Gestión de Redes

Introducción a Netflow

Agenda

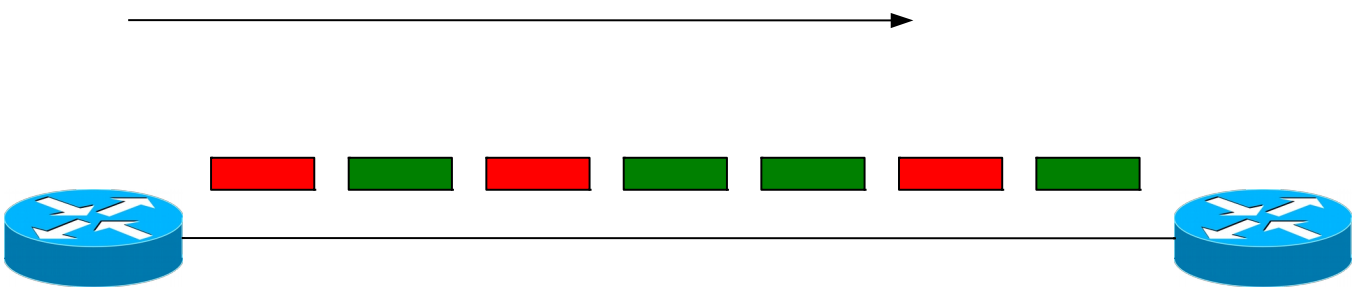
1. Netflow
   - Qué es y cómo funciona
   - Aplicaciones
2. Generar y exportar registros de flujo
3. Nfsen Nfdump
   - Arquitectura
   - Uso
4. Laboratorio

¿Qué 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)

Flujos Simples



= Paquete que pertenezca a flujo X

= Paquete que pertenezca a flujo Y

Flujo: Definición de Cisco IOS

Secuencia unidireccional de paquetes que comparten:

- Dirección IP origen.
- Dirección IP destino.
- Puerto de origen para UDP o TCP, ó “0” para otros protocolos.
- Puerto de destino para UDP o TCP, tipo y código para ICMP, ó “0” para otros protocolos
- Protocolo de IP.
- Interfaz de Ingreso (SNMP ifIndex)
- Tipo de Servicio IP

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

	Src IP	*Dst IP*	*Protocol*	*Src Port*	*Dst Port*
A	1.2.3.4	5.6.7.8	6 (TCP)	4001	22
B	5.6.7.8	1.2.3.4	6 (TCP)	22	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

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

	Src IP	*Dst IP*	*Protocol*	*Src Port*	*Dst Port*
A	1.2.3.4	5.6.7.8	6 (TCP)	4001	22
B	5.6.7.8	1.2.3.4	6 (TCP)	22	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

¿Qué pasa con los paquetes "C" y "D"?

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 y tipo de trafico, 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

