UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.
ESCUELA DE SISTEMAS Y TECNOLOGÍAS

TESIS DE GRADO

Previa a la Obtención del Título de:

INGENIERO EN SISTEMAS

TEMA:

"IMPLEMENTACIÓN DE LA CALIDAD DE SERVICIOS (QoS) Y MONITOREO DE REDES PARA GESTIONAR EL BALANCEO DE CARGA DEL ENLACE A INTERNET EN LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA".

AUTORES:

MORALES COELLO MARÍA LUCÍA

ILBAY ZATÁN MARÍTZA PILAR

DIRECTOR:

ING. RAÚL RAMOS MOROCHO

LECTOR:

ING. GEOVANNY VEGA

BABAHOYO-LOS RIOS– ECUADOR

2012

UNIVERSIDAD TECNICA DE BABAHOYO

ESCUELA DE SISTEMAS Y TECNOLOGÍAS

MEMORIA DE TESIS

“IMPLEMENTACIÓN DE LA CALIDAD DE SERVICIOS (QoS) Y MONITOREO DE REDES PARA GESTIONAR EL BALANCEO DE CARGA DEL ENLACE A INTERNET EN LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA”.

PRESENTADA AL TRIBUNAL EXAMINADOR COMO REQUISITO PARA OBTENER EL TITULO DE:

INGENIERO DE SISTEMAS

TRIBUNAL EXAMINADOR

_____

PRESIDENTE DEL TRIBUNAL

_____ _____

MIEMBRO DEL TRIBUNAL **MIEMBRO DEL TRIBUNAL**

TRIBUNAL RESPONSABLE Y NOTA

Ing. Washington Ávila

DIRECTOR DE ESCUELA DE SISTEMAS Y TECNOLOGIAS _____

Ing. Raúl Ramos

DIRECTOR DE TESIS _____

Ing. Geovanny Vega

LECTOR DE TESIS _____

MIEMBRO DEL TRIBUNAL _____

NOTA DE TESIS: _____

CERTIFICACIÓN DE AUTORÍA

A: Universidad Técnica de Babahoyo, Facultad de Administración Finanzas e Informática.

Por la presente dejamos constancia de ser las autoras del proyecto de tesis "Implementación de la Calidad de Servicio (QoS) y monitoreo de redes para gestionar el balanceo de carga del enlace a Internet en la Facultad de Administración, Finanzas e Informática.".

Dejamos constancia que el uso de marcos, inclusión de opiniones, citas e imágenes son de nuestra absoluta responsabilidad, quedando la UTB exenta de toda obligación al respecto.

Autorizamos, en forma gratuita, a la UTB a utilizar este material.

Autoras: Firma:

María Lucia Morales Coello ……

Maritza Pilar IlbayZatán ……

Babahoyo, 10 de septiembre del 2011.

DEDICATORIA

En primer lugar, le dedicamos este trabajo a Dios todo poderoso por ser nuestra guía espiritual que nos conduce siempre hacia el camino del bien y el éxito. Y por darnos la conformidad de tener a nuestros padres con vida y mucha salud solo él sabe lo importante que son ellos para nosotros. Al igual que todas esas personas que nos apoyaron y confiaron en nosotros. Gracias Dios por darnos la dicha de escribirles hoy esta dedicatoria.

A nuestros Padres, por ser ellos nuestro árbol principal que nos cobijó bajo su sombra dándonos así la fuerza para seguir caminando y lograr alcanzar esta meta anhelada. Dios los bendiga, les de salud y mucha vida para poder retribuirles un poco de lo que nos han dado, para ustedes este logro y todos los que nos faltan por alcanzar este es solo el comienzo de una vida llena de éxitos para ustedes. Gracias por su persistencia y confiar en nosotros.

A nuestros hermanos para que siempre tengan en cuenta que todo lo que nos propongamos en la vida lo podemos lograr si trabajamos fuerte y continuamente con rectitud, sigan adelante y para que nuestros éxitos de hoy sean los suyos mañana y siempre.

A nuestros Profesores por que han sido una fuente fundamental de nuestro desarrollo por habernos brindado su ayuda y amistad incondicional.

A nuestros amigos por ofrecernos siempre esa mano amiga en los momentos más difíciles de nuestra vida tanto personal como profesional, Dios los bendiga.

María Lucía Morales Coello y Marítza Pilar Ilbay Zatán

AGRADECIMIENTO

Son numerosas las personas a las que debemos agradecer por ayudarnos en el logro de nuestra carrera, es demasiado poco, el decir gracias, pero en el fondo de nuestro ser eternamente les estaremos agradecidos y siempre prestos a tenderles una mano cuando así lo requieran. Sin embargo, resaltaremos solo algunas de estas personas las cuales no hubiésemos hecho realidad este sueño tan anhelado como es la culminación de nuestra carrera universitaria.

Ante todo y en primer lugar a Dios por darnos la vida y por habernos guiado por el camino de la felicidad hasta ahora; en segundo lugar a cada uno de nuestros padres quienes a lo largo de toda nuestra vida nos han apoyado y motivado en nuestra formación académica, creyendo en nosotros en todo momento y no dudaron de nuestras habilidades. A nuestros profesores a quienes les debemos gran parte de nuestros conocimientos, gracias a su paciencia y enseñanza y finalmente un eterno agradecimiento a esta prestigiosa universidad la cual abrió sus puertas a jóvenes como nosotros, preparándonos para un futuro competitivo y formándonos como personas de bien.

María Lucía Morales Coello y Marítza Pilar Ilbay Zatán

TABLA DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

CAPÍTULO I

EL PROBLEMA

1. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Durante la visita a la Universidad Técnica de Babahoyo se puede notar que la Facultad de Administración, Finanzas e Informática no cuenta con un adecuado monitoreo, clasificación del tráfico, marcación del tráfico y aplicación de políticas dentro de la red ocasionando colisiones e interferencias en caso de que más de un usuario emita al mismo tiempo lo cual provoca que muchas veces el ancho de banda no se distribuya de acuerdo a las necesidades de cada usuario.

Siendo esto evidente cuando nos encontramos navegando en internet muchos estudiantes están realizando consulta de texto mientras que otros revisan tutoriales en video por poner un ejemplo el primero necesita un ancho de banda normal mientras que el segundo necesitará mayor velocidad de la misma.

Al momento que los usuarios quieran realizar transferencia de voz o video, o se produce una descarga de datos, estas podrían ocupar todo el ancho de banda disponible, provocando que ocasione grandes molestias al resto de usuarios conectados a la red

Otra situación es que no se puede realizar videoconferencia por el mismo motivo que el ancho de banda se encuentra mal distribuido y entonces existe un retardo en la misma; también al momento de transferir información hay pérdida de datos.

Cuando tenemos un router conectado a internet, hay ocasiones en las que no es suficiente con realizar el encaminamiento a través de un solo proveedor de acceso a internet, sino que es necesario realizar un balance de carga entre varias líneas de conexión a internet, como por ejemplo dos líneas ADSL.

Al balancear la carga entre varias líneas podemos decidir qué parámetro tener en cuenta para realizar ese balanceo: podemos realizarlo en base a las direcciones IP origen, la dirección IP destino, el puerto origen o destino u otros factores. La configuración que se muestra a continuación balancea la carga de forma aleatoria entre los dos accesos a internet en base al peso que se otorgue a cada enlace. Con esto se consigue repartir la carga entre los dos enlaces en base a su disponibilidad de ancho de banda, por ejemplo. En el laboratorio de la facultad no se cuenta con los equipos necesarios para realizar el trabajo de balanceo de carga de enlace a Internet, es así que se convierte en una necesidad de la facultad en implementar este tipo de servicios de calidad en la misma; además esto causa molestias en profesores como alumnos que al momento de realizar actividades de mayor uso de ancho de banda no se pueden realizar con la velocidad adecuada por cuanto no hay un reparto del servicio de internet sino que todos los usuarios están conectados directamente a la red.

Todos los problemas descritos anteriormente se pueden resumir en los siguientes puntos:

- La pérdida de paquetes, debido a la imposibilidad de entregarlos a un receptor que tiene un buffer (cola de entrada) lleno, lo que puede obligar a la retransmisión de los paquetes perdidos.
- Retardo, debido a las esperas de los paquetes en distintos nodos de la red (colas) o, simplemente, al rutado a través de un camino más largo que el directo para evitar congestiones.
- Jitter, que no es más que la llegada de una secuencia de paquetes con retardos dispares para cada uno de ellos, lo que perjudica gravemente a

las comunicaciones ordenadas, como las secuencias de audio, por ejemplo.

- Llegada en desorden, causada por el rutado por distintos caminos de los paquetes de una secuencia, que sólo puede ser corregido por determinados protocolos de transmisión.
- Errores en la transmisión, que provocan la corrupción de los datos o la combinación errónea de paquetes.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo mejorar la distribución del ancho de banda con la implementación de QoS, y beneficios del monitoreo de la red informática en la Facultad de Administración, Finanzas e Informática?

1.3. DELIMITACIÓN

Objeto de Estudio:

Ingeniería en Sistemas

Campo de Acción:

Redes y Comunicaciones

Este estudio se lo realizará en la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo durante el año 2011.

1.4. OBJETIVOS

1.4.1. Objetivo General

Implementar la Calidad de Servicio (QoS) y monitorear las redes para gestionar el balanceo de carga del enlace a Internet en la Facultad de Administración, Finanzas e Informática.

1.4.2. Objetivos Específicos

- Investigar las necesidades de conectividad de la Facultad de Administración Finanzas e Informática de la Universidad Técnica de Babahoyo.
- Fundamentar base teóricas y científicas que permita el desarrollo de esta investigación.
- Analizar y preparar información para conocer las mejores soluciones.
- Validar la investigación y resultado con la ayuda de un experto.

1.5. JUSTIFICACION

El presente trabajo de investigación propone buscar elementos tecnológicos que permitan favorecer y mejorar los servicios para los usuarios que se conectan a la red en la facultad.

- La implantación de calidad de servicio (QoS) en el backbone es esencial para el éxito de aplicaciones avanzadas, como telemedicina, videoconferencia y VoIP (voz sobre IP o telefonía sobre IP). Estas aplicaciones demandan, además de gran ancho de banda, un servicio diferenciado.En muchos casos es necesario garantizar que la transmisión de los datos sea realizada sin interrupción o pérdida de paquetes.
- Se pretende gestionar el ancho de banda para que cuando los usuarios estén realizando actividades que demanden gran ancho de banda lo puedan obtener sin desmejorar la calidad del servicio de los demás usuarios.
- Con el balanceo de carga de internet se disminuirá la presencia de Jitter, que no es más que la llegada de una secuencia de paquetes con retardos dispares para cada uno de ellos, lo que perjudica gravemente a las comunicaciones ordenadas, como las secuencias de audio, por ejemplo.
- También se puede reducir la llegada en desorden, causada por el rutado por distintos caminos de los paquetes de una secuencia, que sólo puede ser corregido por determinados protocolos de transmisión. Se busca evitar errores en la transmisión, que provocan la corrupción de los datos o la combinación errónea de paquetes.

- El servicio de internet de la FAFI permite conectividad a la red a todos los usuarios de la institución, que por diversos motivos hacen uso frecuente de un computador como estación de trabajo. Con la implementación de Calidad de Servicio se podrá mejorar los siguientes requerimientos:
    - Asignar ancho de banda en forma diferenciada
    - Evitar y/o administrar la congestión en la red
    - Manejar prioridades de acuerdo al tipo de tráfico
    - Modelar el tráfico de la red
- Con la mejora de estos requerimientos podremos tener la satisfacción de los usuarios conectados a la red.
- El manejo del ancho de banda es una parte esencial del trabajo diario de todo ISP, usuario comercial o doméstico. Hay varias formas diferentes de hacer esto con el RouterOSMikrotik ya sea usando QoS, límite de tasa de transferencia, límite de paquetes, solo por nombrar algunos.

1.6. ALCANCE DEL PROYECTO

La presente disertación de grado concluirá en el momento que se presente un documento y una demostración del balanceo de carga con Calidad de Servicio y monitoreo de la red, utilizando como sistema operativo CENTOS 6.0 y las siguientes herramientas: NTOP para monitoreo de puertos, SQUID funciona como proxy, Sarg para realizar reportes, IpTable bloqueo de protocolos L7.

1.7. RECURSOS Y PRESUPUESTOS

1.7.1. Recursos Humanos

- 2 Egresados de la Facultad de Administración Finanzas e Informática.
- 1 Director de Tesis.
- 1 Profesor Asesor.

1.7.2. Recursos Materiales

Los Recursos materiales serán detallados más adelante dentro de los Requerimientos **hardware y software.**

Hardware

PC portátil

Disco Duro 512 GB

Memoria RAM 4GB 2.4GH

Procesador

CentOS soporta casi las mismas arquitecturas que Red Hat Enterprise Linux:

Intelx86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP).

AMD64(Athlon 64, etc) e IntelEM64T (64 bit).

Las versiones 3.x y 4.x (pero no la 5.0 y posteriores) además soportaron:

Intel Itanium (64 bit).

PowerPC/32 (AppleMacintoshPowerMac corriendo sobre procesadores G3 o G4 PowerPC).

IBMMainframe (eServerzSeries y S/390).

También se tuvo soporte para dos arquitecturas no soportadas por Red Hat Enterprise Linux.

Alpha procesador (DEC Alpha) (sólo en CentOS 4)

SPARC (beta en CentOS 4)

Software

CentOS 6.0

Virtual Machine WorkStation

SARG

CACTI

WEBMIN

NTOP

1.7.3. Recursos Económicos

Los recursos económicos son aporte de los autores del proyecto.

1.7.4. Presupuesto y Costos

Total	**Egresos**
Autofinanciamiento (Recursos Propios) **Total** **$480,00**	Viáticos $ 300,00 Movilizaciones $ 120,00 Celular $ 80,00 Alimentación $100,00
	Gastos de investigación $ 100,00 Internet $100,00
	Papelería $40,00 Resmas 4 $20,00 Fotocopias $5,00 CD/DVD $5,00 Pen Drive $10,00
	Impresión $40,00 cartuchos $40,00
	Total **$ 480,00**

Tabla 1.- Presupuesto

CAPÍTULO II

MARCO TEÓRICO

2. MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACION

Al presente trabajo de investigación, no le antecede proyecto similar luego de buscar en las nóminas de tesis de la Biblioteca Virtual en la Facultad de Administración, Finanzas e Informática, surgiendo este proyecto en base al análisis realizado al internet que se reparte en los laboratorios de nuestra facultad.

Durante el tiempo de revisión del internet se observó que existen grandes retrasos en el envío y recepción de paquetes, lo que causa molestias a quienes usan el internet para diferentes clases de investigación.

Se ha observado que en la facultad no existe ningún control de balanceo de carga a pesar de que se cuenta con un importante ancho de banda del internet.

Bajo estos antecedentes, el trabajo que se plantea se orienta a la optimización del uso del internet, evitando los retrasos de los paquetes en la red.

2.2. FUNDAMENTACIÓN TEÓRICA

2.2.1. Facultad de Administración, Finanzas e Informática

2.2.1.1. Reseña Histórica

A los 20 años de creada la Universidad Técnica de Babahoyo, con sus dos facultades de Ciencias de la Educación e Ingeniería Agronómica, la institución se sintió presionada por la comunidad, ya que, las carreras que ofertaba, si bien no habían sido objetadas, el desarrollo de la provincia exigía nuevos horizontes profesionales para su desarrollo.

Es así, como el H. Consejo Universitario de la Universidad Técnica de Babahoyo en sesiones del 4 y 14 de febrero de 1992 aprobó la creación del Centro de Carreras Profesionales y Tecnológicas (C E P I T) con las escuelas

de Enfermería, Ingeniería Comercial, Informática y Computación; y Contabilidad y Auditoría. La acogida de la comunidad se tradujo en una alta matrícula.

La organización de los aspectos docentes y administrativos estuvo a cargo del vicerrector de entonces; el Pensum se elaboró tomando como base los de las universidades de Guayaquil y Central de Quito.

La Facultad de Administración Finanzas e Informática es una Unidad Académica de la Universidad Técnica de Babahoyo, cuyo gobierno se estructura conforme lo determina el vigente Estatuto Universitario, su campo de acción se enmarca en una concepción moderna del que hacer educativo nacional propendiendo la formación de profesionales y técnicos a nivel superior, altamente calificados, a fin de que puedan afrontar con total profesionalización y eficiencia los retos que imponen el avance y desarrollo de la sociedad moderna.

Dentro de esta concepción esta unidad académica provee la fórmula de sistema educativo que profesionalice a entes capaces de planear, dirigir, ejecutar y controlar sistemas administrativos, económicos productivos de salubridad en su radio de acción local, regional y nacional haciendo hincapié fundamentalmente en actividades que constituyen fuentes de riquezas para mejorar las actuales condiciones de vida de nuestra población.

En 15 de junio y el 22 de septiembre de 1996 el H. Consejo Universitario creó la Facultad de Administración, Finanzas e Informática, teniendo entre las Escuelas de Administración de Empresas y Gestión Empresarial, Ingeniería de Sistemas e Informática, Contaduría y Auditoria. [1]

1 ESPAÑA, Ángel & MEJIA, José. RESEÑA HISTORICA. 2010

2.2.1.2. Estructura orgánica

- El Consejo Directivo de Facultad
- El Decano de Facultad
- El Subdecano de Facultad
- Comisión Académica
- Direcciones de Escuela

2.2.1.3. Organigrama

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Organigrama Académico y Administrativo[2]

URL: http://fafi.utb.edu.ec/index.php?option=com_content&view=article&id=5&Itemid=12

[2]ESPAÑA, Ángel & MEJIA, José.

URL: http://fafi.utb.edu.ec/index.php?option=com_content&view=article&id=3&Itemid=11

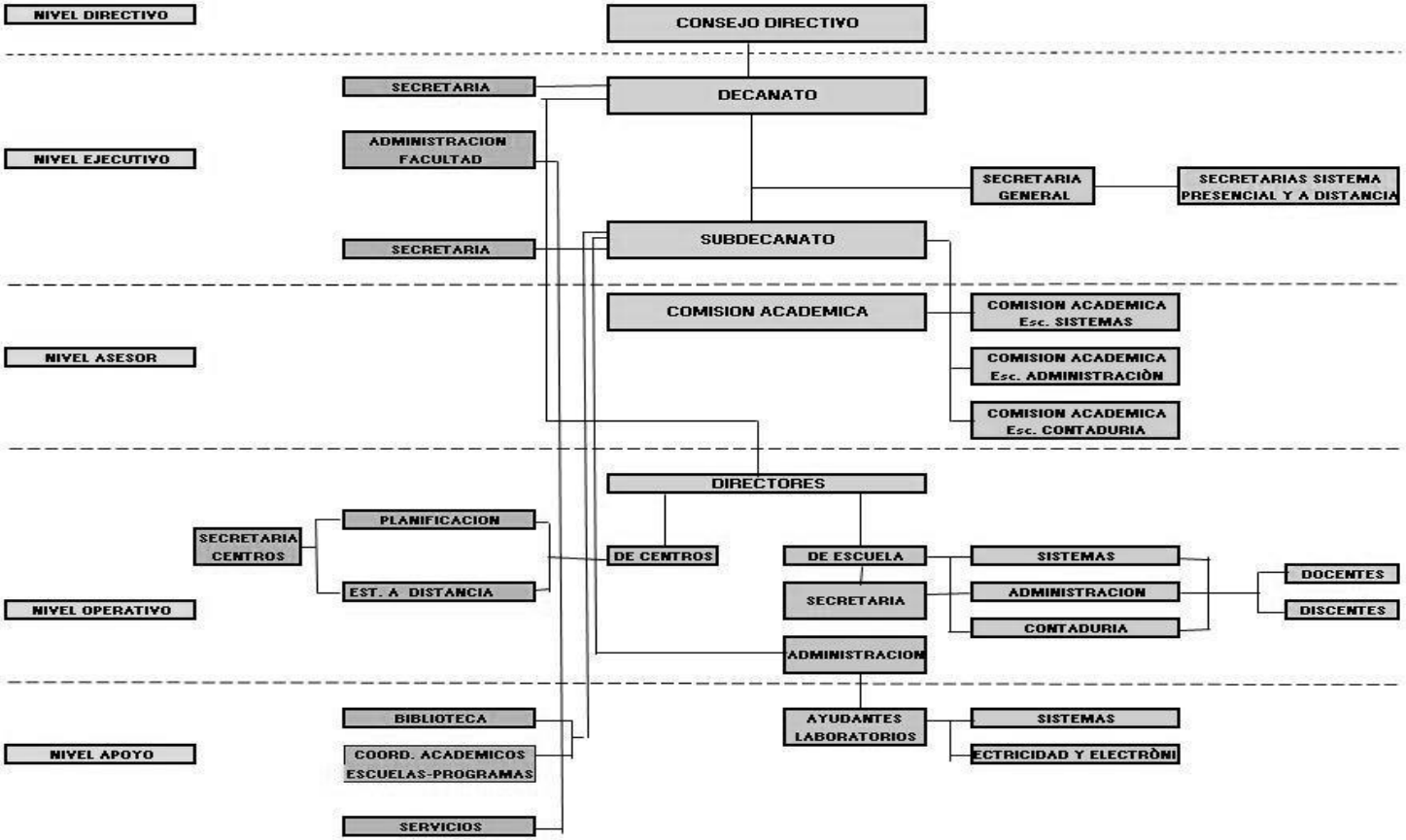


Ilustración 1.- Organigrama de la FAFI

2.2.1.4. Misión

La Facultad de Administración, Finanzas e Informática como unidad académica de la Universidad Técnica de Babahoyo, educa para la formación del talento humano, capacitándolo para el ejercicio profesional en las áreas administrativas, contables, sistemas informáticos, eléctricos y electrónicos con profundos conocimientos de la ciencia y la técnica, el cultivo y práctica de valores, comprometidos con el servicio comunitario y el desarrollo sustentable y sostenible del país, cuyo desempeño fomente la calidad de vida de la sociedad. [3]

2.2.1.5. Visión

La Facultad de Administración, Finanzas e Informática hasta el año 2013, será vanguardista en el proceso formativo del talento humano en administración, contaduría, sistemas informáticos, eléctricos y electrónicos con proyección y posicionamiento en el ámbito nacional.4

2.2.1.6. Laboratorios Sistemas de la Facultad de Administración, Finanzas e Informática

La Facultad de Administración, Finanzas e Informática cuenta con cuatro laboratorios destinados al área de Sistemas.

2.2.2. Balanceo de carga

2.2.2.1. Introducción al balanceo de carga

[3]ESPAÑA, Ángel & MEJIA, José. MISION. 2010

URL: http://fafi.utb.edu.ec/index.php?option=com_content&view=article&id=2&Itemid=3

[4]ESPAÑA, Ángel & MEJIA, José. MISION. 2010

URL: http://fafi.utb.edu.ec/index.php?option=com_content&view=article&id=2&Itemid=3

En informática el balanceo de carga se refiere a la técnica usada para compartir el trabajo que se va a realizar en diferentes procesos con varios computadores, discos duros y otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.

El balance de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella.

La Solución de balanceo de carga permite dividir las tareas que tendría que soportar una única máquina, con el fin de maximizar las capacidades de proceso de datos, así como de ejecución de tareas.

Esta Solución permite que ningún equipo sea parte vital del servicio que queremos ofrecer. De esta forma evitamos sufrir una parada del servicio debido a una parada de una de las máquinas.

El balanceo de carga es la manera en que las peticiones de Internet son distribuidas sobre una fila de servidores. Existen varios métodos para realizar el balanceo de carga. Desde el simple "Round Robin" (repartiendo todas las peticiones que llegan de Internet entre el número de servidores disponibles para dicho servicio) hasta los equipos que reciben las peticiones, recogen información, en tiempo real, de la capacidad operativa de los equipos y la utilizan para enrutar dichas peticiones individualmente al servidor que se encuentre en mejor disposición de prestar el servicio adecuado.

Los balanceadores de carga pueden ser soluciones hardware, tales como routers y switches que incluyen software de balanceo de carga preparado para ello, y soluciones software que se instalan en el back end de los servidores.

2.2.2.2. Características del balanceo de carga

Evita la saturación de una máquina. De esta forma, podemos evitar que picos de acceso a las máquinas (como por ejemplo los generados por campañas publicitarias), afecten al normal funcionamiento del aplicativo.

Gestiona los recursos de manera inteligente. Permite gestionar y optimizar todos los recursos disponibles dando como resultado un acceso más rápido y estable a nuestros aplicativos.

2.2.2.3. Tipos de balanceo

Método de balanceo de carga con enrutamiento directo (dr)

El modo de enrutamiento directo (DR) de una rama es el recomendado para la instalación de Loadbalancer porque es una solución de rendimiento muy alto que requiere muy pocos cambios en la infraestructura con la que cuenta el cliente.

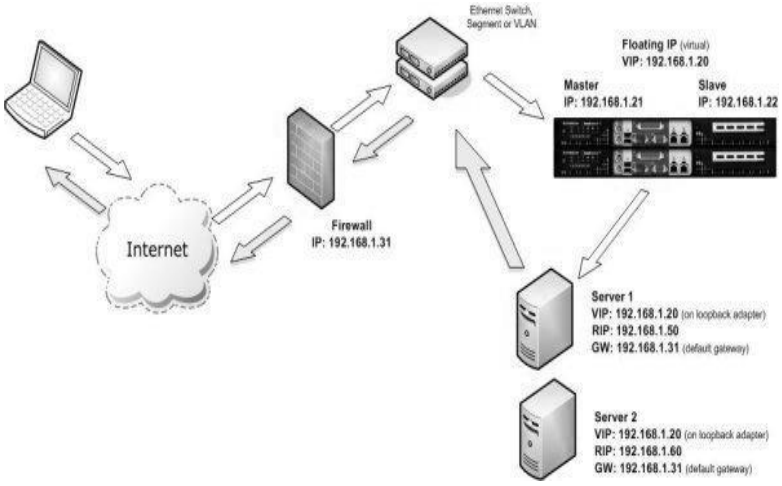


Ilustración 2.- El balanceo por enrutamiento

El enrutamiento directo (DR) funciona cambiando las direcciones MAC de destino del paquete entrante sobre la marcha, lo que es muy rápido.

- Sin embargo, eso significa que cuando el paquete llega al servidor real espera ser el propietario de la VIP. Así se ha de asegurar que el servidor real responde a la VIP, pero no responde a las peticiones ARP.
- De media, el modo DR es 8 veces más rápido que NAT para HTTP, 50 veces más rápido para servicios de terminal y mucho, mucho más rápido para streaming o FTP.
- El modo de enrutamiento directo permite a los servidores de una red conectada acceder bien a las VIP o bien a las RIP. No se requieren subredes o rutas adicionales en la red.
- El servidor real se ha de configurar para responder tanto a la VIP como a su propia dirección IP.

- En el modo DR no es posible realizar traducciones de puerto, es decir, cuando se tiene un puerto diferente para la RIP y la VIP.

