CPG

SEGURIDAD EN REDES

MONITORIZACION CON NETFLOW

TRAFICO EN LAS REDES

GUILLERMO GUTIERREZ RIASCOS

SANTAFE DE BOGOTA
CORPORACION UNIVERSITARIA UNITEC
2007-07-19

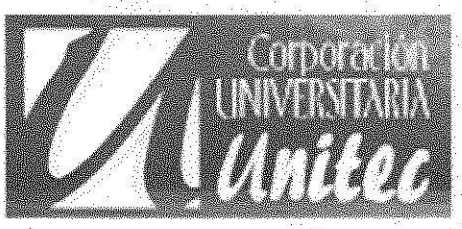
MONITORIZACIÒN
CON
NETFLOW

Tráfico en las redes.

Nombre: Guillermo Gutiérrez Riascos

Código: 36032064

C.P.G. SEGURIDAD EN REDES



Contenido

1) Introducción

Monitorear las redes forma parte un sistema de redes seguro, es por eso que netflow y sflow nos entregan una alternativa de controlar el flujo de datos en una red, para esto debemos entender que netflow es el que nos otorga visibilidad sobre qué aplicaciones están consumiendo ancho de banda, quién las está utilizando y durante cuánto tiempo basándose en el protocolo IP de la web. Permite ver rápidamente la causa de congestión de red y ayuda a evitar problemas y optimizar los recursos de red; que es vital en el funcionamiento empresarial, para esto contamos con múltiples herramientas basadas en cisco que nos permiten analizar cada uno de los paquetes que recorren la red.

Por otra parte sflow describe un mecanismo de captura de trafico mediante el UDP datagramas utilizando un simple mecanismo de colección de estadísticas de los dispositivos por esta razón es de gran ayuda en las redes de alta velocidad como gigabit o mas altas.

2) Planteamiento del problema

Analizar el trafico de una red puede ser un trabajo un poco complicado, esto es porque los datos que recolectamos con cualquier software nos permite dar una vista de los datos reales que están en ese momento pasando por nuestra red; para poder controlar parte de ese tráfico que es usado por nuestros usuarios es necesario conocer los puertos que estos están utilizando y el tamaño de los datos que están manipulando, esto es un problema muy importante para una empresa cuyos empleados desperdician el ancho de banda en páginas de ocio que generan tráfico y que permiten el ingreso de datos o de usuarios maliciosos a la red interna.

3) Objetivos

Actualmente, un aspecto importante tanto para usuarios como para operadores o administradores de redes de comunicaciones es garantizar la calidad de servicio prestado en las redes de datos y servicios asociados. Para ello es necesario realizar medidas que nos permitan comprobar que las redes están proporcionando el servicio contratado.

3.1) Presentar un informe completo y detallado del tráfico en la red, pudiendo utilizar este como medida de aseguramiento o mejoramiento de los paquetes enviados o servicio prestado.

3.2) Definir un procedimiento estándar en la obtención de información referente a los flujos establecidos en las conexiones tcp/ip.

3.3) Controlar los puertos que están abiertos.

3.4) Gestionar los datos de entrada y salida que están circulando a la red interna.

3.5) Bloquear páginas web de ocio, pornografía y temas parecidos para evitar virus en los host de la empresa.

4) Consideraciones técnicas

¿QUE ES UNA RED PETRI?

Las redes de Petri representan una alternativa para modelar sistemas, sus características hacen que, para algunos problemas las redes de Petri funcionen de una manera natural.
Las PN como ahora conoceremos a las redes de Petri (Petri Net) fueron inventadas por el alemán Karl Adam Petri en 1962. En su tesis doctoral "kommunikation mit automaten" (Comunicación con autómatas), establece los fundamentos para el desarrollo teórico de los conceptos básicos de las PN.

Las PN son consideradas una herramienta para el estudio de los sistemas. Con su ayuda podemos modelar el comportamiento y la estructura de un sistema, y llevar el modelo a condiciones límite, que en un sistema real son difíciles de lograr o muy costosas.

La teoría de PN ha llegado a ser reconocida como una metodología establecida en la literatura de la robótica para modelar los sistemas de manufactura flexibles.

Comparada con otros modelos de comportamiento dinámico gráficos, como los diagramas de las máquinas de estados finitos, las PN ofrecen una forma de expresar procesos que requieren sincronía. Y quizás lo más importante es que las PN pueden ser analizadas de manera formal y obtener información del comportamiento dinámico del sistema modelado.

Para modelar un sistema se usan representaciones matemáticas logrando una abstracción del sistema, esto es logrado con las PN, que además pueden ser estudiadas como autómatas e investigar sus propiedades matemáticas.

La explicación de una red de petri es tomada del documento de trabajo de Mabel Gonzales Urmachea www.monografias .com

¿Qué es NETFLOW?

Es un nombre dado por cisco al formato de exportación de información sobre flujos.

Cada flujo esta representado por un flow record, que contiene una serie de datos de información este se actualiza cada vez que los paquetes son conmutados.

El flujo de datos es definido como una secuencia unidireccional de paquetes con ciertas características comunes:
-Direcciones ip fuente y destino
-Numero de protocolo a nivel 3
-Puertos fuente y destino
-Octeto de tipo de servicio
-Índice de la interfaz de entrada

Dentro de los componentes tenemos:
-Exportador (ROUTER O SWITCH) quien crea los archivos o records y los exporta
-Colector es el que escucha los puertos UDP y guarda o reenvia los records a otros colectores
-Analizador es el que muestra, analiza y grafica los datos.

