Taller Gestion de Redes

Gestión de Ancho de Banda

Presentación Original

Esta sesion ha desarrollado a partir de una presentación de Aptivate.org (Chris Wilson, AfNOG 2010 Kigali, Rwanda)

http://nsrc.org/workshops/2010/nsrc-unan-leon/raw-attachment/wiki/Agenda/afnog-bmo-presentation-2010.pdf

Que es Gestión de Banda de Ancha?

Se trata de administrar recursos eficientemente …

- En este caso, capacidad de transferencia de datos de su servicio acceso a Internet
- El uso siempre crecera' hasta que no existe capacidad sin usar
- Logicamente la solucion a largo plazo es aumentar el ancho de banda, pero:

- Ancho de banda no es barato
- Buen gestionamiento puede ahorrar mucho dinero

Como “Atacar” el Problema

Conozca su Red!

- Tiene que saber (con datos fidedignos):
- como se usa su banda de ancha
- patrones de uso
- cuellos de botellas existentes

Sugerencia

- No suponer!
- Hay que medir primero: instrumentacion
- Encontrara’ sorpresas!

Como Atacar el Problema

Políticas de Uso:

- Probablemente la parte mas difícil
- Cual es la misión de su organización?
- Quien toma las decisiones?
- Como van a solucionar? Mas recursos? Menos uso?
- Proceso abierto o cerrado?
  - Sugerencia: processo abierto, con prueba para respaldar las decisiones tomadas
- Existe una Política de Uso Aceptable?
- Cómo hacer cumplir esta política?

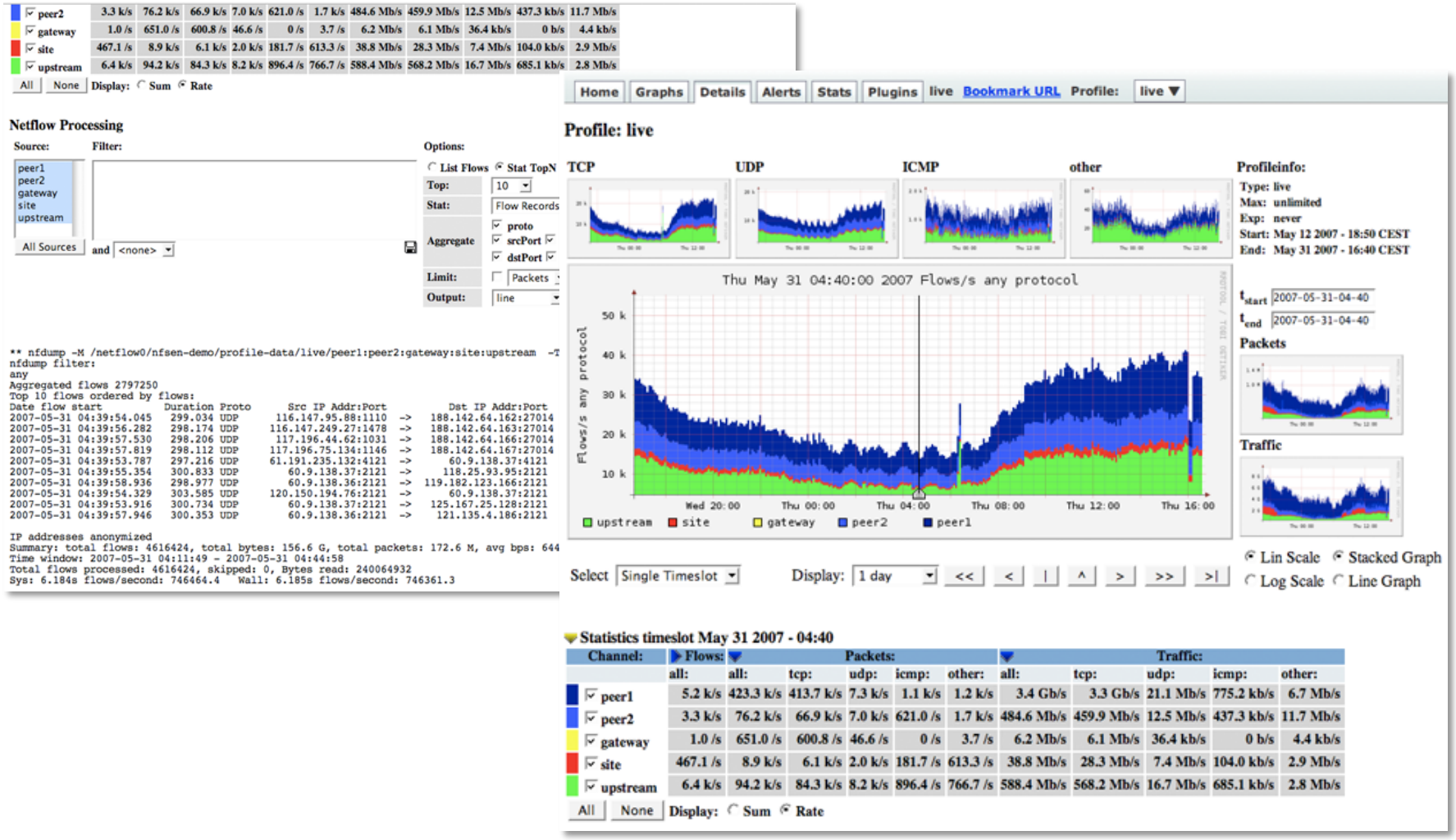
Que debe reflejar la política?

