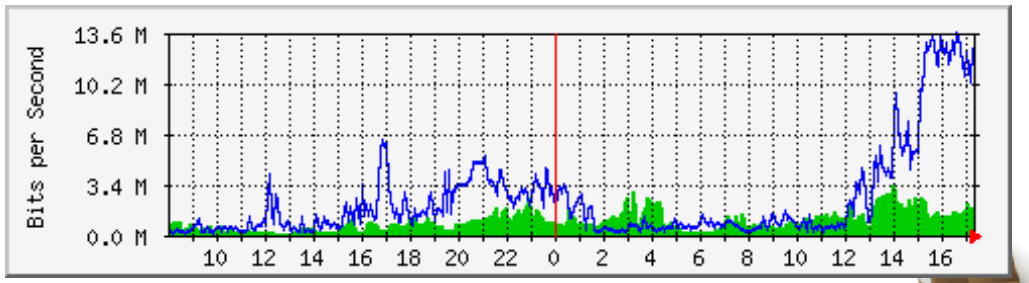
Monitorización de red

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 4º

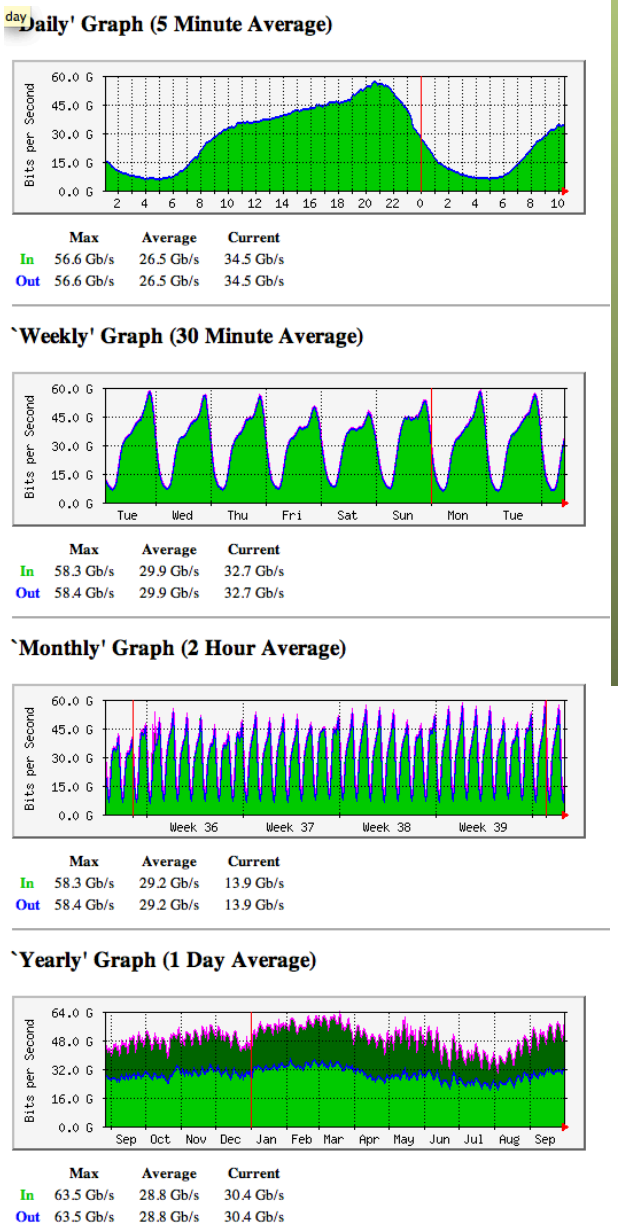
¿Medir qué? Un Ejemplo

- El tráfico en los enlaces entre conmutadores
- A nivel de paquete (ej: tcpdump/wireshark)
- O a nivel de flujo
- Estos son ejemplos de lo que llamamos “medidas pasivas”



