OPTIMIZACIÓN DE ENLACES EN REDES IP. CONTROL DE TRÁFICO

Universidad Nacional de La Plata. Facultad de Informática
2009

Autor
Ing Facundo Velurtas

Director
Javier Diaz

Co-Director
Miguel Luengo

AGRADECIMIENTOS

Miguel Luengo por sus aportes de conceptos y paciencia.
Andrés Barbieri, &res por compartir su conocimiento y ayuda con problemas de Linux, programación, conceptos, etc.
Ambos aportaron ideas y equipamiento para poder desarrollar la tesis y unos buenos mates!

Motivación

La mayoría de las organizaciones privadas y públicas, tienen enlaces que conectan diferentes redes, esos enlaces pueden ser enlaces entre redes privadas y enlaces a redes públicas, caso típico Internet. Estos tipos de conexiones tienen problemáticas diferentes. La presente tesis trata estos enlaces, sin embargo tendrá más foco en las que conectan a Internet. Cuando se hace uso de la palabra "problemática" se refiere a un escenario de redes. Una de las problemáticas en las conexiones a Internet de una organización, es el "buen" uso de este recurso. Es un desafió para quienes definen políticas de uso, establecer las métricas, tecnologías que permitan su mantenimiento y perfección a lo largo de tiempo forzando un uso racional de tales enlaces. Otro desafió es proveer la tecnología que permita controlar y evitar abusos, sin llegar a ser excesivamente restrictivo [2]. Las restricciones hacen surgir definiciones como "Shadow IT" [3] que en algunos casos pueden comprometer la seguridad de una organización. En este estudio se parte de la premisa que se trata de una red académica Universitaria, con filosofía es ser "una red abierta" sin mayores restricciones, tal que suministre a los estudiantes e investigadores el escenario ideal para aprender y desarrollar sus capacidades. Las restricciones que se hacen en una red Universitaria, se hacen cuando se compromete la operabilidad de la red o usos de recursos.

Planteo del Problema

Se presenta un tema complejo ¿Cómo optimizar las conexiones de datos? Hoy en día, la mayoría de los enlaces, llevan datos sobre la pila de protocolos TCP/IP, en los cuales se montan cada vez más aplicaciones, que necesitan determinadas características para que puedan funcionar correctamente, por ejemplo: requerimientos de seudo tiempo real, determinada tolerancia en el jitter y requerimientos de ancho de banda.
Lo más usual de ver es que las aplicaciones masivas disponibles en Internet tiendan a usar todo el ancho de banda disponible, saturando los enlaces. Menciones que en la definición de IPv4 no se contemplo la calidad de servicio, con la implementación masiva a nivel mundial de IPv4 fueron surgiendo problemas a resolver, uno de ellos fue como asegurar calidad de servicios para la entrega de paquetes. Con IPv4 se logró una aproximación que sirve de base para el nuevo estándar en desarrollo de IPv6.
Podríamos considerar que el concepto de saturación de un enlace, indica buen rendimiento del ancho de banda contratado o disponible, pero esto en general no significa un uso racional del mismo. Esta saturación normalmente provoca una baja calidad de servicio del resto de las aplicaciones montadas en la red. Para cada caso particular se deberá definir que es "uso racional de un enlace".
"Usar racionalmente un vinculo de comunicaciones" es usarlo para los fines que se contrato/configuró, por ejemplo en un ámbito universitario, usar un vinculo IP para fines académicos educativos, búsqueda de información, contacto con otras universidades, etc. No debemos descuidar que la red es usada por estudiantes y profesores, que usan la red con conexión a Internet para estar más en contacto con sus familias y amigos, con aplicaciones que permiten voz y video sobre una red de datos, mensajería instantánea, mensajería tradicional (correo electrónico), etc. Estos son unos de los motivos para controlar o mejor dicho arbitrar y ordenar el tráfico en los enlaces. No esta mal que en los vínculos mencionados se utilice su capacidad ociosa, para otras aplicaciones, siempre y cuando no estorbe con los fines principales del mismo.

Cuando se hace referencia a "casos" se identifican a los diferentes escenarios que podemos encontrar en redes de Internet o privadas. Dentro de redes/enlaces privados estamos englobando redes educativas, gubernamentales, empresas privadas, empresas públicas, cada una con diferentes requerimientos, aplicaciones y recursos de redes.
Para entender la problemática deberemos tener presente cuales son las aplicaciones que usan recursos de la red. Cada una se presenta con características particulares, algunas requieren datos secuenciales, otras retardo fijo o variable, ancho de banda mínimo, etc. Aplicaciones de audio y video requieren a grandes rasgos secuencialidad, delay dentro de ciertos márgenes y baja perdida de paquetes. Mientras que aplicaciones llamadas on-line requieren bajo tiempo de respuesta, estas comúnmente son aquellas que el usuario ingresa datos o consultas y se espera la respuesta del servidor pata interactuar con el mismo. Algunas aplicaciones masivas son las conocidas popularmente con el nombre peer-to-peer o p2p (e-mule, torrent, ares,…) que en general son las responsables de saturación de enlaces. En la actualidad las redes son una combinación de aplicaciones de audio, video, voz y datos que generan nuevos desafíos tecnológicos, que hacerlos funcionar correctamente sobre una misma red, logrando convergencia de aplicaciones en un mismo medio de transporte.
En una red completamente abierta como en el caso de una red académica las aplicaciones las elige cada usuario o grupo académico, muchas veces es siguiendo tendencias o software de moda. Es muy difícil tratar de controlar y elegir las aplicaciones que deben usarse. Internet ofrece software para casi todas las necesidades, se encuentra desde software bajo licencia GNU [4] a software comercial.

Cambia la situación en empresas, donde esta mas restringido el uso e instalación de aplicaciones de software, no obstante es difícil controlar completamente que es lo que hacen los usuarios con los recursos [3].
Para poder realizar mejoras en el uso de la red, es necesario realizar las mediciones adecuadas que permitan clasificar y conocer el tráfico. Tal clasificación depende de muchos factores, algunos de los cuales están relacionados con la función de la organización/empresa y no con aspectos tecnológicos. Ese análisis debe permitir clasificar los protocolos y aplicaciones. Se define "calidad de servicio" como la forma de acomodar una red para que funcionen correctamente las aplicaciones que se deseen transportar.
La "calidad de servicio", debe seguir criterios que dependen de las aplicaciones y servicios ofrecidos. Conocer las aplicaciones es la clave para elegir las correctas calidades de servicio a aplicar. Para cada aplicación, se debe analizar como impacta en el usuario, el aumento del aumento delays (retraso o demora en castellano), descarte de paquetes, jitter, etc.

Objetivo

El crecimiento tecnológico va de la mano con el crecimiento y evolución de las aplicaciones. Con el correr del tiempo las redes de datos requieren más disponibilidad tornándose crítico para una red académica o privada. Pequeños cambios en el uso de la red pueden causar alto impacto en la misma, cuando nos referimos a impacto en general hablamos que es un impacto negativo, por ejemplo saturando un enlace o utilizando recursos asignados para otra aplicación mas prioritaria, esto aumenta el costo de operación de la red y como consecuencia una degradación de servicio.
Se pretende lograr una completa visión de la "salud" de la red, observando en puntos clave para lograr una buena administración y la calidad de servicio de la misma.

Se dará alcance a los siguientes ítems:

- Medir y clasificar el tráfico en una red.
- Detectar las aplicaciones, funcionamiento normal, congestión, fallas, cambios en el tiempo y evolución de una red.
- Rastreo y análisis en la red para identificar actividad no autorizada o actividad que provoque degradación.
- Herramientas para el planeamiento y control.

Pasos Generales y enfoques

- Colectar información sobre el tráfico y problemas en la red. Se hará un enfoque principalmente en redes con acceso a Internet para aplicarlos particularmente a la red de la UNLP y el CeSPI [26].
- Se analizaran dos clases de redes típicas, por un lado la problemática de enlaces privados, sobre la cual una organización/empresa monta su negocio o aplicaciones para el funcionamiento de su negocio y por otro lado están los enlaces de Internet puros con una problemática muy diferente.
- Se analizará una solución para optimizar el uso del ancho de banda, donde se elegirá las calidades de servicio a aplicar. Se estudiará en que casos convendrá recortar tráfico, priorizar o una combinación de ambos. Se contemplarán soluciones que surjan del análisis y consenso con los administradores de la red.

Tabla de Contenidos

1.0 Introducción

Comenzaremos el desarrollo del presente trabajo tratando de entender la complejidad que se enmascara detrás de conocer, que tráfico se cursa en una red.
La complejidad a la cual nos referimos abarca temas técnicos muy específicos, en donde cada tema llevaría a una persona, o grupo de ellas a dedicar toda la vida profesional. Pongamos el ejemplo de entender un protocolo de comunicaciones y más aun, como se combina ese protocolo con una aplicación desarrollada. Para mayor comprensión se considera requisito indispensable lectura de bibliografía sobre TCP/IP [6].
En teoría podríamos decir que comprendemos todo en cuanto a comunicaciones desde la capa 1 a la 7, pero la práctica nos ha demostrado que ante un problema real, tiene que participar en la solución un grupo de personas especializadas en alguna de las capas específicas.

Observación, en el presente documento se hará una mezcla del lenguaje castellano con algunos términos en Ingles, se hace esta convención debido a que algunos términos no tienen una traducción exacta y reemplazarlos por palabras del castellano podrían introducir algún tipo de confusión. Ejemplo, la palabra router se podría traducir como enrutador/encaminador, o como encontramos en algunos libros "enrutador de sobremesa". La palabra "sumarizacion" no es una palabra castellana pero hace referencia a un resumen en este caso de rutas , pero usar la palabra resumen no seria exactamente lo que se quiere decir , podríamos decir agrupamiento de redes, o técnicamente ver como con las mascaras de una red podemos abarcar otras redes mas pequeñas…. Sencillamente una convención.

1.1 Ejemplo de performance en una red metro-lan

Un problema típico se presenta en los enlaces de alta capacidad y alto delay; Una red LAN (capa 2 o layer 2) de 100Mpbs o más tiene un delay típico menor a 1mseg. Hoy en día es común que las empresas contraten a proveedores enlaces metro-LAN (entre ciudades), con delay típicos que dependientes de la distancias varían entre unos 3 a 8mseg, esto es muy alto para lo que están calculados los parámetros TCP de los sistemas operativos. Relacionado con este problema se encuentran las diferentes implementaciones de TCP, las implementaciones base son Reno, Tahoe, Vegas, y SACK [7].
Un enlace del 100Mbps metro-LAN o lan-to-lan como se los conoce comercialmente, de 400Km de distancia tiene unos 8mseg aprox. de delay (mseg es mili-segundos 10^-3 segundos). Hoy en día los sistemas operativos tienen implementaciones de TCP, que no están preparadas para los enlaces mencionados.
Una empresa, solicitó probar si realmente un enlace lan-to-lan, tenia en ancho de banda que figuraba por contrato, supuestamente el enlace era de 100Mbps pero observaron mediante pruebas que solo obtenían como máxima tasa de transferencia 10Mbps. El enlace metro lan tenia una distancia de 400Km. Del estudio del problema se concluyó que los enlaces son del ancho de banda contratado (a ese proveedor) y la limitación es la implementación TCP del sistema operativo de los servidores. Esto se observaba tanto en sistemas operativos UNIX como Microsoft. En los sistemas Microsoft el problema era más notorio.

Microsoft no tiene mal la implementación de TCP, sino que no están preparados para redes de alta capacidad y alto delay, los mismos están optimizados para enlace LAN de alta capacidad con bajo delay o enlaces WAN de 2 a 4 Mbps y delay típicos de 200 a 400 mseg
Derivado del problema de performance se dedujo que había que modificar valores del stack TCP/IP del sistema operativo Windows en ambos extremos, pero usando el RFC 1323.
Se calcularon los parámetros de TCP adecuados, también se le agrega la opción para que calcule automáticamente la ventana de TCP con el rfc1323. El cálculo de los valores óptimos de una ventana TCP es simple, veamos la formula teórica:

window size = bandwidth * delay

RFC1323 en sistemas operativos Microsoft

En el registro de configuración del sistema Operativo Microsoft, hay que agregar estos parámetros, que no vienen por defecto y se muestran a continuación.

Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"GlobalMaxTcpWindowSize"=dword:0003E800
"TcpWindowSize"=dword:0003E800 En hexadecimal.
"Tcp1323Opts"=dword:00000003

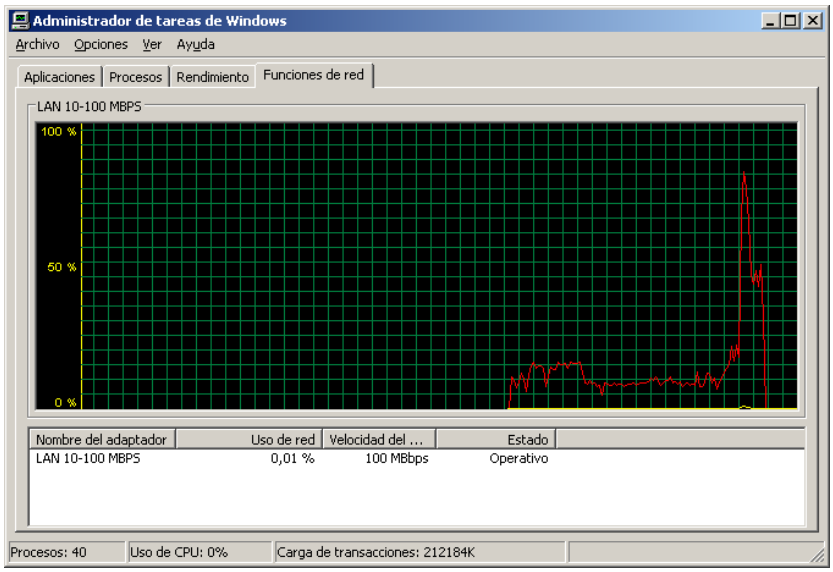
Aplicando esto en ambos extremos cliente y servidor, se obtienen mejoras notables. Cliente y servidor están en distintas ciudades en los extremos del mencionado enlace metro-lan. Las pruebas que se verán a continuación son simplemente transferir el mismo archivo completo, por ftp. Tanto el cliente como el servidor de esta prueba, están en switches marca Cisco conectados a 100Mbps y full duplex. Se uso el "task manager" del sistema operativo Microsoft para ver los resultados sin cambiar la base de tiempo, entre pruebas y usando el mismos archivo. El servidor es un "windows2003 server" y el cliente es un "windows XP profesional". El servidor tiene como recursos procesador Intel dual-core de 1,8GHz con 2GigaBytes de RAM y el cliente es de capacidades menores con procesador Intel centrino de 1,4GHz y 512Mbyte de RAM).
Se utilizo el servicio nativo de FTP del IIS [8] en un Windows 2003 server.

Primera prueba

Parámetros: Sin modificar nada del sistema operativo del cliente ni del servidor, tamaño de ventana anunciada 17500bytes.

ftp>inicio de FTP
150 Opening BINARY mode data connection for Prueba.bin.
226 Transfer complete.
ftp: 409528215 bytes enviados en 216,53 segundos **1891,31 a KB/s**. [9]
ftp>Fin de FTP

Notar en el grafico de tráfico siguiente el tiempo que tarda la transferencia y la forma del mismo.



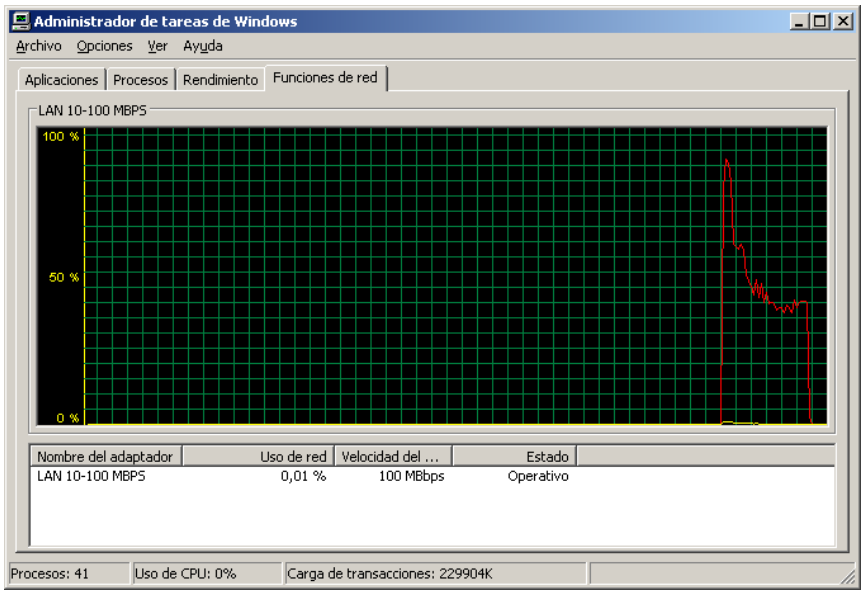
Segunda Prueba

Parámetros: Si se agregan opciones de rfc1323 solo del lado del servidor. [10]

Se repite la misma Prueba y se logra:

ftp> inicio de FTP
200 PORT command successful.
150 Opening BINARY mode data connection for Prueba.bin.
226 Transfer complete.
ftp: 409528215 bytes enviados en 68,22 segundos **6003,05 a KB/s** [9].
ftp>Fin de FTP

Ídem grafico anterior pero veamos como el mismo archivo pasa en menos tiempo, por lo tanto a mas velocidad. Observemos que el 50% son 50Mbps y el 100% son 100Mbps.



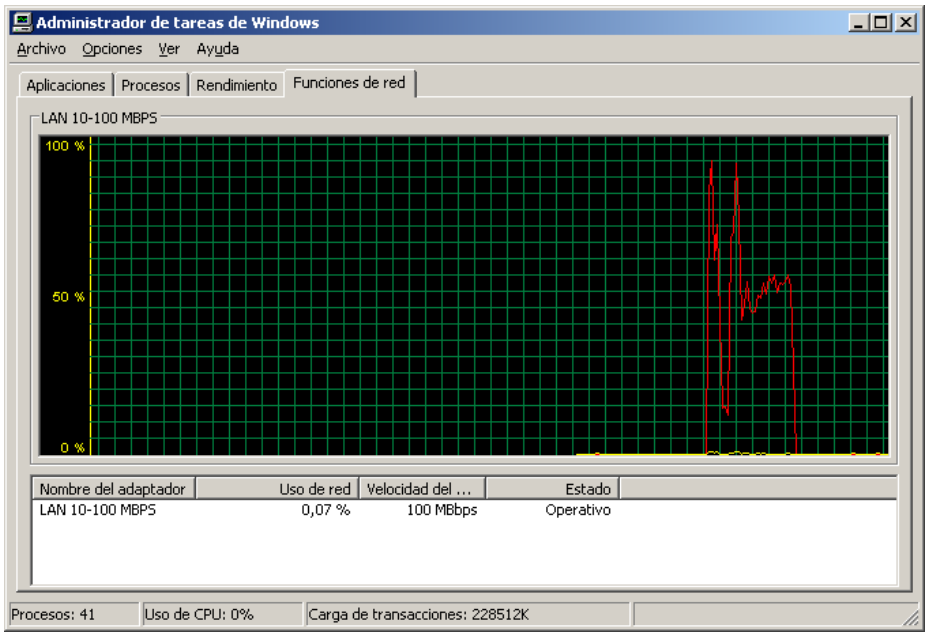
Tercera prueba

Parámetros: Se aplican opciones rfc1323 en ambos extremos (cliente y servidor)

Se logra lo siguiente:

ftp>
200 PORT command successful.
150 Opening BINARY mode data connection for Prueba.bin.
226 Transfer complete.
ftp: 409528215 bytes enviados en 62,74 segundos 6527,28 a KB/s [9].
ftp>

El servidor es el que envía los datos vía el FTP por lo tanto no varia mucho que ventana de TCP negocia y le anuncia el cliente hacia el servidor, esto se observa en el siguiente gráfico. No se capturó paquetes pero probablemente transcurridos pocos segundos del inicio de la transferencia se han perdido paquetes, obligando a retransmitir y renegociar la ventana TCP. Observar el grafico siguiente.



Esto mismo se probó con sistemas operativos Linux pero no se tomaron los datos. Con sistemas operativos Linux se lograron tasas de transferencia más parejas en 80Mbps constantes, se uso el iptraf [11] para ver las estadísticas. Normalmente los sistemas operativos Microsoft tienen una ventana de TCP de 17500Bytes, mientras que los sistemas operativos Unix 65000bytes.

Análisis de las pruebas

Para los casos de redes de alta capacidad y alto delay se debe modificar los parámetros TCP en los sistemas operativos para lograr un óptimo rendimiento. En el rfc 1323 se da con acierto solución a este problema.

Podríamos decir que las aplicaciones comerciales se desarrollan, para resolver problemas generales de la mayoría de los posibles consumidores (de estas aplicaciones), o simplemente los desarrolladores de software saben mucho de programación, pero usan en forma muy ineficiente los recursos de comunicaciones.

1.2 Netflow - sFlow

Recordemos el objetivo de este trabajo, es saber "quien, como, donde, cuando y ¿porque?" se usan los recursos de una red. Conocer lo puntos mencionados, nos permitirá tomar decisiones, resolver problemas, planificar el crecimiento de una red, dimensionar, distribuir y administrar recursos.
Distribuir y administrar recursos de la red, debería estar alineado con una "política" definida. Cuando hablamos de "política" hacemos referencia a las normas/pautas en cuanto a seguridad, distribución de recursos para aplicaciones y usuarios.
Una "política" puede ser totalmente distinta según el ámbito en que se la defina. Las políticas se definen en referencia al contexto en que se las pretenda aplicar. Estas definiciones no tienen porque ser iguales. Una empresa financiera, una industria, un banco o ámbito académico, tienen requerimientos distintos, por lo tanto las políticas en general son diferentes. Por ejemplo un banco va a pretender extremar las medidas de seguridad, evitando incidentes informáticos, también va a pretender que sus sistemas tengan las mas alta disponibilidad, estabilidad y seguridad, con lo cual van a tener muchas medidas de control y políticas rígidas.
Una industria va a pretender que no se divulguen sus secretos industriales. Así cada ámbito en el que este montada una red va a tener sus particularidades y definiciones especificas, a ese conjunto lo llamaremos "Políticas de una red".
Una "Políticas de una red" en comunicaciones busca básicamente objetivos comunes de seguridad, privacidad, control de usuarios, accesos, alta disponibilidad, calidad de servicios. La aplicación de estas medidas, estará fuertemente ligada a la disponibilidad de recursos económicos con los que se cuente para implementar una red.
Nos basaremos en un nuevo estándar de la IETF que se denomina sFlow, un consorcio de empresas desarrollando un estándar en muestreo de tráfico en equipos de comunicaciones, switches y router. Existen actualmente dos estándares, sFlow y netflow ambas son tecnologías de análisis de tráfico.
Netflow es una tecnología de Cisco y sFlow de un consorcio de empresas. Ambas tecnología tienen puntos en común, el mas importantes es que los servidores de monitoreo de tráfico están dentro de los equipos de comunicación, implementados en hardware y software, estos es una ventaja, ya que al estar dentro de los equipos de red, pueden ver todo el trafico cursan.

Tanto netflow como sFlow, son de un modelo cliente-servidor, que típicamente hay clientes uno o dos por red, mientras que servidores puede haber tantos como equipos de comunicaciones existan (en una determinada red). Los servidores son llamado agentes, estos "agentes" reportan el tráfico monitoreado a un cliente llamado típicamente "colector de datos". El colector, simplemente almacena lo que envían los agentes, en una base de datos. Luego esa base de datos es interpretada y accedida por otros procesos que analizan esa información para buscar datos específicos, hacer estadísticas de tráfico, etc.

Leyendo e interpretando esa base de "base de datos" base de datos podremos conocer las preguntas que se enumeran abajo:

- ¿Quién esta usando la red?
- ¿Para que la están usando?
- ¿Se cumplen las políticas de seguridad?
- ¿Cómo puedo detectar fallas de seguridad?
- ¿Hay actividad no permitida en la red?
- ¿Hay alguna anomalía? ¿Que la provoca?
- ¿Por qué una aplicación o servidor es lento?
- ¿Es problema de la red?
- ¿Es problema del servidor o de la aplicación?
- ¿Se pude controlar los recursos de red y la distribución de los mismos?
- ¿Cómo impacta una aplicación en la performance de la red?
- ¿Es posible voz sobre IP o video sobre IP en la red? ¿Como funciona?
- ¿Hay transferencias de archivos entre usuarios en la red?
- ¿Hay virus en la red?

Estas son algunas de las preguntas y necesidades que justifican el origen y desarrollo de estas tecnologías de monitoreo de tráfico o visualización de red.-

2.0 Globalización de las comunicaciones

2.1 Internet

A continuación presentamos una reseña cronológica de avances de la red Internet y sus servicios.

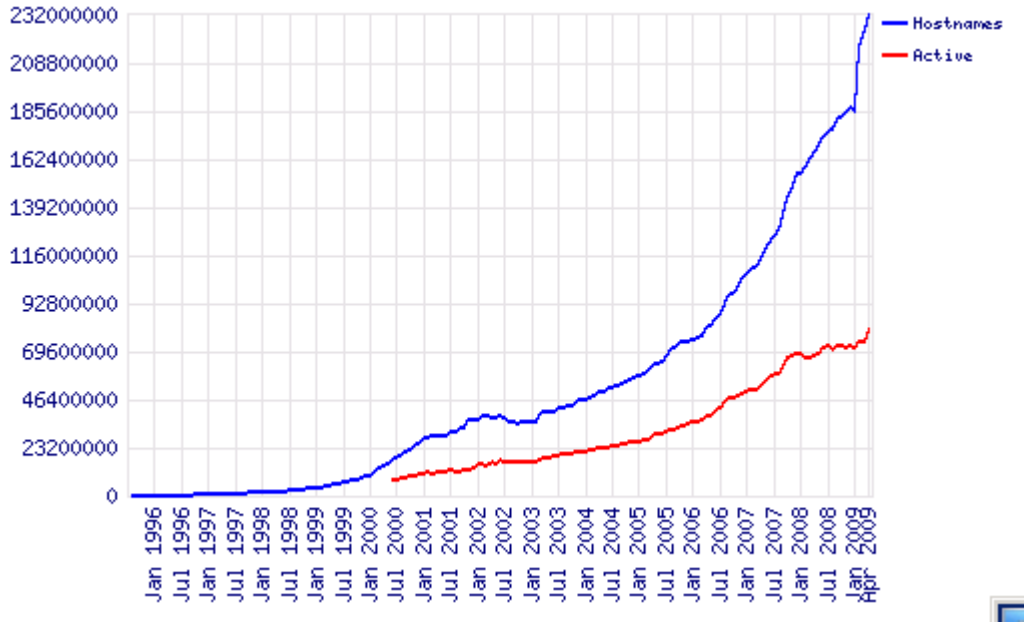
Años 1970: los comienzos. ARPAnet, pruebas de IP/TCP. Aplicaciones: pruebas de protocolos.
Años 1980: el paso a la estabilidad. NFSnet, integración con BSD Unix, nace la "comunidad Internet". Se comienza a usar los protocolos IP/TCP. Aplicaciones: uso a gran escala de correo electrónico, ftp, telnet y news.
Años 1990: se hace universal. Aparecen los de proveedores de Internet conocidos como ISPs (Internet service providers). Aplicaciones: el WWW integra casi todo. Se afianza el desarrollo de sistema de nombre para independizarse del direccionamiento IP conocido como DNS o "domain name system".
Años 1999: Se comienzan desarrollarse algunos motores de búsqueda e indexación en Internet, muchas empresas comienzan a crear sus páginas Web, presentando sus productos ofreciendo servicios.
Años 2004: Antes de este paso ocurrieron muchas mejoras a nivel de escala de integración de componentes electrónicos, esto significa que se desarrollaron componentes electrónicos cada vez más pequeños, estos componentes son de estado sólido. Este avance permitió el desarrollo de computadoras más pequeñas y de fácil producción. Evolucionaron dos o tres tipos de arquitecturas de procesadores, los llamados SISC, con muchas instrucciones resueltas por hardware, estas hacían la programación simple, pero programas menos eficientes; otra línea de procesadores, con programación laboriosa, pero extremadamente eficiente se los conoció RISC. Surgieron paralelamente muchas empresas y lenguajes de programación cada vez más complejos. Se desarrollaron equipamientos de seguridad conocidos como firewall, se fueron perfeccionando los

router y los switches de conectividad en Internet. Aparecieron aplicaciones de telefonía IP, video y streaming de radios comerciales. La introducción de la criptografía/cifrado a nivel digital, permitió en la actualidad las aplicaciones de comercio electrónico y home banking.
La evolución es impresionante y seria tema de otro trabajo recopilar e investigar sobre los avances que se han suscitando desde las primeras pruebas de interconexión, hasta las redes actuales. Si bien la tecnología y velocidades de interconexión han evolucionado, el concepto no ha cambiado mayormente y si uno presta atención a detalles, la comunicación conservar rasgos similares a lo que necesita para entenderse un humano con otro, cuando se encuentra cara a cara.
La maravilla del mundo Internet es la "visibilidad", de casi todos los puntos del planeta que cuenten con una infraestructura básica de tecnología, quedan excluidos muchos países donde la extrema pobreza y necesidades básicas hacen que esta tecnología no tenga importancia alguna.
Hace 30 años era muy difícil la comunicación, tener contacto con personas al otro lado del planeta como Rusia, Europa o Singapur, era muy dificultosa y lenta. Entiéndase como "comunicación" al intercambio de cualquier tipo de información desde información científica, profesional hasta afectiva. Los miles de Km. que tenia que viajar la información en "papel" demoraba horas y días. En la actualidad algunas aplicaciones sobre TCP/IP han transformado esos miles de Km., en pocos mili segundos (1seg=1000mseg o 1seg x 10^-3) la actual velocidad y capacidad de los enlaces permite transferir volúmenes información en pocos segundos. Alguna de esas aplicaciones son el correo electrónico, FTP y las nuevas aplicaciones del tipo P2P (peer to peer).Estos protocolos permiten la transferencia de información.
Hoy Internet ha generado una transformación en la sociedad, los más jóvenes que han nacido con esta tecnología raramente conozcan que es una estampilla postal o ponerle el remitente a un sobre de papel, mientras que las personas de mayor edad se han ido adaptando. Hoy en día personas de 50 años edad o más, han aprendido a usar aplicaciones básicas, como correo electrónico, paginas Web, etc., personas que nunca en 50 años han tocado una PC hoy en día con una breve introducción comienzan a usar estas aplicaciones.
Aplicaciones como las conocidas como p2p, se usan para compartir información. Los software p2p, tiene la funcionalidad de comportarse como clientes y como servidores e incluso como transito. Permiten compartir archivos. Si bien están diseñadas para compartir archivos, ofrecen también cierta seguridad para evitar el espionaje o robo de información no deseada. Estas aplicaciones tienen algunos potenciales baches de seguridad, en artículos "Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network That Never Forgets" [14] y "Exploiting P2P Systems for DDoS Attacks" [15], se describen como son potencialmente vulnerables estas aplicaciones.

2.2 Impacto social de Internet

Algunas líneas de pensamiento sostienen, que Internet se diseño inicialmente como una forma para controlar y auditar las comunicaciones, una forma estratégica de lograr supremacía económica, social y política. Más allá de estas cuestiones, el desarrollo de Internet permitió compartir y divulgar información.
La red de Internet adquirió dimensiones poco imaginables al momento de sus inicios. Internet sigue en crecimiento observemos estadísticas al respecto.
Las estadísticas que mencionaremos a continuación fueron obtenidas de Internet World Stats [16] y de Netcraft [17].

Para notar el crecimiento veamos como fue creciendo el de Internet citemos el siguiente grafico, en el cual se observan el total de dominios dados de alta de Internet, las estadísticas van de agosto 1995 a abril 2009



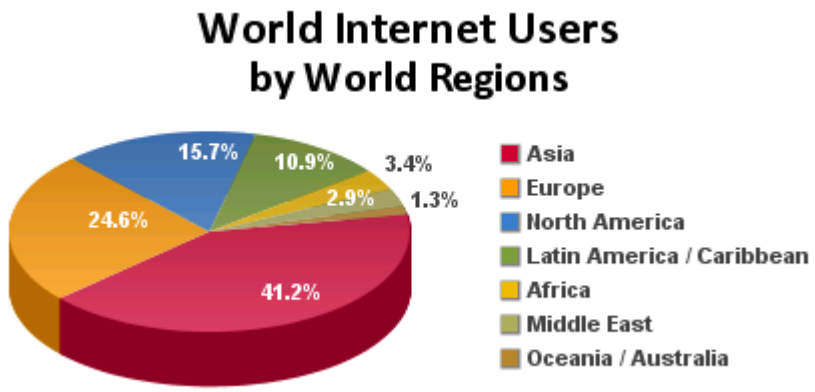
Estadísticas de Netcraft a la fecha, indican que en Internet se ha alcanzado los 600000 sitios Web seguros, cifrado con SSL [18]. Los sitios seguros, son usados para comercio electrónico, banco en línea o home banking, servicios financieros, etc. Las compañías que tienen páginas Web seguras, pretenden proteger la integridad de los datos y autenticidad de los mismos.