Cuando se usa un balanceador de carga en modo DR de una rama, todos los servicios balanceados se pueden configurar en la misma subred que los servidores reales.

Los servidores reales se han de configurar para responder a la dirección IP del servidor virtual, así como a su propia dirección IP.

Método de balanceo de carga con Network AddressTranslation (NAT)

A veces no es posible usar el modo DR. Los motivos más comunes son: si la aplicación no puede tomar la RIP y la VIP al mismo tiempo; o si el sistema operativo anfitrión no se puede modificar para ocuparse de la cuestión del ARP.

La segunda opción es el modo Network AddressTranslation (NAT).

También es una solución de rendimiento bastante alto, pero requiere la implementación de una infraestructura de dos ramas con una subred interna y externa para llevar la traducción (igual como funciona un cortafuegos). Los ingenieros de redes con experiencia en hardware balanceador de carga habrán utilizado este método a menudo.

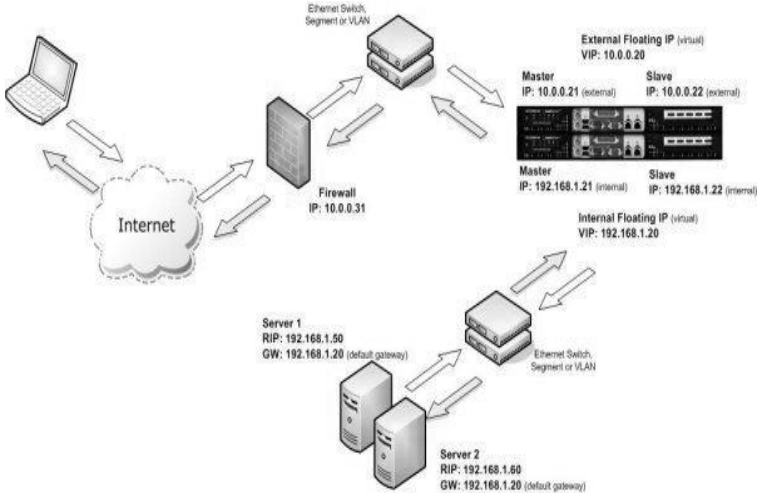


Ilustración 3.- El balanceo mediante NAT

- En el modo NAT de dos ramas, el balanceador de carga traduce todas las peticiones del servidor virtual externo a los servidores reales internos.
- Los servidores reales han de tener su puerta de enlace predeterminada configurada para que apunte al balanceador de carga.
- Para que los servidores reales puedan acceder a Internet por su cuenta, y navegar, el asistente de configuración añade automáticamente la regla de ENMASCARAMIENTO necesaria en el script de los cortafuegos.
- Si desea que los servidores reales sean accesibles en su propia dirección IP para servicios que no requieran balanceo de carga, como SMTP, deberá configurar reglas individuales SNAT y DNAT en el script de los cortafuegos para cada servidor real. O puede

configurar un servidor virtual dedicado que sólo tenga como objetivo un servidor real.

Cuando se usa un balanceador de carga en modo NAT de dos ramas, todos los servicios balanceados se pueden configurar en la IP externa. Asimismo, los servidores reales han de tener sus puertas de enlace predeterminadas dirigidas a la IP interna. También puede configurar los balanceadores de carga en modo NAT de una rama, pero para que los servidores sean accesibles desde la red local deberá cambiar alguna información de enrutamiento en los servidores reales.

Es posible añadir reglas de enrutamiento a los servidores reales con el fin de realizar el balanceo de carga NAT en una única subred (1 rama), consulte el manual de administración para más información.

Método de balanceo de carga con Source Network AddressTranslation (SNAT).

Si la aplicación requiere que el balanceador de carga se ocupe de la inserción de cookies, entonces ha de usar la configuración SNAT. Este método tiene también la ventaja de requerir una configuración de una rama, y no hace falta efectuar cambios en los servidores de aplicaciones. Sin embargo, como el balanceador de carga actúa como un proxy completo, no tiene la misma tasa de transferencia sin procesar como los métodos basados en enrutamiento.

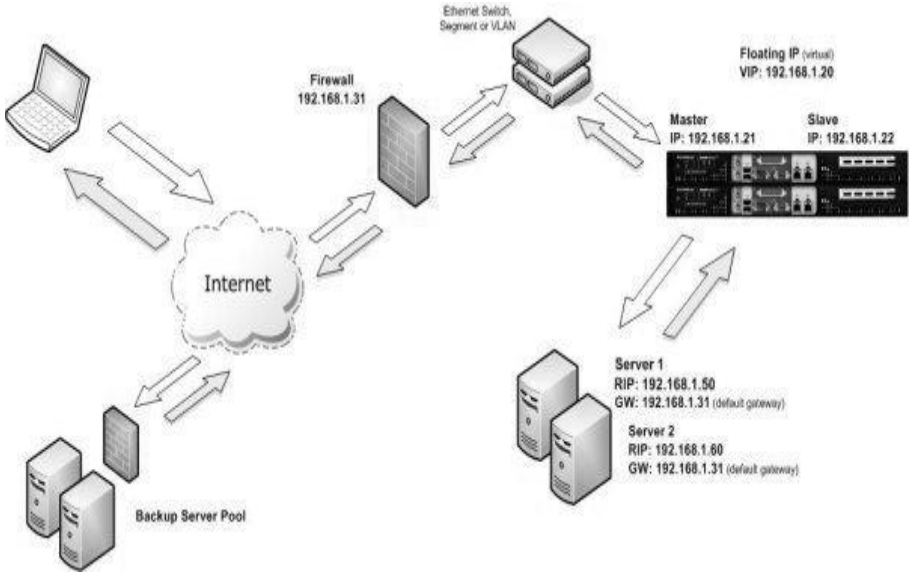


Ilustración 4.- El balanceo por SNAT

El diagrama de red para el modo HAProxy SNAT de capa 7 es muy similar al ejemplo de enrutamiento directo salvo que no es necesario reconfigurar los servidores reales. El balanceador de carga hace de proxy para el tráfico de la aplicación a los servidores de modo que el balanceador de carga sea el origen de todo el tráfico.

- Al igual que con otros modos, una unidad sola no requiere una IP flotante.
- SNAT es un proxy completo y por lo tanto los servidores balanceados no necesitan ser cambiados de ningún modo.

Como SNAT es un proxy completo, cualquier servidor del clúster puede estar en cualquier subred accesible, incluyendo Internet y WAN.SNAT no es TRANSPARENTE por defecto, es decir, los servidores reales verán la dirección de origen de cada petición como la dirección IP de los

balanceadores de carga. La dirección IP de origen del cliente estará en el encabezado X-Forwarded-For (XFF).

Método de balanceo de carga con TransparentSource Network AddressTranslation (SNAT-TPROXY)

Si la dirección de origen del cliente es un requisito, entonces HaProxy se puede forzar a un modo transparente usando TPROXY, esto requiere que los servidores reales utilicen el balanceador de carga como puerta de enlace predeterminada (como en el modo NAT) y sólo funciona para subredes enganchadas directamente (como en el modo NAT).

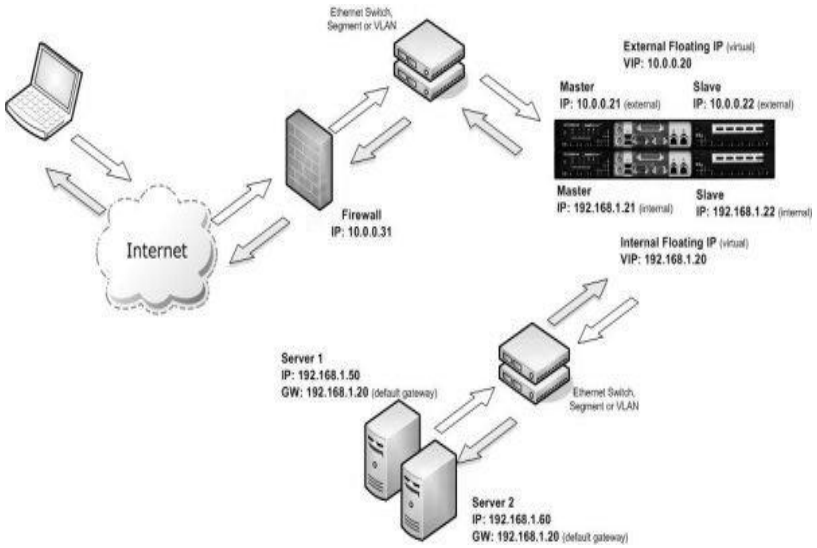


Ilustración 5.- El balanceo por SNAT-PROXY

Al igual que con otros modos, una unidad sola no requiere una IP flotante.

- SNAT actúa como un proxy completo, pero en el modo TPROXY todo el tráfico del servidor ha de pasar por el balanceador de carga.

- Los servidores reales han de tener su puerta de enlace predeterminada configurada para que apunte al balanceador de carga.

Es imposible implementar un proxy transparente en una red enrutada, es decir en una WAN como Internet. Para conseguir un balanceo de carga transparente en una WAN se puede usar el método de balanceo de carga con TUN (enrutamiento directo sobre túnel seguro) sólo en sistemas Linux o UNIX.

Terminación o aceleración SSL (SSL) con o sin TPROXY

Todos los métodos de balanceo de carga de capa 4 o 7 pueden ocuparse del tráfico SSL en modo de paso, es decir los servidores back-end se encargan del descifrado y cifrado del tráfico. Esto es muy escalable pues puede añadir más servidores al clúster para obtener más transacciones por segundo (TPS). Sin embargo, si desea inspeccionar el tráfico HTTPS para leer e insertar cookies necesitará descodificar (terminar) el tráfico SSL en el balanceador de carga.

Esto lo puede hacer importando su clave segura y su certificado de firma al balanceador de carga, autorizándolo así para descifrar el tráfico.

El balanceador de carga utiliza certificados estándar del formato Apache/PEM.

Puede definir un servidor virtual Pound SSL con un único back-end, bien un servidor virtual en modo NAT de capa 4 o lo que es más normal, un HAProxy VIP de capa 7, que puede insertar cookies.

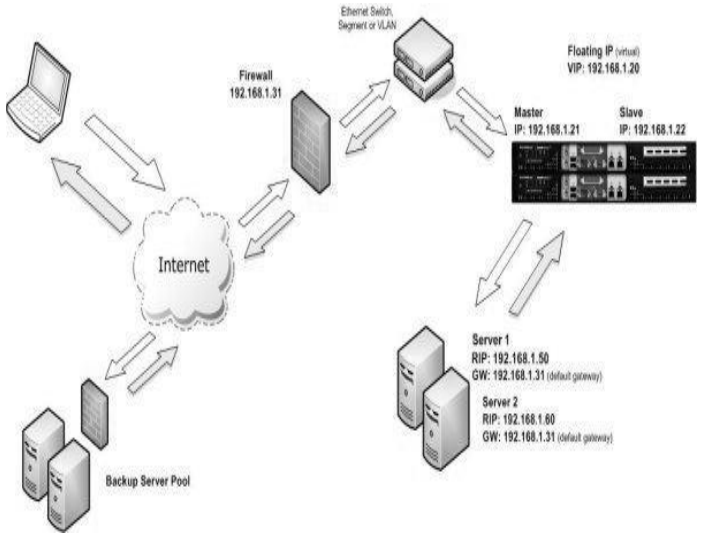


Ilustración 6.- El balanceo por SSL – con o sin PROXY

Pound-SSL no es TRANSPARENTE por defecto, es decir, el back-end verá la dirección de origen de cada petición como la dirección IP de los balanceadores de carga. La dirección IP de origen del cliente estará en el encabezado X-Forwarded-For (XFF). Sin embargo Pound-SSL también se puede configurar con TPROXY para garantizar que el back-end pueda ver la dirección IP de origen de todo el tráfico.[5]

2.2.2.4. Ventajas

- Mayor capacidad de ampliación
- Mayor disponibilidad de los servicios
- Mayor capacidad de gestión
- Permite al usuario priorizar que páginas desea visitar.
- Permite optimizar el uso en clúster de varias máquinas a la vez, aprovechando al máximo la totalidad de la capacidad de procesamiento de los servidores.

[5]Loadbalancer Ltd. Métodos de Balanceo de Carga.
URL: http://es.loadbalancer.org/load_balancing_methods.php

- Permite al cliente la selección de los servicios a los que desea acceder a internet.

En definitiva es una interesante herramienta para priorizar los servicios de acceso a Internet eligiendo el tráfico de interés para la empresa en el momento que el cliente lo desee.

2.2.3. Redes

2.2.3.1. Definición de red

Una red informática se puede definir como un sistema de comunicación que conecta computadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos.

A través de la compartición de información y recursos en una red, los usuarios de los sistemas informáticos de una organización podrán hacer un mejor uso de los mismos, mejorando de este modo el rendimiento global de la organización. Entre las ventajas que supone el tener instalada una red, pueden citarse las siguientes:

- Mayor facilidad en la comunicación entre usuarios
- Reducción en el presupuesto para software
- Reducción en el presupuesto para hardware
- Posibilidad de organizar grupos de trabajo
- Mejoras en la administración de los equipos y programas
- Mejoras en la integridad de los datos
- Mayor seguridad para acceder a la información

2.2.3.2. Servicios de redes

Si queremos obtener todas las ventajas que supone el uso de una red, se deben tener instalados una serie de servicios de red, como son:

Acceso: Los servicios de acceso se encargan tanto de verificar la identidad del usuario (para asegurar que sólo pueda acceder a los recursos para los que tiene permiso) como de permitir la conexión de usuarios a la red desde lugares remotos.

Ficheros: El servicio de ficheros consiste en ofrecer a la red grandes capacidades de almacenamiento para descargar o eliminar los discos de las estaciones. Esto permite almacenar tanto aplicaciones como datos en el servidor, reduciendo los requerimientos de las estaciones. Los ficheros deben ser cargados en las estaciones para su uso.

Impresión: Permite compartir impresoras entre varios computadores de la red, lo cual evitará la necesidad de tener una impresora para cada equipo, con la consiguiente reducción en los costes.

Las impresoras de red pueden ser conectadas a un servidor de impresión, que se encargará de gestionar la impresión de trabajos para los usuarios de la red, almacenando trabajos en espera (cola de impresión), asignando prioridades a los mismos, etc.

Información: Los servidores de información pueden almacenar bases de datos para su consulta por los usuarios de la red u otro tipo de información, como por ejemplo documentos de hipertexto.

Otros: En el campo de la comunicación entre usuarios existen una serie de servicios que se deben comentar. El más antiguo y popular es el correo electrónico (e-mail) que permite la comunicación entre los usuarios a través de mensajes escritos. Los mensajes se enviarán y se recuperarán usando un equipo servidor de correo.

2.2.3.3. Elementos de una red

Para poner a disposición de los usuarios los servicios anteriormente comentados, se necesita lógicamente montar el hardware adecuado. En la primera parte de la documentación de este proyecto ya se describieron componentes tales como tarjetas de red, concentradoras, repetidoras, puentes, routers, etc. Nos referimos ahora a los tipos de computadores existentes en una red.

Servidores

Un servidor es un computador que ejecuta un sistema operativo de red y ofrece servicios de red a las estaciones de trabajo. El servidor debe ser un sistema fiable con un procesador potente, con discos de alta capacidad y con gran cantidad de memoria RAM. Una configuración que nos podremos encontrar (en el caso de redes locales) es un equipo con procesador Pentium, disco duro SCSI de más de 4Gb, con 64Mb de RAM y sistema operativo Windows NT.

Debo comentar aquí que es posible montar una red sin servidor (o más bien donde cada equipo se comporta como servidor y cliente al mismo tiempo). En este caso, el sistema operativo se debe instalar en cada

estación de trabajo (activando el soporte para red) y los recursos se distribuyen entre las estaciones. No obstante, en este tipo de configuración, aspectos como la seguridad y la administración de usuarios se ven seriamente restringidos.

Estaciones de trabajo

Cuando un computador se conecta a una red el primero se convierte en un nodo o estación de trabajo de la última. Las estaciones de trabajo pueden ser computadores personales con el DOS, sistemas Macintosh de Apple, sistemas Windows o estaciones de trabajo sin disco.[6]

Protocolos de redes

Los protocolo de red son una o más normas standard que especifican el método para enviar y recibir datos entre varios computadores. Su instalación está en correspondencia con el tipo de red y el sistema operativo que la computadora tenga instalado.

No existe un único protocolo de red, y es posible que en un mismo computador coexistan instalados varios de ellos, pues cabe la posibilidad que un mismo computador pertenezca a redes distintas.

La variedad de protocolos puede suponer un riesgo de seguridad: cada protocolo de red que se instala en un sistema queda disponible para todos los adaptadores de red existentes en dicho sistema, físicos (tarjetas de red o módem) o lógicos (adaptadores VPN).

[6] DELGADO, Héctor & Juan Rodríguez. Redes.
URL: http://www.gobcan.es/educacion/conocernos_mejor/paginas/redes.html

Si los dispositivos de red o protocolos no están correctamente configurados, se puede dar acceso no deseado a los recursos de la red. En estos casos, la regla de seguridad más sencilla es tener instalados el número de protocolos indispensable; en la actualidad y en la mayoría de los casos debería bastar con sólo TCP/IP.

Protocolos

Dentro de la familia de protocolos se pueden distinguir

Protocolos de transporte:

- ATP (Apple TalkTransactionProtocol)
- NetBIOS/NetBEUI
- TCP (Transmission Control Protocol)

Protocolos de red:

- DDP (Delivery Datagram Protocol)
- IP (Internet Protocol)
- IPX (Internet Packed Exchange)
- NetBEUI Desarrollado por IBM y Microsoft.
- Protocolos de aplicación:
- AFP (Appletalk File Protocol)
- FTP (File Transfer Protocol)
- Http (Hyper Text transfer Protocol)

Dentro de los protocolos antes mencionados, los más utilizados son:

- IPX/SPX, protocolos desarrollados por Novell a principios de los años 80 los cuales sirven de interfaz entre el sistema operativo de red Netware y las distintas arquitecturas de red. El protocolo IPX es similar a IP, SPX es similar a TCP por lo tanto juntos proporcionan servicios de conexión similares a TCP/IP.
- NETBEUI/NETBIOS (Network Basic Extended User Interface / Network Basic Input/Output System) NETBIOS es un protocolo de comunicación entre computadores que comprende tres servicios (servicio de nombres, servicio de paquetes y servicio de sesión, inicialmente trabajaba sobre el protocolo NETBEUI, responsable del transporte de datos. Actualmente con la difusión de Internet, los sistemas operativos de Microsoft más recientes permiten ejecutar NETBIOS sobre el protocolo TCP/IP, prescindiendo entonces de NETBEUI.
- APPLE TALK es un protocolo propietario que se utiliza para conectar computadoras Macintosh de Apple en redes locales.
- TCP/IP (Transmission Control Protocol/Internet Protocol) este protocolo fue diseñado a finales de los años 60, permite enlazar computadoras con diferentes sistemas operativos. Es el protocolo que utiliza la red de redes Internet.[7]

2.2.3.4. Ventajas y desventajas de una red

[7] SUAREZ, Ivis. Redes Informáticas. URL: http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas2.shtml#protocolo

Ventajas:

- Compartir archivos y recursos informáticos como almacenamiento, impresoras, etc.
- Compartir internet.
- Comunicación de todo tipo entre las computadoras.
- Es muy barato crear una red de computadoras en un mismo edificio, especialmente con el uso de WI-FI (inalámbrico).

Desventajas:

- La instalación puede ser costosa si las computadoras están muy distanciadas entre sí físicamente (a cientos de kilómetros); aunque esto es cada vez más barato de hacer, incluso internet solucionó muchos de estos problemas.
- Todavía sigue siendo un poco complicado crear la red (por lo menos para los usuarios más inexpertos).

2.2.4. Monitoreo de Redes

2.2.4.1. Seguimiento del tráfico

Control de fallas.

Esta operación tiene que ver con la configuración de la red (incluye dar de alta, baja y reconfigurar la red) y con el monitoreo continuo de todos sus elementos.

Administración de cambios.

La administración de cambios comprende la planeación, la programación de eventos e instalación.

Administración del comportamiento.

Tiene como objetivo asegurar el funcionamiento óptimo de la red, lo que incluye: El número de paquetes que se transmiten por segundo, tiempos pequeños de respuesta y disponibilidad de la red.

Servicios de contabilidad.

- Este servicio provee datos concernientes al cargo por uso de la red. Entre los datos proporcionados están los siguientes:
- Tiempo de conexión y terminación.
- Número de mensajes transmitidos y recibidos.
- Nombre del punto de acceso al servicio.
- Razón por la que terminó la conexión.
- Control de Inventarios.

Se debe llevar un registro de los nuevos componentes que se incorporen a la red, de los movimientos que se hagan y de los cambios que se lleven a cabo.

Seguridad.

La estructura administrativa de la red debe proveer mecanismos de seguridad apropiados para lo siguiente:

- **Identificación y autentificación del usuario.-**Una clave de acceso y un password.
- **Autorización de acceso a los recursos**.-Es decir, solo personal autorizado.

- **Confidencialidad.-**Para asegurar la confidencialidad en el medio de comunicación y en los medios de almacenamiento, se utilizan medios de criptografía, tanto simétrica como asimétrica.

Un administrador de redes en general, se encarga principalmente de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Se encarga de administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración rendimiento, seguridad e inventarios.

Llave privada.

En éste método los datos del transmisor se transforman por medio de un algoritmo público de criptografía con una llave binaria numérica privada solo conocida por el transmisor y por el receptor. El algoritmo más conocido de este tipo es el DES (Data Encription Standard).

2.2.4.2. Tasa de transferencia

La tasa de transferencia se refiere al ancho de banda real medido en un momento concreto del día empleando rutas concretas de internet mientras se transmite un conjunto específico de datos, desafortunadamente, por muchas razones la tasa es con frecuencia menor al ancho de banda máximo del medio que se está empleando.

Los siguientes son algunos de los factores que determinan la tasa de transferencia:

- Dispositivos de Internet-Working
- Tipos de datos que se van a transferir

- Topología de la red
- Número de usuarios en la red
- La computadora del usuario
- El servidor
- Condiciones de la energía
- Congestión

El ancho de banda teórico de la red es una consideración importante en el diseño de la red, porque la tasa de transferencia de la red nunca es mayor que dicho ancho de banda, debido a las limitaciones puestas por el medio y a las tecnologías de red elegidas.

La unidad con que el Sistema Internacional de Unidades expresa el bit rate es el bit por segundo (bit/s, b/s, bps). La b debe escribirse siempre en minúscula, para impedir la confusión con byte por segundo (B/s). Para convertir de bytes/s a bits/s, basta simplemente multiplicar por 8 y viceversa.

Que la unidad utilizada sea el bit/s, no implica que no puedan utilizarse múltiplos del mismo:

- Kbit/s o kbps (kb/s, kilobit/s o mil bits por segundo)
- Mbit/s o Mbps(Mb/s, Megabit/s o un millón de bits por segundo)
- Gbit/s o Gbps (Gb/s, Gigabit, mil millones de bits)
- Byte/s (B/s u 8 bits por segundo)
- Kilobyte/s (kB/s, mil bytes u ocho mil bits por segundo)

- Megabyte/s (MB/s, un millón de bytes u 8 millones de bit por segundo)
- Gigabyte/s (GB/s, mil millones de bytes u 8 mil millones de bits)

La tasa de transferencia de datos corresponde a la velocidad media con que los datos son transferidos desde la red del ISP(Internet ServiceProvider) al usuario conectado a éste, durante períodos de tiempo determinados, medida en bits por segundo y presentada en tres parámetros: promedio, máxima, mínima.

Tipos de bits

La velocidad de transferencia de datos puede ser constante o variable:

1. Tasa de bits constante (CBR): Aplica una cuantificación uniforme, por lo que no tiene en cuenta si en la señal hay zonas con mayor o menor densidad de información, sino que cuantifica toda la señal por igual.

2. Tasa de bits variable (VBR): Aplica una cuantificación no uniforme, que sí que hace diferenciación entre las zonas con mayor o menor densidad de información, por lo que la cuantificación resulta más eficaz.[8]

1.2.1.1.1. Paquetes de internet

En internet la información se divide en paquetes para ser enviados ya que si se enviaran completo sería muy pesado, además de que permite que si un paquete no llega pueda ser enviado solamente ese paquete y o toda la información, al inicio de una conexión se envían paquetes para sincronizarse el emisor y el receptor, el emisor envía paquetes para

[8] Licencia de CreativeCommons Atribución Compartir Igual. Tasa de Bits. URL: http://es.wikipedia.org/wiki/Tasa_de_bits

solicitar una conexión, y el receptor envía paquetes al emisor para aceptar o rechazar la petición y si lo acepta entonces se envían los paquetes del archivo a enviar.

Todo lo que uno hace en Internet, involucra paquetes de información. Por ejemplo, cada página Web que uno recibe, viene en una serie de paquetes, cada correo electrónico que uno manda, sale como una serie de paquetes.

En Internet, la red rompe un correo electrónico en partes de cierto tamaño de bytes. Estos son los paquetes de información. Cada paquete carga la información que le va a ayudar a llegar a su destino “la IP del remitente, la del destinatario, algo que le dice a la red de cuantos paquetes consiste el correo electrónico, y el número de cada uno de esos paquetes”. El paquete carga los datos en los protocolos que Internet usa: TCP/IP (Transmission Control Protocol / Internet Protocol “Protocolo de control de transmisión / Protocolo de Internet). Cada paquete contiene parte del cuerpo total del mensaje. Un paquete típico contiene más o menos entre 1,000 y 1,500 bytes.

Cada paquete es enviado a su destino por la mejor ruta disponible “una ruta que puede o no ser tomada por el resto de los paquetes del mensaje”. Esto hace a la red más eficiente. Primero, la red puede balancear la carga de transmisión a través de distintos equipos en milisegundos. Segundo, si hay algún problema con un equipo de la red mientras un mensaje está siendo transferido, los paquetes pueden ser

desviados del problema por otra ruta, asegurando la entrega del mensaje completo.

La mayoría de los paquetes están divididos en tres partes:

Encabezado: Contiene instrucciones sobre los datos cargados por el paquete, que puede incluir los siguientes:

Tamaño del paquete (algunas redes tienen paquetes de tamaño fijo, mientras que otras dependen del encabezado para contener esta información)

Sincronización (algunos bits que le ayudan al paquete encajar en la red)

Número del paquete (que paquete es en la secuencia de paquetes)

Protocolo (en redes que cargan distintos tipos de información, el protocolo define qué tipo de paquete está siendo transferido: correo, Web, video, etc.)

Dirección del destinatario (hacia dónde va el paquete)

Dirección del remitente (de dónde vino el paquete)

Cuerpo: En esta parte se almacena los datos que el paquete está entregando al destino. Si un paquete tiene un tamaño fijo, entonces el cuerpo puede contener espacio vacío para rellenar el espacio del cuerpo necesario para hacerlo del tamaño correcto.

