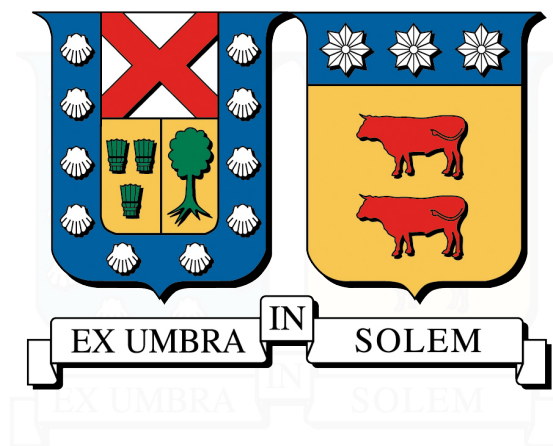


UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE ELECTRÓNICA
VALPARAÍSO - CHILE



**IMPLEMENTACIÓN DE UN SISTEMA ADMINISTRADOR
DE ANCHO DE BANDA EN LA RED INSTITUCIONAL DE
LA UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN**

ALEXIS CRISTÓBAL GAETE OLIVARES

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL TELEMÁTICO

PROFESOR GUÍA : WERNER CREIXELL FUENTES
PROFESOR CORREFERENTE : ALEJANDRA BEGUELLI ZAPATA

ENERO - 2014

Contenido

Índice de Ilustraciones.	4
Capítulo 1: Introducción.....	6
1.3. Administración del ancho de banda.....	9
1.4. Contribución de este trabajo de título	11
Capítulo 2: Red de la UTFSM	12
2.1. Administración del ancho de banda en la UTFSM	15
Capítulo 3: Propuesta de nueva administración de ancho de banda y políticas de calidad de servicio	24
Capítulo 4: Administrador de ancho de banda <i>ALLOT</i>	27
4.1. <i>Capa de Hardware: NetEnforcer AC-3000</i>	27
Descripción de los LED del panel frontal.....	27
Conectores del panel frontal:.....	28
Unidad <i>Bypass</i> :	28
4.2. <i>NetExplorer</i>	29
4.2.1 Términos y conceptos del <i>NetXplorer</i>	30
Catálogo	31
Línea	31
Tubería	32
Canal virtual.....	32
4.2.2 Interfaz de usuario	33
4.2.3 Catálogos	35
4.2.4 Definición de políticas de calidad de servicio	36
4.2.5 Asignación de ancho de banda y priorización de tráfico	40
Capítulo 5: Implementación del administrador de ancho de banda <i>ALLOT</i>	46
5.1. Instalación de NetEnforcer.....	46
5.1. Configuración de políticas de QoS	50
5.1.1 Líneas.....	50
5.1.2 Tuberías.....	52
5.1.3 Canales virtuales	56
5.1.4 Políticas ante ataques <i>DoS</i>	57

Capítulo 6: Resultados y gráficos	60
6.1. Tráfico interno.....	60
6.1.1 Análisis entre los meses de mayo a agosto del 2013	60
6.2 Tráfico nacional	63
6.2.1 Análisis entre los meses de mayo a agosto del 2013	63
6.3 Tráfico Internet2	65
6.3.2 Análisis entre los meses de mayo a agosto del 2013	65
6.4 Tráfico Internacional	67
6.4.1 Análisis diario	67
6.4.2 Análisis entre los meses de mayo a agosto del 2013	69
6.5 Tráfico de redes WiFi.....	72
6.6 Reglas de DoS.	74
Capítulo 7: Conclusiones	75
Referencias	77

Índice de Ilustraciones.

Ilustración 1: Red institucional UTFSM	13
Ilustración 2: Diagrama resumido de conexiones de todas las sedes de la universidad hacia internet.....	15
Ilustración 3: Regla de ancho de banda para pregrado de electrónica.	18
Ilustración 4: Regla de ancho de banda para la red de profesores de electrónica limitada a 7 Mbps.	18
Ilustración 5: Regla de ancho de banda para la red de informática limitada a 16 Mbps.....	18
Ilustración 6: Regla de ancho de banda para la sede de Viña del Mar limitada a 21 Mbps.	19
Ilustración 7: Regla de ancho de banda para la red de servidores públicos limitada a 15 Mbps.	19
Ilustración 8: Regla de ancho de banda para la red Wifi institucional limitada a 40 Mbps.....	19
Ilustración 9: Vista frontal del <i>NetEnforcer AC-3000</i> , extraída del manual de usuario.	27
Ilustración 10: Unidad Bypass	28
Ilustración 11: Conexión entre <i>NetEnforcer</i> y unidad <i>Bypass</i>	29
Ilustración 12: Resumen jerárquico en el <i>NetXplorer</i>	31
Ilustración 13: Acceso de administración del <i>NetXplorer</i>	33
Ilustración 14: Componentes de la interfaz de usuario del <i>NetXplorer</i>	34
Ilustración 15: Relación entre línea, tubería, canal virtual y condiciones.....	36
Ilustración 16: Proceso de asignación de recursos.	37
Ilustración 17: Proceso de creación de políticas.	39
Ilustración 18: Editor del catálogo de <i>QoS</i>	40
Ilustración 19: Ejemplo 1 de asignación de ancho de banda.	42
Ilustración 20: Ejemplo 2 de asignación de ancho de banda.	43
Ilustración 21: Ejemplo 3 de asignación de ancho de banda.	44
Ilustración 22: Diagrama de red con la instalación del equipo <i>ALLOT</i>	47
Ilustración 23: Líneas creadas en el <i>NetXplorer</i>	51
Ilustración 24: Regla de <i>QoS</i> para el tráfico nacional.....	51
Ilustración 25: Regla de <i>QoS</i> para el tráfico internacional.	52
Ilustración 26: Tuberías creadas en la línea de tráfico nacional.	55
Ilustración 27: Tuberías creadas en la línea de tráfico internacional.	55
Ilustración 28: Canales virtuales creados dentro de cada tubería.	56
Ilustración 29: Regla creada para el principal servidor web de la Universidad.	58
Ilustración 30: Configuración de la regla de <i>DoS</i>	58
Ilustración 31: Tráfico interno durante los meses de mayo a agosto del 2013.	61
Ilustración 32: Protocolos del tráfico interno durante los meses de mayo a junio del 2013.	62
Ilustración 33: Tráfico nacional entre los meses de mayo a agosto del 2013.	63
Ilustración 34: Protocolos del tráfico nacional durante los meses de mayo y agosto del 2013.	64
Ilustración 35: tráfico hacia redes académicas entre los meses de mayo a agosto del 2013.	65
Ilustración 36: Protocolos traficando hacia redes académicas entre los meses de mayo a agosto del 2013.....	66

Ilustración 37: Tráfico internacional entre los días 20 a 26 de agosto del 2013.....	67
Ilustración 38: Análisis diario de protocolos traficando datos internacionalmente.....	68
Ilustración 39: Tráfico internacional entre los meses de mayo y agosto del 2013.....	69
Ilustración 40: Tráfico internacional durante los días 25, 26, 28 de noviembre y 2 de diciembre del 2013.....	70
Ilustración 41: Conexiones descartadas en la línea de tráfico internacional.....	71
Ilustración 42: Protocolos traficando hacia redes internacionales entre los meses de mayo a agosto del 2013.....	72
Ilustración 43: Tráfico cursado por redes inalámbricas el día 2 y 5 de diciembre del 2013.....	73
Ilustración 44: Conexiones descartadas para las redes inalámbricas el día 5 de diciembre del 2013.	73
Ilustración 45: Conexiones descartadas debido a ataques <i>DoS</i> durante el mes de abril del 2013...	74

Capítulo 1: Introducción

En el área de conectividad y redes de datos, se define al ancho de banda como la cantidad de datos que pueden ser transmitidos por una conexión de red durante un tiempo determinado [1]. Generalmente se mide bits (unidad mínima de información) por segundo o múltiplos de ellos (Kilo, Mega, Giga, Tera o Peta bits por segundo). El ancho de banda se utiliza para representar la capacidad de transmisión disponible o utilizada de un sistema de comunicación, tal como una red de computadores.

Debido a las restricciones en la capacidad física de los enlaces y dispositivos presentes en una red de datos, el ancho de banda resulta ser un recurso limitado y por lo tanto, costoso. Por ello, las organizaciones deben asegurarse de contratar una cantidad adecuada de este recurso para poder desarrollar a diario las actividades que utilizan la red de la institución, especialmente la conexión hacia Internet, que se ha convertido en un componente crítico en el éxito de investigadores, profesores y estudiantes en los sistemas de educación superior, especialmente en universidades [2].

Teniendo en cuenta el crecimiento exponencial que han tenido los contenidos digitales disponibles en Internet en los últimos años, los usuarios perciben que el ancho de banda disponible no es suficiente para satisfacer sus necesidades. Sin embargo, en muchas ocasiones la realidad es que el problema reside en la utilización ineficiente de este recurso.

La principal razón detrás de la utilización ineficiente del ancho de banda radica en la incapacidad (por parte del administrador de la red) para identificar aquellas aplicaciones improductivas (por ejemplo, redes sociales, Youtube, *streaming*, prensa digital, etc.) que consumen una gran cantidad de recursos disponibles en la red. La utilización de recursos por parte de aplicaciones improductivas es uno de los efectos que se obtienen de la mala administración del ancho de banda contratado por una institución como una universidad, en donde se vive una desagradable y frustrante experiencia de congestión en la red provocada por una inundación de tráfico IP [3].

Es un deber de los departamentos de tecnologías de la información de las distintas organizaciones el utilizar el ancho de banda de la mejor forma posible. Para ello no solo se debe limitar el uso abusivo de ciertos usuarios sobre este recurso, sino también se debe dar acceso a la mayor cantidad de usuarios que sea posible para maximizar la utilización de este, ya que el ancho de banda que no se utiliza es equivalente a una pérdida de dinero [2].

Para dar acceso a Internet a los usuarios se requiere una cadena de entrega de información consistente en cuatro enlaces fundamentales [4]:

1. Contenido: El contenido debe ser accesible para el usuario. El lenguaje y la información relevante son importantes, pero un factor más importante aún es el formato. Si los usuarios poseen un pequeño ancho de banda disponible, el contenido debe estar en un formato que sea rápidamente accesible.
2. Conectividad: Es necesario proveer al usuario con una conexión para acceder al contenido.
3. Recursos locales: La institución debe poseer los recursos necesarios para entregar el contenido al usuario. Estos recursos incluyen la red local, computadores, herramientas y las habilidades técnicas del equipo de administración de red.
4. Administración del ancho de banda: Sin una administración proactiva, la capacidad de la red se ve afectada por virus y tráfico inapropiado, los problemas no pueden ser diagnosticados y las conexiones se vuelven inefectivas.

Los administradores de red de las instituciones deben preocuparse de utilizar de manera correcta el ancho de banda disponible y asegurarse que este sea utilizado en aquellos servicios que la institución determine importantes para su misión. En este sentido, la administración de red se vuelve esencial para poder entregar un servicio que satisfaga las necesidades de los usuarios.

La administración de red se define como el control, planificación, adquisición, distribución, desarrollo, coordinación y monitoreo de los recursos de la red. Dentro de estos recursos se encuentra el ancho de banda contratado por la institución.

1.2. La necesidad de administrar el ancho de banda

Mientras más grande sea el ancho de banda, mayor es la velocidad de la conexión, lo que implica que la carga y/o descarga de contenidos sea más rápida. Existen distintos tipos de conexiones a Internet que utilizan diferentes velocidades. Por ejemplo, la antigua conexión por línea conmutada (*Dial-up* en inglés) alcanzaba una velocidad de 56 Kbps. Hoy en día esta velocidad es demasiado baja para el contenido que se encuentra disponible en internet, que no solo crece de forma exponencial sino que cada vez consume más ancho de banda. Por ejemplo, aplicaciones como el aprendizaje electrónico o sala de clases virtuales requieren una gran cantidad de ancho de banda, alrededor de 3 Mbps, debido a que el principal tráfico que se cursa en estas aplicaciones corresponde a voz y video en forma simultánea. La mayoría de las conexiones actuales superan fácilmente los 2 Mbps.

Para atender los requerimientos de ancho de banda de este tipo de aplicaciones, en muchas ocasiones se recurre a un aumento del ancho de banda contratado. Este es un proceso complejo que consume gran cantidad de tiempo administrativo. El proceso se inicia con la planificación del ancho de banda necesario para satisfacer las necesidades de los usuarios hasta conseguir los

permisos de las unidades correspondientes para realizar los cambios. Si bien esta estrategia es muchas veces necesaria, no es suficiente por sí sola.

Por una parte, al experimentar una mejor experiencia de navegación (debido al mayor ancho de banda) y no tener restricciones de uso, existe una tendencia a generar flujos no productivos (por ejemplo, *streaming* de alta definición, descargas vía P2P, juegos en línea , etc.) que saturan rápidamente la nueva capacidad de ancho de banda. Como resultado, se dificulta el normal desenvolvimiento de las actividades que sí están alineadas con los objetivos de la organización.

En la medida que se aumente el ancho de banda total de la institución, se disminuye el ancho de banda requerido por cada usuario. Esta situación se puede explicar por dos razones.

- Mientras más grande sea el ancho de banda disponible, menor es la necesidad que el usuario tiene de este recurso ya que sus requerimientos pueden ser atendidos de forma más rápida. Como resultado, deja el resto de los recursos disponibles para otros usuarios. Adicionalmente, disminuye significativamente el ancho de banda utilizado en procesos no productivos tales como la retransmisión de paquetes que se produce al no poder atender un requerimiento.
- No todos los usuarios conectados utilizan ancho de banda al mismo tiempo ya que mientras crean conexiones a páginas *web*, también están leyéndolas.

De lo anterior se concluye que aumentar el ancho de banda es una buena opción para satisfacer las necesidades de los usuarios de la red, pero al no administrar el ancho de banda, los usuarios volverán a consumir todos los recursos disponibles y no se puede asegurar que se están utilizando para aquellos fines que la universidad estima correctos.

Aumentar el ancho de banda contratado al proveedor de Internet solo provoca aumentar los gastos por parte de la universidad sin solucionar el problema de fondo, que es repartir eficientemente los recursos de ancho de banda a los usuarios de la red de la institución.

En vez de simplemente aumentar el ancho de banda contratado, la velocidad de una conexión a Internet puede mejorarse significativamente mediante la aplicación de mecanismos de monitoreo y de control. El monitoreo permite detectar la existencia de flujos de tráfico indeseados (no alineados con los objetivos de la institución) que consumen ancho de banda y dificultan la ejecución de las aplicaciones que son necesarias para el desarrollo de la misión de la organización ya que no tienen ancho de banda disponible. El control consiste en remover aquellos flujos indeseados de la red para que el ancho de banda disponible sea efectivamente usado en actividades alineadas con la misión de la organización. La combinación de los mecanismos de monitoreo y control de las conexiones de la red se conoce como administración del ancho de banda. La administración del ancho de banda es una actividad clave del área de Tecnologías de la Información de cualquier institución ya que permite el uso eficiente de un recurso crítico como es el ancho de banda.

1.3. Administración del ancho de banda

El objetivo de administrar el ancho de banda es tener la cantidad correcta de este recurso en el lugar y momento requeridos para un grupo específico de usuarios y aplicaciones.

La principal función del administrador de ancho de banda es catalogar el tráfico saliente de la red en varias clases, de acuerdo al servicio y tipos de aplicaciones que cursan información por la red. Cada clase de tráfico debe luego ser planificada de acuerdo a cantidades máximas y mínimas de ancho de banda que requerirá. Para lograr esto, el administrador requiere llevar a cabo 3 actividades: monitoreo, creación de políticas, e implementación [2].

Monitoreo: el monitoreo es necesario para diagnosticar fallas o problemas dentro de la red. Es importante para la definición de políticas y su posterior implementación ya que entrega información detallada y en tiempo real del tráfico circulando por la red. En base a los datos entregados por este monitoreo, es posible conocer el tráfico real de los usuarios, identificando el consumo de ancho de banda que consumen en distintas aplicaciones. Conociendo estos datos es posible crear políticas que se adapten a la real situación de la institución.

Políticas: Si la institución no posee un manual de *“Políticas de uso aceptable de internet”* no existiría una cantidad de ancho de banda suficiente para satisfacer las necesidades de los usuarios usuario, ya que estos no tienen restricciones. Por ejemplo, la descarga de música y otros archivos para el uso personal puede utilizar todo el ancho de banda de una institución. Este acto es frecuente, en donde pequeños grupos de usuarios suelen consumir una gran cantidad de ancho de banda. Las políticas de las instituciones deben ser conocidas y se deben hacer cumplir dentro de esta. Esto se convierte en tarea del administrador, el cual debe identificar aquellos usuarios que no se adhieren a las políticas y darles una sanción.

Implementación: Existen diversas herramientas y técnicas que ayudan al administrador de red a asegurarse que el ancho de banda es administrado de manera correcta y que las políticas se están cumpliendo. Algunos de los componentes claves de una implementación son:

- Analizadores de tráfico, para monitorear el estado de utilización de la red, la actividad de cada usuario y detectar cuellos de botella.
- Cortafuegos, para bloquear tráfico malicioso y no deseado
- Anti virus, para proteger la red de *software* malicioso
- *Cachés*, para utilizar eficientemente el ancho de banda
- *Traffic Shapers*, para priorizar y controlar el consumo de ancho de banda de los usuarios a través de reglas que limitan la velocidad de transferencia
- Cuotas de sistema, para administrar el tráfico de los usuarios asignándoles una cantidad limitada de datos a traficar.

Es importante destacar que el proceso de administración del ancho de banda no es una tarea de una sola vez, sino es un ciclo continuo en donde se debe monitorear constantemente el tráfico de la red e implementar soluciones en base a políticas de uso.

Podemos tomar como referencia las siguientes directrices para crear políticas (sugeridas por el software de seguridad informática “Elron” [5]):

1. Inicialmente el sistema debe generar de forma detallada y comprensible gráficos, reportes y tablas de los niveles de consumo de ancho de banda en la red. Estos datos proveen una importante fuente del uso del servicio de internet.
2. Luego de obtener los datos de cómo se está utilizando el ancho de banda dentro de la institución se debe crear la “Política de uso aceptable de recursos computacionales”, la cual se aplicará implementando ciertas soluciones técnicas y administrativas. Esta política consiste en un número de reglas que definen cuánto ancho de banda es asignado y priorizado para el tráfico de individuos, grupos y tipos de aplicaciones.
3. El sistema debe ser lo suficientemente sofisticado para reaccionar dinámicamente a cambios en las condiciones de la red, tales como permitir al tráfico de baja prioridad aumentar su consumo si hay ancho de banda que no está siendo utilizado.
4. Una vez que las políticas de ancho de banda han sido implementadas, es necesario seguir capturando datos sobre el estado de la red, especialmente estadísticas de consumo para poder monitorear la efectividad de las políticas. Es importante que existan alertas automáticas cuando una regla de calidad de servicio se ve sobrepasada en tráfico.
5. Finalmente y por sobre todas las anteriores, el sistema administrador de ancho de banda debe ser simple de administrar y operar, pero lo bastante sofisticado para que provea un control total del ancho de banda según los requerimientos propios de la institución en donde se está implementando.

1.4. Contribución de este trabajo de título

En la presente memoria se reporta la implementación de un servicio de administración de ancho de banda para la red de la Universidad Técnica Federico Santa María. Esta implementación tiene por objetivo mejorar la calidad de los servicios de red entregados por la Universidad a sus usuarios. Para ello se implementarán políticas de calidad de servicio (*QoS*, por sus siglas en inglés) que permitan aprovechar de manera eficiente el recurso del ancho de banda.

El resto de esta memoria se estructura de la siguiente manera: en el capítulo 2 describe la configuración de la red de datos de la Universidad Técnica Federico Santa María y cómo se administraba el ancho de banda en la institución; en el Capítulo 3 se propone un nuevo sistema de administración de ancho de banda así como las nuevas políticas de calidad de servicio. El capítulo 4 trata sobre las características que posee el administrador de ancho de banda *ALLOT* y luego en el capítulo 5 se describe cómo este equipo fue configurado y utilizado para mejorar la eficiencia en la administración del ancho de banda de la universidad. En el capítulo 6 se muestran los resultados de rendimiento de la red una vez que el nuevo administrador fue puesto en marcha. Finalmente, el capítulo 7 concluye la presente memoria.

Capítulo 2: Red de la UTFSM

La red corporativa de la universidad se puede separar en 6 grandes áreas:

- Núcleo de red o *Core*:
 - En el núcleo de la red se encuentran interconectadas todas las redes internas, tanto de casa central como de las sedes. Dentro de este equipo están definidas más de 100 *Vlans* [6]. Estos equipos corresponden físicamente a 3 Switch Cisco 3750 de 24 puertos 1000Base-T[7] más 4 puertos SFP[8].
 - El cortafuegos principal también forma parte del núcleo de la red, en este equipo se implementan las reglas de acceso desde y hacia la red de la universidad
- Red de servidores
 - En la red *DMZ* [11] se encuentran alojados los servidores públicos de la universidad.
- Red WiFi
 - Las redes WiFi[12] están concentradas en dos sistemas diferentes, uno bajo plataforma Cisco y la otra bajo PfSense[13].
- Red administrativa
 - La red administrativa está compuesta por todas aquellas unidades internas que poseen un alto nivel de seguridad por las tareas que ellas realizan.
- Red intercampus
 - Es la red compuesta por todos los campus y sedes comunicados con casa central.
- Internet
 - Enrutadores que conectan la red de la universidad con Internet.

A continuación se puede observar el diagrama general de red en la figura 1.

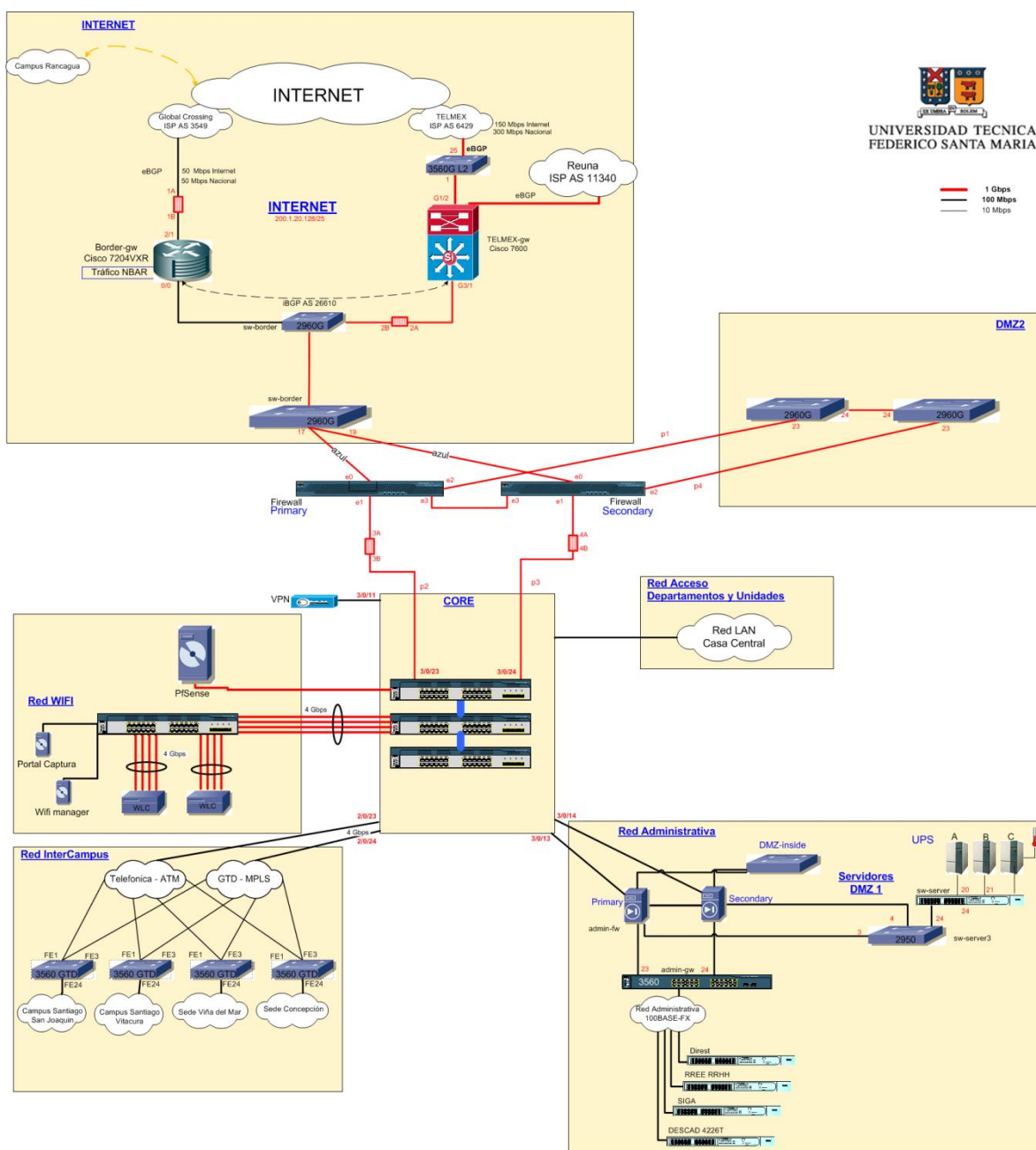


Ilustración 1: Red institucional UTFSM

El administrador de red se debe enfrentar a los usuarios que existen dentro de su institución, dentro de un campus universitario, como es este caso, nos podemos encontrar básicamente con 2 tipos de usuarios: los estudiantes y los funcionarios.