Debemos tener en cuenta que para utilizar estos métodos de monitorear la red en este caso el flujo de datos controlado por NETFLOW necesitamos entender la topología de una red y el protocolo tcp/ip; Empecemos por definir qué es y cuál es la arquitectura de tcp/ip.

El nombre "TCP/IP" se refiere a una suite de protocolos de datos, el nombre viene de 2 de los protocolos que lo conforman:

Transmission Control Protocol (TCP)

Internet Protocol (IP)

Hay muchos otros protocolos en la suite TCP/IP e Internet

TCP/IP son los protocolos fundamentales de Internet (Aunque se utilizan para Intranets y Extranets)

Stanford University y Bold, Beranek and Newman (BBN) presentaron TCP/IP a comienzos de los 70 para una red de conmutación de paquetes (ARPA-Net).

También se usa en redes de área local

¿Por qué es popular TCP/IP?

Los estándares de los protocolos son abiertos: interconecta equipos de diferentes fabricantes sin problema.

Independiente del medio de transmisión físico.

Un esquema de direccionamiento amplio y común.

Protocolos de alto nivel estandarizados (¡muchos servicios!)

Protocolos

Protocolos: reglas formales de comportamiento

Para que los computadores puedan comunicarse necesitan establecerse reglas ó protocolos (AppleTalk, IPX/SPX, SNA,etc.)

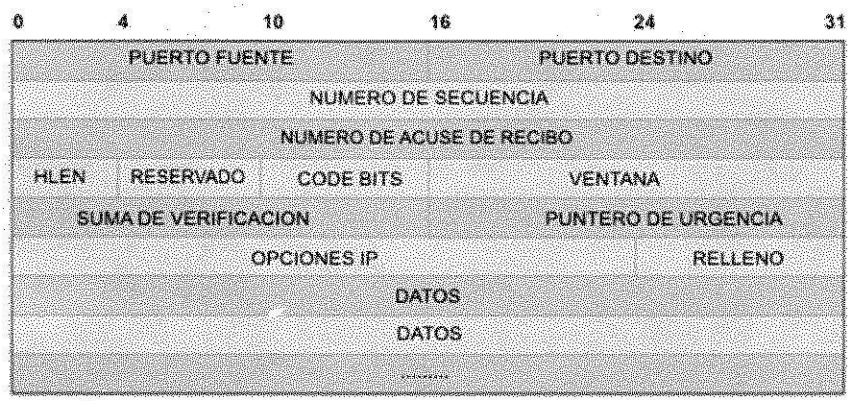
Los protocolos de TCP/IP no depende del S.O. ni del computador (es "abierto"): cualquiera puede desarrollar productos que se ajusten a las especificaciones de TCP/IP

"Estándares" de TCP/IP

Para garantizar que TCP/IP sea un protocolo abierto los estándares deben ser públicamente conocidos.

La mayor parte de la información sobre los protocolos de TCP/IP está publicada en unos documentos llamados Request for Comments (RFC's) - Hay otros dos tipos de documentos: Military Standards (MIL STD), Internet Engineering Notes (IEN) -.

Encabezado TCP



Arquitectura de TCP/IP

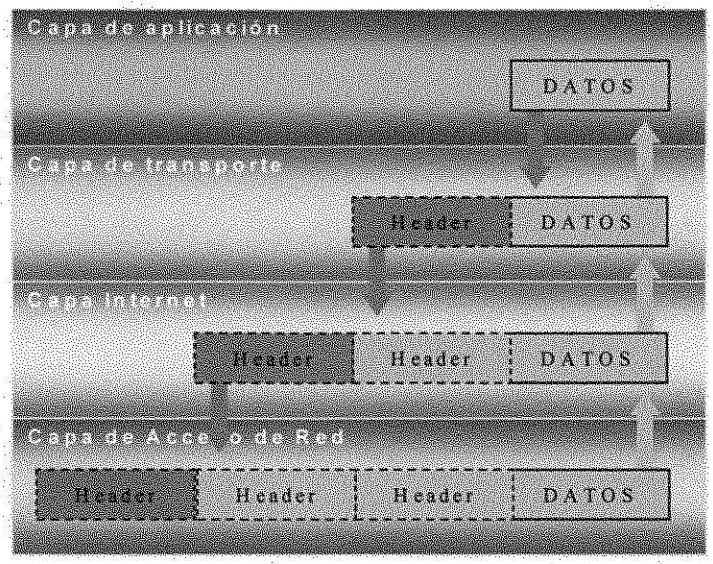
No hay un acuerdo sobre como representar la jerarquía de los

Protocolos de TCP/IP con un modelo de capas (utilizan de tres a cinco).

