PROPUESTA PARA EL CONTROL DEL CONSUMO DE ANCHO DE BANDA EN LA UNIVERSIDAD DEL MAGDALENA, BASADO EN IDENTIDAD CENTRALIZADA, GARANTIZANDO ALTA DISPONIBILIDAD Y USANDO IMPLEMENTACIONES LIBRES

AQUILES COHEN LLANES

HILDEMAR QUINTANA HERNÁNDEZ

UNIVERSIDAD DEL MAGDALENA

FACULTAD DE INGENIERÍA

PROGRAMA INGENIERÍA DE SISTEMAS

SANTA MARTA, D.T.C.H.

2006

PROPUESTA PARA EL CONTROL DEL CONSUMO DE ANCHO DE BANDA EN LA UNIVERSIDAD DEL MAGDALENA, BASADO EN IDENTIDAD CENTRALIZADA, GARANTIZANDO ALTA DISPONIBILIDAD Y USANDO IMPLEMENTACIONES LIBRES

AQUILES COHEN LLANES
HILDEMAR QUINTANA HERNÁNDEZ

Trabajo de Memoria de Grado presentado para optar al título de Ingeniero de Sistemas

Director
EIRA ROSARIO MADERA
Ingeniero de Sistemas

UNIVERSIDAD DEL MAGDALENA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
SANTA MARTA, D.T.C.H.
2006

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Santa Marta D.T.C.H., ___ de_____ de 200__

DEDICATORIAS

A mi padre Alfonso y a mi madre Emilse, por darme la vida y por su apoyo incondicional

A Sandra por todo el amor e inmenso cariño que siempre me ha brindado.

A mis hermanos Xiomara, Yamith y Mario Alfonso; por estar ahí siempre, por su comprensión.

A mis hijos Camilo y Sergio, frutos del amor y aliciente de mi vida.

A toda mi familia por el inmenso apoyo y cariño.

A todos mis amigos por todo lo aprendido a lo largo de estos años, en especial al Doctor Carlos Eduardo.

A José Hilario López Castillo, in memorian.

HILDEMAR

A Dios por su promesa.

A Mílvida y Mateo David, mi esposa e hijo, mis amores y regalos de Dios.

A mi abuela Otilia, mi padre Jorge y mi hermano Aroldo por todo su amor, sacrificio y apoyo incondicional.

A mis amigos, en especial al Dr. Carlos Eduardo Caicedo por la confianza depositada.

A la memoria de mi madre Emelinda y mi abuelo Cesar.

AQUILES

AGRADECIMIENTOS

Los autores expresan sus sinceros agradecimientos a:

La Universidad del Magdalena por brindarnos la oportunidad de convertirnos en profesionales y personas integras.

A todos los profesores del programa de ingeniería de sistemas y de la Universidad del Magdalena, por todas sus enseñanzas

A las Ingenieras Eira, Emperatriz, Karen; por su confianza y apoyo profesional, humano y apoyo en la elaboración de este proyecto.

A nuestros Amigos Pablo, Rafael, Roberto y William con quienes creamos sueños fuera de las aulas.

Al Centro de Desarrollo del Software, por su apoyo e inmensa colaboración.

A todas aquellas personas que de una manera u otra hicieron posible este sueño.

TABLA DE CONTENIDO

INTRODUCCION 11
1. PRESENTACION DEL PROYECTO 12
1.1 PLANTEAMIENTO DEL PROBLEMA 13
1.2 ANTECEDENTES 17
1.2.1 En otras universidades del Mundo 17
1.2.2 En Universidades Colombianas 26
1.3 IMPORTANCIA Y JUSTIFICACION 29
1.3.1. Seguridad 29
1.3.2. Costos 30
1.3.3. Mejoramiento del Servicio 30
1.3.4. Gestión 32
1.4 OBJETIVOS 33
1.4.1 Objetivo General 33
1.4.5 Objetivos Específicos 33
2. FUNDAMENTACION TEORICA 34
2.1 REDES Y COMUNICACIONES 34
2.1.1 Ancho de Banda 34
2.1.2 Frecuencia de Onda 35
2.1.3 Velocidad de Transmisión 35
2.1.4 Indicadores 36
2.1.5 Tipos de Señal 37
2.1.5.1 Señales Análogas. 37
2.1.5.2 Señales Digitales. 38
2.1.6 Modelo OSI y sus Niveles 38
2.1.6.1 Capa Física. 39
2.1.6.2 Capa de Enlace. 39
2.1.6.3 Capa de Red. 40
2.1.6.4 Capa de Transporte. 40
2.1.6.5 Capa de Sesión. 41
2.1.6.6 Capa de Presentación. 42
2.1.6.7 Capa de Aplicación. 42
2.1.7 Arquitectura de Redes de Computadores 43
2.1.8 Protocolos de Comunicación 45

2.1.8.1 Protocolo TCP/IP. (Transmissión Control Protocol / Internet Protocol) 46
2.1.9 Servicios de Comunicación 47
2.1.10 Internet 48
2.1.10.1 Historia de Internet 48
2.1.11 RADIUS (Remote Access Dialin User Service) 49
2.1.11.1 MODELO AAA 49
2.1.12 Base de Datos 51
2.1.12.1 SQL 51
2.1.12.2 DBMS (Database Management System) 52
2.1.12.3 MySQL 53
2.1.13 VPN 53
2.1.14 SINGLE SIGN ON – SSO 53
2.1.14.1 Password Vault 55
2.1.14.2 Administración centralizada con almacenamiento local de la Identidad 57
2.1.14.3 Administración y almacenamiento de la Identidad centralizados .. 58
2.1.14.4 Arquitectura SSO totalmente distribuida 60
2.1.14.5 Administración y almacenamiento de la Identidad centralizados garantizando alta disponibilidad y redundancia 62
2.1.15 TECNICA CAPTIVE PORTAL. 63
2.1.16 Cuotas de Ancho de Banda 65
2.1.17 Asignación de tasas de transferencias 66
2.1.18 LINUX 67
2.1.19 IPTABLES 67
2.1.20 PPPoE 67
3. DISEÑO METODOLOGICO 70
3.1 Análisis y Definición de Requerimientos 70
4 PROPUESTAS DE SOLUCION. 74
4.1 AUMENTAR EL ANCHO DE BANDA 74
4.2 ADQUIRIR PRODUCTOS COMERCIALES 75
4.3 IMPLEMENTACION DE LA SOLUCION COMERCIAL USANDO LINUX 77
4.4 IMPLEMENTAR USANDO PORTAL CAPTIVO. 82
4.4.1 PROCESO DE IMPLEMENTACION 90
4. RESULTADOS Y PRODUCTOS ESPERADOS 95
5. CRONOGRAMA DE PRUEBAS 97
6. PRESUPUESTO 98
7. CONCLUSIONES 100
8. RECOMENDACIONES 104
9. BILIOGRAFIA 105

LISTA DE TABLAS

Tabla 1. Uso del canal por parte de los protocolos TCP y UDP 16
Tabla 2. Métodos Para el Control del Ancho de Banda..... 21
Tabla 3. Atributos soportados por Chillispot..... 91
Tabla 4. Actividades del cronograma..... 97

LISTA DE FIGURAS

Figura 1. Medición del tráfico de la Universidad del Magdalena 13
Figura 2. Tráfico de la red de la U. del Estado de Dakota del Norte – Antes 18
Figura 3. Tráfico de la red de la U. del Estado de Dakota del Norte – Ahora 19
Figura 4. Estructura adoptada por la Universidad de Berkeley 20
Figura 5. Red de acceso a Internet de la Universidad del Magdalena. 27
Figura 6. Red de distribución LAN Alámbrica/Inalámbrica de la Universidad del Magdalena 28
Figura 7. Arquitectura Password Vault 56
Figura 8. Administración centralizada con almacenamiento local de la Identidad . 57
Figura 9. Administración centralizada con almacenamiento local de la Identidad . 59
Figura 10. Arquitectura SSO totalmente distribuida 60
Figura 11. Admón. y almacenamiento de la Identidad centralizados garantizando alta disponibilidad y redundancia 62
Figura 12. Diagrama de Secuencia de la Técnica de Captive Portal 64
Figura 13. Paquete PPPoE 69
Figura 14. Modelo para propuesta usando productos comerciales. 77
Figura 15. Arquitectura del Sistema 84

INTRODUCCION

Todas las especies de organismos tienen su origen en un proceso de evolución biológica, cuyo mecanismo de cambio evolutivo reside en los genes, las unidades básicas hereditarias. Estos cambios genéticos pueden mejorar la capacidad de los organismos para sobrevivir, reproducirse y, en animales, criar a su descendencia. Este proceso se denomina adaptación[1].

Las redes de computadoras tienen un comportamiento similar al de las especies, se invierte en ellas para que crezcan y evolucionen, acorde a las necesidades de sus usuarios, mejorando su condición y/o capacidad, haciéndolas mas eficientes y confiables. Sin embargo, esta evolución trae consigo el aumento en complejidad y mayores retos en la administración.

Con este trabajo se presenta un propuesta para el control del consumo de ancho de banda, basado en identidad centralizada, garantizando alta disponibilidad y usando implementaciones libres; de tal manera que permita, a la Universidad del Magdalena, configurar políticas de uso y contar con una herramienta para administrar y controlar el acceso al ancho de banda hacia Internet.

[1] Biblioteca de Consulta Microsoft ® Encarta ® 2005. © 1993-2004 Microsoft Corporation.

1. PRESENTACION DEL PROYECTO

Esta propuesta va encaminada a brindar un primer estadio para el mejoramiento del servicio de Internet, suministrando a la red un sistema que permita controlar el acceso a Internet a la comunidad universitaria.

Para solventar esta necesidad, se aplican conceptos claves como el de la autenticación basada en identidades, para no asignar ancho de banda o demás recursos usando las direcciones IP, y restringir de este modo el acceso a Internet, sin importar quien o cuando se usó la máquina y que uso le dió al servicio (revisar correo, cometer delitos informáticos, descargar películas, escuchar música por la red, etc.).

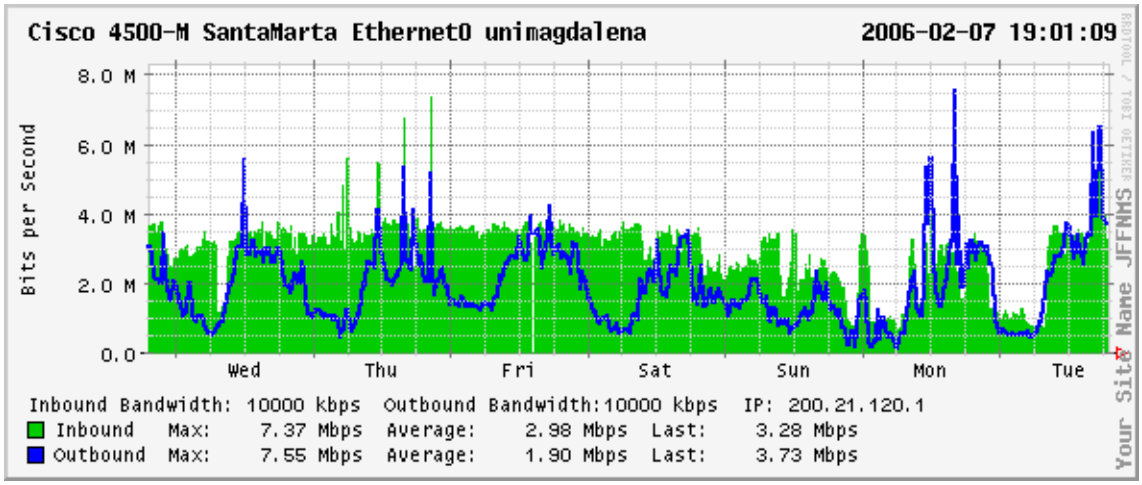
Todo este sistema toma elementos o características de la arquitectura SSO (Single Sign On) en la que solo es necesario registrarse una vez para obtener múltiples servicios como IP, el DNS, Ancho de Banda, Calidad de Servicio, Enrutamiento, Firewall; independientemente del sistema operativo o del lugar físico en el Campus Universitario donde esté ubicada la identidad, agregando una nueva capa de seguridad implícita en el sistema.

1.1 PLANTEAMIENTO DEL PROBLEMA

Los indicadores de crecimiento en número de computadores en la Universidad del Magdalena, así como el número de estudiantes, docentes y personal administrativo que accede al servicio de Internet, muestran un comportamiento ascendente, trayendo consigo una serie de situaciones que han provocado congestionamiento en la red de la Institución y en especial el servicio de Internet. Este detrimento, ha ocasionado que la oferta al 2005, de este servicio, el cual es de 4096Kbps[4] y a partir del 15 de febrero de 2006 es de 6400Kbps sea insuficiente.

En una medición realizada por la empresa Dialnet de Colombia S.A. E.S.P. entre los días Sábado 13 de noviembre y Martes 16 de noviembre de 2004 la Universidad envío solicitudes de 9.5 Mbps entrante y de 7.6 Mbps saliente; lo cual se muestra en la siguiente figura:

Figura 1. Medición del tráfico de la Universidad del Magdalena



La Universidad del Magdalena, no posee políticas claramente definidas sobre el uso de Internet por parte de sus usuarios; el avance más significativo en esta materia se constituyen las salas de recursos informáticos de la institución y el centro de desarrollo de software, en donde se tienen normas sobre el comportamiento de los usuarios dentro de las mismas y hacen mención a que no se deben usar para chatear, ver películas, etc,. No obstante, la Comunidad Universitaria, utiliza desmedida e indiscriminadamente el ancho de banda, sin que hasta el momento se haya podido encontrar una solución eficaz y efectiva.

Ante la necesidad de suministrar el ancho de banda equitativamente, entre quienes solicitan el servicio, se requiere establecer controles que garanticen un nivel de fservicio aceptable. A la fecha, la universidad no cuenta con ningún sistema que permita controlar y registrar el tráfico hacia Internet. Los esfuerzos realizados por los funcionarios del centro de cableado se han centrado en realizar filtrados en capa 3, cerrando puertos y restringiendo direcciones IP´s, restringiendo el ancho de banda por usuario, por redes y a nivel de agregado pero solo a las solicitudes tipo http, y https. Un claro ejemplo del escaso control existente lo proporciona la actividad vírica; pues se ha dado el caso que un puesto de trabajo infectado (en las salas del bloque III, por ejemplo), satura el ancho de banda, dejando al resto de equipos sin posibilidad de navegar.

Además, el mal uso dado por parte de algunos de los usuarios en la universidad, ha provocado que el ancho de banda sea siempre insuficiente para satisfacer sus necesidades, que en muchos casos, podrían verse como vicios, lo cual se ve reflejado en el servicio que reciben otros usuarios que pueden estar utilizándolo para mejores fines.

De otra parte, el ancho de banda en la Institución es literalmente "devorado" por las aplicaciones P2P[2] (vea la Tabla 1), que además de los problemas de congestión que ocasionan, traen consigo implicaciones de carácter legal que pueden perjudicar la universidad, por ser la directa responsable del uso que se le de al servicio de Internet y quien responde legalmente ante su proveedor, entidades de control y terceros del daño o delitos que se cometan desde su red.

Esto obedece a que la mayoría de los contenidos que se intercambian usando esta tecnología están sujetos a derechos de autor, como bien lo afirma Joe St Sauver, Ph.D. "mientras las aplicaciones para compartir archivos pueden ser usadas de tal forma que no infrinjan la ley, la simple observación nos dice que para muchos usuarios P2P un trabajo con copyright es simplemente un texto[3]". Y no es solo la libre observación, la Universidad de Oregon realizó mediciones en su campus sobre el tráfico p2p y confirmo la afirmación; solo unos cuantos contenidos eran libres.

Todo esto refleja la falta de conciencia en los usuarios, sobre la importancia de dar un buen uso al servicio y la poca capacidad de control que es posible tener sobre el acceso a este tipo de aplicaciones, ya que si se identifica un puerto, de forma inmediata los desarrolladores dedicados a ello, se ingenian la manera de ocultar su tráfico, es decir, logran encapsular su información y "disfrazarla", de modo que hacen más difícil la tarea de filtrado.

---

2 Informe de Consultoría realizado por la Empresa Dialnet

3 The Case for Traffic Shaping At Internet2 Schools, p14

Tabla 1. Uso del canal por parte de los protocolos TCP y UDP

Protocolo	Subprotocolos	%Packets	%Bytes
TCP	Citrix ICA	0,002%	0,000%
	DNS	0,023%	0,004%
	Ftp-Command	0,089%	0,019%
	Ftp-Data	0,187%	0,300%
	Gopher	0,093%	0,153%
	HTTP	24,886%	22,204%
	HTTPS	0,356%	0,390%
	p2P	1,001%	41,568%
	Microsoft-DS	9,736%	12,976%
	Netbios Session	11,067%	0,000%
	NFS	0,001%	0,000%
	NNTP	0,003%	0,000%
	POP3	0,001%	0,000%
	Q.931	0,001%	0,000%
	SMTP	0,053%	0,012%
	SSH	0,054%	0,028%
	StartSRV	0,002%	0,000%
	T.120	0,003%	0,004%
	T.120 Terminal Srv	0,001%	0,000%
	telnet	0,002%	0,000%
	Time	0,001%	0,000%
	Xwindow	0,000%	0,000%
	Other	40,321%	15,954%
UDP	BootPC	0,011%	0,013%
	DNS	0,646%	0,201%
	Netbios DataGram	0,076%	3,500%
	Netbios-ns (WINS)	0,235%	0,054%
	Real Time Streaming Protocol	0,014%	0,017%
	Otros.	10,745%	5,982%

1.2 ANTECEDENTES

1.2.1 En otras universidades del Mundo

Los esfuerzos realizados por diferentes universidades del mundo al respecto han sido de gran beneficio para sus comunidades, pero cada enfoque tratado para solucionar el problema ha traído consigo puntos a favor y en contra. De lo que se trata es de buscar un nivel satisfactorio para nuestras necesidades actuales con la posibilidad de poder escalar a nuevas soluciones a futuro sin grandes traumas.