Los estudiantes, generalmente poseen más tiempo libre que los funcionarios, están menos supervisados y están bajo una menor presión de trabajo. Un campus universitario es uno de los ambientes más desafiantes para administrar, esto dado que los estudiantes tienen gran curiosidad en experimentar con la infraestructura de una red existente y los servicios ofrecidos por la institución [2].

Los usuarios de un campus universitario usan su conexión a internet de distintas maneras y generalmente no es un problema que un estudiante descargue música, juegue *on-line*, o vea un partido de fútbol vía *Streaming*, pero sí se convierte en un problema cuando el ancho de banda que consume no permite a un investigador obtener información útil para su investigación en la web [3].

Además los estudiantes están más expuestos a infectar sus equipos con virus, gusanos, *spyware*, etc. Esto debido a la gran cantidad de información que trafican, tanto descargando como compartiendo. El *p2p*, especialmente el uso de *Torrent*, es muy popular entre los estudiantes, esto dado la gran cantidad de contenidos compartidos en internet, pero es una de las aplicaciones que más ancho de banda consume dado la gran cantidad de conexiones que utiliza.

La universidad cuenta con 3 enlaces a internet, cada uno de ellos representados por una nube con el nombre del proveedor. Estos enlaces son contratados a las siguientes empresas proveedoras de internet [14]:

1. Global Crossing [15]: Este enlace fue dado de baja a principios del año 2013, pero aún sigue activo. Dicho enlace es de una capacidad de 50 Mbps de tráfico nacional y 50 Mbps de tráfico internacional. Dado que este enlace está funcionando de forma irregular, no se tomará en cuenta en los cálculos de asignación de ancho de banda, pero es importante reconocer su existencia para poder interpretar gráficos que se verán más adelante en esta memoria.
2. Claro Chile [16]: Este es el enlace primario para la conexión a internet de la universidad. Tiene una capacidad de 300 Mbps para tráfico nacional y 150 Mbps para tráfico internacional.
3. Reuna [17]: Este enlace provee a la universidad un acceso a internet comercial de tráfico nacional a una velocidad de 100 Mbps. También entrega acceso a la red académica y de investigación *Internet2*[18]. Este acceso tiene una capacidad de 1 Gbps hasta las redes de Reuna, que es en donde se encuentra en Chile la interconexión con *Internet2*.

Estos 3 enlaces son los que comunican la red institucional de la universidad hacia el exterior, sean redes nacionales, internacionales o de investigación. El tráfico proveniente de cada sede de la universidad llega hasta casa central, en donde se encuentra el núcleo de la red institucional y que también es el lugar donde se encuentran físicamente los 3 enlaces que proveen servicios de internet.

Casa central es el núcleo de la red corporativa, es en este lugar donde se encuentran físicamente los enlaces a internet y el núcleo de red. Todos los enlaces provenientes desde las distintas sedes de la universidad y departamentos de casa central se concentran en este núcleo, el cual enruta el tráfico hacia internet.

Esto se puede observar de forma resumida en la figura 2.

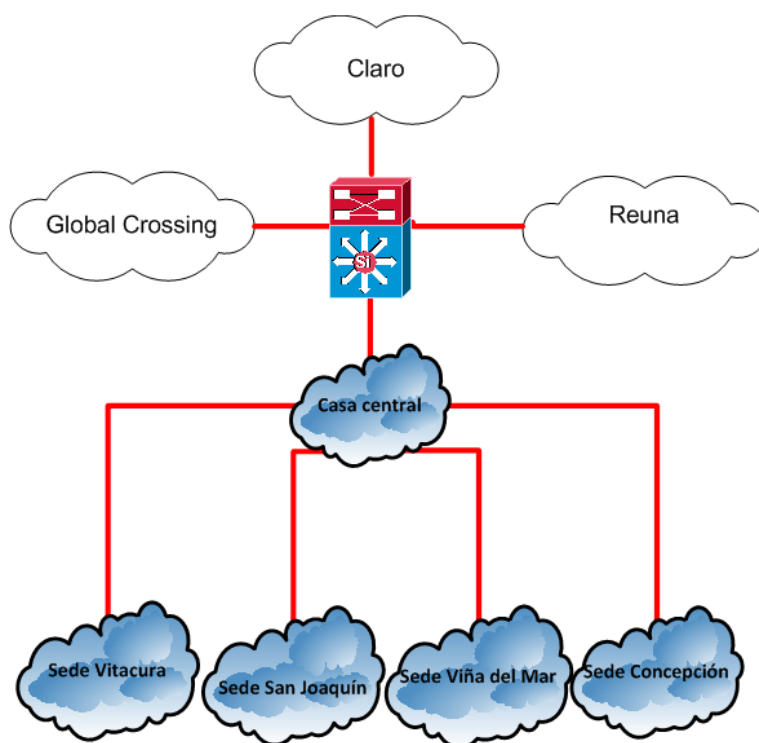


Ilustración 2: Diagrama resumido de conexiones de todas las sedes de la universidad hacia internet.

2.1. Administración del ancho de banda en la UTFSM

En esta sección se describe la manera en que se llevaba a cabo la administración del ancho de banda en la universidad, empezando por la tecnología que se utilizaba para luego conocer las distintas políticas que se implementaban en el equipo a cargo de esta labor.

El administrador de ancho de banda que se ha utilizado en la Universidad es un servidor con sistema operativo FreeBSD[19], el cual realiza catalogación y adaptación de tráfico mediante reglas creadas en su cortafuegos.

La técnica de adaptar el tráfico a algún perfil predeterminado corresponde a una técnica de administración de ancho de banda llamada *traffic shaping* [20]. Para esto, típicamente se limita el

tráfico cursado por una conexión, por ejemplo retrasando algunos paquetes[21] para darle prioridad a otros. De aquí en adelante, este servidor será referenciado en esta memoria como adaptador de tráfico.

La catalogación de tráfico permite identificar la información que se trafica en la red para tratarla de alguna manera determinada. Una forma de tratar el tráfico es limitándolo cuando se cumple alguna condición, como por ejemplo cuando se alcanza una determinada velocidad de transferencia. El tráfico que es menor o igual a una velocidad dada es transmitido, a diferencia del tráfico que es mayor, el cual es descartado o retrasado. La limitación de la velocidad es implementada a través de políticas (descartando paquetes), colas (retrasando el envío de paquetes) o control de congestión[22] (solamente por aquellos protocolos que soportan control de congestión, tal como TCP[23]).

Las reglas implementadas en el cortafuego del adaptador de tráfico, dividen lógicamente los flujos de información circulando a través de la red. Cada vez que un tráfico es catalogado, es asignado a una tubería de ancho de banda. Estas tuberías representan la segmentación lógica de un enlace físico. La capacidad de dicho enlace se puede dividir en una o más tuberías que se reparten la capacidad total del enlace, es decir, la suma del ancho de banda de todas las tuberías debe ser igual al ancho de banda del enlace físico. Las tuberías (*Pipe* en inglés) son usadas para definir la cantidad de tráfico que puede ser cursado a través de un enlace. Una forma simple de explicarlo es la siguiente.

Supongamos que tenemos una piscina, la cual posee una pequeña tubería para sacar el agua de ella. En esta situación, cuando se quiera vaciar la piscina, toda el agua que está dentro de ella saldrá por una delgada tubería, lo que implica que el flujo que pasará por ella es pequeño, por lo tanto se demorará bastante en vaciarse.

Ahora supongamos que tenemos una piscina que posee una tubería de mayor área. En este escenario, la tubería es mucho más grande que el caso anterior, por este motivo, cuando se quiera vaciar la piscina, el flujo que descargue la tubería será mayor al anterior, lo que provocará que la piscina se vacíe más rápido.

En el caso de un enlace la analogía es similar, se puede tener todo el tráfico sin catalogar de forma que no se discrimina los distintos protocolos que circulan a través de la red, esto puede provocar por ejemplo que una ráfaga de tráfico *P2P* ocupe todos los recursos disponibles, dejando sin servicio a otros requerimientos tales como tráfico web o envío de correos.

Al segmentar lógicamente el enlace a través de tuberías, se puede catalogar el tráfico y asignar recursos de acuerdo a las políticas de la institución, identificando aquellas aplicaciones permitidas y relacionarlas con una tubería determinada, por ejemplo, asociar una tubería con el tráfico web, otra con *ftp* y otra con *P2P*. De esta manera, limitando el tráfico de cada protocolo (es decir, de cada tubería) se limita el tráfico que circula por el enlace físico. Se pueden crear las tuberías que se necesiten (como por ejemplo, una por cada unidad académica), con el debido cuidado de que la

sumatoria del tráfico de cada tubería debe ser igual o menor que la capacidad del enlace para garantizar el tráfico.

Se pueden crear tuberías cuyas suma de ancho de banda sean mayores al del enlace, sabiendo que es muy poco probable que todos utilicen al máximo la capacidad de sus tuberías. Las políticas de la universidad indican que el ratio de venta nunca debe ser mayor a 1:5, es decir, que el ancho de banda total sea mayor a una quinta parte del ancho de banda total asignado. Es decir, si institución posee un enlace de 100 Mbps, a lo más podría vender un máximo de 500 Mbps. Esto es netamente un tema administrativo que deciden las autoridades de la universidad.

Por ejemplo, si queremos asegurar el máximo de tráfico en un enlace de 100 Mbps, se pueden crear 10 tuberías de 10 Mbps (o 20 de 5 Mbps o 100 de 1Mbps, etc.), ya que la suma del tráfico permitido de cada tubería es menor o igual a la capacidad del enlace. Al crear más de 10 tuberías de 10 Mbps en un enlace de 100Mbps, se superaría la capacidad máxima del enlace y no sería posible que todos transmitieran a dicha velocidad al mismo tiempo. Sin embargo, debido a la baja probabilidad de que eso ocurra, se pueden crear más tuberías dependiendo de lo que permitan las políticas de la institución en donde se está implementando el administrador de ancho de banda.

Las reglas de ancho de banda implementadas en el cortafuego del adaptador de tráfico implementan las tuberías de igual manera que una lista de acceso. Este tipo de reglas, catalogan el tráfico de una interfaz de red. Esto lo realiza recorriendo una lista de reglas de principio a fin hasta encontrar un calce entre el tráfico de la interfaz y una regla, catalogando de esta forma el tráfico. Una vez realizado este calce, se aplican las acciones definidas en la regla, las cuales generalmente permiten o deniegan tráfico.

En el caso de las reglas de ancho de banda, cada vez que llega tráfico, se lee en el encabezado del paquete el campo de la dirección origen, la cual es buscada en todas las reglas que existen en la lista de acceso. Al encontrar una regla que calce, se revisa el ancho de banda asignado a esa dirección IP y si existe ancho de banda disponible en la tubería, el paquete será enviado, en caso contrario será retrasado (almacenado en buffer) o descartado.

El adaptador de tráfico no tiene forma de saber si el tráfico analizado corresponde a redes nacionales, internacionales o de investigación. Por este motivo el equipo limita el ancho de banda total de cada tubería.

El adaptador de tráfico tiene configuradas más de 100 tuberías en sus listas de acceso, en las cuales se limita una cierta cantidad de tráfico a un rango de direcciones IP específicas. Estos rangos de direcciones IP corresponden a las distintas unidades académicas o administrativas dentro de la universidad, las cuales contratan una cierta cantidad de ancho de banda. A continuación, en la figura 3, se muestra a modo de ejemplo la regla para las direcciones IP asociadas a pregrado de electrónica.

```
# usmbw Elo_Pregrado 123 122 5
VAR="200.1.17.100,200.1.20.234"
${fwcmd} pipe 122 config bw 5000kb/s
${fwcmd} pipe 123 config bw 5000kb/s
${fwcmd} add 11220 pipe 122 ip from $VAR to any
${fwcmd} add 11230 pipe 123 ip from any to $VAR
```

Ilustración 3: Regla de ancho de banda para pregrado de electrónica.

En esta regla se observa que existen 2 tuberías, la 122 y la 123, ambas configuradas con un máximo de 5 Mbps. Estas tuberías son agregadas a las reglas número 11220 y 11230 respectivamente, y serán aplicadas a todo el tráfico IP que se genere desde las direcciones 200.1.17.100 y 200.1.20.134.

Nótese que ambas reglas son similares a excepción del orden entre el emisor y receptor. En la regla 11220 se está limitando el tráfico desde las direcciones IP de electrónica hacia cualquier otra y en la regla 11230 es desde cualquier dirección IP hacia las de electrónica. Esta es una forma para limitar el tráfico de subida y el de bajada en forma independiente.

Las Figuras 4-8 muestran el comportamiento del tráfico sometido a distintas reglas. En el eje horizontal de cada figura se muestran los días de la semana, mientras que en el eje vertical se observa el ancho de banda consumido.

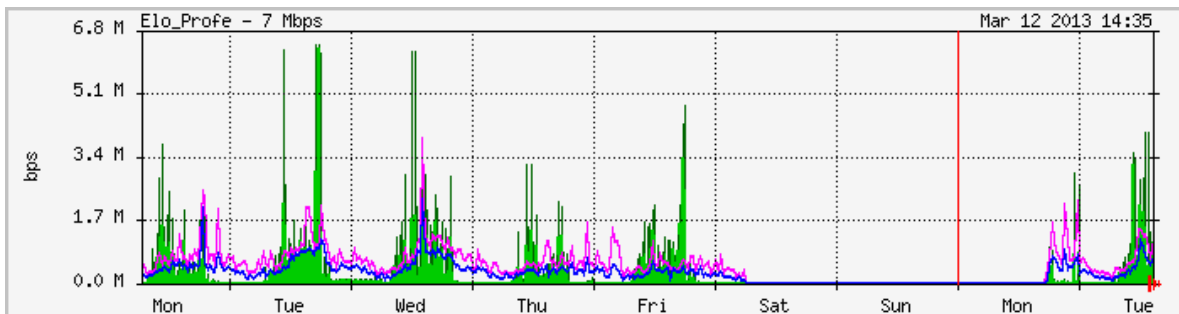


Ilustración 4: Regla de ancho de banda para la red de profesores de electrónica limitada a 7 Mbps.

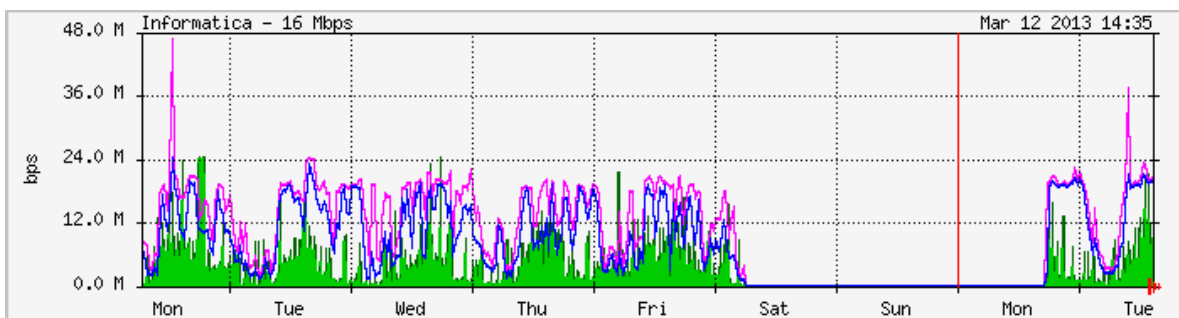


Ilustración 5: Regla de ancho de banda para la red de informática limitada a 16 Mbps.

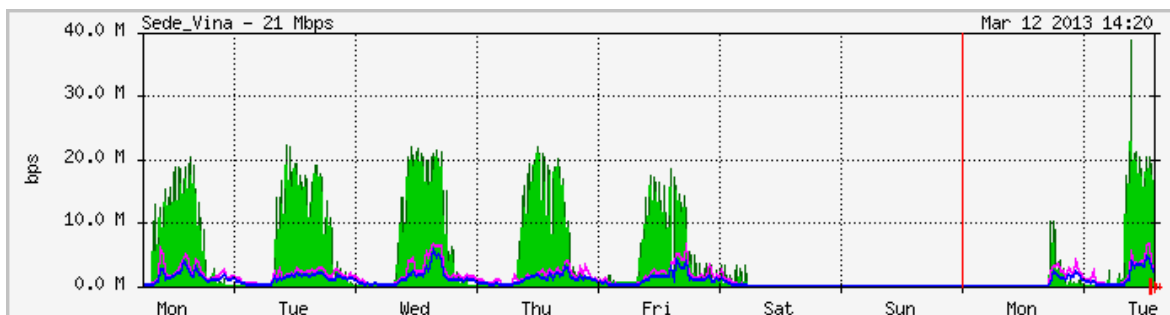


Ilustración 6: Regla de ancho de banda para la sede de Viña del Mar limitada a 21 Mbps.

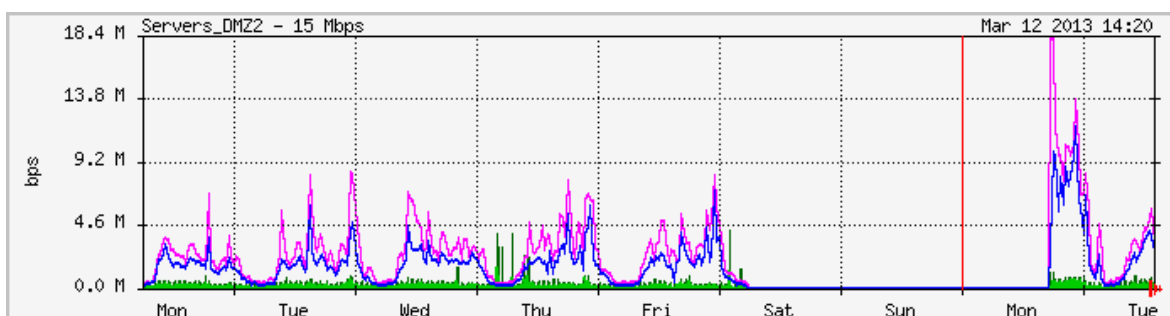


Ilustración 7: Regla de ancho de banda para la red de servidores públicos limitada a 15 Mbps.

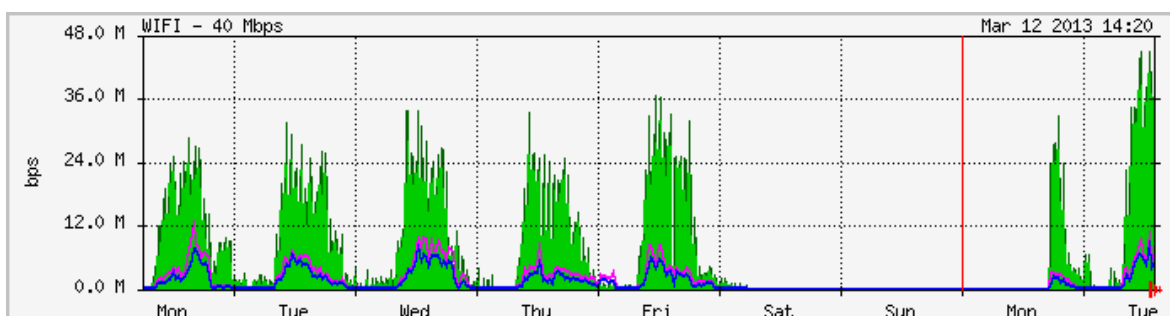


Ilustración 8: Regla de ancho de banda para la red Wifi institucional limitada a 40 Mbps.

Si bien el adaptador de tráfico es un buen sistema para repartir el ancho de banda disponible entre todos los participantes de la comunidad universitaria, presenta 2 falencias críticas para poder administrar en forma eficiente el ancho de banda.

- Solo limita el tráfico por su cota superior:
No garantiza un mínimo de tráfico, solo indica que no podrá transmitir cuando supere una cierta cantidad de tráfico.
- No distingue el tipo de tráfico que se está cursando. Es decir, no se distingue cual es el tráfico útil del no deseado. Un usuario que consuma todo el tráfico de una tubería en actividades no productivas como *streaming* dejará sin ancho de banda a aquellos usuarios deben ocupar el recurso para actividades clasificadas como útiles o productivas (Por ejemplo, navegación web, correo electrónico, revisar publicaciones digitales, etc.). Tampoco es posible distinguir el tráfico nacional del internacional y académico, este punto

es muy importante ya que la mayor demanda se produce en el enlace internacional y este debería ser tratado de manera diferente al resto del tráfico.

Es decir, el equipo no permite implementar las dos actividades claves de un sistema de administración de ancho de banda: monitoreo (no es posible monitorear en detalle, identificando distintos tipos de flujos de tráfico) y control (sólo permite limitar tráfico, en vez de catalogarlo según el protocolo y el tipo de enlace que utilizará).

En particular, para cada uno de las etapas de una administración continua de ancho de banda (descritas en la sección 3 del Capítulo 1), el actual servicio presenta las siguientes falencias:

1. *Inicialmente el sistema debe generar de forma detallada y comprensible gráficos, reportes y tablas de los niveles de consumo de ancho de banda en la red. Estos datos proveen una importante fuente del uso del servicio de internet.*

El actual sistema provee un sistema de gráficos a través de MRTG[25] (*The Multi Router Traffic Grapher*), que es donde se obtuvieron las Figuras 7-11, desde donde se puede obtener el nivel de consumo de ancho de banda. Sin embargo, los gráficos no son lo suficientemente detallados como para obtener información específica, como por ejemplo, cuanto ancho de banda está siendo utilizado por una aplicación o que usuarios son los que utilizan esas aplicaciones.

Por este motivo es imposible determinar qué cantidad de ancho de banda se está utilizando en tráfico deseado y en aquél tráfico considerado como no útil.

2. *Luego de obtener los datos de cómo se está utilizando el ancho de banda dentro de la institución se debe crear la “Política de uso aceptable de recursos computacionales”. EL sistema de administración de ancho de banda debe asegurarse de que estas políticas se cumplan.*

Como el sistema no permite distinguir qué aplicaciones están utilizando el ancho de banda, no hay manera de verificar si están cumpliendo o no las políticas de uso aceptado de recursos computacionales[26].

3. *El sistema debe ser lo suficientemente sofisticado para reaccionar dinámicamente ante cambios en las condiciones de la red, tales como permitir al tráfico de baja prioridad aumentar su consumo si hay ancho de banda que no está siendo utilizado.*

El actual sistema no reacciona dinámicamente ante cambios en los requerimientos de conexiones de la red institucional, ya que este equipo se preocupa de monitorear el tráfico de cada tubería para que al momento de llegar a su límite, retrase los paquetes

de datos o simplemente los descarte. En ningún momento se puede utilizar más del límite establecido a pesar de que pudiera existir ancho de banda disponible.

4. *Una vez que las políticas de ancho de banda han sido implementadas, es necesario seguir capturando datos sobre el estado de la red, especialmente estadísticas de consumo para poder monitorear la efectividad de las políticas. Es importante que existan alertas automáticas cuando una regla de calidad de servicio se ve sobrepasada en tráfico.*

Al igual que en los casos anteriores, esto no se cumple ya que no es posible conocer el detalle de que (es lo que) se está traficando en la red, lo que conlleva a que sea imposible determinar si las políticas se están cumpliendo o no.

Tampoco existen alertas cuando una regla se ve sobrepasada en tráfico, por lo que no existe un mecanismo de control y monitoreo adecuados para poder administrar eficientemente el ancho de banda.

5. *Finalmente y por sobre todas las anteriores, el sistema administrador de ancho de banda debe ser simple de administrar y operar, pero lo bastante sofisticado para que provea un control total del ancho de banda según los requerimientos propias de la institución en donde se está implementando.*

El sistema está implementado en el firewall de FreeBSD, cuya documentación es amplia en la web. Sin embargo, presenta un ambiente poco amigable para la administración ya que las acciones deben ejecutarse a nivel de línea de comando [27]. Cuando hay demasiadas reglas implementadas en el equipo, editarlas se vuelve complicado. En particular, cuando se debe ingresar una regla en una posición específica, ya que puede ocurrir que se necesite modificar la línea del resto de las reglas para mantener un orden establecido.

A pesar de esto, FreeBSD es una plataforma confiable y robusta para este tipo de tareas, pero no entrega las herramientas necesarias para poder monitorear el tráfico de manera de verificar que las políticas existentes en la institución se cumplan.

Este análisis permite concluir que el actual sistema administrador de ancho de banda es una buena herramienta para limitar tráfico, lo que asegura al proveedor entregar como velocidad máxima aquella que le fue contratada. Sin embargo, no cumple con las exigencias mínimas para realizar su tarea de manera eficiente (monitoreo y control).