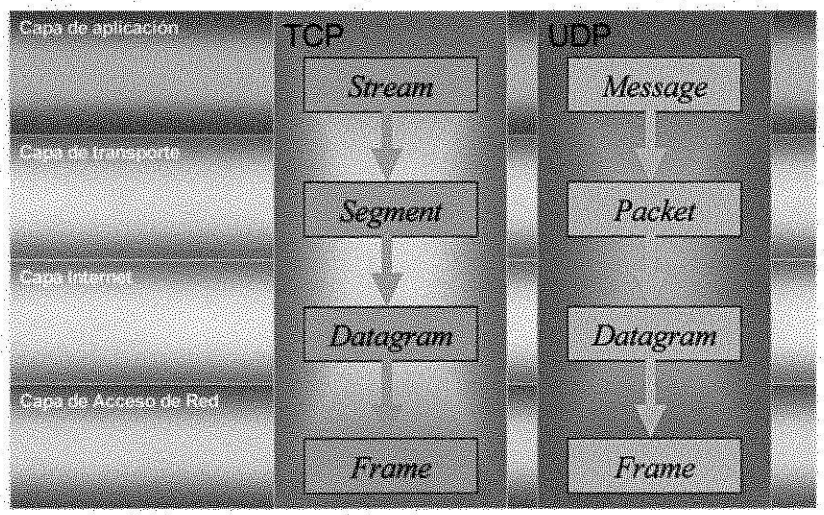
Aplicación	Aplicaciones y procesos que usan la red
Transporte	Servicios de entrega de datos entre nodos
Internet	Define el datagrama y maneja el enrutamiento
Acceso de Red	Rutinas para acceder el medio fisico

Encapsulación de datos

- Cada capa de la pila TCP/IP adiciona información de control (un "header") para asegurar la entrega correcta de los datos.
- Cuando se recibe, la información de control se retira.



Estructuras de datos



(**UDP**) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco sabemos si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

Un **datagrama** es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el DTE receptor, de manera independiente a los fragmentos restantes.

Que es un FIREWALL?

Otra parte vital es entender que es un firewall? Y su configuración; El FIREWALL es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar a los cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente.

5) Herramientas

En internet encontramos un gran número de herramientas que nos permiten analizar el flujo de datos que hay en la red; dentro de las cuales encontramos las siguientes:

ManageEngine NetFlow Analyzer v4.0
PRTG Traffic Grapher 6.1.0.756
ManageEngine NetFlow Analyzer 5
Plixer-scrutinizer-win32

Cada una de estas herramientas cuenta con características propias, que de una u otra manera entregan la información general necesaria para optimizar el rendimiento de una red, esto nos permite utilizar una alternativa a la hora de monitorear; por ejemplo esta herramienta de CISCO para redes corporativas llamada **NetFlow Analyzer** que es una herramienta de monitorización de ancho de banda basada en tecnología web. Nos Permite analizar la utilización de ancho de banda y nos ofrece visibilidad completa sobre routers y switches Cisco. Gracias a sus informes detallados y gráficos en tiempo real, **NetFlow Analyzer** nos proporciona información muy completa sobre el tráfico de red, sin necesidad de utilizar sondas.

Esta es una pequeña descripción de Scrutinizer NetFlow & sFlow Analyzer 4 que por cierto voy a utilizar en mi practica de laboratorio.

Este es un analizador de Flujo de Red o Net Flow, el cual provee información increíblemente detallada de la red y utilización de la misma, por parte de los usuarios y las aplicaciones que se encuentran en esta.

Es capaz de guardar detalles del tráfico, captura de los acontecimientos que necesites y representarlos gráficamente.
Con SCRUTINIZER se puede saber: ¿Quién?, ¿Qué?, ¿Cuándo? Y ¿Dónde? En forma detallada de la forma, su utilización de la red y del ancho de banda.

Además se puede tener conocimiento de ¿Qué tanto tráfico circula por las interfaces y su contenido? Y ¿Por qué se encuentra lento el sistema o la red?

WHO = QUIEN? -------» El sistema que está causando el tráfico.
WHAT = QUE? -------» Aplicación/Protocolo se está utilizando.
WHEN = CUANDO? -------» El intervalo de tiempo en el que está ocurriendo.
WHERE = DONDE? -------» Parte de la Red o conexión que está siendo afectada.

A través de SCRUTINIZER, podemos averiguar:

• Cuáles son las tendencias de ciertas aplicaciones por el tráfico de usuario.
• Qué tanto tráfico de VoIP se tiene en la red y quién está o ha hecho el mayor número de llamadas, mostrando así los picos mas altos de duración en las mismas.
• Qué tráfico se puede beneficiar por prioritización.
• Cuáles son los sistemas que pueden estar afectados por virus.
• Por qué ciertos servidores usan protocolos extraños.
• Cuáles son las aplicaciones que están teniendo grandes impactos en la infraestructura.

La gran mayoría de los fabricantes de switches y routers soportan tecnología Net Flow, tales como: Cisco, Enterasys, Extreme, Foundry, Juniper, Riverstone y Packeteer.

6) Configuraciones

En cada ROUTER se debe realizar unas configuraciones previas para recolectra los flujos de datos, estas se hacen asi:

En cada interfaz donde se quieren colectar flujos:

```
Router(config-if)# ip route-cache flow
```

Configurar los timers:

```
Router# ip flow-cache timeout active 30 (minutos)
Router# ip flow-cache timeout active inactive 120 (segundos)
```

Luego de esto una verificación

Revisar las estadísticas localmente:

```
Router# show ip cache flow
Router# show ip cache verbose flow
Router# show ip flow export
Router# show ip route flow top-talkers
```

Por último exportar los datos recogidos

Exportar los flujos a un colector:

```
Router(config)# ip flow-export destination 192.168.1.10 9996
Router(config)# ip flow-export version 5 [ peer-as | origin-as ]
Router(config)# ip flow-export source loopback 0
```

7) Procedimientos

Para un router, un flujo de datos está constituido por un grupo de paquetes ip con una misma combinación (direcciones y puertos origen y destino, tipo de protocolo de transporte, tipo de servicio e interfaz de entrada) en un intervalo de tiempo. Cuando se detecta un nuevo flujo netflow guarda en la memoria interna la correspondencia entre el flujo y su interfaz de salida, de forma que para posteriores paquetes pertenecientes a ese flujo no será necesario recurrir a consultas en sus tablas de encaminamiento, ahorrando de este modo, valiosos ciclos de CPU.