Una buena política:

- Medidas basadas en hechos (no opiniones)
- Consultando opinion de todos (consenso)
- Abierta y conocida por todos
- Monitorear constantemente
- Verificar cumplimiento, y comunicar a todos
- Revisión periódica, pues “los tiempos cambian”
  - Ejemplo: Es Twitter una herramienta o no?
  - Es Facebook necesario para el trabajo?

Como visualizar el uso?

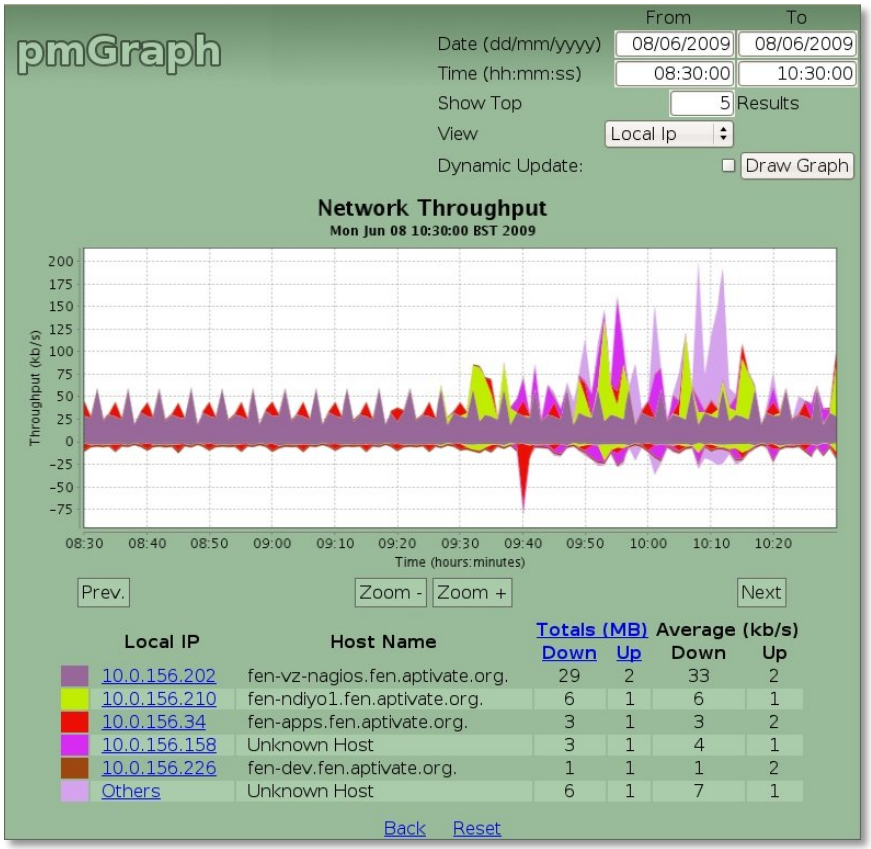
Netflow…



Como visualizar el uso?