En el siguiente capítulo se presentará el diseño de una nueva administración de ancho de banda, indicando que características debe poseer el administrador para crear políticas de acuerdo a las

necesidades de la institución y entregando un sistema que permita monitorear y auditar la red para dar seguridad a que las políticas se cumplan, y de esta forma, poder administrar el ancho de

Capítulo 3: Propuesta de nueva administración de ancho de banda y políticas de calidad de servicio

Las deficiencias encontradas en el administrador de ancho de banda que se había estado usando hizo necesario definir claramente qué funciones debe cumplir el nuevo sistema. Estas se describen a continuación:

- Interfaz gráfica:

A diferencia del administrador de ancho de banda descrito en el Capítulo anterior, que funciona en base a líneas de comando, el nuevo administrador de ancho de banda debe poseer una interfaz gráfica sencilla e intuitiva para el usuario. Sencilla en términos de la visualización y edición de las reglas de calidad de servicio, ya que es una de las funciones más críticas de un administrador de ancho de banda. Intuitiva de modo que el monitoreo del estado de la red y la toma de eventuales acciones correctivas resulte fácil y rápido.

- Gráficos de utilización de la red:

El administrador de ancho de banda debe presentar la información de la utilización de la red con gráficos que detallen el uso de ancho de banda por parte de los distintos usuarios y aplicaciones o protocolos en uso en la red. La información debe ser presentada en tiempo real para que, ante una eventual lentitud en la red, se pueda identificar la causa del problema en forma rápida y fácil. También debe tener la capacidad de almacenar gráficos a lo largo del tiempo, principalmente para poder realizar auditorías relativas al consumo de ancho de banda histórico de cada unidad académica.

- Asignación de ancho de banda:

El administrador de ancho de banda debe permitir la creación de reglas de asignación de ancho de banda de forma simple.

Una de las reglas que la Universidad considera importante, es que se pueda asignar un ancho de banda mínimo y máximo.

El límite inferior (mínimo), indica cuánto es el ancho de banda que se le asegura a un equipo o aplicación. Es decir, que no importando el nivel de utilización de la red, los equipos o aplicaciones que sean catalogados en una regla que posee un mínimo de ancho de banda configurado, tendrán siempre garantizado al menos esa cantidad de ancho de banda.

La implementación de esta regla permite entregar ancho de banda dedicado, lo que es muy importante por ejemplo, en video conferencias, en donde se debe asegurar una calidad de audio y video que permita comunicarse con otra persona en tiempo real.

El límite superior (máximo), indica cuánto es el máximo ancho de banda que puede utilizar un equipo o una aplicación. Si bien este límite es fijo, el administrador puede, si fuese necesario, re-asignar ancho de banda dinámicamente entre distintas reglas cuando algunos equipos o aplicaciones no están usando su capacidad máxima y otros requieren más de su límite superior. De esta forma el administrador de ancho de banda tratará de utilizar todo el ancho de banda disponible para la institución.

Por ejemplo, supongamos que una institución tiene contratada una velocidad de 10 Mbps y existen 2 reglas de asignación de ancho de banda, la regla "A" y la regla "B". Ambas reglas establece un límite superior de 5 Mbps. Si los equipos que operan bajo la regla "A" están transmitiendo al máximo de su velocidad y los equipos que operan bajo la regla "B" solo están usando 3 de sus 5 Mbps, el administrador de ancho de banda debe permitir que los equipos que operan bajo la regla "A" puedan, si lo necesitan, traficar a una velocidad de 7 Mbps, ya que de esta forma se está utilizando el 100% del ancho de banda disponible. Si equipos que operan bajo la regla "B" llegan a requerir esos 2 Mbps restantes, el administrador debe detectar esta situación, y realizar una re-asignación oportuna de ancho de banda, volviendo a limitar ambos tipos de tráfico a un máximo de 5 Mbps. Este aspecto dinámico en la asignación del ancho de banda es una característica fundamental que debe poseer el administrador de ancho de banda a implementar.

Este aspecto dinámico es una característica fundamental que debe poseer el administrador de ancho de banda a implementar.

- Políticas de calidad de servicio:

El administrador de ancho de banda debe ser capaz de gestionar políticas de calidad de servicio con un nivel detallado de profundidad, permitiendo identificar el tráfico a nivel de subredes completas, equipos y aplicaciones. Las políticas deben implementar las siguientes funcionalidades.

- Debe permitir discriminar el tráfico según su destino. De esta forma es posible crear reglas distintas para la administración del ancho de banda nacional, internacional e Internet2.
- Debe permitir aplicar reglas de asignación de ancho de banda tanto a subredes completas como a equipos y aplicaciones específicas.
- Debe permitir asignar ancho de banda mínimo y máximo, además de diferenciar el tráfico de subida y de bajada.

- Debe permitir aceptar o denegar tráfico, de forma de controlar lo que se está traficando en la red.
- Debe identificar el tráfico según protocolos, de forma de diferenciar el tráfico útil del no deseado.
- Debe permitir asignar reglas durante intervalos de tiempo, de forma de automatizar la administración y poder crear reglas dinámicas en el tiempo.

Con estas características, las políticas de calidad de servicio que se creen en el administrador de ancho de banda podrán atender los requerimientos que posee la Universidad y monitorear el estado de la red.

- Delegación de administración:

Existen unidades dentro de la Universidad que poseen sus propios administradores de red y de sistemas. Por este motivo es importante poder delegar administración de forma tal que los administradores de cada unidad manejen el ancho de banda según sus requerimientos internos.

- Alarmas:

El sistema debe ser capaz de activar alarmas cuando se producen ciertos eventos definidos por el administrador de red. Por ejemplo, cuando una regla definida por el administrador de red como crítica se viola, se puede enviar un correo electrónico a un grupo de personas para que verifiquen y solucionen aquellos problemas que provocaron la violación de la regla.

Debido a un convenio que la Universidad realizó con el proveedor de servicios de Internet “Claro Chile”, recibió a la Universidad de un administrador de ancho de banda de la empresa *ALLOT*.

En el siguiente capítulo se describen las principales características que posee este equipo y se verifica si cumple con los requisitos aquí establecidos.

Capítulo 4: Administrador de ancho de banda *ALLOT*

En este capítulo se describen las características del administrador de ancho de banda *ALLOT*. Se analizará por separado la capa de *hardware* de la de *software*. El *hardware* corresponde al modelo *NetEnforcer AC-3000*. El *software* posee el nombre de *NetXplorer* y se ejecuta en un servidor dedicado para esta función. *NetXplorer* es la interfaz a través de la cual se configura el administrador. Las características técnicas de ambos se encuentran en el manual de usuario [30] y de administración[31].

Posteriormente, se verificará si el administrador de ancho de banda *ALLOT* cumple con los requisitos listados en el capítulo anterior.

4.1. Capa de Hardware: *NetEnforcer AC-3000*

La serie *NetEnforcer AC-3000* de *Allot Communications* permite administrar tráfico de internet en múltiples enlaces *Ethernet*[28] a velocidades de hasta 8Gbps. Provee monitoreo en tiempo real, aplicación de políticas y direccionamiento de tráfico.

Este equipo permite controlar la utilización de ancho de banda mientras asegura calidad de experiencia (QoE[29] , Quality of experience) para todos los usuarios de la red que utilizan protocolos definidos como productivos por la institución.

En la figura 9 se muestra la vista frontal del dispositivo, identificando a aquellos indicadores visuales de conectores a través de la palabra *LED*.

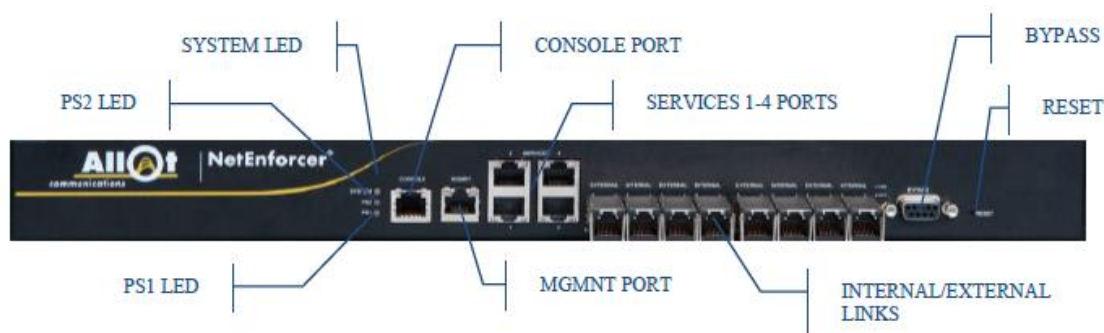


Ilustración 9: Vista frontal del *NetEnforcer AC-3000*, extraída del manual de usuario.

Descripción de los LED del panel frontal

- *System LED*: Muestra el estado actual del sistema. Si el LED está con una luz verde permanentemente encendida significa que el *NetEnforcer* está funcionando normalmente.

En cambio, si la luz es roja, es indicación de un error fatal . Si el LED se encuentra apagado significa que la unidad se encuentra en el modo *Bypass*.

- *PS1*: Indica el estado de la primera fuente de poder. Si el LED se encuentra con una luz verde permanentemente encendida, la fuente de poder está funcionando correctamente. Si se encuentra con un color rojo , significa que la fuente está instalada correctamente pero no entrega energía al equipo. Si no hay ninguna luz presente, significa que la fuente de poder no funciona correctamente.
- *PS2*: Indica el estado de la segunda fuente de poder. El código de colores es exactamente el mismo que para el LED *PS1*.
- *Internal/External link LED*: 2 por cada interfaz de red. Posee un LED verde que indica un enlace activo y un LED amarillo, que indica la actividad del puerto.

Conectores del panel frontal:

- *Internal/External Links*: Existen 8 conectores para interfaces de red de 1 *GigabitEthernet* cada una. Cada uno de estos conectores permite administrar el tráfico de hasta 4 enlaces físicos.
- *Console port*: Puerto de consola RS232 implementado como una conexión RJ-45. Este conector permite conectarse al equipo para administrarlo mediante línea de comandos.
- *MGMNT*: Es la interfaz de red para administrar el equipo. Se utiliza principalmente para monitorear, configurar y realizar mantenimiento al equipo.
- *Bypass*: Conector tipo D. Solo se utiliza para conectar el *NetEnforcer* a la unidad *Bypass*. El funcionamiento de esta unidad se explica a continuación.

Unidad *Bypass*:

El *NetEnforcer* opera con una unidad de *Bypass* externa, que se puede observar en la figura 10. Esta unidad es un subsistema de misión crítica que está diseñado para asegurar la conectividad en la red frente a fallas del *NetEnforcer*.



Ilustración 10: Unidad *Bypass*

A continuación, en la figura 11, se muestra como se realizan las conexiones entre el *NetEnforcer* y la unidad *Bypass* para asegurar la conectividad en la red ante una falla.

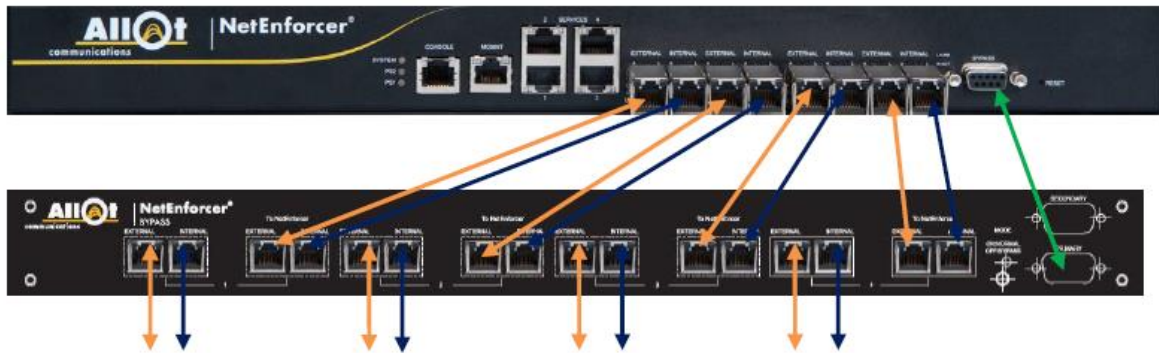


Ilustración 11: Conexión entre *NetEnforcer* y unidad *Bypass*.

El *NetEnforcer* permite recoger estadísticas de tráfico desde la red, tales como número de conexiones establecidas, conexiones descartadas, consumo de ancho de banda por parte de aplicaciones y equipos. Estas estadísticas se van entregando en tiempo real y también se almacenan para entregar información histórica del estado de la red.

Además de recolectar información detallada sobre el tráfico que circula a través de él, el *NetEnforcer* también puede catalogar el tráfico, dependiendo del origen/destino de los datos y el protocolo utilizado, aplicando parámetros de calidad de servicio definidos por el administrador de red, tales como priorizar y asignar ancho de banda a protocolos específicos.

En la siguiente sección se estudiará como el *NetEnforcer* puede realizar su labor de administrador de ancho de banda a través de su software *NetExplorer*.

4.2. *NetExplorer*

El *NetExplorer* es un sistema de red altamente escalable, ya que permite administrar volúmenes de tráfico de hasta 8 Gbps (la universidad cuenta una licencia para traficar hasta 1 Gbps, lo que es suficiente ya que los cortafuegos poseen una capacidad física de 1 Gbps en sus interfaces de red). Permite la toma de decisiones estratégicas sobre la base de una aplicación de red, instalada en un servidor dedicado y el análisis de tráfico de los abonados al servicio.

NetExplorer permite el monitoreo en tiempo real de la red, permitiendo analizar y solucionar problemas en un corto plazo. Además proporciona informes basados en el tráfico pasado, los cuales pueden ir desde días hasta años hacia atrás, lo que permite obtener datos para realizar planificaciones de capacidad, el seguimiento del uso y análisis de tendencias en la red.

También permite la gestión proactiva del tráfico, ya que a medida que llegan requerimientos de ancho de banda, el equipo toma decisiones en base a las políticas de calidad de servicio y al consumo actual de ancho de banda de la institución. Además provee alarmas de todo el sistema,

las cuales son elegidas por el administrador de red, realiza auditorias, recolección y exportación de datos para fines de facturación y cuotas.

El *NetXplorer* configura el dispositivo *NetEnforcer* y un catálogo central permite el aprovisionamiento global de políticas.

4.2.1 Términos y conceptos del *NetXplorer*

Una política informática se define como el conjunto de reglas, procedimientos, asignación de funciones y demás elementos que rigen la implantación de sistemas de información en una institución.

Una política de calidad de servicio es el conjunto de reglas y acciones que buscan entregar un servicio que satisfaga de mejor manera los requerimientos de red de los usuarios de la institución.

Las características de estas políticas en el *NetXplorer* son definidas en un catálogo, el cual contiene todas aquellas variables que se utilizarán en las reglas de asignación de ancho de banda del equipo.

Estas reglas son aplicadas a nivel de línea, tubería o canal virtual. Cada uno de estos niveles corresponde a una abstracción del enlace físico, los cuales, en el caso particular de la universidad, son utilizados para lo siguiente:

- Líneas: En este primer nivel de abstracción del enlace físico se separan los tráficos interno, nacional, internacional y hacia Internet2 en líneas distintas.
- Tuberías: En este segundo nivel de abstracción se definen las distintas unidades de la Universidad, de esta forma es posible tratar de forma independiente el tráfico de cada unidad o departamento de la Universidad.
- Canales virtuales: Es el último nivel de abstracción del enlace físico, acá se definen las reglas específicas para cada protocolo o equipo específico correspondiente a una unidad académica.

De esta forma, por ejemplo, se puede administrar el tráfico web (un canal virtual para el tráfico http) del departamento de electrónica (una tubería creada para el departamento) traficando en sitios internacionales (una línea creada para el tráfico internacional).

La jerarquía de la abstracción del canal físico se puede observar en la figura 12, en donde se observa que un enlace se puede dividir en 1 o más líneas, a su vez, cada línea se puede dividir en 1 o más tubería y la vez, cada tubería puede contener 1 o más canales virtuales.

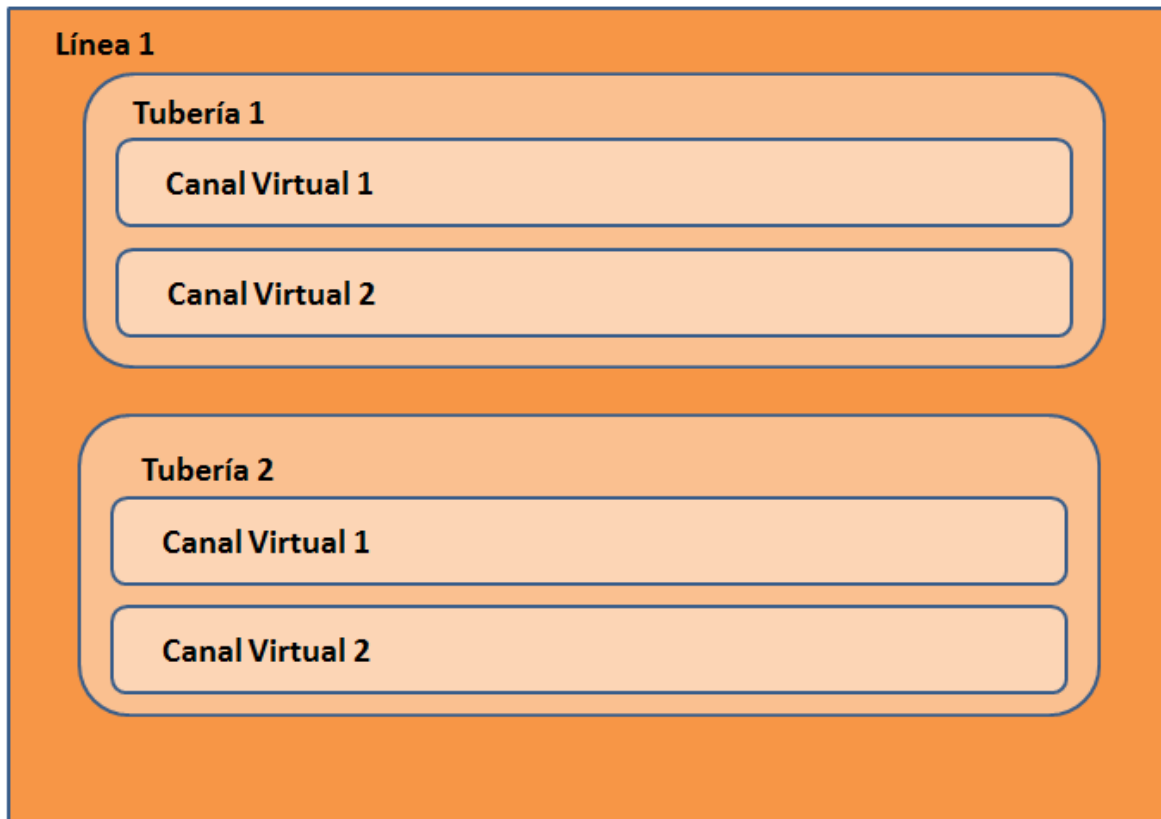


Ilustración 12: Resumen jerárquico en el *NetXplorer*.

A continuación se explicará en detalle los términos que son importantes para entender el funcionamiento del NetXplorer.

Catálogo

Las entradas del catálogo, que se definen en el editor del catálogo, sirven como condiciones o acciones en las reglas que constituyen una política, como por ejemplo direcciones de origen/destino, asignación de ancho de banda, denegación de tráfico, etc. De esta manera, las entradas del catálogo pueden ser vistas como los bloques de construcción de las políticas. Una vez que un catálogo se ha definido en el editor de catálogos, puede ser utilizado en diferentes reglas.

Línea

Una línea es el primer nivel de abstracción de un enlace físico y representa el nivel más alto de jerarquía. El ancho de banda total del enlace que es cursado a través del *NetEnforcer* se puede dividir en líneas y cada línea puede ser manejada como si se tratara de un enlace independiente.

Una línea se compone de una regla basada en una o más conjuntos de condiciones y un conjunto de acciones que se aplican cuando todas las condiciones se cumplen. Existe la línea *Fallback* por defecto en todas las Políticas. Las líneas adicionales se pueden añadir por encima de la línea *Fallback* en la tabla de políticas y esta no puede ser modificada ni eliminada. El tráfico que no se

clasifica en ninguna de las líneas de arriba en la jerarquía se clasificará en la línea *Fallback*. Cada línea, incluyendo la línea *Fallback*, contiene una o más tuberías.

Tubería

El ancho de banda total asignado a través de cada línea se puede dividir en tuberías, y cada tubería puede entonces ser gestionada de forma independiente.

Cada tubería se compone de una regla basada en uno o más conjuntos de condiciones y un conjunto de acciones que se aplican cuando todas las condiciones se cumplen. Por defecto, cada línea contiene por lo menos una tubería, la *Fallback*. Tuberías adicionales se pueden añadir por encima de la tubería *Fallback* en la tabla de políticas, y esta no puede ser modificada o eliminada, y el tráfico que no se clasifique en otras tuberías dentro de una línea dada, se clasificará en la tubería *Fallback*. Cada tubería, incluyendo la *Fallback*, contiene uno o más canales virtuales.

Canal virtual

Un canal virtual (VC) representa el nivel más granular en la jerarquía de aplicación de políticas. El ancho de banda total circulando a través de cada tubería se puede dividir en VC, y cada VC puede ser gestionado de forma independiente. Cada VC consiste en una regla basada en uno o más conjuntos de condiciones y un conjunto de acciones que se aplican cuando todas las condiciones se cumplen. Por defecto, cada tubo contiene al menos un VC, el *Fallback*. VCs adicionales se pueden añadir por encima de la VC *Fallback* en la tabla de aplicación de políticas y este no puede ser modificado o eliminado, y el tráfico que no se clasifique en ningún otro VCs dentro de una tubería dada se clasificará en el VC *Fallback*.

Resumiendo, una línea puede contener 1 o más tuberías, y su vez, cada tubería puede contener 1 o más canales virtuales. De esta forma se puede administrar de forma más eficiente y ordenada el ancho de banda contratado por la institución, esto se podrá observar de forma más simple cuando se explique la implementación en la red corporativa de la universidad.

4.2.2 Interfaz de usuario

La interfaz de usuario del *NetXplorer* es una aplicación JAVA, desde la cual se puede administrar todas las características del equipo. Por motivos de seguridad, antes de ingresar a la ventana principal del programa, se debe ingresar el usuario y contraseña del dispositivo. Esta interfaz se aprecia en la figura 13.

Ilustración 13: Acceso de administración del *NetXplorer*.

Una vez autenticado en el servidor, se despliega la interfaz de usuario del software, la cual se aprecia en la figura 14 destacando sus principales componentes.

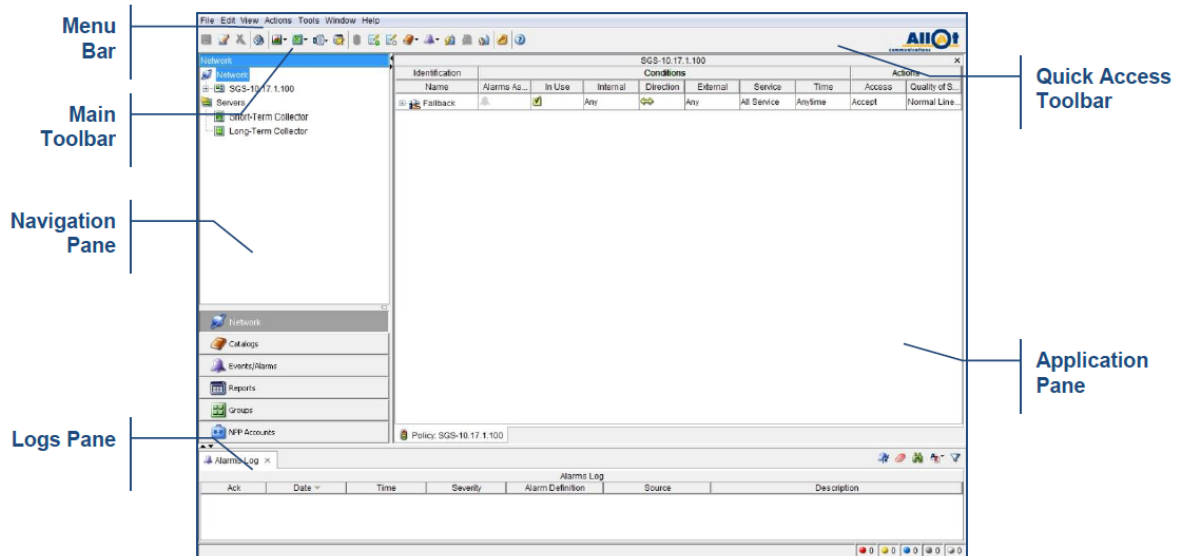


Ilustración 14: Componentes de la interfaz de usuario del NetXplorer.

A continuación se describirán los principales componentes de la interfaz, para más detalle dirigirse al manual de usuario[30].

