

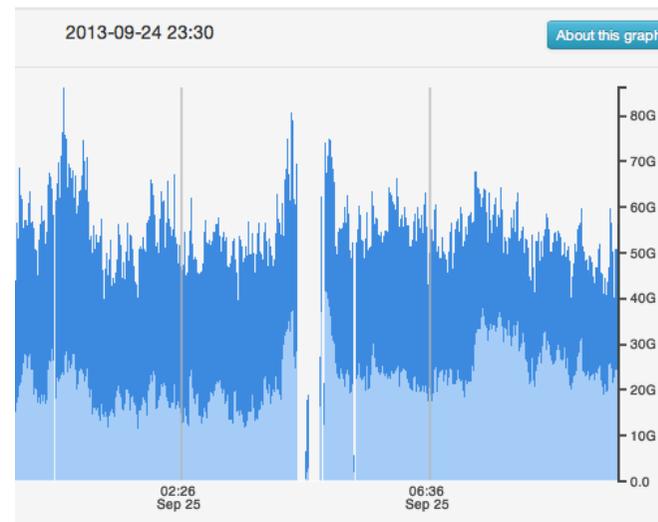
Monitorización de red

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

Grado en Ingeniería en Tecnologías de
Telecomunicación, 4º

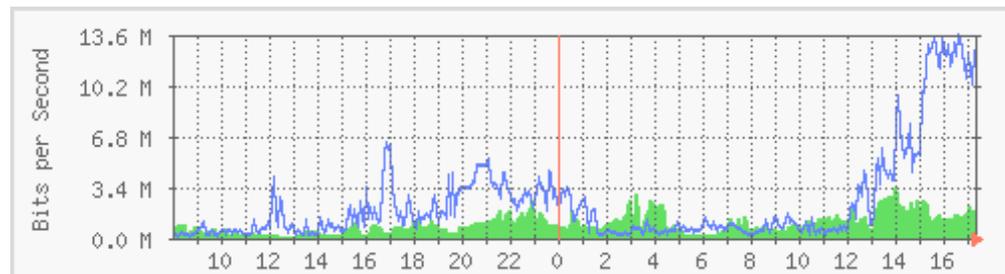
“Monitorización” de red

- 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...



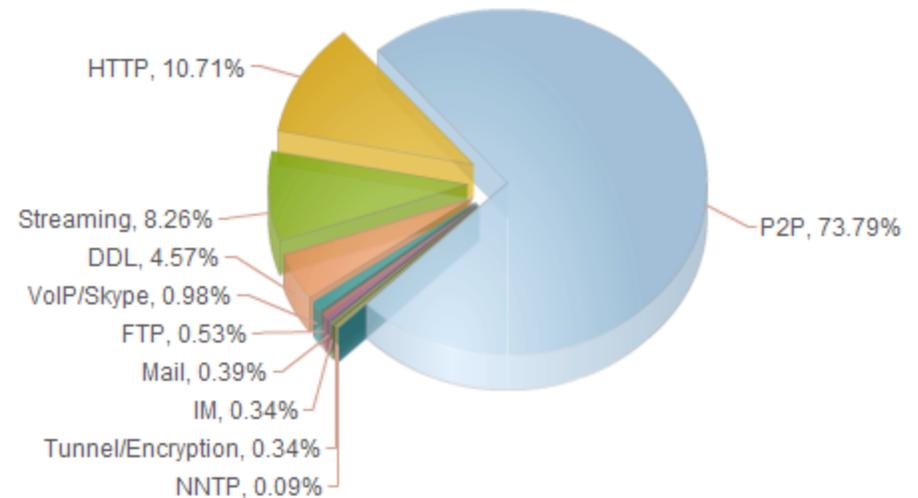
¿Para qué monitorizar?

