Taller Gestion de Redes
NSRC-UNAN León

Gestión de Banda de Ancha

Presentación Original

Esta presentación esta basada en una presentación de Chris Wilson de Aptivate.org que fue dada en AfNOG 2010 en Kigali, Rwanda, África:

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

Que es Gestión de Banda de Ancha?

Es una tema grande:

- **Curso de un ano**
  http://www.widernet.org/programs/BandwidthManagement.htm
- **Curso de dos semanas (*excelente curso*)**
  http://sdu.ictp.it/lowbandwidth/program
- **Aptivate (**http://www.aptivate.org**)**
  - Libros
  - Cursos
  - Herramientas
  - Conocimient

Que es Gestión de Banda de Ancha?

Se trata de…

Gestion de Redes de enlaces lentos y las Redes que se lo usan?

Tal vez necesitas mas banda de ancha, pero:

- El uso siempre cresca hasta que el recurso no vale la pena usar.
- Ancho de banda es muy caro
- Buen gestionamiento puede ahorrarle mucho dinero

Como “Atacar” el Problema

Conocimiento de su Red!

- Tiene que saber (con prueba) donde va su banda de ancha.
- Los patrones de uso.
- Los cuellos de botellas existentes.

Sugerencia

- No presumir que esta usando su banda de ancha antes de medir. Hay sorpresas!

Como Atacar el Problema

Políticas

- Probablemente el parte mas difícil.
- Que es la misión de su organización?
- Quien toma las decisiones?
- Como va a hacerlo?
- Proceso abierto o cerrado?
  - Sugiero abierto con prueba para respaldar las decisiones que están tomados.
- Tiene una Política de Uso Aceptable?
- Cómo hacer cumplir la política de uso aceptable?

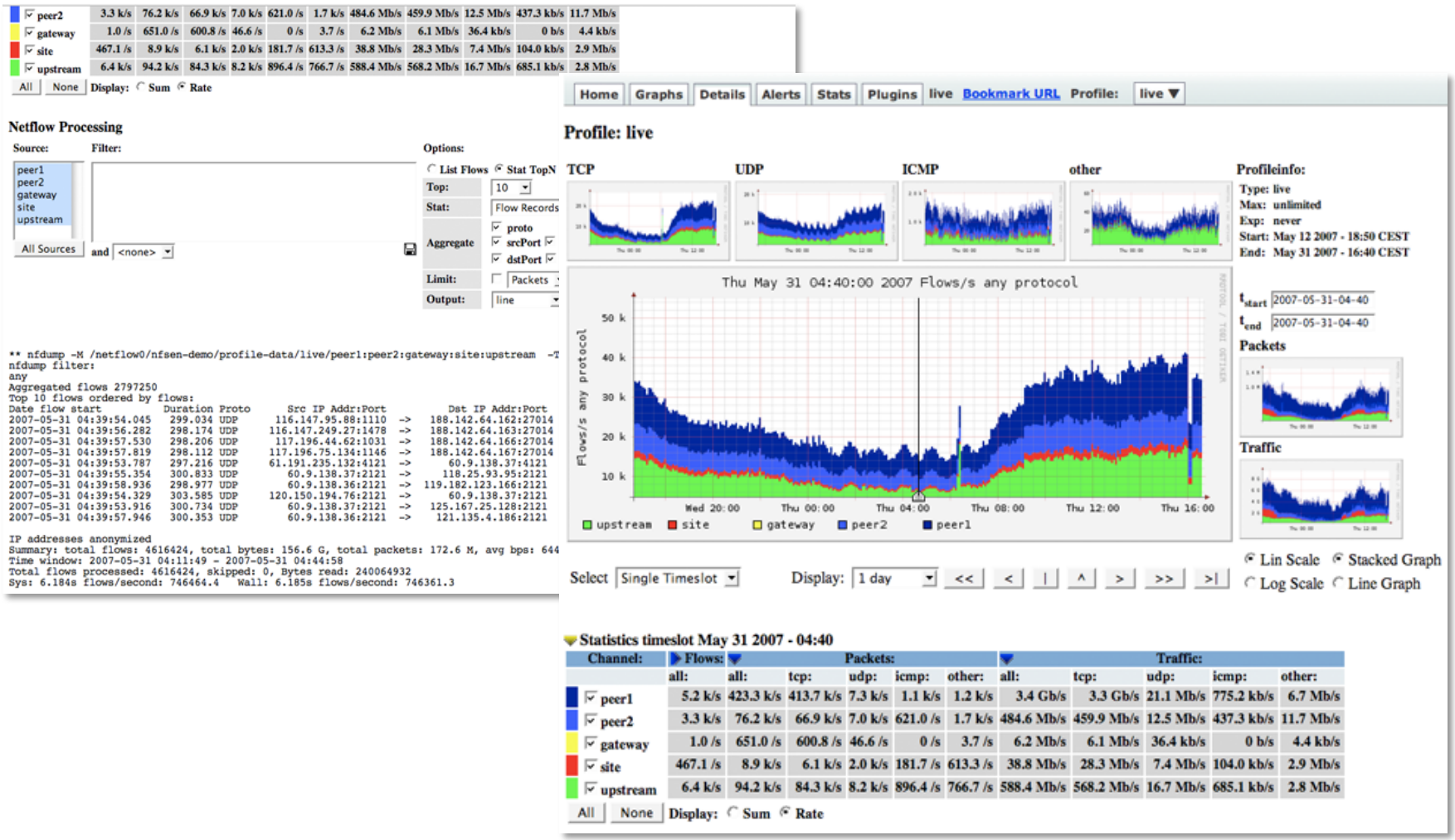
Que Hay en Una Política?

