



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

Flow-tools

- Cuestiones con la arquitectura
- Herramientas de software, etc.

Laboratorio

Flujos de red (flows)

- Paquetes que tienen atributos comunes
- Política de creación y terminación – condiciones que afectan el inicio y final de un flujo.
- Contadores – paquetes, octetos, tiempo.
- Información de enrutamiento– AS, máscara de red, interfaces.

Flujo: Definición de Cisco

Secuencia uni-direccional de paquetes que comparten:

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

Flujos de red

- Unidireccionales o bidireccionales.
- Los flujos bidireccionales pueden contener otra información tal como el tiempo de ida y vuelta o el comportamiento TCP
- Los flujos de aplicación van más allá de los encabezados para clasificar los paquetes por su contenido.
- Flujos agregados – Flujos de flujos.

Trabajando con Flows

- Hay que generar los flujos en el equipo (router).
- Exportar los flujos a un colector
 - Configurar la versión de NetFlow
 - Tasas de muestras
- Recopilar los flujos
 - Herramientas – flow-tools, nfcap, etc
- Analizarlos
 - Muchas herramientas, o puede escribir la suya propia

Descriptores de flujos

- Una definición con más elementos generará más flujos.
- Mayor número de flujos implica:
 - Más tiempo para generar reportes
 - Más RAM y CPU para el dispositivo que genera los flujos
 - Más espacio de almacenamiento en la máquina que almacena/procesa los flujos
- Depende de la aplicación
 - Ingeniería de tráfico vs. detección de intrusiones

Contabilidad de Flujos

- Se acumula información de contabilidad.
- Paquetes, octetos, tiempo de inicio, tiempo de fin, etc.
- Información de enrutamiento – máscaras y números de sistema autónomo.