La tabla a continuación colecta datos de usuarios en Internet divididos por continente

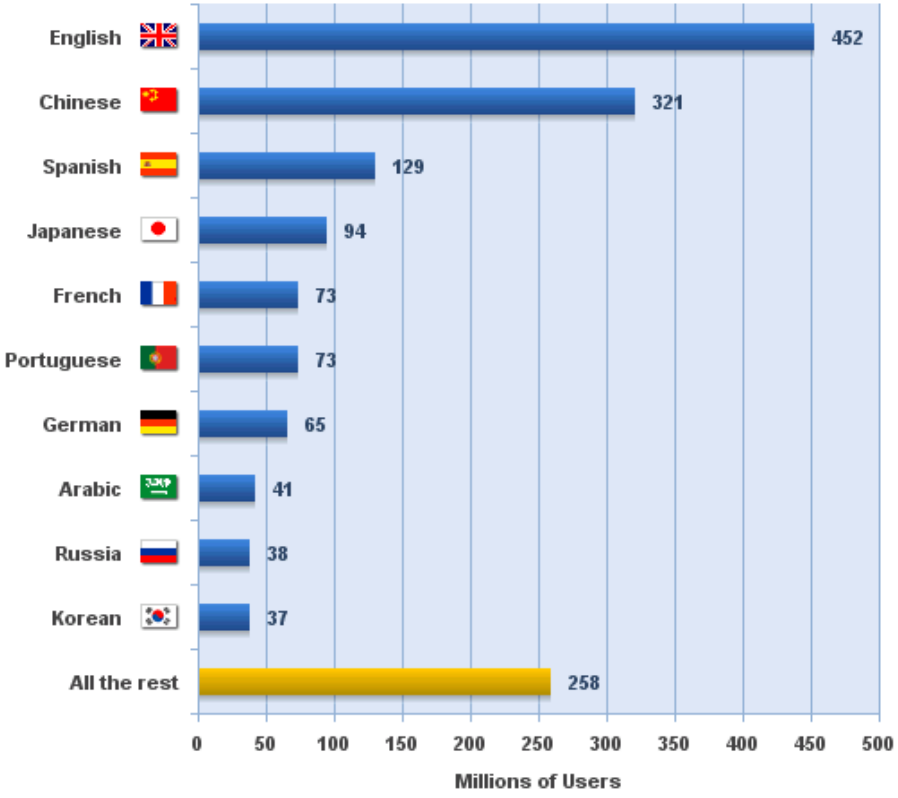
WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2008 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Users Growth 2000-2008	Users % of Table
Africa	975,330,899	4,514,400	**54,171,500**	5.6 %	1,100.0 %	3.4 %
Asia	3,780,819,792	114,304,000	**657,170,816**	17.4 %	474.9 %	41.2 %
Europe	803,903,540	105,096,093	**393,373,398**	48.9 %	274.3 %	24.6 %
Middle East	196,767,614	3,284,800	**45,861,346**	23.3 %	1,296.2 %	2.9 %
North America	337,572,949	108,096,800	**251,290,489**	74.4 %	132.5 %	15.7 %
Latin America/Caribbean	581,249,892	18,068,919	**173,619,140**	29.9 %	860.9 %	10.9 %
Oceania / Australia	34,384,384	7,620,480	**20,783,419**	60.4 %	172.7 %	1.3 %
WORLD TOTAL	6,710,029,070	360,985,492	**1,596,270,108**	**23.8 %**	342.2 %	100.0 %

Los números son un reflejo de las condiciones de pobreza como en África, donde se indica un crecimiento de 1100% pero el uso y acceso al recurso de Internet los posiciona en poco menos del 6%.

El Siguiente grafico veremos la distribución de usuarios de Internet



Los idiomas más usados para comunicarse en Internet



Estadísticas de este estilo nos permiten con números, tener una idea clara del crecimiento de Internet. También existe un crecimiento de redes privadas, de esto no se han encontrado estadísticas concretas, pero no es difícil imaginar, que las tecnologías que se usa en Internet se apliquen y usen en redes privadas. En general cada empresa de mediano a gran tamaño, cuenta con una red privada, esta puede ser más o menos compleja dependiendo de su tamaño, quizá buscando en la cantidad de empresas de mediano a gran porte podamos inferir números y estadísticas para redes privadas, pero a la fecha no se encuentran datos objetivos en la web.

En principio las redes eran militares, luego se probaron conectando Universidades.
La historia de la humanidad señala que el que contaba con mejor tecnología y aplicaba buenas estrategias de dominación tenía ventajas de acomodar las cosas en su favor. Ciertas líneas de

pensamiento sostienen, que Internet fue creada para controlar las comunicaciones y proveer tecnología al resto de los países pata obtener incalculables réditos económicos. La Fuente de esta línea de pensamiento fue escuchada en una conferencia de una universidad Española, publicada en Internet **[19]**. Pero esto no pudo haber tenido éxito sin un real impacto en las sociedades. La sociedad o mejor dicho usuarios fueron encontrando utilidades, se fueron desarrollando utilidades y servicios en torno a Internet. Ha generado muchos avances en las carreras Universitarias, por ejemplo logrando mejor acceso a la información, muchas cosas dejaron de ser un misterio. También se puede obtener mucho más rápido información, noticias, difusión de ideas, foros de discusión, reservorio de datos técnico, sociales, bibliografía, distribución de software, todo en cuestión de instantes, hasta espacio físico para almacenamiento de información. Esta tendencia permitió financiar mejoras en las comunicaciones y en la infraestructura de Internet, logrando un avance permanentemente. Evolucionaron los sistemas operativos y aplicaciones sobre los mismos.
Con el crecimiento mencionado se crearon nuevas necesidades, una de ella fue poder analizar el tráfico de datos, para planificar o remediar problemas. Los volúmenes de información (tráfico de datos) se hicieron tan grandes que comenzó a hacer falta el desarrollo de herramientas de análisis más eficientes y con otro enfoque. Así nacieron dos tecnologías como Netflow y sFlow, en mi opinión creo que estas dos tecnologías van a estar casi óptimas en cuanto a su desarrollo recién en 10años, y si no cambia la dominación del mercado, en mi opinión personal sFlow tenderá desaparecer o limitarse solo a áreas de desarrollo e investigación. Mas adelante en este trabajo se va a profundizar en este tema.

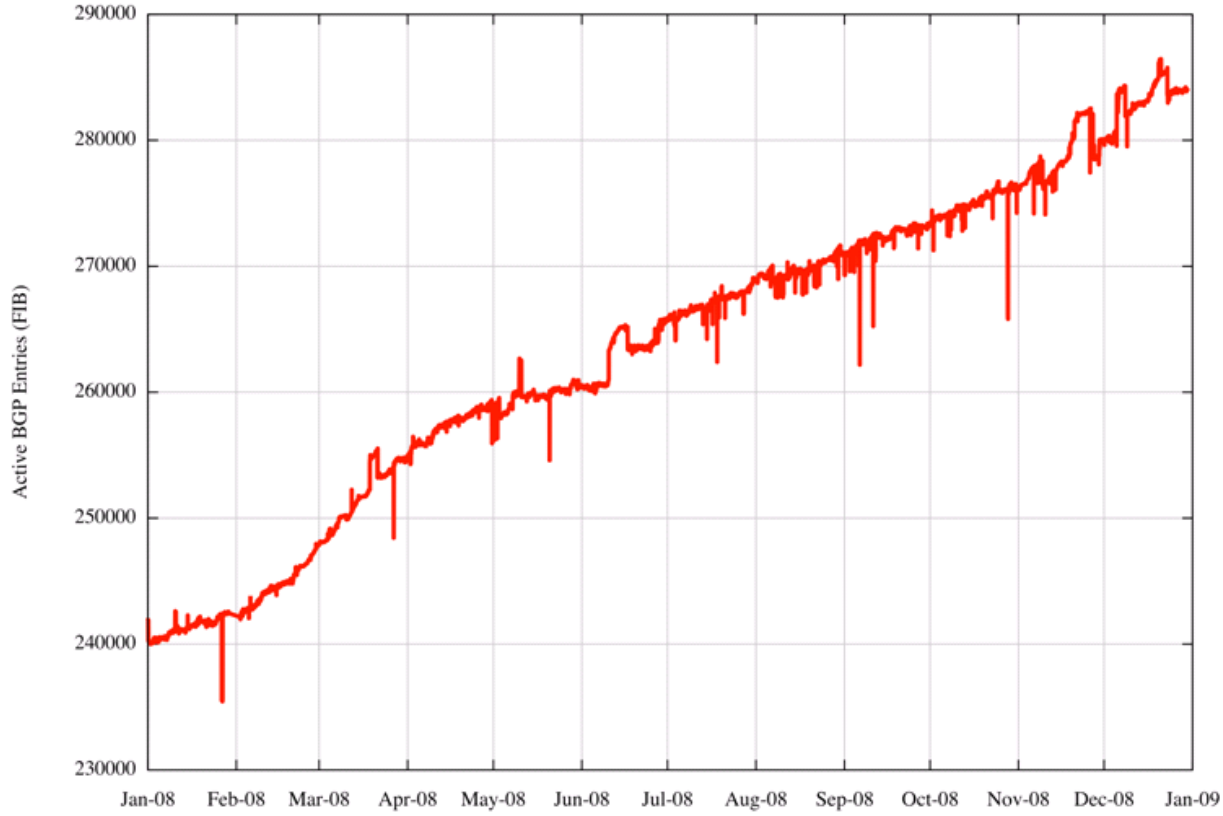
3.0 Estructura de Internet y tecnologías de transmisión

Los medios de transmisión utilizados son muy diversos, existen una cantidad importante de tecnologías para transmitir “bits”, sobre pares de cobre, coaxial, fibra óptica, enlaces radioeléctricos, satélite, etc. Los medios mencionados transportan “bits” entre equipos terminales que usan TCP/IP, si bien hay otros protocolos de comunicaciones, nos enfocaremos a TCP/IP. Los medios de transmisión, convierten la los bits a un formato adecuado a sus tecnologías, estos conversores se llama MODEM, porque modulan una señal y luego las demodulan para dejarlas en sus estado original, transportándolas así de extremo a extremo.
Técnicamente la estructura de Internet puede definirse como: redes de área local interconectadas por routers.
Internet esta compuesta por miles de ISP “Internet service provider” o en castellano “proveedores del servicio de Internet”, interconectados entre si.
Cada ISP tiene un AS (Autonomous Systems) un AS o mas, es un número que identifica al ISP, esos AS tienen delegada la administración de un rango de direccionamiento IP. El direccionamiento se debe solicitar a entidades de Internet, que se agrupan por área geográfica se puede observar en la organización Iana [20].
Veamos como se dividen los RIR Regional Internet Registries y sus áreas de cobertura

- AfriNIC África
- APNIC Asia/Pacífico
- ARIN América del norte y latín anglo parlantes.
- LACNIC América latina e islas del Caribe
- RIPE NCC Europa y Asia Central

Existe en Internet una organización que administra el direccionamiento IP y asignación de dominios, se llama ICANN (Internet Corporation for Assigned and Numbers) [21].
La gestión del direccionamiento se delega en cinco RIR "Regional Internet Registries", indicado en el cuadro y mapa previos. Existe una jerarquía de direccionamiento, la ICANN asigna a los RIR de al menos direccionamiento mascara de 8 bit, los RIR asignan direccionamientos menores a 20 bits a los LIR que son los ISP, los ISP asignan a usuarios finales esas direcciones en mascaras mucho menores. Los LIRs o ISP son los responsables de la asignación del direccionamiento a usuarios finales. Los ISP cuentan con un número AS "sistema autónomo" que fue asignado por el RIR regional.
Los IPS usan en común el mismo protocolo de ruteo, llamado BGP "Border Gateway Protocol" que permite a dos ISP que intercambien las direcciones IP, que son accesibles detrás de cada uno de ellos. El protocolo BGP es el encargado de anunciar las rutas en Internet. Existen dos tipos de acuerdo de interconexión, el primero es para publicar la tabla completa de rutas de Internet (full-table) a otro ISP, el ISP que publica toda la tabla se convierte en "operador/proveedor de transito", el segundo tipo de interconexión dos ISP solo anuncian las direcciones propias, normalmente se llama peering.
Una forma en la que los ISP se conectan es usando puntos de interconexión, llamados NAPs "Networks Access Points" o IXPs "Internet Exchange Points", el uso de los NAPs es para bajar los costos de Interconexión ya que hacer acuerdos de peering es muy económico si es en una misma LAN. La otra forma de interconectarse es tener un enlace "punto a punto" entre los ISP pero es más costoso. Los NAPs son organizaciones que proporcionan espacio físico, energía, acondicionado del espacio, seguridad física e infraestructura LAN, para la interconexión.
En la url: *www.pch.net/ixpdir/Main.pl* encontraremos el listado de los Naps y algunas estadísticas de tráfico y cantidad de interconectados. Un NAP de Argentina es CABASE.
Los acuerdos de peering entre ISP son simplemente acordar que redes se van a publicar y si van a servir de transito.
BGP actualmente es versión 4, que solo trata con direccionamientos, no abarca QoS "quality of service" en castellano "calidad de servicio", BGP solo provee conectividad tratando de minimizar los cambios para lograr estabilidad y evitar bucles.
Actualmente la tabla de ruteo completa de Internet es mas de 280000 rutas esta es la full-table que mencionamos. La tabla completa tiene la información de todos los destinos en Internet. Surge un cuestionamiento de ¿porque un ISP necesita la tabla competa de ruteo? este tabla se usa cuando un proveedor tiene mas de un vecino BGP o acuerdo de interconexión, con esa tabla se podrá elegir la mejor ruta y lograremos mayos visibilidad a Internet. Los proveedores de transito pueden manipular las rutas en Internet, mejorando o empeorando propiedades de cada ruta.

El gráfico siguiente se observa el crecimiento de las rutas publicadas en Internet desde 1994 al 2009, gráficos y estadísticas sobre el comportamiento de BGP en Internet se pueden obtener de Potaroo [22].



Los medios de transmisión han seguido el crecimiento de la tecnología, hace unos años un enlace de 2Mbps o 1,5Mbps, E1 en norma Europea y T1 en norma EEUU respectivamente y múltiplos de ellos eran considerados enlaces WAN de alta capacidad. Los enlaces para larga distancia, típicamente usan/usaban protocolos de transmisión derivados de RS232, como el HDLC o protocolos que encapsulan en Frame-Relay, este tipo de tecnología de transmisión se usan en enlace WAN Wide Area Network.
Los enlaces se los agrupa generalmente en los tipo LAN "Local Area Networks" se usa para redes locales y los WAN para interconectar redes LAN a mayores distancias.
Hoy en día ha aumentado la capacidad de los enlaces y se han hecho económicamente más "accesibles". Los enlace de 2Mbps se han reemplazado por enlace que antes eran considerados LAN, como el Ethernet, usándose como enlaces WAN, típicamente de 10Mbps, 100Mbps y 1000Mbps (M = Mega= 10^6) llamados "Metro Ethernet", "Metro LAN" y comercialmente como "lan-to-lan". La transmisión de los lan-to-lan son generalmente en fibra óptica.

Una de las formas de transmitir los datos puede ser sobre plataformas SDH, Sonet, transportados sobre tecnologías DWDM []; esto puede ir combinado con enlaces ATM (evolución del Frame-Relay que se esta dejando de usar). Los proveedores de conectividad física se los conoce como "Carrier". Existen numerosas tecnologías de transmisión de datos y su uso depende del punto del enlace que nos encontremos, en general no es la misma tecnología que se usa para un acceso a Internet, que la empleada para mayores volúmenes de tráfico o en distancias grandes.

La velocidad de acceso a Internet (al día de la fecha de inicio de este documento) va variando de unos pocos kbps para enlaces domésticos, a enlaces de 10 a 100Mbps en medio físico Ethernet para empresas que cuentan con medios económicos para afrontar el costo. Accesos con tecnología xDSL para enlaces domésticos o empresas con menores recursos. Los xDSL pueden ir desde pocos Kbps a 24Mbps y evolucionando con el paso del tiempo. Los "xDSL" es el nombre de un grupo de tecnologías que transportan señales digitales de alta velocidad sobre pares trenzados de cobre, esos pares de cobre normalmente son los mismos pares telefónicos de una casa, la tecnología mas conocida e implementada es el ADSL la "A" de se asimétrico, esto significa que las velocidades de subida y bajada no son las mismas.
Lo que permitió la evolución de Internet fue que casi todos los proveedores de equipos de comunicaciones y software trataron de basar sus desarrollos en estándares. Algunos estándares fueron "de facto" impuestos por los fabricantes que tomaron la delantera en lo tecnológico y otros muchos fueron desarrollados en base a acuerdos comerciales y políticos, basados en estrategias de dominio tecnológico.
La "popularidad" en el uso de esas normas y protocolos fue decisivo en la supervivencia y evolución de determinada tecnología, determinados protocolos y determinados formatos.

4.0 Características generales de TCP/IP

4.1 El protocolo TCP/IP

La tarea del protocolo TCP/IP es transmitir paquetes de datos desde la máquina origen a la máquina destino. Esas maquinas que mencionamos normalmente con computadoras y servidores. Todo paquete IP tiene un formato y estructura fija, dentro de él se encuentra la "dirección origen" desde la cual salio el paquete y la "dirección destino". La "dirección destino" permite a los diferentes router tomar la decisión para orientar ese paquete. Dentro del paquete IP hay muchos campos, cada uno con su función especifica. Cuando las maquinas pertenecen al mismo direccionamiento IP (red y marcara iguales) se comunican solo con el protocolo de "capa 2", que usa la "mac-address" "Medium Access Control address" para llevar los paquetes de una maquina a otra. Aparecen en escena los switches y los hubs, los primeros son la evolución de los hubs. Los switches usan esas mac-address para transportar los paquetes por un camino único (en condiciones normales) entre dos o maquinas, en cambio los hubs, son simplemente amplificadores que copian el tráfico entrante en todos sus puertos.
En la actualidad los switches tienen puertos Ethernet de 10/100/1000Mbps dependiendo del costo de los mismos y de los modernos que sean, también existen switches con puertos de 10Gbps pero por el momento reservados para con otros switches. Los hubs solo tienen puertos de 10/100Mbps, estos equipos ya están quedando en desuso.
Cada maquina o computadora necesita un medio para conectarse a la red normalmente usa "placas de red" que pueden ser Ethernet de 10/100/1000Mbps por pares de cobre o inalámbricas del estándar WIFI.
La palabra mac-address es un identificador único de cada "placa de red" que consta de un numero de 48bit, cada fabricante de placas Ethernet tiene un rango asignado, con lo cual los 24bit mas significativos identifican al fabricante. Pero la mayoría de las placas de red Ethernet y wireless modernas, permiten modificar la mac-address manualmente.

La versión actualmente en uso es IPv4, existe otra versión en desarrollo IPv6.
IPv6 que es la evolución de IPv4, mejora cosas que no se tuvieron en cuenta cuando se creo el estándar de IPv4, digo que no se tuvieron en cuenta no por falta de visión sino porque era muy difícil de imaginar en los comienzos, la dimensión que tomaría Internet. Algunas de las cosas que mejoró la cantidad de bits reservados para direccionamiento IP.
El direccionamiento se divide en cinco clases A, B, C para tráfico unicast y D para Multicast, la clase E aun esta sin definir.

Clase	**Red**	**Mascara**
A	1.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255

La comunicación "unicast" se refiere a cuando dos direcciones IP, se comunican solamente entre si. Una red se define por la dirección IP y la mascara, con estos dos valores se obtiene la dirección de red y la dirección de broadcast para esa red.
Broadcast es una dirección en la que en condiciones "normales" se transmiten servicios que todos deben escuchar dentro de la misma red. "Multicast" se usa para una comunicación desde una sola dirección IP origen a una dirección IP de multicast, el multicast es solo tomado solo por los que están escuchando en esa dirección.
En una red LAN de capa 2, el multicast es visto como broadcast porque a menos que hagamos filtros se distribuye por toda la red. Las direcciones de multicast permiten se rutean en router de capa 3. Típicamente el multicast se usa para transmisiones de video dentro de una red, para no generar un flujo de tráfico por cada uno que quiera ver esa transmisión.

4.2 Ruteo

Los routers encaminan o ruteando esos paquetes IP fijándose en la dirección IP destino, también hay router que tienen la capacidad de rutear en base a la dirección IP origen, se lo conoce como "source routing". Los routers utilizan sus tablas de ruteo. Las tablas de ruteo de los router, son "base de datos" que está cargadas en la memoria RAM de los mismos. Esa base de datos se puede actualizar dinámicamente o estáticamente de pendiendo de la estrategia de ruteo elegida por los administradores. Las entradas en esas "tablas de ruteo" o "base de datos" contienen básicamente dirección de red de destino y próximo salto (dirección IP) pero también puede contener datos adicionales para que el router use o publique rutas. Esos datos adicionales se usan hacer elección de la mejor ruta.

Existen varios mecanismos o sistemas de ruteo para actualizar las tablas:

- *Ruteo estático*: típicamente usado sólo en los extremos de la red o en nodos terminales.
- *Ruteo dinámico*: los routers intercambian información que le permitirán llegar a destinos, evitar bucles, elegir rutas con mejores métricas. Las métricas es información extra que usan protocolos de ruteo, para ingresar en una formula y hacer una ponderación de las rutas que van aprendiendo. Los protocolos de ruteo más conocidos son RIP, OSPF, EIGRP, IGRP, IGP, BGP, IS-IS entre otros.

Hay dos grandes divisiones en los protocolos de ruteo, aquellos diseñados para usar dentro de un sistema autónomo y otro para usarse entre sistemas autónomos. Los diseñados para usar dentro de un mismo sistema autónomo son el RIP, el EIGRP y el OSPF entre otro. Los diseñados para ruteo entre diferentes sistemas autónomos son típicamente BGP, típicamente usando en Internet. También existe el iBGP que se usa para conexiones dentro de un mismo sistema autónomo.

4.3 Garantías y Calidad de Servicio

IP sólo garantiza best effort, aunque con diversas técnicas se puede "asegurar" cierta calidad de servicio. Son soluciones basadas en el marcado de paquetes o en la lectura de cierto contenido dentro del paquete IP.
El método más básico es leer la IP origen o destino para tomar una decisión, pero existen otras técnicas que se usan para dar mas flexibilidad, una de ellas consiste es leer el campo TOS o DSCP "Differentiated Services Code Point" del paquete IP.
Esto tiene el problema debido a que debe existir un acuerdo entre proveedores, para acordar como marcar los paquetes y que tratamiento darle a los mismos. No hay una forma única de marcar esos paquetes y no hay acuerdo global para el tratamiento de los mismos y si lo hubiera seria muy fácil violar el acuerdo, marcando los paquetes en forma "ilegal", de tal manera que el proveedor siguiente confunda el tráfico. Tendría que haber un control más para que los paquetes no sean modificados, eso existe, pero quitaría flexibilidad, dejando en manos de las aplicaciones modificar a gusto el campo DSCP, lo cual también seria poco conveniente y fácil de vulnerar por parte de la aplicación. Llamamos "aplicación" a un software que se comunica con otro por medio de la red.

La nuevas técnicas de calidad de servicio sobre IPv4 comúnmente llamada "QoS" quality of service se basan en un modelo de colas. El más moderno se denomina CBWFQ, seria la evolución de viejas técnicas de priorización, solo mostraremos un diagrama básico ya que este tema es muy extenso y podría ser encarado para su comprensión a fondo en un libro o tesis al respecto tema de estudio.
Demos una recorrida por las definiciones de estrategias de calidad de servicio de la empresa Cisco Systems, similares estrategias tienen los principales proveedores de equipos de comunicaciones. El tema es por demás extenso y merece mucho más tratamiento que el que le daremos, pero es importante que demos un pantallazo al respecto para entender temas que trataremos mas adelante.

Se le recuerda al lector que los diferentes fabricantes tienen sus estrategias de manejo de colas de calidad de servicio, en general tienen lineamientos similares, haciendo selección de paquetes, marcando los mismos, posicionándolos en colas para ir formando clases de servicios y luego dándole un tratamiento especifico cada clase.

4.4 Clasificación y marcado

Para aplicar calidad de servicios en una red, el tráfico debe poder ser clasificado. Existen varias técnicas de clasificación, las dos mas usadas son, "confiar en la aplicación" la cual marca los paquetes IP en el campo DSCP , ver Figura 1 estructura del paquete IP y los equipos de comunicaciones confían en esa clasificación; en la otra técnica utilizada con frecuencia es que los mismos equipos de comunicaciones se encargan de reconocer las aplicaciones y remarcar el campo DSCP, la inteligencia de los equipos de comunicaciones para reconocer aplicaciones hoy en día es un tanto limitada pero evoluciona constantemente.

Figura 1 Estructura paquete IP

+	Bits 0–3	4–7	8–15	16–18	19–31
0	Version	Header length	Differentiated Services	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options				
160 or 192+	Data				

Normalmente no se confía en lo que viene de la red y se remarca, con esto nos aseguramos de una efectiva clasificación.
Los filtros de clasificación deben ser precisos para identificar correctamente las aplicaciones.
Para lograr establecer una adecuada calidad de servicio de una red, es necesario conocer la empresa/organización, su estructura, sus servicios/servidores, sus usuarios y objetivos. Se debe realizar un minucioso análisis del tráfico en los sectores de interés y posteriormente aplicar las reglas para mejorar el uso de los enlaces. Se debe considerar que las calidades de servicios aplicadas requieren un continuo monitoreo de variables de la red y del tráfico para que sea sostenible en el tiempo, permitiendo así ajustes adecuados.

4.4.1 Clases de servicio

Mencionemos algunas clases de servicio:

Class-based weighted fair queuing (CBWFQ), este método extiende las funcionalidades de la estrategia WFQ, para proveer soporte a las colas definidas por el usuario, el usuario puede definir colas de calidad de servicio siguiendo varios criterios como características del encabezado del paquete IP (header como se lo conoce), access-list o listas de accesos, interfaces de entrada, etc. Provee mucha flexibilidad para las políticas de selección de tráfico que necesite el usuario.

First In First Out (FIFO) Queuing
First In, First Out (FIFO) Queuing (encolamiento) Los paquetes son transmitidos por la interfase correspondiente en el mismo orden con que fueron arribaron por una interfase. Este es casi el primero de los métodos de transmisión utilizados.

Priority Queuing (PQ)
Esta característica asegura que el tráfico elegido como importante será despachado sin importar que exista otro tráfico esperando por ser transmitido. Este método es considerado casi obsoleto ya que mientras exista trafico de prioridad mas alta no pasara tráfico de prioridad mas baja, muriendo de starvation los flujos de datos de baja prioridad.

Weighted Fair Queuing (WFQ)
WFQ esta estrategia va encolando paquetes llevándolos al frente de la cola de transmisión para reducir el tiempo de despacho de paquetes elegidos siguiendo un algoritmo especial diseñado por

Cisco y simultáneamente va repartiendo el ancho de banda restante con los otros flujos considerados importantes.

Las tecnologías de QoS (Quality of Service, calidad de servicio) garantizan que se transmitirá cierta cantidad de datos en un tiempo dado (throughput). Una tecnología de transmisión que nació con QoS es ATM (Asynchronous Transfer Mode – Modo de Transferencia Asíncrona) soporta calidades de servicio .Esto permite que los proveedores de servicios que cuentas como transmisión ATM garanticen a sus clientes que el retardo de extremo a extremo no excederá un nivel específico de tiempo, o que garantizaran un acho de banda específico para un servicio.
Una red IP esta basada en el envío de paquetes de datos, estos paquetes de datos tienen una cabecera que contiene información sobre el resto del paquete. Esta información de header o encabezado del paquete IP sirve para clasificarlos y tratarlos de manera diferencial, así cada router de transito podrá clasificar y despachar con la calidad de servicio fijada para ese tipo de tráfico.
Claro esto es casi perfecto, "casi" es porque no controlamos de extremo a extremo la red, un enlace pasa por múltiples proveedores de servicios, múltiples plataformas de transporte cada uno con su tecnología y particularidad, que hace muy difícil tener control absoluto. Un ejemplo típico de hoy en día son los proveedores que ofrecen enlaces sobre redes MPLS, donde estos proveedores a su vez sub-contraten a proveedores de ultima milla, estos proveedores típicamente ofrecen tres o cuatro clases de servicios para transportar VoIP (del ingles voice over IP, en castellano voz sobre IP) donde el jitter es importante o aplicaciones que usan ancho de banda variable que probablemente no sea importante el jitter, ídem con otros tipos de patrones de tráfico. Mencionamos muy a menudo VoIP porque es la tendencia actual en la que se tiende a integrar las comunicaciones de telefonía tradicional con el mundo IP, y para que pueda competir en calidad de audio (el VoIP) debe haber calidad de servicio que asegure que vamos a escuchar bien en ambas puntas de la conexión VoIP.

4.5 Funciones de la Calidad de Servicio en una red

La calidad de servicio es la capacidad de la red de proporcionar un mejor servicio al tráfico seleccionado:

- Asignación de ancho de banda.
- Manejar la sobre-suscripción
- Evitando y/o administrando la congestión en la red.
- Manejo de prioridades a través de toda la red de extremo a extremo.
- Modelación del tráfico de la red
- Políticas y funciones de administración para el control y administración de tráfico de principio a fin a través de una red.
- Colas y características del tráfico. Selección del tráfico

Para el caso de Voz sobre IP (VoIP) el objetivo de aplicar calidad de servicio es que se escuche bien, que para el oído Humano sea confortable hablar por telefonía sobre IP. Para mayores referencias sobre la percepción humana y formulas para cuantificar esa percepción humana del audio de VoIP habría que buscar temas referidos a métricas ICPIF (del idioma ingles Calculated Planning Impairment Factor loss/delay busyout threshold) es un estándar de ITU llamado ITU-T G.113 es un

estándar de medición de calidad de servicio, a grandes rasgos esta métrica toma en cuenta la sensación humana y la lleva a números aproximados. Algunos proveedores tienen otros indicadores como el MOS de Cisco (del idioma ingles Mean Opinion Score) que tiene también por objetivo cuantificar numéricamente las sensaciones humanas al escuchar VoIP. Este esfuerzo por cuantificar sensaciones humanas es a los efector de medir y poder comparar numéricamente sensaciones que no tienen números, mas allá de estos números he visto estadísticas en casos reales de ICPIF y MOS y se aproxima enormemente a la realidad y reacciones de los humanos, por ejemplo las personas de mas de 40 años en general son muy sensibles y poco tolerante a fallas en el sistema VoIP y los números que entrega ICPIF y MOS son bastante acertados. Estos parámetros tienen en cuenta la perdida de paquetes, el eco, el codec de audio utilizado y el jitter en la comunicación.

Sobre Internet o en el camino de extremo a extremo el tráfico sufre o puede sufrir:

- Pérdida de paquetes en enlaces (ruido, micro-cortes, saturación de enlaces).
- Pérdida de paquetes en nodos (buffer de equipos de comunicación se llenan).
- Desorden de paquetes (en los nodos, cambios de ruta, etc.). Los paquetes pueden llegar a destino en distinto orden en el que se enviaron
- No hay prioridades o preferencias (todo el tráfico es “igual”).
- No hay reserva de recursos ni garantías
- Sólo se pueden conseguir “garantías estadísticas” sobredimensionando enlaces.

El QoS mencionado solo sirve dentro de un contexto cerrado de una Red en la que todos los router y equipos de comunicaciones sean administrados por un solo grupo de administradores con políticas comunes acordadas. Como hemos visto es muy distinta la problemática de calidad de servicio en Internet y en redes privadas.

4.6 Transporte

Hasta ahora hemos visto IP y no nos hemos referido a TCP, UDP, guía para aplicaciones.
En Internet se usan dos protocolos para transportar datos uno es TCP y el otro es UDP.
TCP de las siglas en ingles Transmission Control Protocol, este protocolo usa canales FIFO y fiables. TCP es sin pérdidas de datos, sin errores (protocolo de reenvío y asentimiento o Acknowledgment Ack), esto parece ir en contra mano de lo que mencionamos que en Internet o en una red se pueden perder datos, pero en realidad los paquetes se pierden, se alteran, se desordenan, para solucionar esto TCP tiene mecanismos de seguimiento y recuperación. TCP cuenta con mecanismos de entrega ordenada (se esperan datos” antiguos” antes de entregar los” nuevos”).

UDP: de las siglas en ingles User Datagram Protocol, UDP no confiable, no garantiza más que IP (usado por aplicaciones en tiempo real con VoIP que no tendría sentido retransmitir un paquete).

TCP: en TCP tenemos demasiadas garantías innecesarias:

- Reenvío de paquetes: no sirve si llegan demasiado tarde.
- Orden: puede retrasar la entrega de datos que llegan “a tiempo”.

Para redes con grandes delay, las aplicaciones TCP pueden ser tediosas y lentas para usarse ya que cada paquete tiene que tener su confirmación de recepción.

5.0 Desarrollo de la Tecnologías actuales en el análisis de tráfico

Dedicaremos esta sección a presentar las dos tecnología, llamadas Netflow y otra sFlow.
Cuando hablamos de tecnología Netflow y sFlow es muy difícil decir porque la mencionamos como tecnología, básicamente podríamos resumir como técnicas de visualización de una red, seria como ver con un una lupa un objeto, en este caso el objeto es una red de datos en las que conviven audio, video, aplicaciones de todo tipo y diseño.
Cuando hacemos referencia a mirar con una lupa, decimos que vemos con cierto nivel de detalle, para este caso podrimos observar ciertos detalles de un paquete de datos, como ser puerto origen destino, tamaño de paquete, origen y destino de un paquete, casi todo referente al header de un paquete.
No deberíamos confundirnos con ver la red con un microscopio, ahí ya depende de una captura completa de los paquetes para analizarlos con un sniffer manualmente o sniffer con potencia de análisis automático y las tecnologías de análisis de flujos de datos como sFlow y Netflow no servirían al menos por el momento.
Existen algunas diferencias fundamentales entre las tecnologías Netflow y sFlow.
Netflow es propietario de Cisco Systems, sFlow en cambio nació como un consorcio de empresas intentando crear un RFC, para un estándar en Internet.

Ambas tecnologías comparten un objetivo y premisas en común entre las más importantes, esta que de una u otra forma mostrar lo que pasa por la red la otra y quizás la que tiene más potencial es que tener un agente de netflow o sFlow incluido en el propio equipo de comunicaciones, router o switch. Esto que mencionamos tiene ventajas estratégicas, económicas y comerciales.
La ventaja estratégica es en cuanto a la ubicación de mencionado agente ya que a estar incluido en el equipamiento de red cuenta con una posición privilegiada para la tarea que se lo creo y es que literalmente ver pasar los paquetes, sabe de que interfase provino, sabe el destino, etc.
En cuanto a estrategia económica y comercial es con poco costo de hardware-software adicional dentro del equipo de comunicaciones pueden ofrecer a los consumidores de estos productos los beneficios de saber que tipo de tráfico cursa por su red, ya profundizaremos en estos temas.

