Introducción a *Network Flows*

José Domínguez
Universidad de Oregon

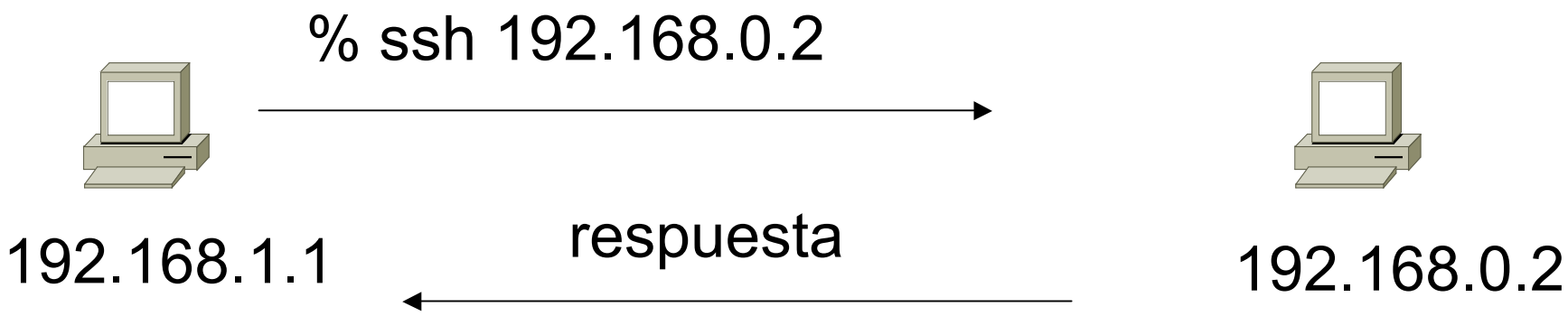
Contenido

- Qué es un *Flow*
- *Usos prácticos en gestión de redes*
- Componentes de la arquitectura
- Qué es *NetFlow*
  - Versiones
- Configuración en Cisco
- Alternativas a *NetFlow*
- Análisis
- Herramientas

Qué es un F*lujo* (*Flow)*

- Se define como una secuencia *unidireccional* de paquetes con ciertas características comunes:
  - Direcciones IP y mascara de origen y destino
  - Sistema Autónomo de origen y destino
  - Número de protocolo a nivel 3
  - Puertos origen y destino
  - Octeto de ToS (Tipo de Servicio)
  - Índice de la interfaz de entrada (ifIndex)

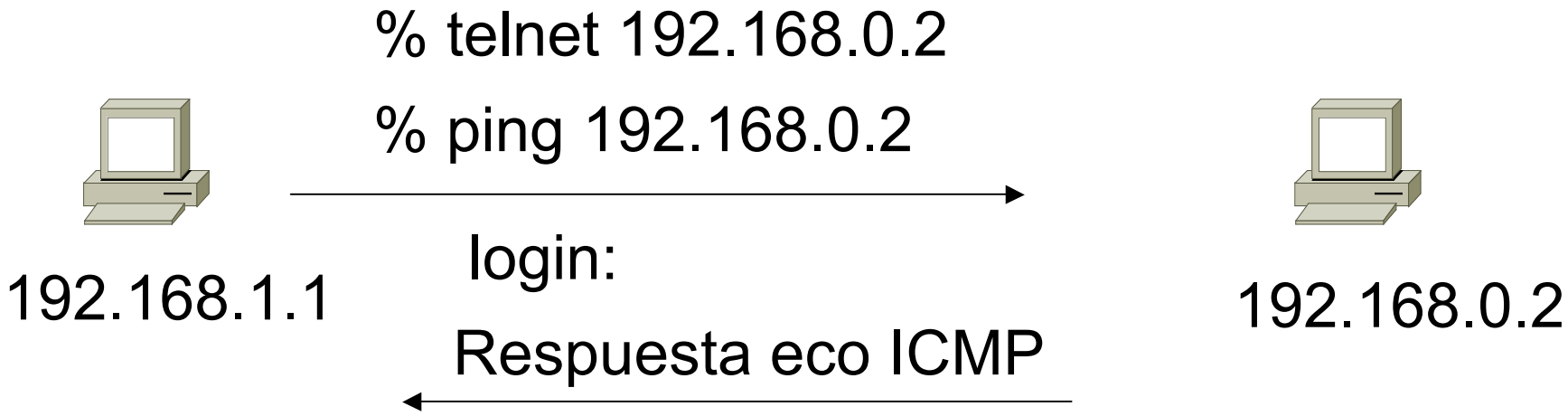
Flujo Unidireccional con IP Origen/Destino como clave



Flujos Activos

Flujo	IP Origen	IP Destino
1	192.168.1.1	192.168.0.2
2	192.168.0.2	192.168.1.1

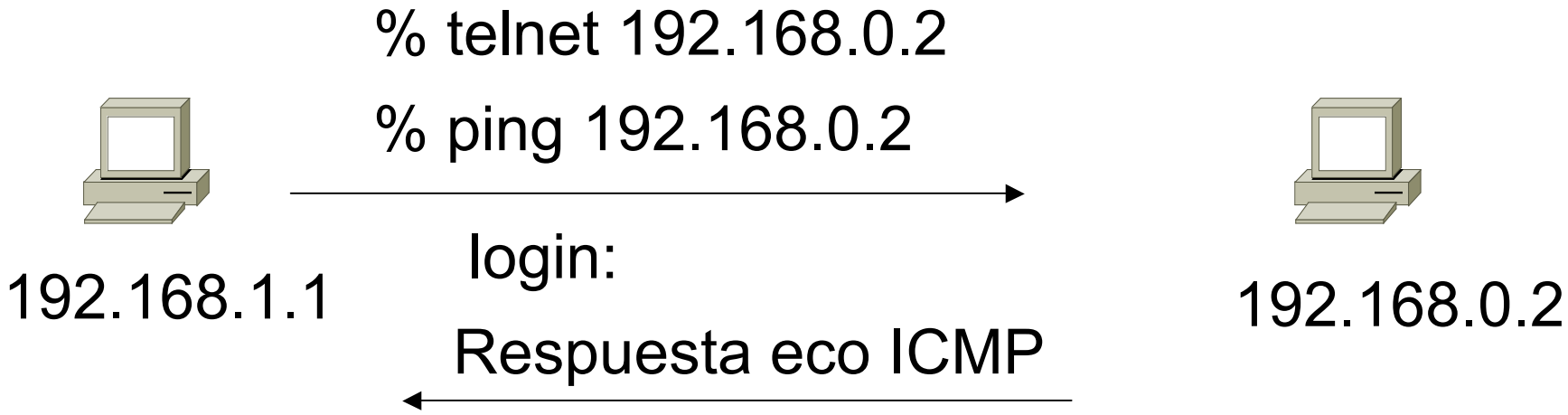
Flujo Unidireccional con IP Origen/Destino como clave



Flujos Activos

Flujo	IP Origen	IP Destino
1	192.168.1.1	192.168.0.2
2	192.168.0.2	192.168.1.1

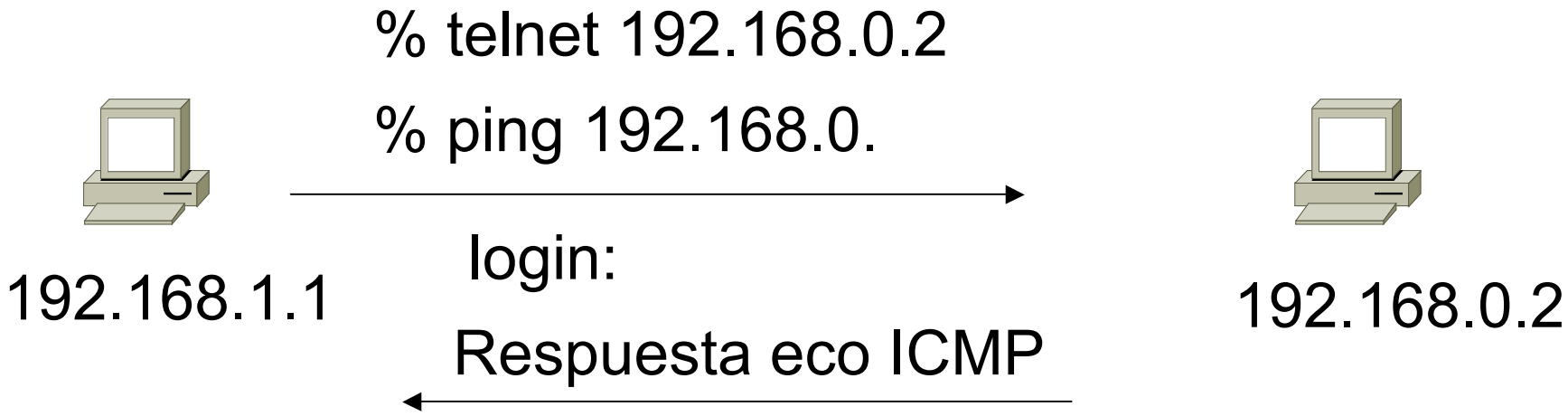
Flujo Unidireccional con IP, Puerto y Protocolo como clave



