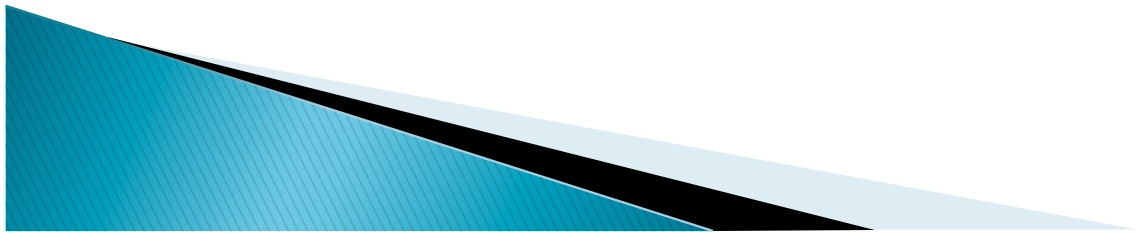
Introducción a *Netflow*

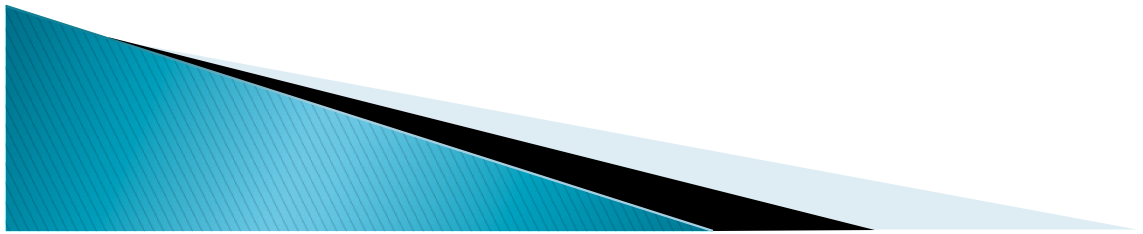
Hervey Allen
Carlos Armas

Agradecimientos:
Carlos Vicente
Universidad de Oregon



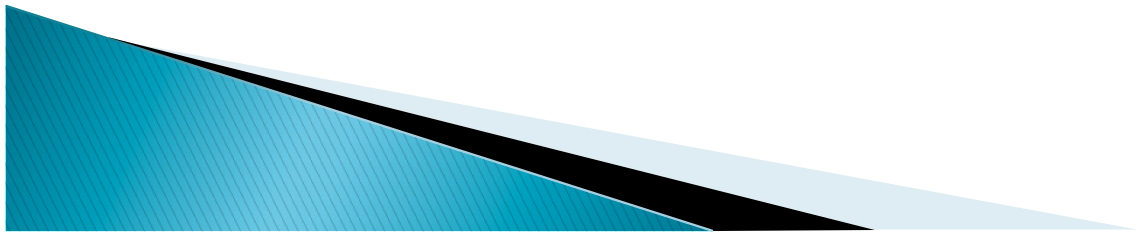
Contenido

- Definición de “flujo de red”
- Usos prácticos en gestión de redes
- Componentes de la arquitectura
- Qué es NetFlow
  - Versiones
- Configuración en equipamiento Cisco
- Alternativas a NetFlow
- Análisis
- Herramientas



Qué es un "*flujo de red*"

- Secuencia *unidireccional* de paquetes
- Todos los paquetes del flujo tienen denominadores comunes:
  - Misma dirección IP fuente, y destino
  - Mismo número de protocolo de capa 3
  - Mismo puerto fuente, y destino
  - Mismo octeto de Tipo de Servicio
  - Mismo índice de la interfaz de entrada (ifIndex)