Una de las universidades que ha invertido gran cantidad de recursos en esta tarea es *The University of Pennsylvania*[4] la cual posee 22.000 estudiantes 4000 facultades y 10000 trabajadores, 48.000 direcciones IP registradas 200 subredes. Se interconecta usando SONET y Gigabit Ethernet. Tiene conexión OC-12c a Abilene – (Internet2) y tres conexiones a Internet: una OC-3, dos Gigabit Ethernet. Aunque parecen cifras astronómicas en cuanto a ancho de banda a Internet, racionan su uso para lo cual han hecho grandes inversiones en materia de hardware y software, sin embargo existe una tendencia marcada a asignar los recursos según la IP registrada.

Algo diferente es el caso de *North Dakota State University*[5] en donde el alto uso de salida a Internet en las noches no tenía límites en efecto, para lo cual se aplicaron

[4] http://qos.internet2.edu/wg/calendar/200210-LA/200210-kassabian.pdf, Universidad de Pennsylvania.

[5] http://qos.internet2.edu/wg/calendar/200205-Arlington/200205-ross.pdf, Universidad del Estado de Dakota del Norte

políticas de disminución del ancho de banda para quienes abusaban del servicio, iniciaron un proceso en el que las acciones de un usuario lo afectaran directamente a el, aunque para el usuario las restricciones por exceso aplicadas hicieran que navegara con lentitud, pero impidiendo que la lentitud de la red se extendiera a la comunidad entera. El tráfico de entrada es limitado debido al número de estudiantes en las residencias estudiantiles y el de salida es limitado por el número de usuarios en el Internet.

La figura 2, muestra la gran cantidad de consumo del ancho de banda por parte de aplicaciones P2P en la institución en mención, sobre todo en los horarios nocturnos, luego de la aplicación de las políticas de restricción mencionadas con anterioridad, se puede apreciar en la figura 3 una disminución del uso de aplicaciones como kazaa.

Figura 2. Tráfico de la red de la U. del Estado de Dakota del Norte – Antes

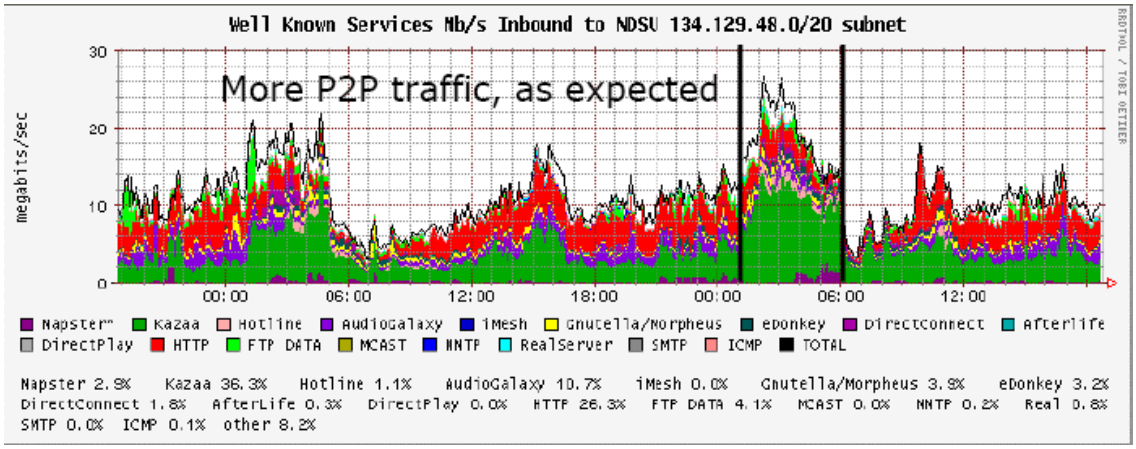
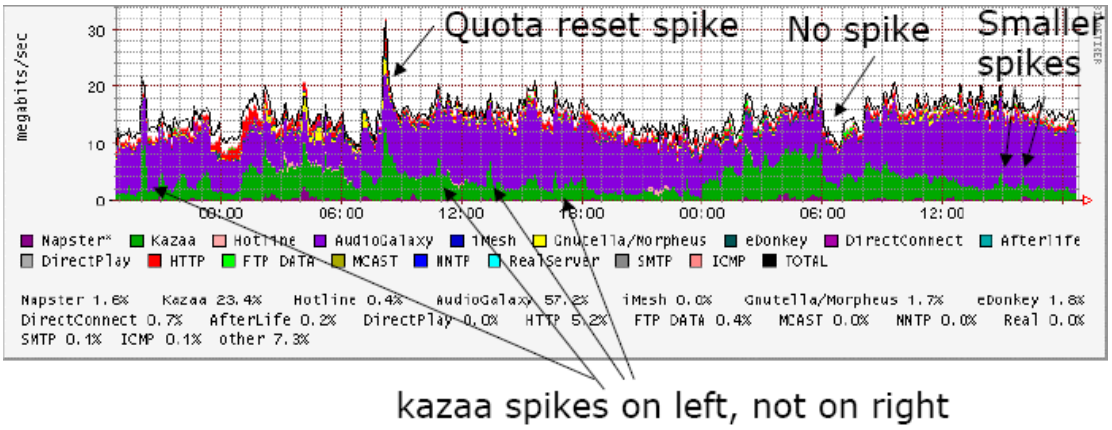


Figura 3. Tráfico de la red de la U. del Estado de Dakota del Norte – Ahora



La *University* of W*aterloo*[6], inició su proceso controlando el tráfico externo, es decir el tráfico que llegaba hacia la red, luego continuó controlando el de su red LAN, garantizando un mínimo de ancho de banda por sectores y ahora pasarán de controlar por flujo de red y direcciones IP a controlar el tráfico por usuario.

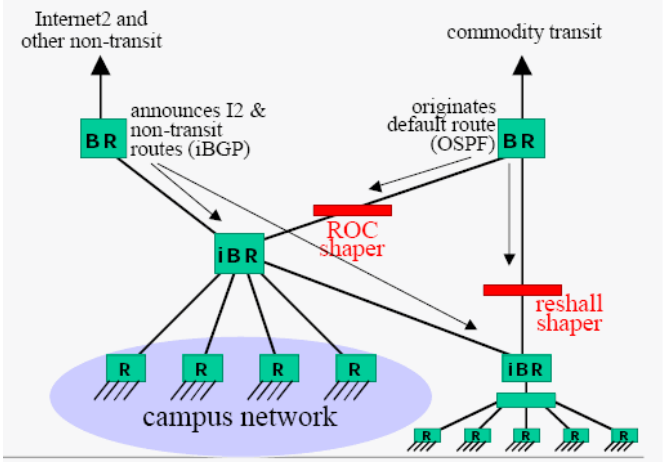
Por su parte la *Berkeley UC*[7], inició su lucha por controlar el tráfico de su red con "*packetshaper*" en acoplamiento rápido de Ethernet entre el backbone de la red de las residencias estudiantiles y el router del Campus, lo que funcionó pero que tuvo ciertos inconvenientes: nunca se encontraba tiempo de mantener actualizadas las clases de excepción, el número de prefijos Abilene anunciados creció en un tiempo, se hizo más grande el número de otros prefijos que no eran controlados por los filtros establecidos. Adicionalmente, el hecho de no tener ningún dato sobre el resto del Campus era preocupante, por lo cual reestructuraron el anterior esquema

[6] http://ist.uwaterloo.ca/cn/Residence/history.html, University of Waterloo

[7] http://qos.internet2.edu/wg/calendar/200201-Tempe/lindahl.pdf, Berkeley UC.

colocando un segundo packetshaper para el resto de la institución. Esta nueva alternativa se puede apreciar en la figura 4.

Figura 4. Estructura adoptada por la Universidad de Berkeley



Los resultados de este esquema fueron la limitación de la rata asignada a las residencias estudiantiles a 40 Mbps y la del resto del Campus a 70 Mbps. En un futuro planean seguir implementando *packetshapers*.

Por último, *The University of Washington*, ha establecido políticas del uso de Internet en las residencias estudiantiles, como lo son el poder instalar servidores solo de uso personal para los ensayos de clase que deban realizar, no usar software que consuman ancho de banda de forma desproporcionada, no utilizar conexiones de red en la institución para proporcionar servicios a clientes externos, no configurar el computador de trabajo con el fin de proveer Internet o acceso a las redes de la universidad a cualquier persona que no sea miembro de la Institución y no copiar o utilizar ningún software, imágenes, música, u otra característica intelectual si no posee el debido copyright para ello. Con el establecimiento de estas políticas, La Universidad transfiere la responsabilidad del servicio a cada usuario del mismo, de

manera que si alguien hace algo indebido y esto tiene repercusiones legales, la institución salva su responsabilidad.

En general, Los métodos o enfoques utilizados para ejercer control sobre el uso de Internet y el ancho de banda demandado por los estudiantes en Campus Universitarios, de los cuales se tiene conocimiento, se relacionan en la Tabla 2, con ejemplos de instituciones en donde han sido aplicados.

Tabla 2. Métodos Para el Control del Ancho de Banda.

Enfoque	Ventajas	Desventajas	Ejemplos
No hacer Nada	• Simple	• Injusto. • Costoso. • Desacuerdos entre el uso y la recuperación del costo, especialmente severos si la universidad carga por bit, pero realiza la recuperación de costo cargando honorarios planos. • La misión de la universidad puede verse impedida por uso inadecuado.	*Muchos*
Por Rangos de IP (Basados en Rata)	• Discutiblemente "justo" • Puede contemplar Cuotas de modo que el tráfico experimente raramente la congestión • No hay necesidad de clasificación en el nivel de aplicación • Portabilidad en el sistema de salida(todas las direcciones IP de Residencias Estudiantiles tienen políticas idénticas)	• Las direcciones IP se convierten en una rara comodidad (considere el impacto en IPv6) • Complejidad adicional del Router. • Puede impedir el despliegue de aplicaciones que merecen alto ancho de banda (especialmente si los límites se aplican al tráfico Internet2). • Inhabilidad de aumentar el umbral límite de vez en cuando	*U. Pennsilvanya.* Una rata límite se aplica al tráfico de salida de Residencias Estudiantiles. Además, los limitadores de rata (uno por IP ADDRESS) están instalados en el Router de borde y aplicados solamente al tráfico de salida.

Enfoque	Ventajas	Desventajas	Ejemplos
Por Rangos de IP (Basados en Volumen)	• Los estudiantes que más generan tráfico pueden ser aislados colocándolos en una caja de penalización • El ciclo de retroalimentación negativa anima a usuarios que modifiquen su propio comportamiento • No necesidad de la clasificación del nivel de aplicación • Capacidad de estallar de vez en cuando	• Las direcciones IP se convierten en una materia artificial rara (considere el impacto en IPv6) • Puede impedir el despliegue de aplicaciones que merecen alto ancho de banda (especialmente si los límites se aplican al tráfico Internet2). • Complejidad adicional del Router. • Complejidad adicional de las cuentas • El estado del uso y de las penalizaciones necesita ser comunicado rápidamente para hacer un promedio de usuarios	*Universidad De Estado De Dakota Del norte* Los Rangos se aplican solamente a los usuarios de Residencias Estudiantiles. El Rango es 300 MB por día por usuario. Colocan a los usuarios que exceden su Rango en un grupo compartido limitada a solo 256kbps. *Universidad de Waterloo* Los usuarios de los recintos de la residencia escolar fueron sujetos a los Rangos por usuario de la forma " *x MB* en los últimos *y* días". En Retribución, al tráfico de los recintos de la residencia se le garantiza un mínimo del ancho de banda externa a través de los CB-WFQ. *Estado De Iowa* Transfieren a los usuarios de la residencia que exceden un nivel específico (actualmente 200 MB), a una "conexión de Internet más lenta". Si el abuso continúa, los usuarios ofendidos son cambiados a clases de tráfico mucho más restringidas. Los rangos del usuario se reajustan al finalizar el día, a excepción de ésos en las clases tarifa-limitadas, para los cuales se aplica un movimiento de 24 horas en promedio para determinar si vuelven a una clase menos restrictiva del tráfico. *Virginia Tech* vea abajo
Por Rangos de Clase (Basados en Tarifa)	• Puede balancearse el uso entre diversas comunidades de usuario • Pueden contemplarse de modo que conformando o exceptuando las clases experimente raramente la congestión • Fácil implementación (si no discriminamos entre la materia y tráfico	• Ninguna imparcialidad dentro de clases • Puede impedir el despliegue de aplicaciones que merecen alto ancho de banda (especialmente si los límites se aplican al tráfico Internet2).	*Berkeley UC* Packeteers delante del Router de salida del Campus maneja por separado el tráfico de tarifa limitada hacia/desde las Residencias Estudiantiles y hacia/Desde el resto del campus (ROC). Se requieren dos Packet Shapers porque el ancho de banda total excede de los 100 Mbps. El enrutamiento se ha ideado para mantener el tráfico de Residencias Estudiantiles y de ROC separado.

Enfoque	Ventajas	Desventajas	Ejemplos
	Internet2) • No necesidad de la clasificación del nivel de aplicación		*Virginia Tech* Es un híbrido complejo que emplea primeramente evacuación basada en clases, pero también basada en el uso y usa el esquema de caja de penalización. El tráfico del muerto del campus procedente de las subredes de las Residencias Estudiantiles es evacuado a 60 Mbps en agregado y el tráfico muerto del campus procedente del servidor de noticias es evacuado a 5 Mbps. Las "aplicaciones fastidiosas" se evacuan a 10 Mbps en agregado (los perfiles se generan manualmente). Finalmente los usuarios individuales son ubicados en una de tres clases: Clase 0 (sin evacuar), clase 1 (evacuado a 1,5 Mbps), y clase 3 (evacuado a 250 Kbps). Cuando los usuarios exceden cierto umbral (actualmente 650 MB) en un período 24hr, se incrementa su clase; si permanecen bajo umbral, su clase decrece. *Universidad de Washington* El ancho de banda total desde la red de las Residencias Estudiantiles hasta el resto del campus se limita a 100 Mbps. el acceso del resto del campus a los puertos comunes del servidor (tela, ftp, IRC, etc) es bloqueado en las residencias estudiantiles. El tráfico peer to peer entrante es limitado por tarifa a 20 Mbps; el tráfico peer to peer de salida se limita a 2 Mbps. *Santa UC Cruz* vea abajo
Por Clase (Compartido proporcionalmente)	• Las clases de tráfico restringidas pueden utilizar capacidad no utilizada.	• No hay imparcialidad dentro de clases • Puede impedir el despliegue de aplicaciones que merecen alto ancho de banda (especialmente si los límites se aplican al tráfico Internet2).	*Universidad de Waterloo* Al tráfico de las Residencias Estudiantiles se le garantiza un mínimo de ancho de banda externo con CB-WFQ. (véase arriba) *Tejas A&M* Planeando soportar cuatro clases de aplicaciones. Por admisión de la sesión a las clases, marcando el borde del servicio Diff, evacuación, y hacer cola apátrida de la base. (Actualmente usan límites en la tarifa por

Enfoque	Ventajas	Desventajas	Ejemplos
			aplicación.)
Por Ip (Compartido Proporcionalmente)	• Discutiblemente "justo" • No existen sorpresas (los usuarios consiguen el servicio que pagan)	• Las direcciones IP se convierten en una materia artificial rara (considere el impacto en IPv6) • Puede impedir el despliegue de aplicaciones que merecen alto ancho de banda (especialmente si los límites se aplican al tráfico Internet2). • Complejidad adicional de el Router • Requiere usar muchas colas • El cuidado se debe tomar para no restringir el funcionamiento de Internet2	*No se conocen ejemplos de su aplicación.*
Basada en el uso (Cargas después del umbral)	• Económicamente racional (los usuarios consiguen la mayor parte del valor de un pago escaso por el recurso) • Justo • Ciclo de Retroalimentación negativo para los usuarios pesados • Puede ser contemplado de modo que la mayoría de los usuarios paguen tarifa mensual plana; similar a los precios del departamento de impresoras para estudiantes, de	• Complejidad adicional en la contabilización y la facturación • Necesita un sistema para recolectar las estadísticas de uso (*e.g.* NetFlow)	*Cornell* Planeando diseñar un horario mensual para cada departamento en donde se incluya un componente de uso de la WAN. Se clasifica la estructura para incluir una mezcla de los honorarios del puerto, del impuesto de la infraestructura, y de los honorarios de uso. Los honorarios de uso por megabit solamente bajarán para el uso sobre cierto umbral (ajustado de modo que el 80% de direcciones del IP eviten honorarios de uso). Las cuentas mensuales de los departamentos incluirán gran detalle para apoyar cargas basadas en usos recurrentes de los usuarios individuales o de los grupos de investigación. Sistema de facturación basado en el flujo de la red usando software de apogeo y scrips hechos en casa. *Universidad de Kansas* Aplicando artificialmente la carga basada en bajo uso a los usuarios de Residencias Estudiantiles. Solamente los usuarios pesados sentirán los honorarios basados en uso; cargarán a los usuarios ordinarios una tarifa plana.