Flujos Activos

Flujo	IP Origen	IP Destino	prot	srcPort	dstPo
1	192.168.1.1	192.168.0.2	TCP	32000	23
2	192.168.0.2	192.168.1.1	TCP	23	320
3	192.168.1.1	192.168.0.2	ICMP	0	0
4	192.168.0.2	192.168.1.1	ICMP	0	0

Flujo Bidireccional con IP, Puerto y Protocolo como Clave



Active Flows

Flujo	IP Origen	IP Destino	prot	srcPort	dstPort
1	192.168.1.1	192.168.0.2	TCP	32000	23
2	192.168.1.1	192.168.0.2	ICMP	0	0

Usos Prácticos en Gestión de Redes

- Análisis detallado de patrones de tráfico
  - Contabilidad y Facturación por utilización (más allá de bytes)
  - Estadísticas por tipo de aplicación (SMTP, HTTP, etc.)
  - Detección de ataques y utilización anómala (DDoS, virus, gusanos, abuso)
  - Necesidad de Peerings BGP
  - Verificación y optimización de Calidad de Servicio (QoS)
  - Resúmenes de tráficos por subred
  - Detectar estaciones con mucho tráfico o anomalías
  - etc.

Componentes

- Netflow Exporter
- Netflow Collector
- Netflow Analyzer

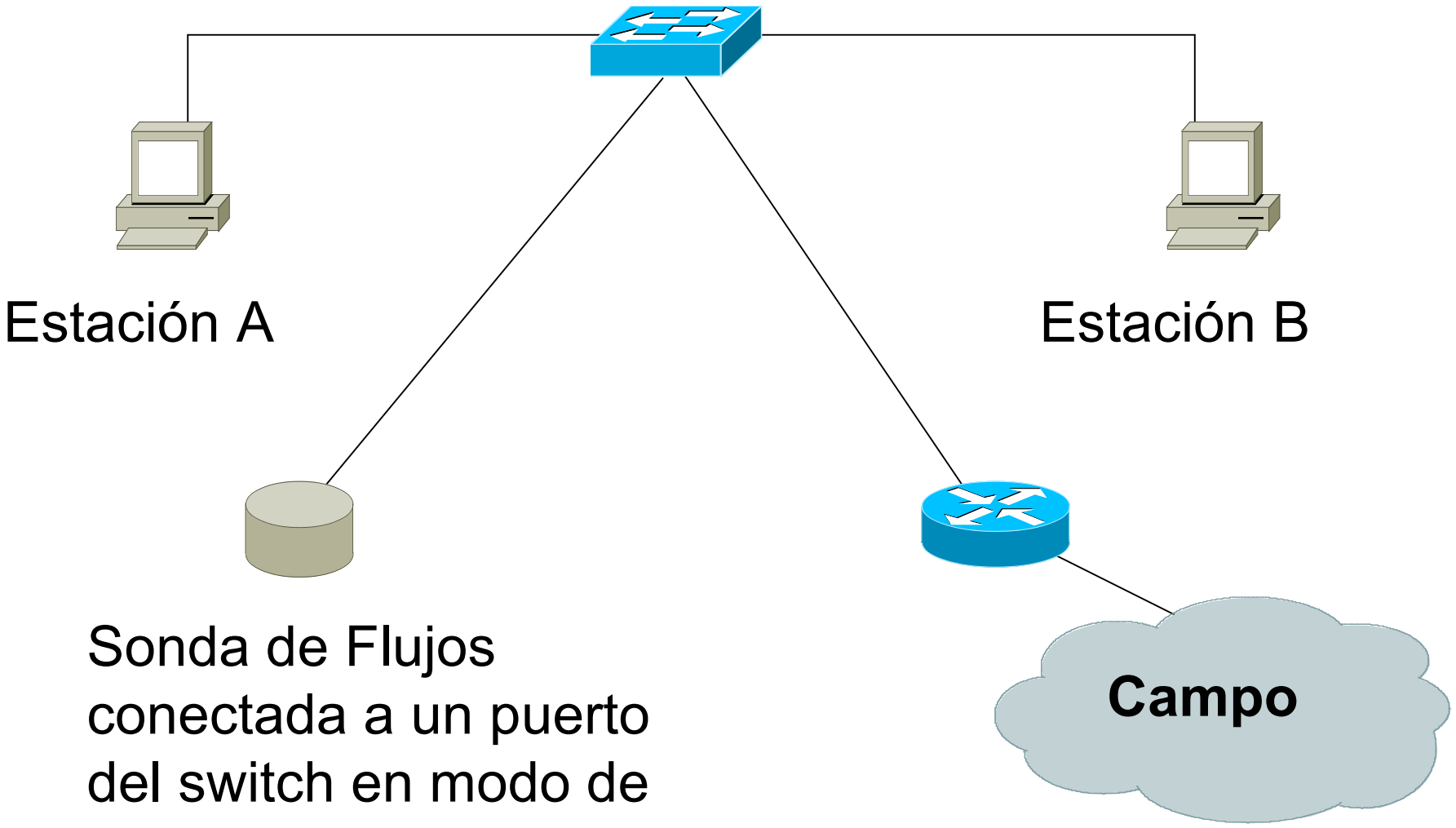
Descriptores de Flujos

- Una clave con mas elementos generará mas flujos.
- Al mayor número de flujos mayor será el tiempo de procesamiento para generar reportes y mayores requerimientos de memoria y CPU para el dispositico que gereá los flujos.
- Dependerá de la aplicación -- Ingeniería de Tráfico Vs. Detección de Intrusiones.

