ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO

ESCUELA DE POSTGRADO Y EDUCACION CONTINUA

"ANÁLISIS DEL PROTOCOLO NETFLOW Y SU APLICACIÓN EN LA DETERMINACIÓN DEL NIVEL DE USO DE LA RED DE DATOS DE LA FACULTAD DE MECÁNICA"

EDGAR ROBERTO MORALES MUCHAGALO

Tesis presentada ante la Escuela de Postgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del Grado de Magister en Interconectividad de Redes.

RIOBAMBA – ECUADOR

2013

ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO
CERTIFICACIÓN

EL TRIBUNAL DE TESIS CERTIFICA QUE:

El trabajo de investigación titulado "ANÁLISIS DEL PROTOCOLO NETFLOW Y SU APLICACIÓN EN LA DETERMINACIÓN DEL NIVEL DE USO DE LA RED DE DATOS DE LA FACULTAD DE MECÁNICA", de responsabilidad del Sr. EDGAR ROBERTO MORALES MUCHAGALO, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal de Tesis:

Dr. Juan Vargas _____
PRESIDENTE FIRMA

Ing. M. Sc. Marcelo Donoso _____
DIRECTOR FIRMA

Ing. M. Sc. Marcelo Allauca _____
MIEMBRO FIRMA

Dr. Alonso Álvarez _____
MIEMBRO FIRMA

Riobamba, Marzo 2013

DERECHOS INTELECTUALES

Yo, Edgar Roberto Morales Muchagalo, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en la presente Tesis, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

FIRMA
180249619-8

AGRADECIMIENTO

Mi agradecimiento más sincero a los miembros de mi tribunal de tesis por su colaboración en el desarrollo de esta investigación y de forma muy especial al Ing. Alberto L. Arellano A., quien supo orientarme en la investigación con total apego a su vocación de maestro.

DEDICATORIA

Este trabajo de investigación lo dedico en primer lugar a DIOS, ser supremo que sin sus bendiciones nada es posible; a mi MADRE a quien le debo todo en mi vida por ser la persona más maravillosa que Dios pudo darme para que sea mi ángel amoroso y fuerte, mi amiga y ejemplo diario de dedicación, honradez, responsabilidad y trabajo.

RESUMEN

La presente investigación analizó el protocolo NetFlow y su aplicación en la determinación del nivel de uso de la red de datos de la Facultad de Mecánica en la Escuela Superior Politécnica de Chimborazo.

Para cumplir con el objetivo se utilizó la arquitectura del protocolo de NetFlow y a través de la herramienta de monitoreo NetFlow Analizer se analizó el tráfico que atraviesa por la red. Estos datos fueron enviados por el Switch Catalyst 4507R, ubicado en el Data Center del Departamento de Sistemas y Telemática, hacia la estación de monitoreo de la Unidad de Computo de la Facultad de Mecánica utilizando el puerto UDP 9996, para su posterior caracterización.

Mediante el protocolo y la herramienta de monitoreo se obtuvieron datos que muestran el comportamiento de la red de datos durante los tres períodos de muestreo (en la mañana, medio día y tarde). Se determinó un mapa de aplicaciones que mostró que las redes de mayor generación de tráfico fueron: http y Microsoft-ds. Considerando los resultados medidos se desprendió que el porcentaje proyectado de crecimiento del número de paquetes para diciembre del año 2012 fue del 0,18%.

De lo expuesto se concluye que el equipo activo de red (switch Cisco 3560G) no necesita ser actualizado.

Se recomienda utilizar la metodología propuesta de planeación de capacidad de carga, para elaborar una guía de planeación de capacidad para la Intranet Institucional, con la finalidad de poder dimensionar los recursos de Networking que la institución necesitaría en los próximos años.

ABSTRACT

This research analyzed NetFlow protocol and its application in determining the level of network usage data of the Faculty of Mechanics at the Polytechnic University of Chimborazo.

To meet the objective a NetFlow protocol architecture with a monitoring tool to measure traffic across the network was used. These data were sent by Catalyst 4507R Switch, Data Center located in the Department of Systems and Telematics, to the central station of the Computer Unit of the Faculty of Mechanics using UDP port 9996, for further characterization.

By protocol and monitoring tool data that show the network behavior was obtained. These data were measured during three sampling periods (morning, midday and evening). It was determined, by a control map, that the networks with increased traffic generation were: http and Microsoft-ds. Considering this measured results, it emerged a projected percentage growth in the number of packages for December 2012 equivalent to 0.18%.

From the above results, it is concluded that the active network equipment (Cisco 3560G) need not be updated.

It is recommended the usage of this proposed methodology for capacity planning, to develop a capacity planning guide for Institutional Intranet, in order to gauge the Networking resources that the institution would need in the coming years.

INDICE DE ABREVIATURAS

AS	Sistema Autónomo (*Autonomous Systems*)
DESITEL	Departamento de Sistemas y Telemática
FTP	Es un protocolo de transferencia de archivos (*File Transfer Protocol*)
HTTP	Protocolo de Transferencia de Hipertexto (*Hyper Text Transfer Protocol)*
ICMP	Protocolo de Mensajes de Control de Internet o ICMP (*Internet Control Message Protocol*)
IP	Protocolo de Internet
IMAP	Protocolo de Acceso a Mensajes de Internet
LAN	Red de área local
MB	Mega Bytes
POP3	Protocolo 3 de Correo (*Post Office Protocol 3*)
PPS	Protocolo y parámetros de selección (Protocol and Parameter Selection)
P2P	Una red *peer-to-peer*, red de pares, red entre iguales, red entre pares o red punto a punto
RMON	Monitoreo remoto (*Remote Monitoring*)
RTT	Tiempo Límite de Renvió (*Resent Timeout Time*)
SCTP	Protocolo de transmisión de control de flujo (*Stream Control Transmission Protocol*)
SNMP	Protocolo de administración simple de red (*Simple Network Management Protocol*)
TCP/IP	Protocolo de control de transmisión/Protocolo de Internet
UDP	Protocolo de Datagrama de Usuario

INDICE GENERAL

LISTA DE FIGURAS

LISTA DE TABLAS

CAPITULO I

INTRODUCCIÓN

En los distintos planteles educativos a nivel universitario y empresarial a gran escala, la utilización de equipos de cómputo conectados mediante un dispositivo de red son de gran necesidad para las actividades que se desarrollan en las mismas y un mejor manejo de la información, ya que se tiene todo en forma compartida por medio de los equipos de la red. Conforme al avance de las tecnologías surgen mayores necesidades de servicios sobre la infraestructura de red y por ende los riesgos sobre la red de datos aumentan.

En el ámbito de las redes de datos hay un instrumento de trabajo que ha tomado una importante relevancia como es el protocolo NetFlow. Este instrumento ha comenzado a crecer para, en algunos casos, convertirse en una especie de "estándar" para el análisis de tráfico de la red y del nivel de utilización de los dispositivos. NetFlow a través de NetFlow Analyzer, permite recolectar información histórica referida al flujo de tráfico de la red, generar gráficos o tablas de información en función de tiempo, relevar el nivel de utilización de enlaces en función de subredes o monitorear el nivel de

utilización de un enlace.

Se trata de un protocolo propietario de Cisco soportado en la actualidad por 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.

Entre las aplicaciones posibles de NetFlow se pueden contar el monitoreo de la red, el monitoreo de aplicaciones específicas, el monitoreo de usuarios, el planeamiento de actualizaciones o modificaciones de la red, el análisis de seguridad, la implementación de sistemas de accounting y facturación, data warehousing y minig del tráfico de red, etc., lo que nos ayudara el un mejor manejo de los recursos de la red.

1.4 Problematización

Con el surgimiento de nuevas y más rápidas tecnologías de redes LAN, así como con la incorporación de nuevos servicios como telefonía IP, videoconferencia, educación virtual y comercio electrónico entre otras; han provocado que hoy en día se considere de fundamental importancia contar con una plataforma para el monitoreo detallado de las diferentes actividades que se realizan a diario en las redes.

El monitoreo meticuloso del tráfico que atraviesa por la red de datos mediante la medición del mismo, le permite al personal que administra la red determinar las aplicaciones y usuarios que mayor uso hacen de los recursos; así como de la posibilidad de definir matrices y patrones de tráfico que les permiten tener una fuente de información para encontrar anomalías en la red.

La Facultad de Mecánica distribuida en sus cuatro escuelas: Ingeniería Mecánica, Ingeniería Industrial, Ingeniería de Mantenimiento e Ingeniería Automotriz dispone de cuatro laboratorios conectados en red y que acceden a los recursos del BackBone institucional. En la actualidad la Facultad de Mecánica tiene una estructura de red tipo estrella, interconectados a través de enlaces de fibra óptica entre los edificios de las escuelas antes mencionadas; centralizada en la Unidad de Computo de la facultad a través de un proxy que brinda el acceso al servicio internet y a los servicios institucionales como: Sistema Académico, Recursos Humanos, Servicio Médico, entre otros. Cabe mencionar que la infraestructura de red de la facultad cuenta con equipos activos de red, de la siguiente manera: Ingeniería Mecánica un switch 3COM Baseline, Laboratorio de Internet un switch 3COM Baseline, Ingeniería Industrial un switch 3COM 4400, Ingeniería de Mantenimiento un switch 3COM 4400, Ingeniería Automotriz un switch Cisco 2960G y la Unidad de Computo un switch Cisco 3560G.

La facultad no cuenta con un sistema de monitoreo que permita ver el comportamiento de la red de datos y el uso del ancho de banda, por lo que a través de la investigación se desea detectar el comportamiento de la red y del uso del ancho de banda durante los períodos de uso de los laboratorios por parte de los estudiantes así como el determinar el tiempo que los equipos activos de la facultad pueden dar un perfomans adecuado de acuerdo a una proyección basado en los datos proporcionados por la herramienta de monitoreo.

1.5 Objetivos

1.5.1 Objetivo General

Analizar el protocolo NetFlow y su aplicación en la determinación del nivel de uso de la red de datos de la Facultad de Mecánica.

1.5.2 Objetivos Específicos

- Analizar la arquitectura del protocolo NetFlow para el análisis de flujos IP.
- Instalar y configurar el software de monitoreo de Flujos IP NetFlow Analyzer en la red de datos de la Facultad de Mecánica.
- Determinar los parámetros de rendimiento (aplicaciones y los usuarios con mayor uso de recursos) en la red de datos de la Facultad de Mecánica.
- Diseñar una propuesta de Planificación de Carga de la red de datos de la Facultad de Mecánica, con la finalidad de establecer el crecimiento futuro de infraestructura de la misma.

1.6 Justificación

El conocimiento del uso y de los recursos utilizados de las redes es sumamente importante para la gestión y planificación de las capacidades de las mismas. El entorno de red actual, dominado por la arquitectura TCP/IP, es muy dinámico y a diario aparecen nuevas aplicaciones que no solo brindan servicios tradicionales como las páginas web, correo electrónico o transferencia de ficheros; sino que trasponen al ámbito del comercio electrónico, los servicios multimedia, video vigilancia, telefonía IP, incluso sistemas de control y automatización de proceso en tiempo real.

Con la posibilidad del uso de los nuevos servicios que nos permiten las redes se crea un importante impacto en las infraestructuras académicas que a más de brindar servicios en las aéreas académicas y de investigación; incorporan servicios adicionales como Videoconferencia, E-learning y Telefonía IP. En ambos casos es necesaria el monitoreo del tráfico con la finalidad de determinar el uso de los recursos de la red.

NetFlow es un protocolo de red usado para **análisis y monitorización de redes** su propósito es recoger información de **tráfico IP** y enviar paquetes **UDP** y **SCTP (**los registros**)** a un servidor **NetFlow Collector** o **NetFlow Analyzer.**

Este protocolo es útil para los administradores ya que brinda la posibilidad de identificar el tráfico que pasa a través de la red y recopilar información sobre el uso del ancho de banda, el tipo de tráfico, el volumen de tráfico, cuellos de botella, información por protocolo, etc.

Cisco NetFlow puede recopilar información de acuerdo a una base muy granular y estos datos pueden analizarse para presentar dicha información como:

- Host principales (para cada una de las aplicaciones principales)
- Aplicaciones principales (para cada interfaz o grupo de interfaces)
- Volúmenes, velocidades y utilización de los datos (para interfaces, aplicaciones, hosts y conversaciones)

Justificación Aplicativa

La infraestructura de red de la Facultad de Mecánica se encuentra distribuida en cuatro laboratorios que corresponden a las escuelas de: Ingeniería Mecánica, Ingeniería Industrial, Ingeniería de Mantenimiento e Ingeniería Automotriz, además de sus correspondientes partes administrativas las mismas que acceden a los recursos del BackBone institucional y a los servicios que brinda el mismo.

La infraestructura de la Facultad consta en cada edificio correspondiente a las escuelas y a la parte administrativa de equipos activos conectados mediante enlaces de Fibra Óptica centralizados en su mayoría a la Unidad de Computo de la Facultad,

con excepción de la escuela de Ingeniería Automotriz que depende físicamente del DESITEL; pero operativa dependen todos los enlaces antes mencionados de los equipos principales de la Unidad de Computo.

Para la elaboración de la investigación se utilizará como principal herramienta al protocolo NetFlow el mismo que será instalado el Switch Multilayer 4507R que se encuentra ubicado en el Data Center del DESITEL, y que nos permitirá obtener información sobre:

- Análisis de red / planificación de la capacidad
- Supervisión de redes, servidores, aplicaciones / Solución de problemas

Para realizar la presente investigación se utilizara la red de datos de la Facultad de Mecánica, que tiene un direccionamiento de red 172.30.102.0/24 que está compuesto por los siguientes laboratorios:

Tabla I.1 Detalle de Host y Equipo activo

Dependencia	Host	Equipo Activo
Laboratorio de Internet	15	Switch 3COM Baseline
Laboratorio de Esc. Ing. Industrial	20	Switch 3COM 4400
Laboratorio de Esc. Ing. de Mantenimiento	20	Switch 3COM 4400
Laboratorio de Esc. Ing. Automotriz	22	Switch Cisco 2960G
Administrativos Facultad de Mecánica	24	Switch 3COM 4400
Unidad computo	3	Switch Cisco 2960G

Elaborado por: Autor
Fuente: Infraestructura de red Fac. Mecánica

En la figura I.1 se muestra los componentes de la arquitectura del protocolo NetFlow, en la infraestructura de la red de datos de la Facultad de Mecánica:

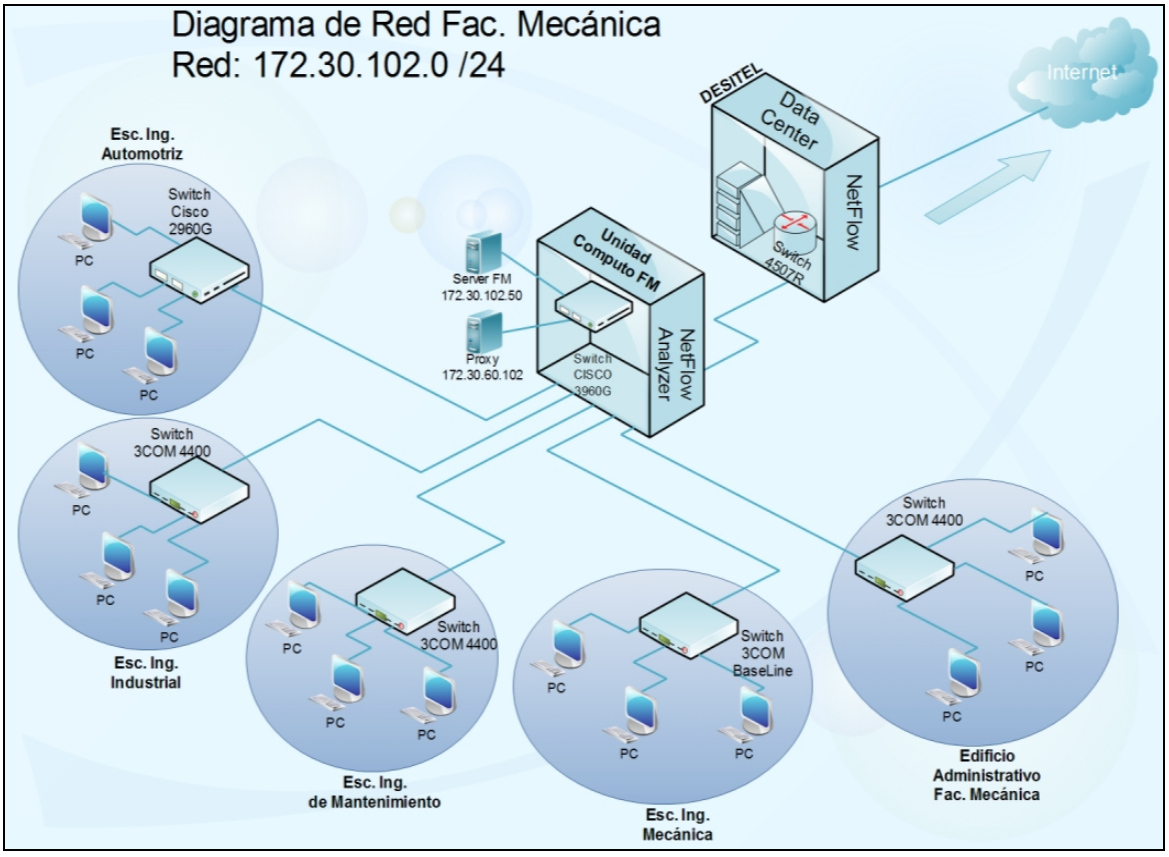


Figura I.1: Arquitectura NetFlow
Fuente: Autor

La infraestructura nos permitirá a través de NetFlow el análisis del tráfico que atraviesa la red de datos de la Facultad de Mecánica con la finalidad de determinar el mapa de aplicaciones y de usuarios; y los períodos de mayor demanda del ancho de banda y en base a esto poder determinar el tiempo que mantendrá el performans el equipo activo.

CAPITULO II

REVISIÓN DE LITERATURA

2.1 NetFlow

NetFlow [11] es un protocolo de red usado para análisis y monitorización de redes inicialmente desarrollado por Cisco System. Aunque también es compatible con muchos otros dispositivos de redes lo que hace posible desplegarlo en plataformas como FreeBSD, OpenBSD, Juniper, Alcatel, Foundry etc.

El propósito de NetFlow es recoger información de tráfico IP y enviar paquetes UDP y SCTP (los registros) a un servidor NetFlow Collector o NetFlow Analyzer.

NetFlow es útil para los administradores ya que nos brinda la posibilidad de tener el tráfico que pasa a través de la red y recopilar información sobre el uso del ancho de banda, el tipo de tráfico, el volumen de tráfico, cuellos de botella, información por protocolo, etc.

Cisco define un flujo de datos como una secuencia unidireccional de paquetes que comparten 5 elementos en común:

- Dirección IP de origen.
- Dirección IP destino.
- Número de puerto de origen.
- Número de puerto de destino.
- Protocolo

Cisco NetFlow puede recopilar información de acuerdo a una base muy granular y estos datos pueden analizarse para presentar dicha información como:

- Host principales (para cada una de las aplicaciones principales)
- Conversaciones principales (para cada una de las aplicaciones principales)
- Aplicaciones principales (para cada interfaz o grupo de interfaces)
- Volúmenes, velocidades y utilización de los datos (para interfaces, aplicaciones, hosts y conversaciones)
- Marcas ToS (utilizadas frecuentemente para ciertas aplicaciones como Voz y Vídeo)

En la siguiente figura se describe la información que se puede registrar mediante NetFlow:

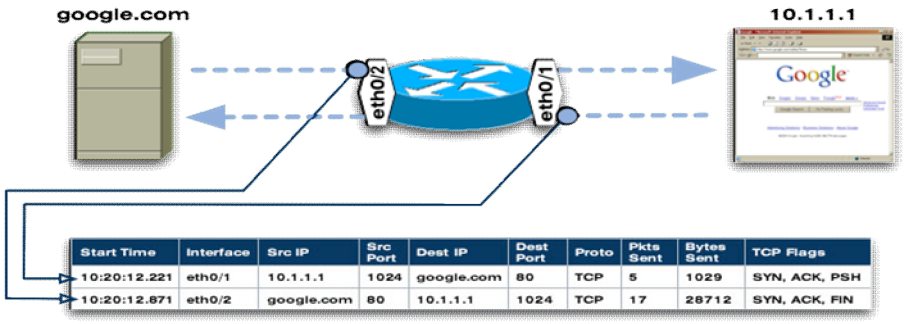


Figura II. 1: Descripción de NetFlow
Fuente: http://es.wikipedia.org/wiki/netflow

Entre las aplicaciones posibles de NetFlow se pueden contar el monitoreo de la red, el monitoreo de aplicaciones específicas, el monitoreo de usuarios, el planeamiento de actualizaciones o modificaciones de la red, el análisis de seguridad, la implementación de sistemas de accounting y facturación, data warehousing y minig del tráfico de red, etc.

2.1.1 Aplicaciones de NetFlow [14]

NetFlow proporciona los datos necesarios para analizar, representar tendencias y establecer líneas de base sobre datos de las aplicaciones a medida que recorren la red. Luego, pueden exportarse a un paquete de generación de informes y también pueden ofrecer la información necesaria para gestionar aplicaciones comerciales críticas. El tipo de información que NetFlow puede proporcionar incluye [10]:

- 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 en la red.

En la figura se muestra los componentes de la arquitectura de la tecnología NetFlow:

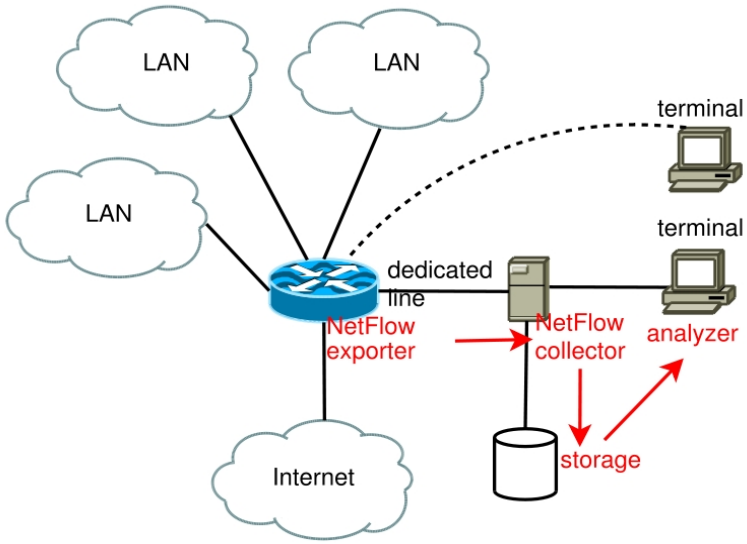


Figura II-2: Arquitectura NetFlow
Fuente: http://www.ecured.cu/index.php/Netflow

2.1.3 Herramienta de Monitoreo NetFlow Analyzer [12]

NetFlow Analyzer es una solución de monitoreo de redes basada en tecnología NetFlow de Cisco. Utilizando la información NetFlow de los dispositivos compatibles, NetFlow Analyzer otorga visibilidad sobre qué aplicaciones están consumiendo ancho de banda, quién las está utilizando y durante cuánto tiempo. Permite ver rápidamente la causa de congestión de red y ayuda a evitar problemas y optimizar los recursos de red.

NetFlow Analyzer es con lo que el mundo de los negocios cuenta para optimizar su red para un alto rendimiento. Para sacarle el mejor provecho a su red necesita una visión profunda de la misma. Es justamente lo que NetFlow Analyzer ofrece: Una visión sin igual de su red en tiempo real y una visión detallada del impacto del tráfico de su red

en el buen estado de la red entera. Esta información le permite señalar instantáneamente las causas de los incidentes en la red, entender los patrones del desempeño de la red, tomar decisiones correctas en cuanto a la planeación de la capacidad y ahorrar tiempo.

Permite analizar la utilización de ancho de banda y ofrece visibilidad completa sobre routers y switchs Cisco. Gracias a sus informes detallados y gráficos en tiempo real, NetFlow Analyzer proporciona información muy completa sobre el tráfico de red, sin necesidad de utilizar sondas.

La figura II.3 muestra un ejemplo de los reportes gráficos generados por la aplicación:

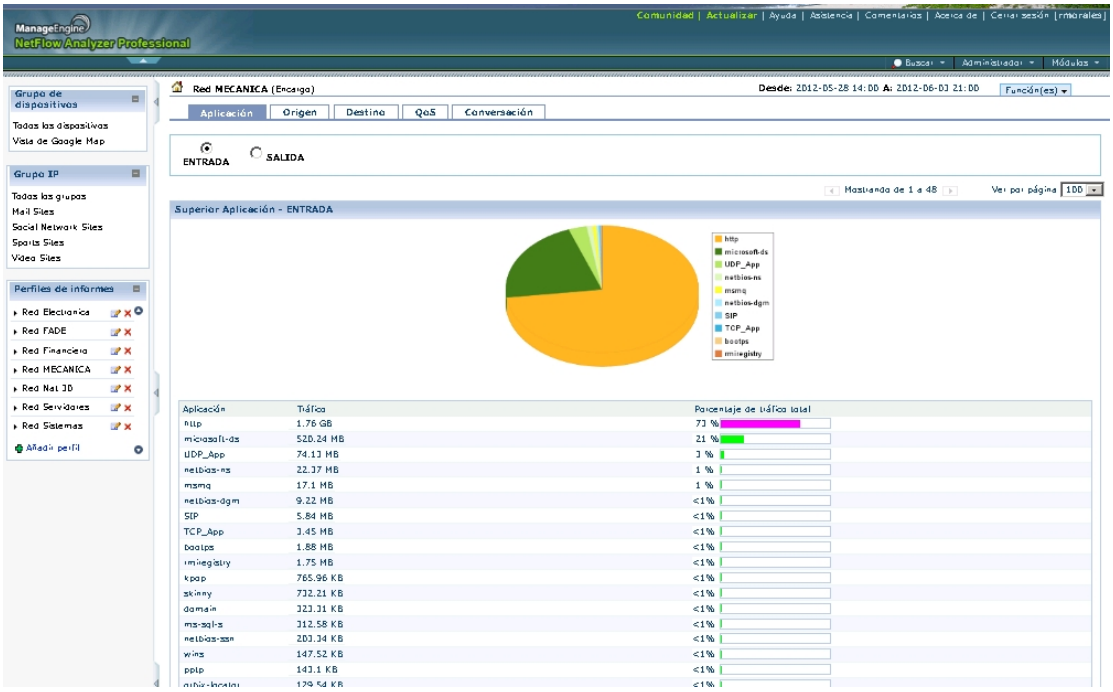


Figura II.3 Reportes generados por NetFlow Analyzer
Fuente: Autor (Captura de Pantalla)

Las características de la herramienta NetFlow Analyzer se describen a continuación [5]:

- Alertas personalizables basadas en niveles y umbrales: Se generan alertas

cuando la utilización de tráfico supera los parámetros definidos por el usuario. Envía los traps SNMP a otras aplicaciones para las alertas críticas.

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

2.5 Monitoreo de red [15]

El término **Monitoreo de red** describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico, pager u otras alarmas. Es un subconjunto de funciones de la administración de redes.

Mientras que un sistema de detección de intrusos monitorea una red por amenazas *del exterior* (externas a la red), un sistema de monitoreo de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web, el software de monitoreo puede enviar periódicamente peticiones HTTP (*Protocolo de Transferencia de Hipertexto*) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (*Protocolo de Transferencia de Correo Simple*), para luego ser retirados mediante IMAP (*Protocolo de Acceso a Mensajes de Internet*) o POP3 (*Protocolo Post Office*).

Comúnmente, los datos evaluados son: tiempo de respuesta y disponibilidad (o uptime), aunque estadísticas tales como consistencia y fiabilidad han ganado popularidad. La generalizada instalación de dispositivos de optimización para Redes de área extensa tiene un efecto adverso en la mayoría del software de monitoreo, especialmente al intentar medir el tiempo de respuesta de punto a punto de manera precisa, dado el límite visibilidad de ida y vuelta.

Fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitoreo. Estas acciones pueden variar: una alarma puede ser enviada al administrador, ejecución automática de mecanismos de controles de fallas, etc.