Para hacer una política en forma buena (opinión del autor!):

- Basado en pruebas
- Hecho con todos (consenso)
- Abierto y conocido por todos
- Monitoreado
- Cumplimiento
- Revisión periódica

Como Ver Que Uso Hay?

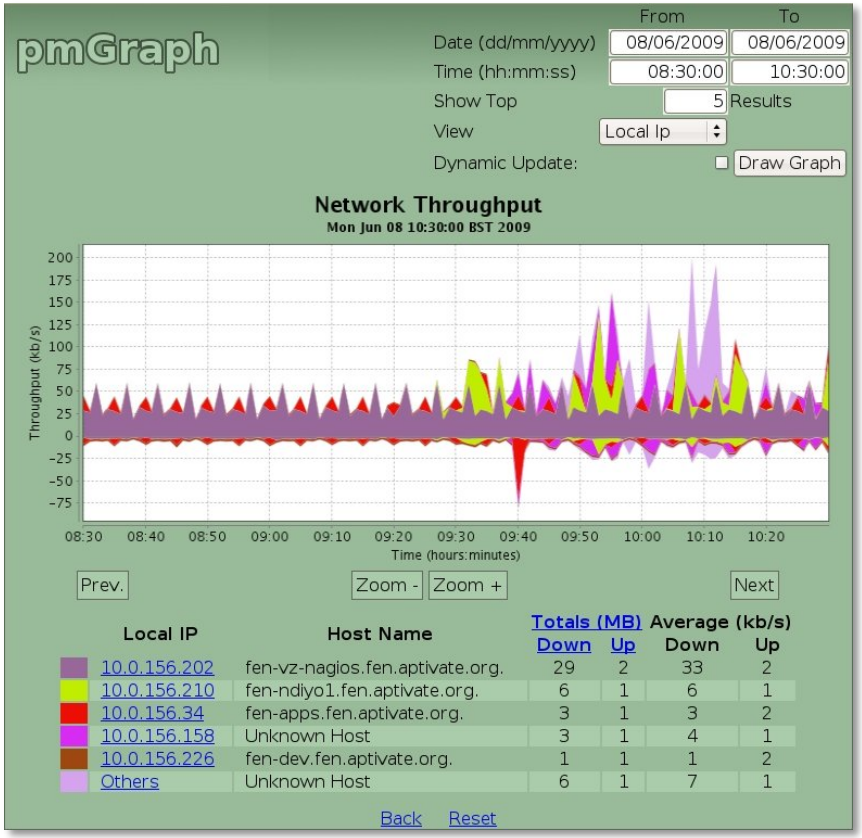
Netflow…



Como Ver Que Uso Hay?

…Mas herramientas de flujos…

- **pmGraph**
  http://www.aptivate.org/Projects.BMOTools.pmGraph.html
- **ARGUS**
  http://www.qosient.com/argus/



Despues

Ya sabes que esta usando su Red, ahora tiene que monitorear el resto:

- **Cache/Proxy de Web**
- **DNS (Caching) local y remoto**
- **Salud de las conneciones local y remoto**
- **Uso de enrutadores local y remoto**
- **Tiempo de respuesta de sitios de web remoto**

Usa herramientas que mantiene historia para conocer bien las patrones del uso de su Red (mrtg/rrdtool).