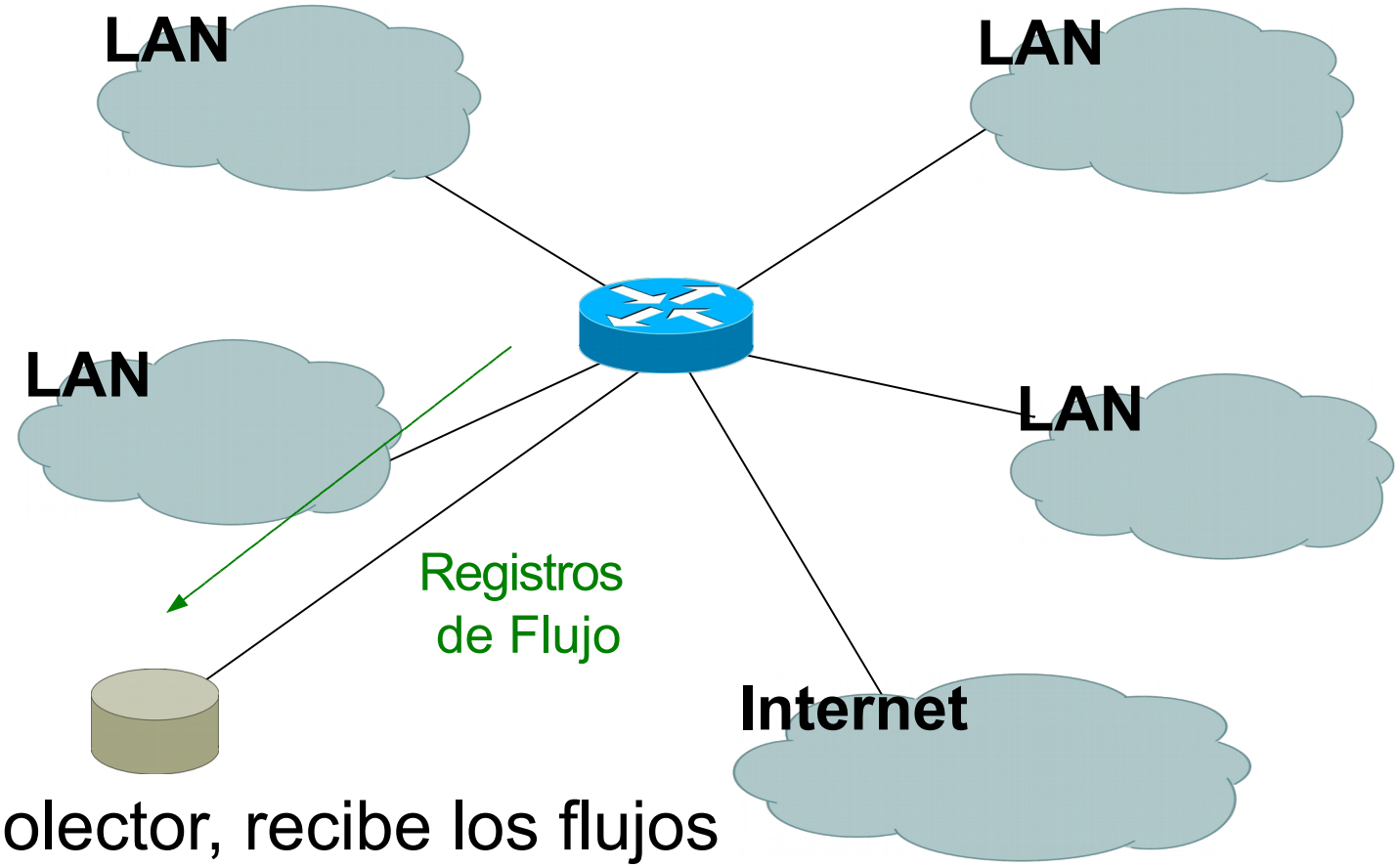
1. Configurar dispositivo (ej. enrutador) genere registros contabilidad de flujos.
2. Exportar los flujos desde dispositivo (enrutador) a un colector (PC)
   - Configurar protocolo, versión y destino
3. Recopilar los flujos, escribirlos al disco.
4. Analizarlos

Hay muchas herramientas disponibles, tanto gratuitas 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