Enfoque	Ventajas	Desventajas	Ejemplos
	teléfonos celulares, etc.		
Por rangos de Aplicación (Basados en Tarifa)	• La Mayoría de problemas causados a menudo por un número pequeño de aplicaciones. • Herramienta para reducir el uso ilegal de la red (*e.g.* la distribución ilegal de materiales con copyright) • "Magic Bullet", caja media. • Mantenimiento automático con "bad apps du jour"	• Debe pasar el juicio donde cuales aplicaciones son "buenas" y cuales son "malas" • Impacto del desempeño (los dispositivos QoS se diseñan para manejar un recurso escaso, de tal forma que no permite que los routers, que están diseñados para manejar el tráfico a la mayor velocidad cumplan su función, aumentando la latencia del trafico "bueno") • Pérdida de la transparencia (e.g. el reescribir del tamaño de la ventana de TCP) • Las configuraciones complejas y dinámicas complican la eliminación de errores de funcionamiento • Perfiles de aplicación creados un juego del gato y del ratón que el ratón gane (*e.g.* HTTP, https, proxies, números randomicos de acceso, ssh, etc.)	*Santa UC Cruz* Asigne NetEnforcer desplegado entre Redes Residenciales y link de acceso a Internet2. El tráfico se clasifica en cuatro niveles de la prioridad: Alto (web, ssh), medio (todo excepto P2P), bajo (P2P), bloqueado (gusanos). *Virginia Tech* vea arriba *Universidad de Washington* vea arriba
Establecimiento de una red Residencial De Outsource			*Universidad de Nuevo México*
Servidores de bloque (con NAT o firewall)	• Puede aplicarse solamente en "malas vecindades" (*e.g.* pasillos de la residencia)	• La transparencia end-to-end que destruye puede restringir el despliegue de usos avanzados numerosos (*e.g.* VoIP, peer to peer, investigación-orientado) • Potencialmente separe los	*¡Sabemos que usted está hacia fuera allí!*

Enfoque	Ventajas	Desventajas	Ejemplos
		impactos del funcionamiento • Los usuarios motivados aprenderán perforar a través	

1.2.2 En Universidades Colombianas

En Colombia no se encuentran referencias de trabajos realizados que permitan controlar los problemas de red en los campus universitarios. A nivel público las instituciones hacen lo que financieramente les es posible, a nivel privado las grandes universidades como los Andes invierten tanto en ancho de banda como en equipos dedicados a tal fin.

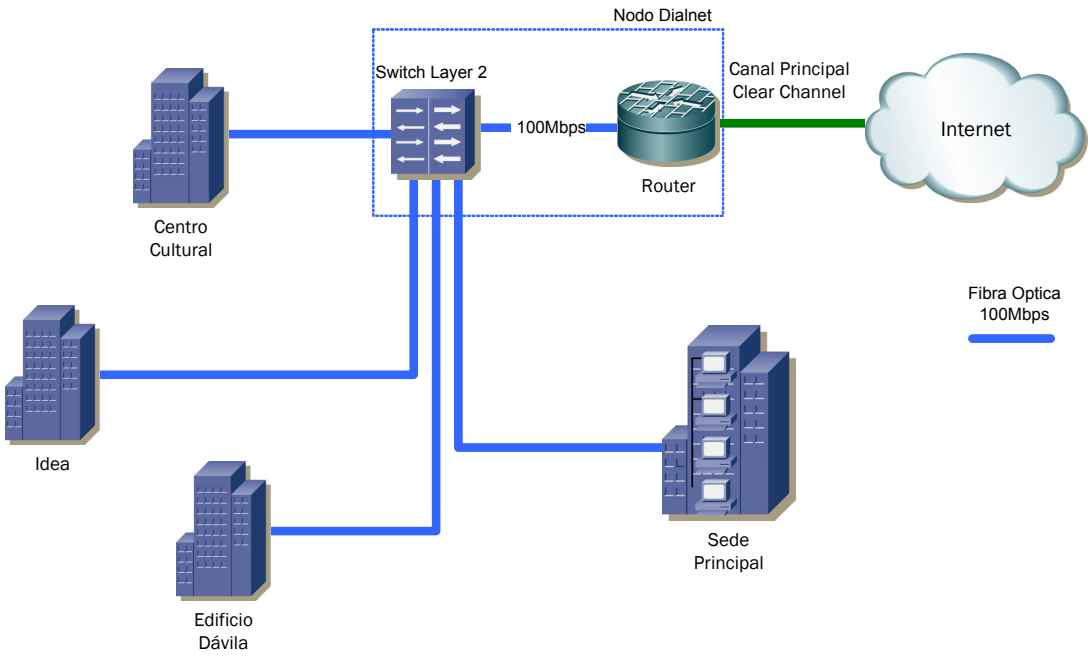
En la Universidad del Magdalena la red de computadoras ha experimentado un crecimiento rápido. Cuando la institución inició su proceso de Refundación, solo existían tres redes básicas: ARCA (Admisiones, Registro y control Académico), Administrativa y Salas de Sistemas. Para el año de 1998, estas redes estaban conformadas por 52 computadoras en total, al cierre del año 2003, la universidad poseía 466 computadoras, incrementándose la cifra para el 2004 a 806 y para el 2005 a 816, habiéndose incluido a todas en la red y proporcionado acceso a Internet a toda la institución con un ancho de banda de 1024 Kbps en el año 2003, aumentado a 2048Kbps en el 2004, 4096Kbps durante el 2005 y que se incrementará a partir de mitad de febrero de 2006 a 6400Kbps, en una topología tipo estrella en fibra óptica a 100Mpbs que interconecta el Campus Universitario y

todas las sedes de la institución incluyendo el Instituto de Educación Abierta y a Distancia (IDEA), el Claustro San Juan Nepomuceno, y el Instituto de Postgrados[8].

Para realizar control sobre los usuarios la Universidad del Magdalena ha implementado un control[9] basado en protocolo HTTP utilizando la aplicación SQUID Proxy Server, el cual realiza dicho control de tráfico a las solicitudes HTTP y FTP, haciendo las respectivas lecturas en la URL de la página solicitada. De esta misma forma permite o niega algunos sitios, basándose en el contenido y en la URL.

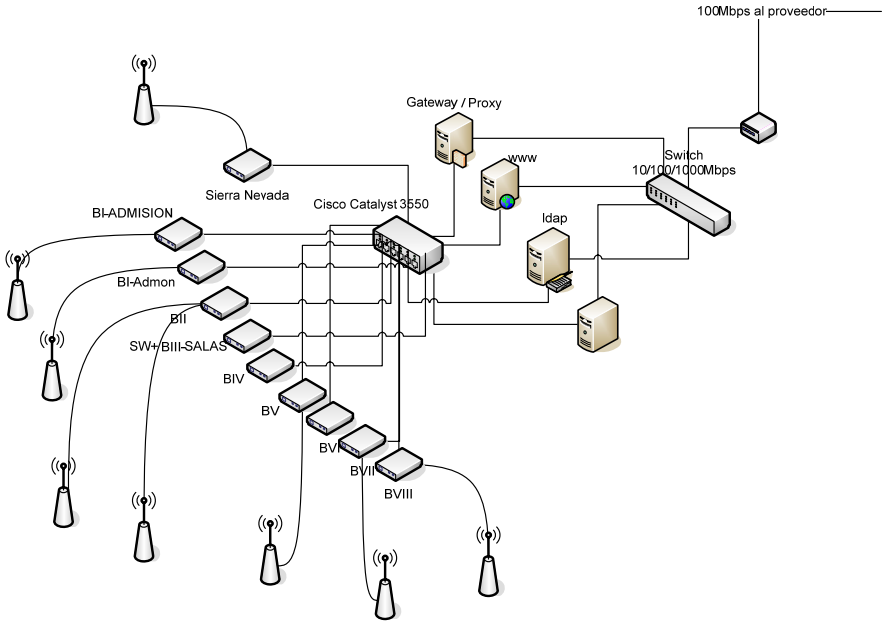
Para referencia de la red de la Universidad del Magdalena están las figuras 5 y 6.

Figura 5. Red de acceso a Internet de la Universidad del Magdalena.



[8] Fuente Oficina Asesora de Nuevas Tecnologías.
[9] Fuente. Oficina Asesora de Nuevas Tecnologías

Figura 6. Red de distribución LAN Alámbrica/Inalámbrica de la Universidad del Magdalena



1.3 IMPORTANCIA Y JUSTIFICACION

El control de los recursos informáticos tiene su origen en el sector productivo, siendo una manifestación clara de eficiencia y eficacia en el uso del servicio. Pero el cumplimiento de un modelo que permita racionar este recurso, sin perder de vista la función para la cual esta destinado el servicio de Internet, suponen establecer una serie de medidas que respalden la implementación de esta propuesta; estas consideraciones son:

1.3.1. Seguridad

Para alcanzar esta misión la universidad posee unos recursos físicos y humanos limitados. Pero como es responsabilidad de la Universidad del Magdalena el buen uso que se le de al servicio de Internet, se hace necesario por parte de la institución tener información del uso de ese recurso, así como es responsabilidad de cada miembro de la institución el buen uso del mismo.

Sin un sistema que permita a la institución recolectar información acerca de quién, cuándo, dónde y cuánto tiempo estuvo conectado, se incrementa la complejidad de la administración de la red. Más aún cuando en la mayor parte de los salones y bloques hay puntos de red disponibles para que cualquier persona pueda hacer uso de ellos, ya sea con algún computador de la misma institución, o quizás externo a la institución, y esto sin realizar algún tipo de verificación o autenticación.

1.3.2. Costos

El acceso a Internet se obtiene mediante contratación de bps con proveedores de servicios de valor agregado. En el año 2004 la Universidad del Magdalena contrató para sus sedes (Principal, Claustro San Juan Nepomuceno, Instituto de Postgrados) con la Empresa Dialnet de Colombia S.A. E.S.P. $14.000.000 mensuales, por un E1 Clear Channel (2048Kbps), en el año 2005 por una cifra casi similar $13.500.000 mensuales, se contrataron 4096Kbps Para el presente año la contratación asciende a $16.600.000 mensuales por 6400Kbps a partir del 15 de febrero de 2006.

Sin embargo el consumo de tráfico siempre ha mantenido durante las semanas normales de labores un consumo de 99% del contratado y es muy común que ese consumo sea simétrico, es decir tanto de subida como de bajada.

En la actualidad existen solicitudes por ancho de banda cuatro veces mayor que el contratado para la vigencia 2006 en las actuales condiciones de la red. Se estaría ante una situación desproporcionada en cuanto a uso de los recursos económicos de la entidad, más aun cuando esos montos pueden ser invertidos en otras áreas.

1.3.3. Mejoramiento del Servicio

Si bien los costos juegan un papel muy importante ante muchos otros factores, se debe tener en cuenta las reglas que actualmente usa la Universidad del Magdalena en cuanto a "dosificación" del ancho de banda a sus usuarios.

El actual acceso a Internet (incluido los servicios propios de la universidad como el correo electrónico y el portal) se limita según la subred. Por ejemplo una sala de Internet tiene un acceso de 128Kbps, la biblioteca accede a 192Kbps y así sucesivamente (esta suma puede ser más de el ancho de banda contratado) con las demás subredes, y cada máquina en dicha red se le entrega aproximadamente 4Kbps.

Sin embargo la limitación se hace solamente a cierto tipo de solicitudes (Actualmente solo se realiza a nivel de las tramas HTTP, HTTPS, FTP, por limitantes del software que realiza tal función) que no son las de mayor demanda de ancho de banda y que llegan a representar menos de un 50% del ancho de banda consumido[10], y las solicitudes tipo p2p (peer to peer) que se conectan a redes de usuarios para compartir archivos y descargar música, video, software, documentos, consumen mucho ancho de banda tanto downstream como upstream.

Este tipo de solicitudes son muy complejas de manipular, ya que enmascaran sus puertos en otros para salir a Internet, y le hacen "trampa" a las restricciones que actualmente realiza la Universidad del Magdalena, trayendo consigo un detrimento del servicio a las demás subredes y por consiguiente a las máquinas conectadas a la red.

Con esta propuesta se podrá delimitar los recursos en formas muy flexibles, por ejemplo asignando cuotas (tipo tarificación) a las identidades, no importa que software este usando o que tipo de tráfico, cada usuario autenticado registra el consumo. Además cuando no se esta autenticado no esta conectado a Internet,

[10] Informe de Consultoría realizado por la Empresa Dialnet

evitando que redes p2p sigan consumiendo ancho de banda aun en ausencia de alguna persona frente a la máquina, esto mismo permite un control de propagación de gusanos hacia otras redes.

También permite descentralizar el ancho de banda de las máquinas es decir, puedo seguir teniendo las mismas políticas que la universidad defina sin estar trabajando en la misma oficina.

Estas características permiten un mejoramiento que puede seguir escalando según las políticas que la universidad desee tener.

1.3.4. Gestión

Delimitar el ancho de banda con las actuales herramientas con que cuenta la universidad es una tarea de solo administradores de red experimentados, además de confusa, inexacta y manual.

El sistema necesita flexibilidad para gestionar los usuarios y la posibilidad de integrarse a una interfaz Web que permite crear las identidades de acceso y asignarlas a las diferentes políticas. Cada identidad puede tener particularidades, a fin de cuentas el requerimiento de un investigador, no es igual al de un estudiante que solo necesita hacer una tarea (en el mejor de los casos).

1.4 OBJETIVOS

1.4.1 Objetivo General

Proponer un sistema de control y acceso a Internet de acuerdo a las necesidades de cada identidad o grupo de identidades, a partir de la evaluación de la situación actual de la red de la Universidad del Magdalena.

1.4.5 Objetivos Específicos

- Realizar un seguimiento a las condiciones actuales de la red.
- Analizar estrategias aplicables a la situación de la Institución.
- Integrar tecnologías que permitan la aplicación flexible de políticas de uso.
- Aplicar criterios de control de acceso y control de ancho de banda independiente del tipo de tráfico.
- Integrar herramientas de software libre para realizar control de tráfico y autenticación.

2. FUNDAMENTACION TEORICA

2.1 REDES Y COMUNICACIONES

La transmisión de datos utilizando cualquier elemento físico de transmisión, se realiza por medio de ondas de transmisión; tales ondas están parametrizadas por ciertas características que influyen sobre el conjunto de datos transmitidos. De ahí que es necesario definir cada una de estas características.

2.1.1 Ancho de Banda[11]

Se define como ancho de banda la medida del rango de frecuencia de un canal de transmisión sobre un medio físico (Cable UTP, Fibra Óptica, Microondas).

Físicamente expresamos el ancho de banda como un intervalo de frecuencia de ondas (Δf) en las cuales se acumula la mayor energía de la señal. La unidad física asociada al ancho de banda es el Hertz (*Hz*). La expresión (1) muestra la relación que define el ancho de banda.

$$\Delta f = f_2 - f_1 \quad (1)$$

[11] CASTRO, Antonio y FUSARIO, Rubén. Teleinformática Aplicada. Madrid, España. Mc Graw Hill, 1994. V. I, 657 p.

Donde los valores de $f_2 \; y \; f_1$ son los límites inferior y superior del ancho de banda de la señal respectivamente.

Existe una relación de equivalencia entre el medio físico de transmisión y el ancho de banda de una señal; esta relación da como resultado una deformación de onda que se denomina *distorsión de onda.* De esta manera el medio físico de transmisión actúa como un filtro permitiendo el paso de señales que se encuentra entre los límites de la señal $f_2 \; y \; f_1$.

2.1.2 Frecuencia de Onda[12]

Frecuencia es el numero de ciclos que tiene una onda en un periodo de un segundo (1 seg). La frecuencia se mide en Hertz. La expresión (2) ilustra la forma matemática que define la frecuencia en función del período de una onda.

$$F = \frac{1}{T\ seg}\ Hertz \qquad (2)$$

2.1.3 Velocidad de Transmisión[13]

La velocidad de transmisión está relacionada directamente con la capacidad del medio físico empleado para transportar la información. La velocidad de transmisión es la cantidad de bits que se pueden transmitir en un instante de tiempo de un segundo (1 seg) por un medio físico o canal de comunicación. La expresión que la define es "*bits/seg*", se lee "bits por segundo".

