



Gestión de Redes

Introducción a Netflow



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license
(<http://creativecommons.org/licenses/by-nc/3.0/>)

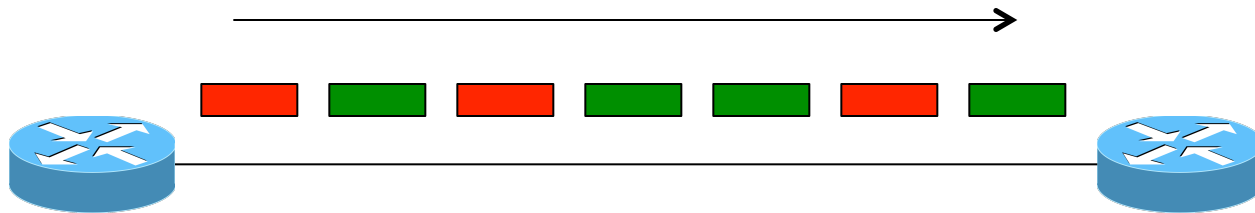
Agenda



- Netflow
 - Qué es y cómo funciona
 - Aplicaciones
- Generar y exportar registros de flujo
- Nfsen Nfdump
 - Arquitectura
 - Uso.
- Laboratorio

Que es un Flujo de Red (Flow)?

- Paquetes que tienen atributos comunes.
- En la práctica esto significa: paquetes que pertenecen a la misma conexión de transporte.
por ejemplo:
 - TCP, misma IP origen, puerto origen, IP destino, puerto de destino
 - UDP, misma IP origen, puerto origen, IP destino, puerto de destino
 - Algunas herramientas consideran "flujos bidireccionales", es decir, A-> B y B-> A como parte del mismo flujo.
- [http://en.wikipedia.org/wiki/Traffic_flow_\(computer_networking\)](http://en.wikipedia.org/wiki/Traffic_flow_(computer_networking))

Flujos simples



-  = Paquete que pertenesca a flujo X
-  = Paquete que pertenesca a flujo Y

Flujo: Definición de Cisco

Secuencia unidireccional de paquetes que comparten:

1. Dirección IP origen.
2. Dirección IP destino.
3. Puerto de origen para UDP o TCP, ó “0” para otros protocolos.
4. Puerto de destino para UDP o TCP, tipo y código para ICMP, ó “0” para otros protocolos
5. Protocolo de IP.
6. Interfaz de Ingreso (SNMP ifIndex)
7. Tipo de Servicio IP

IOS: cuál de estos seis paquetes se encuentran en el mismo flujo?

	<i>Src IP</i>	<i>Dst IP</i>	<i>Protocol</i>	<i>Src Port</i>	<i>Dst Port</i>
A	1.2.3.4	5.6.7.8	6 (TCP)	4001	80
B	5.6.7.8	1.2.3.4	6 (TCP)	80	4001
C	1.2.3.4	5.6.7.8	6 (TCP)	4002	80
D	1.2.3.4	5.6.7.8	6 (TCP)	4001	80
E	1.2.3.4	8.8.8.8	17 (UDP)	65432	53
F	8.8.8.8	1.2.3.4	17 (UDP)	53	65432

Contabilidad de flujos

- Un resumen de todos los paquetes que se observan en un flujo (hasta el momento).
 - Identificación del flujo: protocolo, IP origen/destino, puerto....
 - Conteo de paquetes,
 - Conteo de Bytes.
 - Tiempos de inicio/finalización.
 - Tal vez información adicional, como por ejemplo; números de Sistemas Autónomos (AS), máscaras de red.
- Registrar el volumen de tráfico, no el contenido.

Usos y Aplicaciones

- Puede responder a preguntas como:
 - ¿Que usuario o departamento ha estado cargando o descargando mas?
 - ¿Cuáles son los protocolos más utilizados en la red?
 - ¿Qué dispositivos están enviando más tráfico SMTP, y para dónde?
- Identificación de anomalías y ataques.
- Visualización mas minuciosa (representación grafica) que se puede hacer a nivel de interfaz.

Trabajando con flujos

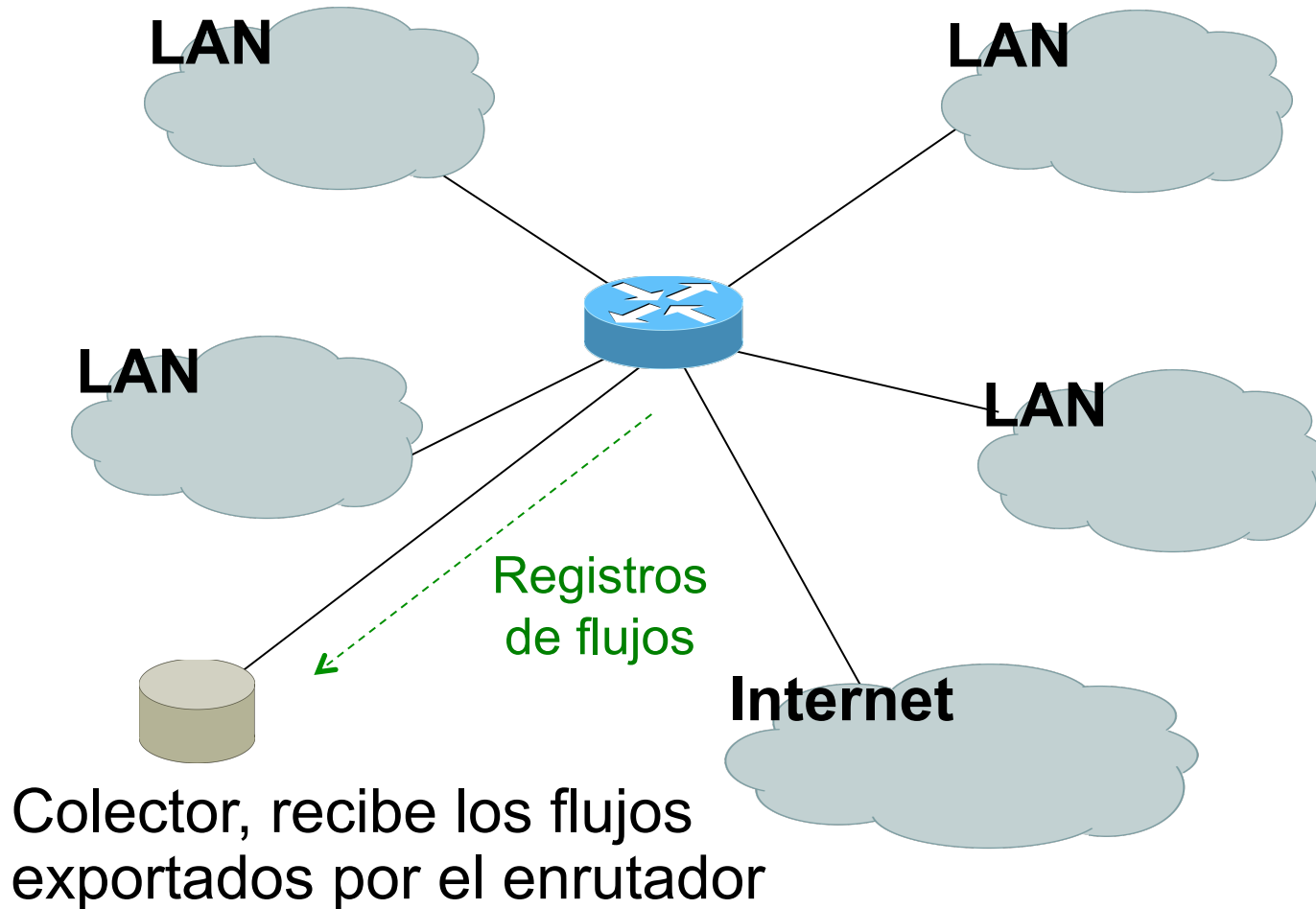
1. Hay que generar los flujos en el dispositivo (enrutador o conmutador).
2. Exportar los flujos desde el dispositivo a un colector
 - Configurar protocolo, versión y destino.
3. Recopilar los flujos, escribirlos al disco.
4. Analizarlos