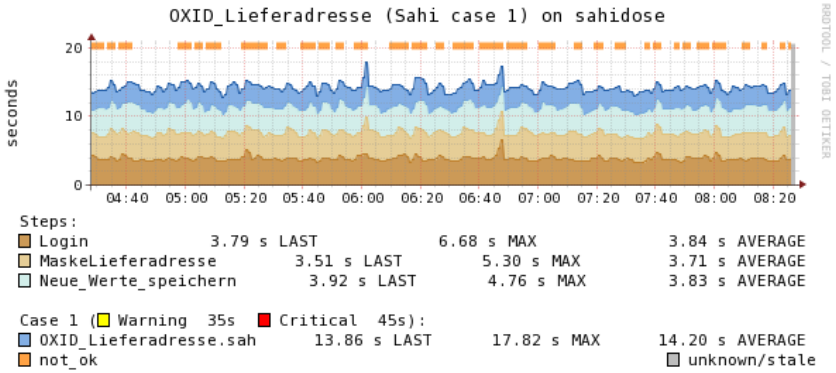
Casos comunes: MRTG

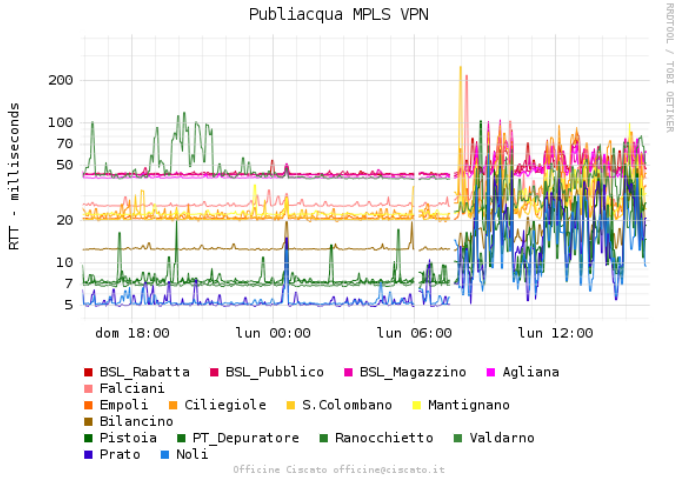
- Multi Router Traffic Grapher
- http://oss.oetiker.ch/mrtg
- Monitoriza variable SNMP
- Comúnmente es utilización de enlaces
- Crea páginas HTML con imágenes
- Consolida datos antiguos
- Free, GPL
- Puede emplear RRDtool
  - (…)



Casos comunes: MRTG

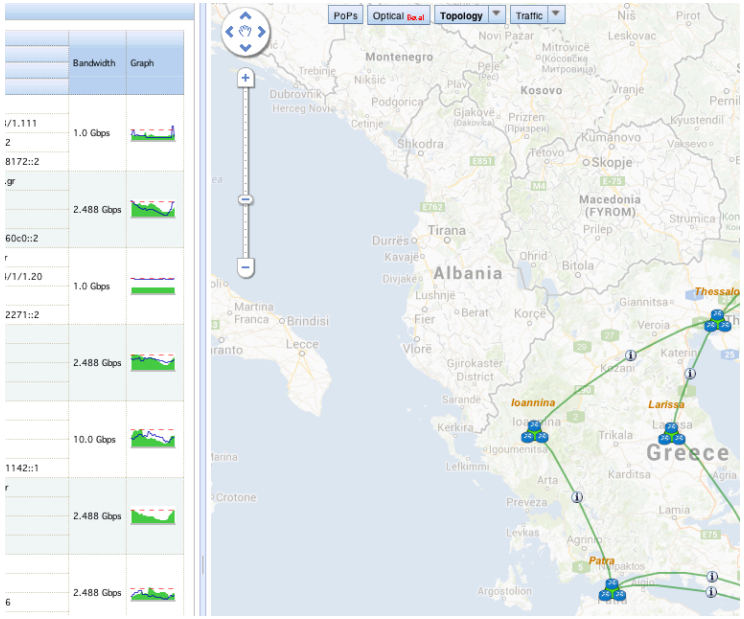
- Multi Router Traffic Grapher
- http://oss.oetiker.ch/mrtg
- Monitoriza variable SNMP
- Comúnmente es utilización de enlaces
- Crea páginas HTML con imágenes
- Consolida datos antiguos
- Free, GPL
- Puede emplear RRDtool
  - http://oss.oetiker.ch/rrdtool/
  - Mayor flexibilidad en las gráficas y mejor rendimiento