Monitorear la eficiencia del estado del enlace de subida se denomina *Medición de tráfico de red.*

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 administrador de redes.

Existen muchos sistemas que son capaces de examinar el tráfico de manera exhaustiva y detectar actividades maliciosas, monitorear complejas métricas de desempeño, o capturar trazas del tráfico. Una técnica que en la actualidad está siendo muy utilizada, es la medición pasiva incorporando la utilización de flujos, como elementos de agregación de la información, pues muestra grandes ventajas, determinadas por su poca interacción con el tráfico que se quiere analizar, los relativamente pequeños niveles de almacenamiento que se necesitan, y otras consideraciones adicionales sobre la confidencialidad y privacidad de la información.

2.5.1 Tipos de Monitoreo de Redes

Existen al menos dos puntos de vista para abordar el proceso de monitorear una red: un enfoque activo y un enfoque pasivo.

2.5.1.1 Monitoreo Activo

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

Las técnicas utilizadas para el monitoreo activo incluye las siguientes:

- Basadas en ICMP
  - ✓ Diagnosticar problemas en la red

- ✓ Detectar retardos y perdidas de paquetes
- ✓ RTT
- ✓ Disponibilidad de hosts y redes

- Basados en TCP
  - ✓ Tasa de transferencia
  - ✓ Diagnosticar problemas a nivel de aplicación
- Basados en UDP
  - ✓ Pérdida de paquetes en un sentido (one way)
  - ✓ RTT (traceroute)

2.5.1.2 Monitoreo Pasivo

Se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como sniffers, ruteadores, computadores con software de análisis de tráfico y en general dispositivos con soporte de snmp, rmon y NetFlow. Esta perspectiva no agrega tráfico en la red como lo hace el monitoreo activo. Es utilizado para caracterizar el tráfico en la red y para registrar su uso.

Las técnicas utilizadas para el monitoreo pasivo incluye las siguientes:

- Solicitudes remotas

  Mediante SNMP, esta técnica es utilizada para obtener estadísticas sobre la utilización del 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 indica que un evento inusual se ha producido.

- Captura de trafico

  Se puede llevar a cabo de dos formas: 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 realizara la captura; o también 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 más 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).

2.6 Análisis de Flujos IP [19]

Un flujo IP es una secuencia unidireccional de paquetes con ciertas características comunes que incluye:

- Direcciones IP de origen y destino
- Número de puerto origen y destino
- Índice de la interfaz de entrada
- Byte del Tipo de Servicio
- Nombre de la interfaz lógica de entrada

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

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

El internet se ha convertido como la red telemática más extendida y utilizada a nivel mundial. El crecimiento de la infraestructura y del número de usuarios conectados ha sido vertiginoso; y este crecimiento ha dado lugar al crecimiento de un conjunto de nuevos servicios y aplicaciones y nuevos paradigmas, como las comunicaciones peer-to-per, P2P. Al mismo tiempo ha dado lugar al surgimiento de amenazas, en la forma de ataques de seguridad a través de la red.

Para realizar el análisis de la seguridad de las redes de datos, existen muchas 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 y guarda o renvía los flows a otros colectores.

Analizador.- Filtra, muestra, analiza y/o gráfica los datos.

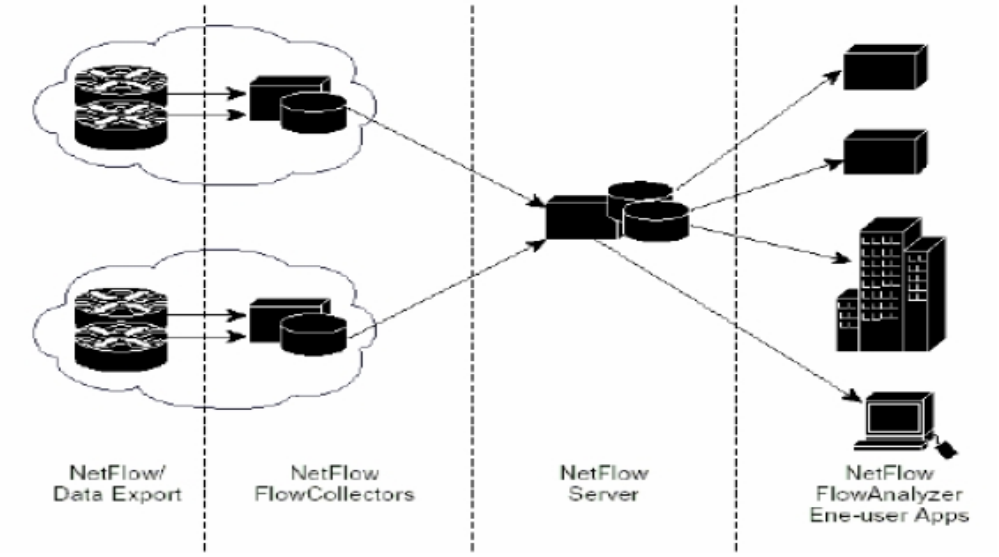


Figura II.4: Arquitectura del análisis
Fuente: http://www.universidadcarlosIII.com/area_ingenieria/mira/

2.7 Planificación de Carga

El dimensionamiento de las redes de comunicaciones es una tarea esencial a la hora de su despliegue, de forma que se pueda planificar la capacidad necesaria de dicha red para atender las necesidades de sus usuarios. [4] Sin embargo, dimensionar redes de datos que soporten tráfico de Internet no es una actividad que actualmente cuente con herramientas adecuadas, debido en parte a las características altamente variantes de dicho tráfico. Además, la aparición de nuevas aplicaciones y tecnologías de soporte hacen que dimensionados pasados no sean útiles a medida que evolucionen las redes.

El objetivo de la planeación de la capacidad es asegurar que el contenido puede llegar a todos los usuarios sin retrasos ni interrupciones. La planeación de la capacidad se

basa en tres variables: volumen de la audiencia, tipo y tamaño del contenido, y número y velocidad de los servidores. En la mayoría de los casos, la planeación de la capacidad se usa para determinar los requisitos del servidor necesarios para ofrecer una cantidad de contenido a una audiencia seleccionada, aunque se puede decidir una planeación para determinar otras variables bajo determinadas circunstancias.

Se puede estimar la capacidad de red necesaria con la siguiente fórmula [17]:

Capacidad de red necesaria = Velocidad en bits del contenido × número estimado de clientes

En ocasiones éste servicio puede estar estrechamente relacionado con el Servicio de Monitoreo y Análisis, con el fin de determinar la “salud” de la red de datos. De ésta forma, se podrá planificar futuros cambios en la red, basados en el conocimiento preciso del estado actual de la misma.

CAPITULO III

MATERIALES Y MÉTODOS

3.1. Diseño de la investigación

La investigación a realizarse es cuasi-experimental ya que los contenidos a ser enviados en el entorno de pruebas no serán tomados al azar, sino que se los tendrá definidos antes de realizar dicho entorno.

3.2. Tipo de estudio

Por la naturaleza de la investigación se considera que el tipo de estudio que se va a realizar es una investigación descriptiva y aplicada; ya que se utilizará el conocimiento conceptual para realizar un estudio de la tecnología de análisis de flujos IP, con la finalidad de determinar el uso de los recursos de la red e implementar una plataforma de monitoreo en la red de datos de la Facultad de Mecánica.

3.4. Métodos, Técnicas e Instrumentos

3.3.1 Métodos

Para este proyecto se utilizarán los siguientes métodos de investigación:

Método Científico: Se utilizará este método ya que las ideas, conceptos, y teorías expuestas en la investigación son verificables, además que servirá para recopilar la información necesaria para determinar el uso de los recursos de la red de datos de la Facultad de Mecánica.

Método Deductivo: Debido que al estudiar en forma general la tecnología de análisis de flujos IP mediante el protocolo NetFlow, nos permitirá determinará el procedimiento adecuado para la implementación de la plataforma de monitoreo de la red de datos de la Facultad de Mecánica.

3.5.2 Técnicas

Además se utilizará las técnicas que se detallan a continuación:

- Observación
- Razonamiento
- Recopilación de información.
- Análisis
- Pruebas

3.5.3 Fuentes de Información

- Textos
- Revistas especializadas
- Documentos de Internet

3.5.4 Instrumentos

- Guías
- Manuales técnicos
- NetFlow
- MySQL
- NetFlow Analyzer
- NetFlow Exporter
- NetFlow Collector

3.5. PLANTEAMIENTO DE LA HIPÓTESIS

3.5.1. Hipótesis

La utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica, permitirá determinar el adecuado nivel de utilización de la infraestructura de la red.

3.5.2. Operacionalización Conceptual.

VARIABLE	TIPO	DEFINICIÓN
Utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica.	Independiente	Protocolo para el análisis de flujos IP, que permitirá la medición de las cargas de consumo de los recursos de red y el monitoreo de redes de datos.
Nivel de utilización de la infraestructura de la red.	Dependiente	Análisis e interpretación de resultados obtenidos a través de la herramienta de monitoreo.

3.5.3. Operacionalización Metodológica.

HIPÓTESIS	VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTOS
La utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica, permitirá determinar el adecuado nivel de utilización de la infraestructura de la red.	**V. Independiente** Utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica.	✚ Arquitectura de la tecnología ✚ Captura de datos ✚ Recolección de datos ✚ Análisis de datos	✚ Observación ✚ Razonamiento ✚ Recopilación de información. ✚ Análisis	✚ Guías ✚ Manuales Técnicos ✚ Netflow ✚ Netflow Exporter
	V. Dependiente Nivel de utilización de la infraestructura de la red.	✚ Carga de trafico útil ✚ Carga entrante y saliente de las aplicaciones ✚ Aplicaciones con mayor consumo ✚ Usuarios con mayor consumo ✚ Ancho de banda	✚ Medición de tráfico ✚ Pruebas ✚ Generación de Reportes	✚ NetFlow ✚ NetFlow Exporter ✚ NetFlow Collector ✚ NetFlow Analyzer ✚ MySQL

3.6. POBLACIÓN Y MUESTRA

3.6.1. Población

La población considerada para la investigación son: los hosts de los laboratorios, el equipo activo de red (ver Tabla I.1), las diferentes aplicaciones (http, microsoft-ds, netbios-ssn, UDP_App, netbios-ns, SIP, TCP_App, bootps, etc.) y usuarios que tienen acceso a la infraestructura de datos de la Facultad de Mecánica y el efecto que tienen los mismos sobre el ancho de banda asignado; a través del protocolo NetFlow y de la herramienta de análisis de tráfico NetFlow Analyzer.

3.6.2. Muestra

La muestra para la investigación, corresponde al análisis del tráfico que se realizó en las dependencias que para el efecto se eligieron de forma planificada (ver Tabla I.1), por ser las que generan el mayor consumo de recursos de la infraestructura de red de la Facultad de Mecánica en el mes de Junio, tiempo durante el cual se analizó las aplicaciones que mayor uso tenían y los usuarios que con mayor frecuencia accedían a la infraestructura; y a partir de esta información ver el uso del ancho de banda.

3.7. VALIDACIÓN DE INSTRUMENTOS

La validez permitira definir el grado de aceptación que el instrumento tiene al medir una variable. La herramienta de monitoreo es validada, fundamentada en la investigación de la misma en el sitio web de la compania cisco systems[1]; en la que se realizó la evaluación de las herramientas comerciales que soporta el NetFlow. NetFlow Analyzer es una poderosa herramienta de monitoreo de redes de datos que permiten

[1] http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps6601/

tener una visión completa y detallada del tráfico que se va generando dentro de la red; existe una gran cantidad de empresas[2] que usan esta herramienta de monitoreo, entre las principales tenemos: Movistar, Microsoft, Cisco Systems, Fedex, DHL, etc.

3.8. PROCESAMIENTO DE LA INFORMACIÓN

Para el procesamiento de la información partimos de la recolección de datos a través de una base de datos que almacena NetFlow en MYSQL; en la estación de monitoreo para su posterior uso.

Para el análisis de los datos se usó el software de monitoreo NetFlow Analyzer 9.0; el cual se instaló en la estación de monitoreo que físicamente está ubicada en el edificio de la Unidad de Computo de la Facultad de Mecánica; para a través de la interfaz web de la herramienta proceder a extraer la información sobre:

- Carga de tráfico útil
- Carga entrante y saliente de las aplicaciones
- Aplicaciones con mayor consumo
- Usuarios con mayor consumo
- Ancho de banda

El tráfico fue analizado del 4 al 29 de Junio del 2012, divido en tres períodos:

Tabla III.2 Períodos de análisis

Período	Horario
Mañana	07:00 a 12:00
Medio día	13:00 a 14:00
Tarde	15:00 a 21:00

Realizado por: Autor
Fuente: Períodos de Monitoreo considerados

[2] http://manageengine.adventnet.com/products/netflow/customers.html

CAPITULO IV

ANÁLISIS E INTEPRETACIÓN DE RESULTADOS

4.1 PROCESAMIENTO DE LA INFORMACIÓN

Con la finalidad de caracterizar y determinar el uso del ancho de banda de la red de datos de la Facultad de Mecánica se realizaron las pruebas de monitoreo correspondientes, mediante el uso de la herramienta NetFlow Analyzer la cual recolecta los flujos IP que son enviados por el switch CISCO Catalyst 4507R que físicamente se encuentra ubicado en el Data Center del Departamento de Sistemas y Telemática; ya que este es el único dispositivo que soporta la tecnología NetFlow dentro de la infraestructura de red existe en la ESPOCH.

La exportación de los flujos IP se realizó mediante el puerto UDP 9996, hacia la estación de monitoreo ubicado en la Unidad de Computo de la Facultad de Mecánica. En la herramienta de monitoreo NetFlow se creó un grupo para toda la red IP de la Facultad de Mecánica; como se muestra en la tabla:

Tabla IV.3 Grupos IP Definidos en la Herramienta de Monitoreo

Grupo IP	Dirección de Subred	Máscara de Subred
Mecánica	172.30.60.102	255.255.255.0

Realizado por: Autor
Fuente: DESITEL

Para cuantificar los indicadores de la variable dependiente y poder caracterizar el tráfico en la red, se analizó los siguientes índices:

- Carga de trafico útil
- Carga entrante y saliente de las aplicaciones
- Aplicaciones con mayor consumo
- Usuarios con mayor consumo
- Ancho de banda

4.2 DETERMINACIÓN DE LA CARGA DE TRÁFICO

Se realizó el análisis del tráfico de entrada y salida total, generado por la red de datos de la Facultad de Mecánica. El análisis se lo realizo para cada una de las cuatro semanas de monitoreo, durante 3 períodos: mañana, medio día y en la tarde; como se muestra en la Tabla III.2. El tráfico esta medido en Megabytes.

4.2.1 GRUPO IP: MECÁNICA

Semana 1: 7/06/2012 – 11/06/2012

Horario: 07:00 – 12:00

Tabla IV.4 Resumen de tráfico en MB 4 al 8 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
4 Junio	0,8440527	9,7455762	10,59

5 Junio	0,7415137	11,2165039	11,96
6 Junio	0,9094434	13,7486719	14,66
7 Junio	0,6450293	10,2508008	10,90
8 Junio	0,4902051	6,9745313	7,46
	TOTAL:		55,57

Realizado por: Autor
Fuente: Netflow Analyzer

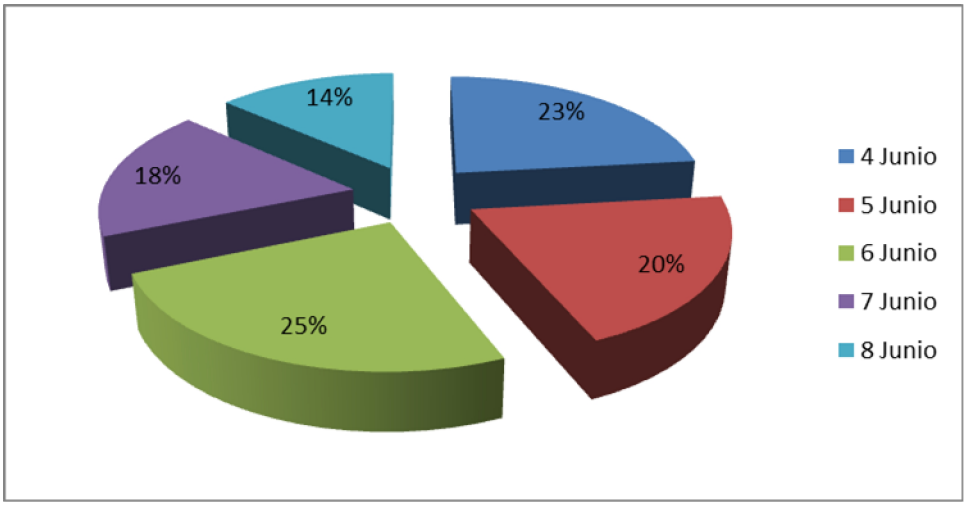


Figura IV.1 Distribución de tráfico de ENTRADA en MB 4 al 8 de Junio

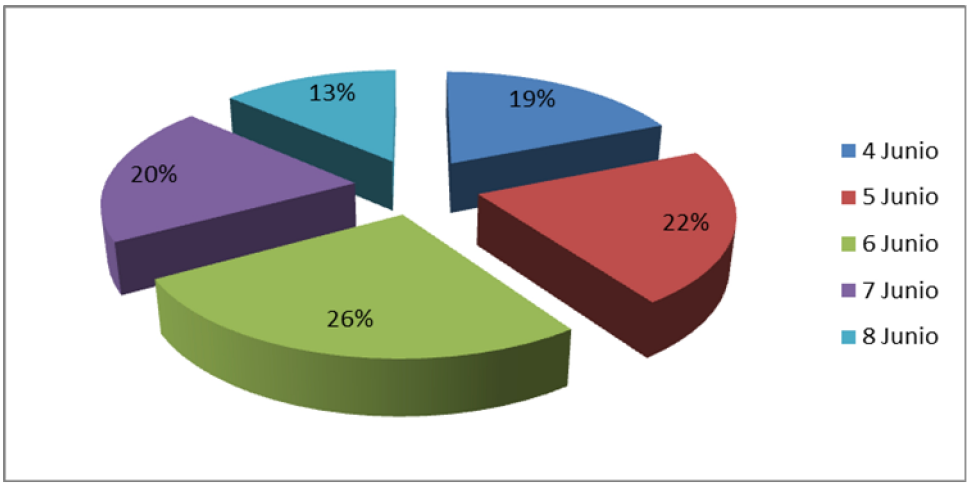


Figura IV.2 Distribución de tráfico de SALIDA en MB 4 al 8 de Junio

Como se puede observar en la tabla IV.4 y en las figuras IV.1 y IV.2 el día 6 de Junio es el de mayor consumo, con 0,91 y 13,75 Megabytes que corresponde al 25% y 26% del tráfico de Entrada y Salida respectivamente.

Semana 1: 4/06/2012 – 8/06/2012

Horario: 13:00 – 14:00

Tabla IV.5 Resumen de tráfico en MB 4 al 8 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
4 Junio	0,16128	3,09000	3,25
5 Junio	0,13616	2,89000	3,03
6 Junio	0,11798	2,54000	2,66
7 Junio	0,09805	4,92790	5,03
8 Junio	0,08021	2,02382	2,10
	TOTAL:		16,07

Realizado por: Autor
Fuente: Netflow Analyzer

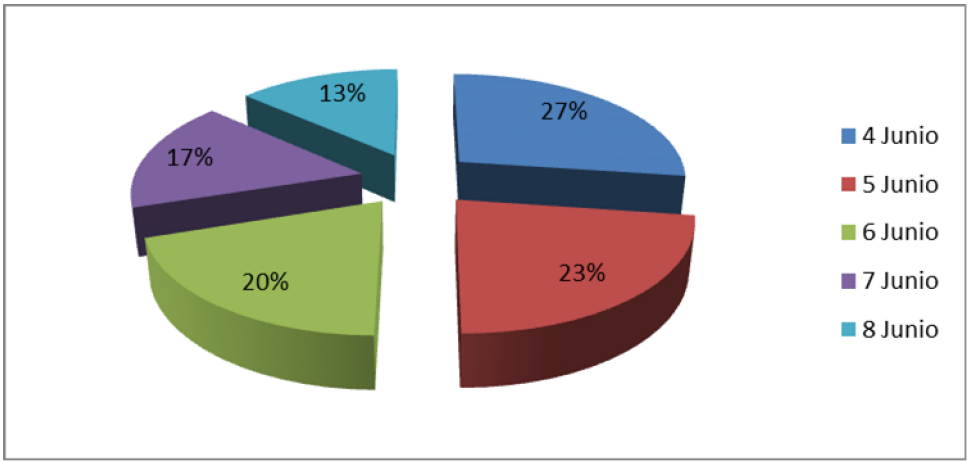


Figura IV.3 Distribución de tráfico de ENTRADA en MB 4 al 8 de Junio

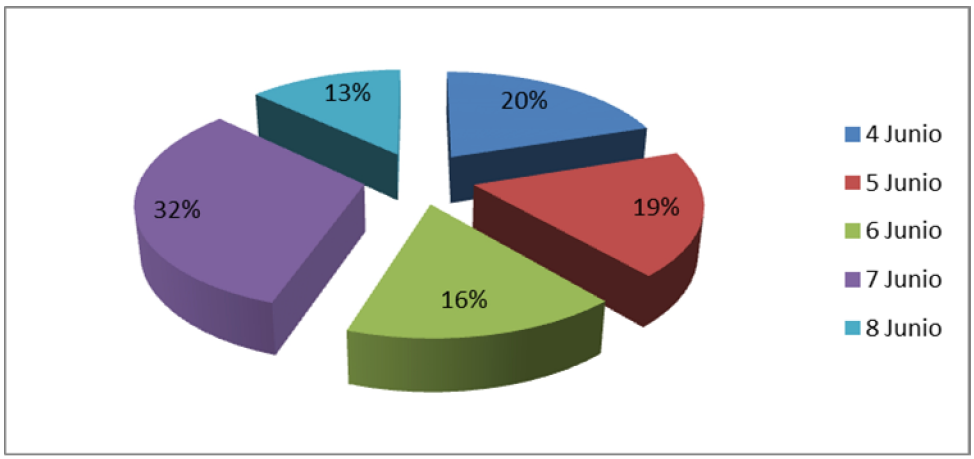


Figura IV.4 Distribución de tráfico de SALIDA en MB 4 al 8 de Junio

Como se puede observar en la tabla IV.5 y en las figuras IV.3 y IV.4 los días 4 y 7 de Junio son los de mayor consumo, con 0,16 y 4,93 Megabytes que corresponde al 27% y 32% del tráfico de Entrada y Salida respectivamente.

Semana 1: 4/06/2012 – 8/06/2012

Horario: 15:00 – 21:00

Tabla IV.6 Resumen de tráfico en MB 4 al 8 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
4 Junio	0,7418262	13,2502539	13,99
5 Junio	0,6750977	8,5646680	9,24
6 Junio	0,7588867	17,4005664	18,16
7 Junio	0,8383691	18,0357129	18,87
8 Junio	0,3621484	2,1738184	2,54
	TOTAL:		62,80

Realizado por: Autor
Fuente: Netflow Analyzer

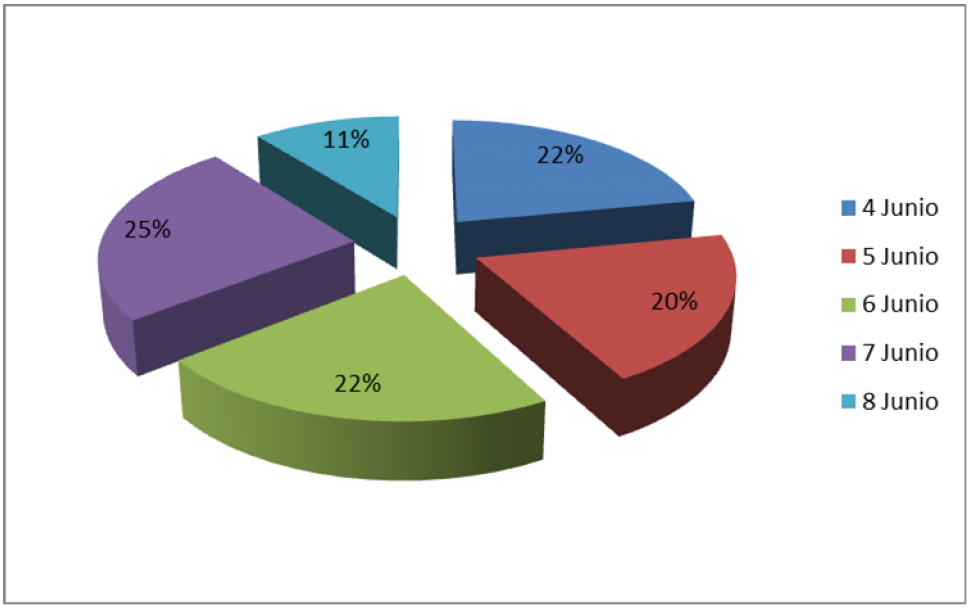


Figura IV.5 Distribución de tráfico de ENTRADA en MB 4 al 8 de Junio

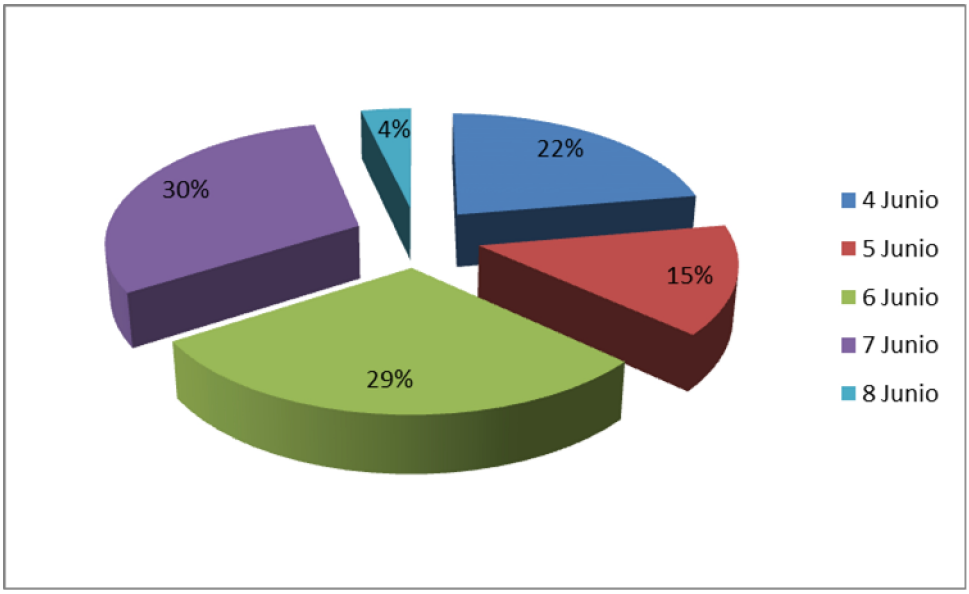


Figura IV.6 Distribución de tráfico de SALIDA en MB 4 al 8 de Junio

Como se puede observar en la tabla IV.6 y en las figuras IV.5 y IV.6 el día 7 de Junio es el mayor consumo, con 0,8383691 y 18,0357129 Megabytes que corresponde al 25% y 30% del tráfico de Entrada y Salida respectivamente.

