

# Introducción a los Flujos de Red (Network Flows)

Carlos Vicente  
Servicios de Red  
Universidad de Oregon

# Contenido

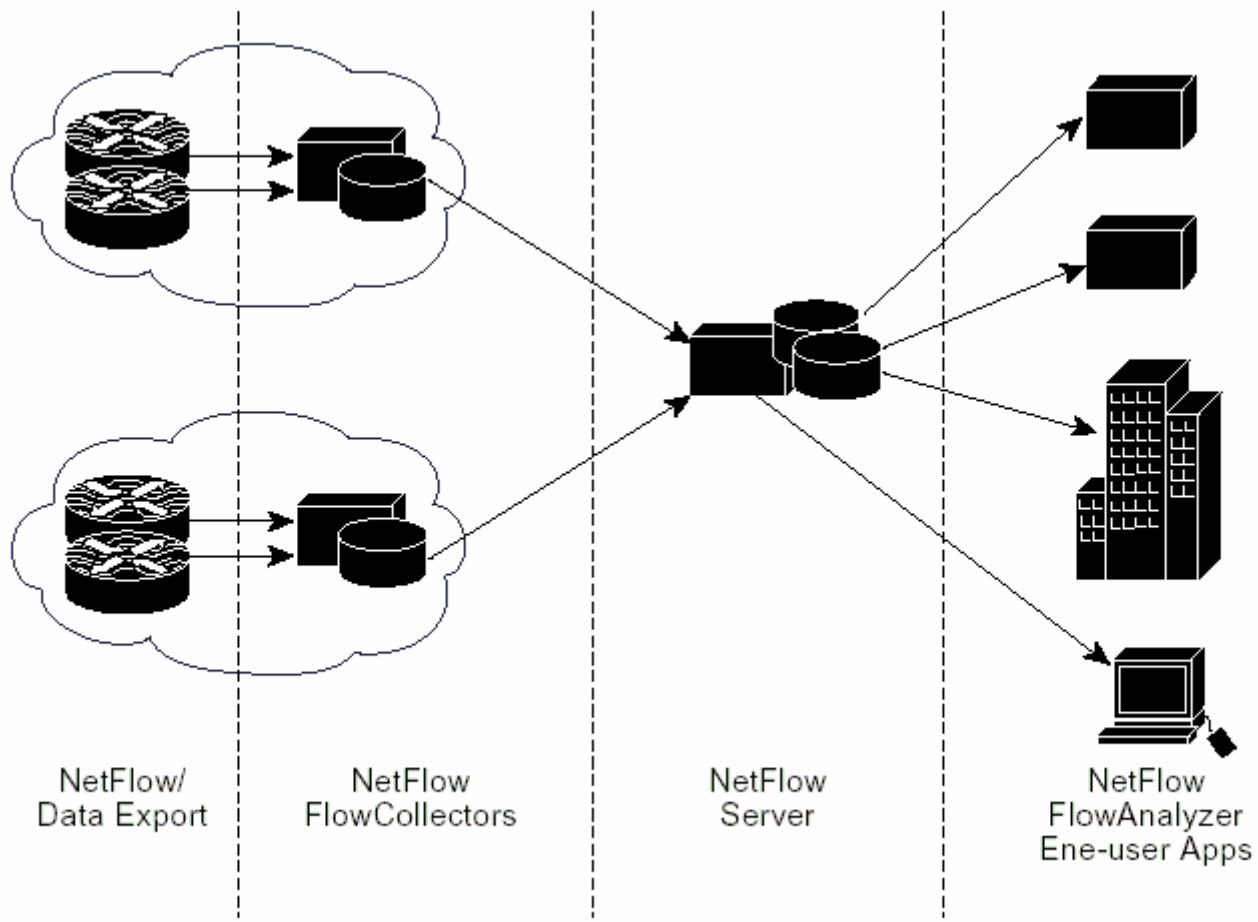
- Qué es un flujo
- Usos prácticos en gestión de redes
- Componentes de la arquitectura
- Cisco *NetFlow*: versiones, configuración
- Otras implementaciones
- Análisis
- Herramientas

# Flujo según Cisco

- Se define como una secuencia *unidireccional* de paquetes con ciertas características comunes:
  - Direcciones IP fuente y destino
  - Número de protocolo a nivel 3
  - Puertos fuente y destino
  - Octeto de ToS (Type of Service)
  - Índice de la interfaz de entrada (ifIndex)

# Componentes

- Exportador (Router o Switch)
  - Crea un flow cache y exporta los récords
- Colector
  - Escucha en un puerto UDP
  - Guarda o reenvía los flows a otros colectores
- Analizador
  - Filtra, muestra, analiza y/o grafica los datos



# 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 Records

- Bajo ciertas circunstancias, los records 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

Srctf	Srct Paddr	Dstf	Dst Paddr	Protocol	TOS	Frgs	11000	00A2	Src Msk	Src AS	00A2	Dst Msk	Dst AS	Next Hop	Bytes/Pkt	Active	Idle
Fa 1/0	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
Fa 1/0	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
Fa 1/0	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
Fa 1/0	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

Srctf	Srct Paddr	Dstf	Dst Paddr	Protocol	TOS	Frgs	11000	00A2	Src Msk	Src AS	00A2	Dst Msk	Dst AS	Next Hop	Bytes/Pkt	Active	Idle
Fa 1/0	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