- **Barra de herramientas principal:** En este componente de la interfaz, es posible realizar y acceder a las funciones más importantes del equipo, entre ellas destacan: guardar la configuración, acceder a propiedades del sistema, eliminar configuraciones, monitorear el tráfico en tiempo real, monitorear el tráfico histórico cursado en el equipo, acceder al editor de políticas, acceder a los catálogos y revisar alarmas y eventos del sistema.
- **Panel de navegación:** Se divide en 2 partes, una superior y una inferior. En la superior se muestra un árbol que despliega todas las entradas y subcomponentes existentes en el sistema. La parte inferior es un menú rápido para acceder a las principales aplicaciones del *NetXplorer*, las cuales son: Red, catálogos, eventos y alarmas, reportes, gráficos y las cuentas de delegación de administración.
- **Panel de aplicación:** Esta es la sección principal de la interfaz, acá se despliega la información de la aplicación seleccionada. Por ejemplo, al seleccionar el catálogo, en el panel de aplicación se mostrarán todas las entradas definidas por el administrador, al seleccionar un gráfico, en el panel de aplicación se desplegará dicho gráfico.
- **Panel de registros:** En esta sección se puede visualizar los registros de alarmas, las cuales son configuradas en la aplicación de eventos y alarmas.

4.2.3 Catálogos

Uno de los principales componentes con los que se trabaja en el administrador de ancho de banda son los catálogos, por ese motivo, a continuación se describirá en detalle las principales características de este componente.

Los catálogos contienen los valores disponibles que se utilizarán al crear o editar una política. Por ejemplo, al seleccionar la condición que hace calzar el tráfico que pasa por el equipo en una tubería, canal virtual o filtro, los valores posibles de tal condición están definidos en el catálogo de *Host*. Es posible, cambiar o eliminar entradas en catálogos.

Una entidad del catálogo, como un *host* específico o una definición de calidad de servicio, se define una vez en el catálogo correspondiente y, después se puede utilizar las veces que sean necesarias en el editor de políticas.

Los catálogos principales con los que se trabaja en esta implementación son los siguientes:

- Catálogo de *host*: Las entradas definidas en este catálogo, son los posibles valores que pueden tomar las condiciones internas y externas definidas en una línea, tubería, canal virtual o filtro. Las condiciones internas y externas se refieren al origen y destino del tráfico, y estos se pueden definir como una dirección IP, un segmento de red, una red completa y por nombre del equipo.
- Catálogo de servicios: Las entradas de este catálogo son los posibles valores para la condición servicio definido en una línea, tubería, canal virtual o filtro. El servicio se refiere al protocolo utilizado en una conexión.
- Catálogo de tiempo: Las entradas de este catálogo son los posibles valores para la condición tiempo definido en una línea, tubería, canal virtual o filtro. La condición tiempo se refiere a la aplicabilidad de reglas en un cierto período de tiempo.
- Catálogo de *QoS*: Las entradas de este catálogo son los posibles valores para la condición de calidad de servicio (*QoS*) definido en una línea, tubería, canal virtual o filtro. La condición *QoS* asigna ancho de banda y prioriza tráfico.
- Catálogo *DoS*: Las entradas en el Catálogo de *DoS* (denegación de servicio[32]) permiten controlar el número de conexiones y la tasa de las nuevas conexiones establecidas. Esta es una importante característica del equipo, ya que permite detectar, mitigar y bloquear ataques de denegación de servicio.

Cada catálogo posee su propio editor, en donde se pueden agregar entradas o modificar entradas existentes.

4.2.4 Definición de políticas de calidad de servicio

El software *NetXplorer* permite clasificar el tráfico y asegurar calidad de servicio. El tráfico puede ser lógicamente agrupados en categorías tales como de misión crítica, tiempo crítico, de alta o baja prioridad.

Las políticas de QoS consisten en un conjunto de condiciones y acciones que se aplican para atender un requerimiento específico. El tráfico se clasifica utilizando líneas, tuberías y canales virtuales. Una línea, tubería o canal virtual se define por una o más condiciones y un conjunto de acciones. Una línea incluye una o más tuberías. Una tubería incluye uno o más canales virtuales.

En la figura 15 se muestra un ejemplo de políticas que muestra la relación entre líneas, tuberías, canales virtuales y condiciones.

Identification		Conditions							Actions	
Name	Alarms As...	In Use	Internal	Direction	External	Service	Time	Tethering	Access	Quality of S...
CDMA All Trffi		☒	Any	↔	Any	All IP	Anytime	Ignore	Accept	Normal Line...
aaae.mym		☒	aaae.my...	↔	Any	All IP	Anytime	Ignore	Accept	Normal Pip...
Encrypt		☒	Any	↔	Any	SSL	Anytime	Ignore	Accept	Normal Virtu...
Tetherin		☒	Any	↔	Any	Tethering_TM	Anytime	Ignore	Accept	Normal Virtu...
Android		☒	Any	↔	Any	Android Mar...	Anytime	Ignore	Accept	Normal Virtu...
Pandora		☒	Any	↔	Any	Pandora	Anytime	Ignore	Accept	Normal Virtu...
Facebo		☒	Any	↔	Any	Facebook G...	Anytime	Ignore	Accept	Normal Virtu...
Email		☒	Any	↔	Any	Mail	Anytime	Ignore	Accept	Normal Virtu...
File Tra		☒	Any	↔	Any	File Transfer	Anytime	Ignore	Accept	Normal Virtu...
Stream		☒	Any	↔	Any	Streaming_...	Anytime	Ignore	Accept	Normal Virtu...
Stream		☒	Any	↔	Any	Streaming A...	Anytime	Ignore	Accept	Normal Virtu...
Browsi		☒	Any	↔	Any	Web Applica...	Anytime	Ignore	Accept	Normal Virtu...
Fallbac		☒	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Virtu...
aaaf.myme		☒	aaaf.mym...	↔	Any	All IP	Anytime	Ignore	Accept	Normal Pip...
aaag.mym		☒	aaag.my...	↔	Any	All IP	Anytime	Ignore	Accept	Normal Pip...
Fallback		☒	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Pip...
Fallback		☒	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Line...
Fallback		☒	Any	↔	Any	All Service	Anytime	Ignore	Accept	Normal Pip...

Ilustración 15: Relación entre línea, tubería, canal virtual y condiciones.

Al llegar una conexión al *NetXplorer*, éste busca en la tabla de políticas de arriba hacia abajo. Tan pronto como se encuentra una condición de una línea que coincida con la conexión, *NetXplorer* deja de buscar en el resto de las líneas. Dentro de la línea seleccionada, se busca una condición de tubería que coincida con la conexión, una vez encontrada, el *NetXplorer* deja de buscar en las tuberías. Del mismo modo, dentro de la tubería seleccionada, se busca una condición de algún canal virtual que coincida con la conexión. Una vez terminado este proceso, el administrador de ancho de banda asigna recursos según lo definido en el canal virtual.

Tal como se mencionó anteriormente, existe una línea, tubería y canal virtual especial, llamada *FallBack*. Cuando no existe una coincidencia del tráfico, se asignan recursos según lo definido en ella.

En resumen, el proceso de asignación de recursos a través de políticas se realiza de la siguiente forma, mostrada en la figura 16.

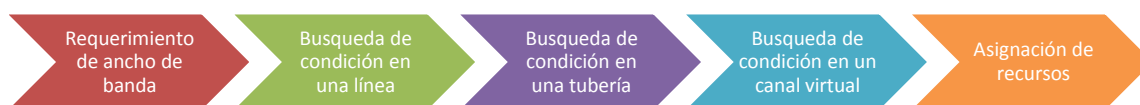


Ilustración 16: Proceso de asignación de recursos.

Las condiciones pueden ser definidas a nivel de línea, tubería o a nivel de canal virtual. El *NetXplorer* busca coincidencias entre las conexiones y las condiciones, primero a nivel de línea, a continuación, a nivel de tubería y luego a nivel de canal virtual.

A continuación se describirán las condiciones, acciones y opciones que conforman una política.

- *Alarms Assignment*: Indica si se ha asignado una alarma a la regla.
- *In use*: Habilita o deshabilita el objeto.
- *Internal*: Define el origen del tráfico. Por ejemplo, una IP específica, direcciones MAC, un rango de direcciones IP, direcciones de subred IP o nombres de host. El valor predeterminado "Any" cubre el tráfico procedente de cualquier fuente.
- *Direction*: Indica el sentido del tráfico entre el origen y el destino seleccionado (bidireccional, "Internal to External" o "External to Internal"). El valor predeterminado es bidireccional

- *External*: Define el destino del tráfico. Por ejemplo, una IP específica, direcciones MAC, un rango de direcciones IP, direcciones de subred IP o nombres de host. El valor predeterminado “Any” cubre el tráfico de cualquier fuente.
- *Service*: Define los protocolos pertinentes a una conexión. Los protocolos pueden ser TCP, UDP o IP. Los protocolos TCP y UDP se definen basándose en el tipo de puerto. El protocolos HTTP pueden incluir definiciones de contenido, como los directorios específicos Web, páginas o patrones de URL. El valor predeterminado “Any” cubre todos los protocolos.
- *Time*: Define el período de tiempo durante el cual se recibe el tráfico. Por ejemplo todos los días entre las 8.00 y 6.00 PM, domingos de 12:00 AM a 12:00 PM. o en el día 1 y 15 de cada mes. El valor por defecto es “Any”, que cubre el tráfico en cualquier momento.

Cuando se crea una nueva línea, tubería o canal virtual, se le asigna una condición por defecto, con valores por defecto para cada condición y se puede modificar estos valores según sea necesario.

Las líneas, tuberías y canales virtuales incluyen un conjunto de acciones que se asigna al tráfico una vez que se cumpla alguna de las condiciones definidas. Sólo acciones de QoS pueden ser definidas en una línea. Hay seis acciones que se pueden definir para una tubería o canal virtual.

Las acciones que toma el administrador de ancho de banda son las siguientes:

- *Access*: Esta acción determina el acceso al tráfico. Si el control de acceso para una línea, tubería o canal virtual se especifica como *Reject* o *Drop*, todo tráfico que cumpla con las condiciones de la línea, tubería o canal virtual es descartado y no se aplican las acciones de QoS o de control de conexiones. Si el control de acceso para una línea, tubería o canal virtual se especifica como *Bypass* todo tráfico que cumpla con las condiciones de la línea, tubería o canal virtual se enruta a su destino, pero no se aplican las acciones de QoS y el tráfico no puede ser visualizado en gráficos.
- *QoS*: Esta acción determina la calidad de servicio entregada al tráfico. La calidad de servicio entregada por defecto a las líneas, tuberías o canales virtuales es la prioridad normal, dentro de la cual no se definen valores de ancho de banda permitidos y no hay limitación de conexiones. En la siguiente sección se explicará cómo se asigna ancho de banda a una política.
- *DoS* (denegación de servicio): Esta acción permite limitar la frecuencia y el número de conexiones hacia equipos de la red, lo que da protección contra los ataques a los recursos de la red (por ejemplo, los servidores conectados internamente). *NetXplorer* analiza la distribución del tráfico entre los distintos protocolos y puertos, y admite o descarta el tráfico cuando se han superado los umbrales predefinidos.

A continuación se muestran 3 ejemplos de cómo pueden ser utilizadas las líneas, tuberías y canales virtuales.

- Un proveedor de servicios de Internet vende porciones de ancho de banda a los clientes (que se define en una tubería), cada uno basado en la calidad de servicio concedidas a esta categoría de clientes (por ejemplo, los clientes de Oro, Plata y Bronce).
- Una universidad quiere controlar la congestión del tráfico de Internet a través de la red, incluyendo el tráfico de los estudiantes y profesores, en particular, para limitar el uso de FTP y conceder una asignación de ancho de banda preferencial a los profesores durante las horas entre semana. La universidad define canales virtuales para el uso de los profesores, el uso normal de los estudiantes, y el uso de los estudiantes durante las horas nocturnas. Otra condición se define entonces en el canal virtual del uso de los estudiantes, que especifica un servicio diferente para los estudiantes que trafican a través de FTP.
- Una organización posee varios enlaces a Internet. Sólo se requiere un *NetEnforcer* con tuberías definidas para el tráfico de cada enlace permitiendo gestionarlos de forma independientes.

Para una correcta definición de políticas se deben seguir los siguientes pasos de la figura 17.

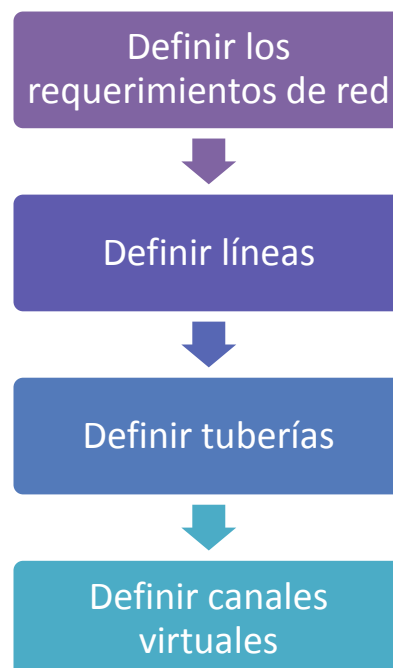


Ilustración 17: Proceso de creación de políticas.

4.2.5 Asignación de ancho de banda y priorización de tráfico

La asignación de ancho de banda y la priorización de tráfico se realizan en el editor de catálogo como se mencionó antes. En la figura 18 se observa las opciones que posee el editor de QoS.

Line Enhanced QoS Entry Properties

Name:

Description:

Line Based QoS Coverage:

Inbound and Outbound

Minimum Bandwidth (Kbps):

Maximum Bandwidth:

☒ Maximum Allowed

☐ in Kbps:

☒ Priority (Best Effort)

☐ Priority (1 Lowest, 4 Highest)

If Minimum Line Bandwidth not Allocated:

Save Reset Cancel

Ilustración 18: Editor del catálogo de QoS.

La definición es exactamente igual tanto para las líneas, tuberías y canales virtuales, por lo que a continuación se explicará cada parámetro de la política de QoS.

A cada entrada de QoS se le puede asignar un nombre lógico de forma de ser entendible para las personas que administren el equipo.

El equipo permite asignar ancho de banda de dos formas, definiendo el tráfico entrante igual al saliente, es decir, tráfico simétrico. La otra opción es definir el tráfico entrante distinto al saliente, es decir tráfico asimétrico. Generalmente el tráfico será simétrico, ya que los clientes de una red descargan y suben material, a diferencia de un servicio, por ejemplo, un servidor web, este equipo descargará muy poca información desde la red, pero al entregar un servicio, el tráfico de subida es muy superior al de bajada. Por este motivo existen condiciones en que es mejor definir cada tipo de tráfico en forma independiente.

Luego se deben definir las cotas, tanto superior como inferior, de ancho de banda asignado a la política de QoS.

- *Minimum Bandwidth* (Kbits/sec): Se asigna la cota inferior de ancho de banda asignado a la regla, mientras exista tráfico que requiera ancho de banda en este canal, nunca será inferior a este límite. La obtención de ancho de banda por encima del mínimo, sin embargo, depende de la prioridad de tráfico, en donde debería haber competencia por el ancho de banda.
- *Maximum Bandwidth*: Tiene la opción de asignar el máximo ancho de banda (la máxima capacidad que posea el canal físico) o ingresar el ancho de banda máximo que se asignará al canal en Kbits/seg. El ancho de banda total del tráfico asignado en este canal no superará dicho límite.

Una vez asignados los valores de ancho de banda mínimo y máximo se debe escoger la prioridad que tendrá la política de QoS, para esto existen 2 opciones.

- *Best Effort*: Esta prioridad del mejor esfuerzo, que es la forma en que funcionan la mayoría de conexiones a internet, si todos los objetos del mismo nivel de políticas se configuran en mejor esfuerzo, no habrá priorización entre ellos. Cuanto más tráfico un objeto requiere, más ancho de banda que se asignará a la misma, sin perjuicio de la cantidad de ancho de banda libre disponible.
- *Prioridad manual*: Se define una escala desde 1 hasta 4, en donde 1 es la prioridad más baja y 4 es la más alta. No se recomienda el uso de Prioridad *Best Effort* si otros elementos tienen Prioridades asignadas del 1 al 4. En tales situaciones, un elemento que se ha asignado con prioridad *Best Effort* puede recibir un porcentaje muy bajo del ancho de banda disponible en comparación a uno priorizado entre 1 a 4.

Cuando no es posible asignar el mínimo ancho de banda configurado en la regla, como por ejemplo, en el caso que no quedan recursos disponibles, el administrador entrega 2 opciones.

- *Admit by Priority*: Admitir por prioridad, se acepta la nueva conexión, pero no asigna el ancho de banda mínimo. La nueva conexión obtiene ancho de banda por prioridad.
- *Drop*: Todos los paquetes se descartan. El usuario se desconecta y puede ver el mensaje de conexión en tiempo de espera.

A continuación se presentan tres ejemplos prácticos de como el administrador asigna ancho de banda en distintas situaciones.

Example #1: Different Priority Levels



- **Priority Levels:** Bandwidth is allocated by priority weighting irrespective of ingress



$$\text{Allocated Bandwidth} = \frac{\text{Element Weight}}{\text{Total Weight}} \times \text{Total Bandwidth Available}$$



Ilustración 19: Ejemplo 1 de asignación de ancho de banda.

En este ejemplo, se tienen 2 peticiones de asignación de ancho de banda, 200 Mbps de tráfico HTTP y 100 Mbps de tráfico FTP. Ambos requerimientos deben ser asignados en una tubería que tiene definido un tráfico máximo de 100 Mbps. Si el administrador del *NetXplorer* asigna una prioridad de 1 al canal virtual correspondiente a HTTP, y una prioridad de 4 al canal virtual correspondiente a FTP, el administrador de ancho de banda asignará 20 Mbps al tráfico HTTP y 80 Mbps al tráfico FTP.

Esta asignación de ancho de banda es realizada independientemente de la tasa de ingreso de tráfico. La asignación es realizada a cada elemento dividiendo el peso de cada uno de ellos (en este caso 1 para HTTP y 4 para FTP) por el peso total de ambos canales virtuales, en este caso es 5 (4+1). Este valor se multiplica por el ancho de banda total disponible (en este caso corresponde a los 100 Mbps que posee asignado la tubería) lo que da como resultado el ancho de banda que se le asignará a cada tipo de tráfico.

Example #2: Equal Priority vs Best Effort



- **Equal Priority: Bandwidth assigned irrespective of ingress**



- **Best Effort: Bandwidth is allocated proportionately to ingress**



Ilustración 20: Ejemplo 2 de asignación de ancho de banda.

En este ejemplo, se tienen 200 Mbps de tráfico HTTP y 100 Mbps de tráfico FTP que al igual que el ejemplo anterior, deben ser asignados en una tubería que tiene definido un tráfico máximo de 100 Mbps. Ahora se compararán 2 mecanismos de asignación.

En el ejemplo superior, ambos canales virtuales tienen asignadas la misma prioridad, por lo que el ancho de banda será asignado igualitariamente para ambos servicios, sin importar la tasa de ingreso de tráfico. En este caso, cada canal virtual recibirá una parte igual de los 100 Mbps asignados a la tubería, es decir, 50 Mbps cada uno.

En el ejemplo inferior, el administrador del *NetXplorer* asigna a cada canal virtual una prioridad de *Best Effort*. Esto significa que no existe una repartición equitativa de los recursos entre ambos canales virtuales y eventualmente aquel canal virtual que posea mayor tasa de ingreso de tráfico reciba una mayor cantidad de ancho de banda. En este caso, el tráfico HTTP recibirá el doble de ancho de banda que el tráfico FTP, específicamente 66,66 Mbps para HTTP y 33,33 Mbps para FTP.

Esto se obtiene de la siguiente formula:

- HTTP: $[200/(200+100)] \times 100 = 66,66 \text{ Mbps}$

- FTP: $[100/(200+100)]*100 = 33,33$ Mbps

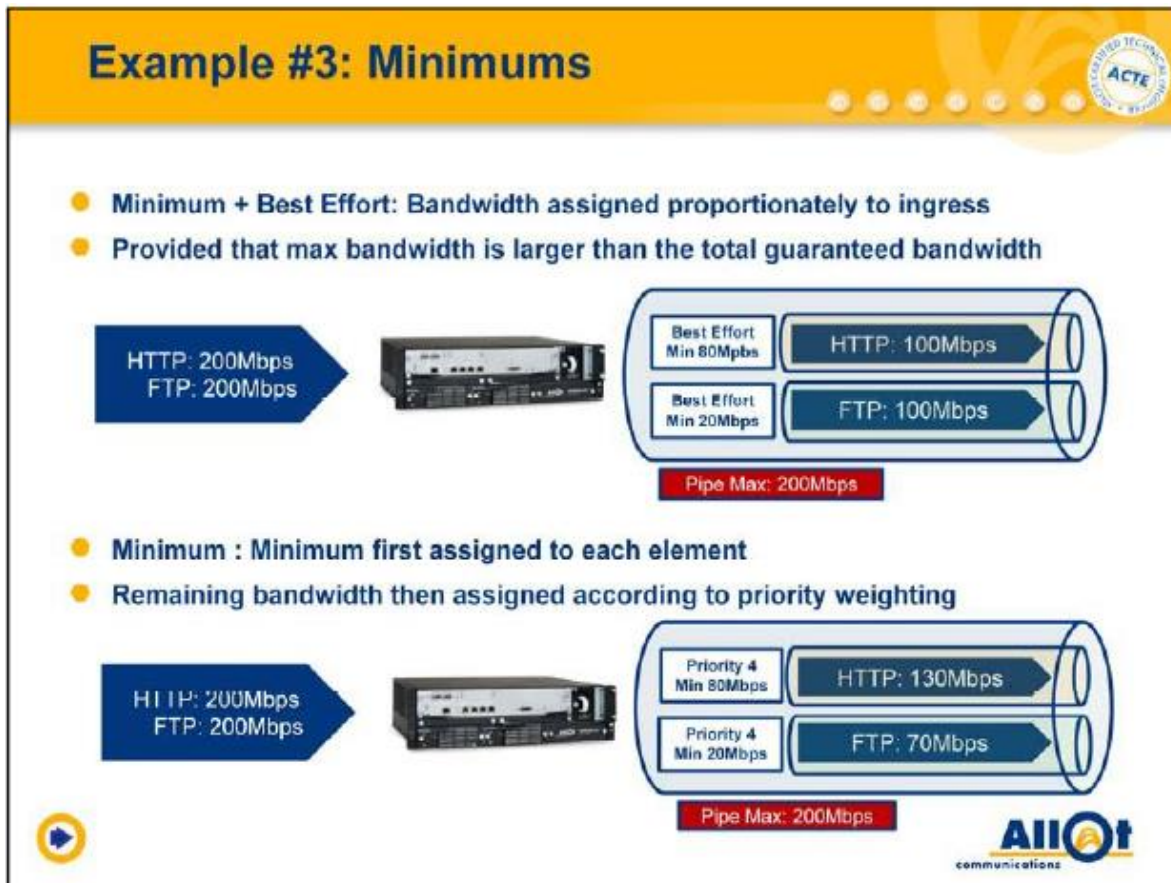


Ilustración 21: Ejemplo 3 de asignación de ancho de banda.

En este último ejemplo, se tienen 200 Mbps de tráfico HTTP y 200 Mbps de tráfico FTP. Ambos requerimientos deben ser atendidos en una tubería que posee un tráfico máximo de 200 Mbps. En ambos casos el administrador del *NetXplorer* desea asegurar que el tráfico HTTP reciba garantizado un mínimo de 80 Mbps, mientras que el tráfico FTP recibe un mínimo garantizado de 20 Mbps.

Si el administrador del *NetXplorer* le asigna a cada canal virtual una prioridad de *Best Effort*, el ancho de banda será repartido en proporción al tráfico entrante, dado que el ancho de banda máximo es más grande que el total garantizado ($200 \text{ Mbps} > (80+20) \text{ Mbps}$), en este caso, a cada canal virtual se le asignarán 100 Mbps. Si no existiese un mínimo definido, el ancho de banda total para cada canal virtual vendría dado por $[200/(200+200)]*200 = 100$ Mbps. Si el mínimo garantizado para cada canal virtual es menor que el valor esperado, el resultado será el mismo que si no existiese un mínimo.

Si ahora el administrador asigna el mismo nivel de prioridad, adicionando el mínimo, el ancho de banda asignado será distinto para cada canal virtual, aun cuando la tasa de entrada es la misma.

En este caso HTTP recibirá 130 Mbps, mientras que FTP recibirá 70 Mbps, esto se puede comprobar con lo siguiente.

- HTTP: ancho de banda disponible después de asignar el mínimo = $200 - (80+20) = 100$ Mbps
ancho de banda total = $80 + (100/2) = 130$ Mbps
- FTP: ancho de banda disponible después de asignar el mínimo = $200 - (80+20) = 100$ Mbps
ancho de banda total = $20 + (100/2) = 70$ Mbps

Una vez comprendido el funcionamiento del administrador de ancho de banda, su estructura, capacidades y forma de asignar recursos, se procederá a explicar la implementación del administrador en la red corporativa de la universidad.