Hay muchas herramientas disponibles, tanto gratuitos como comerciales

Donde generar registros de flujo

1. En un router u otro dispositivo de red
 - Si el dispositivo lo soporta.
 - No se requiera hardware adicional.
 - Podría tener algún impacto en el rendimiento.
2. Colector pasivo (por lo general Unix)
 - Recibe una copia de cada paquete y genera los flujos.
 - Requiera un puerto espejo.
 - Muchos recursos.

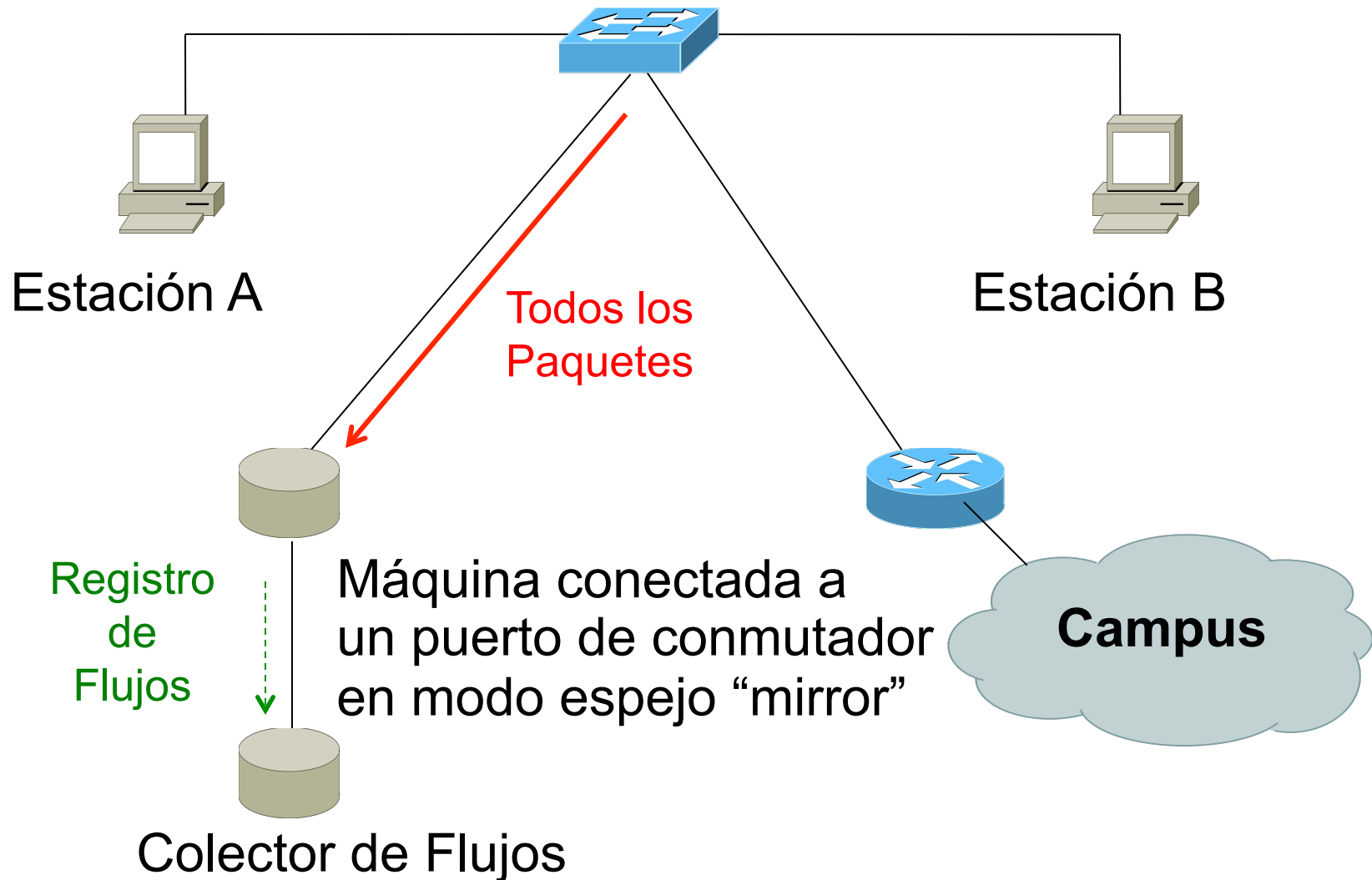
Recopilación en el enrutador



Recopilación desde enrutador

- Con este método se pueden observar todos los flujos en la red
 - Pero el enrutador tiene más carga porque tiene que procesar y exportar los flujos
- Opcionalmente se pueden seleccionar para cuales interfaces se habilitara la generación de flujos, y no activarlo para demás
- Además, si hay enrutadores en cada segmento de red local, se puede habilitar la recopilación y exportación de flujos en esos enrutadores, y así reducir la carga en el enrutador central.