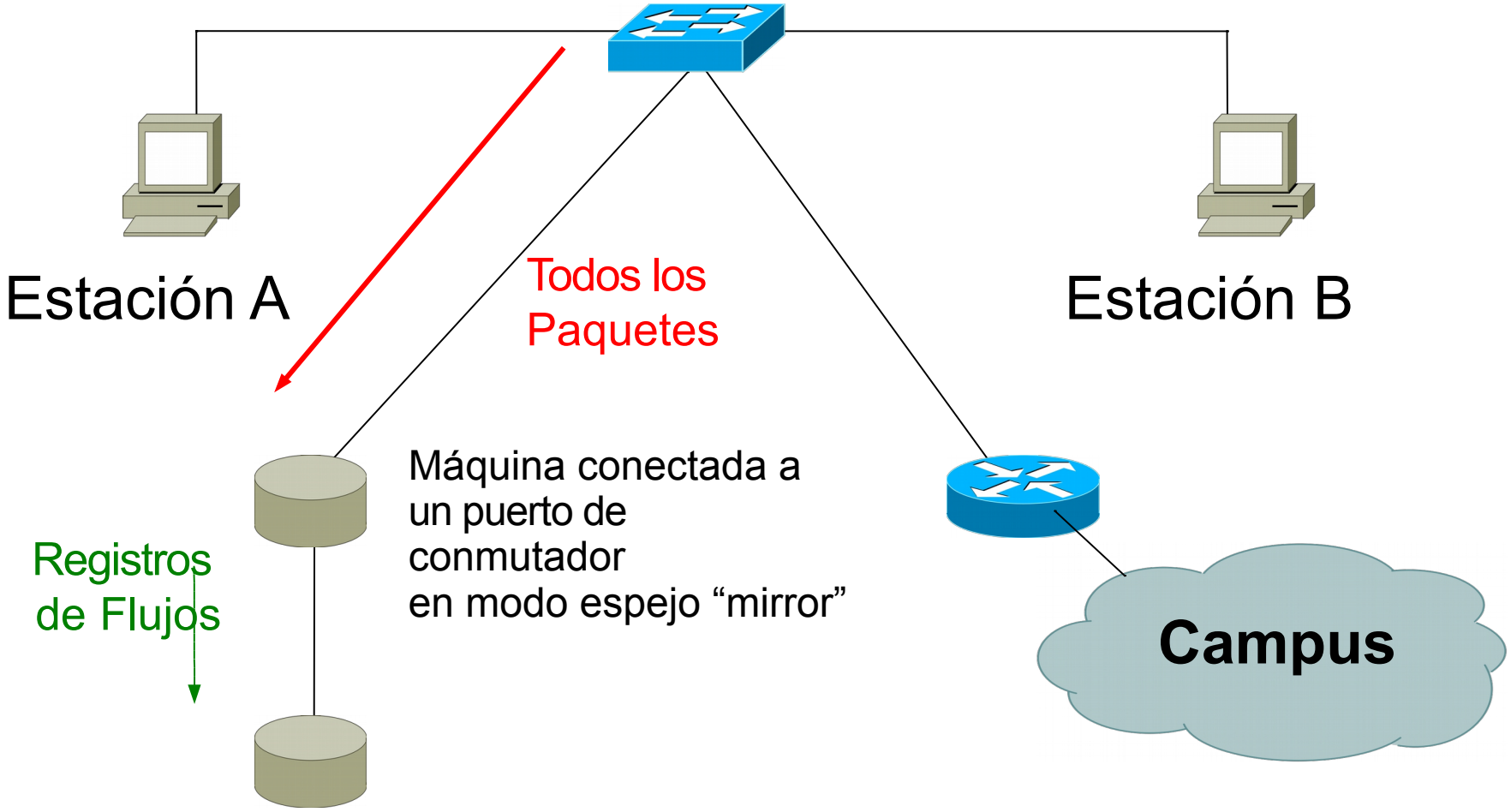


Colector, recibe los flujos exportados por el enrutador

Recopilación desde enrutador

- Con este método se pueden observar todos los flujos en la red
- El enrutador tiene más carga por procesar y exportar los flujos
- Se pueden seleccionar en qué interfaces se habilita recolección Netflow, y no activarlo para demás
- Con enrutadores en cada LAN, se puede habilitar recopilación y exportación de flujos en ellos, y así reducir carga en enrutador central.

Recopilación Monitor Pasivo



Recopilación Pasiva

- 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 libera al enrutador del trabajo de procesar tráfico, generar y exportar los flujos

Recopilación Pasiva

- Útil para enlaces:
  - con un solo punto de entrada a la red
  - 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
- IP Flow Information Export (**IPFIX**):
  - Estándar IETF, basado en NetFlow v9
- **sFlow**: Basado en muestreo, se encuentra comúnmente en switches
- **jFlow**: 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 hay un estándar en particular, de uso común 2055 y 9996
- Soportado en las plataformas IOS,ASA y CatOS – Pero con diferentes implementaciones

Configuración de Cisco IOS

- Se configura en cada interfaz
  - Entrada y salida
  - IOS viejos solo permite de entrada
- Definir la versión
- Definir la dirección IP y el puerto del colector (donde se enviarán los flujos)
- Opcionalmente habilitar tablas de agregación
- Opcionalmente configurar los tiempos de caducidad de flujos y el tamaño de tabla principal (v5) de flujos
- Opcionalmente configurar la frecuencia de muestreo

