ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERIA EN SISTEMAS

TEMA:

ESTUDIO DE LAS TÉCNICAS DE ANÁLISIS DE FLUJOS IP Y SU APLICACIÓN EN EL MONITOREO DE REDES DE DATOS EN LA ESCUELA DE INGENIERIA EN SISTEMAS PERTENECIENTE A LA FIE

TESIS DE GRADO

Previo a la obtencion del titulo de:

INGENIERO EN SISTEMAS INFORMATICOS

Presentado por:

Ana Belén Castro Romero

Andi del Cisne Estrella Escudero

RIOBAMBA – ECUADOR

2009

AGRADECIMIENTO

Queremos expresar nuestra gratitud a nuestros padres que siempre nos han apoyado, en particular queremos agradecer al Ing. Alberto Arellano y al Ing. Diego Ávila por su incondicional apoyo y dedicación, del mismo modo quisiéramos agradecer a la Escuela de Ingeniería en Sistemas y al Departamento de Sistemas y Telemática por permitirnos la implementación de nuestra tesis.

Hacemos extensivo nuestro más sincero agradecimiento a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de esta investigación.

Ana Belèn Castro

Andi Estrella

DEDICATORIA

Queremos dedicar esta tesis a Dios, a nuestros padres como reconocimiento a lo mucho que han hecho por nosotras, por su comprensión, motivación y apoyo.

También deseamos dedicar a las Autoridades y Profesores de la Facultad por su constante apoyo, sin ellos habría resultado imposible la realización de esta tesis.

Finalmente queremos dar las gracias a nuestros amig@s por sus diversas formas de apoyo durante toda nuestra carrera.

Ana Belèn Castro

Andi Estrella

Nosotras Ana Belén Castro Romero y Andi del Cisne Estrella Escudero, somos responsables de las ideas vertidas en esta tésis y el patrimonio intelectual pertenece a la ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO.

---------- ----------

ANA BELÉN CASTRO ANDI ESTRELLA

RESPONSABLES

NOMBRES	FIRMAS	FECHA
Dr. Romeo Rodríguez **DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	----------	----------
Ing. Iván Menes **DIRECTOR DE LA ESCUELA DE INGENIERÍA EN SISTEMAS**	----------	----------
Ing. Alberto Arellano **DIRECTOR DE TESIS**	----------	----------
Ing. Diego Ávila **MIEBRO**	----------	----------

Tlgo. Carlos Rodríguez
Dir. Dpto CENTRO DOCUMENTACION ---------- ----------

INDICE DE TABLAS

INDICE DE GRAFICOS

INTRODUCCION

En la actualidad las redes de computo de las instituciones se vuelven más complejas y la exigencia de la operación es cada vez mas demandante, por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter proactivo para prevenir problemas en un futuro.

Existen diversas metodologías herramientas y técnicas que son capaces de examinar el trafico de manera exhaustiva, están disponibles pues es muy popular en la infraestructura de red los dispositivos Cisco con ellos NetFlow, sFlow e IPFIX. Hay herramientas que utilizan la información de los flujos de tráfico para obtener monitoreo del comportamiento de la red y los usuarios, planeamiento de las redes, análisis de seguridad, contabilidad del tráfico IP, ingeniería de tráfico, etc. La prestación de servicios de calidad a los usuarios de una red depende de una gran cantidad de factores que involucran tanto aspectos de eficiencia como de seguridad.

La investigación de técnicas de análisis de flujos IP permitirá definir características, ventajas, y desventajas de las tecnologías NetFlow, sFlow e IPFIX y seleccionar la que mejor se adapte a las necesidades de la red de la Escuela de Ingeniería en Sistemas.

El desarrollo de la tesis contendrá cinco capítulos los cuales abarcan información importante para obtener resultados satisfactorios al usuario final. El capítulo I Marco Referencial se describirá antecedentes, justificación, objetivos e hipótesis que se deberán cumplir al finalizar la misma. El Capitulo II Marco Teórico en el cual se detallara información de cada una de las tecnologías. En el Capítulo III se realizara un estudio comparativo de los parámetros más relevantes de cada una para de esta manera seleccionar la mejor. En el capítulo IV se analizara los aspectos generales de

la EIS, el equipo a utilizar, se realizaran escenarios de simulación y finalmente el escenario a ejecutar en el Departamento de Sistemas y Telemática. El capitulo V es el análisis y evaluación final en el cual se mostraran los reportes obtenidos del monitoreo realizado y la comprobación de la hipótesis.

CAPITULO I

MARCO REFERENCIAL

1.1 Antecedentes

El Análisis de Flujos IP [16] permite especificar técnicas que faciliten implementar sistemas de monitoreo y control completo en tiempo real sobre desempeño, disponibilidad, administración de fallos, entre otros en toda la red, que es de gran utilidad para la gestión así como la optimización de los recursos y la detección de usos irregulares.

El análisis, la medición y la caracterización del tráfico de flujo en cualquier red IP o en Internet, son parámetros ampliamente utilizados y necesarios para cualquier operador de redes

Existen muchos sistemas que son capaces de examinar el tráfico de manera exhaustiva, detectar actividades maliciosas, monitorear complejas métricas de desempeño, capturar trazas del tráfico, capturar trafico de broadcast, que sitio Web es el más visitado entre otros.

Los requisitos para desarrollar estas mediciones actualmente están disponibles, pues es muy popular entre la infraestructura de red, los dispositivos Cisco con ellos NetFlow, sFlow e IPFIX.

Para realizar el análisis de la seguridad de las redes de datos, existen muchas y diversas metodologías, herramientas, y técnicas; y a su vez existen infinidad de manifestaciones en el comportamiento tanto de usuarios como de aplicaciones, que en el entorno de estas redes puede clasificarse como dañino, es por esto que se puede decir que no existe una manera absoluta de analizar todos los fenómenos.

NetFlow [8] es parte integral del IOS de Cisco, que realiza la medición y colección de los datos, a la entrada de las interfaces ya sea del router o del switch, de forma extremadamente granular y exacta, lo que da lugar a los flujos, que no son mas, que agregados de tráfico de alto nivel.

Sflow [5], es una tecnología que sirve para monitorizar el tráfico en las redes de datos que dispongan de switches y routers, define los mecanismos de muestreo implementados en un agente Sflow encargado de manejar el tráfico. Cuando se usa con una aplicación de gestión de red, Sflow proporciona una visión global de los patrones de tráfico de esa red, ayudando a predecir las posibles congestiones y permitiendo al usuario planificar futuras actualizaciones.

IpFix (IP Flow Information Export) [9], define los requerimientos para exportar flujos de información IP de salida de los router y pruebas de medición de tráfico. Está documentado en el RFC 3917.

A menudo estas herramientas proporcionan el contexto necesario para confirmar o desactivar una alerta de seguridad, entre las principales aplicaciones que se pueden desarrollar utilizando la información de los flujos de tráfico, encontramos: monitoreo del comportamiento de la red y los usuarios, planeamiento de las redes, análisis de seguridad, contabilidad del trafico IP, ingeniería de tráfico, etc.

En los últimos años, en la red académica española (RedIRIS) se han llevado a cabo diferente proyectos relacionados con la monitorización y la caracterización del tráfico de Internet, como por

ejemplo los proyectos CASTBA, MEHARI y MIRA. Estos proyectos se realizaron de forma conjunta entre la Universidad Politécnica de Madrid, la Carlos III de Madrid, la Politécnica de Catalunya (UPC), y con la participación como EPOs de RedIRIS, Telefónica Investigación y Desarrollo, el Centre de Supercomputación de Catalunya (CESCA) y el Instituto Catalá de Tecnología.

Hoy en día la red de la Escuela de Ingeniería en Sistemas perteneciente a la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo “ESPOCH” dispone únicamente de acceso a aplicaciones de Intranet, pero no existen herramientas que permitan especificar un monitoreo detallado de la red.

Uno de los principales problemas en una red de múltiples usuarios es el bajo rendimiento debido a que no existe un control adecuado de los procesos que retardan y dificultan al usuario final y a los técnicos, usos irregulares, ataques, entre otros, los mismos que no permiten obtener la información necesaria de todo lo que ocurre en la misma.

Por tal motivo realizaremos un análisis comparativo entre las técnicas de análisis de flujo IP (NetFlow, Sflow, IPFIX), con lo cual implementaremos una aplicación que permita realizar un control detallado de la red de la EIS, utilizando los equipos Cisco que se encuentran en la misma.

Nuestra aplicación será implementada bajo la plataforma Linux para obtener una utilización adecuada de todos los recursos que existen en la red.

1.2 Justificación

1.2.1 Justificación Teórica

Conocer el uso que se da a las redes es sumamente importante para el diseño y gestión de las mismas. El entorno de red actual, dominado por la arquitectura TCP/IP (Internet) es muy dinámico y en expansión aparecen nuevas aplicaciones día a día que no se restringen a los servicios básicos como Web, correo electrónico o transferencia de ficheros, sino que traspasan al ámbito del comercio electrónico, los servicios multimedia, etc. Los usuarios, a su vez, modifican sus hábitos

(número y tipo de peticiones, duración de las sesiones, etc.) aprovechando nuevos tipos de contratos (SLA, Service Level Agreement) que ofrecen distintos niveles de calidad de servicio. Finalmente, la comercialización de Internet ha puesto de manifiesto el replanteamiento de los métodos de tarificación (tarifa plana, etc.), ya que la tarificación aplicada en los servicios de telecomunicaciones existentes hasta el momento no parece satisfacer los requisitos del nuevo medio de comunicación de masas que es Internet.

Esto mismo ha supuesto un impacto importante en las redes de ámbito académico, a través de las cuales hoy en día se puede acceder a servicios no estrictamente académicos ni de investigación. Por consiguiente, las redes académicas deben adecuarse a políticas de uso aceptable (AUP) que impidan que dichas redes supongan una competencia desleal con las redes comerciales y por otro lado, empezar a aplicar una corresponsabilización de los gastos sin esperar una subvención completa de las instituciones públicas. En ambos casos es necesaria la monitorización del tráfico.

La gestión eficaz y eficiente de agregados de flujos es uno de los principales problemas a los que se enfrentan las redes IP actuales. Independientemente de los protocolos utilizados por cada uno de los flujos individuales que componen un agregado, éste debe comportarse y responder adecuadamente a las variaciones en los niveles de carga de la red como una sola entidad. Nuestro objetivo es el estudio de distintas técnicas de análisis de flujos IP y diseño de un esquema de control capaz de gestionar agregados heterogéneos en entornos dinámicos de manera totalmente transparente a los usuarios de la red.

1.2.2 Justificación Aplicativa

El estudio de las técnicas de análisis de Flujos IP permitirá aprovechar al máximo las ventajas que ofrece cada una de éstas, enfocadas a la creación de un sistema de gran versatilidad, eficiencia y disponibilidad brindando servicios de alta calidad a la comunidad.

La necesidad de agilizar los procesos de Internet para la comunidad de la EIS, proyectan una solución capaz de resolver los problemas de disponibilidad que existen en la actualidad en red de

la misma.

Esta solución proporciona información detallada sobre el uso de la red, que es de gran utilidad para su gestión y dimensionado, así como para la optimización de los recursos y la detección de usos irregulares y ataques, además permite automatizar y acelerar todos los procesos que han venido retardando y dificultando al usuario final y a los técnicos en la obtención de la información necesaria de todo lo que ocurre en la misma; mediante el diseño e implementación de una aplicación que permita monitorear el trafico que día a día ocurre en la red de la EIS, a través de los equipos disponibles. De esta manera el usuario final que actualmente se demora en obtener información por causa de algún fallo que ocurra, lo podrá realizar de manera más eficiente y rápida debido a que se realizara un control constante de la red.

Una vez que los usuarios finales palpen la facilidad y rapidez con la que se obtendrán la información se incrementara la demanda del uso de la red por parte de los estudiantes, docentes y empleados ayudando en el aspecto investigativo a la comunidad politécnica y permitirá realzar la imagen de la ESPOCH al contar con este servicio de punta en el área tecnológica y de calidad de servicio a la comunidad politécnica.

1.3 Objetivos

1.3.1 Objetivo General

Analizar las técnicas de análisis de flujos IP para la prestación de servicios de control y su aplicación en el monitoreo de redes de datos en la Escuela de Ingeniería en Sistemas – FIE.

1.3.2 Objetivos Específicos

- Estudiar y realizar un análisis comparativo de las tecnologías de análisis de flujo IP NetFlow, Sflow, IPFIX

- Determinar la tecnología que mejor se ajusten a la Infraestructura del monitoreo de la red de la EIS.
- Implementar la aplicación de monitoreo utilizando el Sistema Operativo Linux en su versión SUSE.
- Presentar los resultados obtenidos de la aplicación de monitoreo para que contribuya a la futura realización de políticas de seguridad y estrategias para un mejor control de la red.

1.4 Hipótesis

La aplicación de las TÉCNICAS DE ANÁLISIS DE FLUJOS IP en la red de la Escuela de Ingeniería en sistemas perteneciente a la Facultad de Informática y Electrónica, permitirá realizar un mejor monitoreo y determinar de una manera más detallada las aplicaciones y los usuarios que mayor uso hacen de la red.

CAPITULO II

MARCO TEÓRICO

2.1 Definición de Monitoreo de Redes

Introducción

En la actualidad las redes [18], cada vez mas, soportan aplicaciones y servicios estratégicos de las organizaciones, las cuales si fallan, sin saber cual es el punto de ruptura, puede causar perdidas para la corporación o entidad.

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante.

Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas en el futuro.

La seguridad no sólo radica en la prevención, sino también en la identificación. Entre menos tiempo haya pasado desde la intrusión e identificación, el daño será menor; para lograr esto es importante

hacer un constante monitoreo del sistema con la finalidad de identificar áreas vulnerables que los intrusos utilizan para atacar a los servidores, PC, aplicaciones, entre otros, así como proporcionar los conocimientos necesarios para monitorear las principales actividades de cada uno de ellos.

La prestación de servicios de calidad a los usuarios de una red depende de una gran cantidad de factores que involucran tanto aspectos de eficiencia como de seguridad.

En el aspecto de la eficiencia el ancho de banda disponible y la utilización que se haga del mismo representa un factor crítico.

Mientras que en el caso de la seguridad, es importante conocer el tipo de tráfico que está siendo cursado en la red, así como tener la capacidad de detectar tráfico de carácter malicioso.

En relación al aspecto de eficiencia, el administrador y el diseñador de redes deben estar en capacidad de determinar el ancho de banda requerido de acuerdo a las necesidades de la organización y la forma efectiva como éste se utiliza cuando la red se encuentra en producción. Es importante recordar que los costos de comunicación de las empresas es uno de los rubros presupuestarios por servicios más importante. Por lo que durante el diseño de una red se deben realizar planes pilotos para monitorear y determinar los anchos de banda que serán requeridos durante su funcionamiento. Los monitoreos se requieren tanto para el tráfico que se genera hacia la misma red de área local como al exterior.

Una vez que la red entra en producción, el administrador debe efectuar monitoreos de forma constante con el fin de determinar el tipo de tráfico que es enviado por medio de ésta y cuáles tipos de tráfico genera cada usuario o dispositivo. Lo anterior con el fin de detectar posibles fallas de dispositivos específicos, de diseño de la topología y de seguridad. En muchos casos reales los problemas de calidad de servicio no se deben a un limitado ancho de banda, sino a problemas de diseño de la topología y de la seguridad de la misma.

El contar con conocimiento detallado sobre el tráfico regular que envían los usuarios de una red y el tipo de tráfico que se está enviando en un momento determinado permite detectar posibles ataques a determinados dispositivos.

De acuerdo a los puntos enumerados anteriormente, la realización del monitoreo de tráfico de red sirve tanto para detectar problemas de eficiencia, como problemas de seguridad y diseño en una red. Sin embargo, para un administrador de red o diseñador de la infraestructura, efectuar el análisis y la interpretación de los resultados del monitoreo de red no es una tarea fácil de realizar. Por lo que la forma como éstos le sean presentados puede brindarle una gran cantidad de información útil o simplemente un grupo de datos difíciles de relacionar y sin significado coherente. Teniendo esto en consideración, es fácil llegar a la conclusión de que la visualización correcta y apropiada de los resultados del monitoreo de una red resultan críticos para que se puedan tomar decisiones correctas con respecto a ésta.

Estrategia de monitoreo

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear así como las herramientas que se utilizarán para esta tarea.

Una consideración muy importante es delimitar el espectro sobre el cual se va a trabajar.

TABLA II.01

CONDICIONES GENERALES DE LA ESTRATEGIA DE MONITOREO

Que monitorear	**Alcance dispositivos a ser monitoreados**	**Métricas**	**Alarmas**
• Utilización de ancho de banda • Consumo de CPU	• Dispositivos de interconexión (Ruteadores, switches, hubs, firewall)	Permiten establecer patrones de comportamiento de los dispositivos a ser monitoreados.	Son consideradas como eventos con comportamiento inusual. **Tipos** • Alarmas que reportan cuando el estado operacional de un

• Consumo de memoria • Estado físico de las conexiones • Tipo de tráfico • Alarmas • Servicios (Web, correo, base de datos)	• Servidores (Web, mail, DB) • Red de Administración (Monitoreo, Logs, Configuración)	Ejemplos: • Métricas de tráfico de entrada y salida • Métricas de utilización de procesador y memoria • Métrica de estado de las interfaces. • Métrica de conexiones lógicas	dispositivo o servicio cambia. • Alarmas basadas en patrones (son valores máximos conocidos como umbrales o threshold). • Alarmas de procesamiento • Alarmas de conectividad • Alarmas ambientales • Alarmas de Utilización • Alarmas de disponibilidad (estado operacional)

FUENTE: http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html

ELABORADO POR: Las autoras

Elección de herramientas

Existe un gran número de herramientas para resolver el problema del monitoreo de una red. Las hay tanto comerciales como basadas en software libre. La elección depende de varios factores, tanto humanos, económicos como de infraestructura:

- El perfil de los administradores, sus conocimientos en determinados sistemas operativos;
- Los recursos económicos disponibles
- El equipo de cómputo disponible.

2.2 Tipos de Monitoreo de Redes

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

Monitoreo Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento de una red.

Técnicas de monitoreo activo

- Basado en ICMP
  - Diagnosticar problemas en la red
  - Detectar retardo, perdida de paquetes
  - RTT
  - Disponibilidad de host y redes.
- Basado en TCP
  - Tasa de transferencia
  - Diagnosticar problemas a nivel de aplicación
- Basado en UDP
  - Perdida de paquetes en un sentido (one-way)
  - RTT (traceroute)

Monitoreo Pasivo

Este tipo se basa en la obtención de datos a partir de recolectar y analizar el trafico que circula por la red. Se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de .analisis de trafico y en general dispositivos con soporte para snmp, rmon y Netflow. Este enfoque no agrega trafico en la red como lo hace el activo. Es utilizado para caracterizar en la red y para contabilizar su uso.

Tecnicas de monitoreo pasivo

- **Solicitudes remotas**

Mediante SNMP

Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados *traps* que indican que un evento inusual se ha producido.

Otros métodos de acceso

Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante para monitorear. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública, etc.

- ***Captura de tráfico***

Se puede llevar a cabo de dos formas:

1) Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura.

2) Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

- ***Análisis de Tráfico***

Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son mas utilizadas. Se puede implementar haciendo uso de dispositivos *probe* que envíen información mediante RMON o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino,etc.

- ***Flujos***

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing).

2.3 Análisis de Flujos IP

Flujo [6]

Se define como una secuencia unidireccional de paquetes con ciertas características comunes:

- Direcciones IP fuente y destino
- Número de protocolo a nivel 3
- Puertos fuente y destino
- Octeto de ToS (Type of Service)
- Índice de la interfaz de entrada (ifIndex)

Cisco llama a esta una "definición quíntuple de tráfico" en alusión a que se utilizan 5 elementos para la misma.

La medición, el análisis y la caracterización del tráfico de Internet o en general de cualquier red IP, se ha convertido en una técnica ampliamente utilizada y necesaria para cualquier operador de redes.

Como parte de las tareas de administración y explotación de una red de datos, deben realizarse disímiles acciones, enfocadas a la solución de los problemas de desempeño, el planeamiento, la seguridad, etc. Para realizar estas tareas de manera efectiva es necesario realizar la medición, cuantificación y análisis del tráfico que se cursa utilizando la red

En la actualidad, Internet se ha consolidado como la red telemática más extendida y utilizada a nivel mundial. El crecimiento en lo que respecta a infraestructuras así como al número de usuarios conectados ha sido vertiginoso en los últimos tiempos.

Este crecimiento ha dado lugar al surgimiento de un conjunto de nuevos servicios y aplicaciones (tales como las comunicaciones multimedia o el comercio electrónico) y nuevos paradigmas, como las comunicaciones peer-to-peer, P2P (entre iguales), que no existían hace algunos años. También ha dado lugar al surgimiento de amenazas, en la forma de ataques de seguridad a través de la Red.

Esta continua evolución en el tráfico que circula por Internet hace necesario contar con herramientas adecuadas y flexibles que permitan conocer las características de dicho tráfico. En

este sentido, se va a describir los diferentes sistemas de captura y monitorización de trafico flexible, basado en el análisis de patrones, adaptable a múltiples escenarios de utilización y con un conjunto de características avanzadas.

Para realizar el análisis de la seguridad de las redes de datos, existen muchas y diversas metodologías, herramientas y técnicas, y a su vez existen infinidad de manifestaciones en el comportamiento tanto de usuarios como de aplicaciones, que en el entorno de estas redes puede clasificarse como dañino, es por eso que se puede decir que no existe una manera absoluta de analizar todos los fenómenos.

Arquitectura del Análisis

Exportador (Router o Switch)

-Crea un flow cache y exporta los récords

Colector

-Escucha en un puerto UDP

-Guarda o reenvía los flows a otros colectores

Analizador

-Filtra, muestra, analiza y/o grafica los datos

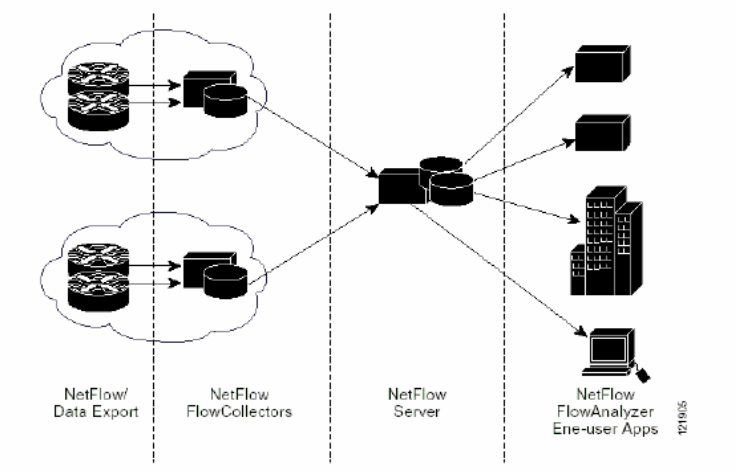


Figura N°II.I Arquitectura del análisis

En la figura (arriba) se observa :

- Los routers crean una serie de **registros por cada flujo** que los atraviesa.
- En principio esta técnica pretendía facilitar el **proceso de enrutamiento**.
- La **información** que contiene normalmente un registro es:

  Tiempo de **inicio** y **fin**

  Numero de **paquetes** y **bytes**

  Interfaces de salida y entrada

  Direcciones IP y **puertos** origen y destino

  Mascaras.

Los routers consideran que un flujo ha concluido, y que por tanto, **deben exportar la información** contenido en memoria, cuando sucede algunas de estas situaciones:

- Se encuentra una bandera de fin de conexión
- Cuando un flujo no produce tráfico en 15 segundos
- 30 minutos después del comienzo
- Cuando el router se queda sign recursos

Sin embargo, se ha comprobado que a las velocidades actuales **no es posible en cuanto a recursos de memoria y velocidad de acceso** capturar y actualizar los contadores por cada paquete de cada flujo

La solución que se implementa es la de **muestrear sólo un porcentaje de los paquetes**.
Esto implica que la **precisión de las estadísticas** de los registros **no será exacta** en métricas como el tiempo de inicio y fin.
Métricas tales como **el número de paquetes quedarán divididas** según la tasa de muestreo.

TABLA II.02

APLICACION DE LOS FLUJOS Y HERRAMIENTAS UTILIZADAS

Aplicación de los flujos	**Herramientas**
Determinación de problemas • Clasificación de tráfico • Análisis de ataques de denegación de servicio Ingenieria de tráfico • Análisis de tráfico Inter-AS • Uso de proxies Contabilidad • Completa información SNMP	• Múltiples paquetes Open-Source y evolucionando • Flow-tools, Flowscan, FlowViewer, nfdump/nfsen, Starger, etc. Aplicaciones comerciales • Cisco NetFlow Collector • Árbol Networks

Fuente: www.cisco.com/univercd/cc/td/doc/cisictwk/intsolns/netflsol/nfwhite.htm

Elaborado por: Las autoras

2.4 Descripción de tecnologías de análisis de flujos IP

2.4.1 NetFlow

NetFlow es una tecnología abierta pero desarrollada por cisco, sirve para generar gráficos o tablas de información en función de tiempo que permitan ver en que estamos gastando el ancho de banda, que equipos, aplicaciones o protocolos consumen los recursos de la red, relevar nivel de utilización de enlaces en función de subredes o monitorear el nivel de utilización de un enlace y otra información útil para el administrador de la red

Como la tecnología es abierta, otros fabricantes la implementan, como 3Com, Enterasys, Nortel, Juniper, Alcatel oHP Procurve, entre otros.

NetFlow de Cisco. Es una herramienta adecuada para el desarrollo de tareas de "accounting" en una red.

¿Qué es NetFlow?

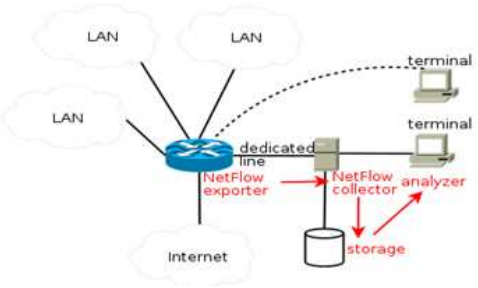


Figura N° II.02 NetFlow

Es un protocolo propietario de Cisco soportado en la actualidad por casi todas las líneas de switches y routers Cisco. Este protocolo permite a los dispositivos colectar información referida a todo tráfico que atraviesa los enlaces y enviar la información referida a ese tráfico utilizando UDP a un dispositivo que recibe la denominación de NetFlow Collector para la generación de informes, estadísticas, etc..

La ventaja de NetFlow [13] respecto de SNMP es que este protocolo brinda, fundamentalmente, información y funcionalidades de gestión, mientras que a esa información NetFlow le agrega la referida al tráfico que provoca el estado de utilización de cada dispositivo.

Entre las aplicaciones posibles de NetFlow se pueden contar el monitoreo de la red de forma grafica y sencilla, principalmente para saber cómo, quien y en que se está usando el ancho de banda disponible, el monitoreo de aplicaciones específicas, detectar y prevenir cuellos de botella, el monitoreo de usuarios, el planeamiento de actualizaciones o modificaciones de la red, el análisis de seguridad, la implementación de sistemas de contabilidad y facturación, data warehousing y minig del tráfico de red, y tomar acciones correctivas o preventivas,etc.

NetFlow realiza la creación de los flujos a la entrada del tráfico al router, y no a su salida, por lo que los flujos solo se actualizan por paquetes que provienen de la red (y no por paquetes que provienen de otras interfaces).

¿Qué es un NetFlow Collector?

NetFlow Collector es un dispositivo (PC o servidor) ubicado en la red para recoger toda la información de NetFlow que es enviada desde los dispositivos de infraestructura (routers y switches).

NetFlow es un protocolo que genera y recoge esta información, pero también se necesita software que permita realizar la clasificación, almacenamiento y análisis de toda esta información de tráfico. Para esto hay en el mercado una amplia diversidad (por prestaciones y precio) de aplicaciones en el mercado que permiten trabajar sobre la información de NetFlow.

Registro Netflow

Un registro NetFlow puede contener un ancho de variedad de información a cerca del tráfico en un flujo dado. La versión 5 de NetFlow (una de las versiones más comúnmente usadas, siguiéndole la versión 9) constan de lo siguiente:

- Numero de Versión
- Numero de Secuencia
- Índices de interfaces de entrada y salida usados por SNMP
- Timestamps para el tiempo de inicio y finalización del flujo, en milisegundos desde el ultimo boot
- Cabeceras de la capa 3:

  Direcciones IP fuente y destino.

  Números de puerto de fuente y destino

  Protocolo IP

  Valor del tipo de Servicio (ToS)

- En el caso de flujos TCP, la unión de todos los flags TCP observados a lo largo de la vida del flujo.
- Información de ruteo en la capa 3:
    - Direcciones IP del siguiente salto a lo largo del router de destino.
    - Mascaras IP de fuente y de destino (Longitud de prefijos en la notación CIDR).

Algunos routers pueden incluir el número del Sistema Autónomo (AS) en la fuente y el destino. Dependiendo de la configuración en el router, este puede ser inmediatamente el vecino AS.

La versión 9 de netflow puede incluir todos estos archivos y puede incluir opcionalmente información adicional tal como Multiprotocol Label Switching (MPLS) y direcciones y puertos IPv6.

Para analizar los flujos de datos, un cuadro del flujo de tráfico y volumen de tráfico en una red puede ser construido.

Los registros netflow son usualmente enviados vía UDP o SCTP y por razones de eficiencia, los routers no almacenan registros de flujo, estos son exportados.

Exportación de Registros

- Bajo ciertas circunstancias, los registros caducan en la cache de flujos cuando:

  Tiempo de vida activo/inactivo (por defecto: 15seg/30 min)

  La cache se llena

  Conexiones TCP con FIN o RST

- Al caducar, los flujos se agrupan y se exportan en datagramas de hasta 30 registros.

TABLA II.03
VERSIONES DE NETFLOW

Versión	Descripción
v1	Versión original. Ya no se utiliza
v5	Agregó información sobre sistemas autónomos (BGP) y números de secuencia. La más utilizada hoy día
v6	Encapsulamiento de información.
v7	Básicamente igual a la 5, pero en Catalyst
v8	Agregación en el router
v9	Más flexible, basada en plantillas, soporta agregación en el router. Sirviendo como base para el nuevo estándar IPFIX de la IETF

Fuente: www.universidadoregon.com/introduccion_network_flows/

Elaborado por: José Domínguez

TABLA II.04

CARACTERISTICAS DE LA EXPORTACIÓN DE REGISTROS

Descripción		
Cacteristicas	**Rendimiento**	Factores que afectan el rendimiento Número de flujos activos Control de timers Número de flujos exportados Uso de muestreo (sampling) Agregación en el enrutador Cantidad de memoria asignada a la cache (algunos modelos)
	Muestreo	• Colecta estadísticas para un subconjunto del tráfico que pasa por una interfaz • Reduce significativamente el impacto en el CPU • Imagen inexacta del tráfico No sirve para contabilidad y facturación Aún así útil para la planificación • Alternativa para routers del backbone con alto número de interfaces y flujos

		Tipos de Muestreo • Determinístico: selecciona uno de cada N paquetes • Basado en tiempo: selecciona un paquete cada N milisegundos • Aleatorio: de cada N paquetes selecciona uno al azar, considerado como la mejor opción.
	Planificación	Planificar cuidadosamente donde se van a colectar los flujos • Routers de borde o de agregación por donde pasa la mayoría de tráfico. • Evitar recoger flujos duplicados en routers de backbone Buscar la configuración óptima para los tiempos de expiración (timer). Determinar que AS BGP interesa más • Peer AS • Origin AS

Fuente: www.cisco.com/univercd/cc/td/doc/cisictwk/intsolns/netflsol/nfwhite.htm

Elaborado por: Las autoras

Información empaquetada del IOS de Netflow

Cisco Netflow 7200/7500/7400/MGX/AS5800- aunque funcionalmente esta físicamente incluido en todas las imágenes del software para estas plataformas, los clientes deben adquirir una licencia de Netflow para poder hacer uso de la misma. Las licencias de netflow se venden para cada nodo base.

Otros routers-Netflow su funcionalidad es soportada solo en imágenes Plus para estas plataformas. Los clientes están obligados a adquirir una imagen mas adecuada a fin de utilizar las funcionalidades de Netflow en estas plataformas. No hay ningún distintivo de licencia para la mayoría de las plataformas de cisco, excepto los siguientes requieren una licencia de software de Cisco 7200/7500/7400/MGX/AS5800.

Reforma a los IOS de lso Paquetes-Netflow está actualmente disponible en el paquete base de propiedad intelectual y superiores.

Interfaces que soporta Netflow, encapsulación y protocolos

Netflow soporta trafico de router en IPv4 (y encapsulación IPv4) por encima de un rango ancho de tipos de interfaces y encapsulación. Esto incluye Frame Relay, Modo de transferencia Asincrono, Inter-Switch Link, 802.1q, protocolo Punto a Punto de Enlace Multipunto, encapsulación de ruteo general, VPNs, tuneles IP Sec.

Netflow es soportado por sub-interfaces. Si netflow es configurado en la interface principal entonces todas las sub-interfaces pueden ser contabilizadas. También están disponibles las características de las sub-interfaces de Netflow para ser contabilizadas por paquetes o sub-interfaces especificas.

Netflow soporta multicast existents en algunas plataformas Cisco.

¿Cómo saber si los dispositivos soportan NetFlow?

NetFlow está incorporado en Cisco IOS, por lo que ante todo es preciso verificar si la versión de IOS que estamos utilizando incluye NetFlow. Para esto podemos utilizar una herramienta específica del sitio web de Cisco que es el Cisco Feature Navigator.

Un modo más sencillo y directo, puede ser ingresar a la línea de comando de nuestro dispositivo y aprovechar las facilidades que da el sistema de ayuda de Cisco IOS. Si obtenemos una respuesta como la que sigue, nuestra versión de IOS incluye las funcionalidades NetFlow:

```
Router#configure terminal
```

Ponga los comandos de configuración. Finalice con CNTL/Z.

```
Router(config)#ip flow?
flow-aggregation flow-cache flow-export
Router(config)#ip flow
```

Atención: el comando debe ser ejecutado en modo configuración global.

Aplicaciones, Licencias y precios

Cisco desarrolla e implementa la tecnología netflow en sus dispositivos, pero no dispone de una aplicación para su utilización.