Colector pasivo



Colector pasivo

- Ejemplos: softflowd (Linux/BSD), pfflowd (BSD), ng_netflow (BSD)
- El colector sólo verá los flujos desde el punto de vista de la red donde se encuentra
- Tiene la ventaja de que releva al enrutador del trabajo de generar y exportar los flujos
- Útil para enlaces con un solo punto de entrada a la red, o donde sólo se requiere observar un segmento de la red.
- Se puede implementar en conjunto con un IDS.

Un pensamiento:

- Su red probablemente tiene un dispositivo que mantiene un registro de las direcciones IP y números de puerto de tráfico que fluye a través de él.

¿Cual es?

Protocolos de exportacion de flujo

- Cisco Netflow, diferentes versiones.
 - v5: ampliamente desplegado.
 - v9: nueva, extensible, incluye soporte IPv6.
 - IPFIX: estándar IETF, basado en NetFlow v9.
 - sFlow: Basado en muestreo, se encuentran comúnmente en los switches.
 - Flow: Juniper.
- Nos concentraremos en Netflow, pero muchas herramientas soportan varios protocolos.

Netflow de Cisco

- Flujos unidireccionales.
- IPv4 unicast y multicast.
 - (IPv6 en Netflow v9)
- Flujos exportados utilizando UDP.
 - Elija un puerto. No existe un estándar en particular, aunque son de uso común 2055 y 9996.
- Soportado en las plataformas IOS, ASA y CatOS – Pero con diferentes implementaciones.

Configuración de IOS

- Se configura en cada interfaz de entrada
- Definir la versión.
- Definir la dirección IP del colector a donde se van a enviar los flujos
- Opcionalmente:
 - Se puede habilitar tablas de agregación
 - Configurar los tiempos de caducidad y el tamaño de tabla (v5) de flujos
 - Configurar el período y tipo de muestreo.

Resumen de comandos (1)

➤ Activar CEF (por defecto)

```
ip cef
```

➤ Activar flujos en cada interfaz

```
ip route cache flow
```

```
0
```

```
ip flow ingress
```

```
ip flow egress
```

➤ Ver los flujos

```
show ip cache flow
```

```
show ip flow top-talkers
```

Resumen de comandos (2)

```
ip flow-top-talkers
top 10
sort-by bytes
```

```
gw-169-223-2-0#sh ip flow top-talkers
```

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Bytes
Fa0/1	169.223.2.2	Fa0/0	169.223.11.33	06	0050	0B64	3444K
Fa0/1	169.223.2.2	Fa0/0	169.223.11.33	06	0050	0B12	3181K
Fa0/0	169.223.11.33	Fa0/1	169.223.2.2	06	0B12	0050	56K
Fa0/0	169.223.11.33	Fa0/1	169.223.2.2	06	0B64	0050	55K
Fa0/1	169.223.2.2	Local	169.223.2.1	01	0000	0303	18K
Fa0/1	169.223.2.130	Fa0/0	64.18.197.134	06	9C45	0050	15K
Fa0/1	169.223.2.130	Fa0/0	64.18.197.134	06	9C44	0050	12K
Fa0/0	213.144.138.195	Fa0/1	169.223.2.130	06	01BB	DC31	7167
Fa0/0	169.223.15.102	Fa0/1	169.223.2.2	06	C917	0016	2736
Fa0/1	169.223.2.2	Local	169.223.2.1	06	DB27	0016	2304

```
10 of 10 top talkers shown. 49 flows processed.
```

Resumen de comandos (3)

➤ Exportar los flujos al colector

```
ip flow-export version 5 [origin-as|peer-as]  
ip flow-export destination x.x.x.x <udp-port>
```

➤ *origin-as* incluirá el número del AS de origen en el flujo mientras que *peer-as* sólo incluirá el número de AS del AS vecino de donde se aprendió la ruta para el prefijo

➤ Exportación de flujos agregados

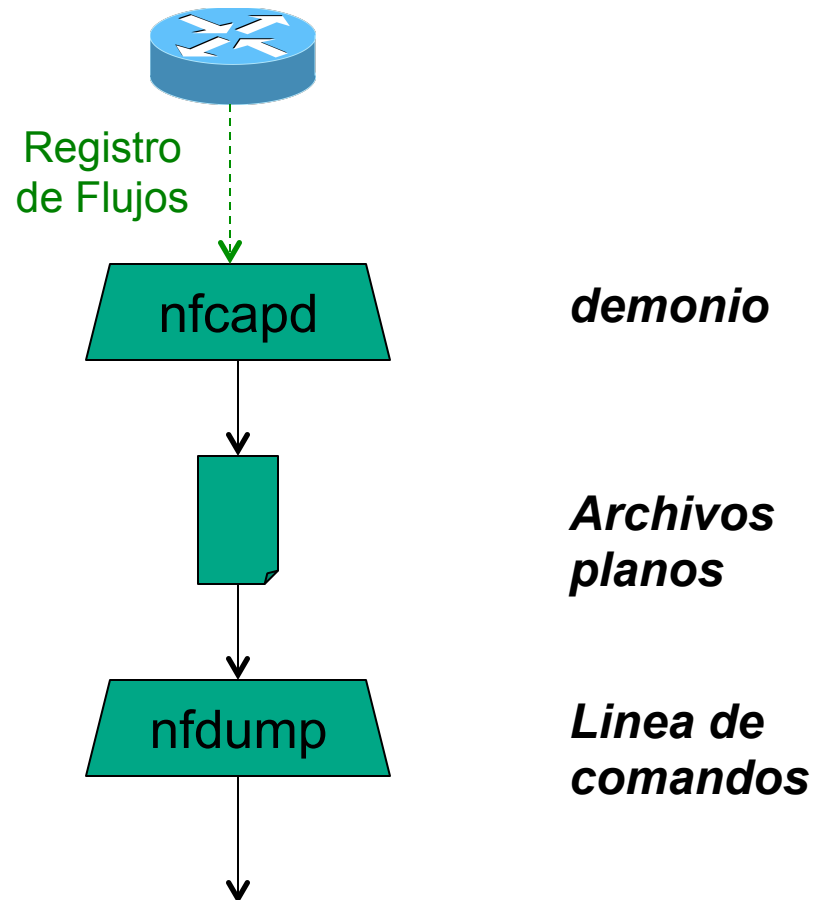
```
ip flow-aggregation cache as|prefix|dest|source|proto \  
    enabled  
export destination x.x.x.x <udp-port>
```

¿PREGUNTAS?