Configurando Netflow: de forma antigua

- Habilitar CEF

```
ip cef
ipv6 cef
```

- Habilitar flujos en cada interfaz

```
ip route cache flow      (antes de IOS 12.4)
```

O

```
ip flow ingress    (IOS 12.4 en adelante)
ip flow egress
```

- Exportar flujos a un recolector

```
ip flow-export version [5|9] [origin-as|peer-as]
ip flow-export destination <x.x.x.x> <udp-port>
```

“Flexible Netflow”: la nueva forma

- Única manera de monitorizar flujos IPv6 en los IOS modernos
- Comienza a usarlo ya – IPv6 viene / ya llegó
- Muchas opciones que pueden confundir, pero configuración básica es fácil

Configuración de Flexible Netflow

- Define uno o más exportadores

```
flow exporter EXPORTER-1
 destination 192.0.2.99
 transport udp 9996
 source Loopback0
 template data timeout 300
```

Configuración de Flexible Netflow

- Define uno o más monitores de flujo

```
flow monitor FLOW-MONITOR-V4
 exporter EXPORTER-1
 cache timeout active 300
 record netflow ipv4 original-input

flow monitor FLOW-MONITOR-V6
 exporter EXPORTER-1
 cache timeout active 300
 record netflow ipv6 original-input
```

Configuración de Flexible Netflow

- Aplicar monitores de flujo a interfaces activas

```
interface GigabitEthernet0/0/0
 ip flow monitor FLOW-MONITOR-V4 input
 ip flow monitor FLOW-MONITOR-V4 output
 ipv6 flow monitor FLOW-MONITOR-V6 input
 ipv6 flow monitor FLOW-MONITOR-V6 output
```

“Top-talkers”

- Puedes agregar flujos directamente en el enrutador, ejemplo:

```
show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 source
address ipv4 destination address sort counter bytes top 20
```

- Sí, es un comando largo!
- Antiguo comando no disponibles para Flexible Netflow

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

– Hacer un Alias:

```
conf t
alias exec top-talkers show flow..
```

Questions?

Recopilacion de flujos: Nfdump

- Libre y de código abierto – corre en recolector
- *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

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 como port tracker, SurfMap

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

Usaremos *nfsen* para encontrar mayores usuarios de ancho de banda

Perfiles y canales

- Un "canal" identifica un tipo de tráfico para graficar, 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, tráfico SMTP (etc.)
  - Tráfico hacia y desde el “Departamento de Ciencia”
  - ...
- Utilice filtros para definir el tráfico de interés
-

Referencias - Herramientas

- nfdump y nfsen:

  http://nfdump.sourceforge.net/
  http://nfsen.sourceforge.net/
  http://nfsen-plugins.sourceforge.net/

- pmacct y pmgraph:

  http://www.pmacct.net/
  http://www.aptivate.org/pmgraph/

- flow-tools:

  http://www.splintered.net/sw/flow-tools

Referencias – Información Adicional

- 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

Fin

- (Materiales de referencia adicionales a continuación)
-

Ejemplos de filtros

```
any    todo el trafico
proto tcp     solo trafico TCP
dst host 1.2.3.4     solo trafico para 1.2.3.4
dst net 10.10.1.0/24        solo trafico para este rango
not dst net 10.10.1.0/24   solo trafico no de ese rango
proto tcp and src port 80  solo TCP con puerto 80 origen
dst net 10.10.1.0/24 or dst net 10.10.2.0/24
                                solo trafico para estas redes.
dst net 10.10.1.0/24 and proto tcp and src port 80
       sólo el tráfico HTTP de respuesta a esa red
(dst net 10.10.1.0/24 or dst net10.10.2.0/24) and proto tcp and src port 80

   ...posibles combinaciones más complejas
```