Semana 2: 11/06/2012 – 15/06/2012

Horario: 07:00 – 12:00

Tabla IV.7 Resumen de tráfico en MB 11 al 15 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
11 Junio	336,20	5698,74	6034,94
12 Junio	355,94	5188,40	5544,34
13 Junio	425,02	8800,79	9225,81
14 Junio	301,10	5284,11	5585,21
15 Junio	249,25	4096,78	4346,03
	TOTAL:		30736,33

Realizado por: Autor
Fuente: Netflow Analyzer

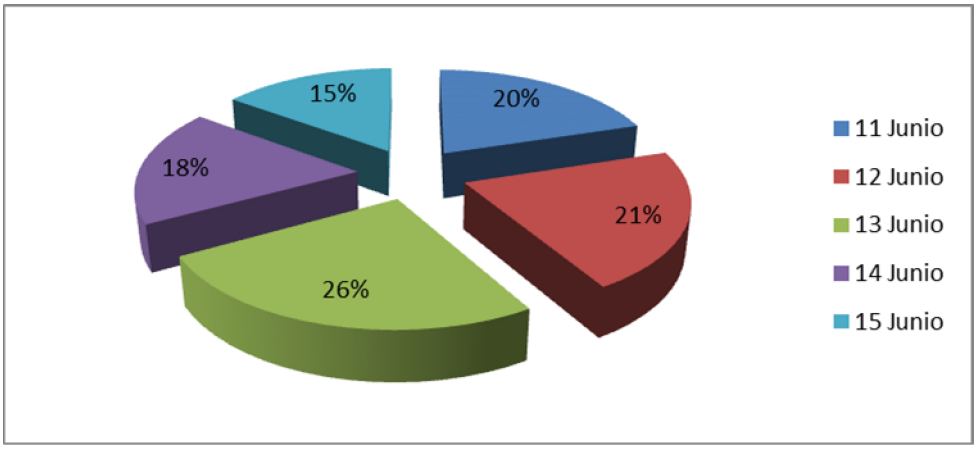


Figura IV.7 Distribución de tráfico de ENTRADA en MB 11 al 15 de Junio

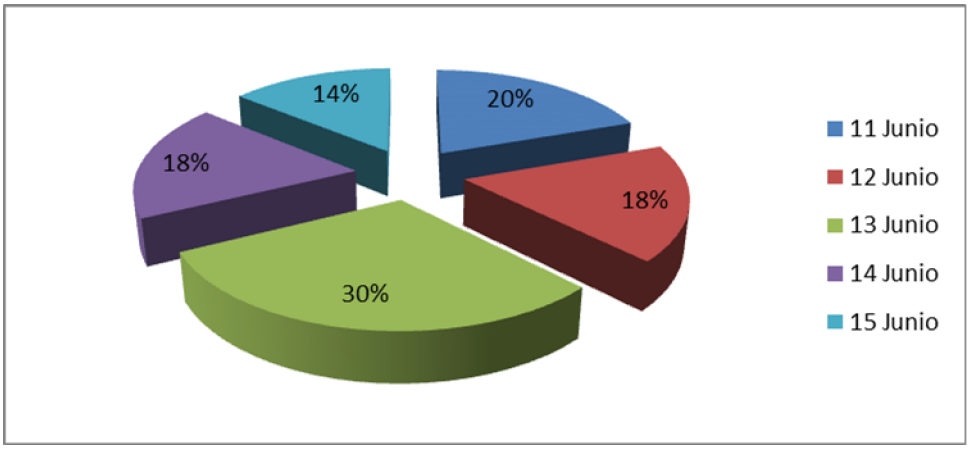


Figura IV.8 Distribución de tráfico de SALIDA en MB 11 al 15 de Junio

Como se puede observar en la tabla IV.7 y en las figuras IV.7 y IV.8 el día 13 de Junio es el mayor consumo, con 425,02 y 8800,79 Megabytes que corresponde al 26% y 30% del tráfico de Entrada y Salida respectivamente.

Semana 2: 11/06/2012 – 15/06/2012

Horario: 13:00 – 14:00

Tabla IV.8 Resumen de tráfico en MB 11 al 15 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
11 Junio	13,49	69,49	82,98

12 Junio	35,82	755,09	790,91
13 Junio	254,29	2343,40	2597,69
14 Junio	44,55	898,50	943,05
15 Junio	36,36	346,89	383,25
	TOTAL:		4797,88

Realizado por: Autor
Fuente: Netflow Analyzer

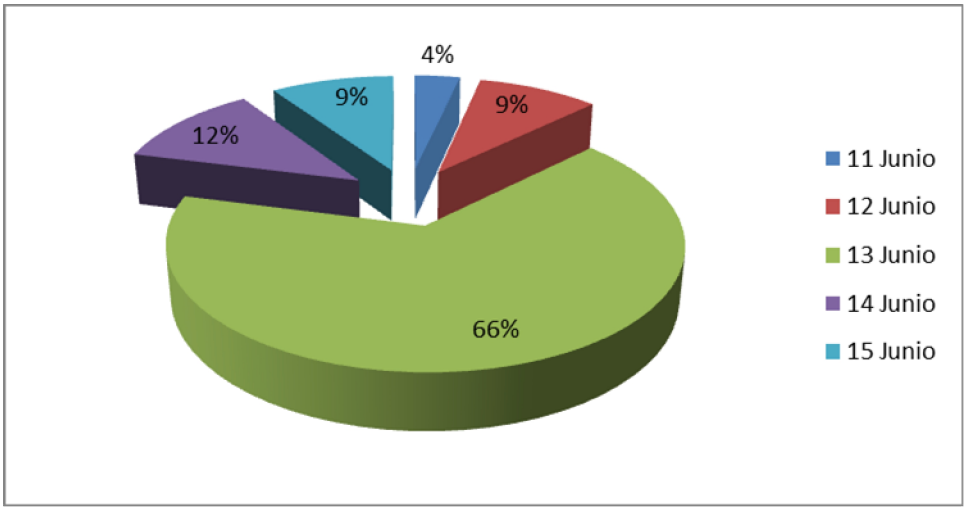


Figura IV.9 Distribución de tráfico de ENTRADA en MB 11 al 15 de Junio

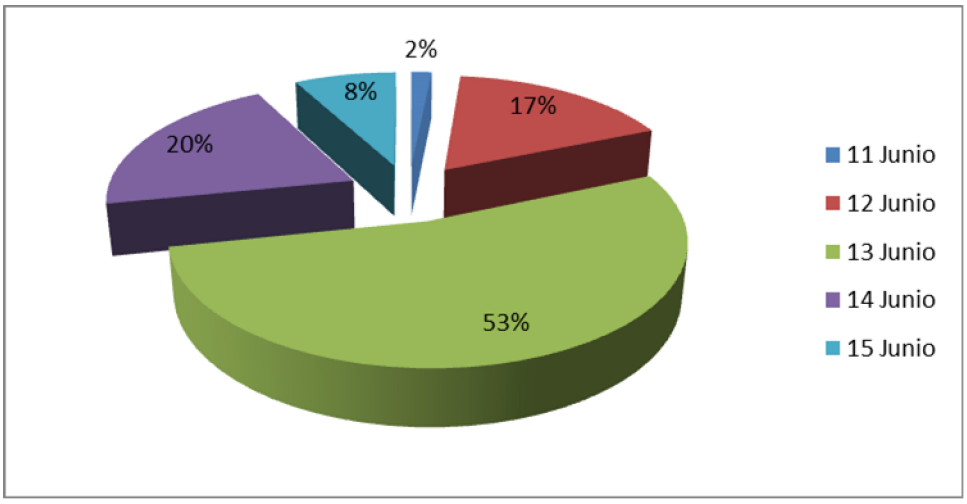


Figura IV.10 Distribución de tráfico de SALIDA en MB 11 al 15 de Junio

Como se puede observar en la tabla IV.8 y en las figuras IV.9 y IV.10 el día 13 de Junio es el mayor consumo, con 254,29 y 2343,40 Megabytes que corresponde al 66% y 53% del tráfico de Entrada y Salida respectivamente.

Semana 2: 11/06/2012 – 15/06/2012

Horario: 15:00 – 21:00

Tabla IV.9 Resumen de tráfico en MB 11 al 15 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
11 Junio	129,74	1349,41	1479,15
12 Junio	437,41	9110,37	9547,78
13 Junio	362,53	7115,42	7477,95
14 Junio	382,41	11017,69	11400,10
15 Junio	104,35	1283,83	1388,18
	TOTAL:		31293,16

Realizado por: Autor
Fuente: Netflow Analyzer

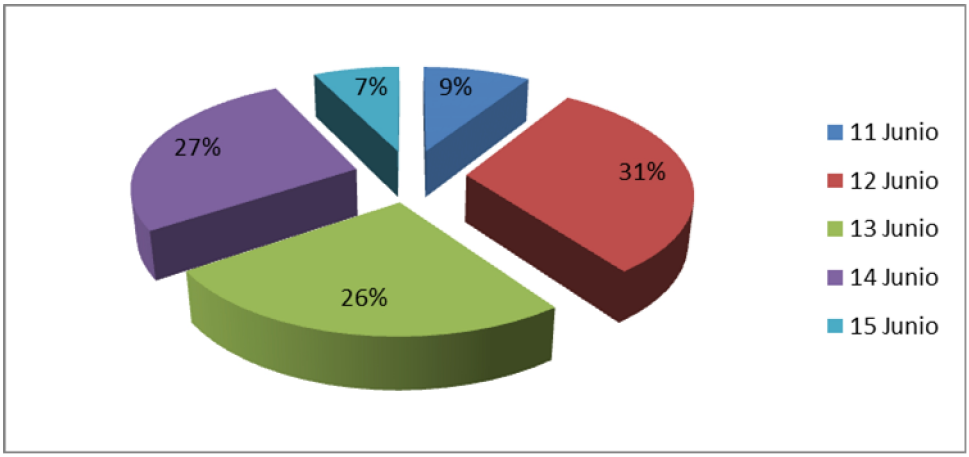


Figura IV.11 Distribución de tráfico de ENTRADA en MB 11 al 15 de Junio

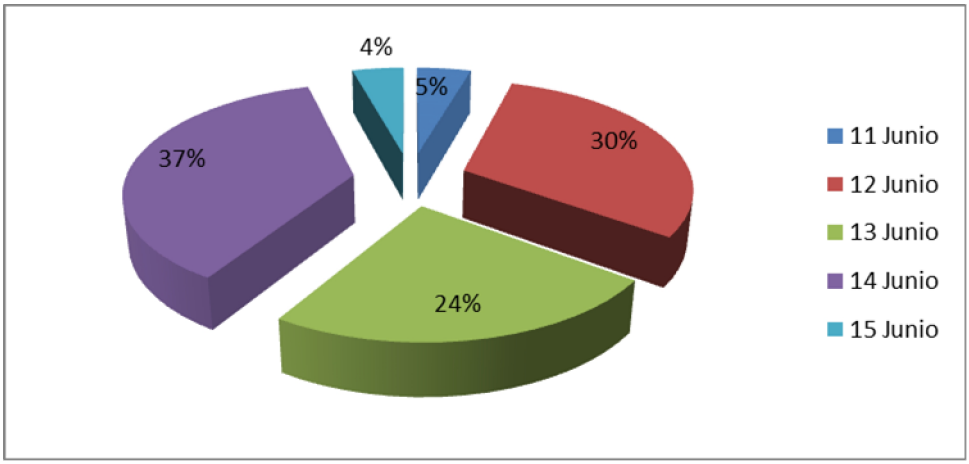


Figura IV.12 Distribución de tráfico de SALIDA en MB 11 al 15 de Junio

Como se puede observar en la tabla IV.9 y en las figuras IV.11 y IV.12 los días 12 y 14 de Junio son los de mayor consumo, con 437,41 y 11017,69 Megabytes que corresponde al 31% y 37% del tráfico de Entrada y Salida respectivamente.

Semana 3: 18/06/2012 – 22/06/2012

Horario: 07:00 – 12:00

Tabla IV.10 Resumen de tráfico en MB 18 al 22 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
18 Junio	403,00	6258,10	6661,1
19 Junio	360,88	6388,33	6749,21
20 Junio	344,01	7434,93	7778,94
21 Junio	418,03	8505,69	8923,72
22 Junio	26536,06	34633,55	61169,61
	TOTAL:		91282,58

Realizado por: Autor
Fuente: Netflow Analyzer

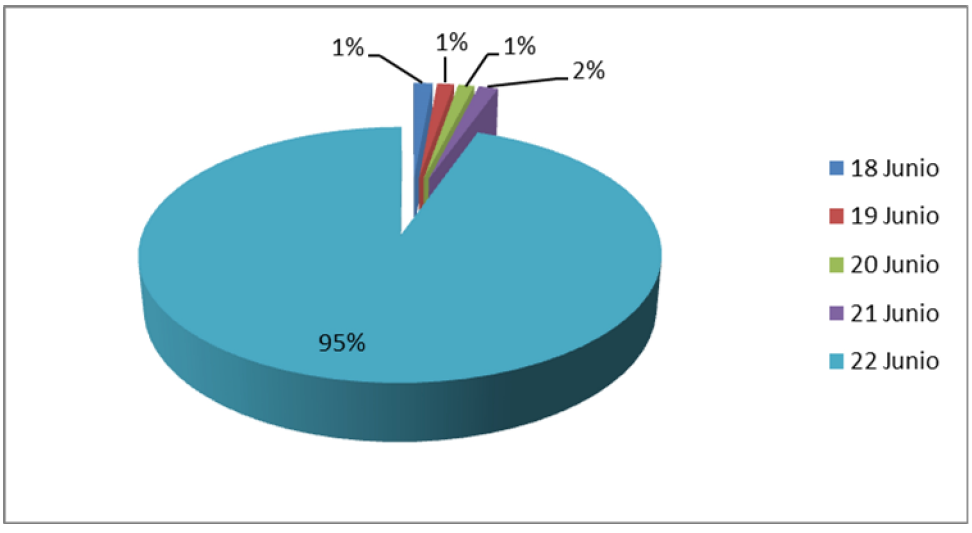


Figura IV.13 Distribución de tráfico de ENTRADA en MB 18 al 22 de Junio

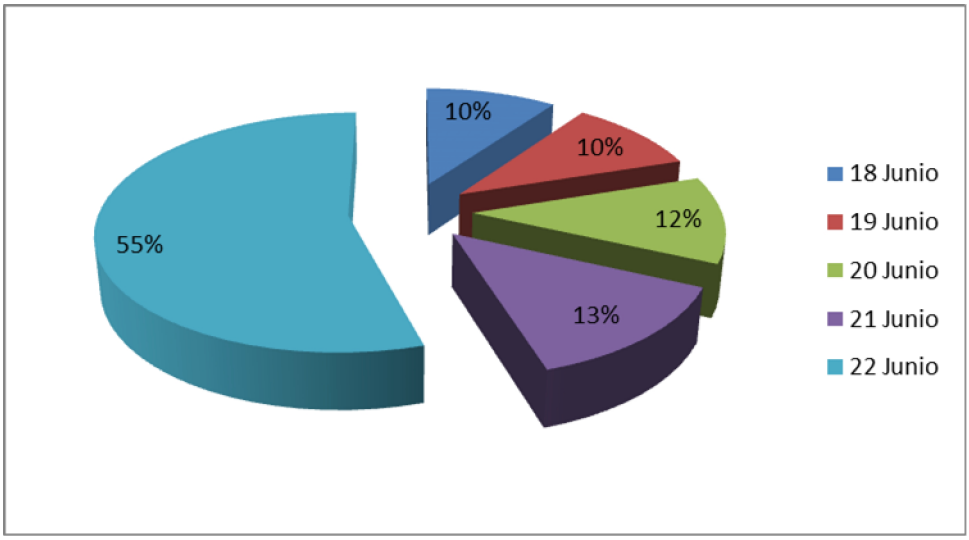


Figura IV.14 Distribución de tráfico de SALIDA en MB 18 al 22 de Junio

Como se puede observar en la tabla IV.10 y en las figuras IV.13 y IV.14 el día 22 de Junio es el mayor consumo, con 26536,06 y 34633,55 Megabytes que corresponde al 95% y 55% del tráfico de Entrada y Salida respectivamente.

Semana 3: 18/06/2012 – 22/06/2012

Horario: 13:00 – 14:00

Tabla IV.11 Resumen de tráfico en MB 18 al 22 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
18 Junio	50,33	1451,7	1502,03
19 Junio	188,34	5048,89	5237,23
20 Junio	35,76	634,38	670,14
21 Junio	44,03	454,13	498,16
22 Junio	47,32	898,76	946,08
	TOTAL:		8853,64

Realizado por: Autor
Fuente: Netflow Analyzer

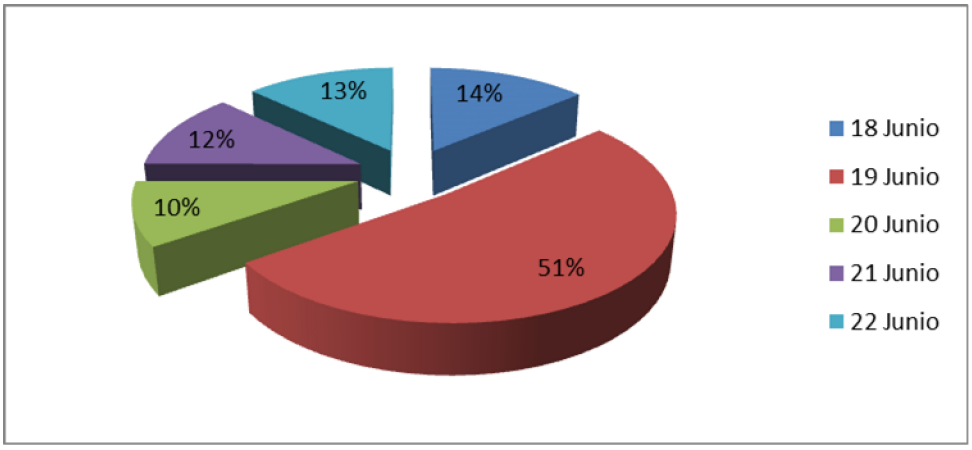


Figura IV.15 Distribución de tráfico de ENTRADA en MB 18 al 22 de Junio

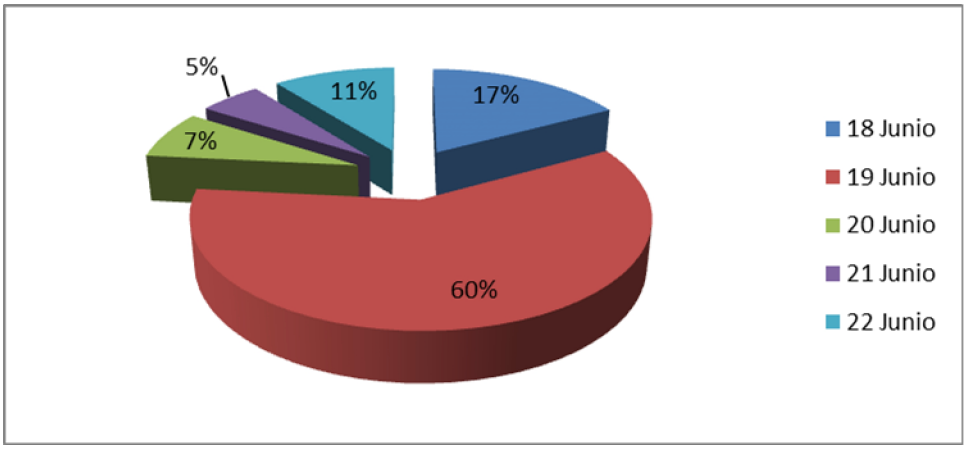


Figura IV.16 Distribución de tráfico de SALIDA en MB 18 al 22 de Junio

Como se puede observar en la tabla IV.11 y en las figuras IV.15 y IV.16 el día 19 de Junio es el mayor consumo, con 188,34 y 5048,89 Megabytes que corresponde al 51% y 60% del tráfico de Entrada y Salida respectivamente.

Semana 3: 18/06/2012 – 22/06/2012

Horario: 15:00 – 21:00

Tabla IV.12 Resumen de tráfico en MB 18 al 22 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
18 Junio	426,67	11253,16	11679,83

19 Junio	313,06	5097,44	5410,5
20 Junio	375,54	9632,21	10007,75
21 Junio	3798,24	10924,62	14722,86
22 Junio	434,05	4257,08	4691,14
	TOTAL:		46512,08

Realizado por: Autor
Fuente: Netflow Analyzer

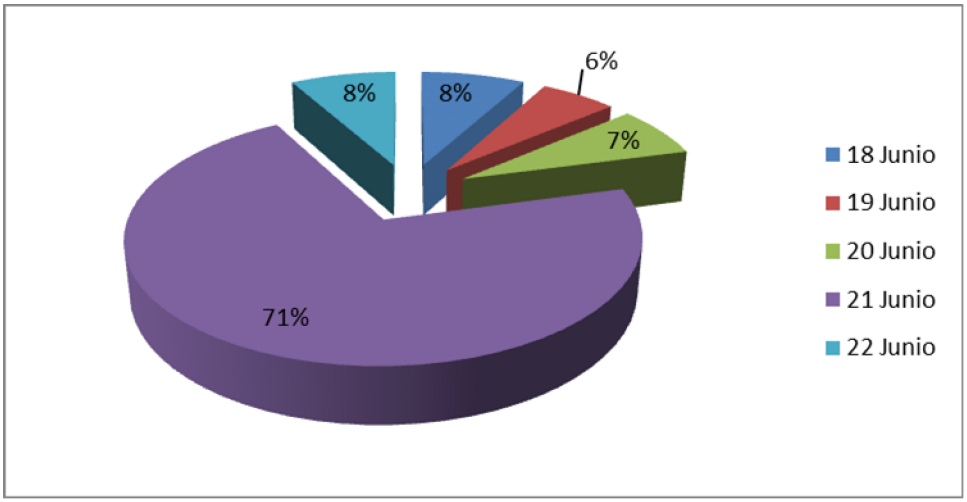


Figura IV.17 Distribución de tráfico de ENTRADA en MB 18 al 22 de Junio

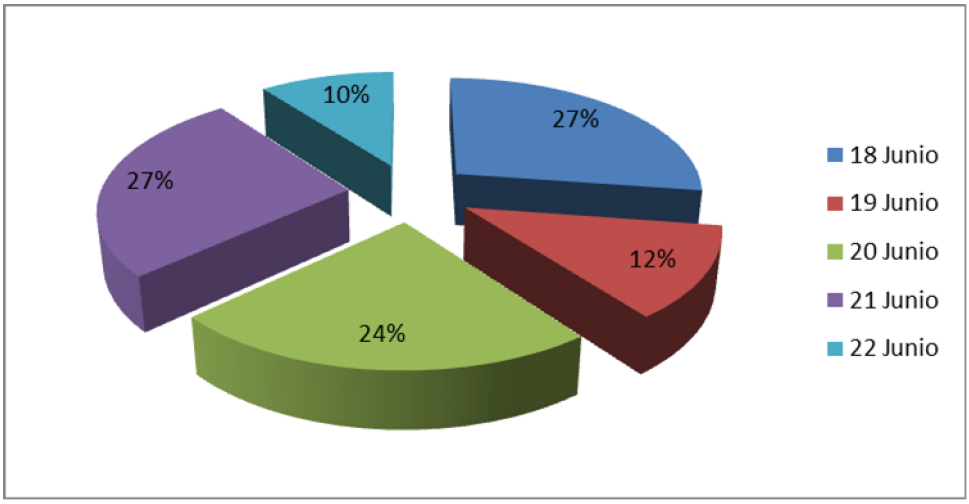


Figura IV.18 Distribución de tráfico de SALIDA en MB 18 al 22 de Junio

Como se puede observar en la tabla IV.12 y en las figuras IV.17 y IV.18 el día 21 de Junio es el mayor consumo, con 3798,24 y 10924,62 Megabytes que corresponde al 71% y 27% del tráfico de Entrada y Salida respectivamente.

Semana 4: 25/06/2012 – 29/06/2012

Horario: 07:00 – 12:00

Tabla IV.13 Resumen de tráfico en MB 25 al 29 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
25 Junio	401,51	8045,2	8446,71
26 Junio	451,62	11301,37	11752,99
27 Junio	415,26	7061,46	7476,72
28 Junio	317,01	4801,35	5118,36
29 Junio	519,95	16483,81	17003,76
	TOTAL:		49798,54

Realizado por: Autor
Fuente: Netflow Analyzer

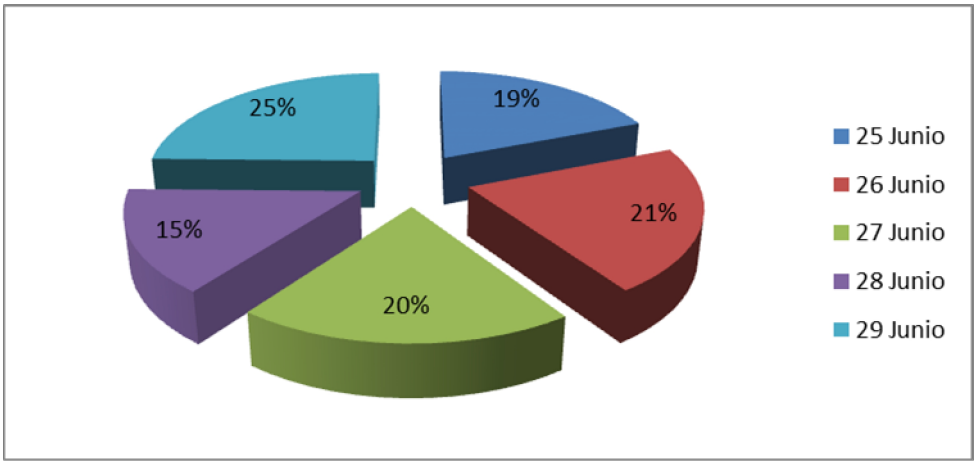


Figura IV.19 Distribución de tráfico de ENTRADA en MB 25 al 29 de Junio

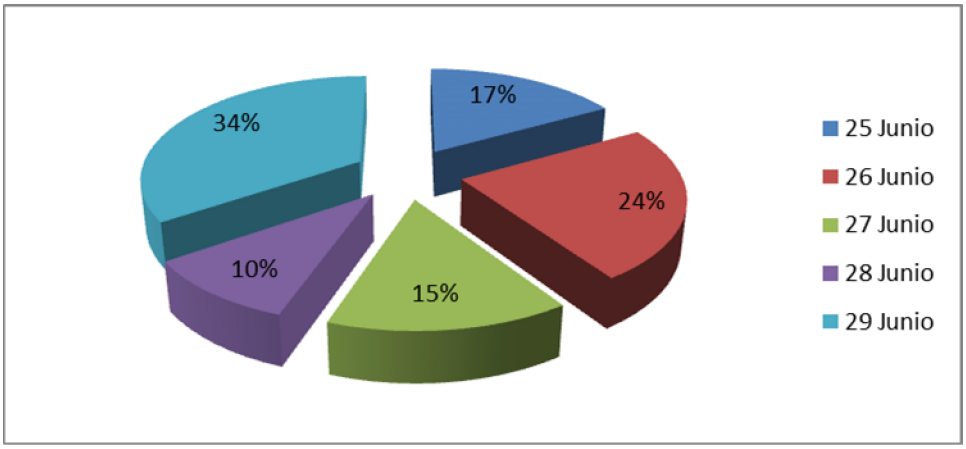


Figura IV.20 Distribución de tráfico de SALIDA en MB *25 al 29 de Junio*

Como se puede observar en la tabla IV.13 y en las figuras IV.19 y IV.20 el día 29 de Junio es el mayor consumo, con 519,95 y 16483,81 Megabytes que corresponde al 25% y 34% del tráfico de Entrada y Salida respectivamente.