Recopilacion de flujos: Nfdump

- Libre y de código abierto.
- nfcapd escucha los registros de flujo de entrada y los escribe en el disco (archivos planos)
 - normalmente inicia un nuevo archivo cada 5 minutos.
- nfdump lee los archivos y los convierte en una salida legible.
- nfdump tiene opciones de línea de comandos para filtrar y agregar los flujos.

Arquitectura de Nfdump

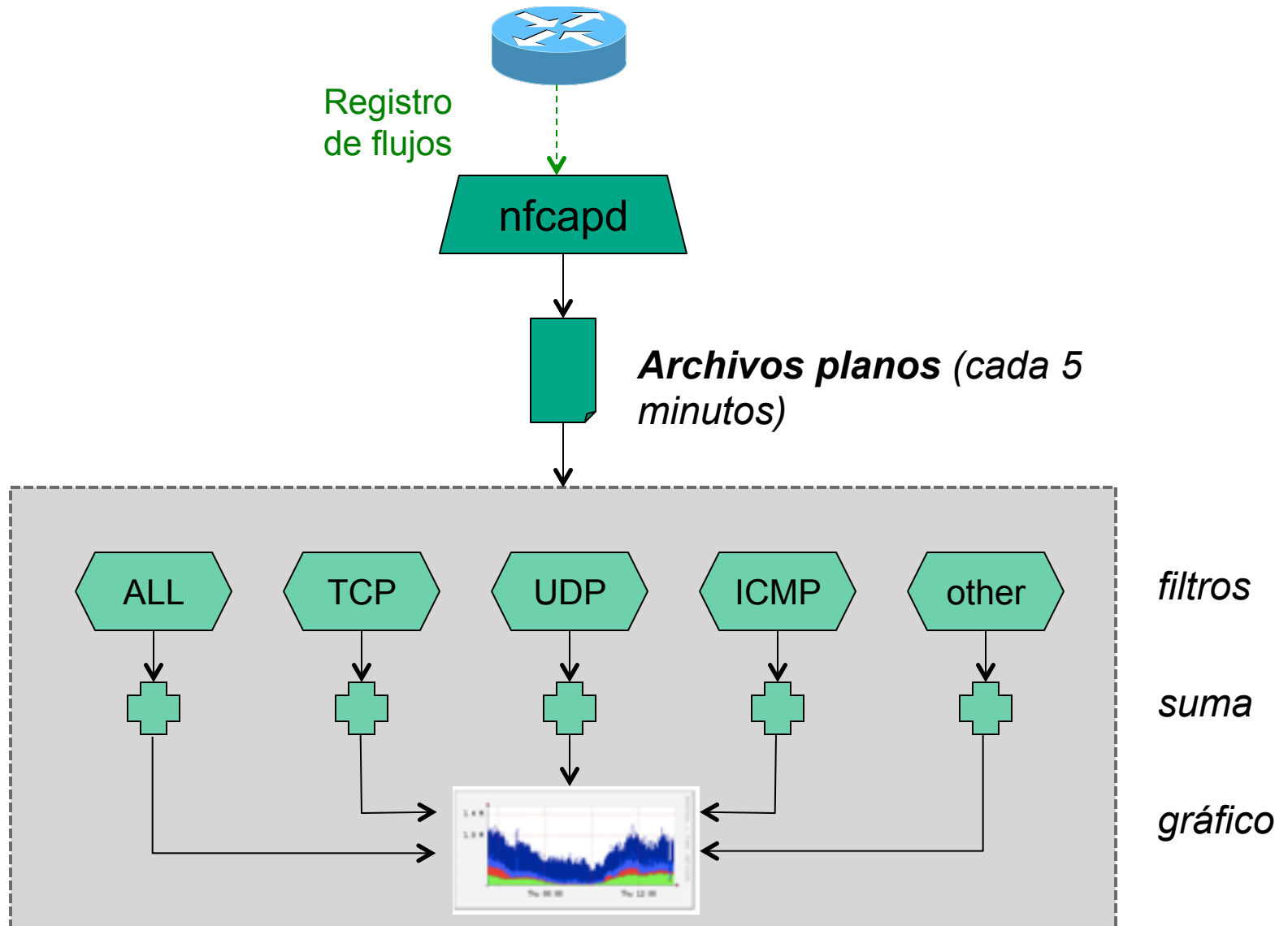


Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2013-04-18 13:35:23.353	1482.000	UDP	10.10.0.119:55555	->	190.83.150.177:54597	8683	445259	1
2013-04-18 13:35:23.353	1482.000	UDP	190.83.150.177:54597	->	10.10.0.119:55555	8012	11.1 M	1
2013-04-18 13:48:21.353	704.000	TCP	196.38.180.96:6112	->	10.10.0.119:62099	83	20326	1
2013-04-18 13:48:21.353	704.000	TCP	10.10.0.119:62099	->	196.38.180.96:6112	105	5085	1

Analisis de Flujos: Nfsen

- Compañero de nfdump.
- web GUI.
- Crea gráficos RRD de los totales de tráfico.
- Permite aumentar zoom a un momento de interés y hacer un análisis nfdump.
- Administra instancias nfcapd para usted
 - Puede ejecutar varias instancias nfcapd para escuchar los flujos de múltiples routers.
- Plugins disponibles, por ejemplo; port tracker, SurfMap.

Arquitectura de Nfsen



NFSen: puntos a tener en cuenta

- Cada 5 minutos nfcapd inicia un nuevo archivo, y nfsen procesa el anterior.
- Por lo tanto cada punto de gráfico cubre 5 minutos.
- El gráfico muestra el total de tráfico seleccionado en ese período de 5 minutos.
- Para obtener información más detallada de los flujos individuales en ese período, la interfaz gráfica de usuario le permite profundizar con nfdump.