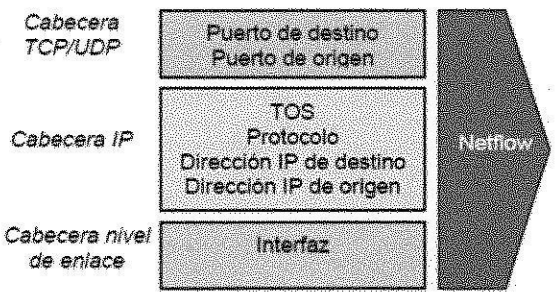


Figura 1. Información obtenida mediante Netflow

Precisamente, esta capacidad de los dispositivos de encaminamiento de obtener información referente a los flujos cursados puede ser aprovechada para medir y caracterizar el tráfico que atraviesa el *router* prácticamente en tiempo real, y ello de una manera convenientemente agregada facilita el análisis de la calidad de servicio.

Debemos tener en cuenta que para monitorear estos paquetes es necesario utilizar uno o más equipos conectados a la red para poder realizar un muestreo con todos los detalles de los paquetes TCP/IP que viajan en la red en ese momento.

También es importante dejar claro que la información obtenida es posteriormente analizada y organizada con el fin de comprender los puertos y direcciones origen y destino que los usuarios de una red están utilizando, de esta manera podremos revisar la variación de los puertos, cantidad de datos, retardo, velocidad y consumo de ancho de banda que están utilizando estos paquetes que viajan en nuestra red.

Los siguientes gráficos nos muestran un ejemplo de recolección de datos con netflow y sflow.

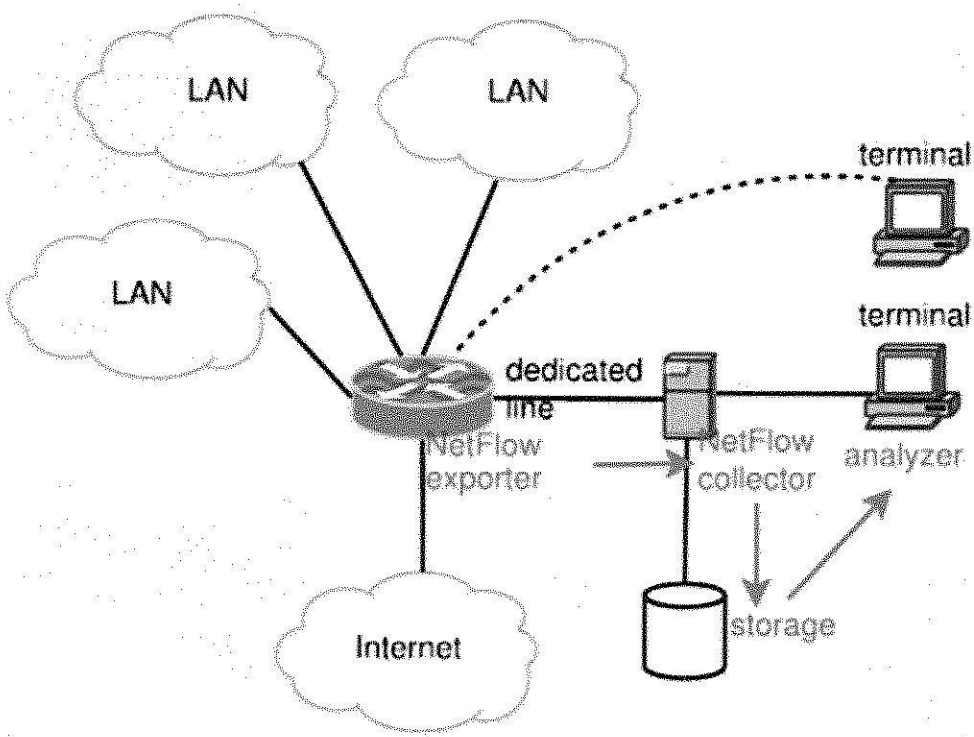
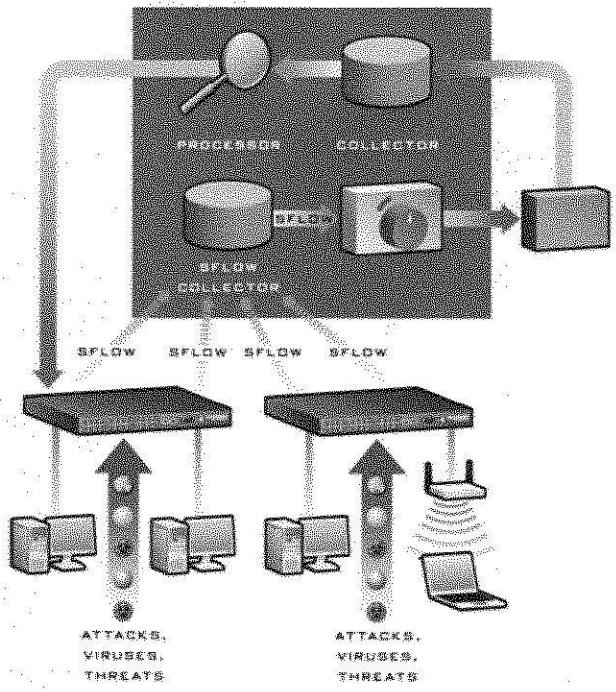