---

12 Ibid p. Ancho de Banda.

13 Ibid p. Ancho de Banda.

2.1.4 Indicadores

Son aquellos que afectan a la velocidad con la que los mensajes individuales pueden ser transferidos entre dos computadores interconectados. Estos son:

- **Latencia**: Es el intervalo de tiempo que ocurre entre la ejecución de la operación de envío y el instante en que los datos comienzan a estar disponibles en el destino.
- **Tasa de Transferencia de Datos**: Es la velocidad a la cual se pueden transferir datos entre dos computadores conectados a la red. La transmisión, una vez ya inicializada es medida en bits por segundos.
- **Tiempo de Transmisión:** Es el tiempo requerido por una red para la transmisión de un mensaje de 1 bit de longitud entre dos computadores es:

Tiempo de transmisión del mensaje = Latencia + Longitud / Tasa de transferencia.

Esta ecuación es válida para mensajes cuya longitud no supere un máximo que viene determinado por la tecnología de las redes subyacentes. Para mensajes más largos se los segmenta y el tiempo de transmisión es igual a la suma del tiempo de transmisión de cada segmento.

La tasa de transferencia de una red viene determinada por sus características físicas y la latencia estará determinada por las sobrecargas del software, los retrasos en el enrutamiento y una componente estadística derivada de los conflictos en el uso de los canales de transmisión.

El ancho de banda total del sistema de una red es una medida de la productividad (throughput), del volumen de tráfico que puede ser transferido a través de la red en un intervalo de tiempo dado. En muchas tecnologías de LAN, se utiliza toda la

capacidad de transmisión de la red en cada transmisión y el ancho de banda es igual a la tasa de transferencia. Sin embargo, en la mayoría de las redes WAN los mensajes pueden ser transferidos simultáneamente sobre varios canales diferentes de modo que el ancho de la banda no guarda relación directa con la tasa de transferencia.

2.1.5 Tipos de Señal[14]

En los sistemas de comunicación se utilizan dos tipos de señales para la transmisión, estas señales son: *señales análogas* y *señales digitales*, cada una de estas señales utiliza dispositivos diferentes para su implementación.

2.1.5.1 Señales Análogas.

Una señal análoga es aquella que es representada por funciones que pueden tomar un número infinito de valores en un intervalo de tiempo.

Una señal análoga presenta las siguientes características:

- Puede transmitir voz, textos, imágenes y datos.
- Se varían las características de la onda (amplitud, frecuencia y fase) para la transmisión de la voz, textos, imágenes y datos.
- Los circuitos eléctricos que soportan este tipo de señal se denominan "circuitos análogos".

14 Ibid p. Ancho de Banda.

2.1.5.2 Señales Digitales.

Una señal digital es aquella que puede ser representada por funciones que toman valores finitos en cualquier intervalo de tiempo.

Al utilizar este tipo de señal en un sistema de comunicación se le denomina "Sistema de Comunicación Digital".

Una señal digital presenta las siguientes características:

- Las señales digitales al ser transportadas por un medio físico sufren deformaciones producto de la influencia del medio físico de transmisión utilizado o debido a agentes externos.
- Las señales digitales necesitan un proceso de regeneración constante. El dispositivo empleado para este fin se llama regenerador. Este dispositivo se encarga de modular y reconstruir la señal digital que está sujeta a distorsiones debido al medio utilizado.
- Una señal digital consume menos ancho de banda que una análoga.

2.1.6 Modelo OSI y sus Niveles

El modelo está basado en una propuesta que fue desarrollado por la Organización Internacional de Normas (ISO), y su objetivo era la normalización internacional de varios protocolos. Este modelo de referencia se le conoce como modelo de referencia OSI, ya que se refiere a la conexión de sistemas diferentes; es decir, a sistemas dispuestos a establecer comunicación con otros que son distintos.

2.1.6.1 Capa Física.

Esta capa se encarga de la transmisión de bits por medio de un canal de comunicación. El propósito de la capa física es asegurar que si una máquina M1 transmite un bit con un valor uno (1) a través de un canal, la máquina M2 debe recibir este mismo bit con el valor de uno (1). La transmisión de un bit de valor uno (1) o cero (0) se específica por los voltios que lo representa, también cuantos microsegundos deberá durar un bit.

Estos medios físicos son los medios magnéticos, par trenzado, cable coaxial de banda base, cable coaxial de banda ancha, fibra óptica, transmisión por trayectoria óptica y transmisión por satélite.

2.1.6.2 Capa de Enlace.

La capa de enlace sirve de interfase entre dos máquinas adyacentes[15], las cuales están conectadas por un medio físico de transmisión. Ella transforma el medio físico de transmisión en una línea sin error. La capa de enlace es de transmisión para la capa de red; convirtiendo la información que sale del emisor en tramas de datos transmitiéndola de una manera secuencial y recibiendo las repuestas del receptor. Esta debe reconocer los límites de las tramas, y también se encarga de los errores de transmisión, regula el flujo de la trama de manera que los receptores lentos no se vean desbordados por los emisores rápidos y el enlace en general.

---

15 El término adyacente hace referencia a máquinas que son continuas.

2.1.6.3 Capa de Red.

Se encarga de controlar todas las operaciones de la subred. Su función es encaminar los paquetes de datos desde el origen al destino; controla la obstrucción mutua de paquetes en la subred (cuello de botella).

En ésta capa se controla el problema de interconectar redes heterogéneas que pueden tener diferentes protocolos. Además brinda servicios a la capa de transporte; se encarga de contabilizar cuantos paquetes ha enviado el emisor al receptor.

2.1.6.4 Capa de Transporte.

Esta es la capa más importante del modelo OSI, ya que se considera centro de control de los protocolos. Su gran labor es la de hacer que el transporte de los datos se realice de manera segura, económica y eficiente, desde la máquina origen a la máquina destino. Independiente de la red o de las redes que se encuentran en uso. También en esta capa se determina que tipo de servicios se les debe dar a la capa de sesión y en última instancia a los usuarios de la red. Existen otros dos tipos de servicios de transporte que son: orientados a conexión y sin conexión. Una diferencia de esta capa es que el servicio que presta la capa de transporte está libre de errores; ya que los errores que provienen de la capa de red los detectan las entidades de transporte y son recuperados por el protocolo de transporte.

Algo muy importante es que si la conexión se interrumpe la capa de transporte puede establecer una nueva y continuará con la conexión a partir de donde se interrumpió la anterior. También define para quien va dirigido el destino.

2.1.6.5 Capa de Sesión.

Es la primera capa de las capas superiores, proporciona servicio orientado a usuarios comenzando con un canal sin error. Esta capa permite sesiones a los usuarios de diferentes máquinas que están en la red. La capa de sesión ofrece los siguientes servicios:

1. Servicio de gestión de control de diálogo entre dos (2) máquinas.
2. El de administrador de testigos, para que en un instante dado ambas máquinas no realicen una misma operación.
3. Sincronización, consiste en insertar puntos de verificación en el flujo de datos con el objeto de que después de cada caída solo se repitan los datos que están después del último punto de verificación.

La capa de sesión le ofrece permisos a la capa de presentación que consiste en establecer una conexión entre dos (2) máquinas llamada sesión, pudiendo así transferir datos, archivos o realizando otra actividad. Para que exista una sesión, primero deberá haber una conexión en la capa de transporte que soporte la conexión. Una de las características más importantes de esta capa es el intercambio de datos.

2.1.6.6 Capa de Presentación.

En esta capa se tratan los problemas relacionados con la representación de los datos transferidos, es decir, la manera sintáctica y semántica de la información que se transmite, incluyendo los aspectos de conversión, cifrado y compresión de datos.

Esta capa es la encargada de la preservación del significado de la información transportada. Cada computador puede tener su propia forma de representación y es en esta capa donde se realizan los acuerdos y las conversaciones para poder llegar al entendimiento entre computadores diferentes. Por lo tanto, la capa de presentación se encarga de la codificación de los datos estructurados, del formato interno de la máquina que transmite, para luego decodificarlos y representarlos en el formato de la máquina destino.

2.1.6.7 Capa de Aplicación.

Esta capa tiene varios protocolos y/o programas de usuarios (llamadas aplicaciones), los cuales realizan el trabajo real para el cual fueron adquiridos los computadores. Estos programas se sirven de los servicios que ofrece la capa de presentación para suplir las necesidades de comunicación.

Los protocolos se utilizan para comunicar grandes cantidades de computadores incompatibles que se encuentran en cualquier lugar geográficamente disperso. En algunas redes se pueden tener diferentes tipos de computadores, cada uno de ellos con diversas formas de distribución de pantalla, movimiento de cursor y otras diferencias.

Este tipo de problemas se pueden resolver en la capa de aplicación definiendo un computador virtual de red de abstracción con el que los editores y otros programas pueden ser escritos para tratar con el, en este computador se debe describir un software que facilite el manejo de cada tipo de computador. Otra función de la capa de aplicación es la transferencia de archivos, correo electrónico, la entrada de trabajo a distancia, el servicio de directorio y otros servicios de propósito general o específico.

2.1.7 Arquitectura de Redes de Computadores

Se le denomina arquitectura de redes de computadores al conjunto de capas y protocolos que se crearon para realizar una comunicación entre dos máquinas.

A continuación se enumeran algunos objetivos que deben tenerse en cuenta para diseñar una arquitectura de redes:

1. Ser una red transparente para el usuario final y el programador de aplicaciones.
2. Mejorar la manipulación de los cambios en cualquiera de los elementos de la red.
3. Permitir conectar a la red sistemas centrales múltiples o dispositivos inteligentes.
4. Habilitar computadores con funciones diferentes.

Necesidad de las Arquitecturas.

Existen cuatro (4) tendencias fundamentales que son[16]:

1. La falta de protocolos de comunicación de datos que trasciendan los límites de los protocolos ya existentes.
2. La capacidad de trasladar "inteligencia" a pequeños dispositivos.
3. Desarrollar la comunicación entre nuevos dispositivos.
4. Realizar la interconexión con medios nuevos de transporte de datos.

Propósito de las Arquitecturas.

La arquitectura de red pretende mantener una comunicación multicapa. La arquitectura se encarga del diseño y control de la capa que hace parte de la conversación entre dos (2) computadores no necesariamente de una misma red y sus protocolos, para facilitar la comunicación. La división por niveles o capas tiene mucha importancia porque facilita la comunicación y corrige problemas como los mencionados anteriormente.

Su objetivo es el vínculo de unión para todos los productos de comunicación de datos mostrando una serie de reglas básicas para la interconexión. De este modo, la arquitectura nos asegura que los productos de comunicación trabajen conjunta, confiable y consistentemente.

---

[16] GONZALEZ, Néstor. Comunicaciones y Redes de Procesamiento de Datos. Mc Graw Hill, México. 1987, 396 p.

2.1.8 Protocolos de Comunicación

Definición[17].

Es un conjunto de reglas y procedimientos que proporcionan técnicas uniformes para administrar una línea de comunicación. Estas reglas se utilizan para administrar y controlar los recursos que están involucrados en la comunicación.

Características de los protocolos de comunicación.

Para que dos (2) computadores puedan comunicarse, es necesario, en primer lugar, que se realice la notificación entre ambas máquinas de estar dispuestas a la conversación. Una vez establecida la comunicación deben tener un método o protocolo de comunicación que ambas entiendan, de lo contrario se podrá perder alguna información desde el primer envío.

Otra característica es tener un mecanismo para que la máquina receptora sepa reconocer los datos a medida que van llegando, utilizando una base de tiempo mutuo o un mismo reloj "común" a los dispositivos que emiten y reciben llamado también *sincronismo.*

[17] GONZALEZ NESTOR, Op. Cit. p 119

2.1.8.1 Protocolo TCP/IP. (Transmissión Control Protocol / Internet Protocol[18])

El TCP/IP literalmente son nombres de dos (2) protocolos, el TCP y el IP utilizados para la comunicación entre redes. Es un mecanismo de comunicación entre procesos.

Características Principales del TCP/IP

- Independencia de la tecnología de las redes. Esta basado en una tecnología convencional, conmutación de paquetes independientes de cualquier hardware.
- El TCP/IP proporciona un mecanismo de propósito general eficaz y fuerte.
- No es coincidencia que el TCP y el IP trabajen bien juntos. Aunque los protocolos se pueden utilizar por separado fueron diseñados al mismo tiempo para trabajar como parte de un sistema unificado y también para cooperar uno con el otro y complementarse. Por lo tanto el TCP resuelve todos los problemas que el IP no puede, sin duplicar el trabajo del IP y proporciona a las aplicaciones una comunicación confiable.
- Una red TCP/IP enruta mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje.
- Define la transmisión de datos llamada *datagrama*.
- Interconexión universal. Permite comunicar dos computadoras de diferentes redes, por que cada uno tiene una dirección única universal dentro de la red, además el datagrama lleva las direcciones fuentes y destino, los

[18] Protocolo de Transmisión/ Protocolo de Internet .http://es.wikipedia.org/wiki/TCP_IP

computadores intermedios dedicados de conmutación especial (enrutadores) utilizan la dirección destino para tomar la decisión de enrutar.

- Acuse de recibo punto a punto. Los protocolos TCP/IP proporcionan acuse de recibo entre el emisor y el último receptor en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aun cuando las dos máquinas no estén en la misma red física.

TCP/IP con Internet

El TCP/IP proporciona los recursos básicos de comunicación utilizados por Internet, es la base donde se sustentan todos los servicios. La fiabilidad es la clave de lo que sucede en Internet. Es por eso que Internet tomó todos los componentes de control del protocolo TCP y la versatilidad del protocolo IP.

2.1.9 Servicios de Comunicación

Los principales servicios existentes en materia de comunicaciones son:

- Internet.
- Redes digitales de servicios integrados.
- Servicio integrado de datos, voz y video.
- Servicio de correo electrónico.
- Redes Móviles.
- Acceso remoto a redes.

2.1.10 Internet

2.1.10.1 Historia de Internet

A finales de los años 70 el departamento de defensa de los E.U., se interesó en utilizar redes computacionales. Debido a que la idea de las redes computacionales era nueva, a través de ARPA (Advanced Research Projects Agency[19]), el ejército apoyó la investigación sobre las redes utilizando una gran variedad de tecnologías. Pero más adelante ARPA se convirtió en ARPANET, que es una red de área amplia. El ejército se dió cuenta más tarde de que esta red encontraría problemas, porque no existían conexiones entre las computadoras de redes separadas. De allí, que los investigadores de ARPA examinaron la manera de interconectar todas las máquinas de una empresa grande. Una idea clave en la investigación de ARPA fue un enfoque sobre la interconexión entre las LAN y las WAN, que llegó a conectarse como *interredes* (internetwork). Luego el término se abrevió en ***Internet.***

El software diseñado para la comunicación en **Internet** está conformado por dos (2) partes: El protocolo Internet (IP) que proporciona la comunicación básica y el Protocolo de Control de Transmisión (TCP) que proporciona facilidades adicionales que necesitan las aplicaciones. Este proyecto de **Internet** fue concebido como un sistema abierto, porque estaba disponible para todos.

[19] Agencia de Proyectos de Investigación Avanzada, a esta red se le llamó DARPA, durante los últimos años de la década de los 80.

2.1.11 RADIUS (Remote Access Dialin User Service)

Fue desarrollado originalmente por las empresas Livington. Es un protocolo de control de acceso que verifica y autentica usuarios basados en el método desafío/respuesta. Aunque RADIUS tiene un lugar prominente entre los proveedores del servicio de Internet, también puede ser usado en cualquier ambiente donde la autentificación central, la autorización regulada y el registro detallado del usuario sean necesarios o deseados.

A pesar que RADIUS es conocido como un proceso AAA, consistente en Autenticación, Autorización y Registro (Accounting), este protocolo fue creado antes que fuese desarrollado el modelo AAA, pero este fue el primer protocolo basado en AAA brindando la funcionalidad AAA para ganar aceptación en la industria y permanencia en uso.

2.1.11.1 MODELO AAA

El modelo AAA, se enfoca en tres aspectos cruciales del control de acceso a usuarios: Autenticación, Autorización y Registro (Accounting), respectivamente. Estos tres aspectos son los que se definen a continuación:

Autenticación

Es el proceso de verificación de la identidad declarada por una persona o máquina. Un ejemplo es cuando se ve un formulario común de autenticación, usando una combinación de usuario/contraseña en donde el conocimiento del la contraseña es una representación de que el usuario es auténtico.

El aspecto fundamental de la autenticación es que permite que dos objetos únicos formen una *verdadera interrelación* ambos son tenidos en cuenta para ser usuarios válidos. La confianza entre sistemas permite para tal funcionalidad clave como el servidor Proxy Radius, el cuál concede la petición en favor de otro sistema y admite implementaciones AAA para atravesar redes heterogéneas soportando diversos tipos de clientes y servicios. Las relaciones de confianza pueden llegar a ser absolutamente complejas.

Autorización

Este proceso involucra un conjunto de reglas u otras plantillas para decidir que puede hacer en el sistema un usuario autenticado. Por ejemplo, si una IP se entrega dinámicamente a un usuario o siempre se le entrega la misma IP. Estas reglas son definidas por el administrador.

