ayuda a proteger la integridad de los mensajes que se transmiten de ida y vuelta entre los dispositivos, así como hacer un uso eficiente de los datagramas de Protocolo de Internet que están presentes.

ICMP, es uno de los protocolos que asume la responsabilidad directa de los mensajes de error de procesamiento. Esto puede ser especialmente útil en un entorno de red, ICMP permite a un servidor enviar mensajes de error para todos los puestos de trabajo conectados, en caso de que un programa se desconecta o no está disponible temporalmente por alguna razón. Esto hace que ICMP sea una herramienta valiosa en la interfaz del sistema operativo de la red, sin ocupar muchos recursos, al mismo tiempo.

Cada Mensaje ICMP, está compuesto por los siguientes campos: tipo, código, checksum y otras variables. Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla 2.1. El resto de campos son distintos para cada tipo de mensaje ICMP.

Tabla 2.1 Tipos de mensaje ICMP

Tipo	Tipo de mensaje
0	Respuesta de Eco
3	Destino Inalcanzable
4	Origen saturado
5	Redirección (cambiar ruta)
8	Solicitud de eco
11	Tiempo excedido para un datagrama
13	Problema de parámetros en un datagrama
13	Solicitud de fecha y hora
14	Respuesta de fecha y hora
17	Solicitud de mascara de dirección
18	Respuesta de mascara de dirección

Un host, puede comprobar si otro host es operativo mandando una solicitud de eco. Esta aplicación recibe el nombre de “Ping”. Esta utilidad, encapsula la solicitud de eco del ICMP (tipo 8) en un datagrama IP y lo manda a la dirección IP. El receptor de la solicitud de eco intercambia las direcciones del datagrama IP, cambia el código a 0 y lo devuelve al origen.

Tabla 2.2 Formato del mensaje de Eco ICMP

	Octet +0								Octet +1								Octet +2								Octet +3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
+0	Type								Code								Checksum															
+4	Identifier																Sequence number															
	Optional Data																															

Si un Gateway no puede enviar un datagrama a la dirección de destino, este manda un mensaje de error ICMP al origen. Como se puede ver en la tabla 2.3, el valor de tipo 3 corresponde a un puerto inalcanzable, y el tipo de error viene dado por el campo código, a esto se le llama códigos inalcanzables de ICMP.

Tabla 2.3 Códigos Inalcanzables.

Código	Descripción
0	Red no alcanzable
1	Host no alcanzable
2	Protocolo no alcanzable
3	Puerto no alcanzable
4	Necesaria fragmentación con la opción DF
5	Fallo de la ruta de origen
6	Red de Destino desconocida
7	Host de Destino desconocido
8	Fallo del Host de Origen
9	Red prohibida administrativamente
10	Host prohibido administrativamente
11	Tipo de servicio de Red no alcanzable
12	Tipo de servicio de Host no alcanzable

Tabla 2.4 Formato del mensaje ICMP de destino inalcanzable.

Octet +0								Octet +1								Octet +2								Octet +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Type								Code								Checksum															
Internal header plus 64 bits of datagram																															

Para contener los datagramas IP, los Gateway disponen de un buffer, si el número de datagramas es grande, el buffer se satura. En este momento, los Gateway descartan todos los mensajes que recibe, hasta que obtiene un nivel de buffer aceptable. Cada datagrama descartado, hace que el Gateway mande un mensaje ICMP de control de flujo al origen. Esto informa que un mensaje ha sido descartado. Originalmente el mensaje ICMP de control de flujo, se enviaba cuando

el buffer estaba lleno, pero esto llegaba demasiado tarde, y el sistema ya estaba saturado. El algoritmo se cambio para que el mensaje ICMP de control de flujo se enviara cuando el buffer estuviera al 50%. El formato del mensaje de control de flujo es idéntico al mensaje de inalcanzable, excepto que el tipo es 4 y el código es 0.

El formato del mensaje ICMP de control de flujo es igual al del mensaje del inalcanzable, excepto que el tipo es 5 y el valor del código es variable entre 1 y 3 como se puede ver en la tabla 2.5.

Tabla 2.5 Códigos de Redirección.

Código	Razón para la redirección
1	Por el Host
2	Por el tipo de servicio y red
3	Por el tipo de servicio y Host

Para prevenir bucles en la redirección, el datagrama IP contiene un tiempo de vida definido por el origen. A medida que cada Gateway procesa el datagrama, el valor del campo disminuye en una unidad, posteriormente el Gateway verifica si el valor del campo es 0. Cuando se detecta un 0, el Gateway manda un mensaje de error ICMP y descarta el datagrama.

El formato del mensaje de error, es igual al del mensaje de inalcanzable, pero el tipo es 11, y el código es igual a 0 (contador sobrepasado), o 1 (tiempo de re-ensamblaje de fragmento excedido). Los errores de parámetros, se producen cuando el que origina el datagrama, lo construye mal, o el datagrama está dañado. Si un Gateway encuentra un error en un datagrama, manda un mensaje ICMP de error de parámetros al origen y descarta el datagrama. El formato del mensaje ICMP de error de parámetros, es igual al de inalcanzable, pero el tipo es 12, y el código es 0 si se utilizan punteros, o 1 si no se utilizan.

El mensaje, fecha y hora del ICMP, es una herramienta útil para diagnosticar problemas de internet, y recoger información acerca del rendimiento. El protocolo ***NTP*** (Protocolo de Tiempo de Red), puede utilizarse para marcar el tiempo inicial, y puede guardar la sincronización en milisegundos del reloj.

Como se puede observar en la tabla 2.6, el mensaje fecha y hora tiene los siguientes campos: tipo, código, checksum, identificador, numero de secuencia, fecha y hora de origen, fecha y hora del receptor y fecha y hora de transmisión. El tipo es igual 13 para el origen y 14 para el Host remoto. El código es igual a cero. El identificador y el número de secuencia se usan para identificar la respuesta. La fecha y hora de origen, es el tiempo en el que el emisor inicia la transmisión, la fecha y hora del receptor, es el tiempo inicial en el que el receptor recibe el mensaje, la fecha y hora de transmisión, es el tiempo en que el receptor inicia el retorno del mensaje.

Tabla 2.6 Formato ICMP de fecha y hora.

Octet +0								Octet +1								Octet +2								Octet +3							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Type								Code								Checksum															
Identifier																Sequence number															
Originate Timestamp																															
Receive Timestamp																															
Transmit Timestamp																															

Cuando un Host quiere conocer la máscara de subred de una LAN física, puede mandar una solicitud ICMP de mascara de subred. El formato es igual a los primeros ocho octetos del ICMP de fecha y hora. El valor del campo tipo es 17 para la solicitud de mascara de subred y 18 para la respuesta. El código es 0, y el identificador y el número de secuencia se utilizan para identificar la respuesta.

Los mensajes ICMP, son construidos en el nivel de capa de red. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP y transmite el datagrama resultante de manera habitual. Por ejemplo, cada router que reenvía un

datagrama IP, tiene que disminuir el campo de tiempo de vida (***TTL***) de la cabecera IP en una unidad; si el TTL llega a 0, un mensaje ICMP "Tiempo de Vida se ha excedido en transmitirse" es enviado a la fuente del datagrama.

Cada mensaje ICMP es encapsulado directamente en un solo datagrama IP, y por tanto no garantiza la entrega del ICMP. Aunque los mensajes ICMP son contenidos dentro de datagramas estándar IP, los mensajes ICMP se procesan como un caso especial del procesamiento normal de IP. En muchos casos, es necesario inspeccionar el contenido del mensaje ICMP y entregar el mensaje apropiado de error a la aplicación que generó el paquete IP original, aquel que solicitó el envío del mensaje ICMP. [9]

2.3 SYSLOG

En SYSLOG, existe un equipo servidor ejecutando el servidor de syslog, conocido como syslogd (demonio de syslog). El cliente envía un pequeño mensaje de texto (de menos de 1024 bytes).Los mensajes de syslog se suelen enviar vía ***UDP*** (Protocolo de Datagrama de Usuario), por el puerto 514, en formato de texto plano. Algunas implementaciones del servidor, como syslog-ng, permiten usar TCP en vez de UDP, y también ofrecen *Stunnel* para que los datos viajen cifrados mediante *SSL/TLS*.

Aunque Syslog tiene algunos problemas de seguridad, la sencillez con la que se ha creado hace que muchos dispositivos lo implementen, tanto para enviar como para recibir paquetes. Eso hace posible integrar mensajes de varios tipos de sistemas en un solo repositorio central. El mensaje enviado, se compone de tres campos: prioridad, cabecera y texto. Entre estos tres han de sumar no más de 1024 bytes, pero no hay longitud mínima. La prioridad es un número de 8 bits, que indica tanto el recurso (tipo de aparato que ha generado el mensaje) como la severidad (importancia del mensaje), números de 5 y 3 bits respectivamente. Los códigos de recurso y severidad, los decide libremente la aplicación, pero se suele

seguir una convención para que clientes y servidores se entiendan. En la tabla 2.7 se muestran los códigos observados en varios sistemas. Fuente: **RFC 3164.**

Tabla 2.7 Códigos de severidad.

0	Mensajes del kernel
1	Mensajes del nivel de usuario
2	Sistema de correo
3	Demonios de sistema
4	Seguridad/Autorización
5	Mensajes generados internamente por syslogd
6	Subsistema de impresión
7	Subsistema de noticias sobre la red
8	Subsistema UUCP
9	Demonio de reloj
10	Seguridad/Autorización
11	Demonio de FTP
12	Subsistema de NTP
13	Inspección del registro
14	Alerta sobre el registro
15	Demonio de reloj
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4
21	Uso local 5
22	Uso local 6
23	Uso local 7

Los 3 bits menos significativos del campo prioridad dan 8 posibles grados. Fuente: **RFC 3164**. La tabla 2.8 muestra el cálculo de prioridad:

Tabla 2.8 Cálculo de la prioridad.

0	Emergencia: el sistema está inutilizable
1	Alerta: se debe actuar inmediatamente
2	Crítico: condiciones críticas
3	Error: condiciones de error
4	Peligro: condiciones de peligro
5	Aviso: normal, pero condiciones notables
6	Información: mensajes informativos
7	Depuración: mensajes de bajo nivel

Para conocer la prioridad final de un mensaje, se aplica la siguiente fórmula:

Prioridad = (Recurso X 8) + Severidad

Por ejemplo, un mensaje de kernel (Recurso=0) con (Severidad=0) (emergencia), tendría Prioridad igual a 0*8+0 = 0. Uno de FTP (11) de tipo información (6) tendría 11*8+6=94. Como se puede observar, valores más bajos indican mayor prioridad.

El segundo campo de un mensaje syslog, la cabecera, indica tanto el tiempo como el nombre del ordenador que emite el mensaje. Esto se escribe en codificación ASCII (7 bits), por tanto es texto legible.

Posteriormente viene el nombre de ordenador (hostname), o la dirección IP si no se conoce el nombre. No puede contener espacios, ya que este campo acaba cuando se encuentra el siguiente espacio.

Lo que queda de paquete syslog al llenar la prioridad y la cabecera, es el propio texto del mensaje. Éste incluirá información sobre el proceso que ha generado el aviso, normalmente al principio (en los primeros 32 caracteres) y acabado por un carácter no alfanumérico (como un espacio, ":" o "["). Después, viene el contenido real del mensaje, sin ningún carácter especial para marcar el final. [10]

Implementaciones de SYSLOG

- UNIX:

  - sysklogd.
  - rsyslogd: Implementa syslog sobre TCP y sigue el RFC 3195.
  - syslog-ng: TCP, SSL, SQL.

- Windows 2000, 2003, XP:

  - HDC Syslog: parte de los productos HDC.
  - Kiwi Syslog Daemon.
  - NetDecision LogVision.
  - WinSyslog.
  - NTsyslog.
  - Syslserve.
  - Syslog Watcher.

2.4 SNMP

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

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

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

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

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

Un NMS, ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's, deben existir en cualquier red administrada. Los dispositivos administrados, son supervisados y controlados usando cuatro comandos SNMP básicos: lectura, escritura, notificación y operaciones transversales.

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

El comando de escritura, es usado por un NMS para controlar elementos de red. El NMS, cambia los valores de las variables almacenadas dentro de los dispositivos administrados. El comando de notificación es usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS.

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

Para realizar las operaciones básicas de administración, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes. Utilizar un mecanismo de este tipo, asegura que las tareas de administración de red no afecten al rendimiento global de la misma, ya que se evita la utilización de mecanismos de control y recuperación como los de un servicio orientado a la conexión, por ejemplo TCP. Los puertos comúnmente utilizados para SNMP se pueden ver en la tabla 2.9.

Tabla 2.9 Puertos para SNMP.