Cola: También llamada pie, contiene unos bits que le indican al equipo receptor que se ha llegado al fin del paquete. También puede contener algún tipo de verificador de estado ó de errores. El verificador más común utilizado en los paquetes es el CRC (CyclicRedundancyCheck "Control por Redundancia Cíclica"). Este verificador suma todos los unos en el Cuerpo del paquete, el resultado es almacenado como un valor hexadecimal en la Cola. El equipo receptor suma también esa misma información y la compara con la que se encuentra en la Cola del paquete. Si los valores concuerdan, el paquete es correcto. Pero si no concuerdan, el equipo receptor le envía una solicitud al equipo transmisor para que reenvié el paquete.[9]

2.2.5. QoS (Calidad de Servicio)

2.2.5.1. ¿Qué es un QoS?

QoS o Calidad de Servicio son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). La calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

Por otra parte el concepto de calidad de servicio (o QoS) en telecomunicaciones puede tener, al menos, dos interpretaciones habituales. En primer lugar, se refiere a la capacidad de determinadas redes y servicios para admitir que se fije de antemano las condiciones en

[9] BARRIOS, Joel. URL: http://www.alcancelibre.org/article.php/20070626123555360

que se desarrollarán las comunicaciones (dedicación de recursos, capacidades de transmisión, etc.). En segundo lugar, se habla calidad de servicio como una serie de cualidades medibles de las redes y servicios de telecomunicaciones, como el tiempo que se tarda en realizar una llamada telefónica (desde que el usuario marca hasta que suena el teléfono en el otro extremo).

La Calidad de Servicio (QoS, Quality of Service) es el efecto colectivo del desempeño de un servicio, el cual determina el grado de satisfacción a la aplicación de un usuario. Para que en una red pueda ofrecer el manejo de QoS extremo-a-extremo (end2end), es necesario que todos los nodos o puntos de interconexión por los que viaje el paquete de información, posean mecanismos de QoS que ofrezcan un desempeño adecuado a la aplicación en cuestión. Los puntos de interconexión por los que pasa la información son los enrutadores, conmutadores, incluso los puntos de acceso al servicio (SAPs, Service Access Points) entre las capas del modelo (o stack) de comunicación que se use. Cuando se establece una conexión con un nivel de QoS especificado, los parámetros de éste se traducen y negocian entre los diferentes subsistemas involucrados. Solamente cuando todos los subsistemas han llegado a acuerdos y pueden otorgar garantías respecto a los parámetros especificados, será que se satisfagan los requerimientos de QoS de extremo a extremo.

QoS o Calidad de Servicio son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado, es la capacidad de dar un buen servicio

Es un método para asegurar el desempeño de aplicaciones de voz, datos y/o video basadas en IP sobre la LAN & WAN.

Con todas las nuevas aplicaciones basadas en IP utilizando la LAN & WAN, QoS es una necesidad para garantizar que no todo el tráfico sea utilizado equitativamente. Es importante hacer notar que QoS no es una tecnología, sino un atributo de la LAN & WAN definida a través de muchas tecnologías.

Decimos que una red o un proveedor ofrecen 'Calidad de Servicio' o QoS (Quality of Service) cuando se garantiza el valor de uno o varios de los parámetros que definen la calidad de servicio que ofrece la red. Si el proveedor no se compromete en ningún parámetro decimos que lo que ofrece un servicio 'besteffort'.[10]

2.2.5.2. Mecanismos de QoS

Un alternativa a los mecanismos complejos del control de QoS es proporcionar la comunicación de la alta calidad por abundante sobre-aprovisionamiento una red para basar la capacidad en carga del tráfico punta estime. Este acercamiento es simple y económico para las redes con las cargas fiables y ligeras del tráfico. El funcionamiento es razonable para muchos usos. Esto pudo incluir los usos exigentes que pueden

[10]CUDI. QoS. URL: http://telematica.cicese.mx/internetII/qcudi/qos_cudi.html

compensar variaciones en anchura de banda y retrasan con grande, recibiendo así con almacenadores intermediarios.

Los servicios comerciales de VoIP son a menudo competitivos con servicio telefónico tradicional en términos de mecanismos de QoS de la calidad de la llamada aun cuando son generalmente separados en la conexión del usuario a su ISP y la conexión del abastecedor de VoIP a una diversa ISP. Bajo altas condiciones de carga, sin embargo, la calidad de VoIP degrada calidad del célula-teléfono o peor. Las matemáticas del tráfico del paquete indican que una red con QoS puede manejar cuatro veces tantas llamadas con requisitos apretados de la inquietud como uno sin QoS. La cantidad de sobre-aprovisionamiento en los acoplamientos interiores requeridos para substituir QoS depende del número de usuarios y de sus demandas del tráfico. Pues del Internet los servicios ahora con más de mil millones usuarios, allí son poca posibilidad que el sobre-aprovisionamiento puede eliminar la necesidad de QoS cuando VoIP llega a ser más corriente.

Para las redes de banda estrecha más típicas de empresas y de gobiernos locales, sin embargo, los costes de la anchura de banda pueden ser substanciales y el aprovisionamiento excesivo.

Usos de QoS por ejemplo VoIP y IPTV, porque ellos requieren los bitrates en gran parte constantes y el estado latente bajo no pueden utilizar TCP, y no puede reducir de otra manera su tarifa del tráfico a la ayuda previene la fusión cualquiera. QoS contrae el tráfico del límite que puede ser

ofrecido al Internet y de tal modo hacer cumplir formar del tráfico que pueda evitar que el sobrecargarse, por lo tanto son una parte imprescindible de la capacidad del Internet de manejar una mezcla del tráfico en tiempo real y no en tiempo real sin la fusión.

“**DIFFSERV“O SERVICIOS DISTINGUIDOS**.- En el modelo de DiffServ, los paquetes están marcados según el tipo de servicio que necesitan. En respuesta a estas marcas, las rebajadoras y los interruptores utilizan varias estrategias que hacen cola para adaptar funcionamiento a los requisitos. (En la capa del IP, punto de código distinguido de los servicios (DSCP) las marcas utilizan los 6 pedacitos en el jefe del paquete del IP. En la capa del MAC, VLAN IEEE 802.1Q y IEEE 802.1D puede ser utilizado llevar esencialmente la misma información).

Adicional gerencia de la anchura de banda los mecanismos se pueden utilizar para dirigir más lejos funcionamiento, para incluir:

- El formar del tráfico (limitación de la tarifa):
    - Cubo simbólico
    - Cubo agujereado
    - Control de la tarifa del TCP - artificial ajustando tamaño de la ventana del TCP así como controlar el índice de ACKssiendo vuelto al remitente
- Algoritmos del Scheduling:
    - El hacer cola cargado de la feria (WFQ)

- La clase basó hacer cola cargado de la feria
- Cargado alrededor de robin (WRR)
- Déficit cargado alrededor de robin (DWRR)

- Evitación de la congestión:
  - ROJO, WRED - Disminuye la posibilidad de almacenador intermediario portuario de la coleta cola-gotas y esto baja la probabilidad de Sincronización global del TCP
  - El limpiar (marca/caer el paquete superior al tamaño confiado de la tarifa y de la explosión del tráfico)
  - Notificación explícita de la congestión
  - El templar del almacenador intermediario

2.2.5.3. QoS en ATM

Una de las grandes ventajas de ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona) respecto de técnicas como el Frame Replay y Fast Ethernet es que admite niveles de QoS. Esto permite que los proveedores de servicios ATM garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo o que garantizarán un ancho de banda específico para un servicio. Esto es posible marcando los paquetes que provengan de una dirección IP determinada de los nodos conectados a un gateway (como por ejemplo la IP de un teléfono IP, según la puerta del router, etc.). Además, en los servicios satelitales da una nueva perspectiva en la utilización del ancho de banda, dando prioridades a las aplicaciones de extremo a extremo con una serie de reglas.

Una red IP está basada en el envío de paquetes de datos. Estos paquetes de datos tienen una cabecera que contiene información sobre el resto del paquete. Existe una parte del paquete que se llama ToS (Type of Service), en realidad pensada para llevar banderas o marcas. Lo que se puede hacer para darle prioridad a un paquete sobre el resto es marcar una de esas banderas (flags, en inglés).

Para ello, el equipo que genera el paquete, por ejemplo una puerta de enlace (gateway, en inglés) de voz sobre IP, coloca una de esas banderas en un estado determinado. Los dispositivos por donde pasa ese paquete después de ser transmitido deben tener la capacidad para poder

discriminar los paquetes para darle prioridad sobre los que no fueron marcados o los que se marcaron con una prioridad menor a los anteriores. De esta manera podemos generar prioridades altas a paquetes que requieren una cierta calidad de envío, como por ejemplo la voz o el vídeo en tiempo real, y menores al resto.

2.2.5.4. QoS en escenarios Inalámbricos

El entorno inalámbrico es muy hostil para medidas de Calidad de Servicio debido a su variabilidad con el tiempo, ya que puede mostrar una calidad nula en un cierto instante de tiempo. Esto implica que satisfacer la QoS resulta imposible para el 100% de los casos, lo que representa un serio desafío para la implementación de restricciones de máximo retardo y máxima varianza en el retardo (jitter) en sistemas inalámbricos. Los sistemas de comunicaciones ya estandarizados con restricciones QoS de retardo y jitter en entornos inalámbricos (por ejemplo en GSM y UMTS) sólo pueden garantizar los requisitos para un porcentaje (<100%) de los casos. Esto implica una caída del servicio (Outage o downtime en inglés), generando los cortes de llamadas y/o los mensajes de “red ocupada”.

2.2.5.5. Protocolos que proporcionan una calidad de servicio

- Servicios distinguidos (DiffServ)
- Relais del capítulo
- X.25
- Algunos ADSL módems

- Servicios integrados (IntServ)
- Protocolo de la reservación del recurso (RSVP)
- RSVP-TE
- Asynchronous Transfer Mode (Atmósfera)
- Conmutación Multiprotocol de la etiqueta (MPLS) proporciona ocho clases de QoS
- IEEE 802.1p
- IEEE 802.11e
- IEEE 802.11p
- Tipo de servicio Campo (TOS) en el jefe del IP
- HomePNA Alambres caseros del coaxial y del teléfono del excedente del establecimiento de una red.[11]

2.2.5.6. Factores que afectan la calidad de servicio

Paquetes sueltos: Los ruteadores pueden fallar en liberar algunos paquetes si ellos llegan cuando los buffers ya están llenos. Algunos, ninguno o todos los paquetes pueden quedar sueltos dependiendo del estado de la red, y es imposible determinar qué pasará de antemano. La aplicación del receptor puede preguntar por la información que será retransmitida posiblemente causando largos retardos a lo largo de la transmisión.

[11] MORGAN, Kaufmann. Calidad de Servicio. URL: http://www.worldlingo.com/ma/enwiki/es/Quality_of_service

Retardo: Puede ocurrir que los paquetes tomen un largo período en alcanzar su destino, debido a que pueden permanecer en largas colas o tomen una ruta menos directa para prevenir la congestión de la red. En algunos casos, los retardos excesivos pueden inutilizar aplicaciones tales como VoIP o juegos en línea.

Jitter: Los paquetes del transmisor pueden llegar a su destino con diferentes retardos. Un retardo de un paquete varía impredeciblemente con su posición en las colas de los ruteadores a lo largo del camino entre el transmisor y el destino. Esta variación en retardo se conoce como jitter y puede afectar seriamente la calidad del flujo de audio y/o vídeo.

Entrega de paquetes fuera de orden: Cuando un conjunto de paquetes relacionados entre sí son encaminados a Internet, los paquetes pueden tomar diferentes rutas, resultando en diferentes retardos. Esto ocasiona que los paquetes lleguen en diferente orden de cómo fueron enviados. Este problema requiere un protocolo que pueda arreglar los paquetes fuera de orden a un estado isócrono una vez que ellos lleguen a su destino. Esto es especialmente importante para flujos de datos de vídeo y VoIP donde la calidad es dramáticamente afectada tanto por latencia y pérdida de sincronía.

Errores: A veces, los paquetes son mal dirigidos, combinados entre sí o corrompidos cuando se encaminan. El receptor tiene que detectarlos y justo cuando el paquete es liberado, pregunta al transmisor para repetirlo así mismo.

2.2.5.7. Parámetros de Calidad de Servicios

Calidad de diseño: Es el grado en el que un producto o servicio se ve reflejado en su diseño.

Calidad de conformidad: Es el grado de fidelidad con el que es reproducido un producto o servicio respecto a su diseño.

Calidad de uso: El producto ha de ser fácil de usar, seguro, fiable, etc.

El cliente es el nuevo objetivo: Las nuevas teorías sitúan al cliente como parte activa de la calificación de la calidad de un producto, intentando crear un estándar en base al punto subjetivo de un cliente. La calidad de un producto no se va a determinar solamente por parámetros puramente objetivos sino incluyendo las opiniones de un cliente que usa determinado producto o servicio.

2.2.5.8. Qos en Internet

Se han desarrollado y estandarizado los dos mecanismos de QoS, reserva y prioridad:

- **IntServ (IntegratedServices) y protocolo RSVP(**Protocolo De Reserva De Recursos**)**.- El usuario solicita de antemano los recursos que necesita; cada router del trayecto ha de tomar nota y efectuar la reserva solicitada.
- **DiffServ (DifferentiatedServices).-** El usuario marca los paquetes con un determinado nivel de prioridad; los routers van agregando las demandas de los usuarios y propagándolas por el trayecto.

Esto le da al usuario una confianza razonable de conseguir la QoS solicitada.

Ambos son compatibles y pueden coexistir.

2.2.5.9. Usos que requieren QoS

Una calidad definida del servicio se puede requerir para ciertos tipos de tráfico de la red, por ejemplo:

- El fluir multimedias puede requerir garantizar rendimiento de procesamiento para asegurarse de que un nivel mínimo de la calidad está mantenido.
- Internet ProtocolTelevision (***IPTV***).- Ofrecido como servicio de un abastecedor de servicio por ejemplo AT&T's U-verso.
- Telefonía del IP o el IP excesivo de la voz (VOIP) puede requerir límites terminantes en inquietud y retrasa.
- **El Teleconferencing video (VTC).-** Requiere la inquietud y el estado latente bajos.
- El señalar del alarmar (Alarmar de ladrón).
- La emulación dedicada del acoplamiento requiere garantizar rendimiento de procesamiento e impone límites ante máximo retrasos.
- A seguridad-crítico uso, por ejemplo cirugía alejada puede requerir un nivel garantizado de disponibilidad (esto también se llama QoS duro).

- Un administrador de sistema alejado puede desear dar la prioridad a variable, y generalmente pequeño, las cantidades de SSH trafique para asegurar una sesión responsiva incluso sobre un acoplamiento pesado-cargado.
- Juegos en línea, tales como simulaciones en tiempo real establecidas el paso rápidas con los jugadores múltiples. La carencia de QoS puede producir el “retraso”.

Estos tipos de servicio se llaman inelástico, significando que requieren cierto nivel mínimo de la anchura de banda y de cierto estado latente máximo funcionar.

Por el contrario, elástico los usos pueden aprovecharse sin embargo de mucho o poca anchura de banda está disponible. Usos a granel de la transferencia de archivo que confían encendido TCP sea generalmente elástico.

2.2.6. CENTOS

(CommunityENTerpriseOperatingSystem) es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la

Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de las fuentes de Red Hat.

CentOS usa yum para bajar e instalar las actualizaciones, herramienta también utilizada por Fedora.

Requisitos de Sistema

Hardware recomendado para operar:

- Memoria RAM: 64 MB (mínimo).
- Espacio en Disco Duro: 1024 MB (mínimo) - 2 GB (recomendado).
- Procesador

  CentOS soporta casi las mismas arquitecturas que Red Hat Enterprise Linux:

  - Intelx86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP).
  - AMD64(Athlon 64, etc) e IntelEM64T (64 bit).

Las versiones 3.x y 4.x (pero no la 5.0 y posteriores) además soportaron:

- Intel Itanium (64 bit).
- PowerPC/32 (AppleMacintoshPowerMac corriendo sobre procesadores G3 o G4 PowerPC).
- IBMMainframe (eServerzSeries y S/390).

También se tuvo soporte para dos arquitecturas no soportadas por Red Hat Enterprise Linux.

- Alpha procesador (DEC Alpha) (sólo en CentOS 4)
- SPARC (beta en CentOS 4)

Arquitecturas

CentOS soporta casi las mismas arquitecturas que Red Hat Enterprise Linux:

- Intelx86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP).
- AMD64(Athlon 64, etc) e IntelEM64T (64 bit).

Las versiones 3.x y 4.x (pero no la 5.0 y posteriores) además soportaron:

- Intel Itanium (64 bit).

- PowerPC/32 (AppleMacintoshPowerMac corriendo sobre procesadores G3 o G4 PowerPC).
- IBMMainframe (eServerzSeries y S/390).

También se tuvo soporte para dos arquitecturas no soportadas por Red Hat Enterprise Linux.

- Alpha procesador (DEC Alpha) (sólo en CentOS 4)
- SPARC (beta en CentOS 4)

2.2.7. NTOP

NTop (de Network Top) es una herramienta que permite monitorizar en tiempo real una red. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y para ayudarnos a detectar malas configuraciones de algún equipo, (facilitando la tarea ya que. justo al nombre del equipo, aparece sale un banderín amarillo o rojo, dependiendo si es un error leve o grave), o a nivel de servicio.

Posee un microservidor web desde el que cualquier usuario con acceso puede ver las estadísticas del monitorizaje.

El software está desarrollado para plataformas Unix y Windows.

En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una

interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico. Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

Es una herramienta de monitorización de red en la que prima la presentación de informes de los datos recogidos sobre la recolección de paquetes de red.

Destacamos las siguientes características de NTOP:

- Es un proyecto de software libre ya consolidado, con 10 años de historia.
- Su interfaz es web y muy intuitivo.
- Dispone de gran variedad de informes: informes globales de carga de red, de tráfico entre elementos, de sesiones activas de cada elemento, etc.
- Detecta posibles paquetes perniciosos.
- Permite exportar los datos a una base de datos relacional MySQL para su análisis.

- Es capaz de analizar datos proporcionados por dispositivos de red que soporten NetFlow y sFlow.
- Es un software multiplataforma (Windows, Linux, *BSD, Solaris y MacOSX) y muy fácil y rápido de instalar.

Instalación NTOP

La instalación de NTOP es muy sencilla pero en CentOS 5 maneja una versión muy atrasada por lo cual se recomienda la instalación a través de código fuentes. Podremos instalar NTOP sin problemas con yum pero existen muchas mejoras extras en la nueva versión por lo cual mejor compilaremos el paquete.

Dependencias Compilación.

Para poder instalar NTOP primero tendremos instalar los compiladores de C y algunas librerías necesarias para la compilación.

[root@ascariote ~]# yum install gcc make libtool gdbm-devel zlib-devel

Dependencias NTOP.

NTOP también requiere algunos paquetes extras para su buen funcionamiento, necesitamos el lenguaje de programación python con sus librerías y libcap que no permite habilitar funcionalidades de POSIX. Nota: POSIX (Portable Operating System Interface para UNIX). Familia de estándares relacionados especificados por la IEEE para definir APIs para

la compatibilidad de software entre los diferentes sistemas operativos Unix.

Instalaremos las siguientes dependencias.

[root@ascariote ~]# yum install libpcap-devel libpcap php-pear python python-devel httpd ruby

Herramienta RRDTOOL.

RRDtool es el acrónimo de Round Robin Database tool. Se trata de una herramienta que trabaja con una base de datos que maneja planificación. Esta técnica trabaja con una cantidad de datos fija, definida en el momento de crear la base de datos, y un puntero al elemento actual. Su finalidad principal es el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador. Dentro de CentOS 5 ya podremos utilizar rrdtool en la versión 1.4, pero varias aplicación incluyendo NTOP todavía no utilizan esta versión por lo cual tendremos que descargar el rrdtool 1.3. Podremos descargarlo de la siguiente manera.

root@ascariote ~]# wget http://www.express.org/~wrl/rrdtool/rrdtool-perl-1.3.9-1.el5.wrl.i386.rpm

[root@ascariote]# wget http://www.express.org/wrl/rrdtool/rrdtool-1.3.9-1.el5.wrl.i386.rpm [root@ascariote]# wget http://www.express.org/wrl/rrdtool/rrdtool-devel-1.3.9-1.el5.wrl.i386.rpm }}}

Termina la descarga de los 3 paquetes solamente queda instalarlos.

[root@ascariote ~]# rpm -ivh *.rpm

Herramienta GEOIP

GeoIP es una herramienta para identificar de que país viene el trafico de un sitio. Instalaremos las herramientas necesarias: Para esto tendremos que agregar el repositorio de Dag Wieers a nuestro sistemas por lo cual lo instalaremos de la siguiente manera.

rpm -Uhv http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.3.6-1.el5.rf.i386.rpm

Solo queda actualizar la lista de paquetes e instalar geoip.

[root@ascariote ~]# yum update && yum install geoip geoip-devel

Instalamos la aplicación geoip para poder utilizar los mapas.

[root@ascariote ~]# pecl install geoip

Compilación NTOP.

Comenzaremos la compilación de NTOP para nuestro sistema, NOTA: Se recomienda instalar NTOP en el servidor que funcionara como Gateway/Proxy para su red local.

Descarga NTOP.

Descargaremos la última versión de NTOP, podremos descargarla desde su sitio web oficial http://www.ntop.org/.

Podremos compilar NTOP dentro /opt o /usr/share.

[root@ascariote opt]# wget http://freshmeat.net/urls/e9949c704e3f73c9c0bf8ab4ab85fbc1

Descomprimir NTOP

Descomprimiremos el fichero descargado.

[root@ascariote opt]# tar xvfz ntop-3.4-pre2.tar.gz

Instalación de NTOP

Entraremos al fichero descomprimido y comenzaremos la compilación, por lo cual primero iniciaremos el comando autogen que analizara si las dependencias necesarias de NTOP como también verificara las rutas en donde se instalara.

[root@ascariote ntop-3.4-pre2]# ./autogen.sh

Ya terminado este proceso solamente tendremos que compilar y instalar NTOP.

[root@ascariote ntop-3.4-pre2]# make && make install

Password Admin

Terminada la compilación tendremos que asignarle un password al administrador de NTOP para poder hacer los cambios pertinentes dentro de la consola web.

root@ascariote NTOP-3.4-pre2]# ntop -A

Fri Feb 5 13:38:49 2010 NOTE: Interface merge enabled by default Fri Feb 5 13:38:49 2010 Initializing gdbm databases NTOP startup - waiting for user response! Please enter the password for the admin user: Please enter the password again: Fri Feb 5 13:38:56 2010 Admin user password has been set root@ascariote NTOP-3.4-pre2]#}}}

Cambiando Permisos.

Debemos cambiar el usuario y grupo apropiados para el buen funcionamiento de NTOP.

[root@ascariote ntop-3.4-pre2]# chown ntop:root /usr/local/var/ntop/

[root@ascariote ntop-3.4-pre2]# chown ntop:ntop /usr/local/share/ntop/}}}

Iniciando NTOP.

Ahora iniciaremos nuestra herramienta NTOP, podremos iniciarlo de la siguiente manera:

ntop -d -L -u ntop -P /usr/local/var/ntop --skip-version-check –use-syslog=daemon

Otro manera de iniciar la herramienta NTOP:

ntop -i "eth0,eth1" -d -L -u ntop -P /usr/local/var/ntop --skip-version-check --use-syslog=daemon

Nomenclatura:

Parámetro	**Descripción**
-i	Especificamos la interfaz o interfaces en donde monitorea NTOP.
-d	NTOP iniciara como demonio.
-L	Manda todos los mensajes del estado de NTOP a /var/log/messages
-u	Iniciamos la aplicación con el usuario NTOP.
-P	Especificamos en donde se localiza la BDs de NTOP.
--skip-version-check	Verifica periódicamente que si nuestra versión de NTOP es la actual, esta opción desactiva verificación.
--use-syslog=daemon	Usa el demonio de syslog.

Tabla 2 Parámetros NTOP

Podremos acceder a la consola administrativa web de NTOP de la siguiente manera: http://localhost:3000

2.2.8. SQUID

Squid es el software para servidor Proxy más popular y extendido entre los sistemas operativos basados sobre UNIX®. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios.

Entre otras cosas, Squid puede hacer Proxy y cache con los protocolos HTTP, FTP, GOPHERy WAIS, Proxy de SSL, cache transparente, WWCP, aceleración HTTP, cache de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

NOTA ESPECIAL: Squid no puede funcionar como proxy para servicios como SMTP, POP3, TELNET, SSH, etc. Si se requiere hacer proxy para cualquier cosa distinta a HTTP, HTTPS, FTP, GOPHER y WAIS se requerirá o bien implementar enmascaramiento de IP a través de un NAT (Network AddressTranslation) o bien hacer uso de un servidor SOCKS como Dante.

Dentro de los servidores más importantes que existen en GNU/Linux existe el servidor proxy, el cual se encarga de administrar el acceso a internet de tu red local y también es conocido como servidor intermedio, el servidor proxy que se ocupa en GNU/Linux en sus diferentes distribuciones es squid. Squid es un programa que hace cache de datos

obtenidos de internet para poder optimizar recursos de banda ancha de internet, entre sus características más importantes son:

- **Proxy/cache:** Proporciona servicio proxy a peticiones del tipo http, https y ftp a equipos que se encuentran en nuestra red local para que puedan acceder hacia internet y a su vez provee la funcionalidad de cache en el cual se almacenan localmente las paginas consultadas por los usuarios de forma que incrementa la rapidez de acceso a la información web y ftp.

- **Proxy SSL:** Es un servicio de squid compatible con SSL, con el cual se aceleran las peticiones y las peticiones hacia internet estarían cifradas.

- **Jerarquías de Cache:** Nuestro squid puede pertenecer a una jerarquía de cache que trabajan conjuntamente sirviendo peticiones. En este caso tendremos varios servidores squid resolviendo peticiones de una página web, si no la tiene registrada le pregunta a otro hasta que es encontrada la información.

- **ICP, HTCP, CARP, Cache digests:** Squid sigue los protocolos ICP, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado.

- **Proxy Transparente:** Puede ser configurado para ser usado como proxy transparente de manera que las solicitudes son enrutadas

por medio de unas reglas de firewall y sean enviadas al squid sin tener que configurar los clientes dentro de una red.

- **WCCP:** Permite interceptar y redirigir el tráfico que recibe un router hacia uno o más proxys caché, haciendo control de la conectividad de los mismos.

- **Control de Accesos:** En este parte establecemos reglas de control de acceso, esto permite establecer políticas de denegación o aceptación.

- **Aceleración de servidores HTTP:** Cuando hacemos peticiones hacia intenet la información es almacenada en el cache del squid y si hay otra solicitud hacia el mismo recurso el squid le devolverá la información que tiene el squid en cache. Si hay algún cambio entonces la información deberá ser actualizada.