5.1 Tecnología sFlow y netflow objetivos

Una diferencia de concepto es que Netflow fue creado para abarcar arrancando de layer 3, y sFlow comienza desde layer 2 siempre hablando del modelo OSI, ruteo y switching respectivamente. Esta característica distintiva, excluye a la tecnología netflow de ambientes switcheados, si bien parece una limitación de implicación creo que cuando tomaron la decisión de analizar a partir de layer 3 pesaron donde están los mayores requerimientos de que es lo que por ejemplo satura un enlace, y es donde los enlaces son mas costosos típicamente los enlaces WAN de larga distancia donde en el 90% de los casos hacer algún tipo de análisis de trafico. Conociendo la arquitectura de los equipos Cisco parece que tiene que ver que mucho del esfuerzo de ruteo en un router esta implementado en software mientras que en una red típicamente una LAN los equipos Cisco (referido a los switches) el switcheo de paquetes esta fuertemente ligado a implementaciones en hardware para lograr velocidad y confiabilidad dejando la carga mas pasada al hardware mientras que otras que requieren menor potencia al CPU o software del equipo. Los consumidores de equipos Cisco les es muy costoso renovar todo el plantel de router por nuevos que tenga incluido hardware de netflow, en cambio es mucho más accesible físicamente y económicamente hablando, realizarle un up grade de IOS (que es el software nativo de cisco).

Otro tema no menor es que son tecnología que tienen continuos avances y mejoras, incluyéndole nuevas características o corrigiendo Bugs o falla.
No seria nada extraño que ambas tecnologías evolucionen hasta un punto de ser técnicamente iguales o muy parecidas, ya lo son en cuanto a la configuración en la práctica.
Otra diferencia muy importante y no tan fácil de visualizar es que todos los flujos de netflow son referidos a los que entra al router, quizás no se note en esta teoría pero en la practica muchas veces se transforma en limitante cuando se pretende ver el tráfico que entra y sale de una interfase del un router Cisco, igualmente esto lo resuelven los colectores y procesadores de estos flujos de netflow.
sFlow envía flujos de datos de la entrada y la salida de paquetes de una interfase

5.2 Evolución a Netflow y a sFlow

5.3 sFlow

Antes de comenzar definamos que es sFlow: originalmente desarrollado por InMon Corp. luego se fueron agregando desarrolladores, sFlow es un estándar multi-proveedor para el monitoreo de flujos de trafico desde baja a alta tasa de tasa de transferencia, escalable a velocidades de 10 Gbps de redes switcheadas y ruteadas. sFlow se escribe así por convención de sus desarrolladores.
sFlow es una tecnología embebida dentro del equipo de red que brinda una completa visibilidad de la actividad de la red, facilitando un efectiva administración y control de los recursos de una red. InMon es un miembro fundador de sFlow.org un consorcio de industrias.

Definiremos la tecnología sFlow para hacer las convenciones de un vocabulario común
sFlow fue definido inicialmente al un RFC (request for comment) buscando un estándar en esta Tecnología, el numero de RFC es 3176 en la cual se define la funcionalidad de agente sFlow versión 4, en esta sección entenderemos que queremos decir cuando hablamos de “agente sFlow “
Posteriormente evolucionó a la versión 5 de este estándar propuesto. Tomaremos las ideas principales del RFC que describe sFlow.
sFlow es una tecnología para monitorear tráfico en redes de Datos contenido en switches y routers (equipos de comunicaciones), define mecanismos de muestreo de tráfico llevado a la práctica en “agentes sFlow”. Los “agentes de sFlow” son configurables vía SNMP “Simple Network Management Protocol”.
En este RFC se describe el formato del datagrama o paquete IP que llevara hasta un colector de sFlow que interpretara dicha información de tráfico contenida en los paquetes IP

En este documento contiene:

- Terminología y Arquitectura. sFlow un modelo de referencia.
- Mecanismos de Muestreo de paquetes y contadores.
- sFlow SNMP y una descripción de la MIB “Management Information Base”.
- sFlow formato del datagrama IP
- Consideraciones de seguridad. Configuración-Transporte y confidencialidad

La tecnología sFlow para monitoreo de tráfico se encuentra físicamente dentro del switches y router. El sistema de monitoreo sFlow consiste en un "agente sFlow (embebido en un switch o router o en una punta de prueba conectada a la red) y un colector central.
La arquitectura y las técnicas de muestreo [25] usadas en el sistema sFlow fue diseñada para proveer un continuo monitoreo de tráfico, independientemente de si son redes de baja o alta velocidad.

El diseño de las especificaciones son tendientes a:

- Precisión en el monitoreo de trafico en redes de velocidades gigabit [24] o mayores
- Escalable para decenas o miles de agentes sFlow con un solo colector de sFlow
- Bajo costo de implementación de "agentes sFlow"

El "agente sFlow" usa técnicas de muestreo para capturar estadísticas de trafico del dispositivo de red que quiere ser monitoreado. Los datagramas sFlow son usados para inmediatamente pasados al "muestreador de tráfico" para luego ser enviados al colector de sFlow para que lo analice.
El RFC describe los mecanismos de muestreo usados por el "agente sFlow", la Mib de sFlow es usada por el Colector central para controlar el "agente sFlow" y el formato del datagrama sFlow es usado por el "agente sFlow" para enviar los datos al Colector de sFlow.

Definiciones

En esta sección nos vemos obligados a transcribir definiciones planteadas en el estándar sFlow para hablar/escribir el mismo lenguaje adoptando la misma terminología, que por otra parte no es mas que poner en claro los conceptos que cualquier persona que se dedica a las redes de datos ya tiene incorporada en su vocabulario.

Dispositivo de red (Network device): equipamiento de una red tal como switch o router que pueden transportar o tomar decisiones sobre el destino de paquetes de datos.

Fuente de Datos: se refiere a una ubicación dentro de un dispositivo de red que tiene la posibilidad de realizar mediciones de tráfico. Las fuentes de datos incluyen interfases, entidades físicas dentro de un dispositivo como puede ser backplane y Vlan. Una fuente de datos puede ser definida en las interfases lógicas o físicas por donde transitan los paquetes de datos, para que cada paquete pueda ser observado.

Flujo de paquetes: un flujo de paquetes es definido como el camino o trayectoria que toma un paquete a través de un dispositivo (componente) de una red. Hagamos un pequeños refresco del concepto general de componente de una red, o dispositivo/equipamiento de red, estos tienen la posibilidad de tomar decisiones sobre la trayectoria de los de un paquete, toma decisión en base a reglas.

Un paquete puede entrar por una interfase y salir por otra del mismo equipo de red o incluso puede volver a salir por la misma interfase. Recordemos que un router básicamente toma decisiones sobre capa 3 (layer 3) y un switch toma decisiones de capa 2 (layer) dentro del modelo OSI. Aclaremos que los actuales equipos de backbone tienden a parecerse mas a switches que a

routers, lo podríamos ver como switches que básicamente manejar por hardware la mayoría de las funciones de switching de layer 2 que incorporan de a poco características de equipos de layer 3, una combinación que por el momento parece barrer con todos los otros equipos de red.

Muestreo de Flujo de Paquetes: muestreo de flujo de paquetes se refiere a una selección aleatoria de una fracción de los flujos.

Velocidad de muestreo: la velocidad de muestreo especifica la porción aritmética de los paquetes observados (en una "fuente de datos") con la totalidad de los flujos de paquetes, seria la especificación de cada cuantos paquetes que "veo" tomo uno como muestras. Cuando nos referimos a "veo" nos estamos tomando como punto de vista del "agente sFlow".

Registro de flujo de paquetes: un registro de estos contiene los atributos de un flujo de paquetes (o flujo de datos).

Contadores de muestreo: muestreo periódico o poleo de contadores asociados a la fuente de dato. Contadores que inician luego que se tomo una muestra.

Instancia de sFlow: una instancia de sFlow refiere a la medida del proceso asociado con una fuente de datos, puede haber una o mas instancias de sFlow asociadas con una sola fuente de datos (data source).

Agente sFlow: el agente de sFlow provee una interfase para configurar una instancia de sFlow dentro de un equipo (referido a un equipo de comunicaciones), un agente de sFlow puede configurarse vía snmp. Un agente de sFlow es el responsable de mantener una sesión de medición con un colector de sFlow. Un agente de sFlow es responsable además de liberar los recursos cuando una sesión expira.

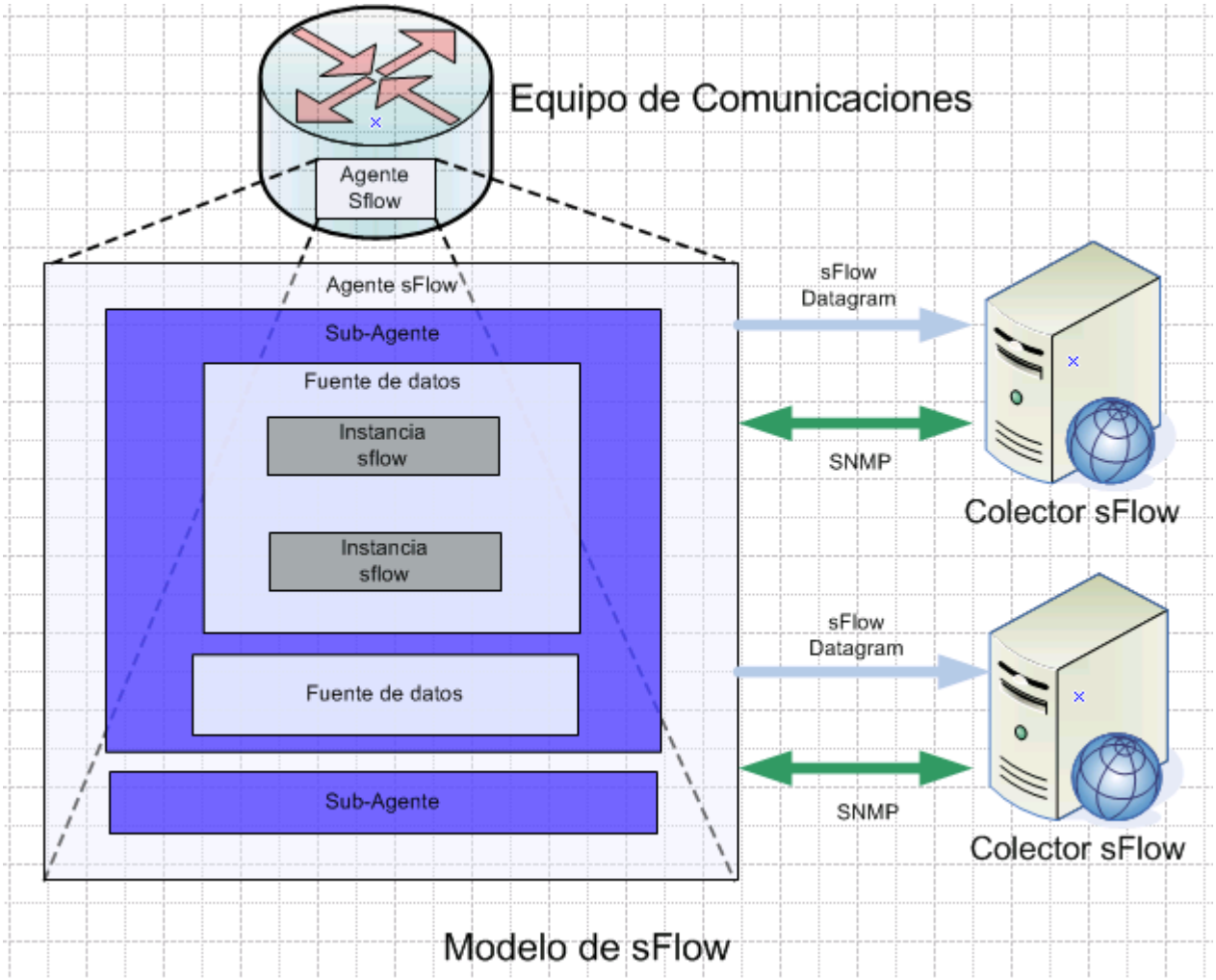
Sub-Agente de sFlow: este es otro componente para el caso que un dispositivo de red este implementado de manera distribuida, cada sub-agente se encarga de un subconjunto de fuentes de datos (data source).

Colector de sFlow: un colector de sFlow recibe datagramas de sFlow de uno o más agentes de sFlow. El colector de sFlow puede configurar el agente de sFlow.

Datagramas sFlow: un datagrama de sFlow es un datagrama UDP que contiene datos de una muestra de tráfico e información sobre la fuente de medición (típicamente una interfase físico o virtual). Mas adelante mostraremos el formato de este paquete IP

5.3.1 Modelizado de RFC sFlow

A continuación adjuntamos un Modelo de Referencia que muestra la relación entre los componentes de la tecnología sFlow, en la figura siguiente.



Un Colector de sFlow hace uso del protocolo snmp, para comunicarse con un agente de sFlow, con el fin de configurarlos y pasarle parámetros.
En este RFC, también describe la MIB de SNMP, esa MIB describe como configurar un agente sFlow. Los tiempos de muestreo y contadores de muestreo de sFlow, son ejecutados por una instancia sFlow, asociada individualmente con una fuente de datos del agente sFlow. Del proceso de muestreo de datos (tráfico de ahora en mas) se obtienen como resultado la generación de registros de flujo paquetes (Packet flow Record). Con el fin de hacer correr los contadores de muestreo, una instancia sFlow es configurada con un intervalo de muestreo. De los procesos de contadores de muestreo, se obtienen registro de contadores. Un agente de sFlow colecta los registros de contadores y los registros de flujo de paquetes, para luego enviarlos formateados en un datagrama sFlow, a un colector. El formato del datagrama sFlow también esta definido en la RFC.

5.3.2 Mecanismos de Muestreo

El agente sFlow, usa dos modos para muestrear tráfico (muestreo de flujo), uno es un muestreo estadístico y el otro modo es muestreo basado en timer. Muestrear en base a timer o contadores, es un muestreo sistemático a periodos regulares, se los define como “contadores de muestreo”

5.3.3. Muestreado de flujos de datos

Los mecanismos de muestreo de tráfico de sFlow deben asegurar, que cada paquete tiene las mismas probabilidades de ser tomado como muestra, independientemente del flujo de datos al que pertenezca.
Para que un paquete tenga oportunidad de ser muestreado, se tiene que cumplir la condición que el contador de muestreo llegue a cero y que el paquete ya haya sido asignado a una interfase, mediante el proceso de routing/switching del equipo de red, hay un contador que cuenta la cantidad de paquetes "total_packets" que se incrementa sea o no muestreado el paquete.
Este contador "total packets" es para tener la idea de la cantidad de paquetes que pueden haber sido muestreado, esto también será un indicador del error en la medición/estimación realizada por el colector central.
Cuando hablamos de tomar una muestra de un paquete, estamos hablando de copiar el header del datagrama o encabezado del paquete IP, también puede implicar tomar cierta característica que esta más allá de header del paquete.
Cada muestra que se toma genera un incremento de otro contador, llamado "Total_Samples" muestras_totales, este contador indica el total de muestras generadas. Las muestras son enviadas por la instancia de sFlow al agente sFlow, para ser procesada. La muestra incluye información del paquete y los contadores de "cantidad de paquetes totales" y "cantidad de paquetes muestreados" (Total_Packets y Total_Samples counters).
El agente sFlow une la muestra de tráfico tomada para obtener información sobre la trayectoria de los paquetes dentro del dispositivo de red. La información anterior depende únicamente de las funciones de forwardeo de paquetes en el equipo de red. Por ejemplo con esto también se puede obtener información de la interfase de entrada y salida, vlan origen, vlan destino, next-hop, datos como el AS, etc.
Una vez que una muestra es tomada , se inicia un contador que indica cuantos paquetes deben ser descartados antes de tomar la siguiente muestra cuando ocurre esto el contador se reinicia nuevamente. El valor cargado en el contador para iniciarlo debe ser un entero aleatorio, donde la secuencia del entero aleatorio usado en el tiempo de cumplir con:

(1) Total_Packets/Total_Samples = Sampling Rate

Mas adelante explicaremos un estudio en el cual se presentan tres formas de muestrear indicando ventajas y desventajas. El estudio antes mencionado fue realizado en los laboratorios AT&T.

5.3.4 sFlow MIB

sFlow define una serie de objetos snmp, para mantener una sesión entre el agente sFlow y el colector sFlow. Una de las funciones del colector sFlow, es mantener informado al agente sFlow de que él existe (el Colector) para evitar consumir recursos del equipo de comunicaciones (no olvidemos que el agente sFlow esta embebido al equipo de red) y evitar generar paquetes que no son recibidos o procesados.
El agente sFlow tiene capacidades limitadas por diseño para evitar que afecte a la performance del equipo de comunicaciones.
El colector sFlow debe pasarle parámetros al agente, como ser dirección IP (destino del los datagramas sFlow normalmente la IP del colector), el puerto UDP utilizado y el máximo tamaño de los datagramas sFlow para prevenir fragmentación de paquetes.

En la RFC que describe la tecnología sFlow se documenta también, los objetos snmp y su utilidad, creados básicamente para controlar el agente sFlow. El agente sFlow puede ser configurado íntegramente vía snmp por el colector.

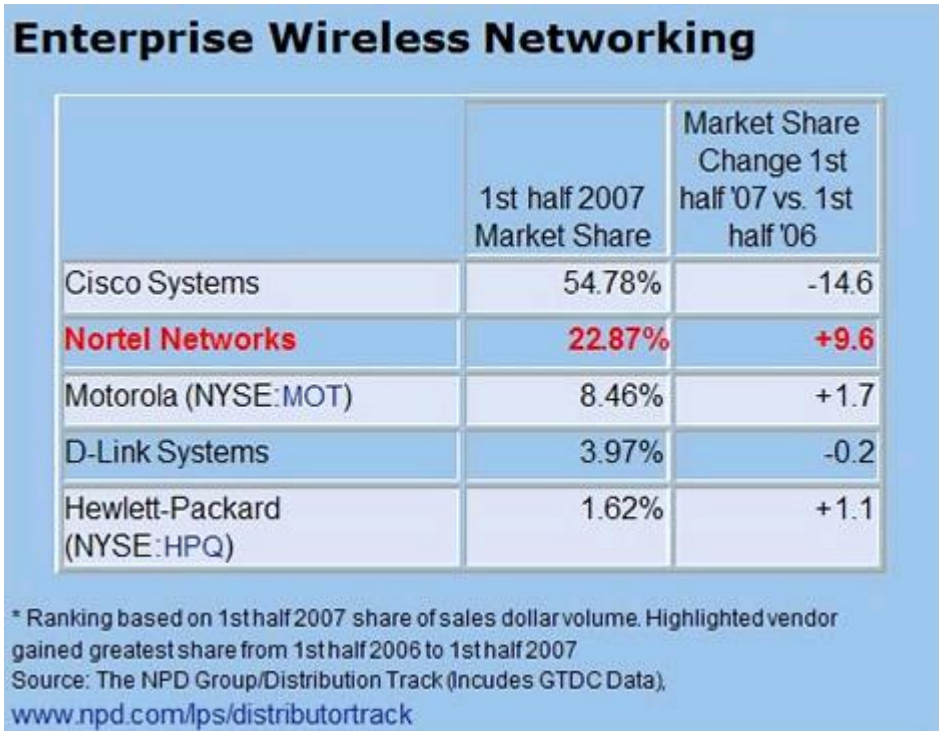
5.3.5 Formato del datagrama o paquete de sFlow

El formato de los paquetes se regirá por otro RFC que define lineamientos generales.
Las muestras son enviadas como un paquete UDP a un host y puerto específico.
El puerto por defecto es *UDP 6343*. Esto pretende evitar problemas de configuración entre el agente, el colector de sFlow y eventualmente con un firewall que los separa.
La falta de certeza en que un paquete UDP llego no representa un problema y no afecta significativamente al error en el muestreo de tráfico.
El uso de UDP reduce la cantidad de memoria requerida para contener los datos. Sin embargo UDP presenta muchas ventajas en momento que se registran pico de tráfico o potenciales ataques ya que los paquetes, solo se les incrementa el tiempo de viaje pero no se produce el efecto negativo de las retrasmisiones porque el colector no recibió tal o cual paquete. El delay en la transmisión solo incrementa la memoria usada por el agente sFlow.
El objetivo buscado con esta tecnología, es ver el tipo de tráfico que circula por una red o por muchas redes, sin que esto genere un impacto en la misma, por ejemplo causando incrementos sustánciales del tráfico. La idea es que el incremento de tráfico, generado por el agente sFlow al enviar paquetes sFlow al conector central, sea insignificante con respecto al volumen de tráfico muestreado o observado.
Otro objetivo es no incrementar el uso de CPU/memoria del equipamiento de red, ni tener que invertir en un súper procesador para colectar y procesar la información generada por la tecnología sFlow.
El proceso de muestreo de tráfico esta pensado para no incrementar el tiempo de tránsito de un paquete por un equipo de red, ya que de nada serviría muestrear si esto incrementa en 10ms el tránsito de un paquete por un router o switch, 10ms (mili segundos mili =10^ -3) .Es absolutamente inaceptable para una red Lan ethernet que los delay mencionados los genere un switch, tanto sea de 10, 100, 1000 Mbps. Recordemos que el delay no solo afecta al tránsito del paquete, sino que a la respuesta de las aplicaciones cliente-Servidor.
Adicionalmente demorar los paquetes dentro de un equipo de red provocaríamos que los buffer de entrada de las interfaces, si estos buffer se llenan, el equipo de red no tiene mas remedio que descartarlos. Los buffer de un equipo de comunicaciones son memorias que actúan como elásticos o amortiguadores, allí se depositan los paquetes, hasta que el equipo de red los puede procesar ya sea por hardware o por software. Procesar un paquete por software significa, hacer uso del CPU del equipo de comunicaciones, para tomar la decisión si el paquete es descartado o enviado por alguna interfase. Procesar por hardware implica que la dedición sobre un paquete, se hace por circuitos electrónicos dedicados a tal fin, sin que un CPU/software intervenga en el proceso.
La representación de esos datos en el colector de sFlow se debe hacer de manera eficiente, a fin de tener gráficos y estadísticas lo más rápido posible.
Forzar que los paquetes de sFlow sean pocos, es un problema de costos, si el volumen de información a almacenar es muy elevada, implica acopiarlos en bases de datos muy extensas y ocupar mucho disco rígido. Si la información almacenada es mucha, proporcionalmente elevamos el esfuerzo computacional en procesarlo y esto se traduce directamente a términos monetarios.

5.4 Netflow y sFlow

Con la tecnología de Cisco Netflow se buscan objetivos similares, tiene algunas diferencias conceptuales pero en esencia los objetivos son los mismos que sFlow, con la desventaja que no hay mucha información, de la forma en que trabaja o muestrea esto hablando de la documentación. De la observación de netflow en los equipos de comunicaciones se pueden sacar muchas conclusiones que no distan mucho de lo descrito para sFlow. Cisco confina hasta la fecha de esta redacción, la tecnología Netflow a los equipos de Layer 3, es decir routers, ya que estos hacen la mayoría de las tareas por CPU/Software/memoria , esto es potencialmente una desventaja si lo vemos con una determinada óptica, pero esta supuesta desventaja bien manejada es una real ventaja, ya que equipos que no fueron pensados con Netflow, con un simple upgrade de IOS (IOS es el software propietario de Cisco para la mayoría de sus equipos de comunicaciones) , en cambio en equipos de layer 2 básicamente switches con un up grade de IOS no se puede lograr incluir la tecnología Netflow, ya que los CPU de estos equipos es más limitado en capacidad, porque simplemente hacen un switcheo de paquetes por hardware dedicado. Esto hace que la decisión de que interfase va a ser destinado un paquete una vez que esta dentro del switch, es en cuestión de micro segundos, pudiendo acercarse a cursar el tráfico a la velocidad física de las interfases.
En los switches de alta gama de Cisco (los más grandes y más caros) netflow puede lograrse con la adición de una placa especial de Netflow, pero esto tiene sentido solo para los equipos switches de layer 2 que incluyen funciones de layer 3.
Seguramente se preguntara el lector porque tanto esfuerzo de escritura y dedicación a Netflow, la respuesta es una y la siguiente: sFlow se plantea como una plataforma abierta tratando de generar un estándar en la industria pero la Empresa Cisco tiene gran parte del mercado de equipos de comunicaciones, con mucha fortaleza en equipos de layer 2 y layer 3, con una cartera de soluciones desde layer 1 layer 7, todos con una simplicidad de uso y sofisticación que no deja de sorprender e innovar. No se han encontrado estadísticas del “market share o división del mercado” referido a equipamiento de comunicaciones.

Solo se encuentran estudios parciales como los de la figura siguiente.



Enterprise Wireless Networking

	1st half 2007 Market Share	Market Share Change 1st half '07 vs. 1st half '06
Cisco Systems	54.78%	-14.6
Nortel Networks	**22.87%**	**+9.6**
Motorola (NYSE:MOT)	8.46%	+1.7
D-Link Systems	3.97%	-0.2
Hewlett-Packard (NYSE:HPQ)	1.62%	+1.1

* Ranking based on 1st half 2007 share of sales dollar volume. Highlighted vendor gained greatest share from 1st half 2006 to 1st half 2007
Source: The NPD Group/Distribution Track (Incudes GTDC Data),
www.npd.com/lps/distributortrack

Tienen en común sFlow y Netflow es el costo elevado, de los analizadores/colectores de paquetes Netflow y sFlow, hoy en día a pesar del costo son herramientas que requieren mucho entrenamiento y debido a la complejidad de las tecnologías le falta mucho pulido a las aplicaciones, además no todos los usuarios desean ver la información de la misma manera ni les interesa ver los mismos datos , con lo cual lograr una plataforma que satisfaga a todos los clientes es bastante difícil , con lo cual complica aun mas la generación de productos estándar o de simple comprensión. Veremos mas adelante que la lectura de datos de los colectores requiere personal muy entrenados y entendidos en networking, no hace falta un Albert Einsten pero si una persona con muchas horas y horas de estudio y experiencia en networking. El estudio no es más que el medio para el desarrollo de los conceptos dentro de la mente del ser humano, esa maravillosa maquina auto superable.
La motivación de este trabajo es debido al avance de la tecnología, tecnología que tiene como objetivo primordial integrar servicios, donde el transporte son las redes IP.
Los proveedores van entendiendo que deben simplificar el uso de sus plataformas sin perder calidad-adaptabilidad-versatilidad.
Conforme el avance de la tecnología las plataformas se van haciendo cada vez mas robustas y con gran variedad de opciones que se ajustan a cada necesidad.
Es inminente la Integración de Voz y Datos en las redes IP, reemplazando la telefonía tradicional conmutada a voz sobre IP, hoy en día no se nota diferencia de calidad entre la telefonía tradicional conmutada y la telefonía sobre IP incluso se nota mejor calidad en la telefonía sobre IP.
En un futuro el cableado para telefonía y para datos tiende a desaparecer, fusionándose en un solo cableado que sirva de transporte para vos sobre IP y datos IP.

6.0 Evaluación e Implementación de herramientas de análisis de tráfico

La implementación se realizó en hardware de plataforma Intel pentium 4, con sistema operativo Debian distribución Ubuntu.
El objetivo fue el uso de herramientas GNU y probar algunas herramientas comerciales.
Fue una ardua tarea organizar y elegir las herramientas a usar, las mismas se encuentran listadas a continuación:

Tcpdump para hacer muestreo y comparaciones con la realidad.

Ethereal ahora conocida como wireshark [26] para la captura y análisis de tráfico. Versiones Este sniffer trae incorporado herramientas de análisis de los paquetes capturados, muy útiles para un análisis desglosado.

Iptraf [11], esta utilidad muestra estadísticas de paquetes de una placa de red seleccionada.

Agente de sFlow, la página para el nuevo estándar ofrece para los desarrolladores el código fuente de un agente básico para generación de paquetes sFlow versión 5. [30].

Fprobe [30], este agente de netflow se comportó de manera estable. También pensado para reportar a un colector central de netflow.

Ntop [29]. Esta herramienta cumple con muchas de las necesidades de visualización de tráfico.
Esta herramienta funciona colectado información de varias fuentes, por ejemplo directamente capturando paquetes en las placas de red, colectando paquetes sFlow y paquetes netflow para procesarlos y graficarlos. La filosofía de NTOP agrupando por los "ntop" donde "n" es los primero 10 que mas consumen un recurso, o que mas paquetes envían/reciben, que mas hosts contactan, etc.

NetflowLive, de la empresa Cranong, es un analizador básico de paquetes netflow, no proporciona gráficos.

Sentinel de la empresa Inmon, desarrolladores del estándar sFlow. Es una herramienta comercial muy potente.

sFlowTrend [28], de la empresa Inmon. Es una herramienta simple de usar, no tiene la potencia de producto "centinela" pero sirve para resolver problemas y hacer análisis en tiempo real. Se uso inicialmente sin filtros y luego se crearon filtros para ver particularidades. Es una herramienta que con un poco de entrenamiento y lectura se aprende a usar. En sFlowTrend los filtros llevan expresiones regulares como las mostradas a continuación, donde cada línea es uno de los múltiples posibles filtros y usados para análisis específico.

- srcPort == "TCP:443" || destPort == "TCP:443"
- srcPort == "TCP:80" || destPort == "TCP:80"
- srcPort == "TCP:25" || destPort == "TCP:25"
- srcPort == "UDP:53" || destPort == "UDP:53"
- srcPort != "TCP:80" && destPort != "TCP:80" && srcPort != "TCP:25" && destPort != "TCP:25"

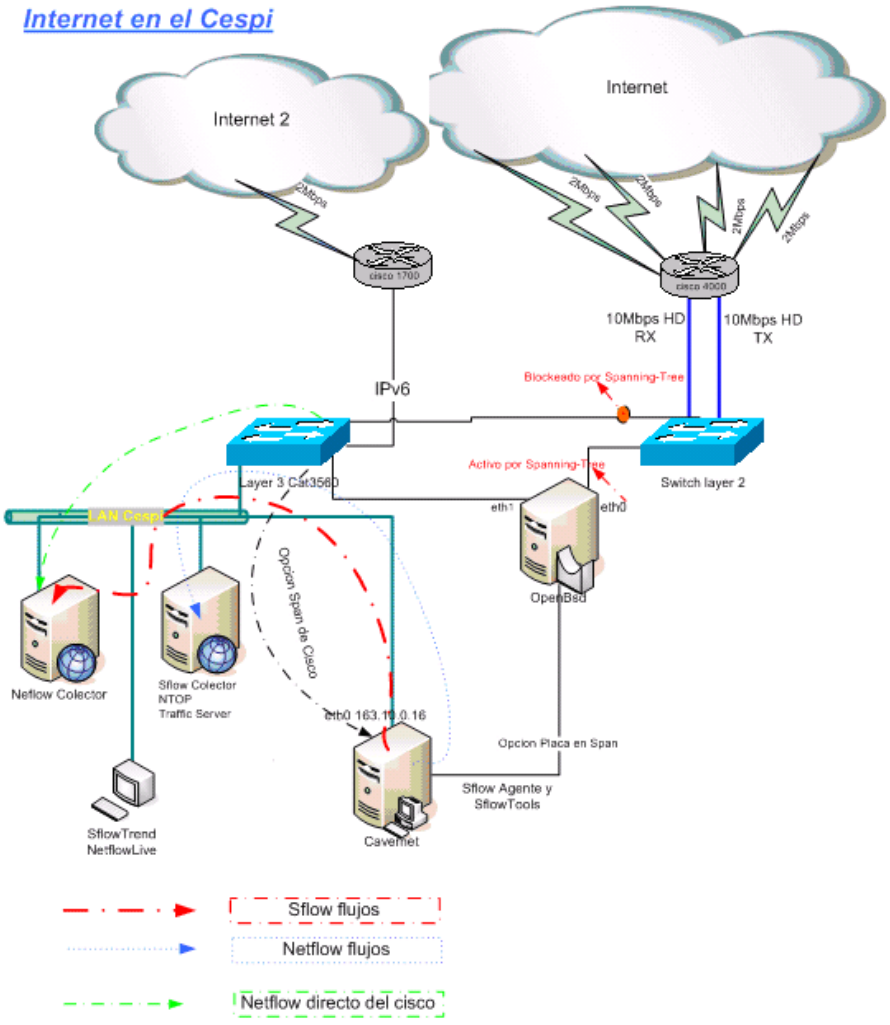
- srcPort != "TCP:80" && destPort != "TCP:80" && srcPort != "TCP:25" && destPort != "TCP:25" && srcPort != "TCP:443" && destPort != "TCP:443" && srcPort != "UDP:53" && destPort != "UDP:53" && srcPort != "TCP:110" && destPort != "TCP:110" && srcPort != "IPv4:47" && destPort != "IPv4:47" && destPort != "TCP:8080" && srcPort != "TCP:8080" && destPort != "TCP:22" && srcPort != "TCP:22"
- srcPort== "TCP:0" || destPort== "TCP:0"
- srcPort== "UDP:0" || destPort== "UDP: 0"

No se explicara como se crean los filtros en la herramienta sFlowTrend ya que son muy intuitivos y en la misma herramienta se encuentran un manual completo, cada uno de estos filtros fue usado para aislar algún trafico que nos interesó durante el análisis.
Avanzando en el presente documento veremos como luce esta herramienta y que nos puede ofrecer.