Número	Descripción
161	SNMP
162	SNMP-trap

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el formato de la tabla 2.10

Tabla 2.10 Formato de paquetes SNMP.

Versión	Comunidad	SNMP PDU

- **Versión:**
  Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1).
- **Comunidad:**
  Nombre o palabra clave que se usa para la autenticación. Generalmente, existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private".

- **SNMP PDU**:
  Contenido de la unidad de datos del protocolo, el que depende de la operación que se ejecute.

Los mensajes *GetRequest, GetNextRequest, SetRequest* y *GetResponse* utilizan la estructura en el campo SNMP PDU de la tabla 2.11

Tabla 2.11 Estructura de los mensajes SNMP.

Tipo	Identificador	Estado de error	Índice de error	Enlazado de variables

- **Identificador:** Es un número utilizado por el NMS y el agente para enviar solicitudes y respuesta diferentes en forma simultánea.

- **Estado e índice de error:** Sólo se usan en los mensajes GetResponse´ (en las consultas siempre se utiliza cero). El campo "índice de error" sólo se usa cuando "estado de error" es distinto de 0 y posee el objetivo de proporcionar información adicional sobre la causa del problema. El campo "estado de error" puede tener los siguientes valores:

- 0: No hay error.
- 1: Demasiado grande.
- 2: No existe esa variable.
- 3: Valor incorrecto.
- 4: El valor es de solo lectura.
- 5: Error genérico.

- **Enlazado de variables:**
  Es una serie de nombres de variables con los valores correspondientes (codificados en ASN.1).

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

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

El mensaje SetRequest, es utilizado por el NMS para solicitar a un agente y modificar valores de objetos. Para realizar esta operación, el NMS envía al agente una lista de nombres de objetos con los correspondientes valores.

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

Una trap, es generada por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente, como se puede ver en la tabla 2.12

Tabla 2.12 Formato de la PDU.

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

- **Enterprise:**

  Identificación del sub-sistema de gestión emitido por el trap.

- **Dirección del agente:**

  Dirección IP del agente emitido por el trap.

- **Tipo genérico de trap:**
  - Coldstart (0): Indica que el agente ha sido inicializado o reinicializado.
  - Warm start (1): Indica que la configuración del agente ha cambiado.
  - Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva).
  - Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa).
  - Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad).
  - EGP neighbor loss (5): Indica que en sistemas en que los ruteadores están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio.
  - Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.

- **Tipo específico de trap:**
  Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico.
- **Timestamp:**
  Indica el tiempo que ha transcurrido entre la reinicialización del agente y la generación del trap.
- **Enlazado de variables:**
  Se utiliza para proporcionar información adicional sobre la causa del mensaje.

El mensaje GetBulkRequest,es usado por un NMS que utiliza la versión 2 ó 3 del protocolo SNMP, en este sentido, es similar al mensaje GetNextRequest usado en la versión 1 del protocolo, sin embargo, GetBulkRequest es un mensaje que implica un método mucho más rápido y eficiente, ya que a través de un solo mensaje es posible solicitar la totalidad de la tabla. Un NMS que utiliza la versión 2 ó 3 del protocolo SNMP, transmite un mensaje de este tipo a otro NMS con las mismas características, para notificar información sobre objetos administrados.[11]

2.5 NTP

Network Time Protocol (NTP), es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como una capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

El demonio NTP de Unix, es un proceso de nivel de usuario que se ejecuta continuamente en la máquina que soporta NTP, y la mayor parte del protocolo está implementado en este proceso de usuario. Para obtener el mejor rendimiento de NTP, es importante tener un reloj NTP estándar con lazo de seguimiento de fase implementado en el kernel del sistema operativo, en vez de sólo usar la intervención de un demonio NTP externo: todas las versiones actuales de GNU/Linux y Solaris soportan esta característica. [12]

CAPITULO III: ESTABLECIMIENTO DE PARÁMETROS DE MONITOREO

La función principal de IP SLA, es supervisar el trafico activo de la red de manera continua y esta debe ser con un alto grado de eficiencia y de manera confiable, tratar de predecir cuales son y como poder resolver de manera eficiente, los problemas que se pueden presentar, esto es, garantizar el rendimiento de la red de un punto a otro sobre la misma red.

El trafico que se genera en la red, son las aplicaciones de la misma tales como VoIP, videoconferencia y datos, esta información se recopila generando los parámetros de monitoreo tales como “jitter”, “troughput”, “latencia” y “perdida de paquetes”.

3.1 Latencia

La latencia, es el tiempo transcurrido entre un evento y el instante en el que el sitio remoto lo escucha u observa, y puede ser inducida por el proceso de codificación y decodificación de los equipos de videoconferencia, los sistemas intermedios en la red y la distancia que deben recorrer los paquetes para llegar al destino.

Es poco lo que se puede hacer para resolver un asunto de latencia, a menos que se trabaje de cerca con los proveedores de acceso a la red o se forme parte de una red de alto desempeño. Mientras que un enlace intercontinental de fibra óptica, puede tener una latencia de 90 o 100 milisegundos (ms), otro donde se empleen transmisiones satelitales, alcanza hasta los 200 ms. [15]

El efecto de una latencia muy alta es lo que se conoce como la comunicación “cambio y fuera” o de “walkie-talkie”. Dado que los paquetes de datos tardan en llegar, las personas que participan en una sesión interactiva no tienen noción exacta de cuándo el sitio remoto dejó de hablar, y la persona que acaba de dar el mensaje percibe que no le responden lo rápido que debería ser y, en ocasiones, asume que el enlace se ha caído. Para latencias de 50 ms el efecto es casi imperceptible, pero arriba de 150 ms ya los usuarios lo detectan, o al menos hay que hacerlo saber. Adicionalmente, puede presentarse la falta de sincronía entre el movimiento de los labios del ponente y la voz. Algunos equipos terminales tratan de compensar esto con bancos de memoria que almacenan los datos que arriban primero, para sincronizarlos con los de latencia más alta.

Ejemplo de latencia por periodo:

Figura 3.1 Gráfico Diario (5 Minutos Promedio).

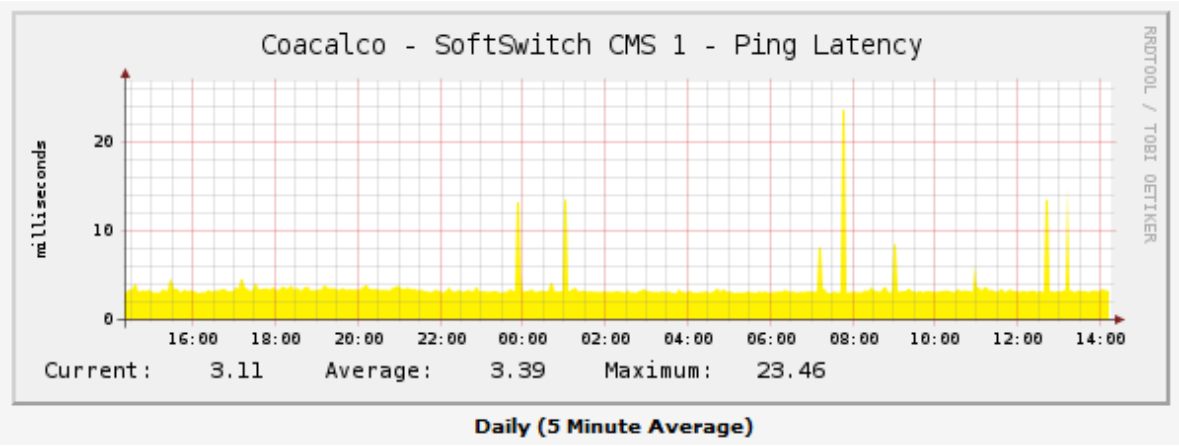


Figura 3.2 Gráfico Semanal (30 Minutos Promedio).

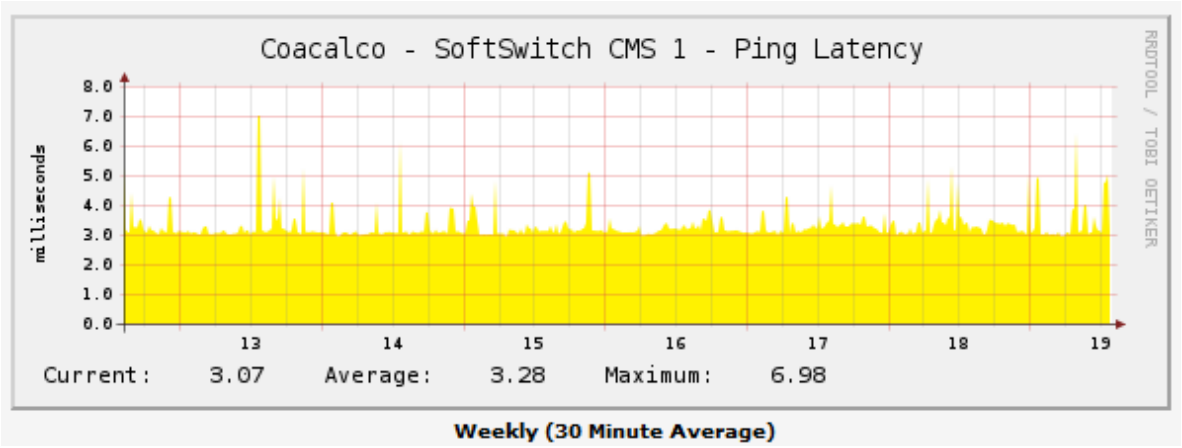


Figura 3.3 Gráfico Mensual (2 Horas Promedio).

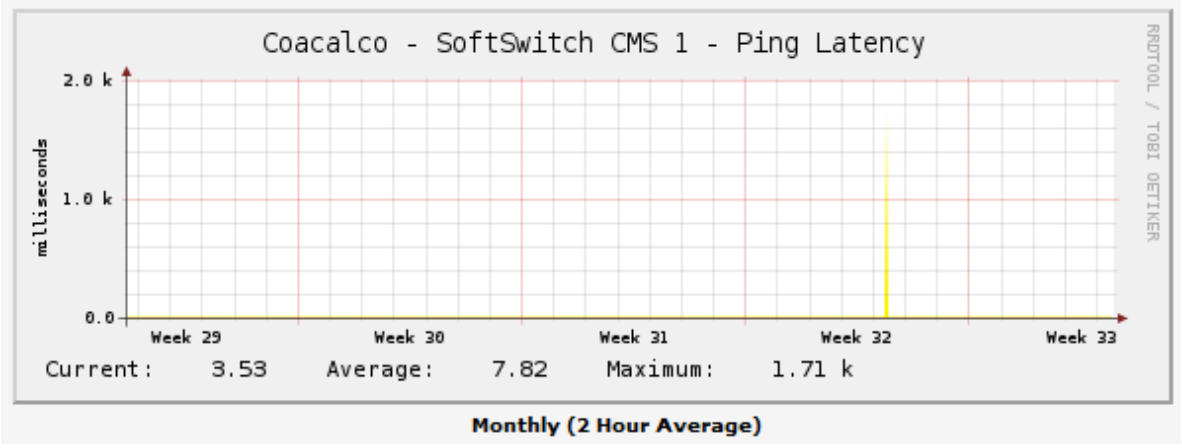
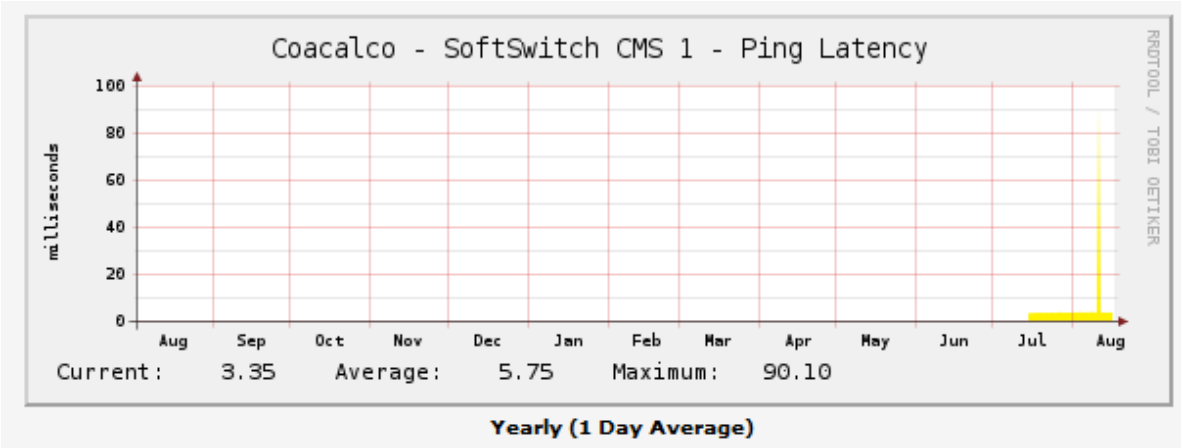


Figura 3.4 Gráfico Anual (1 Día Promedio).