- **SNMP:** Permite activar el protocolo SNMP, esto permite la administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas, pudiendo detectar problemas y proporcionar mensajes de estados.

- **Caché de resolución DNS:** Squid está compuesto también por el programa dnsserver, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos dnsserver, y cada uno de ellos realiza su

propia búsqueda en DNS. De este modo, se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS.

Instalación de squid

Para poder instalar el servicio de squid tendremos que ejecutar los siguientes como usuario root.

[root@mantis ~]# yum install squid

Con este instalaremos nuestro servidor squid más las dependencias que tenga.

Archivos de configuración del squid

Ya teniendo instalado nuestro servidor squid, ahora deberemos saber en dónde se encuentra toda la configuración del mismo.

/etc/squid

Ya dentro de esta carpeta se encontraran varios archivos pero el mas importante es el squid.conf el cual se encarga de la configuración del servicio.

Por recomendación antes de editar un archivo de configuración de algún servicio, siempre deberemos hacer una copia de respaldo original del mismo.

[root@mantis squid]# cp squid.conf squid.conf-orig

Configuración Squid

Comenzaremos a configurar nuestro servidor squid.

[root@mantis squid]# vim squid.conf

Parámetro http_port

En este parámetro configuramos el puerto de escucha de nuestro servidor squid, por default es el puerto 3128, pero también puede ser utilizado el 8080.

http_port 3128

Parámetro cache_mem

Establece la cantidad de memoria RAM dedicada para almacenar los datos más solicitados. Esta opción viene comentada por los cual la descomentaremos para darle un valor reservado en memoria RAM.

cache_mem 8 MB

por

cache_mem 50 MB

El valor ya depende del administrador y de la carga que tenga el squid.

Parámetros cache_swap

Dentro del cache_swap, existen dos parámetros: cache_swap_low cache_swap-hight Con estos le indicamos a squid que mantenga los

niveles del espacio del área de intercambio o también conocido como swap. Estos parámetros vienen siempre desactivados por cual los buscaremos para activarlos.

#cache_swap_low 90

1. cache_swap_high 95 }}}

por

cache_swap_low 90

cache_swap_high 95}}} Con esto decimos al squid que mantenga los niveles del espacio del area de intercambio entre 90% y 95%.

Parámetros maximum_object_size

Utilizamos esta directiva para indicar el tamaño máximo para los objetos a almacenar en la cache.

#maximum_object_size 4096 KB

por

maximum_object_size 10240 MB

Parámetro hierarchy_stoplist

Este parámetro es útil para indicar a squid que páginas que contengan ciertos caracteres no deben almacenarse en cache. También se pueden incluir como sitios de webmail y paginas locales en su red ya que no sería

necesario almacenarlas en el cache, esta opción ya viene habilitada solamente tendremos que modificarle algunos datos de la misma.

hierarchy_stoplist cgi-bin ?

por

hierarchy_stoplist cgi-bin ? hotmail gmail yahoo escuela.factor.com.mx

Parámetro visible_hostname

Es el nombre del equipo, el nombre debe ser igual a los siguientes ficheros /etc/hosts y en /etc/sysconfig/network. Este parámetro no viene configurado en el archivo de configuración, tendremos que agregar y que en ocasiones pueda ser que nuestro servicio de squid no quiera iniciar.

visible_hostname mantis

Parámetro cache_dir

Con este parametro establecemos el tamaño que deseamos que tenga la cache en el disco, lo cual tendremos que habilitar y modificar el siguiente dato.

#cache_dir ufs /var/spool/squid 100 16 256

por

cache_dir ufs /var/spool/squid 700 16 256

Con esto establecemos el tamaño que deseamos que tenga la cache en el disco, se puede incrementar hasta el tamaño que desee el administrador, nosotros establecemos 700MB de cache con 16 directorios subordinados y 256 niveles cada uno.

Parámetro access_log

Especifica en que directorio se realizara el registro de accesos al squid, este parámetro es importante para definir un análisis de estadísticas con webalizer.

access_log /var/log/squid/access.log squid

Parámetro cache_log

Define en donde se almacenaran los mensajes del comportamiento de la cache de squid. Por default viene desactivado.

cache_log /var/log/squid/cache.log

Reglas acl

Una ACL es una definición de control de acceso, que utiliza squid para especifica mediante el, existen varios tipos de reglas ACL que comentaremos en la tabla.

Src	Time
Dts	url_regex

Srcdomain	urlpath_regex
Dstdomain	req_mime
srcdom_regex	Macaddress
dstdom_regex	Password

Tabla 3 Reglas ACL

Regla Tipo src

Esta regla especifica una o varias direcciones IP de origen o un segmento de red con su máscara de red. Nomenclatura:

acl [Nombre] src [Contenido]

Ejemplos:

1) El nombre de la regla es llamada redlocal la cual tendría asignada un segmento de red 192.168.1.0 a 24 bits.

acl redlocal src 192.168.1.0/24

2) Esta regla es llamada jefes de los cuales solamente se le proporcionan algunas IP de nuestro segmento de red.

acl jefes src 192.168.1.10 192.168.1.20

3) Esta regla que se llama sistemas en la cual manda a llamar al archivo permitido el cual se encuentra en /etc/squid, contiene las IP de la gente que trabaja en el area de sistemas.

acl sistemas src “/etc/squid/permitidos”

Regla Tipo dts

Especifica una dirección de destino en formato IP y mascara o el nombre del sitio a visitar. Nomenclatura:

acl [Nombre] dts [Contenido]

Ejemplos:

1) En esta regla es llamada webmial la cual contendrá como destino final las direcciones de webmail más conocidos de internet.

acl webmail dst www.gmail.com www.hotmail.com www.yahoo.com

2) En esta regla es llamada iplocales la cual contendrá algunas de la IP de nuestro segmento de red.

acl iplocales dst 192.168.1.109 192.168.1.103

Regla Tipo srcdomain.

La regla de tipo srcdomain se establecen permisos sobre dominios web de origen y se determina por la resolución de DNS inversa. Para poder ocupar esta regla es necesario contar un DNS local. Nomenclatura:

acl [Nombre] srcdomain [Contenido]

Ejemplo:

La regla repos indica que máquinas de nuestra red local están agregadas a la misma.

acl repos srcdomain repoubu.dyndns.net repodeb.dyndns.net repocen.dyndns.net

Regla Tipo dstdomain

La regla de tipo dstdomain se establecen permisos sobre dominios web de destino. Nomenclatura:

acl [Nombre] dstdomain [Contenido]

Ejemplo:

La regla permitidos indicamos que dominios pueden están hacia la salida a internet

acl pemitidos dstdomain .linuxparatodos.net .factor.com.mx .eluniversal.com .reforma.com

Regla Tipo srcdom_regex

Esta regla se encarga de evaluar palabras de entrada a nuestra red, ocupándose expresiones regulares. Nomenclatura:

acl [Nombre] srcdom_regex [Contenido]

Ejemplo:

La regla intranet análisis todas las posibles palabras de factor en mayúsculas y minúsculas de nuestra red local.

acl intranet srcdom_regex -i factor\..*

Regla Tipo dstdom_regex

Esta regla se encarga de evaluar palabras de salida, ocupándose expresiones regulares. Nomenclatura:

acl [Nombre] dstdom_regex [Contenido]

Ejemplo:

La regla google_todos análisis todas las posibles palabras de google en mayúsculas y minúsculas.

acl google_todos dstdom_regex -i google\..*

Regla Tipo time

Esta regla estable un tiempo límite de conexión dentro de una semana. Parámetros por días de la semana:

Parámetros	Días
S	Domingo
M	Lunes
T	Martes
W	Miércoles
H	Jueves
F	Viernes
A	Sábado

Tabla 4 Parámetros

En el manejo de las horas se establece un horario de 24:00 hrs Nomenclatura:

acl [Nombre] time [días][horas]

Ejemplo:

La regla horario estable que está habilitada los días Lunes a Viernes de 09:00 a 18:00 hrs.

acl horario time MTWHF 09:00-18:00

Esta regla es muy útil en las escuelas, universidades ya que con esto podemos tener un control de horarios en laboratorios.

Regla Tipo url_regex

Permite especificar expresiones regulares para comprobar dicha url, a este tipo de regla se recomienda tener un archivo en cual agregamos todas la palabras que nosotros creamos que importantes. Nomenclatura:

acl [Nombre] url_regex “Path”

Ejemplo de archivo porno.txt:

Sex

xxx adult pornotube chicas porn playboy lolitas}}}

Ejemplo:

Esta regla se llama porno el cual manda a llamar a un archivo que contiene palabras relacionadas a pornografía.

acl porno url-regex “/etc/squid/listas/porno.txt”

Regla Tipo urlpath_regex

Esta regla nos permite la administración de descargas por medio de la extensión de los archivos, se recomienda tener Nomenclatura:

acl [Nombre] urlpath_regex “Path”

Ejemplo de archivo extensiones.txt:

\.avi$

\.mpg$ \.mpeg$ \.avi$ \.flv$ \.exe$ \.bat$ \.zip$ \.mp3$}}}

Ejemplo:

Esta regla se llama extensiones la cual administrara las descargas por medio de las extensiones de los archivos.

acl extensiones urlpath_regex “/etc/squid/listas/extensiones.txt”

Regla Tipo req_mime

Esta regla nos permite comprobar el tipo de petición mime que realiza un cliente. Nomenclatura:

acl [Nombre] req_mime “mime”

Ejemplo:

Esta regla se llame MSN la cual contiene el mime del mensajero MSN.

acl MSN req_mime type application/x-msn-messenger

Regla Tipo macaddress

Este tipo de regla nos permite administrar squid por medio de Mac Address. Nomenclatura:

acl [Nombre] arp “Mac Address”

Ejemplo: Esta regla se llama adminmac en la cual nosotros proporcionamos las Mac Address de las máquinas clientes.

acl adminmac arp 09:00:2b:23:45:67 00:1f:3c:5f:fd:b1 00:1e:ec:70:7e:24

Regla Tipo password

Este tipo de regla, se controla el acceso a internet por medio de un usuario y password, para poder habilitar este método tendremos que hacer lo siguientes pasos de configuración. 1) Creamos el archivo que contendrá las claves.

[root@mantis squid]# touch claves

2) Le asignamos permisos de Lectura/Escritura y el usuario encargado del archivo.

[root@mantis squid]# chmod 600 claves

[root@mantis squid]# chown squid.squid claves}}} 3)Creación de usuario y password para el acceso a internet.

[root@mantis squid]# htpasswd claves clientes

4) Habilitaremos las siguientes opciones dentro del fichero de configuración del servidor squid, busquemos el primer parámetro llamado auth_param basic.

#auth_param basic program <uncomment and complete this line>

Este parámetro lo modificaremos de la siguiente manera.

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves

Estamos enlazando la aplicación que nos permitiría autenticarnos y en donde se encuentra el archivo donde se encuentran las cuentas de los usuarios.

acl password proxy_auth REQUIRED

5) Por ultimo tendremos que habilitar la regla acl encargada de la autenticación de password.

#acl password proxy_auth REQUIRED

por

acl password proxy_auth REQUIRED

Con esto ya tendremos habilitada la regla para la autenticación de los usuarios.

Control de Acceso

El control de acceso define si se permite o deniega el acceso a las reglas para que empecemos a crear el filtrado. Nomenclatura:

http_access allow/Deny Regla

Ejemplo:

Como sabemos la regla jefes contendrá la IP de la personas encargadas de cada area de la empresa y tendrán acceso a todo el internet.

http_access allow jefes

Toda los de más clientes de la red no tendrán acceso a internet.

http_access deny redlocal

Dentro de la configuración http_access, existe una expresión “!” que significa no, esto permite que una regla se permitida o denegada. Es lo contrario a la primera definición del control de acceso.

Ejemplo: Esta regla permite navegar a todo la red en un horario de 09:00 a 18:00 Hrs y solamente a la paginas permitidas por el administrador. Pero no pueden entrar hacia los otros recursos de internet.

http_access deny redlocal !horario !permitidos

Configuración básica squid

Como vemos en el siguiente diagrama de red, especificaremos los siguientes reglas que tendrá nuestra red.

- Todas las computadoras de la empresa se encuentran dentro del segmento de red 192.168.1.0/24.
- Los jefes de cada departamento tienen salida a sin ninguna restricción a internet y sus IP son 92.168.1.10, 192.168.1.20.
- El resto de la red solamente tiene acceso a la pagina de la empresa Factor y de interés social, con un horario de 08:00 a 19:00 hrs, sin poder descargar archivos de música y vídeos.

Crearemos las reglas del squid.

acl redlocal src 192.168.1.0/24

acl jefes src 192.168.1.10 192.168.1.20 acl permitidas dstdomain “/etc/squid/permitidas” acl horario time MTWHF 08:00-19:00 acl extensiones urlpath_regex “/etc/squid/extensiones”}}} Comenzaremos a configurar el control de accesos.

http_access allow jefes

http_access deny redlocal !permitidas !horario extensiones}}} Con esto tendremos ya configurado nuestro squid, para poder exportar en proxy desde consola tendremos que hacer lo siguiente:

[root@mantis ~]# export http_proxy=http://192.168.1.254:3128

Configuración de Navegadores Web.

Solo nos falta que en las mas máquinas clientes configuremos la salida a internet por proxy.

Ejemplos:

- Firefox/Iceweasel

Menú Editar ---> Avanzadas ---> Red ---> Configuración de red.

- Opera.

Menu Herramientas ---> Preferencias ---> Avanzadas ---> Red

- Internet Explorer.

Menú Herramientas ---> Opciones de Internet --->Conexiones ---> Configuración de LAN

Configuración Squid Transparente

Este tipo de configuración de squid transparente, lo que hace es que conexiones son enrutadas al proxy sin hacer ninguna configuración en los clientes para que tengan salida a internet. Este tipo de configuración depende de reglas de nuestro firewall.

Parámetro http_port

Solamente tendremos que configurar este parámetro para que se un proxy transparente. Se le debe indicar la IP del servidor squid, puerto de escucha y la palabra transparente.

http_port 3128

por

http_port 192.168.1.254:3128 transparent

Reglas del Firewall

Para poder configurar este tipo de proxy transparente, tendremos que configurar reglas de firewall, en nuestro caso usaremos reglas de iptables ya que es la herramienta más utilizada en todas distribuciones GNU/Linux. Pero para que funcione de manera transparente debemos de aplicar la siguiente regla en iptables.

iptables -t nat -A PREROUTING -i eth1 -p tcp –dport 80 -j REDIRECT --to-port 3128

Con esto estamos desviando el trafico que venga por la LAN que vaya por web al puerto 3128. Con esto ya hicimos transparente nuestro proxy pero no se pueden desplegar las paginas seguras, para eso necesitamos aplicar otras reglas en iptables liberando el puerto 443, y lo hacemos de la siguiente manera:

iptables -t nat -A PREROUTING -i eth1 -p tcp –dport 443 -j REDIRECT --to-port 3128

Habilitamos el reenvío de paquetes dentro de la red.

echo 1 > /proc/sys/net/ipv4/ip_forward

Y Guardamos las reglas con el siguiente comando.

iptables-save > /etc/sysconfig/iptables

Reiniciamos el servicio de firewall

/etc/init.d/iptables restart

Con esto tendremos configurado nuestro squid transparente.

Squid con DMZ

Este tipo de configuración conecta a dos tipos de redes:

- Red local.
- DMZ.

Lo más importante de estas dos redes es la DMZ, la cual se le llama zona desmilitarizada, es una red que se ubica entre redes internas de una empresa. Dentro de una red DMZ habitualmente encontramos servidores que son necesarios para la empresa como:

- Servidor de Correo.

- Servidor de web.
- Servidor de FTP.
- Etc.

Parámetros en squid

Este tipo de configuración se recomienda tener a nuestro servidor squid escuchando varios puertos de comunicación ya que se tendría mejor control sobre las dos redes administradas. Para esto configuraremos el parámetro http_port en cual habilitaremos a dos puerto de escucha.

http_port 192.168.1.254:3128 transparent

Reglas del Firewall

Como podemos ver una configuración también de un proxy transparente.

#REDLOCAL

iptables -t nat -A PREROUTING -i eth1 -p tcp –dport 80 -j REDIRECT --to-port 3128

1. DMZ

iptables -t nat -A PREROUTING -i eth2 -p tcp –dport 80 -j REDIRECT --to-port 3129}}} Con esto estamos desviando el tráfico de la red local y DMZ a sus puerto correspondientes del squid de cada uno y tener salida hacia internet.

RED LOCAL

iptables -t nat -A PREROUTING -i eth1 -p tcp –dport 443 -j REDIRECT --to-port 3128

1. DMZ

iptables -t nat -A PREROUTING -i eth2 -p tcp –dport 443 -j REDIRECT --to-port 3129}}} Habilitamos el reenvío de paquetes dentro de la red.

echo 1 > /proc/sys/net/ipv4/ip_forward

Y Guardamos las reglas con el siguiente comando.

iptables-save > /etc/sysconfig/iptables

Reiniciamos el servicio de firewall

/etc/init.d/iptables restart

Con esto tendremos configurado nuestro squid transparente.

Configuración squid transparente con DMZ

Como vemos en el siguiente diagrama de red, especificaremos los siguientes reglas que tendrá nuestra red.

- La red local de la empresa se encuentra en segmento de red 192.168.1.0/24
- La DMZ de la empresa se encuentra en un segmento de red 10.2.0.0/8

- Los jefes de cada departamento tienen salida a sin ninguna restricción a internet y sus IP son 92.168.1.10, 192.168.1.20.
- El resto de la red solamente tiene acceso a la pagina de la empresa Factor y de interés social, con un horario de 08:00 a 19:00 hrs, sin poder descargar archivos de música y vídeos.
- Dentro la red DMZ tienen permiso a todo menos a descargar música, vídeos, programas.

Crearemos las reglas del squid.

acl dmz src 10.2.0.0/6

acl redlocal src 192.168.1.0/24 acl jefes src 192.168.1.10 192.168.1.20 acl permitidas dstdomain “/etc/squid/permitidas” acl horario time MTWHF 08:00-19:00 acl extensiones urlpath_regex “/etc/squid/extensiones”}}} Comenzaremos a configurar el control de accesos.

http_access allow dmz !extensiones

http_access allow jefes http_access deny redlocal !permitidas !horario extensiones}}} Con esto tendremos ya configurado nuestro squid.

Configuración de squid + DansGuardian + clamav

Squid puede apoyarse de otras aplicaciones como:

- SquidGuard.

- Clamav.

Estos nos apoyan a tener un control del acceso a internet.

Instalación DansGuardian/clamav

Para poder instalar DansGuardian es necesario instalar los siguientes y librerias para su funcionamiento:

1) Tendremos que instalar el antivirus clamav.

[root@mantis ~]# yum install clamd

Hay que actualizar nuestro antivirus.

[root@mantis ~]# fleshclam

Solo falta iniciar el servicio.

[root@mantis ~]# /etc/init/clamd start

2) También tendremos que instalar openssl, es un herramienta de seguridad y tiene herramientas de cifrado.

[root@mantis ~]# yum install openssl-devel openssl

3) Tendremos que instalar las librerías de compilación.

[root@mantis ~]# yum install rpm-build gcc-c++ gcc zlib

4) Descargaremos las librerías de smtp, este se encarga de envío de correo.

wget http://download.fedora.redhat.com/pub/epel/5/i386/libesmtp-1.0.4-5.el5.i386.rpm

wget http://download.fedora.redhat.com/pub/epel/5/i386/libesmtp-devel-1.0.4-5.el5.i386.rpm}}} Ya que los tenemos descargados tendremos que crearemos un enlace simbólico a la libreria de clamav.

[root@mantis ~]# ln -s /usr/lib/libclamav.so.6 /usr/lib/libclamav.so.1

Instalaremos los paquetes libestmp libesmtp-devel de la siguiente manera:

[root@mantis ~]# rpm -ivh libesmtp*.rpm

5) Descargaremos dansguardian con su parche de antivirus.

wget
http://www.mirrorservice.org/sites/download.sourceforge.net/pub/sourceforge

/d/dg/dgav/dansguardian-antivirus-6.4.4.2-1.src.rpm}}} Ya descargado, ahora tendremos que compilar el paquete.

[root@mantis ~]# rpmbuild --rebuild dansguardian-antivirus-6.4.4.2-1.src.rpm

La compilación del paquete puede tardar varios minutos dependiendo de las características de la máquina. Cuando termine la compilación, tendremos que acceder a la siguiente ruta.

[root@mantis ~]# cd /usr/src/redhat/RPMS/i386/

En esta ruta es donde se encuentra el rpm compilado de dansguardian, solo queda instalarlo.

[root@mantis i386]# rpm -ivh dansguardian-antivirus-6.4.4.2-1.i386.rpm

6) Por momento solamente queda configurar nuestro dansguardian, su archivo de configuración se encuentra en /etc/dansguardian/dansguardian.conf.

[root@mantis ~]# vim /etc/dansguardian/dansguardian.conf

Modificaremos o habilitaremos los siguientes parametros:

language = 'spanish'

filterip = 192.168.1.254 filterport = 8080 proxyip = 192.168.1.254 proxyport = 3128 daemonuser = 'clamav' daemongroup = 'clamav' clamdsocket = '/tmp/clamd.socket' virusengine = 'clamdscan, clamav' loglocation = '/var/log/dansguardian/access.log'}}} Crearemos el archivo access.log que contendrá los acceso al dansguardian.

[root@mantis ~]# touch /var/log/dansguardian/access.log

[root@mantis]# chown root.root /var/log/dansguardian/access.log [root@mantis]# chmod 666 /var/log/dansguardian/access.log}}} Iniciamos los servicios de antivirus, proxy y dansguardian:

[root@mantis ~]# /etc/init.d/clamd restart

[root@mantis]# /etc/init.d/squid restart [root@mantis]# /etc/init.d/dansguardian start}}}

Configuración de DansGuardian/Squid

Ya que tenemos funcionando el dansguardian y clamav solo falta modificar algunos parámetros dentro de la configuración del squid para que tengan comunicación entre squid y dansguardian. Como siempre debemos indicar la IP del servidor y puerto de escucha, y agregaremos otros parámetros de los cuales permite crear el enlace entre las dos aplicaciones.

http_port 192.168.1.254:3128 transparent

tcp_outgoing_address 192.168.2.1 cache_peer 127.0.0.1 sibling 8080 7 cache_peer 192.168.2.1 parent 3128 7 }}} Con esto ya tendremos configurado nuestro squid solo queda reiniciarlo.

[root@mantis ~]# /etc/init.d/squid restart

Configuración de iptables

Que configurar nuestras reglas de ruteo y de acceso a la red interna

###Hacemos limpieza de reglas existentes de entrada, salida, Ruteo y nateo

iptables -F iptables -X iptables -Z iptables -t nat -F iptables -t nat -X iptables -t nat -Z

1. Habilitamos el renvío de paquetes y como a máquinas dinámicas

echo "1" > /proc/sys/net/ipv4/ip_forward echo "1" > /proc/sys/net/ipv4/ip_dynaddr

1. Aceptamos conexiones locales

iptables -A INPUT -i lo -j ACCEPT

1. Aceptamos conexiones de tipo de DNS a nuestro servidor

iptables -A INPUT -p udp --dport 53 -j ACCEPT iptables -A INPUT -p tcp --dport 53 -j ACCEPT

1. Aceptamos conexiones del segmento de red 192.168.2.0 por la interfaz eth1

iptables -A INPUT -s 192.168.2.0/24 -i eth1 -j ACCEPT

1. Creamos un nateo de la red interna hacia afuera de la red.

iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -d 0.0.0.0/0 -j MASQUERADE

1. Aceptamos peticiones de la tarjeta de red eth1

iptables -A FORWARD -i eth1 -j ACCEPT

1. Aceptamos peticiones de la red local al puerto 80.

iptables -A FORWARD -s 192.168.2.0/24 -p tcp --dport 80 -j ACCEPT

1. Aceptamos peticiones de entrada/salida por medio de protocolo udp del servidor DNS 192.168.1.1

iptables -A INPUT -s 192.168.1.1 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -s 192.168.1.1 -p udp -m udp --dport 53 -j ACCEPT

1. Todo petición que venga de la red local que vaya hacia el puerto 80 mandalo al puerto 8080

iptables -t nat -A PREROUTING -s 192.168.2.0/24 -p tcp --dport 80 -j REDIRECT --to-port 8080

1. Toda conexión que venga de la red local haz un nateo con salida de la ip del servidor.

iptables -t nat -A POSTROUTING -i eth1 192.168.2.0/24 -o eth0 -j SNAT --to-sources 192.168.1.240

1. Genera un archivo de configuracion de la reglas y lo guardas en la ruta indicada

iptables-save > /etc/sysconfig/iptables

1. reinicia el servicio de iptables o firewall

/etc/init.d/iptables restart}}} Con esto ya tendremos configurado nuestro servicio de Squid Transparente con DansGuardian y Clamav.

Quedando de la siguiente manera nuestra configuración como se muestra en el siguiente diagrama, toda petición al puerto 80 sera reenviada al 8080 que tiene DansGuardian, analizada con el antivirus y al terminar todo este proceso sera enviada a squid.

Herramientas de Análisis de tráfico

Dentro de squid existen dos herramientas:

- sarg
- calamaris

Esta herramientas nos permite generar reportes de la información que está pasando por el squid, como podemos ver la información de cada máquina que paginas han visitado, es como u histórico de cada computadora de nuestra red. Para poder ocupar estas herramientas es necesario tener instalado el servicio de apache dentro de squid, porque si no sera posible utilizar estas herramientas.

[root@mantis ~]# yum install httpd

Instalación/configuración SARG

Tendremos que instalar la herramienta de Sarg.

[root@mantis ~]# yum install sarg

Ahora tendremos que habilitaremos o modificaremos algunas de las opciones del archivo de configuración de sarg.

language Spanish

access_log /var/log/squid/access.log title "REPORTE DE SQUID" font_face Arial header_color darkblue header_bgcolor blanchedalmond background_color white text_color black text_bgcolor beige title_color green output_dir /var/www/sarge date_format u weekdays 0-6 hours 0-23 overwrite_report yes report_type topsites users_sites sites_users date_ time denied auth_failures site_user_time_date time_by bytes}}} Tendremos que reiniciar el servicio de apache, para que agregue a la configuración del fichero /etc/httpd/conf.d/sarg.conf al apache.

[root@mantis ~]# /etc/init.d/httpd restart

Ahora tendremos que inicia la aplicación de sarg.

[root@mantis ~]# sarg

SARG: Records in file:436, reading:100.0 %}}} Con esto indica que nuestro sarg ya empezó a crear el informe y fue creado al 100%. Solo falta entrar con nuestro navegador a la dirección http://127.0.0.1/sarg o http://IP/sarg.

Instalación/configuración CALAMARIS

Tendremos que instalar la herramienta de calamaris.