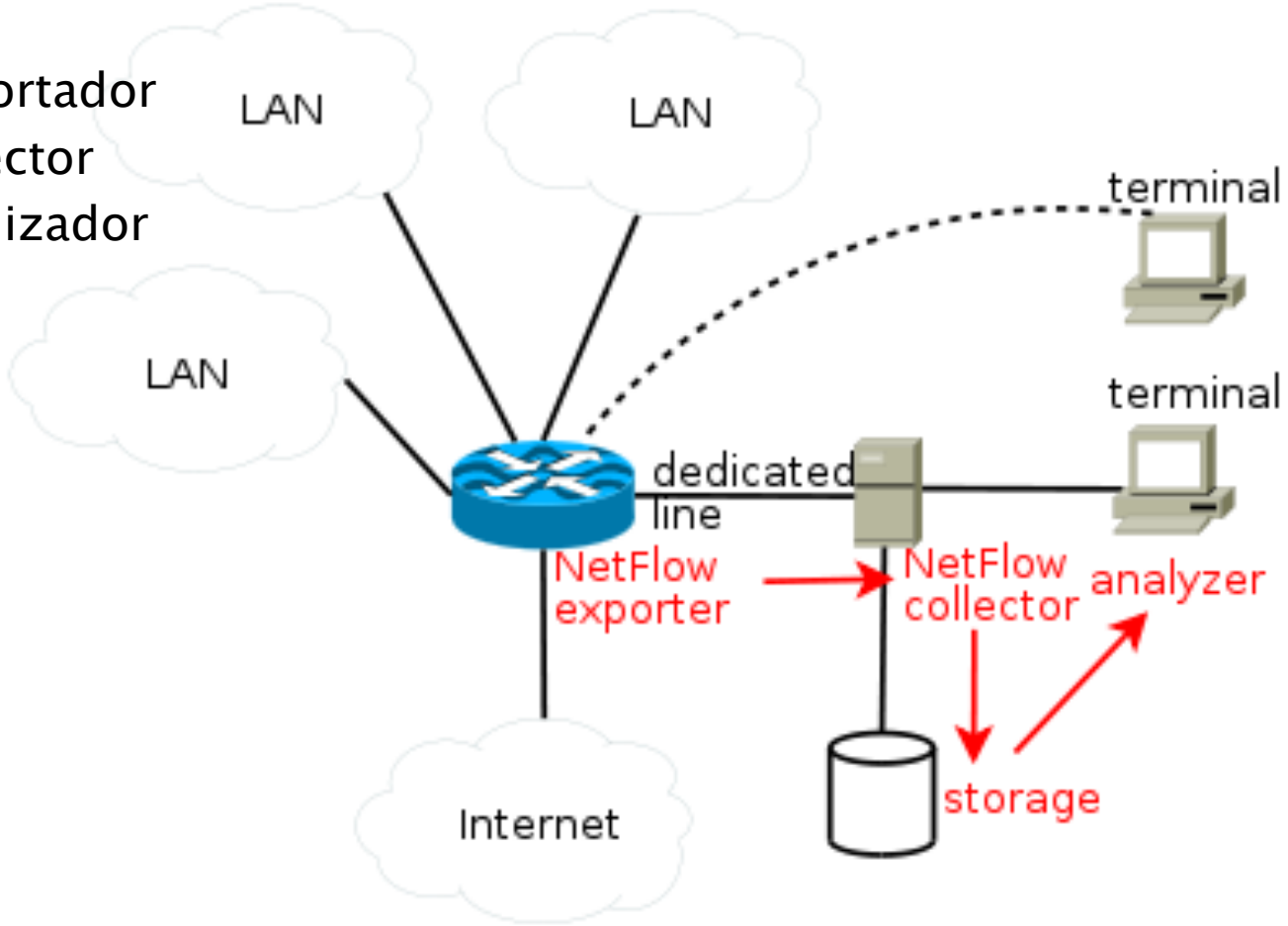


Usos Prácticos en Gestión de Redes

- Análisis de patrones de tráfico para:
  - Facilitar facturación por utilización
    - (volúmen, calidad de servicios, etc)
  - Compilar estadísticas por tipo de aplicación
  - Detección de situaciones anómalas
    - Ataques de negación de servicio
    - Abuso del servicio
  - Determinar cuando se necesita negociar un intercambio directo (BGP) con otro proveedor
  - Ayudar a erificación y optimización de Calidad de Servicio.

Componentes

- Netflow Exportador
- Netflow Colector
- Netflow Analizador

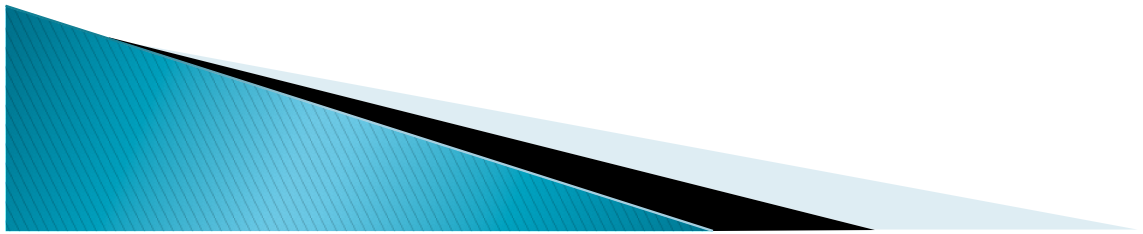


NetFlow

- Nombre dado por Cisco al formato de exportación de información sobre flujos
  - Se facilitó con la tecnología CEF (Cisco Express Forwarding)
- El *flow cache* contiene información activa, donde
  - cada flujo está representado por un *registro de flujo*,
    - el cual contiene una serie de campos de información
  - El *registro de flujo* se actualiza cada vez que un paquete que se determina como componente del flujo es conmutado (transmitido).