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



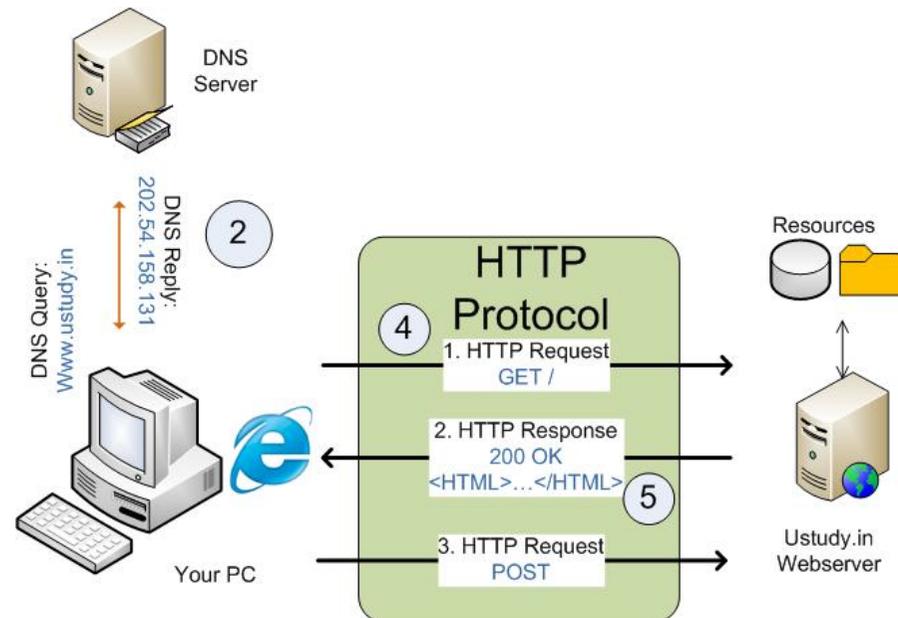
¿Para qué monitorizar?

- 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)
- (...)



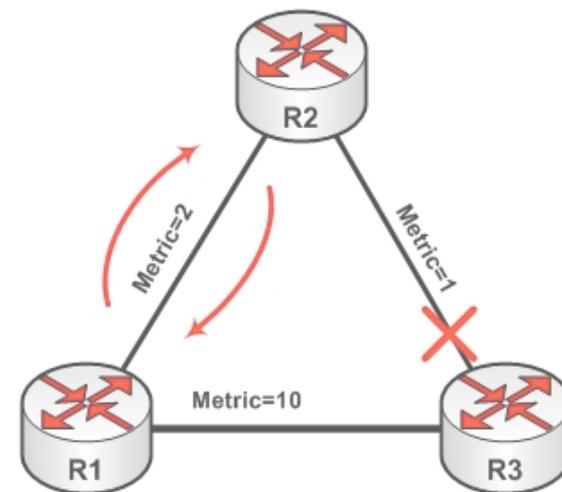
¿Para qué monitorizar?

- 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 con los protocolos (ej: interacción entre DNS y protocolo de aplicación)
- (...)



¿Para qué monitorizar?

- Detectar problemas en la red (ej: problema con el encaminamiento, congestión en enlaces)
- 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)





Medidas activas y pasivas



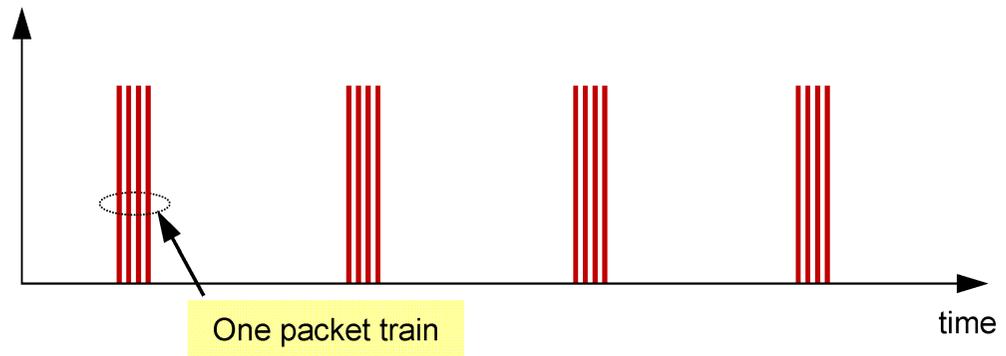
Tipos de medidas

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



Tipos de medidas

- **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)

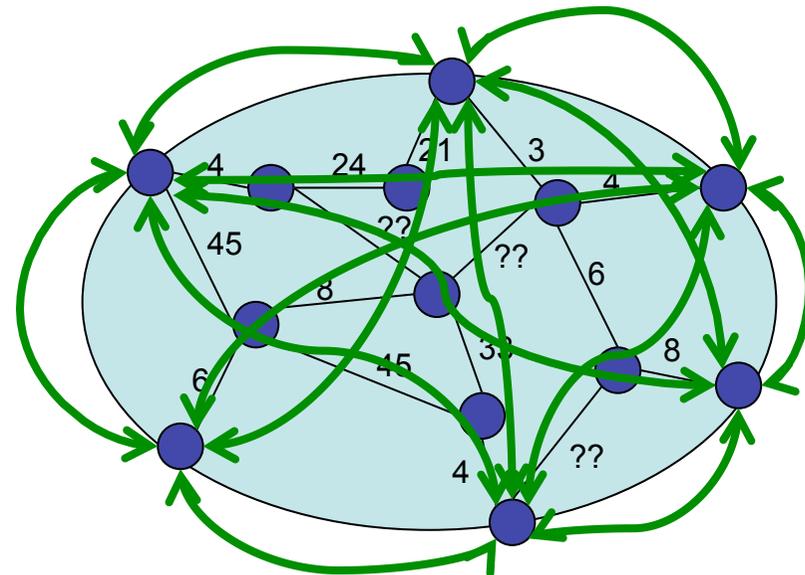


Limitaciones de SNMP

¿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? (...)