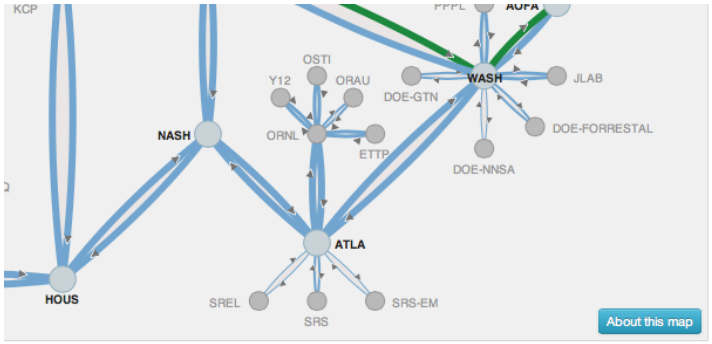


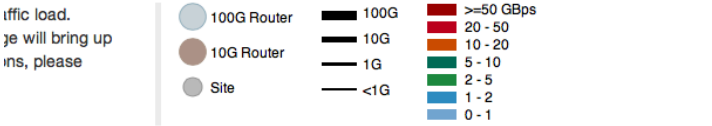


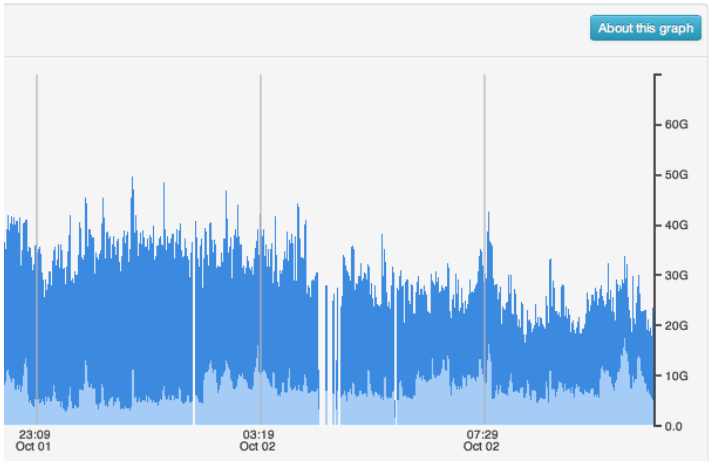
Otros ejemplos

- http://netmon.grnet.gr
- https://my.es.net



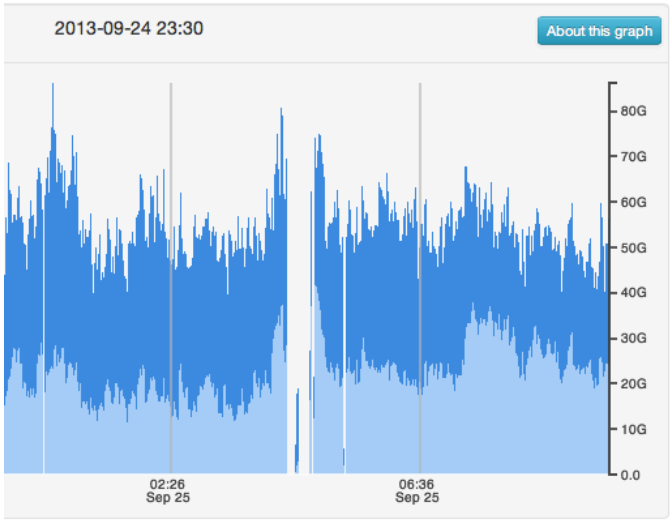






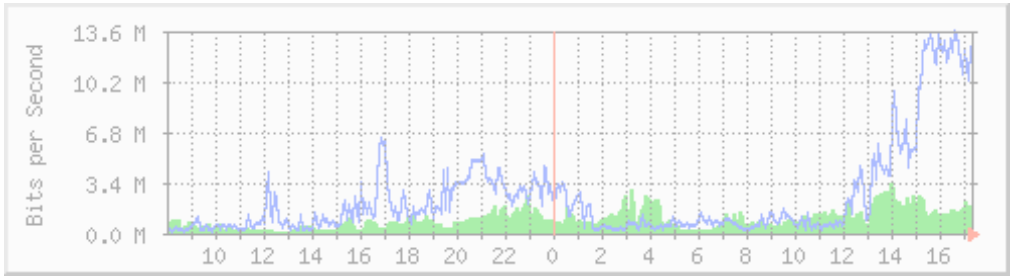
"Monitorización" de red

- No es solamente "medir", eso es la parte de recolectar los "datos"
- Incluye el **interpretarlos**, crear informes sobre rendimiento, crear "información"
- Aunque la diferencia tampoco es muy trascendente y la expresión se emplea con mucha libertad
- Hay muchos parámetros que se pueden monitorizar: por dispositivo, por segmento, por servicio…



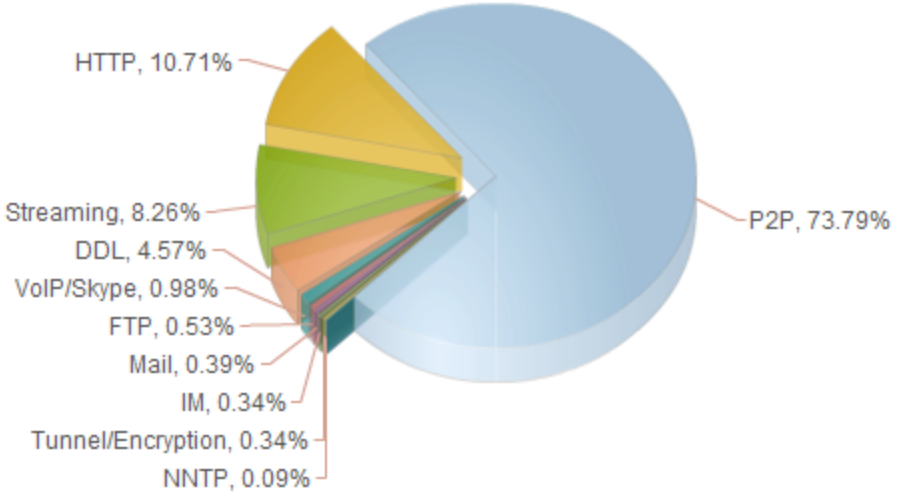
¿Para qué monitorizar?

- Para obtener información
- Utilización de un enlace
- Utilización de un conmutador
- (…)



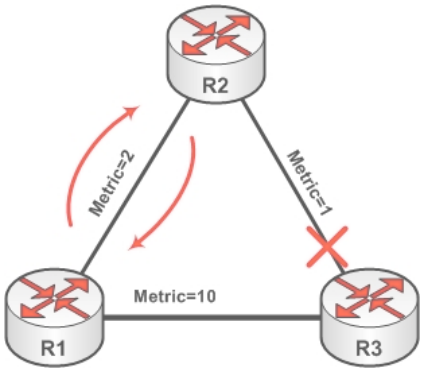
¿Para qué monitorizar?

- Para obtener información
- Utilización de un enlace
- Utilización de un conmutador
- Tráfico por usuarios (matrices de tráfico, facturación)
- Tráfico por servidores (ej: tráfico al servidor de email o al de backups, disponibilidad)
- Tráfico por servicios (ej: tráfico web/email/p2p)
- (…)



¿Para qué monitorizar?