## 4. Export version

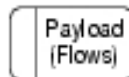
Non-Aggregated Flows—Export Version 5 or 9

e.g. Protocol-Port Aggregation Scheme Becomes

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

## 5. Transport protocol

Export Packet

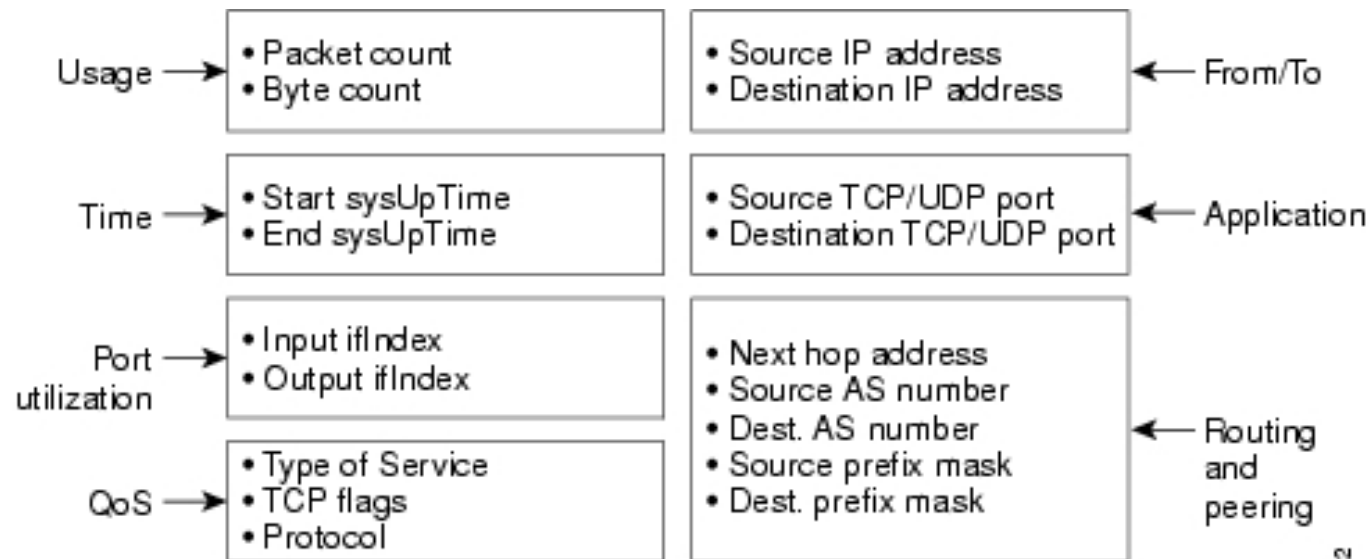


Aggregated Flows—Export Version 8 or 9

# Versiones de NetFlow

- 1: Versión original. Ya no se utiliza
- 5: Agregó información sobre sistemas autónomos (BGP) y números de secuencia. La más utilizada hoy día
- 7: Básicamente igual a la 5, pero en Catalyst
- 8: Agregación en el router
- 9: Más flexible, basada en plantillas, soporta agregación en el router. Sirviendo como base para el nuevo estándar IPFIX de la IETF

# Campos de NetFlow v5



# Rendimiento

- Diversos factores afectan el rendimiento del enrutador al exportar flujos
  - Número de flujos activos
    - Controlar los timers
  - Número de flujos exportados
    - Uso de muestreo (*sampling*)
  - Agregación en el enrutador (versiones 8 ó 9)
  - Cantidad de memoria asignada a la cache (en algunos modelos)

# Muestreo

- Colecta estadísticas para un subconjunto del tráfico que pasa por una interfaz
- Reduce significativamente el impacto en el CPU
- Imagen inexacta del tráfico
  - No sirve para contabilidad y facturación
  - Aún así útil para planificación
- Alternativa para routers del backbone con alto número de interfaces y flujos

# Tipos de Muestreo

- Determinístico
  - Seleccionar uno de cada  $N$  paquetes
- Basado en tiempo
  - Seleccionar un paquete cada  $N$  milisegundos
- Aleatorio
  - De cada  $N$  paquetes, seleccionar uno al azar
  - Considerado como la mejor opción

# Planificación

- Planificar cuidadosamente dónde se van a coleccionar los flujos.
  - Routers de borde o de agregación por donde pasa la mayoría del tráfico
  - Evitar recoger flujos duplicados en routers de backbone
- Buscar la configuración óptima para los tiempos de expiración (timers)
- Determinar qué AS BGP interesa más
  - Peer AS
  - Origin AS

# Configuración

En cada interfaz donde se quieren coleccionar flujos:

```
Router(config-if)# ip route-cache flow
```

Configurar los timers:

```
Router# ip flow-cache timeout active 30 (minutos)
```

```
Router# ip flow-cache timeout active inactive 120 (segundos)
```

# Verificación

Revisar las estadísticas localmente:

```
Router# show ip cache flow
```

```
Router# show ip cache verbose flow
```

```
Router# show ip flow export
```

```
Router# show ip route flow top-talkers
```

# Exportar

Exportar los flujos a un colector:

```
Router(config)# ip flow-export destination 192.168.1.10 9996
```

```
Router(config)# ip flow-export version 5 [ peer-as | origin-as ]
```

```
Router(config)# ip flow-export source loopback 0
```

# Otras implementaciones

- Cflowd (Juniper)
  - No confundir con el colector cflowd
- sFlow (Force10)
- IPFIX (en proceso de estandarización en IETF)

# Usos de los Flujos

- Determinación de problemas
  - Clasificación de tráfico
  - Análisis de ataques de denegación de servicio
- Ingeniería de tráfico
  - Análisis de tráfico Inter-AS
  - Uso de proxies
- Contabilidad
  - Complementa información SNMP

# Herramientas

- Múltiples paquetes open-source disponibles y evolucionando
  - Flow-tools, Flowscan, FlowViewer, nfdump/nfsen, Stager, etc...
- Aplicaciones comerciales
  - Cisco NetFlow collector
  - Arbor Networks
  - Etc.

# Referencias

- Cisco Netflow Services Solution Guide

[www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.htm)