Capítulo 5: Implementación del administrador de ancho de banda *ALLOT*

El equipo *ALLOT* fue adquirido por la universidad gracias a un convenio con el proveedor de servicio CLARO, el cual prestará soporte a través de la empresa NetSecure [33]. Esta empresa es la encargada de entregar a la Universidad el equipo con la configuración básica de forma tal que el personal del DTI solo realice la configuración de políticas en el *NetXplorer*.

La implementación del nuevo administrador de ancho de banda constó de 2 partes: la instalación física del *NetEnforcer* y la configuración del *NetXplorer*.

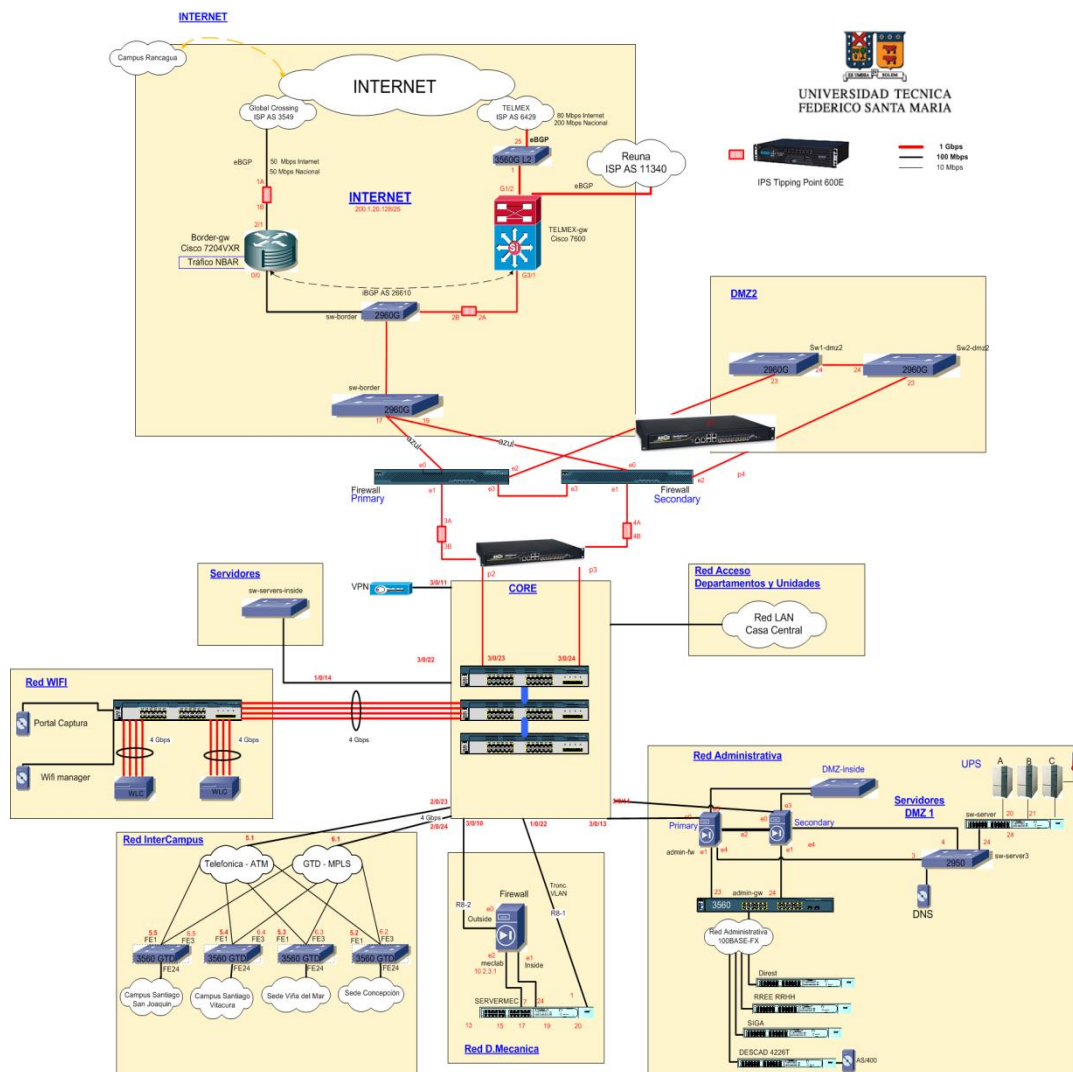
5.1. Instalación de NetEnforcer

El equipo ALLOT posee 4 interfaces de red y dada la topología redundante de la red UTFSM, el equipo fue localizado entre el núcleo, la red DMZ y ambos cortafuegos de la red de la Universidad.

Los cortafuegos de la Universidad están configurados en alta disponibilidad operando en modo activo/pasivo, es decir, hay un equipo que presta servicio, y cuando este equipo falle, el de respaldo está preparado para tomar su lugar. Por este motivo las interfaces se utilizaron de la siguiente forma.

- Interfaz 1: Para el tráfico entre el núcleo de red y un cortafuego.
- Interfaz 2: Para el tráfico entre el núcleo de red y el segundo cortafuego.
- Interfaz 3: Para el tráfico entre la red DMZ y un cortafuego.
- Interfaz 4: Para el tráfico entre la red DMZ y el segundo cortafuego.

Con esta disposición, todo el tráfico cursado por la Universidad, esto se puede apreciar en la figura 22.



El nuevo administrador de ancho de banda fue instalado entre el núcleo, *DMZ* y cortafuegos principales. De esta forma todo el tráfico de la universidad debe pasar por el administrador de ancho de banda, lo que permite que todo el tráfico pueda ser analizado y administrado. Es importante mencionar que el equipo es transparente para la red. Es decir, no fue necesario cambiar configuraciones en el resto de los dispositivos, ya que el administrador es invisible para ellos.

Una vez instalado el equipo se comenzó a trabajar en la configuración de políticas de calidad de servicio.

La Universidad reparte el ancho de banda contratado a los proveedores de servicios de acuerdo a las necesidades de cada Departamento. La velocidad contratada por cada unidad académica o administrativa posee un costo de \$17.000 por cada Mbps [34]. Cabe mencionar, que solo se vende

el ancho de banda internacional, ya que el nacional e Internet2 no posee un costo para la Universidad debido a convenios con proveedores de servicio y REUNA.

A continuación, en la tabla 1, se presenta un listado con el ancho de banda contratado por cada unidad.

Unidad	Ancho de banda internacional contratado [Mbps]
Arquitectura	7,0
Ciencia de Materiales	3,0
Defider	2,0
Electricidad	4,0
Electrónica Pregrado	5,0
Electrónica Postgrado	5,0
Electrónica Profesores	7,0
E. Humanísticos	2,0
Física	7,0
Industrias	11,0
Industrias VideoConferencia	2,0
Informática	16,0
Matemática	5,0
Mecánica Profesores	1,5
Mecánica Labs	1,0
Mecánica Servidores	1,5
Obras Civiles	2,0
Obras Civiles Labs	2,0
Procesos Químicos Profe	4,0
Procesos Químicos Labs	3,0
Química	3,0
Ing. Diseño Productos	5,0
3ie	7,0
Biotecnología	5,0
Casa Bari Magister	2,0
CIMA	3,0
CASIM Jorge Pontt	2,0
CMITT	6,0
Rectoría	4,0
VRA	2,0
DGD	2,0
CIAC + Museo	2,0
VREA	4,0
DGAF	2,0
DDC	2,0
D.Infraestructura	2,0
DGC	4,0

DCSC Office	5,0
DCSC_Desarrollo	4,0
DCSC_Soporte	5,0
SIGA servers	10,0
DGIP	2,0
DGPD	2,0
DGAT	6,0
Biblioteca	4,0
Dir. Estudios	2,0
RRHH	2,0
RREE	2,0
DESCAD	3,0
Movilización Bari	2,0
DIRSAC CentroEventos	3,0
DIRSAC Campus	2,0
VREA - Sansanet	4,0
Alumnos Organizaciones	2,0
Feutfsm	2,0
DCSC Lab	10,0
Sede Viña del Mar	21,0
Sede Concepción Profesores	10,0
Sede Concepción Labs	5,0
Campus Santiago Vitacura Labs1	5,0
Campus Santiago Vitacura Labs2	5,0
Campus Santiago Vitacura Profes	10,0
Campus Santiago Vitacura Salas	2,0
Campus Santiago SJ Labs INF	16,0
Campus Santiago SJ Labs	5,0
Campus Santiago SJ Profes	13,0

Tabla 1: ancho de banda contratado por cada unidad

Dado que el principal criterio para repartir el ancho de banda es la velocidad contratada por cada departamento, la implementación de las políticas de administración de ancho de banda del equipo *ALLOT* se llevó a cabo siguiendo estos mismos parámetros. Luego de 1 mes de recolección de datos para conocer el verdadero estado de la red, se crearon reglas específicas para priorizar el tráfico de ciertas aplicaciones.

Cabe volver a enfatizar que la administración del ancho de banda es una actividad permanente. Por lo tanto, si bien en este Capítulo se describen las políticas creadas en el marco de este trabajo de título, estas deben ser revisadas constantemente para ser actualizadas según sean los requerimientos futuros. Por este motivo, la implementación aquí descrita solo representa la configuración inicial del equipo.

5.1. Configuración de políticas de QoS

Para crear las distintas políticas que deben ser configuradas en el administrador se debe seguir una serie de pasos. A continuación se describe cómo se realizó la creación de líneas, tuberías y canales virtuales así como sus respectivas reglas de *QoS* y *DoS* en el administrador de ancho de banda.

5.1.1 Líneas

Se crearon 4 líneas en el administrador de ancho de banda, cada una de ellas corresponde a una segmentación virtual del enlace físico provisto por el proveedor de servicios de Internet. Se separaron 4 tipos de tráfico: el tráfico interno de la universidad, el tráfico nacional, el internacional y el tráfico dirigido desde y hacia redes académicas de Internet2. Para esto se utilizó una funcionalidad del *NetXplorer* llamada *Country Classification* que posee una base de datos con los rangos de direcciones IP asignado a cada país del mundo. Si bien esta información no es 100% confiable debido a la reventa de direcciones IP entre distintas ISP a nivel mundial, es una buena referencia para realizar la clasificación de tráfico, especialmente para el tráfico nacional.

La línea a cargo del tráfico interno de la universidad se configuró de manera tal que el origen y destino del tráfico corresponda a cualquiera de las redes de la universidad, considerando tanto direcciones públicas como privadas. De esta forma, todo tráfico que sea originado desde una dirección de la universidad y que tenga como destino otra dirección de la universidad, será ingresado a esta línea.

El tráfico nacional fue configurado en una línea que posee como destino todo el tráfico hacia el país Chile utilizando el *Country Classification*. Es importante recordar que el equipo permite definir el sentido de la conexión, en esta implementación el tráfico es trabajado en forma bidireccional, es decir, si el tráfico proviene desde la red interna hacia páginas nacionales, este será tratado como tráfico nacional. Lo mismo ocurre si el tráfico es originado desde sitios nacionales hacia la red interna de la Universidad.

Para la direcciones de Internet2 se resumieron las tablas *BGP* [35] del router de borde de la universidad. Estas direcciones IP fueron asignadas al país Islas Salomón. De esta forma, se creó una línea para el tráfico de Internet2 que tiene como destino todo el tráfico hacia las Islas Salomón utilizando el *Country Classification*. Para mayor compresión para el administrador, luego se cambió el nombre del país Islas Salomón a Internet2.

El tráfico internacional corresponde a la última línea que tiene configurado el origen y destino del tráfico en *ANY*, es decir, si un tráfico no es catalogado como interno, tráfico nacional o hacia internet2, será categorizado como internacional.

La información de las líneas creadas se puede observar en la figura 23.

Identification	Conditions							Actions	
	Name	Alarms A...	In Use	Internal	Direction	External	Service	Time	Access
 Trafico DMZ a interno			☒	REDUSM_2		REDUSM_2	All IP	Anytime_1385095416...	Accept
 Trafico Nacional			☒	Any		Chile	All IP	Anytime_1385095416...	Accept
 Trafico Internet 2			☒	Any		Internet2	All IP	Anytime_1385095416...	Accept
 Trafico Internacional			☒	Any		Any	All IP	Anytime_1385095416...	Accept
 Fallback			☒	Any		Any	All Service	Anytime_1385095416...	Accept

Ilustración 23: Líneas creadas en el NetXplorer.

En la última columna de la Figura 26 se especifica la regla de QoS asociada a cada línea. En el caso del tráfico interno se mantuvo la regla por omisión, es decir, el tráfico no es priorizado. Como el tráfico cursado hacia los servicios internos es bajo, no se consideró necesario crear una regla especial para esto. Para el caso de la línea nacional, la universidad tiene contratada una velocidad de 300 Mbps, por este motivo se creó una regla (llamada “Línea nacional”) que tiene configurado un ancho de banda mínimo de 300 Mbps para asegurar que siempre se trate de utilizar el máximo ancho de banda disponible.

La regla de ancho de banda para el tráfico nacional se muestra a continuación en la figura 24.

Line Enhanced QoS Entry Properties

Name: Linea nacional

Description:

Line Based QoS Coverage:

Inbound and Outbound Defined the Same

Inbound and Outbound

Minimum Bandwidth (Kbps): 300000

Maximum Bandwidth:

☒ Maximum Allowed
☐ in Kbps:

☒ Priority (Best Effort)
☐ Priority (1 Lowest, 4 Highest) 4

If Minimum Line Bandwidth not Allocated:

Admit by Priority

Save

Reset

Cancel

Ilustración 24: Regla de QoS para el tráfico nacional.

Al igual que la línea del tráfico interno, la línea de Internet2 está configurada con la regla por omisión de QoS ya que el tráfico hacia redes internas es pequeño (no supera los 10 Mbps) y no necesita ser administrado.

El caso de la línea de tráfico internacional, se creó una regla (llamada “Tráfico internacional”) que tiene configurado un ancho de banda mínimo de 150 Mbps, que es la velocidad contratada por la universidad.

A continuación, en la figura 25 se aprecia la regla de ancho de banda creada para el tráfico internacional.

The screenshot shows a window titled "Line Enhanced QoS Entry Properties". It contains several input fields and a "Save" button. The "Name" field is filled with "Tráfico internacional". The "Description" field is empty. The "Line Based QoS Coverage" dropdown menu is set to "Inbound and Outbound Defined the Same". Below this, there is a section for "Inbound and Outbound" settings. The "Minimum Bandwidth (Kbps)" is set to 150000. The "Maximum Bandwidth" section has two radio buttons: "Maximum Allowed" (selected) and "in Kbps" (unselected). The "Priority" section has two radio buttons: "Priority (Best Effort)" (selected) and "Priority (1 Lowest, 4 Highest)" (unselected). The "If Minimum Line Bandwidth not Allocated" dropdown menu is set to "Admit by Priority". At the bottom right, there are three buttons: "Save", "Reset", and "Cancel".

Ilustración 25: Regla de QoS para el tráfico internacional.

Con la definición de estas 4 líneas fue posible catalogar todo el tráfico que se cursa en la Universidad para darle el tratamiento que corresponde según sea el destino (u origen, según el punto de vista, se recuerda que el tráfico es tratado de forma bidireccional) de este.

5.1.2 Tuberías

La configuración de tuberías tiene por finalidad cumplir con los requerimientos de ancho de banda de cada unidad (departamento) de la universidad. Por esta razón que la estructura de las tuberías con iguales para el tráfico nacional e internacional, cambiando solo las reglas de ancho de banda de cada una de ellas.

Debido a que el anterior administrador de ancho de banda solo permitía limitar el máximo tráfico generado por una unidad, la universidad solo cobraba (internamente, a sus unidades) por el máximo ancho de banda que le asegura a cada unidad. Como el nuevo administrador de ancho de banda permite además limitar el mínimo ancho de banda, se realizó un cambio en el modelo de cobro de ancho de banda. El nuevo modelo de cobro implementa un costo distinto para los

departamentos dependiendo si contratan ancho de banda internacional dedicado o compartido. Como dedicado se entiende al ancho de banda mínimo configurado en la regla de ancho de banda, compartido se refiere al máximo. En el período de prueba del nuevo modelo de cobro, 2 unidades fueron contactadas para testear esta nueva modalidad (Departamento de Informática y el Instituto 3ie). El departamento de informática pagó para tener garantías de un ancho de banda mínimo de 10 Mbps y aumentó a 26 Mbps el máximo. En el caso del Instituto 3ie, pagó por 2 Mbps de ancho de banda mínimo y aumentó a 7 Mbps el máximo.

Al resto de las unidades se les asignó un mínimo de 300 Kbps y se mantuvo el máximo que ya tenían contratado. La excepción fueron las reglas para equipos de video conferencia, las cuales fueron configuradas con un mínimo de 1 Mbps. El detalle de la nueva asignación de ancho de banda a cada unidad se encuentra en la Tabla 2.

Unidad	Ancho de banda máximo [Mbps]	Ancho de Banda mínimo [Mbps]
Arquitectura	7,0	0,3
Ciencia de Materiales	3,0	0,3
Defider	2,0	0,3
Electricidad	4,0	0,3
Electrónica Pregrado	5,0	0,3
Electrónica Postgrado	5,0	0,3
Electrónica Profesores	7,0	0,3
E. Humanísticos	2,0	0,3
Física	7,0	0,3
Industrias	11,0	0,3
Industrias VideoConferencia	2,0	1,0
Informática	26,0	10,0
Matemática	5,0	0,3
Mecánica Profesores	1,5	0,3
Mecánica Labs	1,0	0,3
Mecánica Servidores	1,5	0,3
Obras Civiles	2,0	0,3
Obras Civiles Labs	2,0	0,3
Procesos Químicos Profe	4,0	0,3
Procesos Químicos Labs	3,0	0,3
Química	3,0	0,3
Ing. Diseño Productos	5,0	0,3
3ie	7,0	2,00
Biotecnología	5,0	0,3
Casa Bari Magister	2,0	0,3
CIMA	3,0	0,3
CASIM Jorge Pontt	2,0	0,3

CMITT	6,0	0,3
Rectoría	4,0	0,3
VRA	2,0	0,3
DGD	2,0	0,3
CIAC + Museo	2,0	0,3
VREA	4,0	0,3
DGAF	2,0	0,3
DDC	2,0	0,3
D.Infraestructura	2,0	0,3
DGC	4,0	0,3
DCSC Office	5,0	0,3
DCSC_Desarrollo	4,0	0,3
DCSC_Soporte	5,0	0,3
SIGA servers	10,0	0,3
DGIP	2,0	0,3
DGPD	2,0	0,3
DGAT	6,0	0,3
Biblioteca	4,0	0,3
Dir. Estudios	2,0	0,3
RRHH	2,0	0,3
RREE	2,0	0,3
DESCAD	3,0	0,3
Movilización Bari	2,0	0,3
DIRSAC CentroEventos	3,0	0,3
DIRSAC Campus	2,0	0,3
VREA - Sansanet	4,0	0,3
Alumnos Organizaciones	2,0	0,3
Feutfsm	2,0	0,3
DCSC Lab	10,0	0,3
Sede Viña del Mar	21,0	1
Sede Concepción Profesores	10,0	1
Sede Concepción Labs	5,0	1
Campus Santiago Vitacura Labs1	5,0	1
Campus Santiago Vitacura Labs2	5,0	1
Campus Santiago Vitacura Profes	10,0	1
Campus Santiago Vitacura Salas	2,0	1
Campus Santiago SJ Labs INF	16,0	1
Campus Santiago SJ Labs	5,0	1
Campus Santiago SJ Profes	13,0	1

Tabla 2: Asignación de ancho de banda para las tuberías de cada unidad

Para identificar el tráfico generado por cada unidad se crearon grupos de máquinas en el catálogo con las direcciones IP de cada unidad. Estos datos pueden observarse en las Figuras 26 y 27, pero por motivos de seguridad no se entregará el detalle de las direcciones.

Identification		Conditions						Actions	
Name	Alarms A...	In Use	Internal	Direction	External	Service	Time	Access	Quality of Service
Trafico Nacional			Any		Chile	All IP	Anytime_1385095416...	Accept	Linea nacional
FET			USMFET		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
Liberados			Liberados_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
Radio			Radio server_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
MCU			MCU		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
VC Salon Honor			VC salon de ho...		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
HPC-INF			HPC_inf_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
CIAC-LAB			CIAC-LAB_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
LABP1			LABP1_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
LABP2			LABP2_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
VC-cruch			VC-cruch		Any	All IP	Anytime_1385095416...	Accept	Max6000-Min2000Prio2
VC-A1			VC-A1_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
VPN			VPN_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
BB-PublicServer			Publicserver_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
Salas DHCP			Salas DHCP_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
WIFI			Wifi_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
CCTVAL			CCTVAL_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
AEXA			AEXA_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
Admision			Admision_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
MSDN			MSDN_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS
ServerInside_28			ServerInside_2		Any	All IP	Anytime_1385095416...	Accept	Normal Pipe QoS

Policy: NE_3000 Catalog: Host Real-Time Monitoring

Ilustración 26: Tuberías creadas en la línea de tráfico nacional.

Identification		Conditions						Actions	
Name	Alarms A...	In Use	Internal	Direction	External	Service	Time	Access	Quality of Service
Liberados			Liberados_2		Any	All IP	Anytime_1385095416...	Accept	Liberados
Radio			Radio server_2		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min1000
MCU			MCU		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min1000
VC-ociv-SJ			VC ociv SJ		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min1000
VC-cruch			VC-cruch		Any	All IP	Anytime_1385095416...	Accept	Max6000-Min2000Prio2
VC-CTAM			VC-CTAM_2		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min1000
VC-A1			VC-A1_2		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min1000
VC Salon Honor			VC salon de ho...		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min1000
Centro Eventos			DIRSAC-centroe...		Any	All IP	Anytime_1385095416...	Accept	Max3000-Min300
HPC-INF			HPC_inf_2		Any	All IP	Anytime_1385095416...	Accept	Max1000-Min300
CIAC-LAB			CIAC-LAB_2		Any	All IP	Anytime_1385095416...	Accept	Max1000-Min300
LABP1			LABP1_2		Any	All IP	Anytime_1385095416...	Accept	Max10000-Min2000
LABP2			LABP2_2		Any	All IP	Anytime_1385095416...	Accept	Max20000-Min2000
VPN			VPN_2		Any	All IP	Anytime_1385095416...	Accept	Max5000-Min300
BB-PublicServer			Publicserver_2		Any	All IP	Anytime_1385095416...	Accept	Max1000-Min300
Salas DHCP			Salas DHCP_2		Any	All IP	Anytime_1385095416...	Accept	Max5000-Min1000
WIFI			Wifi_2		Any	All IP	Anytime_1385095416...	Accept	Max60000-Min20000
ServerInside_28			ServerInside_2		Any	All IP	Anytime_1385095416...	Accept	Max2000-Min300
server DMZ1			server DMZ1_2		Any	All IP	Anytime_1385095416...	Accept	Max10000-Min500
Server DMZ2			Servers DMZ2_2		Any	All IP	Anytime_1385095416...	Accept	RED DMZ
Server DMZ Inside			Server DMZ Insi...		Any	All IP	Anytime_1385095416...	Accept	Max5000-Min1000

Ilustración 27: Tuberías creadas en la línea de tráfico internacional.

Los servicios de la Universidad (web, directorio, DNS, correo, etc.) tienen creadas sus propias reglas con las direcciones IP correspondientes y ancho de banda asignado, pero por motivos de seguridad no se incluirán en esta memoria.

Una vez creadas las tuberías para dar cumplimiento a los requerimientos de ancho de banda de cada unidad se procedió a la creación de los canales virtuales.

5.1.3 Canales virtuales

Los canales virtuales permiten la configuración más detallada de un administrador de ancho de banda. En el caso de este trabajo de título, se crearon reglas para tratar los distintos tipos de tráfico que circulan por cada una de las tuberías creadas en las líneas de tráfico nacional e internacional. Estas reglas fueron creadas de acuerdo al tráfico que se considera aceptable por la Universidad, manifestado en la política de uso aceptable de recursos computacionales [26]. Dado que esta política no ha sido actualizada en los últimos años, fue necesario agregar una regla para priorizar tráfico hacia Youtube, dada la importancia que la plataforma de videos en línea tiene para usos académicos.

Las aplicaciones o protocolos a los que se les asignó prioridad son los siguientes.

- Youtube: Acceso hacia la red social de videos dado el alto material académico disponible en él.
- HTTP: El tráfico web es algo esencial dentro de cualquier institución.
- HTTPS: Tráfico web seguro a través de SSL.
- IMAPS, SMTP, POP3S, EXCHANGE y GMAIL: Son los protocolos utilizados por los servidores de correo electrónico de la universidad.

A todos estos protocolos se les asignó una prioridad de 1. Todo el resto de los protocolos tienen asignada la prioridad del canal virtual *Fallback* que está configurada como de mejor esfuerzo (*best effort*).

Los protocolos a los que se les denegó acceso son principalmente protocolos P2P, especialmente el uso de *BitTorrents*[36] y actualización de juegos de la empresa *Blizzard*. Estos protocolos fueron detectados como grandes consumidores de ancho de banda (y no alineados con la misión institucional) durante la recolección de datos.