Exportación de Registros

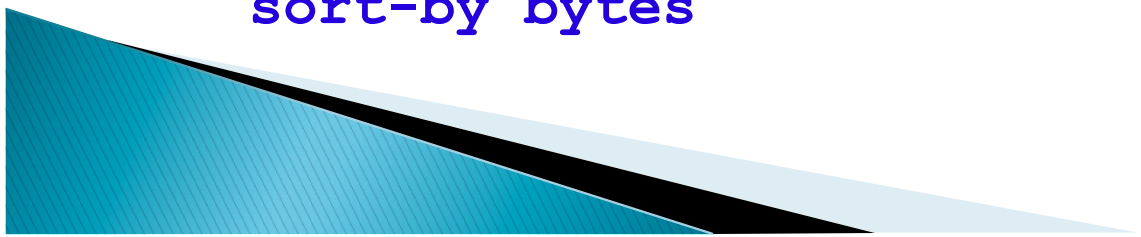
- Bajo ciertas circunstancias, los registros caducan en el *flow cache:*
  - Tiempo de vida activo/inactivo
    - (por defecto: 15seg/30 min)
  - El espacio destinado a *cache* se llena,
  - Conexiones TCP terminadas (FIN o RST)
- Al caducar, los flujos se agrupan y se exportan en datagramas de hasta 30 records



Configurar Netflow (Cisco)

```
interface FastEthernet0/0
   description Local network
   ip address 192.168.163.101 255.255.255.0
   ip flow egress
   ip flow ingress
   duplex auto
   speed auto
.......

ip flow-export version 5
ip flow-export destination 10.10.10.5 2002
ip flow top-talkers
   top 10
   sort-by bytes
```



Configurar Netflow II (Cisco)

En esta interface, coleccionar datos de flujo:

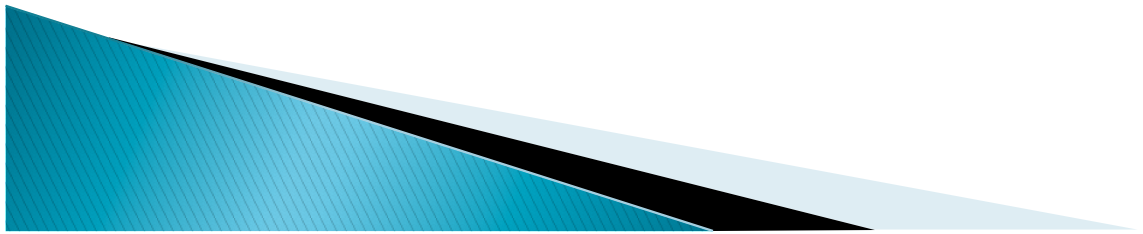
```
ip flow egress
ip flow ingress
```

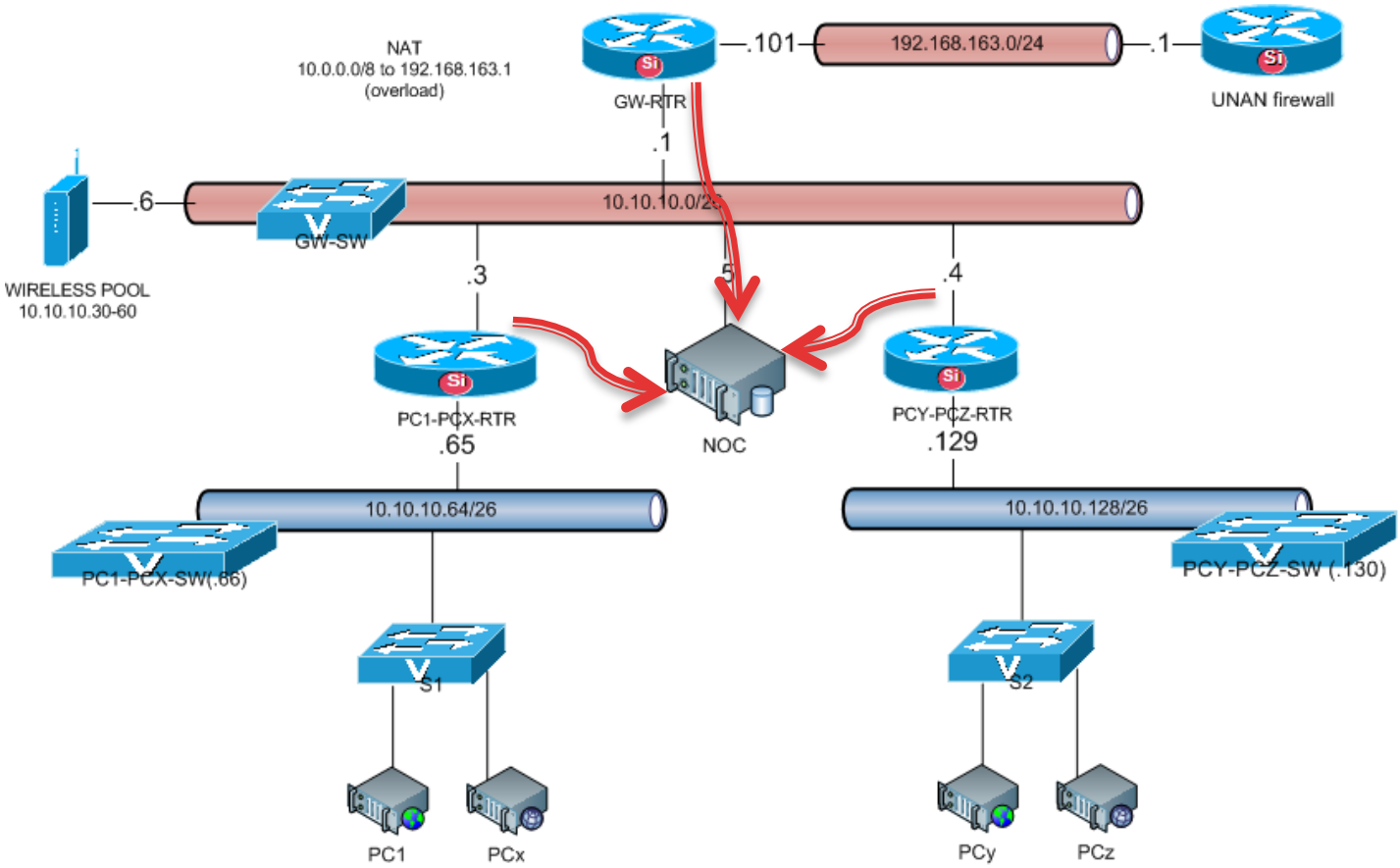
Y exportarlos,

- **en version 5**
- **al NOC, puerto 2002**
- **solo colecciona los 10 más significativos**
- **ordena según volúmen descendente:**

```
ip flow-export version 5
ip flow-export destination 10.10.10.5 2002

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

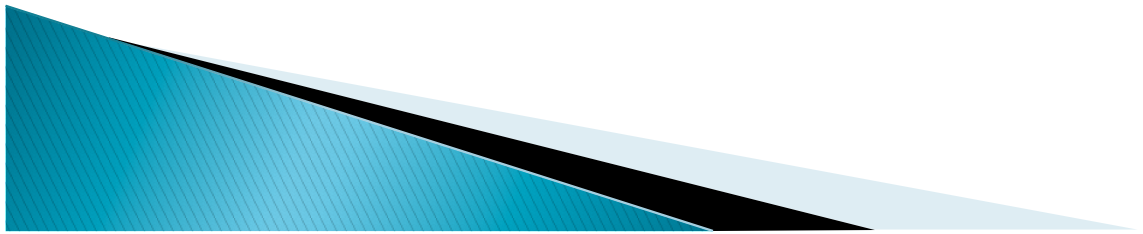




UNAN-2010		
	8/1/2010	

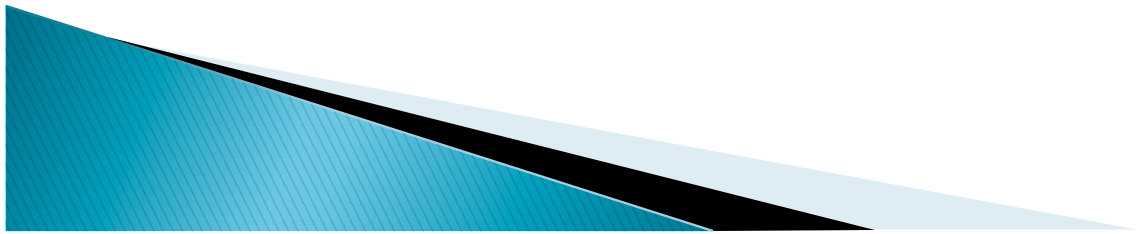
Usos

- Identificación de problemas
  - Clasificación de trafico
  - Analisis de ataques de negación de servicio
- Analisis de tráfico
  - Inter-AS
  - Reportes sobre proxies de aplicaciones
- Contabilidad
  - Para verificar contra otras fuentes, como datos de SNMP



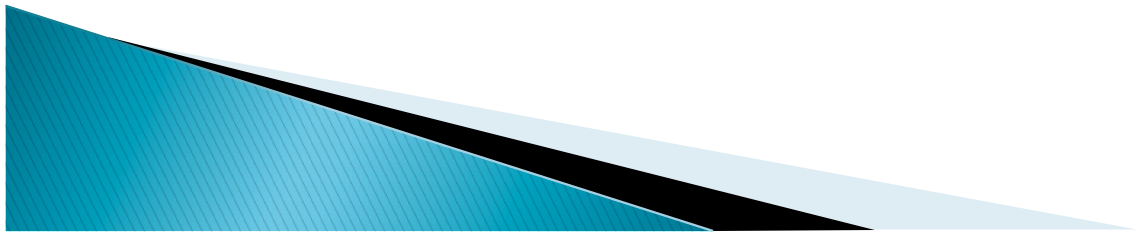
Clasificación de Tráfico

- Basado en protocolo, puertos fuente o destino
  - Identificación de protocolo (TCP, UDP, ICMP)
  - Puede verificar “puertos bien conocidos”