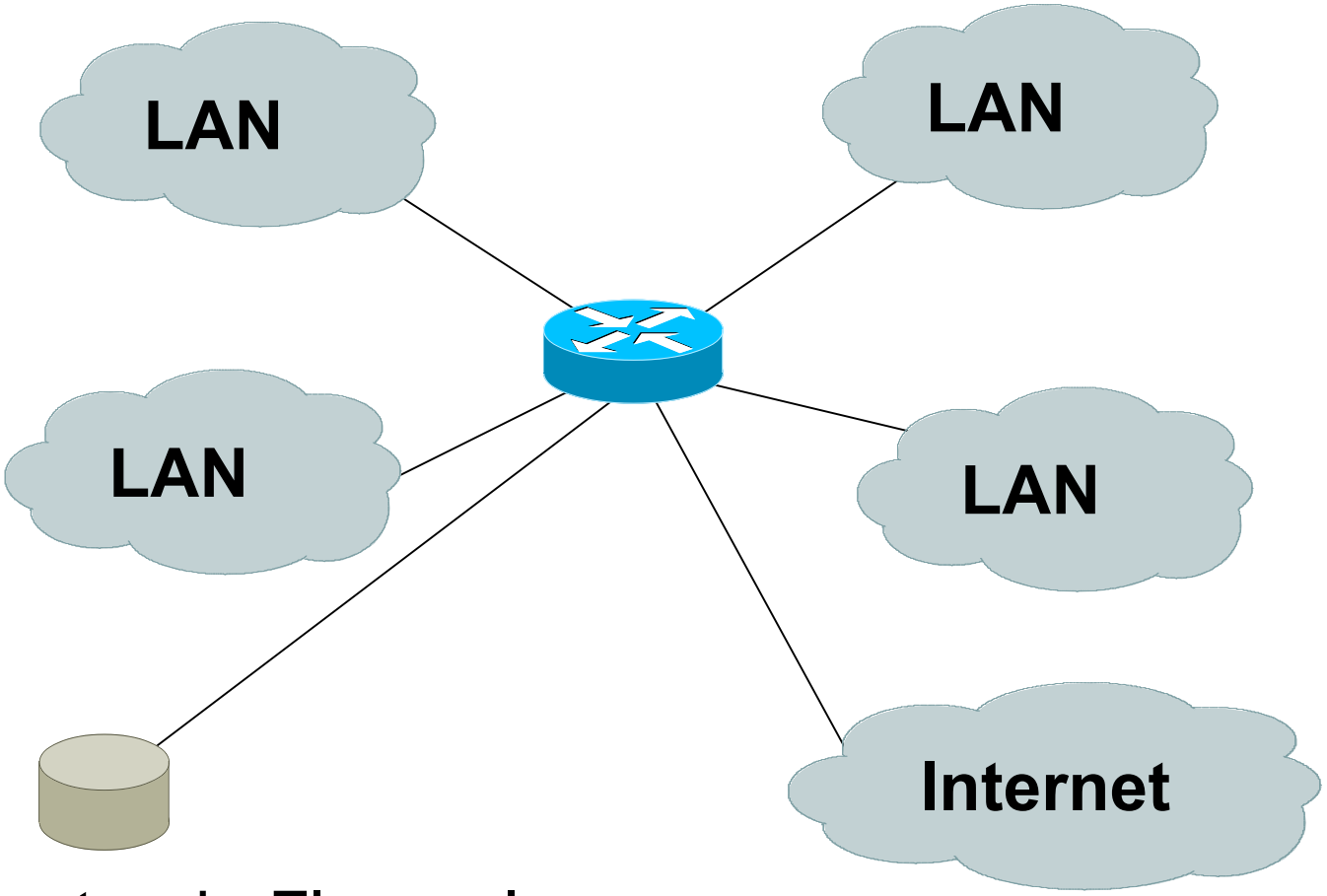
Contabilidad de Flujos

- Información de contabilidad acumulada con los flujos.
- Paquetes, Bytes, Tiempo de Inicio, Tiempo de Término.
- Información de enrutamiento -- mascaras y números de sistemas autónomos.

Monitor de Colección Pasiva



Colección via Enrutador



Colector de Flows almacena los flujos exportados por los enrutadores.

Monitorización Pasiva

- Directamente conectada al segmento de redes via un puerto de un switch/enrutador en modo “mirror”, separador optico, o un segmento replicado. Generate flows for all local LAN traffic.
- Debes tener una interfaz o monitor en cada segmento de red.
- Soporte para flujos mas detallados - bidireccionales y de aplicación (la sonda externa tiene mas recursos).

Colección via Enrutador

- Enrutador genera flujos para el tráfico que pasa por el enrutador.
- Flujos no son generados para el trafico local er el segmento (no es un sniffer).
- Limitado a un criterio “simple” de flujos (encabezados de los paquetes).
- Generalmente mas fácil de desplegar - no hay necesidad de equipos nuevos.

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 sobre todos los flujos activos
  - Cada flujo está representado por un *flow record*, que contiene una serie de campos de información
  - El flow record se actualiza cada vez que los paquetes que pertenecen al flujo son conmutados

Exportación de Registros

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

NetFlow Cache

1. Create and update flows in NetFlow cache

Srdf	Srd Padd	Dstlf	Dsf Padd	Protocol	TOS	Rgs	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

2. Expiration

- Inactive timer expired (15 sec is default)
- Active timer expired (30 min (1800 sec) is default)
- NetFlow cache is full (oldest flows are expired)
- RST or FIN TCP flag

Srdf	Srd Padd	Dstlf	Dsf Padd	Protocol	TOS	Rgs	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

3. Aggregation

No

Yes

4. Export version
   Non-Aggregated Flows—Export Version 5 or 9

e.g. Protocol-Port Aggregation Scheme Becomes

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

Aggregated Flows—Export Version 8 or 9

5. Transport protocol

Cisco NetFlow

- Flujos unidireccionales.
- IPv4 unicast y multicast.
- Agregados (v8) y no agregados (v1,5,6,7).
- Flujos exportados via UDP.
- Soportado en plataformas de IOS y CatOS.
- La implementación de flujos en Catalyst es diferente a la de los enrutadores.

Versiones de Cisco NetFlow

- 4 tipos no agregados (1,5,6,7).
- 14 tipos agregados (8.x).
- Cada version tiene su propio formato de paquetes.
- Version 1 no tiene números de secuencia -- no hay forma de detectar si se han perdido flujos.
- La “version” define el tipo de datos en el flujo.
- Algunas versiones son específicas de la plataforma Catalyst.

NetFlow v1

- Campos claves: IP Origen/Destino, Puerto Origen/Destino, Protocolo IP, ToS, Interfaz de Entrada.
- Contabilidad: Paquetes, Octetos, tiempos de inicio/fin, Interfaz de Salida.
- Otros: OR Binario de los indicadores de TCP.
- Historico – no es recomendable usarlo por la falta de números de secuencia.

Formato de Paquetes Netflow

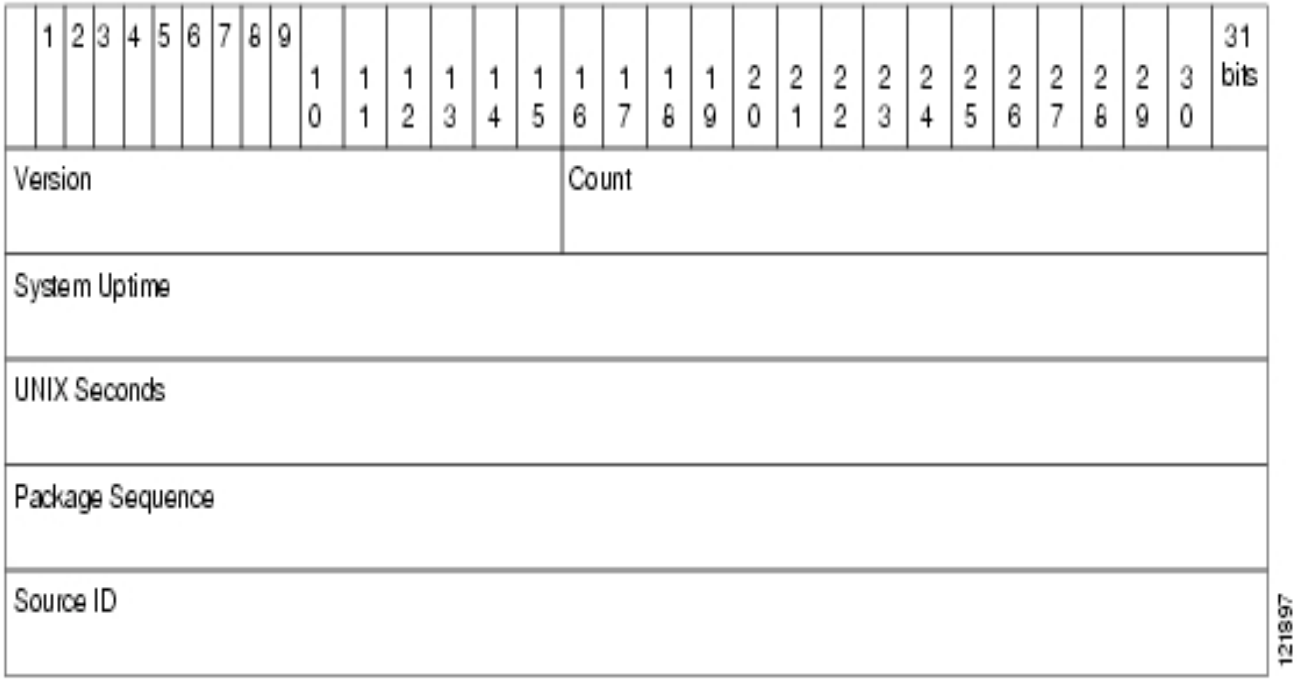
- Encabezado común para todas las versiones.
- Todas las versiones, excepto V1, tienen número de secuencia.
- El campo de datos es específico a cada version con N registros para exportar.
- N es determinado por el tamaño de la definición del flujo. El tamaño del paquete es mantenido por debajo de ~1480 octetos. No se fragmentan en Ethernet y no usa PMTU.