Imagen extraída de la página http://pusanbear-network.blogspot.com/search/label/Protocol



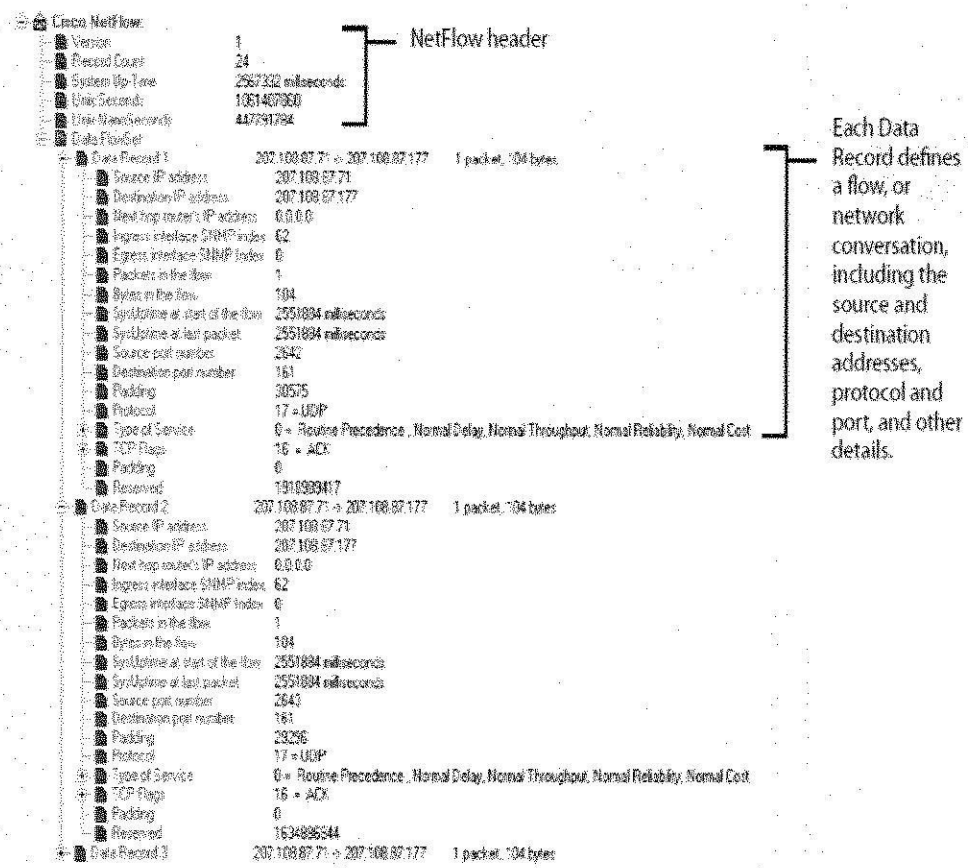
8) Análisis de resultados

Datos recolectados por NETFLOW

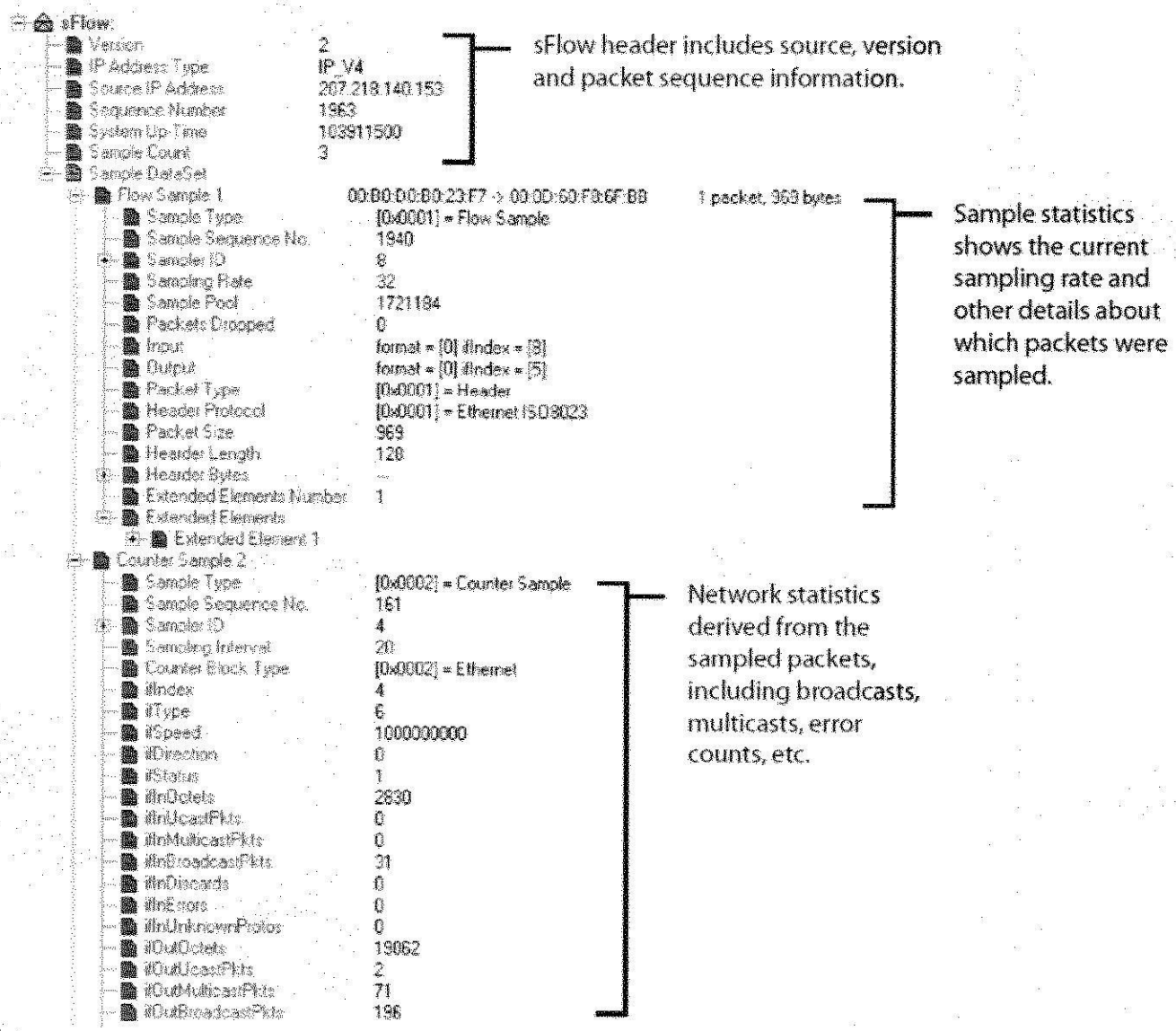
NetFlow records data per "flow," a flow being the traffic stream passing between a pair of addresses on a particular port.