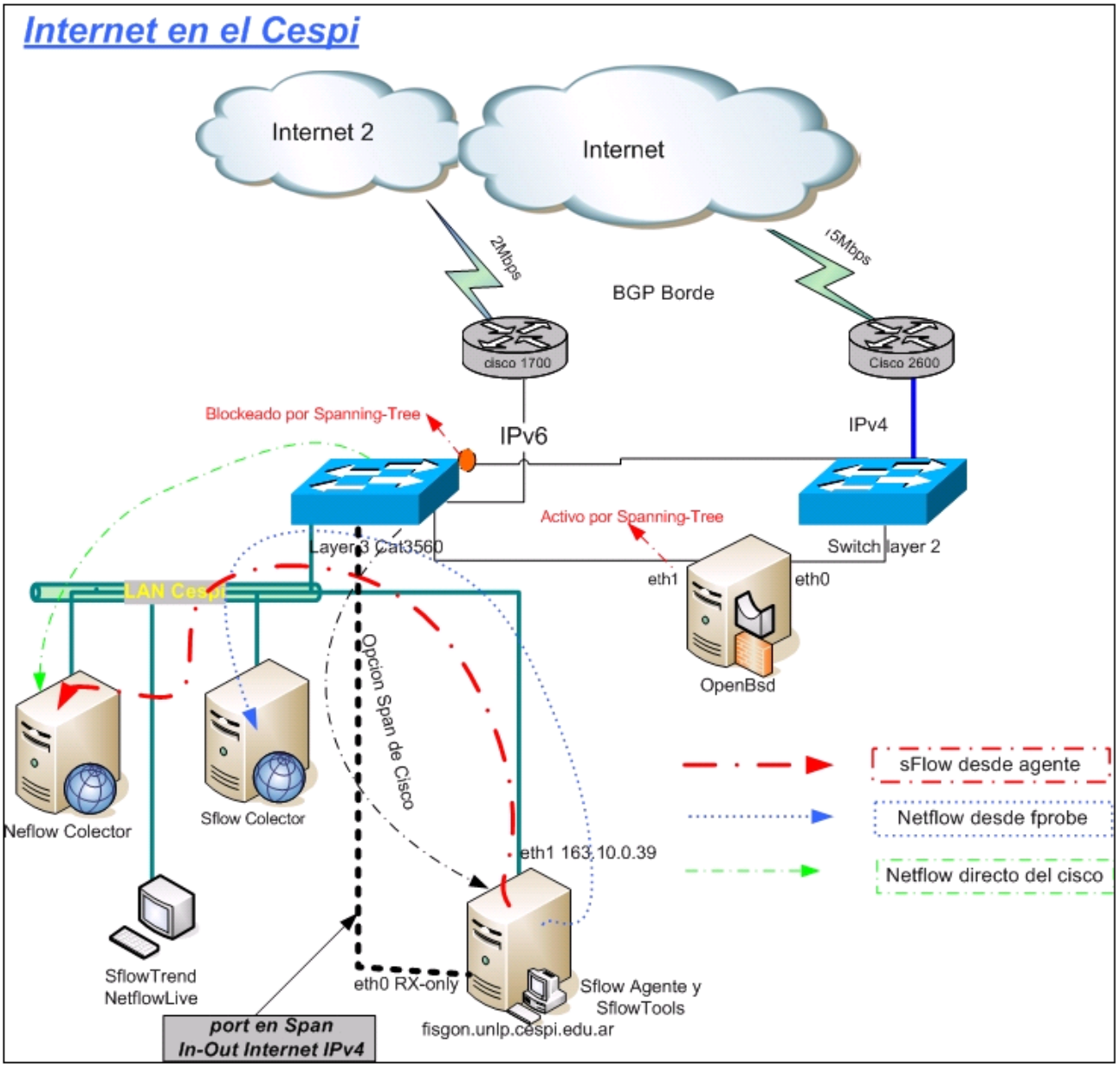
Topología de de red Utilizada

La red del CeSPI, tiene como frontera con Internet equipamiento Cisco y usando la característica de Span (tecnología propietaria de Cisco Systems) se configuraron puertos en Span para tener una copia todo el trafico de entrada y salida del Internet al CeSPI, uno de estos puertos se conecto un servidor llamado "fisgon.cespi.unlp.edu.ar", este servidor de desarrollo contó con dos placas de red una para análisis de tráfico y otra placa para fines de administración.
La idea fue no mezclar el tráfico de entrada salida al servidor con el tráfico de entrada salida de Internet en el CeSPI. Este servidor contó con la seguridad para restringir y protegerlo de posibles accesos no autorizados. Todas las herramientas antes enumeradas (ntop, sentinel, fprobe, etc.) se instalaron en el servidor mencionado.

La idea y topología original era:



La topología que veremos continuación surgió de un cambio de tecnología de acceso a Internet.



Pasemos a explicar el diagrama, para simplificar se dibujan tres servidores independientes nombrados como fisgon.unlp.cespi.edu.ar, sFlow colector y Netflow Colector, pasemos a definir sus funciones

Servicios:

- Agente sFlow, colecta datos de la placa eth0 y genera paquetes IP según el RFC sFlow
- Como agente netflow se usó fprobe, colecta datos de la placa eth0 y genera paquetes según la tecnología Netflow
- Netflow colector, se usa como colector/analizador de netflow la herramienta NTOP, Sentinel y NetflowLive.
- Netflow sFlow, se usar como colector/analizador de Ntop, Sentinel y sFlowTrend.

Todo fue instalado en un solo servidor en “fisgon.unlp.CeSPI.edu.ar”.

Las herramientas están muy bien documentadas por los desarrolladores así que solo daremos una breve reseña.

Agentes Netflow y sFlow, procesan paquetes que capturan de la placa y según sus estándares envían los datos a un colector para que posteriormente sean analizados.
sFlowTrend, es una herramienta programada en JAVA para graficar instantáneamente flojo de datos proveniente de los agentes sFlow, desarrollada para ser corrida en Windows de Microsoft.
NetflowLive cuenta con la misma funcionalidad que el sFlowTrend, fue creado y prontamente discontinuado, es una útil herramienta que desplaza la primitiva herramienta de cisco de "IP accounting".
Sentinel, es la segunda generación de herramientas de colección y análisis de paquetes de la tecnología sFlow, anteriormente se lo conocía como "Traffic Server" con muchas fallas y con primitiva interfase, corregidas y mejoradas es esta nueva generación. Permite hacer reportes y tener un historial de lo ocurrido con el trafico de la red, combinando con monitoreo estándar por SNMP, logrando una potente herramienta que además de contar con el volumen de tráfico en una interfase (interfases o router completo) tiene detalle de que tipo de trafico conforma ese volumen.

6.1 Herramienta Traffic Server y Traffic Sentinel de la Inmon

Como ya hemos mencionado hay una herramienta comercial que desarrollo la empresa Inmon Inc., Esta empresa parte importante del consorcio encargado del desarrollo e implementación de la tecnología sFlow.
Esta herramienta fue desarrollada para ser instalada sobre RedHat o Fedora principalmente, por lo tanto tuvimos que hacer que el servidor fisgon.cespi.unlp.edu.ar antes mencionado, corra con este sistema operativo, reinstalando las mismas herramientas de análisis para este caso. La herramienta puesta bajo análisis llamada en la primera generación "*traffic server*" y la segunda generación "*traffic Sentinel*", esta herramienta permite analizar en servicio continuo la tecnología sFlow.
El primer problema con el que nos hemos topado fue que disponíamos solo de equipamiento Cisco que maneja la tecnología Netflow, esto no era una limitante ya que traffic Sentinel tiene la capacidad de colectar y analizar datos de netflow.
Pero nuestro objetivo era usar la tecnología sFlow y necesitábamos un generador de datos sFlow. Recordemos que la potencia de netflow y sFlow a grandes rasgos radica en que esta embebido en los mismos equipos de comunicaciones, esto permite visión completa de lo que ocurre y pasa en una red o redes.
Sobre un servidor Linux (fisgon) montamos en una de las placa un demon (servicio en Linux) que toma datos de una placa de red y genera los paquetes con el formato sFlow, este desarrollo es llamado "sFlow agent" que puede tomar y muestrear trafico IP de una placa ethernet, este muestreo es mandado según el estándar sFlow por trafico udp a un colector, para su análisis en este caso usamos los productos de Inmon.
Un paso previo a ver si funcionaba correctamente sFlow usamos un producto también de Inmon que se llama sFlowTrend. Idéntica operación se realizo con Netflow se probaron varios agentes pero se optó por usar el mismo embebido en los router Cisco, y se probaron varias herramientas mas difundidas para medir el desempeño.
Como se explicó anteriormente a la herramienta *traffic sentinel,* se le envió el muestreo de todo el trafico de entrada y salida del CeSPI a Internet, se muestreo con sFlow y Netflow buscando adicionalmente un comparativo del ambas tecnologías. El tráfico máximo que debía muestrearse era en ese momento aprox. 17Mbps.

Con esta herramienta pudimos detectar tráfico peer-to-peer, variados tipos de ataques, trafico de tiempo real de VoIP, abusos de servicios.
También se detecto escaneos desde y hacia Internet.
Se encontró una potencialidad especial en esta herramienta (Traffic Server) ya que integra con el análisis de trafico intrínseco de la herramienta, con el uso y aplicación de reglas de detección de patrones de Snort, usando muchas de sus reglas. Esta herramienta Snort es un desarrollo que se aplica a soluciones de IDS (intruction detection system) [31].
Inmon llama a esta tecnología NBAD (Network Behavior Anomaly detection o en castellano detección de tráfico anormal en la red). Esta tecnología permite detectar los problemas más típicos y ataques más comunes, como gusanos, ataques intensivos a Servidores, etc. Y adicionalmente tiene la flexibilidad de escribir reglas de detección manualmente o las propias reglas de Snort. Se pueden definir con reglas claras cual es la política de lo permitido sobre una red y esta herramienta verifica el cumplimiento, esto es una idea muy innovadora para imitar ya que esto permite mucha flexibilidad y adaptabilidad a cada red.
Las reglas de Snort aplican solo a las que se refieren a los primeros 127bytes del paquete IP ya que es lo que por defecto analiza y muestrea sFlow, esto para el caso que se pretenda buscar patrones en el payload.
Con esto detectamos gran cantidad de patrones de tráfico que nos ha dejado absolutamente sorprendidos. Con esto permitió a los administradores de la red de filtrar atacantes internos y externos.
Con estas herramientas se hicieron reportes como los que se muestran a continuación.
Permitiendo analizar patrones de tráfico, consumo de recursos de un usuario o un servidor, sobre todo se busco lo anormal.
Otra ventaja de netflow y sFlow es detectar servidores aun sin conocer los mismos, esto a una persona como un administrador con amplio conocimiento de la red es de suma utilidad.

7.0 Optimización de tráfico

7.1 Introducción

Una de las aplicaciones de este trabajo es ser la guía para optimizar trafico, pero primero debemos entender porque queremos hacerlo, considerando también si es necesario tal optimización. Necesitamos saber con que equipamiento de red contamos para aplicar mencionada optimización, debemos planear estrategias basando el diseño, pensando en un sistema distribuido o centralizado de control. Establecer diferencias entre “control de tráfico” y “optimización de tráfico”.
Es muy importante: Conocer las posibilidades técnicas con las que cuentan los equipos de comunicaciones para aplicar este control/optimización del tráfico. La topología de la red puede ser tipo mallada, estrella o combinación, puede tener varios puntos de concertación. Caracterizar las aplicaciones si son del modelo cliente-servidor, si tiene servidores centralizados o distribuidos, si hay aplicaciones con bases de datos, etc. Este punto debería llevar bastante atención ya que muchas veces nos encontramos con aplicaciones que usan en forma poco eficiente los recursos de red en pro de simplificar y acortar tiempos de desarrollo o esfuerzos de procesamiento. Otras aplicaciones dejan gran parte del procesamiento a los clientes o por cada solicitud hacen pequeñas transferencias de datos, esto hace que las aplicaciones se vean como pesadas o lentas si la red tiene mucho delay. Es común hoy en día encontrar aplicaciones que fueron diseñadas para correr en una arquitectura como minino a 100Mbps cuando todavía no es común ver muchas redes con esa capacidad.

7.2 Definiciones

Antes de proseguir tratemos de aproximarnos a la definición de "optimizar tráfico" y "controlar trafico", marcando la diferencia entre ambos. Generalmente cuando hablamos de optimizar tráfico nos referimos literalmente a tratar de hacer que las aplicaciones de red funcionen lo mejor posible con el/los enlaces y ancho de banda del que disponemos. Un problema típico es que se compran o usan aplicaciones sin tener en cuenta el impacto en una red o si la red montada va a soportar la aplicación.

7.3 Optimizar tráfico

Apunta a tratar a que con el enlace/red que disponemos las aplicaciones funcionen regularmente bien apuntando a la sensación o percepción del usuario de esa aplicación sea siempre la misma. Acá se introdujo un concepto "percepción del usuario" casi el mas importante ya que las redes son usadas en general por personas, que son las que le dan el concepto variables y dinámicas. Si los usuarios observan que la aplicación que usan responde siempre igual no le generara sensación de malestar, como si ve que un día o a una hora determinada le responde en 1seg y en otro momento le responde en 3 o 4seg.

7.4 Control de tráfico

El control de trafico pasa mas por restricciones de acceso de uso o limitaciones de uso de recursos que tienden a ser objeto de abuso por parte de los usuarios, un ejemplo típico es el acceso a navegación Internet sin restricciones , hay usuarios que respetan y entienden que no pueden abusar de los recursos, porque están en un ambiente compartido o en un ámbito laboral , mientras que otros usuarios no tienen el mas mínimo reparo en cuestiones mínimas de respeto o uso, a estos usuarios hay que tratar de controlar. Otro objeto de control frecuente es la distribución de parches de los sistemas operativos, distribución de patrones de antivirus, up-date/up-grade de aplicaciones, instalación de aplicaciones en los servidores y estaciones de trabajo conectados a la red. Es normal que no se preste atención hasta que generan un "denied of service". El control de trafico debería ser de uso mas frecuente tratando de evitar estas denegaciones de servicios por los mismos administradores de sistemas, que sin medir consecuencia muchas veces degradan el servicio porque aumentan los delay y aumentan la perdida/descarte de paquetes, con lo que aumentan las retransmisiones de aplicaciones TCP que contribuyen a degradar aun mas los enlaces. Si bien la situación comentada mas arriba no es buena, sirve para conocer la capacidad del enlace o de una red. Otro caso típico es las aplicaciones o procesos que se descontrolan y saturan la red, un ejemplo es los resolver de DNS que se enloquecen y comienzan a hacer pedidos a la máxima capacidad del procesador. Si nos ponemos a pensar en la cantidad de posibles factores que pueden saturar una red nos damos cuenta que es muy vulnerable si los router se dedican solo a rutear paquetes, los router mas modernos traen implementados controles para analizar y tomar decisiones con determinados patrones de tráfico. Hay servicios críticos de red que hay que proteger/monitorear como los servidores de DNS ya que la mayoría de las aplicaciones dejan de funcionar porque dependen altamente de los DNS. Con esto queremos resaltar que hay servicios vitales en una red que tenemos que proteger de abusos haciendo control de tráfico. Control de trafico también apunta a dejar pasar solo las aplicaciones aprobadas en una red, este es el caso ideal tener bien controlado que si y que no en una red pero si bien parece el ideal es muy laboriosos de mantener, con lo cual generalmente se llega a la concesión de limitar o denegar lo malo (pero malo conocido).

Nuestro objetivo es optimizar tráfico para esto tenemos que "definir políticas".

7.5 Políticas

Para definir políticas de uso en una red o políticas de tráfico requiere de muchos factores, pero podríamos definir que son reglas a aplicar basados en "indicadores""métricas", "criterios políticos/corporativos", requerimiento de las aplicaciones, etc. Para definir políticas tenemos que fijar criterios y establecer las métricas a utilizar, no dejando de lado la caracterización de las aplicaciones.

7.6 Métricas

Las métricas casi obligatorias son el volumen de tráfico, errores en las interfases, pérdida de paquetes, uso de CPU de los equipos de comunicaciones y paquetes por segundo (pps). Estas métricas son actualmente incompletas sin una forma eficiente y escalable de medir y caracterizar que tipo de tráfico ocupa ese volumen. El delay rtt (round trip time) es otro parámetro importante, así como el one-way-delay, esto nos da detalles para caminos asimétricos o enlaces con diferencias de carga en transmisión que en recepción y nos permitirá establecer en que sentido del trafico tenemos problemas. Todo lo que hablamos apunta a ofrecer calidad de servicio en los enlaces.
No debe perderse de vista es que siempre deben funcionar las aplicaciones en producción, en lo que dependen de las redes de datos, es decir que la interrupción de servicio o de una aplicación no se deba a un mal diseño o previsión de la red. Lo anteriormente es el ideal, en la realidad, se debe considerar que todo tiene un costo económico o al menos la mayoría de las cosas, por ejemplo si a un lugar se accede por un solo enlace, si se cae (este único vinculo) es inevitable la pérdida de servicio. Los router con capacidad de realizar muchas de las tareas mencionadas son obviamente más costosos que los que simplemente rutean o similar es el caso de los switch (de capa 2 modelo OSI), por suerte es muy importante es los casos de bajo presupuesto los Linux y las aplicaciones GNU para esto, ya que muchas de las capacidades de un router cisco se pueden implementar en Linux, claro a un alto costo de desarrollo y conocimiento. Lo que estamos describiendo es este documento trata de ser de índole general pero esta enfocado a una red universitaria en la que hay un cierto presupuesto para equipamiento pero es mas valiosos y abundante la capacidad de los estudiantes y egresados de la misma que pueden aportar conocimiento y horas de desarrollo para suplir faltas de presupuesto, también muchas veces no se justifica el costo.
Antes de seguir adelante definamos los siguientes términos:

Sitio, sería una oficina o lugar remoto que depende de uno o más vínculos para conectarse a los servicios/servidores de red.

Vínculos, para este caso nos referimos a enlaces WAN o LAN, por el medio físico que sea (cobre, fibra, radio-enlace, etc.) conectando sitios.

Punto o centro de estrella, nos referimos a la topología de red, seria donde por costos o por ubicación geográfica concentra enlaces a varios sitios de la red. En este punto de estrella generalmente se encuentra por conveniencia los servidores donde corren las aplicaciones y servicios de red.

Red mallada o estrella, se refiere a topología de red.

7.7 Métricas adoptadas

Definamos que métricas deberíamos a tener en cuenta.

Volumen de tráfico, el estándar hasta el momento es obtener esta métrica, vía el protocolo conocido como SNMP (Simple Network Management Protocol). Para servir debería estar detallado básicamente por enlace y como se lo colecte depende de la topología y tecnología de red utilizada. Debe estar discriminada entre transmisión y recepción por enlace. Todas las estadísticas colectadas por SNMP deberían tener la granularidad adecuada para hacer un análisis de por ejemplo perfil de tráfico o crecimiento del mismo.

CPU, también vía SNMP monitorear el uso del los CPU de los equipos de comunicaciones, que es muy importante para tener una visión de la performance de la red. Un equipo que hace la función de layer 2 o 3 que hacer el forwardeo y análisis de trafico con el CPU y que esta cercano al 100% afecta al forwardeo de paquetes aumentando en el mejor de los casos el tiempo de transito de paquetes dentro del equipo en cuestión o descartando paquetes que no puede procesar. Claro esta que no todos los equipos de comunicaciones soportan esto.

Estadísticas de PPS, los pps son los paquetes por segundo en un enlace, esta métrica están importante como el volumen de trafico antes mencionado ya que puede por ejemplo se el causante de aumento de uso de CPU en un equipo de comunicaciones y la consiguiente degradación de performance de un enlace no por volumen de trafico sino por volumen de paquetes.

Estadísticas de Dropeos o Descartes, la estadística de descartes de paquetes depende de la estrategia utilizada en el tratamiento de los mismos en un equipo de comunicaciones. Tener una visión de cuantos paquetes son transmitidos y que cantidad son descartados (o dropeados) podemos conocer y estimar o corregir los buffer de las colas de calidad de servicio implementados en los router, o incrementar la cantidad de memoria utilizada para buffers de transmisión por los interfases físicas. Deberíamos tener en cuenta que tocar los buffer de memoria de los routers hace que haya menos paquetes descartados y un uso mas eficiente de los enlaces pero todo tiene costos ya que con esto se aumenta el delay de paquetes de llegar de un extremo a otro de un vinculo no solo por el delay intrínsico del medio de transmisión utilizado sino también al delay de transito por el equipo de comunicación.

Delay rtt y one-way-delay, cuando nos referimos al delay hacemos referencia al retardo de ida y vuelta del un paquete típicamente se mide con ICMP y es la suma del retardo de ida y vuelta es valido pero nos falta información ya que un enlace puede tener mas carga en un sentido que en otro , los caminos de ida y vuelta de un paquete puede no ser el mismo , como con túneles de la nueva tecnología de conmutación de paquetes llamado mpls (un protocolo que esta en el medio de capa 2 y 3 del modelo OSI , se le dice que es capa 2 ½). El delay es la suma del tiempo que tarda un paquete en ir y venir desde un punto de partida. Pero nos falta información por eso hay que buscar técnicas para medir el tiempo de ida y vuelta por separado conocido como one-way-delay. La suma de tiempo de transito de ida y vuelta se lo conoce como delay rtt (round trip time). Tener la medida más la variación de paquetes one-way-delay es de suma importancia para aplicaciones de video y voz sobre IP, ya que esta medida va a ser correlativa con la calidad de video y audio. Estas

aplicaciones soportan relativamente alto delay pero no soportan muy bien las variaciones, claro esta que si las aplicaciones de VoIP y VidoIP pueden estar diseñadas para agregar buffers que aumenten el delay para amortiguar las variaciones de Delay en la red, pero esto va en desmedro de el real-time buscado en una llamada con VoIP por ejemplo, igualmente el cerebro humano puede compensar esa falla, pero en la practica y de mi experiencia se deduce que se dificulta la comunicación entre las personas ya que hace que el intercambio de palabras sea dificultoso sobre todo cuando se intercambian opiniones. Con este último párrafo hacemos otra vez referencia a percepción del ser humano en las aplicaciones.
Retomando el tema del delay debemos conocer el delay que soportan las aplicaciones y los usuarios de las aplicaciones. Hay aplicaciones interactivas llamadas on-line en la que se ingresan caracteres y se espera una respuesta. Una aplicación de las llamadas on-line a través de un enlace con un delay en el orden de los segundos puede provocar la ira del usuario (y puede provocar daños a las instalaciones hasta puede llegar a insultar al jefe… bueno es una forma de decir).

Estadísticas de tráfico, esta es la aplicación de esta tesis, debe obtenerse un detalle del tráfico, la tecnología escalable es sFlow y netflow ya explicados en la tesis. Haremos una breve reseña sobre este tema, lo primero que se desarrollo fue un programa que captura y muestra paquetes llamado tcpdump, que toma paquetes de la placa de red Lan para ser analizados por los humanos mediante una interfase de texto. Este método para analizar grandes volúmenes de tráfico genera a una cantidad de datos difícil de manejar y muy costoso en tiempo y uso de CPU de la PC que no analiza. Este problema fue inicialmente solucionado con las estadísticas Rmon evolucionando hasta llegar a un RFC que es el sFlow que usa estadística de muestreo haciendo escalable a redes con enlaces Giga bit por segundo, esto reduce tiempo de CPU para generar la información y reduce capacidad necesaria para procesar esos paquetes de información. Otro método similar es el Netflow de Cisco un poco menos ambicioso pero adaptado a las redes actuales, lo único que aun no abarca aun es layer 2 pero no esta tan desacertado ya que la mayoría de los problema están en los enlace de baja velocidad y con capacidad de saturarse. sFlow esta también pensado para la facturación en base al tráfico cursado en el medio que sea. Ambas tecnologías son un modelo cliente servidor particular, hay mas servidores que clientes, muchos equipos de comunicaciones que generan paquetes sFlow y netflow y generalmente un solo colector para centralizar y analizar la información.
Con netflow y sFlow podemos tener estadísticas agrupadas por protocolo, por aplicaciones por origen, por destino, la combinación que sea más útil.
En base a estas estadísticas podemos idealmente tener una visión completa de una red, y nos brindaría los indicadores que estamos buscando.

Luego definiremos con que producto colectaremos estos datos.

7.8 Indicadores y criterios

Pasemos a definir indicadores y criterios.

Criterios:

- Buscar la no interrupción del servicio en lo que dependa de las redes, esto es lo ideal y no siempre es posible
- Enlaces optimizados para aplicaciones productivas
- Caracterizar y agrupar aplicaciones

Grupos posibles: VoIP, VideoIP, on-line, Web, non-on-line (por defecto, default en ingles)
Esta lista define prioridades:

- Medir abusos y restringirlos
- Asignar un volumen de tráfico por semana a cada sitio, pasado este volumen de tráfico penalizarlo (al sitio). Esto se aplica en algunas universidades con campus universitario.
- Usuarios VIP
- Separar en Vlan cada unidad académica (aplica al la UNLP)
- Contar con todos los elementos de seguridad de una red, IDS, Firewall, estadísticas

7.9 Métricas y caracterización de aplicaciones

El nivel de detalle de tráfico obtenido con sFlow y Netflow debería ser tal que se pueda guardar estadísticas por el mayor tiempo y con la mayor granularidad posible, esto naturalmente debe forzosamente ajustar a la capacidad de almacenamiento con que se dispone y al mismo tiempo evaluando si se justifica guardar las estadísticas por el tiempo que se desde.

Seria importante que se colecten varios reportes como:

- Discriminación por puertos TCP, UDP
- Estadísticas que reconozcan aplicaciones, como VoIp, video, streaming, p2p
- Estadísticas por Servidor
- Estadísticas por enlace o por redes, con esto podríamos determinar y analizar el funcionamiento de un enlace, patrones normales, incrementos de cierta aplicación
- Una métrica muy importante es el tiempo de respuesta de un servidor. Por ejemplo tener un equipo que intercepte los paquetes y analice y capture la respuesta de un servidor, como los "get" de http a un servidor y sus respectivas respuestas, con estos dos paquetes y descontando el one-way-delay obtener el tiempo de respuesta de un servicio. Esto puede ayudar a diagnosticar un problema y corregirlo. Es común encontrar usuarios que se quejen que la red anda lenta y teniendo estas estadísticas podremos determinar si lo que falla es la red o el tiempo de respuesta del servidor/servicio. Con esto también podremos dimensionar un servidor/servicio o balancear carga ofreciendo calidad de servicio.

7.10 Tiempo de respuesta

Es importante medir el tiempo de respuesta de los enlaces y sumado a la carga del mismo nos ayudará a medir la calidad del enlace. Con esto veremos que es lo normal de un enlace y controlar el SLA contratado a un proveedor. SLA del ingles service level agreement, y es el nivel de servicio acordado y contratado a un proveedor. Es típico en enlace de hoy en día la sobre-suscripción en los enlaces por parte de un proveedor para hacerlos económicamente mas rentables, pero esto va es desmedro del usuario final (hace unos años típico problema de enlaces de Frame-Relay y hoy en día enlace hdsl o adsl). También este es un problema en las redes con tecnología mpls muy de moda en estos días. Con mpls se acuerda con el proveedor varios parámetros que conformaran el SLA, los

más habituales con el ancho de banda de acceso al medio, tiempos de respuestas, variación del mismo, colas de calidad de servicio y por sobre todo disponibilidad.

7.11 Disponibilidad

Esta métrica es muy importante tenerla disponible y la se define como el porcentaje del tiempo que el medio/enlace esta disponible para transmitir datos, generalmente se acuerda con el proveedor el intervalo de medición. Se habla en general de 99,7% como un buen enlace y cuanto mas cercano al 100% mas caro es el enlace (claro esta que muchas veces los proveedores no lo respetan y son solo métricas comerciales, ya que muchos proveedores de enlaces saben que los cliente no verifican ni miden esto). Para el caso de ser dueños del enlace nos va a permitir medir la calidad para futuras mejoras.
Todo lo definido en este Apéndice, servirá para controlar los niveles de servicio de un enlace o red, evitar cuellos de botella en la red, haciendo ingeniería de tráfico, evitando abusos y congestionamiento, todo apuntando un nivel de servicio.

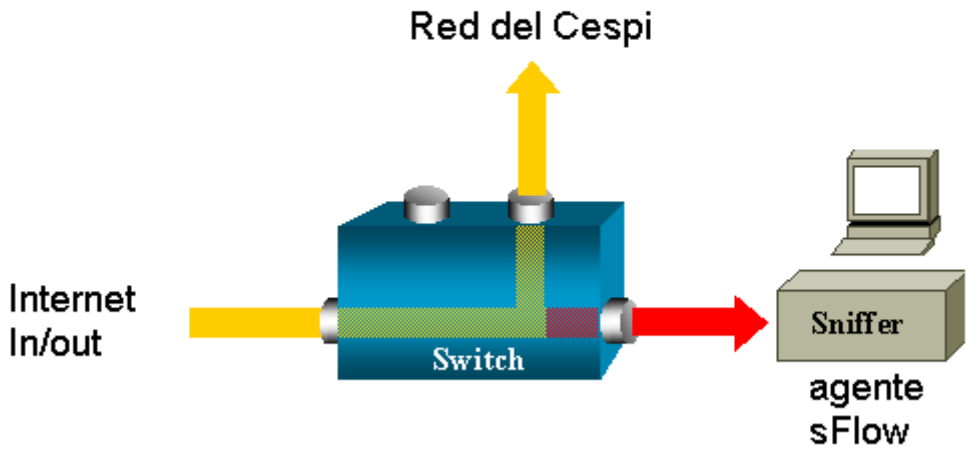
8.0 Medidas Realizadas

A continuación se mostraran algunas de las medidas tomadas utilizando netflow, sFlow y sniffer. También se muestran gráfico para presentar como lucen las herramientas utilizadas.
En la red del CeSPI se usó la tecnología "Span" de Cisco, para generar una copia de tráfico de entrada y salida a Internet.
Se instaló bajo Linux el agente de sFlow [30] con el fin de generar datos sFlow, esos datos fueron enviados al colector sFlowTrend [28], para su análisis.
Se uso la herramienta iptraf [11] para corroborar los datos obtenidos vía estadísticas sFlow.
La herramienta sFlowTrend toma los flujos de datos más significativos, por eso es necesario realizar filtros.
Para un volumen aproximado de 30Mbps de Internet Internet, el agente sFlow genera un tráfico continuo de datos, en sentido "agente" a "colector" de aproximadamente 19Kbps. Esto indica que el "agente" muestreando a 1 paquete cada 10, genera un 0,07% del total del tráfico muestreado, esto ya es considerando el overhead de udp.
Por lo tanto para este ejemplo de tener 30Mbps de tráfico, producto de la suma de entrada más salida de Internet, el agente sFlow genera 19Kbps contra el colector sFlow.

Se usaron las siguientes herramientas:

- wireshark
- sFlowTrend usado como "colector sFlow"
- sFlow Agent
- Iptraf
- Snort integrado con el "colector sFlow"
- Tecnología Span/Rspan de Cisco
- Sistema operativo servidor de captura/análisis fue Linux-Debian.

Esquema basico Utilizado



Agente sFlow, expliquemos brevemente el agente sFlow, el mismo esta programado en el lenguaje de programación "C", el agente sFlow tiene parámetros para seleccionar la placa de red en la que se necesita escuchar y cada cuantos paquetes tomamos una muestra, esas muestras es referidas al mismo un mismo flujo de datos. En la página de la empresa Inmon existen documentos y desarrollos que indican que muestrear genera un error despreciable para las mediciones que necesitamos hacer. El ejecutable del agente sFlow es "sflsp" mas los parámetros que se deseen.

La sintaxis para ejecutar el sflsp:

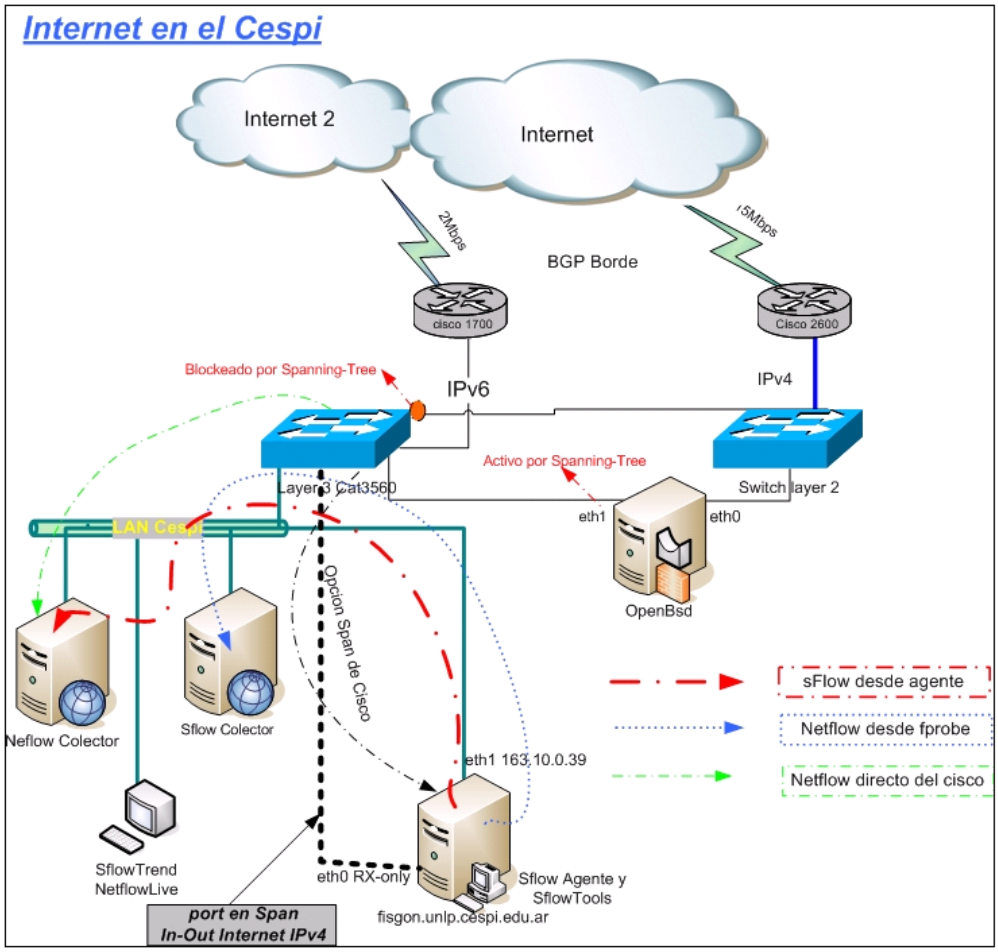
./sflsp [-d device] [-C collectorIP] [-c collectorPort] [-s samplingRate] [-v][-i ifIndex] [-S ifSpeed] [-A agentIP] [-P] [-T]

Copio la ayuda del mismo

-*d device*: la interfase a monitorear ejemplo 'eth0'
-*C collectorIP*: la IP del collector al cual queremos enviarle los sFlow
-*s samplingRate*: 1-in-N muestreo de paquetes
-*v: verbose* - log output (-vv for more detail)
-*i ifIndex*: sobrescribir el ifIndex de snmp
-*S ifSpeed*: sobrescribir el ifSpeed (ejemplo 1000000000)
-*A agentIP*: sobrescribir la dirección IP del agente sFlow
-*P:* forzar la interfase en modo promiscuo
-*T:* mode Test – muestra algunas estructuras

Del agente sFlow se cuenta con el código, por lo tanto si uno desea mandar datos de sFlow a mas de un colector o con parámetros distintos, se puede editar el código fuente y volver a compilarlo. En nuestro caso enviamos datos al mismo colector pero que escuchaba en un puerto UDP distinto del estándar para sFlow.