NetFlow Version 9

- v9 es la nueva version. El formato de paquetes es mas flexibles y permite que nuevos campos puedan ser agregados sin la necesidad de que haya que crear una version nueva y mantener un empaquetado compacto.

Version 9

Version 9



NetFlow v8

- Flujos v5 agregados.
- 3 versiones específicas al Catalyst 65xx que corresponden a las mascaras configurables de flujos.
- Mucho menos data para procesar, pero se pierde la granularidad de v5 -- no direcciones de IP.

NetFlow v8

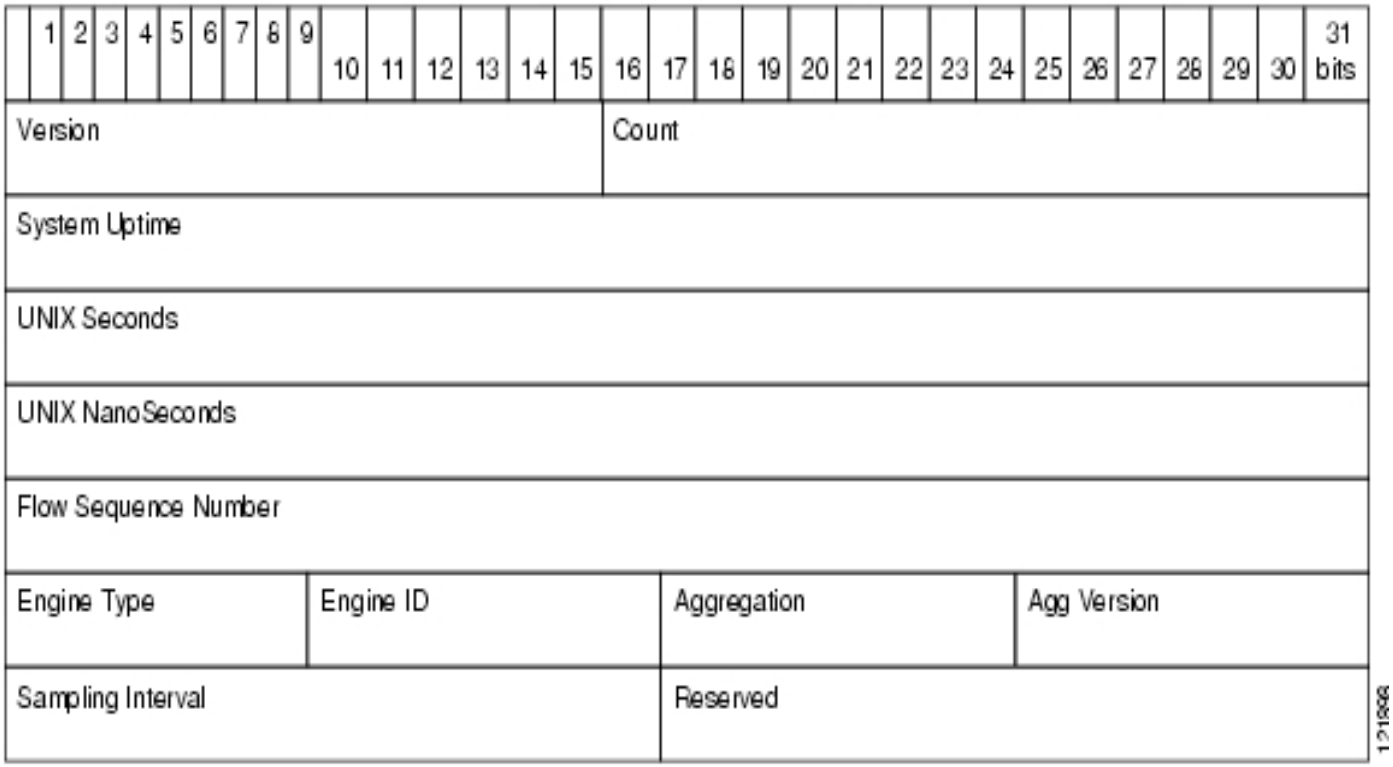
- AS
- Protocolo/Puetto
- Prefijo de Origen
- Prefijo de Destino
- Prefijo de mascara
- Destino (Catalyst 65xx)
- Fuente/Destino (Catalyst 65xx)
- Flujo Completo (Catalyst 65xx)

NetFlow v8

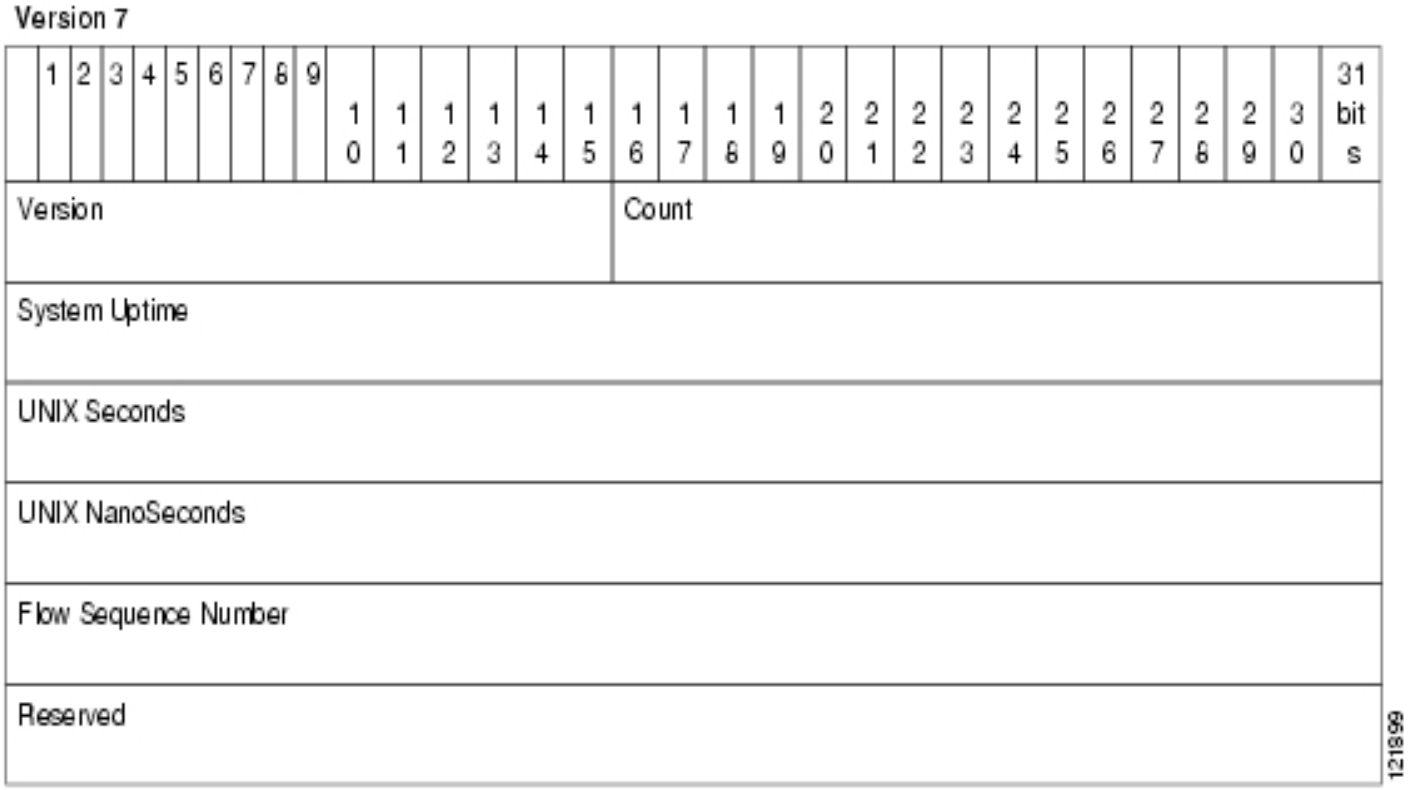
- ToS/AS
- ToS/Protocolo/Puerto
- ToS/Prefijo de Origen
- ToS/Prefijo de Destino
- Tos/Prefijo Origen/Destino
- ToS/Prefijo/Puerto