- Para obtener información
- Utilización de un enlace
- Utilización de un conmutador
- Tráfico por usuarios (matrices de tráfico, facturación)
- Tráfico por servidores (ej: tráfico al servidor de email o al de backups, disponibilidad)
- Tráfico por servicios (ej: tráfico web/email/p2p)
- Tiempos de respuesta de servicios (ej: tiempo de respuesta de un servidor de ficheros)
- Evaluar comportamientos de protocolos (ej: reacción de TCP ante pérdidas)
- Detectar problemas en la red (ej: problema con el encaminamiento, congestión en enlaces)
- Detectar problemas con los protocolos (ej: interacción entre DNS y protocolo de aplicación)
- Detectar violaciones de seguridad (ej: escaneos)
- Etc.

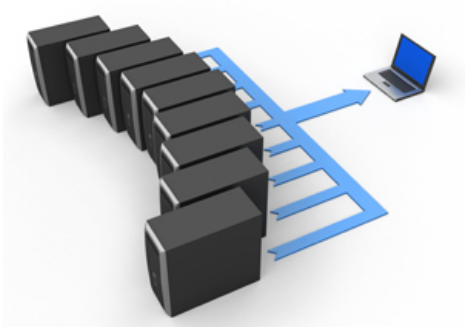


¿Qué medir para esto?

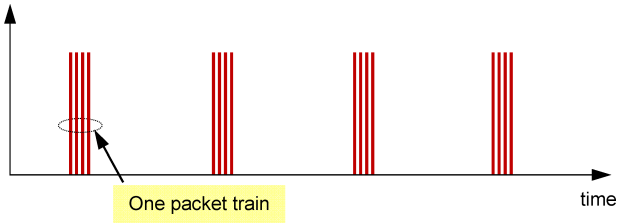
- Según la información que queramos obtener
- Podemos necesitar el tráfico a nivel de cuentas de **paquetes** (ej: pkts/s que reenvía un router) como una estimación de volumen
- O a nivel de volumen de **bytes** por dirección origen (ej: matriz de tráfico por host)
- O a nivel de origen y destino de **flujos** (ej: conexiones TCP simultáneas que mantiene un NAT)
- O necesitar **cabeceras** de paquetes hasta nivel de transporte (ej: analizar el comportamiento de control de flujo de TCP)
- O necesitar los **datos** de nivel de aplicación (ej: reconocer las peticiones HTTP dentro de una conexión TCP)

Tipos de medidas

- **Pasivas**
  - No afectan al tráfico
  - Recoger todos los paquetes en un punto de medida (enlace o equipo)
  - o recoger una muestra de esos paquetes
  - o directamente contadores dados por SNMP
  - y otros que comentaremos



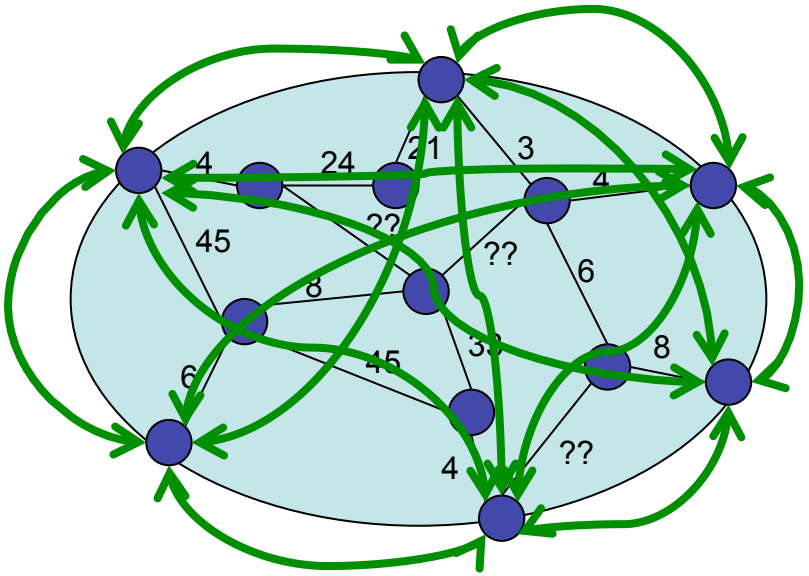
- **Activas**
  - Generamos tráfico y lo recogemos (intrusivo)
  - Según cómo, cuándo y cuáles de los paquetes llegan ofrecemos estadísticas
  - Puede ser un simple *ping*
  - o hacer una llamada a un teléfono IP para comprobar que responde
  - o generar tráfico similar al de voz y medir cómo llega al destino (SLA)
  - u otros patrones de tráfico que permitan inferir el comportamiento de la red
  - Podríamos hacer transferencias masivas aunque es muy intrusivo (se hace)



¿Nos vale con SNMP?

- ¿Podemos monitorizar la red con lo que ofrecen las MIBs?
- Las MIBs suelen dar contadores, por ejemplo por interfaz o protocolo
- Son datos muy agregados
- Solo podemos conseguir series temporales haciendo *polling* de ellos
- Matriz de tráfico para *network capacity planning*
  - Predecir tendencias
  - Escenarios *what-if*
- ¿Matriz a partir de contadores y tablas de rutas? (...)