3.2 Jitter

El Jitter, es la medida en micro o nano segundos de las diferencias de latencia entre los paquetes de una transmisión y en las medidas en el punto de llegada. Si el valor del jitter es alto, la calidad en una aplicación de tiempo real, como la voz sobre ip (VoIP), se verá afectada. Existen varias formas de medir el jitter, una de ellas es obteniendo el promedio de la diferencias, en el tiempo de llegada de paquetes consecutivos, para esto se calcula el absoluto de la diferencia del delay de dos paquetes consecutivos t1 y t2: abs(t2-t1) y se obtiene:

MPPDV = promedio (abs (t (i) – t (i-1)))donde t(i) es el delay de cada paquete a través del tiempo.

El jitter es la variación aleatoria de la latencia, cuyo origen puede estar en el mismo equipo terminal (aplicaciones en una PC que compiten por el uso de la red), en el tráfico que temporalmente reduce las capacidades de la red a lo largo de toda la ruta ó con cambios en el camino que siguen los paquetes (saltando de un router a otro). Estos cambios aleatorios son los que provocan que los paquetes lleguen en un orden distinto al que fueron emitidos.

Para compensar dicha situación, los sistemas de videoconferencia emplean memorias temporales que permiten presentar al usuario el audio y video cuando se posee un grupo de paquetes en orden. En consecuencia, el jitter incrementa la latencia y diferentes efectos.

El dispositivo de destino, puede ser cualquier dispositivo de red que soporte ICMP, como un servidor o estación de trabajo. Debe disponer de mediciones estadísticas para el funcionamiento de IP SLA basadas en ICMP y no requiere de configuración de la característica de IP SLA de respuesta en el dispositivo de destino.

IP SLA Jitter basado en ICMP proporciona, de extremo a extremo, las medidas de rendimiento entre un dispositivo de Cisco (origen) y cualquier otro dispositivo IP (destino), utilizando ICMP, además de un umbral de violación de monitoreo proactivo a través de SNMP, como notificaciones trampa y mensajes de Syslog.

IP SLA Jitter ICMP soporta las siguientes medidas estadísticas:

- Jitter (de origen a destino y de destino a origen).
- Latencia (de origen a destino y de destino a origen).
- Ida y vuelta en tiempo de latencia.
- Pérdida de paquetes.
- Pérdida de paquetes sucesivos.
- Paquetes fuera de secuencia (de origen a destino y de destino a origen y de ida y vuelta).
- Paquetes de última hora.

Al realizar pruebas de medición distintas para el origen, destino y las rutas de destino a origen de datos, es el jitter de mucha utilidad para identificar problemas en la red, ya que los caminos de las rutas pueden ser diferentes.[13]

Configuración de IP SLA Jitter ICMP

Se configura a través de una serie de comandos o pasos.

- Habilitar.
- Configura terminal.
- IP SLA de operación-número.
- ICMP-jitter destino dirección IP.
- Segundos de frecuencia.
- La historia de la historia-parámetro.
- Identificación de propietario del propietario.

- Etiquetas de texto.
- Umbral de milisegundos.
- TOS (Type Of Service) número.
- Milisegundos de tiempo de espera.
- VRF VRF-nombre.
- Salida.
- Reacción IP SLA de configuración de la operación-número de reacción y seguimiento de elementos
- IP SLA de horario de operación
- Salida
- Muestra del resultado de la configuración de IP SLA.

Para configurar la IP SLA Jitter ICMP se siguen varios pasos, los cuales se pueden ver en la tabla 3.1

Tabla 3.1 Pasos Para configurar IP SLA JitterICMP.

Comando o acción	Propósito	
Paso 1	Habilitar Ejemplo: `Router> enable`	Activa el modo EXEC privilegiado. Introduzca la contraseña si se le solicita.
Paso 2	Configura terminal Ejemplo: `Router # configure terminal`	Entra en el modo de configuración global.
Paso 3	IP SLA de operación-número Ejemplo: `Router(config)# ip sla 10`	Comienza la configuración para una operación de IP SLA y entra en el modo de configuración IP SLA.
Paso 4	ICMP-jitter destino dirección IP Ejemplo: `Router(config-ip-sla)# icmp-jitter (IP)interval 40 num-packets 100 source-ip (IP)`	Configura la operación de IP SLA como una operación jitter ICMP y entra a IP SLA jitter ICMP en modo de configuración.

Paso 5	Segundos de frecuencia Ejemplo: `Router(config-ip-sla-icmpjitter)# frequency 30`	(Opcional) Establece la velocidad a la que una determinada IP SLA repite la operación.
Paso 6	La historia de la historia-parámetro Ejemplo: `Router(config-ip-sla-icmpjitter)# history hours-of-statistics-kept 3`	(Opcional) Especifica los parámetros utilizados para la recopilación de información de estadística para la historia de una operación de IP SLA.
Paso 7	Identificación de propietario del propietario Ejemplo: `Router(config-ip-sla-icmpjitter)# owner admin Router (config-IP-SLA-icmpjitter) # propietario admin`	(Opcional) Configura el Simple Network Management Protocol (SNMP), propietario de una operación de IP SLA.
Paso 8	Etiquetas de texto Ejemplo: `Router(config-ip-sla-icmpjitter)# tag TelnetPollServer1 Router (config-IP-SLA-icmpjitter) tag # TelnetPollServer1`	(Opcional) Crea un identificador de usuario especificado para una operación de IP SLA.
Paso 9	Umbral de milisegundos Ejemplo: `Router(config-ip-sla-icmpjitter)# threshold 10000 Router (config-IP-SLA-icmpjitter) Umbral # 10000`	(Opcional) Establece el umbral de aumento (histéresis) que genera un evento de reacción y almacena la información de la historia para una operación de IP SLA.
Paso 10	milisegundos de tiempo de espera Ejemplo: `Router(config-ip-sla-icmpjitter)# timeout 10000 Router (config-IP-SLA-icmpjitter) de tiempo de espera # 10000`	(Opcional) Establece la cantidad de tiempo que una operación de IP SLA espera una respuesta del paquete de solicitud.
Paso 11	TOS (Type Of Service) número Ejemplo: `Router(config-ip-sla-icmpjitter)# tos 160 Router (config-IP-SLA-icmpjitter) # tos 160`	(Opcional) Define un tipo de servicio (TOS) de bytes en la cabecera IP de una operación de IP SLA.
Paso 12	VRF VRF-nombre Ejemplo: `Router(config-ip-sla-icmpjitter)# vrf vpn-A Router(config-IP-SLA-icmpjitter) # VRF VPN-A`	(Opcional) Permite la supervisión, en conmutación de etiquetas multiprotocolo (MPLS), redes privadas virtuales (VPN) con operaciones IP SLA.

Paso 13	Salida
	
	Ejemplo:
	
	`Router(config-ip-sla-icmpjitter)# exit`
	`Router (config-IP-SLA-icmpjitter) # exit`
		Sale de IP SLA jitter- ICMP, submodo de configuración y vuelve al modo de configuración global.

Paso 14	Reacción IP SLA de configuración de la operación-número de reacción y seguimiento de elementos Ejemplo: `Router(config)# ip sla reaction-configuration 1 react jitterAvg threshold-value 5 2 action-type trap threshold-type immediate`	(opcional) Configura algunas acciones que se produzcan sobre la base de eventos bajo el control de IOS de Cisco IP SLA.
Paso 15	IP SLA de horario de operación Ejemplo: `Router(config)# ip sla schedule 10 start-time now life forever`	Configura los parámetros de programación para un individuo de operación IP SLA.
Paso 16	Salida Ejemplo: `Router(config)# exit Router (config) # exit`	(Opcional) Sale del modo de configuración global y vuelve al modo EXEC privilegiado.
Paso 17	Muestra del resultado de la configuración de IP SLA Ejemplo: `Router# show ip sla configuration 10`	(Opcional) Muestra la configuración de los valores incluidos y los valores predeterminados para todas las operaciones de IP SLA o una operación especificada

3.3 Troughput

El throughput es la cantidad de datos en bits o bytes por segundo, es decir, la transferencia desde un origen hasta un destino, ó proceso en un tiempo especifico, por ejemplo la velocidad de transferencia de un disco duro o de una red. El throughput es medido en bits por segundo (bps), bytes por segundo (Bps), por paquetes (frames) ò por segundo (fps), una excelente utilidad para medir el throughput entre dos puntos es “Iperf”.Con IPerfse puede medir el ancho de banda y el rendimiento de una conexión entre dos host. Iperf es una herramienta cliente-servidor.

La latencia, en comparación con el troughput, es la medida de tiempo en mili o micro segundos que un paquete demora en viajar desde un origen hasta un destino. Esta medida es difícil de obtener con exactitud en una red, debido a la dificultad de la sincronización del reloj de los puntos extremos que normalmente están lejanos entre si. Para superar esta dificultad, la latencia se mide como el tiempo de ida y vuelta dividido por dos, las siglas en ingles son: Round Trip Time (***RTT***). Un ejemplo de Round Trip Time se obtiene al realizar un ping, por ejemplo al sitio www.google.com.

PING www.l.google.com (64.233.169.103): 56 data bytes

64 bytes from 64.233.169.103: icmp_seq=0 ttl=240 time=193.715 ms
64 bytes from 64.233.169.103: icmp_seq=1 ttl=240 time=215.816 ms
64 bytes from 64.233.169.103: icmp_seq=2 ttl=240 time=193.357 ms
64 bytes from 64.233.169.103: icmp_seq=3 ttl=240 time=178.569 ms
64 bytes from 64.233.169.103: icmp_seq=4 ttl=240 time=193.595 ms

Estadisticas de ping a `www.l.google.com`

6 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max/stddev = 178.569/195.010/215.816/11.913 ms

El resultado proporciona el mínimo, máximo, promedio y desviación estándar del RTT en milisegundos, para el ejemplo se tiene que el promedio a www.google.cl fue de 195.010 ms. Aquí es importante entender que el RTT es una aproximación de la latencia entre dos puntos, en este caso el primer dato se calcula en base al tiempo que un ping enviado desde el equipo se demora en ir a www.google.com y volver nuevamente al equipo y esta da como resultado 387.43ms, asumiendo que la velocidad de ida y vuelta es la misma se puede decir entonces que la latencia para el primer ping es de 193.175ms. [15]

3.4 Perdida de Paquetes

Cuando se detecta la red lenta o varios paquetes perdidos, esto puede ser ocasionado por una mala configuración en la interfaz de la misma. Así la presencia de colisiones tardías, puede indicar que nuestra interfaz esté trabajando en modo

half-duplex y que posiblemente el extremo contrario lo esté haciendo en full-duplex.

Existen una serie de pruebas que se realizan para comprobar el aumento de errores en el interfaz. Primero se reinicia los contadores.

```
Router#clear counters
```

Posteriormente se manda un ping entre las 2 interfaces problemáticas, mientras se detecta el problema, y en el momento que se detecten problemas se procederá a la revisión de los errores, como de las colisiones tardías, que proporciona la interfaz. Para dicho proceso se ejecuta el siguiente comando:

```
Router#show interf [nombre de la interfaz]
```

Dentro de la información de la interfaz, también se observa el modo de funcionamiento del mismo, y forzar en ambos extremos a trabajar en el mismo modo de trabajo. La pérdida de paquetes, significa que los elementos de la comunicación, los paquetes de datos, no llegan al destino. El problema puede tener un origen en el ancho de banda a través de toda la ruta (un usuario con un excelente enlace a Internet experimenta fallas hacia un destino que emplea un módem a 56 Kbps, lo que convierte esto en un problema) o bien, en errores de transmisión, cuyo origen más común corresponde a que alguna parte del enlace es del tipo inalámbrico, ya sea por microondas, satélite o redes locales del tipo 802.11x. Sin embargo, el problema a veces aparece en redes por cable de cobre o fibra óptica. Los efectos son sesiones de videoconferencia con video entrecortado, chasquidos de audio, video estático e incluso, la pérdida de la comunicación. [16]

CAPITULO IV:
HERRAMIENTAS DE MONITOREO.

4.1 IP SLA

IP SLA, permite a los clientes realizar diferentes análisis de los niveles de servicios y aplicaciones IP, aumenta la productividad, reduce los costos operativos y las frecuencias de interrupciones de la red de manera continua y confiable. Los clientes mediante IP SLA, pueden hacer verificaciones de los niveles de servicio, verificar la calidad de servicio, facilitar la administración de nuevos servicios y ayudar a las personas que se encargan de administrar, a solucionar problemas de la red.