Herramientas Tipicas

De fuente abierto…

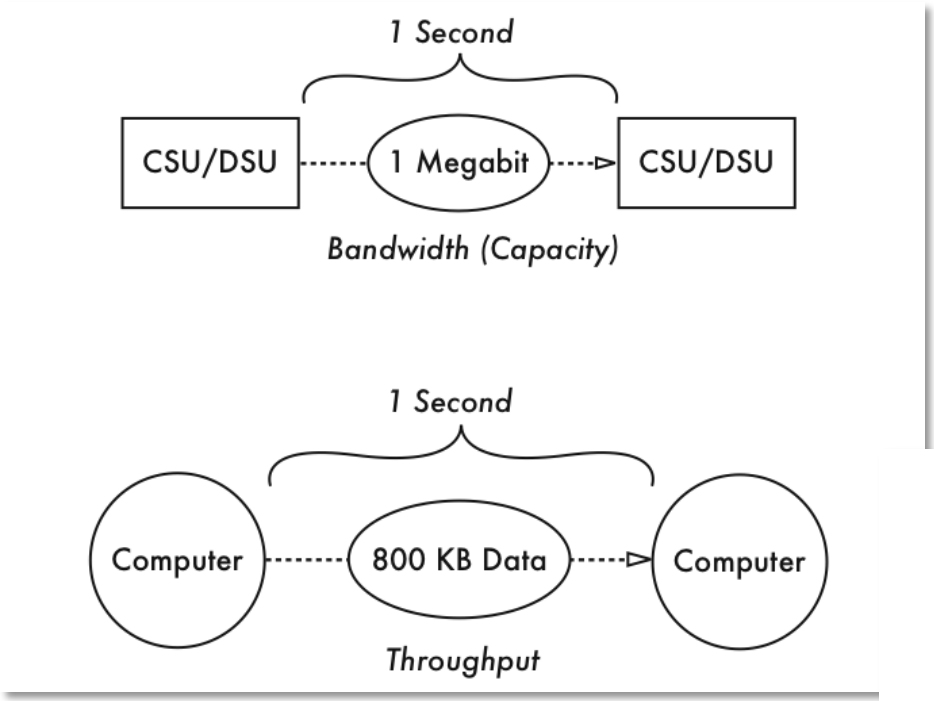
Variable	Spot Check	Trending
End-to-end HTTP	wget, fetch, httperf	Smokeping, Nagios
Ping latency	Ping, Traceroute, MTR	Smokeping, Nagios
Ping packet loss	Ping, Traceroute, MTR	Smokeping, Nagios
DNS latency	Host, Resperf	Smokeping, Nagios
DNS errors	Host, Resperf	Smokeping, Nagios
Total bandwidth use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

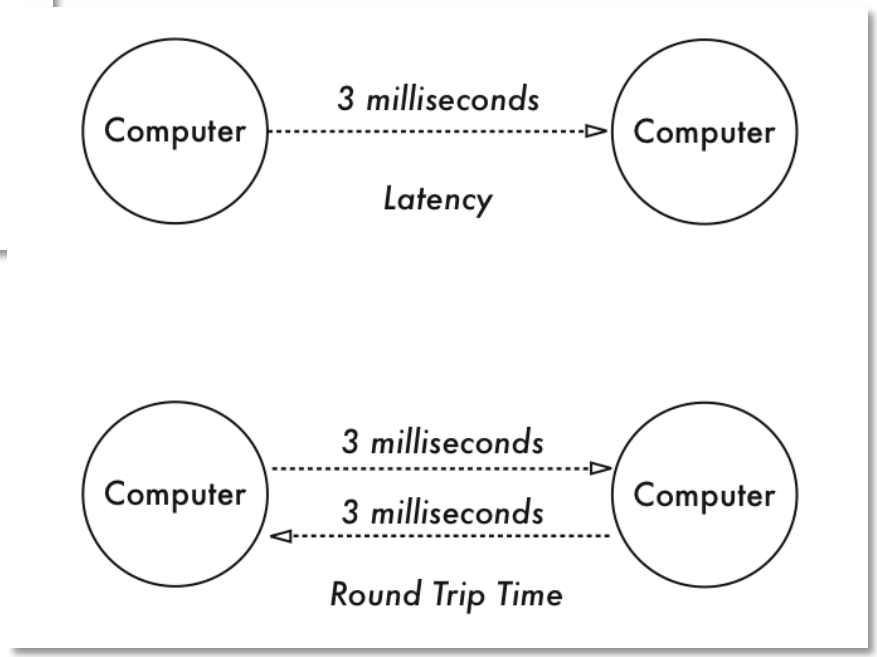
Uso de Las Herramientas

De repente, pero no siempre, el problema es que su coneccion ya esta llena:

- 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 (subjectivo, tal vez unos 20 ms sobre el stdev)
  - Tambien puede ser una coneccion mala por el otro lado.