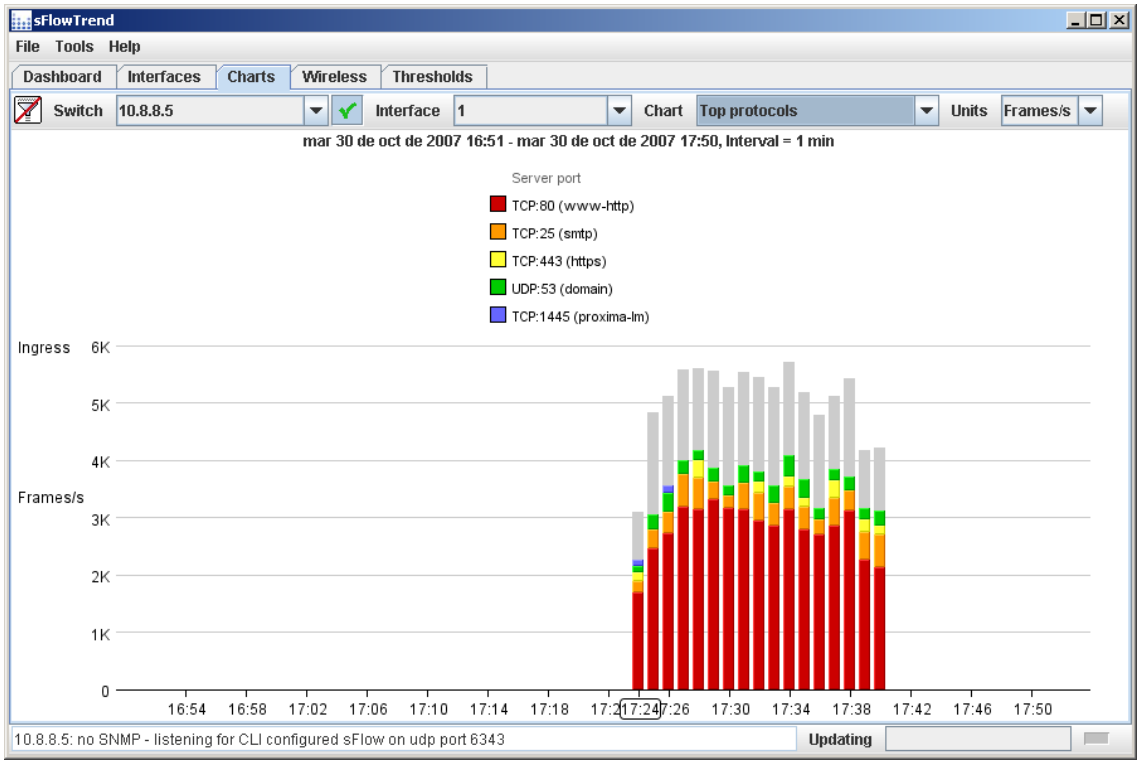
Mostramos nuevamente el esquema utilizado en la figura siguiente

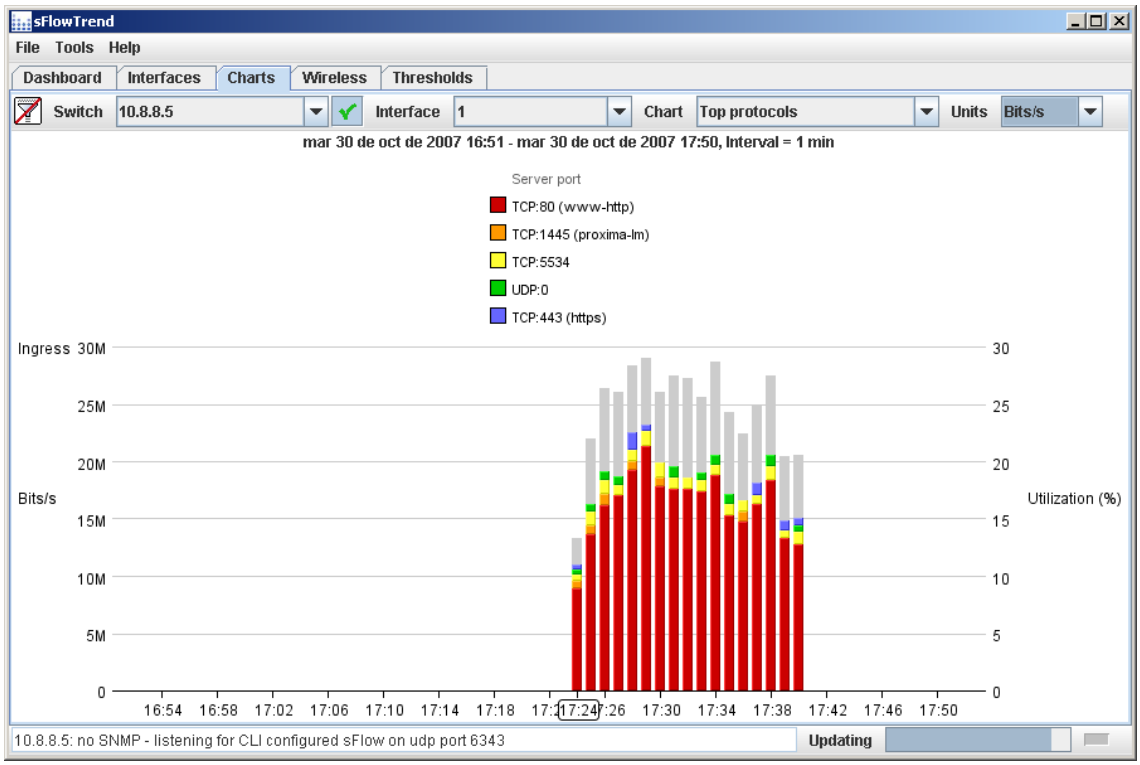


La herramienta sFlowTrend es una herramienta programada en el lenguaje de programación Java, es también de la empresa Inmon, es libre pero no es de código abierto. Esta herramienta puede configurarse básicamente, haciendo filtros o utilizando los preexistentes. Puede mostrar los datos en paquetes por segundo o en bits por segundo. La herramienta sFlowTrend no guarda historial.

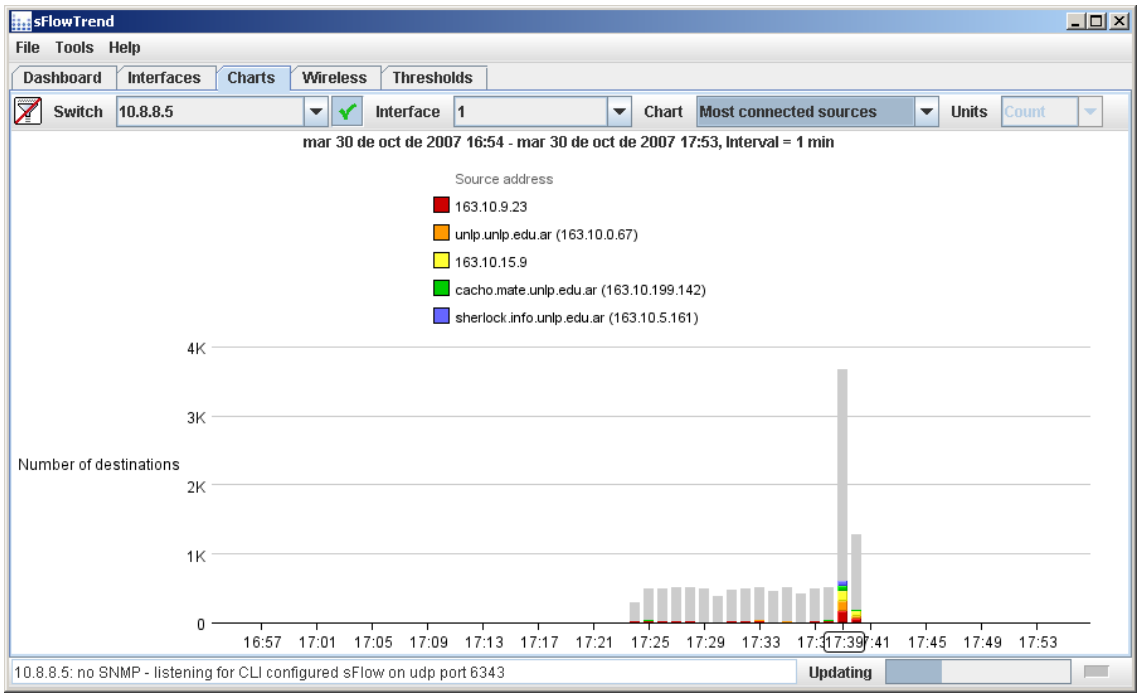
8.1 sFlowTrend luce según vemos a continuación:
Mencionemos que los datos fueron tomados en varios momentos pero estos son de octubre del 2007. Con sFlowTrend es muy difícil encontrar anomalías, no obstante es una excelente herramienta para una visión detallada de lo que esta pasando "instantáneamente" en la red.

Filtro "Top protocols" tanto en paquetes como en bits por segundo, observemos que sigue por color y por barrar cada protocolo, solamente los primeros 5 en volumen de flujo de datos. De este filtro surgió la necesidad de contar con un listado de servicios en la red de la Universidad.

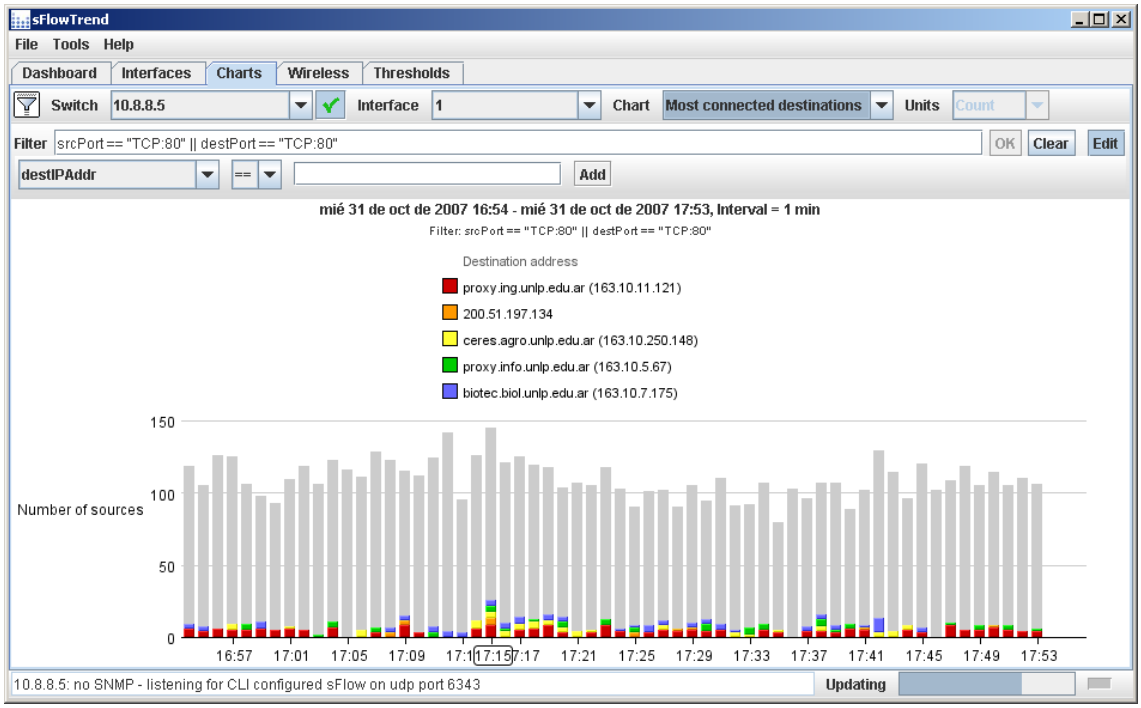


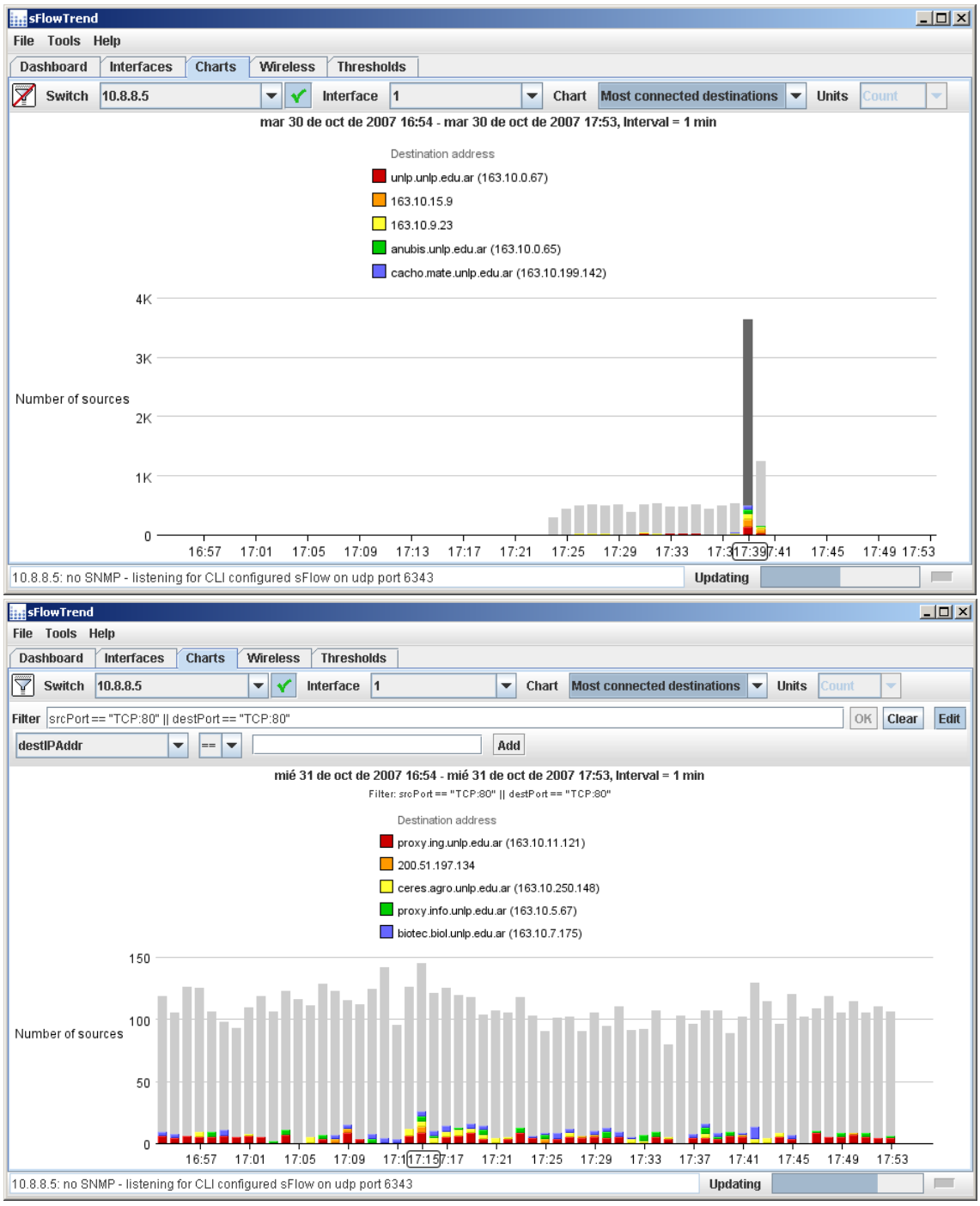


Filtro "Most Connected source", son las Ip origen con mas destinos conectados, de este filtro salió la idea de que había que tener un listado de servidores. Podemos observar que algunos tienen las Inversas de DNS creadas por lo tanto sFlowTrend puede identificarlos, pero otro tanto no los tiene. Al no contar con esa lista no podemos saber si un servidor que tiene 300 conexiones es normal.

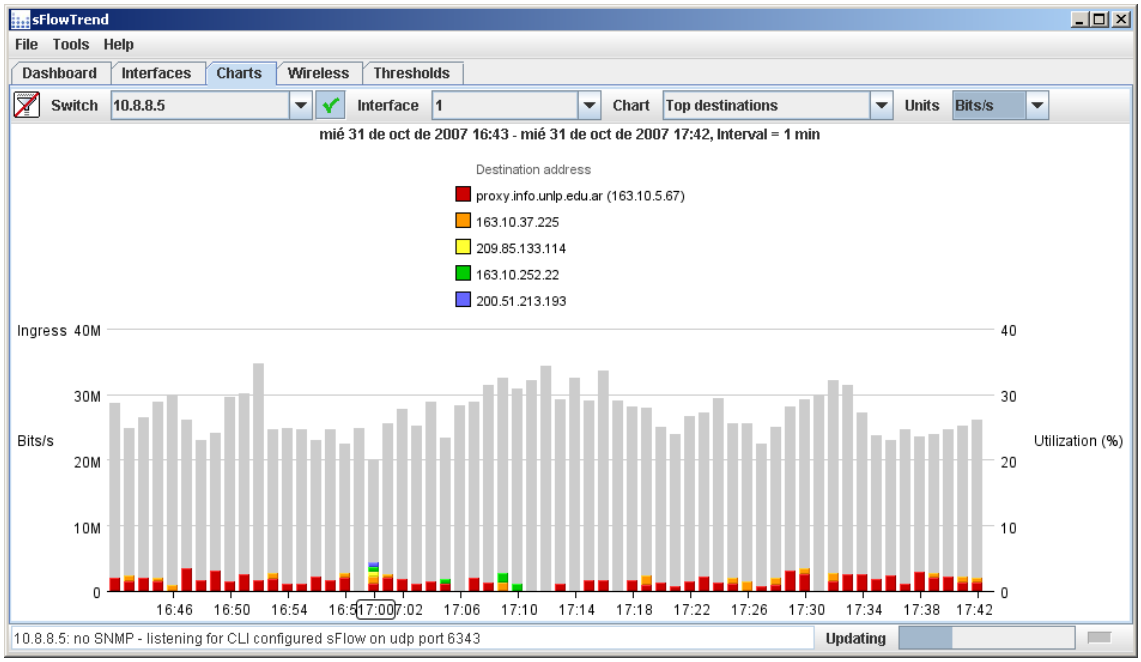


Filtro "Most Connected Destination" similar al anterior pero con el agregado de un filtro personalizado que es filtrar el puerto "http" TCP 80. Otra vez necesario la lista de servidores y servicios, para saber que controlar.

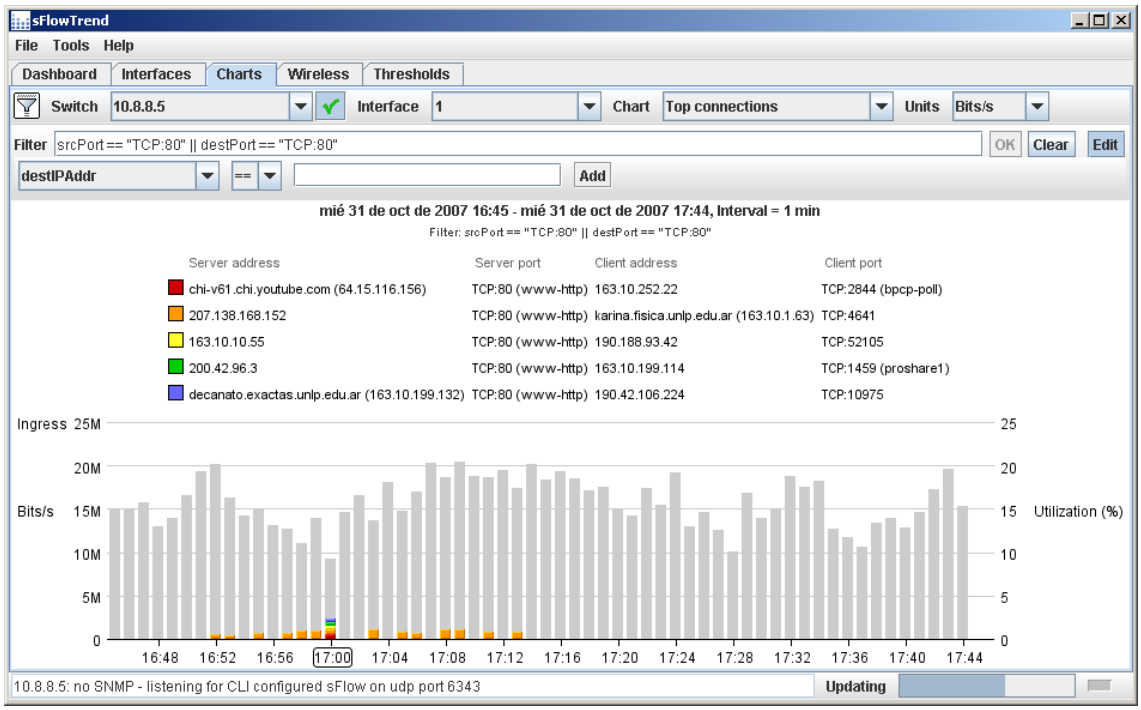




Filtro "Top destination" si se tiene la lista de servicios y servidores se podría aplicar clases de servicio.

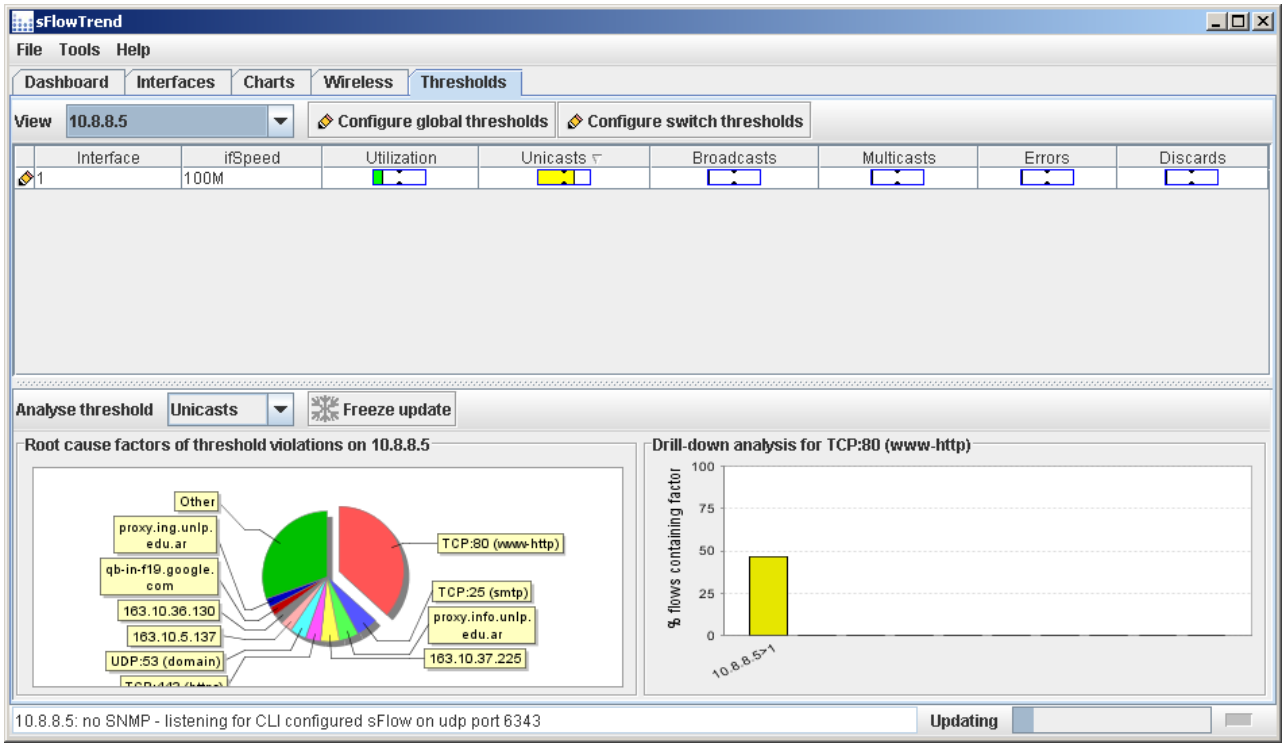


Filtro "top connection", es un filtro interesante donde podemos ver rápidamente cuales son los flujos establecidos con más tráfico. Aquí es donde esta herramienta tiene un lado débil, ya que para una red con muchas conexiones pero de poco tráfico se hace difícil analizar los problemas.

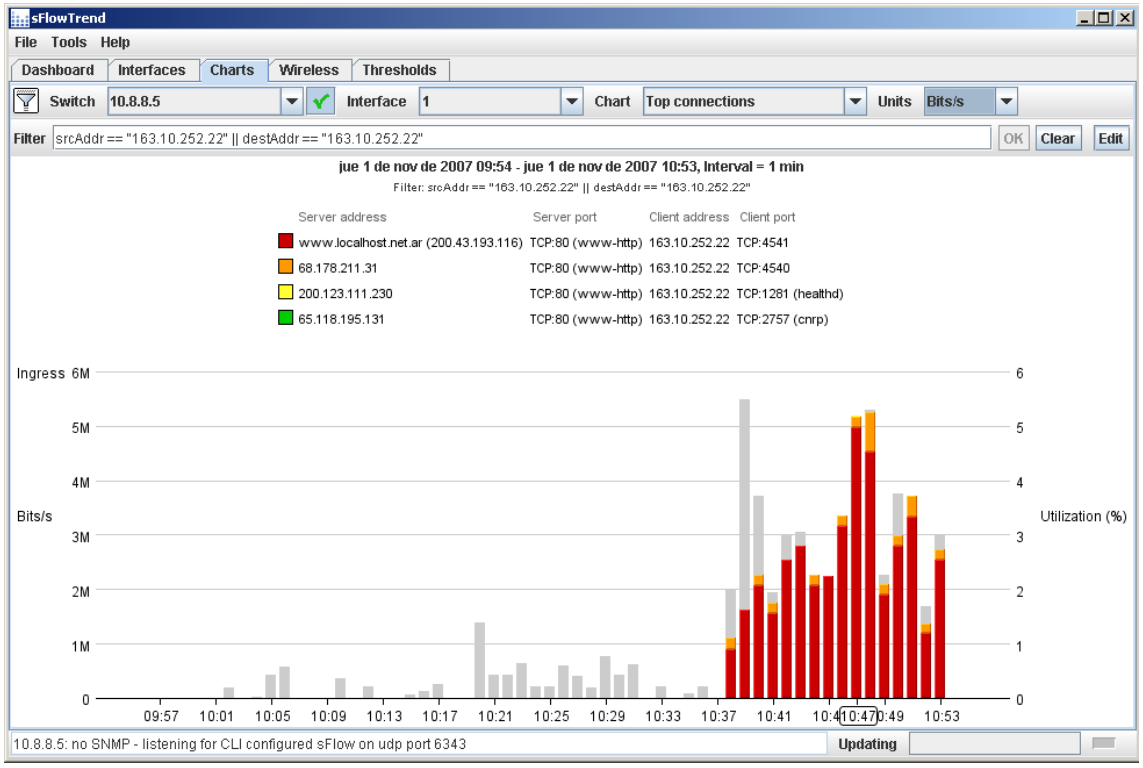


Finalmente una vista interesante es la vista que sigue, allí se observa de manera muy resumida los porcentajes, protocolos, host que más usan recursos.

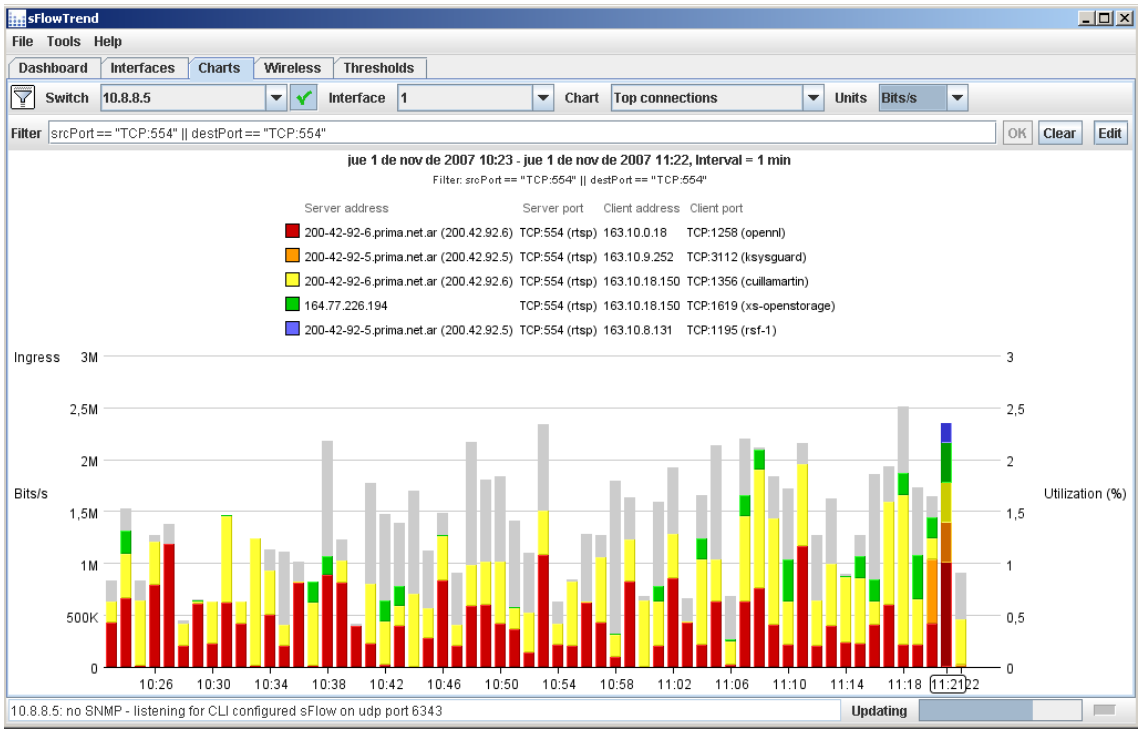
TCP: 80 (http) presente en 55% de los flows
TCP: 25 (smtp) presente en 7% de los flows
Proxy.info.unlp.edu.ar presente en 4% de los flows
Proxy.ing.unlp.edu.ar presente en 4% de los flows
Udp: 53 presente en 3% de los flows



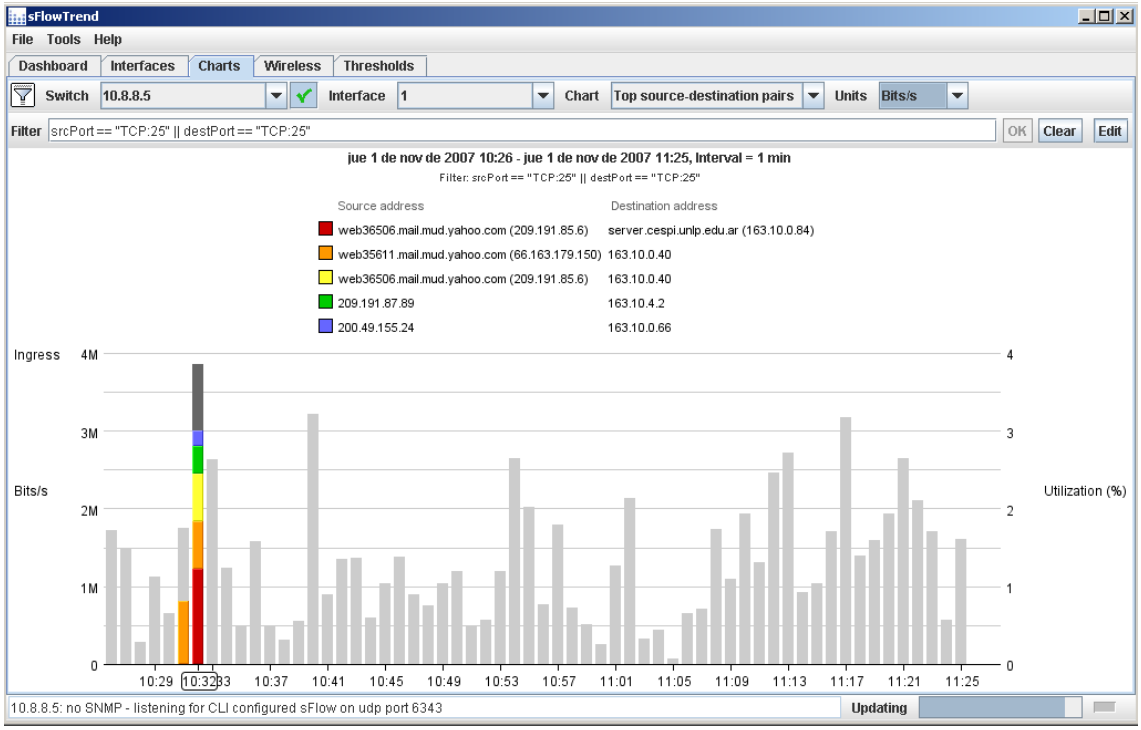
Una anomalía encontrada, un host con 4Mbps de consumo, es normal? Debe limitarse el consumo de este host?