Generación/Recopilación

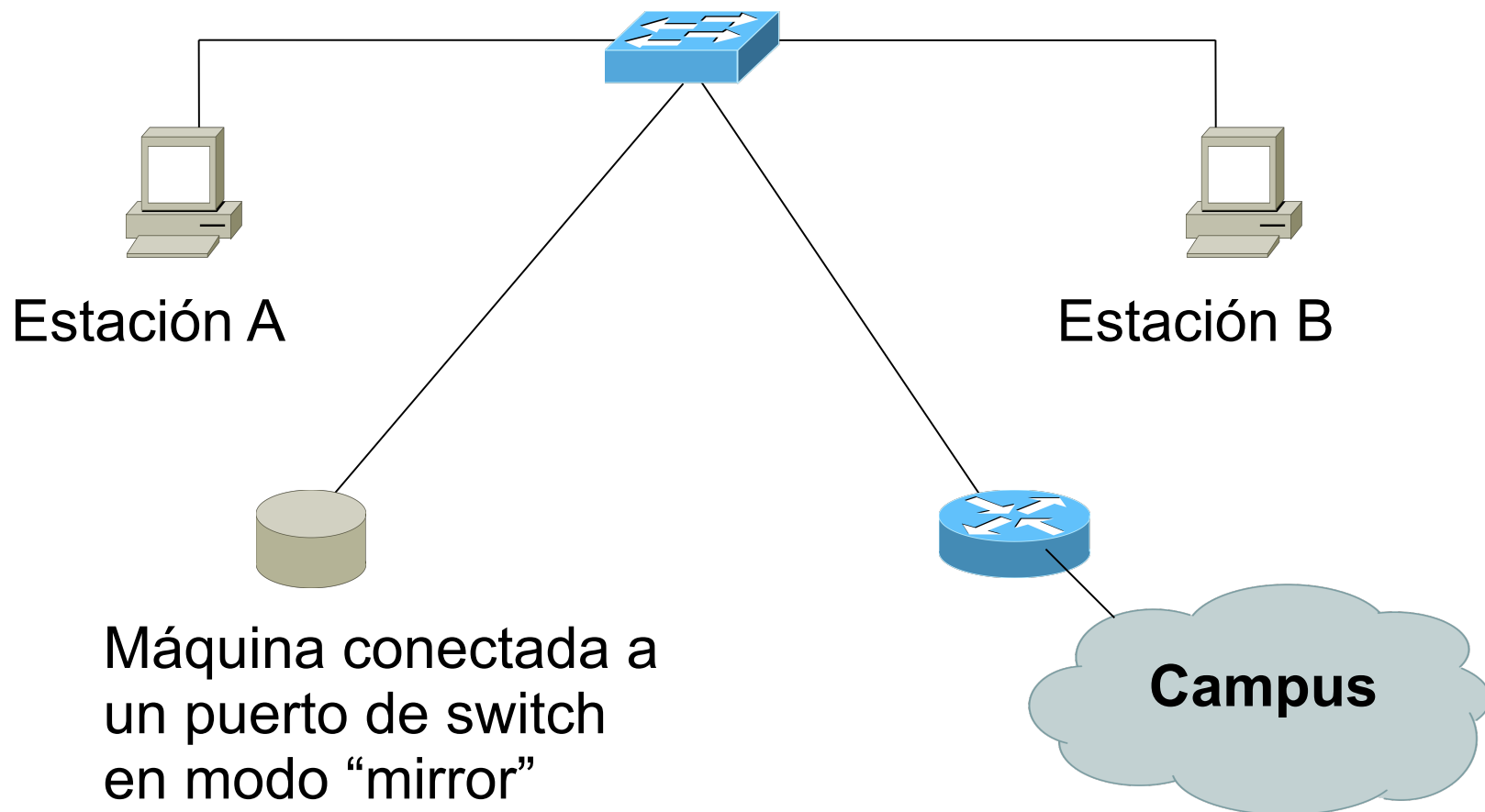
Monitor pasivo

- Un monitor pasivo (servidor Unix/Linux) recibe todos los paquetes y genera los flujos.
- Uso intensivo de recursos

Enrutador u otro dispositivo

- Un enrutador (o switch) genera los flujos
- Es posible hacer muestreo
- No es necesario nada más