…Mas herramientas de flujos…

- **pmGraph**
  http://www.aptivate.org/en/work/projects/pmgraph/
- **ARGUS**
  http://www.qosient.com/argus/



Y despues?

Ahora que se conoce el perfil de uso, hay que monitorear el estado de la red, ejemplo:

- **Estado de las conneciones locales y remotas**
- **Uso de CPU e interfaces de enrutadores local y remoto**
- **Tiempo de respuesta de sitios de web remoto**

Use herramientas que mantienen historia para conocer los patrones de uso de su red (mrtg/ rrdtool).

Herramientas Tipicas

De fuente abierto…

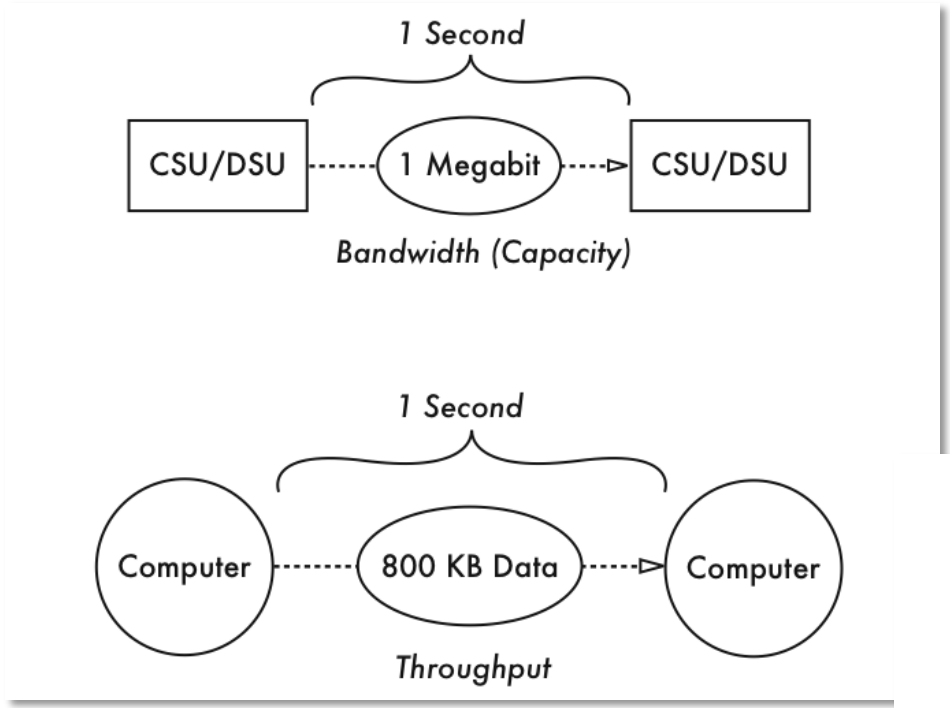
Variable	Spot Check	Trending
End-to-end HTTP	wget, fetch, httperf	Smokeping, Nagios
Ping latency	Ping, Traceroute, MTR	Smokeping, Nagios
Ping packet loss	Ping, Traceroute, MTR	Smokeping, Nagios
DNS latency	Host, Resperf	Smokeping, Nagios
DNS errors	Host, Resperf	Smokeping, Nagios
Total bandwidth use	Cisco “show interfaces”	Cacti, MRTG
Traffic flows	Cisco Top Talkers, Ntop	NfSen, Argus, pmGraph
Individual packets	Wireshark	tcpdump, Argus