Semana 4: 25/06/2012 – 29/06/2012

Horario: 12:00 – 14:00

Tabla IV.14 Resumen de tráfico en MB 25 al 29 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
25 Junio	80,5	1268,91	1349,41
26 Junio	109,46	4321,28	4430,74
27 Junio	101,72	3618,61	3720,33
28 Junio	47,85	1258,84	1306,69
29 Junio	41,01	684,02	725,03
	TOTAL:		11532,2

Realizado por: Autor
Fuente: Netflow Analyzer

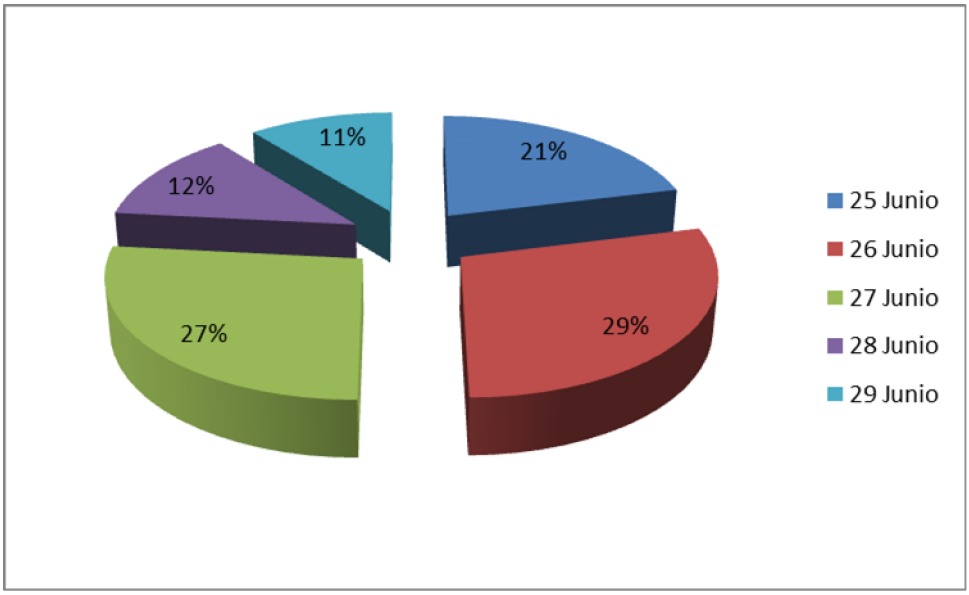


Figura IV.21 Distribución de tráfico de ENTRADA en MB 25 al 29 de Junio

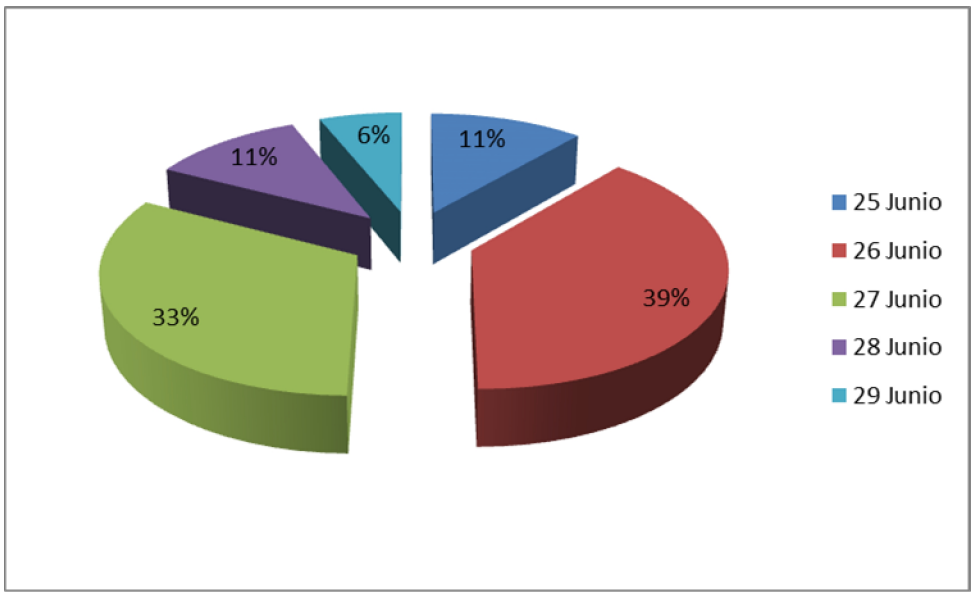


Figura IV.22 Distribución de tráfico de SALIDA en MB 25 al 29 de Junio

Como se puede observar en la tabla IV.14 y en las figuras IV.21 y IV.22 el día 26 de Junio es el mayor consumo, con 109,46 y 4321,28 Megabytes que corresponde al 29% y 39% del tráfico de Entrada y Salida respectivamente.

Semana 4: 25/06/2012 – 29/06/2012

Horario: 15:00 – 21:00

Tabla IV.15 Resumen de tráfico en MB 25 al 29 de Junio

	Tráfico (MB)		
Día Medición	**Entrada**	**Salida**	**Total**
25 Junio	259,53	3548,26	3807,79
26 Junio	185,11	3136,37	3321,48
27 Junio	314,47	8122,09	8436,56
28 Junio	366,22	7390,40	7756,62
29 Junio	131,40	1771,22	1902,62
	TOTAL:		25225,07

Realizado por: Autor
Fuente: Netflow Analyzer

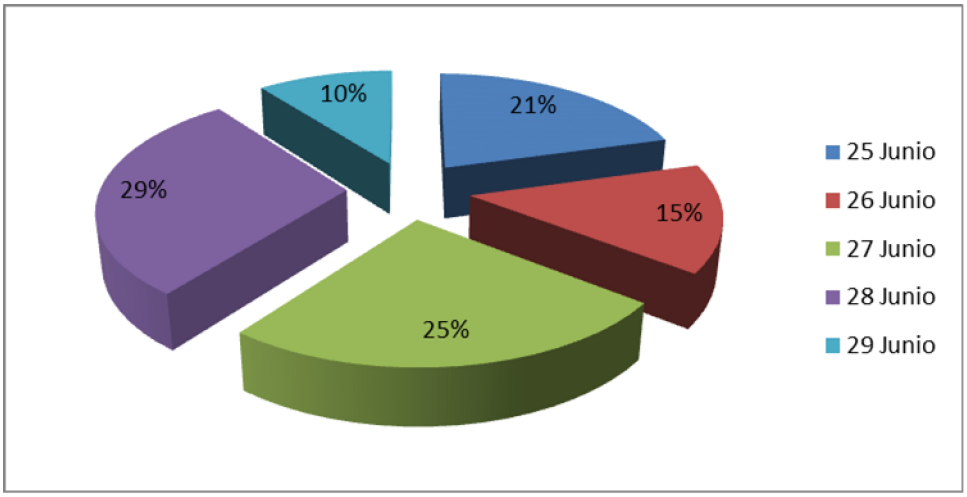


Figura IV.23 Distribución de tráfico de ENTRADA en MB 25 al 29 de Junio

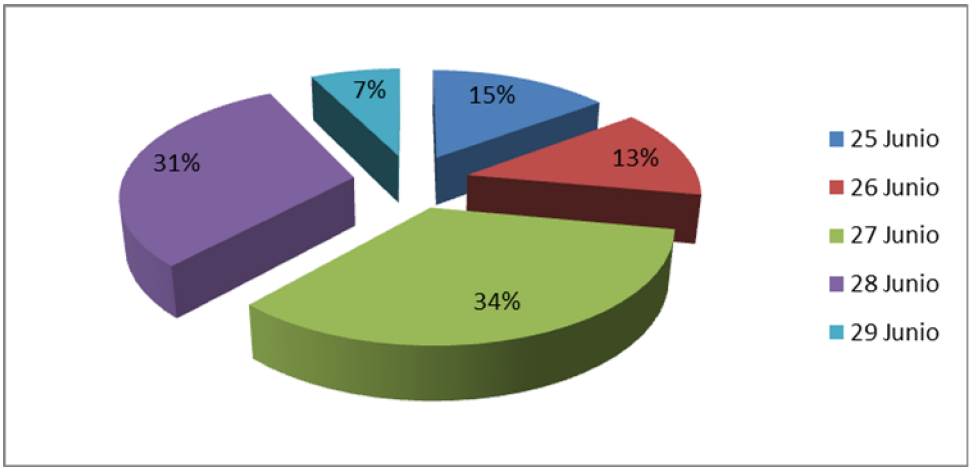


Figura IV.24 Distribución de tráfico de SALIDA en MB 25 al 29 de Junio

Como se puede observar en la tabla IV.15 y en las figuras IV.23 y IV.24 los días 28 y 27 de Junio son los de mayor consumo, con 366,22 y 8122,09 Megabytes que corresponde al 29% y 34% del tráfico de Entrada y Salida respectivamente.

RESUMEN SEMANAL

Tabla IV.16 Resumen total de tráfico en MB por semanas

Semana	Mañana	Medio día	Tarde	Total
4 - 8 Junio	55,57	16,07	62,80	134,43

11 - 15 Junio	30736,33	4797,88	31293,16	66827,37
18 - 22 Junio	91282,58	8853,64	46512,08	146648,30
25 - 29 Junio	49798,54	11532,20	25225,07	86555,81
			TOTAL:	300165,91

Realizado por: Autor
Fuente: Netflow Analyzer

Como se puede observar en la tabla IV.16, la cantidad de tráfico total que se ha generado durante el período de monitoreo es de 300165,91 Megabytes**.**

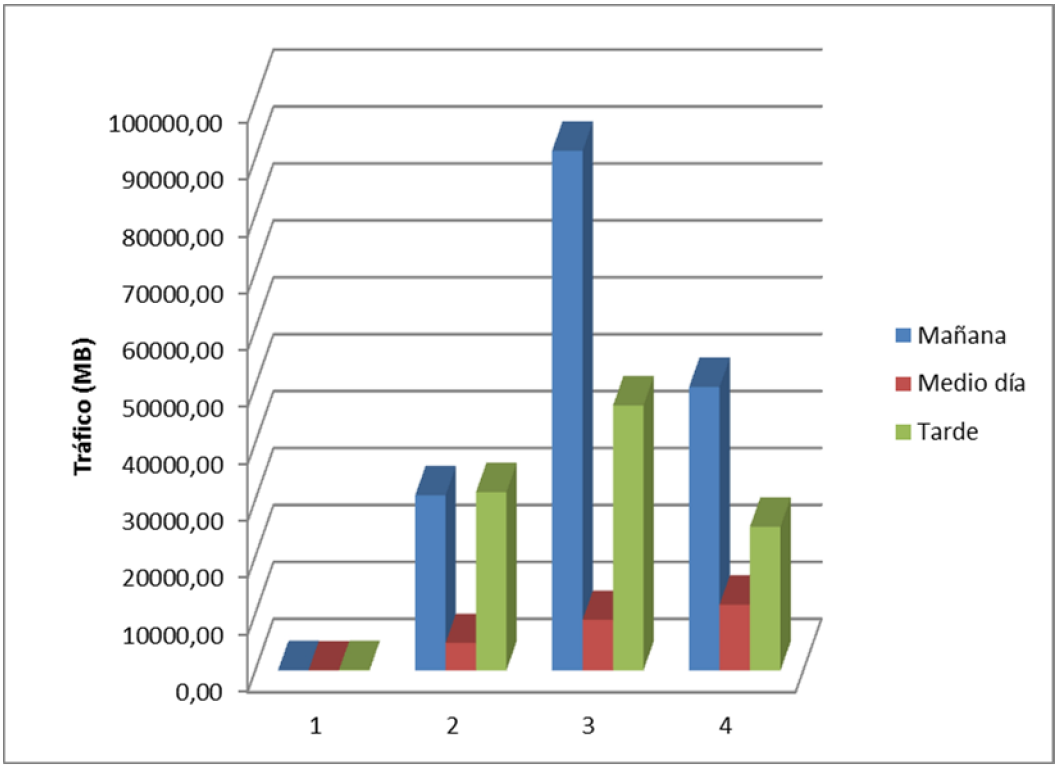


Figura IV.25 Distribución de tráfico en MB por semanas

En la figura IV.25 se puede observar que en el período de la mañana de monitoreo correspondiente a la semana del 18 al 22 de Junio es la de mayor consumo, generando 146648,30 Megabytes de tráfico lo que corresponde al 49% del tráfico total monitoreado.

4.3 DETERMINACIÓN DE LA CANTIDAD DE PAQUETES

Un parámetro importante al momento de determinar el uso de los recursos de la red es la cantidad de paquetes generados en el período de monitoreo y que permiten determinar si existe o no sobrecarga de trabajo del equipo de comunicación.

La tabla IV.17 muestra el detalle del número de paquetes medidos en el período de monitoreo así como la tasa de reenvió (Forwarding Rate) del switch cisco Catalyst 3560G.

Tabla IV.17 Distribución del Número de Paquetes por segundo

	Número Paquetes		**Forwarding Rate**	
DÍA MEDICIÓN	**Entrada**	**Salida**	**Total**	**PPS**
4 Junio	6350938	9318055	15668993	290,17
5 Junio	5365927	8782262	14148189	262,00
6 Junio	7205449	12139151	19344600	358,23
7 Junio	6840788	11735570	18576358	344,01
8 Junio	2949594	4373998	7323592	135,62
11 Junio	3641098	3641098	7282196	134,86
12 Junio	7745388	7745388	15490776	286,87
13 Junio	8342917	8342917	16685834	309,00
14 Junio	7680639	7680639	15361278	284,47
15 Junio	3027919	3027919	6055838	112,15
18 Junio	9626104	14566675	24192779	448,01
19 Junio	7362280	12722547	20084827	371,94
20 Junio	8751720	13245995	21997715	407,37
21 Junio	10414923	15294713	25709636	476,10
22 Junio	32829814	36286709	69116523	1279,94
25 Junio	6111205	10279567	16390772	303,53
26 Junio	8937908	13865102	22803010	422,28

27 Junio	7322889	14209422	21532311	398,75
28 Junio	6187124	10690858	16877982	312,56
29 Junio	7103732	13846274	20950006	387,96
		TOTAL	**395593215**	**7325,80**

Realizado por: Autor
Fuente: Netflow Analyzer

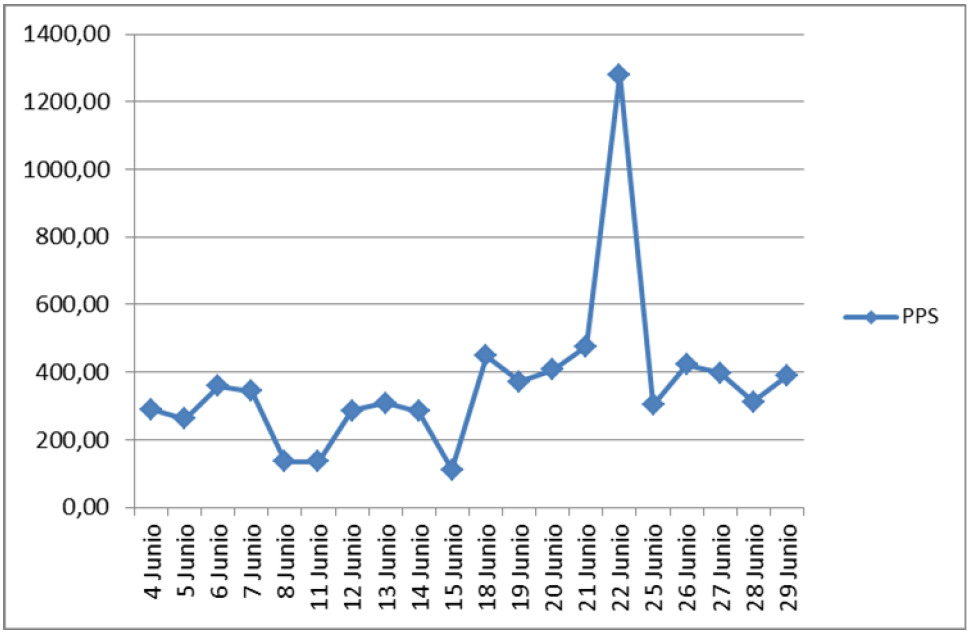


Figura IV.26 Distribución del número de paquetes por segundo

Con los datos obtenidos se procedió a calcular el promedio de paquetes por segundo para determinar el nivel de uso de la tasa de reenvió (Forwarding rate) del switch Cisco Catalyst 3560G; que según los documentos técnicos (Anexo 2) soporta un máximo de 6500000 paquetes por segundo. Este nivel de uso nos permitirá posteriormente comprobar si existe o no sobrecarga de trabajo en el equipo mencionado.

El cálculo del promedio de PPS, se realizó de la siguiente manera:

Promedio PPS = Total PPS / # Días monitoreo

Promedio PPS = 7325,80/ 20

Promedio PPS = 366,29

% Uso = (366,29*100)/6500000

% Uso = 0,5635

De los resultados obtenidos claramente se puede observar que durante el periodo que se monitoreo la red de datos de la Facultad de Mecánica la tasa de reenvió es inferior al 1%.

4.4 DETERMINACIÓN DEL MAPA DE APLICACIONES

A través de la herramienta de monitoreo se determinó que en la red de datos de la Facultad de Mecánica circulan más de cincuenta aplicaciones; de las cuales las de mayor generación de tráfico son las que a continuación se detallan:

PERÍODO DE LA MAÑANA

Tabla IV.18 Tráfico por aplicaciones Entrada - Mañana

Aplicaciones	4-8 Junio	11-15 Junio	18-22 Junio	25-29 Junio	Total
microsoft-ds	32,17	10,52	26275,84	18,49	26337,02
http	2949,12	3082,24	3409,92	3266,56	12707,84
netbios-ssn	9,27	7,21	3409,92	13,13	3439,53
UDP_App	141,96	103,01	106,4	129,99	481,36
bootps	55,3	52,3	48,18	50,31	206,09
netbios-ns	44,3	42,38	42,5	52,08	181,26
SIP	35,77	37,54	37,38	37,91	148,60
TCP_App	32,19	31,18	38,87	40,1	142,34
domain	12,53	14,17	15,76	17,13	59,59
netbios-dgm	10,94	11,23	11,03	17,22	50,42
nessus	0,650771484	7,37	1,19	0,752451172	9,96
skinny	1,8	2,11	2,17	1,93	8,01
https	1,39	1,77	2,55	1,81	7,52
icmp	1,53	1,48	1,38	1,96	6,35
rmiactivation	1,11	1,56	0,730019531	1,24	4,64
rmiregistry	1,45	1,45	0,589091797	0,771953125	4,26

kpop	1,18	0,893105469	0,743242188	0,854199219	3,67
lotusnote	1,03	1,07	0,734550781	0,396230469	3,23
kazaa	0,720068359	0,806787109	1	0,634023438	3,16
wins	0,845878906	0,773857422	0,833789063	0,440410156	2,89
direct_connect	0,8075	0,971855469	0,376621094	0,479335938	2,64

Realizado por: Autor
Fuente: Netflow Analyzer

Tabla IV.19 Tráfico por aplicaciones Salida - Mañana

Aplicaciones	4-8 Junio	11-15 Junio	18-22 Junio	25-29 Junio	Total
http	55500,8	61931,52	78100,48	80363,52	275896,32
microsoft-ds	32,35	8,83	26275,84	25,2	26342,22
netbios-ssn	9,3	7,25	3409,92	13,17	3439,64
UDP_App	85,96	51,92	52,49	81,04	271,41
netbios-ns	44,03	42,05	42,74	51,86	180,68
domain	37,77	43,65	47,26	49,68	178,36
SIP	37,06	38,36	38,39	38,79	152,60
rmiregistry	68,44	53,42	11,34	13,08	146,28
rmiactivation	14,67	80,68	10,41	31,13	136,89
TCP_App	29,54	24,65	34	34,51	122,70
lotusnote	37,16	52,31	22,86	5,47	117,80
wins	20,05	13,12	51	3,89	88,06
kpop	36,39	12,94	13,4	16,35	79,08
NFS	0,5471582	1,09	3,29	72,65	77,58
nessus	6,57	6,34	40,52	16,45	69,88
direct_connect	13,13	48,73	3,72	4,1	69,68
kazaa	5,72	18,09	21,75	8,02	53,58
ms-sql-s	38,82	3,31	7,27	3,53	52,93
netbios-dgm	10,91	11,2	11	17,1	50,21
pptp	10,74	12,03	10,74	9,47	42,98
xfer	0,37125977	0,33000977	0,04125	42,13	42,87

Realizado por: Autor
Fuente: Netflow Analyzer

Tabla IV.20 Resumen de Tráfico por aplicación - Mañana

Aplicación	Entrada	Salida	Total (MB)
http	12707,84	275896,32	288604,16
microsoft-ds	26337,02	26342,22	52679,24
netbios-ssn	3439,53	3439,64	6879,17
UDP_App	481,36	271,41	752,77

netbios-ns	181,26	180,68	361,94
SIP	148,60	152,60	301,20
TCP_App	142,34	122,70	265,04
domain	59,59	178,36	237,95
bootps	206,09	31,35	237,44
rmiregistry	4,26	146,28	150,54
rmiactivation	4,64	136,89	141,53
lotusnote	3,23	117,80	121,03
netbios-dgm	50,42	50,21	100,63

Realizado por: Autor
Fuente: Netflow Analyzer

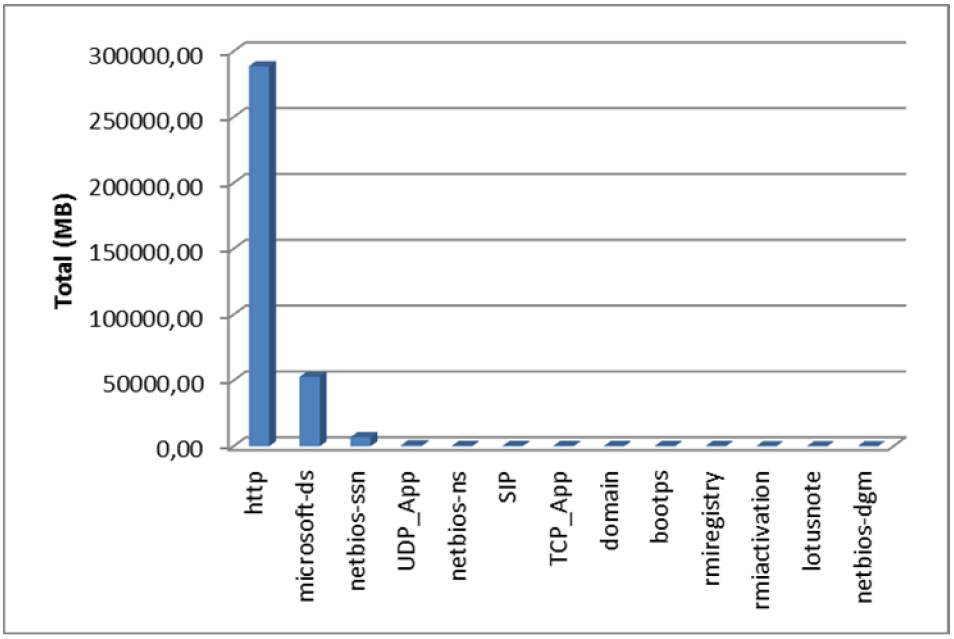


Figura IV.27 Distribución de tráfico en Mbps por aplicación

En la figura IV.27 se puede observar que las aplicaciones que generan la mayor cantidad de tráfico en la red de datos de la Facultad de Mecánica es el acceso a sitios web (http) y la compartición de archivos (microsoft-ds) que se obtiene al acceder al ServerFM (IP:172.30.102.50) que se utiliza como repositorio de software, utilizado por los técnicos para las labores de instalación de aplicaciones en los hosts de la red.

PERÍODO DEL MEDIO DÍA

Tabla IV.21 Tráfico por aplicaciones Entrada – Medio día

Aplicación	4-8 Junio	11-15 Junio	18-22 Junio	25-29 Junio	Total
microsoft-ds	32,07	10,44	26245,12	1,65	26289,28
http	2641,92	2795,52	3112,96	2959,36	11509,76
netbios-ssn	8,39	6,62	3399,68	11,69	3426,38
UDP_App	140,49	104,68	92,95	110,58	448,7
bootps	53,18	49,67	45,31	47,23	195,39
netbios-ns	41,92	39,11	38,06	47,45	166,54
SIP	35,72	35,41	35,39	35,38	141,9
TCP_App	31,5	28,48	36,36	32,03	128,37
domain	11,82	13,19	14,14	15,44	54,59
netbios-dgm	10,28	10,26	10,26	16,24	47,04
nessus	0,63446289	7,29	1,06	0,700625	9,68508789
skinny	1,72	2,04	2,1	1,85	7,71
https	1,23	1,68	2,27	1,63	6,81
icmp	1,35	1,39	1,27	1,76	5,77
rmiactivation	1,04	1,03	0,628095703	1,17	3,8680957
rmiregistry	1,38	1,23	0,523603516	0,72763672	3,86124023
kpop	1,18	0,81888672	0,682255859	0,8118457	3,49298828
kazaa	0,68871094	0,7515625	0,937470703	0,59354492	2,97128906
lotusnote	0,80875977	1,01	0,671201172	0,37344727	2,8634082
wins	0,75814453	0,52376953	0,808925781	0,41207031	2,50291016
direct_connect	0,62708008	0,9012793	0,369697266	0,45319336	2,35125

Realizado por: Autor
Fuente: Netflow Analyzer

Tabla IV.22 Tráfico por aplicaciones Salida – Medio día

Aplicación	4-8 Junio	11-15 Junio	18-22 Junio	25-29 Junio	Total
http	52531,2	56606,72	72652,8	73041,92	254832,64
microsoft-ds	32,24	8,73	26245,12	8,24	26294,33
netbios-ssn	8,42	6,65	3399,68	11,73	3426,48
UDP_App	85,73	53,87	42,55	64,72	246,87
netbios-ns	41,67	38,8	38,32	47,27	166,06
domain	35,5	40,54	42,74	44,64	163,42
SIP	36,96	36,16	36,29	36,14	145,55
rmiregistry	67,82	51,11	10,58	12,35	141,86
jrun_ejb	1,77	0,35880859	124,91	3	130,04
TCP_App	28,82	22,59	31,45	27,58	110,44
lotusnote	23,81	51,62	22,53	5,48	103,44
rmiactivation	14,13	34,56	9,87	30,09	88,65

wins	14,92	12,64	50,77	3,37	81,70
kpop	42,7	11,09	12,39	14,72	80,90
NFS	0,43782227	1,08	3,28	72,56	77,36
nessus	8,37	5,77	33,75	16,28	64,17
direct_connect	4,21	48,42	3,68	3,75	60,06
ms-sql-s	38,57	3,17	7,22	3,46	52,42
kazaa	5,43	16,26	21,29	7,17	50,15
netbios-dgm	10,25	10,24	10,23	16,12	46,84
xfer	0,37125977	0,20625977	0,04125	42,13	42,75

Realizado por: Autor
Fuente: Netflow Analyzer

Tabla IV.23 Resumen de Tráfico por aplicación – Medio día

Aplicación	Entrada	Salida	Total (MB)
http	11509,76	254832,64	266342,40
microsoft-ds	26289,28	26294,33	52583,61
netbios-ssn	3426,38	3426,48	6852,86
UDP_App	448,7	246,87	695,57
netbios-ns	166,54	166,06	332,60
SIP	141,9	145,55	287,45
TCP_App	128,37	110,44	238,81
bootps	195,39	29,02	224,41
domain	54,59	163,42	218,01
rmiregistry	3,86124023	141,86	145,72
jrun_ejb	2,19513672	130,04	132,23
lotusnote	2,8634082	103,44	106,30

Realizado por: Autor
Fuente: Netflow Analyzer

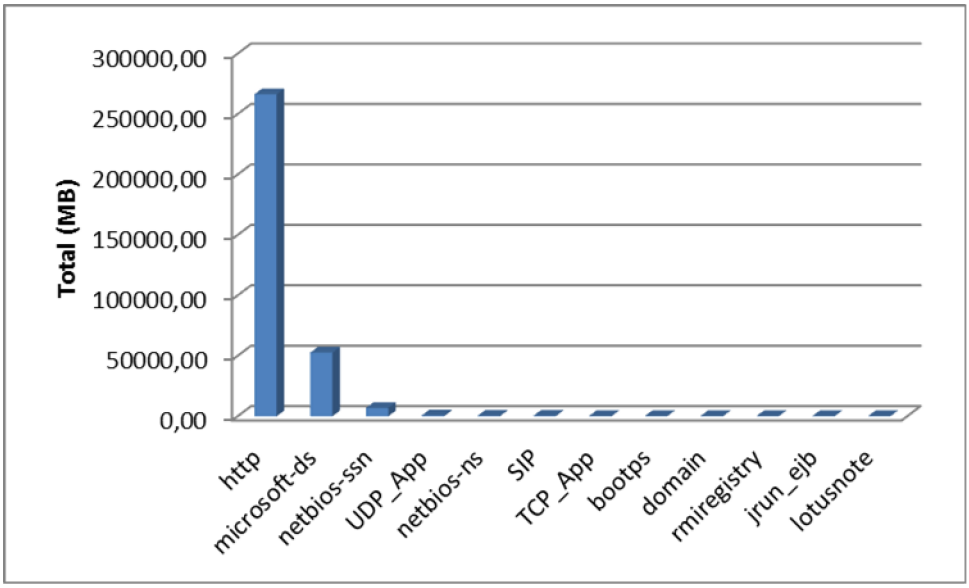


Figura IV.28 Distribución de tráfico en Mbps por aplicación

En la figura IV.28 se puede observar que las aplicaciones que generan la mayor cantidad de tráfico en la red de datos de la Facultad de Mecánica es el acceso a sitios web (http) y la compartición de archivos (microsoft-ds).