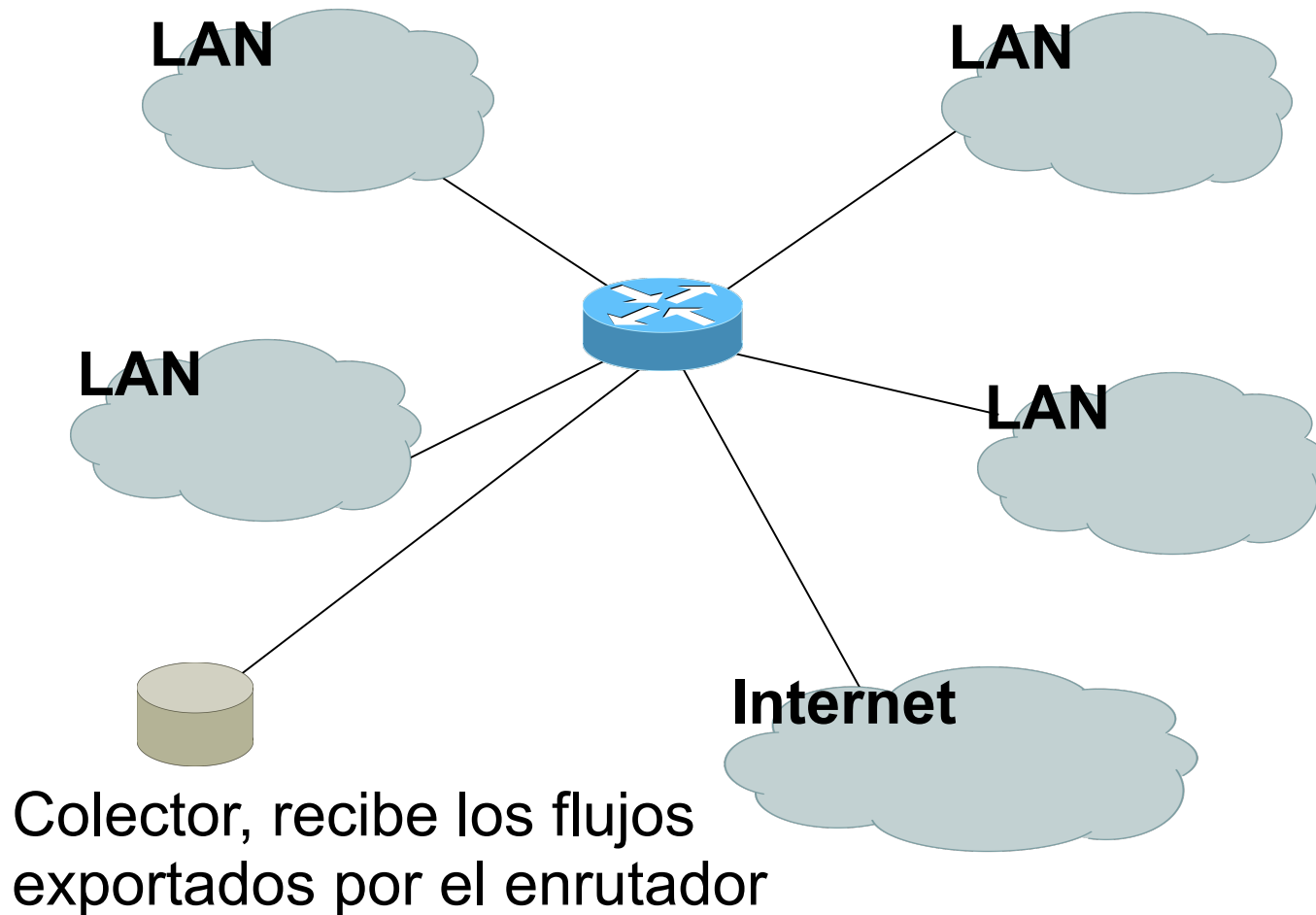
Colector pasivo



Colector pasivo

- Si se usa un colector pasivo no se verán todos los flujos de la red (a diferencia de hacerlo desde el enrutador mismo)
 - El colector sólo verá los flujos desde el punto de la red donde se encuentra
- Pero tiene la ventaja de que alivia al enrutador del trabajo de generar y exportar los flujos
- Útil en casos en los que hay un sólo punto de salida de la red, o donde sólo se requiere observar una sección del tráfico

Recopilación desde enrutador



Recopilación desde enrutador

- Con este método se pueden observar todos los flujos de la red
 - Pero el enrutador tiene más carga
- Una opción es seleccionar algunas interfaces en las cuales se generarán flujos, y dejar otras fuera
- Además, si hay otros enrutadores conectados a otras redes locales, puede exportarse flujos desde éstos para evitar cargar al enrutador del core.

Netflow de Cisco

- Flujos unidireccionales.
- IPv4 unicast y multicast.
- Agregados y sin agregar.
- Exportados sobre UDP.
- Soportado en las plataformas IOS y CatOS.
- El Netflow de Catalyst es una implementación distinta.

Versiones de Netflow de Cisco

- 4 tipos sin agregación (1,5,6,7).
- 14 tipos con agregación (8.x, 9).
- Cada versión tiene su formato de paquete distinto.
- La Versión 1 no tiene números de secuencia.
- La “version” define que tipo de datos hay en el flujo
- Algunas versiones son específicas para la plataforma Catalyst

NetFlow Version 1

- Campos clave: IP destino/fuente, Puerto destino/fuente, Protocolo IP, ToS, Interfaz de entrada.
- Contabilidad: Paquetes, Octetos, tiempo de inicio/fin, paquete de salida
- Otros: OR lógico de las banderas TCP.
- Obsoleto