IP SLA, se origino de una tecnología antes conocida como Service Assurance Agent (***SAA***), esta tecnología lleva a cabo un seguimiento activo, este seguimiento hace un análisis de tráfico para medir el rendimiento entre dispositivos y los servidores de aplicaciones de red. IP SLA lo hace mediante un enlace remoto de dispositivos IP, como por ejemplo un servidor de aplicaciones de red.

IP SLA, envía datos a la red para hacer mediciones del rendimiento entre varias ubicaciones de la red o a través de varias rutas de la red, esto lo hace en tiempo real. La información que se recopila, contiene datos sobre el tiempo de

respuesta, el periodo de ida de un solo sentido, la variación de retraso (jitter), la perdida de paquetes, la disponibilidad de los recursos de la red, el rendimiento de todas las aplicaciones que se tengan y el tiempo de respuesta del servidor. Todo esto se recopila para analizar y solucionar problemas y para diseñar topologías de red.

Dependiendo de la operación específica de IP SLA, las estadísticas de retrasos, pérdida de paquetes, jitter, la secuencia de paquetes, conectividad, ruta, tiempo de respuesta del servidor y el tiempo de descarga se supervisan en los diferentes dispositivos y se almacenan en el Protocolo Simple de Administración de Red (SNMP) y en la Base de Información de Gestión (MIB).

Al ser de nivel 2 de transporte independiente, IP SLA se pueden configurar de extremo a extremo, a fin de reflejar mejor las métricas de un usuario final. IP SLA, recoge un subconjunto único de las métricas de rendimiento como:

- Delay (tanto de ida y vuelta).
- Jitter (variación de retraso).
- Pérdida de paquetes (direccional).
- Secuencia de paquetes (pedido de paquete).
- Ruta de acceso (por salto).
- Conectividad (direccional).
- tiempo de descarga web.
- Calidad de voz.

Al basar los datos recogidos por una operación de IP SLA en notificaciones de SNMP se hace que el router reciba alertas cuando el rendimiento cae por debajo de un nivel determinado y cuando los problemas se han corregido.

IP SLA, utiliza la MIB para la interacción entre lo externo Network Management System (NMS), las aplicaciones y operaciones que se ejecutan en los dispositivos. Los administradores de red son cada vez más necesarios para apoyar los acuerdos de nivel de servicios que apoyan las soluciones de aplicación.

IP SLA ofrece varias mejoras sobre los acuerdos de nivel de servicio tradicionales.

- **Mediciones de extremo a extremo:**
  La capacidad de medir el rendimiento de un extremo de la red a la otra, permite un mayor alcance y una representación más precisa de la experiencia del usuario final.

- **Sofisticación:**
  Estadísticas tales como retardo, jitter, la secuencia de paquetes, conectividad de capa 3 y la ruta y el tiempo de descarga que se desglosan en bidireccional y números de ida y vuelta y aportan más datos que sólo el ancho de banda de un enlace de Capa 2.

- **Precisión:**
  Las aplicaciones que son sensibles a cambios en el rendimiento de la red, requieren de precisión en la medición de milisegundos.

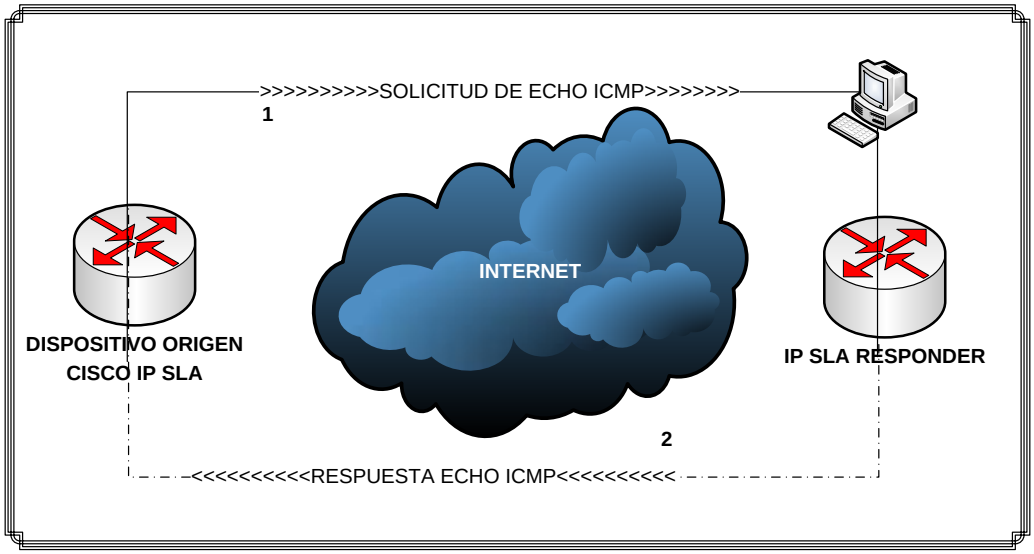
- **Facilidad de despliegue:**
  Al aprovechar la existencia de dispositivos en una gran red, hace que IP SLA sea más fácil y más barato de implementar.

La aplicación consciente de seguimiento de IP SLA, puede simular y medir el desempeño de las estadísticas generadas por aplicaciones que se ejecutan en la capa 3 a través de la capa 7. Los tradicionales acuerdos de nivel de servicio,

solamente se puede medir el rendimiento en la capa 2. IP SLA se utiliza para medir el rendimiento de tráfico generado de la red entre dos routers.

En la figura 4.1se muestra cómo IP SLA se inicia cuando el ***IOS*** (Sistema Operativo de Interconexión de Redes) de un dispositivo envía un paquete generado para el dispositivo de destino. Después de que el dispositivo de destino recibe el paquete, y dependiendo del tipo de IP de IOS SLA de operación, el dispositivo responderá con un sello de la información del tiempo de la fuente para hacer el cálculo de métricas de rendimiento. IP SLA realiza una medición de la red del dispositivo de origen y del destino a la red mediante un protocolo específico, como UDP.

Figura 4.1 IOS de IP SLA.



Para implementar IP SLA en la medición del desempeño se necesitan realizar varias tareas:

1. Habilitar el IOS de IP SLA de respuesta.
2. Configure los IOS de IP SLA en tipo de operación.
3. Configurar las opciones disponibles para el tipo específico de operación de IOS IP SLA.

4. Configurar las condiciones de umbral, si es necesario.
5. Programar la operación para ejecutar, a continuación, dejar que la operación dirigida por un período de tiempo para recopilar las estadísticas.
6. Mostrar e interpretar los resultados de la operación mediante un sistema con SNMP o NMS.

IP SLA’s permite a los clientes analizar los acuerdos de nivel de servicio de las aplicaciones y servicios IP, para incrementar la productividad, para disminuir costos operacionales y para reducir la frecuencia de cortes de la red.

IP SLA’s monitoriza el trafico que está activo para medir el rendimiento. Usando IP SLA’S, los clientes proveedores de servicios pueden proporcionar y medir los acuerdos de nivel de servicio y los clientes de la empresa pueden verificar los niveles de servicio, los acuerdos de nivel de servicio subcontratados y comprender el rendimiento de la red.

IP SLA’s puede realizar evaluaciones a la red, verificar la calidad del servicio, facilitar la implementación de nuevos servicios y ayudar a los administradores con la solución de problemas de la red.

La tabla 4.1 muestra las diferentes operaciones de IP SLA:

Tabla 4.1 Operaciones de IP SLA.

Operación De IP SLA	Mediciones	Claves de aplicaciones de seguimiento
UDP Jitter	Medida de ida y vuelta de retraso, retraso en un solo sentido, encaminamiento de una vía, perdida de paquetes en una sola vía y las pruebas de conectividad de las redes que transportan el trafico UDP, como la voz. **NOTA:** el retardo de una vía requiere la sincronización de tiempo entre los routers de origen y de destino.	• Voz y datos rendimiento de la red. • Rendimiento general de IP.
ICMP Jitter	Medidas de jitter hop – by – hop, la perdida de paquetes y las estadísticas en el retraso de medición de una red IP.	• Rendimiento de la voz y datos de la red. •Rendimiento general de la red IP.
ICMP Echo	Medidas de ida y vuelta de retardo para la Ruta completa.	• Rendimiento de la IP. • Medición de la conectividad.
Ruta de ICMP Echo	Medidas de demora de ida y vuelta y retraso Hop – by – hop de ida y vuelta.	• Medición de la conectividad. • Identificar cuellos de Botella en el camino.
HTTP	Medidas de tiempo de ida y vuelta para recuperar una página WEB.	• El rendimiento del servidor WEB.
TCP	Mide el tiempo necesario para conectarse a un dispositivo de destino con TCP.	• Rendimiento de las aplicaciones del servidor.
FTP	Medidas de ida y vuelta a la hora de Transferir un archivo.	• Rendimiento del servidor FTP.

UDP Jitter Para VoIP	Medidas de demora de ida y vuelta , retraso de un solo sentido, jitter y perdida de un solo sentido de paquetes para trafico de VoIP. Códec de simulación G.711 y G.729ª. MOS y Voz ICIPF capacidad de puntuación de la calidad.	• VoIP y el rendimiento de la red.
UDP Echo	Retraso de las medidas de ida y vuelta en el trafico de UDP.	• Rendimiento del servidor y aplicaciones IP. • Conectividad de las pruebas.
Protocolo de Configuración Dinámica de Host (DHCP)	Medidas de tiempo de ida y vuelta para obtener Una dirección IP de un servidor DHCP.	• Servidor DHCP de tiempo de respuestas.
Sistemas de Nombres de Dominio (DNS)	Medidas de búsqueda DNS tiempo.	• Rendimiento de la WEB o del servidor DNS.
Data Link Switches Plus (DLSw +)	Medidas para túneles de tiempo de respuesta.	• El tiempo de respuesta Entre DLSw + y compañeros
Frame Relay	Medidas de la disponibilidad del circuito, el retraso de ida y vuelta y la relación de la entrega del frame relay.	• Convenio del nivel de servicio de desempeño WAN.

Los beneficios al monitorear a través de ICMP es que puede realizarse remotamente, utilizando los recursos IP e Internet. También maneja la posibilidad de realizar un monitoreo a routers y a las interfaces así como de servidores IP, a pesar de que por ICMP se dé un tiempo de espera agotado, lo que puede pasar por saturación del enlace. Por ese motivo se empleara solo operaciones IP SLA de ICMP.

4.2 CACTI

Cacti es una herramienta que permite monitorear y visualizar gráficas y estadísticas de dispositivos que se encuentran conectados a una red. Se escogió esta material para monitorear debido a que en determinados momentos, se puede visualizar gráficas del estado de nuestra red como por ejemplo: ancho de banda

consumido, detectar congestiones o picos de tráfico, también como el de monitorear determinados puertos de un equipo de red.

Con Cacti podremos monitorizar cualquier equipo de red ya sea un switch, un router o un servido. Siempre que se tengan activado el protocolo SNMP y conozcamos las MIBs con los distintos ***OIDs*** (identificadores de objeto) que podemos monitorear y visualizar, podremos programar la colección de gráficas con las que queramos realizar el seguimiento. Cacti es una aplicación que funciona bajo entornos Apache, PHP y MySQL, por lo tanto, permite una visualización y gestión de la herramienta a través del navegador web. La herramienta que utiliza es ***RRDtool***, que captura los datos y los almacena en una base de datos circular, permitiendo visualizar de forma gráfica los datos capturados mediante MRTG.

RRDtool es un método que ayuda a seleccionar todos los elementos en un grupo de manera equitativa y en un respectivo orden, empezando por el primer elemento de la lista hasta llegar al último y empezando de nuevo desde el primer elemento, es decir, dentro de un sistema operativo se asigna a cada proceso una porción de tiempo equitativa y ordenada, tratando a todos los procesos con la misma prioridad.

El funcionamiento de Cacti es bastante sencillo, la aplicación sondea a cada uno de los hosts que tiene configurados solicitando los valores de los parámetros, OIDs, que tiene definidos y almacenando el valor. El período de sondeo es configurable por el administrador, éste determinará la precisión de la información a visualizar, ya que un período bajo aumentará la cantidad de datos capturados y, por tanto, la resolución de la representación gráfica. Sin embargo, un período corto de muestreo aumentará la carga del sistema.

En general, Cacti es una herramienta que está bastante bien y permite bastante juego, existen bastantes templates hechos (para distintos fabricantes, equipos, servicios, etc), y si no se encuentra lo que se busca, siempre que se tengan las MIBs de los fabricantes, uno se puede construir templates a medida (OIDs de los que extraer datos, gráficas a dibujar y hosts completos), por lo que la flexibilidad de uso es total. GPLI tiene un plugin para Cacti que permite la visualización de las gráficas de un equipo, generadas por Cacti, desde la ficha de inventario del helpdesk de GPLI, una funcionalidad bastante interesante para integrar aplicaciones.