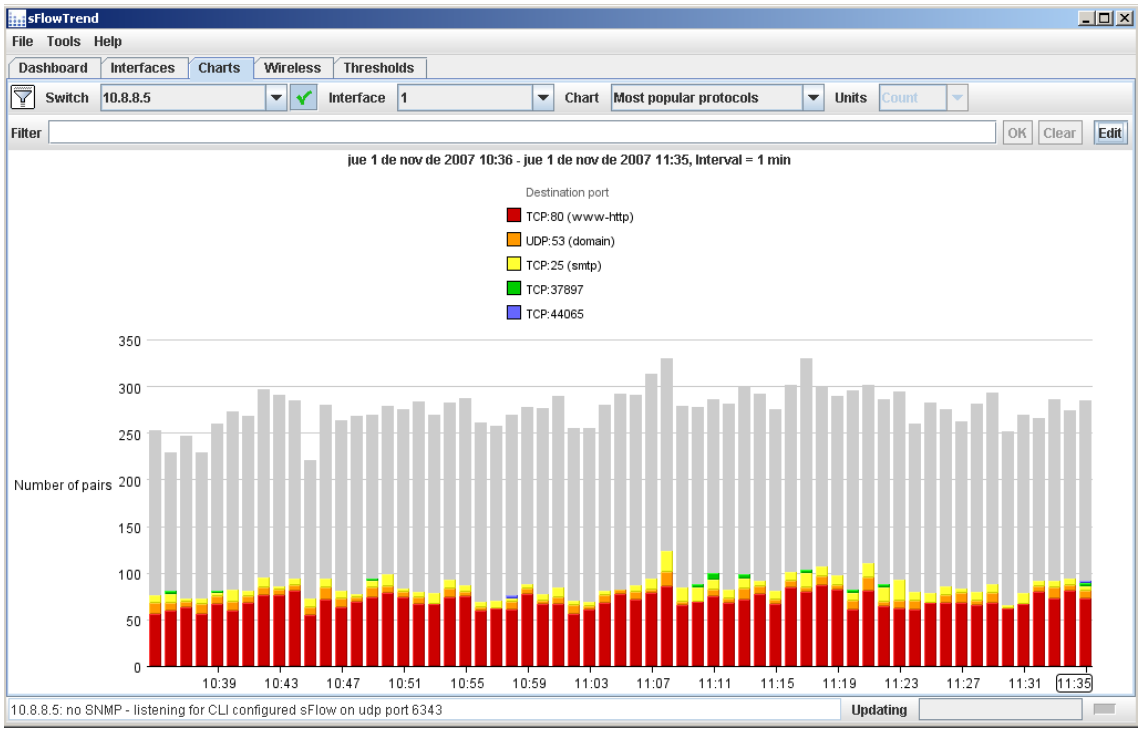
Filtrando por el protocolo TCP puerto 554, filtros como estos sirven para analizar y decidir que hacer con estos puertos.



Filtro TCP puerto 25, es posible que cualquier servidor de la universidad levante el servicio de SMTP? Esta configurado de manera segura para no ser fuente de spam? Planteos como este pueden servir para hacer un uso racional del ancho de banda disponible y no contribuir a los spam.



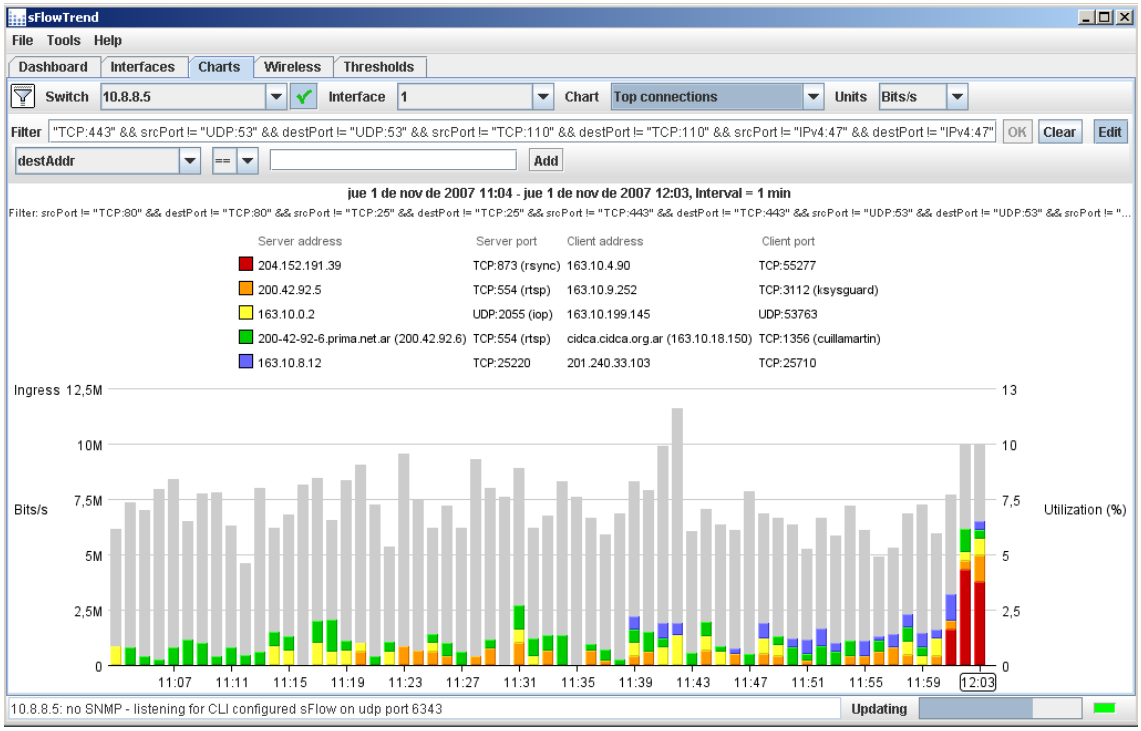
Filtro "most Popular Protocols" para ver los puertos mas relevantes en cuanto al consumo, gráficos como esto mantenidos en el tiempo pueden dar indicación de tendencias o anomalías.



Filtro para detectar anomalías, la idea es filtros eliminativos de los protocolos top, por ejemplo no puerto tcp 80, 443, 53, 25, 110, etc. La idea es ir viendo lo que normalmente es tapado por los protocolos más consumidos.

Sintaxis:

srcPort != "TCP:80" && destPort != "TCP:80" && srcPort != "TCP:25" && destPort != "TCP:25" && srcPort != "TCP:443" && destPort != "TCP:443" && srcPort != "UDP:53" && destPort != "UDP:53" && srcPort != "TCP:110" && destPort != "TCP:110" && srcPort != "IPv4:47" && destPort != "IPv4:47"

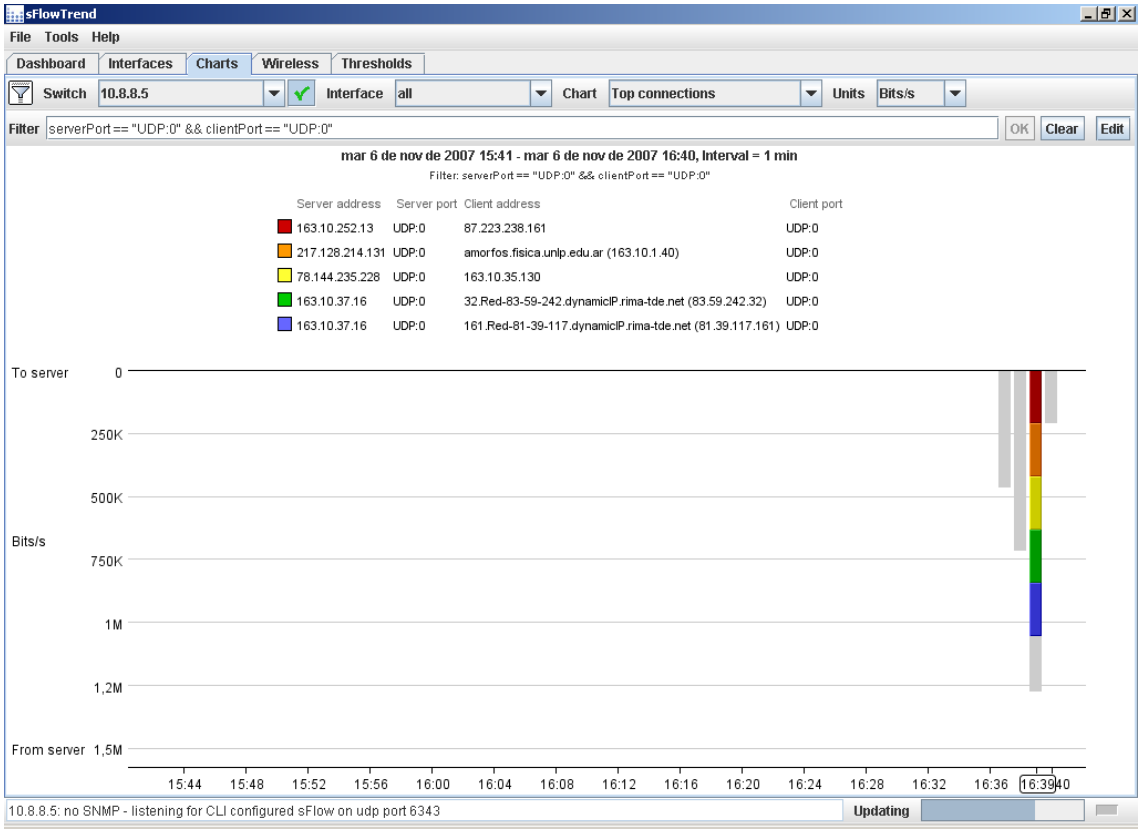


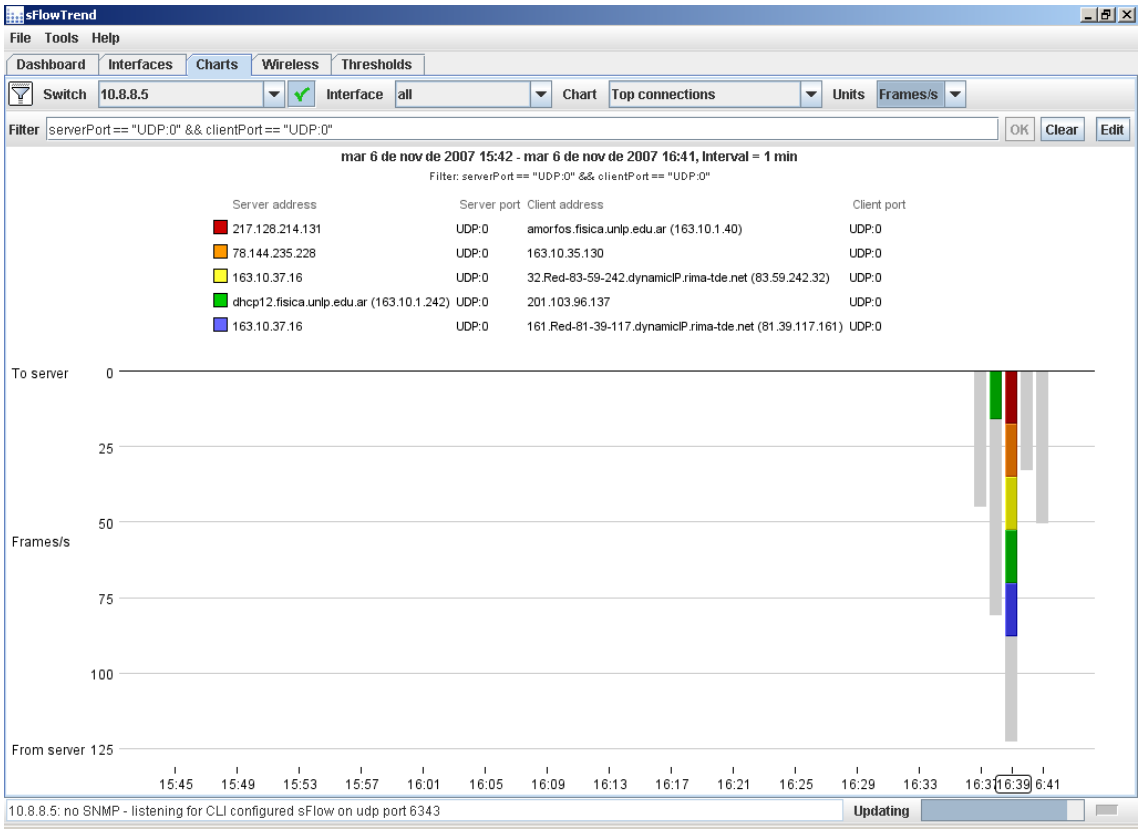
Filtro para sacar lo conocido y detectar anomalías

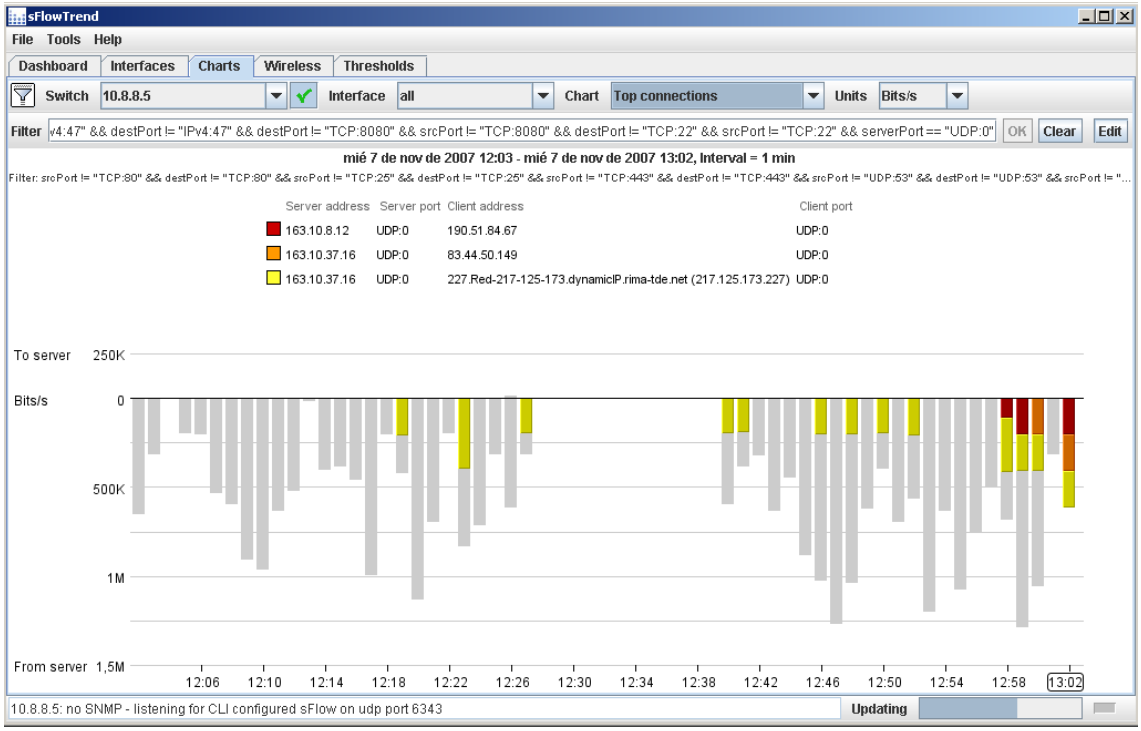
Esta seria la sintaxis:

srcPort != "TCP:80" && destPort != "TCP:80" && srcPort != "TCP:25" && destPort != "TCP:25" && srcPort != "TCP:443" && destPort != "TCP:443" && srcPort != "UDP:53" && destPort != "UDP:53" && srcPort != "TCP:110" && destPort != "TCP:110" && srcPort != "IPv4:47" && destPort != "IPv4:47" && destPort != "TCP:8080" && srcPort != "TCP:8080" && destPort != "TCP:22" && srcPort != "TCP:22"

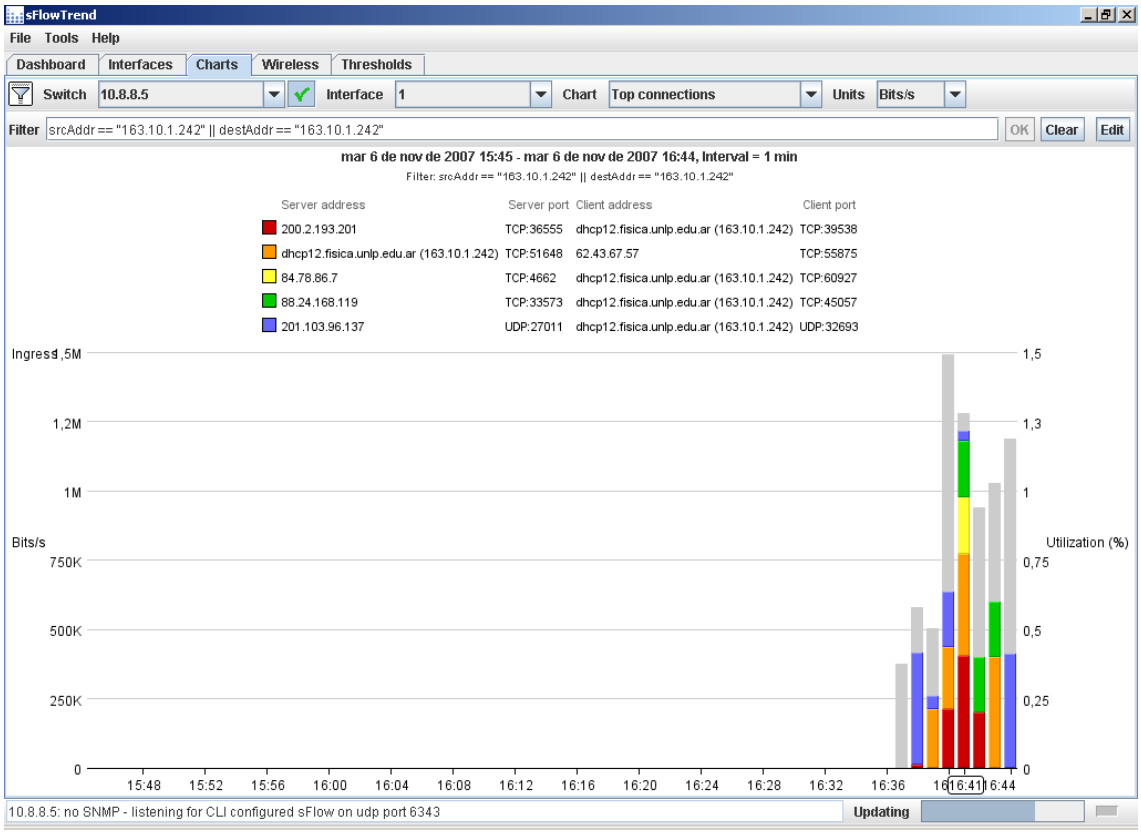
Filtro "UDP port 0" debería estar filtrado, si es que no hay ningún servicio de la Universidad en ese puerto.



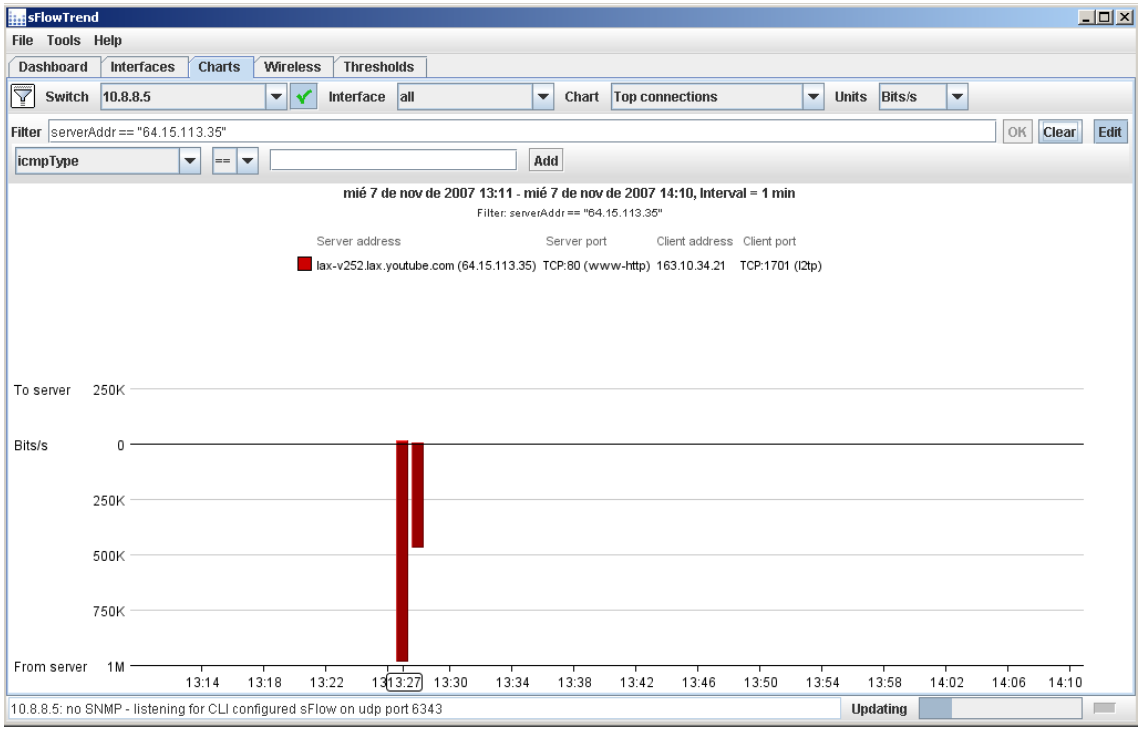

sFlowTrend
File Tools Help
Dashboard Interfaces Charts Wireless Thresholds
Switch 10.8.8.5 Interface all Chart Top connections Units Frames/s
Filter serverPort == "UDP:0" && clientPort == "UDP:0" OK Clear Edit
mar 6 de nov de 2007 15:42 - mar 6 de nov de 2007 16:41, Interval = 1 min
Filter: serverPort == "UDP:0" && clientPort == "UDP:0"
Server address Server port Client address Client port
217.128.214.131 UDP:0 amorfos.fisica.unlp.edu.ar (163.10.1.40) UDP:0
78.144.235.228 UDP:0 163.10.35.130 UDP:0
163.10.37.16 UDP:0 32.Red-83-59-242.dynamicIP.rima-tde.net (83.59.242.32) UDP:0
dhcp12.fisica.unlp.edu.ar (163.10.1.242) UDP:0 201.103.96.137 UDP:0
163.10.37.16 UDP:0 161.Red-81-39-117.dynamicIP.rima-tde.net (81.39.117.161) UDP:0
To server
From server
Frames/s
0
25
50
75
100
125
15:45 15:49 15:53 15:57 16:01 16:05 16:09 16:13 16:17 16:21 16:25 16:29 16:33 16:39 6:41
10.8.8.5: no SNMP - listening for CLI configured sFlow on udp port 6343
Updating


sFlowTrend
File Tools Help
Dashboard Interfaces Charts Wireless Thresholds
Switch 10.8.8.5 Interface all Chart Top connections Units Bits/s
Filter v4:47" && destPort != "IPv4:47" && destPort != "TCP:8080" && srcPort != "TCP:8080" && destPort != "TCP:22" && srcPort != "TCP:22" && serverPort == "UDP:0" OK Clear Edit
mié 7 de nov de 2007 12:03 - mié 7 de nov de 2007 13:02, Interval = 1 min
Server address Server port Client address Client port
163.10.8.12 UDP:0 190.51.84.67 UDP:0
163.10.37.16 UDP:0 83.44.50.149 UDP:0
163.10.37.16 UDP:0 227.Red-217-125-173.dynamicIP.rima-tde.net (217.125.173.227) UDP:0
To server
From server
Bits/s
250K
0
500K
1M
1,5M
12:06 12:10 12:14 12:18 12:22 12:26 12:30 12:34 12:38 12:42 12:46 12:50 12:54 12:58 13:02
10.8.8.5: no SNMP - listening for CLI configured sFlow on udp port 6343
Updating

Filtro para ver un host en particular:



El gráfico a continuación, es un túnel desde la Universidad a un host en Internet, es normal, esto se podría resolver con la lista de servidores y servicios. En el caso de que no este registrado se puede informar al usuario que tiene a cargo esa IP.



8.2 Herramienta Iptraf

En los gráficos que están a continuación vemos las estadísticas de tráfico tomadas durante un poco más de una hora en horario, vemos los puertos más usados y los tamaños de paquetes. Estos datos son tomados del programa "iptraf", observamos muchos paquetes en el rango de 1 – 75 bytes de tamaño, eso habría que ver a que se debe.
La sintaxis utilizada:
iptraf -s eth1 -t 1440 -L tcp_udp_services-eth1_24hs.log

IPTraf			
Packet Distribution by Size			
Packet size brackets for interface eth1			
Packet Size (bytes)	**Count**	**Packet Size (bytes)**	**Count**
1 to 75:	3792636	**751 to 825:**	42560
76 to 150:	610974	**826 to 900:**	43779
151 to 225:	214115	**901 to 975:**	31211
226 to 300:	119601	**976 to 1050:**	23268
301 to 375:	96537	**1051 to 1125:**	39077
376 to 450:	87574	**1126 to 1200:**	25483
451 to 525:	99992	**1201 to 1275:**	18069
526 to 600:	145331	**1276 to 1350:**	24562
601 to 675:	122291	**1351 to 1425:**	275394
676 to 750:	41587	**1426 to 1500+:**	3003546
Interface MTU is 1500 bytes, not counting the data-link header			
Maximum packet size is the MTU plus the data-link header length			
Packet size computations include data-link headers, if any			

La siguiente tabla vemos que hace falta filtrar, por ejemplo netbios hacia y desde Internet, snmp, udp y TCP 1, servicios como la hora por NTP podría brindarse en el CeSPI, etc. Se investigo más y se encontró una de las recomendaciones brindadas y es seguir algunas de las medidas de seguridad analizadas por la agencia NSA [34].

IPTraf						
Proto/Port	Pkts	Bytes	PktsTo	BytesTo	PktsFrom	BytesFrom
TCP/443	269816	117188K	138252	34748423	131564	82440357
TCP/80	4865028	3735M	2086702	280381K	2778327	3454M
TCP/25	660631	360263K	375708	340931K	284923	19332069
TCP/22	148265	33753681	45030	3053465	103235	30700216
UDP/53	403565	47952627	236114	19064196	193154	31951966
TCP/20	47118	40728384	20504	1925601	26614	38802783
TCP/21	6116	429682	3139	169440	2977	260242
TCP/554	24264	17834568	10813	510172	13451	17324396
TCP/113	9776	556474	8113	483018	1663	73456
TCP/85	3926	2835931	2584	2776882	1342	59049
TCP/90	1214	602369	600	146532	614	455837
TCP/110	28548	17423558	11047	547156	17501	16876402
TCP/53	926	66996	473	23592	491	44940
UDP/21	182	23750	167	22007	15	1743
TCP/995	20618	11514054	8187	524029	12431	10990025
UDP/123	2979	226544	2901	220616	2880	218880
UDP/85	4	296	1	46	3	250
TCP/23	229	12680	218	11335	11	1345
UDP/202	3	288	0	0	3	288
UDP/137	930	89699	868	84623	192	18437
UDP/1	146	17005	81	9915	65	7090
TCP/143	1517	396384	628	109588	889	286796
TCP/993	2211	388815	1075	100378	1136	288437
TCP/445	493	23764	459	22404	34	1360
UDP/443	2	262	2	262	0	0
TCP/667	55	2640	55	2640	0	0
UDP/1000	8	893	4	516	4	377
UDP/126	2	361	1	214	1	147
UDP/81	22	2079	12	1193	10	886
TCP/1001	88	55066	46	12657	42	42409
UDP/161	2845	237454	1665	134712	1180	102742
UDP/80	165	20083	112	13426	53	6657
UDP/203	1	96	0	0	1	96
TCP/1	290	87706	186	12284	104	75422
UDP/55	14	985	2	144	12	841
UDP/204	1	96	0	0	1	96
UDP/138	10	2264	9	2186	10	2264
UDP/113	4	933	2	670	2	263
TCP/135	46	2160	40	1920	6	240
258 entries ——— Elapsed time: 1:22						
Protocol data rates (kbits/s): 0.00 in 153.00 out 153.00 total						

Exportando los datos generados por “iptraf” en una planilla de cálculo se observa a simple vista que están todos los puertos TCP y UDP del puerto 0 a 1024.

Este barrido de puertos con mucha cantidad de paquetes y poco tamaño da una idea que se trata de scan de puerto.

Junto con este trabajo están las planillas de cálculo y la fuente de los datos para ser analizados y reordenados para análisis.

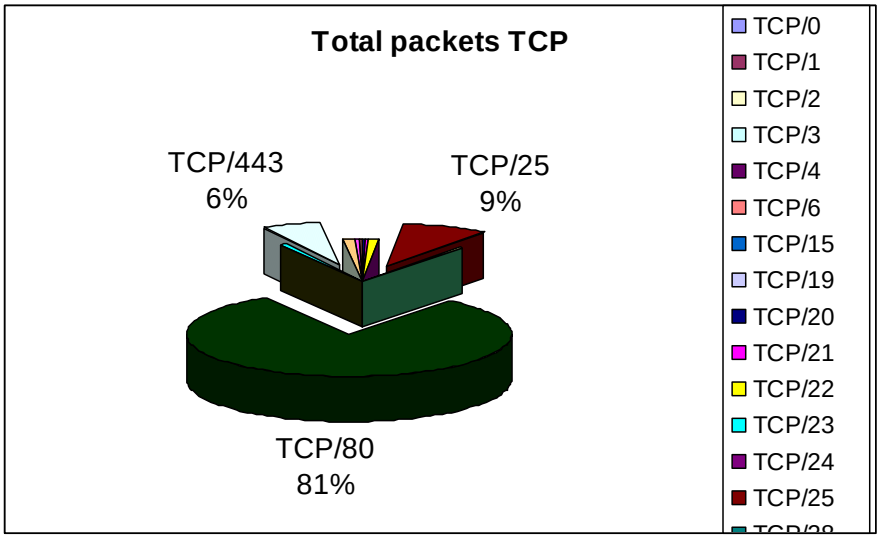
Abajo observamos dos gráficos globales. Son sobre un total de 16000 segundos (un poco más de 4 horas) donde se cursaron 42,5Gbytes y 65.000.000 paquetes. Si bien estos datos son poco para sacar conclusiones exactas y absolutas, dan un perfil de tráfico que hay en la red del CeSPI. Estas medidas

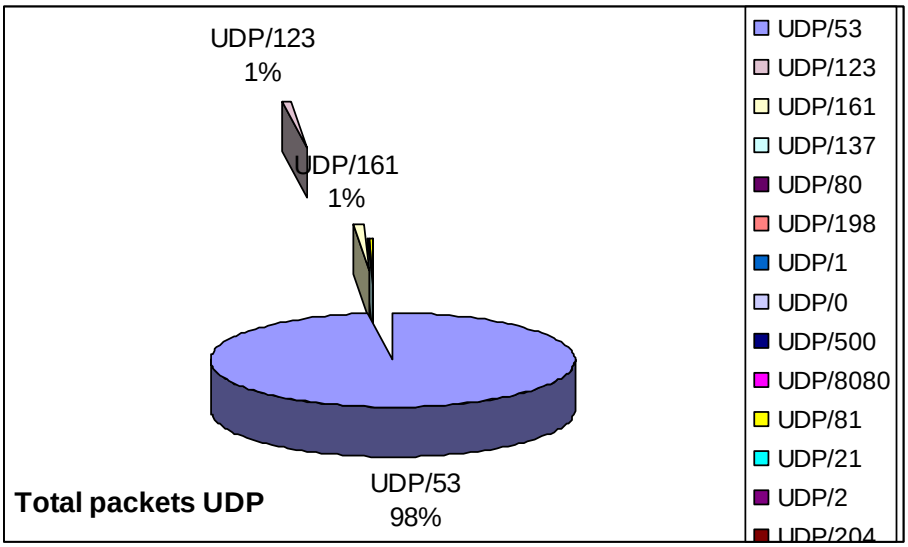
se realizaron varios días consecutivos y diferentes horarios, observándose solo diferencias en los horarios después de las 18hs sobre el trafico http, https y smtp estos como es deducible bajan notablemente.
Veamos un cuadro que resume los datos:

Total TCP+UDP		503	66895152	42490326869	125
Total TCP		135	63414161	42073849496	158
Total UDP		368	3480991	416477373	113
Total TCP %			**95**	**99**	
Total UDP %			**5**	**1**	

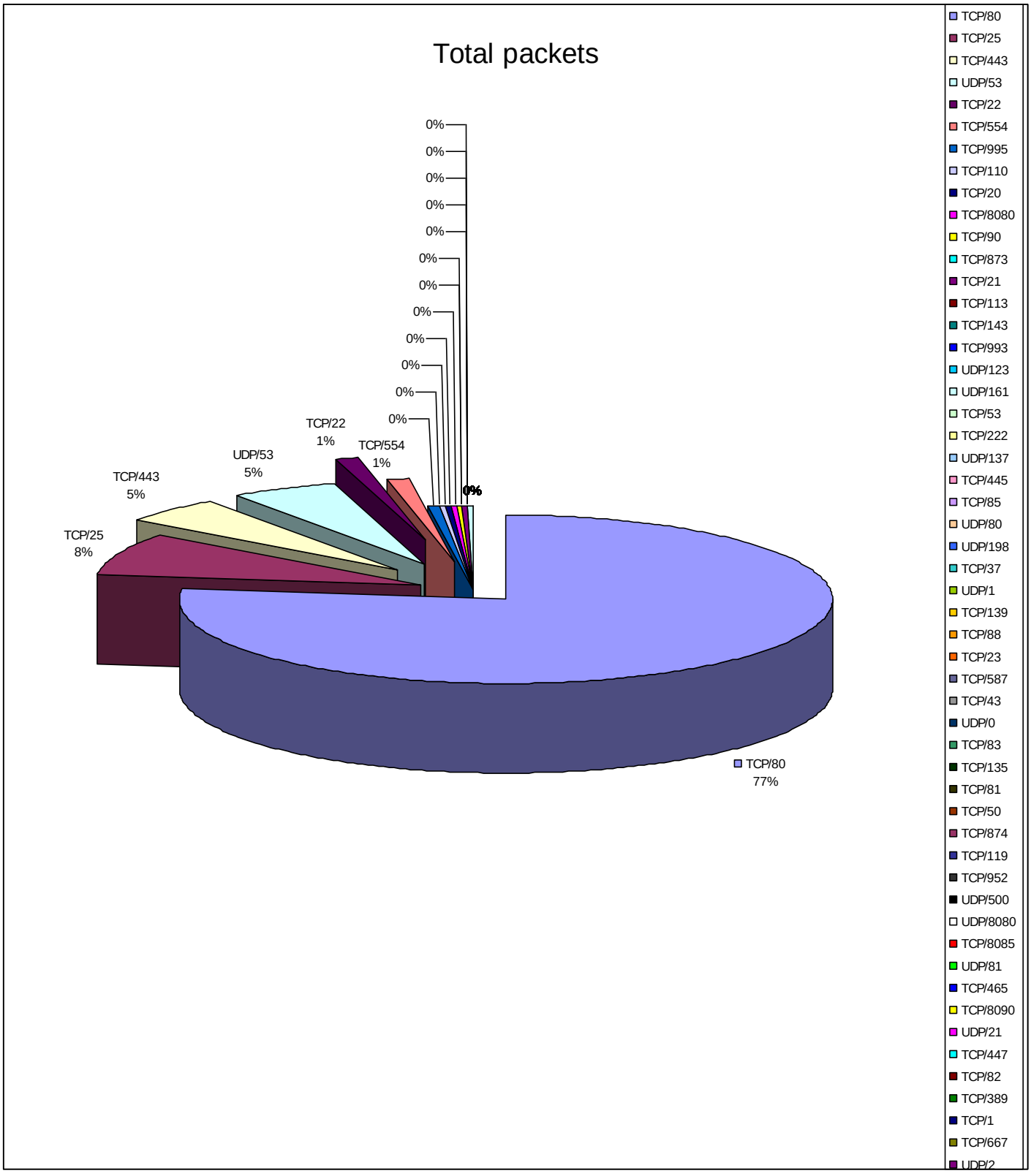
La columna “port” es la cuenta de puertos diferentes durante la medición.
UDP representa solo el 5% del tráfico total, de ese 5% el 98% el UDP/53 DNS.
TCP representa el 95% de tráfico total, compuesto mayormente por el 81% de http/80, 9% de SMTP/25 , un 6% de https/443 y el resto se divide en los puertos TCP restantes.