[root@mantis ~]# yum install calamaris

La configuración de calamaris es un poco mas tediosa que sarg. En calamaris no tiene un archivo de configuración propio cuando se instala aplicación, lo que tendremos que hacer es crear el archivo manualmente.

[root@mantis ~]# vim /etc/calamaris.conf

Y tendremos que agregarle los siguientes parámetros:

Reporte Por Dia

daily:root:/var/www/calamaris/daily.html:both:'Squid daily'

1. Reporte por Semana

weekly:root:/var/www/calamaris/weekly.html:both:'Squid weekly'

1. Reporte por Mes

monthly:root:/var/www/monthly.html:both:'Squid monthly' }}} También crearemos el archivo de configuración para apache.

[root@mantis ~]# vim /etc/httpd/conf.d/calamaris.conf

Deberá contener a los siguientes parámetros.

Alias /calamaris "/var/www/calamaris"

<Directory "/var/www/calamaris"> Options Indexes MultiViews AllowOverride None Order allow,deny

1. Allow from all

Allow from 192.168.1.0/24 </Directory> }}} Se creara el directorio de alojamiento de reportes, tambien se le otorgara permisos al usuario squid y grupo apache.

[root@mantis ~]# mkdir /var/www/calamaris

[root@mantis]# chown squid.apache /var/www/calamaris -R}}} Reiniciamos el servicio de apache.

[root@mantis ~]# /etc/init.d/httpd restart

Generando el reporte.

[root@mantis ~]# cat /var/log/squid/access.log |

calamaris -R -1 -a -F html > /var/www/calamaris/reporte-hoy.html}}} Solo falta entrar con nuestro navegador a la dirección http://127.0.0.1/calamaris o http://IP/calamaris. Con esto ya podremos ver toda la información que es genera en la red cuando los usuarios acceden a internet

2.2.9. SARG

Sarg es un programa para ver los informes de uso del Squid de una red. En palabras de su programador: Sarg es un SquidAnalysisReportGenerator que te permite ver "dónde" están yendo tus usuarios dentro de Internet. Sarg genera informes en html, con muchos campos, como: usuarios, Direcciones IP, bytes transmitidos, sitios web y tiempos.

La instalación puede hacerse mediante paquetes, aunque no he probado ninguno. Si se hace con el fichero comprimido que hay en la web se instala rápidamente con la secuencia mundialmente conocida de configure, make y makeinstall (de verdad, últimamente me resulta más entretenido instalar cosas en Windows, en Linux es todo asquerosamente fácil).

Sarg es el Generador de Reportes de Análisis para Squid (***Squid Analysis Report Generator***)el cual genera reportes de accesos de los usuarios que pasan por el proxy de la red.

Antes de iniciar se asume que está instalado y configurado el servicio de SQUID en el servidor GNU/Linux CentOS. Sino conoce como hacerlo visite este enlace. Para hacer la descarga del paquete existen dos formas:

1) Se descarga el paquete sarg desde acá.

Nota: recuerde descargar el paquete correspondiente a su arquitectura de hardware.

Descargado el paquete se instala;

rpm -Uvh sarg-2.2.3.1-1.el5.rf.x86_64.rpm

2) Con el repositorio instalado de nombre **rpmforge,** puede descargarlo de acá, ejecute la siguiente sintaxis;

yum install sarg

Se edita el archivo de configuración ubicado en **/etc/sarg/sarg.conf**

Idioma desplegado;

language **Spanish**

Ruta de acceso al directorio squid;

access_log /var/log/squid/access.log

Titulo;

title “**Reporte de Acceso de Usuarios de Squid**”

font_face Arial

header_color darkblue

header_bgcolor blanchedalmond

header_font_size -1

background_color white

text_color black

text_bgcolor beige

title_color green

Directorio Publico;

output_dir **/var/www/sarg**

Resolución por IP;

resolve_ip yes

topuser_sort_field BYTES reverse

user_sort_field BYTES reverse

date_format u

remove_temp_files yes

index yes

overwrite_report yes

use_comma no

topsites_num 100

topsites_sort_order CONNECT D

max_elapsed 28800000

report_type topsites users_sites sites_users date_time denied

auth_failures site_user_time_date

long_url no

date_time_by bytes

Como usuario **root** ejecute el siguiente comando;

sarg

Se generará un fichero al cual puedes acceder a través del navegador Web;

http://localhost/sarg/

2.2.10. IPTABLES

IPtables es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo.

Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación (esto es una pequeña mentira, ha tenido alguna vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): iptables está integrado con el kernel, es parte del sistema operativo. Para ponerlo en marcha lo que se hace es aplicar reglas. Para ello se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shellen el que se van ejecutando las reglas de firewall.

2.2.11. CACTI

Cacti. Nos permite monitorizar en tiempo real las redes, Dispositivos de red, servidores y servicios que tengamos implementados en nuestro servidores, El mismo Cacti esta escrito en PHP y genera gráficas utilizando la herramienta RRDtool.

Instalación Cacti

Para poder instalar Cacti en nuestro servidor es necesario seguir los siguientes pasos:

Dependencias

Instalaremos las siguientes dependencias necesarias para el buen funcionamiento de cacti.

[root@ascariote ~]# yum install vim-enhanced net-snmp net-snmp-utils php-snmp initscripts ruby

Instalación RRDTOOL

RRDtool es el acrónimo de Round Robin Database tool, es una herramienta que trabaja con una BD que maneja Planificación Round-robin. Esta herramienta es la que nos va permitir crear los reportes de los estado de la red, servidores y servicios en gráficas.

Para CentOS 5 es necesario descargar RRDTOOL desde su sitio oficial ya que en los repositorios de CentOS se encuentra un desactualizado y Cacti genera muchos problemas.

Por lo cual descargaremos RRDTOOL de la siguiente manera.

wget [[http://www.express.org/~wrl/rrdtool/rrdtool-perl-1.3.9-1.el5.wrl.i386.rpm|http://www.express.org/~wrl/rrdtool/rrdtool-perl-1.3.9-1.el5.wrl.i386.rpm]]

wget http://www.express.org/wrl/rrdtool/rrdtool-1.3.9-1.el5.wrl.i386.rpm }}}

Instalamos los paquetes descargados.

[root@ascariote]# rpm -ivh rrdtool-*.rpm

Preparando... ### [100%] 1:rrdtool-perl ### [50%] 2:rrdtool

[100%]

[root@ascariote]# }}}

Instalación/Configuración MySQL y PHP

Cacti requiere de una BDs como MySQL por lo cual lo tendremos que instalar.

[root@ascariote ~]# yum -y install mysql mysql-server

Como también debemos instalar PHP y el conector hacia la BDs MySQL

[root@ascariote ~]# yum install php php-mysql php-cli php-common httpd

Iniciamos el servidor de MySQL

[root@ascariote ~]# service mysqld start

Le creamos un password al administrador de MySQL.

[root@ascariote ~]# mysqladmin -u root password cursolpt

Creando BD Cacti

Conectaremos a la consola de administracion de MySQL.

[root@ascariote]# mysql -u root -p

Enter password: Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL connection id is 3 Server version: 5.0.77 Source distribution Type 'help;' or '\h' for help. Type '\c' to clear the buffer. mysql> }}}

Creamos la BD para cacti.

mysql> create database cacti;

Query OK, 1 row affected (0.01 sec) }}} Configurando usuario admincacti con los permisos con su contraseña.

mysql> GRANT ALL PRIVILEGES ON cacti.* TO “admincacti”@”localhost” IDENTIFIED BY “cursolpt”;

Query OK, 0 rows affected (0.00 sec) mysql> FLUSH PRIVILEGES; Query OK, 0 rows affected (0.00 sec) }}}

Configuración CACTI

Para poder instalar Cacti tendremos que agregar un nuevo repositorio llamado dag wieers, lo podremos agregar de la siguiente manera.

rpm -Uhv [[http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.3.6-1.el5.rf.i386.rpm|http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.3.6-1.el5.rf.i386.rpm]]

}}}

Instalamos la herramienta de monitoreo de redes Cacti

[root@ascariote ~]# yum install cacti

Creando estructura BD Cacti

Ya teniendo configurado MySQL y instalado Cacti ahora tendremos que ejecutar el siguiente comando el cual nos ayudara a crear toda la estructura de nuestra BD de Cacti.

[root@ascariote]# mysql -u admincacti -p cacti < /var/www/cacti/cacti.sql

Enter password: }}}

Configurando Conexión a MySQL

Se debe configurar dentro de Cacti el archivo config.php que se encuentra dentro del portal del mismo

[root@ascariote ~]# vim /var/www/cacti/include/config.php

Solamente tendremos que modificar algunos parámetros de nuestra conexión a MySQL.

$database_type = "mysql";

$database_default = "cacti"; $database_hostname = "localhost"; $database_username = "admincacti"; $database_password = "cursolpt"; $database_port = "3306"; }}}

Con esto ya tendremos todo configurado en cacti.

Configuración Apache

Ahora tendremos que configurar el servidor Apache para que nos permita visualizar el Cacti desde cualquier equipo, para esto Cacti creo un archivo

de configuración en /etc/httpd/conf.d/cacti.conf. Este archivo lo tendremos que editar.

[root@ascariote ~]# vim /etc/httpd/conf.d/cacti.conf

Dentro de este archivo contiene los siguientes parámetros:

Alias /cacti/ /var/www/cacti/

<Directory /var/www/cacti/> DirectoryIndex index.php Options -Indexes AllowOverride all order deny,allow deny from all allow from 127.0.0.1 AddType application/x-httpd-php .php php_flag magic_quotes_gpc on php_flag track_vars on </Directory> }}}

Dentro de este archivo solamente tendremos que comentar con un # el parámetro deny from all.

#deny from all

Con esto ya tendremos conexión a Cacti por medio de cualquier equipo de la red local.

Iniciando servicios necesarios Cacti

Iniciaremos o reiniciaremos los servicios necesarios para Cacti.

[root@ascariote]# service httpd restart

[root@ascariote]# service mysqld restart [root@ascariote]# service crond restart}}}

Para terminar la instalacion de Cacti es necesario abrir nuestro navegador favorito y teclear la siguiente url http://localhost/cacti/install o http://192.168.1.201/cacti/install

Post-Instalación Cacti

Para terminar la instalación de Cacti seguiremos los siguientes pasos en donde solamente tendremos que aceptar algunas opciones.

- Nueva: Instalación limpia dentro del sistema.
- Actualización: Permite actualizar una versión ya instalada anteriormente.

Como también verifica las conexiones hacia la BD de Cacti.

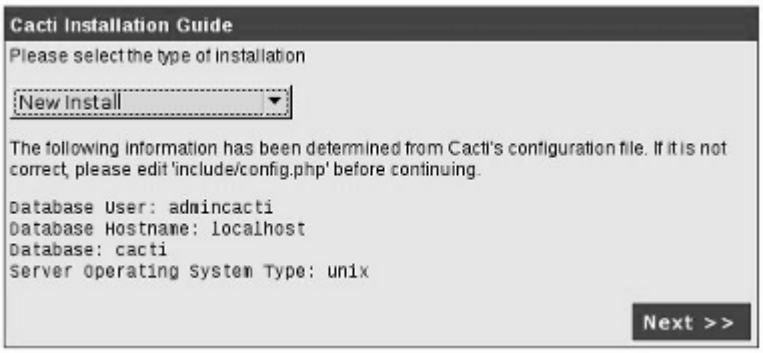


Ilustración 7 Indicando que va ser una instalación nueva de Cacti. Detectando dependencias en cacti.

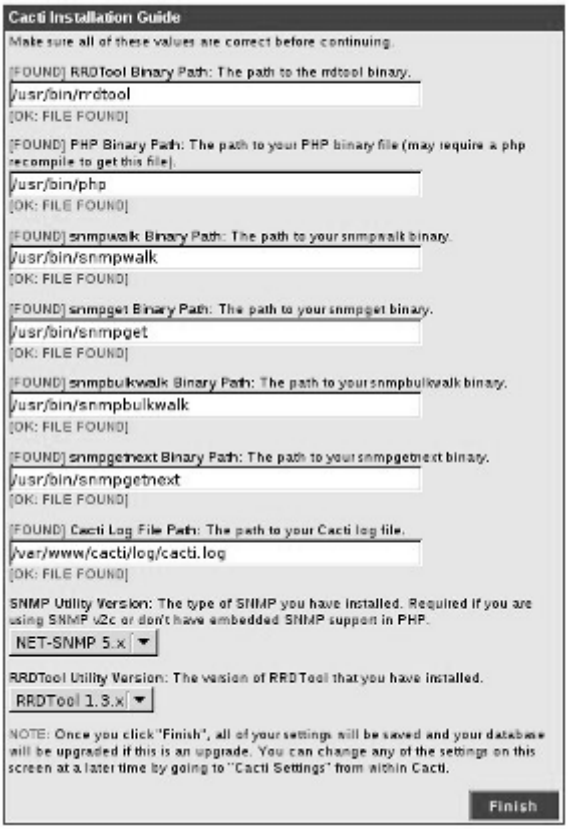


Ilustración 8 Verificando Dependencias de Cacti

Terminado este proceso solamente nos queda acceder al sitio por default el usuario es admin y contraseña admin.

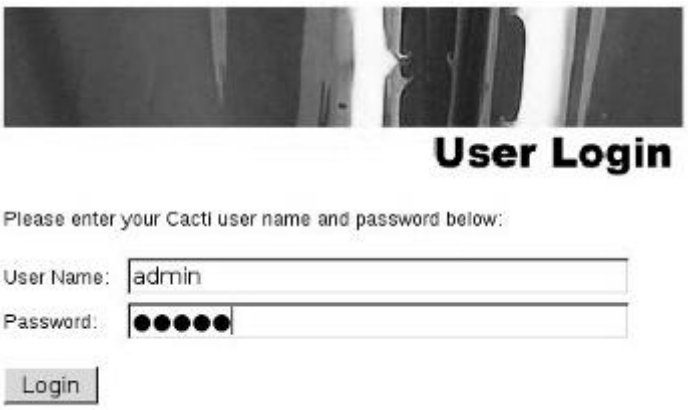


Ilustración 9 Accediendo al aplicación de Cacti.

Al momento de acceder al sitio este nos indicara que cambiemos el password del admin de Cacti, ya que es una contraseña muy débil.

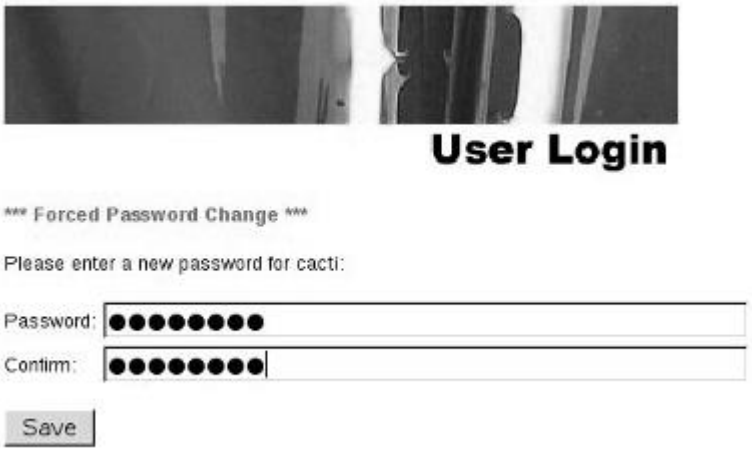


Ilustración 10 Cambiando contraseña del admin en cacti

Analizar Clientes en la red

Nosotros podremos analizar el estado actual de nuestro servidor remotamente con cacti, solamente se requiere que tenga instalado y configurado el SNMP en las maquinas clientes para que Cacti pueda obtener la información de los equipo en tiempo real.

Configurando Cliente

Como podremos agregar clientes para que sean analizados, en cacti se pueden agregar de la siguiente manera, existe un menú llamado Management el cual tiene la opción de Devices a ese le damos un click..

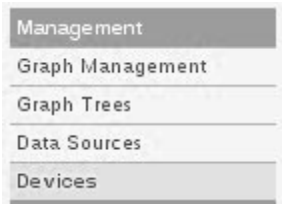


Ilustración 11 Menu de Managent en Cacti

Dentro de la opción Device nos mostrara los equipos ya configurado en Cacti por default ya viene configurado el localhost, para poder agregar mas equipos lo que tenemos que hacer dar un click en la opción de Add que se encuentra en la parte superior.

Ilustración 12 Agregando Maquinas a Cacti.

Configuración Dispositivo.

En la configuración del dispositivo o server que se desee analizar por me cacti, tendríamos que llenar los siguientes parámetros.

- Descripción: Una pequeña descripción del dispositivo a analizar, como también puede ser el nombre la maquina
- Hostname: Nombre el equipo o IP para que se conecte cacti y empiece a capturar información.
- Host Template: Seleccionamos el tipo de template que usaremos para nuestro dispositivo o server, tenemos varios templares a nuestra disposición.

Cisco Router.	Karlnet Wireless Bridge	Netware 4/5 Server
Generic SNMP-enabled Host.	Local Linux Machine	ucd/net SNMP Host
Windows 2000/XP Host		

Tabla 5 Host Template

- Disable Host: Para deshabilitar un dispositivo o servidor.

Ilustración 13 Configurando las opciones de Devices del dispositivo o cliente de la red.

Configuración Detectando el dispositivo.

En esta parte configuraremos el método por el cual nuestro servidor de monitoreo va detectar los dispositivos de la red local. Por lo general se recomienda el ping.

- Downed Divice Detection: Tendremos que determinar el metodo por él se a detectar el cliente de cacti, tenemos las siguiente opciones:

PingPing And SNMP

Ping Or SNMPSNMP

- Ping Method: Seleccionaremos el metido de envío del PING

IMCP PingTCP Ping

- Ping Port: Que puerto de Conexión que usara el ping.
- Ping Timeout Value: Tiempo de espera del ping.
- Ping Retry Count: Cuantas ocasiones se debe repetir este proceso del ping.

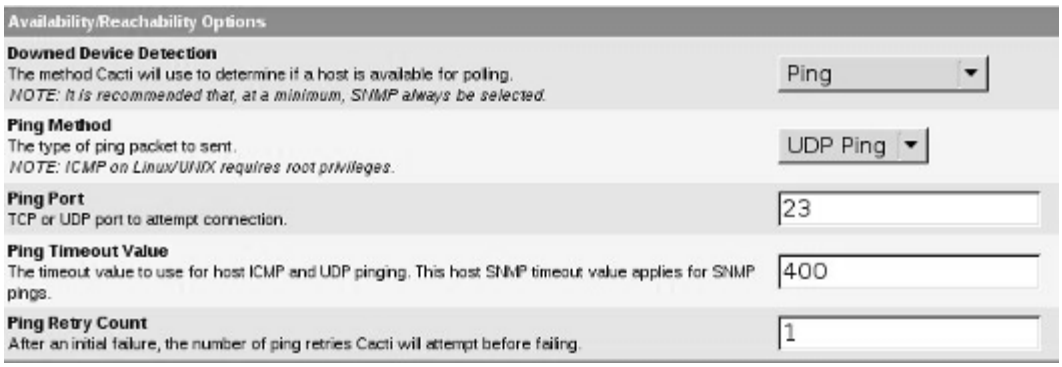


Ilustración 14 Configurando la detección del cliente cacti.

Configuración SNMP

Configuraremos el tipo de conexión SNMP que usaremos para conectarnos a los clientes SNMP.

- SMPD Versión: Podremos seleccionar la versión del protocolo SNMP a utilizar, entre sus opciones tenemos las versiones 1, 2,3.

- SNMP Community: Preguntara usuario de conexión o contraseña del grupo, esta configuración debe estar en el SNMP del cliente
- SNMP Port: Puerto del servicio SNMP de los clientes.
- SNMP Timeout: Tiempo de espera para el servicio SNMP en los clientes
- Maximum OID's Per GetRequest: Número máximo de OID “Identificadores de objetos”

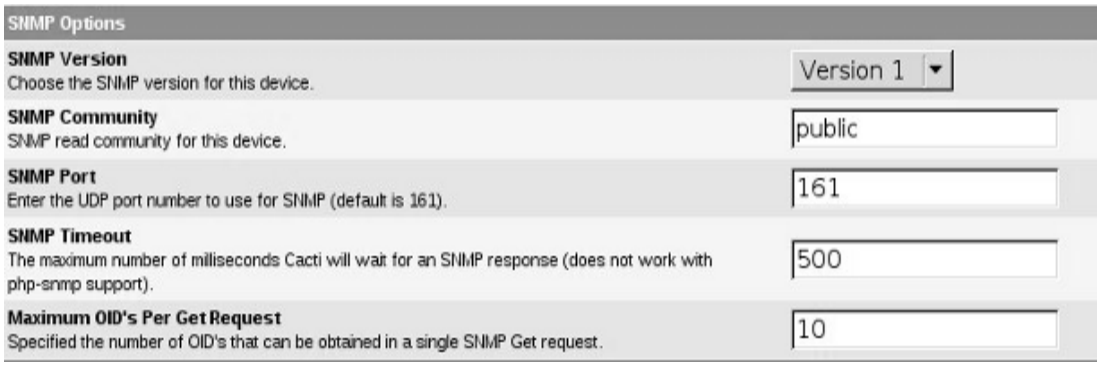


Ilustración 15 Configurando las opciones de conexión con los cliente Cacti.

Comentarios

En esta parte solamente pondremos unos simples comentarios relacionados hacia el dispositivo o servidor que se va analizar.

Ilustración 16 Comentarios del cliente Cacti.

Templates de gráficas

En esta parte seleccionaremos los templates de tipo gráficas para algunos servicios o recursos del servidor.

Fig. 4.10 Seleccionando gráficas para algunos servicios.

Consultas a clientes Cacti.

En esta parte solamente mandaremos a llamar algunos templates que nos ayudaran a realizar consultas a los clientes de cacti.

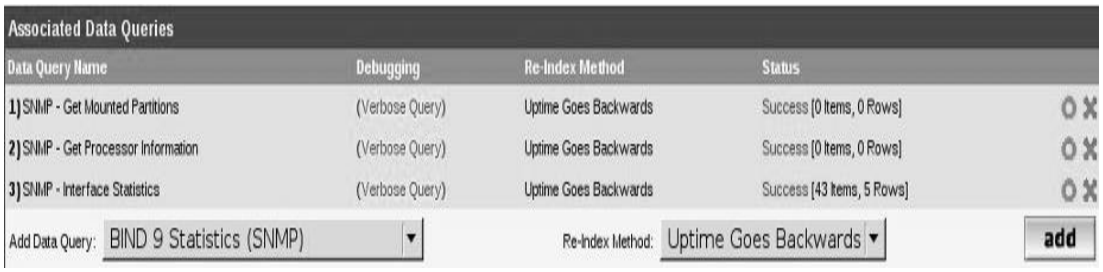


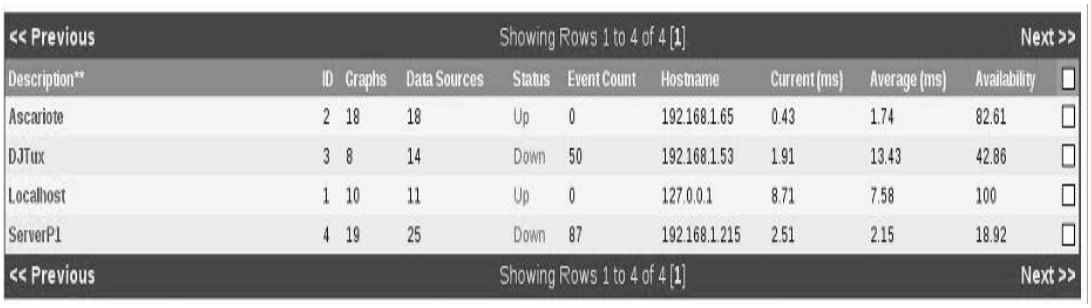
Ilustración 17 Agregando templates para hacer las consola.

Guardamos la configuración y esperaos que el cliente nos devuelva toda la información recolectada.

Visualizar Clientes.

Visualizar los clientes que cacti ya tiene registrados es muy facil solamente tendremos que ir al menu Management ---> Device, en ka

siguiente mostrara el nombre de los equipo registrador en cacti. Con esto ya tendremos monitoreados los clientes dentro cacti.



<< Previous | Showing Rows 1 to 4 of 4 [1] | Next >>

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability
Ascariote	2	18	18	Up	0	192.168.1.65	0.43	1.74	82.61
DJTux	3	8	14	Down	50	192.168.1.53	1.91	13.43	42.86
Localhost	1	10	11	Up	0	127.0.0.1	8.71	7.58	100
ServerP1	4	19	25	Down	87	192.168.1.215	2.51	2.15	18.92

<< Previous | Showing Rows 1 to 4 of 4 [1] | Next >>

Ilustración 18 Visualizando los clientes configurados en cacti.

Visualizar reportes.

Con los clientes agregados ahora como puedo visualizar las gráficas de un cliente, para esto tendremos que ir a la pestaña de graphs.

Ilustración 19 Para visualizar las gráficas de los clientes.

Al momento de entrar a los reportes este nos mostrara todas las gráficas que existen cacti de todos los clientes, pero existe la opción de poder seleccionar solamente gráficas de un equipos, para entrar a esta opción solamente tendremos que ir a la pestaña de gráficas.

Ilustración 20 Para visualizar las gráficas de los clientes.

Con esto solamente tendremos que seleccionar que cliente queremos que nos despliegue sus gráficas, debemos de ir en la opción de Host

seleccionar el cliente que solamente deseamos obtener su información. Es posible obtener información del día en transcurso, varios días anteriores, por horas y hasta por fechas, esta información puede ser desplegada por estos formatos.

Ilustración 21 Visualizando información por medio de gráficas.

Tomando en cuenta estas acciones Cacti solamente mostrara las gráficas de nuestro equipo elegido como también tomando las características de la información a desplegado.

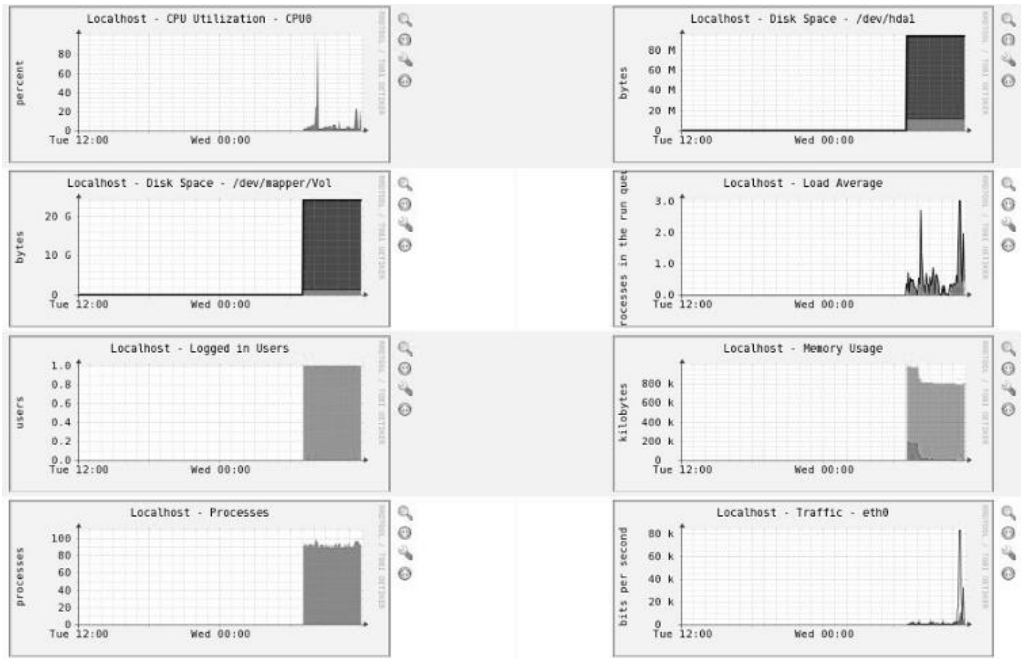


Ilustración 22 Visualizando información de un servidor.