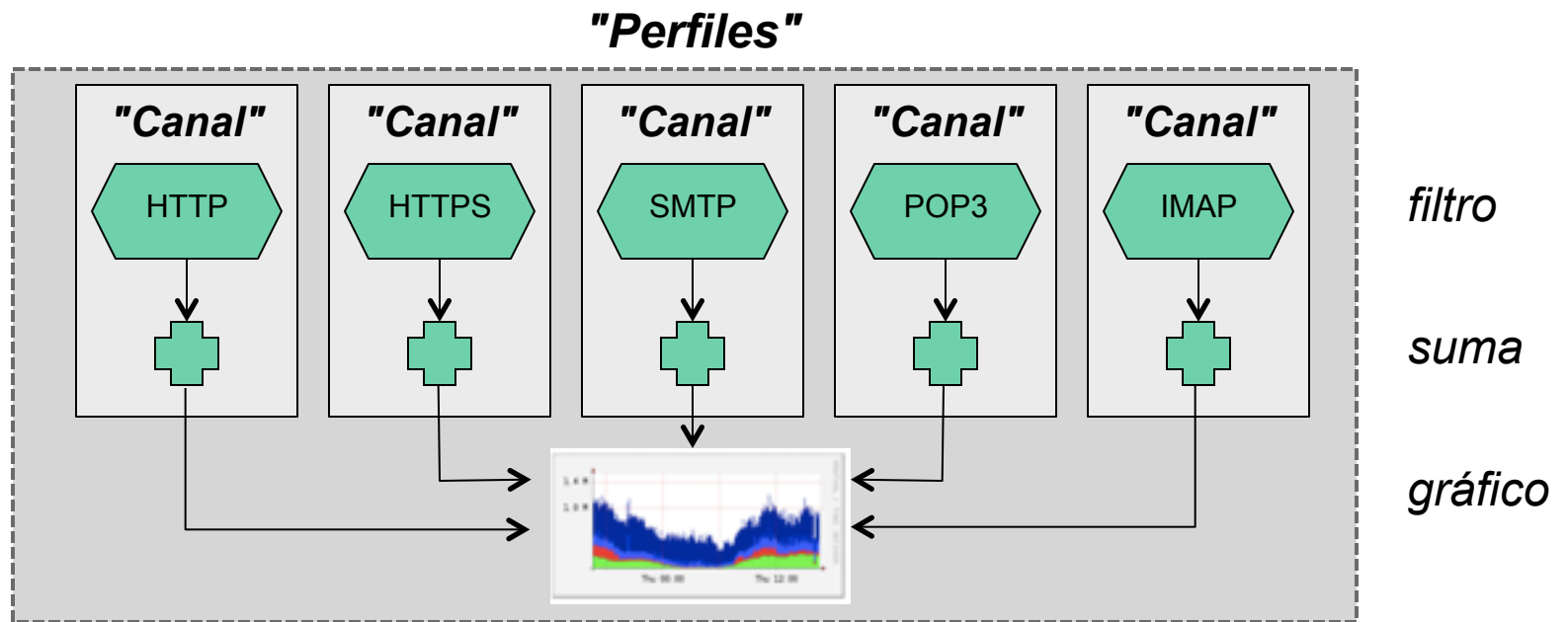
Demostración

- Usando nfsen para encontrar mayores usuarios de ancho de banda.

Perfiles y canales

- Un "canal" identifica un tipo de tráfico para gráficar, y un "perfil" es un conjunto de canales, que pueden ser mostrados juntos.
- Usted puede crear sus propios perfiles y canales, y por lo tanto los gráficos. por ejemplo;
 - Total HTTP, HTTPS, el tráfico SMTP (etc)
 - El tráfico hacia y desde el “Departamento de Ciencia”.
 - ...
- Utilice filtros para definir el tráfico de interés.

Perfiles y canales



Referencias - Herramientas

- **nfdump and nfsen:**
<http://nfdump.sourceforge.net/>
<http://nfsen.sourceforge.net/>
<http://nfsen-plugins.sourceforge.net/>
- **pmacct and pmgraph:**
<http://www.pmacct.net/>
<http://www.aplivate.org/pmgraph/>
- **flow-tools:**
<http://www.splintered.net/sw/flow-tools>

Referencias – Mas información

- Wikipedia:
<http://en.wikipedia.org/wiki/Netflow>
- IETF standards effort:
<http://www.ietf.org/html.charters/ipfix-charter.html>
- Abilene NetFlow page
<http://abilene-netflow.itec.oar.net/>
- Cisco Centric Open Source Community
<http://cosi-nms.sourceforge.net/related.html>
- Cisco NetFlow Collector User Guide
http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/6.0/tier_one/user/guide/user.html

El fin

- (Materiales de referencia adicionales a continuación)

Ejemplos de filtros

<code>any</code>	<i>todo el trafico</i>
<code>proto tcp</code>	<i>solo trafico TCP</i>
<code>dst host 1.2.3.4</code>	<i>solo trafico para 1.2.3.4</i>
<code>dst net 10.10.1.0/24</code>	<i>solo trafico para este rango</i>
<code>not dst net 10.10.1.0/24</code>	<i>solo trafico no de ese rango</i>
<code>proto tcp and src port 80</code>	<i>solo TCP con puerto 80 origen</i>
<code>dst net 10.10.1.0/24 or dst net 10.10.2.0/24</code>	<i>solo trafico para estas redes.</i>
<code>dst net 10.10.1.0/24 and proto tcp and src port 80</code>	<i>sólo el tráfico HTTP de respuesta a esa red</i>
<code>(dst net 10.10.1.0/24 or dst net 10.10.2.0/24) and proto tcp and src port 80</code>	

...posibles combinaciones mas complejas

Flujos y Aplicaciones: Más ejemplos

Usos para NetFlow

- Identificación y resolución de problemas
 - Clasificación del tráfico
 - Rastreo de DoS (ver presentación de Danny McPherson)
- Análisis e ingeniería de tráfico
 - Análisis de tráfico entre sistemas autónomos
 - Reportes de proxis de aplicación
- Contabilidad (o facturación)
 - Verificación de la información obtenidas de otras fuentes
 - Se puede verificar contra datos obtenidos vía SNMP