Version 8

Version 8



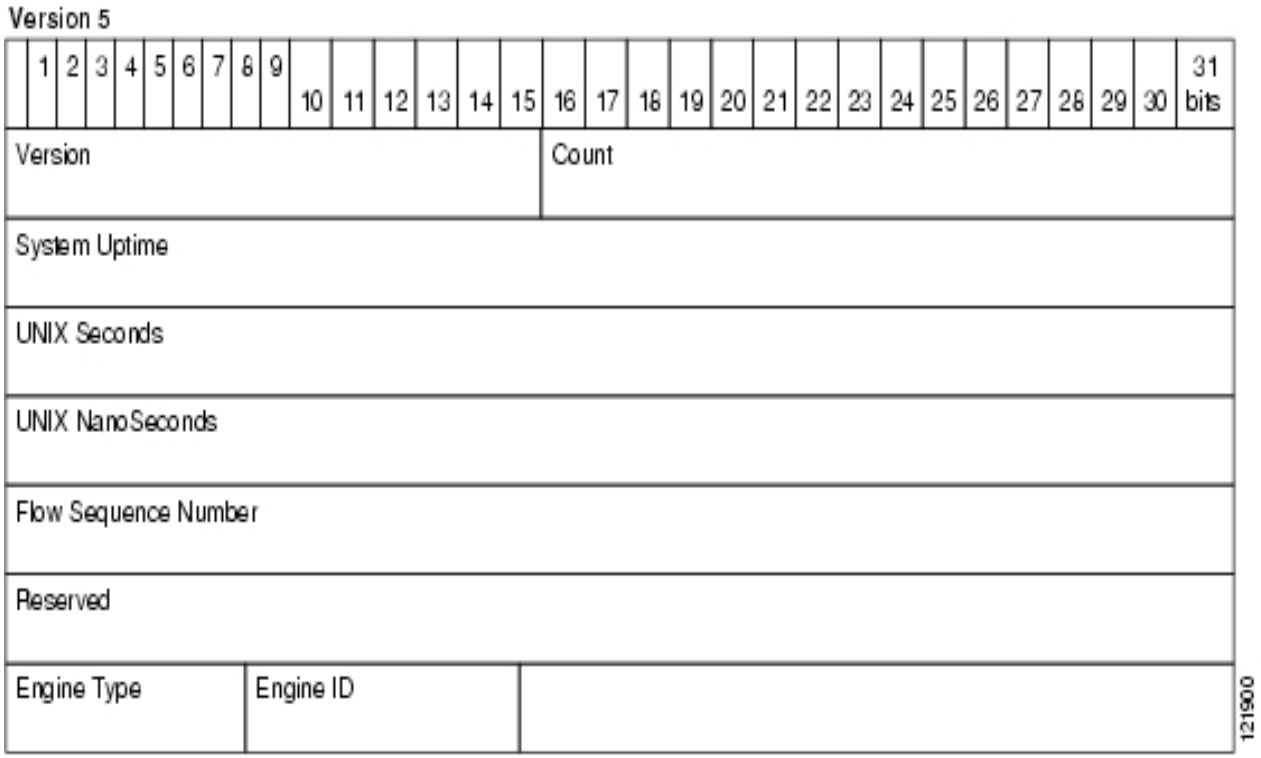
Version 7


Version 7
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
121699

NetFlow v5

- Campos claves: IP Origen/Destino, Puerto Origen/Destino, Protocolo IP, ToS, Interfaz de Entrada.
- Contabilidad: Paquetes, Octetos, tiempo inicio/fin, Interfaz de salida.
- Otros: OR binary de los indicadores de TCP, AS Origen/Destino, Mascara de IP.
- El formato de los paquetes incluye números de secuencia para detectar perdidas de flujos.

Version 5


Version 5
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
Engine Type
Engine ID
121900

NetFlow v5 Packet (Header)

```
struct ftpdu_v5 {
  /* 24 byte header */
  u_int16 version;      /* 5 */
  u_int16 count;        /* Numero de registros en el PDU */
  u_int32 sysUpTime;    /* Tiempo actual en milisegundos desde que
                           el enrutador se inicializó */
  u_int32 unix_secs;    /* Número de segundos desde el EPOCH (0000 UTC 1970)*/
  u_int32 unix_nsecs;   /* Nanosegundos residuales desde el EPOCH*/
  u_int32 flow_sequence;/* Contador secuencial del número de flujos vistos */
  u_int8  engine_type;  /* Typo de dispositivo de conmutado de flujos
                           (RP,VIP,etc.) */
  u_int8  engine_id;    /* Numero de puerto del dispositivo de conmutado de
                           flujos */
  u_int16 reserved;
```

NetFlow v5 Packet (Records)

```
 /* 48 byte payload */
  struct ftrec_v5 {
    u_int32 srcaddr;    /* Dirección IP origen */
    u_int32 dstaddr;    /* Dirección IP destino */
    u_int32 nexthop;    /* Drección IP del próximo enrutador */
    u_int16 input;      /* Indice de la interfax de entrada */
    u_int16 output;     /* Indice de la interfaz de salida */
    u_int32 dPkts;      /* Paquetes enviados en el tiempo de muestreo */
    u_int32 dOctets;    /* Octetos enviados en el tiempo de muestreo. */
    u_int32 First;      /* SysUptime al inicio del flujo */
    u_int32 Last;       /* y del último paquete del flujo */
    u_int16 srcport;    /* Puerto TCP/UDP origen o equivalente */
    u_int16 dstport;    /* Puerto TCP/UDP destino o equivalente */
    u_int8  pad;
    u_int8  tcp_flags;  /* OR binario de indicadores de tcp */
    u_int8  prot;       /* Protocolo IP, e.g., 6=TCP, 17=UDP, ... */
    u_int8  tos;        /* Tipo de Servicio IP */
    u_int16 src_as;     /* AS originador de la IP de origen */
    u_int16 dst_as;     /* AS originador de la IP de destino */
    u_int8  src_mask;   /* prefijo de mascara de dirección origen */
    u_int8  dst_mask;   /* prefijo de mascara de dirección destino */
    u_int16 drops;
  } records[FT_PDU_V5_MAXFLOWS];
};
```

Configuración de Cisco IOS

- Configurar para cada interfaz de entrada.
- Definir la versión.
- Definir la dirección de IP del colector (a donde se envian los flujos).
- Opcionalmente, abilitar la agregación de tablas.
- Opcionalmente, configurar el tiempo de expiración de los flujos y el tamaño de la tabla (v5).
- Opcionalemente, configurar el tiempo/tamaño de muestreo.

Cisco IOS Configuration

```
interface FastEthernet0/0
 ip address 150.185.180.237 255.255.254.0
 no ip directed-broadcast
 ip route-cache flow

interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 no ip directed-broadcast
 ip route-cache flow

interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast

ip flow-export version 5 origin-as
ip flow-export destination 192.168.0.2 9991
ip flow-export source loopback 0

ip flow-aggregation cache prefix
 export destination 192.168.0.2 8888
 enabled
```

Cisco IOS Configuration

```
track4-gw#sh ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       192.168.0.1 (FastEthernet0/1)
    Destination(1)  192.168.0.2 (9991)
  Version 5 flow records, origin-as
  1663010 flows exported in 60827 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failure
```

Cisco IOS Configuration

```
track4-gw#sh ip ca fl
IP packet size distribution (15137447 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  4
   .000 .378 .298 .019 .031 .018 .011 .008 .001 .001 .002 .003 .002 .000 .(

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .001 .016 .014 .187 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  83 active, 4013 inactive, 1666353 added
  28823363 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  83 active, 941 inactive, 1666353 added, 1666353 added to flow
  0 alloc failures, 1785 force free
  1 chunk, 115 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(S
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Fl
TCP-Telnet        1242      0.0       440    65      1.6       8.2        9
TCP-FTP             61      0.0        20    72      0.0       3.7        1
TCP-FTPD             2      0.0         1    42      0.0       0.0        0
```