4.3 Otras Herramientas para el Monitoreo de Redes

Nagios: es un sistema que permite monitorear redes de código abierto ampliamente utilizado, que vigila los equipos y servicios que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran el monitoreo de servicios de red (SMTP, POP3, HTTP, SNMP...), Nagios puede monitorear por ejemplo la carga del procesador, uso de los discos, memoria, estado de los puertos, independencia de sistemas operativos y la posibilidad de hacer un monitoreo remoto mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

*Nessus***:** Es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

Ethereal: es un analizador de protocolos de red para Unix y Windows, y es libre. Permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que se quiera ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal.

Snort: es una sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ejemplo: buffer overflows, escaneos indetectables de puertos, ataques a CGI, pruebas de SMB, intentos de reconocimientos de sistema operativos y mucho más. Snort utilizar un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular. Mucha gente también sugirió que la Consola de Análisis para Bases de Datos de Intrusiones (Analysis Console for Intrusion Databases, ACID) sea utilizada con Snort.

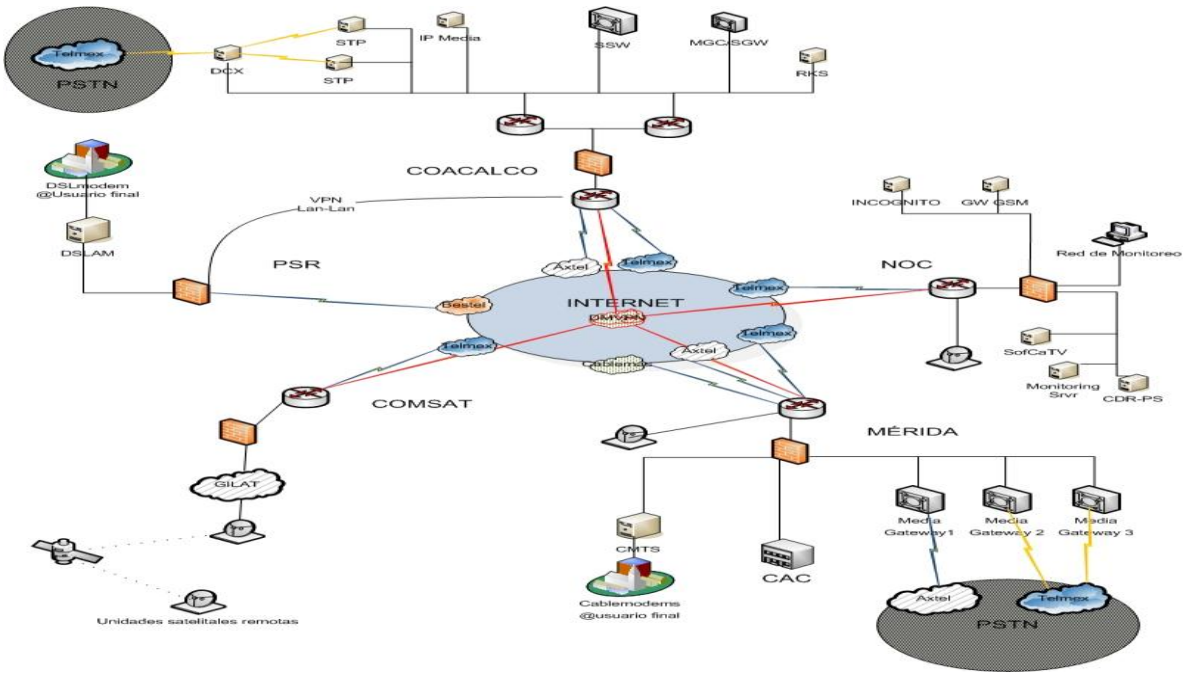
Retina: Escáner para la evaluación de vulnerabilidades no libre hecho por eEye. Al igual que Nessus y ISS Internet Scanner, la función de Retina es escanear todos los hosts en una red y reportar cualquier vulnerabilidad encontrada. Una revisión de 5 herramientas de análisis de vulnerabilidades en la revista "Information Security" de marzo del 2003 está disponible acá.

SARA: Asistente de Investigación para el Auditor de Seguridad (Security Auditor's Research Assistant). SARA es una herramienta de evaluación de vulnerabilidades derivada del infame escáner SATAN. Tratan de publicar actualizaciones dos veces al mes y de fomentar cualquier otro software creado por la comunidad de código abierto (como Nmap y Samba).

CAPITULO V: IMPLEMENTACIÓN DEL MONITOREO DE SERVICIOS.

Para la implementación del monitoreo se muestra el escenario propuesto en la figura 5.1, en el cual se observa nuestra red de área amplia, así como los dispositivos que la conforman. En un equipo de cómputo se instaló Cacti el cual permitirá monitorear cada uno de los elementos de la red haciéndole peticiones de respuesta, es decir, por medio de ICMP con el fin de conocer la información de los parámetros de monitoreo tales como: jitter, latencia, troughput, pérdida de paquete y delay.

Figura 5.1 Escenario de la red.



Se pondrán en práctica los conocimientos teóricos adquiridos y mencionados en los capítulos anteriores, como los elementos de gestión de red y elementos técnicos en la administración de una red, así como herramientas de monitoreo que permitan saber el comportamiento y conocer los parámetros que estos con llevan en una red de área amplia, esto para garantizar y brindar a un cliente un servicio con un grado de confiabilidad elevado, y con esto, aprovechar al máximo los recursos en el ancho de banda, obteniendo un beneficio al generar considerablemente los bajos costos.

Se conocerá el estado de la red, instalando la herramienta de Cacti y la configuración necesaria para gestionar los elementos y componentes de la red.

5.1 CACTI y sus Servicios

Cacti brinda muchas ventajas que se mencionaran a continuación:

- Monitorea servicios de redes (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
- Monitorea los recursos de equipos hardware en varios sistemas operativos, con los plugins NRPE_NT o NSClient++.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de las necesidades que se requieran, usando herramientas preferidas. (Bash, C++, Pert, Ruby, Python, Php, C,etc.
- Chequeo de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre hosts caídos y hosts inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos a través del correo electrónico, busca personas, SMS, o cualquier método definido por el usuario junto con el correspondiente complemento).

- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o hosts para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar host de monitores redundantes.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y graficas de comportamiento, sistemas monitorizados, y visualización de listado de notificaciones enviadas, historial de problemas, archivos de registros, etc.

Procedimiento para monitorear servicios públicos en Cacti

El libre acceso a través de la red significa que se pueden monitorear los servicios y aplicaciones ya sea en la red local o por internet. Algunos protocolos que manejan los servicios públicos son HTTP, POP3, IMAP, FTP, SSH, etc. Lo cual significa que pueden ser monitoreados por la herramienta Cacti sin necesidad de realizar alguna configuración. Al contrario de los servicios públicos, los servicios privados necesitan de un agente para poder ser monitoreados. Para que los servicios privados puedan ser monitoreados a través de diferentes sistemas operativos se necesita el protocolo SNMP, este agente permite monitorear remotamente información privada acerca del equipo.

Monitoreando routers y switches

Todos los routers y switches se pueden monitorear dependiendo del tipo de funciones que ofrece, generando así el poder asignar direcciones que pueden ser monitoreados por medio, un ping o utilizando SNMP para solicitar información sobre el estado.

El ping permite solicitar una respuesta de eco perteneciente al protocolo ICMP hacia los switches y routers, para poder visualizar o conocer el comportamiento de la perdida de paquetes, jitter, latencia, troughput, etc. Si el switch soporta SNMP, se puede monitorear el estado de diversos puertos, con el "plugincheck_snmp" y el ancho de banda, y si se utiliza MRTG se monitorea con el "plugincheck_mrtgtraf". Como se observa en la fig.

5.2 Implementación e Instalación de Cacti.

Para el correcto funcionamiento de Cacti y asegurar la escalabilidad con orden, se debe de seguir una estructura de configuración y tener previamente planteados temas como:

- Definición de una estructura de archivos y directorios acorde a la situación, haciéndolo cada vez más entendible para una posterior administración.
- Configurar apache para permitir el acceso vía web por http o https.
- En la mayoría de los equipos a monitorear mientras fuera posible instalar y dejar corriendo los servicio de SNMP.
- Configurar servicio de envío de email.
- Definir grupos de contactos a los cuales se les enviaran los avisos de notificaciones, dependiendo de qué host o servicio se trate.
- Definir grupo de host y servicios, al tenerlos agrupados y verlos más fácilmente.

Cacti se instaló en el sistema operativo Ubuntu 10, para efectuar este proceso primero se necesita:

- RRDtool 1.0.49 o 1.2.x o superior.
- MySQL 4.1.xo 5.x o superior.

- PHP 4.3.6 o superior, 5.x más recomendable para funciones avanzadas.
- Un servidor web Apache.

Instalación sobre UNIX:

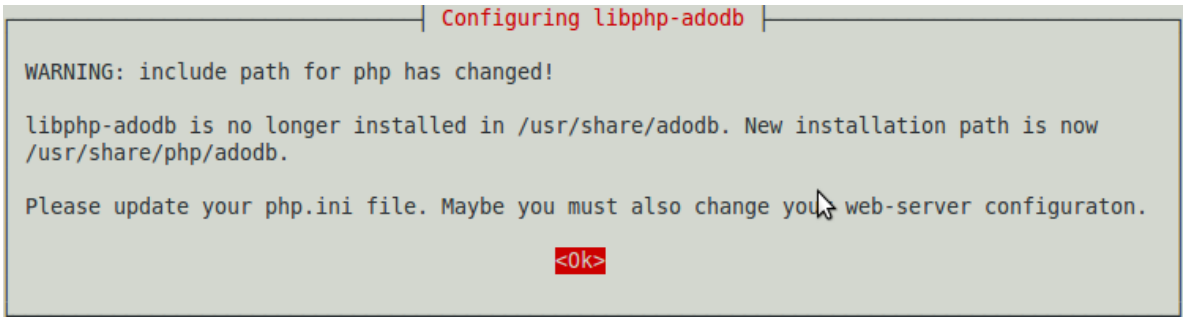
1 `sudo aptitude install php5 php5-gd php5-mysql`

Instalar Cacti usando el siguiente comando.

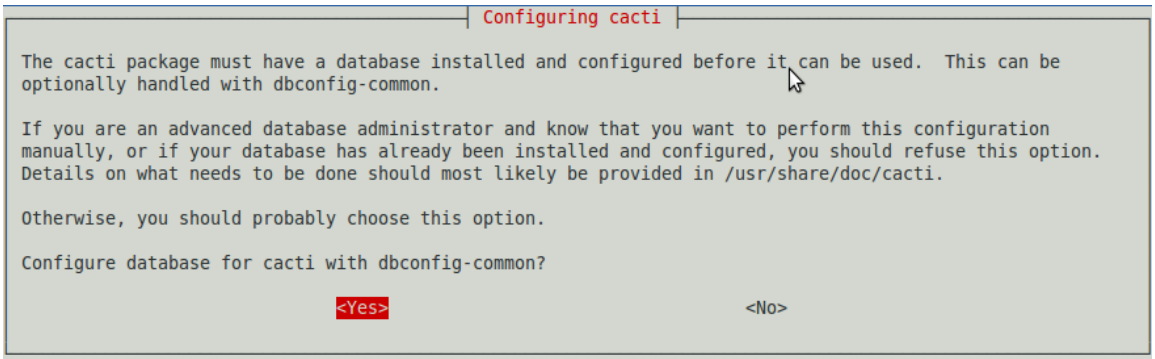
2 `sudo aptitudet install Cacti-spine`

Esto iniciara la instalación de Cacti y hará preguntas rápidas.

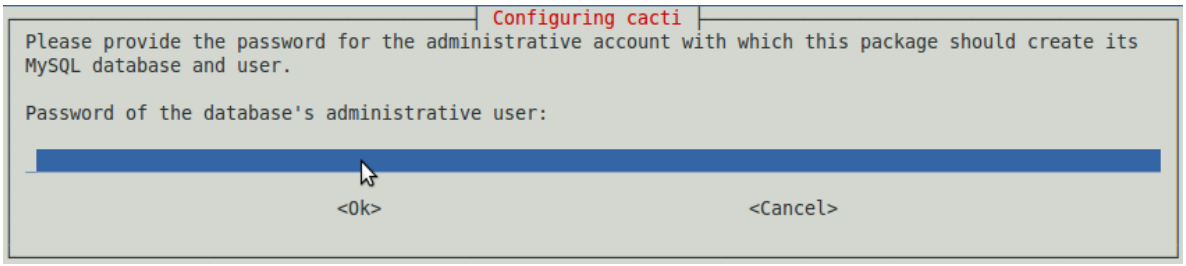
Seleccione su servidor web, en este caso estamos usando apache2, seleccione OK para continuar.