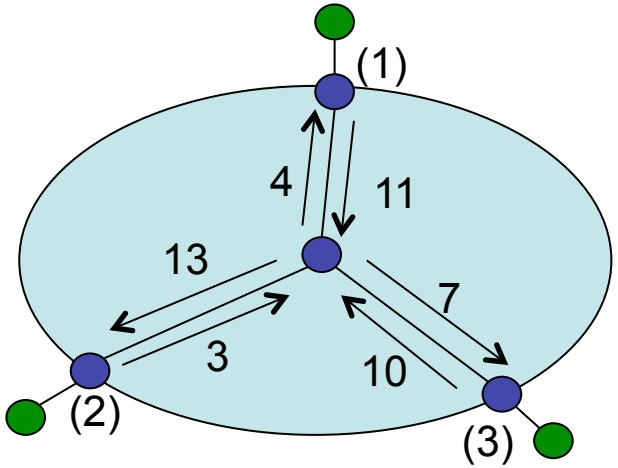
$$TM = \begin{pmatrix} 0 & I_{12} & I_{13} & I_{14} & I_{15} & I_{16} \\ I_{21} & 0 & I_{23} & I_{24} & I_{25} & I_{26} \\ I_{31} & I_{32} & 0 & I_{34} & I_{35} & I_{36} \\ I_{41} & I_{42} & I_{43} & 0 & I_{45} & I_{46} \\ I_{51} & I_{52} & I_{53} & I_{54} & 0 & I_{56} \\ I_{61} & I_{62} & I_{63} & I_{64} & I_{65} & 0 \end{pmatrix}$$



Ejemplo: matriz de tráfico

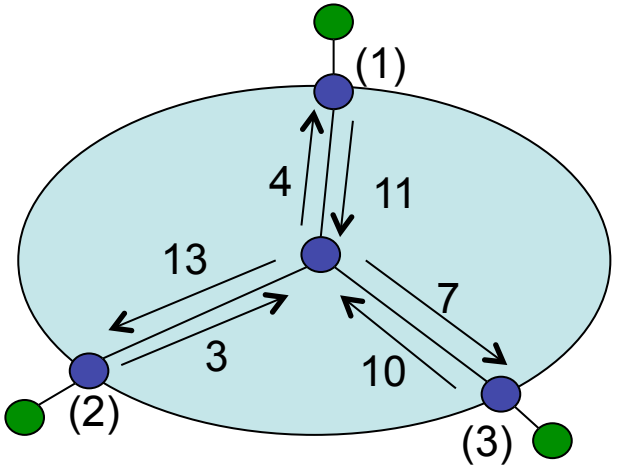
- Intensidad de tráfico para cada (origen, destino) frontera de la red
- Ejemplo:
  - Lo que sabemos con contadores
  - Solución (...)

$$TM = \begin{pmatrix} 0 & I_{12} & I_{13} \\ I_{21} & 0 & I_{23} \\ I_{31} & I_{32} & 0 \end{pmatrix}$$

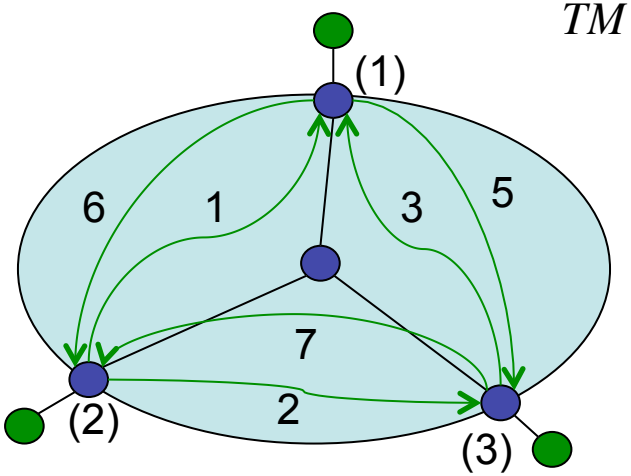


Ejemplo: matriz de tráfico

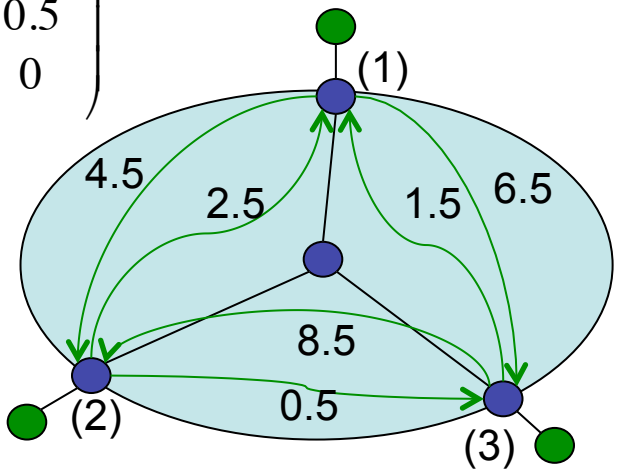
- Intensidad de tráfico para cada (origen, destino) frontera de la red
- Ejemplo:
  - Lo que sabemos con contadores
  - ¿Solución? (...)