Definiciones





ping

Util por chequeos del instante:

- disponibilidad (intenta www.google.com, 4.2.2.2)
- tiempo de viaje (RTT o retardo)
- Perdida de paquetes:
  - `ping –f`
  - `ping –c 1000 –s 1400`
- jitter (`ping –c 1000` y chequea mdev/stddev)
- fragmentacion (`ping –s 1483`)
- fragmentation (ping -s 1483)

Matt's Traceroute (MTR)

Version repetida y interactiva de traceroute

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

```
HOST: rocio.int.aidworld.org       Loss%   Snt   Last   Avg  Best  Wrst StDev
   1. 196.200.217.254               0.0%    10    1.6   1.7   1.6   1.8   0.1
   2. rtr-tedata.mtg.afnog.org      0.0%    10    2.0   2.2   2.0   3.2   0.4
   3. host-196.219.220.81-static.t  0.0%    10    5.5   8.4   4.0  45.0  12.9
   4. host-163.121.160.229.tedata.  0.0%    10    6.7   4.8   4.3   6.7   0.8
   5. host-163.121.189.73.tedata.n  0.0%    10    4.4  11.3   4.4  63.4  18.4
   6. host-163.121.186.253.tedata.  0.0%    10    4.5   5.1   4.5   7.4   0.9
   7. host-163.121.184.61.tedata.n  0.0%    10    5.0   5.7   4.6  13.5   2.8
   8. pal6-telecom-egypt-1-eg.pal.  0.0%    10   72.3  66.4  54.5 100.7  15.4
   9. ash1-new11-racc1.ash.seabone  0.0%    10  150.3 154.2 150.3 175.9   7.8
  10. ntt-1-ash1.ash.seabone.net   40.0%    10  153.7 152.7 146.7 154.5   3.0
  11. as-3.r20.snjsca04.us.bb.gin.  0.0%    10  153.7 182.7 146.1 219.0  36.8
  12. as-3.r20.snjsca04.us.bb.gin. 10.0%    10  215.9 255.3 214.3 370.0  54.4
  13. ge-3-3.r03.snjsca04.us.ce.gi 10.0%    10  216.9 253.5 216.2 402.0  63.7
  14. border2.te8-1-bbnet2.sfo002. 10.0%    10  216.9 218.7 215.8 230.7   5.0
  15. border2.te8-1-bbnet2.sfo002. 50.0%    10  215.2 215.6 214.9 216.9   0.8
  16. ???                         100.0     10    0.0   0.0   0.0   0.0   0.0
```

Monitoreando una Coneccion Internet

Que queremos monitorerar?

- Las mismos factores que queremos usar para resolver problemas.
- Los mismos factores que afectan la calidad de servicio
- Disponibilidad de enrutadores local y remoto y los tiempos de respuesta de ping (pedida de paquetes y retardo)
- Disponibilidad local y remoto de servidor de DNS de aching y los tiempos de respuesta de las consultas (razon de falla y retardo)
- Trafico en general do los links y por nodo y por tipo
- Sitios de web (extremo-a-extremo)

El monitoreo de largo plazo ayuda a indetificar patrons y cambios grandes de repentes.

Que Tipo de Monitoreo?

- Herramientas del momento puede ayudar con problemas mientras que pasen.
- Muchas problemas requiere que ya tiene un base de conocimiento de que es normal por su Red.
- Herramientas de tendencia pueden coleccionar estes datos.
- Herramientas de tendencia pueden ayudar con la investigacion de problemas despues que se pasen
- Requieren un inversion en tiempo para instalar bien estas tipas de herramientas.

Monitoreo de Calidad de Servicio

- **Nagios** para monitorear sitios de webs, enrutadores, servidores de DNS (local y remoto) y para mandar alertas.
- **Cacti** para monitorear uso total de banda de ancha en cada interfaz, uso de Memoria y CPU en entrutadores y conmutadores.
- **Smokeping** para monitorear sitios de web, retardo y perdida de paquetes en sus conecciones de carga.
- **pmGraph** y/o **Netflow** para monitorear flujos de traficos en sus conecciones al Internet.

Ya Hemos Visto Todo Esto…

No cierto?

Esta semana:

- NOC
- SNMP
- Nagios
- Smokeping
- Cacti
- Request Tracker
- NetFlow

Monitorear Enrutadores c/ Nagios

Abre */usr/local/etc/nagios/objects/templates.cfg* y agrega esta lineas al final:

```
define host {
        host_name router-serena
        use generic-host
        address 196.200.215.254
        max_check_attempts 5
    }
define host {
        host_name router-kist
        use generic-host
        address 196.200.217.254
        max_check_attempts 5
    }
```

(Se continua...)