    - Medir tráfico de proxy – http , ftp
    - Para verificar (y despues limitar) tráfico de P2P
    - Producir reportes de uso, y distribución de tráfico



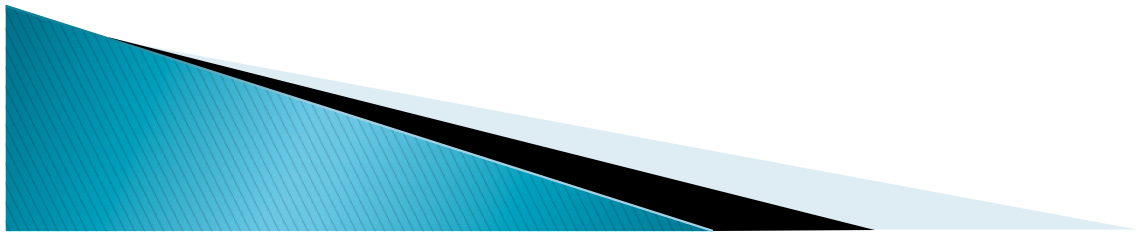
Traceback: herramienta basada en Netflow

- Trazar ataque por coincidencia (“trazas”) en cada interface via monitoreo pasivo:
  - Flow datos (ej., NetFlow, cflowd, sFlow, IPFIX)
  - Datos de “span”
  - PSAMP (muestreo de paquetes, IETF PSAMP WG)

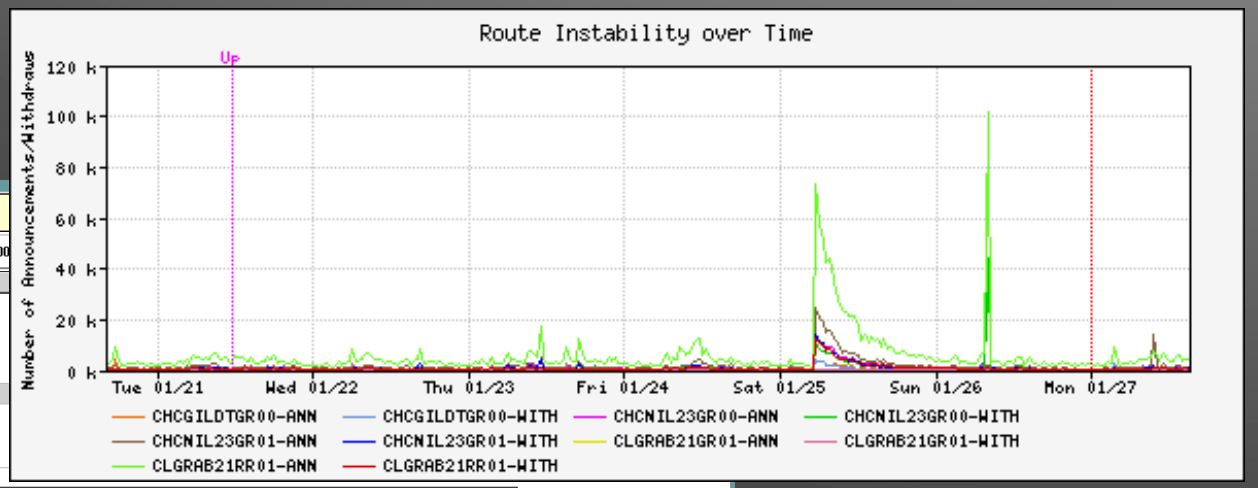


Detección basada en flujos

- Monitorear flujos (ej., transacciones de capa de Red y Transporte) en la red, y construir linea base para saber de antemano cual es el comportamiento “normal” :
  - Por interface
  - Por prefijo
  - Por capa de transporte (protocolo y puerto)
  - Conocer como se comporta el tráfico en diferentes ventanas de tiempo



Detectar eventosd anómalos
Ejemplo: SQL “Slammer”



peakflow DoS

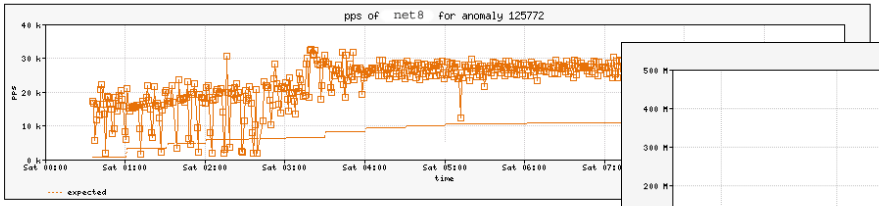