Hay varias empresas que han desarrollado herramientas para ello, como Fluke NetflowTracker, SolarWinds Netflow Analyzer, y algunas gratuitas, pero no con la misma calidad.

Los precios y las licencias van en función del número de interfaces que se desee monitorizar.

Hay una versión gratuita que permite monitorizar solo 2 interfaces.

2.4.2 sFlow

sFlow es una tecnología para monitorear el tráfico en redes de datos que contienen switches y routers. En particular, esto define los mecanismos de muestreo puestos en práctica en un Agente sFlow para supervisar el tráfico, el sFlow MIB para controlar al Agente sFlow, y el formato de datos de la muestra usados por el Agente sFlow enviando estos a un colector de datos central.
La arquitectura y técnicas de muestreo usadas en el monitoreo sFlow del sistema son diseñadas para proporcionar un continuo site-wide (and network-wide) del monitoreo de tráfico de la alta velocidad en la red con switches y routers

El diseño asocia especificamente las direcciones con :

- Monitorea con exactitud redes con tráfico en Gigabit o en velocidades más altas.
- Escalamiento para manejar las decenas de miles de agentes de un solo punto.
- Extremadamente bajo costo de implementación.

El sistema de monitoreo sFlow consiste en un Agente sFlow (integrado en un switch o router) y una central colectora de datos, o el Analizador sFlow.
El Agente sFlow usa la tecnología de muestreo para capturar la estadística de tráfico desde el dispositivo que monitorea. Los datagramas sFlow son usado para inmediatamente enviar las estadísticas de tráfico probadas a un Analizador sFlow para el análisis.

Mecanismos de Muestreo

El Agente sFlow usa dos formas de muestreo: muestreo estadístico a base de paquete de flujos cambiados, y muestreo a base de tiempo de estadística de interfaz de red.

Muestreo de Flujos Cambiados

Un flujo es definido como todos los paquetes que son enviados sobre una interfaz, entran al Modulo Switching/Routing y son enviados a otra interfaz. En el caso de un one-armed router, la fuente y la interfaz de destino podrían ser los mismos. En el caso de una broadcast o el paquete de multicast puede haber múltiples interfaces de destino.

El mecanismo de muestreo debe asegurar que cualquier paquete implicado en un flujo tiene una posibilidad igual de muestreo, independientemente del flujo al cual esto pertenece.

Los flujos de muestreo son logrados así: Cuando un paquete llega sobre un interfaz, una decisión de filtración es hecha lo que determina si el paquete debería ser dejado caer. Si el paquete no es filtrado a una interfaz de destino es asignado por la función del switching/routing .

En este punto una decisión es hecha sobre si realmente probar el paquete. El mecanismo implica un contador que es decrementado con cada paquete. Cuando el contador se pone a cero una muestra es tomada.

Si realmente una muestra es tomada, el contador Total_Packets es incrementado. Total_Packets es una cuenta de todos los paquetes que podrían haber sido probados.

La toma de una muestra implica copiar el jefe del paquete, o la extracción de rasgos del paquete. Siempre que una muestra es tomada, el contador Total_Samples, es incrementada. Total_Samples es una cuenta del número de muestras generadas. Las muestras son enviadas por la entidad de muestreo al Agente sFlow para el tratamiento. La muestra incluye la información de paquete, y los valores de los contadores Total_Samples y el Total_Packets.

Cuando una muestra es tomada, el contador que indica cuantos paquetes se debe saltar antes de la toma de la siguiente muestra deberían ser reinicializados. El valor del contador debería ser puesto a un número entero arbitrario donde la secuencia de números enteros arbitrarios usados con el tiempo debería ser igual a ese.

Una estrategia alternativa para el muestreo de paquete es de generar un número aleatorio para cada paquete, comparar el número aleatorio a un umbral predeterminado y tomar una muestra siempre que el número aleatorio sea más pequeño que el valor de umbral. El cálculo de un valor de umbral apropiado depende de las características del generador de número aleatorio, sin embargo, la corriente de muestra que pasa todavía debe satisfacer.

Switching Distribuido

El sFlow MIB permite a entidades de muestreo separadas ser asociadas con los elementos diferentes físicos o lógicos del switch (como interfaces, backplanes o VLANS). Cada motor de muestreo tiene su propio estado independiente (ej., Total_Packets, Total_Samples, Skip y Rate), y hacia adelante sus propios mensajes de la muestra al Agente sFlow. El Agente sFlow es responsable de empaquetar las muestras dentro de datagramas para la transmisión a un Analizador sFlow.

Generación de números aleatorios

La característica esencial del generador de número aleatorio es que el valor de los números que esto genera converge a la tarifa de muestreo requerida.

Un generador de número aleatorio de distribución uniforme es muy eficaz.

El rango de salto de las cuentas (la varianza) considerablemente no afectan resultados; la variación de + el-10 % del valor es suficiente.

El generador de número aleatorio debe asegurar que todos los números en la gama entre sus valores máximos y mínimos de la distribución son posibles; un generador de número aleatorio sólo es capaz de generar números pares, o números con cualquier divisor común es inadecuado.

Muestreo de Estadística de Interfaz de Red

El objetivo del muestreo debe ser de manera eficiente, de vez en cuando sondear cada fuente de datos sobre el dispositivo y extraer la estadística clave.

Por la eficacia y adaptabilidad, el Sistema sFlow pone en práctica el contador que sondea en el Agente sFlow. Un máximo que sondea el intervalo es asignado al agente, pero el agente es libre de programar el sondeo para maximizar la eficiencia interna.

El muestreo de flujo y el contador de muestreo son diseñados como la parte de un sistema integrado. Ambos tipos de muestras son combinados en Datagramas sFlow. Ya que el muestreo de flujo será constante, pero arbitrario, la cadena de datagramas será enviado al Analizador sFlow, contadores de muestras pueden ser tomadas de una manera oportuna para llenar estos datagramas.

Una estrategia para el contador de muestreo hace el Agente sFlow mantener una lista de fuentes de muestras probadas. Cuando una muestra de flujo es generada el agente sFlow examina la lista y añade contadores al datagrama de la muestra, lo menos recientemente probado primero. Los mostradores sólo son añadidos al datagrama si las fuentes son dentro de un período corto, 5 segundos.

De no encontrar el intervalo de muestreo requerido. Siempre que la estadística de una fuente contraria sea añadida a un datagrama de la muestra, el tiempo de la fuente contraria era la última probada, entonces es puesto al día y la fuente contraria es colocada al final de la lista. De vez en cuando, cada segundo, el Agente sFlow examina la lista de fuentes contrarias y envía cualquier contador que tiene que ser enviado para encontrar la exigencia de intervalo de muestreo.

Alternativamente, si el agente con regularidad programa el contador de muestreo, entonces esto debería programar cada contador fuente en un tiempo de principio diferente (preferentemente al azar) de modo que el contador de muestreo no sea sincronizado dentro de un agente o entre agentes.

sFlow MIB

El sFlow MIB define una interfaz de control para un agente sFlow.

Esta interfaz proporciona un mecanismo estándar para el control de forma remota y la configuración de un agente sFlow.

The SNMP Management Framework

En el SNMP Management Framework actualmente consta de cinco grandes componentes:

- Una arquitectura general, que se describe en el RFC 2571
- Mecanismos para la descripción y denominación de objetos y eventos para el propósito de la gestión. La primera versión de esta estructura de Información de Gestión (SMI) se llama SMIv1 y que se describen en las ETS 16,
- Mensaje o protocolos para la transferencia de información de gestión. La primera versión del protocolo de mensajes SNMP se llama SNMPv1 y se describe en el STD 15, RFC 1157. Una segunda versión del protocolo de mensajes SNMP, que no es una pista de estándares del protocolo de Internet, se llama SNMPv2c y se describe en el RFC 1901 y RFC 1906. La tercera versión del protocolo de mensaje se llama SNMPv3 y esta descrito en el RFC 1906, RFC 2572 y RFC 2574.

Consideraciones de seguridad

El despliegue de un sistema de vigilancia del tráfico plantea una serie de cuestiones de seguridad conexas. sFlow no prevé mecanismos de seguridad, apoyándose en cambio en el despliegue y la configuración adecuada para mantener un nivel adecuado de seguridad.

Si bien el despliegue de sistemas de monitoreo de tráfico crea algunos riesgo, sino que también proporciona un medio poderoso de detección y rastreo la actividad de la red no autorizado.

Esta sección está destinada a proporcionar información que ayudará a entender los riesgos potenciales y las opciones de configuración para mitigar esos riesgos.

Control

El sFlow MIB se utiliza para configurar la generación de muestras sFlow.

La seguridad de SNMP, con listas de control de acceso, se considera por lo general adecuado para el establecimiento de una empresa. Sin embargo, hay situaciones en que estas medidas de seguridad son insuficientes (por ejemplo una red WAN del router) y control de configuración de SNMP se desactivará.

SNMP Cuando está desactivada, un interfaz de línea de comandos es típicamente siempre. Los siguientes son los argumentos necesarios para configurar sFlow muestreo en una interfaz.

Transporte

Tráfico de información que se envía sin cifrar a través de la red del Agente sFlow al analizador sFlow y, por tanto, son vulnerables a la escucha. Este riesgo puede ser limitado mediante la creación de un seguro de medición de la red y encaminamiento de datagramas sFlow durante el tiempo que este en la red. La elección de la tecnología para crear el seguro medición es el despliegue de red específicas, pero podría incluir el uso de VLANs o túneles VPN.

El Analizador sFlow es vulnerable a ataques con falsos datagramas sFlow. Para limitar la vulnerabilidad de este analizador sFlow debe comprobar y verificar los números de secuencia de las direcciones fuente. Si un seguro de red de medición se ha construido sólo en datagramas sFlow recibidos de la red que debe ser procesada.

Confidencialidad

Información de tráfico que puede revelar información confidencial sobre los usuarios individuales de la red. El grado de visibilidad de la solicitud de datos a este nivel pueden ser controlados por la limitación del número de octetos de cabecera sFlow capturado por el agente. Además, el paquete de muestreo hace prácticamente imposible para capturar secuencias de paquetes de una transacción individual.

Los patrones de tráfico discernibles por la descodificación de los datagramas en sFlow el analizador puede revelar detalles de una persona de la red las actividades relacionadas con el debido cuidado y deben tomarse medidas para garantizar el acceso al sFlow Analyzer.

2.4.3 IPFIX

Introduccion

IPFIX provee una plantilla en formato binario, generica, extensible, para la transferencia de flujos y eventos de datos en una red. Este formato puede ser usado para almacenamiento persistente tal

como datos; sin embargo, las aplicaciones de almacenamiento persistente no son asunto de restricciones largas que se obligan en el protocolo IPFIX.

Que es IPFIX?

Internet Protocol Flow Information Export (IPFIX) pertenece al grupo de trabajo IETF. Este fue creado por la necesidad común, estándar universal de exportación de información de flujo por el protocolo de Internet para routers, sondeos, y otros dispositivos que son usados para sistemas de mediación, sistemas contables, y sistemas de administración de redes para facilitar servicios tal como mediciones, contabilidades. El estándar IPFIX podría ser definido como formato de información de flujo IP y transferencia a un colector de exportación. El estándar IPFIX fueron requerimientos originales del RFC 3917. El grupo de trabajo escogido por Netflow de Cisco versión 9 son base para IPFIX.

Arquitectura

Un proceso de **Medicion** (metering) colecta paquetes de datos en un punto de observación, opcionalmente estos son filtrados y agregan información acerca de los paquetes. Usando el protocolo IPFIX, un **Exportador** (exporter) envía esta información al **Colector** (collector). El exportador y colector tiene mucha relación: Un exportador puede enviar datos a muchos colectores y un colector puede recibir datos desde muchos exportadores.

Protocolo

Similar al protocolo Netflow, IPFIX considera un flujo como un numero de paquetes observado en un tiempo de ranura y un numero de porciones de propiedades, ejemplo, “mismo recurso, mismo destino, mismo protocolo”. Usando IPFIX, los dispositivos semejantes a los routers pueden tener un panorama total de redes grandes por medio de estaciones de monitoreo centrales de información.

IPFIX es un protocolo de empuje, cada envió seria periódicamente enviando mensajes IPFIX para configurar los recibidos sin ninguna interacción por lo que se recibe.

La actual constitución de datos en los mensajes IPFIX son de gran alcance para los envíos. IPFIX introduce en la composicion para que reciban estos mensajes con la ayuda especial de las plantillas. El envio es libre solo para usar tipos de datos definidos en estos mensajes, como el protocolo es extensamente libre y puede adaptarse a diferentes escenarios.

IPFIX prefiere el SCTP (protocolo de transmisión de control de corriente) como esta en la capa de transporte, pero solo permite el uso del TCP (protocolo de control de transmisión) o UDP.

2.5 Aplicaciones de Análisis de Flujos IP

2.5.1 Comerciales

TABLA II.05

APLICACIONES DE ANALISIS DE FLUJOS IP COMERCIALES

	Plataforma	**Tecnología que soporta**	**Descripción**
Scrutinizer NetFlow Analyzer	Windows 2000/XP/2003	sFlow v2, v4, v5 NetFlow v7, v9 IPFIX	• Proporciona información muy detallada de utilización de red de los usuarios y aplicaciones que están causando más tráfico. • Recuperar el tráfico que se necesita y presentarlos en una vista gráfica detallada.
Professional Look at Net	Windows 2000/XP/2003	Depende de la versión registrada	• Herramienta portátil de monitoreo de red. • La vigilancia no requiere los privilegios de un administrador. • Solo se requiere derecho de administrador anfitrión para la explotación y escaneo silencioso y tramas Ethernet o captura de paquetes IP, filtrado de paquetes IP en direcciones IP, puertos, salidas, entradas y más
Net-Probe 3.0.0	Windows		• Monitoreo de dispositivos, integrando

	2000/XP/2003		gráficas, alarmas, acciones, seguimientos GPS y acciones. • Basado en un asistente de configuración utilizando para escanear y establecer una red en unos pocos pasos
PacketTrap Network Discovery 2.2	Windows 2000/XP/2003	Apoyando al SNMP	• Desarrolla un escaneo rapidísimo de la red para descubrir todos sus dispositivos. • Los resultados se plasman en una interfaz de última generación. • Busca información específica para realizar un análisis granular
ManageEngine NetFlow Analyzer 7	Win2000/NT/XP /2003/Vista/Linux	NetFlow	• Monitorización de ancho de banda basado en tecnología Web. • Ofrece visibilidad completa sobre routers y switch cisco. • Informes detallados y gráficos en tiempo real. • Proporciona información muy completa sobre el tráfico de red, sin necesidad de utilizar sondas.

Fuente: http://globaldata.com.uy/whitepaper/PacketShaperSystem_SpaLA.pdf

Elaborado por: Las autoras

2.5.2 Software Libre para la representación numérica y grafica en el monitoreo de una red

TABLA II.06
APLICACIONES DE ANALISIS DE FLUJOS IP LIBRES

	Plataforma	**Tecnología**	**Descripción**
NetFlow Tracker	Linux, Unix	NetFlow/IPFIX	• Información completa del tráfico que permite realizar un importante análisis en profundidad de la información de aplicaciones y protocolos incluyendo actividad de usuario, conversación, sistema y aplicación • Soporta multicast • Genera bases de datos únicas que coleccionan, almacenan y permiten ofrecer valiosos informes del comportamiento de la red. • Seguridad, convergencia de voz y datos, servicios de

			soporte
MIRA	FreeBSD, GNU/Linux	NetFlow CoralReef	• Sistema de captura y monitorización avanzada de tráfico altamente configurable y flexible, adecuado para su utilización tanto en redes de área local como en redes de gran cobertura. • Análisis de contenidos: detección de contenidos de tipo lúdico y la detección de incidentes de seguridad. • Soporte del Ipv6
NAGIOS			• Sirve para monitorear servidores (SMNTP, POP3, HTTP, NNTP, ping), reporta problemas de la red de sus clientes, usuarios finales o encargados. • Supervisión de los recursos del host • Diseño simple • Capacidad de definir jerarquía de host de la red • Notificaciones • Escalada opcional de las notificaciones del dispositivo • Interfaz del web para el estado de la red de visión
NetSupport Manager 10.5	Windows 2008, Vista, XP, 2003, 2000, ME y 9x, Linux, Solaris, Mac, Pocket PC, CE, Windows Mobile		• Mejoras en la seguridad, comunicación o transferencia de datos. • Autenticación de Smartcards • Directorio Activo • Internet Gateway • Transferencia de archivos • Miniaturas ampliables • NetSupport School

Fuente: http://www.zonagratuita.com/a-internet/varios_internet.htm

Elaborado por: Las autoras

CAPITULO III

COMPARACIÓN DE TECNOLOGÍAS DE ANÁLISIS DE FLUJOS IP, NETFLOW, SFLOW, IPFIX Y EQUIPOS A UTILIZARSE

3.1 Determinación de los parámetros y criterios de comparación

Debido a la gran importancia que hoy tienen las redes de datos LAN/WAN en la productividad y eficiencia de las empresas e instituciones educativas, es indispensable contar con la Plataforma de Conectividad y Comunicaciones que nos asegure un acceso rápido y mejore el desempeño de las aplicaciones y nos brinde seguridad.

El crecimiento constante y la incorporación de nuevas tecnologías, gradualmente se van complicando y muchas veces degradando la performance de la red. Por esta razón hay que realizar un “Análisis Comparativo”, orientado a prevenir, plantear soluciones concretas ante nuevos problemas o requerimientos y, a elegir la tecnologia que mas convenga de este modo asegurar la estabilidad, operabilidad y flexibilidad en el tiempo del Sistema en General.
Para brindar el mejor servicio en el control y mantención de la Red y ser un apoyo real en la incorporación de las soluciones tecnológicas, se propone un analisis de los parametros y criterios de comparacion mas relevantes y de vital importancia dentro de cada tecnologia con el objetivo de seleccionar la mejor para una implementacion adecuada.

Los parámetros a comparar en las tecnologías NetFlow, Sflow e IPFIX son [14, 15 y 17]:

- Tipo de Información
- Cantidad de datos
- Colección de Información
- Estado de Estandarización
- Enfoque de recolección
- En que se basa cada una de las tecnologías
- Usos
- Proveedores de equipos que incluyen las tecnologías
- Exanimación de paquetes o flujos
- Propiedades
- Recursos del agente

  CPU, Memoria

Acontinuacion se detalla en las tecnolgias Netflow, sFlow e IPFIX cada uno de los parametros.

NETFLOW

Netflow es la principal tecnología de monitoreo de tráfico en la red.

Todos los principales proveedores de equipos tienen la capacidad de proporcionar Netflow.

Con Netflow los conmutadores, routers y otros componentes recopilan y mantienen información sobre el tráfico que atraviesa la red. Es decir información lógica de extremo a extremo entre los flujos de origen y destino de los servidores, así como lo físico es de punto a punto entre las corrientes principales de los elementos de la red.

- NetFlow controla la inactividad en el tráfico que no excede los 15 segundos (es configurable)
- NetFlow controla la expiración de los flujos que se mantienen activos por más de 30 minutos, mediante esto se asegura un reporte periódico (es configurable)
- En NetFlow periódicamente las estadísticas de tráfico de todos los flujos que caducan son exportados desde el dispositivo que mantiene la caché (router o switches) por UDP (también mediante SCTP).

En tiempo real en netflow las fuentes de datos están siempre disponibles y transmiten una gran cantidad de información vital sobre el tráfico de la red.

Cisco NetFlow, es un sistema de monitoreo el cual envía información del flujo del tráfico a un colector central. Descifra cada paquete IP, mantiene tablas de flujos activos, y envían información periódicamente a una aplicación de administración de red.

Cuando se introdujo por primera vez Netflow de Cisco se trataba de una técnica de almacenamiento en cache basado en “corrientes”. Este enfoque hoy en día se sigue dando pero ya Netflow se basa más en recolectar estadísticas.

Netflow caché todavía está presente y puede ayudar mucho cuando se tiene acceso a listas.

El seguimiento de las estadísticas cruciales en Netflow se cuenta con paquetes y bytes. Al habilitar Netflow en un router o switch, se recogen estadísticas sobre el tráfico IP que genera ese dispositivo.

El flujo de datos que expira puede ser exportado a un sistema de recogida de post-procesamiento y almacenamiento. El Software de presentación de informes le da acceso a la información. El Flujo de vencimiento se basa en la evidente extinción de la corriente (TCP RST o FIN) y temporizadores, incluyendo un temporizador para garantizar que los datos se exportan a veces, o para impedir la pérdida de información.

Uso de datos Netflow

El alcance de los datos en Netflow es considerable. Netflow ofrece información sobre los puertos de origen y de destino, direcciones, las redes de tráfico y protocolos de las clases, el tráfico y la cuenta de paquetes, las interfaces de entrada y salida, el tipo de servicios y aplicaciones, entre otras.

Cómo se obtengan los datos esto determinará su utilidad e influencia en el rendimiento de la red global de gestión.

Netflow para controlar gran volumen de información disponible no únicamente extrae los datos sino dispone de un colector Netflow que puede reunir y agrupar los datos de toda la empresa.

El exportador de datos de Netflow le permite recolectar datos de toda la red sobre el tráfico que pasa por esa red.

Los informes que se pueda sacar dependen de la herramienta que se elija.

Netflow contiene información sobre las interfaces. Información como:

- Cantidad de tráfico que pasa a través de cada interfaz
- Informar sobre los transmisores y receptores.

Netflow puede proporcionar en tiempo real casi (hay un pequeño retraso con la exportación) la misma información como al trabajar con los usos distribuidos de un sniffer

Otro uso es la recuperación de los costos debido a la identificación de desperdicio de ancho de banda. Es decir puede identificar a las aplicaciones que son los principales consumidores de ancho de banda le ayuda a centrarse en dónde concentrar los esfuerzos para aumentar la eficiencia. Varios vendedores de Netflow, así como Cisco Netflow dicen que Netflow puede proporcionar una buena información sobre los brotes de virus o gusanos y otras actividades inusuales.

Al estar recibiendo datos en todos los IP de origen y de destino, así como los puertos, se puede ver lo siguiente:

- Tráfico dirigido al puerto 445
- Un informe sobre las fuentes ordenada de los flujos de tráfico del puerto 445 como:

Identifica rápidamente los equipos infectados. Si el ordenador infectado es decir serverlet es un FTP para descargar el malware, también se puede buscar en los clientes, es decir, el envío de tráfico FTP acoge a ese equipo.

Usos NetFlow

Contabilidad y Cobro (Accounting /Billing).- al proveer métricas finas por ejemplo direcciones IP, cantidad de paquetes y bytes, timestamps, tipo de servicios y puertos de aplicación, permite gran flexibilidad y detallado del seguimiento del uso de recursos.

Planificación y Análisis de Red.- provee información clave que puede ser utilizada por herramientas para planificación y toma de decisiones estratégica, minimizando el costo total de las operaciones de la red y maximizando la performance, capacidad y confiabilidad.

Monitoreo de Red.- al dar información casi en tiempo real NetFlow permite realizar monitoreo de red.

Las técnicas de análisis basado en flujos pueden utilizarse para visualizar los patrones de tráfico asociados a routers o switches individuales, siendo útil para detectar fallas y actuar de forma más rápida para solucionarlas.

Monitoreo y Profiling de aplicaciones.- Provee a los administradores de red una vista detallada y basada en tiempos del uso de las aplicaciones en la red.

Monitoreo y Profiling de Usuario.- Provee a los administradores de red información de la utilización de los recursos de red y de aplicaciones de los usuarios o clientes. Esta información puede servir

para planificar el uso de recursos de aplicación, como también detectar y resolver potenciales violaciones de seguridad.

NetFlow Data Warehousing and Mining. - Los datos exportados o la información derivada de NetFlow puede ser analizada para soportar de forma proactiva programas para servicios de marketing o clientes. Esto es especialmente útil para los Internet Service Providers (ISPs), ya que NetFlow permite a éstos indagar en sus paquetes de servicio.

Consideraciones clave

Netflow, tiene una verdadera comprensión en el rendimiento de la red y está bien posicionada para el usuario final al optimizar la calidad del uso.

Netflow proporciona:

Compatibilidad Universal - Soporte de TI, trabajando con todos los beneficios de Netflow por lo que la información puede ser obtenida de todos los elementos heterogéneos en un entorno de red para el análisis.

Mostrar jerárquica - Mejorar la eficiencia de TI mediante la presentación de datos en Netflow a través de resúmenes de alto nivel y facilitar los flujos de tráfico según sea necesario.

Granular la gestión de datos - que pueda decidir cuánto tiempo puede conservar Netflow los datos y con qué frecuencia debe recoger de los dispositivos de red. Tiempos de retención ampliada de apoyo a la identificación y resolución de problemas intermitentes. Colección de datos en intervalos de un minuto, en tiempo real ayudan a encontrar anomalías transitorias.

Profundidad ilimitada - le permiten mirar más allá de las "Top N", las conversaciones, los protocolos, o cualquier otra métrica. Al examinar la parte superior de una lista clasificada puede ayudar en la identificación de problemas obvios. Este enfoque no siempre refleja lo que está sucediendo realmente en la red, donde se producen mayormente anomalías causadas por virus, gusanos y piratas informáticos.

No hay inversión de capital: Casi todas las redes ya contienen dispositivos con capacidad Netflow. Al encender los datos de Netflow, estos dispositivos pueden inmediatamente comenzar a exportar estadísticas de la red.

Rendimiento de netflow

TABLA III.07

APROXIMADO DE UTILIZACIÓN DE CPU POR NÚMEROS DE FLUJOS ACTIVOS

Número de flujos activos en la cache	Utilización de CPU adicional
10000	<4%
45000	<12%
65000	<16%

Fuente: http://www.netflow.es/index2.html

Elaborado por: Eduardo Prieto

La reducción significativa de la utilización de CPU con Netflow se logra mediante

- Sampled NetFlow
- Optimización de los tiempos
- Una arquitectura distribuida

Tener una exportación doble no tiene un impacto relevante en la utilización del CPU

Memoria

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 y uso de memoria.

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.

El tipo de información que NetFlow puede proporcionar incluye:

Análisis de red / planificación de la capacidad: Los datos de NetFlow permiten tomar mejores decisiones técnicas sobre la red al revelar si el tráfico ha superado un umbral definido (utilización, velocidad o volumen) en un enlace de red. Mediante los datos NetFlow, un ingeniero puede determinar si el aumento de la capacidad resolverá un problema en un enlace o si se pueden reducir enlaces para ahorrar dinero.

Supervisión de redes, servidores, aplicaciones / Solución de problemas: NetFlow permite la supervisión exhaustiva, en tiempo real, de las redes para ayudar a detectar problemas y solucionar problemas de manera efectiva y rápida.

Detección de virus: NetFlow mide el tráfico en los enrutadores y los conmutadores e incluye información detallada sobre los puertos de origen, destino y servicio de los paquetes. Esta información puede utilizarse para identificar los patrones de tráfico de red anómalos y la actividad de barrido de puertos: indicaciones frecuentes de gusanos.

SFLOW

sFlow combina contadores exactos de paquetes con muestreo estadístico del estado de las tablas de ruteo, para que el switch envíe paquetes de forma randómica. La muestra seleccionada es enviada inmediatamente a un colector central para ser analizado.

Arquitectura de sFlow

Los elementos básicos de un sistema sFlow son el Agente y el Colector.

El Agente sFlow es un proceso de software que corre como parte del software de administración de red dentro de un switch o router. Combina contador de interfaces y muestras de flujos en datagramas sFlow que son enviados a través de la red hacia el Colector sFlow.

El muestreo de paquetes es típicamente realizado por switcheo/ ruteo ASICs.

El Agente sFlow realiza muy poco procesamiento, simplemente empaqueta datos en los Datagramas sFlow que son enviados inmediatamente a la red. Este envío inmediato minimiza los requerimientos de memoria y CPU del Agente.

El colector se encarga de recolectar y analizar los datos, pudiendo generar información detallada del tráfico en tiempo real.

Recursos del Agente

Cuando se comparan tecnologías embebidas en aplicaciones de monitoreo, se deben considerar tres recursos principales que la aplicación consumirá: CPU, memoria y ancho de banda.

Estos recursos son caros, por lo tanto, la solución debe minimizar el uso, y así hacer una solución menos costosa.

CPU

Los requerimientos computacionales en el monitoreo del tráfico impactan significativamente en los costos del agente y escalabilidad. Las técnicas de monitoreo requieren más alta performance en el manejo de CPU para switches y routers. Además un solo procesador quizás no soporte la demanda de monitorear un gran número de puertos contenidos en muchos switches y por ende más CPU es requerida para monitorear.

En contraste, la función de muestreo del agente sFlow puede ser fácilmente implementada en hardware. Además como el agente de lo único que se encarga es de enviar el cabezal del paquete al servidor, esa tarea no implica una sobrecarga del CPU.

Memoria

La memoria requerida para construir las medidas de tráfico afecta al costo del agente.

El agente NetFlow construye matrices en la RAM del agente. El tamaño de las tablas depende mucho de los patrones de tráfico.

NetFlow tiene la ventaja de que puede ser configurado automáticamente para descargar flujos individuales cada quince minutos o más, y también para descargar bloques de flujos para prevenir quedarse sin memoria suficiente.

El agente sFlow solo necesita RAM para guardar un paquete. Cuando una muestra es tomada es enviada inmediatamente al servidor.

Ancho de banda

La transferencia de datos desde los agentes de monitoreo al colector central consume considerable ancho de banda. Este ancho de banda es quitado a las aplicaciones de la red.

Hay que considerar también que picos altos de transferencia pueden causar congestionamiento en la red.

La carga de red de un agente NetFlow se muestra como streams de largos paquetes UDP. Una vez que la tabla de flujos se llena, un gran número de flujos pueden ser descargados para liberar espacio.

Todos los agentes sFlow realizan un envío sostenido de paquetes hacia el servidor. Cada agente puede controlar el nivel de tráfico ajustando la frecuencia de muestreo.

Recursos del Servidor

El agente de monitoreo es solo una parte de la solución de administración. Un servidor central se precisa para configurar los agentes, bajar y archivar los datos, mostrar los datos en una interface de usuario.

Un factor clave al determinar el costo y escalabilidad de un sistema de monitoreo es determinar los recursos del servidor para gestionar un solo agente.

El consumo de recursos en el servidor determina la cantidad de agentes que un solo servidor puede administrar.

El servidor NetFlow tiene el problema del gran tamaño de las matrices de tráfico de los agentes. Aparte del esfuerzo de recibir la información desde la red, también tienen que consolidar los datos en matrices de tráfico por sitio sin mezclar la información de los distintos agentes.

En sFlow el tamaño de las matrices construidas por el muestreo de paquetes es mucho menor, consiste típicamente de los flujos más ocupados, más una selección de los flujos más pequeños. Por lo tanto la tarea de consolidar las matrices de tráfico es mucho más liviana.

Propiedades Sflow

Sflow provee una amplia vista del uso de la red y de los routers. Permite medir el tráfico de red, recolectar, guardar y analizar los datos del tráfico.

Preciso.- El muestreo es simple como para ser realizado en hardware. Además, el sistema sFlow está diseñado de manera que puede ser determinada con exactitud distintos tipos de medidas.

Detallado.- El contar con información completa de la cabecera de los paquetes y del switching y routing permite un detallado análisis del flujo de tráfico de las capas L2-L7.

Escalable.- En tamaño y velocidad.

Es capaz de monitorear redes a 10Gbps, 100Gbps y más, sin sobrecargar la red. Cientos de dispositivos pueden ser monitoreados por un único Colector sFlow.

Bajo Costo.- El Agente sFlow es simple de implementar y agrega bajo costo a un switch o router. Ha sido implementado en un amplio rango de dispositivos, sin requerir memoria y CPU extra.

Oportuno.- El Colector sFlow tiene una vista del tráfico de la red de los últimos minutos. Esta propiedad es particularmente importante si fuera necesario proveer controles en tiempo real.

Usos SFlow

sFlow da una amplia visibilidad del uso de la red al monitorear los flujos de tráfico en todos los puertos.

Algunos de sus usos son:

Soluciona problemas de tráfico (Troubleshooting Network Problems)

Cualquier uso de la red genera tráfico. Consecuentemente, los problemas son observados en patrones anormales de tráfico. sFlow hace visibles estos patrones anormales, con el detalle como para rápidamente identificar, diagnosticar, y corregir._

Control de congestionamiento (Controlling Congestion)

Al monitorear el flujo de tráfico en todos los puertos, se pueden ver los links de congestionamiento, identificar el origen del tráfico, y las conversaciones entre aplicaciones.

Seguridad y Audit Trail Analysis

Permite de forma rápida, controlar y hacer un seguimiento de ataques y amenazas internas y externas. Para llevar la historia detallada del tráfico se crea una baseline del comportamiento normal, a partir del cual anomalías o actividades sospechosas se pueden identificar. De esta forma se puede prevenir ataques intencionales, minimizar errores no intencionales, y proteger la información.

Perfil de ruteo

Como sFlow contiene información anticipada, puede usarla para perfilar las rutas más activas y los flujos que corren por esas rutas. Al comprender las rutas y flujos permite optimizar las rutas mejorando la conectividad y performance.

Contabilidad y cobro del uso (Accounting and Billing for Usage)

Provee información detallada del uso de los servicios de red, y así poder contabilizar y facturar el uso por cliente. También puede ser usado para proveer a los clientes una lista de su tráfico total, indicar los usuarios y aplicaciones más frecuentes.

IPFIX

Netflow recoge los datos de tráfico, IPFIX normaliza Netflow

IPFIX es compatible con la aplicación, y se incluye como parte del Cisco IOS.

IPFIX **(**IP Flow Information Export), define los requerimientos para exportar flujos de información IP de salida de los router y pruebas de medición de tráfico. Está documentado en el RFC 3917.

Mediante el empleo de técnicas pasivas de análisis como IPFIX se puede disponer de una arquitectura no intrusiva e interoperable para calcular métricas de calidad de servicio. El hecho de ser un método pasivo permite disponer de numerosos puntos de medida sin que el tráfico de datos

se vea afectado, mientras que el hecho de ser interoperable contribuye a que diversos operadores puedan colaborar entre sí para recabar información relacionada con sus enlaces y el tráfico intercambiado entre ellas.

Otra propiedad inherente a las técnicas de análisis basadas en flujos (IPFIX) es la de caracterizar el tipo de tráfico cursado por los usuarios finales, lo cual facilita el desarrollo de metodologías de estimación de QoS orientadas a la percepción del usuario de los servicios de red.