A continuación, en la figura 28, se presenta una imagen de cómo están configurados los canales virtuales en el *NetXplorer*, se puede observar las reglas creadas con un nombre descriptivo, por ejemplo, el primer canal virtual le asigna una prioridad de 1 al tráfico de la aplicación Youtube.

Salas DHCP		✓	Salas DHCP_2	↔	Any	All IP	Anytime_1385095416...	Accept	Max5000-Min1000
Permit-Youtube		✓	Any	↔	Any	YouTube	Anytime_1385095416...	Accept	Default-Prioridad1
Permit-http		✓	Any	↔	Any	HTTP	Anytime_1385095416...	Accept	Default-Prioridad1
Permit-HTTPS		✓	Any	↔	Any	HTTPS	Anytime_1385095416...	Accept	Default-Prioridad1
permit-IMAPS		✓	Any	↔	Any	IMAPS	Anytime_1385095416...	Accept	Default-Prioridad1
Permit-smtp		✓	Any	↔	Any	SMTP	Anytime_1385095416...	Accept	Default-Prioridad1
permit-pop3s		✓	Any	↔	Any	POP3 SSL	Anytime_1385095416...	Accept	Default-Prioridad1
permit-exchange		✓	Any	↔	Any	MS Exchange	Anytime_1385095416...	Accept	Default-Prioridad1
permit-gmail		✓	Any	↔	Any	Gmail	Anytime_1385095416...	Accept	Default-Prioridad1
Block_torrent		✓	Any	↔	Any	BitTorrent	Anytime_1385095416...	Drop	Normal Virtual Channel QoS
Block_torrent2		✓	Any	↔	Any	BitTorrent Enc	Anytime_1385095416...	Drop	Normal Virtual Channel QoS
Block_torrent3		✓	Any	↔	Any	BitTorrent Torrent	Anytime_1385095416...	Drop	Normal Virtual Channel QoS
Block_torrent4		✓	Any	↔	Any	BitTorrent Tracker	Anytime_1385095416...	Drop	Normal Virtual Channel QoS
Block_torrent5		✓	Any	↔	Any	BitTorrentDHT	Anytime_1385095416...	Drop	Normal Virtual Channel QoS
Block_blizzardU		✓	Any	↔	Any	Blizzard Update	Anytime_1385095416...	Drop	Normal Virtual Channel QoS
Fallback		✓	Any	↔	Any	All Service	Anytime_1385095416...	Accept	Normal Virtual Channel QoS

Ilustración 28: Canales virtuales creados dentro de cada tubería.

De esta forma se prioriza el tráfico de aquellos protocolos que la universidad considera aceptable, se deniega el acceso a aquellos que no están alineados con la misión institucional y se deja que todo el resto de los protocolos compitan por ancho de banda (ya que están configurados con una prioridad de *best effort* dentro del canal virtual *Fallback*).

Con la configuración de los canales virtuales se dio por finalizada la configuración del equipo con el objeto de administrar el ancho de banda de forma eficiente para atender los requerimientos de los usuarios de la universidad.

A continuación se describe la configuración de políticas de seguridad creadas en el equipo para resguardar la disponibilidad e integridad de la red corporativa de la universidad.

5.1.4 Políticas ante ataques *DoS*

El administrador de ancho de banda *ALLOT* posee herramientas para controlar los ataques de denegación de servicios de la institución. Este tipo de ataque causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

La universidad es víctima de numerosos ataques de este tipo y muchas veces es la misma universidad la que ataca otros sitios, especialmente debido a equipos infectados dentro de la red. Estos ataques fueron estudiados en profundidad en la memoria de Fernanda Mattar [37], quien implementó políticas de seguridad en la DTI al mismo tiempo que se desarrollaba este trabajo de título.

Dicho estudio mostró que el ataque de tipo *DoS* con mayor impacto en la red de la institución se dirigía al servidor de la universidad que alojaba la mayoría de los sitios web institucionales de la universidad y sus departamentos. Estos ataques provocaban que la CPU del *firewall* principal de la universidad llegara al 100% de utilización, con lo que la red de la universidad quedaba sin conectividad. Estos ataques se producían en promedio 3 veces por semana, con una duración de un par de minutos en cada ocasión. Por este motivo se creó una regla que limita el número de conexiones hacia el servidor, la cual se puede observar en la Figura 29 y 30.

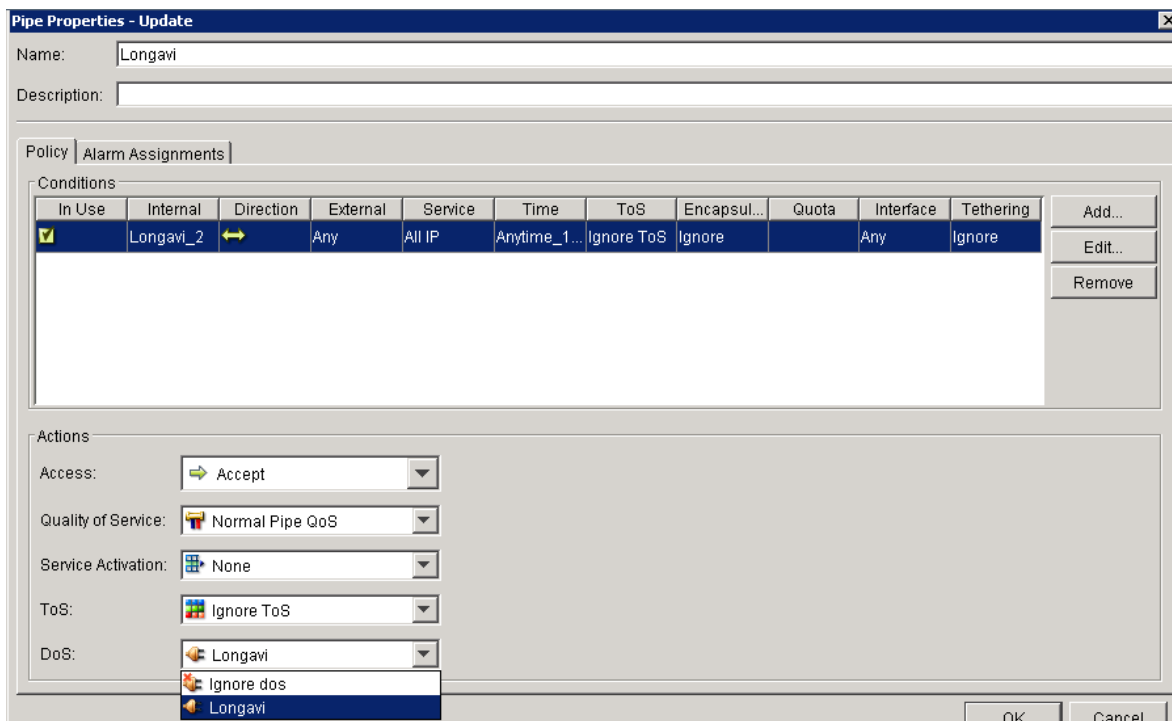


Ilustración 29: Regla creada para el principal servidor web de la Universidad.

Se observa la opción *DoS*, que permite escoger una regla que previene los ataques de este tipo, a continuación se presenta el detalle de esta regla.

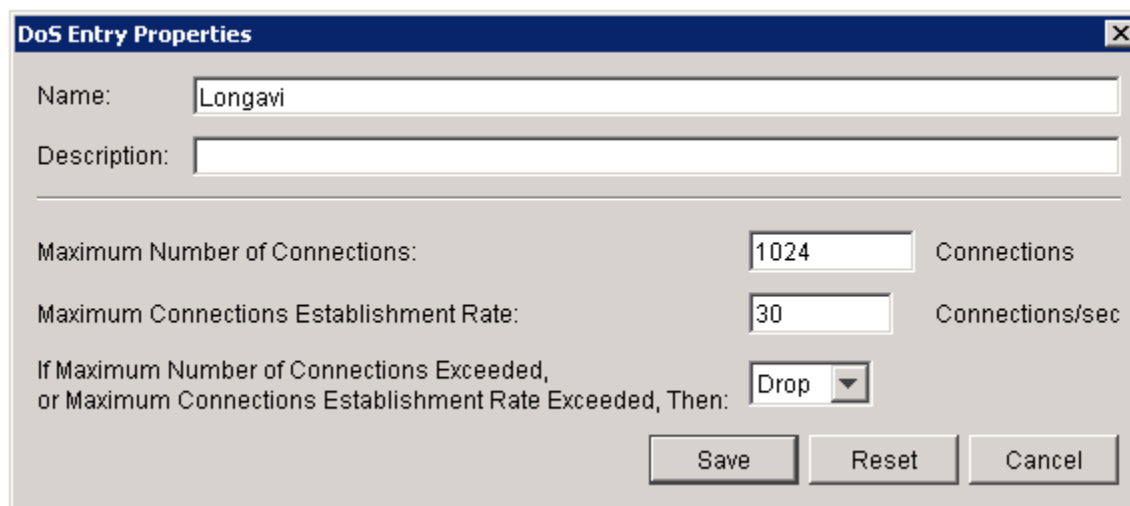


Ilustración 30: Configuración de la regla de DoS.

Esta regla se creó basada en la información entregada por el área de sistemas de la universidad, quienes después de monitorear el tráfico del equipo durante 2 semanas, identificaron el promedio de número de conexiones existentes en el equipo y la tasa de llegada de nuevas conexiones bajo condiciones normales de operación. Basándose en esta información, el número de conexiones como la tasa de llegada fueron limitadas a 1024 y 30 conexiones por segundo, respectivamente,

como se muestra en la ilustración 34. Al registrarse un ataque, el número de conexiones por segundo superaban las 25000.

En el siguiente capítulo se presentan los resultados obtenidos luego de haber implementado el nuevo sistema administrador de ancho de banda en la red corporativa de la universidad técnica Federico Santa María.

Capítulo 6: Resultados y gráficos

En este capítulo se reporta el impacto que el nuevo administrador de banda tiene en el servicio de red que ofrece la universidad. Los resultados se presentan por tipo de tráfico: interno, nacional, Internet2, internacional. También se presentan resultados acerca del tráfico de la red con acceso inalámbrico (WiFi) y el impacto que la nueva regla de manejo de ataques que producen denegación de servicio (DoS, Denial of Service) tiene sobre el sistema.

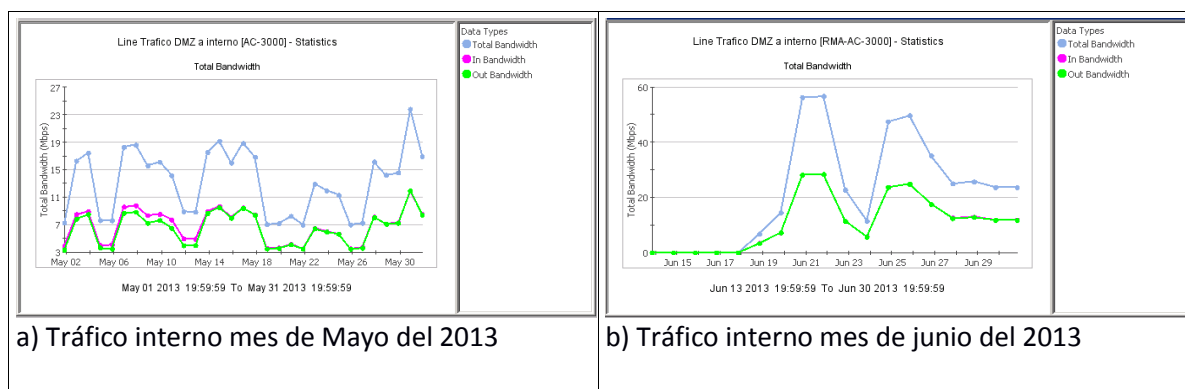
Cabe mencionar que como el antiguo administrador de ancho de banda no permitía separar el tráfico según el destino, muchas de las siguientes secciones no incluyen un gráfico con el rendimiento anterior ya que no existía forma de capturar estos datos.

Todos los datos presentados en esta sección fueron recolectados durante los meses de mayo, junio, julio y agosto del presente año 2013, a excepción de los datos sobre la red con acceso inalámbrico (WiFi), cuyos datos corresponden a los primeros días de diciembre del 2013.

6.1. Tráfico interno

6.1.1 Análisis entre los meses de mayo a agosto del 2013

Una de las principales características del *NetXplorer* es que permite almacenar datos históricos de la red. De esta forma es posible obtener estadísticas acerca del comportamiento de los usuarios en la red. En la Figura 31 se presentan los gráficos de uso de ancho de banda y clasificación por protocolo para los meses de mayo, junio, y agosto del año 2013.



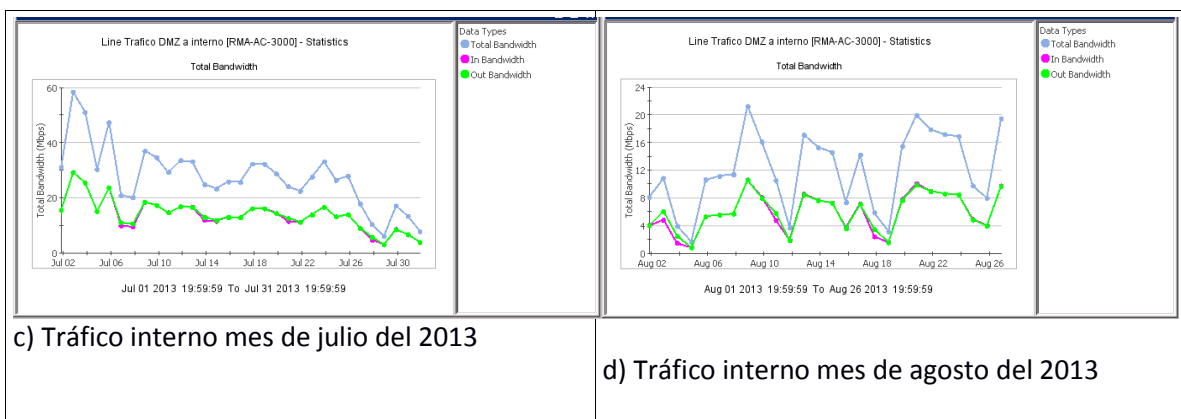
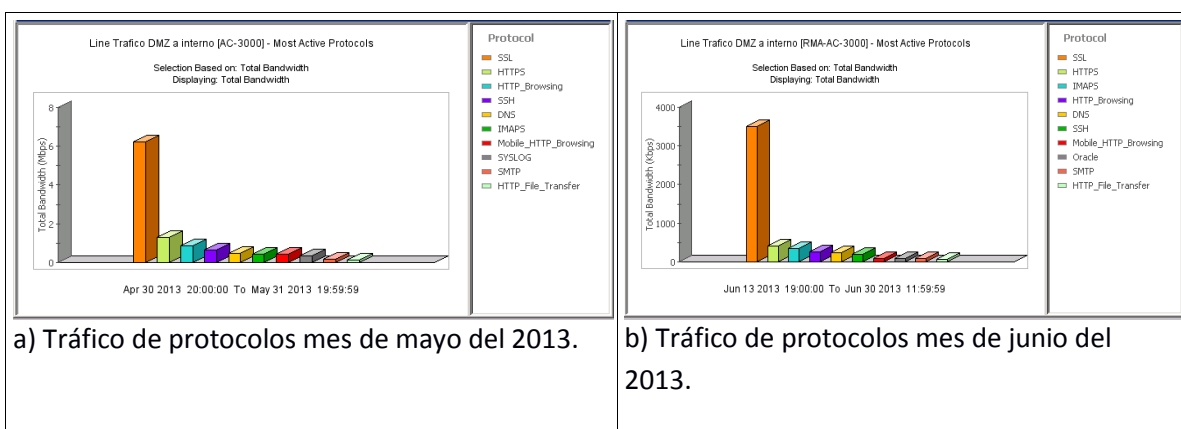


Ilustración 31: Tráfico interno durante los meses de mayo a agosto del 2013.

Se puede observar días con mayor tráfico que otros pero es normal dentro de una red de servicios, el ancho de banda disponible para esta red es de 1 Gbps, por lo que se reafirma la decisión de no administrar el ancho de banda de los servicios internos el tráfico ya que el tráfico nunca ha superado los 60 Mbps.

También se puede observar un ciclo semanal de consumo de ancho de banda, se observa claramente como baja considerablemente el tráfico durante los fines de semana. Los primeros días de junio, el administrador de ancho de banda fue sometido a una mantención, por lo que no es posible encontrar datos en ese periodo. Se aprecia que el tráfico de la red interna es simétrico, esto es esperable ya que en esta red se encuentran todos aquellos servicios académicos y administrativos, dentro de los cuales los usuarios cargan información (principalmente funcionarios) y descargan contenido (funcionarios y estudiantes).

La Figura 32 muestra el consumo de ancho de banda (en Mbps) de los distintos protocolos que se usan para prestar servicios informáticos al interior de la universidad entre los meses de mayo y agosto del 2013. La información de cuando ancho de banda trafica cada protocolo es nueva en la administración de red de la universidad, antes de la actual implementación, no existía un equipo que hiciera esto posible.



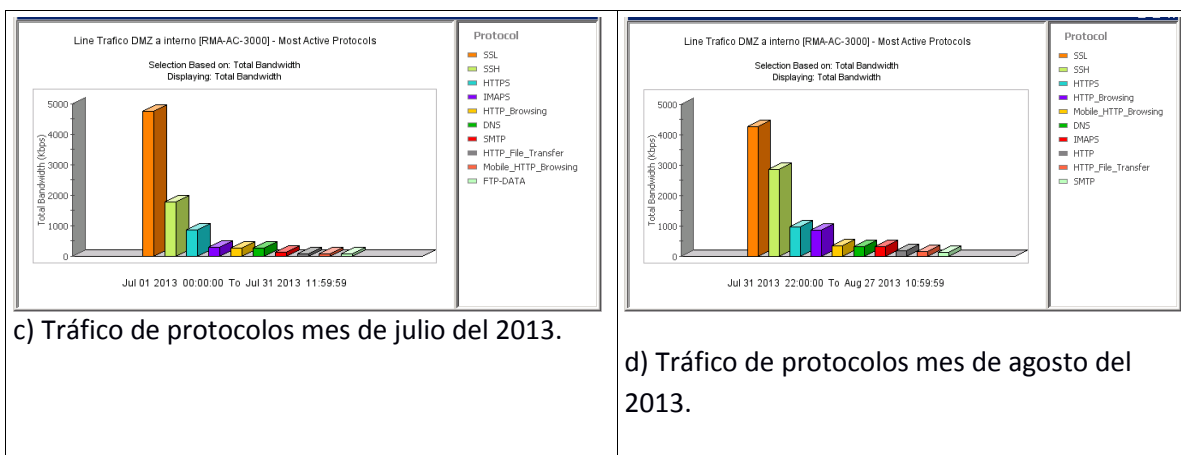


Ilustración 32: Protocolos del tráfico interno durante los meses de mayo a junio del 2013.

Se puede observar un comportamiento similar en los distintos meses respecto a los protocolos y cuando ancho de banda trafica cada uno de ellos. La principal conclusión de este gráfico es que el protocolo más utilizado en la red interna de la universidad es SSL, que es un protocolo criptográfico que proporciona comunicación segura a través de la red, muchos sistemas de la Universidad funciona de esta forma, algunos ejemplos son la plataforma SIGA y el equipo de datos financieros AS400. Otro protocolo importante es SSH, este protocolo es utilizado principalmente por la DTI de la universidad para mantener y actualizar sistemas, es por este motivo que el trafico SSH no tiene un comportamiento similar mes a mes, ya que depende de las labores que se deban hacer sobre los servidores, tales como actualizaciones o respaldos de información.

Esta información no se podía obtener anterior a la implementación del administrador de ancho de banda ALLOT.

6.2 Tráfico nacional

6.2.1 Análisis entre los meses de mayo a agosto del 2013

Al igual que la figura 32 la figura 33 nos muestra el tráfico de ancho de banda nacional cursado por los usuarios de la Universidad durante los meses de mayo a agosto del 2013.

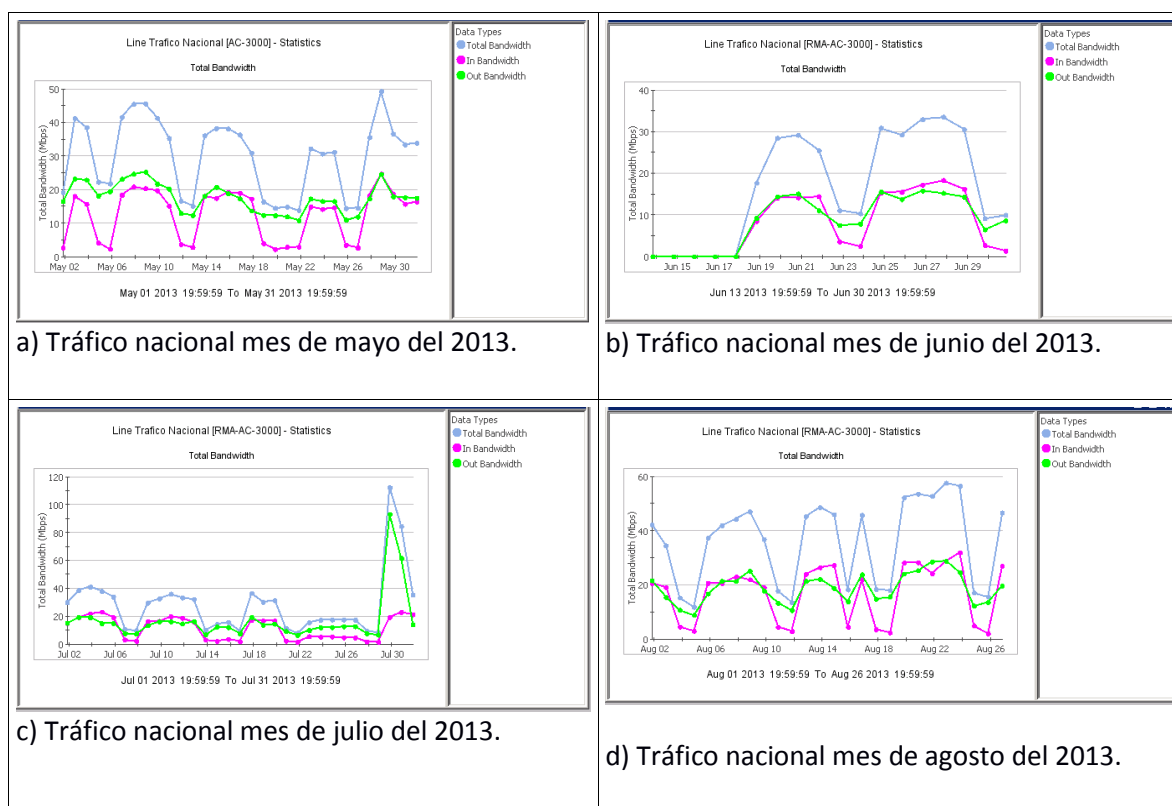


Ilustración 33: Tráfico nacional entre los meses de mayo a agosto del 2013.

Se puede observar que el comportamiento del tráfico nacional promedia los 20 Mbps, existiendo valores máximos de más de 120 Mbps. Esto afirma la propuesta de no administrar el ancho de banda del tráfico nacional ya que existen más de 400 Mbps disponibles. De todas formas se crearon todas las tuberías de cada unidad académica o administrativa de la universidad para poder monitorearlas por separada, tal como se explicó anteriormente.

Se observa que el tráfico nacional posee un alza de tráfico durante la mañana de cada día, alcanzando su máximo entre las 12:00 y las 14:00 horas aproximadamente, para luego decaer durante la noche. Durante los primeros días de junio no se obtienen gráficas dada la mantención que se le efectuó al equipo. Durante el mes de julio, se observa un gran salto en el tráfico nacional,

superando los 120 Mbps, si bien este es un comportamiento anormal, no es significativo a nivel de consumo de recursos, ya que aún ese consumo, existen 280 Mbps disponibles para el tráfico nacional.

A continuación, en la figura 34 se muestran el consumo de los protocolos más utilizados en sitios nacionales.