Recent Anomalies : Anomaly 125772 : Detailed Statistics

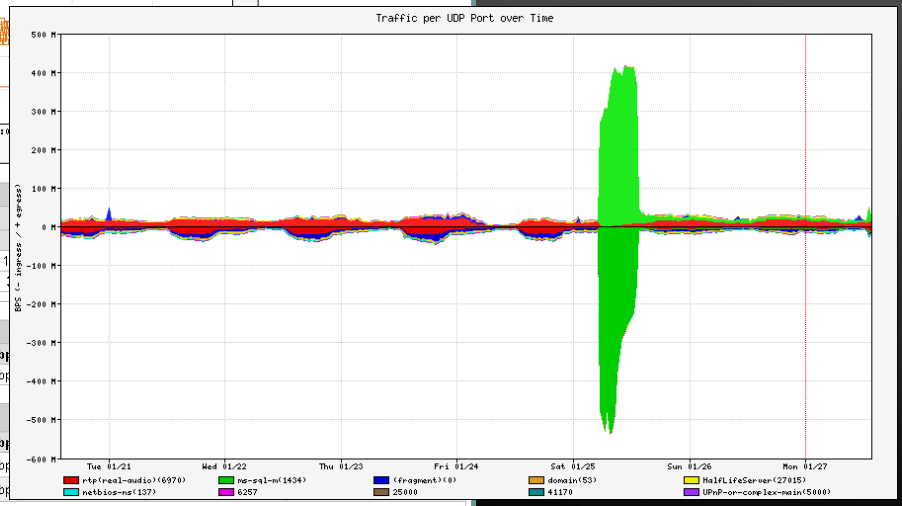
11:51:49 EST 27 Jan 200

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
Bitrate	71.69 Mbps	2.34 Mbps	69.35 Mbps
Packet Rate	**22.20 Kpps**	**712 pps**	**21.49 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	bp
	308.01 GB	762,849,500	404 B	76.05 Mbp

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

Source Addresses

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

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

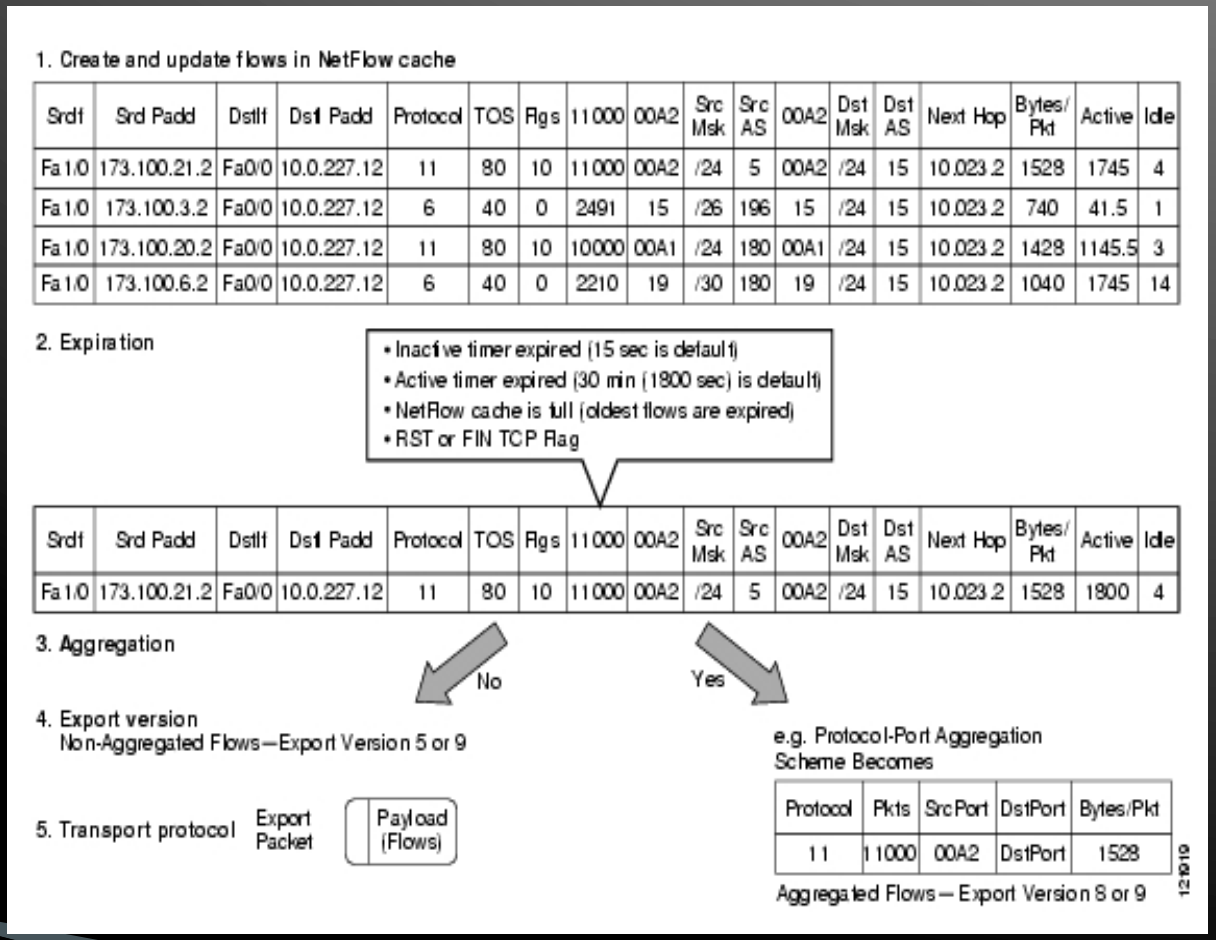
Destination Addresses

Graph

Detección basada en flujo

- Una vez que las líneas bases han sido construidas, comportamiento fuera de la norma puede ser detectado
- Un gran volúmen de tráfico puede ser lo mismo legítimo o malicioso
  - Muchos tipos de ataques pueden ser inmediatamente reconocidos, aun sin lineas base (ej., TCP SYN o inundación de RST)