También llamadas "implementaciones inteligentes" de de los servidores tipo AAA, analizando la lógica de las solicitudes y garantizan el acceso que le es posible entregar. Por ejemplo si un usuario intenta conectarse a la red éste podría simplemente negarse o aceptarse la contraseña según el usuario y la contraseña suministrada, pero las implementaciones inteligentes no solo verifican esa pareja de directivas, también realizan un chequeo de la hora a la que va a conectarse el usuario, el tiempo disponible para navegar, si puede conectarse simultáneamente o tiene un sólo canal habilitado para conectarse,

Registro (Accounting)

La infraestructura AAA tiene la capacidad de poder medir y documentar los recursos a los que se suministra acceso. Esta información puede incluir el monto de

tiempo en el sistema, la hora de conexión, la hora de desconexión, el motivo de la desconexión, la IP desde la que se conectó, el NAS al cual se afilió, etc. Esta información almacenada no solo nos sirve de estadística simple. La mayoría de los sistemas de RADIUS utilizan esta información para realizar los respectivos cargos de consumo a los que tenga lugar el usuario que se conecta a la red. Como la información almacenada también involucra los consumos en octetos de bytes es posible poder suministrar reglas al servicio que controlen cuantos bytes un usuario puede descargar de la red, durante un lapso de tiempo.

Cabe resaltar que RADIUS como servicio no suministra el acceso a la red, simplemente atiende las solicitudes de autenticación del servidor NAS que es quien se conecta directamente al equipo del usuario.

2.1.12 Base de Datos

Una base de datos es un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su uso posterior. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

2.1.12.1 SQL

El Lenguaje de Consulta Estructurado (Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar

diversos tipos de operaciones sobre las mismas. Combina características del álgebra y el cálculo relacional permitiendo lanzar consultas con el fin de recuperar información de interés de una base de datos, de una forma sencilla.

El SQL es un lenguaje de acceso a bases de datos que explota la flexibilidad y potencia de los sistemas relacionales permitiendo gran variedad de operaciones sobre los mismos.

Es un lenguaje declarativo de alto nivel o de no procedimiento, que gracias a su fuerte base teórica y su orientación al manejo de conjuntos de registros, y no a registros individuales, permite una alta productividad en codificación. De esta forma una sola sentencia puede equivaler a uno o más programas que utilizasen un lenguaje de bajo nivel orientado a registro.

2.1.12.2 DBMS (Database Management System)

Los Sistemas Gestores de Bases de Datos son un tipo de software muy específico, dedicado a servir de interfaz entre las bases de datos y las aplicaciones que la utilizan. En los textos que tratan este tema, o temas relacionados, se mencionan los términos SGBD y DBMS, siendo ambos equivalentes, y acrónimos, respectivamente, de Sistema Gestor de Bases de Datos y DataBase Management System, su expresión inglesa.

El objetivo primordial de un sistema manejador base de datos es proporcionar un entorno que sea a la vez conveniente y eficiente para ser utilizado al extraer, almacenar y manipular información de la base de datos. Todas las peticiones de

acceso a la base, se manejan centralizadamente por medio del DBMS, por lo que este paquete funciona como interfase entre los usuarios y la base de datos.

2.1.12.3 MySQL

MySQL es un sistema de administración para bases de datos relacionales (RDBMS) que provee una solución robusta a los usuarios con poderosas herramientas multi-usuario, soluciones de base de datos SQL (structured Query Language) multi-threaded. Es rápido, robusto y fácil de utilizar.

2.1.13 VPN

Una VPN es una Red Privada Virtual, creada por encriptación a través de un medio inseguro, como Internet. Uno de las formas más comunes de VPN es el túnel o tunnelling el cual es un tipo de encriptación que realiza una conexión punto a punto en forma segura. El túnel es llamado virtual por que no puede ser accedido por conexiones externas.

2.1.14 SINGLE SIGN ON – SSO[20]

El concepto de Single Sign-On se refiere al acceso a múltiples recursos por medio de un único proceso de ingreso. Gran cantidad de las arquitecturas implementadas

[20] CONSIDERACIONES PARA IMPLEMENTAR UNA ARQUITECTURA single sign-on, Iván M. Caballero y Jeimy J. Cano

en diferentes organizaciones han sido diseñadas con el objeto de dar acceso a los usuarios a múltiples servicios Web y/o aplicaciones. En la mayoría de los casos se encuentra que cada uno de los servicios o aplicaciones cuenta con su propio componente de seguridad, lo cual generalmente compromete la seguridad de todo el sistema, dado que el nivel de seguridad de todo un sistema es igual al nivel de seguridad del componente más inseguro que lo compone[21]. Una de las posibles soluciones a este problema es implementar la estrategia Single Sign-On.

Single Sign-On no necesariamente se refiere a una sincronización de passwords, ya que en ese caso todas las aplicaciones y servicios funcionan con un mismo password. Aunque una sincronización de passwords le permite al usuario experimentar las ventajas del SSO, ésta no puede considerarse una implementación real, ya que en lugar de fortalecer las características de seguridad del sistema, éstas se estarían debilitando, dado que cuando todas las aplicaciones o servicios utilizan un mismo password, se corre el riesgo de que si un intruso logra conseguir el password de una de las aplicaciones o servicios, inmediatamente tendrá acceso a todas ellas.

Arquitecturas

Existen diferentes tipos de arquitecturas que permiten implementar SSO. Cada una de ellas posee características que la hace más apropiada para algún tipo de organización. La decisión de adoptar una u otra arquitectura básicamente depende de los recursos computacionales y/o económicos disponibles, y las decisiones de diseño establecidas por el equipo del proyecto.

---

21 McGraw, G, *et.al.* (2002). The Weakest Link

Las diferentes arquitecturas SSO están compuestas por tres componentes básicos:

Interfase

El modo en que el SSO interactúa con una determinada aplicación. Usualmente reside en el cliente, y es conocido como Agente SSO.

Administración

El mecanismo que permite configurar, mantener y monitorear el proceso de SSO.

Identidad

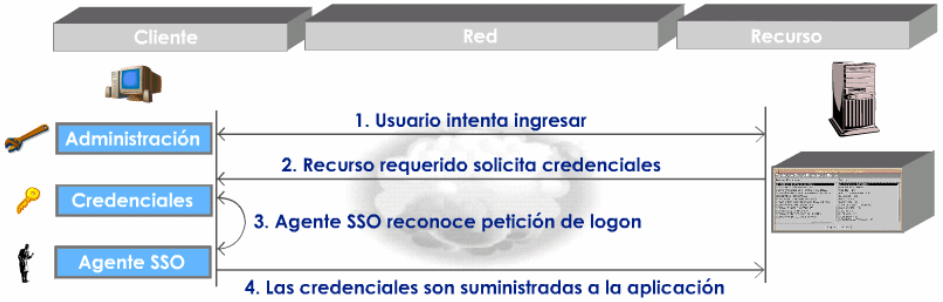
Cada aplicación a la que se accede requiere información confidencial (nombre de usuario, contraseña, etc.), que agrupada recibe el nombre de la Identidad. Las identidades deben almacenarse de manera protegida para que sea únicamente el agente SSO quien pueda acceder a ellas.

2.1.14.1 Password Vault

Se trata de la configuración más básica para implementar SSO utilizando identidades. En este caso los tres elementos de la arquitectura se encuentran ubicados en el cliente y, por lo tanto, es justamente allí desde donde se accede a las aplicaciones, para lo cual se deben previamente almacenar las identidades

correspondientes, para que puedan ser suministradas a las aplicaciones cuando sea necesario, como se ilustra en la figura 7.

Figura 7. Arquitectura Password Vault



Características

- Funciones administrativas limitadas. (La administración de cada uno de los clientes debe realizarse desde la estación correspondiente y por lo tanto generalmente termina quedando a cargo del usuario.)
- No es posible actualizar los clientes de manera masiva en toda la organización, requiere que se realice máquina por máquina.

Ventajas

- Su implementación no es mucho más complicada que instalar un nuevo software en el equipo cliente.
- Pocos recursos computacionales necesarios (Un servidor central donde residen las diferentes aplicaciones y los clientes necesarios.).

Desventajas

- La administración local obliga a tomar medidas adicionales de seguridad informática y control de acceso por parte de la empresa.

- El nivel de transparencia para el usuario es bajo ya que éste generalmente se encuentra comprometido con la administración del proceso de ingreso.
- El almacenamiento local de la identidad no permite que el usuario acceda a las aplicaciones desde múltiples estaciones.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.14.2 Administración centralizada con almacenamiento local de la Identidad

Con el propósito de solucionar los principales inconvenientes que presenta la arquitectura Password Vault, surge la Administración centralizada con almacenamiento local de la Identidad, ofreciendo un mecanismo para controlar y supervisar el proceso de ingreso, y eliminando la necesidad de configurar el SSO en cada uno de los clientes. La arquitectura en mención se ilustra en la figura 8.

Figura 8. Administración centralizada con almacenamiento local de la Identidad

Características

- Incluye un servidor central que permite realizar labores de administración.
- El software cliente es autónomo durante el proceso de autenticación, debido a que durante este proceso, la labor de administración se restringe a realizar monitoreo de los clientes. Las identidades permanecen en el cliente.

Ventajas

- Control centralizado de la configuración y monitoreo del software del cliente.
- Las labores de administración tienen un bajo grado de complejidad.

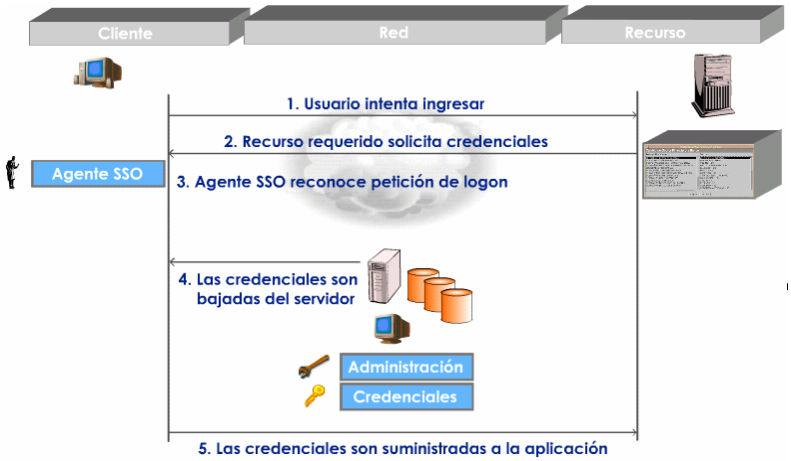
Desventajas

- El hecho de almacenar las identidades en el cliente hace que se deban tomar medidas de control de acceso y confidencialidad de la información.
- Una vez el cliente se ha conectado, el administrador del SSO sólo puede monitorear la conexión y no podría efectuar acciones de desconexión o cambio de configuración de la misma.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.14.3 Administración y almacenamiento de la Identidad centralizados

La arquitectura SSO con administración y almacenamiento centralizado de la Identidad (figura 9) soluciona los principales inconvenientes encontrados en la arquitectura que almacena las identidades localmente, la cual ya ha sido presentada.

Figura 9. Administración centralizada con almacenamiento local de la Identidad



Características

- Las identidades son migradas a un servidor central, quien entrega las identidades al cliente correspondiente en el momento de hacer el ingreso.
- El administrador determina la frecuencia con que se descargan las identidades del servidor (Por sesión, por login, etc.).

Ventajas

- Permite a los usuarios el acceso a las aplicaciones desde cualquier estación, previa autenticación del mismo.
- Ofrece administración centralizada de la identidad disminuyendo posible manipulación de la misma en el cliente.

Desventajas

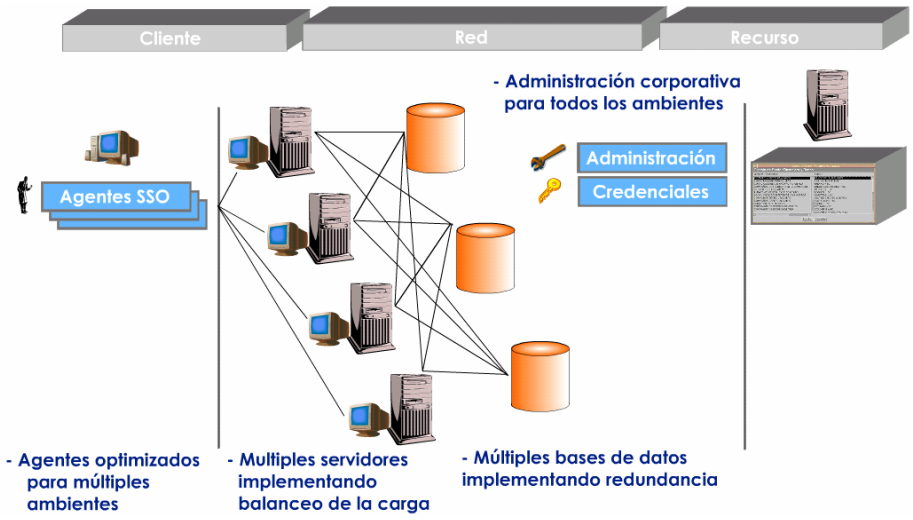
- Se crea un único punto de falla, convirtiendo al SSO en un gateway para todos los recursos de la organización, ya que el servidor debe ser contactado cada vez que se realice un ingreso.
- El acceso a todas las aplicaciones de la organización depende del servidor central.

- La configuración carece de redundancia, recuperación entre fallas y respaldo.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.14.4 Arquitectura SSO totalmente distribuida

La arquitectura SSO totalmente distribuida (mostrada en la figura 10) se caracteriza principalmente por separar el servidor de la base de datos, lo cual la hace completamente modular. Esta arquitectura soluciona los problemas encontrados en las arquitecturas anteriormente presentadas y adicionalmente ofrece múltiples ventajas.

Figura 10. Arquitectura SSO totalmente distribuida



Características

- La información se accede en el momento de ingreso.

- Cuenta con SSOs avanzados que utilizan bases de datos escalables que soportan redundancia (i.e. SQL Server u Oracle).
- Las bases de datos se encuentran sincronizadas con el fin de lograr redundancia y respaldo.
- El proceso de ingreso ha sido migrado a un recurso de red. Siempre y cuando el agente SSO pueda establecer conexión IP a un servidor SSO, las identidades podrán ser solicitadas (y almacenadas en memoria caché para realizar offline logon) y el ingreso podrá ser realizado.
- El servidor resulta ser una aplicación independiente que cuenta con un administrador diferente.
- La información es almacenada en bases de datos comerciales o en directorios de manera encriptada. Sin embargo, la información entre el cliente SSO y el servidor no viaja cifrada.

Ventajas

- Los agentes SSO se encuentran optimizados para múltiples ambientes (Terminal Server, Web, Win32).
- Contiene múltiples servidores implementando balanceo de la carga para aumentar la disponibilidad y la atención de los requerimientos de autenticación.
- El hecho de contar con múltiples servidores adicionalmente hace que se disminuya la latencia de la red.
- Contiene múltiples bases de datos sincronizadas, implementando redundancia.
- Permite realizar funciones de administración corporativa para todos los ambientes.

Desventajas

- Solución altamente costosa por el ambiente distribuido requerido.
- Demorada implementación técnica por interacción entre múltiples sistemas operacionales.
- Soporte y administración complejos por la consideración anterior.

2.1.14.5 Administración y almacenamiento de la Identidad centralizados garantizando alta disponibilidad y redundancia

La arquitectura SSO con administración y almacenamiento centralizado de la Identidad garantizando alta disponibilidad y redundancia (Figura 11) es una adaptación de la arquitectura centralizada, incorporando algunas de las ventajas de la arquitectura totalmente distribuida.

Figura 11. Admón. y almacenamiento de la Identidad centralizados garantizando alta disponibilidad y redundancia

Características

- Las identidades son almacenadas en un servidor central, quien entrega un certificado al cliente correspondiente, y las identidades necesarias a la respectiva aplicación, en el momento de hacer el ingreso.
- Incorpora infraestructura replicada con el fin de manejar la contingencia y redundancia en tiempo real.
- Ofrece alta disponibilidad mediante software.

Ventajas

- Permite a los usuarios el acceso a las aplicaciones desde cualquier estación.
- Ofrece administración centralizada.
- Su infraestructura duplicada permite implementar alta disponibilidad y redundancia.
- Tanto el hardware como el software se encuentran debidamente especificados para enfrentar una situación de contingencia.

Desventaja

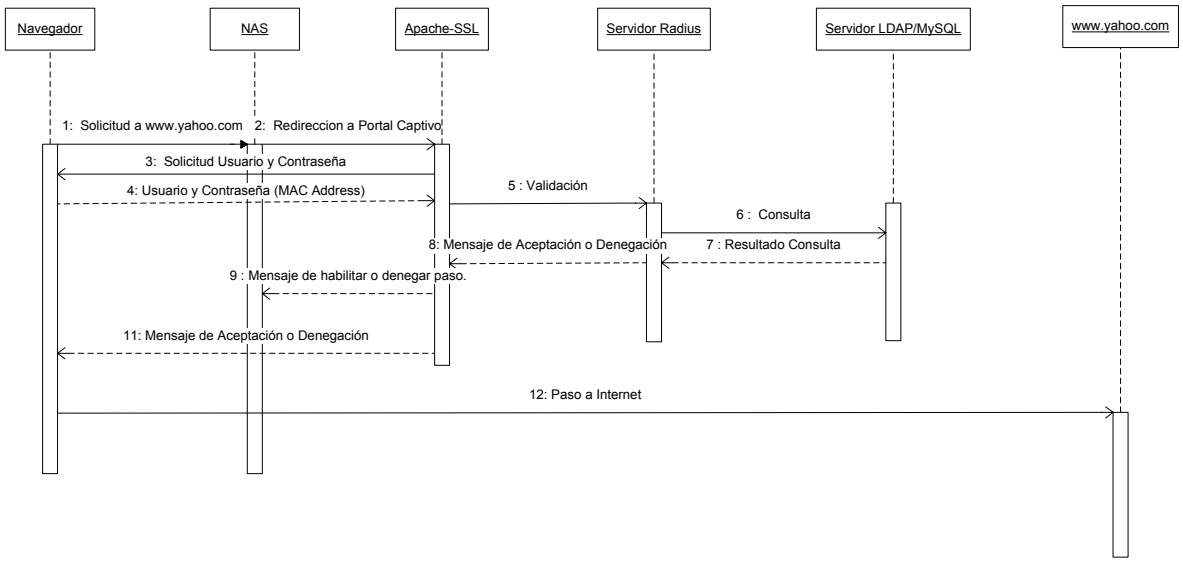
- La alta disponibilidad y redundancia que ofrece se basa en su infraestructura replicada, lo cual la hace costosa a nivel de hardware y software, como a nivel de administración y control de la misma.
- La información entre el cliente SSO y el servidor no viaja cifrada.