PERÍODO DE LA TARDE

Tabla IV.24 Tráfico por aplicaciones Entrada – Tarde

Aplicación	4-8 Junio	11-15 Junio	18-22 Junio	25-29 Junio	Total
microsoft-ds	32,05	8,2	26245,12	1,63	26287,00
http	2734,08	2867,2	3502,08	3010,56	12113,92
netbios-ssn	8,16	6,79	3409,92	11,38	3436,25
UDP_App	136,44	108,69	87,83	106,08	439,04
bootps	54,7	52,51	47,96	49,43	204,60
netbios-ns	42,34	43,23	39,95	48,95	174,47
SIP	36,72	38,46	36,39	37,03	148,60
TCP_App	31,29	29,48	36,84	32,96	130,57
domain	11,89	14,01	14,78	16,06	56,74
netbios-dgm	10,47	10,89	11,32	17,64	50,32
nessus	0,65107422	7,31	1,07	0,7503418	9,78
skinny	1,78	2,12	2,17	1,94	8,01
https	1,22	2,11	2,36	1,66	7,35
icmp	1,36	1,53	1,4	1,82	6,11

rmiactivation	1,02	1,08	0,664658203	1,18	3,94
rmiregistry	1,37	1,25	0,546806641	0,74171875	3,91
kpop	1,17	0,85443359	0,570175781	0,81730469	3,41
kazaa	0,71147461	0,75390625	0,945	0,635	3,05
lotusnote	0,78068359	1,02	0,674140625	0,3744043	2,85
wins	0,75582031	0,53140625	0,788837891	0,43279297	2,51
direct_connect	0,63793945	0,90918945	0,400986328	0,46222656	2,41

Realizado por: Autor
Fuente: Netflow Analyzer

Tabla IV.25 Tráfico por aplicaciones Salida – Tarde

Aplicación	4-8 Junio	11-15 Junio	18-22 Junio	25-29 Junio	Total
http	52121,6	57835,52	75479,04	73574,4	259010,56
microsoft-ds	32,22	8,36	26245,12	8,21	26293,91
netbios-ssn	8,19	6,82	3409,92	11,41	3436,34
netflow			424		424
UDP_App	84,12	54,02	34,13	61,11	233,38
netbios-ns	42,1	42,91	40,2	48,74	173,95
domain	35,52	42,88	44,49	46,46	169,35
SIP	38,03	39,29	37,34	37,79	152,45
rmiregistry	67,64	51,27	11,39	12,45	142,75
jrun_ejb	1,77	0,53279297	124,91	3	130,212793
edonkey2000	6,65	0,15489258	106,81	0,11907227	113,733965
TCP_App	28,37	23,7	31,6	28,25	111,92
lotusnote	23,27	51,7	22,54	5,54	103,05
https		0,2446582	99,76		100,004658
rmiactivation	13,73	34,72	10,05	30,14	88,64
rrac		0,00209961	88	8,3923E-05	88,0021835
xfer	0,37125977	0,20625977	42,24	42,13	84,9475195
kpop	42,61	11,6	12,39	14,75	81,35
wins	14,87	12,69	49,75	3,79	81,1
NFS	0,43225586	1,08	3,29	72,52	77,3222559
snmp	0,32294922	0,18145508	66,47	0,35526367	67,329668

Realizado por: Autor
Fuente: Netflow Analyzer

Tabla IV.26 Resumen de Tráfico por aplicación - Tarde

Aplicación	Entrada	Salida	Total (MB)
http	12113,92	259010,56	271124,48
microsoft-ds	26287,00	26293,91	52580,91

netbios-ssn	3436,25	3436,34	6872,59
UDP_App	439,04	233,38	672,42
netflow	0,00102539	424	424,00
netbios-ns	174,47	173,95	348,42
SIP	148,60	152,45	301,05
TCP_App	130,57	111,92	242,49
domain	56,74	169,35	226,09
bootps	204,60		204,60
rmiregistry	3,91	142,75	146,66
jrun_ejb	2,22	130,212793	132,44
edonkey2000	0,15165039	113,733965	113,89
https	7,35	100,004658	107,35

Realizado por: Autor
Fuente: Netflow Analyzer

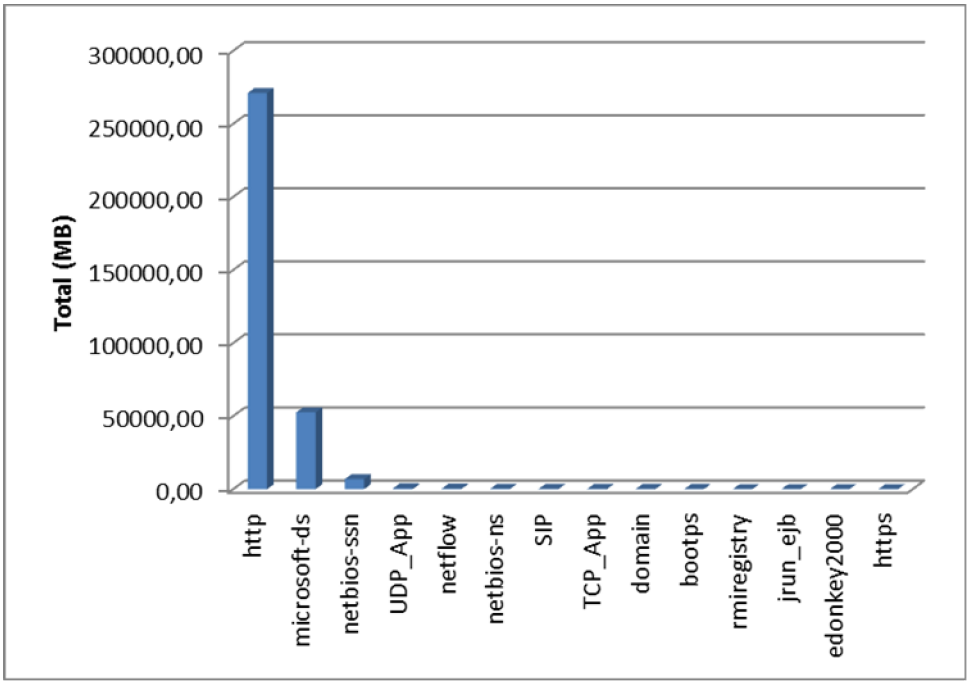


Figura IV.29 Distribución de tráfico en Mbps por aplicación

En la figura IV.29 se puede observar que las aplicaciones que generan la mayor cantidad de tráfico en la red de datos de la Facultad de Mecánica es el acceso a sitios web (http) y la compartición de archivos (microsoft-ds).

4.5 DETERMINACIÓN DE LA MATRIZ DE USUARIOS

Debemos señalar que tras la investigación realizada en la red de datos de la Facultad de Mecánica, se muestra que existe una máquina que realiza la función de servidor proxy, la herramienta de análisis detecto los valores de transferencia de tráfico que se muestran en la tabla IV.27 y que corresponden al servidor antes mencionado.

Tabla IV.27 Tráfico generado por el servidor proxy

Dirección IP	Tráfico (MB)
172.30.60.102	604508,16

Realizado por: Autor
Fuente: Netflow Analyzer

De la misma forma se determinó la matriz de usuarios en cada una de los períodos analizados en la red de datos de la Facultad.

PERÍODO DE LA MAÑANA

Tabla IV.28 Matriz de Usuarios - Mañana

Aplicación	Entrada	Salida	Total (MB)
172.30.102.78	3389,79	3389,44	6779,23
172.30.102.249	623,82	2,19852539	626,02
172.30.102.228	590,40	1,43448242	591,83
172.30.102.246	433,75	1,89723633	435,65
172.30.102.130	425,36	1,84128906	427,20
172.30.102.245	385,41	3,10901367	388,52
172.30.102.247	383,33	1,63861328	384,97
172.30.102.90	370,99	1,68538086	372,68
172.30.102.222	354,29	1,84695313	356,14
172.30.102.252	352,37	4,17902344	356,55
172.30.102.82	316,16	0,44672852	316,61

Realizado por: Autor
Fuente: Netflow Analyzer

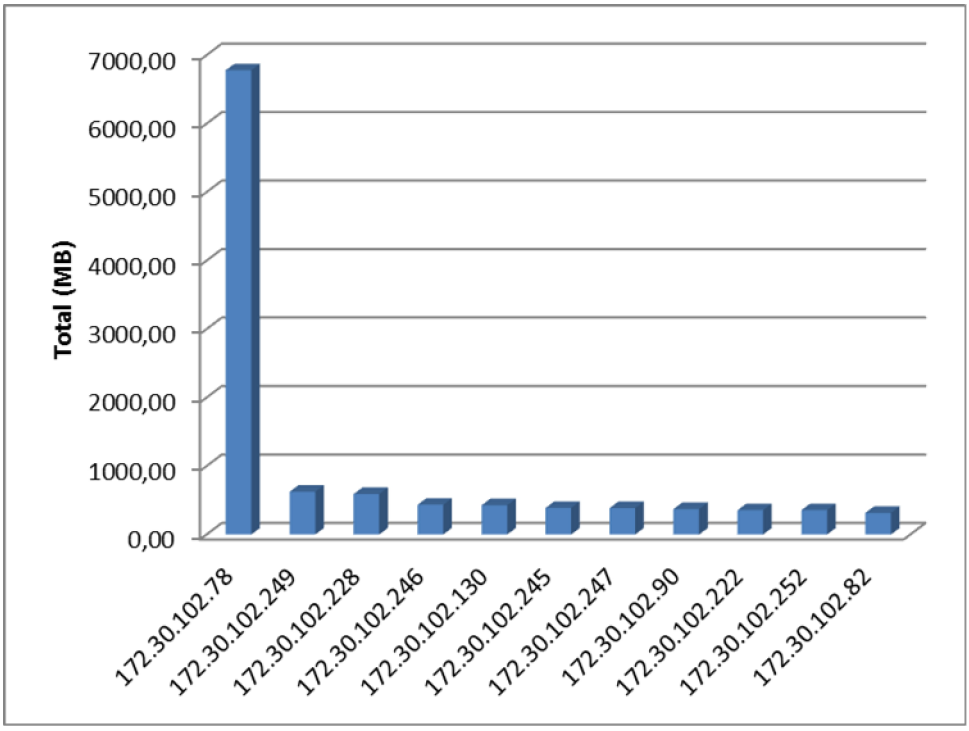


Figura IV.30 Tráfico por usuarios

PERÍODO DEL MEDIO DÍA

Tabla IV.29 Matriz de Usuarios – Medio día

Dirección IP	Entrada	Salida	Total (MB)
172.30.102.50	26113,70	25890,62	52004,32
172.30.102.78	3389,79	3389,44	6779,23
172.30.102.249	592,72	2,04731445	594,77
172.30.102.228	567,49	1,36116211	568,85
172.30.102.130	407,40	1,77482422	409,17
172.30.102.246	403,93	1,82441406	405,75
172.30.102.245	355,47	2,9330957	358,40
172.30.102.247	353,67	1,6053125	355,28
172.30.102.90	348,34	1,55365234	349,89
172.30.102.222	319,59	1,71204102	321,30
172.30.102.252	308,04	3,94868164	311,99

Realizado por: Autor
Fuente: Netflow Analyzer

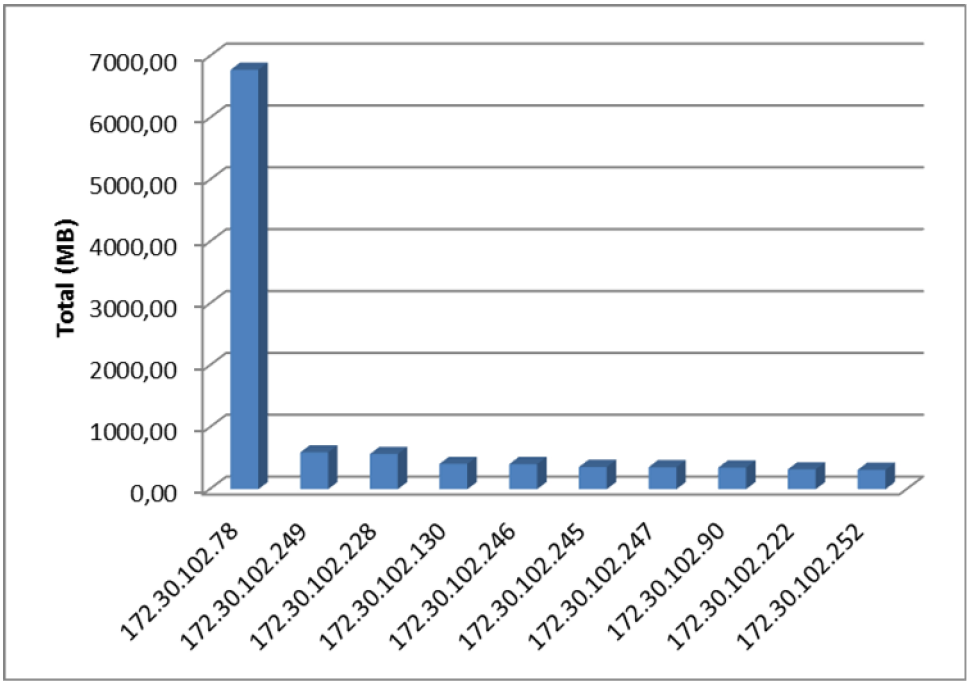


Figura IV.31 Tráfico por usuarios

PERÍODO DE LA TARDE

Tabla IV.30 Matriz de Usuarios - Tarde

Dirección IP	Entrada	Salida	Total (MB)
172.30.102.50	26111,26	25891,11	52002,37
172.30.102.78	3389,7928	3389,44056	6779,23
172.30.102.249	796,1	1,98298828	798,08
172.30.102.228	575,44	1,38457031	576,82
172.30.102.246	415,46	1,81105469	417,27
172.30.102.130	412,73	1,7959668	414,53
172.30.102.247	359,32	1,59726563	360,92
172.30.102.245	355,44	2,99113281	358,43
172.30.102.90	354,63	1,62481445	356,25
172.30.102.222	314,41	1,58336914	315,99
172.30.102.252	313,73	3,89070313	317,62
172.30.102.223	281,77	19,12	300,89

Realizado por: Autor
Fuente: Netflow Analyzer

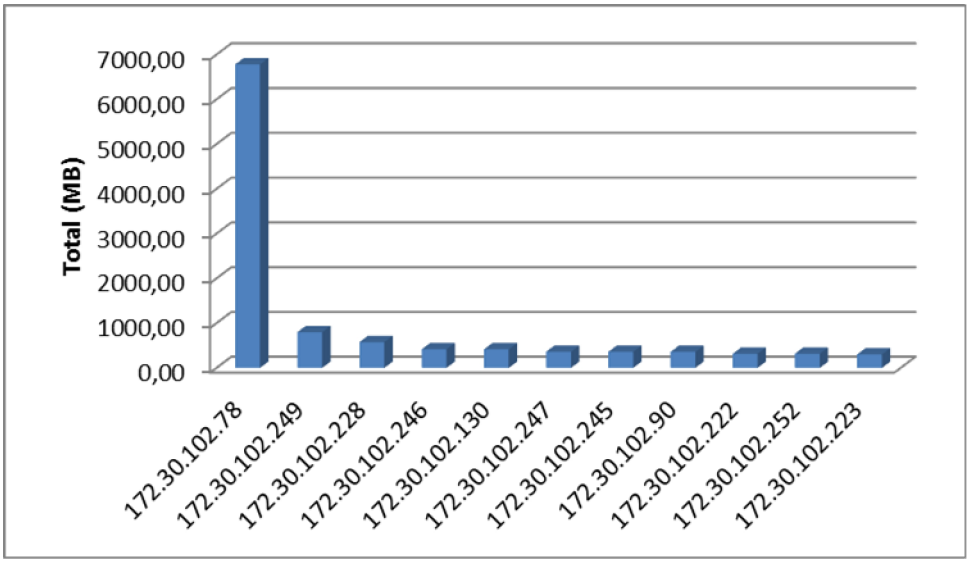


Figura IV.32 Tráfico por usuarios

4.6 COMPROBACIÓN DE LA HIPÓTESIS

4.6.1 Planteamiento de la hipótesis

En los ítems 4.2 y 4.3 se identificó la carga de tráfico y la cantidad de paquetes que se generaron durante el tiempo de monitoreo de la red de datos de la Facultad de Mecánica; parámetros que están íntimamente relacionados con la determinación y caracterización del consumo y utilización del ancho de banda.

La hipótesis nula **Ho** y la hipótesis de investigación **Hi**, se definen a continuación:

Ho: La utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica, no permite determinar el adecuado nivel de utilización de la infraestructura de la red.

Hi: La utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica, permite determinar el adecuado nivel de utilización de la infraestructura de la red.

En función a los resultados obtenidos en los apartados mencionados (4.2 y 4.3) se construyen la tabla de contingencia considerando la variable independiente: ***Utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica*** y la variable dependiente: ***Determinar el adecuado nivel de utilización de la infraestructura de red***.

Tabla IV.31 Tabla de frecuencias observadas

Período	T_Medido	P_Medido
Mañana	171873,0163	213,23025
Medio día	25199,78539	34,166197
Tarde	103093,1092	148,222994

Realizado por: Autor
Fuente: Netflow Analyzer

4.6.2 Descripción de población y muestra

Población

La población considerada para la investigación: los hosts de los laboratorios, el equipo activo de red (ver Tabla I.1), las diferentes aplicaciones (http, microsoft-ds, netbios-ssn, UDP_App, netbios-ns, SIP, TCP_App, bootps, etc.) y usuarios que tienen acceso a la infraestructura de datos de la Facultad de Mecánica y el efecto que tienen los mismos sobre el ancho de banda asignado; a través del protocolo NetFlow y de la herramienta de análisis de tráfico NetFlow Analyzer.

Muestra

La muestra para la investigación, corresponde al análisis del tráfico que se realizó en las dependencias que para el efecto se eligieron de forma predeterminada (ver Tabla

I.1), por ser las que generan el mayor consumo de recursos de la infraestructura de red de la Facultad de Mecánica en el mes de Junio del 2012, en los horarios de la: mañana, medio día y tarde (Tabla III.1); tiempo durante el cual se analizó las aplicaciones que mayor uso tenían y los usuarios que con mayor frecuencia accedían a la infraestructura; y a partir de esta información ver el uso del ancho de banda.

4.6.3 Elección de la prueba Estadística

El análisis de la varianza de un criterio (ANOVA) es una prueba paramétrica para analizar la variación entre muestras y la variación al interior de las mismas mediante la determinación de varianzas. Es llamado de un criterio porque analiza una variable independiente o Factor. Como tal, es un método estadístico útil para comparar dos o más medias poblacionales. El ANOVA de un criterio nos permite poner a prueba hipótesis tales como:

$$H_0 = «_1 = «_2 = «_3 = ... = «_k$$

$$H_1 : Al\ menos\ dos\ medias\ poblacionales\ son\ diferentes.$$

Como el ANOVA de un criterio es una generalización de la prueba de *t* para dos muestras, los supuestos para el ANOVA de un criterio son:

1. Todas las poblaciones *k* son normales.
2. Varianzas poblacionales son iguales: $\pm_1^2 = \pm_2^2 = \pm_3^2 = ... = \pm_k^2 \left(= \pm^2\right)$

Para determinar los valores esperados se usó la técnica de pronóstico de tráfico basado en el Modelo Estadístico de análisis de series de tiempo del Promedio Móvil Centrado para determinar los Índices Estacionales que se describe en el anexo 5.

Los valores de las frecuencias esperadas (T_Proyectado: Tráfico Proyectado y P_Proyectado: Paquetes Proyectados), se obtuvieron sumando los valores del tráfico diario que se pronosticó en la red de la Facultad de Mecánica.

La tabla IV.32 muestra las frecuencias esperadas de la variable dependiente:

Tabla IV.32 Tabla de frecuencias esperadas

Período	T_Proyectado	P_Proyectado
Mañana	512826,1285	431,2288201
Medio día	87816,82944	42,88321445
Tarde	265073,8136	173,6564331

Realizado por: Autor
Fuente: Netflow Analyzer

Obtenidas las frecuencias esperadas, se procede a construir la tabla de totalizados por períodos de tráfico y paquetes; medidos y proyectados (expresada en Megas).

Tabla IV.33 Totalizado por períodos medidos y proyectados

Período	T_Medido	T_Proyectado	P_Medido	P_Proyectado
Mañana	171873,0163	512826,1285	213,23025	431,2288201
Medio día	25199,78539	87816,82944	34,166197	42,88321445
Tarde	103093,1092	265073,8136	148,222994	173,6564331

Realizado por: Autor
Fuente: Netflow Analyzer

A continuación aplicamos la prueba estadística ANOVA, obteniendo los siguientes resultados:

Tabla IV.34 ANOVA de un factor

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Inter-grupos	166378855098,598	3	55459618366,199	4,353	,043
Intra-grupos	101915172665,341	8	12739396583,168		
Total	268294027763,938	11			

Realizado por: Autor
Fuente: SPSS

4.6.4 Nivel de significancia

El nivel de significancia tomada para esta investigación es de 5% (o un nivel de confianza del 95%), es decir **α** = 0,05. Para la interpretación de los resultados se debe considerar el criterio de que si los valores son menores 0,05 aceptamos la hipótesis alternativa caso contrario se la rechaza.

4.6.5 Conclusión de la hipótesis

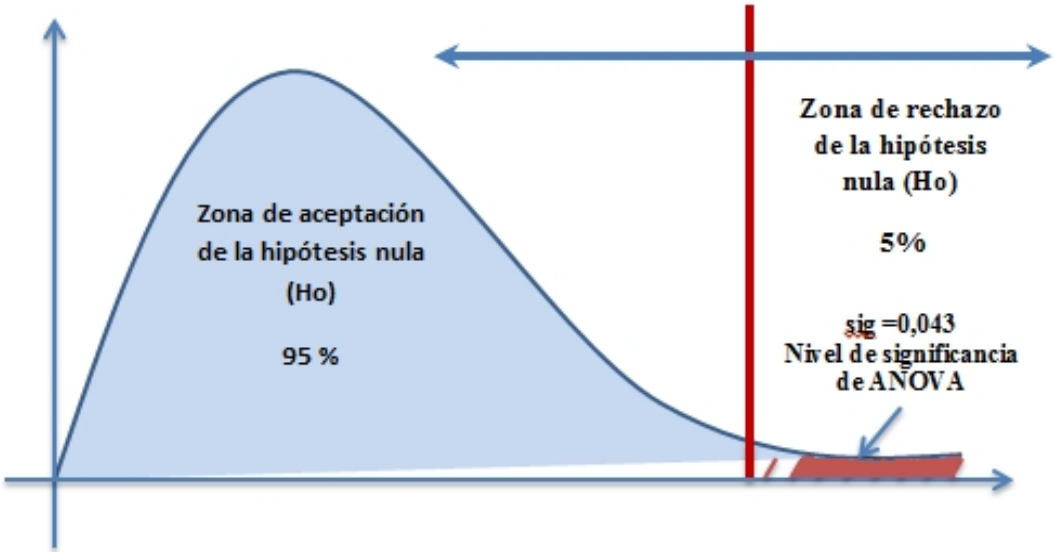


Figura IV.33 Zona de Aceptación de la hipótesis de investigación

Durante la investigación se probó con la prueba estadística chi cuadrado para la demostración de la hipótesis pero entre el valor tabulado y el calculado existía una diferencia muy grande, lo que denotaba que la prueba estadística no era la adecuada. En tal virtud se utilizó la prueba estadística ANOVA, a través de la cual y considerando un nivel de significancia de la prueba α=0,05; al comparar con el nivel de significancia obtenido de la prueba estadística con 3 y 8 grados de libertad, con un valor del nivel crítico de sig =0,043 (Tabla IV.34); concluimos que se rechaza la hipótesis nula y se acepta la hipótesis de investigación, ya que el valor de sig < α como se muestra en la

figura IV.33.

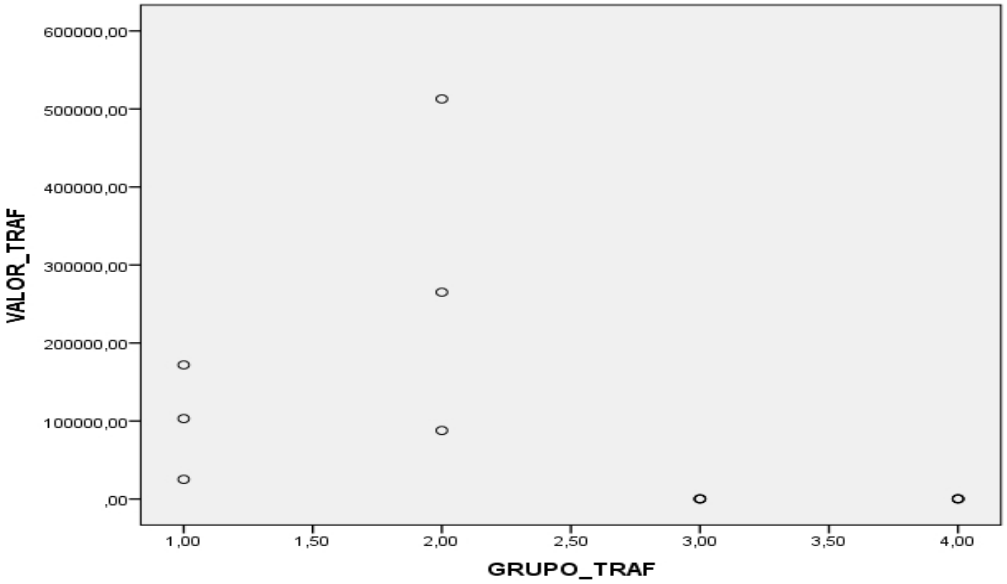


Figura IV.34 Dispersión del Tráfico Medido y Proyectado

Por lo anteriormente expuesto se concluye que:

La utilización del protocolo NetFlow en la red de datos de la Facultad de Mecánica, permite determinar el adecuado nivel de utilización de la infraestructura de la red.

4.7 PROPUESTA METODOLOGICA PARA LA PLANEACION DE CAPACIDAD

Al iniciar el proceso de diseño de redes de datos se deben considerar factores como la disponibilidad y escalabilidad, siendo este último muy importante al momento de considerar la actualización del performance o rendimiento de la infraestructura de red.

La finalidad de la escalabilidad es que la red de datos mantenga niveles de capacidad de carga adecuados para poder soportar el incremento del número de usuarios, servicios, aplicaciones, sitios interconectados, etc. La infraestructura de red debe

poder adaptarse al crecimiento y la demanda de los usuarios en el transcurso del tiempo.

Parámetros importantes para mantener la escalabilidad de una red de datos son:

- Pronosticar el futuro basados en el pasado y en el presente.
- Construir un historial efectivo del tráfico de la red permitirá implementar una solución a los aspectos actuales y futuros de la red.

La Capacidad de planeación (Capacity Planning), ayuda a asegurar que los recursos computacionales estarán disponibles para las futuras demandas de carga de trabajo con un performance adecuado. Por lo expuesto se diseñara una propuesta de planificación de carga de la red de datos de la Facultad de Mecánica, en base al análisis histórico de los datos que se obtuvieron luego del periodo de monitoreo con NetFlow Analyzer 9.0.

Los resultados que se obtengan del Capacity Planning permitirá a los técnicos de la Facultad, dimensionar las necesidades de corto y mediano plazo en lo que a infraestructura de red se refiere; presentar estrategias de administración que permitan optimizar la infraestructura de red existente para el óptimo rendimiento de aplicaciones y servicios; y prever el crecimiento esperado debido al cambio constante en la tecnología.