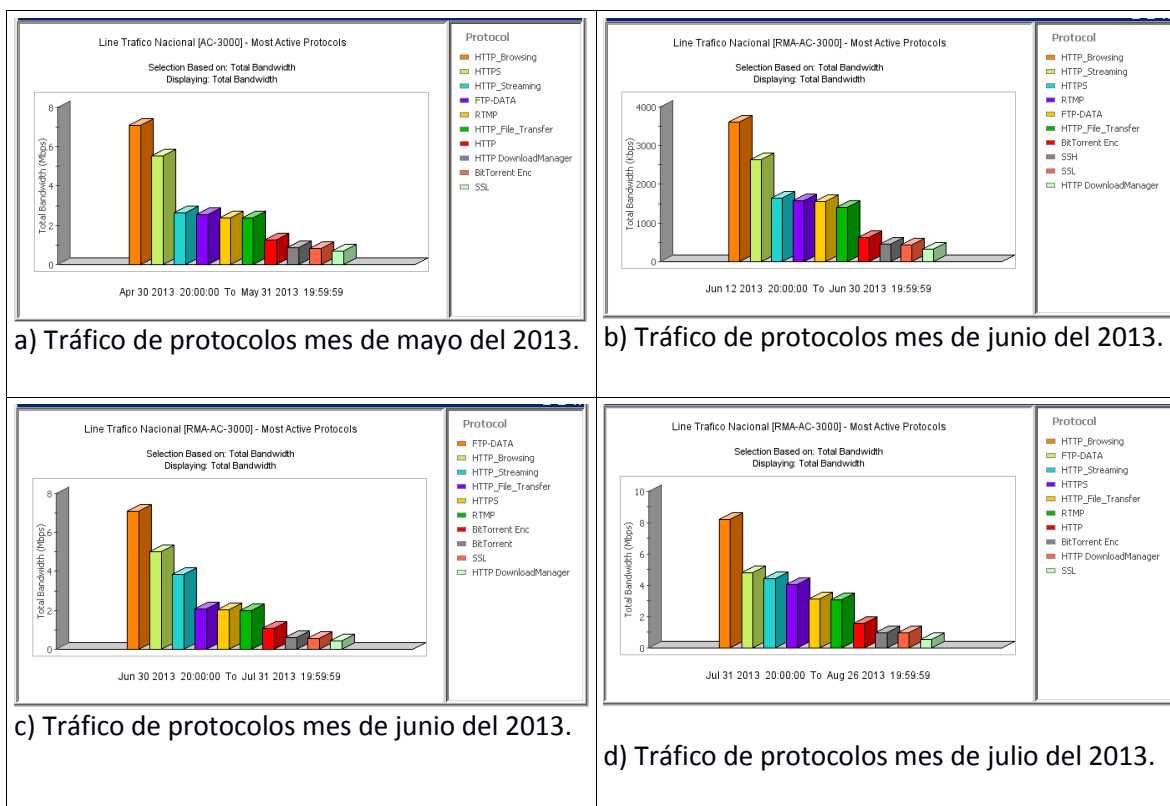


Ilustración 34: Protocolos del tráfico nacional durante los meses de mayo y agosto del 2013.

Se pueden observar los distintos protocolos que cursan tráfico nacional a través de la red de la universidad, es esperable el alto tráfico de navegación web y transferencia de archivos, pero se observa un tráfico considerable de *streaming* de datos, lo que es principalmente desde las redes de funcionarios que escuchan radios a través de internet. A pesar de esto, se reafirma el no administrar los protocolos del tráfico nacional, ya que el máximo consumo de ancho de banda que se ha registrado es de 120 Mbps y existe un ancho de banda disponible de más de 400 Mbps.

6.3 Tráfico Internet2

6.3.2 Análisis entre los meses de mayo a agosto del 2013

A continuación se presentan 4 gráficos en la figura 35, que muestran el tráfico realizado durante los meses de mayo a agosto del 2013 hacia y desde redes académicas.

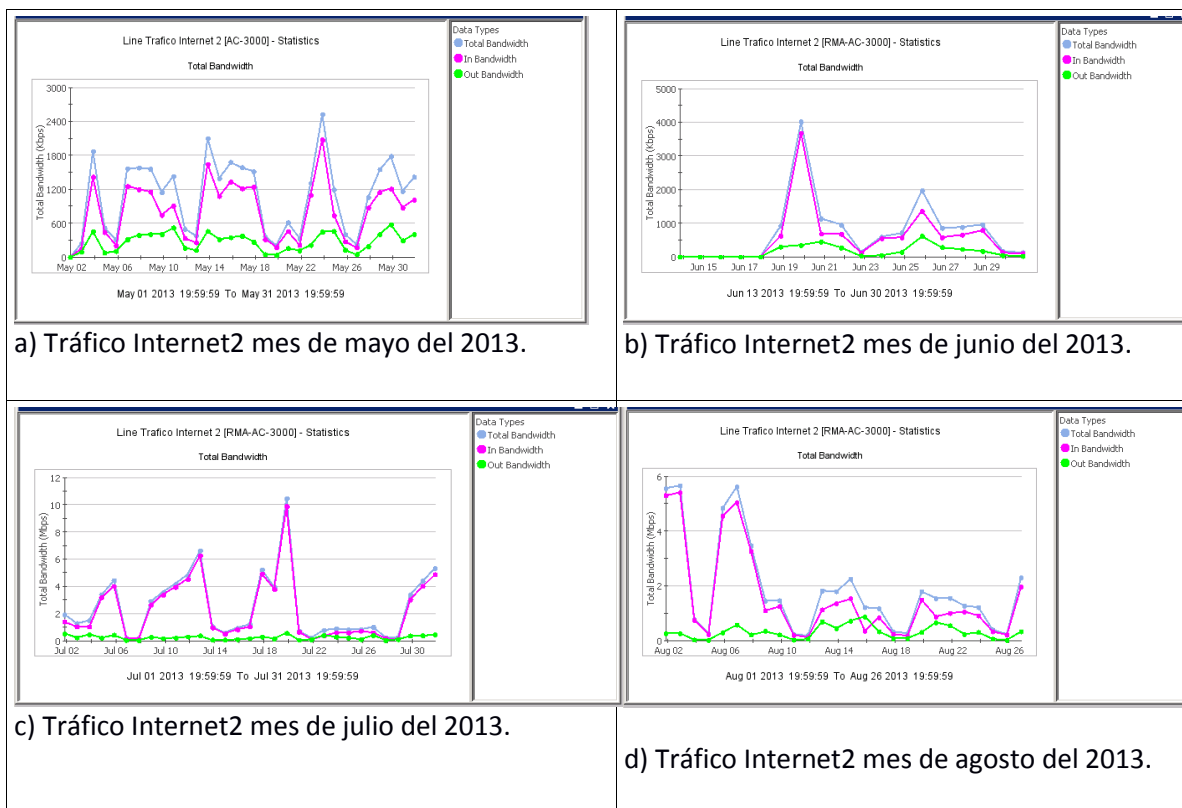


Ilustración 35: tráfico hacia redes académicas entre los meses de mayo a agosto del 2013.

Se puede observar que el tráfico cursado hacia redes académicas promedia los 2 Mbps, alcanzando máximos de hasta 6 Mbps. El consumo de ancho de banda es pequeño dado que los requerimientos hacia estas redes también lo es, a continuación, en la figura 36 podremos ver cuáles son aquellos protocolos que trafican por estas redes académicas durante los meses de mayo a agosto del 2013.

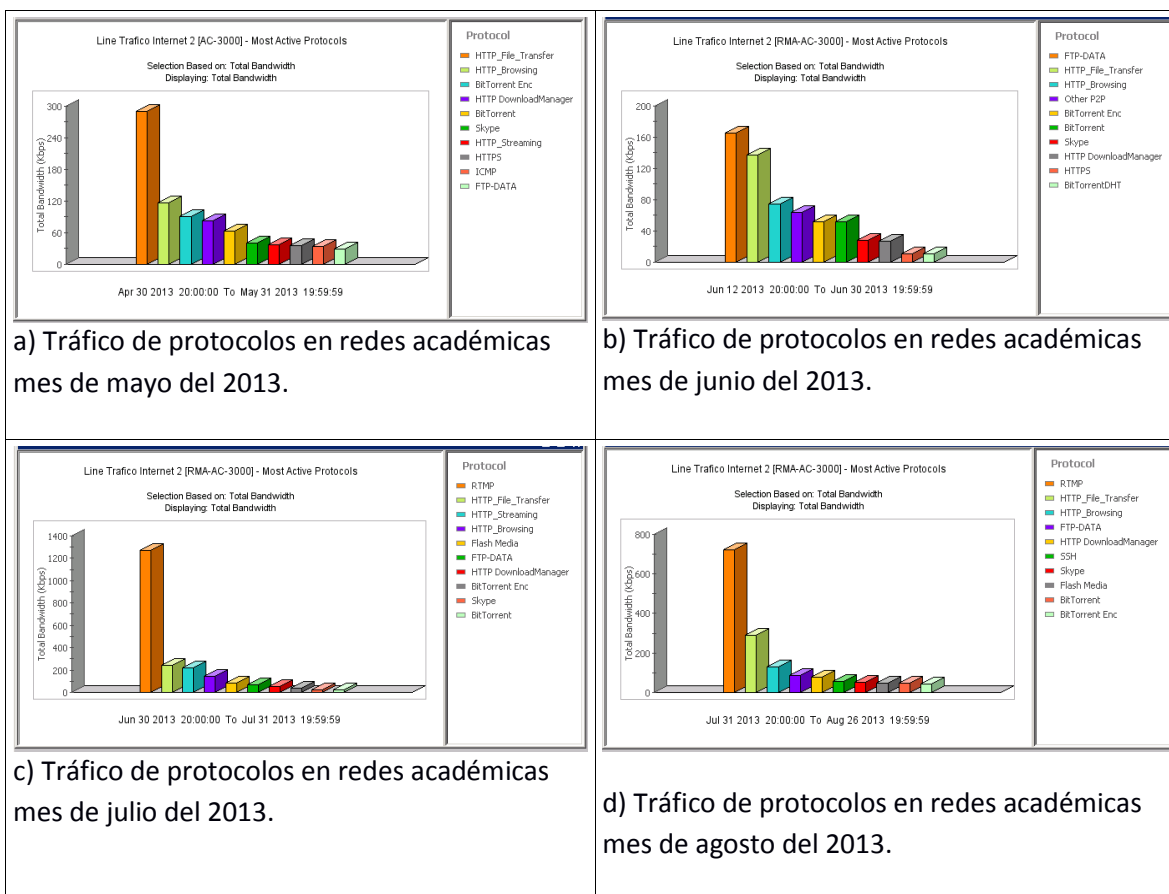


Ilustración 36: Protocolos traficando hacia redes académicas entre los meses de mayo a agosto del 2013.

Se observa que principalmente se trafican datos de navegación web, transferencia de archivos y aplicaciones de tiempo real, algo esperable de redes académicas. Si bien el comportamiento del tráfico no es igual a lo largo del tiempo, el ancho de banda utilizado por cada protocolo es bajo y no necesita ser administrado.

6.4 Tráfico Internacional

Dado que es el tráfico internacional es el que posee más requerimientos de ancho de banda y además es el más costoso, se realizará un análisis más detallado.

6.4.1 Análisis diario

A continuación, en la figura 37 se muestra el gráfico de tráfico internacional durante los días 20 al 26 de agosto del 2013.

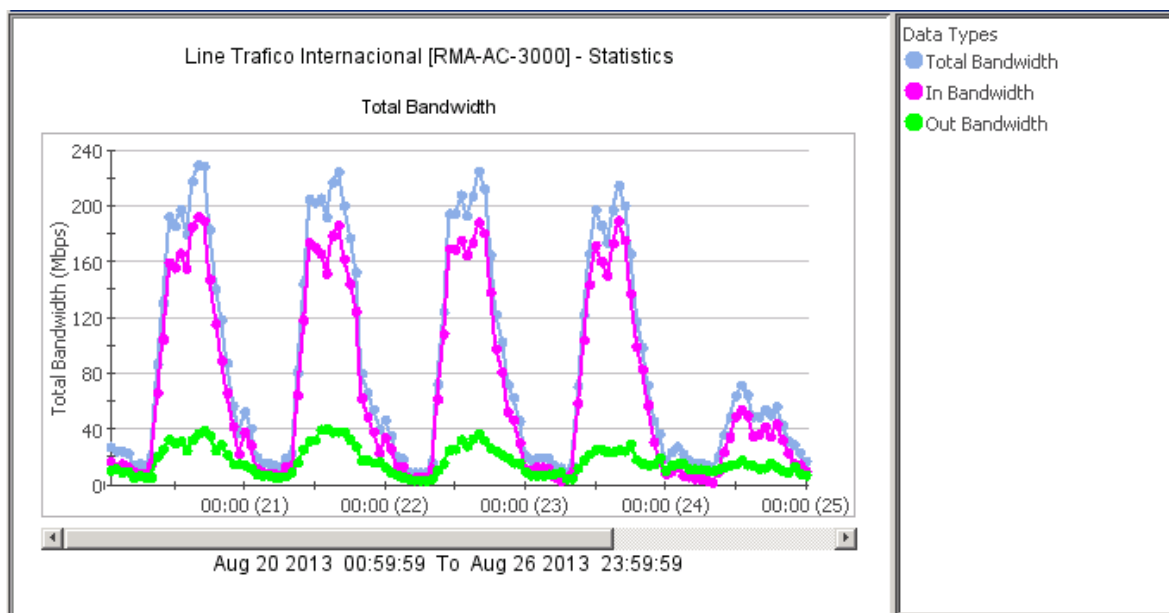


Ilustración 37: Tráfico internacional entre los días 20 a 26 de agosto del 2013.

A diferencia de los tipos de tráfico ya estudiados, en el caso del tráfico internacional se puede observar que el tráfico es principalmente de bajada. Es decir se descarga contenido desde internet. El hecho que el tráfico de subida sea pequeño en comparación al de bajada es esperable por la baja cantidad de servicios que presta la Universidad hacia el exterior.

Se puede observar claramente el tráfico de los usuarios durante los dias de semana, el cual mantiene el mismo comportamiento respecto a los otros días, a diferencia de los fines de semana, donde se nota una clara disminución del tráfico.

Se observa que el tráfico diario bordea los 240 Mbps y tal como se vio en la sección en que se describe la infraestructura de red de la universidad, oficialmente se posee un ancho de banda internacional de 150 Mbps, en las gráficas se observa un tráfico mayor que esto debido al enlace internacional de *Global Crossing*, que aporta 80 Mbps. Vale recordar que este enlace se encuentra en estado irregular dentro de la universidad y no fue calculado para efectos de repartición de ancho de banda.

A pesar de esto el gráfico nos indica que el tráfico atendido a los usuarios es de 240 Mbps cuando el máximo disponible oficialmente es de 150 Mbps. Esto afirma la decisión de si administrar el ancho de banda internacional de acuerdo a los requerimientos de cada unidad académica o administrativa de la universidad.

A continuación, en la figura 38 se muestran aquellos protocolos más utilizados durante los días 25 y 26 de agosto del 2013.

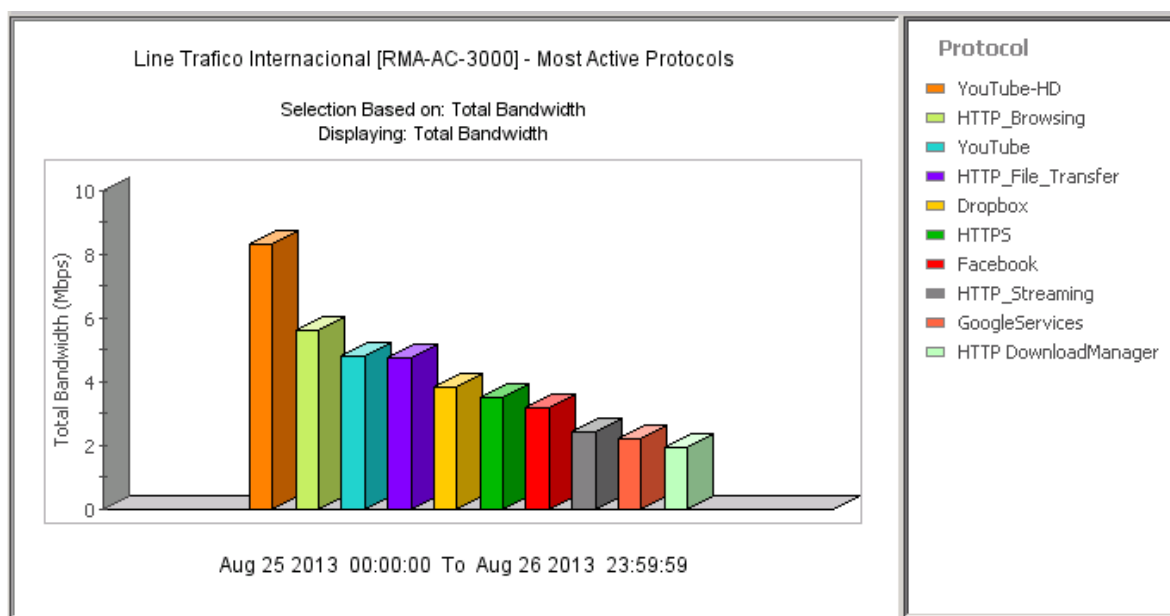


Ilustración 38: Análisis diario de protocolos traficando datos internacionalmente.

Se puede observar que se está priorizando el tráfico de los protocolos definidos como adecuados según la política de uso aceptable de recursos computacionales de la universidad. Se puede observar el alto tráfico que tiene Youtube, pero tal como se mencionó anteriormente, este es considerado un recurso académico, por lo que su tráfico es aceptado. A continuación se realizará el análisis mensual para comprobar que este comportamiento se mantiene.

6.4.2 Análisis entre los meses de mayo a agosto del 2013

A continuación, en la figura 39 se presentan los gráficos de tráfico internacional durante los meses de mayo y agosto del 2013.

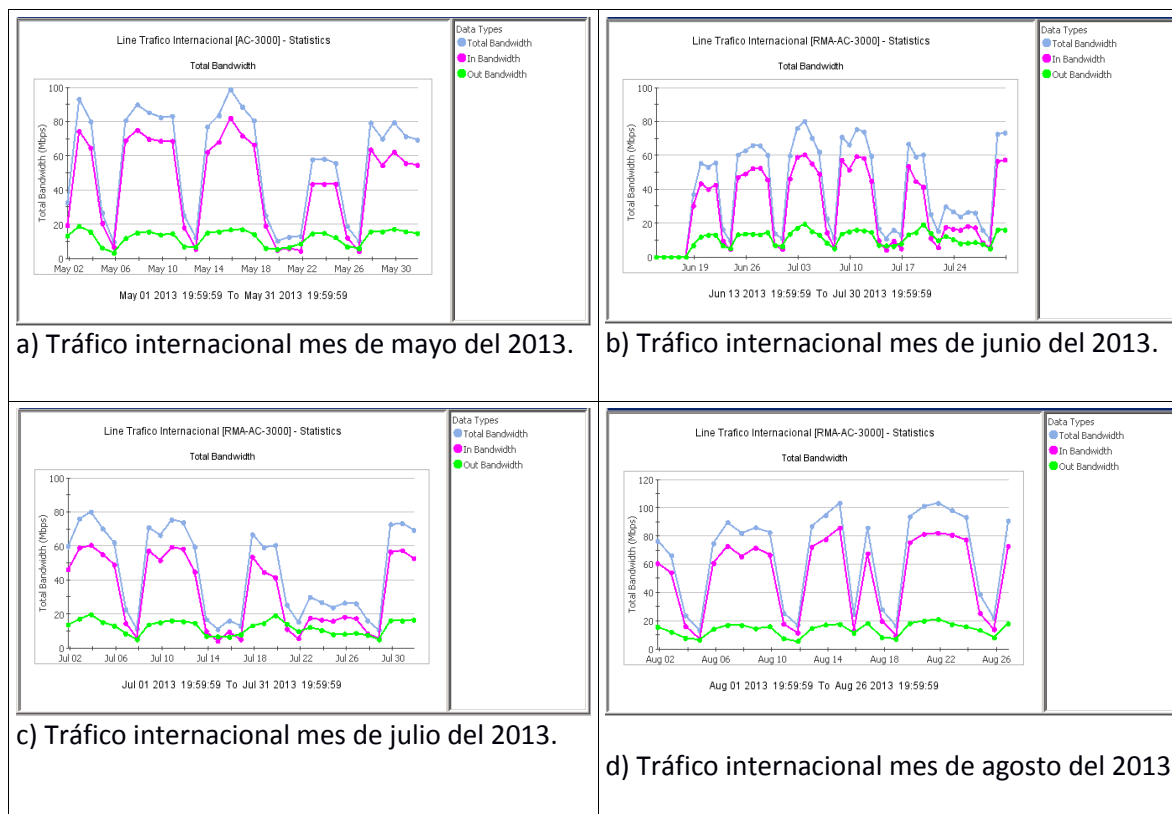


Ilustración 39: Tráfico internacional entre los meses de mayo y agosto del 2013.

Se puede apreciar que el tráfico alcanza máximos de 100 Mbps, pero si lo comparamos con el tráfico diario se puede determinar que este tipo de tráfico no es representativo para la toma de decisiones, ya que al ser diario, se toma un promedio del tráfico durante el día y la noche, por este motivo a continuación se mostrarán gráficos del uso durante el día del tráfico internacional. Esto no se realizó con las otras 3 líneas (Interno, Nacional e Internet2) ya que por sus consumos de ancho de banda son bajos respecto al ancho de banda disponible, por lo que no es necesario realizar un estudio profundo de estos tráficos, no es el caso del tráfico internacional que es el mas requerido y costoso.

A continuación, en la figura 40, se muestra el tráfico internacional diario, durante los días 25, 26 y 28 de noviembre y 2 de diciembre.

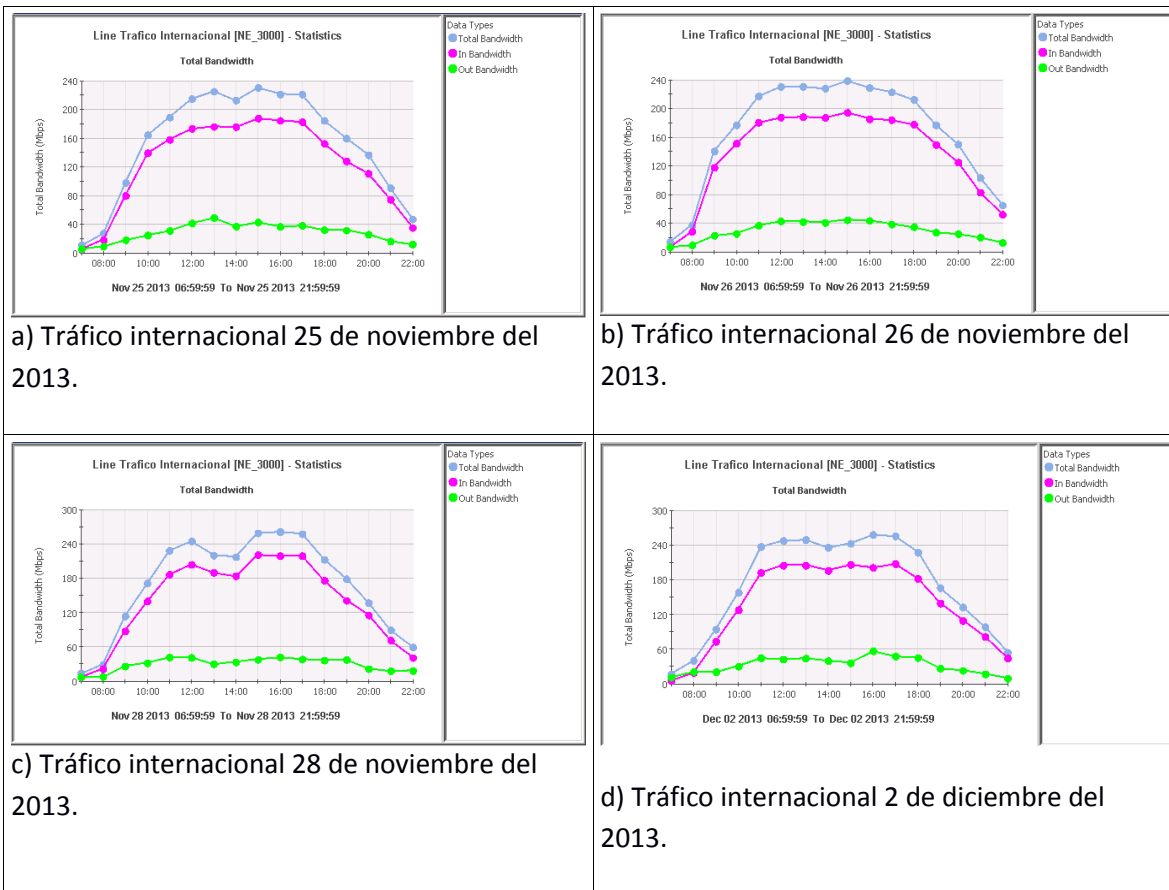


Ilustración 40: Tráfico internacional durante los días 25, 26, 28 de noviembre y 2 de diciembre del 2013.

Con estos gráficos se puede asegurar cuanto es el ancho de banda consumido día a día en la universidad, se observa que el administrador de ancho de banda cumple su función de maximizar el consumo de ancho de banda según sean los requerimientos de la red. Se observa que durante las 11:00 y 17:00 existe el mayor consumo de tráfico diario, a excepción de la hora de almuerzo entre las 12:00 a 14:00, el cual promedia los 240 Mbps.

Esto nos indica que se están atendiendo los requerimientos de los usuarios, pero no es posible conocer cuántos requerimientos no pueden ser atendidos debido a que se está utilizando el máximo ancho de banda disponible.

La Figura 41 muestra el número de requerimientos que no son atendidos debido a que no quedan recursos de ancho de banda disponibles para entregar.