2.1.15 TECNICA CAPTIVE PORTAL.

La técnica "Captive Portal" forza las solicitudes de un cliente HTTP en una red para ver una pagina especial, (usualmente para propósitos de autenticación) antes de

acceder a la Internet u otra red[22]. Esto es posible interceptando todo el tráfico HTTP que el cliente emite y lo redirecciona hacia un portal de autenticación, cuya tarea es capturar la información suministrada por el usuario y validarla contra un servidor de autenticación.

Figura 12. Diagrama de Secuencia de la Técnica de Captive Portal



El proceso de solicitud se inicia en el momento en que el usuario conecta su tarjeta de red a la red. Ya sea Inalámbrica o alámbrica. Un gateway se encarga de suministrar una dirección IP y las direcciones DNS al equipo cliente usando el protocolo DHCP. Esta IP es referenciada con la dirección MAC del equipo cliente, en espera de la primera solicitud HTTP. Si el equipo cliente tiene asignada una dirección IP en su tarjeta de red, esta es validada dentro de las asignaciones que ya se han realizado y verificado si es una IP dentro del rango permitido. Si no ha sido suministrada a otro cliente se referencia la dirección IP asignada en la tarjeta de red y la dirección MAC. Todas las direcciones IP que no se encuentran autenticadas

22 http://en.wikipedia.org/wiki/Captive_portal

son bloqueadas por el Firewall, de forma tal que ellas solo se pueden comunicar entre si en el segmento local.

Tan pronto el usuario abre su navegador, es redireccionado a una página de autenticación. Este es el "Portal Captivo". En este portal el usuario verifica su identidad para ingresar al servicio que se encuentra bajo esta restricción. El Portal los autentica contra algún tipo de base de datos o protocolo (RADIUS,LDAP, etc). Si el usuario es autenticado

Antes del proceso de la autenticación cualquier tráfico diferente de HTTP es bloqueado por el gateway que controla el servicio.

2.1.16 Cuotas de Ancho de Banda

Las cuotas de ancho de banda son un método para la distribución del ancho de banda. Su funcionamiento se basa en la asignación de un límite de consumo, generalmente expresado en megabytes, el cual se puede discriminar como de descarga y subida hacia una red.

Cuando se alcanza este límite, el recurso de red que se encuentra limitado, deja de ser accesible.

Existen dos formas de establecer una cuota. Una es basándose en la dirección IP y otra basándose en la identidad.

Las cuotas basadas en IP, consisten en la identificación de la cantidad de tráfico que se está generando tanto de subida como de bajada desde y hacia una IP específica. Cada byte que se consume, sin importar que aplicación y/o protocolo que se encuentra usando el recurso, es contabilizado a la IP asignada al dispositivo que lo esta solicitando.

Las cuotas basadas en identidad, realizan el mismo procedimiento, pero contabiliza a una identidad que se autentica en la red, independientemente del dispositivo del que se autenticó.

De cualquiera de las dos formas estas cuotas se pueden determinar por los periodos de tiempos que el administrador de la red determine (por horas, diario, semanal, mensual, etc), permitiendo que cumplido este periodo de tiempo se reinicie la cuota asignada, permitiendo acceder nuevamente al recurso que está bajo control.

2.1.17 Asignación de tasas de transferencias

Es la metodología más comúnmente utilizada para controlar el uso de recursos como el acceso a Internet.

Consiste en la asignación de un espacio de uso, el cual generalmente es compartido, sobre el total de ancho de banda disponible.

Esta asignación determina a que rata o tasa de velocidad se accede al recurso limitado, distribuyendo lo más equitativamente posible el ancho de banda total disponible sin afectar significativamente la experiencia del usuario.

2.1.18 LINUX

Linux es un sistema operativo libre y de código abierto, el cual fue creado en el año 1991 por Linus Torvalds, un estudiante finlandés, buscando crear un clon del sistema operativo MINIX. Linux sigue los estándares de POSIX, y es considerado un sistema tipo UNIX. Linux como tal es un kernel, el cual al ser complementado con herramientas conforma una distribución, que comúnmente se referencia como Linux.

2.1.19 IPTABLES

Iptables es una herramienta de gestión para el filtrado de paquetes en Linux. Las tareas de red en Linux se realizan directamente en el kernel el cual define tres cadenas básicas. INPUT, FORWARD y OUTPUT.

INPUT hace referencia a todo paquete que llega a una interfase; OUTPUT a todo el que sale de ella y FORWARD al que atraviesa.

Iptables realiza el filtrado sobre estas cadenas predefinidas pero además puede definir nuevas cadenas, y redireccionarlas a diferentes tablas. PREROUTING, OUTPUT y POSTROUTING, MANGLE.

Las tres primeras redireccionan los paquetes y la última los etiqueta para que otras herramientas puedan utilizarlos.

2.1.20 PPPoE

PPPoE es la sigla de “Point to Point Protocol over Ethernet “ o protocolo punto a punto sobre Ethernet.

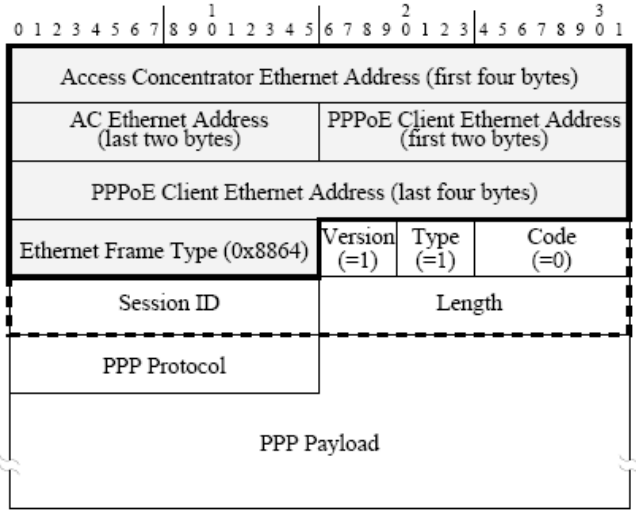
PPPoE es un protocolo que encapsula las tramas PPP en las tramas ethernet. PPP es protocolo de nivel de enlace usado para encapsular paquetes del nivel de red sobre un enlace serial asíncrono. Este modo de uso es llamado PPP asíncrono.

Una sesión PPPoE consiste de una trama PPP dentro de una Ethernet, con seis bytes de información PPPoE. Cada sesión la constan dos puntos de comunicación usando PPP, las cuales se encuentran inicialmente por el enlace ethernet. Cada punto conoce la MAC del otro punto. Adicionalmente se utiliza un numero de sesión para identificar las diferentes sesiones que pueden estar viajando por el enlace ethernet.

Mientras que PPP es un protocolo punto a punto, PPPoE es inicialmente un protocolo cliente servidor. El cliente (usualmente un computador) hace la búsqueda del servidor PPPoE (llamado concentrador de acceso o "NAS") y obtiene la dirección MAC y el numero de sesión. Si el concentrador acepta la sesión previa verificación contra un servidor RADIUS el servidor PPPoE entrega los recursos que RADIUS asigna al cliente.

La principal ventaja que PPPoE suministra es la creación de sesiones entre el cliente y el NAS y esto gracias a que estas sesiones son PPP. Estas sesiones permiten establecer la información necesaria para determinar el tiempo de conexión del usuario, hora, transferencias, encapsulando cualquier protocolo IP sobre PPP, y sometiéndolo a las restricciones que se determinen para cada sesión. Además se puede hacer asignaciones dinámicas de direcciones IP's o asignar estáticamente las IP's a los usuarios.

Figura 13. Paquete PPPoE



3. DISEÑO METODOLOGICO

Para el desarrollo de éste proyecto se realizó un estudio, sobre las metodologías que en la actualidad aplican diferentes universidades e instituciones del mundo para realizar control sobre el ancho de banda a Internet, así como de los esquemas de control de acceso que se aplican en estas instituciones.

El área de estudio en la que se encuentra enmarcada el proyecto está ligada a los conceptos adquiridos en la asignatura de Comunicación de Datos desarrolladas en la Universidad del Magdalena, además conceptos del área de telecomunicaciones y redes de datos y seguridad utilizando bibliografía obtenida en la biblioteca de la Universidad del Magdalena e Internet.

3.1 Análisis y Definición de Requerimientos

Para esta etapa del desarrollo de este proyecto, se utilizó la investigación científica y la consulta bibliográfica.

Los conceptos se reforzaron utilizando libros de la Biblioteca Central Germán Bula Meyer y se ampliaron con información obtenida en Internet.

Además se usaron varias técnicas para recolectar la información ellas son:

- Información recopilada de fuentes bibliográficas y consultas en la red mundial Internet, acompañada con los aportes hechos por el director de tesis.

- Información recolectada por la empresa proveedora del servicio de conexión a Internet; DIALNET DE COLOMBIA S.A., del tráfico general de la Universidad del Magdalena.
- Información recolectada en el centro de cableado de la Universidad del Magdalena mediante las herramientas: JFFNMS[23], TCPDUMP[24], ETHEREAL[25], MRTG[26].

Esta modalidad de recolección de información permite tomar decisiones de una forma más objetiva, teniendo en cuenta que se obtiene el concepto de las personas responsables de la red de datos de la universidad, en este caso, el personal de la Oficina Asesora de Nuevas Tecnologías; Jefe, Ingeniero y Técnico de la red.

Dentro de los hallazgos que se vislumbraron durante esta fase, se incluye la carencia de cultura en los usuarios del servicio de Internet de la Universidad del Magdalena, quienes a pesar de las llamadas de atención por parte de las personas encargadas de la red, siguen utilizando de forma indebida el canal de Internet, realizando descargas por medio de aplicaciones p2p y abusando de la mensajería instantánea, además de que las pocas herramientas con las que cuentan las personas que administran la red son adicionalmente obsoletas, ya que aún se cuenta con equipos de muy bajo nivel (Capa 2) resultando esto muy deficiente teniendo en cuenta la cantidad de ordenadores que posee la red de datos. Sumado a la carencia de políticas claras por parte de la universidad hacia los usuarios.

---

23 http://www.jffnms.org, es un sistema de monitoreo de redes diseñado para recolectar información a través de SNMP.

24 http://www.tcpdump.org, analizador de protocolos en modo texto.

25 http://www.ethereal.com, es un analizador de protocolos, utilizados para solucionar problemas de red, análisis, desarrollo de software y protocolos.

26 http://people.ee.ethz.ch/~oetiker/webtools/mrtg/, software para graficar información a través de SNMP.

Como resultado del análisis realizado en la primera etapa, se establecieron estrategias que condujeran al mejoramiento de la situación planteada con anterioridad, se buscaron alternativas que ayudaran al mejor aprovechamiento del ancho de banda.

Se planteó como opción elegible la posibilidad de no hacer nada al respecto, es decir, el *status quo*, lo que generaría a futuro gran inversión de capital por parte de la institución en adquisición de ancho de banda para el canal según las necesidades de los usuarios del sistema, además continuar con el riesgo permanente de posibles infracciones legales o hechos delictivos generados por los usuarios y debido a la carencia de un sistema que permita determinar el origen de la acción la Universidad deba responder por el uso indebido de sus usuarios.

La segunda alternativa considerada fue adquirir productos comerciales que permitieran controlar el acceso y el ancho de banda a Internet. Estos dispositivos del mercado se distribuyen dependiendo del troughtput real es decir de cuanto tráfico en realidad pueden administrar. Los dispositivos más económicos pueden administrar hasta 10Mbps y en su mayoría se basan en software. Los más costosos se basan en hardware, es decir tienen chips especializados para enrutar y controlar el tráfico. Algo en común tienen ambos y es que no solo cuenta el costo de compra del equipo sino, el crecimiento y actualización a escala de la infraestructura, ya que estas también representan un alto valor, las suscripciones para las tablas de firmas de protocolos las cuales se realizan con el objetivo de mantener actualizadas las bases de datos de los nuevos protocolo usados por aplicaciones, sobre todo las P2P.

La tercera alternativa es sobre la integración de tecnologías libres que se ajusten a la problemática que presenta la institución

4 PROPUESTAS DE SOLUCION.

4.1 AUMENTAR EL ANCHO DE BANDA

Para poder sostener los actuales niveles de consumo la Universidad del Magdalena necesita incrementar el ancho de banda. La institución tiene contratado a partir de15 de febrero de 2006 6400kbps, sin embargo, a solicitud de el proveedor de servicios, y en su necesidad de reorganizar la asignación de direcciones IP's, se habilito 6400Kbps con un nuevo rango de IP's y se mantuvo los 4096Kbps con el antiguo rango de IP's, esto con el fin de que la Universidad del Magdalena gestionara los cambios necesarios ante la Universidad de los Andes quien es la encargada de gestionar los dominios colombianos. Durante ese lapso de 2 días la Universidad del Magdalena consumió el 100% de los 10Mbps de ancho de banda en más del 60% del tiempo aún cuando el semestre académico esta iniciando.

Si se tiene en cuenta que el valor por mes contratado es de $19.047.619 por 6400Kbps durante el año 2006, para contratar 10Mbps se tendría que invertir por mes $30.476.190, y por 20Mbps $60.952.380[27].

[27] Aunque las cifras deben presentar una disminución por contratación de mayor ancho de banda la realidad es que esa disminución tiene un límite. Contratar un DS3 que son 48Mbps le costó a Metrotel en Barranquilla 40.000 dólares mensuales durante el año 2005.

4.2 ADQUIRIR PRODUCTOS COMERCIALES

Existen en el mercado diferentes marcas reconocidas para realizar tareas de control de tráfico o "shaping" y existen dos tipos de estrategias. Control por hardware y por software.

La diferencia fundamental entre estas dos estrategias, es que los equipos que realizan las tareas por hardware tienen chips especializados para realizar el enrutamiento y el control de tráfico, y descargan del sistema operativo y de la memoria del equipo dicha tarea, brindando mayores troughputs. En los dispositivos por software el sistema operativo además de atender las solicitudes debe realizar las tareas de control. Es por esto que este tipo de dispositivos administran menos ancho de banda; comercialmente hasta 10Mbps.

Al ir creciendo el numero de computadores de la universidad y ampliarse le numero de horarios y servicios, así como el numero de usuarios del mismo, se hace necesario controlar un mayor numero de solicitudes, y de una mayor variedad de protocolos de intercambio de archivos.

Este crecimiento y el ingreso a la red de Abilene por parte de la universidad, necesitan de una inversión en dispositivos de control por hardware para que a corto plazo no se vea saturado el dispositivo de control y de esta forma evitar cuellos de botellas en el tráfico a Internet.

Para direccional estos retos, la visibilidad debe ser especialmente granular al nivel de aplicación. Entre mas información exista para clasificar el tráfico, se suministra

una mejor inspección de los paquetes que ingresan y salen de la red, se detectan cambios dinámicos y migración de asignación de puertos, y se distingue entre las diferentes aplicaciones que usan el mismo puerto[28]. Es necesario utilizar los indicadores de Capa 7 para identificar el tráfico generado por las diferentes aplicaciones y de esta forma entender mejor como las aplicaciones usan el ancho de banda, y para que, para establecer políticas que mejoren el servicio.

Uno de estos productos es Packeteer, el cual se recomienda por cumplir con este nivel de filtrado, específicamente el PACKETEER 8500 PACKETSHAPER 47-1000-02 proporciona las tareas de control y administración del ancho de banda basada a nivel de flujo, de agregado, o individual usando la IP o la dirección MAC del equipo que solicita el trafico. Este dispositivo soporta 45Mbps de tráfico y tiene un costo de $USD 27.300[29].

Para realizar las tareas de autenticación de los usuarios es necesario utilizar un dispositivo que pueda gestionar usuarios y crear sesiones. Este dispositivo será un servidor PPPoE. Para esta implementación se usa un SERVPOET BMS 500 que se encargaría de recibir la solicitud del cliente PPPoE y establecer la sesión con el usuario final. Este dispositivo puede sostener hasta 3000 conexiones simultáneas PPPoE.