El IETF ha estado trabajando para normalizar Netflow. Esta normalización se llama IPFIX, que corresponde a la propiedad intelectual de flujo de información de exportación. El IETF considera implementaciones de trabajo como punto de partida, y elegido para el trabajo de Cisco Netflow versión 9. Versión 9 de Netflow se extiende por el uso de plantillas para describir el flujo de expedientes. Esto proporciona extensibilidad, también permite asegurar el flujo de información - SCTP es un flujo seguro de transporte se puede utilizar en lugar de TCP o UDP para el transporte. IPsec o TLS también se puede utilizar.

La norma también permite la muestra de datos de IPFIX, lo que facilita la carga de los dispositivos de clasificación y presentación de informes sobre todos y cada uno de los paquete. Cisco recomienda un muestreo aleatorio (muestreo probabilístico) para garantizar que no se pierdan las corrientes, por ejemplo cuando hay perdidas periódicas los patrones de datos.
La mayoría de los principales proveedores como Cisco tienen la intención de apoyar IPFIX para que pueda seguir adelante.

IPFIX es un estándar que permite a los vendedores proporcionar las exportaciones en el mismo formato de un flujo de datos constante. Con esta tecnología, los routers se utilizan para recopilar datos IPFIX y, por tanto, las empresas tienen las siguientes ventajas:

- No hay inversión de capital: Casi todas las redes ya contienen dispositivos con capacidad IPFIX. Al encender los datos de IPFIX, estos dispositivos pueden inmediatamente comenzar a exportar estadísticas de la red.

- Bajos costes de despliegue: Configurar IPFIX implica unos comandos y una interfaz de comandos para cada interfaz de funcionamiento IPFIX.
- Recursos de Datos completos: IPFIX medidas e informes automáticamente de todos los tráfico IP.
- Se asocia con el mantenimiento de hardware y software en un router Cisco.

Cuando se busca implementar IPFIX, considere lo siguiente:

- IPFIX generalmente aumenta la utilización del CPU en la configuración de dispositivos, en promedio, de un 1% al 2%.
- Sólo el tráfico IP es compatible.

IPFIX es un protocolo de NetFlow v9 más fiable, y define mayor colección de información que NetFlow.

IPFIX utiliza plantillas, lo que hace que el protocolo de transporte sea fiable

Usos de IPFIX

Cada flujo de datos en IPFIX es único y es identificado por siete criterios:

- Fuente dirección IP,
- La dirección IP de destino,
- Número de puerto de origen (TCP / UDP),
- Número de puerto de destino (TCP / UDP),
- Nivel 3: Tipo de protocolo (IP / ICMP),
- Tipo de servicio (TOS),
- Entrada de la interfaz lógica.

Los datos de IPFIX pueden ser analizados para informar lo siguiente:

- Todos los hosts que transmiten la mayoría de los datos en la red

- Todos los hosts que transmiten la mayoría de los datos entre sí
- Todas las solicitudes que ponen más tráfico en la red
- El volumen de datos por entidad (circuito, ubicación remota, región, etc.)
- Datos por tipos de entidad (circuito, ubicación remota, región, etc.)
- ToS, Criterios de presentación de informes sobre NetFlow / IPFIX, los datos requieren un sólida motor de análisis.

Al seleccionar la presentación de solución de su IPFIX tenga en cuenta los siguientes criterios:

Escalabilidad:La gestión y solución de IPFIX debe ser capaz de escalar en pequeñas implementaciones,

En una solución jerárquica, los datos de IPFIX se originan en el router. El envío de datos IPFIX es a un dispositivo de recogida de información agregados al router. Cada dispositivo de recogida reduce los datos de IPFIX remite a la gestión y presentación de informes por consola. Esto tiene un doble efecto de reducir al mínimo los datos que fluyen a través de la red y maximizar el área de red que puede ser cubierta con una solución IPFIX. Cada dispositivo debe tener cuidado de no descartar demasiada información, lo que haría que la solución sea inútil o ineficaz al ganar visibilidad en la red. Idealmente, una solución completa de informes recopila miles de protocolos únicos, los ejércitos, y las conversaciones por enlace de red, además de 100% de datos para aplicaciones de misión crítica.

¿Porque IPFIX aun no esta ampliamente desarrollado?

1. Hace falta:
   - Longitud variable, un problema con las cadenas
   - Seguridad
   - Mensajes de plantillas retiradas
2. El valor esta en el proceso de medición
3. Se aplica el flujo de exportación de IPFIX por SCTP

Limitaciones de IPFIX

1. Campo no observado

- No hay valores a ser observados

Ejemplo: tipo ICMP, numero de puerto, TCP, en Windows tamaño de trafico UDp

¿Qué primero se escoge?

Valor específico por elemento de información

- Si en una información específica. El elemento es requerido por una plantilla, pero no está disponible en paquetes observados, el proceso de exportación podrá optar por los registros de flujo de exportación sin que esos elementos de información de los registros de datos estén definidos en la nueva plantilla RFC5101

2. Datos no estructurados

- "Etiqueta MPLS y posición de la etiqueta MPLS"

El contenido de un valor depende del contenido de otro: esto se rompe en el diseño.

- Lista de exportación

Interfaz de salida por multicast

Si un elemento de información se requiere más de una vez en una plantilla, las diferentes ocurrencias de este elemento de información debe seguir el orden lógico de su proceso de medición.

¿Lo que si podemos empezar desde cero en IPFIX?

- Cabecera flexible

Contiene elementos de información

- Más información sobre algunos atributos de los elementos

En la plantilla de definición: antes o después, clave de campo o no.

En el flujo de registro: observado o no

- Plantillas XML como respuesta a la estructura de datos

Características

- Extrae más estadísticas de tráfico de los elementos de red corporativos.
- Facilita prestaciones como es la facturación por uso o una mayor sencillez en la aplicación de parches a brechas de seguridad.
- Tiene un método para que tanto conmutadores como routers exporten datos sobre flujo de tráfico a los sistemas de gestión. Se incluye en las plataformas de fabricantes de networking como Cisco Systems, Nortel Networks y Riberstone Networks, entre otros.

Todos los productos que soportaran IPFIX estan capacitados para recolectar y analizar los datos sobre flujo de tráfico y correlacionarlos con otras métricas de rendimiento de la red y las aplicaciones a través de una consola de gestión.

Empaqueta de manera automática la información y envia a un punto de recolección para la posterior correlación del conjunto de los datos. De esta forma se evita, por ejemplo, el problema, frecuente en la actualidad, de que la información sobre flujos se pierda en los sistemas de red debido a que los routers y conmutadores carecen de memoria suficiente para mantenerla. Con esto, una vez los datos hayan sido exportados, el software de gestión puede diseccionar minuciosamente toda la información, hoy difícil tanto de reunir como de mantener. IPFIX nace con el propósito de proporcionar el formato en el cual los datos de flujos IP puedan ser transferidos desde el componente de red hasta el punto de recolección para la gestión. Dado que las implementaciones IPFIX incluirán templates, los clientes podrán definir múltiples templates para cuantas variedades de tráficos hayan de ser exportadas. Los sistemas con soporte de IPFIX habrán de empaquetar los datos siguiendo estos criterios y enviarlos a los dispositivos de recolección.

3.2 Estudio de los diferentes equipos que soporta cada una de las tecnologías

DISPOSITIVOS QUE SOPORTAN NETFLOW

Entre los Dispositivos que soportan Netflow podemos encontrar de CISCO [3]:

- Routers
- Switches Catalyst

Existen otros vendedores de equipamientos que también lo soportan

Alcatel, Enterasys, Foundry

ROUTERS

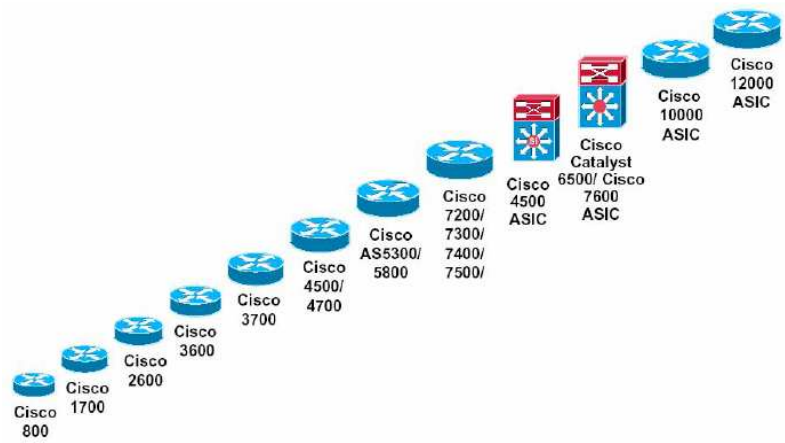


Figura N°III.03 Routers que soportan NetFlow

Las siguientes tablas detallan los diferentes equipos que soporta cada una de las tecnologías de monitoreo.

TABLA III.08

ROUTERS QUE SOPORTAN NETFLOW

Equipo	Interfaz	Descripcion
Cisco 801	1Ethernet y 2 BRI S/T	
Cisco 803	4 Puertos Ethernet (hub), 2 puertos análogicos y 1 BRI S/T	
Cisco 805	1 Ethernet y serie WAN para Frame Relay	Punto a punto (hasta 512 Kbps) o acceso asincróno
Cisco 802 IDSL	1 Ethernet y 1 IDSL (WAN)	
Cisco 827-4V	1 Ethernet, a ADSL (WAN)	

	y 4 puertos para telefono analogico de VoIP	
Cisco 837	4 Interfaces de red Ethernet 10/100 y 1 ADSL sobre RTB (WAN)	
Cisco 851	**Interfaz WAN** 10/100 Mbps Fast Ethernet **Interfaz LAN** 4-port 10/100 Mbps switch	
Cisco 857	**Interfaz WAN** ADSL **Interfaz LAN** 4-port 10/100 Mbps switch	
Cisco 1721	1 Ethernet 10/100 y 2 slots de expansion WIC	Puerto auxiliar y de consola
Cisco 1712	1 Ethernet 10/100 (WAN), 4 puertos (switch) Ethernet 10/100, 1 puerto BRI para backup	IOS con EW, ISD y VPN (3DES)
Router modular multiservicio clase empresarial	2 ranuras para tarjeta de interfaz WAN (WIC), 1 ranura ,odulo de red, 1 ranura para modulo AIM	• Integración multiservicio de voz y datos. • Acceso de redes privadas virtuales • Enrutamiento entre VLAN
Cisco 2650 y 2651	2 puertos Ethernet 10/100 Mbps con autodetección 2 ranuras para tarjeta WIC, 1 ranura para modulo AIM	Hasta 37000 paquetes por segundo
Cisco C2600-IS-M	1 WIC para ADSL	Cable serial V35 original para WIC de serial
Cisco 4700-M	Ranuras para NPMs, E1/T1 de serie	Con 133-Mhz CPU RISC, entrega 30 – 50 % mas que el rendimiento del Cisco 4500-M
Cisco 4500-M		Tiene la reserva para sobresalir en tareas como compresion de datos, cifrado de datos, de túneles, la politica y la seguridad

Fuente: http://www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH010e.dir/doc.pdf

Elaborado por: Las autoras

TABLA III.09

SWITCH QUE SOPORTAN NETFLOW

Equipo	Descripción
Cisco Catalyst 6500	Eficiencia MSFC es para el encaminamiento , PFC con supervisor de conmutación
Cisco Catalyst 7600	Eficiencia MSFC es para el encaminamiento , PFC con supervisor de conmutación
Cisco Catalyst 2950	24 puertos-Auto-Autonegociables-EN, Fast EN – 10Base-T, 100Base-TX
Cisco Catalyst 500Series Switches con RSM	Incluye series de switches Catalyst 5002, Catalyst 5505y Catalysy 5500
Cisco Catalyst 500Series Switches con MSFC	Tipos de switches proporcionados por Cisco
Cisco Catalyst 6500	Analisisn integral del trafico para aplicaciones, servicios y redes basadas en IP. Adminsitraor multidispositivo de DdoS Nuevo motor de control de aplicaciones Modulo de servicios inalambricos Escalabilidad Multicast encriptado sobre GRE Seguridad de voz
Catalyst 6500Virtual Switching System 1440	Con tarjeta de la serie 67xx, la funcionalidad se llama Virtual Switching System y permite utilizar una pareja de Catalyst 6500-E como si solo fuera uno.
Cisco ME 6524 Ethernet switch	Ipv4 Seguridad Multicast Calidad de Servicio MPLS
Cisco Nexus 7000	Switch multicapa orientados a los centros de procesos de datos El sistema operativo es Cisco NX-OS Soporta IPv4 e Ipv6. Multiples protocolos de ruteo (OSPF v2 y v3, IS-IS, BGP e EIGRP) Introduce puntos de control de configuracion, administracion por roles RBAC

	Interfaz programable API XML basada en el estandar industrial NETCONF
Cisco MGX 8800 switches multiservicio	Permite la distribucion de una completa cartera de ofertas de servicios diferenciados. Arquitectura extensible Mayor flexibilidad en el proveedor de servicios de borde MPLS Voz y servicios
Cisco Catalyst 8500	Integran la conmutacion ATM multiservicio con el enrutamiento multiprocolo a velocidad de cable y la conmutacion de Nivel 3 de Gigabit Ethernet en una sola plataforma Ofrece soluciones para redes metropolitanas y de campus con rendimiento ampliable

Fuente: http://www.bibliociencias.cu/gsdl/collect/eventos/index/assoc/HASH010e.dir/doc.pdf

Elaborado por: Andi Estrella y Ana Belén Castro

TABLA III.10

EQUIPOS QUE SOPORTAN sFlow

Modelo	Descripcion
HP ProcureCurve Switch 2524 (J4813A)	24 auto-sensing puertos 10/100 (IEEE 802.3 , tipo 10Base-T, IEEE 802.3u tipo 100Base-TX) Puerta de consola 1 RS-232C DB-9
HP ProcureCurve Switch 2524 (J4812A)	12 auto-sensing puertos 10/100 (IEEE 802.3 tipo 10Base-T, IEEE 802.3u tipo 100Base-TX) Tipo de medio: Auto-MDIX Duplex: half o full
J9085A ProCurve Switch 2610-24	Puertos de E/S externos Montaje en bastidor 16 MB de memoria flash, 128 MB de SDRAM Tamaño de la tabla de direcciones: 8000 entradas Capacidad de encaminamiento :12,8 Gbps
J9088A ProCurve Switch 2610-48	48 puertos 10/100 de deteccion automatica Se monta en un rack telco o armario de equipo de estandar EIA de 19 pulgadas MIPS a 300 Mhz, 16 MB de memoria flash, 128 MB de SDRAM 8000 entradas

J9021A ProCurve Switch 2810-24G	24 puertos 64 MB SDRAM 16 MB Velocidad de transferencia de datos 1Gbps Conmutacion en capa 2, soporte de BOOTP
J8715A ProCurve Switch 8212zl	12 ranuras para modulos Admite un maximo de 288 puertos 10/100/1000 de deteccion automatica 144 Mb de QDR SDRAM 128 MB de memoria flash compacta 10000 entradas
Hp L8770A ProCurve switch 4204VL	64 MB SDRAM 24 MB de memoria flash Protocolo de gestion remota:SNMP 1, SNMP 3, SNMP 2C, RMON 1, RMON 2, RMON 3, RMON 9.
J9022A ProCurve Switch 2810-48G	64 MB de SDRAM 16 MB de memoria flash Puertos: 48 x Ethernet 10Base-T, Ethernet 100Base-T
HP J9049A	24 puertos 10/100/1000T
HP J4905A ProCurve Switch 3400CL-24 G	24 puertos 10/100/1000T Administración en capa 2 y 3 1 modulo abierto para slot
HP J8692A-ProCurve Switch 3500YL-24G	24 puertos 10/100/1000T Administracion en capa 2 y 3 Ipv6
HP J8698A ProCurve Switch	Con chasis 5412zl 12x abierto para slot 10/100/1000 Administracion en capa 2 y 3
HP J9050A ProCurve Switch	48 puertos 10/100/1000T Administracion en capa 2 y 3
HP J8693A ProCurve Switch 3500YL-48G-PWR	48 puertos 10/100/1000T Administracion en capa 2 y 3 Standar PoE Ipv6

Fuente: http://www.techbuy.com

Elaborado por: Las autoras

Otras marcas que utilizan sFlow.

AlaxalA Networks :AX7800R, AX7800S, AX7700R, AX5400S

Alcatel : OmniSwitch 6850, OmniSwitch 9000

Allied Telesis : SwitchBlade 7800R Series, SwitchBlade 7800S Series, SwitchBlade 5400S Series

Comtec Systems : Rex 16Gi & 24Gi & 24Gi-Combo

Extreme Networks : Alpine 3800 series, BlackDiamond 6800 series, BlackDiamond 8800 series, BlackDiamond 10808, BlackDiamond 12804C, BlackDiamond 12804R, Summit X450 Series.

Force10 Networks :E Series

Foundry Networks : BigIron series, FastIron series, IronPoint series, NetIron series, SecureIron series.

Hitachi: GR4000, GS4000, GS3000

NEC: IP8800/R400 series, IP8800/S400 series, IP8800/S300 series

TABLA III.11

EQUIPOS QUE SOPORTAN IPFIX (Marca: Nortel Networks)

Modelo	Descripcion
Ethernet Routing Switch 5520	Ruteo: OSPF, RIP, VRRP SMLT, la igualdad de los costos de multiple camino (ECMP) Deteccion automatica Multi-Link DHCP Manejo de politicas QoS y Seguridad Mejorada Politicas de trafiico , RPS, Port Mirroring
Ethernet Routing Switch 5600	Conmutacion en la capa 3 Soporta BOOTP Concentracion de enlaces, equilibrio de carga Filtrado de direcciones MAC
Ethernet Routing Switch 5510	Flexibilidad maxima Traficos simultaneos bidireccionales en cada puerto

	Permite hasta 48 servidores para conectarse.
Ethernet Routing Switch 5530	Utiliza conexiones de fibra y cobre Conectividad avanzada 24 puertos 10/100/1000Base-T 12 slots SPF compartidos
Ethernet routing Switch 8600	Multiservicio SMLT RSMLT Ipv6

Fuente: http://www.techbuy.com

Elaborado por: Las autoras

3.3 Tablas comparativas de las Tecnologías Netflow, Sflow, IPFIX.

TABLA III.12

PARAMETROS PRINCIPALES DE LAS TECNOLOGIAS

Tecnología / **Parámetros**	**NetFlow**	**sFlow**	**IPFIX**
Tipo de Información	Flujos	Parcialmente paquetes seleccionados por muestreo	Flujos
Cantidad de datos	Desde pequeñas hasta grandes cantidades (depende de la tasa de muestreo y de las condiciones de creación de flujos)	Grandes cantidades (depende de la tasa de muestreo)	Desde pequeñas hasta grandes cantidades
Colección de Información	Datos de la capa de enlace de datos y de la capa de transporte	Datos de la capa de enlace de datos	Datos de la capa de enlace de datos y de la capa de transporte y otros datos que se recoge por medio de extensiones del vendedor
Estado de	RFC3954 (Información	RFC3411 (Información	Etapa inmediata de

Estandarización	dada por cisco)	dada por InMon)	publicación del FRC (estándar)
Enfoque de recolección	Almacenamiento en cache basado en "traps", y recolección de estadísticas	Basada en la muestra	Basado en un muestreo aleatorio (muestreo probabilístico)
En que se basa cada una de las tecnologías	Basada en software	Utiliza un chip dedicado que esta incorporado en el hardware	Basada en software

Fuente: http://www.ietf.org/html.charters/ipfix-charter.html

Elaborado por: Las autoras

TABLA III.13

USOS Y PROVEEDORES DE LAS TECNOLOGÍAS

Parámetro / Tecnología	**Usos**	**Proveedores de equipos que incluyen las tecnologías**
NetFlow	• Ofrece información sobre: Puertos de origen Puertos de destino Direcciones Redes de tráfico Protocolos de las clases Interfaces de entrada y salida Tipo de servicios • Identificación de desperdicio de ancho de banda • Proporciona una buena información sobre los brotes de virus o gusanos y otras actividades inusuales. • Tráfico dirigido al puerto 445 • Identifica rápidamente los equipos infectados • Dispositivos de Intercambio • Planificación de la red • Ingeniería de trafico • Contabilidad y facturación • Seguridad en el monitoreo	Cisco Alcatel o HP Enterasys Foundry 3Com Nortel Juniper Procurve

sFlow	Soluciona problemas de tráfico Control de congestionamiento • Seguridad y Audit Trail Analysis Perfil de ruteo • Contabilidad y cobro del uso (Accounting and Billing for Usage) • Proporciona una vista de toda la red • Es un estándar de la industria • Pronosticar de manera precisa las necesidades de recursos mediante la identificación de los cuellos de botella • Aplicar la modulación del tráfico y control de la velocidad para mantener el rendimiento de la red • Datos detallados permite una rápida resolución de problemas, minimizando costosos de inactividad de la red. • Diseñar y aplicar políticas de seguridad específicas • Identifica la política de acceso y violaciones intrusiones. • Identifica hosts infectados por gusanos y la propagación de infecciones. • Datos detallados sobre el uso de la red • Usuario • Grupos de usuarios • Solicitud origen / destino del tráfico	Alcatel Allied Telesis Extreme Networks Foundry Networks HP Hitachi Jupiter Networks Nec Comtec Systems Force 10 Networks AlaxalA Networks
IPFIX	»Todos los hosts que transmiten la mayoría de los datos en la red » Todos los hosts que transmiten la mayoría de los datos entre sí »Todas las solicitudes que ponen más tráfico en la red » El volumen de datos por entidad (circuito, ubicación remota, región, etc) »Datos por tipos de entidad (circuito, ubicación remota, región, etc) » ToS, Criterios de presentación de informes sobre Netflow / IPFIX , los datos requieren un sólida motor de análisis. » Extrae más estadísticas de tráfico de los elementos de red corporativos. » Facilita prestaciones como es la facturación por uso o una mayor sencillez en la aplicación de parches a brechas de seguridad. » Tiene un método para que tanto conmutadores como routers exporten datos sobre flujo de tráfico a los sistemas de gestión.	Cisco Systems Nortel Networks Riberstone Networks

Fuente: http://www.dric.com.mx/adventnet/netflow.html

Elaborado por: Las autoras

TABLA III.14

PARAMETROS PARA EXAMINACION DE PAQUETES O FLUJOS Y PROPIEDADES DE CADA TECNOLIGIA

Tecnología / **Parámetros**	**NetFlow**	**sFlow**	**IPFIX**
Examinacion de paquetes o flujos	• Direcciones IP fuente y destino • Número de protocolo a nivel 3 • Puertos fuente y destino • Octeto de ToS (Type of Service) • Índice de la interfaz de entrada (ifIndex)	• Formato de cabecera de la muestra • Longitud original antes de paquetes • Dirección física del equipo • El tamaño máximo de la muestra de cabecera. • Tipo de protocolo IP (TCP, UDP) • Fuente dirección IP(ip_v4 src_ip) • Dirección IP de destino(ip_v4 dst_ip) • Fuente o número de puerto equivalente • Número de puerto de destino o equivalente • Banderas TCP • Tipo de servicio de PI • La longitud de la exclusión de paquete IP	• Fuente dirección IP • La dirección IP de destino • Número de puerto de origen (TCP / UDP) • Número de puerto de destino (TCP / UDP) • Nivel 3: Tipo de protocolo (IP / ICMP) • Tipo de servicio (TOS) • Entrada de la interfaz lógica.
	• Comprensión en el rendimiento de la red • Optimización de la	• Preciso • Detallado • Escalable	• Arquitectura no intrusiva e interoperable

Propiedades	calidad del uso • Planificación • Compatibilidad Universal • Mostrar jerarquía • Granular la gestión de datos • Profundidad ilimitada • No hay inversión de capital • Extensibilidad • Facilita la carga de los dispositivos de clasificación	• Bajo Costo • Oportuno	• Caracteriza el tipo de tráfico cursado por los usuarios finales • Extensibilidad • Facilita la carga de los dispositivos de clasificación • No hay inversión de capital: • Bajos costes de despliegue • Recursos de Datos completos • Sólo el tráfico IP es compatible • Escalabilidad

Fuente: www.cisco.com/univercd/cc/td/doc/cisictwk/intsolns/netflsol/nfwhite.htm

Elaborado por: Las autoras

TABLA III.15

RECURSOS DEL AGENTE

Parámetro / **Tecnología**	**CPU**		**Memoria**
NetFlow	Número de flujos activos en la cache 10000 45000 65000	Utilización de CPU adicional < 4% < 12% < 16%	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 y reduciendo la utilización de la memoria.
sFlow	Construyen matrices de tráfico decodificando cada paquete. Esto puede agregar una carga impredecible de CPU, dependiendo de la naturaleza de los patrones de tráfico.		Construyen matrices en la RAM del agente. El tamaño de las tablas depende mucho de los patrones de tráfico. NetFlow tiene la ventaja de que puede ser configurado automáticamente para

	La función de muestreo del agente sFlow puede ser fácilmente implementada en hardware. Además como el agente de lo único que se encarga es de enviar el cabezal del paquete al servidor, esa tarea no implica una sobrecarga del CPU.	descargar flujos individuales cada quince minutos o más, y también para descargar bloques de flujos para prevenir quedarse sin memoria suficiente. El agente sFlow solo necesita RAM para guardar un paquete.
IPFIX	Generalmente aumenta la utilización del CPU en la configuración de dispositivos, en promedio, de un 1% al 2%.	

Fuente: www.cisco.com/univercd/cc/td/doc/cisictwk/intsolns/netflsol/nfwhite.htm

Elaborado por: Las autoras

3.4 Elección de la mejor Tecnología de análisis de Flujo IP para el Monitoreo de la red de la EIS.

Luego de analizar los parámetros más importantes de cada una de las tecnologías, optamos por la solución más eficiente que brinde rentabilidad y optimización de los recursos al utilizarla.

La tecnología seleccionada es NetFlow, la misma que provee los siguientes beneficios frente a sFlow e IPFIX:

Hemos considerado no utilizar sFlow ya que el flujo que este nos presenta es una muestra de tráfico de paquetes por lo que una representación precisa de 100 por ciento del tráfico por interfaz es casi imposible. Complejos algoritmos se han propuesto a manipular estadísticamente los datos recogidos para representar el tráfico total con una probabilidad de exactitud pero no representan el 100 por ciento, los datagramas que se almacenan en la base de datos mediante sFlow no son de fácil manipulación como en el caso de NetFlow. Un aspecto importante que hemos considerado es que sFlow no dispone de Planificación en la gestión de la red y únicamente obtiene información de la capa de enlace de datos, en la tecnología Sflow la colección de información se la realiza en grandes cantidades dependiendo de la taza de muestreo y por utilizar un chip incorporado en el Hardware la actualización resulta más costosa y complicada, además no existe disponibilidad de

tecnología ya que los equipos con los que cuenta la ESPOCH son Cisco y sFlow no se implementa ni viene incorporado en los mismos.

Se descarto la tecnología IPFIX debido a que esta no se encuentra completamente comercializada, pero la mayoría de los principales proveedores como Cisco tienen la intención de apoyar IPFIX para que pueda seguir adelante.

Además, IPFIX normaliza NetFlow es decir toda la gestión de la información realizada por esta tecnología se basa principalmente en NetFlow.

Otro de los principales motivos para descartar esta tecnología es que no dispone de niveles altos de seguridad.

Existe una gran desventaja al utilizar IPFIX debido a que no se pueden controlar cadenas de longitud variable, no da mensajes cuando las plantillas son retiradas y se aplica para el flujo de exportación SCTP

Una de las principales limitaciones de IPFIX es que tiene un campo no observado es decir lo primero que se escoge es el valor especifico por elemento de información, es decir si en una información específica el elemento es requerido por una plantilla, pero no está disponible en paquetes observados, el proceso de exportación podrá optar por los registros de flujo de exportación sin que esos elementos de información de los registros de datos estén definidos en la nueva plantilla RFC5101.

Otra limitación es que los datos no están estructurados, es decir el contenido de un valor depende del contenido de otro con lo cual se rompe el diseño.

Y en las listas de exportación la interfaz de salida es por multicast, es decir si un elemento de información se requiere más de una vez en una plantilla, las diferentes ocurrencias de este elemento de información debe seguir el orden lógico de su proceso de medición.

Se eligió NetFlow por los siguientes motivos:

Uno de los principales motivos por los que se eligió la tecnología NetFlow es la disponibilidad de los equipos dentro de la ESPOCH, debido a que existe el switch capa 3 que soporta la misma en el cual implementaremos la solución planteada en el tema de tesis.

NetFlow es una tecnología que permite monitorizar las redes de forma gráfica y sencilla, principalmente para saber cómo, quién y en qué se está usando el ancho de banda disponible, detectar y prevenir cuellos de botella, y tomar acciones correctivas o preventivas.

NetFlow es una tecnología abierta pero desarrollada por Cisco que permite monitorizar el tráfico de una red y obtener informes que permitan ver en qué estamos gastando el ancho de banda, qué equipos, aplicaciones o protocolos consume los recursos de la red, y otra información útil para el administrador de la red.

Como la tecnología NetFlow es abierta, otros fabricantes la implementan, como 3Com, Enterasys, Nortel, Juniper, Alcatel o HP Procurve, entre otros.

Las implementaciones de Netflow son optimas ya que permiten también a los gestores de la red reducir al mínimo el número de recolectores de datos y reducir costes y aumentar al máximo la cobertura de la red.

En el IOS de un equipo se puede incluir NetFlow debido a que este es un software, por lo que al actualizar el IOS se puede disponer de esta tecnología, por tal motivo es de bajo costo debido a que viene incluido o simplemente se actualiza.

En qué consiste

El protocolo consiste en paquetes UDP enviados por los dispositivos previamente configurados que son recogidas por la aplicación (colector NetFlow) y almacenadas en la base de datos de la misma

para la generación de informes, estadísticas, etc.

Amplia creación de informes.

En la estación de gestión de Netflow la presentación de informes no sólo deben permitir la visibilidad a nivel de empresa, si no tambien los detalles específicos de la aplicación cuando se le solicite. Para esto, la solución debe proporcionar un análisis granular en profundidad tales como los informes de los anfitriones y protocolos en particular, agregados a la información, tales como los informes por el transporte o protocolo de aplicación, las agrupaciones de interfaz, circuito, geográficas región, entidad o empresa.

La cantidad de datos que NetFlow controla va desde pequeñas hasta grandes cantidades (depende de la tasa de muestreo y de las condiciones de creación de flujos)

En la tecnologia NetFlow la coleccion de informacion se realiza a nivel de la Capa de Enlace de Datos y de la Capa de Transporte.

NetFlow también da al usuario la capacidad de ejecutar consultas complejas sobre los datos históricos, ofrecer la solución de problemas con visión de datos en tiempo real, y permitir un análisis más detallado de cada datagrama Netflow en la red.

NetFlow, permite mejorar la capacidad de encaminamiento de sus routers. Siguiendo la filosofía “encaminar una vez, conmutar muchas veces”, identifica los flujos establecidos entre máquinas con el fin de agilizar el encaminamiento de futuros paquetes IP.

Principales beneficios de NetFlow

Dispositivos de Intercambio

Planificación de la red

Ingeniería de tráfico

Contabilidad y facturación

Seguridad en el monitoreo

Vigilancia en el acceso a Internet (distribución de protocolos, ver el trafico va/viene)

Seguimiento del usuario

Solicitud de vigilancia

Facturación de departamentos

Seguridad en el monitoreo

Habilita a los dispositivos ya sean routers o switches que lo soporten a generar records, que pueden ser enviados a un colector a través de una red

Responde las preguntas quién, qué, dónde y cómo basado en el tráfico IP

Provee una visión detallada del comportamiento de la RED (monitoreo de aplicaciones que utilizan puertos dinámicos)

Análisis de seguridad: con el fin de detectar anomalías en el tráfico de la red

Almacenamiento de los Datos NetFlow: para futuros análisis

NetFlow puede informar que aplicación en particular es la que está generando mayor tráfico

Esa información puede ayudarlo a resolver el problema rápidamente y en un menor tiempo

Mercado Actual

Áreas claves de aplicación

Ingeniería de tráfico 50%

Uso de la base de facturación 30%

DPM-rápidamente

Característica de aceleración

Mejora el rendimiento de ACL

Gestión de la red

Con la exportación de datos de NetFlow, la capacidad de gestión del rendimiento en los routers se extiende para proporcionar una monitorización integral de todos los flujos entre subredes.

Las estadísticas de flujo obtenidas permiten diversos beneficios y aplicaciones claves de usuario.

• **Monitorización y perfil del usuario**—Obtiene un conocimiento detallado de la utilización del usuario de los recursos de la red y de las aplicaciones. Esta información puede usarse para planificar y distribuir los recursos de forma eficiente.

• **Monitorización y perfil de la aplicación**—Obtiene una visión detallada de los patrones de tráfico de la aplicación en la red. Por ejemplo, el administrador de la red puede ver el porcentaje de tráfico usado por la Web, File Transfer Protocol (FTP), Telnet y otras aplicaciones TCP/IP muy conocidas.

• **Monitorización de la red**—Hace posible las capacidades de monitorización de la red. RMON, RMON2, y técnicas basadas en análisis de flujos pueden utilizarse para la detección proactiva de los problemas, como una ayuda eficiente y para conseguir rapidez en la solución de los problemas.

• **Planificación de la red**—Ofrece información esencial para herramientas sofisticadas como, por ejemplo, las de Cisco Netsys, para optimizar la planificación estratégica de la red.

• **Contabilidad y facturación**—Ofrece medición (por ejemplo, datos de flujo, incluyendo detalles como las direcciones IP, recuentos de paquetes y bytes, sellos de hora, puertos de aplicaciones) para la contabilidad flexible de la utilización de recursos.

Hay que decir que aunque Cisco desarrolla e implementa la tecnología en sus dispositivos, no dispone de una aplicación para su utilización. Hay varias empresas que han desarrollado herramientas para ello, como Fluke Networks NetflowTracker, SolarWinds Netflow Analyzer, y también algunas gratuitas, obviamente no con la misma calidad.

Luego de un análisis, se selecciono la herramienta NetFlowAnalyzer, que es una tecnología que se ha probado y cada una de las soluciones se obtuvieron buenos resultados.

Hay dos versiones, la Professional y la Enterprise.

Los precios y las licencias van en función del número de interfaces que queremos monitorizar. La versión Professional hasta 10 interfaces cuesta aproximadamente 600€=774 dólares.