$$TM = \begin{pmatrix} 0 & 6 & 5 \\ 1 & 0 & 2 \\ 3 & 7 & 0 \end{pmatrix}$$

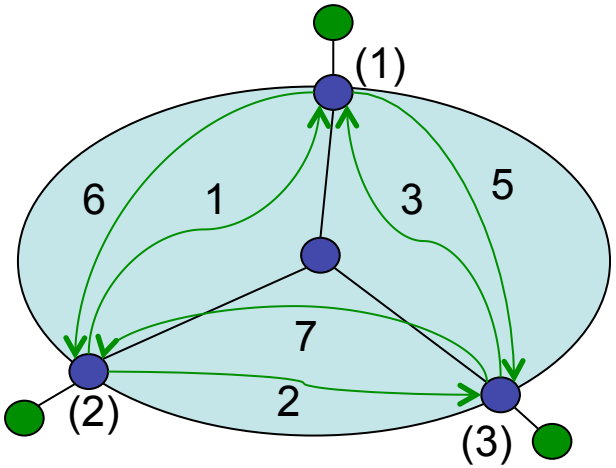


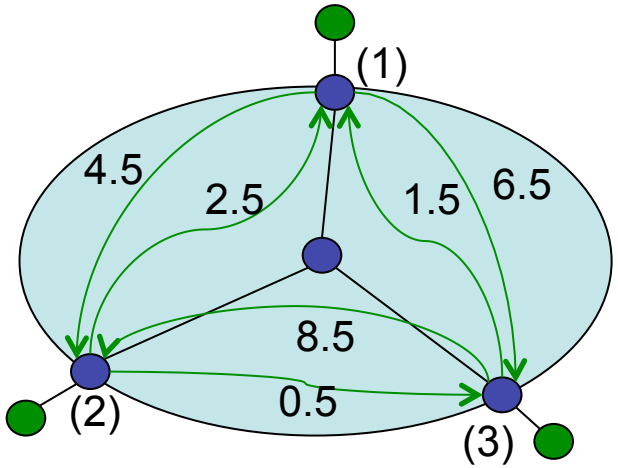
$$TM' = \begin{pmatrix} 0 & 4.5 & 6.5 \\ 4.5 & 0 & 0.5 \\ 6.5 & 8.5 & 0 \end{pmatrix}$$



Ejemplo: matriz de tráfico

- No hay solución única; más incógnitas que ecuaciones
- Múltiples técnicas para calcular la solución *"más probable"*
- Requiere conocer las rutas
- Podemos quererla por servicio/aplicación
- O para cada clase de servicio
- *Network Tomography*: emplear un número limitado de medidas para deducir o estimar otros parámetros de rendimiento



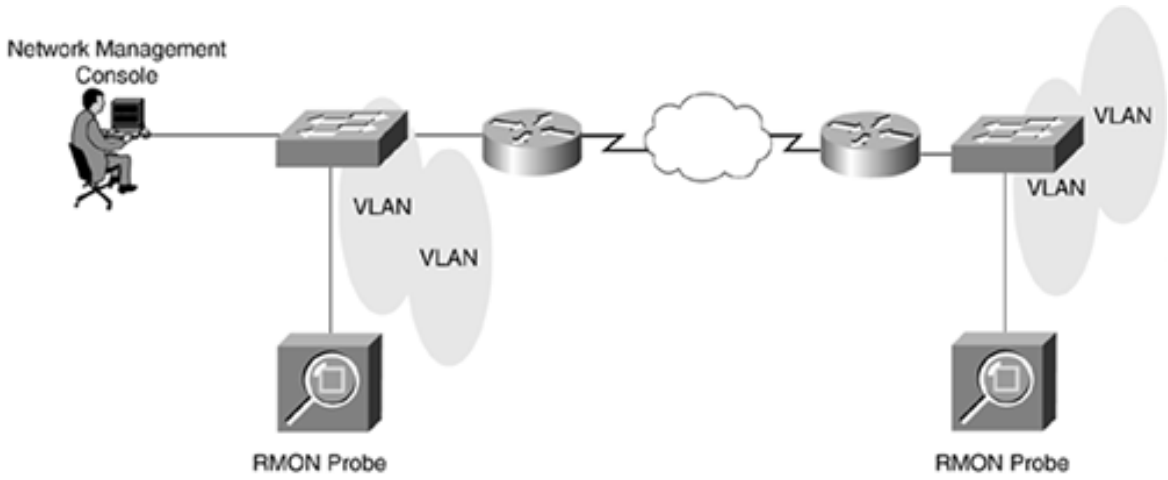


¿Nos vale con SNMP?

- Para las series temporales tenemos que hacer *polling*
- Solo con contadores por enlace no podemos ni tan siquiera calcular matrices de tráfico
- ¿Hay alternativas?
  - RMON
  - Medición de flujos
  - (otras...)