Monitorear Enrutadores c/ Nagios

Abre */usr/local/etc/nagios/objects/templates.cfg* y agrega estas lineas al final:

```
define hostgroup {
        hostgroup_name routers
        members router-serena, router-kist
    }

define service {
        service_description ping
        use generic-service
        hostgroup routers
        check_command check_ping!10,20%!20,40%
    }
```

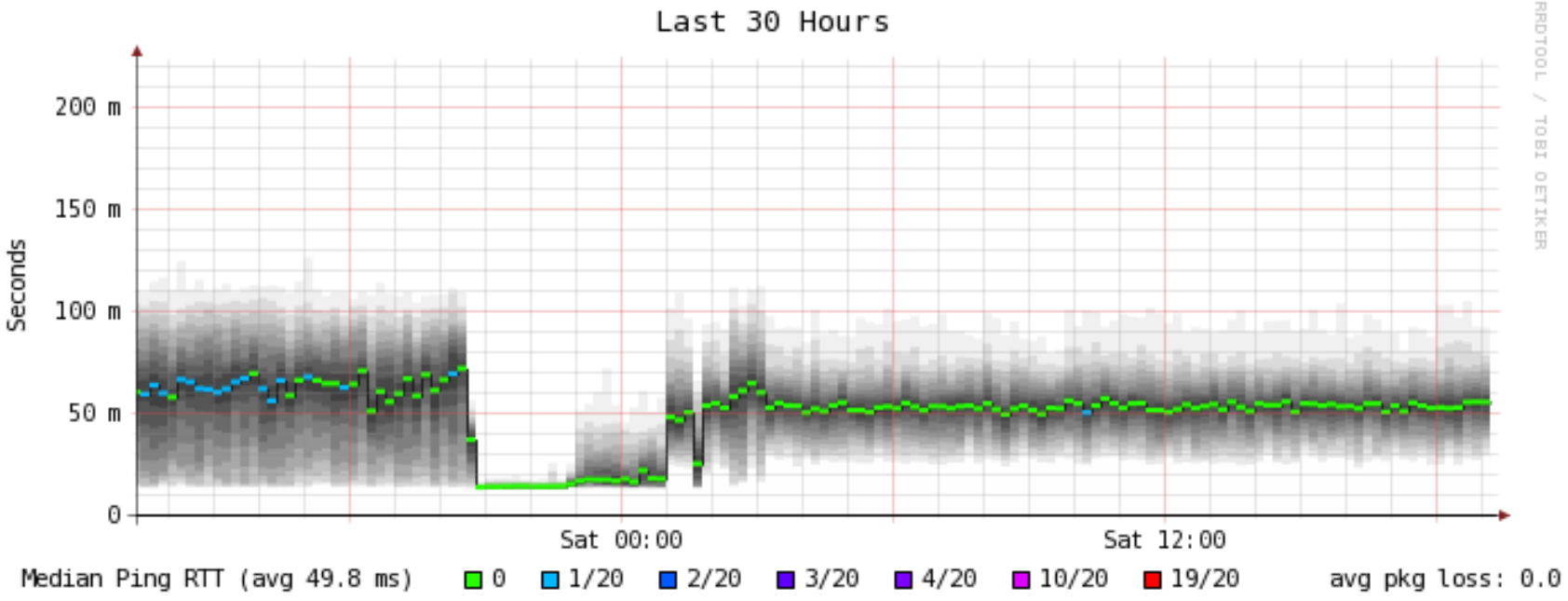
Monitoreo de DNS con Nagios

```
define hostgroup {
        hostgroup_name dns-servers
    }
    define host {
        name dns-server
        max_check_attempts 5
        hostgroups dns-servers
        register 0
    }
    define host {
        host_name soekris
        use dns-server
        address 196.200.223.1
    }
    define host {
        host_name upstream-dns-server
        use dns-server
        address 196.200.223.2
    }
    define command {
        command_name check_dns
        command_line $USER1$/check_dns -H www.yahoo.com -s $HOSTADDRESS$
    }
    define service {
        service_description dns
        use generic-service
        hostgroup dns-servers
        check_command check_dns
    }
```

Monitoreo Siteos de Web c/Nagios

```
define hostgroup {
        hostgroup_name websites
    }
    define host {
        name website
        max_check_attempts 5
        hostgroups websites
        register 0
    }
    define host {
        host_name www.yahoo.com
        use website
        address www.yahoo.com
    }
    define host {
        host_name www.google.com
        use website
        address www.google.com
    }
    define command {
        command_name check_site
        command_line $USER1$/check_http -H $HOSTADDRESS$
    }
    define service {
        service_description http
        use generic-service
        hostgroup websites
        check_command check_site
    }
```

Leyendo un Grafico de SmokePing



- Una **caida significitiva** de retardo y perdida de paquetes por corto plazo.
- Conclusion: Coneccion esta muy cargada la mayoria del tiempo.