Hay una versión gratuita que permite monitorizar sólo 2 interfaces.

NetFlow Analyzer

Herramienta para monitorear el ancho de banda y realizar análisis forense de la red, que permite optimizar redes para lograr un desempeño superior. Utilizando CISCO NetFlow, entrega una visibilidad en profundidad del tráfico de la red y sus patrones, provee conocimiento de negocio sobre el comportamiento de la red en tiempo real y cómo el tráfico impacta la salud y estabilidad de la red

NetFlow Analyzer [1 y 2] recopila información generada, del flujo de red, por switches y routers de la empresa, y genera informes de tráfico que ayudan a comprender la naturaleza del tráfico.

Aparte del análisis de datos y presentación de informes, NetFlow Analyzer incluye una gran variedad de características empresariales que son útiles en la gestión de datos NetFlow que se exportan desde varios dispositivos. Estas características ofrecen grandes beneficios a las empresas, así como a los proveedores de servicios.

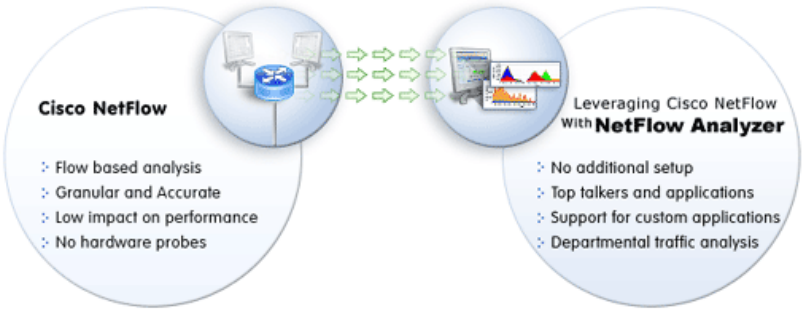


Figura N°III.04 Características NetFlow Analyzer

Beneficios de NetFlowAnalyzer

Agrupación de IPs

Monitoree de forma exclusiva tráfico por departamento, intranet o aplicación utilizando grupos de IPs. Puede crear grupos de IP basado en direcciones IP y / o una combinación de puerto y el protocolo. Esta función es útil en el rastreo del uso de banda ancha por departamento, el cálculo de los costos de ancho de banda, y para garantizar la adecuada utilización de ancho de banda en la red.

Mapas de Aplicaciones

NetFlow Analyzer le permite definir las aplicaciones mostradas en los informes de ancho de banda. La mayoría de las aplicaciones empresariales como Oracle, PeopleSoft, MSSQL, etc. son compatibles, y puede añadir aplicaciones personalizadas a la lista de las aplicaciones conocidas. Como resultado de ello, ver el uso de ancho de banda para las aplicaciones específicas de su empresa ya no es una tarea compleja.

Agrupación de dispositivos

Clasifique routers y switches exportadores de NetFlow, en grupos, y monitoréelo de forma exclusiva. Esta función es especialmente útil para los proveedores de servicios, que tienen que administrar varias redes desde una única ubicación.

Acceso Autorizado

NetFlow Analyzer le permite crear cualquier número de usuarios en función de sus propios permisos de acceso. Esto es especialmente útil para los administradores de la NOC y MSP que necesitan proporcionar a los clientes informes del uso de ancho de banda y tendencias de uso de sus redes específicas.

Política Flexible de Licencias

Las políticas de licencia de NetFlow Analyzer le permiten decidir que dispositivos NetFlow desea administrar en cualquier momento. Esta flexibilidad le permite descargar el sistema durante los periodos de mantenimiento del dispositivo, y utilizar su licencia de manera eficaz para el monitoreo de NetFlow(flujo de red). En general, NetFlow Analyzer ofrece una serie de características que hacen de la administración de dispositivos y monitoreo de datos NetFlow mucho menos complicado.

CAPITULO IV

IMPLEMENTACION DEL MONITOREO EN LA RED DE LA EIS

Una vez seleccionada la tecnología NetFlow y NetFlowAnalyzer como herramienta de monitoreo se procede a la ejecución de la parte practica.

4.1 Análisis de aspectos Generales de la red de la Escuela de Ingeniería en Sistemas

4.1.1 Problemas y necesidades de la Red de la EIS.

Hoy en día la red de la Escuela de Ingeniería en Sistemas perteneciente a la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo “ESPOCH” dispone únicamente de acceso a aplicaciones de Intranet, pero no existen herramientas que permitan especificar un monitoreo detallado de la red.

Uno de los principales problemas en una red de múltiples usuarios es el bajo rendimiento debido a que no existe un control adecuado de los procesos que retardan y dificultan al usuario final y a los técnicos, usos irregulares, ataques, entre otros, los mismos que no permiten obtener la información necesaria de todo lo que ocurre en la misma.

Por tal motivo luego de haber seleccionado la tecnología que mejor se adapta a las necesidades y NetFlowAnalyzer como herramienta de monitoreo por los beneficios y facilidades que proporciona, se procede al desarrollo de la parte aplicativa que consiste en realizar un control detallado de la red

de la EIS, utilizando los equipos Cisco que se encuentran en la misma.

Nuestra aplicación es implementada bajo la plataforma Linux para obtener una utilización adecuada de todos los recursos que existen en la red.

4.1.2 Características del Switch del Departamento de Sistemas y Telemática y de la EIS

Switch Capa 3

Cisco Catalyst 4507 R

Cisco, líder mundial en soluciones de red e infraestructuras de Internet, presenta la serie Cisco Catalyst 4500, una gama de conmutadores modulares inteligentes que ofrecen a los clientes redundancia, mejor control de la red, potencia online integrada, y protección para las inversiones. La serie Catalyst 4500 es un componente clave de la arquitectura Cisco AVVID (Architecture for Voice, Video and Integrated Data). A su vez, la serie Catalyst 4500 permite a las empresas clientes y a los clientes con redes Ethernet metropolitanas desplegar redes convergentes con mayores niveles de rendimiento, flexibilidad, resistencia, seguridad y facilidad de gestión. De esta forma, los clientes pueden hacer converger y controlar mejor los datos IP (Internet Protocol), el streaming vídeo, la telefonía y las aplicaciones comerciales basadas en Internet, con el fin de mejorar la productividad y rentabilidad de los empleados. La serie Catalyst 4500 permite a los clientes extender el control de la red desde el centro al borde de la red a través de servicios de red inteligentes que ofrecen conmutación de Nivel 2/3/4; rendimiento de routing sostenido a velocidad de línea cualquiera que sea la cantidad de servicios inteligentes activados; Calidad de Servicio (QoS) y gestión de tráfico, que permiten clasificar y priorizar tráfico crítico y sensitivo al mismo tiempo.

Switch Cisco 3750

Características y ventajas

Switching de alta velocidad inteligente y asequible

Es un switch Ethernet LAN de altas prestaciones y con amplia variedad de características. Este switch 10/100 inteligente y asequible es totalmente administrable, haciéndolo idóneo para redes de cualquier tamaño.

Rendimiento de alta velocidad, soporte para telefonía en red y dos ranuras uplink se acomodan a las aplicaciones más exigentes. Los módulos de switching opcionales proporcionan conexiones resilientes de alta velocidad tales como Fast Ethernet, incluyendo 100BASE-LX (Ethernet de primera milla) y enlaces de cobre o fibra Gigabit Ethernet.

El Rapid Spanning Tree, el trunking de agregación de enlaces automático en toda la pila, el apilamiento resistente a fallos y el soporte para fuente de alimentación redundante opcional ofrecen un robusto rendimiento y tolerancia a fallos.

El login de red de usuario con IEEE 802.1X y RADIUS, combinado con la característica RADIUS Authenticated Device Access (RADA), basada en la dirección MAC, proporciona un control de acceso seguro en el borde de la red.

Los usuarios autenticados pueden situarse automáticamente en una VLAN específica, limitando el acceso sólo a los datos necesarios.

La encriptación SSH (Secure Shell) de contraseñas de acceso (login), las VLANs de administración y las listas de "direcciones IP fiables" de estaciones de administración ayudan a proteger la red contra amenazas de administración dañinas.

La funcionalidad avanzada de Layer 4 identifica automáticamente y prioriza las aplicaciones en tiempo real o críticas para el negocio, tales como SAP, voz y vídeo.

4.2 Escenario a ejecutar

La Escuela de Ingeniería en Sistemas así como la ESPOCH en general requieren de un análisis minucioso de la red para obtener un rendimiento optimo de los recursos, por tal motivo el escenario a ejecutar es el monitoreo de la red de la EIS, la cual está conformada de 8 VLANs, el rango de red de cada una está dado en subredes a partir de la dirección principal 172.30.40.0, el monitoreo se desarrollara en el switch capa 3 (exportador) que se encuentra en el departamento de Sistemas y Telemática donde se procederá a configurar paso a paso cada uno de los comandos necesarios para habilitar la Tecnología NetFlow, NetFlow colecta el trafico que genera el switch en forma de flujos y los exporta a un analizador en nuestro caso NetFlowAnalyzer el cual presenta estadística y gráficamente la utilización del ancho de banda, direcciones de origen y destino, protocolo, entre otras características fundamentales para un administrador de red.

4.3 Objetivos del monitoreo

- Monitorización de ancho de banda por medio de la herramienta NetFlowAnalyzer basada en tecnología web.
- Monitorear el nivel de utilización de un enlace.
- Permitir la monitorización de la red de la EIS de forma grafica y sencilla, principalmente para saber cómo, quién y en qué se está usando el ancho de banda disponible, detectar y prevenir cuellos de botella, y tomar acciones correctivas o preventivas.
- Permitir el análisis de la utilización de ancho de banda y ofrecer visibilidad completa sobre routers y switches Cisco. Gracias a sus informes detallados y gráficos en tiempo real.
- Obtener a través de NetFlowAnalyzer información muy completa sobre el tráfico de red, sin necesidad de utilizar sondas.
- Generar informes en tiempo real que ayuden a los administradores de la red de la EIS a mejorar la visibilidad de incidencias fundamentales de la red, aumentar las comunicaciones, reducir el tiempo de resolución de incidencias y disminuir los costes de funcionamiento.

- Obtener informes que permitan ver en qué estamos gastando el ancho de banda, qué equipos, aplicaciones o protocolos consumen los recursos de la red, y otra información útil para el administrador de la red.
- Programar capturas específicas, filtrar los datos para obtener informes de uso en determinadas horas, días o por determinados equipos, protocolos, o aplicaciones

4.4 Selección de Equipos

Una vez realizado el análisis de la tecnología y una variedad de pruebas se eligió el equipo necesario para un monitoreo eficiente y que optimice la utilización de los recursos.

En primera instancia se selecciono el Switch capa 3 (exportador) el cual cumple los requerimientos necesarios para que se habilite la tecnología NetFlow.

Un computador (colector) Intel Core 2 Duo con 2,5 GB de RAM, en el cual se instalara Linux SUSE 10.0 (para servidor) como Sistema Operativo, sobre el cual se instalara NetFlowAnalyzer como herramienta para obtener las estadísticas del monitoreo.

4.5 Configuración de Equipos

4.5.1 Configuración del Switch capa 3

Lo primero que tenemos que realizar es la configuración de la comunidad SNMP **e**n el entorno de gestión, una entidad SNMP es una "entidad lógica" en nombre de la cual un agente o una aplicación de gestión están procesando un mensaje.

El entorno de gestión es responsable de proporcionar:

- Autentificación: se refiere a como las entidades SNMP identifican sus mensajes.
- Privacidad: se refiere a como las entidades SNMP protegen sus mensajes.
- Autorización: se refiere a como una entidad agente SNMP determina los objetos

que son accesibles a una entidad de aplicación de gestión dada, y las operaciones que se pueden realizar en estos objetos.

Comandos de la comunidad SNMP

Para habilitar el protocolo SNMP en un router o switch cisco, debemos entrar en el modo de configuración global.

Switch> enable

Switch# configure terminal

Switch (config) #

Y ejecutamos loa siguientes comandos:

Switch(config)#snmp-server enable traps

Este comando se utiliza para habilitar y configurar la generación de traps SNMP sobre una base global.

Los traps son mensajes no solicitados enviados desde un servidor SNMP a un cliente SNMP.

Switch(config)#snmp-server community NETFLOW ro

Lo que hacemos con este comando es agregar una comunidad pública “NETFLOW” con permisos de solo lectura.

Comandos de configuración de NetFlow

Switch(config)#interface GI3/24 //Puerto del switch capa 3 que se conecta al switch EIS

Switch(config-if)#ip route-cache flow

```
Switch(config-if)#exit

Switch(config)#ip flow-export destination 172.30.60.25 9996

Switch(config)# ip flow-export source GI3/24

Switch(config)# ip flow-export version 5

Switch(config)# ip route-cache timeoute active 1

Switch(config)# ip route-cache timeoute inactive 15   //Cuando en este tiempo
                                                       no se exporta el flujo se
Switch(config)#snmp-server ifindex persist             borra de la tabla donde se
                                                       almacenan.
Switch(config)#ctrl Z

Switc#write              //Para guardar los comandos de la configuracion

Switc#show ip flow export   //Para ver la configuración de NetFlow

Switc#show ip cahe flow
```

4.5.2 Configuración del equipo a utilizar para el monitoreo

Descripción del equipo

Para la instalación del sistema operativo SUSE 10.0 para servidor, se busco una computadora con características recomendables para obtener un resultado satisfactorio a los usuarios finales el equipo utilizado es un computador Intel Core 2 Duo con 2,5 GB de RAM.

Sistema Operativo SUSE

Requisitos

La configuración mínima necesaria para correr el sistema operativo en modo texto es una 386 con 16 MB de memoria RAM. Para el entorno gráfico será necesario como mínimo una 486 como

mínimo, con la misma RAM. En estas configuraciones generalmente se usan manejadores de ventanas livianos, como FVWM, WindowsMaker o BlackBox, ya que consumen muy poca memoria.

Si queremos disfrutar al máximo del sistema operativo, entonces una Pentium II de 300 MHz, 64 MB de RAM y 4 GB de espacio de almacenamiento serán más que necesarios para correr Linux con Xwindows, KDE y todas sus aplicaciones.

Herramienta NetFlowAnalyzer versión 7

Requerimientos de hardware

El mínimo de hardware requerido para NetFlow Analyzer es:

- 2.4GHz, Procesador Pentium 4,o equivalentes
- 1GB RAM
- 10GB de espacio de disco para la base de datos

TABLA IV.16

USO DEL PROCESADOR Y RAM DEL NUMERO DE INTERFACES

Interface	Processor	RAM
Upto 50	2.4 Ghz	1 GB
50 -150	3.4 GHz	2 GB
150 – 400	2 * 3.4 GHz	4 GB
400 – 1000	4 * 3.4 GHz	8 GB

Fuente: http://www.netflowanalyzer.com/download.html.

Elaborado por: AdventNet, Inc

NetFlow Analyzer está optimizado para resolución de 1024 x 768 y superiores.

Para los dispositivos que exportan NetFlow, hay que asegurarnos que la versión que exporta NetFlow sea la misma que la que soporta NetFlow en los equipos Cisco, esta puede ser la versión 5 o 7.

Requerimientos de Software

Requerimientos de la Plataforma

NetFlow Analyzer puede ser instalado y corriendo en los siguientes sistemas operativos y versiones:

- Windows 2000 Server/Professional with SP 4
- Windows XP with SP 1
- RedHat Linux 8.0, 9.0
- SUSE Linux

Navegadores Web admitidos

NetFlow Analyzer se ha puesto a prueba en apoyo de los siguientes navegadores y versiones:Internet Explorer 5.5 and later

- Netscape 7.0 and later
- Mozilla 1.5 and later

Para mas informacion ver anexo1 de NetFlow Analyzer7

CAPITULO V

ANALISIS Y EVALUACION FINAL

Para la realizacion del analisis de trafico y su evaluacion final se procedio a realizar una serie de pruebas para su implementacion final en el laboratorio del departamento de sistemas y telematica utilizando la tecnologia NetFlow.

Se procedio a configurar el switch capa 3 que se encuentra en DESITEL, una vez habilitado NetFlow, los flujos exportados por el mismo fueron enviados al analizador NetFlow Analyzer 7 al cual se puede acceder desde una maquina de la misma red de la EIS o desde cualquier maquina dentro de la red, la direccion IP para acceder a monitorear es 172.30.60.25. La direccion para acceder a la aplicacion desde cualquier maquina dentro o fuera de la ESPOCH es 201.218.5.25, esto se puede realizar debido a que la aplicacion esta subida en el servidor.

Una vez puesta la direccion automaticamente aparece la pagina inicial en la cual nos podemos autenticar como administradores (usuario: tesis, contraseña: tesis2009) para realizar las operaciones necesarias o como usuarios, este perfil unicamente permite realizar las tareas de monitoreo.

Para ejecutar este escenario final se realizaron un sinnumero de pruebas para las cuales se utilizo SPAN.

Se utilizo SPAN para capturar el trafico y enviar al puerto de un router que soporta NetFlow debido a que el switch de sistemas no soporta esta tecnologia.

Descripcion General del SPAN

Las sesiones locales SPAN permiten que tu trafico sea monitoreado en uno o más puertos, o en una y mas VLANs, y este tráfico es enviado a uno o más puertos de monitoreo.

El SPAN envía tráfico a un analizador de red como un dispositivo SwitchProbe, o RMON a otros dispositivos como routers. El SPAN no afecta el tráfico del switch o puertos de origen o Vlans. El SPAN envía una copia de los paquetes recibidos o transmitidos por los puertos de origen o VLANs en los puertos de destino.

Una sesión local SPAN es una asociación de puertos de origen y VLANs de origen con uno o más puertos de destino. Se configura una sesión local SPAN en un único router o switch. El SPAN local no tiene sesiones de origen y destino separados.

Las sesiones locales SPAN no copian localmente tráfico de VLANs RSPAN por puertos de origen en modo trunk que alcanzan VLANs RSPAN.

Cada sesión local SPAN puede tener solo puertos de origen o VLANs de origen, pero no ambos.

Las sesiones de SPAN local copian tráfico desde uno o más puertos de origen en cualquier VLAN o desde una o más VLANs a un puerto de destino para el análisis.

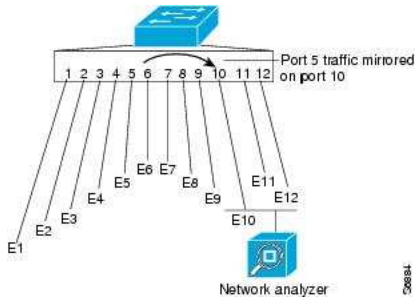


Figura V.05 Ejemplo de Configuración SPAN

Dirección del monitoreo de trafico

Se puede configurar sesiones de SPAN local para monitorear tráfico de ingreso (llamado SPAN de ingreso), o para monitorear tráfico de salida (llamado SPAN de salida), o para monitorear tráfico en ambas direcciones.

El SPAN de ingreso copia el tráfico recibido por el puerto de origen y VLANs para el análisis en el puerto de destino. El SPAN de salida copia el tráfico transmitido desde los puertos de origen o VLANs.

Configurando SPAN Local

EL SPAN local no usa por separado sesiones de origen y sesiones de destino. Para configurar una sesión SPAN local, configure origen y destino del SPAN local con el mismo número de sesión. Para configurar la sesión local SPAN siga los siguientes pasos:

TABLA V.17

PASOS PARA CONFIGURAR SPAN LOCAL

	Command	**Purpose**
Step 1	Router# **configure terminal**	Entre al modo de configuración global
Step 2	Router(config)# **monitor session** *local_span_session_number* **source** {{*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]}}	Asocie el número de sesión de origen con el Puerto o VLANs de origen y seleccione la dirección del tráfico a ser monitoreado.
Step 3	Router(config)# **monitor session** *local_span_session_number* **destination** {*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list*}	Asocie el numero de session del SPAN local y el puerto de destino.

	Router(config)# **no monitor session** {*session_number* | **all** | **local** | **range** *session_range*[[,*session_range*],...]}	Borrar la sesión creada

Fuente: http://www.cisco.com/en/US/tech/tk812/tech_configuration_guides_list.html

Elaborado por: Técnicos de Cisco

Cuando se configura una sesión SPAN local, hay que tener en cuenta la siguiente información:

- El numero de sesión SPAN puede estar dentro del rango de 1 a 66
- single_interface es una interface que puede ser un puerto slot, una interface Ethernet, fastethernet, gigabitethernet o tengigabitethernet.

Cuando se borra un monitor sessions, tenga en cuenta la siguiente información:

- El numero del comando **no monitor sessions** entra con no y otros parámetros y borra la sesión creada

5.1 Pruebas Realizadas

5.1.1 Pruebas de laboratorio

Entre las pruebas realizadas para el monitoreo con NetflowAnalyzer se procedio a implementar dos escenarios:

- Con VLANS
- Maquinas conectadas a Internet
- En el switch de la EIS

5.1.1.1 Con VLANS

Escenario

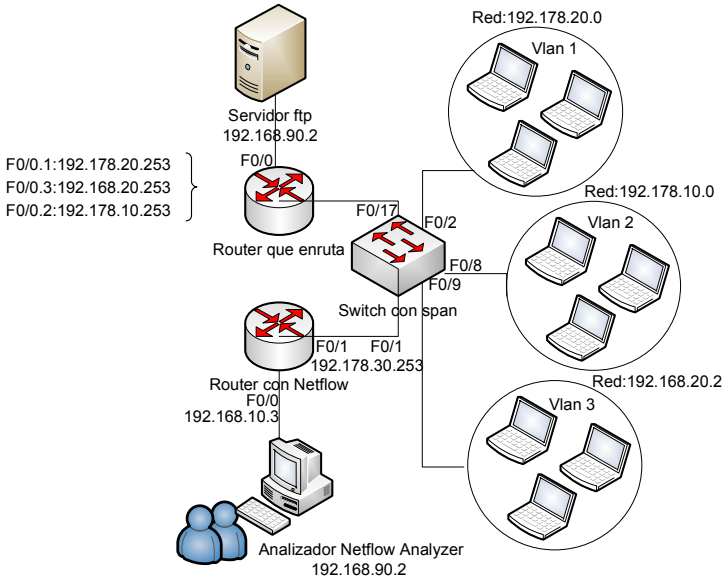


Figura V.VI Escenario con VLANs

Descripción

Iniciamos simulando la red de la EIS, con la construcción de dos VLANS la 10 y la 20, creadas en el Switch, el proceso de enrutamiento se realizo en el router 2811, el cual se conecta a la interface fastethernet 0/17 del Switch por medio de la interface fastethernet 0/0.

La interface FastEthernet 0/1 del switch es donde se realiza el SPAN, este envía trafico a la interface fastethernet 0/0 de otro router 2811 independiente del que realiza el enrutamiento en el cual se implemento NetFlow. En el router la interface fastethernet 0/1 se conecta a la maquina que tiene instalado el NetFlowAnalyzer el cual realizara el proceso de monitoreo.

La VLAN 10 se le asigna a la interface FastEthernet 0/2

La VLAN 20 se le asigna a la interface FastEthernet 0/9

Las vlans no fueron configuradas con internet por tal motivo para generar trafico se procedió a implementar un servidor ftp, el cual da respuesta a peticiones realizadas por los clientes ftp que fueron instalados en las maquinas en las que asignadas a cada vlan.

Configuración

Switch 2960

Creacion de vlans

Para crear VLANs, el switch debe estar en modo VTP “Server”, o “Transparent”. “Server” es el default.

```
Switch#show vtp status

Switch#show vlan

Switch#vlan database

Switch(vlan)#vtp server

Switch(vlan)#vlan 10 name Andi (crear la VLAN)

Switch(vlan)#vlan 20 name Belen

...

exit

Switch#show vlan

Switch#configure terminal

Switch(config)#interface f0/2

Switch(config-if)#switchport access vlan 10 (asigna el puerto a la VLAN 2)
```

interface f0/9

Switch(config-if)#switchport access vlan 20

...

end

Para borrar una vlan:

Switch#vlan database

Switch(vlan)no vlan 2 (borrar la VLAN especificada)

Para la asignación de VLAN a un puerto:

Switch#configure terminal

Switch(config)#interface f0/2

Switch(config-if)#switchport access vlan 10

Primer Router 2811

En este router se realiza el proceso de enrutamiento entre vlans.

Primero en la interface seleccionada en nuestro caso la 0/0 se crean subinterfaces por cada vlan, se ponen los comandos necesarios de encapsulación, dirección IP y se levanta la interface.

Comandos

Vlan 10

Switch#configure terminal

Switch(config)#interface f0/0.1

Switch(config-if)#encapsulation do1Q 10

Switch(config-if)#ip address 192.178.20.253 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

Vlan 20

Switch#configure terminal

Switch(config)#interface f0/0.2

Switch(config-if)#encapsulation do1Q 20

Switch(config-if)#ip address 192.168.20.253 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#exit

SPAN en el switch

Switch(config)#monitor session 1 source interface fastEthernet 0/2

Switch(config)#monitor session 1 source interface fastEthernet 0/9

Switch(config)#monitor session 1 destination interface fastEthernet 0/1

Segundo Router 2811

En este router se procede a configurar NetFlow y las interfaces necesarias para la comunicación con el switch y el analizador con dirección IP 192.168.10.2.

Comandos NetFlow

```
router#enable
router#configure terminal
router-2621(config)#interface FastEthernet 0/0
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination 192.168.10.2 9996
router-2621(config)#ip flow-export source FastEthernet 0/0
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
router#show ip flow export
router#show ip cache flow
```

Configuración y monitorización desde el NetFlowAnalyzer

El uso de la aplicación es muy sencillo e intuitivo, y no necesitamos configurar nada para empezar a obtener información de nuestra red, aunque podríamos programar capturas específicas, filtrar los datos para obtener informes de uso en determinadas horas, días o por determinados equipos, protocolos, o aplicaciones.

Podemos indicar cuánto tiempo se almacenarán los datos importados para ahorrar espacio en disco, o incluso limitar el espacio consumido por la aplicación.

Lo primero que se procedió a hacer es la instalación y configuración de un servidor ftp, luego se realiza la instalación del cliente ftp para realizar las pruebas respectivas.

Pruebas con el cliente y el servidor ftp

Para realizar las pruebas respectivas procedemos a crear un usuario en el servidor ftp para que el cliente tenga acceso al mismo a traves de este usuario

Creación de usuarios y directorio

Seleccionamos la opción usuarios, en la opción page se selecciona General

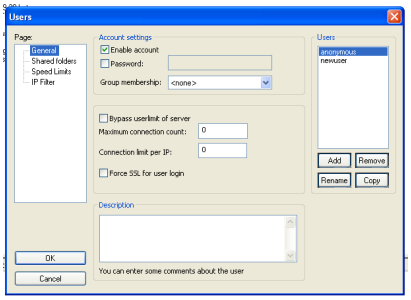


Figura N°V.07 Crear usuarios

Seleccionar add y aparece la siguiente pantalla en la cual se escribe el nombre del nuevo usuario en nuestro caso el nombre de usuario es prueba

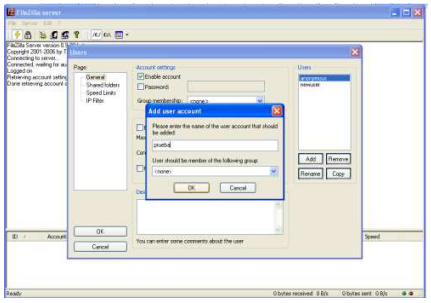


Figura N°V.08 Añadir nuevo usuario

Luego seleccionamos el usuario y elegimos la opción password para mayor seguridad nuestra contraseña es abc123

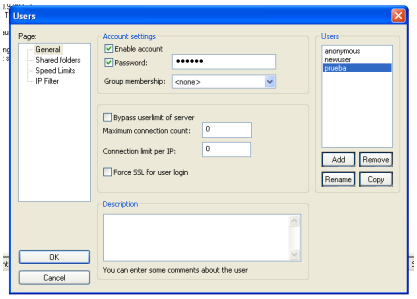


Figura N°V.09 Crear contraseña

Seleccionamos el usuario y le damos los permisos necesarios

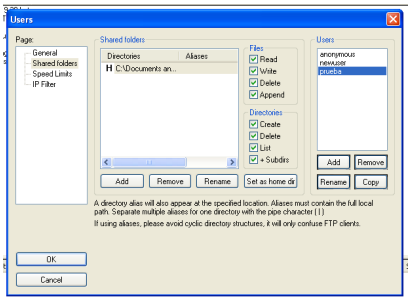


Figura N°V.10 Permisos de usuario

Se procede a la creación de un nuevo sitio dando clic en nuevo sitio

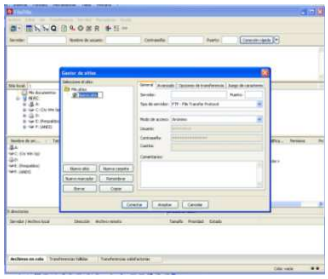


Figura N°V.11 Creación de un sitio

Se procede a llenar los datos con el nombre de usuario y contraseña creados en el servidor ftp

Clic en conectar

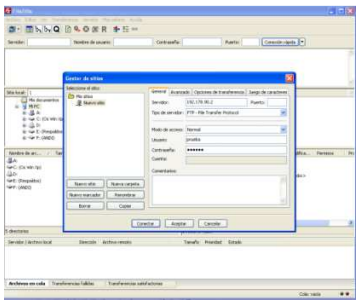


Figura N°V.12 Conectar

Resultados obtenidos al realizar la conexión del cliente con el servidor ftp

Resultado en el servidor de la conexión con el cliente

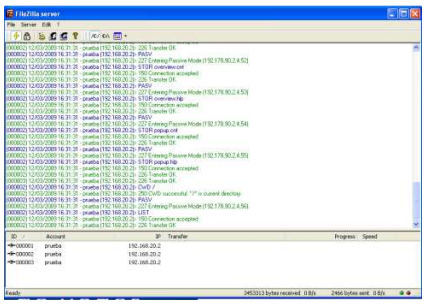


Figura N°V.13 Conexión con el servidor ftp

Una vez llenados correctamente los datos el cliente esta conectado al servidor

Una vez conectado el servidor se procede el envio de archivos, imágenes, etc desde el cliente obteniendo como resultados una transferencia satisfactoria

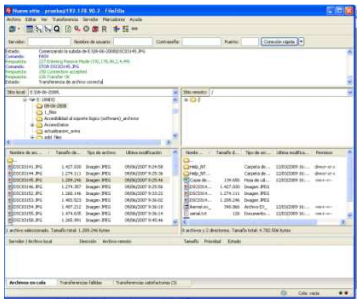


Figura N°V.14 Transferencia de archivos

Al enviar archivos al servidor ftp si son transferidos correctamente se almacenan en la carpeta creada al momento de crear al usuario

Todo este trafico se obtendra en la herramienta netflow analyzer

Resultados de la captura de trafico entrelos clientes y el servidor ftp en la herramineta NetFlowAnalyzer

Trafico con vlans

En esta pantalla se muestra graficamente el trafico de capa 3 generado por cada una de las VLANs que pasan por el router.

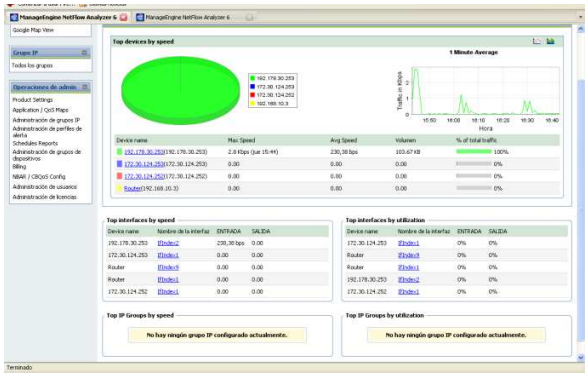


Figura N°V.15 Tráfico de VLANs

Se puede observar el trafico por velocidad, el color verde del grafico significa trafico de entrada y el color azul es trafico saliente.

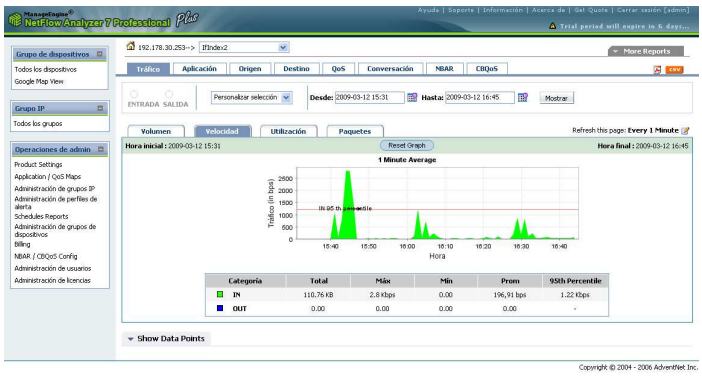


Figura N°V.16 Tráfico por velocidad (VLANs)

En esta pantalla se observa el porcentaje de utilizacion del ancho de banda del trafico de origen de la red que pasa por el router.

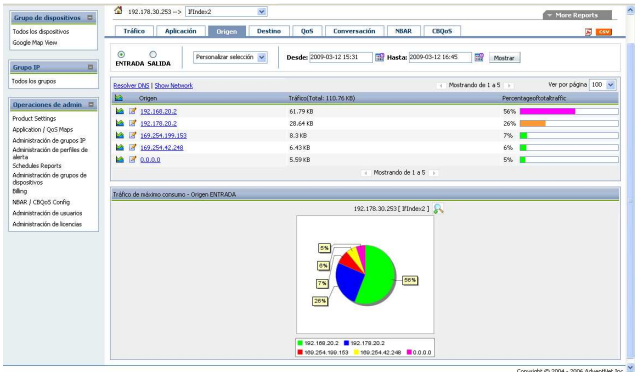


Figura N°V.17 Utilizacion Ancho de banda (tráfico origen VLANs)

En esta pantalla se observa el porcentaje de utilizacion del ancho de banda del trafico de origen de la red que pasa por el router.