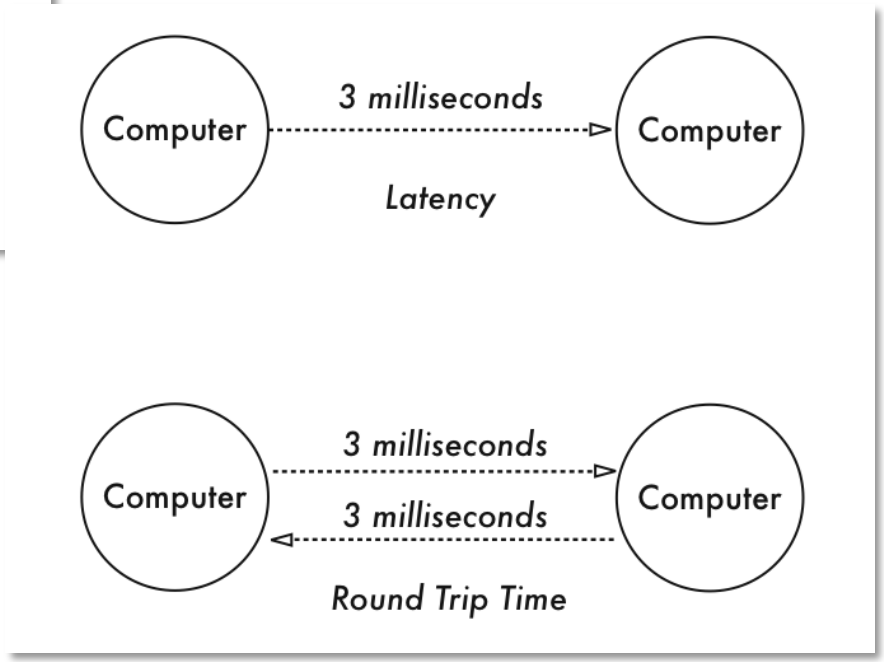
Uso de Las Herramientas

A veces, pero no siempre, el problema es que su coneccion no tiene capacidad disponible:

- Puede hacer un ping al enrutador por su lado sin problemas, pero haciendo un ping al enrutador de su ISP muestra:
  - Nivel de retardo muy alto (mas de 1 segundo)
    - (Mas de 4 segundos y Windows responde con “request timed out”)
  - Perdida de paquetes > 1% a su ISP (proveedor)
  - Respuestas de DNS perdidas o muy lentas desde su ISP (no cache)
  - Jitter muy alto (subjetivo, tal vez unos 20 ms sobre el stdev)
  - Tambien puede ser una coneccion mala al otro lado

Definiciones





Monitoreando una Coneccion Internet

Que queremos monitorear?

- Los mismos parametros que queremos usar para resolver problemas, o que afectan la calidad de servicio
- Disponibilidad de enrutadores local y remoto, los tiempos de respuesta de ping (perdida de paquetes y retardo)
- Disponibilidad local y remoto de servidor de DNS de caching, tiempos de respuesta de las consultas (razon de falla y retardo)
- Trafico total en enlaces, ademas de por nodo y tipo
- Sitios web (extremo-a-extremo)

El monitoreo a largo plazo ayuda a identificar patrones, y subitos cambios de comportamiento

Que Tipo de Monitoreo usar?

- Herramienta de estado actual detectan incidentes al momento que suceden
- Las herramientas de tendencia coleccionan datos a lo largo del tiempo
  - este tipo de herramienta ayuda a establecer cual es la condicion normal (linea base) y que es una anomalia
  - Ayudan en analisis forenses de problemas

Ejemplos de Monitoreo de Disponibilidad de Servicio

- **Nagios** para monitorear servicios como sitios web, estado de interface en enrutadores, memoria utilizada en servidores, estado de servicio de DNS (local y remoto)
- **Cacti** para monitorear usoa lo largo del tiempo de ancho de banda en cada interfaz, memoria y CPU en entrutadores y conmutadores.
- **Smokeping** para monitorear retardo y perdida de paquetes en interfaces
- **pmGraph** y/o **Netflow** para monitorear flujos de traficos en conecciones a Internet, o internas

Estas herramientas son conocidas…

No es cierto?