CAPÍTULO III

MARCO METODOLÓGICO

3. **MARCO METODOLÓGICO**

3.1. MODALIDAD DE LA INVESTIGACIÓN

En este proyecto vamos a utilizar la investigación cualitativa por que se refiere a opiniones obtenidas de encuestas o entrevistas.

Visto de esta manera, la información cualitativa serviría, para clasificar el grado de aceptación del proyecto por parte de los beneficiarios.

3.2. TIPO DE INVESTIGACIÓN

Para este proyecto los tipos de investigación que vamos a utilizar son las siguientes: La investigación bibliográfica y la investigación de campo.

Investigación Bibliográfica

La investigación bibliográfica porque vamos a utilizar un amplio contenido de información a través de documento como por ejemplo libros, publicaciones, material de referencia, internet, etc.

Investigación De Campo

La investigación de campo por que trataremos de comprender y resolver alguna situación, necesidad o problema en un contexto determinado.

Este tipo de investigación nos permitirá obtener los datos más relevantes a ser analizados. Empleando la información obtenida a través de las técnicas de la observación, entrevista y cuestionario. Con sus propios

procedimientos e instrumentos para la recolección de datos, junto a los mecanismos específicos de control y valides de la información.

3.4. HIPOTESIS Y VARIABLES

3.4.1. HIPOTESIS

Con la aplicación de Servicios de Calidad (QoS) a las redes de la facultad de Administración Finanzas e Informática se mejorará la distribución del ancho de banda del enlace a internet

3.4.2. VARIABLES

Variable Independiente: Implementación de un servidor Servicios de Calidad (QoS) y Balanceo de carga del internet

Variable Dependiente: Distribución del ancho de banda de internet en la red informática FAFI.

3.5. POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN

La población o universo para la investigación del balanceo de carga del enlace al internet se obtendrá de la población Usuarios Conectados a la Red de la Facultad de Administración Finanzas e Informática.

Estudiantes	1822
Docentes	112
Personal Administrativo	24
Total	1958

Tabla 6.- Población Y Muestra De La Investigación

FÓRMULA:

n= Tamaño de la muestra

z= V. confianza

p= Población

$$n = \frac{z * p}{(p-1)(z^2/2^2)+z}$$

$$n = \frac{0{,}05^{*}1958}{(1958-1)((0{,}05)^2/2^2)+0{,}05}$$

$$n = \frac{97.90}{(1957)(0.025/4)+0{,}05}$$

$$n = \frac{97.90}{}$$

(1957)(0.000625)+0,05

$$n = \frac{97.90}{1.273125}$$

n=77

El tamaño de la muestra a analizar es 77

3.5. MÉTODOS, TÉCNICAS E INSTRUMENTOS DE LA INVESTIGACIÓN

ENCUESTA DIRIGIDA A: USUARIOS CONECTADOS A LA RED DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA.

OBJETIVOS: Verificar si es necesario la realización de la Implementación de la Calidad de Servicio (QoS) y monitoreo de redes para gestionar el balanceo de carga del enlace a Internet en la Facultad de Administración, Finanzas e Informática.

1) ¿Cree Ud. que con la implementación del monitoreo de redes se gestionará mejor el acceso de alta velocidad a Internet dentro de la facultad?

SI ☐ NO ☐ TALVEZ ☐

2) ¿Cree que se debería mejorar la velocidad del internet?

SI ☐ NO ☐ NO CONTESTA ☐

3) ¿Está de acuerdo en contar con un internet más rápido y seguro?

DE ACUERDO ☐ DESACUERDO ☐ NO RESPONDE ☐

4) ¿Cree usted que es conveniente que exista un administrador de red para su facultad?

SI ☐ NO ☐ TALVEZ ☐

5) ¿Le gustaría que cuando se conecte a la red de la facultad el administrador de la red le asigne la velocidad de Internet de una manera diferenciada?

SI ☐ NO ☐ TALVEZ ☐

6) ¿Le gustaría que cuando a la hora de realizar Descargas de Programas o Investigación no haya retardos ni interrupción en la entrega de la información?

SI ☐ NO ☐ QUIZÁS ☐

7) En un rango del 1 al 10 ¿Cómo considera actualmente la conexión a internet que existe en la facultad?

_____

8) ¿Piensa Ud. que todas las universidades debería por lo menos contar con un Internet Rápido y Seguro?

SI ☐ NO ☐ NO CONTESTA ☐

9) ¿Considera usted factible realizar clases mediante video conferencias en la facultad??

SI ☐ NO ☐ NO OPINA ☐

10) ¿Cómo considera la velocidad de descarga actualmente en la facultad?

BUENO ☐ MALO ☐ REGULAR ☐

3.6. TABULACION DE RESULTADOS

1) ¿Cree Ud. que con la implementacióndel monitoreo de redes se gestionará mejor el acceso de alta velocidad a Internet dentro de la facultad?

OPCIONES	RESPUESTA %	RESPUESTA
SI	65%	50
NO	26%	20
TALVEZ	9%	7
TOTAL	100%	77

Tabla 7.- Tabulación de Resultados

Implementación de Monitoreo

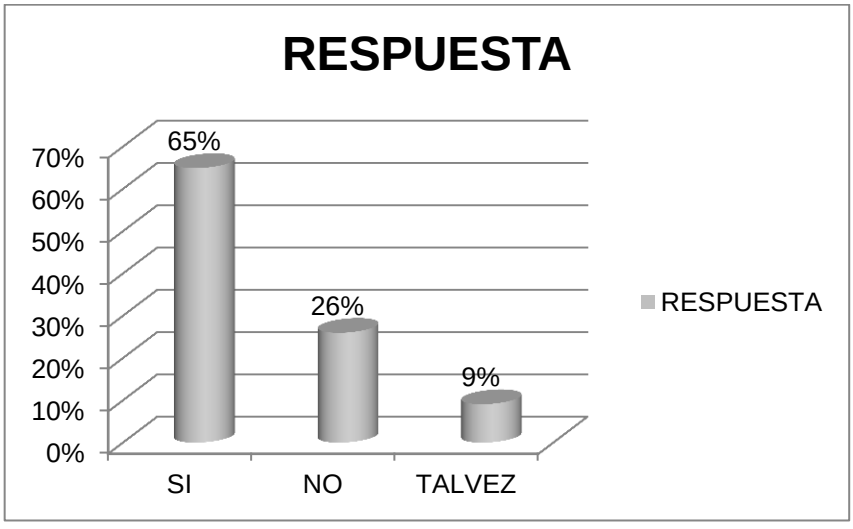


Ilustración 23.- Tabulación de Resultados

Implementación de Monitoreo

Al preguntar a los usuarios sobre la gestión del monitoreo de ancho de banda la gran mayoría cree que se debe implementar este monitoreo. Ellos consideran que todo lo que haga que el internet de la facultad sea más rápido a la hora conectarse a la red bienvenido sea. Por lo que hoy en la actualidad la facultad brinda un servicio de Internet con bajos rendimientos. Esto implica un Internet Lento que proporciona horas y horas de espera para realizar una investigación.

2) ¿Cree que se debería mejorar la velocidad del internet?

OPCIONES	RESPUESTA %	RESPUESTA
SI	81%	62
NO	6%	5
NO CONTESTA	13%	10
TOTAL	100%	77

Tabla 8.-Tabulación de Resultados

Velocidad del Internet

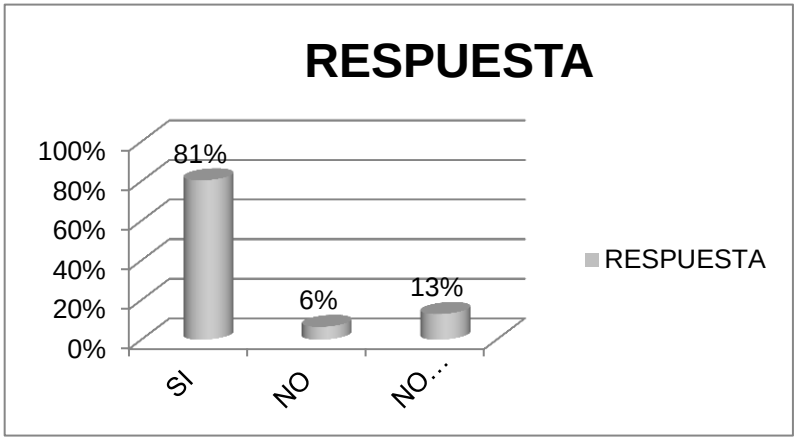


Ilustración 24.- Tabulación de Resultados

Velocidad del Internet

Al consultar a los usuarios un alto porcentaje cree en que se debe mejorar la velocidad del Internet dentro de la facultad esto ayudaría a que no exista retrasos a la hora de bajar informaciones, videos, etc.

3) ¿Está de acuerdo en contar con un internet más rápido y seguro?

OPCIONES	RESPUESTA %	RESPUESTA
DEACUERDO	91%	70
DESACUERDO	6%	5
NO RESPONDE	3%	2
TOTAL	100%	77

Tabla 9.- Tabulación de Resultados

Internet Rápido y Seguro

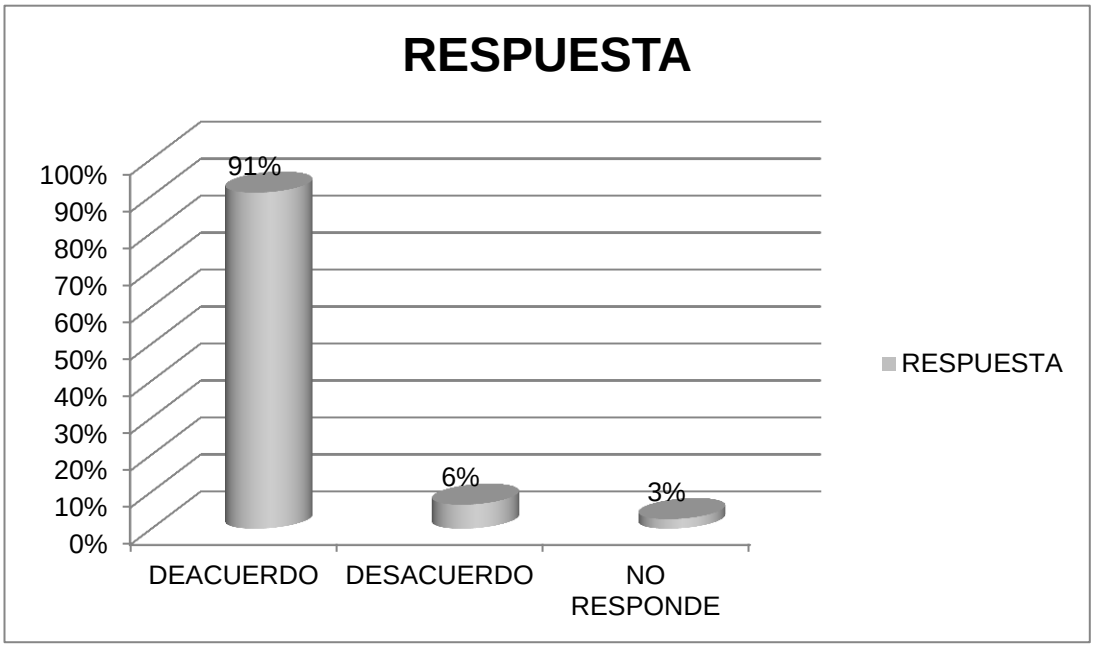


Ilustración 25.- Tabulación de Resultados

Internet Rápido y Seguro

Un alto porcentaje de los encuestados están de acuerdo en contar con un internet más rápido y seguro; ya que esto agilitaría los procesos dentro de las investigaciones y otros trabajos que se realicen desde el internet, además al contar con una seguridad en el mismo no correrán riesgos de pérdida de información sensible.

4) ¿Cree usted que es conveniente que exista un administrador de red para su facultad?

OPCIONES	RESPUESTA %	RESPUESTA
SI	55%	42
NO	40%	31
TALVEZ	5%	4
TOTAL	100%	77

Tabla 10.- Tabulación de Resultados

Administrador de Red

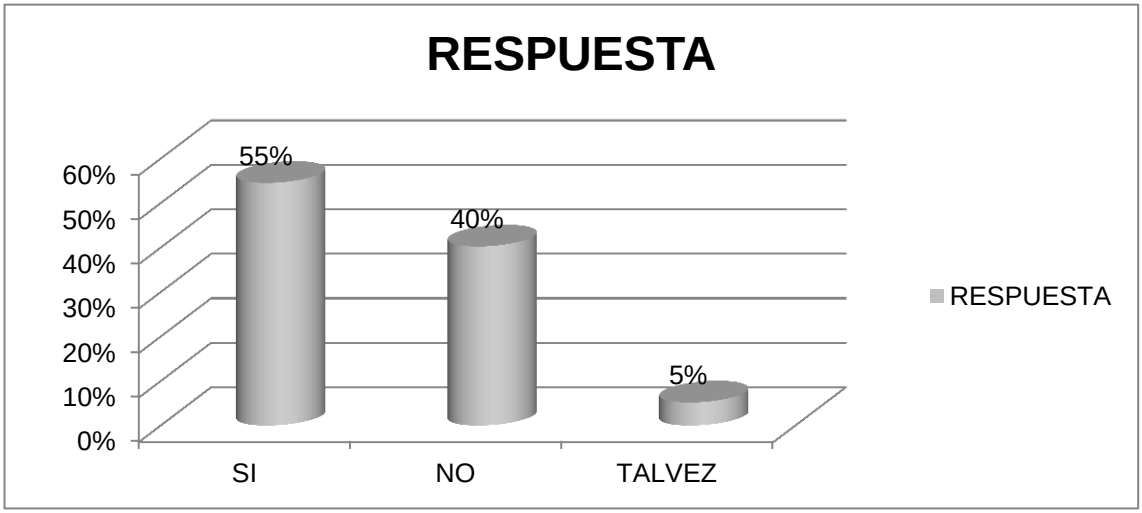


Ilustración 26.- Tabulación de Resultados

Administrador de Red

Aunque muchos de los usuarios piensan que si se debería monitorear la red a través de un administrador, un porcentaje importante no piensa igual debido a que existe el temor de que alguien este constantemente vigilando el tráfico de información en la red.

5) ¿Le gustaría que cuando se conecte a la red de la facultad el administrador de la red le asigne la velocidad de Internet de una manera diferenciada?

OPCIONES	RESPUESTA %	RESPUESTA
SI	51%	39
NO	43%	33
TALVEZ	6%	5
TOTAL	100%	77

Tabla 11.- Tabulación de Resultados

Velocidad de Internet de una manera diferenciada

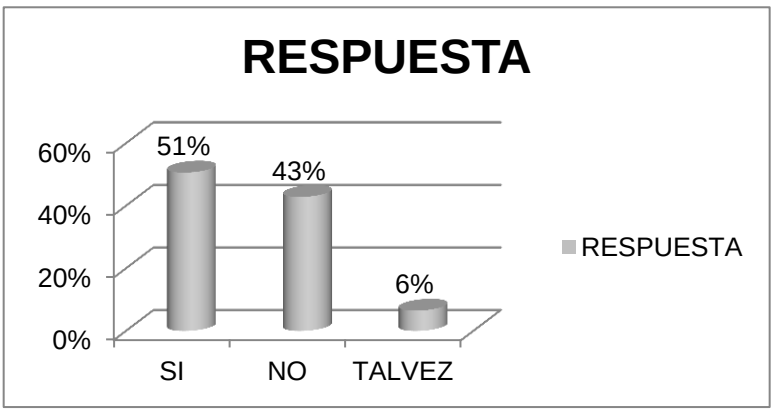


Ilustración 27.- Tabulación de Resultados

Velocidad de Internet de una manera diferenciada.

Al ser consultados los usuarios hay quienes piensan que se debe administrar la velocidad de Internet de manera individual en la facultad aunque otro número significativo de encuestados opina que no es necesario.

6) ¿Le gustaría que cuando a la hora de realizar Descargas de Programas o Investigación no haya retardos ni interrupción en la entrega de la información?

OPCIONES	RESPUESTA %	RESPUESTA
SI	96%	74
NO	1%	1
QUIZAS	3%	2
TOTAL	100%	77

Tabla 12.- Tabulación de Resultados

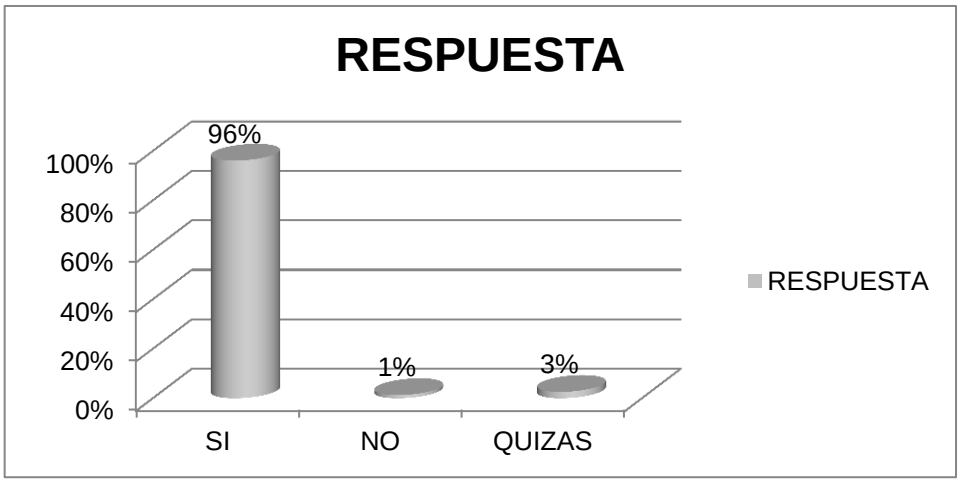


Ilustración 28.- Tabulación de Resultados

Descargas de Programas o Investigación

En un alto porcentaje los encuestados les gustaría contar con descargas más agiles y sin retardos de las mismas.

7) En un rango del 1 al 10 ¿Cómo considera actualmente la conexión a internet que existe en la facultad?

OPCIONES	RESPUESTA %	RESPUESTA
1	6%	5
2	4%	3
3	3%	2
4	16%	12
5	26%	20
6	9%	7
7	13%	10
8	9%	7
9	6%	5
10	8%	6
TOTAL	100%	77

Tabla 13.- Tabulación de Resultados

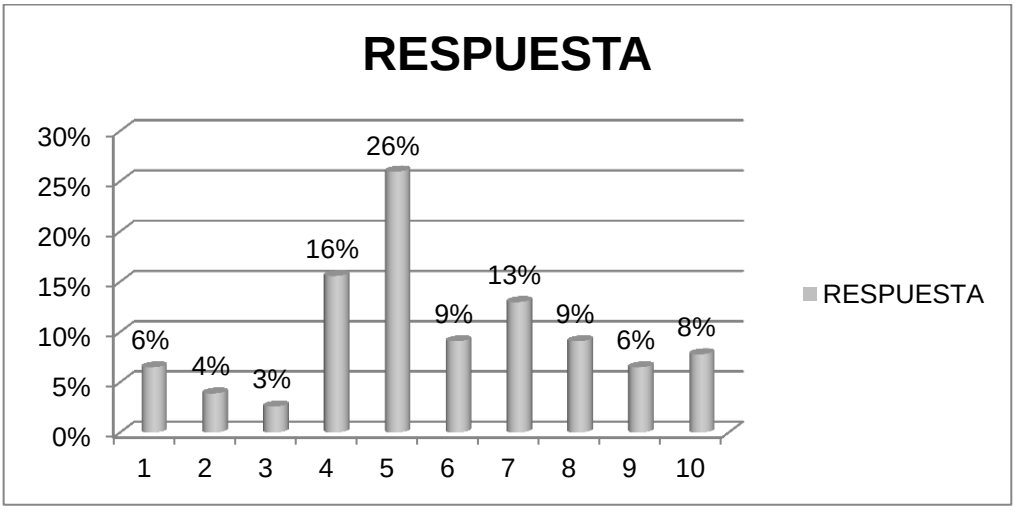


Ilustración 29.- Tabulación de Resultados

Conexión de internet

El mayor porcentaje de los encuestados consideran que la conexión de internet en la facultad es regular; es decir que aunque no es mala la conexión tampoco da las satisfacciones deseadas a los usuarios para trabajar en servicios que necesitan alta calidad del mismo.

8) ¿Piensa Ud. que todas las universidades debería por lo menos contar con un Internet Rápido y Seguro?

OPCIONES	RESPUESTA %	RESPUESTA
SI	79%	61
NO	4%	3
NO CONTESTA	17%	13
TOTAL	100%	77

Tabla 14.- Tabulación de Resultados

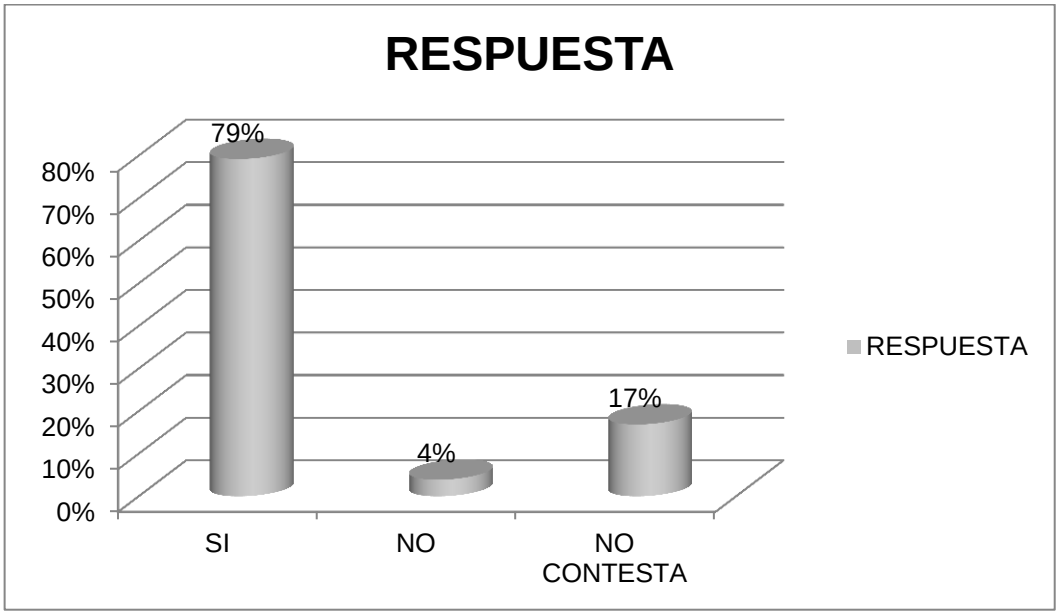


Ilustración 30.- Tabulación de Resultados

Internet rápido y seguro

Los mayoría de los encuestados piensan que si es necesario que las universidades cuenten con un internet rápido y seguro.

9) ¿Considera usted factible realizar clases mediante video conferencias en la facultad?

OPCIONES	RESPUESTA %	RESPUESTA
SI	13%	10
NO	29%	22
NO OPINA	52%	40
TOTAL	94%	72

Tabla 15.- Tabulación de Resultados

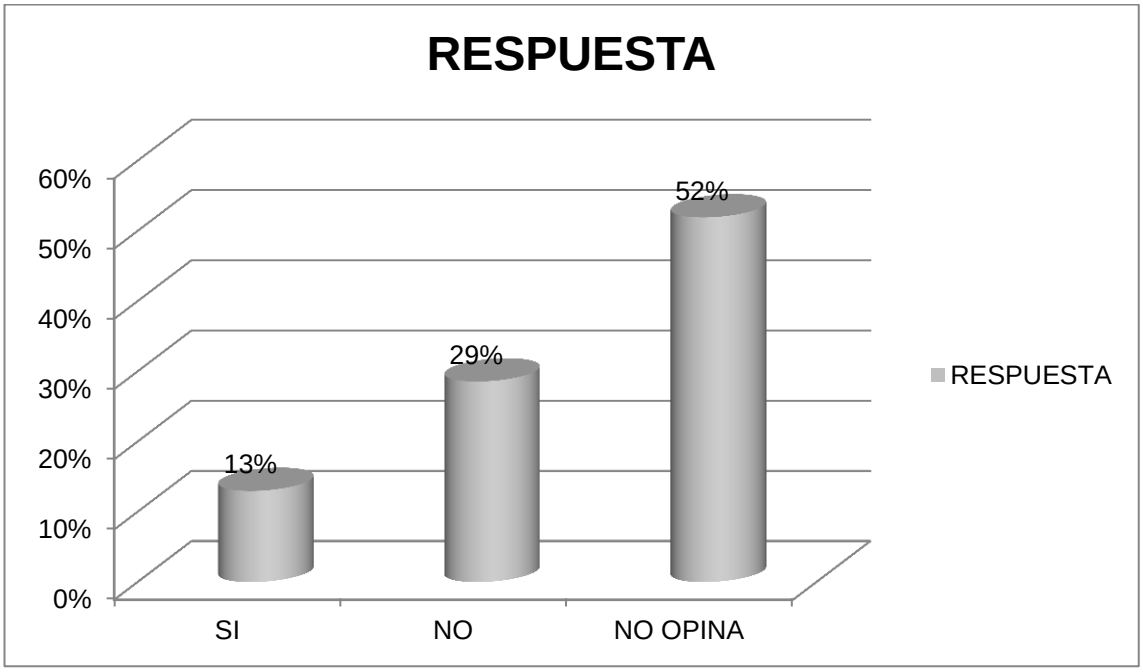


Ilustración 31.- Tabulación de Resultados

Clases mediante video conferencias

Al tabular estos datos podemos notar que existe un gran desconocimiento en cuanto a la realización de clases mediante video conferencia y esto puede ser debido a que los profesores no saben realmente cual es el ancho de banda que poseen para realizar esta actividad.

10) ¿Cómo considera la velocidad de descarga actualmente en la facultad?