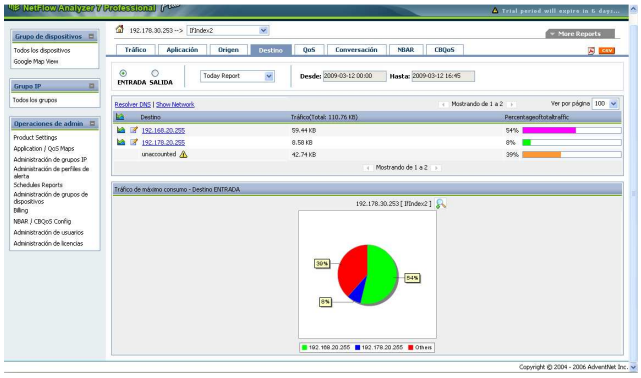


Figura N°V.18 Utilización Ancho de banda (tráfico destino VLANs)

Aqui se puede observar el reporte de conversacion, es decir quie, a donde y que peticiona

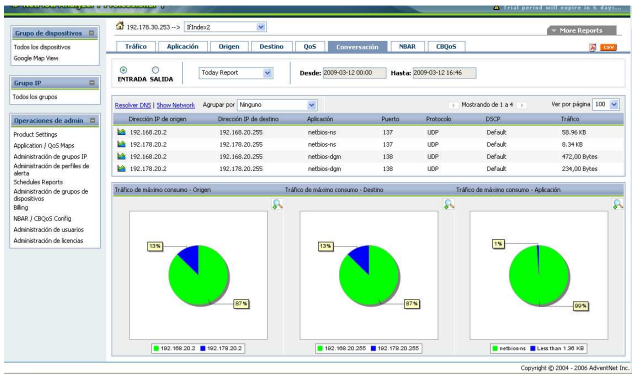


Figura N°V.19 Reporte de conversación (VLANs)

Este reporte muestra el top N de las aplicaciones mas solicitadas.

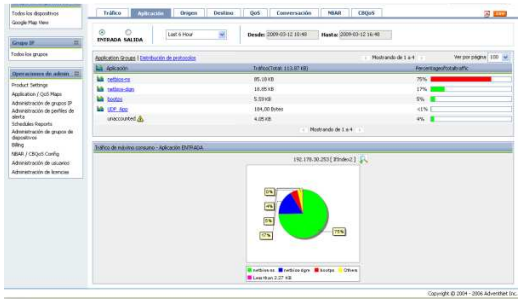


Figura N°V.20 Reporte de aplicaciones (VLANs)

Se pueden generar reportes según criterio, se puede seleccionad de que fecha a que fecha, y si es por velocidad, paquete, aplicacion, protocolo, etc,

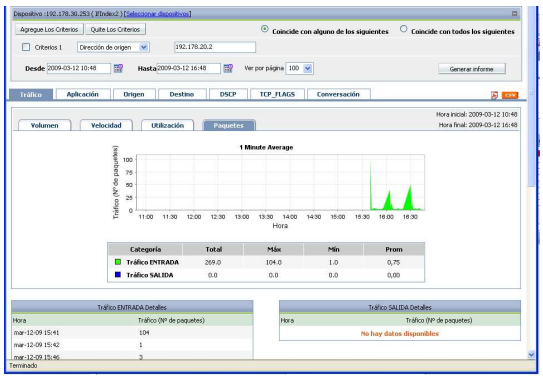


Figura N°V.21 Reporte según criterios (VLANs)

5.1.1.2 Con Internet

Escenario

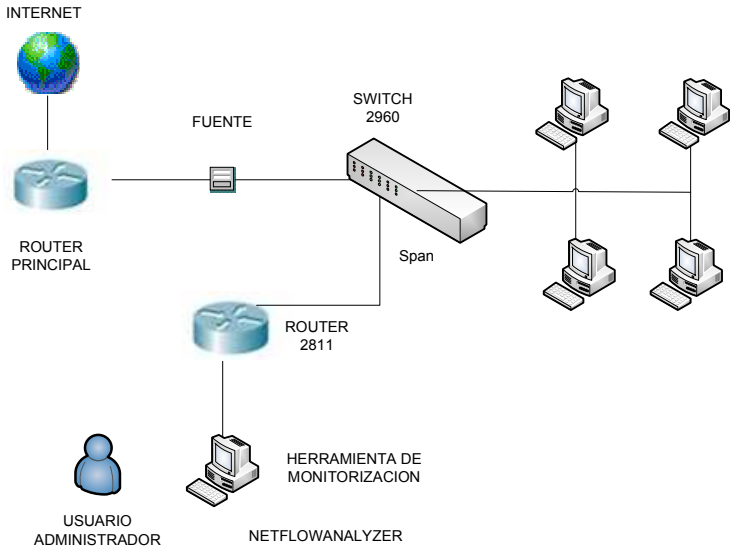


Figura N°V.22 Escenario con Internet

Descripción

Se obtiene el Internet para las maquinas por medio del router principal de DESITEL.

La simulación que se realizo es: por medio de un switch (Cisco series 2960) unido con cable directo se conecta a la fuente que proporciona el Internet obtenido desde el router principal, el cual a través de de cables directos el switch distribuye el internet a cada una de las maquinas que están dentro de la red.

El trafico que realiza cada una de las maquinas será monitorizado por la herramienta NetFlowAnalyzer la cual recoge flujos proporcionados por el router (Series Cisco 2800) configurado con NetFlow.

No todos los equipos soportan NetFlow por tal razón se procedió al desarrollo de este escenario, en el cual se supone que la red tiene un switch que no tiene esta tecnología, por lo que se utilizo SPAN el cual es como un espejo que realiza copias del trafico que entra en cada uno de los puertos que deseamos monitorizar. Este tráfico se copia en un puerto el cual será enviado al router que soporta esta tecnología. El router recoge la información en forma de flujos que son analizados en NetFlowAnalyzer.

Esta herramienta proporciona informes estadísticos y gráficos a los usuarios finales facilitando la administración de la red.

Configuración

Las configuraciones realizadas son las siguientes:

Las maquinas obtienen direcciones IP automáticas, debido a que el switch se conecta a la fuente que proporciona Internet, las siguientes pantallas muestran las direcciones obtenidas por cada máquina.

Máquina 1

Utilizando el comando ipconfig

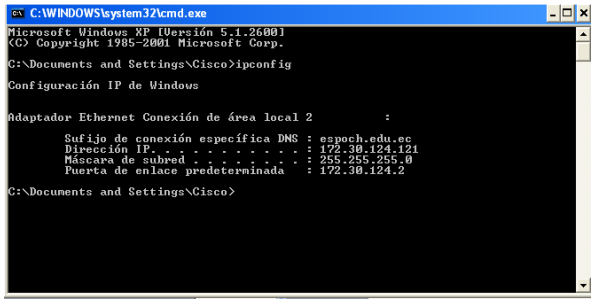


Figura N°V.23 Comando ipconfig en el cmd

La dirección dinámica que obtuvo es 172.30.124.121/24

En la máquina 2 se procedió a realizar lo mismo. La dirección dinámica que obtuvo es 172.30.124.124/24

SPAN

La maquina 1 se une al switch en la interface FastEthernet 0/4

La maquina 2 se une al switch en la interface FastEthernet 0/5

El SPAN se realiza en la interface FastEthernet 0/1

Comandos

Switch(config)#monitor session 1 source interface fastEthernet 0/4

Switch(config)#monitor session 1 source interface fastEthernet 0/5

Switch(config)#monitor session 1 destination interface fastEthernet 0/1

Resultados Obtenidos

Una vez realizadas las configuraciones necesarias NetFlowAnalyzer recoge la información en forma de flujos y muestra estadísticas graficas.

Los resultados obtenidos por la herramienta al realizar la simulación de esta red son los siguientes:

Con Internet

Las siguiente pantalla muestra las aplicaciones que estan entrando al analizador, exportadas por NetFlow, en el periodo desde las 00:00 del 12 de Marzo del 2009 hasta las 17:17 horas del 12 de Marzo del 2009.

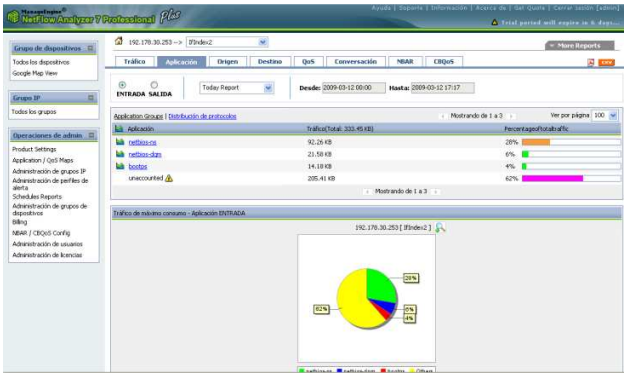


Figura N°V.24 Reporte de aplicaciones (Internet)

Esta pantalla muestra el trafico de origen (Direccion IP), tamaño y porcentaje de utilizacion del ancho de banda, del flujo que esta ingresando por la interfaz 192.178.30.253, en el periodo desde las 00:00 del 12 de Marzo del 2009 hasta las 17:15 horas del 12 de Marzo del 2009.

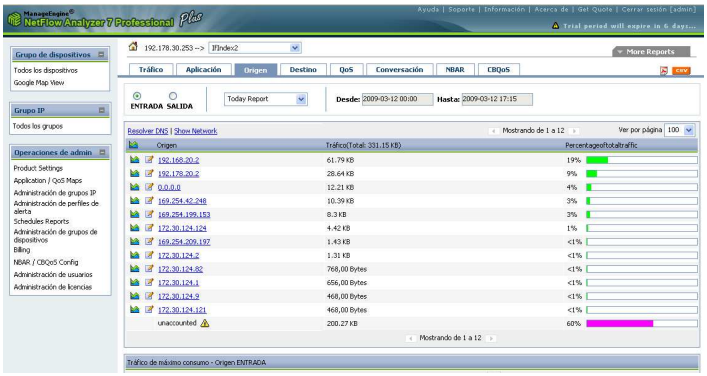


Figura N°V.25 Reporte de trafico de origen (Internet)

La pantalla muestra el top de dispositivos por velocidad, el porcentaje de utilizacion y otras caracteristicas, en el periodo desde las 00:00 del 12 de Marzo del 2009 hasta las 17:17 horas del 12 de Marzo del 2009.

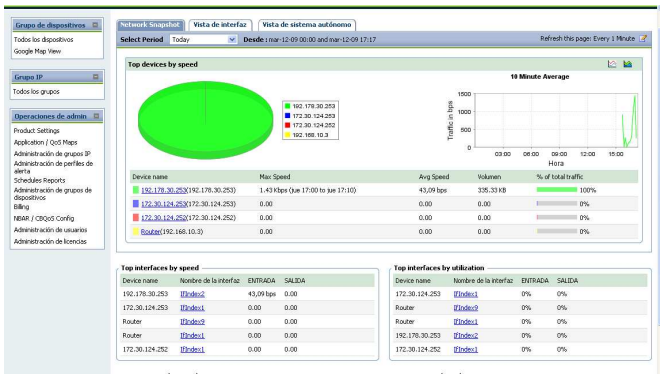


Figura N°V.26 Porcentaje de utilización (Internet)

Se puede observar las interfaces que son analizadas, o que previamente han sido analizadas pero no estan habilitadas, esto se puede observar al dar clic en **Vista de Interfaz.**

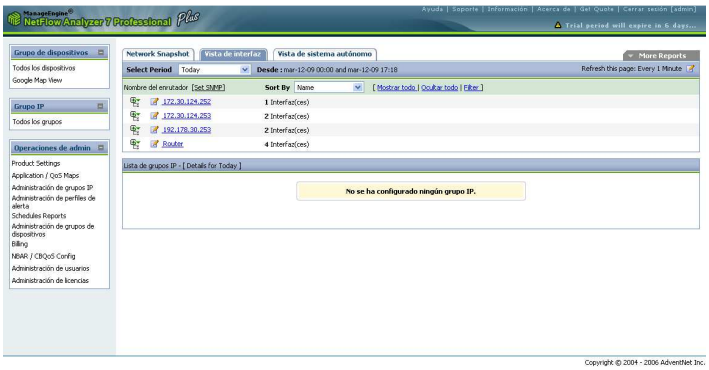


Figura N°V.27 Interfaces analizadas (Internet)

Al dar clic en la interfaz que se este analizando se despliega informacion de flujos recibidos y configuraciones previas para un analisis detallado, en el periodo desde las 00:00 del 12 de Marzo del 2009 hasta las 17:17 horas del 12 de Marzo del 2009.

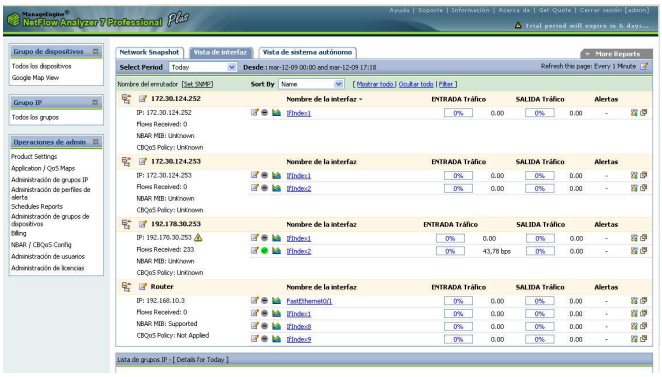


Figura N°V.28 Detalle de las interfaces (Internet)

Esta pantalla muestra el destino del trafico de entrada a la interfaz, es decir muestra la direccion IP y el porcentaje de utilizacion del ancho de banda, esto se puede observar al dar clic en la pestaña **Destino,** todo esto en el periodo desde las 00:00 del 12 de Marzo del 2009 hasta las 17:17 horas del 12 de Marzo del 2009.

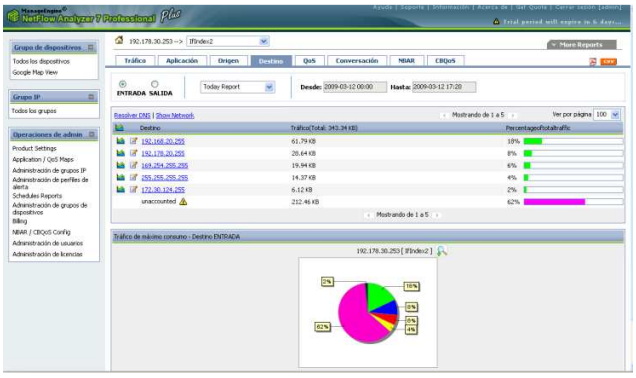


Figura N°V.29 Reporte de trafico de entrada (Internet)

En esta pantalla se pueden observar las conversaciones diarias del trafico de entrada, es decir muestra direccion IP origen, Direccion IP destino, Aplicacion, puerto, protocolo, tamaño, esto se despliega al dar clic en la pestaña **Conversacion,** todo esto en el periodo desde las 00:00 del 12 de Marzo del 2009 hasta las 17:17 horas del 12 de Marzo del 2009.

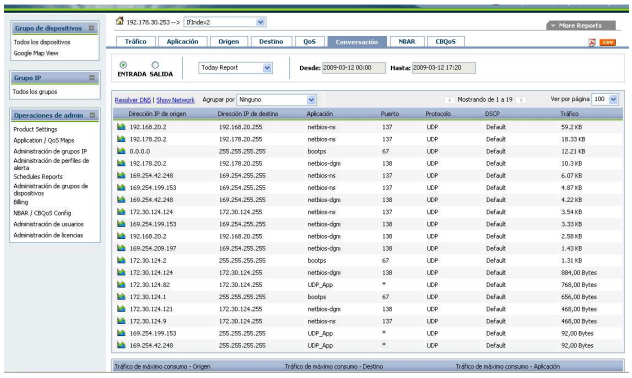


Figura N°V.30 Reporte de conversación (Internet)

Las siguientes pantallas permite observar la creacion de un reporte, esto al dar clic en la pestaña **More reports** de la pagina principal, lo primero que se realiza es dar clic en seleccionar dispositivos, para elegir el dispositivo que se va a monitorear, luego se selecciona el criterio en nuestro caso direccion de origen, en el cuadro de a lado se escribe la direccion de origen de cual se va a generar el reporte, despues de esto se selecciona el periodo desde, hasta y el numero de paginas que se van a mostrar, y clic en **Generar Reporte.** Se visualizara todo el movimiento generado por la maquina.

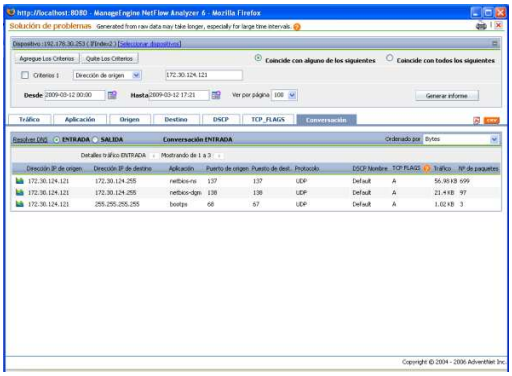


Figura N°V.31 Generaar mas reportes (Internet)

Esta pantalla muestra el grafico de paquetes que estan ingresando por la interfaz. El color verde significa que es el trafico de entrada, y el color azul significa que es el trafico de salida.

Figura N°V.32 Paquetes de entrada (Internet)

Al dar clic en la opcion **Show Network** en la opcion destino, se observan los graficos de las direcciones que mas uso tienen.

En las siguiente pantalla se observan los detalles:

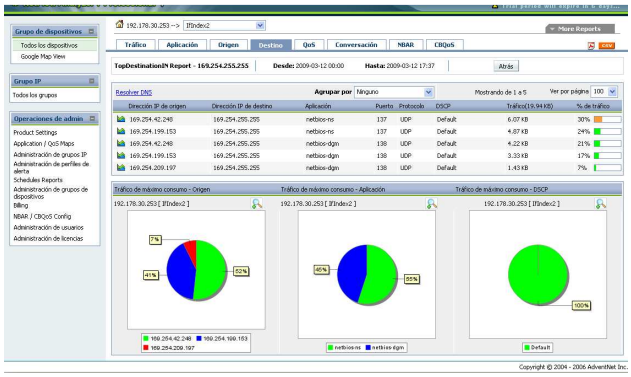


Figura N°V.33 Reporte de direcciones de destino (Internet)

5.1.1.3 En el laboratorio de la EIS

Escenario

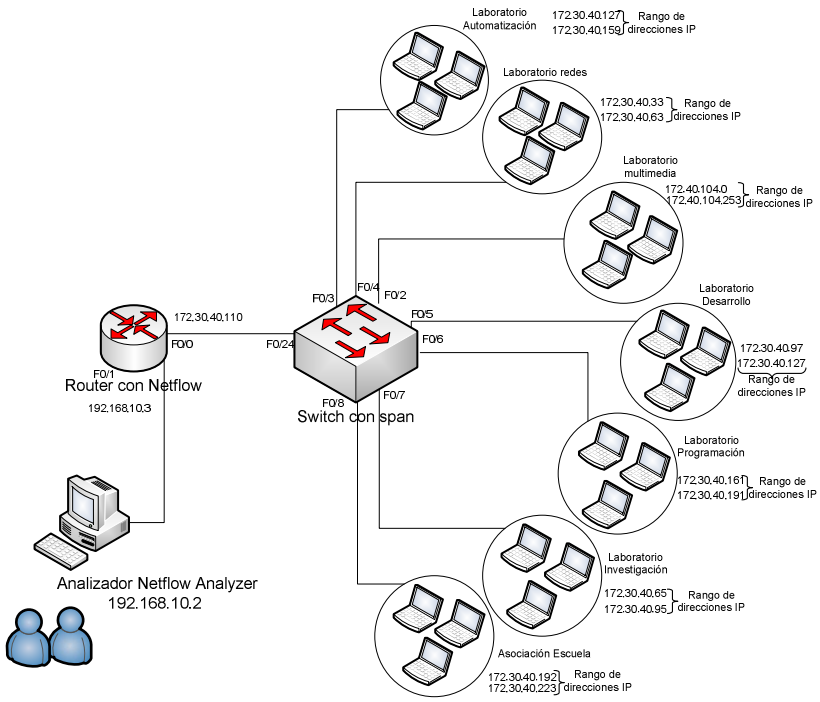


Figura N°V.34 Escenario de la EIS

Descripción

En el laboratorio de sistemas se procedió a implementar una simulación real, la cual consistió en habilitar un puerto en el switch cisco con SPAN, este realizaba una copia completa de todo el tráfico que generan cada uno de los laboratorios de la misma escuela.

El puerto del switch con SPAN fue el 24, este se conectaba a la Fastethernet 0/1 de router 2811, el puerto fastethernet 0/0 se conecta directamente al NetFlowAnalyzer, instalado sobre el sistema operativo SUSE.

De esta manera se inicio el monitoreo respectivo durante dos semanas.

Configuración

Switch Cisco

En el modo de configuración global se crea la sesión para habilitar SPAN.

```
Switch(config)#monitor session 1 source interface fastethernet 0/24

Switch(config)#monitor session 1 destination interface fastethernet 0/0
```

Router 2811

Comandos NetFlow

```
router#enable
router#configure terminal
router-2621(config)#interface FastEthernet 0/0
router-2621(config-if)#ip route-cache flow
router-2621(config-if)#exit
router-2621(config)#ip flow-export destination 192.168.10.2 9996
router-2621(config)#ip flow-export source FastEthernet 0/0
router-2621(config)#ip flow-export version 5
router-2621(config)#ip flow-cache timeout active 1
router-2621(config)#ip flow-cache timeout inactive 15
router-2621(config)#snmp-server ifindex persist
router-2621(config)#^Z
router#write
router#show ip flow export
router#show ip cache flow
```

Creación de Grupos IP en la herramienta de monitoreo NetFlow Analyzer

Para la creación de grupos se accede a la herramienta como usuario administrador, se elige la opción **Grupos IP** en el tab **Operaciones de Admin.**

Primeramente se pone el nombre del grupo IP, debe ser único, luego una descripción para que los próximos administradores sepan porque fue creado, se selección porque tipo va a ser creado el grupo sea por **Dirección IP** o por **puerto o protocolo.**

A continuación, se especifica porque se va a crear:

- IP
- Rango IP
- Red

En nuestro caso seleccionamos por Rango IP, aqui se procede a escribir la mascara de red, la direccion IP origen, y la direccion IP destino.

Si se desea crear mas grupos dar clic en la opcio **AddMore.**

Una vez creados los grupos, dar clic en la opcion **Seleccionar Dispositivos,** para elegir la interface por la cual NetFlow exporta los flujos.

Se crearon grupos para cada laboratorio de la Escuela de Ingenieria en Sistemas.

Creacion del grupo para el Laboratorio de Automatizacion

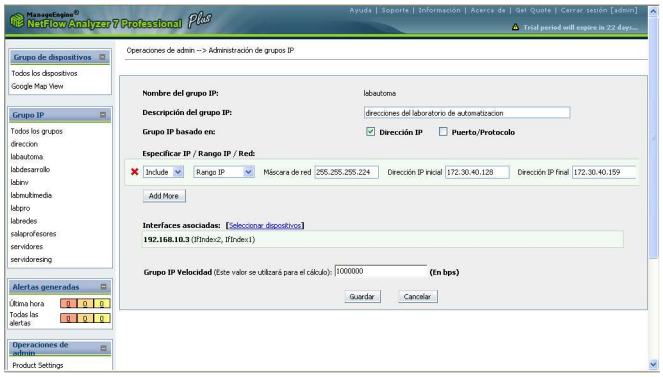


Figura N°V.35 Creación de grupos Laboratorio Autimatización

De igual manera se procedio a la creacion de los grupos para cada laboratorio de la EIS, ademas se creo un grupo para la sala de profesores y otro para el servidor del Ingeniero Danilo Pastor que se encuentra en el laboratorio de los tecnicos.

Resultados Obtenidos

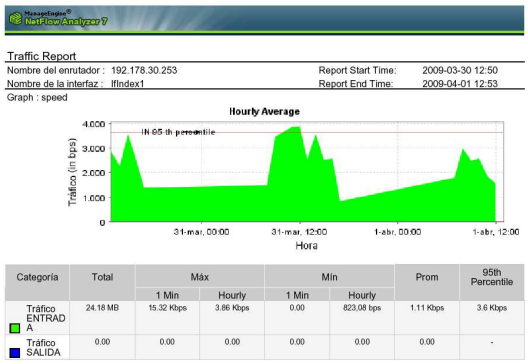
Una vez realizadas las pruebas en el laboratorio de sistemas, se procedió a sacar los reportes necesarios para ofrecer estadísticas del monitoreo realizado. Esto se realizo de cada uno de los laboratorios pertenecientes a la Escuela de Ingeniería en Sistemas

Los reportes obtenidos son:

Martes 31 de marzo del 2009

Reporte de tráfico: Diario

En esta pantalla se observa todo el trafico generado por el switch capa 3, en el grafico podemos observar que el color verde es de entrada y el azul es trafico de salida.

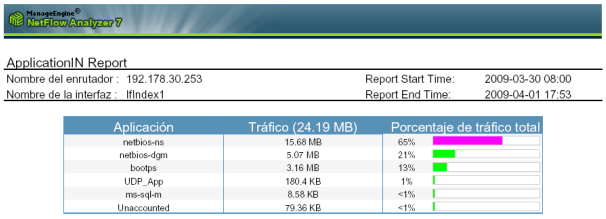


Categoría	Total	Máx		Mín		Prom	95th Percentile
		1 Min	Hourly	1 Min	Hourly		
Tráfico ENTRADA	24.18 MB	15.32 Kbps	3.86 Kbps	0.00	823.08 bps	1.11 Kbps	3.6 Kbps
Tráfico SALIDA	0.00	0.00	0.00	0.00	0.00	0.00	-

Figura N°V.36 Reporte de tráfico (EIS)

Reporte de tráfico de entrada: aplicación

En este reporte se puede observar el porcentaje de tráfico total del top 6 de las aplicaciones más utilizadas en un día.



ApplicationIN Report

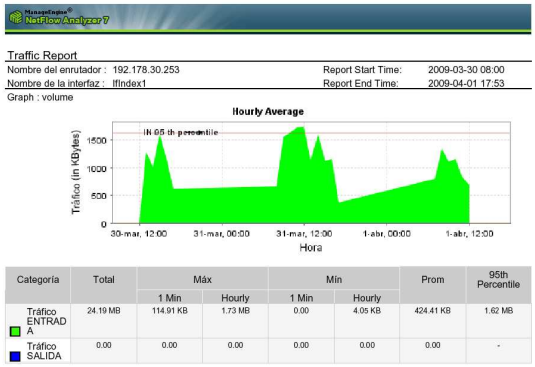
Nombre del enrutador : 192.178.30.253 — Report Start Time: 2009-03-30 08:00
Nombre de la interfaz : IfIndex1 — Report End Time: 2009-04-01 17:53

Aplicación	Tráfico (24.19 MB)	Porcentaje de tráfico total
netbios-ns	15.68 MB	65%
netbios-dgm	5.07 MB	21%
bootps	3.16 MB	13%
UDP_App	180.4 KB	1%
ms-sql-m	8.58 KB	<1%
Unaccounted	79.36 KB	<1%

Figura N°V.37 Reporte del Top N de aplicaciones (EIS)

Reporte de tráfico: volumen

En esta pantalla se observa el grafico del volumen de tráfico en la fecha establecida.



Traffic Report

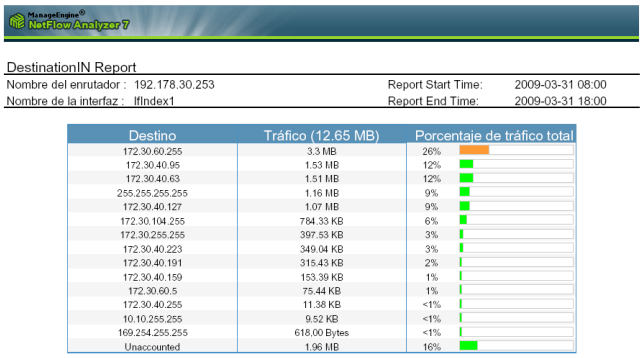
Nombre del enrutador : 192.178.30.253 — Report Start Time: 2009-03-30 08:00
Nombre de la interfaz : IfIndex1 — Report End Time: 2009-04-01 17:53
Graph : volume

Categoría	Total	Máx		Mín		Prom	95th Percentile
		1 Min	Hourly	1 Min	Hourly		
Tráfico ENTRADA	24.19 MB	114.91 KB	1.73 MB	0.00	4.05 KB	424.41 KB	1.62 MB
Tráfico SALIDA	0.00	0.00	0.00	0.00	0.00	0.00	-

Figura N°V.38 Reporte de tráfico por volumen (EIS)

Reporte de entrada (Destino)

En este reporte se puede observar el porcentaje de tráfico total del top 6 de las aplicaciones más utilizadas en un día.



ManageEngine NetFlow Analyzer 7

DestinationIN Report

Nombre del enrutador : 192.178.30.253 — Report Start Time: 2009-03-31 08:00
Nombre de la interfaz : IfIndex1 — Report End Time: 2009-03-31 18:00

Destino	Tráfico (12.65 MB)	Porcentaje de tráfico total
172.30.60.255	3.3 MB	26%
172.30.40.95	1.53 MB	12%
172.30.40.63	1.51 MB	12%
255.255.255.255	1.16 MB	9%
172.30.40.127	1.07 MB	9%
172.30.104.255	784.33 KB	6%
172.30.255.255	397.53 KB	3%
172.30.40.223	349.04 KB	3%
172.30.40.191	315.43 KB	2%
172.30.40.159	153.39 KB	1%
172.30.60.5	75.44 KB	1%
172.30.40.255	11.38 KB	<1%
10.10.255.255	9.52 KB	<1%
169.254.255.255	618.00 Bytes	<1%
Unaccounted	1.96 MB	16%

Figura N°V.39 Reporte de tráfico de destino (EIS)

Reporte de entrada (origen)

En este reporte podemos ver el top N de las direcciones IP más solicitadas que están ingresando al router en un día.

ManageEngine NetFlow Analyzer 7

SourceIN Report

Nombre del enrutador : 192.178.30.253 — Report Start Time: 2009-03-31 08:00
Nombre de la interfaz : IfIndex1 — Report End Time: 2009-03-31 18:00

Origen	Tráfico (12.65 MB)	Porcentaje de tráfico total
172.30.60.181	1.38 MB	11%
172.30.40.80	869.86 KB	7%
172.30.60.197	490.8 KB	4%
172.30.40.122	452.01 KB	4%
172.30.40.126	347.01 KB	3%
172.30.40.74	331.78 KB	3%
172.30.40.58	305.63 KB	2%
172.30.40.219	303.22 KB	2%
0.0.0.0	264.27 KB	2%
172.30.60.187	263.68 KB	2%
172.30.40.53	254.63 KB	2%
172.30.60.190	253.71 KB	2%
172.30.60.22	237.51 KB	2%
172.30.40.222	213.34 KB	2%
172.30.40.36	182.69 KB	1%
172.30.60.21	160.09 KB	1%
172.30.40.48	156.56 KB	1%
172.30.40.132	152.21 KB	1%
172.30.40.35	137.44 KB	1%
172.30.40.46	130.09 KB	1%
172.30.104.79	108.96 KB	1%
172.30.40.42	105.36 KB	1%

Figura N°V.40 Reporte de tráfico de origen (EIS)

Conclusión de las pruebas realizadas

Luego de las pruebas realizadas se pudo concluir que la tecnología NetFlow exporta flujos al analizador el cual saca estadísticas del tráfico, utilización de ancho de banda, protocolos, entre otros.

El router exporto trafico TCP y UDP al analizador debido a que el router envía trafico de la capa 3, pero si se quiere obtener el resto de trafico de las capas superiores como http, la visualización de estos se obtendrá siempre y cuando el router este generando este tráfico, es decir si el router en el que se habilita NetFlow destruye el internet, o genera el enrutamiento entre VLANs todo este tráfico se verá, caso contrario únicamente el de capa 3.

Por tal motivo para obtener todo el trafico real se procedió a implementar la tecnología en el Departamento de Sistemas y Telemática, el cual dispone del switch capa 3 que soporta NetFlow y además genera todo el trafico necesario para obtener estadísticas útiles.

5.2 Escenario en ejecución

DESITEL

Escenario

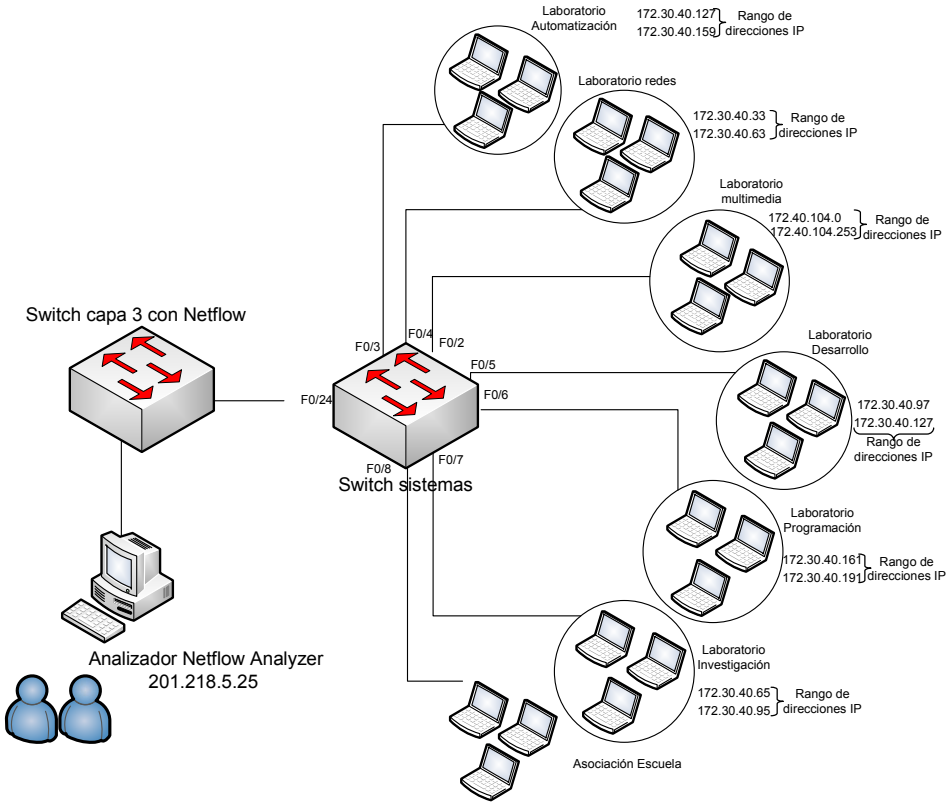


Figura N°V.41 Escenario en ejecución DESITEL

Descripción

Se procedio a configurar el switch capa 3 que se encuentra en DESITEL, una vez habilitado NetFlow, los flujos exportados por el mismo fueron enviados al analizador NetFlow Analyzer 7 al cual se puede acceder desde una maquina de la misma red de la EIS o desde cualquier maquina fuera de la ESPOCH, la direccion IP para acceder a monitorear es 201.218.5.25

Una vez puesta la direccion automaticamente aparece la pagina inicial en la cual nos podemos autenticar como administradores para realizar las operaciones necesarias o como usuarios, este perfil unicamente permite realizar las tareas de monitoreo.