Diagnosticando Conexiones Cargadas

Una coneccioned muy cargada puede ser por:

- Trafico entrando
  - Bajadas, bittorrent, ataques, spam entrando
  - downloads, bittorrent, attacks, incoming spam
- Trafico saliendo
  - Subidas, bittorent, PCs infectados de viruses o gusanos, spam saliendo
  - uploads, bittorrent, virus or worm-infected PCs, outgoing spam
- Los dos al mismo tiempo

El volumen total de trafico no es un dato util . Tiene que identificar el fuente del trafico

- Identificando el destino, tal vez, no ayudara.

Encontrando el Culpable

- Los LEDs (luces) en un conmutador puede ayudar en encontrar puerto ocupados.
  - No discrimina entre trafico local y remoto
- Puede usar SNMP para monitorear el trafico en cada puerto con Conmutadores gestionable .
- Flow son la proxima capa abajo:
  - Cisco o Juniper entrutador con NetFlows/sFlow
  - Enrutador o puente de Unix corriendo pmacct o ntop
- Paquetes estan en el nivel mas bajo
  - Enrutador de Unix o un puente transparente corriendo Wireshark.
  - Hardware caro para analizar la Red.

Vaya con el Flujo…

- Los flujos son sumante utiles par hacer monitoreo de trafico
  - Identifica quien esta “hablando” a quien y, muchas veces, el protocolo o tipo de trafico.
  - Mucho menos detallado y mas facil de entender que los paquetes.
- Un flujo, normalmente, es unico
  - Un paar de direcciones de IP
  - Un paar de puertos
  - protocolo