NetFlow Datagram Example

(Decode provided by Network Instruments' Observer®)



Datos recolectados por sflow

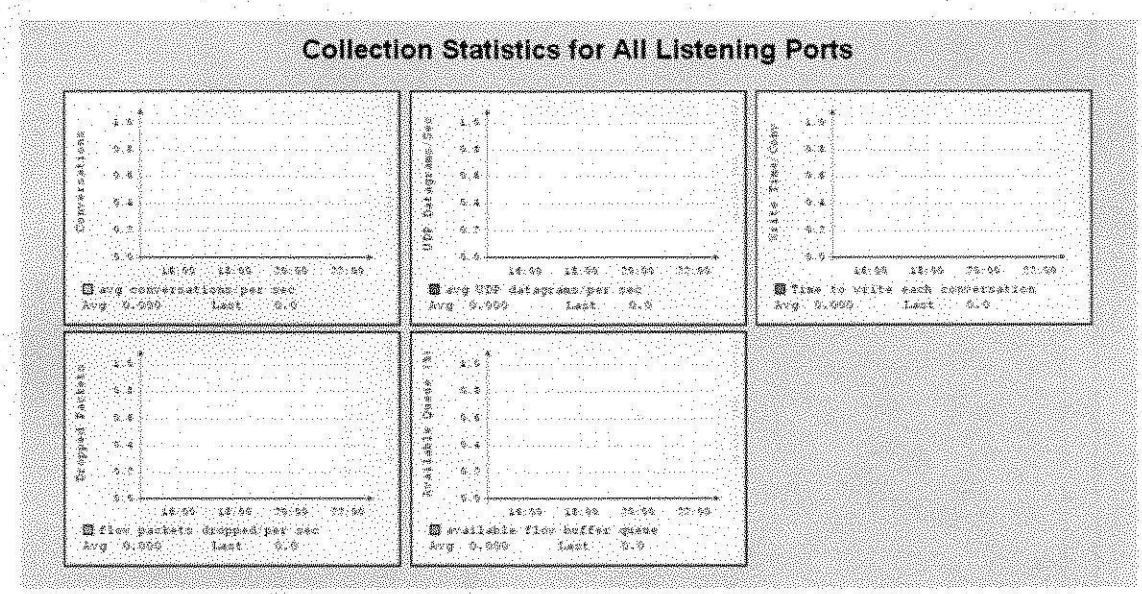


Con los datos que obtenemos podemos verificar que puertos están siendo utilizados el protocolo que se está usando, el intervalo de tiempo, cuales están afectados por virus.

Además de esto podremos tomar medidas correctivas o preventivas según sea el caso y de esta manera poder utilizar las herramientas que nos brinda el software que estemos utilizando, como las nombradas a continuación, que además son características del software de monitorización **ManageEngine NetFlow Analyzer 5:**

- **Alertas personalizables basadas en niveles y umbrales:** Se generan alertas cuando la utilización de tráfico supera los parámetros definidos por el usuario. Envía los traps SNMP a otras aplicaciones para las alertas críticas.
- **Grupos IP:** Se pueden crear grupos, departamentos o divisiones basados en dirección IP, para poder monitorizar el tráfico y filtrar los resultados basado en puertos / interfaces.
- **Informes de utilización de ancho de banda:** Informes sobre los usuarios, conversaciones, fuentes, destinos, hosts y aplicaciones más importantes.
- **Informes de tráfico:** Información completa sobre octets, velocidad, utilización y paquetes.
- **Informes a medida:** Se pueden realizar búsquedas avanzadas basadas en diferentes parámetros por rangos de tiempo.
- **Redireccionamiento de traps SNMP:** Se pueden reenviar traps automáticamente a otras aplicaciones, como soluciones globales de monitorización o gestores de alertas.
- **Reporting BGP:** Se informa sobre las estadísticas de tráfico AS (Autonomous Systems) para cada uno de los AS a los que pertenece el router o switch.
- **Mapeo de aplicaciones:** Permite identificar automáticamente aplicaciones empresariales como PeopleSoft, Oracle, etc. así como aplicaciones a medida.