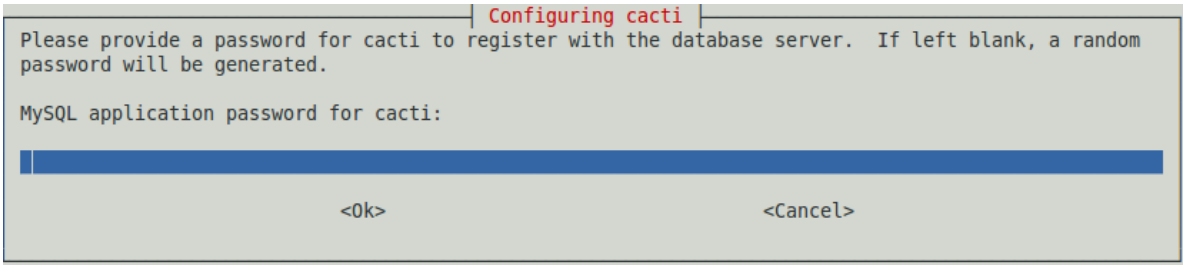
Configurar la base de datos para Cacti, seleccione Yes para continuar.



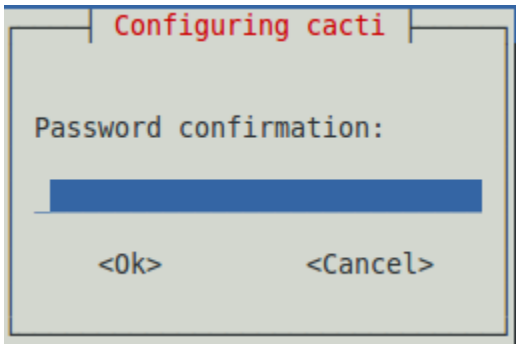
Inserte password de root para su servidor mysql seleccione OK para continuar.



Entra el password (Cacti) para la base de datos de Cacti, seleccione OK para continuar.



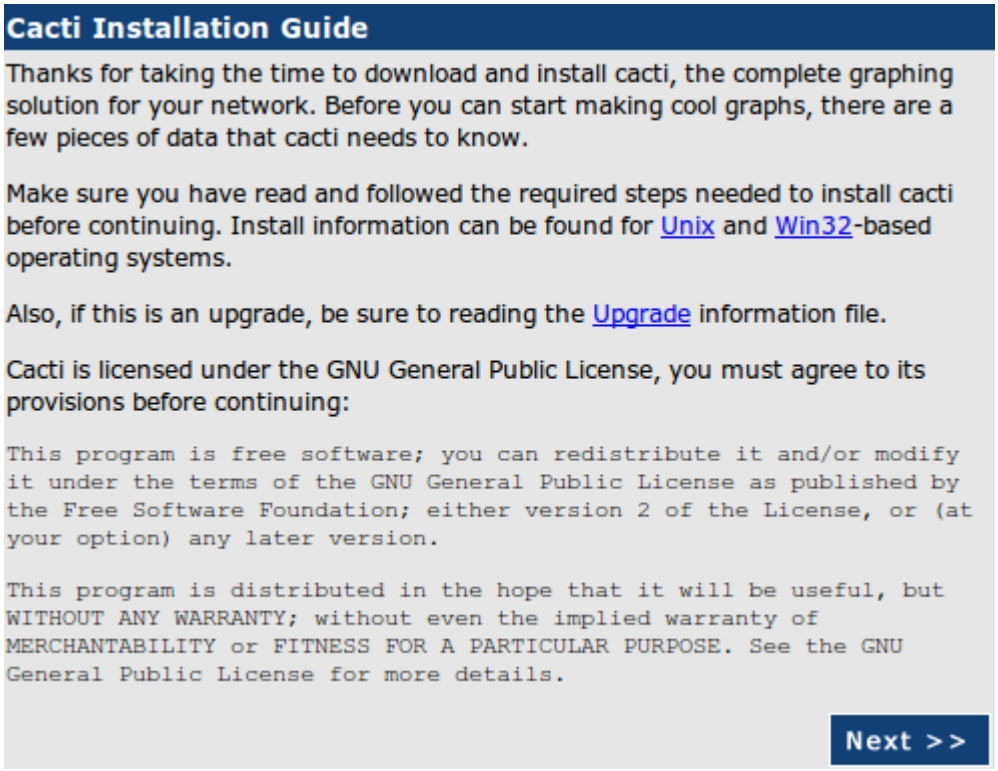
Confirme el password.



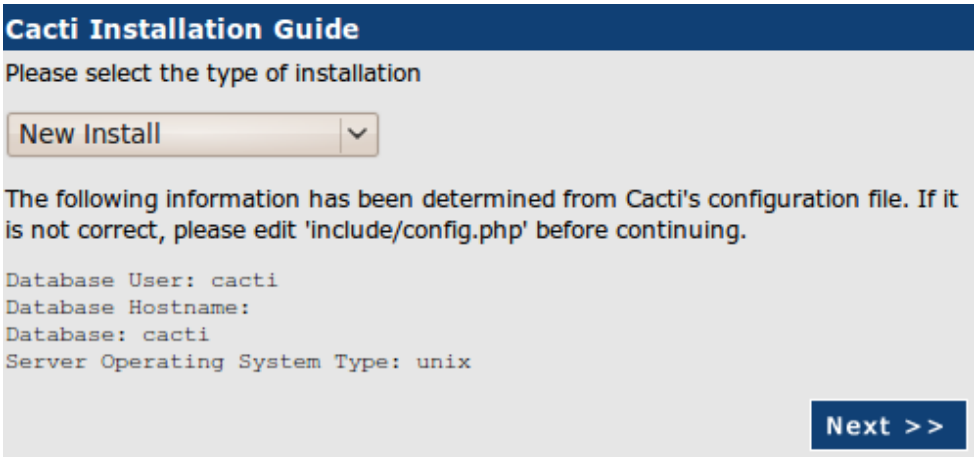
Esto completará la instalación.

Configurando Cacti.

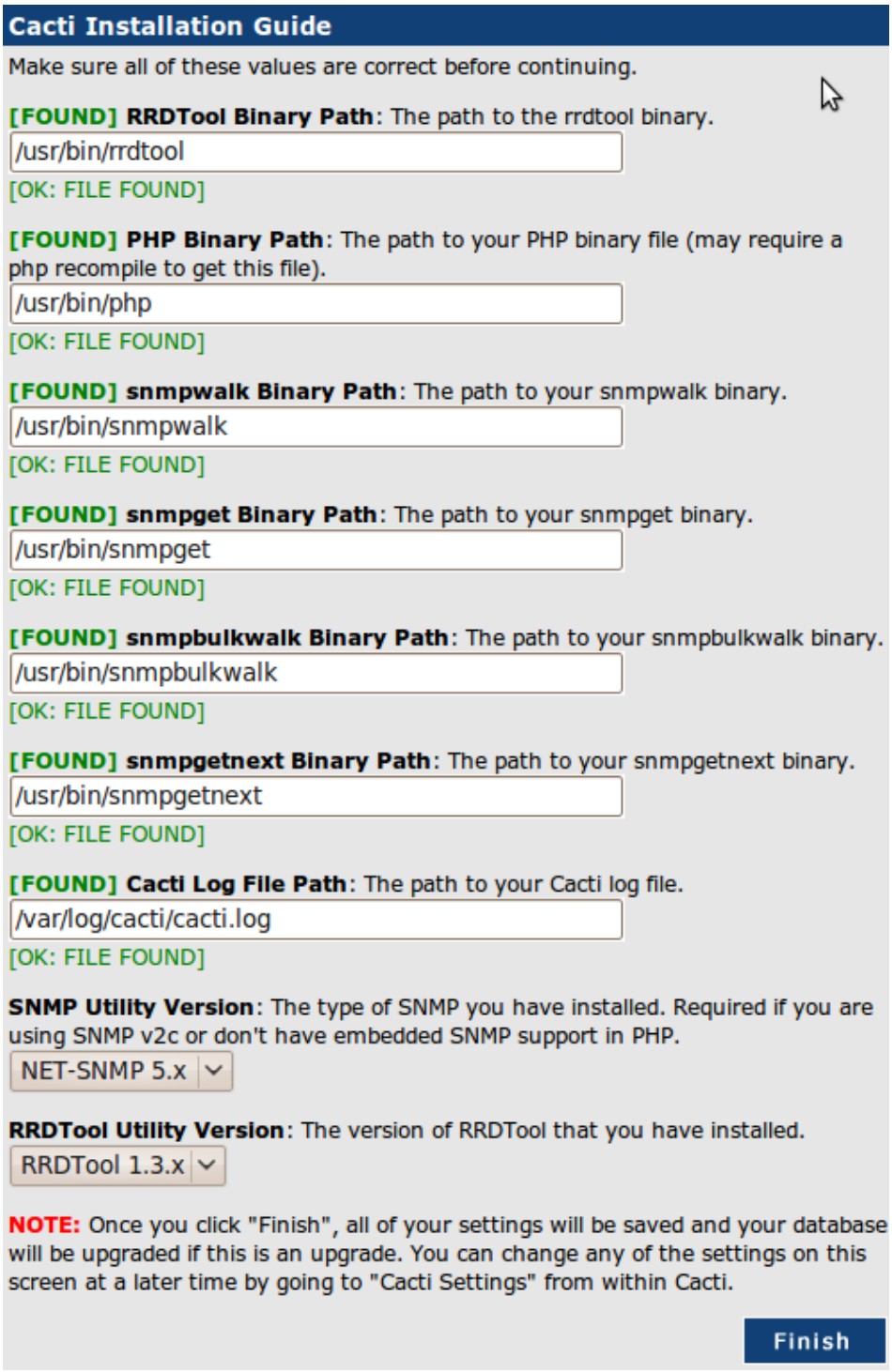
Ahora tiene que apuntar su navegador a *http://serverip/Cacti* precione Enter. Usted debed de ver una pantalla similar a esta de aquí precione Enter para continuar.



Es necesario seleccionar el tipo de instalación como instalación nueva y haga clic en Next para continuar.



Ahora se comprobará todos los caminos necesarios sean correctos o no se podrá ver esto en la siguiente pantalla, haga click en Finish.

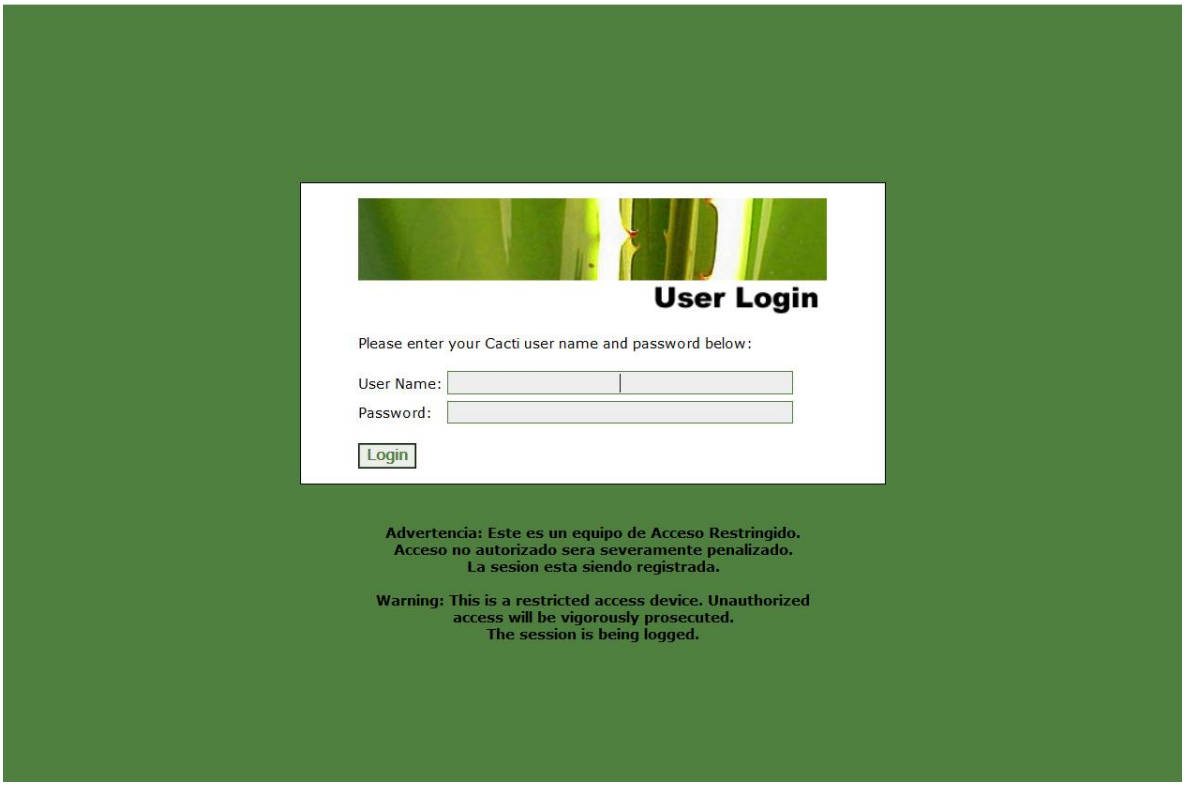


Entrar en la interface Web

Después de verificar que Cacti se haya instalado correctamente, se debe acceder a través de un explorador Web, por lo que se debe de abrir un explorador web y colocar la siguiente dirección *http://201.159.164.7.*