  - **Patrones** pueden ser definidos para identificar tráfico "interesante" (ej, protocolo udp + puerto 1434 + 404 octetos(376 octetos de paquete de datos)) == slammer!)

NetFlow Cache

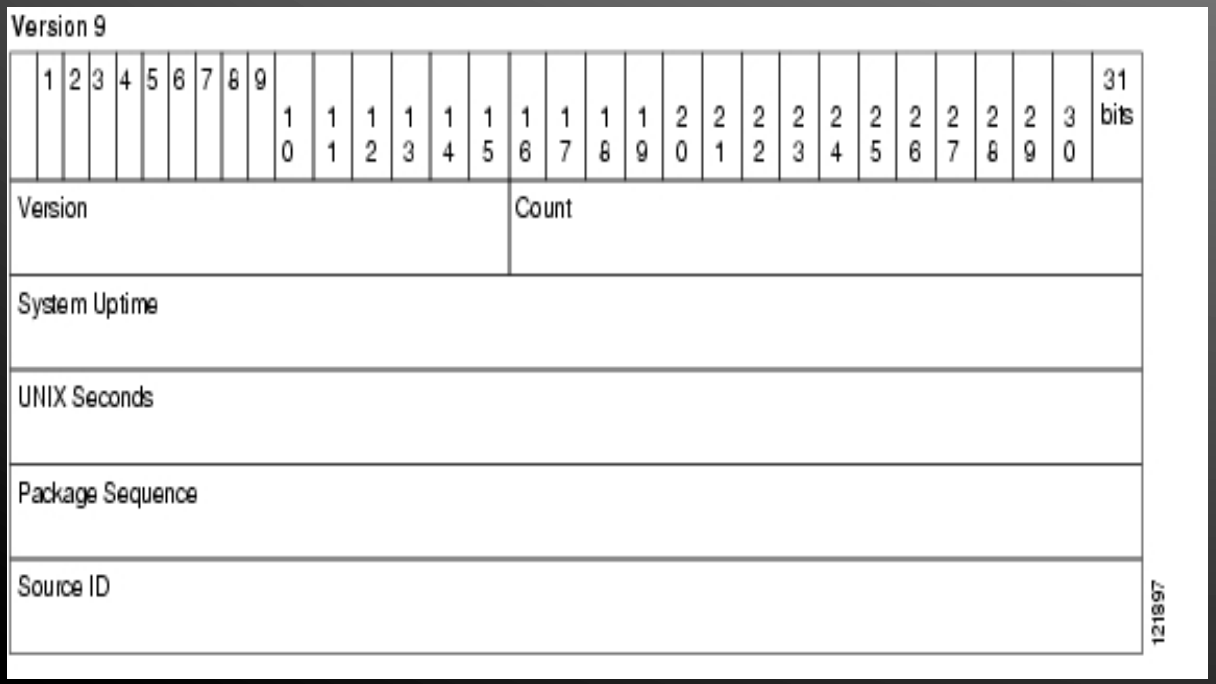


Srdf	Srd Padd	Dstlf	Dst Padd	Protocol	TOS	Flgs	11000	00A2	Src Msk	Src AS	00A2	Dst Msk	Dst AS	Next Hop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.023.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.023.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.023.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.023.2	1040	1745	14

Srdf	Srd Padd	Dstlf	Dst Padd	Protocol	TOS	Flgs	11000	00A2	Src Msk	Src AS	00A2	Dst Msk	Dst AS	Next Hop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.023.2	1528	1800	4

Protocol	Pkts	SrcPort	DstPort	Bytes/Pkt
11	11000	00A2	DstPort	1528

Version 9


Version 9
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 bits
Version
Count
System Uptime
UNIX Seconds
Package Sequence
Source ID
121897