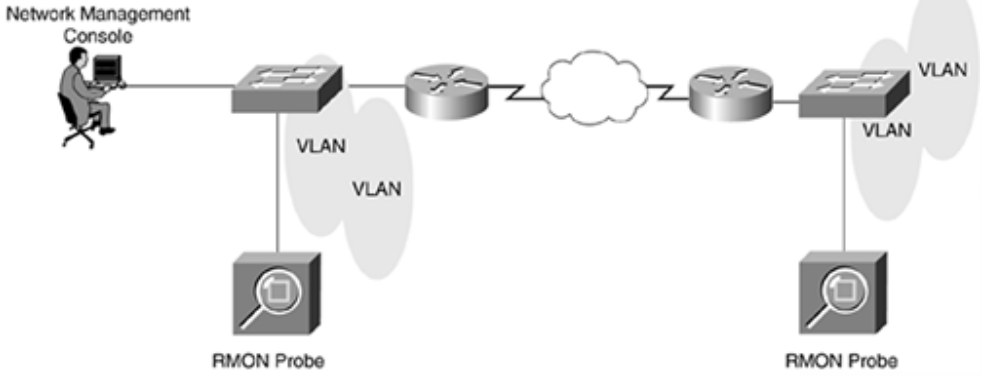
RMON

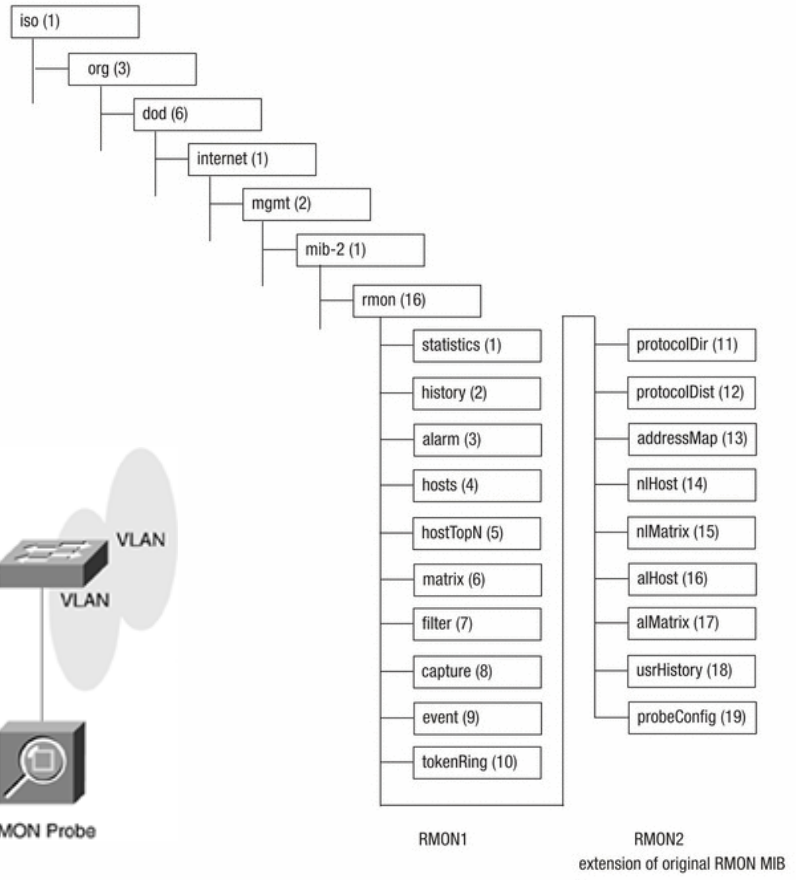
- Sin hacer *polling* puede almacenar series
- RMON1 RFC 2021 (1997), obsoleto por RMON2 RFC 4502 (2006)
- MIB RMON (mib-2.16)
- Desarrollado para dar estadísticas de tráfico Ethernet y diagnóstico de fallos (número de paquetes, errores de CRC, colisiones...)
- Inicialmente en la época de hubs y modo promiscuo
- Se centra en el segmento de red más que en el agente
- Puede analizar el tráfico (por ejemplo cuánto genera cada host)
- RMON1 decodifica hasta nivel 2; RMON2 hasta nivel de aplicación



RMON

- Permite (en teoría) capturar paquetes y que los recoja el NMS
- Las estadísticas son a alto nivel, a nivel de flujos
- SNMP para el acceso
- El trabajo es exigente
- Equipo o tarjeta dedicada
- Con switches requiere *mirror*
- Algunos soportan la parte sencilla





RMON: Ejemplo

- Cisco Catalyst 2960

> - For enhanced traffic management, monitoring, and analysis, the Embedded **Remote Monitoring (RMON)** software agent supports four RMON groups (history, statistics, alarms, and events).