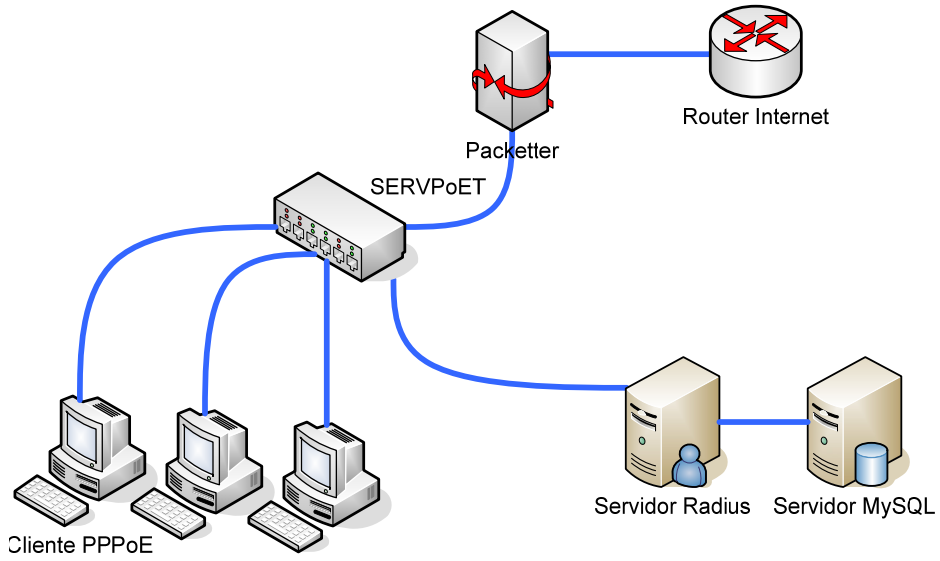
Para la terminación de la conexión en el lado del usuario se sugiere usar WinPoET como cliente de PPPoE, sobre todo para las maquinas que aún no corren el sistema operativo Windows XP. Para las estaciones que funcionan con Windows XP, se puede utilizar el mismo software de conexión de acceso remoto que viene con el

[28] El puerto http es usado también por aplicaciones tipo streaming, de mensajería, p2p, etc.
[29] El precio de referencia se encuentra en www.ebay.com.

sistema operativo. Para las estaciones que usen Linux existe un cliente desarrollado por Roaring Penguin llamado RP-PPPOE.

Cada licencia de cliente WinPoET para compras mayores a 1000 licencias tiene un costo de USD$ 3.35 dólares. La licencia para un servidor SERVPOET BMS 500 es de $USD11.882 dólares[30]. Todos estos costos no incluyen soporte ni entrenamiento para la configuración o la configuración misma de los equipos.

Figura 14. Modelo para propuesta usando productos comerciales.



4.3 IMPLEMENTACION DE LA SOLUCION COMERCIAL USANDO LINUX

Para esta implementación es necesario tener instalado los siguientes paquetes en el servidor:

iproute2, iptables, ppp, rp-pppoe, freeradius, radiusclient.

[30] https://www.soft-express.com/backend/quote.php?N=174&K=675675&L=ES

Además es necesario un servidor con 2 tarjetas de red. Una para recibir la solicitud del usuario y la otra hacia Internet. Este servidor usaría como sistema operativo Linux.

Como rp-pppoe no es un paquete fácil de encontrar una opción es descargarlo de http://www.roaringpenguin.com/pppoe/rp-pppoe-3.5.tar.gz y compilarlo e instalarlo de la siguiente manera:

```
#tar zxvpf rp-pppoe-3.5.tar.gz
# cd rp-pppoe-3.5/src
# ./configure
# make
# make install
```

Luego es necesario editar el archivo /etc/ppp/chap-secrets, elimnar su contenido y reemplazarlo por el siguiente:

```
require-pap
login
lcp-echo-interval 10
lcp-echo-failure 2
ms-dns ipdnsprimario
ms-dns ipdnssecundario
plugin radius.so
plugin radattr.so
```

Luego se edita el archivo /etc/radiusclient/servers y se introduce la IP del servidor RADIUS, así:

```
authserver radius.unimagdalena.edu.co:1812
acctserver radius.unimagdalena.edu.co:1813
```

En el servidor RADIUS se introduce la IP del servidor PPPoE en /etc/raddb/clients

```
client 172.16.0.0/16 {
        secret = mysecretpass
        shortname = servpppoe
        type = other
}
```

En el servidor PPPoE se habilita el rango de direcciones a asignar en /etc/ppp/ips con el siguiente formato.

```
10.10.1.0-255
10.20.1.0-255
```

Se crean nuevas entradas en el diccionario del cliente /etc/radiusclient/dictionary y en el diccionario del servidor RADIUS así:

```
ATTRIBUTE Download 78 integer
ATTRIBUTE Upload 79 integer
ATTRIBUTE Cliente 80 string
```

Se crean en las tablas de usuarios del servidor RADIUS los siguientes parámetros para definir grupos de asignaciones de ancho de banda.

```
DEFAULT Group = "cliente128k", Simultaneous-Use = "1"
Fall-Through = Yes
```

Download = 128

Upload = 64

Cliente = cliente

DEFAULT Group = "cliente256k", Simultaneous-Use = "1"

Fall-Through = Yes

Download = 256

Upload = 64

Cliente = cliente

DEFAULT Group = "cliente328k", Simultaneous-Use = "1"

Fall-Through = Yes

Download = 328

Upload = 64

Cliente = cliente

A este punto todo estaría listo para que ingresaran los usuarios en el servidor RADIUS

usuario Auth-Type = System

User-Service-Type = Framed-User,

Service-Type = Framed-User,

Framed-IP-Address = IPAASIGNAR,

Framed-Protocol = PPP,

Framed-Routing = Broadcast-Listen,

Framed-Filter-Id = "bo",

Framed-MTU = 1500,

Framed-Compression = Van-Jacobson-TCP-IP

Idle-Timeout = 600

Download = 128000

Upload = 128000

Para este ejemplo el usuario se le asignaría 128Kbps de ancho de banda en una sesión PPPoE que quedaría abierta hasta que el usuario la desconecte.

Cada ves que un usuario haga una solicitud el servidor PPPoE recibe y verifica la identidad contra el servidor RADIUS, si es aceptada la solicitud el servidor PPPoE identifica la sesión en un archivo de script llamado "ip-up" el cual inicia la sesión y asigna el ancho de banda según los parámetros que recibe del servidor RADIUS.

Por defecto esta negado el tráfico que pasaría a través de las dos tarjetas que posee el servidor de la siguiente manera.

Iptables –t nat –P POSTROUTING –j DROP

Es decir la política por defecto es no dejar pasar el tráfico. Pero las demás cadenas por defecto están recibiendo tráfico. Esto permite que pueda llegar la solicitud PPPoE al servidor y no sea negada.

Es por esto que cada vez que el script ip-up se ejecuta activa el enrutamiento de la estación a la que se le permitió el servicio.

iptables –t nat –A POSTROUTING –i ppp0 –j DNAT –to-source 192.168.1.1

Donde 192.168.1.1 es la IP de la interfaz que va hacia Internet.

Cuando la sesión termina se ejecuta el script "ip-down" el cual borra la entrada que establece ip-up.

```
iptables –t nat –D POSTROUTING –i ppp0 –j DNAT –to-source 192.168.1.1
```

4.4 IMPLEMENTAR USANDO PORTAL CAPTIVO.

El siguiente software es requerido para el proceso de instalación.

Iptables, ChilliSpot, Freeradius, Apache , MySQL, OpenSSL

Además, es necesario tener configurado en el kernel el soporte para tunneling y NAT. Cualquier distribución de Linux que usa kernel 2.6.x viene con estas opciones habilitadas por defecto sin embargo no esta demás verificar que estén habilitadas.

Chillispot crea una VPN, o más específicamente un tunel IP. Es por eso que el kernel debe estar configurado como módulo. El módulo se llama "Universal TUN/TAP device driver support" y se habilita así

```
Device Drivers  --->
 Network device support  --->
  <M>   Universal TUN/TAP device driver support
```

Es necesario tener habilitado el enmascaramiento IP, NAT o lo que sea necesario para dejar que los clientes de VPN puedan salir hacia Internet.

Configuración de Firewall.

Los servicios que se requieren necesitan de los siguientes puertos abiertos.

- Puerto 443/TCP al menos para la subred 192.168.182.0/24. Este es el puerto HTTPS de Apache.
- Puerto 3990/TCP para la subred 192.168.182.0/24 Este es el puerto del servidor Web de ChilliSpot.
- Puerto 1812/UDP y 1813/UDP hacia el servidor RADIUS.
- El puerto 67/USP a la VPN o la interfase tun0. Esta es usada por el DHCP de Chillispot para el registro de las direcciones IP.

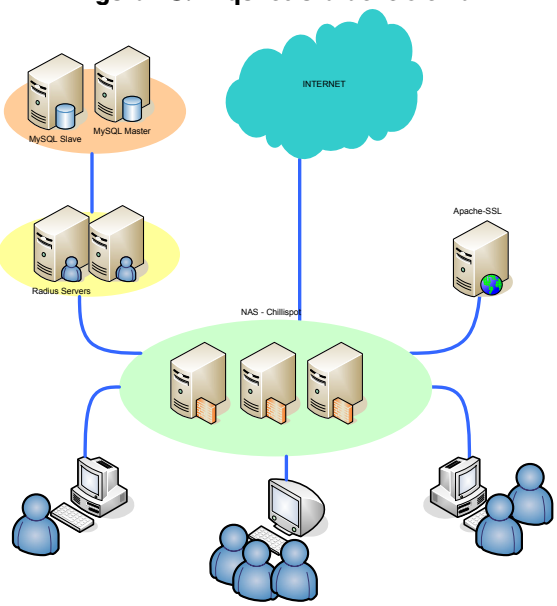
Inicialmente el tráfico no es permitido atravesar el NAS y solo se permite el tráfico hacia el servidor RADIUS o hacia el portal de la institución.

```
iptables –P INPUT –j DROP
```

Instalación del Software.

Instalar el software depende de en que servidor se esté realizando la configuración. En este caso la arquitectura propuesta implica un servidor Apache con soporte SSL, dos servidores RADIUS, dos servidores MySQL replicando, 2 NAS Chillispot.

Figura 15. Arquitectura del Sistema



El nombre de los paquetes a instalar son:

Httpd, freeradius, freeradius-mysql, openssl, Chillispot, php, mysql

Y se instala bajo la siguiente sintaxis.

yum install nombre_del_paquete

Este proceso debe realizarse como usuario root.

Configuración de Chillispot.

La configuración de Chillispot reside en un solo archivo. /etc/chilli.conf. Para un solo servidor la configuración se debe ajustar a la siguiente:

```
radiusserver1 192.168.1.253
radiusserver2 192.168.1.252
radiussecret theradiussecret
dns1 200.21.120.4
dhcpif eth1
uamallowed 192.168.182.1,192.168.1.254,www.unimagdalena.edu.co
uamserver https://192.168.1.254/cgi-bin/hotspotlogin.cgi
uamhomepage https://192.168.1.254/
uamsecret theuamsecret
```

Cada sección se describe así:

Sección RADIUS

```
radiusserver1 192.168.1.253
radiusserver2 192.168.1.252
radiussecret theradiussecret
```

Es necesario especificar dos servidores RADIUS aun si solo se tiene uno, en este Segundo caso radiuserver1 y radiuserver2 contendrán la misma dirección IP. Para este caso las IP de los servidores RADIUS son 192.168.1.253 y 192.168.1.252

```
radiussecret theradiussecret
```

La directiva *radiussecret* contiene una palabra secreta compartida con el servidor RADIUS. Esta palabra permite establecer la autenticidad de la conexión entre el NAS (Chillispot) y nuestros servidores RADIUS.

Sección de Red.

```
dns1 200.21.120.4
```

Es necesario especificar la dirección IP del servidor de nombre DNS. Esta información será enviada a los usuarios vía DHCP. Como la mayoría de los PC's en la Universidad del Magdalena utilizan IP manualmente establecidas el servidor interno DHCP que maneja Chillispot registra la información de las direcciones MAC de los computadores con sus IP, como si el mismo las hubiera asignado

```
dhcpif eth1
```

Al especificar esta directiva se debe asegurar que ésta sea de la interfaz que está apuntando a la red LAN o la red que recibe las peticiones. En cualquier caso debemos asegurarnos que no existe un servidor DHCP suministrando servicios en esa interfaz

Sección UAM

```
uamallowed 192.168.182.1,192.168.1.254,www.unimagdalena.edu.co
```

Las líneas de uamallowed separadas por comas indican que es permitido acceder a esos equipos o dominios sin tener que autenticarse. Esto evita que cuando los usuarios de la red interna de la Universidad necesiten acceder a los servicios de las misma Universidad no tengan que realizar un proceso de autenticación sin embargo tan pronto como se salga del dominio de la institución deberá autenticarse. Además debe permitirse el acceso a los DNS y al servidor que aloja el portal de autenticación.

```
uamserver https://192.168.1.254/cgi-bin/login.cgi
```

Esta línea habilita la URL de la interfase de autenticación la cual administra el registro en la red.

uamhomepage https://192.168.1.254/

Uamhomepage es la página Web a donde los usuarios serán redireccionados cuando intenten navegar a un sitio que no esté referenciado en la lista de uamallowed además permite mostrar una página en la cual se muestra información y el link para ingresar al sistema.

uamsecret theuamsecret

Existe una llave compartida entre el servidor Chillispot y el servidor Apache. Cuando se es redireccionado hacia el script de perl login.cgi. Si Estas llaves o coinciden el proceso de autenticación falla y el servidor registra usuarios con caracteres y contraseñas incorrectas. Es recomendable que nos sea la misma palabra compartida del servidor RADIUS.

Configuración de Apache.

Apache es el encargado de manejar las solicitudes de login. Apache debe poseer soporte para SSL, ya que la comunicación que se realiza entre Chillispot y Apache se cifra usando un certificado. Este servidor debe responder a la solicitud http://192.168.1.254 la cual contiene la uamhomepage definida en el archivo /etc/chilli.conf y a la solicitud https://192.168.1.254, La uamhomepage debe contiene un archive index.html que referencia información relacionada con el servicio y la institución, y además contiene un enlace hacia

http://192.168.182.1:3990/prelogin

Esta redirección apunta hacia el puerto 3990 del servidor Chillispot y a su vez redirecciona hacia el uamserver

```
https://192.168.1.254/cgi-bin/login.cgi
```

```
# cp /usr/share/doc/Chillispot-1.0/login.cgi.gz /var/www/cgi-bin
# gunzip /var/www/cgi-bin/login.cgi.gz
# chmod 755 login.cgi
```

Sólo es necesario realizar un cambio en el archive login.cgi localizando $uamsecret al inicio del archivo y el cual debe coincidir con *uamsecret* en /etc/chilli.conf.

```
$uamsecret = theuamsecret
```

Configuración Freeradius.

FreeRadius es más complejo de configurar pero siguiendo haciendo lo estos cambios nos permite funcionar adecuadamente para nuestras necesidades.
Existen varios archivos ubicados en /etc/raddb uno de ellos es /etc/raddb/clients.conf que permite configurar los NAS o chilli's que se tengan disponibles en nuestra red.

La sintaxis es:

```
client 192.168.1.100 {
 secret     = theradiussecret
 shortname  = nas1
 nastype    = other
}
client 192.168.1.101 {
 secret     = theradiussecret
```

```
 shortname  = nas2
 nastype    = other
}
client 192.168.1.101 {
 secret     = theradiussecret
 shortname  = nas3
 nastype    = other
}
```

Por cada NAS debe configurarse el cliente y el secret debe coincidir con el radiussecret de /etc/chilli.conf

EL siguiente archive a editar es /etc/raddb/sql.conf el cual viene por defecto configurado para trabajar con MySQL, solo hay que ajustarlo a los siguientes datos.

```
# Connect info
server = "192.168.1.150"
login = "freeradius"
password = "mysuperpassword"
# Database table configuration
radius_db = "3asistem"
```

El ultimo archive que requiere modificaciones es /etc/raddb/radiusd.conf. Es necesario buscar la directiva *sql* en la sección *authorize*, y quitarle el comentario

Registro.

FreeRadius viene preconfigurado para realizar registro (Accounting) y almacena su información en el directorio /var/log/radius/radacct. Sin embargo para este

proyecto se opta por almacenar la información en MySQL para lo cual en la sección *accounting* en /etc/raddb/radiusd.conf se modifica así:

```
accounting {
  unix
  radutmp
  sql
                    }
```

Es necesario remover la opción detail de esta sección para que el servidor no realice trabajos innecesarios.

Configuración de MySQL.

FreeRadius requiere consultar en su estructura predefinida las parejas usuarios, contraseñas e información de registro en MySQL. Para tal fin es necesario configurar por el cliente de MySQL nuestra estructura así.

```
> CREATE DATABASE 3asistem;
> GRANT ALL PRIVILEGES ON 3asistem.* to ' freeradius'@'192.168.1.%' IDENTIFIED BY 'mysuperpassword';
> FLUSH PRIVILEGES;
```

Luego importamos el script

```
#cat 3asistem.sql | mysql -ufreeradius -pmysuperpassword 3asistem
```

4.4.1 PROCESO DE IMPLEMENTACION

Los procesos de control de acceso y control de ancho de banda son realizados por Chillispot, pero es el servidor Radius quien define que puede permitir el NAS, como

y cuando, usando diversas directivas de diccionario. La tabla 3 referencia sólo algunas de las directivas que puede admitir el sistema, ya que el número de éste asciende a más de 4000 y siguen creciendo.