4.7.2 METODOLÓGICA PARA LA PLANEACIÓN DE CAPACIDAD

La propuesta metodológica para la planeación de capacidad de carga en redes de datos se desarrolló tomando en cuenta las consideraciones presentadas en la Metodología para Pronósticos de Tráfico desarrollado por Mehdi Danech- Pajouh en el

año 2002 y en la metodología propuesta para la capacidad de planeación de IBM. La metodología presentada incluye las siguientes etapas:

- Recolección de datos históricos
- Caracterización de la carga de trabajo actual
- Determinación del Throughtput
- Pronostico de la Carga Futura de Trabajo

4.7.2.1 FASE DE RECOLECCIÓN DE DATOS HISTÓRICOS

Para el desarrollo de la metodología, lo primero es tomar una muestra de datos, con los que se pueda caracterizar el tráfico de un tipo de red predeterminada. Los datos de tráfico fueron obtenidos a través del protocolo NetFlow, estos datos se capturaron como variables de tráfico de entrada y salida y el número de paquetes de entrada y salida; del 4 al 29 de Junio del presente año, con intervalo de muestreo de una hora, en el horario de 07h00 a 21h00 de lunes a viernes y divididos en tres períodos: mañana(07:00 a 12:00), medio día (13:00 a 14:00) y tarde(15:00 a 21:00).

4.7.2.2 FASE DE CARACTERIZACIÓN DE LA CARGA DE TRABAJO ACTUAL

En esta fase el objetivo es la descripción y caracterización del tráfico actual de la red de datos, a través de la medición del tráfico generado por las aplicaciones que con mayor frecuencia son utilizadas y que consumen mayor ancho de banda, la tabla IV.35; muestra las aplicaciones más utilizadas durante los períodos (mañana, medio día y tarde) monitoreados en la red de datos de la Facultad de Mecánica.

Tabla IV.35 Aplicaciones más utilizadas

Aplicación	Entrada	Salida	Total (MB)
http	36331,52	789739,52	826071,04

microsoft-ds	78913,30	78930,46	157843,76
netbios-ssn	10302,16	10302,46	20604,62
UDP_App	1369,10	751,66	2120,76
netbios-ns	522,27	520,69	1042,96
SIP	439,10	450,60	889,70
TCP_App	401,28	345,06	746,34
domain	170,92	511,13	682,05
bootps	606,08	60,37	666,45
lotusnote	10,51	481,49	492,00
rmiregistry	12,03	430,89	442,92
netflow	0,00102539	424	424,00

Realizado por: Autor
Fuente: Netflow Analyzer

4.7.2.3 FASE DE DETERMINACIÓN DEL THROUGHPUT

Dentro de la metodología la siguiente fase consiste en determinar el Throughput actual de la red mediante el análisis del tráfico total y del número de paquetes generado en la red. La tabla IV.31 y IV.32 indica el resumen del tráfico total y el número de paquetes.

Tabla IV.36 Resumen del tráfico total generado

Día medición	Entrada	Salida	Total (MB)
4 Junio	1,747	26,086	27,83
5 Junio	1,553	22,671	24,22
6 Junio	1,786	33,689	35,48
7 Junio	1,581	33,214	34,80
8 Junio	0,933	11,172	12,10
11 Junio	479,430	7117,640	7597,07
12 Junio	829,170	15053,860	15883,03
13 Junio	1041,841	18259,610	19301,45
14 Junio	728,060	17200,300	17928,36
15 Junio	389,960	5727,500	6117,46
18 Junio	880,000	18962,960	19842,96
19 Junio	862,280	16534,660	17396,94

20 Junio	755,310	17701,520	18456,83
21 Junio	4260,300	19884,440	24144,74
22 Junio	27017,434	39789,393	66806,83
25 Junio	741,540	12862,370	13603,91
26 Junio	746,190	18759,020	19505,21
27 Junio	831,450	18802,160	19633,61
28 Junio	731,080	13450,590	14181,67
29 Junio	692,360	18939,050	19631,41
TOTAL	**40994,005**	**259171,906**	**300165,91**

Realizado por: Autor
Fuente: Netflow Analyzer

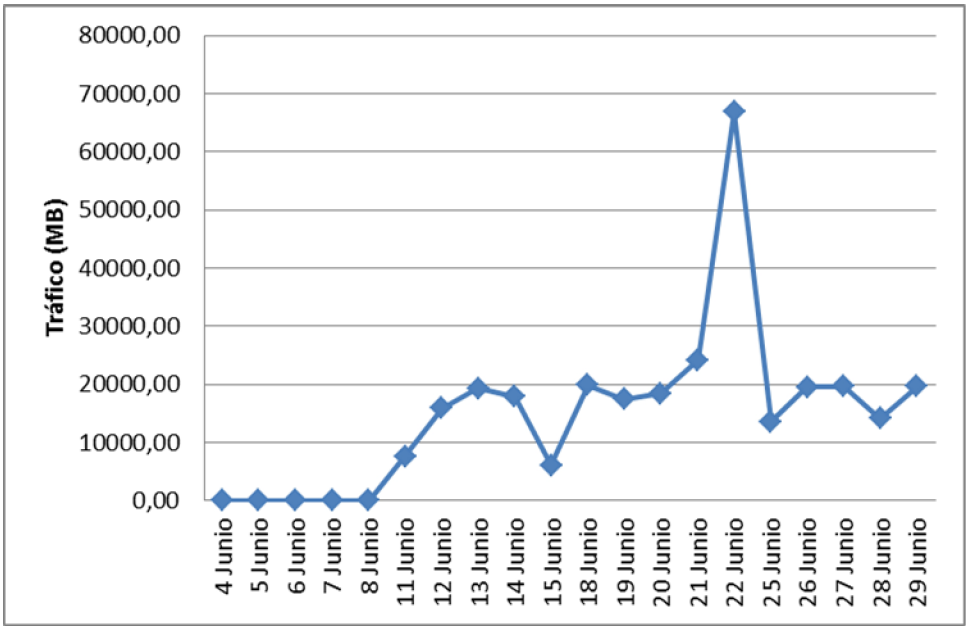


Figura IV.35 Serie de tiempo del tráfico generado

Tabla IV.37 Resumen del número de paquetes generado

	Número Paquetes		Forwarding Rate	
DÍA MEDICIÓN	**Entrada**	**Salida**	**Total**	**PPS**
4 Junio	6350938	9318055	15668993	290,17
5 Junio	5365927	8782262	14148189	262,00
6 Junio	7205449	12139151	19344600	358,23
7 Junio	6840788	11735570	18576358	344,01
8 Junio	2949594	4373998	7323592	135,62

11 Junio	3641098	3641098	7282196	134,86
12 Junio	7745388	7745388	15490776	286,87
13 Junio	8342917	8342917	16685834	309,00
14 Junio	7680639	7680639	15361278	284,47
15 Junio	3027919	3027919	6055838	112,15
18 Junio	9626104	14566675	24192779	448,01
19 Junio	7362280	12722547	20084827	371,94
20 Junio	8751720	13245995	21997715	407,37
21 Junio	10414923	15294713	25709636	476,10
22 Junio	32829814	36286709	69116523	1279,94
25 Junio	6111205	10279567	16390772	303,53
26 Junio	8937908	13865102	22803010	422,28
27 Junio	7322889	14209422	21532311	398,75
28 Junio	6187124	10690858	16877982	312,56
29 Junio	7103732	13846274	20950006	387,96
		TOTAL	**395593215**	**7325,80**

Realizado por: Autor
Fuente: Netflow Analyzer

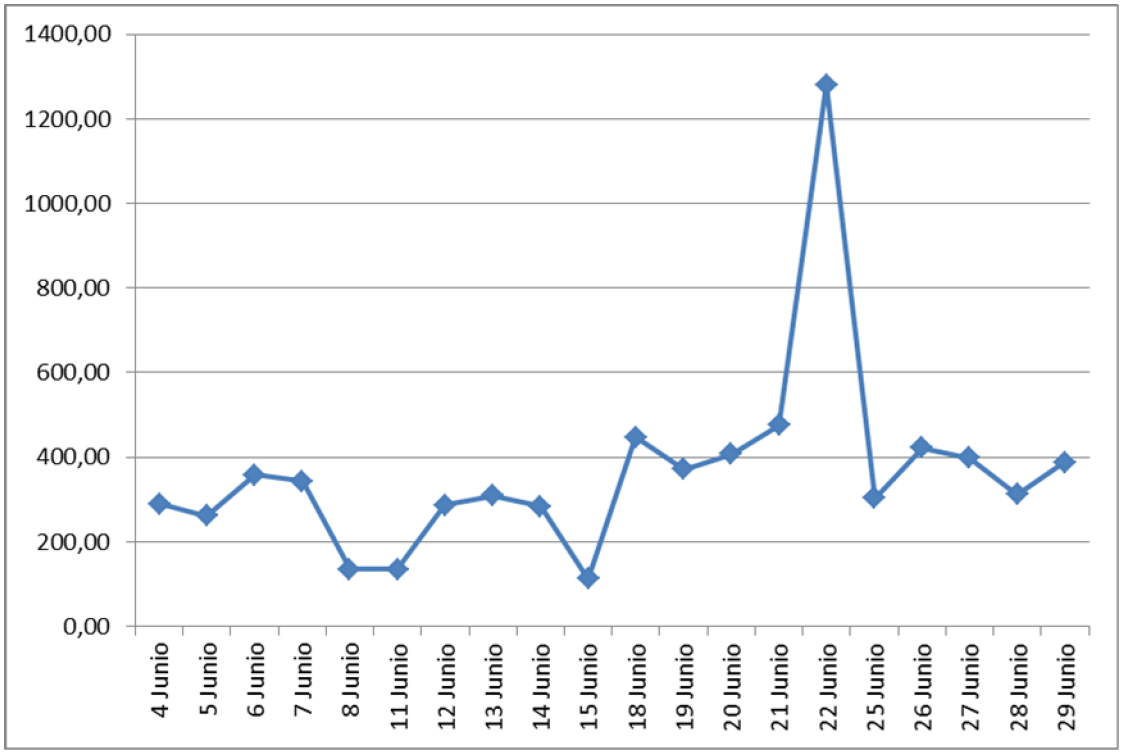


Figura IV.36 Serie de tiempo del número de paquetes

Cálculo del Throughtput

Throughtput (Mbps) = Tráfico Total (Mbits) / Tiempo de Monitoreo (seg.)

Tráfico total = 300165,91 MB

Tráfico total (Mbits) = 2401327,3 Megabits

Tiempo = 15x60x60 = 54000 segundos

Throughput = 2401327,3 / 54000

Throughput = 44,5 Mbps

El Throughput del switch 3560G que se encuentra en la Unidad de Computo de la Facultad de Mecánica tiene una capacidad de 32 Gbps, de los cálculos realizados se determina que durante el periodo de monitoreo se utilizó el 0,14% de la capacidad del equipo; según las investigaciones realizadas el umbral de uso máximo de un switch es del 80%.

Cálculo de la tasa de reenvió de paquetes (Forwarding Rate)

Forwarding_Rate = Número Total de Paquetes / tiempo de monitoreo (seg.)

Número total de paquetes = 395593215

Tiempo = 15x60x60 = 54000 segundos

Forwarding_Rate = 395593215 / 54000

Forwarding_Rate = 7325,80 PPS

Al investigar las especificaciones del switch Cisco Catalyst 3560G, se determinó que la tasa de transferencia de paquetes del es de 38,7 MPPS (millones de paquetes por segundo), por lo que se puedo concluir del cálculo realizado que durante el tiempo de monitoreo se utilizó el 0,0189 % de la tasa de reenvió de paquetes soportada.

4.7.2.4 FASE DE PROYECCIÓN DE LA CARGA DE TRABAJO

Proyectar tráfico en la red de datos de la Facultad de Mecánica tiene como objetivo redimensionar los recursos si fuese necesario, en función de las necesidades, racionalizando el presupuesto, con el tiempo de antelación suficiente.

La proyección del tráfico y del número de paquetes que se generara durante el siguiente mes de uso de la red, en base a los resultados obtenidos en el paso anterior y con la utilización para la determinación de los valores esperados se usó la técnica de pronóstico de tráfico basado en el Modelo Estadístico de análisis de series de tiempo del Promedio Móvil Centrado para determinar los Índices Estacionales.

Los resultados proyectados del tráfico que se generara durante los siguientes veinte días de actividad en la red se detallan en la tabla IV.38.

Tabla IV.38 Resumen del tráfico total proyectado

SEMANA	TOTAL
1	163582,19
2	198671,33
3	233760,47
4	268849,61
TOTAL	**864863,59**

Realizado por: Autor
Fuente: Netflow Analyzer

En la figura IV.37 se hace un contraste entre el trafico medido por la herramienta y el trafico proyectado por el modelo estadístico para observar la tendencia de crecimiento.

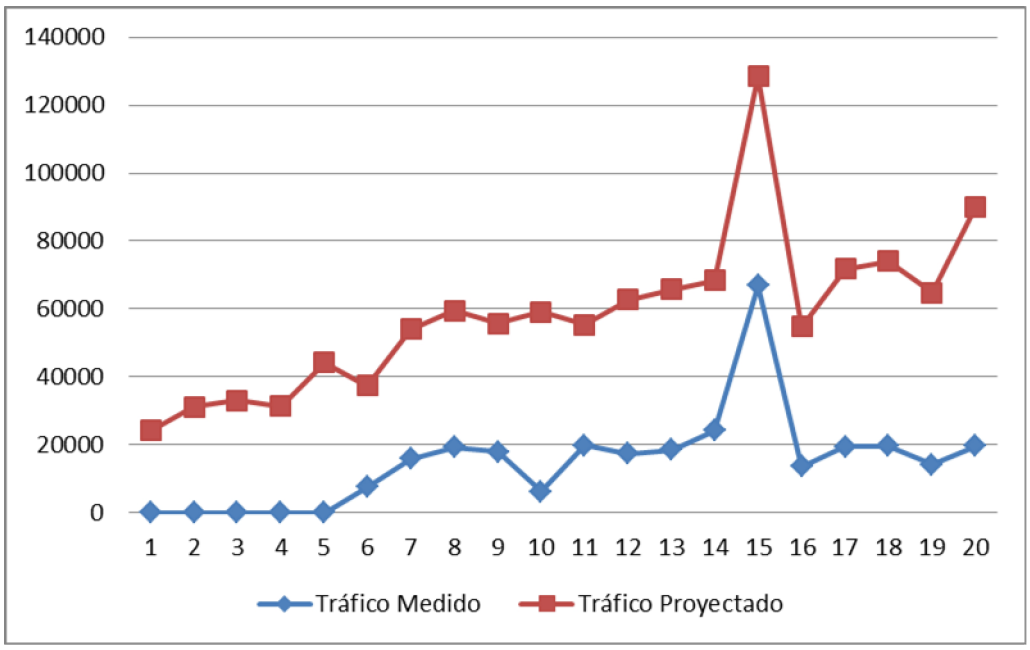


Figura IV.37 Tendencia de crecimiento entre el tráfico medido y proyectado

Con los valores anteriormente proyectados se calcula el Throughput proyectado:

Throughput (Mbps) = Tráfico Total (Mbits) / Tiempo de Monitoreo (s)

Tráfico total = 864863,59 MB

Tráfico total (Mbits) = 6918908,72

Throughput = 6918908,72/ 54000

Throughput = 128,13 Mbps

Uso de la capacidad del Equipo: 0,4%

Con los resultados obtenidos se desprende que el porcentaje proyectado de crecimiento de la carga de tráfico sobre la red de datos de la Facultad de Mecánica para el próximo mes será del 187,93% con relación al mes anterior; lo que significa que para diciembre del año 2012 el uso de la capacidad del switch Cisco 3560G será del 2,4%.

De la misma forma la tabla IV.39 muestra los valores proyectados del número de paquetes que se generaran durante el siguiente mes.

Tabla IV.39 Resumen del número de paquetes proyectado

SEMANA	TOTAL
1	131069436,14
2	148575025,61
3	166080615,09
4	183586204,56
TOTAL	**629311281,39**

Realizado por: Autor
Fuente: Netflow Analyzer

En la figura IV.38 se hace un contraste entre el número de paquetes medido por la herramienta y el número de paquetes proyectado por el Modelo Estadístico de análisis de series de tiempo del Promedio Móvil Centrado para determinar los Índices Estacionales.

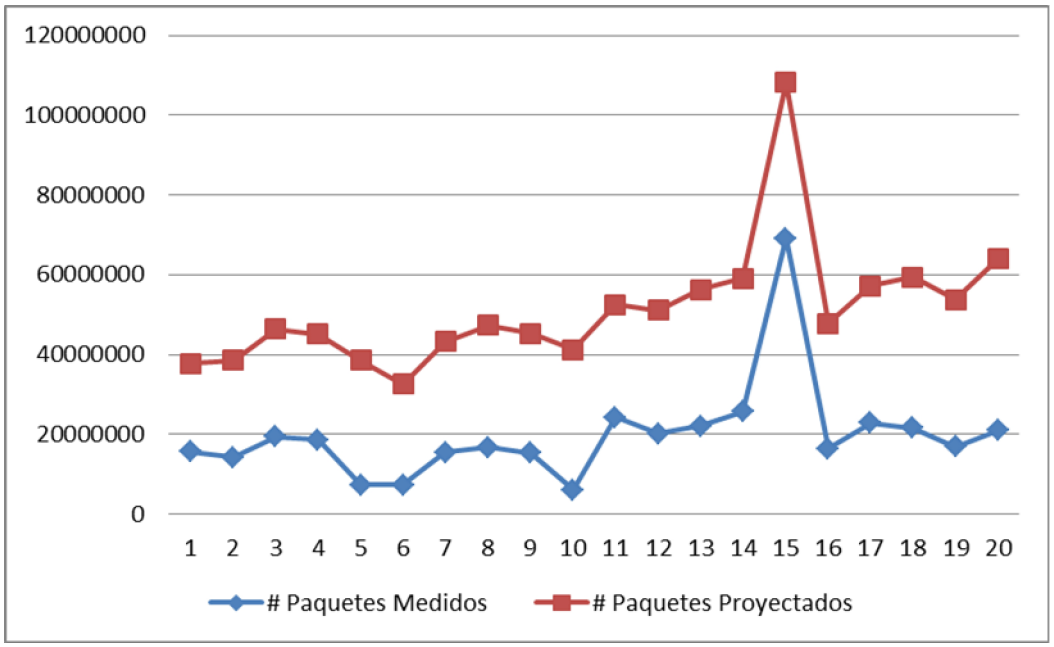


Figura IV.38 Tendencia de crecimiento entre el # paquetes medido y proyectado

Finalmente con estos valores proyectados se calcula la tasa de reenvió de paquetes esperada para el siguiente mes.

Forwarding_Rate = Número Total de Paquetes / tiempo de monitoreo (seg.)

Número total de paquetes = 629311281,39

Tiempo = 15x60x60

Tiempo = 54000 segundos

Forwarding_Rate = 629311281,39 / 54000

Forwarding_Rate = 11653,91 PPS

Con los resultados obtenidos se desprende que el porcentaje proyectado de crecimiento del número de paquetes sobre la red de datos de la Facultad de Mecánica para el próximo mes será del 59,07% con relación al mes anterior; lo que significa que para diciembre del año 2012 el uso de la tasa de reenvió de paquetes del switch Cisco 3560G será del 0,18%.

Tras los resultados que se obtuvieron en el apartado 4.8 y considerando que el patrón de tráfico de crecimiento se mantenga en la red de datos de la Facultad de Mecánica; se puede concluir que no es necesario actualizar el switch Cisco Catalyst 3560G al menos en los próximos 5 años.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. En la investigación se demostró la hipótesis a través de prueba estadística ANOVA, obteniendo un valor del nivel crítico de 0,043 que es menor al nivel de significancia de la prueba α=0,05; por lo que concluimos que se rechaza la hipótesis nula y se acepta la hipótesis de investigación.

2. A través del protocolo NetFlow junto al NetFlow Analyzer, se pudo observar que luego del análisis de flujos IP que atraviesa la red de datos de la Facultad de Mecánica el período de mayor consumo es el de la mañana.

3. Al determinar el mapa de aplicaciones se muestran más de cincuenta aplicaciones de las cuales las de mayor generación de tráfico en los tres períodos de monitoreo son: http y Microsoft-ds.

4. Debemos señalar que tras la investigación y al determinar la matriz de usuarios en cada uno de los períodos analizados en la red de datos, los computadores con las direcciones IP 172.30.102.50 y 172.30.102.78 generan en total un tráfico de 176420,33 Megabytes que corresponde al 37% del tráfico total de la red.

5. Con los resultados obtenidos se desprende que el porcentaje proyectado de crecimiento del número de paquetes sobre la red de datos de la Facultad de Mecánica para el próximo mes será del 59,07% con relación al mes anterior; lo que significa que para diciembre del año 2012 el uso de la tasa de reenvío de paquetes del switch Cisco 3560G será del 0,18%.

6. La metodología de planeación de la capacidad de infraestructura de networking propuesta es una herramienta muy importante para la toma de decisiones a la hora de determinar la conveniencia técnica de actualizar o no la infraestructura existente.

RECOMENDACIONES

1. Implementar herramientas de monitoreo como el protocolo NetFlow para el monitoreo de tráfico en la red de datos de la Facultad Mecánica y en las demás facultades de la ESPOCH, con el afán de proporcionar una herramienta a los administradores de red para caracterizar el tráfico actual de la intranet institucional y los usuarios que generan mayor consumo.

2. Promover futuras investigaciones en el campo del análisis de tráfico IP en redes LAN con la finalidad de determinar patrones de comportamiento en el tráfico que atraviesan las redes, y a través de los resultados poder detectar situaciones anómalas que pongan en riesgo la seguridad de la red, como presencia de malware o ataques internos.

3. Investigar más sobre los diferentes Modelo Estadístico de análisis de series de tiempo para determinar los Índices Estacionales de proyección de tráfico, para mejorar la precisión de planeación de capacidad.

4. Utilizar la metodología propuesta para realizar la guía de planeación de capacidad para la Intranet Institucional, con la finalidad de poder dimensionar los recursos de Networking que la institución necesitaría en los próximos años.

GLOSARIO DE TÉRMINOS

A

Accounting.- Proceso de identificar, medir y reportar información.

B

BackBone.- La palabra ***backbone*** se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica. El término ***backbone*** también se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

C

Capacity Planning.- La planificación de capacidad es la habilidad para planificar y gestionar proactivamente sus necesidades de TI de una manera que efectivamente va a equilibrar costo de los recursos y el rendimiento del sistema. La planificación de capacidad ayuda a garantizar el rendimiento del sistema está siempre en el mejor nivel posible y el menor costo posible.

D

Data Center.- Es un servicio de infraestructura informática a su disposición, creado para preservar y/o administrar la información con seguridad usando tecnología de punta. Dedicado a entidades que deseen reducir sus costos operativos y situar sus

equipos informáticos y/o información físicamente en un lugar diseñado y construido bajo normas internacionales de seguridad e infraestructura, tanto física como logística.

Data warehousing.- En el contexto de la informática, un almacén de datos (del inglés data warehouse) es una colección de datos orientada a un determinado ámbito (empresa, organización, etc.), integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la entidad en la que se utiliza. Se trata, sobre todo, de un expediente completo de una organización, más allá de la información transaccional y operacional, almacenado en una base de datos diseñada para favorecer el análisis y la divulgación eficiente de datos (especialmente OLAP, procesamiento analítico en línea).

Data Minig.- La Minería de Datos, es un conjunto de técnicas provenientes de la Inteligencia Artificial y la Matemática Compleja, cuya finalidad, en el ambiente empresarial, es la de encontrar en grandes bases de datos patrones ocultos, no triviales e imposibles de detectar mediante otros mecanismos estadísticos; para luego extraer dicha información, la cual puede convertirse en el activo más importante de una empresa a la hora de toma de decisiones y encarar futuras estrategias de negocios.

E

E-learning.- Se denomina **aprendizaje electrónico** (conocido también por el anglicismo *e-learning*) a la educación a distancia completamente virtualizada a través de los nuevos canales electrónicos (las nuevas redes de comunicación, en especial Internet), utilizando para ello herramientas o aplicaciones de hipertexto (correo electrónico, páginas web, foros de discusión, mensajería instantánea, plataformas de

formación que aúnan varios de los anteriores ejemplos de aplicaciones, etc.) como soporte de los procesos de enseñanza-aprendizaje.

H

Host.- Un **host o anfitrión** es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web. Un host de Internet tiene una **dirección de Internet** única (dirección IP) y un **nombre de dominio** único o nombre de host. El término **host** también se utiliza para referirse a una compañía que ofrece servicios de alojamiento para sitios web.

M

MySQL.- Es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones. MySQL AB —desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009— desarrolla MySQL como software libre en un esquema de licenciamiento dual. Por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSI C.

Megabytes.- El Megabyte (MB) es una unidad de medida de cantidad de datos informáticos. Equivale a un millón de bytes, o mil kilobytes (exactamente 1,048,576 bytes).

Monitorear.- El monitoreo es una herramienta de gestión y de supervisión para

controlar el avance de los proyectos, programas o planes en ejecución, el cual proporciona información sistemática, uniforme y fiable, permitiendo comparar los resultados con lo que se planificó.

A diferencia de la supervisión, el monitoreo se puede efectuar con el análisis de la información, enviada por los diferentes niveles, sin ir al terreno. Su objetivo es identificar logros y problemas, determinar su importancia, analizar sus causas, y adoptar medidas pertinentes en forma inmediata.

N

NetFlow.- Es un protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP. NetFlow se ha convertido en un estándar de la industria para monitorización de tráfico de red, y actualmente se está soportado para varias plataformas además de Cisco IOS y NXOS, como por ejemplo en dispositivos de fabricantes como Juniper, Enterasys Switches, y en sistemas operativos como Linux, FreeBSD, NetBSD y OpenBSD.

NetFlow Analyzer.- NetFlow Analyzer utiliza tecnología Cisco NetflowTM, Cisco NBARTM, sFlowTM y los MIB Cisco CBQoS para proporcionar información valiosa sobre los detalles de tráfico. Sus potentes herramientas de análisis que interpretan y presentan esta información a través de una consola web, mostrando cómo los usuarios, aplicaciones y dispositivos generan el tráfico, así como datos sobre la utilización de ancho de banda.
La consola es personalizable y permite monitorear todos los aspectos de sus routers y switches.

P

Pager.- Dispositivo pequeño en donde se reciben mensajes por teléfono o email, originalmente sólo se podían leer pero no enviar, ahora ofrecen en ambos sentidos.

Protocolo.- En redes informáticas, un protocolo es el lenguaje (conjunto de reglas formales) que permite comunicar nodos (computadoras) entre sí. Al encontrar un lenguaje común no existen problemas de compatibilidad entre ellas.

R

Routers.- Un **router** (también conocido como **enrutador** o **encaminador de paquetes)** es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

S

Servidor proxy.- Un **proxy**, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina ***A*** solicita un recurso a una ***C***, lo hará mediante una petición a ***B***; ***C*** entonces no sabrá que la petición procedió originalmente de ***A***. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: proporcionar caché, control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, etc.

Sniffers.- El sniffer es un software que permite capturar tramas de la red.

Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas, etc.

Subredes.- Es una forma de organizar los hosts que hay dentro de una red en un grupo lógico. La subred permite subdividir una NetID en dos o más redes.

Switch.- Un **conmutador** o ***switch*** es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

T

Throughput.- Se llama **throughput** al volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos. Particularmente significativo en almacenamiento de información y sistemas de recuperación de información, en los cuales el rendimiento es medido en unidades como accesos por hora.

BIBLIOGRAFIA

[1] BENOIT Claise. Network Management: Accounting and Performance Strategies. Indianapolis-USA. Ciscopress. 2007. p.p. 3-525.

[2] CISCO SYSTEM , Guía de Segundo Año CCNA 3 y 4. 3.ed. Madrid-España. Ciscopress. 2005. 896 p.

[3] CLEMM Alexander. Network Management Fundamentals. Indianapolis-USA. Ciscopress. 2007. 532 p.