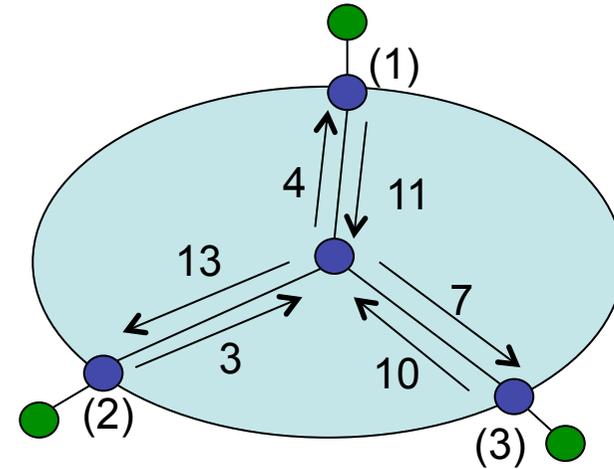
$$TM = \begin{pmatrix} 0 & I_{12} & I_{13} & I_{14} & I_{15} & I_{16} \\ I_{21} & 0 & I_{23} & I_{24} & I_{25} & I_{26} \\ I_{31} & I_{32} & 0 & I_{34} & I_{35} & I_{36} \\ I_{41} & I_{42} & I_{43} & 0 & I_{45} & I_{46} \\ I_{51} & I_{52} & I_{53} & I_{54} & 0 & I_{56} \\ I_{61} & I_{62} & I_{63} & I_{64}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



Ejemplo: matriz de tráfico

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

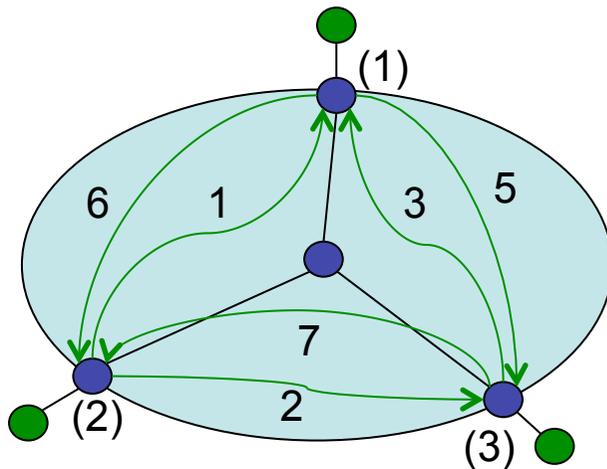
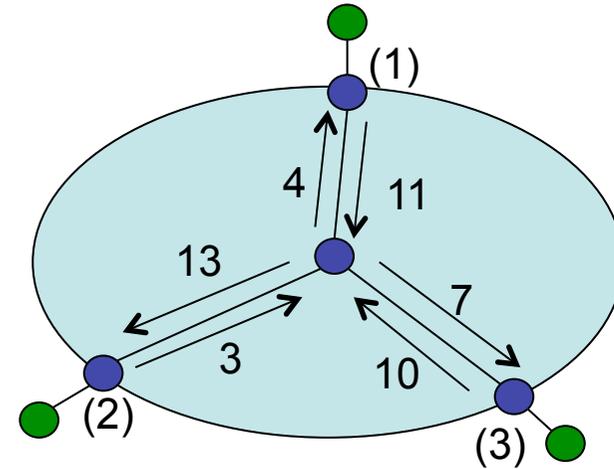
$$TM = \begin{pmatrix} 0 & I_{12} & I_{13} \\ I_{21} & 0 & I_{23} \\ I_{31} & I_{32} & 0 \end{pmatrix}$$