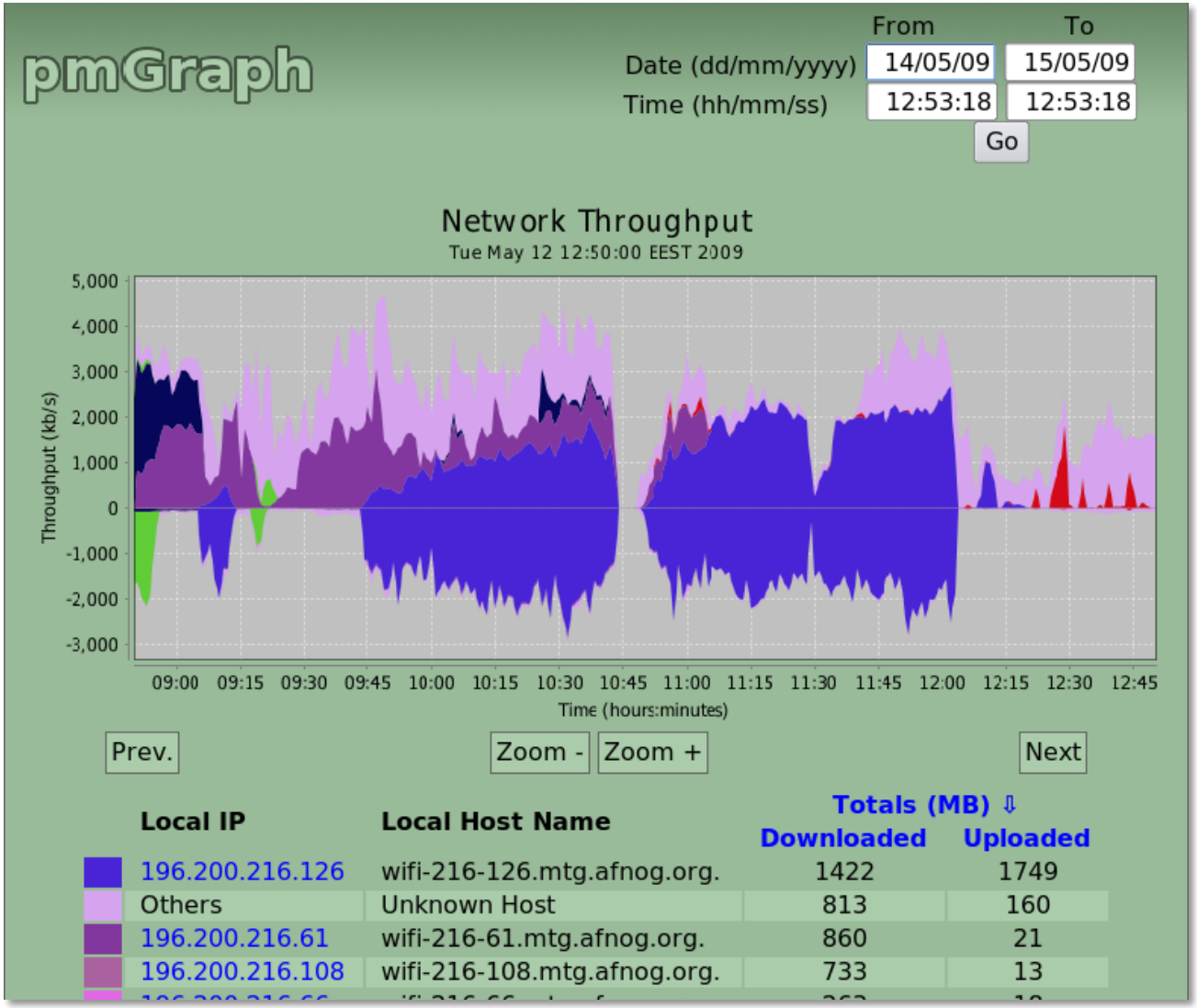
Vaya con el Flujo…

- Los flujos estan medidos (numero de bytes reportados) en intervales fijos para agregar otra dimension a los datos.
- Generado por enrutadores de Cisco, Juniper o algo como pmacct.

Como se Vea 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

Que Podemos Hacer con Flujos



Habilitar NetFlow por Cisco

Habilitar NetFlow por todo las interfaces activas:

rtr-tedata> ***show interface summary***

```
  Interface            IHQ    IQD  OHQ    OQD  RXBS RXPS   TXBS TXPS TRTL
-----------------------------------------------------------------------
  FastEthernet0/0        0      0    0      0     0    0      0    0    0
* FastEthernet0/1        1      0    0      0 1684000 369 1944000 315  0
* Serial0/0/0            0      0    0      0 957000  148 703000  165  0
* Serial0/0/1            0      0    0      0 1324000 182 1223000 201  0
* Serial0/2/0            0      0    0      0 469000  101 887000  140  0
```

```
rtr-tedata# conf t
rtr-tedata(config)# interface FastEthernet0/1
rtr-tedata(config-if)# ip route-cache flow
rtr-tedata(config-if)# exit
rtr-tedata(config)# interface Serial0/0/0
rtr-tedata(config-if)# ip route-cache flow
rtr-tedata(config-if)# exit
```

Ver los “Top Talkers”

```
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.
```

Exportando Datos de Netflow de Cisco

Si la direccion de IP de su colectador es 10.10.10.5:

```
$ ssh gw-rtr
gw-rtr> enable
gw-rtr# conf t
gw-rtr(conf)# ip flow-cache timeout active 1
gw-rtr(conf)# ip flow-cache timeout inactive 60
gw-rtr(conf)# ip flow-export version 5
gw-rtr(conf)#  ip flow-export destination 10.10.10.5 4096
gw-rtr(conf)# exit
gw-rtr# write memory
```

Que Viene?

Haciendo la Politica

- Hacer cumplir la política
  - Medidas sociales
  - Medidas tecnicas
- Resumen y recursos

Que Ahora?

- La coneccion es, de repente, lleno
- Que puede hacer acerca esto?
  - Bloquea el trafico que nadie quiere (viruses, gusanos, spam)
    - ***BCP 38 y 46***
  - Ahorro de eficiencia (tal vez unas 10 a 50%)
  - Cambia el comportamiento de los usuarios
- Cambiendo comportamiento requiere educacion y una politica puesta

Bloqueando Trafico no Querido

Trafico saliendo de los gusanos es el candidato mas probable:

- Identicifcar las maquinas infectados (usando sus herramientas de monitoreo)
- Limpalas y instala software antivirus
- Mantiene actualizado el software antivirus
- Bloque los puertos usados por los gusanos
- Ponga alarmas para detectar maquinas infectadas en el futuro.

Spam Entrando

El spam entrante a su institucion probablemente causa perdida de algo de su capacidad:

- El monitoreo te va a decir cuanto trafico es email.
- Haciendo filtros locales de spam pueden ayudar, pero son dificiles de implementar.
- Servicio remotos de email puede ayudar (Barracuda,
- Servicios de filtracion de correo remoto pueden ayudar (e.j. Barracuda, LBSD, Google U)

Ahorros por Eficiencia

- Corre un servidor de DNS local de Cache
- Corre un servidor de Web local de Cache (Proxy, Squid)
  - Squid: http://www.squid-cache.org/
  - WCCP de Cisco (Web Cache Communication Protocolo)
- Busca archivos bajados mayormente y traealos a un mirror (espejo) local.
- Busca trafico inter-sitio por Active Directory y los VPNs.
- Probablement no habra mucha mejoramienta con estos.

Medidas Sociales

- El abuso de la Red puede ser un problema social, no tecnico.
- En muchos casos las soluciones socials funcionan mejor:
  - Tal vez los usuarios ni saben cuanto banda de ancha estan usando.
  - Probablemente pocos usuarios toman la mayoria de su banda de ancho (aprox. 5%)
  - Probablemente los usuarios con mas habilidades tecnicas.