Tabla 3. Atributos soportados por Chillispot.

Atributo	Tipo	Comment
User-name	String	Usuario ingresado por l interfaz de autenticación
User-Password	String	Contraseña del usuario
NAS-IP-Address	IPaddr	Es la dirección IP del servidor NAS
Framed-IP-Address	IPaddr	IP asignada al usuario.
Reply-Message	String	Mensaje que se envía al usuario
Session-Timeout	Integer	Tiempo en segundos que el usuario puede estar en el sistema ingresado sin enviar o recibir bytes de la red.
Called-Station-ID	String	Dirección MAC del NAS
Calling-Station-ID	String	Dirección MAC del usuario
WISPr-Logoff-URL	String	Dirección URL que el usuario debe usar para salir del sistema por ejemplo "http://192.168.182.1:3990/logoff".
WISPr-Redirection-URL	String	Dirección URL a la que el usuario será redireccionado una vez ingrese al sistema
WISPr-Bandwidth-Max-Up	Integer	Máxima transmisión en bps (b/s). Limita el ancho de banda a la tasa definida en bps
WISPr-Bandwidth-Max-Down	Integer	Máxima recepción en bps (b/s). Limita el ancho de banda a la tasa definida en bps

Atributo	Tipo	Comment
WISPr-Session-Terminate-Time	String	Fecha a la que el usuario será desconectado en formato (YYYY-MM-DDThh:mm:ssTZD). Por ejemplo desconectar el 18 de diciembre de 2006 a las 7pm UTC se especifica así 2006-12-18T19:00:00+00:00.
ChilliSpot-Max-Input-Octets	Integer	Máximo numero de octetos que el usuario puede recibir
ChilliSpot-Max-Output-Octets	Integer	Máximo numero de octetos que el usuario puede transmitir
ChilliSpot-Max-Total-Octets		Máximo numero de octetos que el usuario puede transferir

Estas directivas de almacenan en la base de datos que utiliza el servicio de la siguiente manera:

Por cada usuario se debe especificar una contraseña usando User-Password en la tabla radcheck, que es la encargada de hacer los procesos de verificación o autenticación.

UserName	Attribute	op	Value
95114057	User-Password	==	Mypassword
99142514	User-Password	==	Otropass

Si se necesita autenticar la dirección MAC del usuario 95114057 se debe añadir un atributo y la tabla quedaría así:

UserName	Attribute	op	Value
95114057	User-Password	==	Mypassword
95114057	Calling-Station-Id	~=	(00-0D-AE-FF-AA)
99142514	User-Password	==	Otropass

Si se desea limitar el ancho de banda debemos hacer uso de la tabla radreply que se encarga de suministrar los servicios al usuario (autorización).

UserName	Attribute	op	Value
95114057	WISPr-Bandwidth-Max-Up	==	64000
95114057	WISPr-Bandwidth-Max-Down	==	128000

En este caso el usuario sólo podrá alcanzar 128000 bps de bajada y 64000bps de subida.

El sistema además permite asignar cuotas de consumo las cuales hacen uso de la información recolectada en la tabla radacct realizando internamente un cálculo de sumas de bytes que el usuario ha consumido. Para su funcionamiento se debe especificar en la tabla radreply así.

UserName	Attribute	op	Value
95114057	ChilliSpot-Max-Input-Octets	==	200000000
95114057	ChilliSpot-Max-Output-Octets	==	100000000

De esta forma se pueden ir aplicando diferentes directivas a los usuarios. Este mismo tipo de directivas se pueden aplicar a grupos completos en las tablas radgroupcheck y radgroupreply.

GroupName	Attribute	op	prio	Value
GrupoSalas	ChilliSpot-Max-Input-Octets	==	0	200000000
GrupoAdmon	ChilliSpot-Max-Output-Octets	==	0	100000000

Y se hace uso de la tabla usergroup para indicar que un usuario pertenece a un grupo.

Id	UserName	GroupName
1	95114057	GrupoSalas
2	95242752	GrupoSalas

4. RESULTADOS Y PRODUCTOS ESPERADOS

Este proyecto se convierte en una referencia para realizar ajustes en la red actual que conlleven al mejor aprovechamiento del ancho de banda de la Institución, ya que pone en evidencia las falencias del actual modelo de control del consumo de ancho de banda en la red y propone una alternativa aplicable bajo ciertos preceptos.

Además, se muestran los beneficios de implementar la autenticación por usuario para brindar el acceso al recurso, posibilitando la identificación del usuario que realizó una determinada acción.

Se implementó el sistema en la institución en forma silenciosa en la red inalámbrica de la Universidad del Magdalena, al momento sólo realizando los procesos de autenticación y registro en dicha red.

Aunque el volumen de usuarios no es mayor de 70, se ha podido establecer por parte de la Universidad conexiones de computadoras que no estaban físicamente dentro del Campus registradas, por lo cual se inició un proceso de verificación de las direcciones MAC, las cuales pueden ser autenticadas en conjunto con el usuario y la contraseña.

El sistema se montó en hardware embebido reciclando equipos linksys y lo adoptó la empresa Dialnet de Colombia S.A. E.S.P. que lo instaló en 7 edificios de la Ciudad donde se necesitaba asignar un total de 256Kbps de ancho de banda y existían saturaciones del canal. Se procedió a autenticar los usuarios y asignar

tasas de transferencias, brindando una mejor experiencia de navegación para los usuarios.

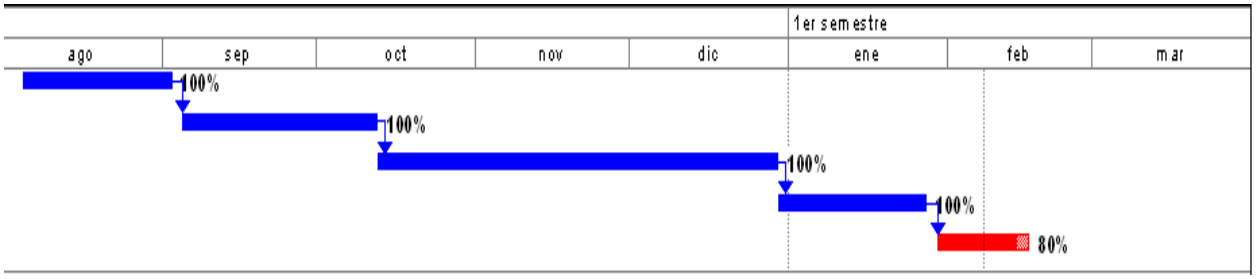
El servidor RADIUS está atendiendo 5 conexiones simultáneas con un sólo servidor de bases de datos instalado en el mismo servidor. Estas 5 conexiones atienden 160 usuarios registrados.

Se espera implementar un sistema de gestión completo que permita además de crear usuarios y consultar la información del registro, pueda crear tickets de atención a los problemas de autenticación que experimenten los usuarios del sistema, tales como contraseñas incorrectas, que ya esté conectado desde otra ubicación, que no sea su horario, etc..

5. CRONOGRAMA DE PRUEBAS

Tabla 4. Actividades del cronograma

Id		Nombre de tarea	Duración	Comienzo	Fin
1	✓	ANÁLISIS DE REQUERIMIENTOS	21 días	vie 05/08/05	vie 02/09/05
2	✓	DISEÑO DEL SISTEMA	28 días	lun 05/09/05	mié 12/10/05
3	✓	DESARROLLO	56 días	jue 13/10/05	jue 29/12/05
4	✓	IMPLANTACION	21 días	vie 30/12/05	vie 27/01/06
5		EVALUACION	14 días	lun 30/01/06	jue 16/02/06



6. PRESUPUESTO

TOTALES GENERALES	
DESCRIPCIÓN	**VALOR**
Personal	$ 27.647.120
Materiales y suministros	$ 238.600
Equipos de cómputo	$ 5.265.000
Otros servicios	$ 2.356.500
TOTAL	**$ 35.507.220**

Personal				
Proponente/ Director/ Asesor	**Función**	**Horas dedicadas**	**Valor hora**	**Subtotal**
Aquiles Cohen Llanes	Proponente	850	$ 15.000	$ 12.750.000
Hildemar Quintana Hernández	Proponente	850	$ 15.000	$ 12.750.000
Eira Rosario Madera	Director	80	$ 21.339	$ 1.707.120
Jorge Lozano Díaz	Asesor	20	$ 22.000	$ 440.000
			Total	**$ 27.647.120**

Materiales y Suministros				
Descripción	**Cantidad**	**Unidad**	**Valor Unitario**	**Subtotal**
Papel de impresión	2	Resma	$ 9.300	$ 18.600
Tinta para impresora – NEGRA	1	Toner	$ 220.000	$ 220.000

Total	**$ 238.600**

Equipos de Cómputo				
Descripción	**Cantidad**	**Origen del Recurso**	**Valor Unitario**	**Subtotal**
Computador	2	Capacidad Instalada Universidad del Magdalena	$ 2.500.000	$ 5.000.000
USB Memory	1	Personal	$ 120.000	$ 120.000
Impresora	1	Personal	$ 145.000	$ 145.000
			Total	**$ 5.265.000**

Otros Servicios				
Descripción	**Cantidad**	**Unidad**	**Valor Unitario**	**Subtotal**
Internet	725	Horas	$ 2.800	$ 2.030.000
Empaste Memoria	2	Empastada	$ 25.000	$ 50.000
Empaste Manuales	2	Empastada	$ 13.000	$ 26.000
Argollado Memoria	3	Argollado	$ 6.000	$ 18.000
Argollado Manuales	3	Argollado	$ 2.500	$ 7.500
Llamadas celular	250	Minutos	$ 300	$ 75.000
Transporte Local	150	Pasajes	$ 1.000	$ 150.000
			Total	**$ 2.356.500**

7. CONCLUSIONES

Mucho se ha demostrado acerca de los beneficios que los medios tecnológicos y el uso de la informática en particular aportan a la sociedad actual. Es indudable que la vertiginosidad del progreso no se presentaría si no intervinieran de manera directa los elementos electrónicos con los que se cuenta hoy en día. Sin embargo, la utilización de dichos medios informáticos, al ser destinados al servicio de la sociedad, requieren de una regulación estandarizada en todos los países del mundo.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnología en diversas actividades, sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquélla. En ese sentido, el presente trabajo se dirige a proveer a la institución de una herramienta administrativa de red para identificar cada uno de los usuarios de la Universidad y así determinar que posibles actores participan en hechos que perjudiquen el buen nombre del Alma Mater.

Una forma de regularlos son los procesos de autenticación ya que estos individualizan a los usuarios de los servicios, brindado a la Universidad la posibilidad de controlar dichos recursos registrarlos o monitorearlos, ayudando en los procesos de diagnósticos y seguimientos en la red.

Y las formas de realizar estas regulaciones se pueden apreciar en la siguiente tabla.

Enfoque	Ventaja	Desventajas
Aumentar el ancho de banda	. No implica cambios en la estructura actual de la red para la universidad. . Es transparente para el usuario.	. Altos costos para la contratación del ancho de banda. . Incremento de tráfico recreativo.
Adquirir productos comerciales	. Aumentar la visibilidad del trafico granular en Capa 7. . Monitoreo en Capa 7 . Herramientas de Gestión integradas. . Reportes . Actualización de las firmas de los tipos de paquetes.	. Altos costos de inversión tanto del packeteer como del la solución PPPoE. . Las actualizaciones de las firmas de identificación de paquetes son en licenciamientos a 1 año. . Implica capacitación a los

Enfoque	Ventaja	Desventajas
	. Aplicación de QoS de extremo a extremo. . Compresión de Paquetes. . Administración de ancho de banda individualmente o a nivel de agregado. . Los clientes PPPoE soportan el paso de mensajes a los usuarios sobre los problemas que presentan. . Se asignan Tasas de Transferencias y Cuotas de ancho de banda usando sesiones PPPoE. . Soporta el Modelo AAA. . La información de usuario es almacenada en bases de datos. . Soporte tecnico.	usuarios de cómo realizar la conexión. . Si se usa el cliente de Windows XP este suprime los mensajes que RADIUS enviar a los usuarios. . Los costos hacen inviable una solución redundante. .
Implementación de la solución comercial usando Linux	. Bajos costos de implementación. . Alta disponibilidad . Redundancia . Funciona sobre equipos x86. . Soporta el Modelo AAA. . Asigna Tasas de Transferencias y Cuotas de ancho de banda usando RP-PPPoE como servidor. . Maneja sesiones de usuarios.	. Implica capacitación a los usuarios de cómo realizar la conexión. . Si se usa el cliente de Windows XP este suprime los mensajes que RADIUS enviar a los usuarios. . No realiza revisión de las tramas en Capa 7. . RP-PPPoE no es un proyecto muy documentado.

Enfoque	Ventaja	Desventajas
	. Flexibilidad para la asignación de las reglas de control de tráfico.	. No existe soporte garantizado para la solución. . PPPoE no es un protocolo que implementen muchos dispositivos de red.
Implementación usando la técnica de portal cautivo.	. Independiente de la Plataforma. . http es un protocolo que todos los sistemas operativos implementan. . La configuración del cliente solo implica abrir el navegador, hacer un clic y el suministrar el usuario y la contraseña. . Permite autenticar dispositivos basados en la dirección MAC. . Soporta el paso de mensajes del servidor RADIUS a la ventana del cliente. . La comunicación de los datos de la identidad son cifrados usando certificados SSL. . Soporta el Modelo AAA. . Redundancia. . Alta disponibilidad	. No realiza revisión de las tramas en Capa 7. . La configuración involucra integrar 7 elementos independientes. . No existe soporte garantizado para la solución.

8. RECOMENDACIONES

La Universidad del Magdalena debe destinar esfuerzos en el establecimiento de políticas claras de acceso a la red y en general del uso proporcionado al ancho de banda contratado, estableciendo un marco legal que permita controlar a los miembros del Alma Mater. A partir de las políticas anteriormente mencionadas, deben establecerse las respectivas medidas técnicas y las restricciones a las que haya lugar.

Estas medidas deben incluir procesos de autenticación para el acceso a la red y la destinación de rangos o segmentos de ancho de banda de acuerdo al usuario.

Se debe hacer una fuerte ofensiva contra el mal uso de la red, se sugiere hacer concientización a los usuarios por medio de capacitaciones y controles.

Debido a que el control del tráfico de la red es uno de los puntos clave para el administrador de la misma, se recomienda implementar una solución de software como sistema3, aunque en una etapa de evolución mayor.

9. BILIOGRAFIA

Jonathan Hassell. RADIUS. Publisher: O'Reilly; 1 edition (October 8, 2002)

Using PacketShapers to control UC Berkeley IP costs

http://www.internet2.edu/qos/wg/calendar/200201-Tempe/lindahl.pdf

Campus Bandwidth Management: Approaches and Tradeoffs

http://www.internet2.edu/qos/wg/cbm/cbm-matrix.html

Campus Bandwidth Management: *What's the Problem?* Spring 2002 Internet2 Member Meeting Arlington, VA Ben Teitelbaum ben@internet2.edu May 7th, 2002

The Case for Traffic Shaping At Internet2 Schools, Internet2 Member Meeting Arlington, Virginia. May 6-8, 2002 Joe St Sauver, Ph.D. (joe@oregon.uoregon.edu) Computing Center University of Oregon

Network Quotas for Individuals –A better answer to the P2P bandwidth problem? Author: Bruce Curtis Presenter: James Ross

Bandwidth Management Strategies and Methodologies, Internet2 Spring 2002 Member Meeting Bandwidth Management, Clark Gaylord Virginia Tech cgaylord@cns.vt.edu http://rdweb.cns.vt.edu/ 7 May 2002

Internet Bandwidth Management at The University of Pennsylvania, Deke Kassabian, Sr. Tech. Director University of Pennsylvania & The MAGPI GigaPoP May 7, 2002 – Internet2 Members Meeting Campus Bandwidth Management BoF

HTB Linux queuing discipline manual, Martin Devera aka devik (devik@cdi.cz) Manual: devik and Don Cohen

Grupo Internet2, Trabajo sobre Control de Tráfico.
http://qos.internet2.edu/wg/calendar/200210-LA/200210-kassabian.pdf
Iowa State University http://www.ait.iastate.edu/policy/residence.html

Linux Advanced and Control Traffic Protocol. http://www.lartc.org

Netfilter Proyect http://www.netfilter.org

IPP2P proyect http://www.ipp2p.org

OpenSSL http://www.openssl.org

Chillispot, http://www.chillispot.org

Apache Software Fundation, http://httpd.apache.org

Freeradius http://www.freeradius.org

MySQL AB http://www.mysql.com

Linux Traffic Control - Next Generation, http://tcng.sourceforge.net/doc/tcng-overview.pdf

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source, Andrés Ricardo Almanza Junco, Junio 2004

Presentación al Consejo Distrital de Santa Marta del informe de Gestión, Noviembre de 2004.