NetFlow Versiones 2-4

- Internas de Cisco
- Nunca se publicaron

NetFlow v5

- Campos clave: IP destino/fuente, Puerto destino/fuente, Protocolo IP, ToS, Interfaz de entrada.
- Contabilidad: Paquetes, Octetos, tiempo de inicio/fin, paquete de salida.
- Otros: OR lógico de banderas TCP, AS destino/origen, máscara de red.
- El formato de paquete añade un número de secuencia para detectar flujos perdidos.
- IPv4 solamente

NetFlow v8

- Flujos v5 agregados
- No 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

Configuración de IOS

- Se configura en cada interfaz de entrada
- Definir la versión.
- Definir la dirección IP del colector
- Agregar tablas de agregación (opcional)
- Configurar los tiempos de caducidad y el tamaño de tabla (v5) principal (opcional)
- Configurar el período de muestreo (opcional).

Configuración de IOS

```
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

- Activar CEF (por defecto)
 - `ip cef`
- Activar flujos en cada interfaz
 - `ip route cache flow`
 - OR
 - `ip flow ingress`
 - `ip flow egress`
- Ver los flujos
 - `show ip cache flow`
 - `show ip flow top-talkers`

Resumen de comandos

- 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 de AS original en el flujo mientras que *peer-as* sólo incluirá el número de AS del vecino con el que se hace peering
- Exportación de flujos agregados

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

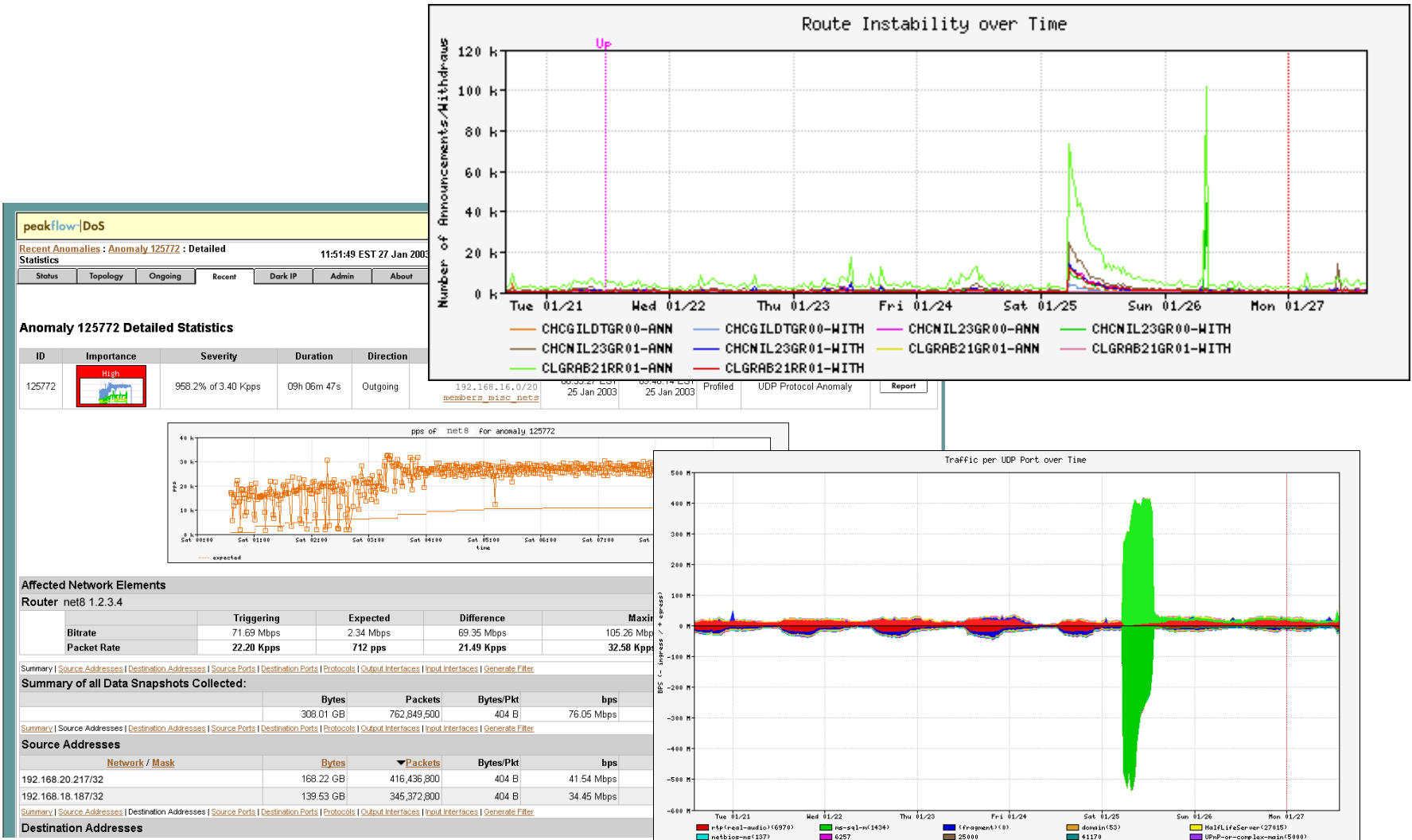



Netflow y Aplicaciones

Usos para NetFlow

- Identificación y resolución de problemas
 - Clasificación del tráfico
 - Análisis de DoS (ver presentación de Danny McPherson)
- Análisis e ingeniería de tráfico
 - Análisis de tráfico entre sistemas autónomos