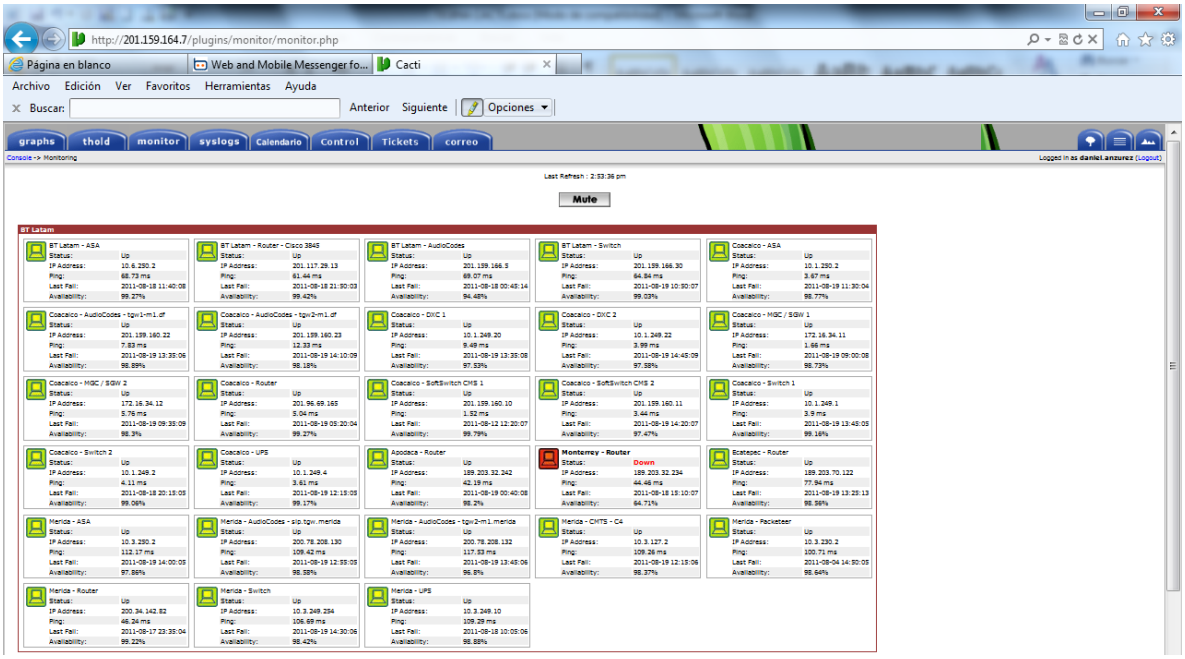
Al ingresar a la dirección IP aparecerá la imagen de la figura 5.1 quien pedirá ingresar nombre de usuario y password, la página de inicio de Cacti es de la siguiente forma.

Figura 5.1 Interfaz web de Cacti.

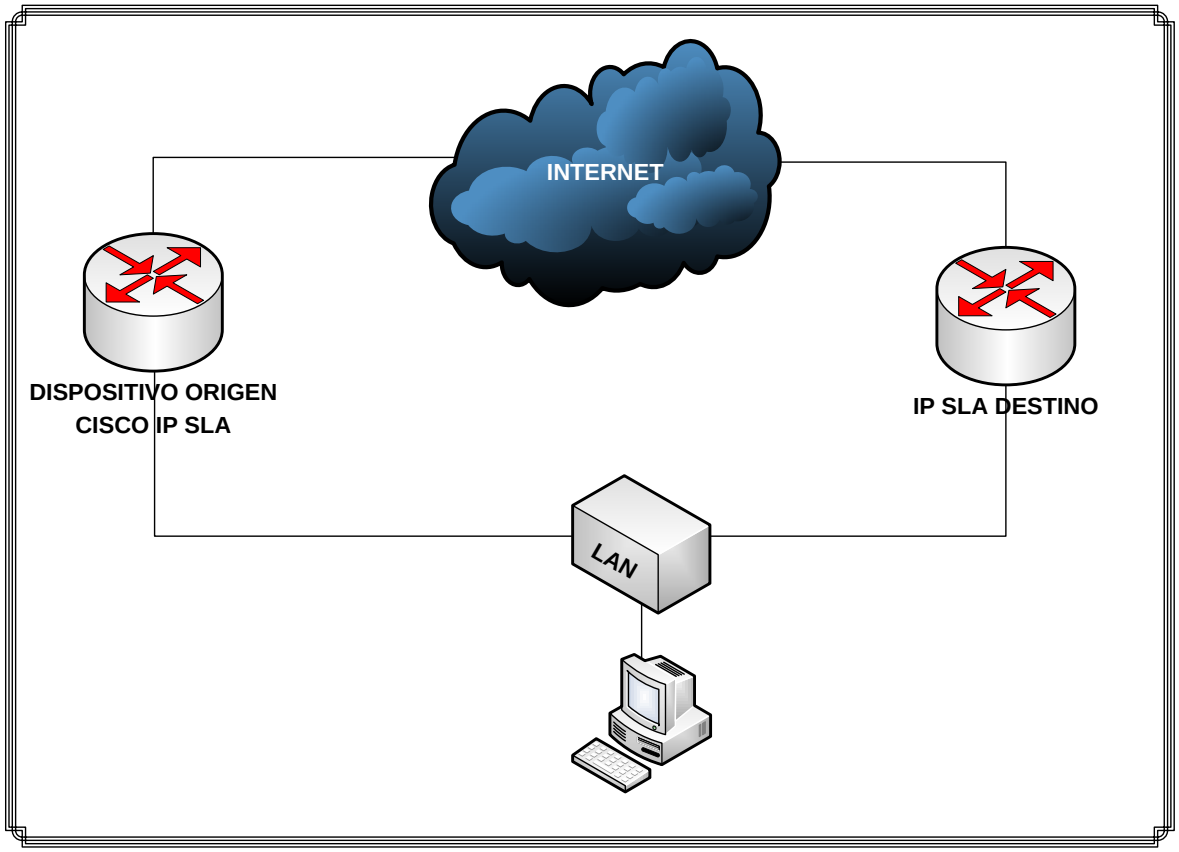


Se diseñan plugins para monitorear todos los equipos de los enlaces que se requieran verificar para conocer y determinar si los mismos operan correctamente. Esto se hace para monitorear todos los hosts de la red como se muestra en la figura 5.2. Los equipos que aparecen de color verde indican que se encuentran estables y que no existe ningún problema de operación en ellos. Los equipos de color rojo indican que se alarman debido a una pérdida de conectividad, por lo que se requiere del operador para saber que está pasando en ese momento y tratar de solucionar el problema.

Figura 5.2 Cacti instalado.



CAPITULO VI: RESULTADOS.

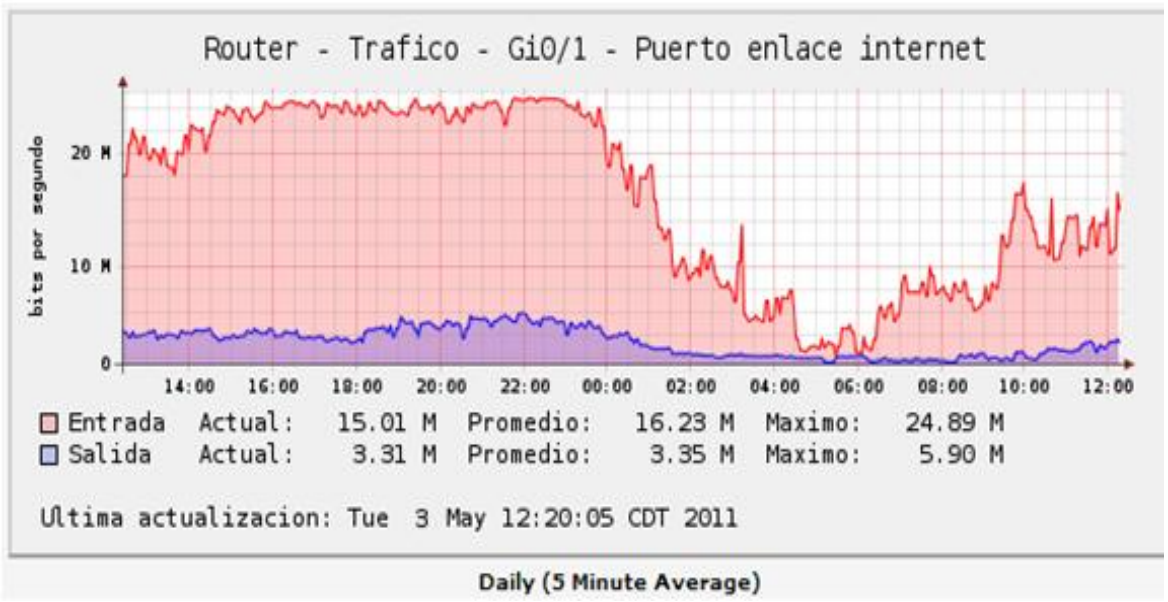


Como se puede observar, en la primera imagen se observa que desde el dispositivo de origen, manda la solicitud de eco de respuesta para monitorear el equipo deseado en el otro extremo, saliendo hacia la red local en donde se obtienen los valores de las solicitudes enviadas y se puede observar el comportamiento del enlace de la red del equipo monitoreado.

El SLA que se comparara debe de cumplir varios puntos como:

- Enlace de datos y voz
- Soporte a clientes y asistencia técnica.
- Tiempo de respuesta de 5 a 15 minutos.
- Conectividad 99.9999999 %.
- Ancho de banda 25 Mbps.

Figura 5.3 Gráfico Diario (5 Minutos Promedio) y diagrama de IP SLA



En esta gráfica se observa como el ancho de banda ha sido sobrepasado de acuerdo a los niveles de servicio establecidos en el contrato, que en su caso era 25Mbps,al observarse este evento en las graficas se le alerta al cliente que es necesario contratar un mayor ancho de banda o tomar las medidas necesarias, para ello garantizar un buen servicio.

Figura 5.4 Gráfico Diario (5 Minutos Promedio)