Esta semana hemos visto:

- **SNMP**
- **Nagios**
- **Cacti**
- **Syslog**
- **Request Tracker**
- **Netdot**

Herramientas de ayuda

Gestion de ancho de banda

- Ping
- Traceroute
- MTR
- Smokeping
- NetFlow/NfSen
- WCCP

Ping y Traceroute

Ping: util para chequeos instantaneos

- Disponibilidad
- tiempo de retorno (RTT o tambien “retardo”)
- perdida de paquetes (aumentando talla de paquete)
  - `ping –c 1000 –s 1400`
- parpadeo (jitter) (`ping –c 1000` y chequea mdev/stddev)
- fragmentacion (`ping –s 1483`)

Traceroute: trazar la ruta de paquetes en la red

- cuantos enrutadores en el camino de A a B?
- funcionamiento basado en “tiempo de vida” de paquetes (TTL)

Matt's Traceroute (MTR)

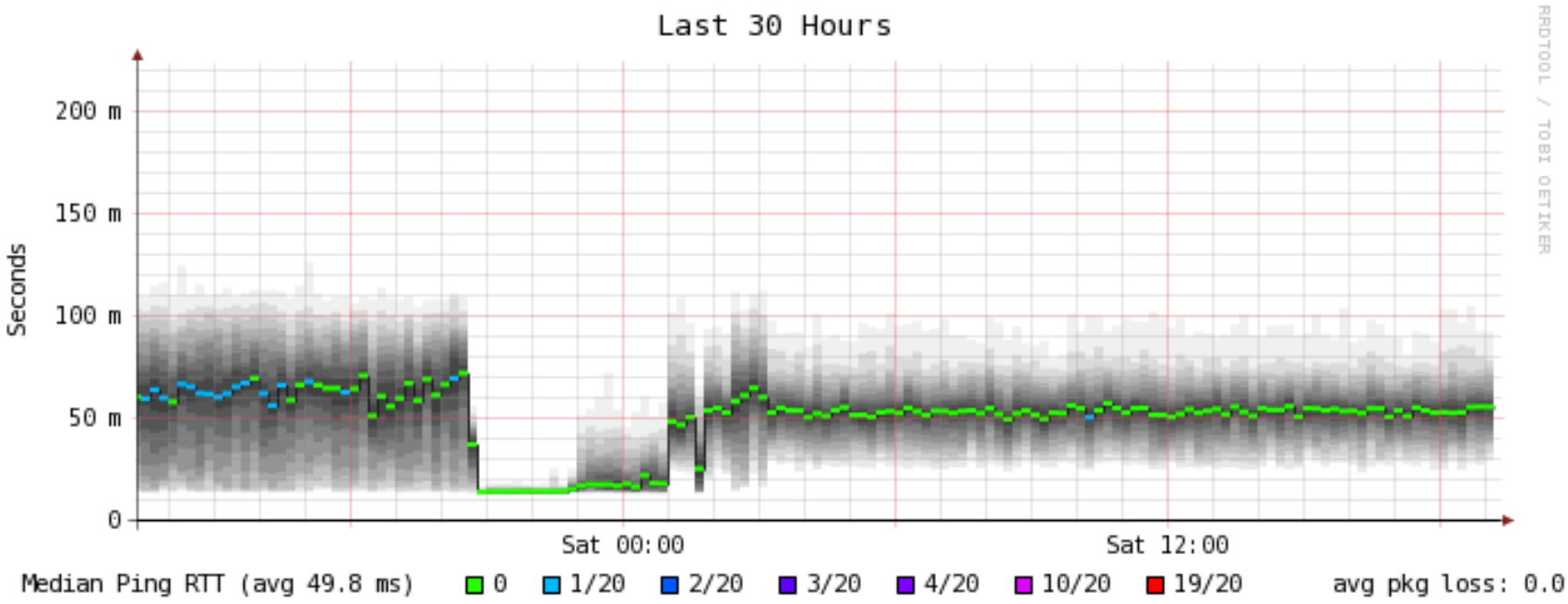
- Combina las funciones de ping y traceroute
- Primero, establece ruta al destino (traceroute)
- Despues, envia secuencias ICMP (echo request)
- Muestra las estadisticas interactivamente
- Opcional, se puede indicar reporte al final de corrida
- Como instalar:

```
$ sudo apt-get install mtr
```