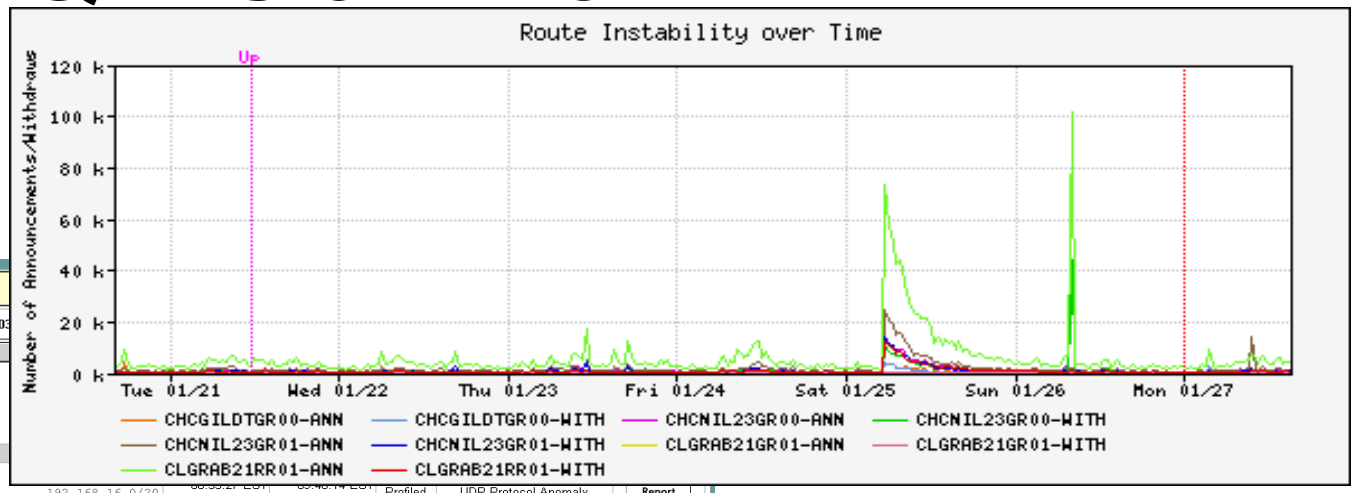
Flujos y Aplicaciones

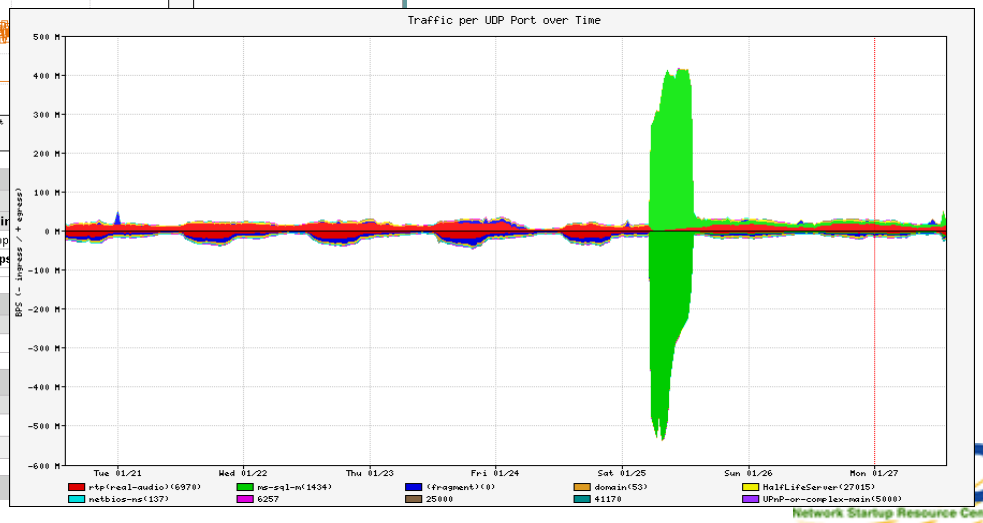
Más ejemplos

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”*





Detección basada en flujo (cont)*

- Una vez se hayan establecido puntos de referencia, se pueden detectar anomalías
  - Anomalías basadas solamente en tasas (pps or bps) pueden ser legítimas o maliciosas
  - Muchos ataques se pueden detectar inmediatamente, incluso sin valores de referencia (baseline) (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