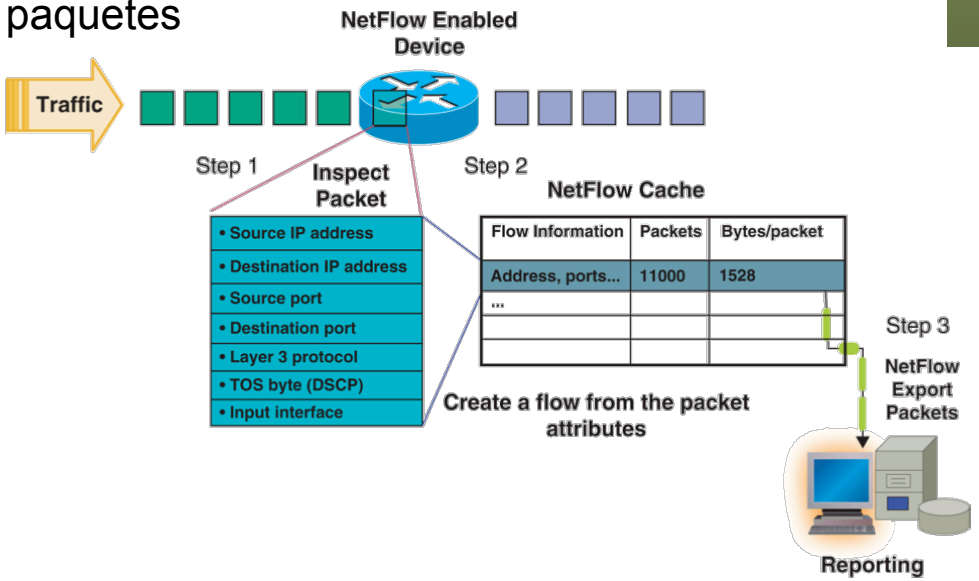
- "History Control Group": configuración del interfaz y periodo de muestreo
- "Ethernet Statistics Group": estadísticas por interfaz (bytes, paquetes, broadcast, multicast, errores CRC, colisiones, etc)
- "Alarm Group": periódicamente (definido en la tabla) toma muestras de variables de la sonda y compara con umbrales, pudiendo producir eventos (implementa una histéresis)
- "Event Group": las entradas describen los parámetros de un evento que se puede producir. Puede llevar a un log (otra tabla de la MIB) o una *trap SNMP*

NetFlow

- Cisco (patentado)
- Origen:
  - IOS mantiene una cache de flujos activos
  - Cache para acelerar la toma de decisiones de reenvío (CEF = *Cisco Express Forwarding*)
  - Con contadores sobre cada uno (bytes, paquetes, etc) en *flow records*
- Para paquetes IPv4 e IPv6 (y MPLS), unicast y multicast
- Se puede emplear para
  - Monitorización y planificación de red
  - Accounting/billing
  - Traffic matrix
  - Detectar ataques
- Ligeramente diferente en routers y switches (switches gama alta)
- Tiene efecto en el uso de CPU del equipo

NetFlow: flujos

- RFC 3954: *"An IP Flow, also called a Flow, is defined as a set of IP packets passing an Observation Point in the network during a certain time interval. All packets that belong to a particular Flow have a set of common properties derived from the data contained in the packet and from the packet treatment at the Observation Point."*
- Flujos unidireccionales
- Una serie de valores (*keys*) del paquete determinan el flujo:
  - Direcciones IP origen y destino
  - Protocolo sobre IP
  - Puertos de transporte origen y destino
  - Interfaz por el que llegan los paquetes
  - DSCP



Netflow: valores

- Número de paquetes y bytes
- Timestamp de primer y último paquete
- Interfaz de entrada y salida
- Next-hop
- ASN origen y destino
- Puede añadir Layer 2
  - Dirección MAC origen y VLAN ID de tramas recibidas
  - Dirección MAC destino y VLAN ID de tramas transmitidas
- Para seguridad puede añadir
  - Máximo y mínimo TTL
  - Máxima y mínima longitud de paquete
  - IPID
  - Código y tipo ICMP
  - Flags TCP acumulados
- Versión 9 provee una definición más flexible del registro para poder añadir campos (*templates*)

NetFlow: agregación

- Versiones: 1 (*legacy*), 5, 7 (solo Catalyst), 8 (agregación), 9 (flexible y extensible), 10 (IPFIX)
- Agregación:
  - Por AS origen y destino
  - Por dirección o prefijo IP origen y destino
  - Por protocolo y puerto
  - etc.

1. Create and update flows in NetFlow cache

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src As	Dst Port	Dst Msk	Dst As	NextHop	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	10.0.23.2	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	10.0.23.2	740	14.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A1	/24	15	10.0.23.2	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	10.0.23.2	1040	24.5	14

2. Expiration

- Inactive Timer Expired (15 Sec Is Default)
- Active Timer Expired (30 Min Is Default)
- NetFlow Cache Is Full (Oldest Flows Are Expired)
- RST or FIN TCP Flag

SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src As	Dst Port	Dst Msk	Dst As	NextHop	Bytes /Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	0	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. Aggregation? (No / Yes)

4. Export version

Non-aggregated flows—export version 5 or 9

5. Transport protocol

Export packet: Header | Payload (Flows)

E.g. Protocol-Port Aggregation Scheme Becomes

Protocol	Pkts	Srcport	Dstport	Bytes/Pkt
11	11000	00A2	00A2	1528

Aggregated Flows—Export Version 8 or 9

B. Claise y R. Wolter, "Network Management: Accounting and Performance Strategies", Cisco Press

NetFlow: exportación

- Los flujos se eliminan de la cache por inactividad
- Con actividad, llegado un tiempo máximo también se eliminan
- Flujos TCP se eliminan ante banderas de FIN o RST
- Si se llena la cache elimina flujos que no han caducado
- Estos *flow records* se exportan a un *collector* por UDP o SCTP (RFC2960)
- Puede ser un ordenador o un módulo en un router/switch
- Exporta múltiples registros en un paquete
- Una aplicación de gestión puede analizar esos registros o exportarse a MIB RMON