Esta es una imagen tomada del programa



Por el momento no podemos observar una gran cambio pero si podemos ver que aplicaciones y que puertos están siendo utilizados

9) Practicas de Laboratorio

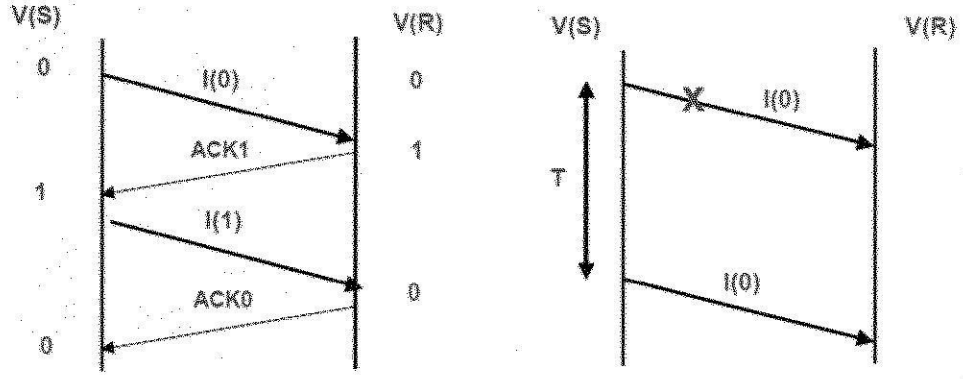
Para la siguiente Practica Vamos a instalar el **Scrutinizer NetFlow & sFlow Analyzer 4**, sobre los computadores de la universidad, Para medir el ancho de banda en tiempo real y analizar todos los datos que recojamos, de tal manera que podamos entregar un informe estadístico de los host que más recursos están consumiendo, las páginas más visitadas y los momentos en que el ancho de banda baja la velocidad.

Para esta práctica necesitamos un equipo conectado a la red que tenga instalado Windows xp, y cuente con los permisos de administración que no restrinja la instalación.

10)Anexos Red De Petri

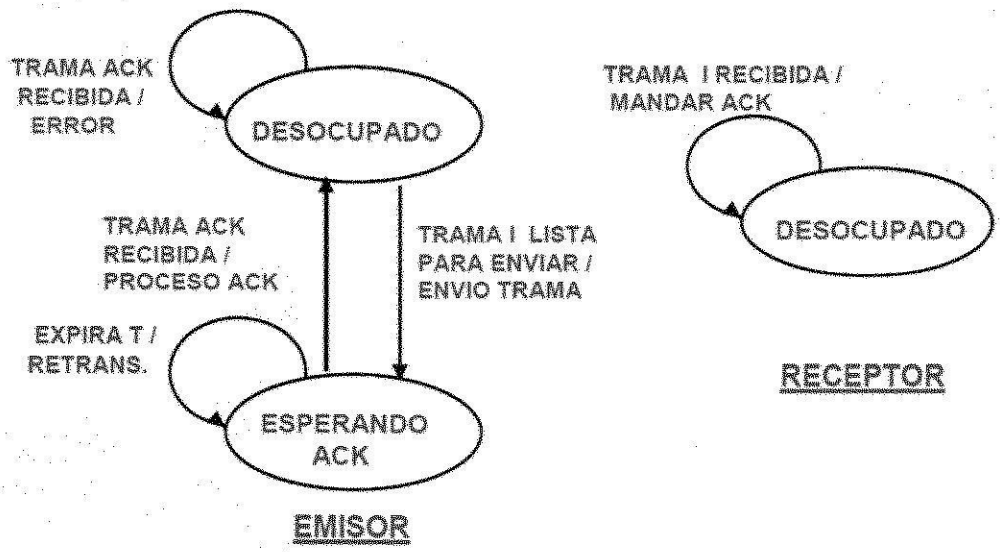
PROTOCOLO PARADA-ESPERA

Este es un protocolo para el control de errores en la comunicación entre dos hosts basado en el envió de tramas o paquetes, de tal manera que no se envía un paquete hasta no contar con un ACK (acuse de recibo).



Se pone a la trama un numero de secuencia de un bit (0,1); se utilizan dos tipos de confirmación: ACK0 y ACK1.

V(S) envía un SYNC para pedir conexión, V(R) admite conexión y envía un SYN con ACK, V(S) comienza el envió de datos, V(R) envía confirmación de recibido de datos.