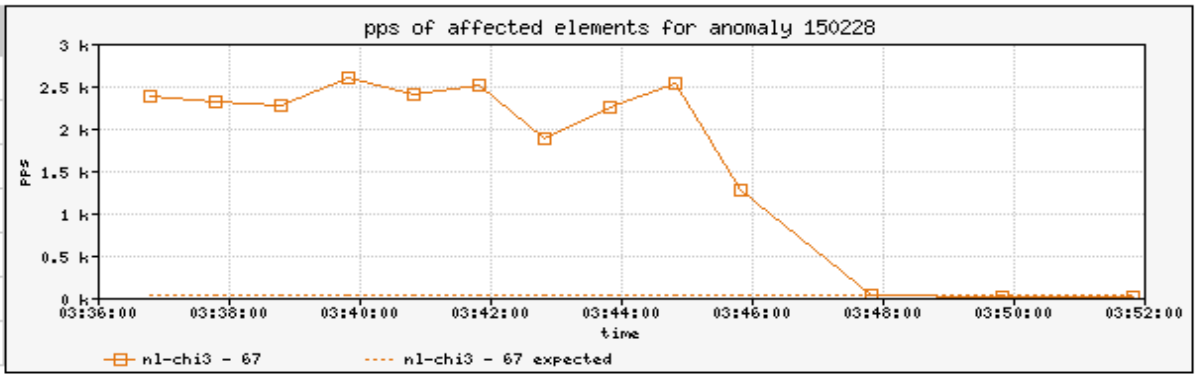
Herramientas comerciales para Flujos…*

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

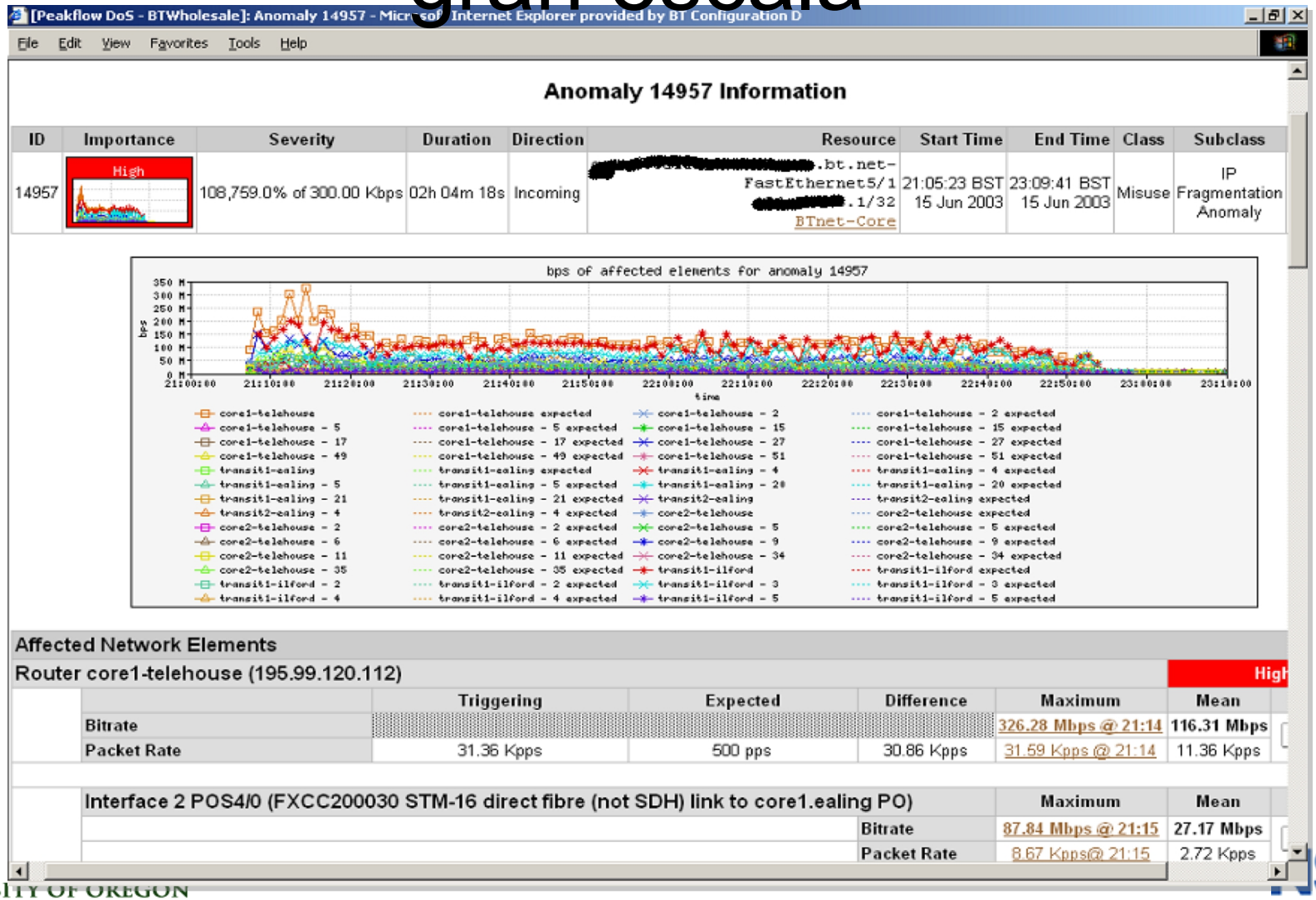
Sources	204.38.130.0/24
	204.38.130.192/26
	1024 - 1791
Destination	207.46.248.234/32
	80 (http)
Protocols	tcp (6)
TCP Flags	S (0x02)