OPCIONES	RESPUESTA %	RESPUESTA
BUENO	29%	22
MALO	23%	18

REGULAR	45%	35
TOTAL	100%	75

Tabla 16.- Tabulación de Resultados

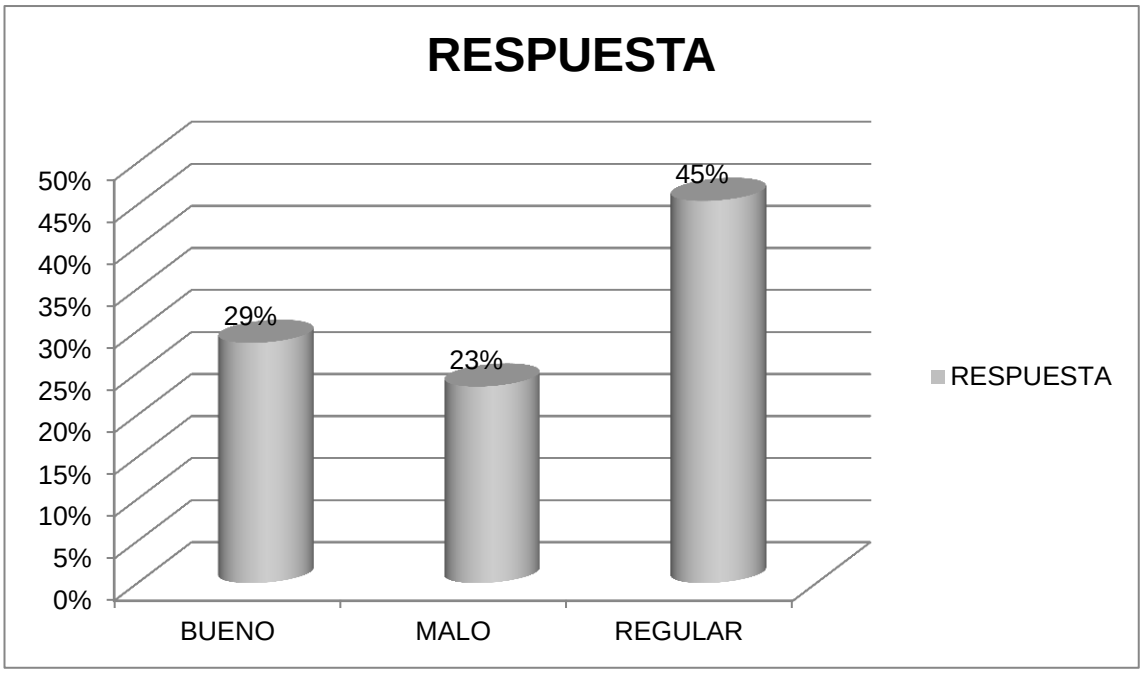


Ilustración 32.- Tabulación de Resultados

Velocidad de Descargas

Muchos de los encuestados consideran que actualmente la velocidad de descargas en la facultad es regular y esto puede ser porque no existe una distribucion personalizada del ancho de banda del internet.

3.7. CONCLUSIONES

En base al análisis e interpretación estadística de los resultados obtenidos mediante la encuesta hemos determinando nuestras propias conclusiones.

Los usuarios conectados a la red de la facultad consideran que toda implementación que mejore con el servicio de internet que ofrece la facultad es buena. Los encuestados piensan que hoy en día la facultad cuenta con un internet con bajos rendimientos a la hora de realización de investigaciones, descargas de programas, acceso a manuales y videos tutoriales. Congestionamiento del tráfico cuando muchos de usuarios están conectados a la red.

La seguridad en la red de la facultad es una necesidad, dadas las características de la información que por ellas se transmite, esto es desde las dependencias administrativas de la misma. Sin embargo, la red de internet actualmente instalada no tiene configurada seguridad alguna, con lo cual se está poniendo en peligro la confidencialidad e integridad de dicha información.

Muchos estudiantes como profesores no realizan clases virtuales a través de video conferencia en algunos casos por desconocimiento del mismo, o en otros casos porque no saben con cuanto ancho de banda de internet van a contar en el tiempo que dure la videoconferencia.

Se cree conveniente tener un administrador de la red para que así pueda distribuir correctamente el ancho de banda a los usuarios de una manera personalizada para que priorice los trabajos individuales de cada uno en cuanto a aquellas tareas que demanden una mayor velocidad.

3.8. RECOMENDACIONES

Analizando todos estos datos podemos realizar las siguientes recomendaciones:

Que el Sr Decano de la Facultad de Administración, Finanzas e Informática debe de realizar la aplicación de monitoreo de red para mejorar el servicio de internet de los usuarios conectados a la red de la facultad.

Es necesario la aplicación de software libre para la realización del monitoreo de la red esto implicaría algunas ventajas a la hora de trabajar bajo software libre, incluso debido a que todas las instituciones públicas deben de contar con las tecnologías de software libre.

Además se recomienda al Decano de la Facultad Administración, Finanzas e Informática que se debe de contar con un administrador de red para que realice el monitoreo de la misma.

Adquirir los equipos necesarios para la implementación del monitoreo de red con estos equipos evitaremos la congestiones de la red, tiempo de espera de paquetes de datos que en muchas ocasiones se ha dado.

CAPÍTULO IV

DESARROLLO TÉCNICO

4. DESARROLLO TECNICO DE LA INVESTIGACION

4.1. INTRODUCCION

La realización de este trabajo de investigación propone buscar elementos tecnológicos que permitan favorecer y mejorar los servicios para los usuarios que se conectan a la red en la facultad. En muchos casos es necesario garantizar que la transmisión de los datos sea realizada sin interrupción o pérdida de paquetes.

Se pretende gestionar el ancho de banda para que cuando los usuarios estén realizando actividades que demanden gran ancho de banda lo puedan obtener sin desmejorar la calidad del servicio de los demás usuarios.

Con el balanceo de carga de internet se disminuirá la presencia de Jitter, que no es más que la llegada de una secuencia de paquetes con retardos dispares para cada uno de ellos, lo que perjudica gravemente a las comunicaciones ordenadas, como las secuencias de audio, por ejemplo. También podremos reducir la llegada en desorden, causada por el rutado por distintos caminos de los paquetes de una secuencia, que sólo puede ser corregido por determinados protocolos de transmisión. Se busca evitar errores en la transmisión, que provocan la corrupción de los datos o la combinación errónea de paquetes.

El servicio de internet de la FAFI permite conectividad a la red a todos los usuarios de la institución, que por diversos motivos hacen uso frecuente de un equipo como estación de trabajo.

Con la implementación de Calidad de Servicio se podrá mejorar los siguientes requerimientos:

- Asignar ancho de banda en forma diferenciada
- Evitar y/o administrar la congestión en la red
- Manejar prioridades de acuerdo al tipo de tráfico
- Modelar el tráfico de la red

Con la mejora de estos requerimientos se puede tener la satisfacción de los usuarios conectados a la red.

4.2. PROPUESTA

4.2.1. OBJETIVO GENERAL

Implementar la Calidad de Servicio (QoS) y monitorear las redes para gestionar el balanceo de carga del enlace a Internet en la Facultad de Administración, Finanzas e Información.

4.2.2. OBJETIVOS ESPECIFICOS

- Proponer un método de conectividad inalámbrica 802.11.n en la estructura de la red.

- Diseñar la gestión del balanceo de carga a internet en base a las necesidades investigadas a los usuarios que se conectan a la red de la Facultad de Administración Finanzas e Informática.
- Probar la implementación del balanceo de carga a internet y monitoreo de la red y verificar la aceptación positiva por parte de los usuarios que se conectan a la red de la Facultad de Administración Finanzas e Informática.

4.3. METODOLOGIA DE DESARROLLO UTILIZADA

La metodología que se aplicará para el siguiente trabajo de investigación será la Metodología Top-Down porque este tipo de metodología consiste en la reutilización de equipos informáticos existentes.

Top-Down Network Design es una metodología que propone cuatro Fases, para el diseño, implementación de redes y reutilización de equipos existentes.

I. Fase1: Análisis: Objetivos yLimitaciones

II. Fase2: Diseño Lógico

III. Fase3: Diseño Físico

IV. Fase4: Pruebas, Optimización y Documentación de la red

4.4. ANALISIS PREVIO

4.4.1. Listado de Requerimiento de la red y Funcionalidad

Requerimientos

- Confiable: Estar disponible cuando se le requiera, poseer velocidad de respuesta adecuada.

- Confidencial: Proteger los datos sobre los usuarios de ladrones de información.

- Integridad: En su manejo de información, asegurando que un paquete no se ha modificado mientras viajaba por la red.

- Autentificación: Determinando que el mensaje proviene de una fuente válida
- Encriptación: Para asegurar que una fuente no autorizada no pueda leer el contenido de los paquetes.

Funcionalidad

- Verificaciones de PCs conectadas a la red
- Monitorear la red :Informar problemas ocurridos en el tráfico de la red
- Balancear la carga del internet de una manera priorizada

Requerimientos de la red, número de puntos, servidores y servicios

Con las Pcs existentes dentro de las instalaciones de la Facultad de Administración, Finanzas e Informática las reutilizaremos porque aún

poseen el hardware propicio para realizar nuestro trabajo de investigación y así poder Implementar Calidad de Servicio y Monitorear el Balanceo de Carga del Internet.

Número puntos de red

Después de haber realizado el estudio de cómo está distribuido los puntos de red dentro de nuestra facultad nos hemos dado cuenta que nuestra facultad cuenta con 157 puntos de red aproximadamente y que no posee un servidor.

Los 105 puntos de red se encuentran distribuidos de la siguiente manera:

Laboratorios de Sistemas:

El área de Los laboratorios de Sistemas están distribuidos por bloques en el bloque 1 se encuentran 2 laboratorios cada uno cuenta con 17 PCs.

Dentro del bloque 2 se encuentran 2 laboratorios que cada una posee 30PCs.

Área de C.P.A

Cuenta con 15 PCs.

Área de Electrónica

Posee 14 PCs

Departamento de Dirección de Escuela

2 PCs

Decanato

1 PC

SubDecanato

2 PCs

Secretaria

5PCs

Departamento de Coordinación

1 PC

Departamento de Vinculación con la Comunidad

1 PC

Administración

1 PC

Biblioteca Virtual F.A.F.I

9 PCs

Pero a la hora de realizar la demostración de la Implementación de la Calidad de Servicio (QoS) y monitoreo de redes para gestionar el

balanceo de carga del enlace a Internet dentro de la facultad .Solo se contara para ese momento con 3 puntos de red donde las 2 primeras funcionaran cono estaciones de trabajo y la otra la convertiremos en un servidor.

Servidores

Realizando el presente estudio dentro de la facultad pudimos notar que no cuenta con un servidor que distribuya el internet, por esta razón nosotros implementaremos una PC que utilizaremos como servidor y así poder realizar el balanceo de carga.

Servicios

- Reparto de internet con balanceo de carga.
- Monitorizar el balanceo de carga.
- Bloquear páginas de redes sociales.
- Seguridad a la hora de realizar descargas de archivos.
- Protección contra la repetición del mensaje, retraso y redirección.