EVENTO / ESTADO ACTUAL	EXPIRA TEMP.	TRAMA I LISTA	TRAMA ACK RECIBIDA	
DESOCUPADO (0)	NA	TRANS. TRAMA	ERROR	ACCION
	0	1	0	NUEVO ESTADO
ESPERANDO ACK (1)	RETRANS. TRAMA	RETARDO	PROC. ACK	ACCION
	1	1	0	NUEVO ESTADO

EVENTO / ESTADO ACTUAL	TRAMA I RECIBIDA	
DESOCUPADO (0)	MANDAR ACK	ACCION
	0	NUEVO ESTADO

$\Pi = \{p_1, p_2, p_3, .. p_r\}$ *Conjunto* *LUGARES*

$\Sigma = \{t_1, t_2, t_3, .. t_s\}$ *Conjunto* *TRANSICIONES*

$F: \Pi \times \Sigma \rightarrow N^*$ *Función incidencia PROGRESIVA*

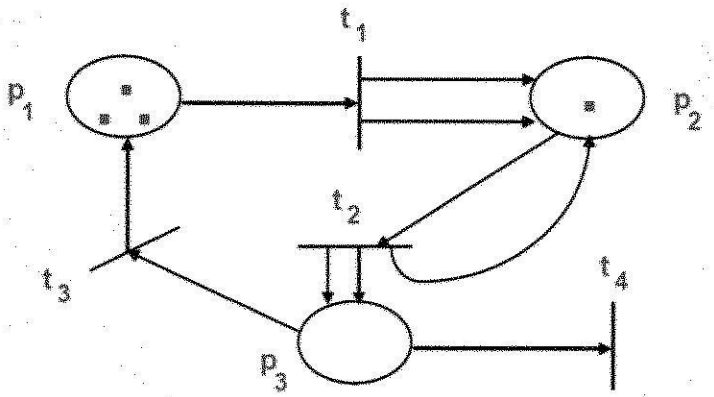
$B: \Pi \times \Sigma \rightarrow N^*$ *Función incidencia REGRESIVA*

$M: \Pi \rightarrow N^*$ *MARCAJE INICIAL*

REDES DE PETRI

$\Pi = \{p_1, p_2, p_3\}$ $\quad M_0 = \{3(p_1), 1(p_2), 0(p_3)\}$

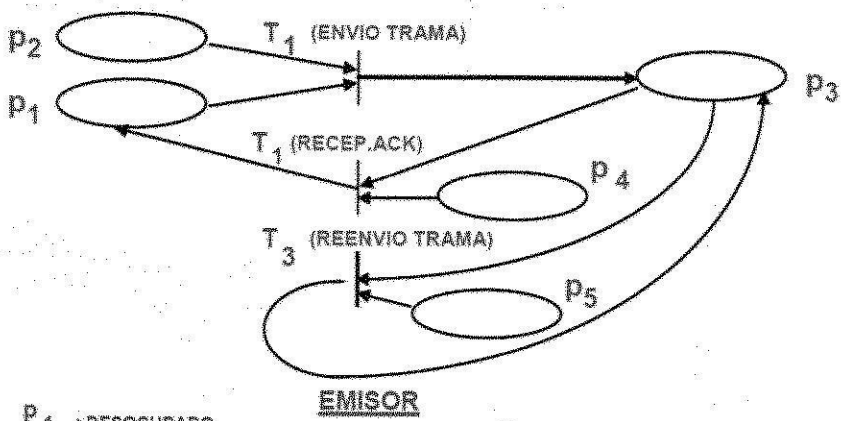
$\Sigma = \{t_1, t_2, t_3, t_4\}$



F	t_1	t_2	t_3	t_4
p_1	1	0	0	0
p_2	0	1	0	0
p_3	0	0	1	1

B	t_1	t_2	t_3	t_4
p_1	0	0	1	0
p_2	2	1	0	0
p_3	0	2	0	0

$p_i \rightarrow t_i$ $\qquad$ $t_i \rightarrow p_i$



p_1 : DESOCUPADO
p_2 : DATOS NIVEL SUPERIOR
p_3 : ESPERANDO ACK
p_4 : ACK RECIBIDO
p_5 :TEMPORIZADOR EXPIRADO

11) Bibliografía

1. Netflow(manage-netflow-analyzer-5.0) http://manageengine.adventnet.com/products/netflow/spanish/index.html
2. "Trafico monitoreado con sflow" http://www.sflow.org
3. Netflow "definición por wikipedia" http://en.wikipedia.org/wiki/Netflow
4. "Ireo soluciones y servicios" http://www.ireo.com
5. Monitorización mediante NETFLOW "universidad autónoma de Madrid"
6. Cortafuegos "henning mankell"
7. Programas http://www.archivospc.com/programas/categorias/Red%20Local%20(LAN).php?sort=2&order=1&page=2
8. Red De Petri http://es.wikipedia.org/wiki/Red_de_Petri
9. Tesis Doctoral "Redes Reconfigurables. Modelización y Verificación" Presentada por: Maria Luisa Llorens Agost – 2003

12)Conclusión

Dentro de los grupos involucrados en el desarrollo de Internet, existe un creciente interés en la prestación de servicios. IPPM (internet protocol performance metrics) constituye el marco de referencia en el cual tanto proveedores como clientes pueden, gracias a un conjunto de métricas comunes, llegar a establecer acuerdos de calidad de servicio y verificar el correcto cumplimiento de los mismos. Como se ha mostrado en el presente proyecto, netflow y sflow nos pueden servir como unas herramientas capaces de implementar en la práctica muchas de las métricas, concretamente el ancho de banda efectivo, el tiempo de respuesta, el retardo unidireccional y la variación del retardo unidireccional.

Cabe resaltar que para proyectos futuros seria de interés presentar nuevas alternativas que no solo nos permitan analizar y medir, sino que de una u otra manera nos ayuden a corregir errores comunes en el flujo de paquetes de una red, para lograr los estándares más elevados al momento de prestar un servicio.