5.3 Resultados Obtenidos

REPORTE MENSUAL DE LA ESCUELA DE INGENIERIA EN SISTEMAS

Para la obtención de datos hemos realizado el monitoreo de la red de la escuela de ingeniería en sistemas desde el 10 de Abril al 10 de Mayo del 2009. Hemos utilizado como técnica de análisis de Flujo ip Netflow y como herramienta de monitoreo NetFlow Analyzer, mediante las opciones de reportes personalizados de NetFlow Analyzer hemos podido obtener las siguientes pantallas.

Tráfico

El gráfico nos muestra en reporte del Tráfico de la escuela de ingeniería en sistemas, podemos observar la cantidad de paquetes que se han recogido durante un mes de entrada son 7.367162231E8 y de salida 5.63753904E8. Teniendo como un máximo de 60.000.000 paquetes recolectados en un tiempo determinado.

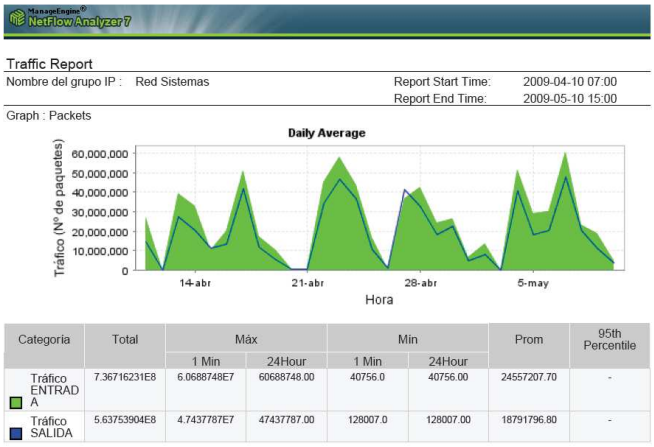


Figura N°V.42 Reporte de tráfico (DESITEL)

Aplicación entrada.

Tenemos el reporte de aplicaciones de entrada donde se muestran las primeras aplicaciones que hacen uso en la red de la escuela de ingeniería en sistemas, podemos ver que con mucha diferencia la que más se utiliza es la aplicación http con un valor de 508,46GB que corresponde al 26% de las aplicaciones totales que monitorea NetFlow Analyzer.

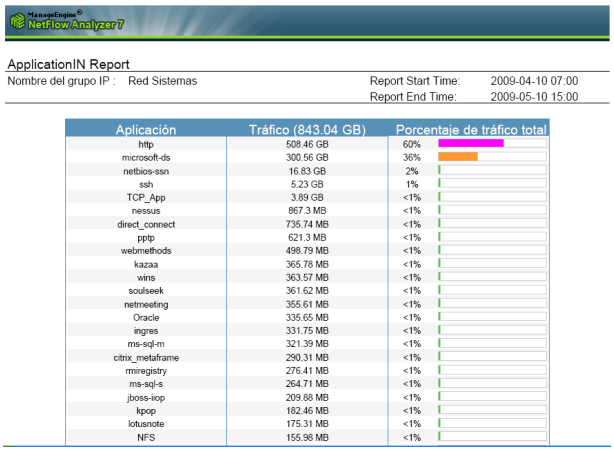
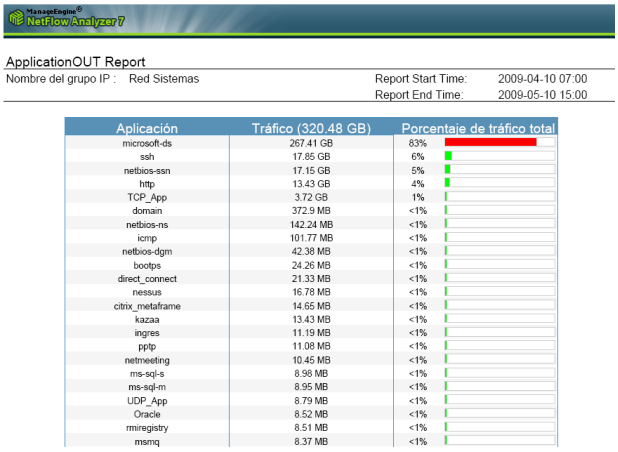


Figura N°V.43 Reporte aplicación de entrada (DESITEL)

Aplicación salida.

Podemos observar las primeras aplicaciones de salida que monitorea Netflow Analyzer, la que mayor uso hace de la red es Microsoft-ds con un valor de 267,41GB que corresponde al 83%.



ManageEngine® NetFlow Analyzer 7

ApplicationOUT Report

Nombre del grupo IP : Red Sistemas

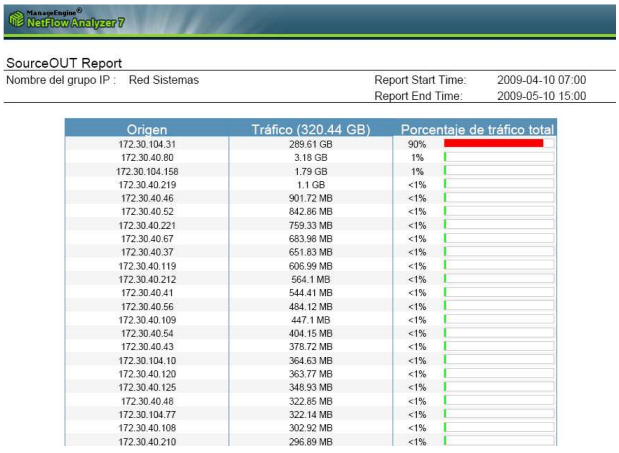
Report Start Time: 2009-04-10 07:00
Report End Time: 2009-05-10 15:00

Aplicación	Tráfico (320.48 GB)	Porcentaje de tráfico total
microsoft-ds	267.41 GB	83%
ssh	17.85 GB	6%
netbios-ssn	17.15 GB	5%
http	13.43 GB	4%
TCP_App	3.72 GB	1%
domain	372.9 MB	<1%
netbios-ns	142.24 MB	<1%
icmp	101.77 MB	<1%
netbios-dgm	42.38 MB	<1%
bootps	24.26 MB	<1%
direct_connect	21.33 MB	<1%
nessus	16.78 MB	<1%
citrix_metaframe	14.65 MB	<1%
kazaa	13.43 MB	<1%
ingres	11.19 MB	<1%
pptp	11.08 MB	<1%
netmeeting	10.45 MB	<1%
ms-sql-s	8.98 MB	<1%
ms-sql-m	8.95 MB	<1%
UDP_App	8.79 MB	<1%
Oracle	8.52 MB	<1%
rmiregistry	8.51 MB	<1%
msmq	8.37 MB	<1%

Figura N°V.44 Reporte de aplicación de salida (DESITEL)

Direcciones Origen.

En el reporte observamos las primeras direcciones que originan mayor tráfico en la red de la escuela de ingeniería en sistemas, tenemos en primer lugar con valor de 289,61GB que corresponde al 90% tenemos la dirección 172.30.104.31.



ManageEngine® NetFlow Analyzer 7

SourceOUT Report

Nombre del grupo IP : Red Sistemas

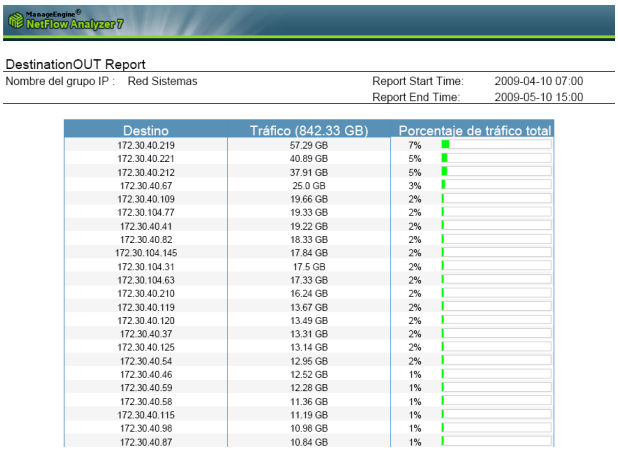
Report Start Time: 2009-04-10 07:00
Report End Time: 2009-05-10 15:00

Origen	Tráfico (320.44 GB)	Porcentaje de tráfico total
172.30.104.31	289.61 GB	90%
172.30.40.80	3.18 GB	1%
172.30.104.158	1.79 GB	1%
172.30.40.219	1.1 GB	<1%
172.30.40.46	901.72 MB	<1%
172.30.40.52	842.86 MB	<1%
172.30.40.221	759.33 MB	<1%
172.30.40.67	683.98 MB	<1%
172.30.40.37	651.83 MB	<1%
172.30.40.119	606.99 MB	<1%
172.30.40.212	564.1 MB	<1%
172.30.40.41	544.41 MB	<1%
172.30.40.56	484.12 MB	<1%
172.30.40.109	447.1 MB	<1%
172.30.40.54	404.15 MB	<1%
172.30.40.43	378.72 MB	<1%
172.30.104.10	364.63 MB	<1%
172.30.40.120	363.77 MB	<1%
172.30.40.125	348.93 MB	<1%
172.30.40.48	322.85 MB	<1%
172.30.104.77	322.14 MB	<1%
172.30.40.108	302.92 MB	<1%
172.30.40.210	296.89 MB	<1%

Figura N°V.45 Reporte de direcciones de origen (DESITEL)

Direcciones Destino.

En el reporte observamos las primeras direcciones a donde se dirige el tráfico en la red de la escuela de ingeniería en sistemas, en primer lugar con un valor de 57,29GB que corresponde al 7% tenemos la dirección 172.30.40.219.



DestinationOUT Report

Nombre del grupo IP : Red Sistemas

Report Start Time: 2009-04-10 07:00
Report End Time: 2009-05-10 15:00

Destino	Tráfico (842.33 GB)	Porcentaje de tráfico total
172.30.40.219	57.29 GB	7%
172.30.40.221	40.89 GB	5%
172.30.40.212	37.91 GB	5%
172.30.40.67	25.0 GB	3%
172.30.40.109	19.66 GB	2%
172.30.104.77	19.33 GB	2%
172.30.40.41	19.22 GB	2%
172.30.40.82	18.33 GB	2%
172.30.104.145	17.84 GB	2%
172.30.104.31	17.5 GB	2%
172.30.104.63	17.33 GB	2%
172.30.40.210	16.24 GB	2%
172.30.40.119	13.67 GB	2%
172.30.40.120	13.49 GB	2%
172.30.40.37	13.31 GB	2%
172.30.40.125	13.14 GB	2%
172.30.40.54	12.95 GB	2%
172.30.40.46	12.52 GB	1%
172.30.40.59	12.28 GB	1%
172.30.40.58	11.36 GB	1%
172.30.40.115	11.19 GB	1%
172.30.40.98	10.98 GB	1%
172.30.40.87	10.84 GB	1%

Figura N°V.46 Reporte de direcciones de destino (DESITEL)

5.4 Análisis de los Resultados

Comprobacion de la hipotesis

Hipótesis general:

La aplicación de las TÉCNICAS DE ANÁLISIS DE FLUJOS IP en la red de la Escuela de Ingeniería en sistemas, permitirá realizar un mejor monitoreo y determinar de una manera más detallada las aplicaciones y los usuarios que mayor uso hacen de la red.

Variables

Independiente: La aplicación de las TÉCNICAS DE ANÁLISIS DE FLUJOS IP en la red de la Escuela de Ingeniería en sistemas.

Dependiente: aplicaciones, usuarios, monitoreo.

Demostración por un análisis cuantitativo.

Población: se tomo como población la Facultad de informática y electrónica de la Escuela Superior Politécnica de Chimborazo a partir de la cual se seleccionara la muestra.

Muestra: para realizar la comprobación de la hipótesis planteada hemos tomado como muestra la escuela de ingeniería en sistemas los cuales se encuentran clasificados según laboratorios como vemos en el siguiente gráfico por un tiempo de monitoreo de un mes, desde el 10 de abril del 2009 al 10 de Mayo del 2009.

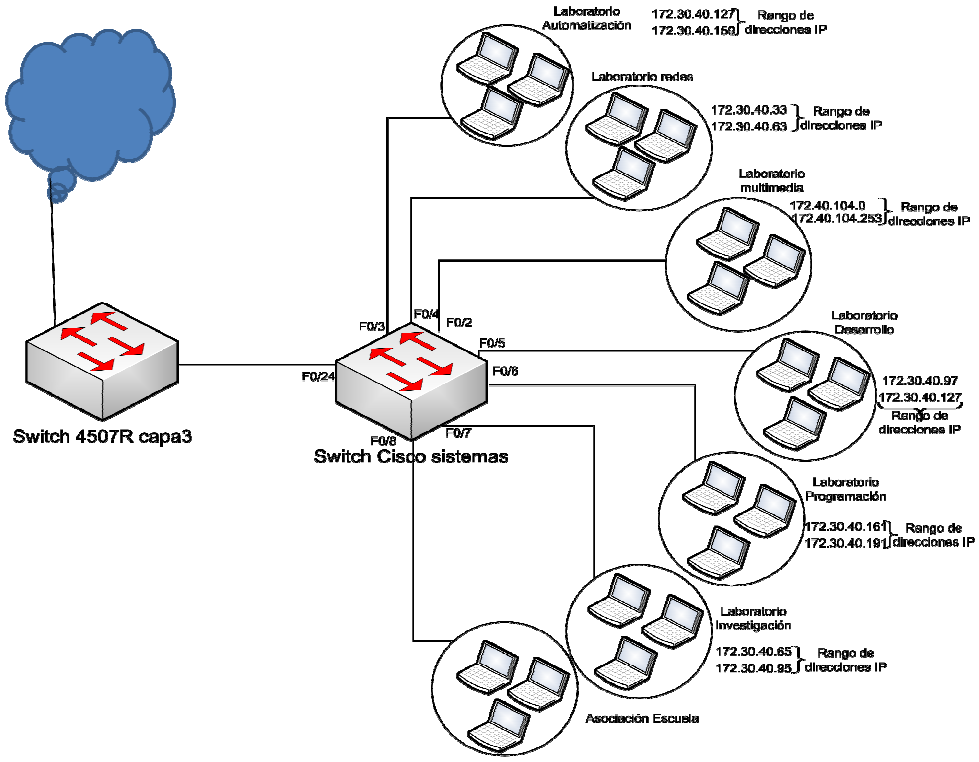


Figura N°V.47 Escenario DESITEL

Monitoreo de la red de la escuela de sistemas sin la herramienta NetFlow Analyzer?

En la actualidad los técnicos de la escuela de ingeniería en sistemas no realizan un monitoreo de flujo ip de las máquinas que dispone la escuela, únicamente realizan un control de la utilización de

cada uno de los laboratorios mediante una identificación entregada por cada uno de los estudiantes en horas no clase y una reservación previa del profesor en horas clase.

Monitoreo de la red de la escuela de sistemas con la Herramienta NetFlow Analyzer?

Mediante la utilización de la herramienta Netflow Analyzer los técnicos de la EIS pueden realizar un monitoreo de la red de manera precisa, podrá observar mediante gráficos que ancho de banda ocupa cada una de las máquinas y en que laboratorio se encuentra, así como también podrá ver el tiempo que cada máquina permanece encendida, y a donde está realizando las peticiones, puede observar estadísticas de las aplicaciones y maquinas que mayor uso hacen de la red, y lo más importante puede detectar anomalías que se pueden presentar en cada uno de los laboratorios y con ello prevenir posibles ataques masivos.

Permitirá realizar reportes planteados en la herramienta así como reportes personalizados en el momento que este requiera.

Para el monitoreo se instalo la herramienta NetFlow Analyzer en un servidor bajo sistema operativo Suse, al cual se puede acceder en la intranet de la Espoch mediante la dirección http://172.30.60.25:8080 y fuera de la espoch mediante la dirección http://201.218.5.25:8080.

Esta aplicación toma los flujos enviados por el switch capa3 4507R donde se ha configurado la técnica de análisis de flujo ip NetFlow.

Estadísticas de aplicaciones que monitorea NetFlow Analyzer?

Hemos considerado de un totol de 100 aplicaciones las10 más usadas tanto de entrada como de salida del switch, considerando las aplicaciones de entrada como las peticiones que cada máquina hace al switch, y las aplicaciones de salida como las respuestas que el switch envía a cada una de los equipos de la red.

Aplicación de Entrada

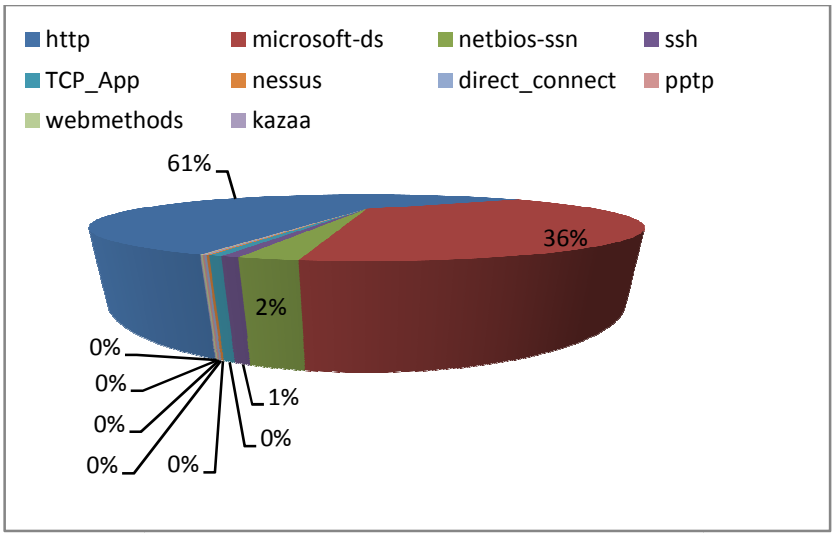


Figura N°V. 48 Top 10 de las aplicaciones de entrada (Hipótesis)

En el gráfico podemos observar cuales son las 10 aplicaciones de entrada que más se utilizan en la red de la escuela de Ingeniería en sistemas, los datos se encuentran graficados en MB por lo que los valores dados en GB han sido transformados a MB.

Con un valor de 508,46GB que corresponde al 61% http, con un valor de 300,56GB que corresponde al 36% Microsoft-ds, con un valor de 16,83GB que corresponde al 2% netbios-ssn, con un valor de 5,23GB que corresponde al 1% ssh, y las aplicaciones TCP_App, nessus, direct_connect, pptp, webmethods y kazaa corresponden valores del 0% .

Podemos concluir que la aplicación de entrada que más se utiliza en la red de la escuela de ingeniería en sistemas es http.

Aplicación Salida

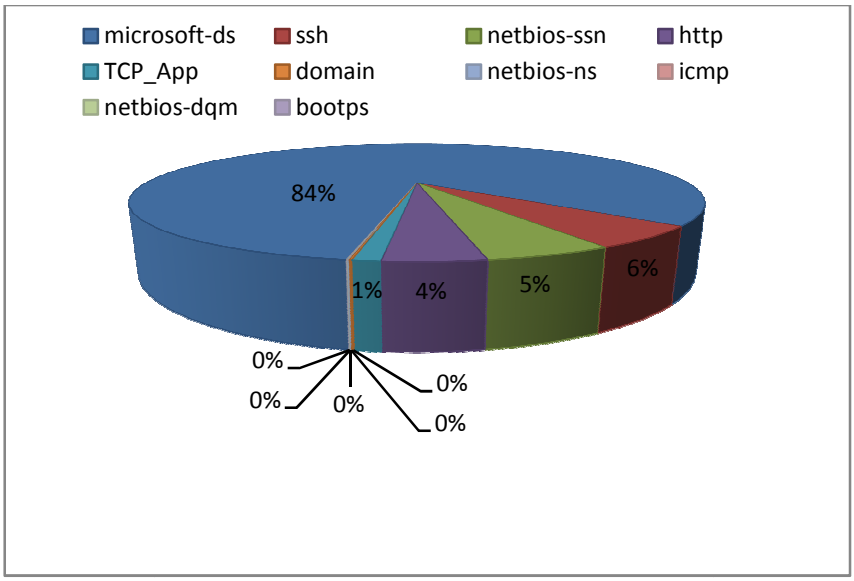


Figura N°V. 49 Top 10 de las aplicaciones de salida (Hipótesis)

En el gráfico podemos observar cuales son las 10 aplicaciones de salida que más se utilizan en la red de la escuela de Ingeniería en sistemas, los datos se encuentran graficados en MB por lo que los valores dados en GB han sido transformados a MB.

Con un valor de 267,41GB que corresponde al 84% micosoft-ds, con un valor de 17,85GB que corresponde al 6% ssh, con un valor de 17,15GB que corresponde al 5% netbios-ssn, con un valor de 13,43GB que corresponde al 4% http, con un valor de 3,72GB que corresponde al 1% TCP_App y las aplicaciones domain, netbios-ns, icmp, netbios-dqm y bootps corresponden valores del 0%.

Podemos concluir que la aplicación de salida que más se utiliza en la red de la escuela de ingeniería en sistemas es Microsoft-ds.

Estadísticas de usuarios que monitorea NetFlow Analyzer?

Para los datos de Usuarios hemos realizado gráficos estadísticos de las 10 usuarios que mayor uso hacen de a red tanto de origen como de destino, siendo el origen la dirección donde cada pc

envía sus peticiones, y siendo el destino las maquinas de cada laboratorio a las que el switch envía respuestas..

Origen

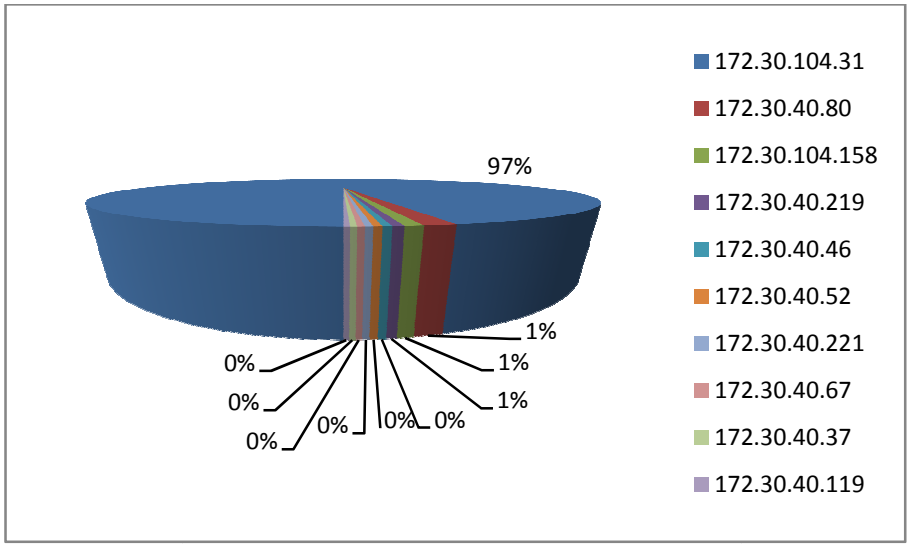


Figura N°V.50 Top 10 de las direcciones origen (Hipótesis)

En el gráfico podemos observar cuales son los 10 usuarios que más se utilizan en la red de la escuela de Ingeniería en sistemas, los datos se encuentran graficados en MB por lo que los valores dados en GB han sido transformados a MB.

Con un valor de 289,61GB que corresponde al 97% tenemos la dirección de 172.30.104.31, que corresponde al laboratorio de Investigación la PC#1 y que es un servidor de Software, con un valor de 3,18GB que corresponde al 1% 172.30.40.80 que pertenece al laboratorio de investigación PC#2 y es un servidor de aplicaciones, con un valor de 1,79GB que corresponde al 1% 172.30.104.158 perteneciente al laboratorio de Multimedia, con un valor de 1,1GB que corresponde al 1% 172.30.40.219 perteneciente a la asociación de escuela de ingeniería en sistemas, y las direcciones 172.30.40.46 , 172.30.40.52, 172.30.40.221, 172.30.40.67, 172.30.40.37 y la dirección

172.30.40.119 contienen valores que corresponden al 0% de los 10 usuarios que mayor uso hacen de la red.

Podemos concluir que la dirección origen que más se utiliza en la red de la escuela de ingeniería en sistemas es 172.30.104.31 del laboratorio de Investigación.

Destino

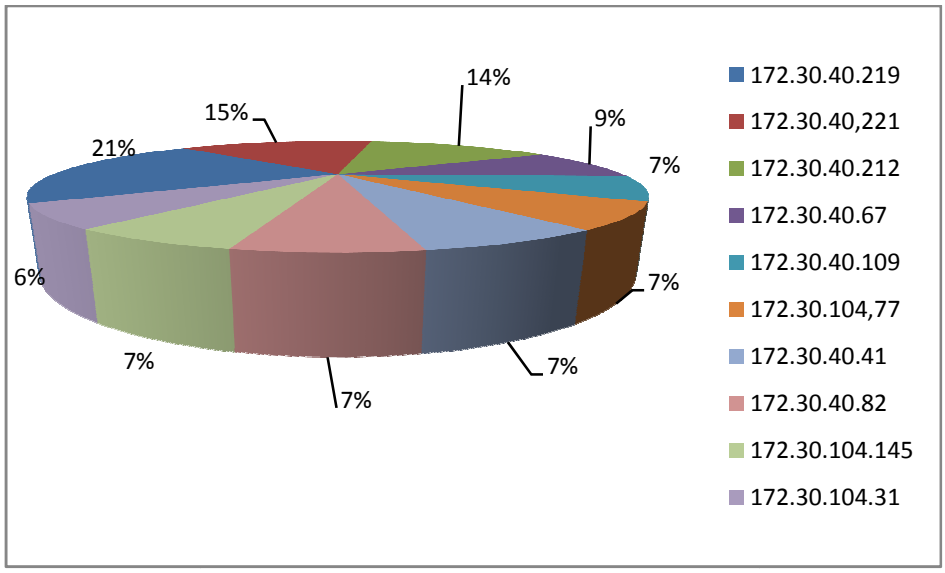


Figura N°V.51 Top 10 de las direcciones destino (Hipótesis)

En el gráfico podemos observar cuales son los 10 destinos que más se utiliza en la red de la escuela de Ingeniería en sistemas, los datos se encuentran graficados en GB.

Con un valor de 57,29GB que corresponde al 21% tenemos la dirección de 172.30.40.219, que corresponde a la red de la asociación de escuela, con un valor de 40,89GB que corresponde al 15% 172.30.40.221 que pertenece a la red de la asociación de escuela, con un valor de 37,91GB que corresponde al 14% 172.30.40.212 perteneciente a la asociación de escuela, con un valor de 25,0GB que corresponde al 9% 172.30.40.67 perteneciente al laboratorio de Investigación, con un valor de 19,66GB que corresponde al 7% 172.30.40.109 perteneciente a la asociación de escuela, con un valor de 19,33GB que corresponde al 7% 172.30.40.77 perteneciente al laboratorio de

Investigación, con un valor de 19,22GB que corresponde al 7% 172.30.40.41 perteneciente al laboratorio de Redes, con un valor de 18,83GB que corresponde al 7% 172.30.40.82 perteneciente al laboratorio de investigación, con un valor de 17,84GB que corresponde al 7% 172.30.104.145 perteneciente a la red de Multimedia, con un valor de 17,5GB que corresponde al 6% 172.30.104.31 perteneciente al laboratorio de multimedia.

Podemos concluir que la dirección destino que más se utiliza en la red de la escuela de ingeniería en sistemas es 172.30.40.219 perteneciente a la asociación de escuela de ingeniería en sistemas.

Podemos concluir mediante los análisis realizados que la hipótesis planteada es verdadera.

CONCLUSIONES

- El contar con conocimiento detallado sobre el tráfico regular que envían los usuarios de red en un momento establecido y realizar la visualización correcta y apropiada de los resultados, permite detectar posibles ataques a determinados equipos de la red, ayudan al administrador y de esta manera ayudar a los técnicos tomar decisiones correctivas y preventivas.
- Una vez estudiadas las técnicas de análisis de Flujo IP concluimos que cada una de las tecnologías presentan ventajas, sin embargo se eligió NetFlow por desempeño, disponibilidad, y principalmente porque nos permite monitorizar las redes a nivel de capa de enlace de datos y de transporte.
- Elegida la tecnología de análisis de Flujo IP, procedimos a seleccionar la herramienta que mejor se ajusto a los requerimientos establecidos, siendo esta NetFlow Analyzer ya que incluye una gran variedad de características que son útiles para la gestión de datos NetFlow, genera informes detallados del trafico total, aplicaciones, usuarios que mayor uso hacen del ancho de banda, posee una interfaz amigable y fácil de utilizar para los usuarios.
- Durante el desarrollo de la tesis se realizaron una variedad de pruebas, simulando escenarios tanto en el laboratorio de cisco, como en sistemas empleando SPAN con trafico real, se obtuvieron resultados únicamente de capa 3, debido a que el router que se uso no generaba el enrutamiento ni proporcionaba internet, era únicamente el paso del SPAN al analizador, por tal motivo se procedió a implementar el escenario final en DESITEL, configurando NetFlow en el switch capa 3 4507 R, NetFlow Analyzer como herramienta de monitorización instalada en un equipo con SUSE como sistema operativo, obteniendo una aplicación que genera informes de tráfico en tiempo real.
- Los resultados obtenidos mediante los reportes personalizados de la herramienta se pueden considerar fundamental para la creación de futuras políticas de seguridad y estrategias para un mejor control, ya que consideramos registros importantes y confiables obtenidos de la infraestructura de red.

- Durante el monitoreo realizado por NetFlow Analyzer en un mes se obtuvieron resultados de vital importancia para la gestión de la red, siendo la aplicación de entrada más usada por parte de los usuarios finales http con el 60%, 83% Microsoft-ds como la más utilizada de las aplicaciones de salida, estos datos son en relación al porcentaje de tráfico total.
- Monitorear la red de la EIS, con la herramienta seleccionada permite además al administrador y técnicos de la misma tener un control detallado del top N de los usuarios potenciales de cada uno de los laboratorios o de la escuela en general, siendo este el usuario con la dirección IP 172.30.40.219, ocupando el 7% del porcentaje del trafico total y la dirección IP mas peticionada es 172.30.104.31 usando el 90% del ancho de banda total, esta dirección es el servidor de descargas que es empleado para que los estudiantes no soliciten directamente al switch capa 3 del DESITEL.
- Finalmente, concluimos que esta solución permite realizar un proceso de gestión y dimensionado, optimización de recursos, automatizar y acelerar los procesos que dificultan al usuario final y a los técnicos en la obtención de información.

RECOMENDACIONES

- Se recomienda considerar la versió la herramienta a utilizar y los sistemas operativos que esta soporta para tener un correcto funcionamiento,
- Investigar sobre la disponibilidad de equipos en la empresa o institución para tener un ambiente propicio al momento de tomar decisiones.
- La realización de pruebas permite tener una idea clara de cómo responden los equipos y la configuración en el campo real, por lo que recomendamos se la realice de forma precisa.
- Investigar toda la información existente sobre equipos y tecnologías ya que de ello depende tomar la mejor decisión.
- Estudiar todas las ventajas que presenta la herramienta empleada para utilizarla al máximo.
- Es recomendable que los administradores usen el mapa de aplicaciones para observar los patrones que se están generando.

RESUMEN

Comparar técnicas de análisis de flujo IP, ɴetFlow, sFlow, IPFIX en la red de la Escuela de Ingeniería en Sistemas (EIS) de la Escuela Superior Politécnica de Chimborazo (ESPOCH), aprovechando las ventajas de éstas, para la prestación de servicios de monitoreo, determinando detalladamente las aplicaciones y usuarios que mayor uso hacen de la red para seleccionar la mejor e implementar un control en tiempo real.

Se utilizó equipos ciscos existentes en el Departamento de Sistemas y Telemática (DESITEL) de la ESPOCH y un servidor de aplicaciones, método investigación deductivo y técnicas de entrevista y observación, las tecnologías estudiadas solucionan problemas de tráfico, los parámetros a comparar fueron cantidad de datos y disponibilidad.

Cantidad de datos: NetFlow exporta de pequeñas a grandes cantidades, sFlow grandes cantidades, IPFIX desde pequeñas a grandes cantidades, teniendo NetFlow e IPFIX valor de 8 y sFlow un valor de 4 en una escala de 0 – 10, Disponibilidad: la ESPOCH dispone de equipos Cisco que soportan NetFlow, teniendo una valoración de 10. Optamos NetFlow porque permite ver trafico de la capa de enlace, capa de transporte, rentabilidad y optimización de recursos, se descarto sFlow ya que permite ver únicamente trafico de capa de enlace, se descarto IPFIX porque no dispone de altos niveles de seguridad, se instalo NetFlow Analyzer como herramienta de monitoreo por su interfaz amigable y generación de informes detallados de tráfico.

Del monitoreo durante un mes obtuvimos que la aplicación de entrada más utilizada fue http con un 61%, de salida Microsoft-ds con 6%, dirección origen 172.30.104.31 con 97%, dirección destino 172.30.40.219 con 21%.

Mediante el análisis y monitoreo se tiene control sobre aplicaciones y usuarios que mayor uso hacen del ancho de banda. Recomendándose realizar actualizaciones y la utilización de esta herramienta al implementar políticas de seguridad y estrategias para un mejor control interno.

SUMMARY

GLOSARIO

Monitoreo: El término monitoreo de red describe el uso de un sistema que constantemente supervisa una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla.

Aplicaciones: Programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.

Usuarios: Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona.

Red: Conjunto de equipos y dispositivos periféricos conectados entre sí. Se debe tener en cuenta que la red más pequeña posible está conformada por dos equipos conectados.

Servidores: Equipos que brindan recursos compartidos para los usuarios mediante un servidor de red.

Ancho de banda: Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).

PC: (derivado de las palabras inglesas Personal Computer), es la expresión estándar que se utiliza para denominar a las computadoras personales en general.

Topología: Es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta.

Dispositivo: Son estructuras sólidas, electrónicas y mecanicas las cuales son diseñadas para un uso especifico, estos se conectan entre sí para crear una conexión en común y obtener los resultados esperados siempre y cuando cumplan con las reglas de configuración.