Ejemplo:

```
 $ mtr -c 10 -r google.com
HOST: nsrc                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. vl-306-gw.uoregon.edu           0.0%    10    1.4  17.5   0.6 140.7  43.5
  2. vl-3.uonet9-gw.uoregon.edu     40.0%    10    0.5   0.4   0.4   0.5   0.0
  3. vl-205.ge-2-0-0.core0-gw.pdx    0.0%    10    3.1   3.2   3.1   3.6   0.1
  4. 2001:1860:110:2008::1           0.0%    10   11.1  13.5   6.5  71.7  20.5
  5. 2001:1860:110:1000::2           0.0%    10    6.7   6.6   6.5   6.7   0.1
  6. 2001:4860::1:0:795              0.0%    10   30.4  13.1   6.8  37.3  11.1
  7. 2001:4860:0:1::183              0.0%    10    7.2   7.0   6.9   7.2   0.1
  8. sea09s15-in-x0e.1e100.net       0.0%    10    6.6   6.7   6.5   7.2   0.2
```

Visualizando Parpadeo: Smokeping



- Una **disminucion significativa** de retardo
- Al igual que disminucion de perdida de paquetes por corto periodo
- Conclusion? Coneccion esta muy cargada la mayoria del tiempo

Diagnosticando Conexiones Sobrecargadas

Una conexion sobrecargada puede ser por:

- Trafico en entrada
  - Bajando files, bit-torrent, ataques DoS, email spam en entrada
- Trafico en salida
  - Subidas, bittorent, PCs infectadas por viruses, spam en salida
- Ambos

El volumen total de trafico no es un dato tan util

- Mucho mas util identificar paquetes que tienen un denominador comun:
- direccion y puerto fuente del trafico
- direccion y puerto destino del trafico
- tipo de protocolo (entre otros)

Vaya con el Flujo…

- Los flujos son sumante utiles par hacer monitoreo de trafico
  - Identifica quien esta “hablando” con quien y en detalle
  - Mas facil de generalizar que paquetes por separado
- Un flujo, normalmente, es unico
  - Un par de direcciones IP
  - Un par de puertos
  - Tipo de protocolo

Que' es un flujo?

- Grupo de paquetes con un denominador comun
- Nos permite clasificar y cuantificar trafico
- Veremos herramientas de flujo esta semana
  - Netflow y NfSen
  - Generado por enrutadores de Cisco, Juniper, otros

Como se Ve un Flujo?

ip_src	ip_dst	sport	dport	proto	pkts	bytes	inserted
41.190.128.29	196.200.216.44	143	63221	tcp	33	21776	25/05/10 13:32
196.200.216.94	213.254.211.14	50155	80	tcp	185	10160	25/05/10 13:32
213.254.211.14	196.200.216.94	80	50155	tcp	277	415500	25/05/10 13:32
213.199.149.57	196.200.216.156	80	50553	tcp	65	68255	25/05/10 13:33
196.200.216.100	213.254.211.8	58626	80	tcp	19	14192	25/05/10 13:32
196.200.216.133	69.64.75.206	49479	80	tcp	262	13374	25/05/10 13:32
69.64.75.206	196.200.216.133	80	49479	tcp	429	602968	25/05/10 13:32
209.85.229.155	196.200.216.133	80	49495	tcp	17	10428	25/05/10 13:32
209.85.229.155	196.200.216.133	80	49494	tcp	16	12119	25/05/10 13:32
69.64.72.239	196.200.216.133	80	49510	tcp	23	29652	25/05/10 13:32

Por ejemplo, ver quien consume mas…

```
gw-rtr# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0           91.189.88.39    Fa1           192.168.163.101 06 0050 83AF   20M
Fa0           150.214.5.135   Fa1           192.168.163.101 06 0050 AAF8   14M
Fa0           128.223.157.19  Fa1           192.168.163.101 06 0050 DB89 1538K
Fa1           192.168.163.101 Fa0*          91.189.88.39    06 83AF 0050  763K
Fa1           192.168.163.101 Fa0*          150.214.5.135   06 AAF8 0050  531K
Fa1           192.168.163.101 Fa0*          66.220.153.19   06 9D3B 0050  307K
Fa0           216.100.5.133   Fa1           192.168.163.101 06 0050 BBB5  228K
Fa0           74.125.159.147  Fa1           192.168.163.101 06 0050 C71F   99K
Fa0           72.21.210.250   Fa1           192.168.163.101 06 0050 ACBE   98K
Fa0           74.125.159.106  Fa1           192.168.163.101 06 0050 D76C   93K
10 of 10 top talkers shown. 310 flows processed.
```

Como ahorrar?