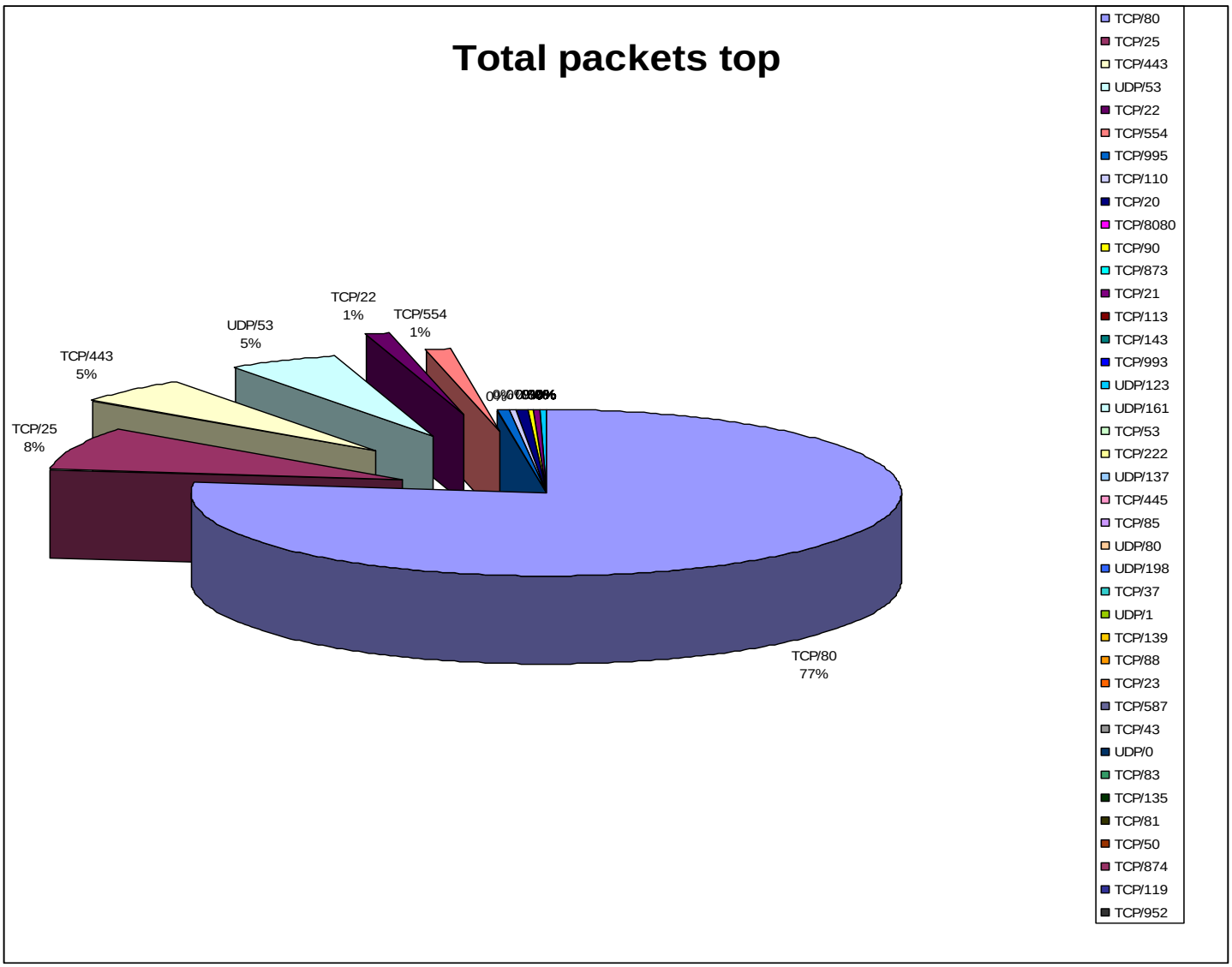
Observemos los gráficos
El segundo eso solo referido a los puertos TCP/UDP con mas del 1000 paquetes durante las 4 horas que duro la medición.
También en un tercer grafico mostramos las diferencias entre los protocolos UDP y TCP en volumen





El gráfico a continuación muestra el total de los datos de la muestra.


Total packets
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
0%
TCP/22
1%
TCP/554
1%
UDP/53
5%
TCP/443
5%
TCP/25
8%
TCP/80
77%
TCP/80
TCP/25
TCP/443
UDP/53
TCP/22
TCP/554
TCP/995
TCP/110
TCP/20
TCP/8080
TCP/90
TCP/873
TCP/21
TCP/113
TCP/143
TCP/993
UDP/123
UDP/161
TCP/53
TCP/222
UDP/137
TCP/445
TCP/85
UDP/80
UDP/198
TCP/37
UDP/1
TCP/139
TCP/88
TCP/23
TCP/587
TCP/43
UDP/0
TCP/83
TCP/135
TCP/81
TCP/50
TCP/874
TCP/119
TCP/952
UDP/500
UDP/8080
TCP/8085
UDP/81
TCP/465
TCP/8090
UDP/21
TCP/447
TCP/82
TCP/389
TCP/1
TCP/667
UDP/2



Resumiendo obtenemos los siguientes cuadros.

Protocolo	Puerto	Porcentaje del total en %
TCP	80/www	81
TCP	25/smtp	9
TCP	443/https	6
TCP	otros	4

Protocolo	Puerto	Porcentaje del total en %
UDP	53/dns	97
UDP	161/snmp	1
UDP	123/https	1
UDP	otros	1

	Total packets en %	Total bytes %
Total TCP %	94,8	99,0
Total UDP %	5,2	1,0

Los gráficos y tablas en si nos sirvieron para tener una visión del perfil de tráfico en la Universidad

8.3 Traffic Sentinel y Traffic Server

Estas son herramientas licenciadas de Inmon, obtuvimos una licencia para las pruebas. La ventaja principal de esta herramienta es que guarda el historial. Cuando comenzamos a ver los resultados de la herramienta nos dimos cuenta que nos hacían falta datos específicos de la red, esos datos fueron mencionados en las recomendaciones de esta Tesis. Traffic Sentinel viene integrada con la herramienta snort, con lo cual es una ventaja importante ya que por sFlow vemos se puede analizar el flujo de paquetes mirando el header de los mismos, y con la herramienta snort se puede procesar el contenido de esos flujos, las reglas de snort a utilizar son validas solo aquellas que utilizan el payload de los paquetes IP hasta un máximo de inspección de los primeros 127byte. Esta herramienta es manejada en un entorno web y los reportes pueden obtenerse en formato PDF.

Gráficos y reportes

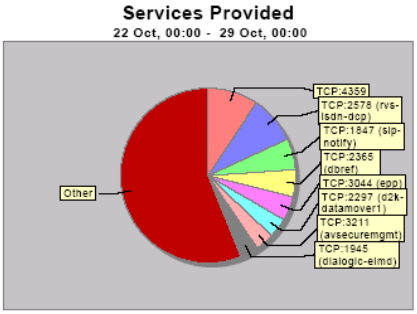
Los datos fueron tomados en noviembre del 2006

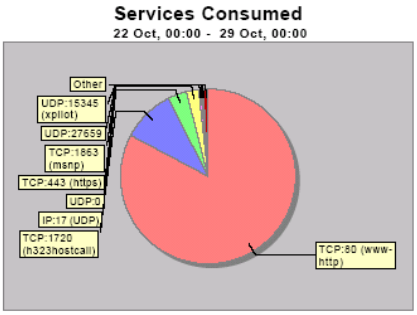
El grafico siguiente muestra el tráfico de un proxy de navegación

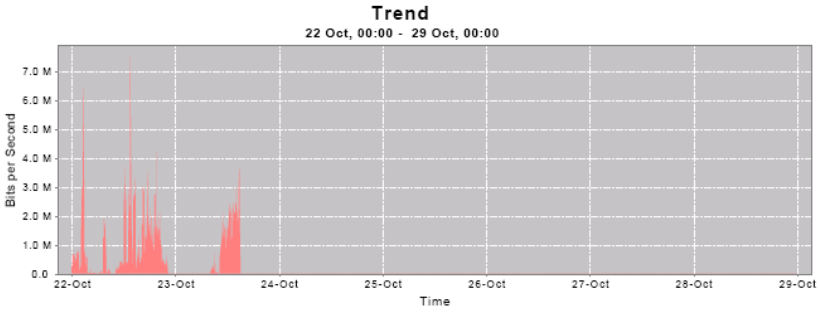
Traffic to Host

Characterise a host's traffic.

1.1. proxy.info.unlp.edu.ar (163.10.5.67)

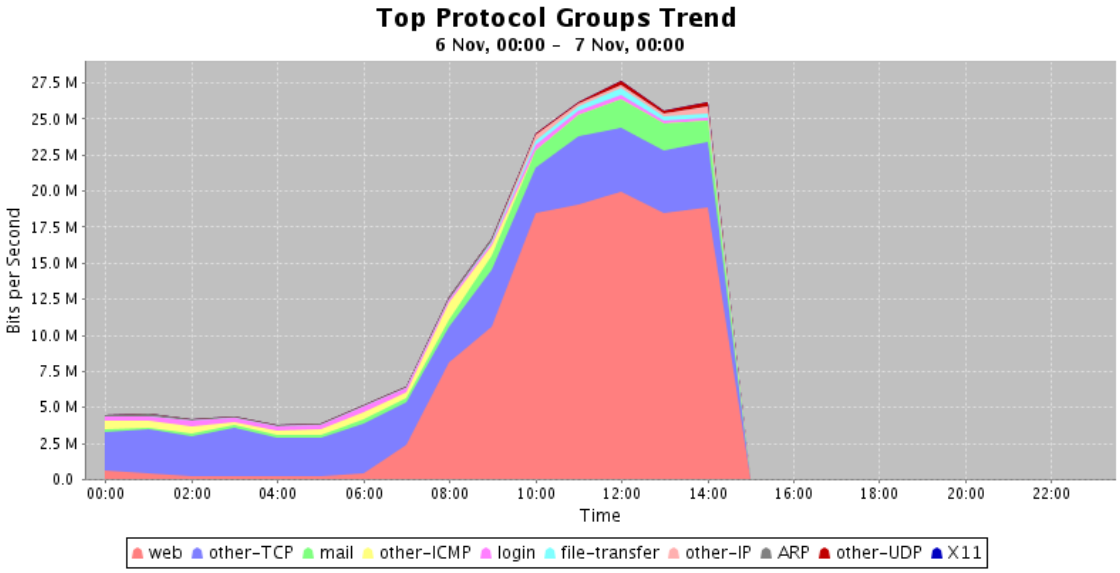


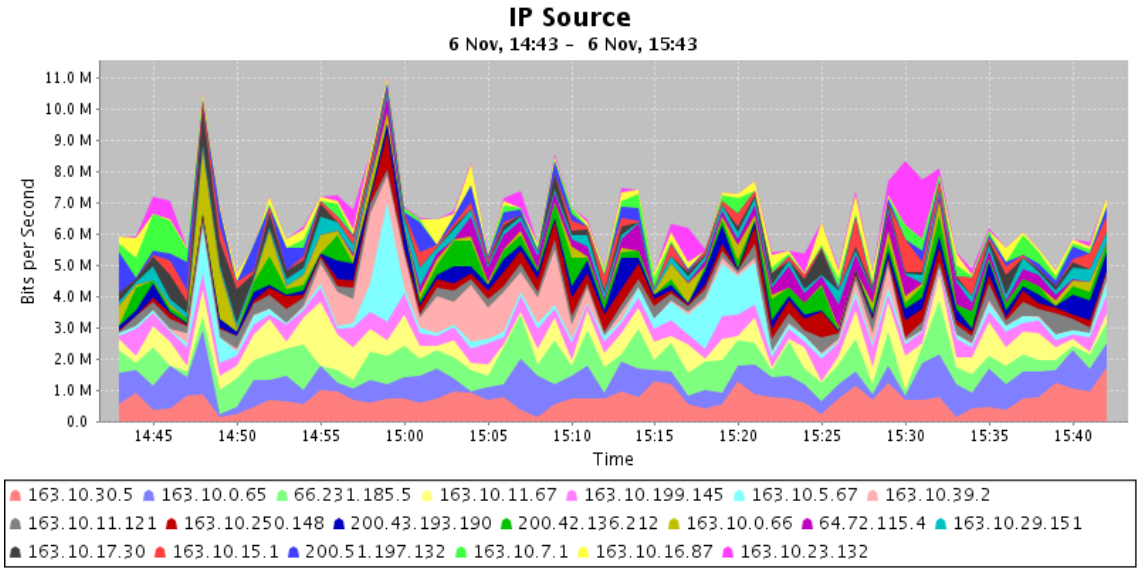




Client Address	Server Address	Server Port	Bits per Second
71.10.18.239	163.10.5.67	TCP:4359	10,616.408
72.13.133.127	163.10.5.67	TCP:2578 (rvs-isdn-dcp)	10,074.336
85.224.32.200	163.10.5.67	TCP:1847 (slp-notify)	6,584.432
68.45.177.104	163.10.5.67	TCP:2365 (dbref)	5,686.912
83.249.68.122	163.10.5.67	TCP:3044 (epp)	5,162.560
163.10.5.67	24.43.212.59	TCP:1720 (h323hostcall)	4,580.816
163.10.5.67	64.72.115.33	TCP:80 (www-http)	4,367.808
67.141.74.47	163.10.5.67	TCP:2297 (d2k-datamover1)	4,165.864
80.202.62.123	163.10.5.67	TCP:3211 (avsecuremgmt)	3,980.208
142.177.89.139	163.10.5.67	TCP:1945 (dialogic-elmd)	3,815.248
203.33.164.127	163.10.5.67	TCP:4143 (oidsr)	3,795.376
82.243.126.240	163.10.5.67	TCP:4331	3,585.448
163.10.5.67	17.250.248.37	TCP:80 (www-http)	3,490.280

Reporte del TOP de protocolos





Recordemos que Fisgon.cespi.unlp.edu.ar, fue nuestro colector de sFlow. El reporte siguiente muestra el ancho de banda consumido y los puertos utilizados.

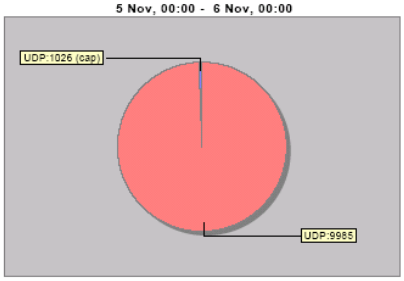
Traffic to Host

Characterise a host's traffic.

1.1. fisgon.cespi.unlp.edu.ar (163.10.0.39)

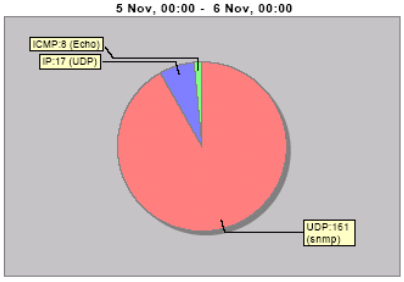
Services Provided

5 Nov, 00:00 - 6 Nov, 00:00



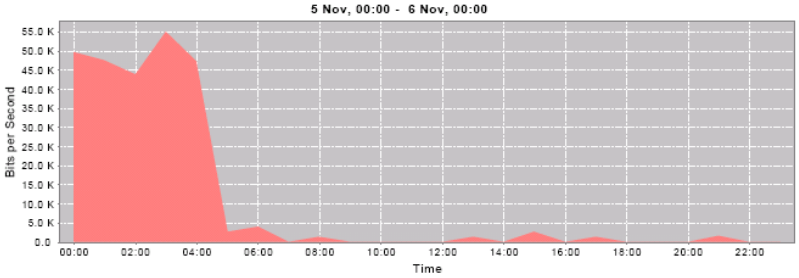
Services Consumed

5 Nov, 00:00 - 6 Nov, 00:00



Trend

5 Nov, 00:00 - 6 Nov, 00:00



Client Address	Server Address	Server Port	Bits per Second
163.10.199.145	163.10.0.39	UDP:9985	10,480.904
163.10.0.39	163.10.199.145	UDP:161 (snmp)	186.760
169.197.62.30	163.10.0.39	UDP:1026 (cap)	65.032
163.10.0.39	163.10.199.145	IP:17 (UDP)	13.648
163.10.0.39	163.10.199.145	ICMP:8 (Echo)	3.056
163.10.0.39	163.10.199.105	UDP:161 (snmp)	0.000
5 Nov, 00:00 - 6 Nov, 00:00			

Aquí veremos una muestra de trafico p2p, peer-to-peer considerados abusos, si bien se puede considerar una forma académica de compartir información este tipo de abusos degradan el uso de la red Universitaria para uso académico ya que la mayor parte de este trafico es para transportar archivos de “distracción y esparcimiento”

Una PC con más de 200 destinos es considerada un abuso absoluto.

Una PC con un volumen de más de 1Gbyte de transferencia en un día es considerada más que anormal.

Aquí veremos una muestra

Peer to Peer Traffic

Identify peer to peer (P2P) hosts and applications.

1. Top P2P Hosts

Find the top P2P hosts by examining the number of peers they talk to using UDP.

IP Source	UDP Source Port	# Destinations
163.10.30.133	UDP:5955	36,618
163.10.8.172	UDP:8838	18,942
209.126.200.104	UDP:1032 (iad3)	15,098
163.10.9.71	UDP:34798	12,252
163.10.0.65	UDP:65212	11,519
163.10.0.67	UDP:48114	11,290
163.10.18.162	UDP:6881	10,899
163.10.8.28	UDP:18293	10,111
163.10.29.108	UDP:49096	9,473
163.10.0.65	UDP:37042	8,691
163.10.1.1	UDP:32768 (filenet-tms)	7,996
163.10.11.65	UDP:53023	7,833
163.10.5.24	UDP:50463	7,820
163.10.4.1	UDP:32771 (filenet-rmi)	7,415
163.10.9.153	UDP:21114	7,207
163.10.8.172	UDP:13991	7,146
163.10.10.2	UDP:50452	7,063
163.10.18.145	UDP:31083	6,423
218.109.14.188	UDP:1160	6,331
163.10.7.1	UDP:58069	5,691
163.10.17.139	UDP:38629	5,529
163.10.5.66	UDP:32777	5,292
163.10.18.150	UDP:3128 (ndl-aas)	5,154
204.16.208.52	UDP:33494	4,812
163.10.18.1	UDP:38374	4,678
163.10.9.71	UDP:9213	4,570
163.10.7.250	UDP:42827	4,361
163.10.0.65	UDP:59095	4,279
163.10.9.65	UDP:36219	4,047
61.153.13.53	UDP:3353 (fatpipe)	3,897
218.75.24.230	UDP:3403 (copysnap)	3,762
163.10.199.254	UDP:32768 (filenet-tms)	3,744
219.146.10.108	UDP:3458 (d3winosfi)	3,714
61.175.163.195	UDP:1062 (veracity)	3,640
61.175.209.180	UDP:1570 (orbixd)	3,563
163.10.30.140	UDP:11254	3,547
220.189.202.109	UDP:1089 (ff-annunc)	3,452
219.153.2.168	UDP:1050 (cma)	3,441
163.10.30.215	UDP:39524	3,158
163.10.25.2	UDP:32769 (filenet-rpc)	3,132
163.10.37.9	UDP:4672 (rfa)	2,884
222.218.156.5	UDP:2762 (dicom-tls)	2,787
163.10.37.215	UDP:4672 (rfa)	2,676
163.10.18.253	UDP:44912	2,615
60.191.0.11	UDP:1232	2,556
163.10.10.5	UDP:19028	2,501
163.10.9.153	UDP:48693	2,471
163.10.8.67	UDP:32768 (filenet-tms)	2,442
163.10.30.227	UDP:4672 (rfa)	2,424

Estas consultas son orientativas para ver que tipo de análisis utilizados.

General Queries

General purpose queries for accessing real-time and historical data.

1. Historical Traffic

Table showing consolidated, long term traffic totals, up to the last hour.

IP Source	Bytes
163.10.37.215	7,926,648,139
163.10.34.186	4,476,236,553
216.113.183.154	4,069,962,116
66.135.202.164	4,013,058,308
66.135.215.44	3,976,819,805
	57,518,374,131
17 Sep, 00:00 - 18 Sep, 00:00	

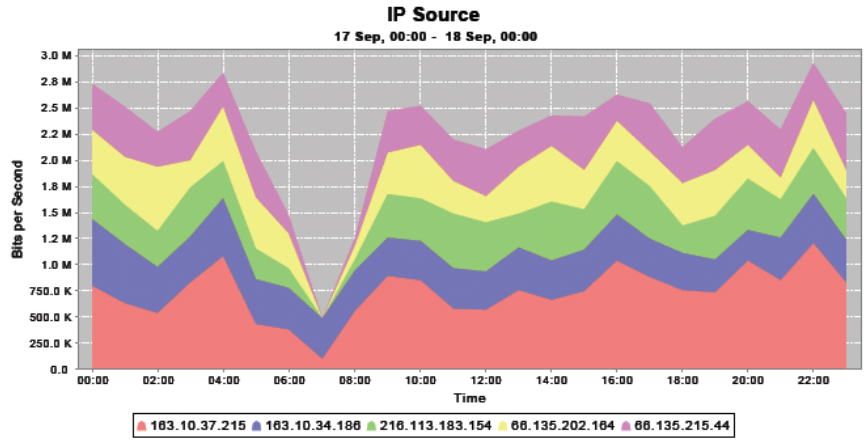
2. Historical Traffic Totals by Time

Table showing top talkers grouped by time interval.

Time	IP Source	Bytes
9/17/06 12:00 AM	163.10.37.215	357,755,474
9/17/06 12:00 AM	163.10.34.186	287,290,684
9/17/06 12:00 AM	216.113.183.151	238,016,335
9/17/06 12:00 AM	66.135.215.44	197,534,023
9/17/06 12:00 AM	216.113.183.154	193,801,645
9/17/06 12:00 AM		2,127,023,478
9/17/06 1:00 AM	163.10.37.215	282,674,179
9/17/06 1:00 AM	163.10.34.186	252,476,490
9/17/06 1:00 AM	66.135.215.44	215,297,261
9/17/06 1:00 AM	66.135.202.164	207,130,377
9/17/06 1:00 AM	66.135.202.161	187,026,591
9/17/06 1:00 AM		1,990,974,217
9/17/06 2:00 AM	66.135.202.164	274,926,707
9/17/06 2:00 AM	163.10.37.215	241,122,067
9/17/06 2:00 AM	66.135.209.247	226,276,333
9/17/06 2:00 AM	66.135.202.161	203,620,521
9/17/06 2:00 AM	163.10.34.186	194,897,548
9/17/06 2:00 AM		1,989,272,070
9/17/06 3:00 AM	163.10.37.215	369,818,889
9/17/06 3:00 AM	66.135.215.44	211,720,550
9/17/06 3:00 AM	216.113.183.154	209,857,383
9/17/06 3:00 AM	163.10.34.186	198,302,512
9/17/06 3:00 AM	66.135.209.247	195,875,777
9/17/06 3:00 AM		1,810,525,145
9/17/06 4:00 AM	163.10.37.215	482,142,612
9/17/06 4:00 AM	163.10.34.186	251,355,819
9/17/06 4:00 AM	66.135.209.247	248,264,466
9/17/06 4:00 AM	66.135.202.164	236,073,836
9/17/06 4:00 AM	66.135.202.161	175,362,607
9/17/06 4:00 AM		1,676,870,159
9/17/06 5:00 AM	216.113.183.151	230,617,378
9/17/06 5:00 AM	66.135.202.164	222,069,041
9/17/06 5:00 AM	66.135.215.44	199,557,998
9/17/06 5:00 AM	163.10.34.186	193,616,074
9/17/06 5:00 AM	66.135.209.247	191,930,758
9/17/06 5:00 AM		1,715,282,551

4. Historical Traffic Trend

Trend traffic by top categories.



5. Historical Traffic Accuracy

Table showing accuracy in long term traffic totals.

IP Source	Bytes	Lower Bound	Upper Bound	% Error
163.10.37.215	7,926,648,139	7,787,905,788	8,065,390,490	1.750
163.10.34.186	4,476,236,553	4,364,185,461	4,588,287,645	2.503
216.113.183.154	4,069,962,116	3,971,205,515	4,168,718,717	2.426
66.135.202.164	4,013,058,308	3,916,372,805	4,109,743,811	2.409
66.135.215.44	3,976,819,805	3,879,354,295	4,074,285,315	2.451
	57,518,374,131	57,209,402,262	57,827,346,000	0.537

6. Recent Traffic

Table showing up to the minute, unconsolidated traffic totals.

Source Address	Bytes
163.10.37.215	479,202,291
163.10.16.95	223,741,366

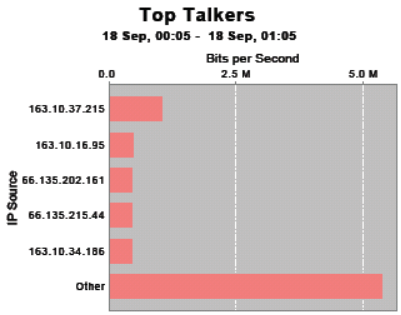
7. Recent Traffic Totals by Time

Table showing recent top talkers grouped by time interval.

Time	Source Address	Bytes
9/18/06 12:05 AM	163.10.37.215	45,495,666
9/18/06 12:05 AM	163.10.7.50	26,992,379
9/18/06 12:05 AM	216.113.183.154	25,176,419
9/18/06 12:05 AM	66.135.202.161	24,031,466
9/18/06 12:05 AM	163.10.34.186	17,706,374
9/18/06 12:05 AM		206,731,774
9/18/06 12:10 AM	163.10.37.215	38,975,974
9/18/06 12:10 AM	66.135.209.247	24,953,675
9/18/06 12:10 AM	66.135.202.161	24,149,731
9/18/06 12:10 AM	163.10.16.95	23,558,654
9/18/06 12:10 AM	66.135.215.44	15,888,061
9/18/06 12:10 AM		199,147,285
9/18/06 12:15 AM	163.10.37.215	110,595,875
9/18/06 12:15 AM	163.10.16.95	28,302,394
9/18/06 12:15 AM	66.135.215.44	26,783,586
9/18/06 12:15 AM	66.135.202.161	26,019,873
9/18/06 12:15 AM	163.10.34.186	20,088,065
9/18/06 12:15 AM		179,615,251
9/18/06 12:20 AM	163.10.37.215	52,403,559
9/18/06 12:20 AM	66.135.215.44	29,845,721
9/18/06 12:20 AM	163.10.34.186	26,928,515
9/18/06 12:20 AM	163.10.16.95	15,956,121
9/18/06 12:20 AM	66.135.202.164	15,384,762
9/18/06 12:20 AM		202,936,617
9/18/06 12:25 AM	163.10.37.215	37,845,618
9/18/06 12:25 AM	216.113.183.154	23,162,730
9/18/06 12:25 AM	66.135.215.44	21,352,710
9/18/06 12:25 AM	66.135.209.247	19,219,945
9/18/06 12:25 AM	163.10.16.95	15,018,930
9/18/06 12:25 AM		155,971,972
9/18/06 12:30 AM	163.10.37.215	51,115,161
9/18/06 12:30 AM	66.135.202.164	34,793,567
9/18/06 12:30 AM	66.135.202.161	32,299,570
9/18/06 12:30 AM	66.135.209.247	28,394,347
9/18/06 12:30 AM	163.10.16.95	19,886,479
9/18/06 12:30 AM		185,842,973
9/18/06 12:35 AM	66.135.202.164	32,421,228
9/18/06 12:35 AM	66.135.215.44	23,793,534
9/18/06 12:35 AM	163.10.16.95	23,703,619
9/18/06 12:35 AM	163.10.34.186	15,706,081
9/18/06 12:35 AM	163.10.37.215	13,577,534
9/18/06 12:35 AM		171,781,842
9/18/06 12:40 AM	216.113.183.151	32,871,295

8. Recent Top N Chart

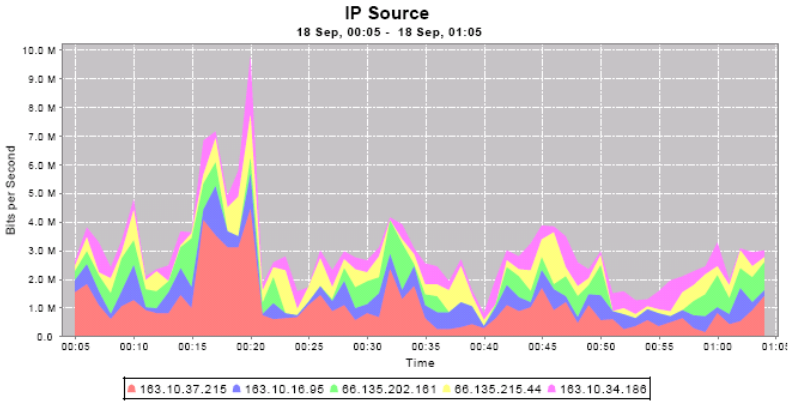
Plot recent value by top contributors.



9. Recent Traffic Trend

Trend recent traffic by top categories.

General Queries

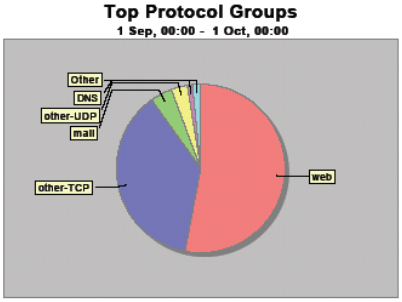


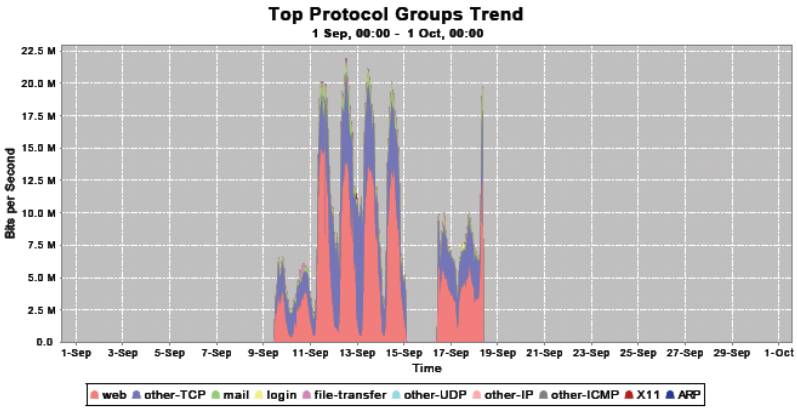
Otro reporte que agrupa por

Top Protocol Groups

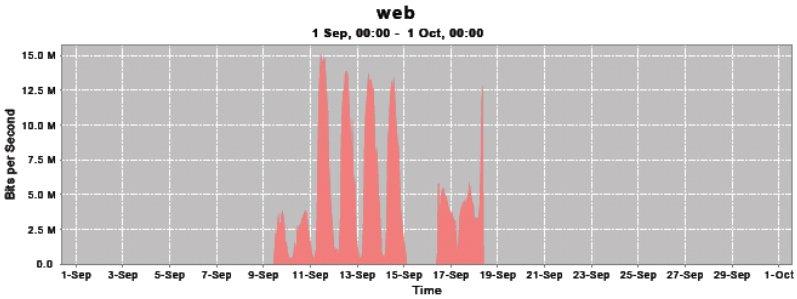
Identify top protocols groups by bytes. Provide detailed information for each of the top groups.