Memoria: Espacio de trabajo del computador (físicamente es una colección de chips RAM). La memoria es un recurso importante, ya que determina el tamaño y el número de programas que

pueden ejecutarse al mismo tiempo, así como también la cantidad de datos que pueden procesarse instantáneamente.

Protocolo: Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

Router: Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios hosts.

TCP: (Transmission Control Protocol - Protocolo de Control de Transmisión). Se trata del protocolo más usado de internet.

ICMP:(Internet Control Message Protocol - Protocolo de Control de Mensajes de Internet). Subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP). Es utilizado para enviar mensajes de errores cuando un servicio no está disponible o cuando un host no puede ser encontrado, etc.

UDP: (User Datagram Protocol - Protocolo de Datagrama de Usuario). Protocolo abierto, no orientado a la conexión (como el TCP) y por lo que no establece un diálogo previo entre las dos partes, ni tampoco mecanismos de detección de errores.

SNMP: Simple Network Management Protocol - Protocolo simple de administración de red). Protocolo que permite supervisar, analizar y comunicar información de estado entre una gran variedad de hosts.

Enrutamiento: En redes de computadora, enrutamiento (o routing o encaminamiento) se refiere a la selección del camino en una red de computadoras por donde se envían datos.

Paquete de red: En redes de computadora, cada uno de los bloques en que se divide la información que se envía a través de una red en el nivel de red del modelo OSI. Por debajo de este nivel el paquete adquiere el nombre de trama de red.

Proxy web: Un proxy web es utilizado para interceptar la navegación de páginas web por motivos de seguridad, anonimato, rendimiento, etc.

Puerto de red: Interfaz para comunicar programa a través de una red.

Cisco Systems: Compañía global con sede en San Jose, California (EE.UU.). Diseña y vende tecnología y servicios de red como ser: routers (enrutadores), switches (conmutadores), hubs, cortafuegos, productos de telefonía IP, software de gestión de red como CiscoWorks.

Software: En computación, todo programa o aplicación, programado para realizar tareas específicas.

Interface: Es el puerto por el cual se envían o reciben señales desde un sistema hacia otros. Por ejemplo, el interfaz USB, interfaz SCSI, interfaz IDE, interfaz puerto paralelo o serial, etc.

Algoritmo: Conjunto finito de instrucciones para llevar a cabo una tarea. Constan de pasos finitos, no ambiguos y, de ser posible, eficientes.

Vlan: Se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación.

BIBLIOGRAFIA

[1] Adventnet, NetFlow Analyzer, [en linea], 20/11/2008, http://demo.netflowanalyzer.com/

[2] Adventnet, NetFlow Analyzer, [en linea], 20/11/2008, http://www.netflowanalyzer.com/download.html.

[3] BONET Jordi, Aplicación web para monitorizar tráfico en router Cisco con NetFlow, [en linea], 20/11/2008, http://scrutinizer-netflow-sflow.sofnic.com/#

[4] BRASSEL Daniel, Una solución para obtener información sobre estado y trafico de enlaces, [en linea], 20/10/2008, http://www.cnc.una.py/

[5] BELLIDO Luis, Sflow, [en línea], 20/10/2008, TUhttp://www.sflow.orgUT

FERNÁNDEZ David, Flow-tools, [en línea], 20/10/2008, TUhttp://www.splintered.net/sw/flow-toolsUT

[6] GALAN Fermín, MIRA: Plataforma de monitorización y análisis de trafico para redes IP, [en línea], 20/10/2008, http:// www.universidadcarlosIII.com/area_ingenieria/mira/

[7] GARCIA Jose, Utilidad de los flujos NetFlow de RedIRIS para análisis de una red académica, http://www.networking.com/researchgroup/utilidad-netflow/, 20/11/2008

[8] GEROMETTA Oscar, Analisis NetFlow, [en linea],20/11/2008, http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

[9] IETF, IP Flow Information Export (IPFIX) Charter, TUhttp://www.ietf.org/html.charters/ipfix-charter.htmlUT.

[10] IETF, Realtime Traffic Flow Measurement (RTFM) Charter, [en línea], 20/10/2008,

TUhttp://www.ietf.org/html.charters/OLD/rtfm-charter.htmlUT

[11] IETF, Packet Sampling (IETF) Charter, [en línea], 20/10/2008, http://www.ietf.org/html.charters/psamp-charter.htmlUT

[12] Jon Mills, Scrutinizer NetFlow & sFlow Analyzer, [en línea], 26/11/2008, http://www.plixer.com/products/free-netflow.php

[13] LOPEZ David, Monitorización de una red académica mediante NetFlow, [en línea], 20/10/2008, http://www.ietf.org/html.charters/rmonmib-charter.html

[14] Network / Systems ,sFlow, [en línea],26/11/2008, http://wwwietf.org/rfc/rfc3176.txt

[15] SHARING Do, NetFlow, [en línea],20/11/2008, http://docsharing.es/2007/12/09/monitorizacion-de-redes-y-analisis-del-trafico-mediante-cisco-netflow/

[16] VICENTE Carlos, Servicios de Red, [en línea], 20/11/2008, http://www.cisco.com/univercd/cc/td/doc/cisictwk/intsolns/netflsol/nfwhite.htm

[17] Welcher, Peter J, "NetFlow collects traffic data; IPFIX standardizes NetFlow", [en línea] 20/01/2009, http://findarticles.com/p/articles/mi_qa4137/is_200510/ai_n15742499

[18] Welcher, Peter J, Análisis y monitoreo de redes, [en línea], 20/11/2008, http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html

ANEXOS

ANEXO 1: DESCRIPCION DE LA ERRAMIENTA NETFLOW ANALYZER

NETFLOW ANALYZER 7

Introducción a NetFlow Analyzer 7

ManageEngine NetFlow Analyzer es una herramienta de monitoreo de ancho de banda basado en la web, realiza un análisis de trafico profundo con datos exportados en forma de flujos desde NetFlow™ / Netstream™ / cflowd™ / J-Flow™ / sFlow™ / IPFIX™.

Estos datos proporcionan detalles acerca del tráfico de red que está pasando a través de una interfaz.

NetFlow Analyzer procesa esta información para permitir ver que aplicaciones están usando el ancho de banda, quien está usando y donde. Los gráficos y reportes hacen que esta información sea fácil para analizar y para solucionar problemas.

A continuación se procederá a describir paso a paso la herramienta y a familiarizarse con la misma.

Arrancar y Apagar

Iniciando NetFlow Analyzer

Windows:

Clic en **Inicio > Programas > ManageEngine NetFlow Analyzer 7 > NetFlow Analyzer 7** para empezar el servicio.

Alternativamente se puede navegar en la carpeta <*NetFlowAnalyzer_Home*>*bin* e invocar el archivo **run.bat**.

Linux:

Navegar en el directorio <*NetFlow Home*>*/bin y ejecutar el archivo* **run.sh**.

Cuando empieza el servidor, un comando se abre en el prompt de Windows el cual permite iniciar la información en los módulos del NetFlow Analyzer. Primeramente todos los módulos han sido creados satisfactoriamente, el siguiente mensaje aparecerá:

Server started.

El cliente se conecta poniendo en el navegador Web lo siguiente http://localhost:8080

Donde 8080 es el puerto que se especifica durante la instalación para el servidor Web.

Empezando como servicio

Windows:

Si se escogió la opción Start as Service durante la instalación, NetFlow Analyzer correrá como servicio en Windows.

Linux:

1. Iniciar como usuario root.
2. Navegar en el directorio <*NetFlowAnalyzer_Home*>*bin*.
3. Ejecutar el archivo **linkAsService.sh**
4. Iniciar el comando /etc/init.d/netflowanalyzer

Este empieza NetFlow Analyzer como servicio en Linux.

En **Fedora / SUSE** hay que abrir el archive mysql-ds.xml en el directorio *server**default**deploy* y cambiar la conexion:

<connection-url>jdbc:mysql://localhost:13310/netflow </connection-url> to

<connection-url>jdbc:mysql://127.0.0.1:13310/netflow </connection-url> y restaurar el servidor NetFlow Analyzer.

Apagando NetFlow Analyzer

Windows:

1. **Inicio > Programa > ManageEngine NetFlow Analyzer 7**
2. Seleccionar la opcion **Apagar NetFlow Analyzer**
3. Alternativamente, se puede navegar en la carpeta <*NetFlowAnalyzer_Home*>*bin* e invocar el archivo **shutdown.bat**.

Linux:

1. Navegar el directorio <*NetFlowAnalyzer_Home*>/*bin*.
2. Ejecutar el archivo shutdown.sh.

Accesando al cliente Web

NetFlow Analyzer es esencialmente una herramienta para el monitoreo de ancho de banda que usa Cisco NetFlow para exportar, esta analiza el trafico de la red y determina el uso del ancho de banda.

Primeramente el servidor ha sido iniciado satisfactoriamente, siga los siguientes pasos para tener acceso a NetFlow Analyzer.

Abra la ventana del navegador Web soportado.

1. Poner la direccion URL **http://*<hostname>*:8080** (donde ***<hostname>*** *es el nombre* de la maquina en la cual esta corriendo NetFlow Analyzer, y **8080 es el puerto del servidor Web por defecto).**

2. Autenticarse en NetFlow Analyzer usando por defecto como username/password **admin/admin, posteriormente se crearan usuarios.**

Una vez autenticados, se puede empezar a administrar dispositivos exportados por Cisco NetFlow, generando reports de ancho de banda y mas.

Como empezar

Primero, una vez que NetFlow Analyzer ha iniciado satisfactoriamente, la siguiente cosa que hay que hacer es empezar a recibir los flujos exportados por NetFlow desde los dispositivos ruteados en la red.

Tan pronto entra al analizador de NetFlow en el cliente Web, se podrá ver la pestaña Global y Dashboard. Esta vista muestra información sobre las interfaces y el envío de las exportaciones de NetFlow y sFlow, así como información sobre el trafico IP de todos los grupos creados hasta el momento. La pantalla muestra el tráfico tan pronto como NetFlow reciba datos desde cualquier Interfaz.

En la vista Global se divide en tres pestañas:

1. En la vista **Network Snapshot** la cual lista los dispositivos, las interfaces y los grupos IP.
2. La Vista **Interface** lista todas las interfaces desde que recibe las exportaciones de NetFlow.
3. La vista **Sistema Autónomo** la cual lista todos los sistemas autónomos configurados en cada router.

Clic en este icono para retornar a la vista global.

Vista Network Snapshot

La vista Network Snapshot es la vista por defecto cuando el usuario inicia la aplicacion NetFlow Analyzer. El periodo de tiempo en el cual se ven los reportes puede ser modificado usando la opcion seleccionar periodo.

Elperiodo de tiempo en el cual se pueden mostrar los reporte p ueden ser Last Hour, Last 6 Hours, Today and Last 24 Hours.

Este permite categorizar en detalle las siguientes cabeceras:

1. Los mejores dispositivos por velocidad
2. Las mejores Interfaces por velocidad
3. Interfaces por utilización
4. Los mejores Grupos IP por velocidad
5. Los mejores Grupos IP por utilización

Las mejores 5 Interfaces/Grupos IP son listados en cada categoría

Los mejores Dispositivos por velocidad

Al inicio de la página en la vista dispositivos se lista los primeros 5 dispositivos (router/switch, clasificados por velocidad. Se muestra cada nombre del dispositivo, detalles de la velocidad máxima, velocidad media, el porcentaje de utilización se muestra en cada nombre de dispositivo. El grafico muestra la representación de la utilización en forma el promedio de velocidad vs tiempo.

Las mejores interfaces por velocidad

Detallan las mejores cinco interfaces por velocidad. Detalla nombre del dispositivo (en la cual la interfaz reside), lista la velocidad de entrada y salida en las interfaces que son listadas.

Al hacer clic en cualquier nombre de la interfaz, es posible observar en la parte de abajo más detalles sobre la información relacionada con la velocidad de esta interfaz

Las mejores interfaces por utilización

Detallan las mejores cinco interfaces por utilización. Detalla nombre del dispositivo (en la cual la interfaz reside), lista la utilización de entrada y salida en las interfaces que son listadas.

Al hacer clic en cualquier nombre de la interfaz, es posible observar en la parte de abajo más detalles sobre la información relacionada con la utilización de esta interfaz

Los mejores Grupos IP por velocidad

Detallan la velocidad de entrada y salida en los Grupos IP que son listados. Al hacer clic en algún nombre del Grupo IP, es posible observar en la parte de abajo más detalles sobre la información relacionada con la velocidad de este Grupo IP.

Los mejores Grupos IP por utilización

Detallan la utilización de entrada y salida en los Grupos IP que son listados. Al hacer clic en algún nombre del Grupo IP, es posible observar en la parte de abajo más detalles sobre la información relacionada con la utilización de este Grupo IP.

El propósito de los iconos y botones en la vista Red Snapshot se explica a continuación.

Icono/ Botón	Descripción
 (cerca de actualizar esta página)	Clic en este icono, para actualizar el contenido de la página en el periodo de tiempo actual.

Ver tablero de interfaces

La pestaña de la vista de interfaces despliega información en todos los intereses desde la cual los flujos exportados por NetFlow son recibidos.

Por defecto la lista de los routers permiten que todos los routers e interfaces desde las cuales exporta NetFlow que son recibidas hasta la fecha, muestre los detalles de cada interfaz.

La vista predeterminada muestra los primeros interfaces del router. Los nombres de la interfaz pueden estar clasificados en orden de uso. El resto de las interfaces del router están ocultas.

Clic en el link [**Mostrar todos los**] para desplegar todas las interfaces del router en el tablero. Clic en el link [**Ocultar todos los**] ocultar todas las interfaces y permitir solo los nombres del router en la lista de routers.

Tú puedes hacer filtros en la vista del tablero para permitir solo las interfaces en las cuales los valores del tráfico entrante o saliente exceden en los valores de los porcentajes especificados. Clic en el link **[filtro]** para especificar el porcentaje mínimo de los valores del tráfico de entrada y salida. Clic en el botón establecer para que los cambios tomen efecto.

Los filtros son mostrados al lado del [filtro] enlace. Haga clic en el icono en cualquier momento para borrar la configuración del filtro y mostrar todos las interfaces en el panel de nuevo.

Clic en el enlace establecer SNMP del router para configurar los parámetros SNMP a nivel mundial o en un enrutador nivel individual.

Al hacer clic en Seleccione el Periodo, el periodo de tiempo elegido podría ser- Última Hora, Ultima 6 horas, de hoy y las últimas 24 horas. Informes correspondientes al período de tiempo elegido se muestra en la vista del panel.

El propósito de los iconos y botones en la lista de routers se explica a continuación.

Icono/ Boton	**Descripcion**
	Clic en este icono, o en el nombre del router , para ver las interfaces correspondientes al router.

	Clic en este icono, s interfaces correspondientes al router.
 (antes del nombre del router)	Clic en este icono, para cambiar el nombre del dispositivo.
 (antes del nombre de la interfaz)	Clic en este icono para cambar el nombre de la interfaz, o el enlace de la interfaz(entrada y salida ()in bps).
 (near Refresh)	Clic en este icono, para establecer el periodo de tiempo para actualizar la página de contenidos.
	Clic en el enlace solucionar problemas en una interfaz. Tu puedes solucionar solo una interfaz al momento. Nota: Los resultados de solución de problemas muestran directamente datos brutos. En consecuencia, los resultados dependen de la materia prima en el perido de tiempo fijado en la configuración.
	Indica que los reportes NBAR estan habilitados para la interfaz.
	Clic en este icono para tener una vista previa de los graficos del trafico sin perforaciones en cada interfaz.
	Indica que los reporte CBQoS estan habilitados en esta interfaz.

La columna nombre de la interfaz muestra la lista de todas las interfaces descubiertas en el dispositivo. Clic en una interfaz para ver los detalles del tráfico para esta interfaz.

La columna estado indica el estado actual de esta interfaz.

Icono	**Descripcion**
	El estado de la interfz es desconocido y los flujos no estan siendo recividos los pasados 10 minutos. La interfaz no esta respondiendo a las solicitudes SNMP.
	La interfaz esta respondiendo a las solicitudes SNMP y el link esta levantado, pero los flujos no han sido recividos los pasados diez minutos.

	El enlace está levantado, y los flujos están siendo recibidos.
	La interfaz esta respondiendo a solicitudes SNMP y el enlaces esta bajo y los flujos no estan siendo recibidos.

Las columnas del tráfico de entrada y tráfico de salida permiten ver la utilización del tráfico de entrada y salida en la interfaz respectiva en la pasada ultima hora.

Puedes hacer clic en el tráfico de entrada (IN) o en el tráfico de salida (OUT) en la barra para ver el grafico del tráfico de la aplicación para esta interfaz. Utilice el vínculo informe personalizado para generar informes personalizados.

Establezca el valor Actualizar esta página para informar a la aplicación la frecuencia con la cual se realizan las actualizaciones para obtener los datos más recientemente.

Más reportes

Clic en más reportes para comparar dispositivos a través de varios periodos de tiempo para generalizar informes personalizados en base a criterios definidos.

Comparar dispositivos

Comparar características de dispositivos que permitan al usuario comparar varios dispositivos para el mismo periodo de tiempo o comparar el mismo dispositivo durante distintos periodos de tiempo, por ejemplo: Informe de cada día, informe de cada hora, informe de cada semana, informe de cada mes.

Campo	Descripcion
Tipo de reporte	Los tipos de reportes pueden ser : • Comparar multiples dispositivos en un mismo periodo de tiempo o

	• Comparar un mismo dispositivo en diferentes periodos de timepo Seguin sea el caso.
Seleccionar periodo	Cuando el tipo de reporte es escogifo como: -Comparar multiples dispositivos en un mismo periodo de tiempo, están disponibles periodos como ultima hora, ultimas 6 horas, hoy, ultimas 24 horas, ayer, ultima semana, ultimo mes, ultimo semestre o selección personalizada. Seleccion personalizada permite elegir el momento en un periodo para el que se desea se genere un informe. Cuando el tipo de reporte es escogido como: comparar dispositivos igales en diferentes periodos de tiempo, estan habilitados periodos como reportes de cada dia, reportes de cada hora, reportes de cada semana, reportes de cada mes.
Seleccionar dispositivo(s)	Este permite a los usuarios seleccionar los dispositivos (los dispositivos iguales estan comparados en varios periodos de tiempo), o establecer los dispositivos (que son comparados en simples periodos de tiempo). La opcion seleccionar dispositivos permite a los usuarios seleccionar los dispositivos internos de las interfaces o grupos IP ()or defecto las mejores 10 interfaces o grupos IP por utilizacion son escogidos), los cuales pueden ser modificados dando clic en el boton Modificar.
Generar Reportes	Generar el informe invoca el informe de los criterios definidos. **Opciones de reportes:** Las opciones de reportes que se pueden elegir son • Mostrar por velocidad • Mostrar por utilizacion • Mostrar por paquetes
Maximizar	Cuando la opcion generar reporte es invocado, la condicion del marco del filtro se minimiza para ofrecer una mejor vision del grafico (informe) sin desplazamiento. El marco del filtro puede ser restaurado usando el boton maximizar.
Minimizar	L boton minimizar puede ser usado para minimizar el marco del filtro para una mejor vista del informe (grafico)que se genero sin desplazaminetos.

Búsqueda de dispositivos

El enlace búsqueda permite establecer criterios y ver los detalles específicos sobre el trafico a través de la red en distintas interfaces. Datos para generar este informe se ha tomado directamente de los datos agregados.

Al hacer clic en el vinculo búsqueda de un pop-up con la provisión de seleccionar dispositivos y establecer criterios. En la ventana emergente que se abre, haga clic en el icono seleccionar dispositivos para elegir las interfaces en las que el informe debe ser generado.

En virtud de los criterios de búsqueda, introduzca los criterios en que el tráfico tiene que ser filtrada. Puede introducir cualquiera de los siguientes criterios para filtrar el tráfico:

- Dirección Origen/Destino
- Red Origen/Destino
- Nodos Origen/Destino
- Aplicaciones
- Rango de puertos

Use el icono  para seleccionar la fecha y la hora con facilidad. Utilice el IN / OUT para mostrar el cuadro de valores basados en el tráfico de entrada o trafico de salida. Ver por página le permite elegir el número de resultados para mostrar.

Una vez que se seleccione todos los criterios deseados, haga clic en el botón generar informa para mostrar el correspondiente informe de tráfico. El valor por defecto muestra informes de las direcciones IP de los host. Haga clic en el vínculo resolver DNS para ver los correspondientes valores de DNS. También puede ordenar los datos mostrados, ya sea por número de paquetes o Bytes.

Vista de los grupos IP

La información en los grupos IP creados hasta ahora, permiten ver la ficha global, esta permite mostrar todos los grupos cuando se da clic en **Grupos IP** en el panel al lado izquierdo.

Inicialmente cuando no han sido creados los Grupos IP, se mostrara el mensaje "**No hay grupos IP configurados**".

La lista de los Grupos IP permite ver todos los grupos IP que han sido creados hasta ahora. Clic en el enlace Descripción para ver la información descrita de todos los grupos IP creados. Alternativamente se puede dar clic en el enlace Vista Descripción de cada grupo IP para ver la descripción de la información únicamente del grupo IP seleccionado.

Clic en nombre del Grupo IP para ver el grafico del grupo IP especificado. Desde el grafico del trafico, se puede navegar para ver las mejores aplicaciones, los mejores hosts, y las mejores conversaciones de este grupo IP.

Las columnas del **tráfico de entrada y del trafico de salida** permiten ver la entrada y salida del trafico del Grupo IP generada por encima de la ultima hora. Se puede dar clic en el tráfico de entrada o el tráfico de salida en la barra para ver el reporte del tráfico de la aplicación respectiva.

Clic en el icono  para ver el reporte del tráfico consolidado para el respectivo grupo IP. Este reporte permite ver todos los detalles del trafico entrante o saliente en este grupo IP en un simple reporte.

Clic en este icono  para ver el grafico de la velocidad del grupo IP en particular.

REPORTES DE TRÁFICO

Informes de Tráfico Netflow

El Analizador NetFlow genera informes de tráfico en tiempo real, cuando datos NetFlow son recibidos de un interfaz.

Los informes de tráfico en el Analizador NetFlow incluyen información sobre:

- Tendencias de Tráfico.
- Últimas aplicaciones.

- Últimos host.
- Conversaciones.

Aparte de estos informes predefinidos, el Informe De búsqueda permiten definir criterios y generar informes específicos sobre la actividad de red.

Los Informes Consolidados le muestran en general la estadística de tráfico para un interfaz, host o aplicación.

Los informes de solución, dejan informes de interfaces que usa datos brutos directamente.

Click en el icono  link de informes de solución.

Gráficos de Tráfico En tiempo real

El Analizador NetFlow genera gráficos de tráfico en cuanto datos Netflow son recibidos. La etiqueta de Tráfico muestra gráficos de tráfico en tiempo real para el tráfico entrante y saliente.

Dependiendo de en cual link se pulse, usted puede ver gráficos de tráfico para un interfaz o el grupo IP.

Las pestañas encima del gráfico de tráfico, dejan ver el gráfico en términos de volumen de tráfico, velocidad, utilización, y el número de paquetes recibidos.

 La etiqueta de Paquetes muestra el número de los paquetes reales de datos de tráfico recibidos. Esta información es incluida en datos exportados Netflow.

Usted puede ver gráficos de tráfico para períodos de tiempo diferentes pero escogiendo los valores apropiados de la caja de Período de tiempo. Use las opciones el **desde** y **hasta** para escoger períodos de tiempo para los gráficos.

Use el icono  para seleccionar la fecha y el tiempo fácilmente. El período de tiempo para estos gráficos está basado en el tiempo de sistema corriente. Una vez que usted selecciona la fecha

deseada y el tiempo, al dar click sobre el botón mostrar el informe aparecerá el reporte del tráfico apropiado.

La tabla de abajo del gráfico muestra la leyenda, con el total, el máximo, el mínimo, y valores de tráfico medios para este interfaz o el grupo IP, para el período de tiempo seleccionado.

El Tráfico **de entrada** y el Tráfico **de salida** muestran ejemplos de valores de tráfico generado sobre el período de tiempo seleccionado.

Filtros de Tiempo.

El gráfico muestra estadísticas de "el día anterior". Usted puede decidir ver datos en base de hora, en los gráficos de tráfico se muestran informes de última hora, diarios, semanales, mensuales y trimestrales. Para hacer esto únicamente seleccionaremos en la barra superior las opciones.

El click en el icono  es para especificar el intervalo de tiempo por hora para cual usted puede ver gráficos de tráfico. El click en el botón **mostrar** para poner el filtro y ver valores a base de hora en el gráfico de tráfico así como la mesa debajo. Click en el botón **reset** para apagar el filtro e interruptor a los gráficos de tráfico regulares.

Últimas Aplicaciones

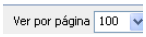
La pestaña de aplicaciones le muestra los últimos protocolos y aplicaciones para el período de tiempo seleccionado. En la parte inferior del reporte de aplicación nos mostrará un gráfico del reporte en forma de pastel. Este informe muestra la distribución de tráfico entrante y saliente según lo escojamos en la parte superior.

El cuadro de texto de Período de tiempo nos permite escoger entre la última hora, el día anterior, la semana pasada, el mes pasado, y los gráficos de tráfico de último trimestre.

Junto a la caja de fecha existen cuadros de texto donde podemos escribir los límites de tiempo **desde** y **hasta**, en la parte inferior tendremos el gráfico respectivo.

Use el icono Calendario para seleccionar la fecha y el tiempo fácilmente. El período de tiempo para estos gráficos está basado durante el tiempo de sistema corriente. Una vez que usted selecciona la fecha deseada y el tiempo, el click en el botón nos mostrará el informe de tráfico apropiado de aplicación.

El click sobre un nombre de la aplicación permite ver las Conversaciones Superiores que contribuyeron al tráfico de este uso.

La caja ver por página 

de la parte superior nos permite escoger cuantas aplicaciones van a ser mostrados. Usted puede poner el valor máximo en esta opción.

El gráfico circular que se encuentra en la parte inferior de la página nos muestra el porcentaje de ancho de banda usado por cada aplicación.

El icono  que se encuentra encima del gráfico nos permite ampliar la imagen para poder observarla de mejor manera.

Usted puede pulsar el icono  PDF para mostrar el gráfico y todo el informe como un archivo PDF.

Últimos host

Para los últimos host tenemos dos pestañas que nos indicarán cada uno de los host.

Pestaña de Origen.- Al dar click en este ícono tendremos una lista de los host que han ocupado ancho de banda.

Pestaña de Destino.- Al dar click en la pestaña nos indicará una lista de los últimas direcciones destino a las cuales han accedido las direcciones origen que se muestran en la pantalla anterior.

Escoja entre **entrada y salida** mostrar a las direcciones con ancho de banda superior en el tráfico entrante o saliente.

Cuando usted tiene conformados grupos ip y ve el tráfico de los host mediante estos, el tráfico es unidireccional, y ahí los íconos de **entrada y salida** como opciones no están disponibles.

Por defecto el reporte que vemos nos muestra las direcciones IP de los host.

Tenemos la opción de sobre el informe **RESOLVER DNS** al dar click en el link nos indicará el valor correspondiente del DNS de acuerdo a la dirección.

Al dar click sobre la opción **SHOW NETWORK** nos indicará las redes que intervienen en el momento de mostrar host origen y destino.

El gráfico circular que se encuentra en la parte inferior de la página nos muestra el porcentaje de ancho de banda usado por cada aplicación.

El icono  que se encuentra encima del gráfico nos permite ampliar la imagen para poder observarla de mejor manera.

Usted puede pulsar el icono  PDF para mostrar el gráfico y todo el informe como un archivo PDF.

Conversaciones Superiores

La pestaña de Conversación muestra las últimas conversaciones que contribuyen al tráfico en el período de tiempo seleccionado.

Escoja entre Entrada y salida para mostrar las conversaciones superiores en el tráfico entrante o saliente.

La caja de Período de tiempo le deja escoger entre la última hora, el día anterior, la semana pasada, el mes pasado, y el último trimestre.

Use el icono Calendario para seleccionar la fecha y el tiempo fácilmente. El período de tiempo para estos gráficos está basado durante el tiempo de sistema corriente. Una vez que usted selecciona la

fecha deseada y el tiempo, el click en el botón permite mostrar el informe de tráfico de conversación apropiado.

La vista de informe muestra las direcciones de IP de los host que han navegado. El click en la Resolución DNS servirá para ver la correspondencia de nombres DNS.

La pestaña de conversación nos permite observar la dirección ip origen, la dirección ip destino, tipo de aplicación, puerto, protocolo, y el porcentaje de tráfico. La lista muestra las conversaciones clasificadas en la orden de tráfico.

Los gráficos que se muestran en la parte inferior de este informe muestran 3 distintos gráficos, según el tráfico máximo de consumo de origen, destino y aplicación, teniendo cada una de ellas la opción de maximizar si cree adecuado y haciendo click en el icono de  pdf podremos tener el informe en este formato.

INFORMES DE TRÁFICO

El informe de Tráfico para sistemas autónomos muestra la cantidad de tráfico entrante y saliente para esto.

Las pestañas encima del gráfico de tráfico le dejan ver el gráfico en términos de volumen de tráfico, velocidad, y el número de paquetes recibidos.

Usted puede ver gráficos de tráfico para períodos de tiempo diferentes para ello debe escoger los valores apropiados de la caja de Período de tiempo.

Use el icono Calendario para seleccionar la fecha y el tiempo fácilmente. El período de tiempo para estos gráficos está basado durante el tiempo de sistema corriente. Una vez que usted selecciona la fecha deseada y el tiempo al hacer click nos mostrará el informe de acuerdo a las fechas seleccionadas.

La parte de abajo del informe nos muestra gráficos entrantes, salientes y de aplicación así como también muestra la leyenda, con el total, el máximo, el mínimo, y valores de tráfico medios para el período de tiempo seleccionado.

Informes de Solución

El link de los informes de solución le deja poner criterios y ver detalles específicos sobre el tráfico a través de una sola interfaz. Los datos para solucionar informes son tomados directamente de datos brutos.

Quiere decir que los informes de Solución estarán disponibles sólo para el período de tiempo máximo para conservar datos brutos, configurados en Ajustes.

Un click en el icono Solucionar en una interfaz, se presenta encima de los gráficos de tráfico de una interfaz, al dar click en agregar criterios nos permitirá poder generar informes de acuerdo a los criterios que creemos, para poder crear los criterios tenemos opción de hacerlo por dirección origen y destino, red de origen y destino, nodos de origen y destino, aplicación, puerto, intervalos de puerto, etc. También en esta opción nos permitirá seleccionar los dispositivos, especificar el rango de tiempo en el cual queremos en informe.

Para que el informe se genere podemos crear uno o más criterios y al momento de buscar también podemos hacerlo por todos los criterios y solo por alguno de ellos, cuando definamos todos los parámetros simplemente damos click en generar informe y en segundos tendremos en informe que deseamos.

Informes Consolidados

Los informes consolidados le dejan ver todos los detalles de tráfico para un interfaz o el grupo IP. Usted entonces puede imprimir este informe o guardarlo como un archivo PDF.

Podemos acceder a generar un informe consolidado al hacer click en el icono  mostrado como vista rápida o cuando estemos en algún grupo o interfaz al ingresar en **more reports** y **consolidated.**

Aquí tenemos también la opción de personalizar el informe y obtener informes de una hora, de un día y de 8am a 8pm.

En este informe tenemos 3 pestañas que son de volumen, de velocidad y de utilización podremos generar el informe en cualquiera de estas opciones.

También en el mismo informe tendremos las estadísticas de aplicaciones de entrada, origen entrada y destino entrada, cada una con en tamaño de utilización en (MB), también tenemos la opción de poder generar el informe en formato pdf  , asi como poder imprimir con el ícono  .

Informes de comparación

Para generar informes de comparación seleccionamos la pestaña que se encuentra en la parte superior derecha **More Reports** esta opción siempre se encontrará activa en la aplicación, una vez seleccionemos **compare,** y se abrirá el informe de comparación.

Ya en el informe tenemos que elegir el tipo de informe es el que necesitamos, tendremos la opción de comparar **múltiples dispositivos en un mismo periodo de tiempo**, y comparar el **mismo dispositivo por diferentes periodos de tiempo**.

También tenemos la opción de seleccionar el periodo de tiempo y si queremos por interface y por grupo ip, una vez seleccionadas todas las propiedades únicamente seleccionamos **generar reporte,** y en unos segundos tendremos el reporte de acuerdo a los parámetros pudiendo seleccionar mostrar por velocidad, utilización y paquetes.

Informe De búsqueda

Informes De búsqueda nos permite poner varios criterios y ver informes específicos.

Esto es sobre todo útil en la averiguación de la utilización de ancho de banda de un host específico o el uso. El Informe de búsqueda también puede mostrarnos en detalle el uso del ancho de banda y cuales direcciones lo usan, así ayudando a solucionar, y aún descubrir actividades de virus.

Bajo Criterios de Informe, se puede especificar un máximo de tres criterios de filtración:

* Dirección Origen/Destino

* Red Origen/Destino

* Nodos Origen/Destino

* Aplicación

* Puerto/Rango de puertos

Mediante las cajas de fecha podemos escoger períodos de tiempo para el informe. Use el icono  Calendario para seleccionar la fecha y el tiempo fácilmente.

También podemos seleccionar si queremos el **tráfico de entrada y salida** o solo **tráfico de entrada o solo el de salida**. Junto tenemos la opción de ver por página aquí seleccionaremos cuantos valores nos mostrará por página.

Para realizar la búsqueda podemos hacerlo por todos parámetros que pongamos o únicamente por alguno de ellos y presionamos **generar informe.**

OPERACIONES DEL ADMINISTRADOR

Aplicación de Mapeo, Grupo de Aplicación, Grupo de Cartografía y DSCP

Mapeo de aplicaciones

La opción mapeo de aplicaciones permite configurar las aplicaciones identificadas por NetFlow Analyzer. Tú puedes añadir nuevas aplicaciones, modificar las existentes, o eliminar estas.