4.5. DISEÑO

4.5.1. DISEÑO DE LA RED

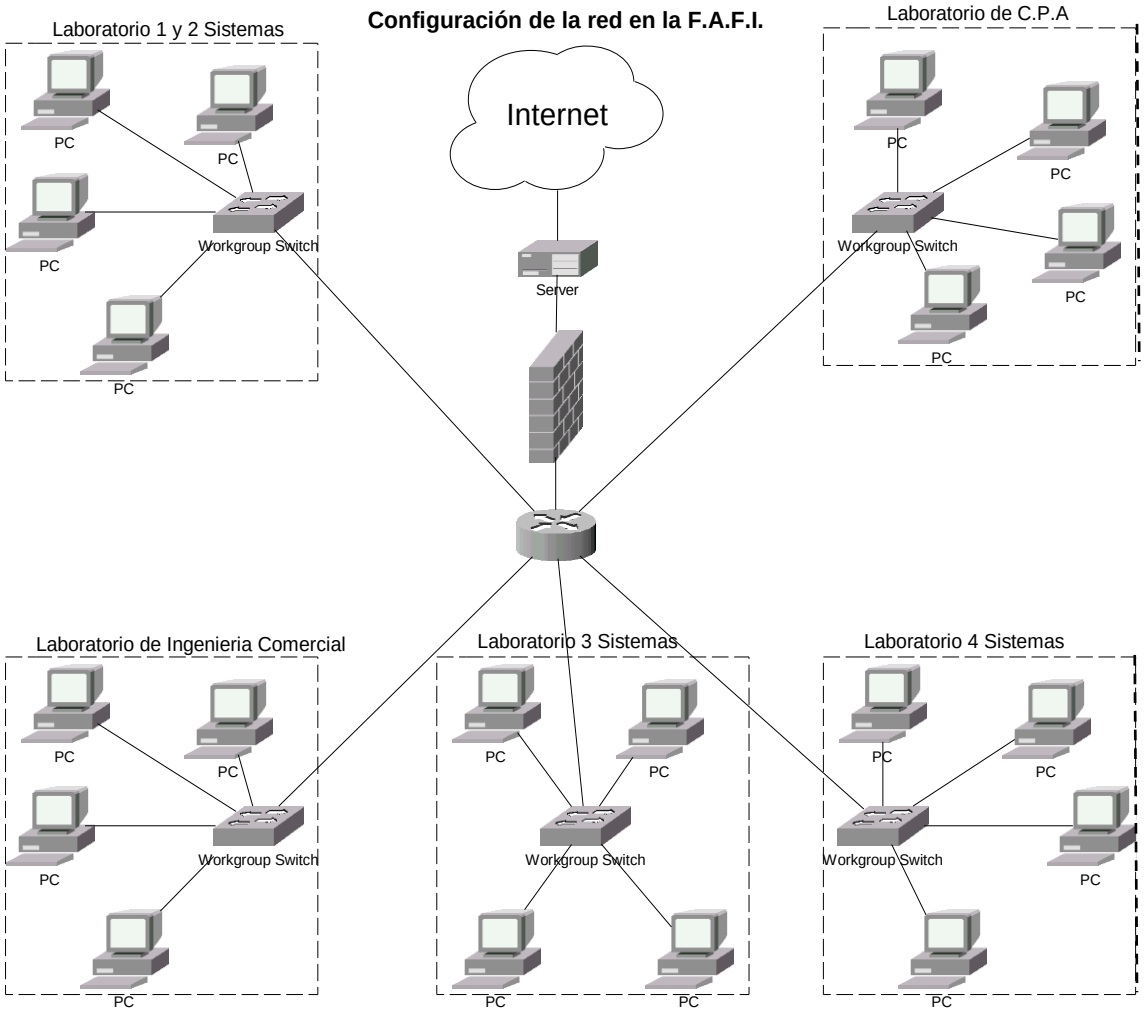


Ilustración 33.- Diseño de la red de la FAFI

4.6. DIAGRAMAS DE CASOS DE USO

Balanceo de Carga

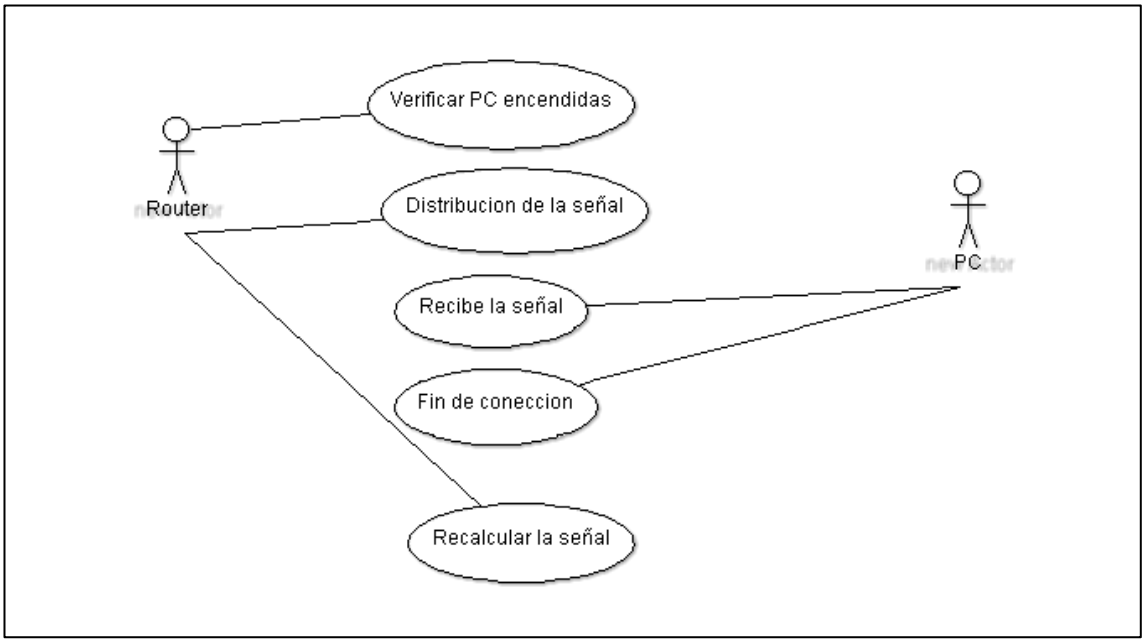


Ilustración 34.- Caso de uso de Balanceo de carga

Monitoreo de red en HTTP

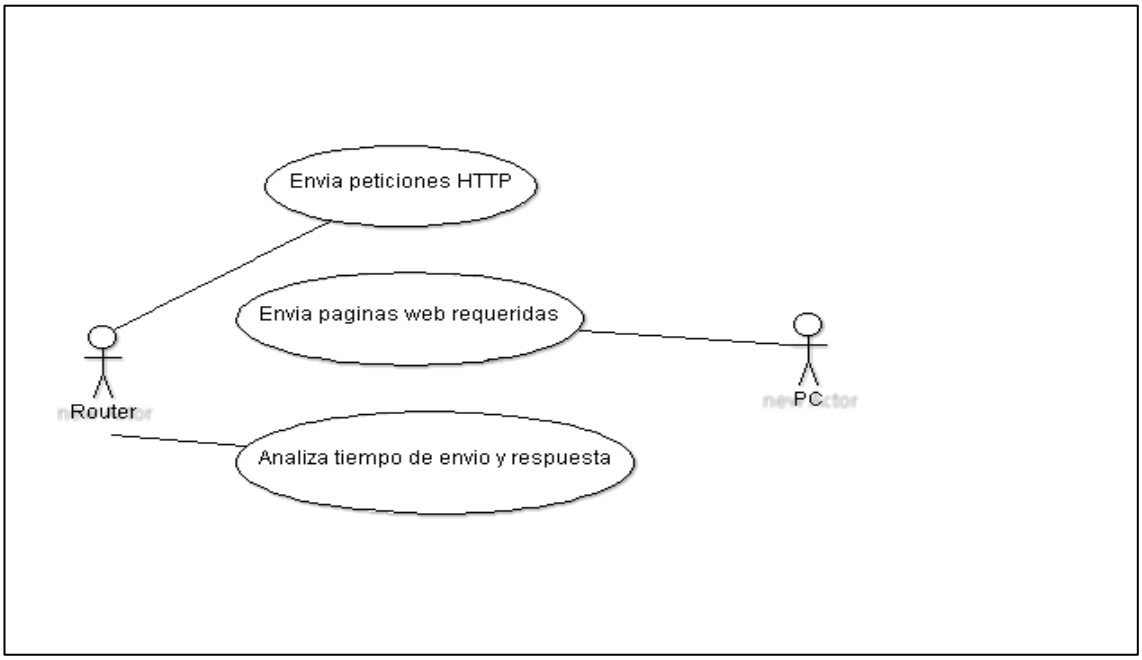


Ilustración 35.- Caso de uso de monitoreo de la red

4.7. DIAGRAMAS DE SECUENCIA

Balanceo de carga

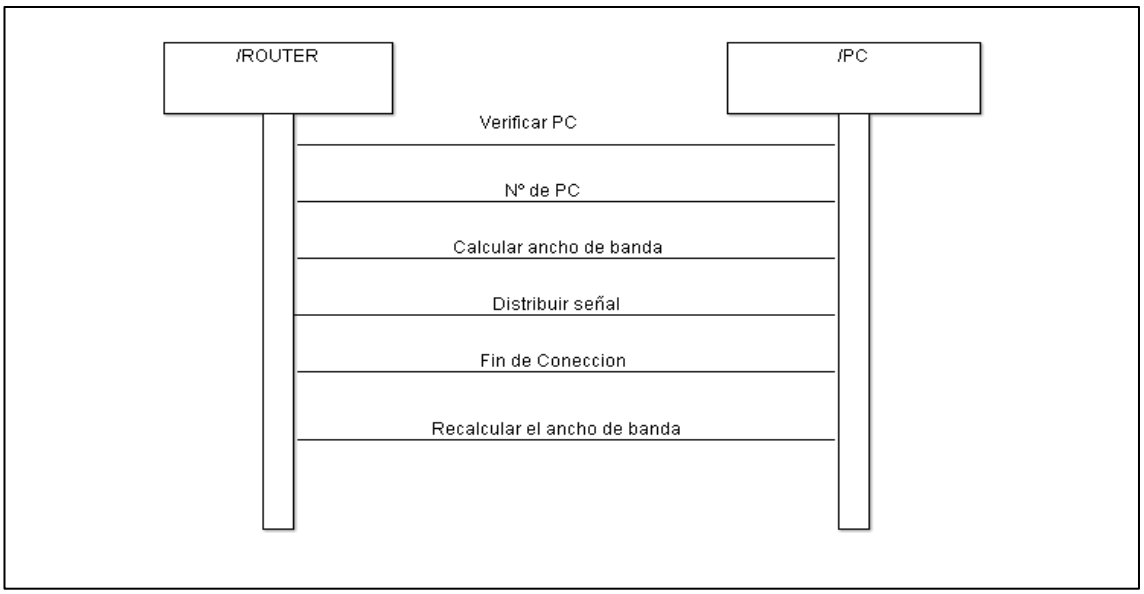


Ilustración 36.- Diagrama de secuencia de Balanceo de carga

Monitoreo de la red

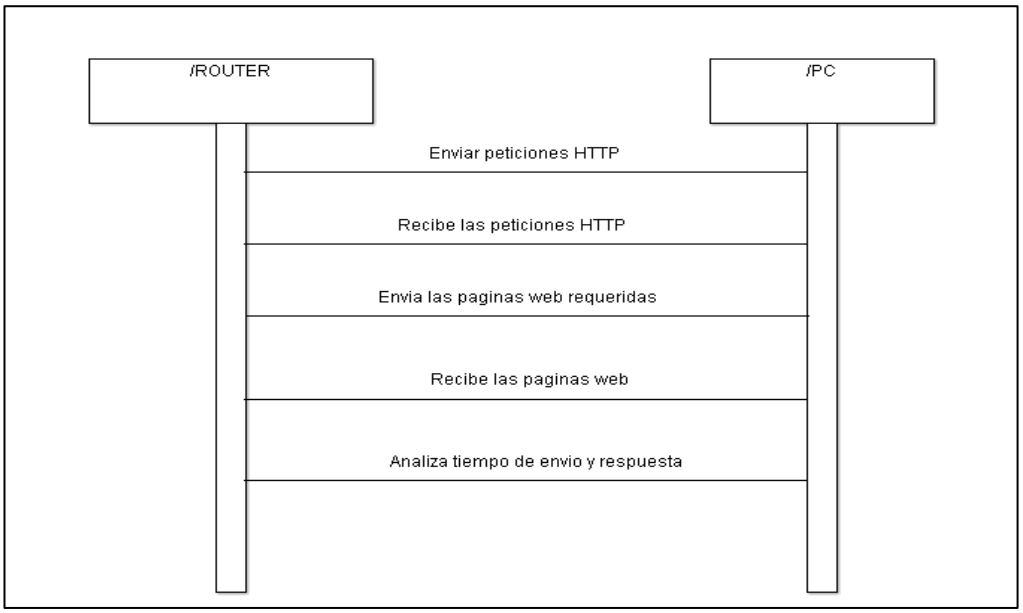


Ilustración 37.-Diagrama de secuencia de Monitoreo de la red

4.8. DIAGRAMAS DE ACTIVIDAD

Balanceo de carga

Actividad del Router

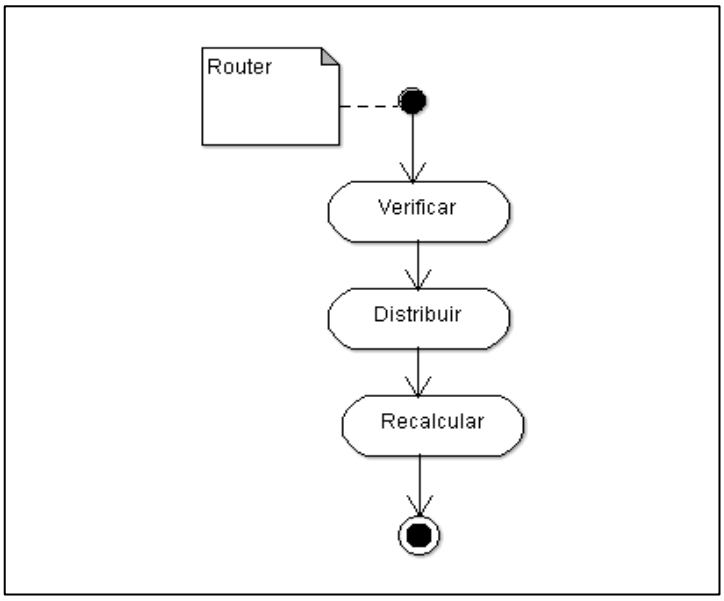


Ilustración 38.- Diagrama de actividad del router en Balanceo de carga

Actividad del PC

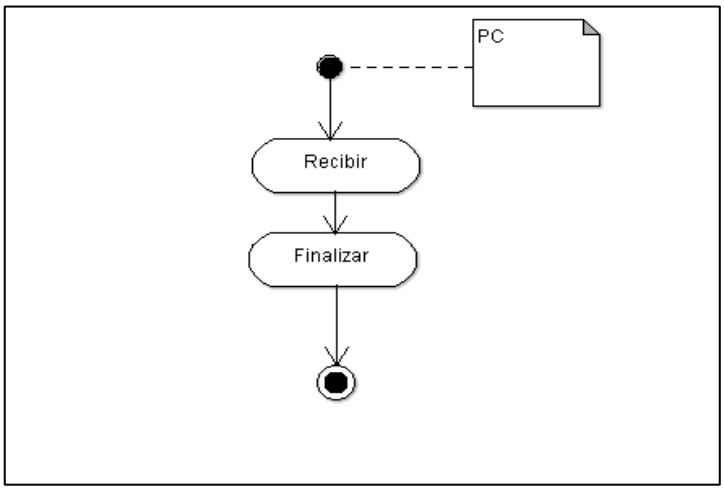


Ilustración 39.- Diagrama de autoridad del PC en Balanceo de carga

Monitoreo de Red

Actividad del router

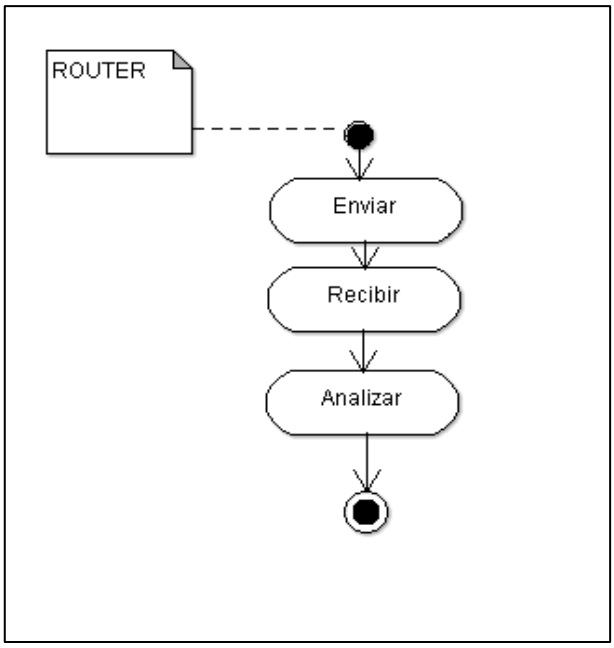


Ilustración 40.- Diagrama de actividad del router en Monitoreo de Red

Actividad del PC

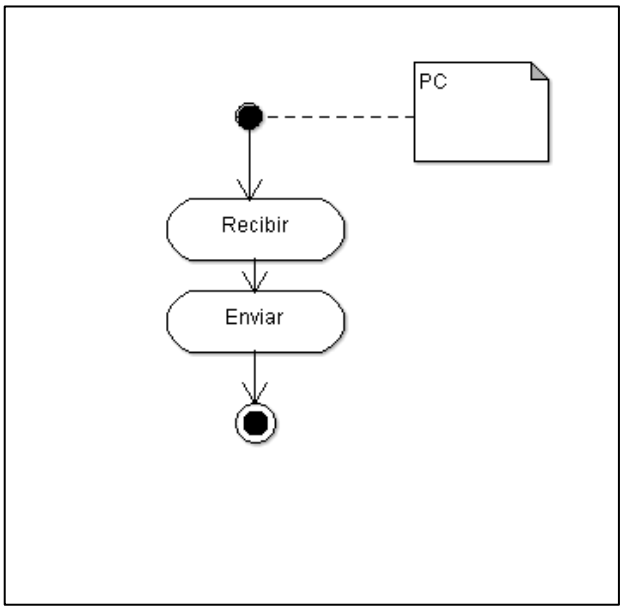


Ilustración 41.- Diagrama de actividad del router en Monitoreo de Red

4.9. DIAGRAMAS DE DESPLIEGUE

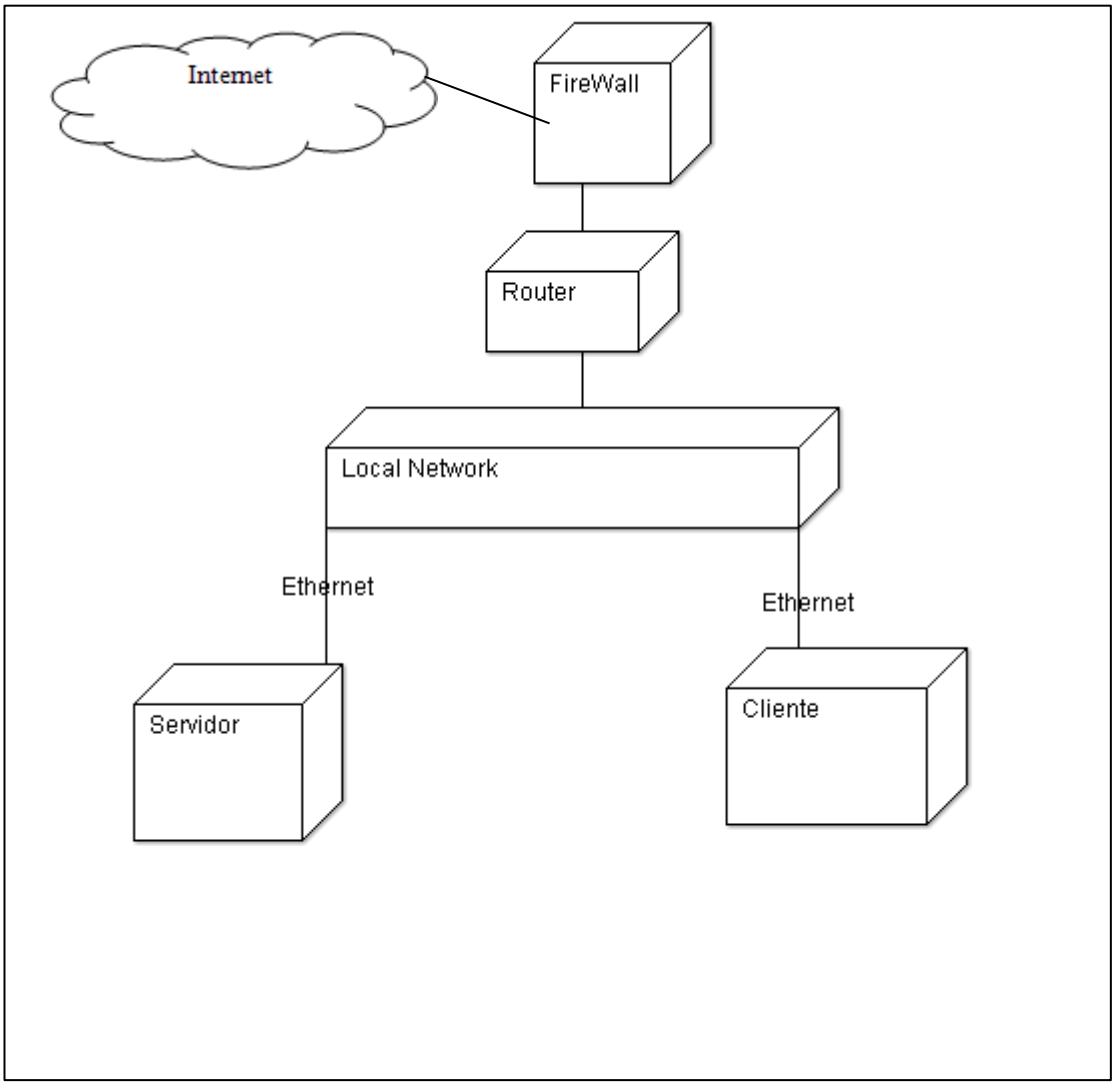


Ilustración 42.- Diagrama de despliegue

4.10. DESARROLLO

4.10.1. PRUEBAS

Pantalla principal de monitoreo y balanceo

Ilustración 43.- Pantalla Principal

Ingreso al CACTI

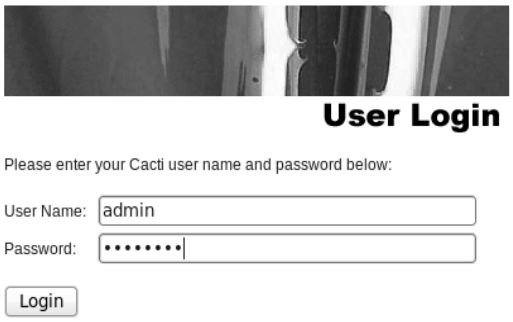


Ilustración 44.- Ingreso al CACTI

PANTALLA PRINCIPAL DE CACTI

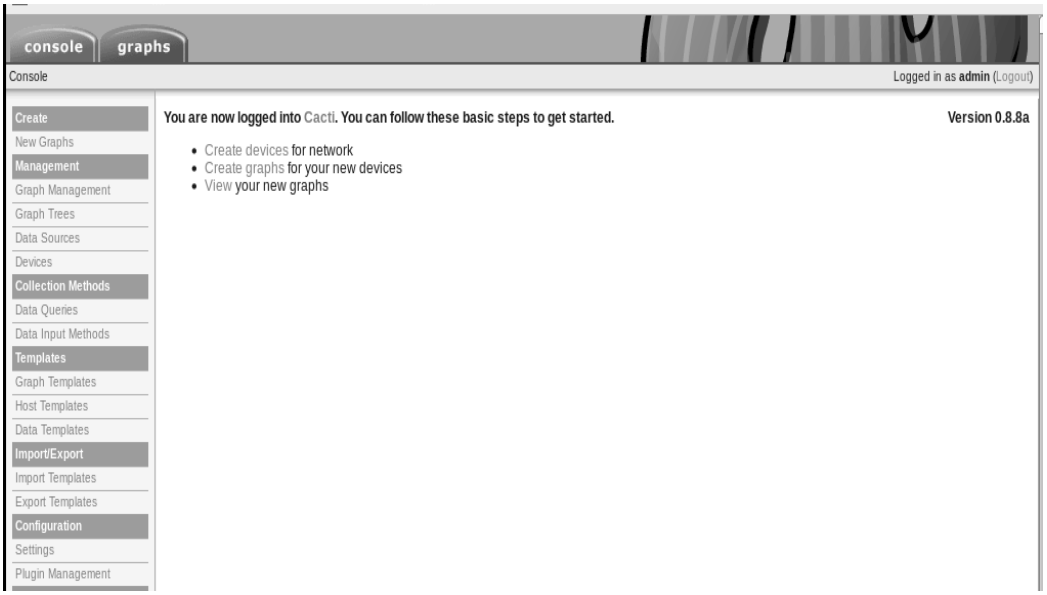


Ilustración 45.- CACTI en modo consola

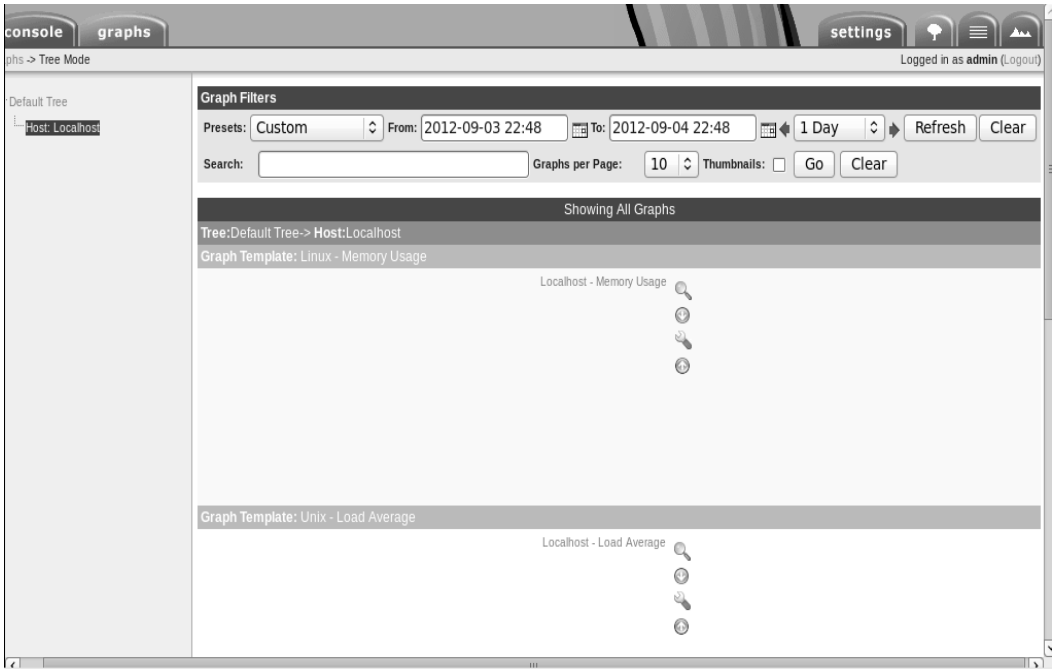


Ilustración 46.- CACTI en modo gráficos

SARG

Squid User's Access Report

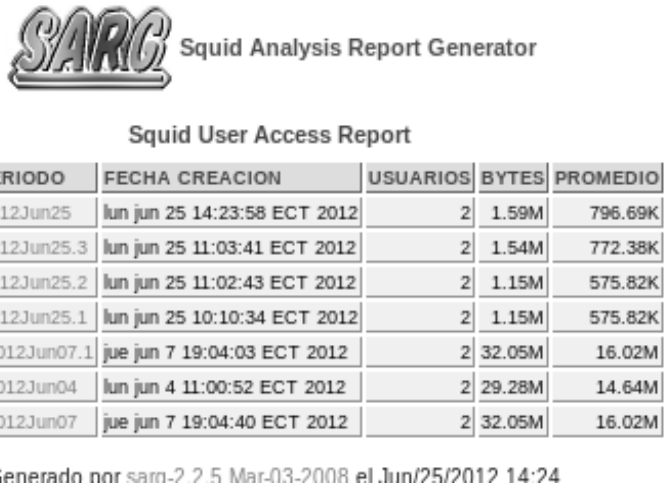
DIRECTORIO	DESCRIPCION
ONE-SHOT	One shot reports
Diario	Reportes Diarios
Semanal	Reportes Semanales
Mensual	Reportes Mensuales

Generado por SARG.

Ilustración 47.- Pantalla Principal del SQUID

Reportes del SARG

One-Shot



Squid Analysis Report Generator

Squid User Access Report

ARCHIVO/PERIODO	FECHA CREACION	USUARIOS	BYTES	PROMEDIO
2012Jun25-2012Jun25	lun jun 25 14:23:58 ECT 2012	2	1.59M	796.69K
2012Jun25-2012Jun25.3	lun jun 25 11:03:41 ECT 2012	2	1.54M	772.38K
2012Jun25-2012Jun25.2	lun jun 25 11:02:43 ECT 2012	2	1.15M	575.82K
2012Jun25-2012Jun25.1	lun jun 25 10:10:34 ECT 2012	2	1.15M	575.82K
2012May30-2012Jun07.1	jue jun 7 19:04:03 ECT 2012	2	32.05M	16.02M
2012May30-2012Jun04	lun jun 4 11:00:52 ECT 2012	2	29.28M	14.64M
2012May30-2012Jun07	jue jun 7 19:04:40 ECT 2012	2	32.05M	16.02M

Generado por sarg-2.2.5 Mar-03-2008 el Jun/25/2012 14:24

Ilustración 48.- Reporte One-ShotSARG

Reporte Diario


Squid Analysis Report Generator

Squid User Access Report

ARCHIVO/PERIODO	FECHA CREACION	USUARIOS	BYTES	PROMEDIO
2012Jun25-2012Jun25	Tue Jun 26 08:42:38 ECT 2012	2	1.75M	879.94K

Generado por sarg-2.2.5 Mar-03-2008 el Jun/26/2012 08:42

Ilustración 49.- Reporte Diario del SARG

Reporte Mensual


Squid Analysis Report Generator

Squid User Access Report

ARCHIVO/PERIODO	FECHA CREACION	USUARIOS	BYTES	PROMEDIO
2012Jun25-2012Jun29	Sat Jun 30 10:18:02 ECT 2012	2	9.32M	4.66M

Generado por sarg-2.2.5 Mar-03-2008 el Jun/30/2012 10:18

Ilustración 50.- Reporte mensual del SARG

WEBMIN

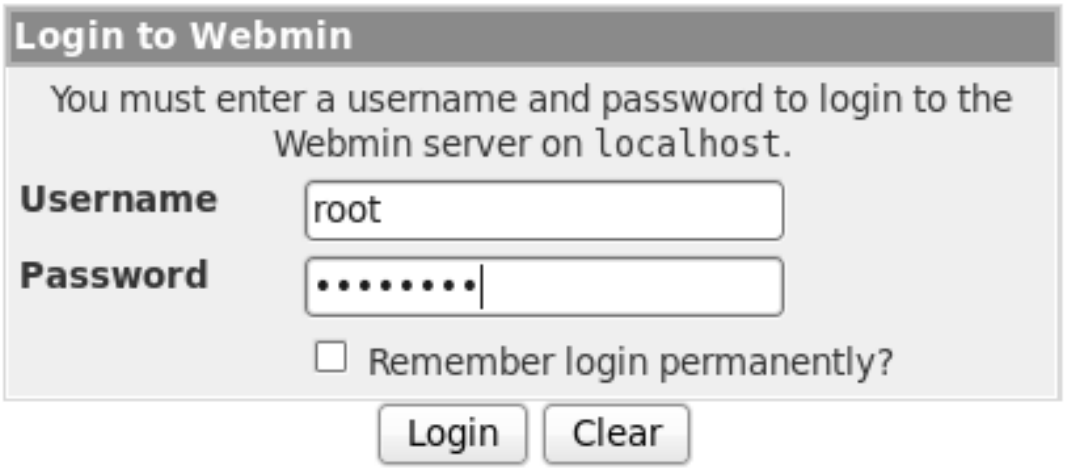


Ilustración 51.- Ingreso al WEBMIN

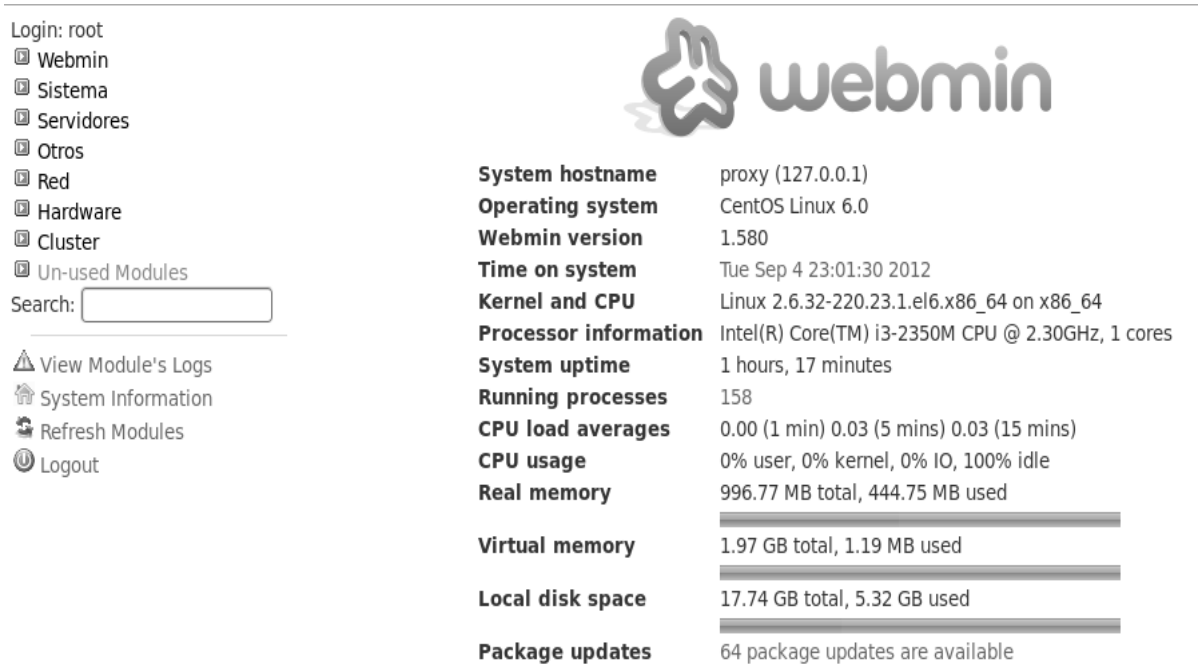


Ilustración 52.- Pantalla principal del WEBMIN

COMANDOS PERSONALIZADOS DENTRO DEL WEBMIN

Bloqueos de páginas, acceso a internet donde configuramos el squid y los QoS personalizados.

Ilustración 53 Comandos personalizados

Aquí se edita el archivo para bloqueos

Ilustración 54 Edición de bloqueos

Aquí se edita el archivo para configuración de Squid

Ilustración 55 Configuración del SQUID

Aquí balanceamos la carga del internet tanto de subida como de bajada

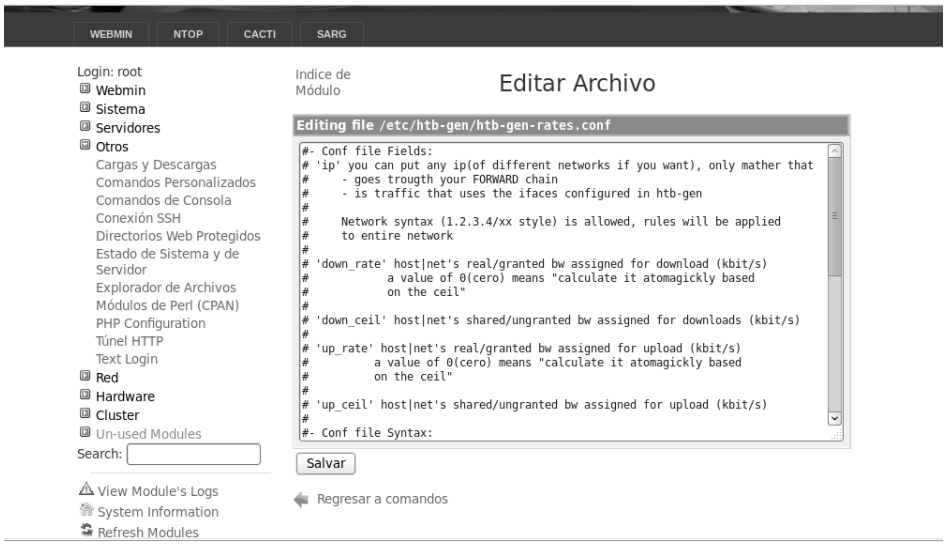


Ilustración 56Configuración de QoS

4.10.2. IMPLEMENTACION DE LA RED

4.10.2.1. REQUERIMIENTOS DE HARDWARE

- Procesador Intel™ o compatible a 2Ghz
- 2Gb de RAM
- Aceleradora gráfica 3D compatible con OpenGL
- 500 Gb de espacio libre en el disco duro
- 2 Tarjetas de Red Intel

4.10.2.2. REQUERIMIENTOS DE SOFTWARE

- Sistema Operativo CENTOS 6.0
- NTOP
- SQUID
- Sarg
- IpTable

4.10.3. SEGURIDADES

Con la implementación de Servicios de calidad (Qos) a la red de la Facultad de Administración finanzas e Informática los usuarios conectados a la red tendrán las siguientes seguridades:

- Rastreo y monitoreo de los paquetes enviados por la red.
- Autenticación del origen de los datos. Permitirá comprobar el origen de los datos exigiendo la identidad del usuario. Corroborará que los datos estén en el lugar donde se originó la petición.
- Confidencialidad de los datos. Permitirá garantizar que los datos no serán accesados por usuarios no autorizados, entidades o procesos desconocidos. Permitirá proteger un mensaje de un determinado retraso e impide la repetición del mismo.

4.11. CONCLUSIONES PARA UNA EFICIENTE IMPLEMENTACIÓN DE LA RED

CONCLUSIONES

Al finalizar el presente trabajo de investigación hemos llegado a la conclusión que es muy importante realizar e implementar Servicios de Calidad dentro del internet en la facultad así como monitorear el balanceo de carga del mismo; también hemos concluido que sería conveniente que la facultad cuente con un departamento de administración de la red para realizar de una manera adecuada el monitoreo de la red.

Es así que utilizando los comandos SNMP la configuración del PC como router resulta sencilla ya que permite ejecutar comandos para especificar el algoritmo a utilizar para el balanceo de carga, así como datos en el servidor y en los nodos de balanceo.

4.12. RECOMENDACIONES PARA UNA EFICIENTE IMPLEMENTACIÓN DE LA RED

RECOMENDACIONES

Recomendamos a las autoridades la creación del departamento antes mencionado para que así podamos crear estándares de calidad del servicio del internet en la facultad de administración finanzas e informática para la evaluación institucional; además recomendamos que se adquieran los equipos necesarios para la implementación del monitoreo de red, con estos equipos evitaremos la congestión de la red ya que se realizará un monitoreo constante en la misma.

También se recomienda que al aplicarse la implementación de QoS en la facultad se debe contar con un administrador de la red para que monitoree la red y en caso de fallas pueda estar presto a corregirlas en el tiempo adecuado.

BIBLIOGRAFIA

AP,No. Calidad de Servicio.

URL:

http://www.anixtersoluciones.com/latam/cl/informacion_general/12188/la_importancia_de_la_calidad_de_servicio_qos___parte_i_es.htm

AP,No. URL: http://umldaniel.blogspot.com/

AP,No. Requerimientos de hardware para un servidor Linux. URL:

http://www.google.com.ec/url?sa=t&rct=j&q=requerimientos%20de%20hardware%20para%20servidor%20linux&source=web&cd=10&sqi=2&ved=0CGgQFjAJ&url=http%3A%2F%2Fwww.debian.org%2Freleases%2Fstable%2Fi386%2Findex.html.es&ei=GmqgTsifFubz0gHc27WOBQ&usg=AFQjCNERYVU7SZswOoEFEpsuz9oLFR7p5Q

AP,No. Requerimientos de hardware para un servidor Linux. URL:

http://www.google.com.ec/url?sa=t&rct=j&q=requerimientos%20de%20hardware%20para%20servidor%20linux&source=web&cd=9&sqi=2&ved=0CGEQFjAI&url=http%3A%2F%2Fr0.unctad.org%2Fdmfas%2Fdocs%2Fhardsoft%2Btrainsp_new.pdf&ei=GmqgTsifFubz0gHc27WOBQ&usg=AFQjCNFXWLjDI0uWkaFzjASQOQiikP7xqA

AP,No. Protocolos. URL:

http://www.cibernetia.com/enciclopedia/protocolo

AP,No. Criptologia. URL:

http://www.iec.csic.es/criptonomicon/articulos/criptologia.html

AP,No. Manual de Seguridad. URL:

http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

AP,No. Evaluación de la metodología de Diseño de Redes Top-Down. URL:

http://www.uniquindio.edu.co/uniquindio/revistadyp/Articulos/6ta%20Edicion/Evaluacion_de_la_metodologia_de_Diseno_de_Redes_Top-Down....pdf

AP,No. URL: http://sedici.unlp.edu.ar/ARG-UNLP-TDG-0000000022/92.pdf

AP,No. Como administrar redes. URL.http://www.aprendaredes.com/downloads/Como_Administrar_Redes.pdf

AP,No. URL:

http://www.dsi.uclm.es/asignaturas/42621/practicas/dmrPrac1.pdf

AP,No. Diagramas de Actividad. URL:

http://es.scribd.com/doc/2568098/UML-Diagramas-de-actividad

AP,No. Manual de Redes. URL:

http://www.monografias.com/trabajos28/manual-redes/manual-redes.shtml

Carling, M., Degler, S., & Dennis, J. (1999). *Guia avanzada de administracion de sistemas linux.* Prentice-Hall .

Sarwar, S. M., Koretsky, R., & Sarwar, S. A. (2003). *El libro de linux.* Pearson Educacion .

Turnbull, J., Lieverdink, P., & Matotek, D. (2009). *Administracion de sistemas linux.* Anaya.