[4] Capacity Planning, Wikipedia.
en.wikipedia.org/wiki/Capacity_planning
[10 – 06 - 2012]

[5] Características NetFlow Analyzer , ManageEngine.
http://me.zma.com.ar/caracteristicas-de-producto-me-netflow-analyzer-8-3.html
[10 – 06 - 2012]

[6] Cisco IOS Netflow, Cisco.
http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
[09 – 06 - 2012]

[7] Flexible NetFlow, CISCO.
http://www.cisco.com/en/US/products/ps6965/products_ios_protocol_option_home.htm
[15 – 08 - 2012]

[8] From Netflow to IPFIX,Brian, Trammell.

http://www.cert.org/netsa/publications/nanog41-ipfix.pdf

[10 – 06 - 2012]

[9] How to do Capacity Planning, TeamQuest.

www.teamquest.com/pdfs/whitepaper/tqwp23.pdf

[10 – 06 - 2012]

[10] NetFlow, Ecured [Online].

http://www.ecured.cu/index.php/Netflow

[16 - 05 - 2012]

[11] NetFlow, Wikipedia.

http://es.wikipedia.org/wiki/Netflow

[16 - 05 - 2012]

[12] NetFlow Analyzer, Manageengine.

http://www.manageengine.es/pages/productos/netflow-analyzer/resumen/

[16 – 05 - 2012]

[13] NetFlow Analyzer, Adventenet.

http://demo.netflowanalyzer.com/

[16 – 05 - 2012]

[14] NetFlow Services Solutions Guide, Cisco.

http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html

[09 – 06 - 2012]

[15] Monitoreo de Red, Wikipedia.

http://es.wikipedia.org/wiki/Monitoreo_de_red

[09 – 06 - 2012]

[16] Multidimensional index structure for Netflow records processing, Alexander Sherikov, Dr. Yuri A. Bogoiavlensky.

http://www.cs.karelia.ru/fdpw/2007/sherikov/sherikov.pdf

[09 – 06 - 2012]

[17] Planeación de Capacidades, Microsoft.

http://technet.microsoft.com/es-es/library/cc732102%28WS.10%29.aspx

[09 – 06 - 2012]

[18] Planificación de Capacidades, Consultores Lanware c.a.

http://www.lanware.com.ve/servicios/catplan.html

[09 – 06 - 2012]

[19] Plataforma de monitoreo y análisis de tráfico para redes IP, MIRA Galán Fermín.

http://www.universidadcarlosIII.com/area_ingenieria/mira/

[10 – 06 - 2012]

[20] Traffic Flow Measurement, Meter MIB.

http://netflow.caligare.com/rfc_2720.txt

[4 – 08 - 2012]

ANEXOS

ANEXO 1

INSTALACIÓN Y CONFIGURACIÓN DEL PROTOCOLO NETFLOW

INSTALACIÓN Y CONFIGURACIÓN DEL PROTOCOLO NETFLOW

Configuración del Switch capa 3

Iniciamos con la configuración de la comunidad SNMP en 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

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

Switch(config)#snmp-server ifindex persist

Switch(config)#ctrl Z

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

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

Switc#show ip cahe flow

ANEXO 2

DATA SHEET SWITCH CATALYST

3560G

ANEXO 3

DESCRIPCION DE LAS APLICACIONES MONITOREADAS

Http

HyperText Transfer Protocol, es el protocolo de transferencia de hipertexto usado en cada transacción de la Web (WWW). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxis) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. *Utiliza el puerto 80.*

Microsoft-DS

Microsoft-DS (Servicios de directorio Microsoft) es un puerto utilizado para compartir archivos. Fue introducido con Windows 2000 y da la posibilidad de utilizar el protocolo SMB (stands for Server Message Block, también es conocido como Samba) directamente a través de TCP-IP en el puerto 445.

Netbios-ssn

NetBios es el protocolo de redes Microsoft, que aporta opciones como resolución de Nombres de máquinas en una misma red, sin necesidad de DNS, es lo que podríamos llamar equipos próximos. Funciona a través del puerto TCP 139, y permite mostrar los recursos compartidos de una máquina.

Netbios-dgm y netbios-ns

NetBIOS, 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. **Netbios-ns** usa el puerto 137/tcp y **netbios-dgm** 138/tcp NETBIOS Datagram Service.

SIP

Session Initiation Protocol (**SIP** o **Protocolo de Inicio de Sesiones**) es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual. Los servidores, por defecto, utilizan el puerto 5060 en TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*) para recibir las peticiones de los clientes SIP.

TCP_App y UDP_App

La herramienta 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.

Domain

El **Domain Name System** (DNS) 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. Utiliza el puerto 53.

Bootps

BOOTP son las siglas de **Boot**strap **P**rotocol. Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de los ordenadores o del sistema operativo. Este protocolo permite a los ordenadores sin disco obtener una dirección IP antes de cargar un sistema operativo avanzado. El número de puerto UDP es el 67 y 68

Rmiregistry

El RMI Registry es una aplicación Cliente-Servidor en Java usando RMI que puede estar localizado en un lugar distinto al servidor, y se encarga de registrar un determinado objeto y asignarle un servidor que se encargará de procesar dicho objeto. rmiregistry utiliza el puerto 1099.

Rmiactivation

El RMI Registry es una aplicación Cliente-Servidor en Java usando RMI que puede estar localizado en un lugar distinto al servidor, y se encarga de activar un determinado objeto.

Lotusnote

Es un sistema cliente - servidor propietario de trabajo colaborativo y correo electrónico, desarrollado por Lotus Software, filial de IBM. La parte del servidor recibe el nombre *Domino*, mientras que el cliente se llama *Notes*. El puerto utilizado es el 443.

ANEXO 4

GUIA DE USUARIO DE

NETFLOW ANALYZER

NetFlow Analyzer[3]

NetFlow Analyzer es una herramienta basada en la Web (sin dispositivos de hardware), para el control y análisis del tráfico de la red, que ha optimizado miles de redes en múltiples sectores para lograr el mayor rendimiento y ayudar a optimizar el uso del ancho de banda. NetFlow Analyzer es un recopilador, analizador y motor de informes NetFlow, sFlow, JFLow (y más) *todo junto*. Con casi **4.000 empresas** que usan NetFlow Analyzer para una visibilidad en profundidad del tráfico de red y sus patrones, NetFlow Analyzer continúa ganándose la confianza de más usuarios al brindar conocimiento comercial del comportamiento de la red en tiempo real y de cómo el tráfico tiene un impacto sobre la salud general de la red.

¿Qué problemas soluciona?

Uno de los problemas claves en la administración de red es saber la autenticidad del tráfico. NetFlow Analyzer brinda información detallada de los patrones de utilización del ancho de banda para el análisis de tráfico, planeamiento de capacidad y la toma de decisiones. Mediante la investigación detallada de aplicaciones específicas, usuarios, puertos o comunicaciones, los administradores de red, son capaces de determinar la fuente exacta de picos y ráfagas y, de esta manera, pueden monitorear, controlar y tomar decisiones actuando proactivamente. NetFlow Analyzer nos termite:

- Conocer el **rendimiento** de su red
- Evaluar el impacto de las diferentes **aplicaciones** en su red
- Validar las **políticas de calidad de servicio** y sus efectos
- Optimizar el **ancho de banda**

[3] ZMA IT Solutions

- Detectar **tráfico WAN** no autorizado en su red

Qué plataformas / vendors / tecnologías admite?

Plataformas: Windows & Linux.

Vendors: CISCO, Juniper, HP, APC, IBM, Intel, Microsoft.

Características

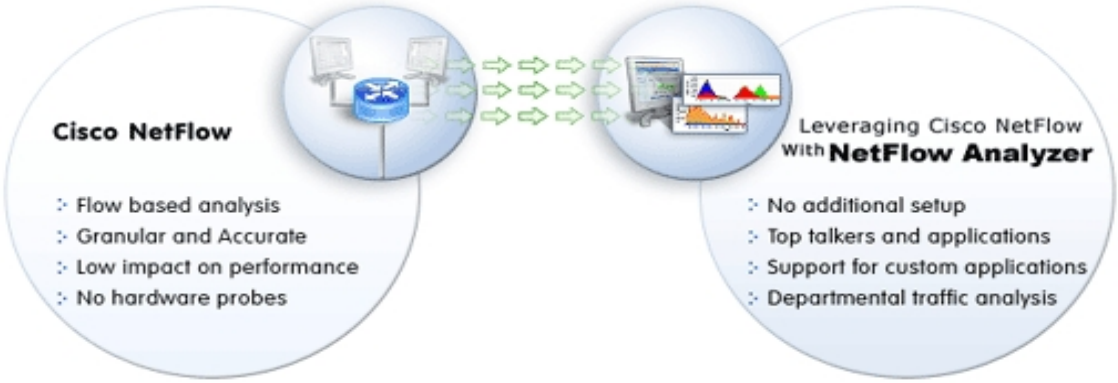
NetFlow Analyzer permite visibilidad en profundidad con top hosts, aplicaciones, DSCP, TCP_Flag e información AS por cada link y por divisiones y departamentos basadas en IP configurable, categorización y reconocimiento minuciosos de aplicaciones, alertas proactivas y programación, acceso de usuarios basados en privilegios.

Control del ancho de banda de la red

El control del ancho de banda de la red es una de las actividades más críticas de un administrador de redes empresariales. NetFlow Analyzer brinda varios informes instantáneos para controlar el ancho de banda, incluidos los principales generadores de tráfico, protocolos, conversaciones y más. Además de estos informes predefinidos de ancho de banda, NetFlow Analyzer también incluye opciones para buscar detalles específicos del uso del ancho de banda en función de la dirección IP, nombre de host, protocolo y más.

Análisis del tráfico de la red

NetFlow Analyzer le permite controlar el ancho de banda y tráfico en un nivel específico de la interfaz con una granularidad de un minuto. El gráfico seleccionable le permite acercar los picos. NetFlow Analyzer también muestra los puntos de datos, que le brinda detalles del tráfico entrante y saliente, como velocidad, volumen, paquetes y utilización del total del ancho de banda.



Informes programados y perfiles de alerta

NetFlow Analyzer le brinda un análisis profundo y genera y envía automáticamente el informe a su casilla de correo. Le permite programar los informes para que se generen periódicamente. Puede seleccionar los criterios para los informes según sus requisitos. También puede crear perfiles de alerta según sus requisitos, las alertas pueden activar trampas SNMP o pueden enviarse como notificación de correo.

Solución más rápida de problemas de la red

El informe de solución de problemas de la red le ayuda a solucionar los incidentes de la red más rápidamente. El informe le permite seleccionar diferentes criterios a partir de los cuales puede generar este informe en particular. Obtiene un informe en el que puede ver el tráfico, la aplicación, el origen, el destino, la conversación y mucho más para el período específico que seleccionó en el gráfico. Así de simple es obtener una

visibilidad en profundidad de la utilización pasada del tráfico de la red y del ancho de banda. Puede exportar el informe como PDF, CSV o incluso enviarlo por correo electrónico.

Control de protocolos y aplicaciones

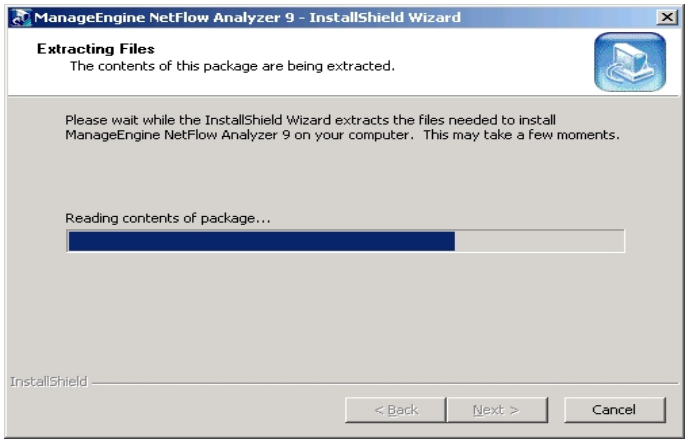
- Los administradores de la red (usuarios) pueden ver qué aplicaciones se están usando en la red
- Se conoce el **ancho de banda consumido** por cada aplicación
- **Asignación de aplicaciones**: las aplicaciones específicas de la empresa se pueden asignar según la necesidad del usuario
- **Agrupación de aplicaciones**: capacidad de agrupar ciertas aplicaciones según los requisitos del usuario para un fácil control
- La capacidad de asignar aplicaciones en función del **puerto, del protocolo** Y **de la dirección IP / red**
- La **distribución de protocolos** puede verse fácilmente

Ajuste de políticas de calidad de servicio con Cisco CBQoS

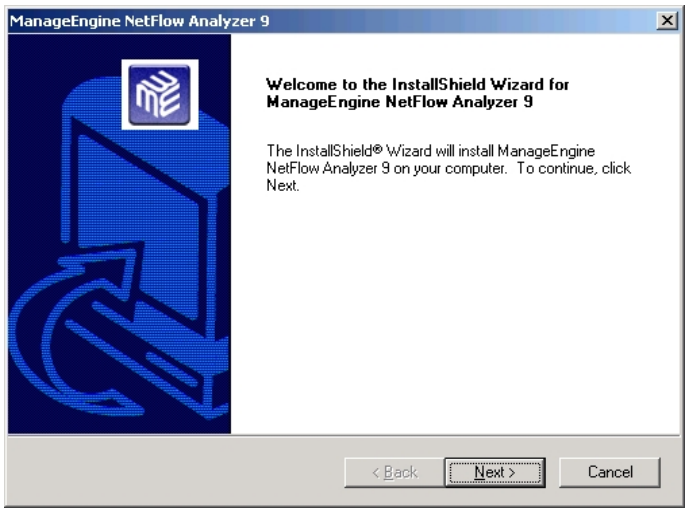
Los administradores de red implementan políticas de calidad de servicio para garantizar que las aplicaciones críticas para el negocio obtengan la prioridad más alta en la red. BQoS puede hacer que el rendimiento de la red sea más predecible y la utilización del ancho de banda más eficaz. CBQoS le brinda visibilidad en profundidad de las políticas aplicadas a sus enlaces y de los patrones de tráfico en sus diferentes tipos.

Instalación de NetFlow Analyzer

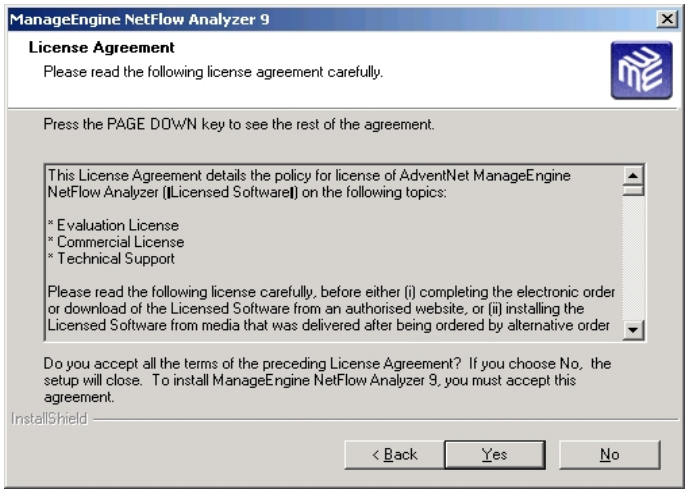
Para poder aprovechar las caractersiticas NetyFlow Analyzer debemos instalarla la herramienta de la siguiente manera. Ejecutamos el instalador y nos muestra la siguiente ventana que nos indica el inicio de la instalacion.



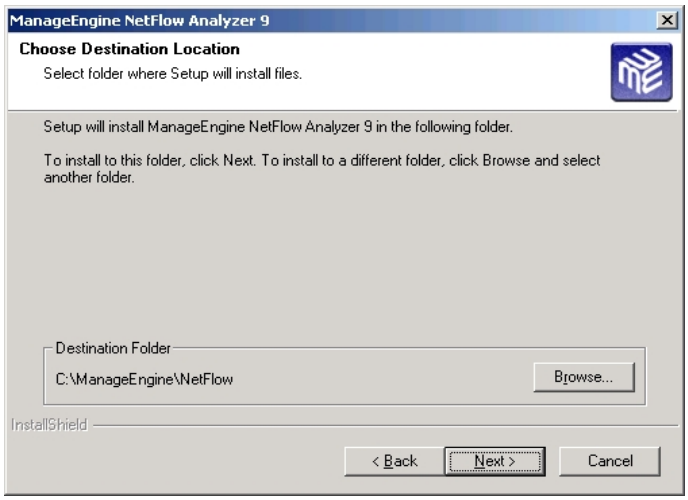
A continuación nuestra la pantalla de bienvenida.



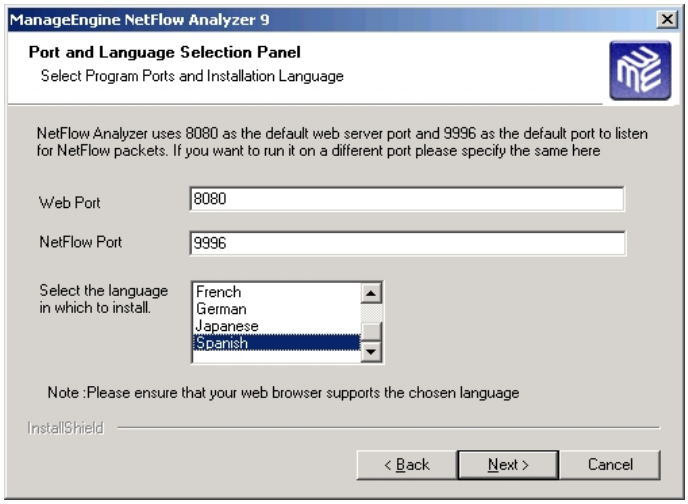
Lo siguiente es Aceptar la licencia de uso dela herramienta.



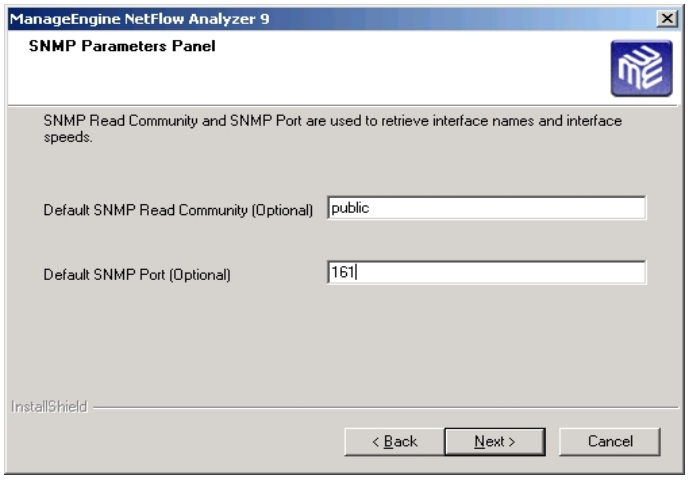
Luego le indicaremos la ruta en donde se instalara el programa.



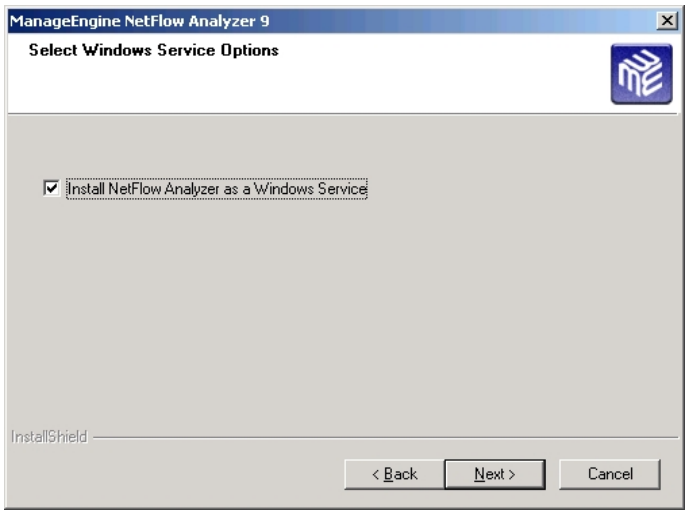
La siguiente pantalla nos pedira que ingresemos los puertos y el lenguaje de instalación.



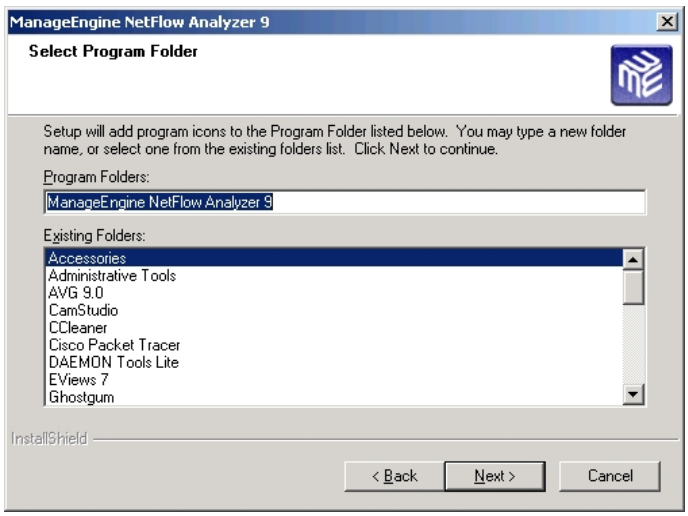
Luego indicar los Parámetros SNMP.



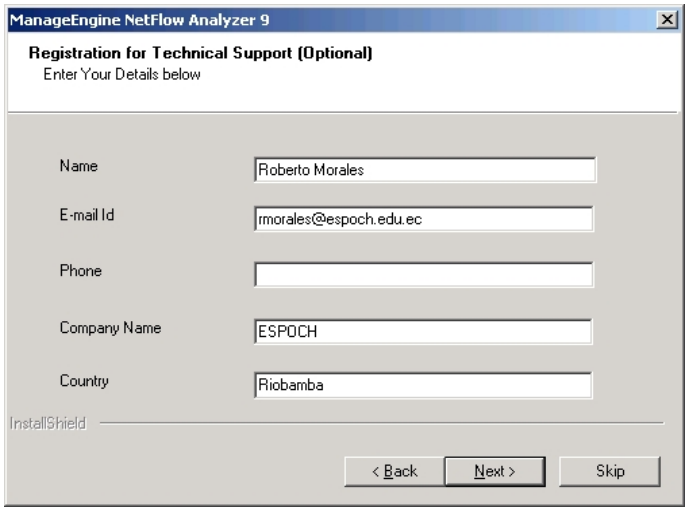
La siguiente pantalla muestra la selección para el Windows Service.



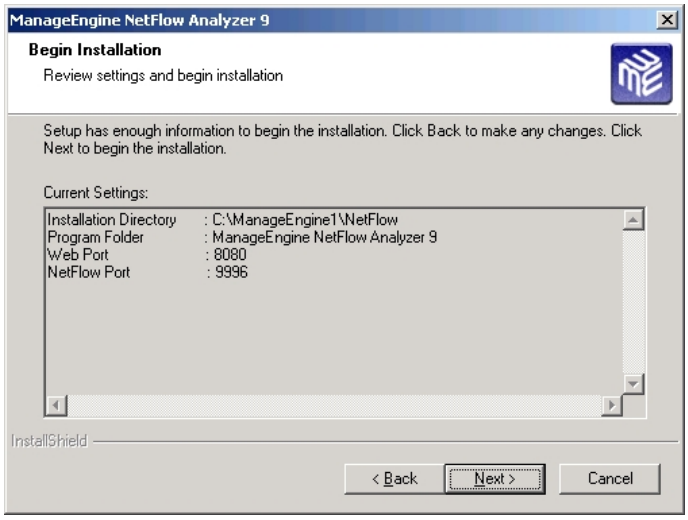
A continuación seleccionamos el folder del programa.



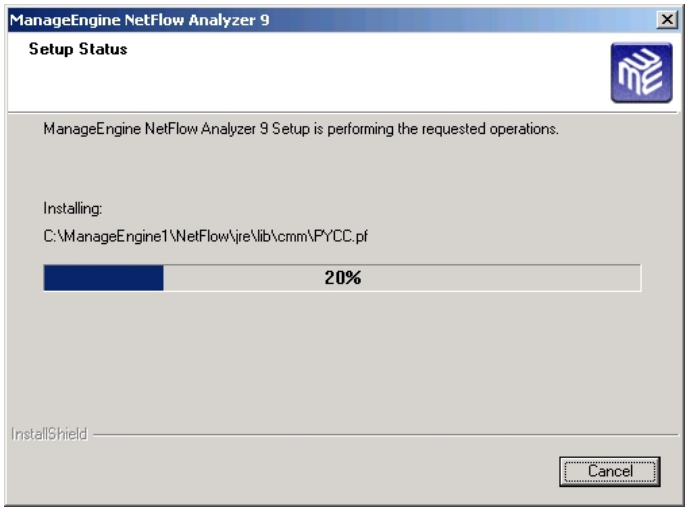
Lo siguiente es ingresar los datos del Técnico de soporte.



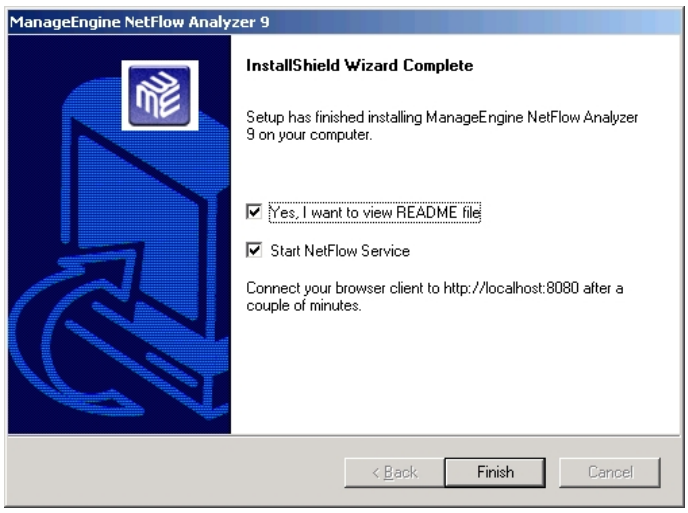
Luego aparace la pantalla que indica el inicio de la instalación.



La pantalla siguiente muestra el progreso de la instalación.



Por último muestra la pantalla de finalización del proceso.



Para poder ingresar a la aplicación se utiliza un explorador web, de la siguiente manera: 172.30.60.2:8080 y la validación correspondiente.

Informes de NetFlow

NetFlow Analyzer le brinda un completo conjunto de informes de ancho de banda incorporados que ofrecen estadísticas exhaustivas del uso de ancho de banda y le permiten obtener el detalle de un host, una aplicación o una conversación en particular que provocó un cuello de botella. Además de poder ver al instante qué enlace se encuentra congestionado, NetFlow Analyzer también le permite monitorear el ancho de banda, o sea, las tendencias de uso de ancho de banda en distintos períodos de tiempo, tomar decisiones críticas sobre la planificación de la capacidad y hacer cumplir políticas de seguridad.

Informes de uso de tráfico

Visualiza los patrones de uso de tráfico actual, promedio y pico de una interfaz, y consulte cuánto ancho de banda disponible fue consumido por una interfaz específica. Así, podrá monitorear el ancho de banda de manera eficiente.

Informes históricos

Visualice los informes de tráfico sobre uso de ancho de banda diariamente, semanalmente o mensualmente. Vea las tendencias de uso en hosts, aplicaciones y períodos de tiempo específicos. Podrá monitorear el uso de ancho de banda de cualquier período de tiempo pasado.

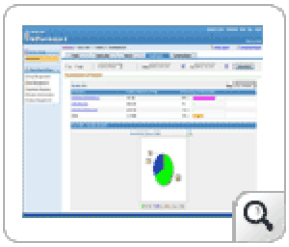
Perfil del tráfico

Visualice los informes sobre principales aplicaciones, hosts y conversaciones en distintos períodos de tiempo y obtenga el detalle de estos informes. Vea quién está consumiendo el

máximo ancho de banda y con qué propósito.

Informes personalizados

Vea los detalles del tráfico para aplicaciones, conversaciones o hosts específicos. Relacione la información para saber quién consumió el ancho de banda, cuándo, para qué aplicación y por cuánto tiempo.