- Medidas sociales
  - Politicas de uso acceptable
  - Educacion a usuarios
  - Consenso y conocimiento
- Medidas Tecnicas
  - Bloqueo de trafico no deseado
  - Cacheo y almacenamiento local
  - Asignacion de cuotas de trafico

Politica de Uso Aceptable

- Facil de establecer,
- Dificil de hacer cumplir
  - Medidas sociales
  - Medidas tecnicas
- Cambiar comportamiento requiere:
  - educacion
  - una politica establecida
  - aceptacion por parte de usuario final

Medidas Sociales

- Tal vez los usuarios no saben cuanto banda de ancha estan usando
- Usualment usuarios con mas habilidades tecnicas son quienes mas abusan
- Habla con los usuarios en privado primero.
- Puede considera publicando una lista de los usuarios que tienen mas uso de la Red (presion social).
- Puede considerar accion disciplinaria si la politica de uso lo estipula (limitando privilegios, accesso)

- Si es necesario hay soluciones tecnicas

Medidas Tecnicas

- Evitar trafico de malware y viruses
  - Mantener actualizado software antivirus
  - Bloquear puertos usados por malware/viruses
  - Alarmas para detectar maquinas infectadas
- Evitar trafico de “spam” en correo electronico
  - tanto en entrada como salida
  - idealmente bloquear antes que afecte a los enlaces de mas baja capacidad
  - monitoreo muestra cuanto trafico es e-mail
  - filtros locales de spam pueden ayudar, pero son dificiles de implementar
  - Servicio comerciales remotos de filtraje de e-mail puede ayudar (Barracuda firewall, GoogleApps)

Ahorrando ancho de banda

- Ideas:
- Servidor local DNS solo-cache
- Web cache local
  - Squid: http://www.squid-cache.org/
  - WCCP de Cisco (Web-Cache Communication Protocol)
- Cache de Aplicaciones
  - apt-cacher para Debian/Ubuntu
  - Repositorios espejo locales

Otras Posibles Medidas Technicas

- **Cuotas fijas**: Limite fijo por usuario
- **Cuotas "blandas"**: Usuarios que sobrepasen su limite del uso de la Red recibe un servicio mas lento
- **Cuotas flexibles**: Progresivamente los usuarios reciben menos banda de ancha

Resumen

- Mientras mas restricciones se apliquen, mas excepciones habra’
- Se hace mas dificil administrar la red
- Sin una politica de uso aceptable y la educacion de los usuarios, es mucho mas dificil administrar eficientemente

Referencias

- Presentacion de Chris Wilson de Aptivate.org de Bandwidth Management
  http://nsrc.org/workshops/2010/nsrc-unan-leon/raw-attachment/wiki/Agenda/afnog-bmo-presentation-2010.pdf
- WALC: Conferencias, Tallers y Capacitacion en America Latina
  http://www.eslared.org.ve/
- Pagina de web explicando fragmentacion de IP
  http://penguin.dcs.bbk.ac.uk/academic/networks/network-layer/fragmentation/index.php
- pfSense (Firewall de FreeBSD)
  http://www.pfsense.com/
- Fair Queuing
  http://en.wikipedia.org/wiki/Fair_queuing
- Gestion Actividad de la Red (Network Activity Auditing)
  http://www.qosient.com/argus/
- Herramientas de Medidas de DNS de Nominum
  http://www.nominum.com/services/measurement_tools.php
- WCCP: Protocolo de Comunicacion de Cache de Web
  - http://en.wikipedia.org/wiki/Web_Cache_Communication_Protocol
  - http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf018_ps1835_TSD_Products_Configuration_Guide_Chapter.html
- Cache de Web Squid
  http://www.squid-cache.org/