Detección de anomalías: El worm SQL “Slammer”

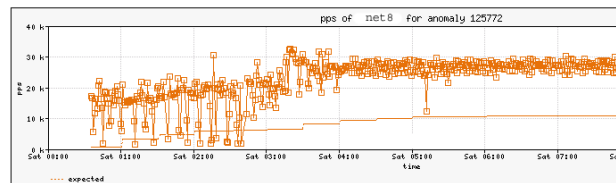
peakflow | DoS

Recent Anomalies : Anomaly 125772 : Detailed Statistics 11:51:49 EST 27 Jan 2003

Status Topology Ongoing Recent Dark IP Admin About

Anomaly 125772 Detailed Statistics

ID	Importance	Severity	Duration	Direction
125772	High	958.2% of 3.40 Kpps	09h 06m 47s	Outgoing



Affected Network Elements

Router net8 1.2.3.4

	Triggering	Expected	Difference	Max
Bitrate	71.69 Mbps	2.34 Mbps	69.35 Mbps	105.26 Mbp
Packet Rate	22.20 Kpps	712 pps	21.49 Kpps	32.58 Kpps

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Summary of all Data Snapshots Collected:

	Bytes	Packets	Bytes/Pkt	bps
	308.01 GB	762,849,500	404 B	76.05 Mbps

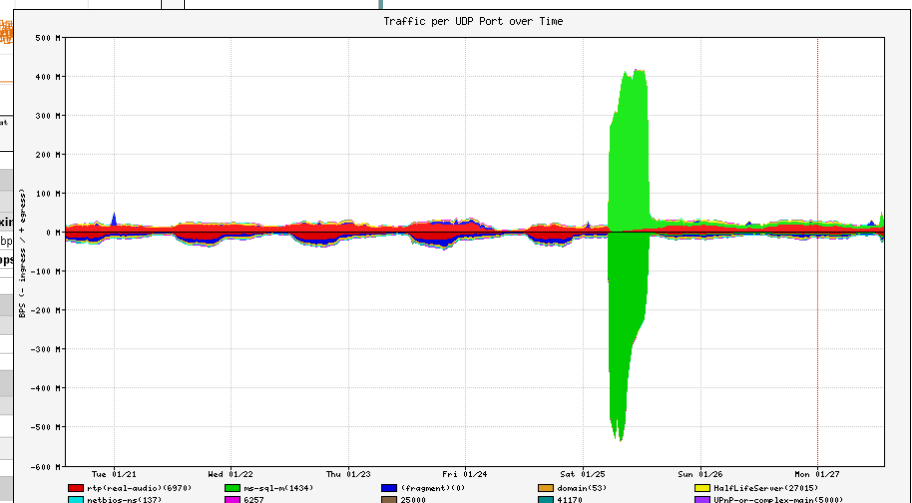
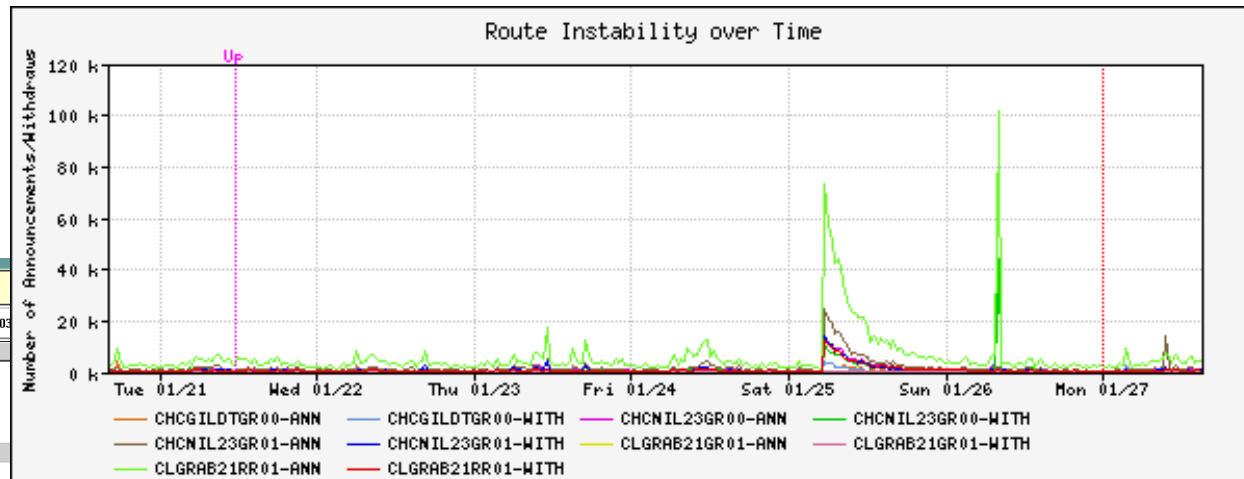
Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Source Addresses

Network / Mask	Bytes	Packets	Bytes/Pkt	bps
192.168.20.217/32	168.22 GB	416,436,800	404 B	41.54 Mbps
192.168.18.187/32	139.53 GB	345,372,800	404 B	34.45 Mbps

Summary | Source Addresses | Destination Addresses | Source Ports | Destination Ports | Protocols | Output Interfaces | Input Interfaces | Generate Filter

Destination Addresses



Detección basada en flujo

Una vez se hayan establecido puntos de referencia, se pueden detectar anomalías

- Basándose puramente en las tasas (pps o bps), puede haber falsas alarmas
- Algunas anomalías pueden detectarse enseguida, incluso sin un punto de referencia (Ej., TCP SYN o RST floods)
- Se pueden definir “**firmas**” o “**huellas**” para detectar tráfico de transacciones “interesantes” (Ej., proto udp y puerto 1434 y 404 octetos (376 payload) == slammer!)
- Se puede mejorar la precisión de la detección añadiendo la dimensión temporal a las firmas