Informes basados en rango de IP y subredes

Visualice los informes de tráfico de una subred específica o de un rango de direcciones IP. Vea el uso de ancho de banda por red o subred y determine cuáles son las horas pico de uso y las tendencias típicas de uso en un grupo de usuarios.

Informes de interfaz

Visualice resúmenes de cada interfaz sobre el uso total del ancho de banda, en distintos períodos de tiempo. Vea las estadísticas de utilización de la interfaz durante las horas pico, y resuelva con facilidad los cuellos de botella.

Direcciones de hosts resolubles

Todos los informes de tráfico incluyen direcciones IP de origen y destino resolubles, con el objetivo de visualizar las estadísticas de ancho de banda desde o hacia un sitio web o un host.

Visualización variable

Vea los gráficos en términos de volumen de tráfico (Kb), tasa de tráfico (bps), o como porcentaje de utilización del enlace.

Informes exportables

No sólo podrá monitorear el ancho de banda, sino que también podrá exportar gráficos e informes como archivos PDF y guardarlos.

ANEXO 5

MODELO ESTADÍSTICO DE ANÁLISIS DE SERIES DE TIEMPO DE PROMEDIO MÓVIL CENTRADO

CONCEPTOS BASICOS DE SERIES DE TIEMPO

INTRODUCCIÓN

La planificación racional exige prever los sucesos del futuro que probablemente vayan a ocurrir. La previsión, a su vez, se suele basar en lo que ha ocurrido en el pasado. Se tiene pues un nuevo tipo de inferencia estadística que se hace acerca del futuro de alguna variable o compuesto de variables basándose en sucesos pasados. La técnica más importante para hacer inferencias sobre el futuro con base en lo ocurrido en el pasado, es el ***análisis de series de tiempo***.

Son innumerables las aplicaciones que se pueden citar, en distintas áreas del conocimiento, tales como, en economía, física, geofísica, química, electricidad, en demografía, en marketing, en telecomunicaciones, en transporte, etc.

Series De Tiempo	***Ejemplos***
1. Series económicas:	▪ Precios de un artículo ▪ Tasas de desempleo ▪ Tasa de inflación ▪ Índice de precios, etc.
2. Series Físicas:	▪ Meteorología ▪ Cantidad de agua caída ▪ Temperatura máxima diaria ▪ Velocidad del viento (energía eólica) ▪ Energía solar, etc.
3. Geofísica:	▪ Series sismologías

4. Series demográficas:	↓ Tasas de crecimiento de la población ↓ Tasa de natalidad, mortalidad ↓ Resultados de censos poblacionales
5. Séries de marketing:	↓ Series de demanda, gastos, ofertas
6. Series de telecomunicación:	↓ Análisis de señales
7. Series de transporte:	↓ Series de tráfico

Uno de los problemas que intenta resolver las series de tiempo es el de predicción. Esto es dado una serie {*x(t1),...,x(tn)*} nuestros objetivos de interés son describir el comportamiento de la serie, investigar el mecanismo generador de la serie temporal, buscar posibles patrones temporales que permitan sobrepasar la incertidumbre del futuro.

En adelante se estudiará cómo construir un modelo para explicar la estructura y prever la evolución de una variable que observamos a lo largo del tiempo. La variables de interés puede ser macroeconómica (índice de precios al consumo, demanda de electricidad, series de exportaciones o importaciones, etc.), microeconómica (ventas de una empresa, existencias en un almacén, gastos en publicidad de un sector), física (velocidad del viento en una central eólica, temperatura en un proceso, caudal de un río, concentración en la atmósfera de un agente contaminante), o social (número de nacimientos, matrimonios, defunciones, o votos a un partido político).

DEFINICIÓN DE SERIE DE TIEMPO

En muchas áreas del conocimiento las observaciones de interés son obtenidas en instantes sucesivos del tiempo, por ejemplo, a cada hora, durante 24 horas, mensuales, trimestrales, semestrales o bien registradas por algún equipo en forma continua.

Llamamos *Serie de Tiempo* a un conjunto de mediciones de cierto fenómeno o experimento registradas secuencialmente en el tiempo. Estas observaciones serán denotadas por $\{x(t_1), x(t_2), ..., x(t_n)\} = \{x(t) : t \in T \subseteq R\}$ con $x(t_i)$ el valor de la variable x en el instante t_i. Si T = Z se dice que la serie de tiempo es discreta y si T = R se dice que la serie de tiempo es continua. Cuando $t_{i+1} - t_i = k$ para todo $i = 1,...,n-1$, se dice que la serie es equiespaciada, en caso contrario será no equiespaciada.

En adelante se trabajará con series de tiempo discreta, equiespaciadas en cuyo caso asumiremos y sin pérdida de generalidad que: $\{x(t1), x(t2), ..., x(tn)\} = \{x(1), x(2), ..., x(n)\}$.

Para la investigación y considerando los conceptos anteriores; la proyección se lo realizo en base a los 5 pasos siguientes:

1.- MÉTODO DEL PROMEDIO MOVIL CENTRADO PARA DETERMINAR LOS ÍNDICES ESTACIONALES DE LA SERIE DE TIEMPO DEL PROBLEMA

Para medir la influencia de la variación estacional se han desarrollado diversos métodos, sin embargo, la mayoría de ellos lo hace a través de un índice estacional (It), el cual indica las altas y bajas esperadas en los niveles de actividad semanal, quincenal, mensual o trimestral, eliminando los efectos ocasionados por los componentes tendencia, Ciclo y Azaroso.

Dentro de los métodos que existen para determinar los índices estacionales de una serie de tiempo, uno de los más comunes es el método del Promedio Móvil Centrado, el cual se describe a continuación.

Semana	Días	# Paquetes Xt	Total mensual centrado Ct	Total de 2 años Tt	Promedio Móvil Centrado Et =Tt/96	It = Xt/Et
1	I	15668993				
	II	14148189	75061732			
	III	19344600	66674935	141736667	1476423,615	13,10
	IV	18576358	68017522	134692457	1403046,427	13,24
	V	7323592	65358756	133376278	1389336,229	5,27
2	I	7282196	62143676	127502432	1328150,333	5,48
	II	15490776	60875922	123019598	1281454,146	12,09
	III	16685834	77786505	138662427	1444400,281	11,55
	IV	15361278	82380556	160167061	1668406,885	9,21
	V	6055838	87692437	170072993	1771593,677	3,42
3	I	24192779	98040795	185733232	1934721,167	12,50
	II	20084827	161101480	259142275	2699398,698	7,44
	III	21997715	153299473	314400953	3275009,927	6,72
	IV	25709636	156017656	309317129	3222053,427	7,98
	V	69116523	155552252	311569908	3245519,875	21,30
4	I	16390772	146720598	302272850	3148675,521	5,21
	II	22803010	98554081	245274679	2554944,573	8,93
	III	21532311				
	IV	16877982				
	V	20950006				

Una vez completada la tabla anterior, podemos observar que se cuenta con diferentes índices estacionales para un mismo período, por esta razón es necesario determinar un único índice estacional representativo para cada uno de ellos. Para esto:

A.- Obtener un índice promedio para cada una de las semanas

En este Caso	SEMANAL					
	I	II	III	IV	V	

	5,48	12,09	13,10	13,24	5,27	
	12,50	7,44	11,55	9,21	3,42	
	5,21	8,93	6,72	7,98	21,30	Sum.Prom.:
Promedio	**7,73**	**9,48**	**10,46**	**10,14**	**10,00**	47,81

La suma de los promedios obtenidos debe ser igual al número de períodos en los que se ha dividido la semana que para este caso es 5. Si se estuviera trabajando con datos mensuales la suma debería ser 12. Si la suma de los promedios cumple con lo anterior, los índices estacionales promedio obtenidos son los que buscamos, de lo contrario sería necesario realizar el siguiente procedimiento:

B.- Normalizar los Índices Estacionales Promedio:

Esto se hace multiplicando los índices promedio obtenidos por un Factor de Normalización, el cual se obtiene mediante:

FN = (5) / SUMA DE LOS PROMEDIOS

FN = 0,104580387

Al multiplicar los Índices Promedio por el Factor de Normalización se obtiene:

Índice I =0,81

Índice II =0,99

Índice III =1,09

Índice IV =1,06

Índice V =1,05

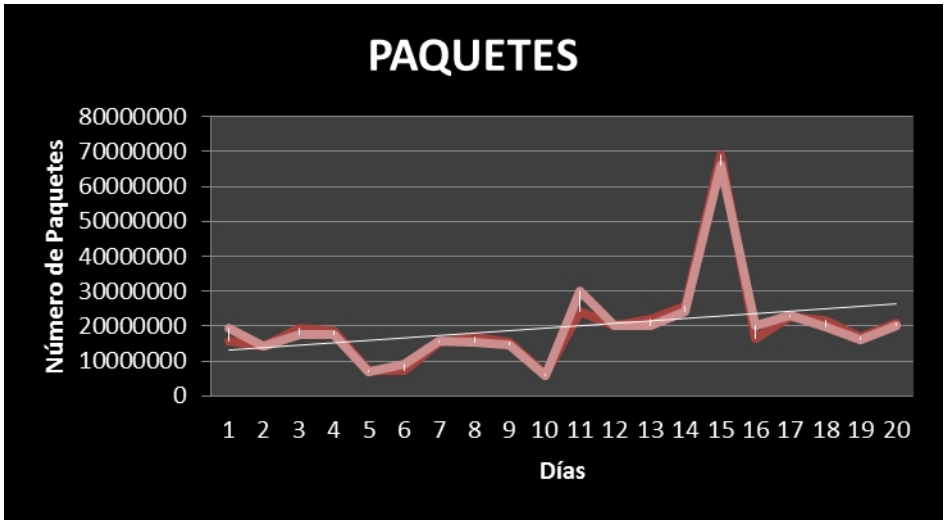
2.- DESESTACIONALIZAR EL ÍNDICE ESTACIONAL DE LA SERIE DE TIEMPO DEL PROBLEMA

Para desestacionalizar una serie de tiempo se debe dividir el Valor Observado (Xt) entre el Índice Estacional (It) correspondiente observado en proporción. En la tabla

siguiente se muestran los cálculos correspondientes para la desestacionalización de los datos del ejemplo.

Semanas	Días	# Paquetes Xt	It	Datos Desestacionalizados (Dt = Xt / It)
1	I	15668993	0,81	19379979,44
	II	14148189	0,99	14263595,71
	III	19344600	1,09	17688817,11
	IV	18576358	1,06	17513801,96
	V	7323592	1,05	7006205,74
2	I	7282196	0,81	9006884,41
	II	15490776	0,99	15617134,18
	III	16685834	1,09	15257625,69
	IV	15361278	1,06	14482622,52
	V	6055838	1,05	5793393,05
3	I	24192779	0,81	29922507,43
	II	20084827	0,99	20248658,84
	III	21997715	1,09	20114841,22
	IV	25709636	1,06	24239060,93
	V	69116523	1,05	66121184,83
4	I	16390772	0,81	20272701,91
	II	22803010	0,99	22989014,04
	III	21532311	1,09	19689273,04
	IV	16877982	1,06	15912572,01
	V	20950006	1,05	20042084,86

En la siguiente gráfica comparativa se muestran los datos originales con respecto a los datos desestacionalizados.



Al analizar los datos desestacionalizados es más fácil observar la tendencia creciente que han seguido las cargas de tráfico en la red de datos. Por esta razón, son los datos desestacionalizados los que se utilizan para realizar el paso siguiente del procedimiento.

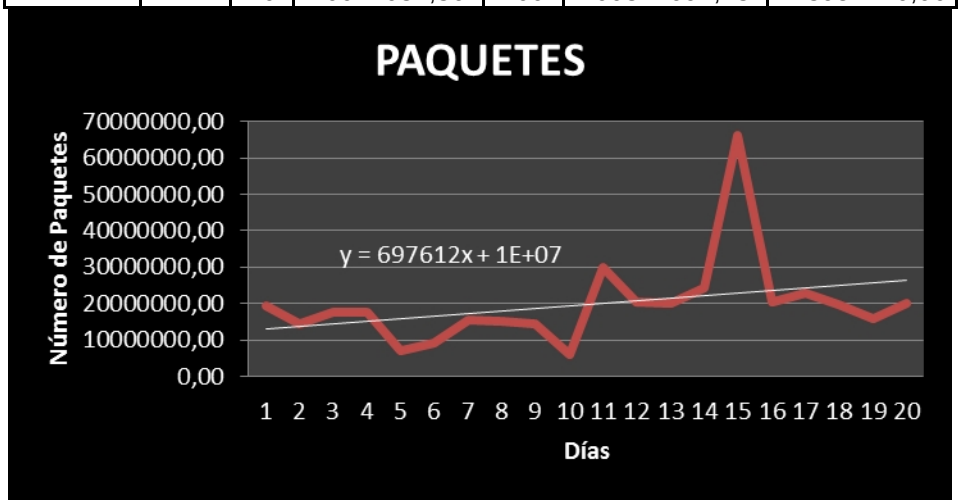
3.- CÁLCULO DE LA TENDENCIA DE LOS DATOS DESESTACIONALIZADOS

Este paso consiste en encontrar la ecuación de la línea recta a los datos desestacionalizados con el período (t). A la ecuación de la línea recta encontrada se le llama Tt, debido a que está ecuación representa la tendencia que siguen a través del tiempo.

Para el cálculo de Tt se debe seguir el procedimiento que se presenta en la siguiente tabla, por si se desea verificar la obtención de la ecuación, que en este caso toma la forma: Tt = 1E+07 + 697612(t).

Semana	Días	t	Dt	T^2	Dt x t	Tt
1	I	1	19379979,44	1	19379979,44	10697612,00
	II	2	14263595,71	4	28527191,42	11395224,00
	III	3	17688817,11	9	53066451,34	12092836,00
	IV	4	17513801,96	16	70055207,85	12790448,00
	V	5	7006205,74	25	35031028,71	13488060,00
2	I	6	9006884,41	36	54041306,45	14185672,00
	II	7	15617134,18	49	109319939,29	14883284,00
	III	8	15257625,69	64	122061005,56	15580896,00
	IV	9	14482622,52	81	130343602,72	16278508,00
	V	10	5793393,05	100	57933930,46	16976120,00
3	I	11	29922507,43	121	329147581,78	17673732,00
	II	12	20248658,84	144	242983906,03	18371344,00
	III	13	20114841,22	169	261492935,92	19068956,00
	IV	14	24239060,93	196	339346853,04	19766568,00
	V	15	66121184,83	225	991817772,48	20464180,00
4	I	16	20272701,91	256	324363230,56	21161792,00

	II	17	22989014,04	289	390813238,71	21859404,00
	III	18	19689273,04	324	354406914,78	22557016,00
	IV	19	15912572,01	361	302338868,11	23254628,00
	V	20	20042084,86	400	400841697,13	23952240,00



Con la ecuación encontrada determinamos los valores de la última columna de la tabla, los cuales representan las estimaciones de los datos desestacionalizados. Estas estimaciones son importantes para el paso siguiente.

4.- ELIMINAR LA TENDENCIA DE LA SERIE DE TIEMPO DESESTACIONALIZADA

Esta eliminación se hace a partir de los datos desestacionalizados, lo cual se logra al dividir los datos desestacionalizados (Dt) entre el valor de la tendencia (Tt). Con esto se logra estimar un índice de los componentes cíclico y azaroso de la serie de tiempo.

Los cálculos y los resultados de este paso se presentan en la tabla siguiente:

Semana	Días	Dt	Tt	Dt/Tt = (Ct x Et)
1	I	19379979,44	10697612,00	1,811617344
	II	14263595,71	11395224,00	1,25171701
	III	17688817,11	12092836,00	1,462751758
	IV	17513801,96	12790448,00	1,369287609
	V	7006205,74	13488060,00	0,519437617
2	I	9006884,41	14185672,00	0,634928286
	II	15617134,18	14883284,00	1,049307007

	III	15257625,69	15580896,00	0,979252136
	IV	14482622,52	16278508,00	0,889677514
	V	5793393,05	16976120,00	0,341267206
3	I	29922507,43	17673732,00	1,693049744
	II	20248658,84	18371344,00	1,102187126
	III	20114841,22	19068956,00	1,054847535
	IV	24239060,93	19766568,00	1,226265527
	V	66121184,83	20464180,00	3,231069353
4	I	20272701,91	21161792,00	0,957986068
	II	22989014,04	21859404,00	1,051676159
	III	19689273,04	22557016,00	0,872866918
	IV	15912572,01	23254628,00	0,684275492
	v	20042084,86	23952240,00	0,836752006

A partir de los datos (Ct Et) anteriores, al igual que en los índices estacionales, se debe determinar un representativo de cada período. Para ello:

A.- Obtener un índice promedio semanal

En este caso:	**SEMANAL**					
	I	**II**	**III**	**IV**	**V**	
	1,811617344	1,25171701	1,462751758	1,369287609	0,51943762	
	0,634928286	1,049307007	0,979252136	0,889677514	0,34126721	
	1,693049744	1,102187126	1,054847535	1,226265527	3,23106935	
	0,957986068	1,051676159	0,872866918	0,684275492	0,83675201	Sum.Prom.:
Promedio	**1,27439536**	**1,113721825**	**1,092429587**	**1,042376535**	**1,23213155**	5,75505485

B.- Normalizar los índices promedios obtenidos

FN = (5) / SUMA DE LOS PROMEDIOS

FN = 0,86880145

Multiplicando los índices promedio de cada período por el Factor de Normalización se obtiene:

(Ct Et)I = 1,107196537

(Ct Et)II = 0,967603136

(Ct Et)III = 0,949104409

(Ct Et)IV= 0,905618245

(Ct Et) V= 1,070477673

5.- OBTENCIÓN DE LOS PRONÓSTICOS DESEADOS

Este es el último paso y el más sencillo. Simplemente consiste en multiplicar los índices estimados para los elementos (It), Ciclo azaroso (Ct Et) y los valores de la tendencia (Tt) correspondientes a los periodos para los que interesa un pronóstico. Es decir, utilizar el modelo multiplicativo:

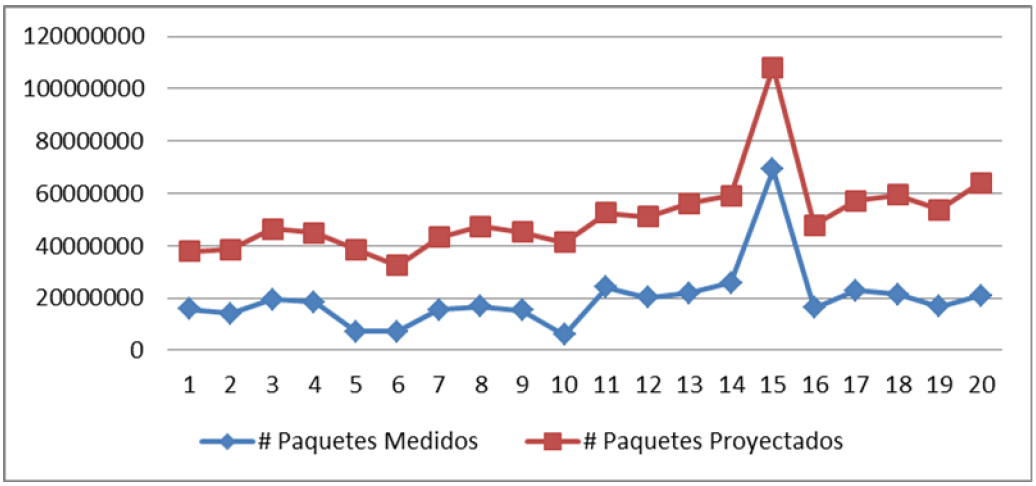
Pt = (It) (Tt) (Ct) (Et)

En la tabla siguiente se ilustra los pronósticos que se obtienen para el tráfico.

Semana	Días	Xt	It	Tt	Ct Et	Pt
1	I	15668993	0,81	10697612,00	1,107196537	9576335,11
	II	14148189	0,99	11395224,00	0,967603136	10936842,71
	III	19344600	1,09	12092836,00	0,949104409	12551716,35
	IV	18576358	1,06	12790448,00	0,905618245	12286015,46
	V	7323592	1,05	13488060,00	1,070477673	15092749,29
2	I	7282196	0,81	14185672,00	1,107196537	12698791,93
	II	15490776	0,99	14883284,00	0,967603136	14284592,92
	III	16685834	1,09	15580896,00	0,949104409	16172135,88
	IV	15361278	1,06	16278508,00	0,905618245	15636512,57
	V	6055838	1,05	16976120,00	1,070477673	18995787,61
3	I	24192779	0,81	17673732,00	1,107196537	15821248,74
	II	20084827	0,99	18371344,00	0,967603136	17632343,14
	III	21997715	1,09	19068956,00	0,949104409	19792555,42
	IV	25709636	1,06	19766568,00	0,905618245	18987009,68
	V	69116523	1,05	20464180,00	1,070477673	22898825,94
4	I	16390772	0,81	21161792,00	1,107196537	18943705,55
	II	22803010	0,99	21859404,00	0,967603136	20980093,35
	III	21532311	1,09	22557016,00	0,949104409	23412974,96
	IV	16877982	1,06	23254628,00	0,905618245	22337506,79
	V	20950006	1,05	23952240,00	1,070477673	26801864,26
5	**I**		0,81	24649852,00	1,107196537	22066162,36
	II		0,99	25347464,00	0,967603136	24327843,57
	III		1,09	26045076,00	0,949104409	27033394,49

	IV		1,09	26742688,00	0,905618245	26485683,40
	V		1,06	27440300,00	1,070477673	31156352,32

La gráfica siguiente ilustra una comparación gráfica de los pronósticos y los valores reales del ejemplo:



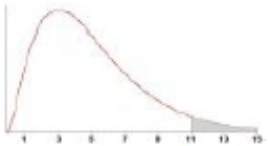
Como puede observarse, debido a que el patrón de la serie de tiempo es muy estable, los pronósticos obtenidos para los periodos en los que se conocen los datos reales, son muy similares.

ANEXO 6

TABLA DE ANOVA

Cátedra: Probabilidad y Estadística
Facultad Regional Mendoza
UTN

Tabla D.9: VALORES CRÍTICOS DE LA DISTRIBUCIÓN F (0,05)



área a la derecha del valor crítico = 0,05

Grados de libertad del Numerador

Grados de libertad del Denominador g.d.l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	g.d.l
1	161,4	199,5	215,7	224,6	230,2	234,0	236,8	238,9	240,5	241,9	243,0	243,9	244,7	245,4	245,9	1
2	18,513	19,000	19,164	19,247	19,296	19,330	19,353	19,371	19,385	19,396	19,405	19,413	19,419	19,424	19,429	2
3	10,128	9,552	9,277	9,117	9,013	8,941	8,887	8,845	8,812	8,786	8,763	8,745	8,729	8,715	8,703	3
4	7,709	6,944	6,591	6,388	6,256	6,163	6,094	6,041	5,999	5,964	5,936	5,912	5,891	5,873	5,858	4
5	6,608	5,786	5,409	5,192	5,050	4,950	4,876	4,818	4,772	4,735	4,704	4,678	4,655	4,636	4,619	5
6	5,987	5,143	4,757	4,534	4,387	4,284	4,207	4,147	4,099	4,060	4,027	4,000	3,976	3,956	3,938	6
7	5,591	4,737	4,347	4,120	3,972	3,866	3,787	3,726	3,677	3,637	3,603	3,575	3,550	3,529	3,511	7
8	5,318	4,459	4,066	3,838	3,687	3,581	3,500	3,438	3,388	3,347	3,313	3,284	3,259	3,237	3,218	8
9	5,117	4,256	3,863	3,633	3,482	3,374	3,293	3,230	3,179	3,137	3,102	3,073	3,048	3,025	3,006	9
10	4,965	4,103	3,708	3,478	3,326	3,217	3,135	3,072	3,020	2,978	2,943	2,913	2,887	2,865	2,845	10
11	4,844	3,982	3,587	3,357	3,204	3,095	3,012	2,948	2,896	2,854	2,818	2,788	2,761	2,739	2,719	11
12	4,747	3,885	3,490	3,259	3,106	2,996	2,913	2,849	2,796	2,753	2,717	2,687	2,660	2,637	2,617	12
13	4,667	3,806	3,411	3,179	3,025	2,915	2,832	2,767	2,714	2,671	2,635	2,604	2,577	2,554	2,533	13
14	4,600	3,739	3,344	3,112	2,958	2,848	2,764	2,699	2,646	2,602	2,565	2,534	2,507	2,484	2,463	14
15	4,543	3,682	3,287	3,056	2,901	2,790	2,707	2,641	2,588	2,544	2,507	2,475	2,448	2,424	2,403	15
16	4,494	3,634	3,239	3,007	2,852	2,741	2,657	2,591	2,538	2,494	2,456	2,425	2,397	2,373	2,352	16
17	4,451	3,592	3,197	2,965	2,810	2,699	2,614	2,548	2,494	2,450	2,413	2,381	2,353	2,329	2,308	17
18	4,414	3,555	3,160	2,928	2,773	2,661	2,577	2,510	2,456	2,412	2,374	2,342	2,314	2,290	2,269	18
19	4,381	3,522	3,127	2,895	2,740	2,628	2,544	2,477	2,423	2,378	2,340	2,308	2,280	2,256	2,234	19
20	4,351	3,493	3,098	2,866	2,711	2,599	2,514	2,447	2,393	2,348	2,310	2,278	2,250	2,225	2,203	20
21	4,325	3,467	3,072	2,840	2,685	2,573	2,488	2,420	2,366	2,321	2,283	2,250	2,222	2,197	2,176	21
22	4,301	3,443	3,049	2,817	2,661	2,549	2,464	2,397	2,342	2,297	2,259	2,226	2,198	2,173	2,151	22
23	4,279	3,422	3,028	2,796	2,640	2,528	2,442	2,375	2,320	2,275	2,236	2,204	2,175	2,150	2,128	23
24	4,260	3,403	3,009	2,776	2,621	2,508	2,423	2,355	2,300	2,255	2,216	2,183	2,155	2,130	2,108	24
25	4,242	3,385	2,991	2,759	2,603	2,490	2,405	2,337	2,282	2,236	2,198	2,165	2,136	2,111	2,089	25
26	4,225	3,369	2,975	2,743	2,587	2,474	2,388	2,321	2,265	2,220	2,181	2,148	2,119	2,094	2,072	26
27	4,210	3,354	2,960	2,728	2,572	2,459	2,373	2,305	2,250	2,204	2,166	2,132	2,103	2,078	2,056	27
28	4,196	3,340	2,947	2,714	2,558	2,445	2,359	2,291	2,236	2,190	2,151	2,118	2,089	2,064	2,041	28
29	4,183	3,328	2,934	2,701	2,545	2,432	2,346	2,278	2,223	2,177	2,138	2,104	2,075	2,050	2,027	29
30	4,171	3,316	2,922	2,690	2,534	2,421	2,334	2,266	2,211	2,165	2,126	2,092	2,063	2,037	2,015	30
31	4,160	3,305	2,911	2,679	2,523	2,409	2,323	2,255	2,199	2,153	2,114	2,080	2,051	2,026	2,003	31
32	4,149	3,295	2,901	2,668	2,512	2,399	2,313	2,244	2,189	2,142	2,103	2,070	2,040	2,015	1,992	32
33	4,139	3,285	2,892	2,659	2,503	2,389	2,303	2,235	2,179	2,133	2,093	2,060	2,030	2,004	1,982	33
34	4,130	3,276	2,883	2,650	2,494	2,380	2,294	2,225	2,170	2,123	2,084	2,050	2,021	1,995	1,972	34
35	4,121	3,267	2,874	2,641	2,485	2,372	2,285	2,217	2,161	2,114	2,075	2,041	2,012	1,986	1,963	35
40	4,085	3,232	2,839	2,606	2,449	2,336	2,249	2,180	2,124	2,077	2,038	2,003	1,974	1,948	1,924	40
60	4,001	3,150	2,758	2,525	2,368	2,254	2,167	2,097	2,040	1,993	1,952	1,917	1,887	1,860	1,836	60