Medidas Sociales cont.

- 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 (saquando privilegios, etc.)

- Si es necesario hay soluciones tecnicas

Medidas Technicas

- **Priorización** de tráfico (tc, dummynet, altq)
- **Limitar** uso del banda de ancha por algunos tipos de trafico.
- **Compartiendo** en forma interactive y justa entre IPs (usuarios):
  - SFQ: Start Time Fair Queuing
  - WFQ: Weighted Fair Queuing
  - http://en.wikipedia.org/wiki/Fair_queuing
  - Hecho en software y/o hardware

Medidas Technicas cont.

- **Cuotas fijas**: Usurioas sobre el limite no tienen mas acceso.
- **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.

Prioritizacion de Trafico en Software

Hay varios proyectos. La mayoria corren bajo BSD y/o FreeBSD.

Dummynet:

```
$ sudo kldload ipfw dummynet
$ sudo ipfw add pipe 1 ip from any to 196.200.218.0/24
$ sudo ipfw add pipe 2 ip from 196.200.218.0/24 to any
$ sudo vi /etc/sysctl.conf
   net.link.bridge.ipfw=1
$ sudo /etc/rc.d/sysctl restart
```

cliente: fetch http://196.200.218.200/archivoGrande

Dummynet

Ejemplos:

Limitar trafico TCP entrante a 2Mbit/s, y UDP a 300Kbit/s.

```
ipfw add pipe 2 in proto tcp
ipfw add pipe 3 in proto udp
ipfw pipe 2 config bw 2Mbit/s
ipfw pipe 3 config bw 300Kbit/s
```

Limitar trafico entrante a 300Kbit/s por cada nodo en la Red 10.1.2.0/24

```
ipfw add pipe 4 src-ip 10.1.2.0/24 in
ipfw pipe 4 config bw 300Kbit/s queue 20 mask dst-ip 0x000000ff
```

http://info.iet.unipi.it/~luigi/dummynet/

Prioritizacion de Trafico

Otro Ejemplo del uso de Dummynet:

```
sudo ipfw queue 1 config pipe 1 weight 100
sudo ipfw queue 2 config pipe 1 weight 50
sudo ipfw queue 3 config pipe 2 weight 100
sudo ipfw queue 4 config pipe 2 weight 50
sudo ipfw flush
sudo ipfw add queue 1 icmp from any to 196.200.218.0/24
sudo ipfw add queue 2 ip from any to 196.200.218.0/24
sudo ipfw add queue 3 icmp from 196.200.218.0/24 to any
sudo ipfw add queue 4 ip from 196.200.218.0/24 to any
```

Cuotas Fijas

Usando los Flujos y una herramienta como `pmacct` para hacer una regla de “firewall” dynamica:

```
echo 'SELECT ip_dst, sum(bytes) AS bytes
FROM acct_v6
WHERE ip_dst LIKE "196.200.218.%"
AND ip_src NOT LIKE "196.200.218.%"
GROUP BY ip_dst
HAVING bytes > 1000000' |
mysql pmacct -u root |
while read ip bytes; do
    ipfw add deny ip from $ip to any
    ipfw add deny ip from any to $ip
done
```

Resumen

Hay muchas herramientas y documentación para la implementación de gestión de banda de ancha, pero…

- La mayoría es en Ingles
- El parte difícil, muchas veces, no es técnico
- Hay un problema en implementar todo esto…

Que es?

Ahora su Red estará lleno de excepciones y so pone mas complicada para resolver problemas, hacer cambios y mantener la Red en general.

Resumen cont.

Hay un problema en implementar todo esto…

Que es?

Ahora su Red estará lleno de excepciones y so pone mas complicada para resolver problemas, hacer cambios y mantener la Red en general.

Asi, pensando “fuera la caja” vale la pena.

Referencias

- Gestion de Banda de Ancha “Briefing Packs”
  http://www.inasp.info/file/72bd90cc575a6c2b3002f773553258bb/bmo-briefing-packs-workshop-materials-and-information-resources.htm
- Presentation 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
- Best Current Practices 38 (Ingress Filtering for DoS)
  http://tools.ietf.org/html/rfc2827
- Best Current Practices 46 (Egress Filtering)
  http://tools.ietf.org/html/bcp46
- How to Measure the Performance of a Caching DNS Server (Reg. Req.)
  http://www.nominum.com/info_center/register.php?iid=1781

Referencias

- 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/
- Cola Justo (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

Referencias

- 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
  - http://articles.techrepublic.com.com/5100-10878_11-6175637.html
- Cache de Web Squid
  http://www.squid-cache.org/