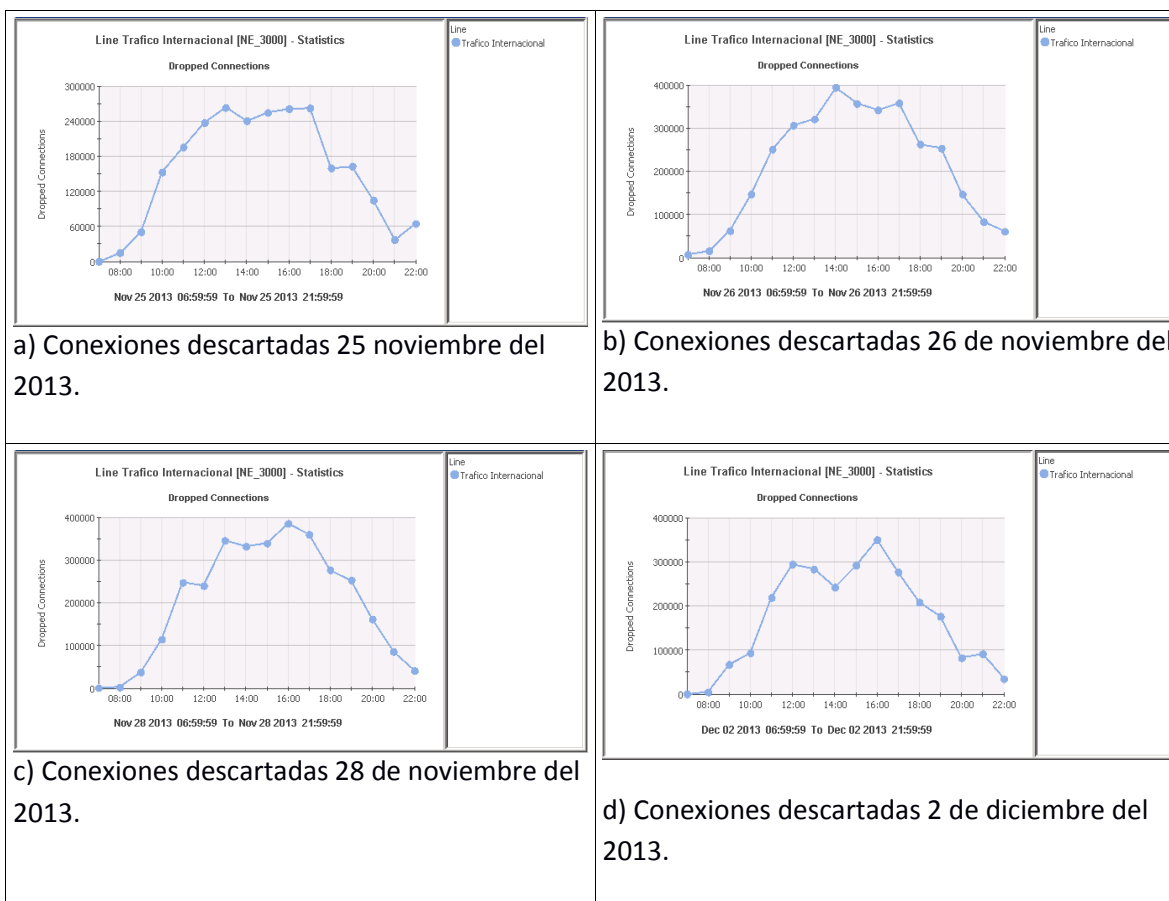


Ilustración 41: Conexiones descartadas en la línea de tráfico internacional.

Se puede observar un gran número de conexiones descartadas, especialmente durante las 12:00 y 17:00 que es el rango de tiempo en que se utiliza todo el ancho de banda disponible, es decir, hay una gran cantidad de tráfico de usuarios que es descartado porque no hay recursos de ancho de banda disponibles. Se utilizaron los datos del mes de noviembre y diciembre ya que son datos actualizados y presentan mayor valor que gráficas de mediado de año. A pesar de estas, el comportamiento, tanto de protocolos, consumo y descarte de paquetes se ha mantenido desde el mes de mayo hasta el diciembre del 2013, por lo que es válido utilizar esta información.

A continuación veremos los principales protocolos que se trafican hacia sitios internacionales, de esta forma se podrá saber si es necesario cambiar las políticas de calidad de servicio o la administración del ancho de banda se está realizando de forma correcta, pero es imposible atender los requerimientos de los usuarios de la universidad con la actual velocidad contratada a los proveedores de servicio de Internet.

Esto se aprecia en la figura 42, que muestra el tráfico internacional provocado por los principales protocolos utilizados por usuarios de la Universidad.

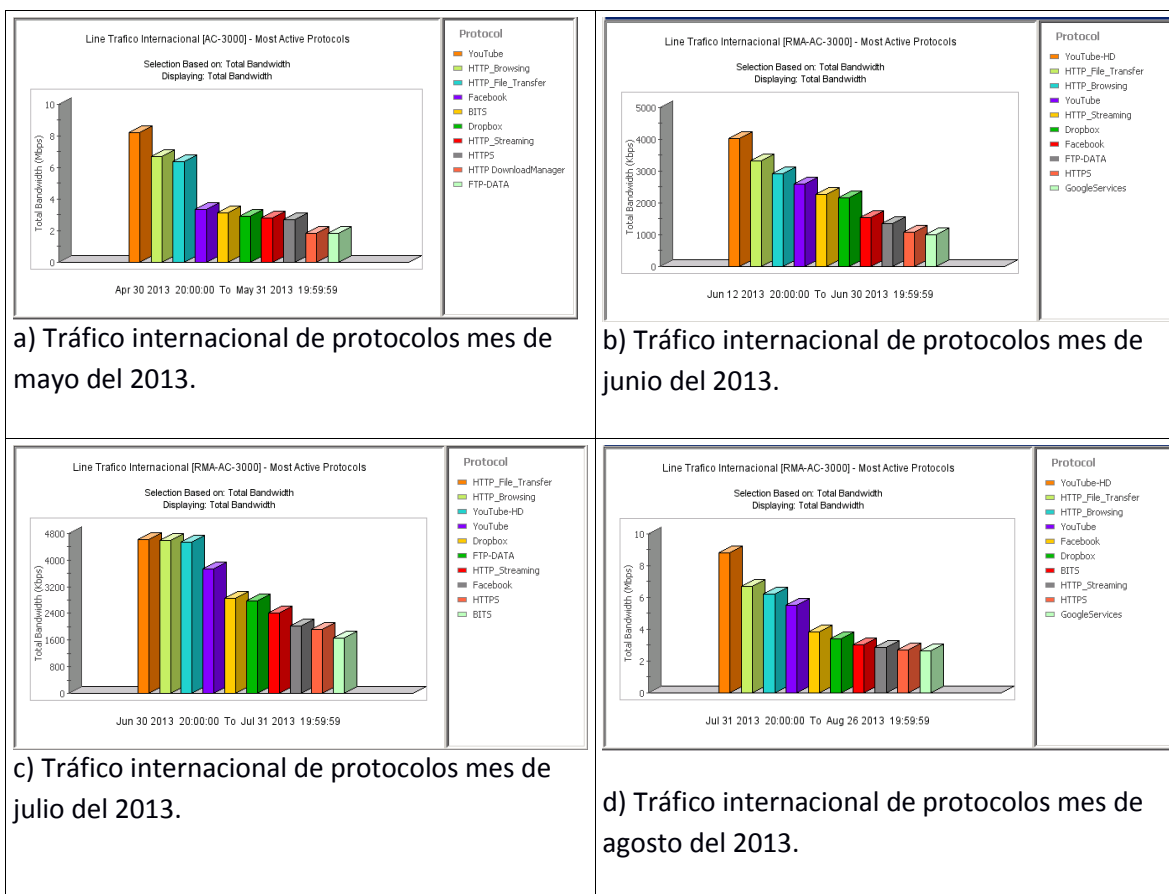


Ilustración 42: Protocolos traficando hacia redes internacionales entre los meses de mayo a agosto del 2013.

Se observa que la priorización de protocolos definida según la política de uso aceptable de recursos computacionales funciona de manera correcta, es decir se está asignando ancho de banda a cada servicio según como lo han determinado las autoridades de la universidad. Esto quiere decir que es necesario aumentar la velocidad hacia sitios internacionales contratada a los proveedores de servicio de Internet, esto se realizará una vez que el nuevo modelo de cobro de ancho de banda se encuentre operativo.

6.5 Tráfico de redes WiFi.

Dado la importancia de este servicio y como la satisfacción de la mayoría de usuarios de la red de la universidad depende del acceso inalámbrico a la red (WiFi), principalmente estudiantes, se muestra el consumo de ancho de banda y los protocolos más utilizados por estas redes.

A continuación, en la figura 43, se muestra el tráfico cursado por las redes inalámbricas en la Universidad.

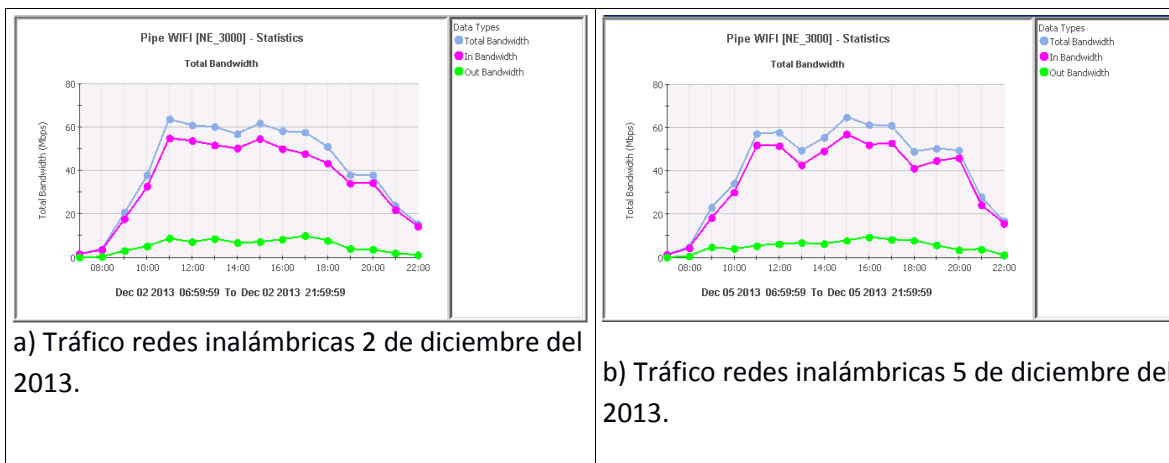


Ilustración 43: Tráfico cursado por redes inalámbricas el día 2 y 5 de diciembre del 2013.

Esta red tiene asignado un mínimo de 20 Mbps y un máximo de 60 Mbps. Se puede observar que durante las 09:00 y las 17:00 horas se trafica al límite de lo permitido para la red, existiendo ocasiones que el administrador le permite navegar a una velocidad mayor a su permitida, esto quiere decir que presenta una gran cantidad de requerimientos de ancho de banda, esto lo comprobaremos observando aquellas conexiones descartadas, lo que se observa en la figura 44.

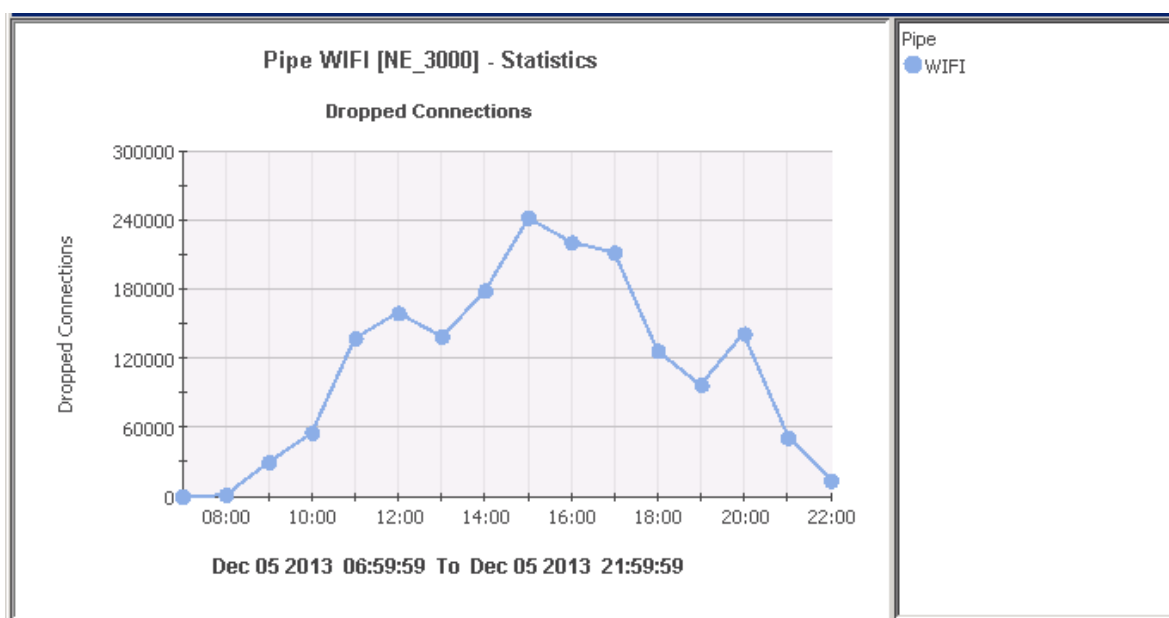


Ilustración 44: Conexiones descartadas para las redes inalámbricas el día 5 de diciembre del 2013.

Se observa que existen un alto número de conexiones que son descartadas, es decir, el requerimiento de ancho de banda es más grande que los recursos asignados. A pesar de esto no es posible modificar la regla aumentando los recursos asignados a este tipo de conexión, ya que como se vio anteriormente, todos los recursos disponibles para el tráfico internacional están asignados y hay una gran cantidad de conexiones que no son posibles de atender por no existir ancho de banda disponible.

6.6 Reglas de DoS.

La universidad es víctima de ataques *DoS* de manera regular. Esto que provoca la interrupción del servicio hacia internet y servicios locales. A continuación veremos el impacto de haber aplicado una regla para controlar el número y tasa de nuevas conexiones hacia el principal blanco de ataques dentro de la universidad.

En la figura 45, se muestran el número de conexiones descartadas gracias a la regla que limita las conexiones hacia el servidor que era atacado constantemente.

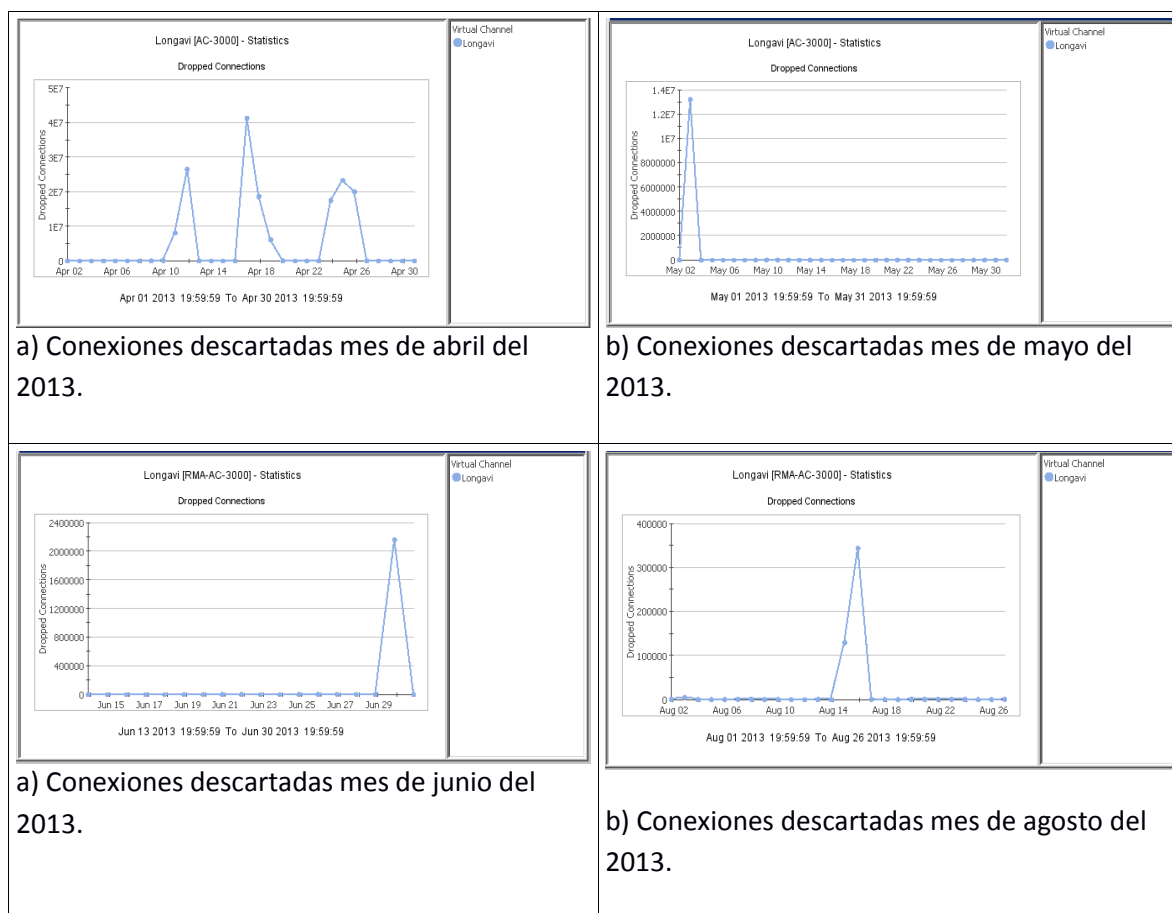


Ilustración 45: Conexiones descartadas debido a ataques *DoS* durante el mes de abril del 2013.

Se puede observar la correcta funcionalidad de la regla creada, ya que es capaz de detectar los ataques y bloquear las conexiones de forma tal que se resguarde la integridad del cortafuego principal de la universidad. Es importante el gran número de conexiones que se establecen cuando ocurre un ataque de estas características, durante el mes de abril se observan más de 40.000.000 de conexiones descartadas por el equipo.

Es importante mencionar que desde que se implementó esta regla, la disponibilidad de la red frente ataques aumento un 100%, es decir, nunca más se interrumpió el servicio de red dentro de la universidad debido a un ataque de denegación de servicio *DoS*.

Capítulo 7: Conclusiones

En este trabajo de título se implementó un administrador de ancho de banda en la red corporativa de la Universidad, creando políticas de calidad de servicio que distribuyen el ancho de banda contratado de por la universidad a todos sus usuarios.

El administrador de ancho de banda *ALLOT* permite generar de forma detallada y comprensible gráficos, reportes y tablas de los niveles de consumo de ancho de banda de toda la red. También permite conocer de forma detallada aquellos protocolos que están haciendo uso del ancho de banda asignado a cada unidad académica o administrativa. De esta manera se puede tener un control total de que es lo sucede en la red, lo que permite verificar si las reglas y políticas definidas por las autoridades son capaces de cumplir con los requerimientos de los usuarios de la red de la universidad.

Además el sistema es lo suficientemente sofisticado para reaccionar dinámicamente ante cambios en las condiciones de la red, tal como permitir a tráficos de baja prioridad aumentar su consumo de ancho de banda si quedan recursos disponibles.

El sistema es simple de administrar y operar. *NetXplorer* es una interfaz amigable con el usuario, presenta los datos de forma sencilla y rápida, lo que permite agilizar la toma de decisiones ante inconvenientes en la red.

El antiguo administrador de ancho de banda solo permitía asignar un límite superior de ancho de banda a cada unidad, no permitía distinguir distintos tráficos según su destino, por lo que no era posible separar el tráfico interno, nacional, internacional e Internet2, lo que es algo clave dentro de la universidad para poder administrar el ancho de banda en forma correcta. El equipo *ALLOT* permite realizar todo esto, además de presentar el detalle de que protocolos se utilizan, cuando ancho de banda consumen, quien lo origina y quien lo recibe. De esta manera se tiene un control total sobre la red.

Gracias a los gráficos presentados en esta memoria, es posible verificar que la universidad posee una baja capacidad en su enlace internacional, el cual no da abasto para satisfacer todas las necesidades de los usuarios. Esto se comprueba con el alto nivel de conexiones descartadas cuando se utiliza todo el ancho de banda disponible. Es necesario que la institución contrate un mayor ancho de banda internacional a los proveedores de internet.

El equipo permite controlar eficientemente los ataques de denegación de servicios, ya que desde que se implementó este administrador la disponibilidad de la red ante ataques aumento en un 100%. Desde marzo hasta el mes de diciembre del 2013, la red de la universidad no ha dejado de prestar servicios debido a ataques. Con el antiguo administrador de ancho de banda la red de la universidad colapsaba en promedio 3 veces a la semana debido a ataques de denegación de servicio.

El administrador de ancho de banda *ALLOT* cumple con todos los objetivos de esta memoria y entrega una alta capacidad de respuesta ante incidencias en la red debido a su gran poder de monitoreo de la situación de la red, sin embargo este equipo posee un alto valor, alrededor de US\$120.000, alrededor de 60 millones de pesos chilenos. Las características y funcionalidades presentes en el equipo *ALLOT* cumplen con las necesidades de cualquier empresa, esto dado la cantidad de modelos que ofrecen, siendo las empresas proveedoras de servicio a Internet sus principales clientes. En el caso de la Universidad, este equipo fue adquirido en modo *leasing* gracias a un convenio realizado con el principal proveedor de Internet para la Universidad, Claro Chile.

Como se mencionó en el comienzo de esta memoria, la administración del ancho de banda es un proceso continuo, las políticas creadas en esta memoria se deben revisar constantemente de forma de entregar el mejor servicio a los usuarios, pero sin dudas la implementación del equipo *ALLOT* permite manejar eficientemente el ancho de banda contratado por la universidad.

Referencias

[1]: Ancho de banda (ancho de banda)

http://en.wikipedia.org/wiki/Bandwidth_%28computing%29

[2]: *"Optimising Internet Bandwidth in Developing Country Higher Education"*

<http://www.inasp.info/uploaded/documents/BMO-chap6.pdf>

[3]: *"Need of bandwidth management and formulation of policy framework for effective utilisation of internet services within a university campus"*

http://www.csjournals.com/IJCSC/PDF2-1/Article_31.pdf

[4]: *"Bandwidth management position paper"*

<http://www.aplivate.org/uploads/filer/2012/12/03/aplivatebmopositionpaper.pdf>

[5]: *"Securing network from the Inside Out"*

<http://www.lansafe.com/elron.html>

[6] Vlan

<http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/VLANs.html#wp1157301>

[7] 1000Base-T

http://www.cisco.com/en/US/tech/tk389/tk214/tech_digest09186a0080091a86.html

[8] SFP

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

[9] Listas de acceso

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

[10] NAT

<http://www.openbsd.org/faq/pf/es/nat.html>

[11] DMZ

[http://es.wikipedia.org/wiki/Zona_desmilitarizada_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica))

[12]WiFi

<http://www.wi-fi.org/discover-and-learn>

[13]PfSense

<http://www.pfsense.org/>

[14]ISP

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

[15]Global Crossing

<http://www.level3.com/>

[16] Claro Chile

<http://www.clarochile.cl>

[17]Reuna

<http://www.reuna.cl/>

[18]Internet2

<http://www.internet2.edu/>

[19]FreeBSD

<http://www.freebsd.org/>

[20]Perfil de tráfico deseado: Sección 2.3 del *RFC* 2475

<http://www.ietf.org/rfc/rfc2475.txt>

[21]Paquete de datos

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

[22]Interfaz de red

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

[23]Control de congestión

http://es.wikipedia.org/wiki/Congesti%C3%B3n_de_red

[24]TCP

<http://www.rfc-es.org/rfc/rfc0793-es.txt>

[25]MRTG

<http://oss.oetiker.ch/mrtg/>

[26] Políticas de uso aceptado de recursos computacionales

http://www.dcsc.utfsm.cl/politicas/PoliticaTI-PUA_v2.pdf

[27]Línea de comando

<http://es.wikipedia.org/wiki/CLI>

[28] Ethernet

<http://ethernethistory.typepad.com/papers/EthernetSpec.pdf>

[29] Quality of Experience

<http://web.gc.cuny.edu/cogsci/private/GHH-intc-PP.pdf>

[30] NX Operation Guide R9 (12.3)

<http://es.scribd.com/doc/138677371/NX-Operation-Guide-R9-12-3>

[31] NX Installation and Admin Guide R9 (12.3)

[ftp://77.48.244.163/allot/NX%20Installation%20and%20Admin%20Guide%20R9%20\(12.3\).pdf](ftp://77.48.244.163/allot/NX%20Installation%20and%20Admin%20Guide%20R9%20(12.3).pdf)

[32]Denegación de servicio

http://www.cert.org/tech_tips/denial_of_service.html

[33]NetSecure

<http://www.netsecure.cl/>

[34]Valor del ancho de banda en la UTFSM

http://www.dcsc.utfsm.cl/redes/red/ancho_de_banda.html

[35]BGP

http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html

[36]BitTorrent

<http://es.wikipedia.org/wiki/BitTorrent>

[37] Diseño e implementación de estrategias de seguridad de la información. Memoria para optar al título de ingeniero civil telemática de Fernanda Mattar Catalán.