Herramientas comerciales para Flujos

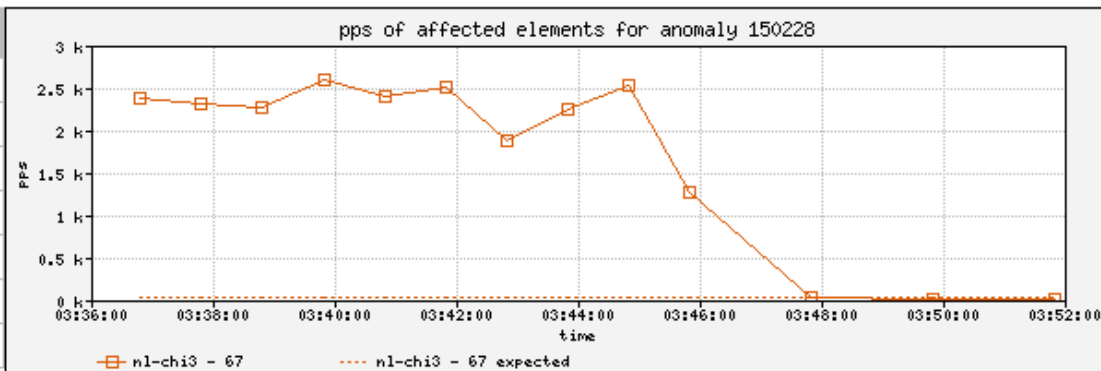
Anomaly 150228

Get Report: [PDF](#) [XML](#)

ID	Importance	Duration	Start Time	Direction	Type	Resource
150228	High 130.0% of 2 Kpps	17 mins	03:34, Aug 16	Incoming	Bandwidth (Profiled)	Microsoft 207.46.0.0/16 windowsupdate.com

Traffic Characterization

Sources	204.38.130.0/24
	204.38.130.192/26
	1024 - 1791
Destination	207.46.248.234/32
	80 (http)
Protocols	tcp (6)
TCP Flags	S (0x02)

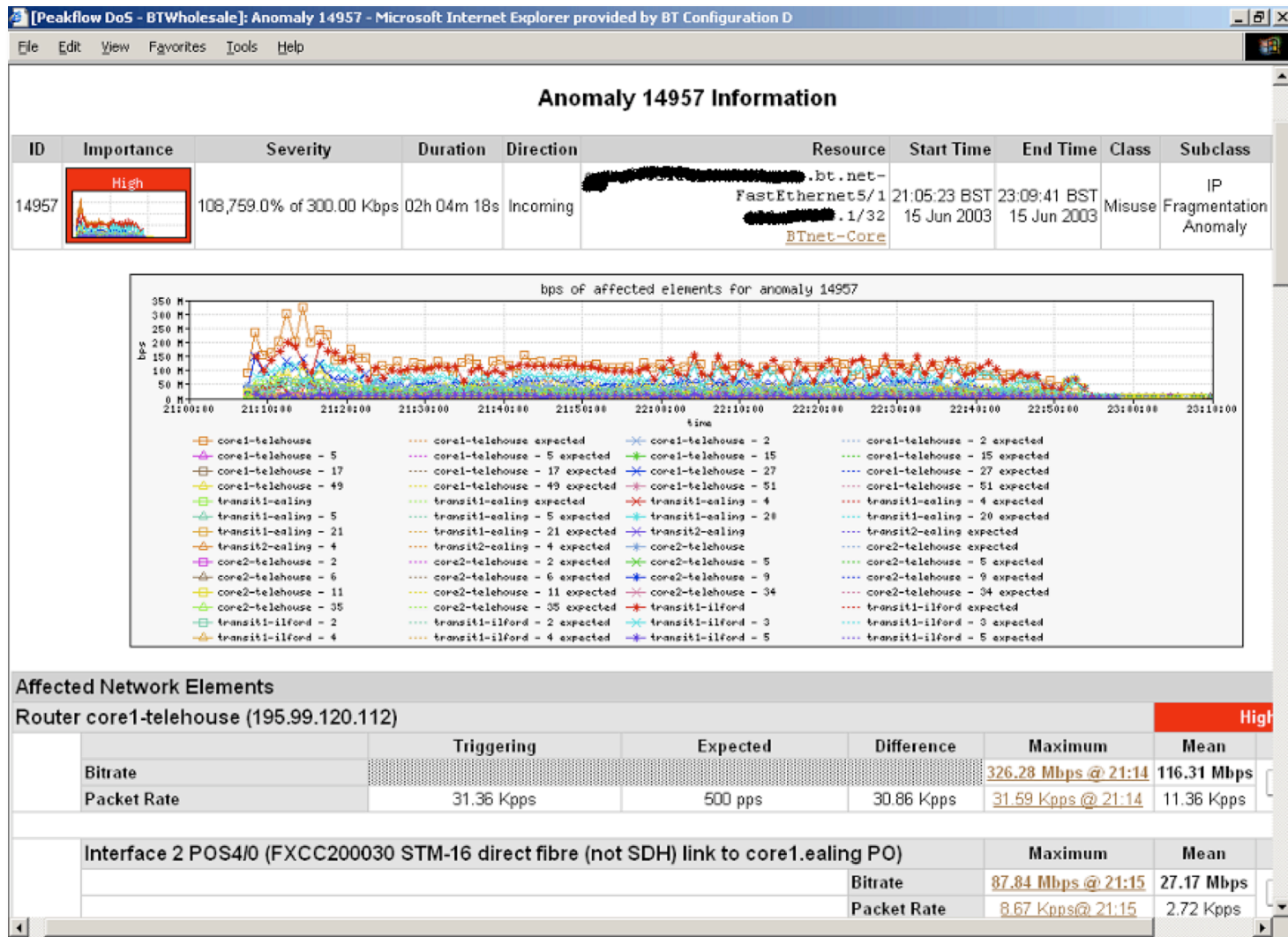


Affected Network Elements

	Importance	Expected	Observed bps		Observed pps		
		pps	Max	Mean	Max	Mean	
Router nl-chi3 198.110.131.125	High						
Interface 67 at-1/1/0.14 <i>pvc to WMU</i>		26	832 K	563.1 K	2.6 K	1.7 K	Details