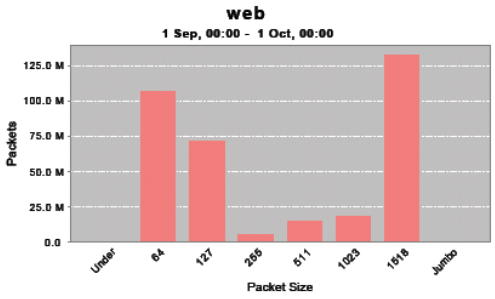
1.1. Summary



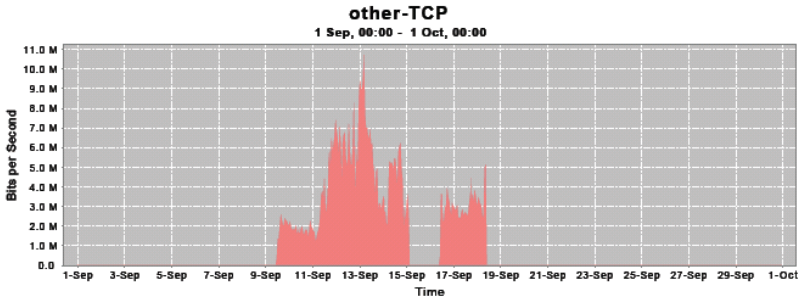


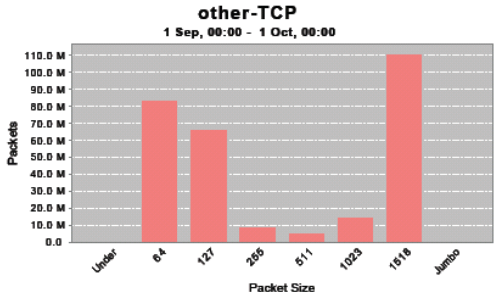
1.2. web



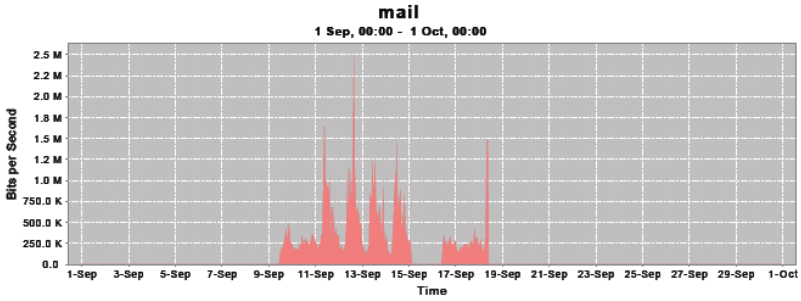


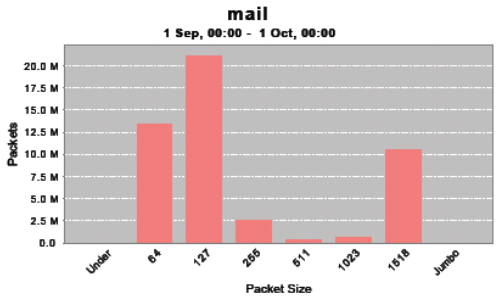
1.3. other-TCP





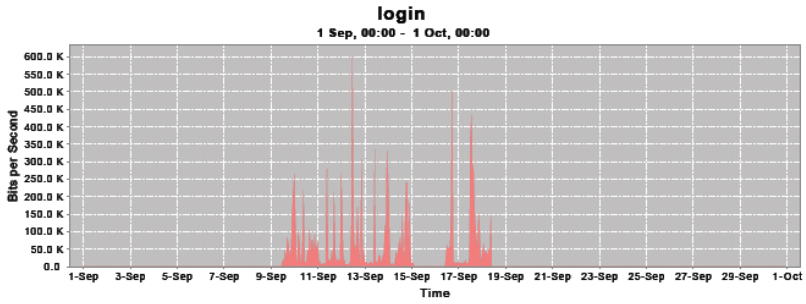
1.4. mail

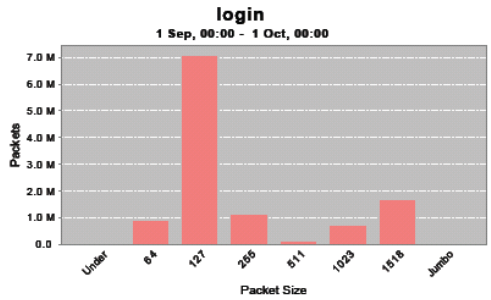




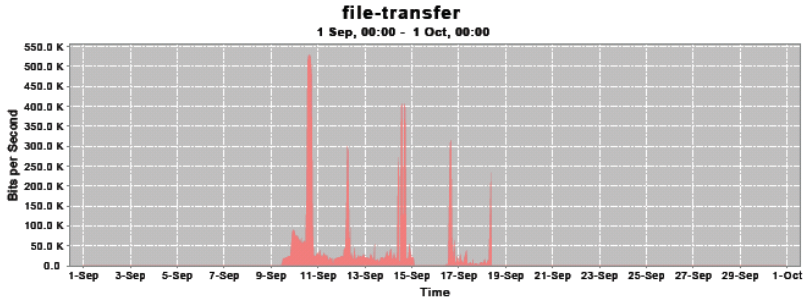
Top Protocol Groups

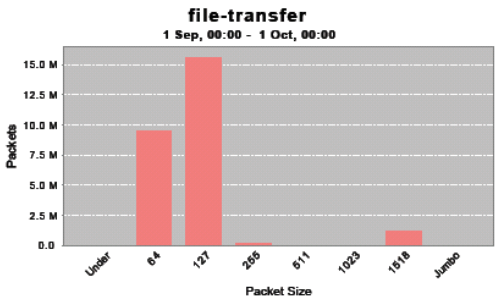
1.5. login





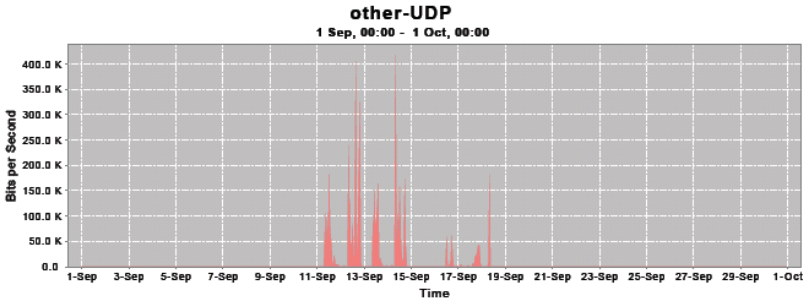
1.6. file-transfer

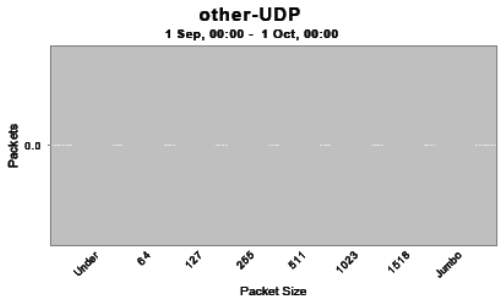




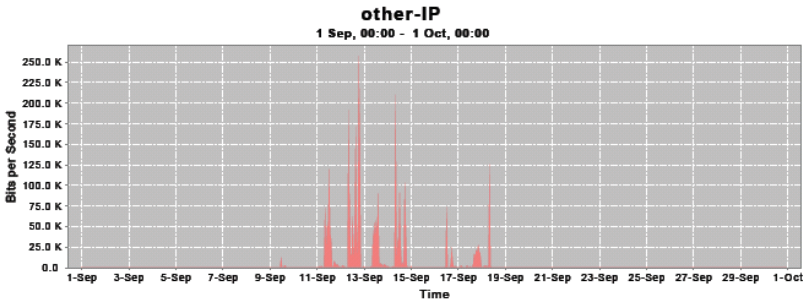
Top Protocol Groups

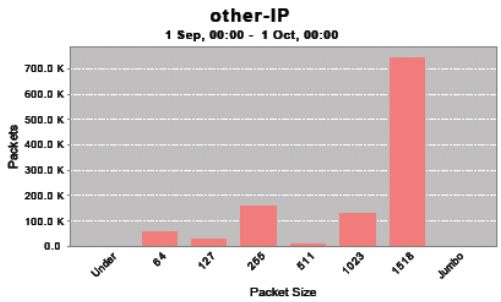
1.7. other-UDP





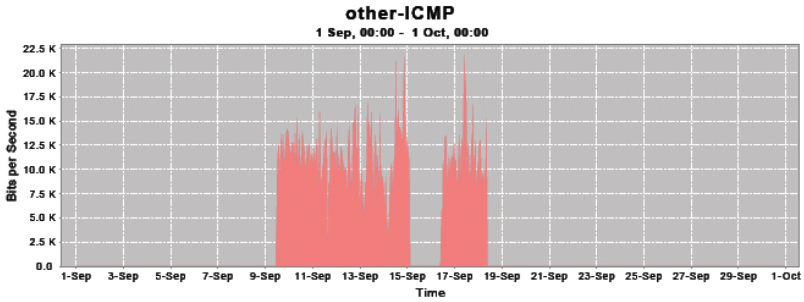
1.8. other-IP

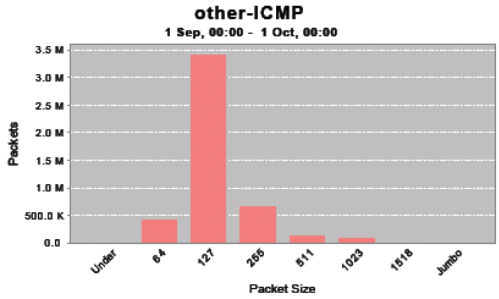




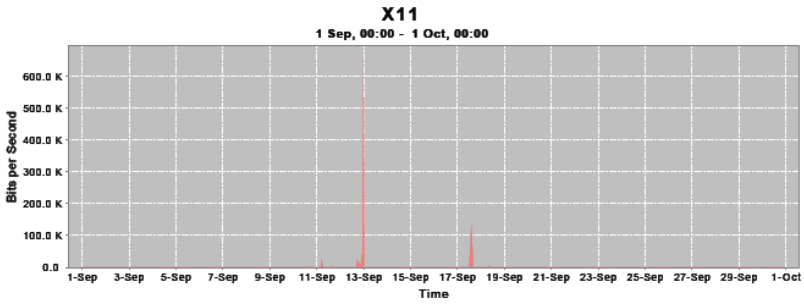
Top Protocol Groups

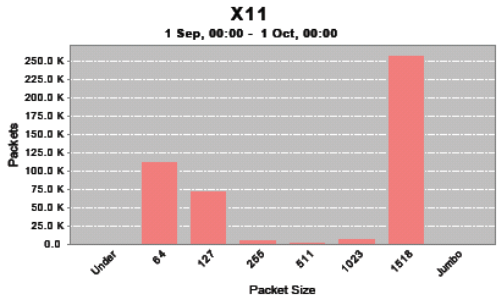
1.9. other-ICMP





1.10. X11



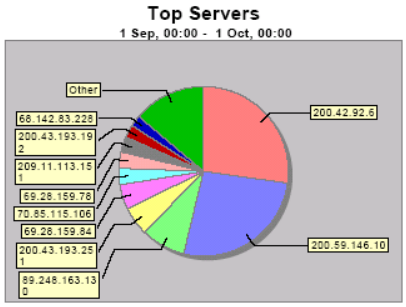


5

Hicimos reportes por un puerto que consideramos peligroso para la explotación que habíamos detectado trafico anormal el TCP 554

Servers

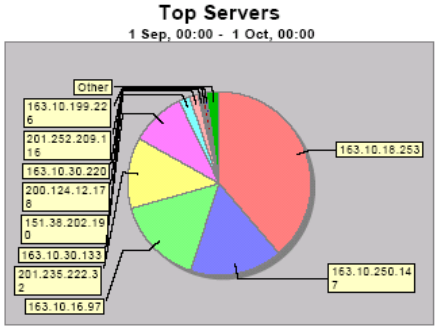
Top servers and their clients.



Ídem anterior parte el puerto TCP 1518

Servers

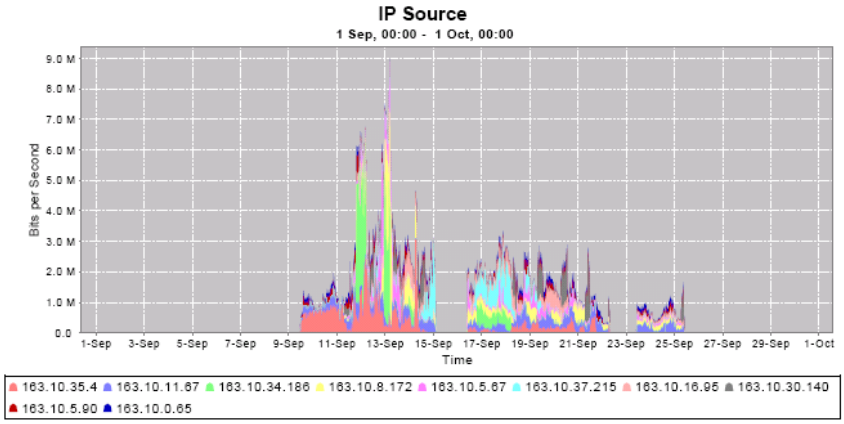
Top servers and their clients.



A continuación se ve un reporte de los mayores consumidores de tráfico en un mes.

Historical Traffic Trend

Trend traffic by top categories.



1.1. Totals

IP Source	Bytes
163.10.35.4	41,107,252,510
163.10.11.67	32,555,885,774
163.10.34.186	31,878,492,922
163.10.8.172	30,102,973,177
163.10.5.67	26,422,277,312
163.10.37.215	23,098,553,378
163.10.16.95	22,004,073,923
163.10.30.140	18,470,684,160
163.10.5.90	17,686,845,441
163.10.0.65	17,430,512,060
	1,155,225,754,990
1 Sep, 00:00 - 1 Oct, 00:00	

Los gráficos vistos en páginas anteriores son una muestra de los reportes y análisis realizados para realizar y realiza la Tesis. Nuevamente gracias a los que colaboraron referirse al párrafo inicial.
Muchas gracias.
El Master en redes de Datos es el puntapié inicial para ver en detalles temas tan extensos como uno quiera ver.

9.0 Políticas a aplicar de control de tráfico CeSPI

Clases de servicio premisas

Lo que buscamos en esta sección es encontrar pautas para las políticas de tráfico. En esta Universidades la filosofía fue tradicionalmente brindar conectividad sin restricciones a la red pública Internet, para lograr una especie de "laboratorio" especialmente en la Facultad de Informática. En la actualidad eso se convierte en un potencial riesgo de seguridad para la Universidad en si misma ya que puede ser no solo destinos de ataques desde Internet, sino que también fuente de los mismos.
Con el paso de los años y los problemas se van configurando restricciones para evitar excesos y abusos.
Para enfocarnos en el tipo políticas de tráfico, vamos a suponer que la red esta física o lógicamente dividida en secciones. Estas divisiones en general se implementan con vlan (virtual LAN) sobre la misma infraestructura de switches.

Las secciones o subredes o vlan pueden ser:

Red de servidores académicos productivos de la Universidad, en esta sección dividiremos la red en servidores académicos productivos y servidores de desarrollo. Los servidores productivos son los que deben tener más protección y restricciones para ser accedidos.

Red de servidores de desarrollo tendrán también accesos protegidos.
Ambas redes deben estar separadas lógica o físicamente para evitar futuros problemas que se generen en la red de laboratorio.

Red servidores de los laboratorios o unidades académicas, estos servidores no tendrán servicios publicados en Internet. Red de laboratorios y gabinetes de computación, serán con las mínimas restricciones posibles, creando reglas que limiten y protejan de ataques conocidos. Esta red debería tener limitaciones de volumen de tráfico que puedan generar. Se deberá buscar la forma de restringir al menos un poco el uso de programas P2P para que por ejemplo bajar películas o música desde y hacia Internet no este permitido o restringirlo al mínimo.

Red de PC de usuarios administrativos de la Universidad , en esta red se pondrán los PC o estaciones de trabajo de personal administrativos de las Facultades , la prioridad en esta red es mantener la más alta disponibilidad posible, protegiendo las PC para que no sean accedidas desde Internet, para evitar propagación de virus, troyanos, códigos maliciosos, spyware/grayware. Tendrán acceso a servicios públicos de Internet limitados a http, https, puertos de mensajeros instantáneos públicos [32] en Internet. Seria recomendable que también se restrinja los puertos y servicios a los que pueden acceder dentro de la misma red interna de la universidad. Las restricciones son tendientes a minimizar los riesgos de seguridad de las mismas. Indisponibilidades en esta red generan problemas y molestias al trabajo administrativo de la Universidad.

Políticas de Seguridad

Las Políticas deben ser simples y claras, cuanto más simples sean más efectivas van a ser. Estas políticas deberán ir evolucionando con el tiempo dando espacio al debate de ideas, el en cual se tratara si se deberán modificar las políticas.

Listado de servidores y aplicaciones, se debe contar con un listado de servidores y aplicaciones, para no bloquear o generar una denegación de servicio al un servidor o servicio académico. No obstante la actividad sospechosa debe ser informada. La lista de servidores debe ser archivada con estricto nivel de seguridad y no debe ser publicada, solo debe conocer esta lista los grupos de trabajo que solo lo necesiten. Esto servirá para ordenar la red y generar recomendaciones, generando las políticas en los Firewall permitiendo solo lo declarado.

Todo lo que no esta en la lista de servidores no podrán abrirse conexiones con origen en Internet y destino la Universidad. Con esta medida de permitir conexiones solo salientes para los usuarios comunes ser mejorar la seguridad.

Detectar escaneos desde la red Interna de la Facultad con destino redes en Internet, bloquearlas.
Los datos de escaneos se sacaran de las estadísticas de sFlow y netflow o con un IDS como el snort.

Parches de Seguridad de los sistemas operativos, exigir que el sistema operativo de los servidores y PC conectado a la red de la Universidad, tengan instalados todos los fixes de seguridad que vayan creándose. Crear una lista de mínimos parches de seguridad instalados para ser conectados.

Sugerir que los servidores tengan firewall para reforzar la seguridad de los firewall globales de la red. Debido al tamaño de la red de la universidad se deberá analizar la instalación de firewall distribuidos y un firewall central capaz de manejar el total tráfico. El firewall central será el encargado de manejar políticas de seguridad globales. Para los casos que se requiera un acceso irrestricto a Internet, será justificado tratando de generar una Vlan para que esos equipos de test o laboratorios no afecten al resto de la red. Las PC (que no figure en la lista de servidores) no podrán tener más de un número determinado de conexiones hacia Internet, ese valor deberá ser discutido y analizado. De la observación de tráfico se observaron PC con mas de 200 destinos, eso es una clara situación de anormalidad, anomalías como esta deben ser tratadas e informadas para ser corregidas.

Limitar que una PC que no es servidor, no pueda tener más de 15 destinos en Internet simultáneos.

Bloquear una PC que esta escaneando la red o con actividad sospechas, e informar a los responsables. Los escaneos pueden provenir de la red interna como desde Internet.

Filtrado de paquetes statefull de ser posible.

Recomendaciones y capacitación, es conveniente un conjunto de recomendaciones y capacitación a los administradores de los sistemas y servicios, para lograr la uniformidad de criterios.

Limitación de volumen de tráfico, una PC (que no figure en la lista de servidores) podrá tener hasta un volumen de 0.5Gbyte de transferencia por día, pasado ese Límite se le aplicará penalización a definir.
Los datos de volumen de tráfico se sacarán de las estadísticas de sFlow y netflow. Deberá contemplarse el NAT [33] y los motivos por el cual este exista, esas redes se natearan cuando se necesite salida a Internet. Esos 0.5Gbytes deberá discutirse, para llegar a un acuerdo o fijar un valor inicial en base a las estadísticas y recursos disponibles. Este es un tema difícil de abordar si no existiera sflow o netflow, recordemos que estadísticas de las tecnologías de monitoreo mencionada pueden llevar un accounting del volumen de tráfico cursado por cada host. Conocer cual es el volumen de tráfico consumido por una PC (de la red interna) plantea algunos problemas técnicos a resolver, cuando se comenzó a desarrollar esta tesis se tenía el concepto que todas las PC de la Universidad tenían direccionamiento público, pero avanzando en la misma, nos dimos cuenta que existen dentro de la algunas unidades o sectores académicos redes privadas detrás de un NAT [33] de una sola dirección publica.

Asignación de IP, cada unidad académica que desee tener acceso a Internet deberá contar con al menos una ip pública asignada (asignada mientras exista direcciones a asignar, tratando de no agotar el rango) para ser usada con NAT cuando su direccionamiento interno sea una red privada. Esto facilitará las estadísticas ya que podrá medir el consumo por unidad académica.

Los servicios académicos no pueden competir con descargas de archivos de uso masivo en Internet.

Si clasificamos y usamos colas de servicio de tráfico, reducíamos los problemas de congestión en el ancho de banda contratado de entrada salida de Internet de la Universidad.

Lista de asignación de Ip publicas y privadas, con sus responsables. Se debería consultar al departamento de asuntos legales de la Universidad, si es necesario cumplir con alguna formalidad legal para las asignaciones de IP publicas, ya que si desde una Ip publica asignada a la Universidad Nacional de La Plata se perpetrara algún abuso o acción ilegal, la Universidad sería legalmente responsable y afrontaría posibles juicios. Por eso parecería conveniente un asesoramiento al respecto por personal entendido en temas jurídicos.

Autenticación, se deberá analizar la factibilidad de hacer un sistema de autenticación contra un firewall centralizado para que alguien que desee salir a Internet primero debe autenticarse con un usuario y password. Los usuarios y password serán personales e intransferibles, haciendo responsable al usuario de cuidar su password. El usuario al autenticarse al firewall podrá acceder a un conjunto de reglas que permitan su salida a Internet de los servicios autorizados. Mencionada autenticación podría ser de una valides de 8 horas. Si se tiene identificado el usuario será más simple informarle al mismo que se ha excedido en el tráfico máximo permitido, o informarle de alguna anomalía de tráfico generada por su estación de trabajo con acceso a Internet.

Filtros Estándar generales, de la colección de tráfico analizada se detectó que hay que aplicar filtros de Ip en el borde en contacto directo con Internet. Se utilizó también las recomendaciones de la agencia de seguridad NSA [34].
Filtrar los conocido y permitir las redes habilitadas en el borde de Internet
Filtro IP básico:

- No permitir ip Origen de redes privadas con destino las redes del CeSPI
- Trafico desde redes del CeSPI a direcciones privadas o no permitidas
- Denegar ip 127.0.0.0 0.255.255.255 any log
- Denegar ip salida o entrada de la red 10.0.0.0 0.255.255.255 any log
- Denegar ip salida o entrada de la red 0.0.0.0 0.255.255.255 any log
- Denegar ip salida o entrada de la red 172.16.0.0 0.15.255.255 any log
- Denegar ip salida o entrada de la red 192.168.0.0 0.0.255.255 any log
- Denegar ip salida o entrada de la red 255.255.255.255 any log
- Denegar redes de multicast si no estuvieran en uso
- Permitir de entrada de host peering bgp
- Denegar de entrada de la redes de la Universidad como origen
- Denegar ip salida de la red de la Universidad
- Denegados finales todo.
- No snmp desde Internet con destino el Cespi y viceversa.
- Limitar tamaño paquete ICMP a 128bytes
- Denegar servicios que no tengan sentido desde Internet Ver recomendaciones de NSA[34]
  Es necesario mysql desde redes de Internet a redes del CeSPI?
  Del análisis se ven muchos ataques al puerto TCP 1434 de mysql, esto nos hace pensar en limitar las conexiones no iniciadas desde las redes 163.10.0.0/16, exceptuando la lista de redes o servidores de la red 163.10.0.0/16, por eso es necesario recortar tráfico que no sea necesario.
- No puerto UDP 0 y no TCP 0, se observó también con sflow tráfico basura.

10.0 Conclusiones generales de la presente Tesis

Para optimizar el tráfico en los enlaces, hay que conocerlo. No alcanza con saber el volumen de tráfico, se necesita más detalles que nos permitan tomar decisiones. Históricamente, se contaba con formas simples de medir el volumen de tráfico y técnicas sofisticadas de conocer el detalle qué tipo de tráfico formaba ese volumen, como capturar con un analizador de protocoles (sniffer) y luego procesarlo buscando algo en particular, insumiendo grandes volúmenes de espacio en disco y poder de procesamiento, que tornaban impracticable un análisis continuo y sostenido en el tiempo. Surgieron así, tecnologías de análisis de datos, que permiten hacer resúmenes acumulativos de perfiles de tráfico, con la utilización de pocos recursos. Ese análisis por flujo permite tomar decisiones de políticas a aplicar, generando una calidad de servicio adecuada a las necesidades y paralelamente, medidas de seguridad restringiendo flujos de datos que no son necesarios en una red. Es reporte de los flujos de datos es generada en "agentes" en diversos puntos de la red, los cuales normalmente se encuentran incluidos en los mismos equipos de comunicaciones switches/routers (equipos activos de la red). Esa información de flujos colectadas por los "agentes" son enviados a un servidor central, donde se generan los análisis para la toma de decisiones.

En este trabajo, se utilizó esta tecnología de análisis por flujos de datos, para conocer el tráfico de entrada y salida a internet de la Universidad Nacional de La Plata. Simultáneamente, se utilizó análisis de captura de paquetes con sniffer, obteniendo dificultosas conclusiones y corroborando que no es ni practico ni sostenible en el tiempo.

Colectada la información de esos flujos de datos, se obtienen reportes como equipos que más utilizan la red, puertos TCP/IP utilizados en porcentajes, etc. Luego de varios días de observación de estos reportes generados continuamente, se logró diferenciar el perfil de tráfico normal de las anomalías, por ejemplo PC con 500 destinos en menos de 2hs. Se logró el reconocimiento de servidores web, proxies, DNS, servidores SMTP, etc. instalados en la red Universitaria.

Con este análisis se arribaron a las conclusiones explicadas en el capítulo 8 "Políticas y Recomendaciones".

El análisis por flujos de datos mantenidos en el tiempo, permite hacer correcciones sobre las políticas originales, modificación de la calidad de servicio implementada y planificaciones, logrando así optimizar el uso de los recursos.

Durante la evolución de este trabajo se pusieron en evidencias las dificultades que se tienen para administrar eficientemente una red, como organizar y planificar la misma, si no se cuanta con una tecnología de análisis de flujos de datos. La herramienta (*herramienta, herramienta es un es un pico y una pala*) utilizada para el análisis de datos se llama sFlow, la cual allana el camino y brinda información eficiente para la planificación, diseño y operación de la red, logrando estabilidad en el tiempo.

Mis sinceros agradecimientos al CeSpi que aportó recursos y conocimientos para la realización de esta tesis.- ☺

11.0 Referencias

[1]. Sonia Pachen perteneciente a la Empresa Inmon, desarrolladores de productos de colección e interpretación de paquetes sflow url :www.inmon.com

[2]. Ser extremadamente restrictivos hace volar la imaginación e ingenio de los seres humanos para saltar y eludir esas restricciones, tómese como una observación del comportamiento humano. El instinto del ser humano es superar los obstáculos.

[3]. Shadow IT es un termino que se esta usando para describir las soluciones usadas por usuarios sin que tenga la aprobación de las organizaciones donde se las usa. Para una introducción puede referirse a la url en.wikipedia.org/wiki/Shadow_IT. También puede encontrarse muchos artículos al respecto, en los que encontrara una descripción y coincidencias con la realidad.

[4]. Definiciones de GNU se encuentran en la url www.gnu.org y en es.wikipedia.org/wiki/gnu.

[5]. Los desarrolladores de sFlow se agrupan en www.sflow.org, allí se encuentra el entorno para los desarrolladores, donde comparten recursos e información.

[6]. Redes de computadoras tercera edición. Andrew S. Tanenbaun.

[7]. Breve reseña de las implementaciones de TCP, url: es.wikipedia.org/wiki/Implementaciones_de_TCP

[8]. IIS es una serie de servicios que ofrecen los sistemas operativos Microsoft se puede encontrar una breve descripción en la url: es.wikipedia.org/wiki/IIS.

[9]. La nomenclatura KB/s es K=1000, B=Byte=8, /s= por segundo.

[10]. Parámetros en el registro de configuración del Windows
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"GlobalMaxTcpWindowSize"=dword:0003E800
"TcpWindowSize"=dword:0003E800 En hexadecimal.
"Tcp1323Opts"=dword:00000003

[11]. Iptraf es un medidor de velocidades de transferencia y uso de puertos, útil para ver con un grado de detalle se puede encontrar en los sistemas Linux, la url de referencia es iptraf.seul.org

[12]. Consultar bibliografía libro Redes de computadoras tercera edición. Andrew S. Tanenbaun

[14]. Artículo donde se encontrará un detalle de vulnerabilidades de p2p url: www.ics.forth.gr/dcs/Activities/papers/gdos.acns06.pdf y http://www.ics.forth.gr/ftp/tech-reports/2006/2006.TR370_Misusing_Unstructured_P2P_Systems.pdf.

[15]. Vulnerabilidades de p2p http://cis.poly.edu/~ross/papers/p2pddos.pdf

[16]. Internet World Stats es un sitio en Internet donde se publican estadísticas de uso y referencias de Internet url: www.internetworldstats.com

[17]. Es una compañía que publica servicios y estadísticas de uso de Internet url: news.netcraft.com

[18]. SSL, una breve reseña del protocolo ssl se encuentra en la url: es.wikipedia.org/wiki/Ssl.

[19]. En España existe una red de divulgación de tecnologías y usos de Internet las url de referencia son www.euskadigital.net y www.euskalencounter.org/es/.

[20]. La entidad que asigna direccionamiento ip es IANA mas información se encuentra en la url:www.iana.org/numbers.

[21]. Pagina principal de ICANN es url: www.icann.org/tr/spanish.html.

[22]. Estadísticas de BGP en url: bgp.potaroo.net/index.html y presentaciones en url: www.potaroo.net/presentations/index.html

[23]. DWDM Dense wavelength Division Multiplexing, que significa Multiplexación por división en longitudes de onda.

[24]. Giga- (símbolo: G) es un prefijo del sistema internacional de unidades que indica un factor de 10exp9 o 1.000.000.000 (mil millones).

[25]. Muestreo significa tomar muestras en este caso de tráfico o flujo de datos generalmente TCP/IP que mediante estadística permita estimar el tráfico real, obteniendo un error acotado, este error en la estimación es un valor razonable, logrando así evitar costoso hardware que pueda analizar paquete por paquete, el muestreo estadístico permite errores.

[26]. La definición en su sitio web url: www.cespi.unlp.edu.ar expresa que el CeSPI es centro superior para el procesamiento de la información (CeSPI), es el centro de cómputos de la de la Universidad Nacional de La Plata. En el mismo se realizan las tareas relacionadas al sistema de liquidación de haberes, manejo de alumnos de las distintas unidades académicas y administración de la red de la UNLP, incluyendo los servicios de Internet. Adicionalmente a los sistemas de apoyo informático, el Ce.S.P.I. Brinda servicios de capacitación y consultaría a empresas y organizaciones. El centro cuenta con una amplia experiencia sobre plataformas IBM, soluciones OpenSources y redes TCP/IP.
En lo personal creo que es el ámbito para el desarrollo de las capacidades de quienes se acerquen con inquietudes, se observa un clima agradable (casi todo el tiempo ☺) y abierto para el desarrollo, donde reina la cordialidad y compañerismo.

[27]. Ethereal y wireshark es un capturador y analizador de trafico url: www.wireshark.org.

[28]. sFlowTrend es una herramienta creada por InMon para analizar datos de sFlow se la puede obtener de la siguiente url: http://www.inmon.com/products/sFlowTrend.php#download.

[29]. Ntop, es una excelente herramienta se encuentra en la url: www.ntop.org.

[30]. Recordemos que se definió en el desarrollo de esta tesis que significa en este contexto un agente de captura, que en resumen es un proceso implementando en hardware o software que ve pasar trafico, toma datos de la misma usa estadística de muestreo, arma datagramas IP y los envía a un colector que los analiza. Este agente esta programado en C++ y fue accesible para modificar y obtener determinados características especiales. El agente de sFlow se puede obtener de la url: www.sflow.org y www.sflow.org/developers/tools.php.

[31]. Explicaciones exhaustivas y profundas sobre "Snort TM" pueden encontrarse en Internet o en la página http://www.snort.org

[32]. Los mensajeros instantáneos públicos de Internet como google talk, msn, yahoo, skype.

[33]. NAT, network address translation, El NAT se utiliza para cambiar la dirección origen, la dirección destino o ambas según se necesite. Uno de los uso es para esconder una red privada atrás de una Ip publica. Las redes privadas no son ruteadas en Internet.

[34]. La Agencia de Seguridad Nacional (en inglés: National Security Agency), también conocida como NSA por sus siglas en inglés, es una agencia del gobierno de los Estados Unidos responsable de obtener y analizar información transmitida por cualquier medio de comunicación, y de garantizar la seguridad de las comunicaciones del gobierno contra otras agencias similares de otros países, fuente http://es.wikipedia.org/wiki/Agencia_de_Seguridad_Nacional y http://www.nsa.org , el documento es "NSA/SNAC Router Security Configuration Guide"

Bibliografía, material de referencia y recursos

- Redes de computadoras tercera edición. Andrew S. Tanenbaun.
- Redes Globales de Información con Internet y TCP/IP tercera edición. Douglas E. Comer.
- RFC 3174. Definición del estándar sFlow. A Method for Monitoring Traffic in Switched and Routed Networks InMon Corporation's sFlow. 2001.
- sFlow versión 5, Al 2009 aun sin número de RFC asignado. 2004.
- RFC 959 an Analysis of international academy research network traffic.1985.
- RFC 813 TCP Windows and acknowledgment strategy in TCP.1982.
- RFC 894 Standards for the Transmission of IP Datagrams over Ethernet Networks.1984.
- RFC1323 Cálculo automático de la ventana TCP. TCP Extensions for High Performance 1992.
- http://www.sFlow.org Sitio que agrupa a los desarrolladores de sFlow
- http://www.inmon.con .Empresa de desarrollo de software para sFlow
- http://www.internetworldstats.com. Estadísticas de Internet
- http://news.netcraft.com . Información general y tendencias en Internet
- IPerf, herramienta de medición de ancho de banda.
- http://www.ietf.org Internet Engineering Task Force.
- http://www.cisco.com Cisco Systems, equipos de comunicaciones.
- http://www.caida.org Cooperative Association for Internet Data Analysis. Herramientas y Análisis para Internet.
- http://www.zakon.org/robert/internet/timeline/ Detalle de la evolución en el tiempo de la red Internet
- http://www.wireshark.org. Sniffer y analizador de red
- http://www.tcpdump.org. Sniffer
- http://www.ntop.org. Analizador de tráfico de licencia GNU, colector de sFlow y netflow
- http://cis.poly.edu/~ross/papers/p2pddos.pdf. Análisis de vulnerabilidades de protocolos p2p
- http://www.ics.forth.gr/dcs/Activities/papers/gdos.acns06.pdf. Análisis de vulnerabilidades de p2p para ataques DoS.

Muchas gracias
En la presente Tesis aprendí y conocí mucho más de lo escrito!
Mis sinceros agradecimientos a los que colaboraron