Cisco IOS Configuration

```
TCP-WWW          713937      2.1          10   527      23.2          1.6          3
TCP-SMTP            553      0.0          21   445       0.0          3.1          1
TCP-X                 2      0.0           1    42       0.0          0.0          8
TCP-BGP               2      0.0           1    42       0.0          0.0          0
TCP-NNTP              2      0.0           1    42       0.0          0.0          0
TCP-other         84079      0.2          22   199       5.5          6.1          8
UDP-DNS           63125      0.1           1    73       0.1          0.0         15
UDP-NTP           48316      0.1           1    76       0.1          0.1         15
UDP-other        597364      1.7           3   235       5.7          4.7         15
ICMP             155127      0.4          17    84       8.1         17.0         15
Total:          1663812      4.9           9   347      44.7          4.3         10

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
Fa0/0         207.46.110.87   Fa0/1         150.185.180.237 06 0747 B93B
Fa0/1         192.168.3.107   Fa0/0         207.46.27.161   06 9DC3 0747
Fa0/1         192.168.3.101   Fa0/1         192.168.1.109   01 0000 0800
Fa0/1         192.168.3.101   Fa0/1         192.168.1.108   01 0000 0800
```

Consideraciones de Seguridad

- Utiliza UDP para la transmisión de los paquetes
- El número de secuencia es el numero total de flujos generados (32 bits)
- No hay checksums
- No hay retransmisión de los paquetes (porque es UDP)
- Posible perdida de flujos
- Posible replicación de ataque DoS

Como mitigar aspectos de Seguridad

- Verificar que no haya escasez de recursos en los enrutadores (*show ip flow export*) o en el colector (*netstat -s | egrep -I 'buf' syslog*)
- Utilizar chequeos de RPF en el camino entre los enrutadores y el colector
- Siempre utilizar la misma interfaz para la exportación de los flujos (*ip flow-export source loopback0*)
- Asegurarse de que el colector solo acepte flujos de enrutadore específicos
- Utilizar muestreo de los flujos en lugar de recibirlos todos
- Conectar el colector directamente a los enrutadores en interfaces dedicadas

Flow-tools

- Colección de programas para colectar y procesar flujos compatible con Cisco netflows.
- Escrito en C, diseñado para que sea rápido (escalable a instituciones grandes).
- Incluye una libraría (ftlib) para aplicaciones customizadas.
- Facil de instalar utilizando “configure;make;make install” en la mayoría de las plataformas.
- Diseño distribuido.

flow-capture

- Recive los paquetes de flujos exportados y los almacena en disco.
- Compresión integrada.
- Administra el espacio en disco mediante la expiración de archivos de flujos viejos definido por los parametros (tamaño del espacio utilizado o el número de archivos).
- Pre-filtrado and Pre-marcado.

flow-capture

- Incluye instrumentación para medida de flujos/segundo, paquetes/segundo, y paquetes perdidos.
- Servidor para clientes que usan TCP.
- Opción de privacidad para remover los bits de estación en los flujos.

flow-fanout

- Replica los paquetes de flujos de un origen a varios destinos.
- El destino puede ser una dirección multicast.
- Incluye la misma instrumentación que flow-capture.
- Puede traducir el formato de los paquetes de salida.
- Soporta mascara de privacidad.

flow-expire

- Expira (remueve) archivos viejos de flujos basado en el tamaño almacenado o el número de archivos.
- Misma funcionalidad que flow-capture.
- Utilizado cuando se trata de administrar el espacio en disco en un ambiente distribuido.

flow-print

- Imprime una salida formateada de los archivos de flujo.

```
root@server:~# flow-print < /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-13.10350(
| head -15
srcIP            dstIP            prot  srcPort  dstPort  octets      packets
192.168.2.102    196.216.2.34     6     58928    80       898         15
150.185.180.203  150.185.181.255  17    138      138      229         1
196.216.2.34     150.185.180.237  6     80       58928    16375       15
198.133.219.25   150.185.180.237  6     80       35363    1820        5
192.168.1.103    198.133.219.25   6     35365    80       1287        18
198.133.219.25   150.185.180.237  6     80       35365    20289       17
192.168.3.107    128.223.157.19   6     47437    80       793         13
128.223.157.19   150.185.180.237  6     80       47437    13015       13
192.168.3.107    192.168.1.102    6     47983    80       376         5
192.168.1.102    192.168.3.107    6     80       47983    1299        5
192.168.3.107    192.168.1.101    6     57773    80       376         5
192.168.1.101    192.168.3.107    6     80       57773    1299        5
192.168.3.107    192.168.2.102    6     51159    80       376         5
192.168.2.102    192.168.3.107    6     80       51159    1299        5
```

flow-cat

- Concatena varios archivos de flujo.

```
root@server:/var/flows/2008/2008-11/2008-11-13# ls
ft-v05.2008-11-13.000001-0430  ft-v05.2008-11-13.002001-0430  ft-v05.2008-11-13.004000-
ft-v05.2008-11-13.000500-0430  ft-v05.2008-11-13.002501-0430  ft-v05.2008-11-13.004500-
ft-v05.2008-11-13.001000-0430  ft-v05.2008-11-13.003000-0430  ft-v05.2008-11-13.005000-
ft-v05.2008-11-13.001500-0430  ft-v05.2008-11-13.003501-0430  ft-v05.2008-11-13.005500-

root@server:/var/flows/2008/2008-11/2008-11-13# flow-cat ft-v05.2008-11-13.00* | flow-p
| head -10
srcIP            dstIP            prot  srcPort  dstPort  octets      packets
192.168.3.102    192.168.2.104    6     80       36518    1299        5
192.168.2.104    192.168.3.102    6     36522    80       376         5
192.168.3.102    192.168.2.104    6     80       36522    1299        5
150.185.130.23   150.185.180.237  17    123      123      76          1
150.185.183.103  150.185.183.255  17    138      138      244         1
150.185.182.58   150.185.182.255  17    631      631      788         4
192.168.2.104    192.168.1.107    6     56670    80       120         2
192.168.2.104    192.168.3.108    6     51752    80       120         2
192.168.2.102    192.168.3.108    6     43148    80       120         2
```

flow-merge

- Es similar a flow-cat excepto que mantiene el orden relativo de los flujos cuando se combina los archivos.
- Tipicamente utilizado cuando se combinan flujos de varios colectores.

flow-filter

- Filtrar los flujos basados número de puerto, protocolo, ASN, dirección IP, bits de ToS, bits de TCP (Historico, se recomienda usar flow-nfilter).

```
root@server:/var/flows/2008/2008-11/2008-11-13# flow-cat . | flow-filter -P80 | flow-
srcIP            dstIP            prot  srcPort  dstPort  octets      packets
192.168.2.104    192.168.3.102    6     36522    80       376         5
192.168.2.104    192.168.1.107    6     56670    80       120         2
192.168.2.104    192.168.3.108    6     51752    80       120         2
192.168.2.102    192.168.3.108    6     43148    80       120         2
192.168.2.104    192.168.1.107    6     56672    80       60          1
192.168.2.104    192.168.3.108    6     51754    80       60          1
192.168.2.102    192.168.3.105    6     34332    80       376         5
192.168.2.101    192.168.3.103    6     52559    80       120         2
192.168.2.101    192.168.3.109    6     59794    80       120         2
192.168.2.102    128.223.157.21   6     54330    80       696         11
192.168.2.102    192.168.3.105    6     34337    80       376         5
192.168.2.102    192.168.3.108    6     43149    80       120         2
```

flow-nfilter

- Filtra flujos basado en cualquiera de los campos definidos, incluyendo operaciones derivada como pps, bbs, y duración.
- Basado en archivos de configuración.
- Suporta operaciones AND y OR.
- Los filtros y primitivas tienen nombres asignados para facilitar su uso.
- Para acelerar el procesamiento utiliza arboles Patricia, tablas de hash busquedas de pila cuando es posible.

flow-nfilter

```
filter-primitive walc-interface
  type ifindex
  permit 1

filter-definition a-internet
  match dst-ifindex walc-interface

filter-definition de-internet
  match src-ifindex walc-interface

filter-primitive UDPTCP
  type ip-protocol
  permit tcp
  permit udp

filter-definition udptcp
  match ip-protocol UDPTCP
```

flow-nfilter

```
filter-primitive taller4
  type ip-address-prefix
  permit 192.168.0/24
  permit 192.168.1/24
  permit 192.168.2/24
  permit 192.168.3/24

filter-primitive DNS
  type ip-port
  permit 53

filter-primitive WEB
  type ip-port
  permit 80,8080,443

filter-definition WALCDNS
  match ip-address taller4
  match ip-protocol UDP
  match ip-destination-port DNS
```

flow-nfilter

- Busqueda de dirección IP usa arbol Patricia, el pero caso es O(w), donde w es el tamaño de la direccion en bits.
- Busqueda del protocolo IP es pila, siempre en el orden O(1).
- Busqueda del puerto IP Port tambien es pila, con orden O(1).
- El rendimiento se mantiene relativamente constante aunque se carge una tabla de prefijos complete (mas de 200,000 entradas).