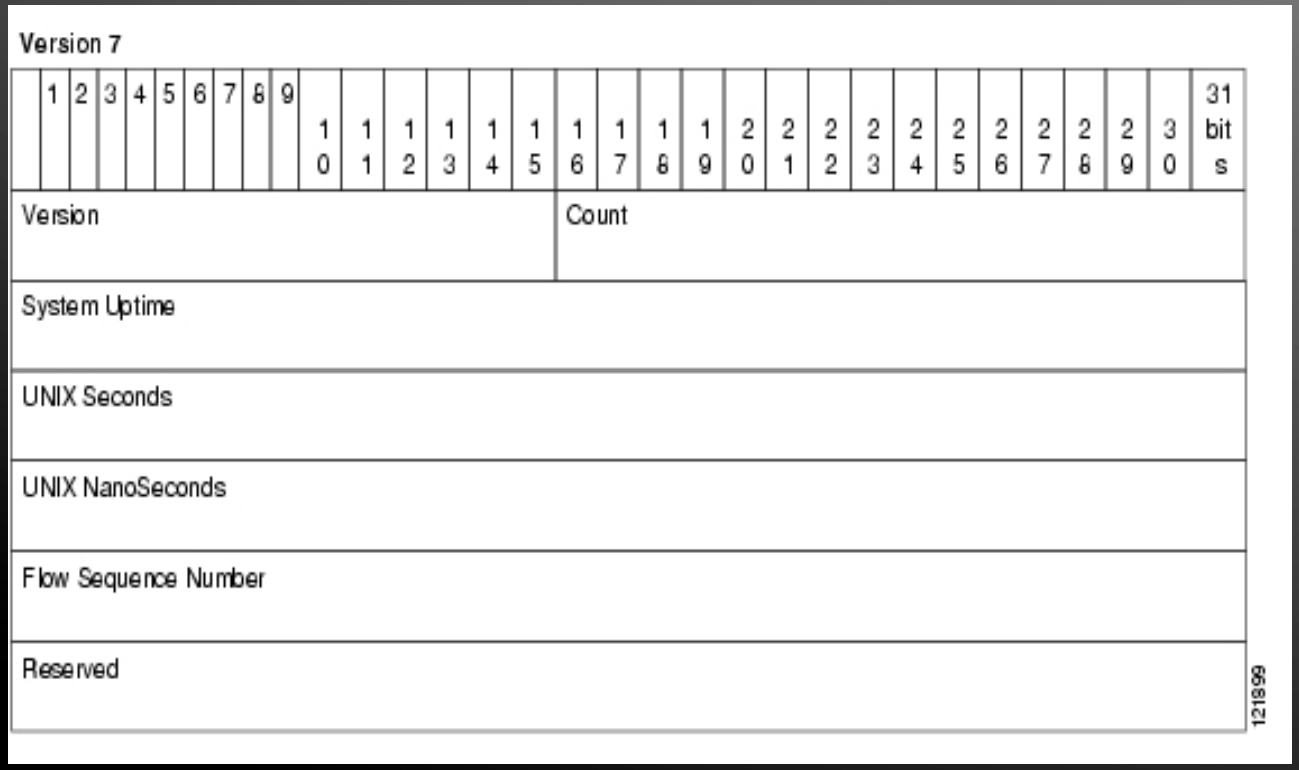
Version 8

Version 8

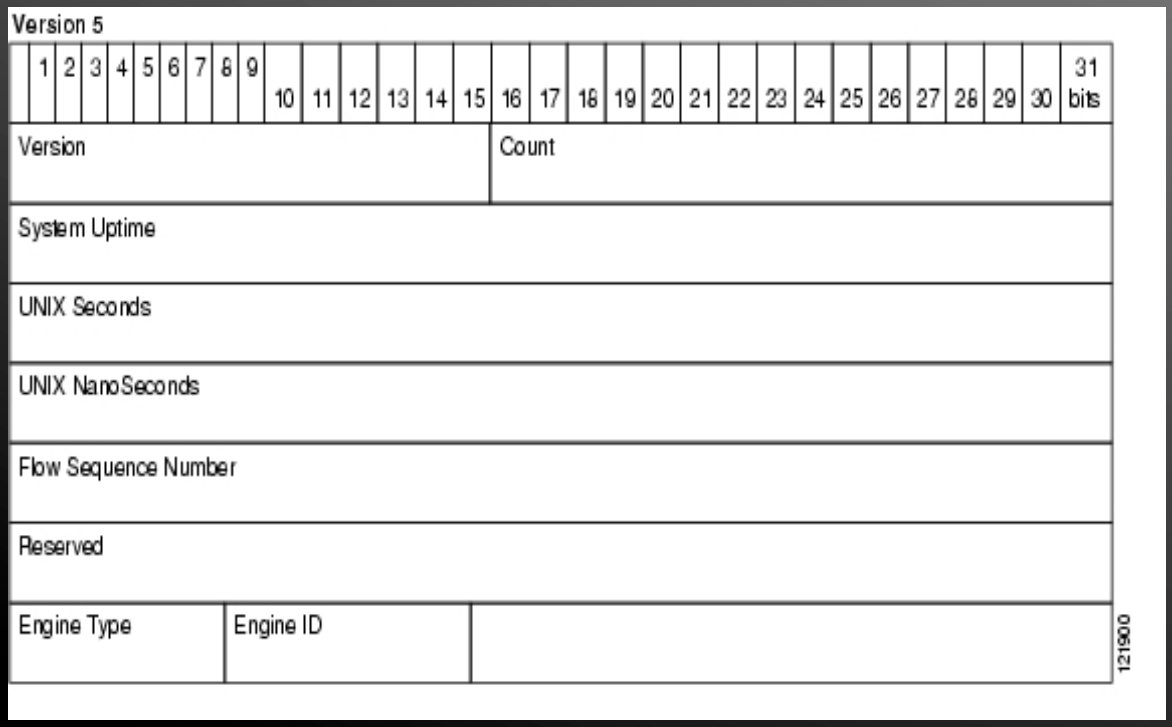
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31 bits
Version																Count															
System Uptime																															
UNIX Seconds																															
UNIX NanoSeconds																															
Flow Sequence Number																															
Engine Type																Engine ID															
Aggregation																Agg Version															
Sampling Interval																															
Reserved																															

121938

Version 7


Version 7
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 bits
Version
Count
System Uptime
UNIX Seconds
UNIX NanoSeconds
Flow Sequence Number
Reserved
121899

Version 5


Version 5
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 bits
Version
Count
System Uptime
UNIX Seconds
UNIX NanoSeconds
Flow Sequence Number
Reserved
Engine Type
Engine ID
121900