 - Reportes en proxies de aplicación
- Contabilidad (facturación)
 - Comprobación cruzada con otras fuentes
 - (SNMP)

Detección de anomalías: El worm SQL “Slammer”

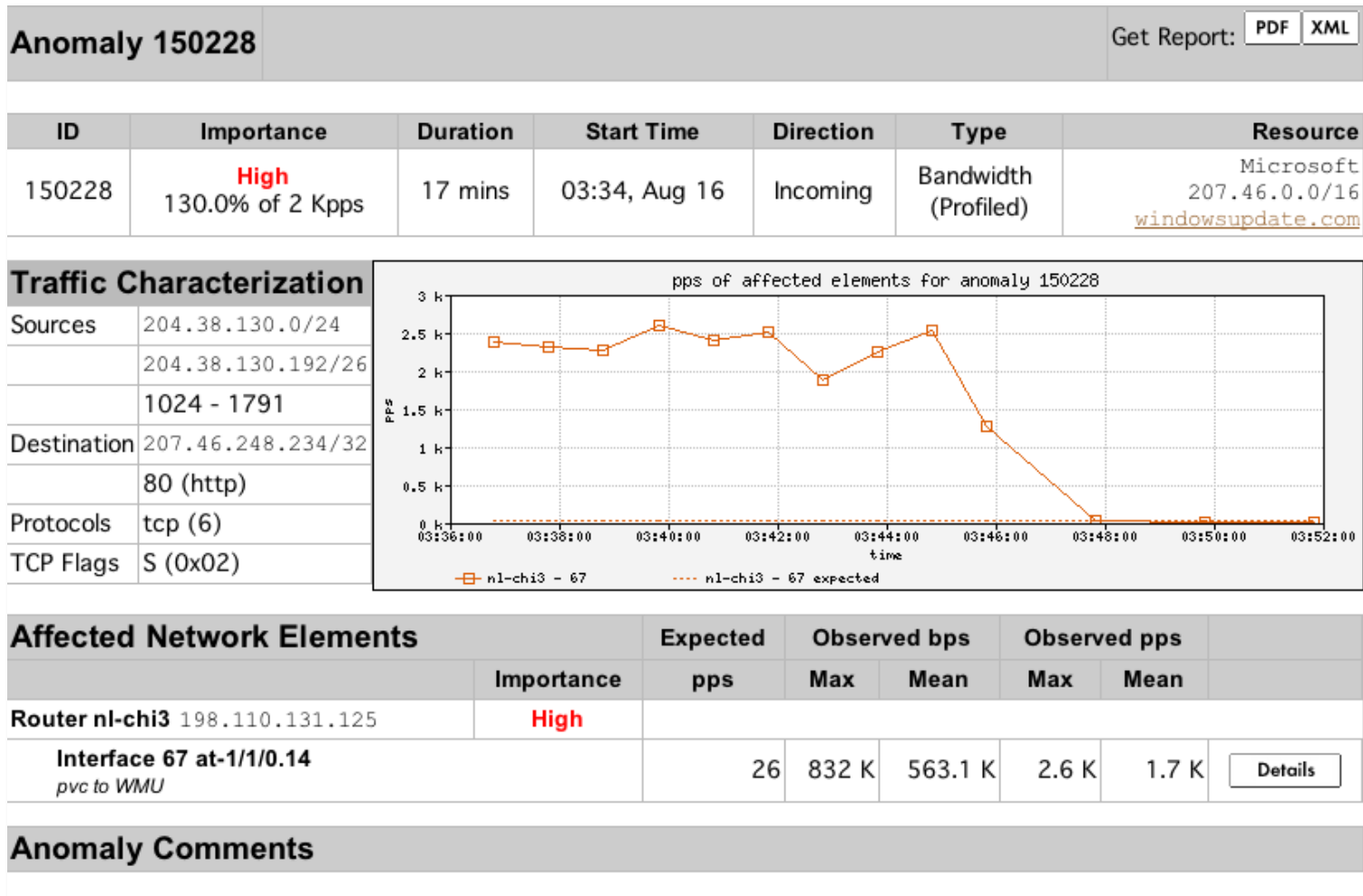


Detección de anomalías

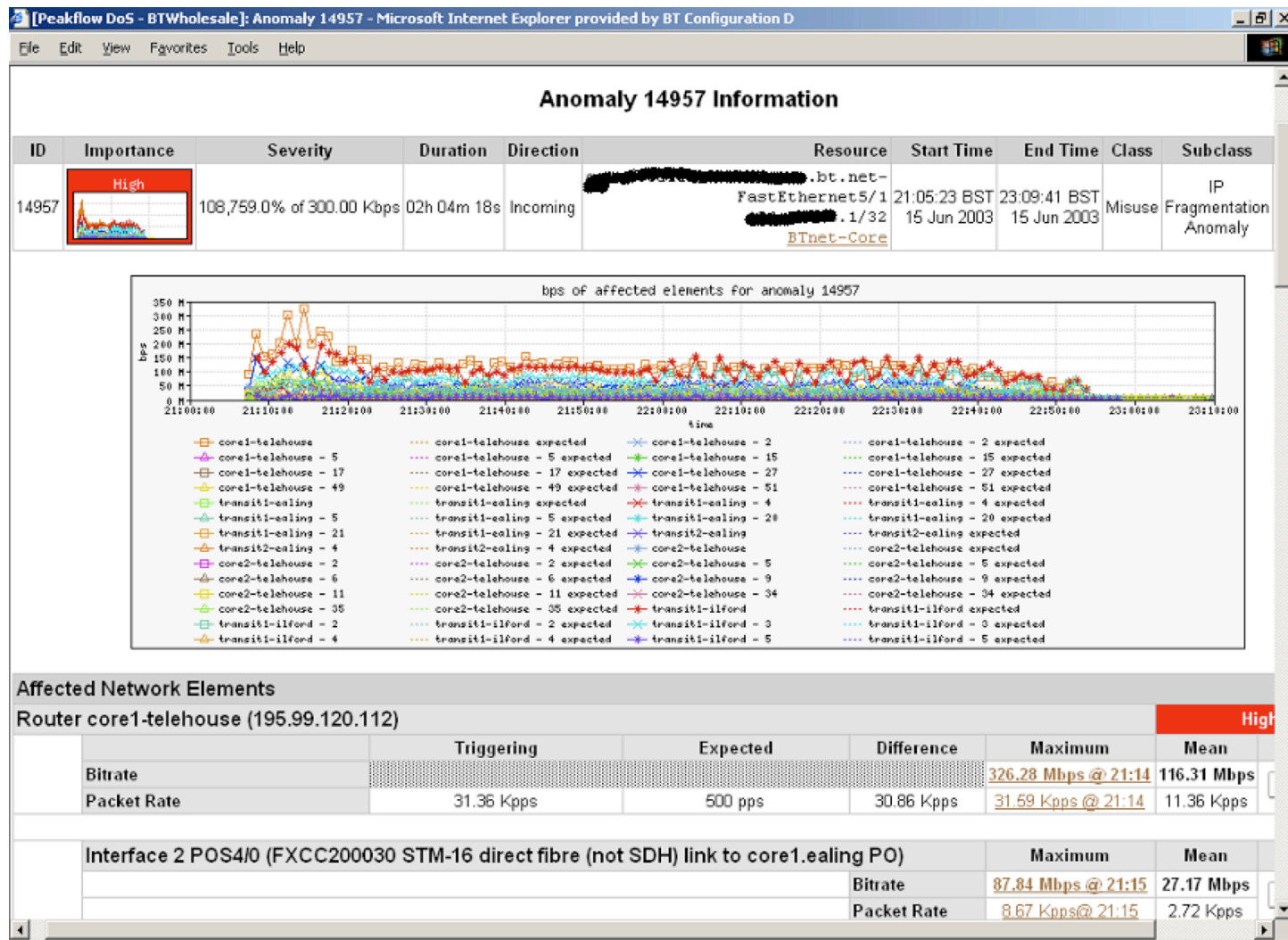
Una vez se hayan establecido puntos de referencia, se pueden detectar anomalías

- 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

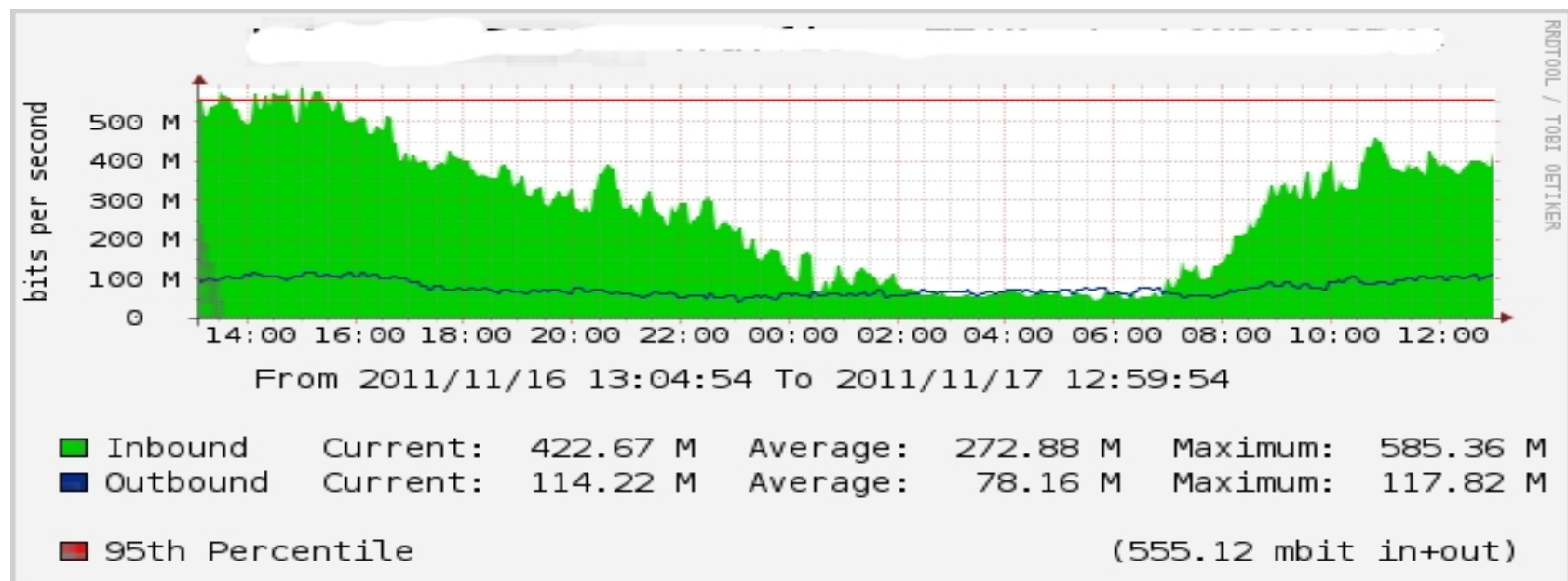
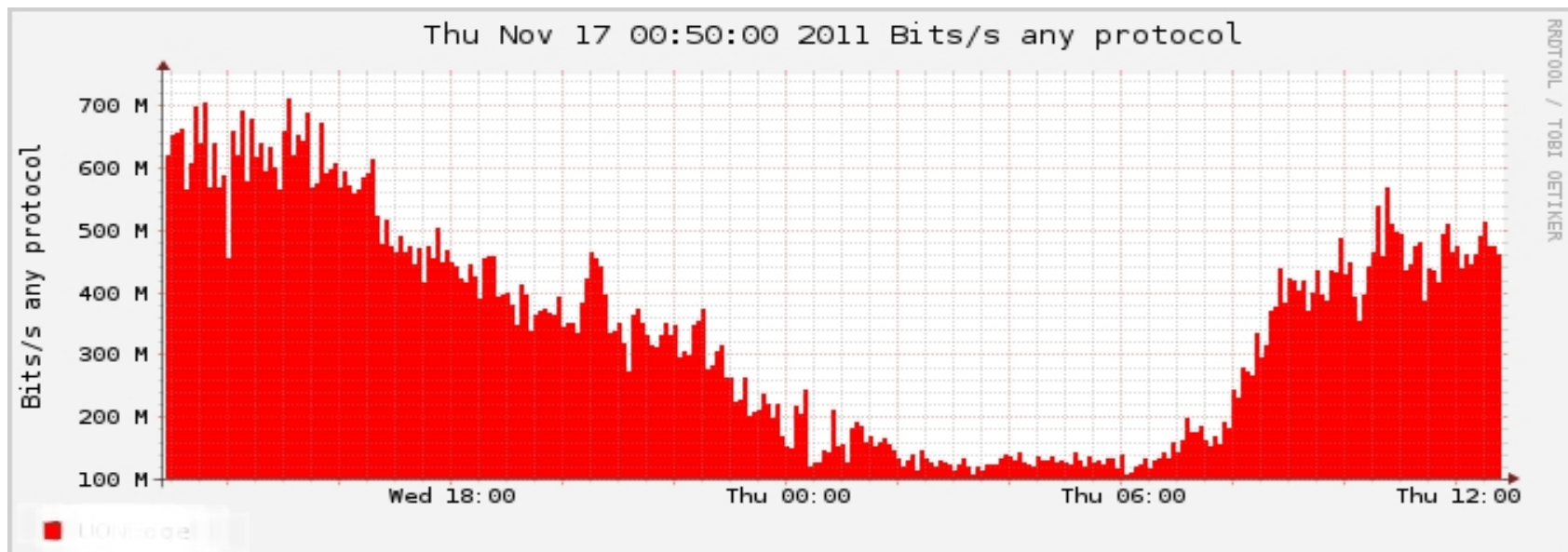


Detección comercial: Un ataque DoS de mayor escala



Contabilidad

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



Referencias

- flow-tools:
<http://www.splintered.net/sw/flow-tools>
- WikiPedia:
<http://en.wikipedia.org/wiki/Netflow>
- Aplicaciones NetFlow
<http://www.inmon.com/technology/netflowapps.php>
- Netflow HOW-TO
<http://www.linuxgeek.org/netflow-howto.php>
- IETF:
<http://www.ietf.org/html.charters/ipfix-charter.html>

Referencias

- Internet2 NetFlow
<http://abilene-netflow.itec.oar.net/>
- Flow-tools:
flow-tools@splintered.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