flow-nfilter

- Otras busquedas utilizan tablas de hash, por ejemplo list de direcciones IP o una list de indicadores de TCP. Usualmente en el orden O(1).
- Algunos filtros requieen busquedas lineales pero regularmente las listas son cortas, por ejemplo filtro de pps, o de tiempo de iniciao.

flow-nfilter

```
root@server:/etc/flow-tools/cfg# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05
    -11-13.103500-0430 | less | flow-nfilter -FWALCDNS | flow-print | head -15

srcIP            dstIP            prot  srcPort  dstPort  octets      packets
192.168.0.2      150.185.130.8    17    56466    53       80          1
192.168.0.2      150.185.130.8    17    26771    53       71          1
192.168.1.105    192.168.0.2      17    47894    53       60          1
192.168.1.105    192.168.0.2      17    40872    53       62          1
192.168.1.106    192.168.0.2      17    35447    53       63          1
192.168.0.2      150.185.130.8    17    26862    53       73          1
192.168.0.2      150.185.130.8    17    45838    53       71          1
192.168.0.2      150.185.130.8    17    48542    53       74          1
192.168.3.102    192.168.0.2      17    43463    53       69          1
192.168.2.101    192.168.0.2      17    50553    53       67          1
192.168.2.101    192.168.0.2      17    44694    53       67          1
192.168.2.101    192.168.0.2      17    53209    53       55          1
192.168.2.101    192.168.0.2      17    51676    53       55          1
192.168.2.101    192.168.0.2      17    34989    53       67          1
```

flow-split

- Divide un archivo de flujos en archivos mas pequeños.
- División basada en tiempo, indicadores, o número de flujos.
- Utulizado, típicamente, con los comandos flow-stat y flow-report para graficar. Por ejemplo, flow-split puede producir intervalos de 5 minutos para una muestra de un dia para un grafico en el tiempo

flow-tag

- Añade un campo de indicadores a los flujos, basado en la IP del exportador, el prefijo IP, AS, o enrutador del próximo salto.
- Utilizado para manejar grupos de prefijos o ASN.
- Por ejemplo, agrupar los flujos por prefijo IP con un identificador de clientes para facturar.

flow-tag

```
#
# tag format
#
# 0       7         15        23        31
# 0000 0000 0000 0000 0000 0000 0000 0000 (32 bits)
# RRRRRRRRRRRRR TTTT NNNNNNNNNNNNNNNNNNN
#               |    |                   | Site name
#               |    | Site type
#               | Reserved
#
# BGP community 65000:X is site name (X -> N)
# BGP community 65001:Y is site type (Y -> T)
#
# SITE_NAME_MASK = 0x0000FFFF
# SITE_TYPE_MASK = 0x00FF0000
#
# ID              Name
#---------------------------------
# 0x0001          OSU
# 0x0002          CWRU
# 0x0003          BGSU
# 0x0004          UC
# 0x0005          UAKRON
# 0x0006          WRIGHT
# 0x0007          KENT
# 0x0008          DAYTON
# 0x0009          OBERLIN
```

```
# ID               Type
#-------------------------
# 0x01          Participant
# 0x02          SEGP
# 0x03          Sponsored-Participant
# 0x04          Gigapop
# 0x05          MULTICAST
```

flow-tag

```
tag-action TALLER4_DST
 type dst-prefix
# CORE
 match 192.168.0/24 set-dst     0x010001
# FILA1
 match 192.168.1/24 set-dst     0x010002
# FILA2
 match 192.168.2/24 set-dst     0x010003
# FILA3
 match 192.168.3/24 set-dst     0x010004
```

```
tag-action OTROS_DST
 type src-prefix
 match 0/0 set-dst 0x0

tag-action OTROS_SRC
 type src-prefix
 match 0/0 set-src 0x0

tag-definition TALLER4
 term
 input-filter 25
 action OTROS_DST
 action TALLER4_DST
 term
 output-filter 25
 action OTROS_SRC
 action TALLER4_SRC
```

flow-header

- Muestra información extra sobre el archivo de flujos.

```
root@server:~# flow-header < /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-13.1035(
#
# mode:                 normal
# capture hostname:     server.track4.ula.ve
# capture start:        Thu Nov 13 10:35:00 2008
# capture end:          Thu Nov 13 10:40:00 2008
# capture period:       300 seconds
# compress:             off
# byte order:           little
# stream version:       3
# export version:       5
# lost flows:           8969
# corrupt packets:      0
# sequencer resets:     0
# capture flows:        19759
#
```

flow-stat

- Genera reportes de los archivos de flujos.
- La salida es facil de leer y puede ser importada facilmente a programas para graficar (por ejemplo gnuplot).
- Por dirección de IP, pares de direcciones de IP puertos, paquetes, octetos, interfaces, próximo salto, AS, bits de ToS, exportador, e indicadore de TCP.
- Historico -- se recomienda usar flow-report.

flow-stat

```
#  --- ---- ---- Report Information --- --- ---
#
# Fields:    Total
# Symbols:   Disabled
# Sorting:   None
# Name:      Overall Summary
#
# Args:      flow-stat -f0
#
Total Flows                          : 111182160
Total Octets                         : 2450050798277
Total Packets                        : 4057574675
Total Time (1/1000 secs) (flows)     : 2414764456464
Duration of data  (realtime)         : 86409
Duration of data (1/1000 secs)       : 88281720
Average flow time (1/1000 secs)      : 21718.0000
Average packet size (octets)         : 603.0000
Average flow size (octets)           : 22036.0000
Average packets per flow             : 36.0000
```

flow-report

- Reemplazo para flow-stat.
- Basado en archivos de configuración.
- Multiples reportes por lectura de datos.
- Salida concurrente por reporte (archivo, programas, opciones de orden, campos).
- Marcado y filtrado integrado para major rendimiento y facilidad de lectura.
- ~ 70 reportes definidos.

flow-report

```
stat-report de-internet-por-protocolo
 type ip-protocol
 filter de-internet
 output
#  path out/de-internet-por-protocolo
  options +header,+names
  fields -pps,-bps,-duration
  sort +octets

stat-definition st1
 report de-internet-por-protocolo

stat-report de-internet-por-cliente
 type ip-source-address
 filter de-internet
 output
#   path out/de-internet-por-cliente
   options +header
   fields -pps,-bps,-duration
   sort +octets

stat-definition st2
 report de-internet-por-cliente
```

```
stat-report a-internet-por-cliente
 type ip-destination-address
 filter a-internet
 output
#   path out/de-internet-por-cliente
   options +header
   fields -pps,-bps,-duration
   sort +octets

stat-definition st5
 report a-internet-por-cliente
```

flow-report

```
stat-report a-internet-tcp
 type ip-destination-port
 filter tcp-a-internet
 output
#  path out/a-internet-tcp
  options +header,+names
  fields -pps,-bps,-duration
  sort +octets
 output
#  path out/a-internet-tcp.p
  options +header,+names,+percent-total
  fields -pps,-bps,-duration
  sort +octets

stat-definition st3
 report a-internet-tcp
```

```
stat-report a-internet-udp
 type ip-destination-port
 filter udp-a-internet
 output
#  path out/a-internet-tcp
  options +header,+names
  fields -pps,-bps,-duration
  sort +octets
 output
#  path out/a-internet-udp.p
  options +header,+names,+percent-
total
  fields -pps,-bps,-duration
  sort +octets

stat-definition st4
 report a-internet-udp
```

Flow-report

- Los siguientes reportes son ejemplos de flujos recibidos en el taller.
- La salida es formateada con flow-rptfmt.