Anomaly Comments

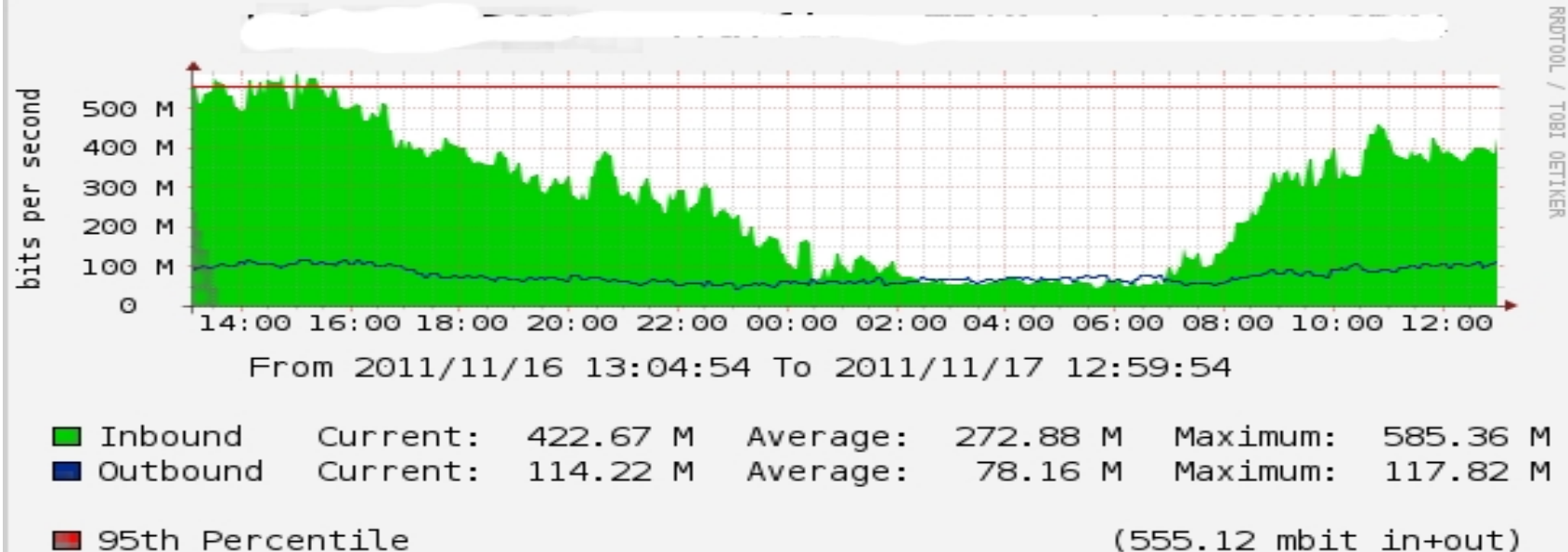
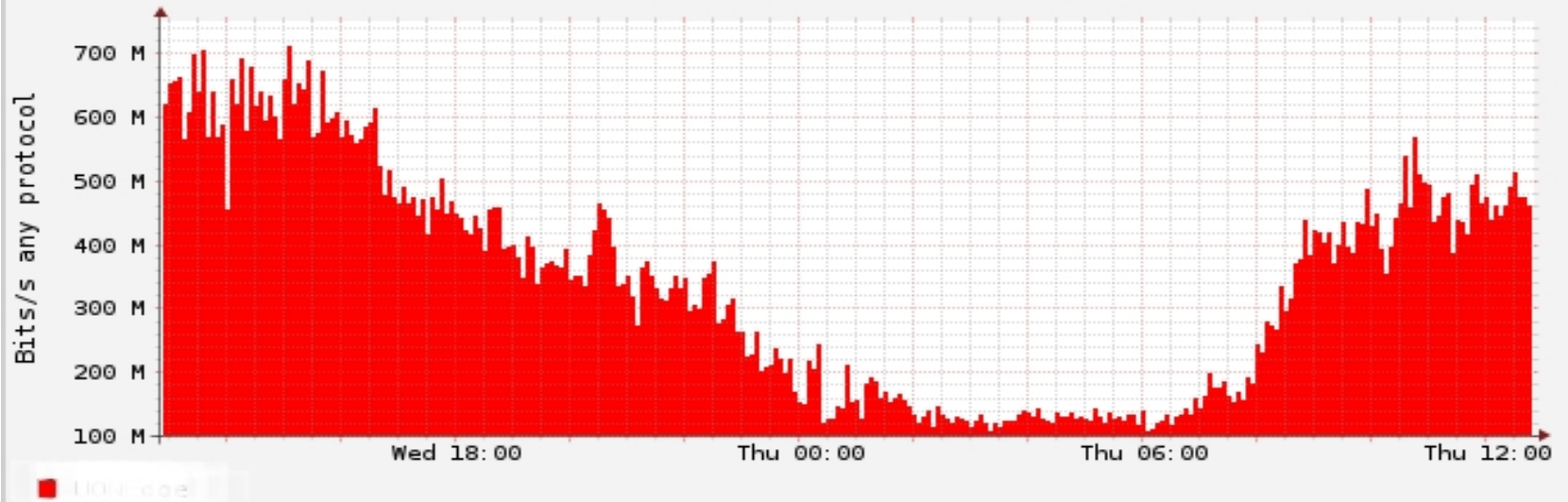
Detección comercial: Un ataque DoS de mayor escala



Contabilidad

Puede suplementarse la contabilidad basada en SNMP con la basada en flujos (ver siguiente gráfico).

Thu Nov 17 00:50:00 2011 Bits/s any protocol



Versiones de Cisco Netflow

NetFlow Version 1

- Campos clave: IP destino/origen, Puerto destino/origen, Protocolo IP, ToS, Interfaz de entrada.
- Contabilidad: Paquetes, Octetos, tiempo de inicio/término, Interfaz de salida
- Otros: O lógico de las banderas TCP.
- Obsoleto

NetFlow Versiones 2-4

- Internas de Cisco
- Nunca se publicaron

NetFlow v5

- Campos clave: IP destino/origen, Puerto destino/origen, Protocolo IP, ToS, Interfaz de entrada.
- Contabilidad: Paquetes, Octetos, tiempo de inicio/término, Interfaz de salida.
- Otros: O lógico de banderas TCP, AS destino/origen, máscara de red.
- El formato de paquete introduce números de secuencia para detectar la pérdida de flujos.
- IPv4 solamente

NetFlow v8

- Flujos v5 agregados
- No todos los tipos están disponibles en todos los equipos
- Muchos menos datos que procesar, pero pierde la granularidad de v5
 - No hay direcciones IP

NetFlow v9

- IPv6
- Campos adicionales como etiquetas MPLS
- Construido sobre las versiones anteriores
- Periódicamente manda un paquete de “plantilla” – todo los campos de datos de flujos refieren a la plantilla.