Añadiendo aplicaciones

Para añadir una nueva aplicacion siga los siguientes pasos:

1. Clic en el botón Añadir para añadir una nueva aplicación
2. Ponga el puerto del número de la nueva aplicación, ponga el rango del puerto, separe los puntos de inicio y fin de los rangos con el hyphen. (eg) 1400-1700
3. Escoja el protocolo desde la lista de protocolos
4. Escoja una de las opciones Dirección IP / Red IP / Rango IP. Dependiendo que opción elegiste se puede llenar lo siguiente:

Si tu opción es dirección IP entonces tú tienes que poner la dirección IP en la caja

Si tu opción es Red IP tú tienes que poner la red IP y la máscara de red en los detalles

Si tu opción es rango IP entonces tienes que poner la IP inicio, la IP final, y la máscara de red.

Entre únicamente en el nombre de la aplicación.

5. El nombre de la aplicación que ha sido puesto finalmente con la dirección IP es asociado con una aplicación.

Asegurese que la combnacion del numero del Puerto y el protocol sean unicos, si no es asi el mapeo de la aplicaion sera eliminado.

Haga clic en el boton **Actualizar** para guardar los cambios..

Modificar una aplicacion

Seleccione una aplicacion y clic en el boton Modificar en las propiedades.

Tu solo cambias el nombre de la aplicacion. Si tu necesitas cambiar el puerto o el protocolo, tu tines que eliminar la aplicacion, y añadir una nueva aplicacion.

Clic en el botón actualizar para guardar los cambios.

Eliminar una aplicación

Seleccionar una aplicación y clic en el botón Eliminar. La aplicación es eliminada permanentemente, el correspondiente puerto es liberado, y puede ser asignado a otra aplicación.

Añadiendo notas en una aplicacion

Las aplicaciones son categorizadas basadas en direcciones de origen, direcciones de destino, puertos de origen, puertos de destino y valores de protocolos en los registros de flujos. Los valores son combinados con las listas de aplicaciones en el mapeo de aplicaciones.

La comprobación es lo primero que por lo menos tenemos que hacer con los dos puertos (puerto de origen / puerto de destino), y si no coinciden no funciona, lo más importante que hay que hacer en los dos puertos es el mapeo.

El mapeo de aplicaciones creado con la dirección IP / Rango IP / Red IP específicos dan mayor prioridad a las aplicaciones mapeadas que las que no tienen dirección IP.

Las aplicaciones son categorizadas basadas en la dirección de origen, dirección de destino, puerto de origen, puerto de destino y valores de protocolo en los registros de flujo. Hay que combinar los dos puertos (origen / destino) y protocolo con el Puerto-protocolo en la lista de la aplicación mapeada.

Si la combinación no funciona, la aplicación es categorizada como protocolo App (TCP App o UDP App)

En este caso el protocolo no es habilitado en el mapeo de la aplicación, la aplicación es categorizada como Unknown App.

La secuencia en la cual el mapeo es chequeado es la siguiente:

1. La aplicación mapeada con la especifica dirección IP / rango IP / red IP es combinada
2. La aplicación mapeada sin la dirección IP y un simple numero de puerto / rango de puerto.

Grupos de Aplicaciones

Los grupos de aplicaciones permiten que tu definas tu propia clase de aplicaciones incluyendo una o mas aplicaciones. Por ejemplo, tu podrias clasificar todas tus aplicaciones en la base de datos que desees Oracle, MySql, MS-Sql en un grupo llamado DataBase. Inicialmente cuando no han sido creados grupos de aplicaciones un mensaje que afecta es mostrado. El reporte del grupo de la aplicacion puede ser visto en el tab de la aplicacion de cada interface.

Añadir un grupo de aplicaciones

Los pasos para añadir una nueva aplicacion son los siguientes:

1. Clic en el botón Añadir para proceder a la pan talla añadir un grupo
2. Ponga el nombre del grupo y la descripción del grupo (eg.) Grupo DataBase contiene la DB Oracle y la BD MySql.
3. Escoja la aplicación desde la lista de aplicaciones en el panel

Seleccione una aplicación y de clic en este

Use el botón “>>” para incluir la aplicación seleccionada en el panel derecho de la lista de “Aplicaciones seleccionadas”

Añadir más aplicaciones como tú desees en este grupo.

4. Clic en actualizar para crear el grupo de la aplicación con lista de aplicaciones que están seleccionadas.

Tu puedes crear adicionalmente grupos de aplicaciones dando clic en el botón añadir.

Modificar un grupo de aplicaciones

Seleccionar el grupo para modificar y dar clic en el botón “Modificar”.

	Tu puedes solo cambiar la descripcion del grupo de aplicaciones y seleccionar de la lista de aplicaciones. No es posible cambiar el nombre del grupo de aplicaciones.

Clic en el botón **Guardar** para guardar los cambios.

Eliminar un grupo de aplicaciones

Seleccionar el grupo de aplicaciones que se desea eliminar y clic en el boton “Eliminar”. Tu puedes confirmar para eliminar y tu puedes confirmar si el grupo es eliminado.

ADMINISTRANDO GRUPOS IP

Las funciones de un grupo IP pueden ser supervisar departamentos, intranet o exclusivamente trafico de aplicaciones. Tu puedes crear grupos IP basados en direcciones IP y/o combinaciones de puertos y protocolos. Tu puedes incluso monitorear trafico desde interfaces especificas cruzando diferentes routers. Despues de crear grupos IP, tu puedes ver las mejores aplicaciones, los mejores protocolos, y las mejores conversaciones solo en este grupo IP.

Definiendo Grupos IP

Los grupos IP pueden ser definidos por direcciones IP y / o combinaciones de Puerto o protocolo. Adicionalmente, tú puedes filtrar tráfico de grupos IP basados en interfaces. La siguiente matriz permite ver las diferentes posibles combinaciones:

Combinación	Dirección IP	Puerto/Protocolo	Interfaces
Dirección IP	Vista de los detalles del ancho de banda por rangos de direcciones IP.	Vista Web (80/TCP, 80/UDP) detalles de trafico de rangos de direcciones IP.	Vista de detalles de ancho de banda cruzando múltiples interfaces, de rangos de direcciones IP.
Puerto/Protocolo	Vista Web (80/TCP, 80/UDP) detalles de trafico de rangos de	Vista Web (80/TCP, 80/UDP) trafico generado a través de	Vista Web (80/TCP, 80/UDP) tráfico generado a través de múltiples

	direcciones IP.	la red.	interfaces.
Interfaces	Vista de detalles del ancho de banda cruzando múltiples interfaces, de un rango de direcciones IP.	Vista Web (80/TCP, 80/UDP) trafico generado cruzando múltiples interfaces.	[No es posible]

Creando un grupo IP

El enlace de administración de Grupos IP en las operaciones de Administrador, se puede crear, modificar y eliminar Grupos IP. Clic en este enlace, y entonces clic en Create para crear un nuevo grupo IP. Llenar la siguiente información y clic en **Añadir** para añadir un nuevo Grupo IP en la actual lista de grupos IP.

Campo	**Descripcion**
Nombre del grupo IP	Ponga unicamente un unico nombre para identificar este grupo IP.
Descripcion del grupo IP	Ponga informacion para describer este grupo IP para ayudar a otros operadores a entender porque este fue creado.
Grupos basados en la IP	Seleccione este si se desea definir este grupo IP basado en direcciones IP o combinaciones de puerto o protocolo. Si tu deseas definir grupos IP basados en direcciones IP y puertos o protocolo, seleccione ambas opciones.
Especifique IP/rangoIP/Red	Seleccione la direccion IP, rango de direcciones, o red que este grupo IP esta basado. Use la opcion **Añadir Mas** para añadir especificaciones adiciconales.
Incluir/Excluir	Incluye la opción de incluir direcciones IP particulares, rangos de direcciones, o redes. Excluye la opción de excluir direcciones IP particulares, rangos de direcciones, o redes.
Interfaces Asociadas	Si tu necesitas promover grupos de filtros IP, basados en dispositivos o diferentes combinaciones de interfaces, clic en el enlace "Seleccionar Dispositivos" y seleccionar los diferentes dispositivos e interfaces cuyo trafico necesita ser incluido en este grupo IP.

Velocidad de Grupos IP	Ponga la velocidad de la interface (en bits por segundos) calculando el porcentaje del trafico para este Grupo IP.

Administrar Grupos IP

Clic en el enlace **Administrar Grupos IP** en el cuadro de las operaciones de Admin para ver la lista de grupos creados hasta ahora. El estado actual del grupo IP solo permite como Seleccionar el grupo IP que se desea modificar, y clic en el botón modificar para editar estos ajustes, lo primero que haces es clic en **Add** para guardar y activar los nuevos cambios, para cambiar el estado habilitado de un grupo IP a deshabilitado o viceversa clic en el estado actual del grupo IP. Esto es posible habilitar o deshabilitar todos los grupos IP que se está usando los botones “Habilitar todo” y “Deshabilitar todo”.

Para eliminar un grupo IP, seleccione el grupo IP y clic en el botón **Eliminar.** Eliminar un grupo IP removiendo el grupo IP desde la lista de administración de grupos IP. Todos los usuarios asignados para este grupo IP no se ve en la lista de grupos IP en el Dashboard.

Cargando Grupos IP

NetFlow Analyzer permite cargar grupos IP usando archives XML (ipGroup.xml) contenidos en la ubicación AdventNet\ME\NetFlow\troubleshooting, usando estos archives es posible para definir múltiples grupos IP. Un simple código de configuración es el siguiente:

```
 <IPGroups ip_group_name="Engineering" ip_group_desc="description in detail"
ip_group_speed="1000000">
<GrpIPAddress addr_id="12.12.12.12" flag="include"/>
<GrpIPNetwork netmask_addr_id="255.255.255.0" network_addr_id="12.12.13.0" flag="include"/>
<GrpIPRange netmask_addr_id="255.255.255.0" start_addr_id="12.12.14.1"
end_addr_id="12.12.14.100" flag="exclude"/>
<ApplicationNames port="80" protocol="TCP"/>
<Selected_Devices>
<Router Router_Name="192.168.111.113">
<Interface interface_name="IfIndex1" />
<Interface interface_name="IfIndex3" />
</Router>
</Selected_Devices>
</IPGroups>
```

Sin esta configuracion es posible tener algún número de GrplIPAddress o GrpIPNetwork o GrpIPRange o Nombres de Aplicaciones con la selección de la interface.

Esto es solo posible añadir criterios/excepciones específicas a los grupos, definiciones tal como:

- Configurando un grupo IP con solo una red
- Configurando un grupo IP con solo una dirección
- Configurando un grupo IP con solo un rango
- Configurando un grupo IP con solo un puerto y protocolo.

El usuario tiene que asegurar que un grupo IP con el mismo nombre no puede existir y que el nombre del grupo IP no puede exceder los 50 caracteres.

Si todos los grupos IP son cargados correctamente, tu puedes mirar el mensaje “Todos los grupos IP son cargados satisfactoriamente” en la interface del usuario. Si tu intentas cargar el mismo grupo IP dos veces tu puedes mirar el mensaje “Error al cargar el grupo IP con el nombre….” En la interface de usuario. Si no hay archivos en el directorio, se puede mirar el mensaje “NETFLOW_HOME\solucionar problemas\ipGroup.xml no funciona” en la interface del usuario.

Después de añadir el grupo IP es posible seleccionar incluir/excluir una red IP/dirección IP/Rango IP desde la interface del usuario del producto.

Listas de Reportes


Es una buena idea para programar los informes que han de ejecutarse en las horas de mayor tráfico, ya que la generación de informes es un proceso de recursos, especialmente para grandes cantidades de interfaces. Una planificación es configurada para poner los parámetros automáticamente en la generación de reportes. Los parámetros a ser puestos para crear una lista son:

- Origen.- las interfaces o grupos IP en los cuales el trafico de origen es:

Interfaces.- en la lista de interfaces se puede observar la utilización del ancho de ancho. Seleccione un reporte a ser generado para cada interfaz seleccionada.

Grupos IP.- en la lista de grupos IP se puede observar la utilización del ancho de banda. Un reporte puede ser creado para cada grupo IP.

- **Tipo de reportes.-** Los tipos de reportes a ser generados: consolidados o personalizados (opciones de reportes personalizados no disponibles en los "Grupos IP")
- **Planificación de generación de reportes.-** cómo y cuando el reporte es generado, diario, semanal, mensual o solo una vez.

Generar reportes en.- Estos valores determina el tiempo en donde los reportes son generados.

Generar reportes para.- Este valor determina el tiempo de inicio y el de fin para los reportes.

- **Direcciones de email.-** estas son las direcciones a las cuales la generación de reportes van a ser enviados.

NetFlow Analyzer calcula la utilización del ancho de banda en interfaces específicas, grupos IP cada minuto. Los reportes son generados en varios intervalos de tiempo. Las características de la lista de reportes permiten crear nuevas listas y eliminar las existentes. La planificación de la pagina de listas permiten ver detalles, estado, tipos de reportes y el tiempo de generación de reportes pasados.

Las columnas mostradas en la planificación de la página de listas son descritas en la siguiente tabla:

Columna	Descripcion
Nombre	El nombre de una lista cuando es creado. Clic en el nombre para ver mas

	informacion acerca de la configuracion de la lista.
Detalles de la lista	Información en donde la lista está corriendo.
Estado	Por defecto todas las listas son habilitadas, las cuales significan que estan activadas. Clic en el icono  para desabilitar una lista. Cuando esto se hace, los reportes no son genrados para esta configuracion. Clic en el icono  para habilitar la lista de nuevo.
Tipo de Reporte	Si es un reporte consolidado son usados los reportes personalizados.
Tiempo del ultimo reporte	Esta columna lista el tiempo pasado cuando este fue planificado y el reporte fue creado y esta corriendo.
Generar reportes	Dando clic en ver reportes esto es posible ver en todos los reportes previamente a ser generados. El numero de reportes que son almacenadaos estan basados en la definicion del usuario en la pagna de ajuste de listas. (Para habilitar el item “Habilitar reportes pasados se debe acceder desde UI” esto es posible recuperar en cada reporte antiguo). Diariamente pueden ser almacenados 90 listas de reportes. Cada semana pueden ser almacenados 104 reportes. Mensualmente pueden ser almacenados 60 reportes.

Operaciones en las listas de Reportes

Se puede crear una nueva lista o eliminar listas desde la página de listas.

Configurar una nueva lista

Los pasos para configurar lista son:

1. Iniciar el cliente de NetFlow Analyzer y clic en “**Lista de reportes**” debajo de las Operaciones de Admin en el panel izquierdo.
2. Clic en **Añadir** para añadir una nueva lista de perfil.
3. Llene los siguientes detalles.

Campo	Descripcion
Nombre de la lista	Ponga un unico nombre para identificar esta lista.
Descripcion	Ponga la informacion que describa a este perfil de la lista para ayudar a otros operadores a entender porque fue creada.
Seleccionar origen	Por defecto todos las interfaces administradas envian exportaciones de NetFlow a las seleccionadas. Si se desea configurar estas listas para aplicar ciertamente en las interfaces clic en el enlace **Modificar seleccion.** En la ventana pop-up, selecciones los dispositivos y las interfaces requeridas y clic en **Actualizar** para guardar los cambios.
	Por defecto todos los grupos IP son seleccionados. Si se desea configurar esta lista para aplicar solo en los Grupos IP, clic en el enlace **Modificar selección.** En la ventana pop-up, seleccionar los dispositivos requeridos y grupos IP y clic en **Actualizar** para guardar los cambios.
Tipo de reportes	Seleccione los reportes que necesitan para ser generados como consolidados y personalizados. Por defecto lod ajustes son consolidados en los reportes. Para optar por el informe personalizado, haga clic en el botón de adelante del informe personalizado
	Si tú deseas un reporte personalizado entonces clic en el botón radio en frente del reporte personalizado. Optar por el reporte personalizado permite que tu pongas criterios para usar esto utilice la opción “Añadir criterio”. Algún numero de criterios pueden ser puestos y el conjunto de reglas para que coincida con todos los criterios o cualquier persona.
Generacion de listas de reportes	Seleccione la frecuencia de generación de informes como: diario, semanal, mensual y una sola vez. Dependiendo de este informe se generará en el momento oportuno intervalos.
Reportes enviados a direcciones de email	Ponga la direccion de email en la cual se generan los reportes. Tu puedes poner multiples direcciones de email separadas por coma.

4. Después de los ajustes de los parámetros requeridos, clic **Guardar.**

Reportes Personalizados

Optar por reportes personalizados permite que se pongan criterios en base al cual el reporte fue generado. Dar clic en el botón “Añadir criterio” para poder poner en condiciones en “Dirección de origen red de origen, nodos de origen, direcciones de destino, red de destino, nodos de destino y

aplicaciones". Para añadir más criterios clic en "Añadir Criterios". Habiendo creado todos los criterios **usted puede decidir si hacer el informe generado para satisfacer todos los criterios de creación o cualquiera de ellos.**

Generación de reportes fijando la hora

La generación de reportes fijando la hora son los siguientes:

Diario: cuando tú optas por diario tú tienes la opción de poner el tiempo en el cual el reporte debería ser generado. Solo el reporte podría ser generado para el día anterior o las últimas 24 horas. Cuando la opción es el día anterior el reporte es generado en el periodo de tiempo de 00:00 horas a las 23:59 horas del día anterior. Tienes la opción para disminuir la bajada de este periodo de tiempo usando el filtro de tiempo  . Para esta instancia si el máximo de flujos ocurre durante las horas que estás trabajando desde las 08:00 horas hasta las 18:00 horas se puede poner en la ventana del pops up.

Cuando se opta por las últimas 24 horas entonces el reporte es generado para los flujos en el intervalo de 24 horas (desde el tiempo en el cual el reporte es generado hoy). Los 30 reportes más recientemente de las listas pueden ser accesibles desde la página de listas.

Excluir semanas: cuando se escoge la opción excluir semanas con "Día anterior", los reportes son generados el martes, miércoles, jueves, viernes, y sábado. Esos reportes son pertenecientes a lunes, martes, miércoles, jueves y viernes respectivamente.

Cuando escoges la opción excluir semanas con "pasadas 24 horas", los reportes van a ser generados en Lunes, Martes, Miércoles, Jueves y viernes.

Semanal: cuando optas por la opción semanal, se tiene la opción para especificar el día y el tiempo en el cual los reportes necesitan ser generados. Los reportes podrían ser generados para la "semana anterior" o para los "pasados 7 días". Adicionalmente la opción "Excluir semanas" los

reportes pueden ser hechos incluyendo solo datos correspondientes de lunes a viernes.

La opción la semana anterior podría generar l reporte para el periodo de tiempo de domingo 00:00 horas hasta el viernes 23:59 horas.

La opción “pasados 7 días” debería generar los reportes de los pasados 7 días desde el tiempo en el cual el reporte es generado. Además, la opción excluir semanas debería generar reportes de los pasados 7 días con los datos para la semana excluida (sábado, domingo). Para esta instancia si el reporte es generado el lunes a las 10:00, con las reglas habilitadas puestas como “pasados 7 días” y “excluir semanas”, el reporte podría ser generado para el periodo de tiempo de la semana pasado de lunes 10:00 horas a viernes 23:59 horas y desde esta semana de lunes 00:00 horas hasta 10:00 horas. Los 52 reportes más recientes para esta lista pueden ser accesibles desde la página de listas.

Mensual: cuando optas por la opcion mensual se puede poner datos a lo largo del mes con el tiempo en el cual el reporte necesita ser generado cada mes. Los reportes pueden ser generados para el “mes anterior” o para los “pasados 30 dias”. Al seleccionar “excluir semanas” los reportes pueden ser hechos para incluir solo datos correspondientes de lunes a viernes.

Entonces la opcion “mes anterior” es habilitada y la fecha de los reportes generados se pone en quinto de cada mes a las 10:00 horas, entonces el reporte va a ser generado unicamente del mes pasado (del primero al ultimo dia del mes). Cuando la opcion “excluir semanas” es habilitado entonces el reporte generado podria excluir todos los intervalos semanasles (sabado y domingo).

Cuando la opción los “pasados 30 días” es habilitada y la fecha del reporte generados se pone el quinto de cada mes a las 10:00 horas, entonces el reporte va a ser generado desde el quinto del pasado mes a las 10:00 horas hasta el quinto de este mes a las 10:00 horas. Cuando la opción “excluir semanas” es habilitada entonces al generar los reportes van a ser excluidos todos los

intermedios de semana (sábado y domingo). Los 12 reportes más crecientes para esta lista pueden ser accesibles desde la página de listas.

Solo una vez: si tu deseas generar reportes solo una vez se especifica el tiempo para poder hacer la opción “solo una vez”. Los datos y el tiempo en el cual el reporte podría estar corriendo se puede especificar. Los datos y el tiempo pueden ser alterados usando el icono  . Los reportes pueden ser generados para el día anterior, pasadas 24 horas, semana anterior, pasados 7 días, mes anterior o los últimos 30 días. Cuando la opción “día anterior” es habilitada entonces el botón  permite ajustar las horas de trabajo. El último reporte para esta lista puede ser accesible desde la página de listas.

Eliminando listas

Seleccionar desde la lista y clic en **Eliminar** para eliminar las listas. Al eliminar una lista solo se elimina de la correspondiente carpeta.

Ajustando listas

Adicionalmente hay el enlace Ajustando listas en la pagina de listas. Este enlace permite poner los parametros que podrian ser aplicados a lo largo de todos los reportes generados. Los parametros que incluyen son:

- **Mostrar el nombre del host en los reportes.-** esto determina como el nombre del host es mostrado en los reportes. Estos pueden ser escogidos entre los siguientes:

Direccion IP o

Nombre DNS

- **Opciones de grafico.-** (tipo de reports a ser mostrados en reportes), estos determinan como los datos están mostrados en los reportes generados. Estos pueden ser escogidos entre los siguientes:

Utilización (en porcentaje) o

Velocidad (en bps)

- **Reportes opción enlace-mail.-** el formato en el cual los enlaces son el correo. Estos pueden ser:

Archivos zipiados o

PDF.- el numero de archives PDF a ser enviados en un mail es especifico. El numero esta en el rango de 5 a 50 en incrementos de cinco.

- **Habilitar reportes antiguos a ser acezados desde la UI**

Listas diarias.- el numero de reportes diarios a ser almacenados (estos pueden tomar valores de 7 / 30 / 60 / 90)

Listas semanales.- el numero de reportes semanales a ser almacenados (estos pueden tomar valores de 4 / 26 / 52 / 104)

Listas mensuales.- el numero de reportes mensuales a ser almacenados (estos pueden tomar valores de 12 / 36 / 60).

Una vez ajustadas las listas a ser configuradas, clic en el botón “guardar” para aplicar los ajustes. Solo clic en el botón “cerrar” para cerrar la ventana y proceder a la página de listas.

Administrar Grupos de dispositivos

NetFlow Analyzer permite crear grupos de dispositivos. Un grupo de dispositivos puede contener varios routers, y un router puede pertenecer a varios dispositivos.

La administración de la opción de grupos de dispositivos permite que tú puedas crear, gestionar, y eliminar grupos de dispositivos. Inicialmente, donde los grupos de dispositivos han de ser creados, tu puedes mirar un mensaje que permite que tu empieces a crear grupos de dispositivos.

La opcion visible debajo de las **Operaciones Admin** en el menu dependes del nivel del usuario como ingreses.

Creando un grupo de dispositivos

Los siguientes pasos permiten crear un nuevo grupo de dispositivos:

1. Clic en el botón **Añadir** para crear un nuevo grupo dispositivos.
2. Ponga un único nombre para identificar el grupo de dispositivos. El mismo nombre es mostrado en el menú de grupo de dispositivos en la parte izquierda, y va a ser listado el grupo de dispositivos disponibles para ser administrados por el usuario.
3. Use el cuadro de la **Descripción del grupo de dispositivos** para poner información útil acerca del grupo de dispositivos.
4. Seleccione los routers necesarios para este grupo de dispositivos desde la lista disponible de los routers mostrados.

Una vez que todos los valores han sido ingresados, clic en el boton **Actualizar** para crear este grupo de dispositivos y comenzar a generar los reportes de trafico de los mismos.

Administrando Grupos de Dispositivos

Seleccione un grupo de dispositivos existente y clic en el boton **Modificar**. Se puede cambiar todas las propiedades del grupo de dispositivos excepto el nombre. Una vez que se tienen hechos los cambios de las propiedades del grupo de dispositivos, clic en el botón **Actualizar** para guardar los cambios.

Seleccione un grupo de dispositivos existentes y clic en el boton **Copiar** para copiar los ajustes. Esto es util cuando tu necesitas crear un nuevo grupo de dispositivos que incluyen los mismos routers. Esto guardas y se soluciona el estar añadiendo todos los routers de nuevo. Entonces se siguen los mismos pasos para crear un nuevo grupo de dispositivos.

Selecciona un grupo de dispositivos y clic en el botón **Eliminar** para eliminar un grupo de dispositivos. Cuando un grupo de dispositivos es eliminado este es removido desde la lista de los

grupos de dispositivos y del menú de grupos de dispositivo. Todos los usuarios asignados al grupo de dispositivos no van a mirar el grupo de dispositivos en el tablero.

Grupos de Interfaces

Los grupos de interfaces permiten combinar interfaces en orden para monitorear el tráfico. Esto puede ser útil para agrupar múltiples sub interfaces en una simple entidad lógica. Los siguientes son los pasos para crear un nuevo grupo de interfaces:

1. Clic en el tab **Grupo de Interfaces** en el siguiente tab de grupo de dispositivos.
2. Ponga un nombre para identificar el grupo de interfaces en el cuadro **Nombre Grupo de Interfaces.**
3. Use el cuadro de **velocidad del grupo de interfaces** para poner el límite de la velocidad para este grupo de interfaces.
4. Seleccione los routers necesarios y las interfaces de debajo de ellos para este grupo de interfaces. Al seleccionar un router por defecto todas las interfaces son seleccionadas. Se puede seleccionar y no seleccionar las interfaces no deseadas de la lista.
5. Clic en **Añadir** para guardar los cambios.

El grupo de interfaces que son creadas están listadas en el Dashboard en el tab de la “Vista Interfaces”. El nombre del grupo de interfaces, del tráfico entrante y el tráfico de salida para la última hora puede ser visto en este. Al dar clic en el nombre del grupo de interfaces es posible adicionar instrucciones de bajada para ver los detalles adicionales. Para eliminar un grupo de interfaces en particular selecciona el grupo de interfaces y clic en eliminar.

Manejo de licencias

La opción **Manejo de licencias** permite que tú administres las interfaces exportando datos NetFlow al NetFlow Analyzer, dependiendo de la licencia que se haya comprado.

La opcion visible debajo del menu **Operaciones admin** depende del nivel del usuario y como in grese este.

El cuadro estado en la parte superior de la pagina indica el tipo de licencia actualmente aplicado, el numero actual de interfaces administradas, y el numero de dias que permanecio la licencia expirada.

La lista de routers muestra todos los routers e interfaces desde el cual las exportaciones de NetFlow son recibidas, y cuales son administradas o no.

Administrando un router/interface

Seleccionar el router y todas las interfaces a ser chequeadas siguiendo el nombre del router. Para seleccionar una interface especifica, seleccione en el checkbox el nombre de la interface.

Una vez seleccionad la interface requerida, clic en el botón **Administrar** para administrar estas interfaces. Esto significa que los flujos recibidos desde estas interfaces van a ser procesados por el NetFlow Analyzer, y el grafico del tráfico y los reportes pueden ser generados.

El máximo numero de interfaces que se pueden administrar, dependen de la licencia actual aplicada.

No administrar un router/interface

Para seleccionar el router y todas las interfaces seleccione el nombre del router en el chekbox. Para seleccionar una interface especifica, seleccione el nombre de la interface en el chekbox.

Clic en el botón no manejar para no administrar esta interface. Esto significa que los flujos recibidos desde estas interfaces podrían ser parados por el NetFlow Analyzer. Una vez no administrada esta interface no se podrá ver en el Dashboard o escuchada en los grupos de

dispositivos. Sin embargo esta va a ser escuchada en la lista de routers de la página de manejar licencias

Eliminando un router / interface

Para seleccionar un router y todas las interfaces seleccionar el nombre del router en el chekbox. Para seleccionar una interface especifica seleccionar el nombre de la interface en el chekbox.

Clic en el boton **eliminar** para eliminar estas interfaces. Esto significa que estas interfaces son completamente removidas desde la pantalla del cliente NetFlow Analyzer.

Sin embargo si los flujos están empezando a ser enviados a la interface del NetFlow Analyzer, ellas reaparecerán en el dashboard. Para prevenir esto, se necesita deshabilitar la exportación de NetFlow para estas interfaces.

Licencias de nuevas interfaces

Si un paquete NetFlow es recibido desde una nueva interface, y el número de interfaces presentes administrables es menor que las permitidas en la licencia actual, estas interfaces son escuchadas en el interior de las listas del router en el dashboard con el mensaje que dice nuevos flujos han sido recibidos.

Tú necesitas entonces dar clic en la opción **Manejar licencias** y cambiar el estados administrado de estas interfaces en el orden en el que incluyen estas interfaces en la lista de interfaces administradas, y solo generan grafico de tráfico y reportes de los mismos.

Si los paquetes de NetFlow son recibidos desde una nueva interfaz, y el numero de interfaces administrables presentes son iguales que las permitidas en la licencia actual, se necesita no administrar una interface, y entonces administrar esta interface, o crear esta interface en un **Nuevo**

estado, el cualquier caso los gráficos y reportes pueden ser generados solo en interfaces administrables.

En cualquier momento se puede comprar más licencias dando clic en la imagen **Comprar en línea.**

Cambiar contraseña

La opción **cambiar contraseña** permite cambiar tu propia contraseña para ingresar a NetFlow Analyzer. Esto está disponible como una opción separada del menú de Operaciones de Admin, para usuarios que ingresaron como operadores o clientes. Para un usuario administrador, la contraseña puede ser cambiada desde la página Administración de usuarios.

Poner una nueva contraseña, confirmar esta, y clic en el botón **Actualizar** para guardar los cambios.

Ponga la nueva contraseña cuando se ingrese de nuevo al NetFlow Analyzer.

ANEXO 2: DESCRIPCION DE APLICACIONES

APLICACIONES MAS UTILIZADAS			
Aplicación	**Significado**	**Descripción**	**Puerto/ Protocolo**
http	Protocolo de transferencia de hipertexto	Es el protocolo usado en cada transacción de la Web (WWW)	80/TCP
microsoft-ds		Active Directory, compartición en Windows, gusano Sasser, Agobot)	445/tcp
microsoft-ds		Microsoft-DS compartición de ficheros	445/udp
netbios-ssn	NetBIOS (Network Basic Input/Output System) Servicio de sesiones	Es una especificación de interfaz para acceso a servicios de red. Permite a las aplicaciones 'hablar' con la red. Su intención es conseguir aislar los programas de aplicación de cualquier tipo de dependencia del hardware. También evita que los desarrolladores de software tengan que desarrollar rutinas de recuperación ante errores o de enrutamiento o direccionamiento de mensajes a bajo nivel.	139/tcp
netbios-ssn			139/udp
netbios-ns	NetBIOS Servicio de nombres.		137/tcp
netbios-ns			137/udp
ssh	Secure SHell, en español: intérprete de órdenes seguro	Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.	22/tcp
pptp	Point to Point Tunneling Protocol	Viene incluido con WindowsNT 4.0 Server y Workstation. Los Pc`s que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red publica como Internet. Una característica importante en el uso del PPTP es su soporte para VPN.	1723/tcp
kazaa		Es una aplicación para el intercambio de archivos Peer to Peer que utiliza el protocolo FastTrack. Kazaa es comúnmente utilizado para intercambiar música (principalmente en formato mp3) y	1214/tcp 1214/udp

		películas (en formato DivX).	
wins	Servicio de nombres Internet de Windows (WINS)	Es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red. A partir de Windows 2000 WINS ha sido relegado en favor de DNS y Active Directory	137 / UDP
soulseek		Es un programa y una red de intercambio de archivos informáticos usado primordialmente para compartir música, aunque permite el tránsito de toda clase de archivos. SoulSeek descansa en un servidor central; asimismo, carece completamente de spyware y de código malicioso, cuenta con una serie de características que lo diferencian en alguna medida de otros programas similares.	2234/tcp aunque el usuario lo puede cambiar
netmeeting		Es un cliente de videoconferencia VoIP y multipunto incluido en muchas versiones de Microsoft Windows (desde Windows 95 OSR2 hasta Windows XP).	Usa el protocolo H.323
Oracle		Es un sistema de gestión de base de datos relacional. Se considera a Oracle como uno de los sistemas de bases de datos más completos, destacando su: • Soporte de transacciones. • Estabilidad. • Escalabilidad. • Soporte multiplataforma.	1521/tcp 2005/udp
ms-sql-m	Microsoft-SQL-Monitor		1434/tcp 1434/udp
ms-sql-s	Microsoft-SQL-Server		1433/tcp 1433/udp
NFS	El Network File System (Sistema	es un protocolo de nivel de aplicación, según el Modelo OSI. Es utilizado para sistemas de	2049/tcp

	de archivos de red)	archivos distribuido en un entorno de red de computadoras de área local. Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales	
domain	Domain Name System (Sistema de Nombres de Dominio)	Es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS.	53/tcp 53/udp
nessus		Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Desde consola nessus puede ser programado para hacer escaneos programados con cron. En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo.	1241/tcp 1241/udp
icmp	Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol)	Es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.	
TCP_App	El porcentaje restante no se presenta ya que la herramienta distingue las aplicaciones más comerciales, cabe resaltar erramienta presenta porcentajes de utilización de aplicaciones que corren sobre TCP y UDP pero que no se las puede reconocer por su nombre comercial, entonces las junta en TCP_App o UDP_App.		
	Es una aplicación peer-to-peer. Los clientes de Direct Connect se conectan a un hub		

direct_connect	central. El protocolo está basado en FTP. Este hub contiene un listado de todos los clientes que se han conectado a él, y todos los archivos que están compartiendo. Al hacer una búsqueda en el hub, éste devuelve todos los archivos que tienen relación con el buscado y qué clientes lo poseen, y a continuación el cliente solicitante descarga el archivo en cuestión mediante FTP directamente desde el cliente que posee el archivo buscado, desvinculándose por completo el ordenador que hace de hub. No hay excesivos problemas con el ancho de banda.
webmethods	Integra Arquitectura Orientada a Servicios, (SOA), administración de procesos de negocio (BPM), y Legacy Modernization. Desarrollo menos codificado, un rehúso extendido de los recursos de TI, y un menor costo de operaciones, son las ventajas que ofrece la nueva suite. La profundidad y extensión de la suite de productos webMethods y el desempeño que entrega a la industria es incomparablemente competitivo.