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

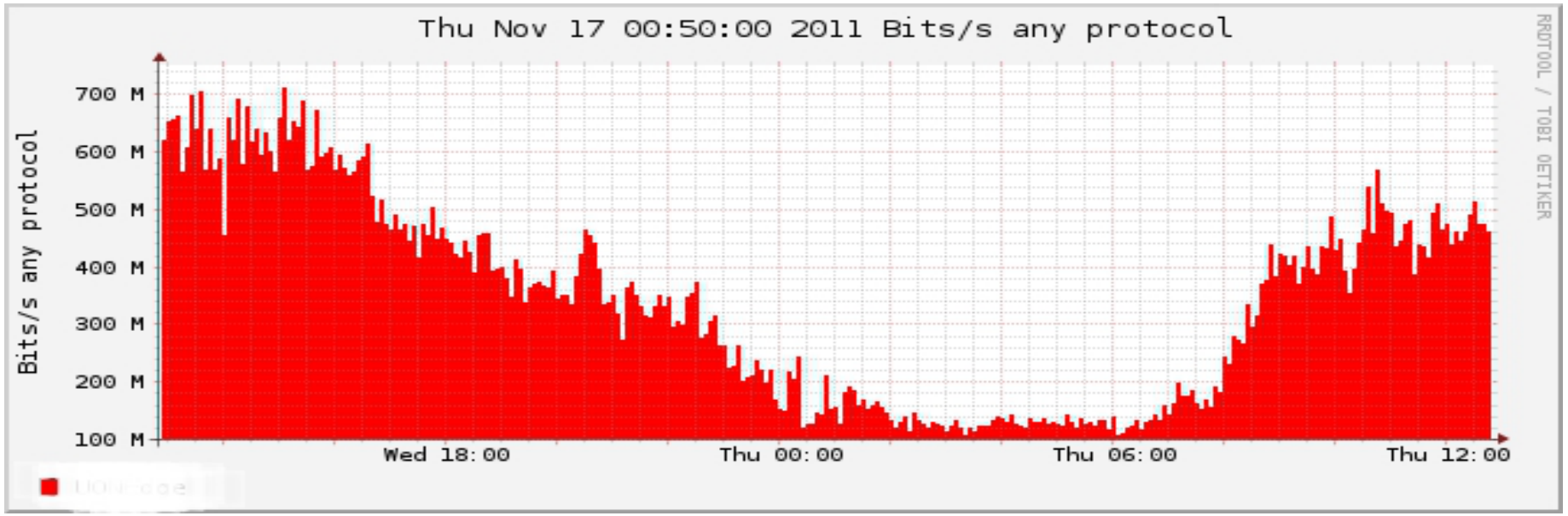
Anomaly Comments

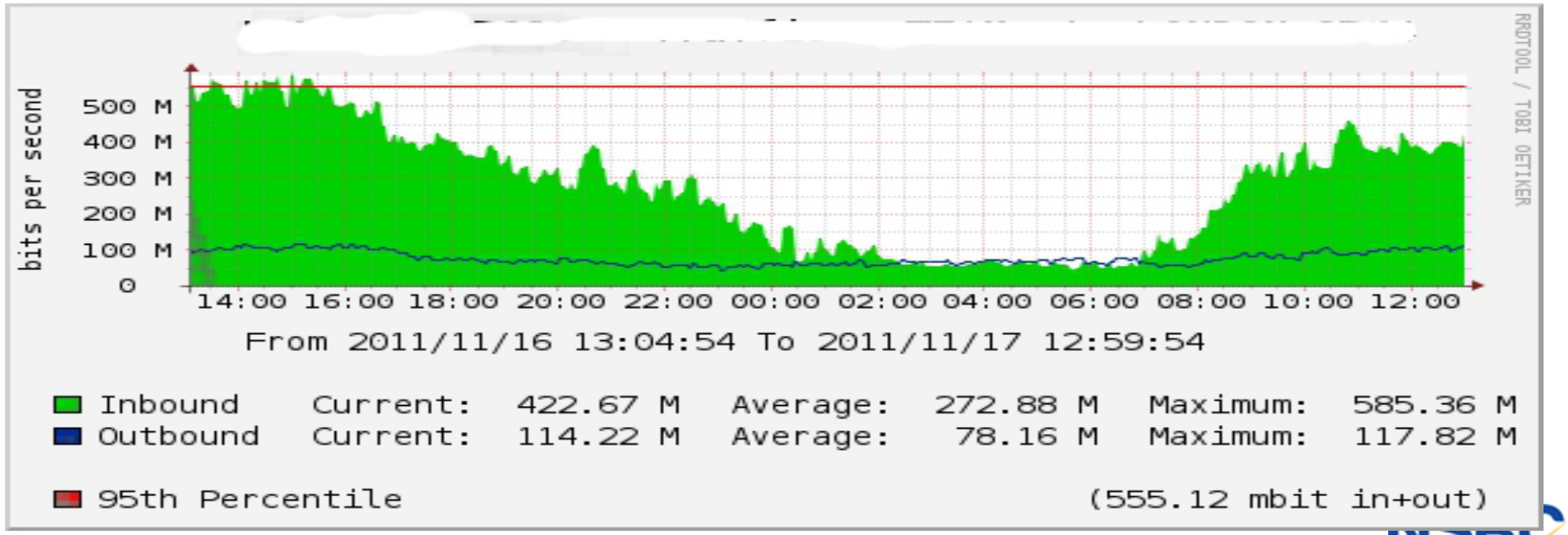
Detección comercial: Ataque DoS a gran escala



Contabilidad

- Puede complemtarse la contabilidad basada en SNMP con la basada en flujos (ver siguiente gráfico)
-


Thu Nov 17 00:50:00 2011 Bits/s any protocol
Bits/s any protocol
700 M
600 M
500 M
400 M
300 M
200 M
100 M
Wed 18:00
Thu 00:00
Thu 06:00
Thu 12:00
RRDTOOL / TOBI OETIKER


bits per second
500 M
400 M
300 M
200 M
100 M
0
14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00
From 2011/11/16 13:04:54 To 2011/11/17 12:59:54
Inbound Current: 422.67 M Average: 272.88 M Maximum: 585.36 M
Outbound Current: 114.22 M Average: 78.16 M Maximum: 117.82 M
95th Percentile (555.12 mbit in+out)
RRDTOOL / TOBI OETIKER

Versiones de Cisco Netflow

Netflow v1

- 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..
- No tiene números de secuencia – no se pueden detector flujos perdidos
- Obsoleto

Netflow v2 a v4

- 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 perdida de exportaciones de flujos.
- IPv4 solamente
-

Netflow v6 y v7

- Usado exclusivamente en la línea de switches Ethernet Cisco Catalyst
- Requiere la tarjeta con funcionalidad Netflow, una máquina de reenvío especializada para los switches Catalyst
- No es compatible ni comparable con Netflow en los routers Cisco

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

- Soporta IPv6
- Soporta ASN de 32-bits
- Campos adicionales como etiquetas MPLS
- Basado en versiones anteriores
- Periódicamente manda un paquete de "plantilla" – todo los campos de datos de flujos refieren a la plantilla
-