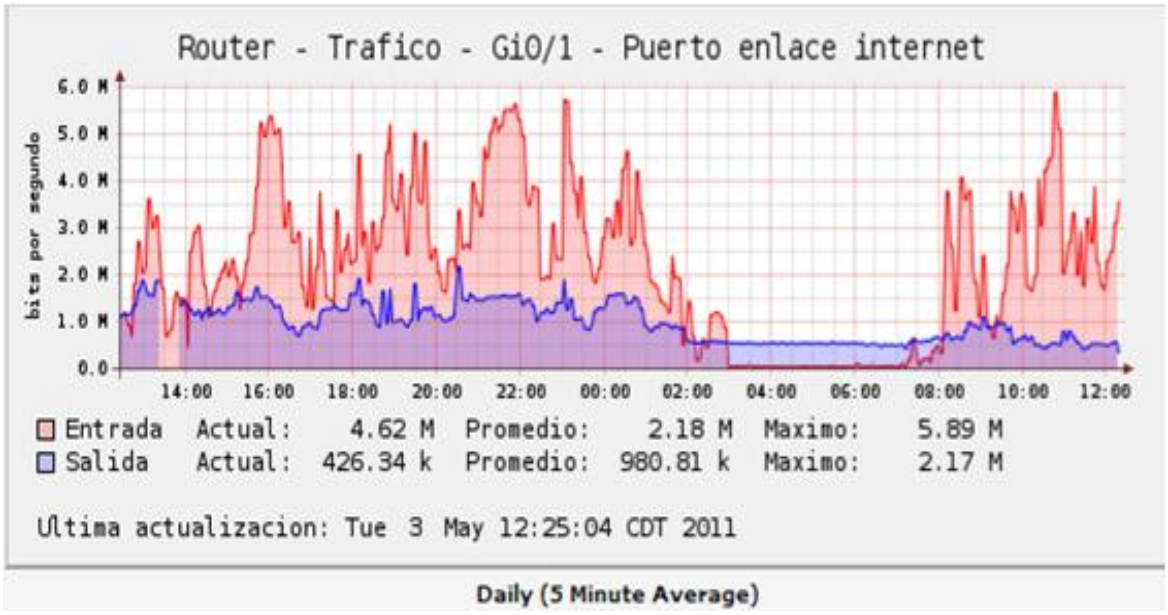


Figura 5.5 Gráfico por semana

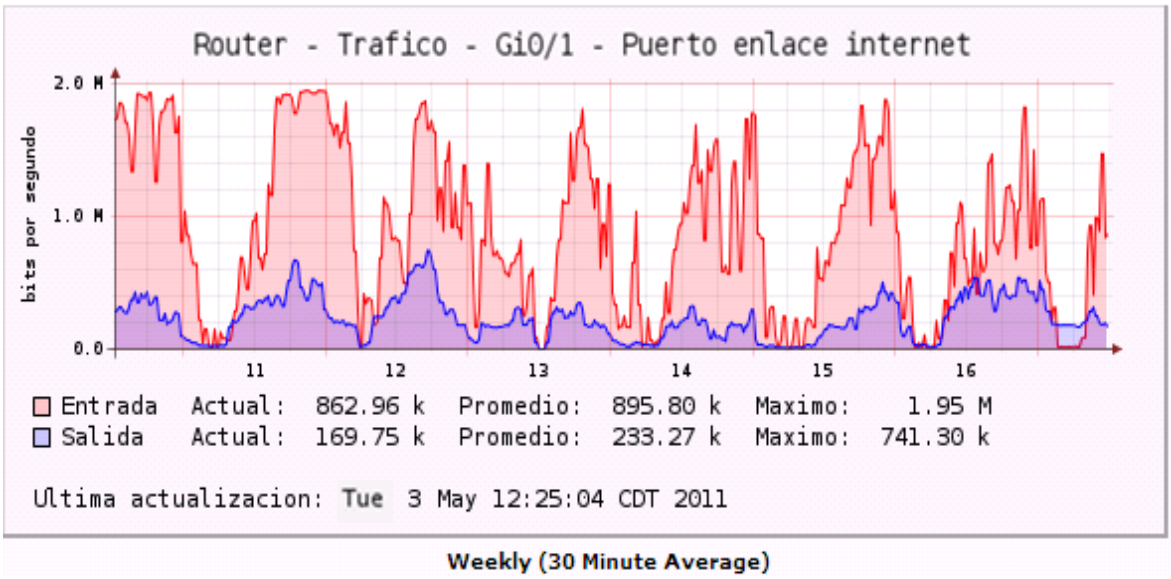
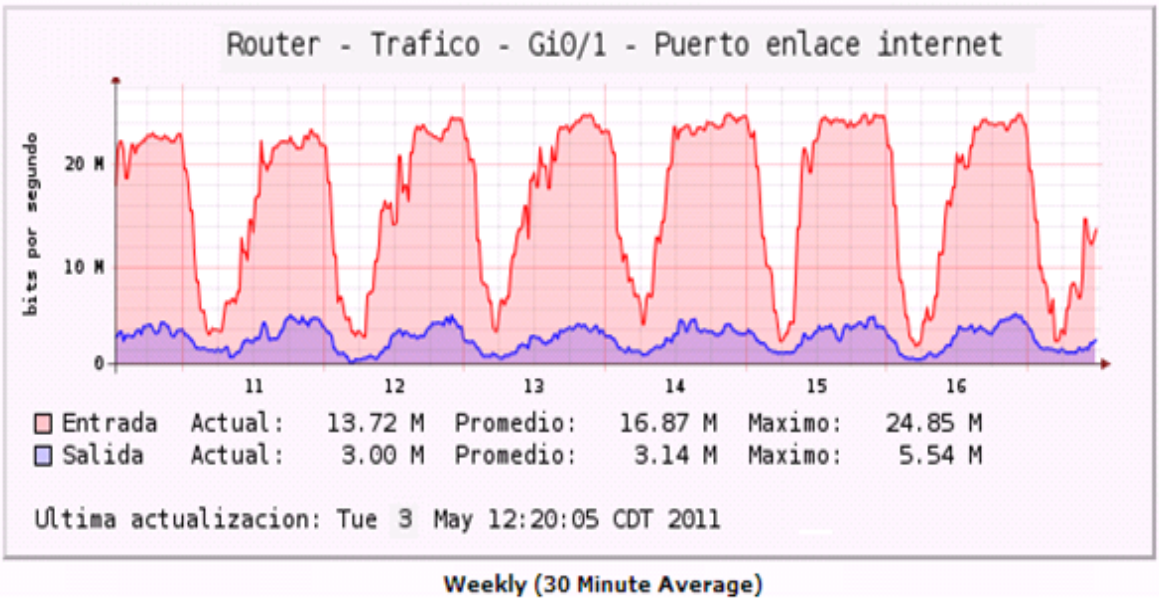


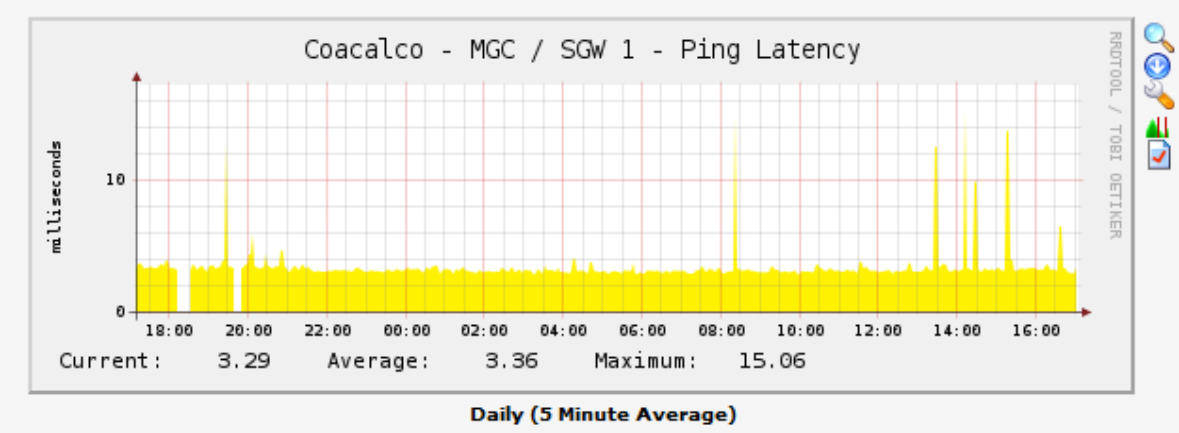
Figura 5.6 Gráfico por semana



Muchas veces se tiene una red instalada, pero no se sabe de forma concreta cómo se encuentra formada. Si en esta situación se tienen momentos de ancho de banda muy bajos, el hecho de saber el estado de servicio de la red, se convierte en algo imprescindible. Evidentemente, es algo que en una empresa puede ser muy conveniente, más aún cuando la herramienta de monitoreo, está montado sobre Linux. Es decir, no es necesario invertir dinero en ello.

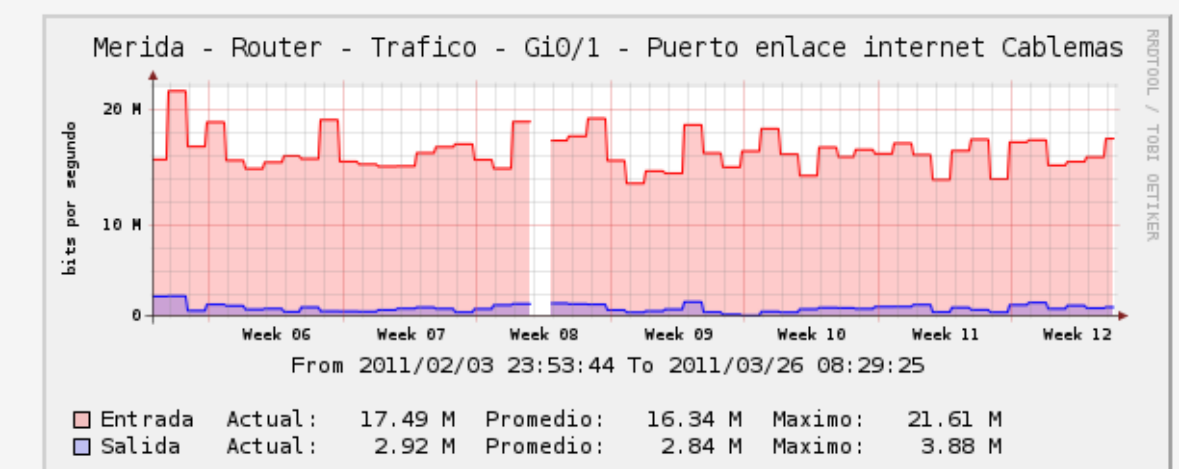
En las gráficas, se puede visualizar el tráfico registrado hora por hora, aunque también permite monitorear ya sea por días, meses o años. Lo que se visualiza en color rojo es el tráfico entrante, como la actividad de navegación, descargas de archivos, envíos de correo, etc., que demanda consumo de ancho de banda en cuanto a navegación. Lo que se visualiza en color azul es el registro de las solicitudes a un dispositivo como por ejemplo al abrir un explorador, cuando cargas un archivo anexo por el correo, el envió de información hacia el servidor o cuando tecleas una consulta en Google, etc.

Figura 5.7 Gráfico de ping



Al realizar una prueba acerca de latencia se puede demostrar que el promedio en tiempo que demora la información en viajar de origen destino es de 3.29 milisegundos.

Figura 5.7 Gráfico de pérdida de paquetes



En esta grafica se puede observar una perdida de paquetes registrados en la semana 8 ya que hubo una perdida de conectividad, la cual creo conflictos por un tiempo determinado, por que se procedió a realizar el reporte correspondiente al proveedor de servicio para verificar y conocer cual fue la causa por la que se genero esta perdida y a su vez que solución pudieron obtener para nuevamente restablecer el servicio.

CONCLUSIONES

Al finalizar esta aplicación, se puede concluir que se cumplieron con los objetivos propuestos, que fueron implementar los acuerdos de niveles de servicio basados en ICMP en una red de área amplia, así como también la gestión de la misma y entender la aplicación de los protocolos de red, ya que se pudo desarrollar el monitoreo con la herramienta Cacti, que es un sistema de código abierto.

Con ellos, se mejora la disponibilidad de los servicios que se prestan, se reducen costos en cuanto a mantenimiento y que se pueden prevenir fallas en la red. La herramienta Cacti nos ayudó a obtener datos de la red, para poder compararlos con los acuerdos de nivel de servicio obtenidos por los proveedores de servicio de ancho de banda, y así poder establecer si se brinda lo contratado y en su caso contrario adquirir o ampliar un ancho de banda adecuado.

La implementación de la red, brinda la fiabilidad de que los servicios siempre estén disponibles en cualquier momento, esto se verá traducido en mejoras económicas de la corporación y para que los clientes estén satisfechos esto hará que sea una empresa proveedora de servicios 99.99…% rentable.

REFERENCIAS

[1]*itSMF. "Fundamentos de gestiónde servicios TI: basados en ITIL."*Ed. Van Haren Publishing, EUA, 2007, 254 pág.

[2] Caballero, José Manuel. "*Redes de banda ancha"*. Ed. Marcombo Boixareu, España, 1998, 252 pág.

[3]http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=14258 20/Feb/2011.

[4]http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.pdf, 22/Feb/2011.

[5] http://www.areas.net/comofunciona/conexion/3.htm 28/Feb/2011.

[6] http://www.alfinal.com/Temas/tcpip.php 10/Marzo/2011.

[7] http://www4.uji.es/~al019803/tcpip/paginas/CapaAplicacion.htm 18/Marzo/2011.

[8]http://es.scribd.com/doc/12252225/Interconexion-de-Redes 29/Marzo/2011.

[9] http://es.scribd.com/doc/12252225/Interconexion-de-Redes 01/Abril/2011.

[10] Lonvinck, C.2001. "The BSD syslog Protocol".RFC 3164, 29pág.

[11] Case, J. 1990. “A Simple Network Management Protocol (SNMP)”. RFC 1157, 35pág.

[12] Mills, Davis L. 1992. “Network Time Protocol (Version 3) Specification, Implementation and Analysis”.RFC 1305, 112pág.

[13]http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/hticmpjt.html 07/Abril/2011.

[14] https://hq.netline.net/users/jaime.cruz/weblog/c1da4/ 15/Abril/2011.

[15]http://www.textoscientificos.com/redes/videoconferencias/beneficios-problemas 16/Abril/2011.

[16]http://www.mundocisco.com/2009/04/como-comprobar-la-perdida-de-paquetes.html19/Abril/2011.