flow-report
Hacia/Desde el track4 por Protocolo

```
root@server:~# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-13.113001-
               | flow-report -Sst1 | flow-rptfmt -fascii
#  --- ---- ---- Report Information --- --- ---
# build-version:        flow-tools 0.68
# name:                 de-internet-por-protocolo
# type:                 ip-protocol
# options:              +names,+header
# sort_field:           +octets
# fields:               +key,+flows,+octets,+packets,+other
# filter:               de-internet
# records:              3
# first-flow:           1226591999 Thu Nov 13 11:29:59 2008
# last-flow:            1226592300 Thu Nov 13 11:35:00 2008
# now:                  1226613664 Thu Nov 13 17:31:04 2008
#  ['/usr/bin/flow-rptfmt', '-fascii']
ip-protocol flows octets   packets
tcp         3485  14358144 49511
udp         4150  6502503  9211
icmp        465   710165   8463
```

flow-report
Al taller4 por puerto TCP destino

```
root@server:~# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-13.113001-0
| flow-report -Sst3 | flow-rptfmt -fascii

ip-destination-port  flows    octets    packets
http                 1966     1380162   15390
telnet               11       334734    8016
imaps                12       277522    3284
https                169      219010    1092
48492                2        141779    1357
60280                2        141739    1356
ssh                  53       114556    1281
34498                3        75666     1244
43607                3        74334     1243
40282                2        72953     1236
1863                 65       57043     607
cfengine             4        17877     182
55641                3        3458      15
55636                2        2598      10
```

flow-report
Desde taller4 por puerto TCP destino

```
root@server:~# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-13.113001-0
| flow-report -Sst3 | flow-rptfmt -fascii

ip-destination-port  flows    octets    packets
http                58.407605 32.544904 37.015658
telnet              0.326797  7.893194  19.279890
imaps               0.356506  6.544106  7.898598
https               5.020796  5.164364  2.626452
48492               0.059418  3.343219  3.263824
60280               0.059418  3.342276  3.261419
ssh                 1.574569  2.701287  3.081030
34498               0.089127  1.784242  2.992039
43607               0.089127  1.752833  2.989634
40282               0.059418  1.720268  2.972797
1863                1.931075  1.345102  1.459942
cfengine            0.118835  0.421549  0.437742
55641               0.089127  0.081541  0.036078
55636               0.059418  0.061262  0.024052
```

flow-report
Al taller4 puerto UDP Destino

```
root@server:~# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-13.113
               001-0430 | flow-report -Sst4 | flow-rptfmt -fascii

ip-destination-port flows     octets    packets
domain              2451      162335    2454
netbios-dgm         111       50495     228
netbios-ns          94        43650     552
snmp                334       24463     339
ntp                 227       17860     235
bootps              35        11480     35
sunrpc              12        10080     72
631                 10        7880      40
snmptrap            4         5578      29
telnet              28        1540      28
49821               1         312       1
48113               1         312       1
```

flow-report
Desde taller4 puerto UDP Destino

ip-destination-port	flows	octets	packets
domain	65.975774	43.824814	55.495251
netbios-dgm	2.987887	13.631897	5.156038
netbios-ns	2.530283	11.783985	12.483039
snmp	8.990579	6.604161	7.666214
ntp	6.110363	4.821580	5.314337
bootps	0.942127	3.099201	0.791497
sunrpc	0.323015	2.721250	1.628223
631	0.269179	2.127326	0.904568
snmptrap	0.107672	1.505866	0.655812
telnet	0.753701	0.415747	0.633198
49821	0.026918	0.084229	0.022614
48113	0.026918	0.084229	0.022614

flow-report
De Internet por IP origen

```
root@server:~# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-
               13.113001-0430 | flow-report -Sst2 | flow-rptfmt -fascii

ip-source-address flows octets  packets
192.168.0.5       14    2629615 4256
128.223.142.89    115   2522994 2578
192.168.0.4       15    2090506 5148
196.216.2.34      116   1878181 1724
192.168.0.3       12    1809118 2461
194.183.242.2     22    1572414 1200
128.223.157.19    111   1444665 1443
192.168.0.2       3096  1323958 10636
128.223.157.21    113   1257351 1243
192.168.0.1       100   391565  4153
128.223.250.133   12    301045  278
129.142.67.19     138   243801  638
207.46.26.115     6     212804  294
128.223.60.195    6     198718  1560
192.168.3.2       53    153711  1503
192.168.3.109     136   149515  2351
```

flow-report
A Internet por IP Destino

```
root@server:~# flow-cat /var/flows/2008/2008-11/2008-11-13/ft-v05.2008-11-
13.113001-0430 | flow-report -Sst5 | flow-rptfmt -fascii

ip-destination-address flows octets packets
192.168.0.2            3021  971514 9993
128.223.60.195         6     261742 3116
192.168.2.105          55    245251 2973
192.168.2.102          232   183111 1260
192.168.1.108          158   178990 1210
150.185.168.7          132   178394 828
192.168.2.101          154   175588 1167
192.168.3.101          164   164211 1021
192.168.3.108          149   162793 1006
192.168.3.104          135   161753 992
192.168.3.109          134   161570 991
192.168.3.106          128   161190 985
192.168.3.107          128   161190 985
192.168.0.5            3     157207 1695
128.223.142.89         115   148108 2574
196.216.2.34           131   109558 1805
```

flow-dscan

- Herramienta para la detección de DoS y de exploración de la red.
- Marca las estaciones que tienen flujos a muchas otras estaciones.
- Marca las estaciones que utilizan un alto número de puertos TCP/UDP.
- Funciona mejor en redes pequeñas con flow-filter para limitar el tráfico a analizar. Por ejemplo, filtrar puerto TCP 25 para detectar estaciones infectadas con gusano de email.

flow-gen

- Herramienta de depuración para generar flujos

```
root@server:~# flow-gen -V8.1 | flow-print | head -15
srcAS   dstAS   in      out     flows       octets      packets     duration
0       65280   0       65280   2           1           1           4294901760
1       65281   1       65281   4           2           2           4294901760
2       65282   2       65282   6           3           3           4294901760
3       65283   3       65283   8           4           4           4294901760
4       65284   4       65284   10          5           5           4294901760
5       65285   5       65285   12          6           6           4294901760
6       65286   6       65286   14          7           7           4294901760
7       65287   7       65287   16          8           8           4294901760
8       65288   8       65288   18          9           9           4294901760
9       65289   9       65289   20          10          10          4294901760
10      65290   10      65290   22          11          11          4294901760
11      65291   11      65291   24          12          12          4294901760
12      65292   12      65292   26          13          13          4294901760
13      65293   13      65293   28          14          14          4294901760
```

flow-send

- Transmite archivos de flujos usando el protocolo NetFlow ahacia otro colector.
- Puede ser utlizado para leer archivos de flujos de flow-tools para enviarlos otro colector compatible con NetFlow.

flow-receive

- Similar a flow-campture pero no maneja el espacio en disco. La salida es hacia standard-out (la pantalla) y puede usarse directamente con otras aplicaciones de flow-tools.
- Utilizado, típicamente, para depuración.

```
root@server:~# flow-receive 0/0/9981 | flow-print
flow-receive: setsockopt(size=4194304)
flow-receive: New exporter: time=1226605200 src_ip=192.168.0.4 dst_ip=0.0.0.0 d_versi
srcIP            dstIP            prot  srcPort  dstPort  octets      packets
192.168.1.108    161.196.183.3    6     45350    80       100         2
192.168.2.101    129.142.67.19    6     35875    80       433         6
192.168.2.101    192.168.1.102    6     51926    80       376         5
192.168.1.102    192.168.2.101    6     80       51926    1299        5
192.168.2.101    192.168.3.106    6     40394    80       376         5
192.168.3.106    192.168.2.101    6     80       40394    1299        5
192.168.1.103    192.168.2.2      17    59608    161      73          1
192.168.2.2      192.168.1.103    17    161      59608    77          1
192.168.1.103    192.168.2.2      17    37630    161      73          1
192.168.2.2      192.168.1.103    17    161      37630    77          1
```

flow-import

- Importa flujos de otros formatos para ser usados con flow-tools.
- Actualmente soporta los formatos ASCII, cflow y Cisco NFC.

flow-export

- Xporta flujos desde archivos de flujos de flow-tools hacia otro formatos.
- Actualmente soporta los formatos ASCII, cflow y MySQL.
- La salida ASCII puede ser utlizada con PERL u otros lenguajes de programación (con una penalización en rendimiento).

flow-xlate

- Traduce flujos entre las diferentes versiones de Netflow.
- Creado originalmente para ser utilizado con switches Catalyst porque exportan algunos flujos en versión 7 y otros en version 5.
- Tambien puede enmascarar los valores de los indicadores.