Ejemplo: matriz de tráfico

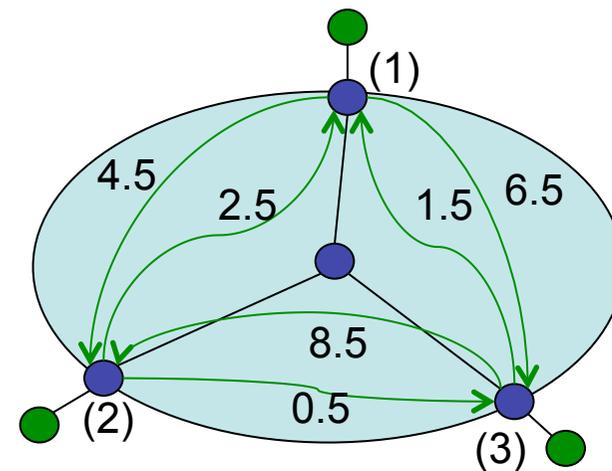
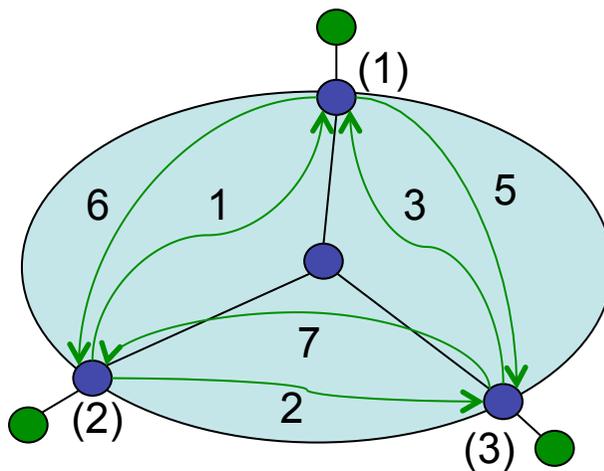
- Intensidad de tráfico para cada (origen, destino) frontera de la red
- Ejemplo:
 - Lo que sabemos con contadores
 - Solución (...)

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



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?

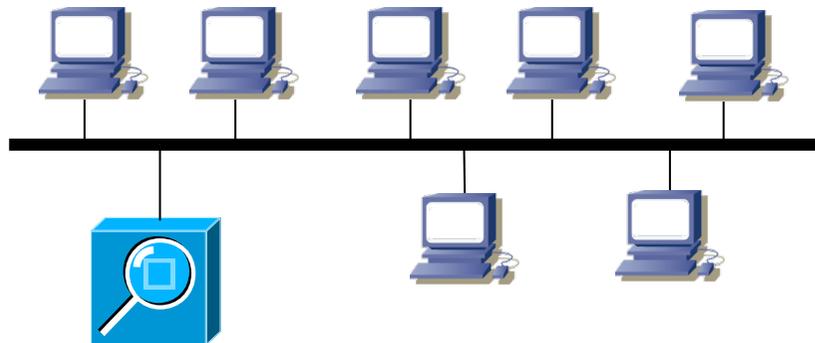
- Para las series temporales tenemos que hacer *polling*
- Solo con contadores por enlace no podemos ni tan siquiera calcular matrices de tráfico
- ¿Hay alternativas?
 - RMON
 - Medición de flujos
 - (otras...)



RMON

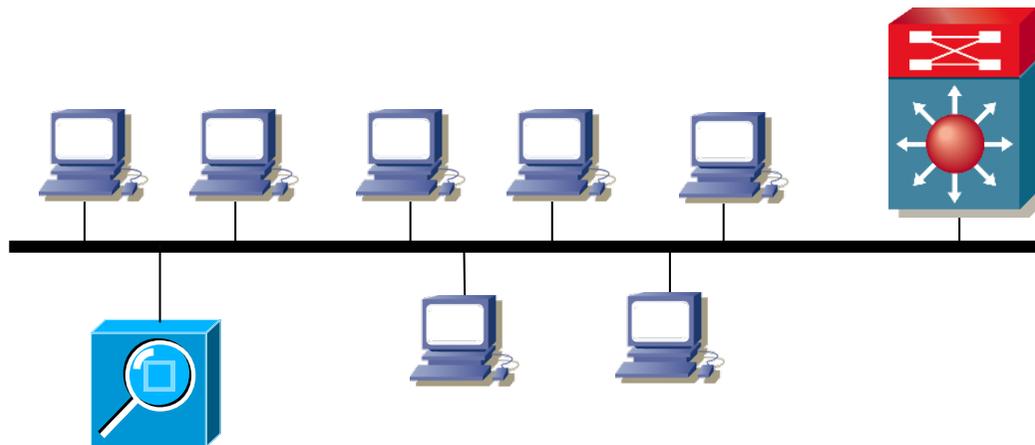
Sonda

- Equipo que inspecciona el tráfico: “sonda”, “sonda de monitorización”, “probe”, “monitoring probe”
- Dos componentes
 - Hardware unido al medio de transmisión que “ve” el tráfico
 - Proceso de análisis de los datos
- Cuando hardware y análisis están en el mismo equipo se habla de “sonda local” (“local probe”)
- Tradicionalmente los hemos llamado también “sniffers”



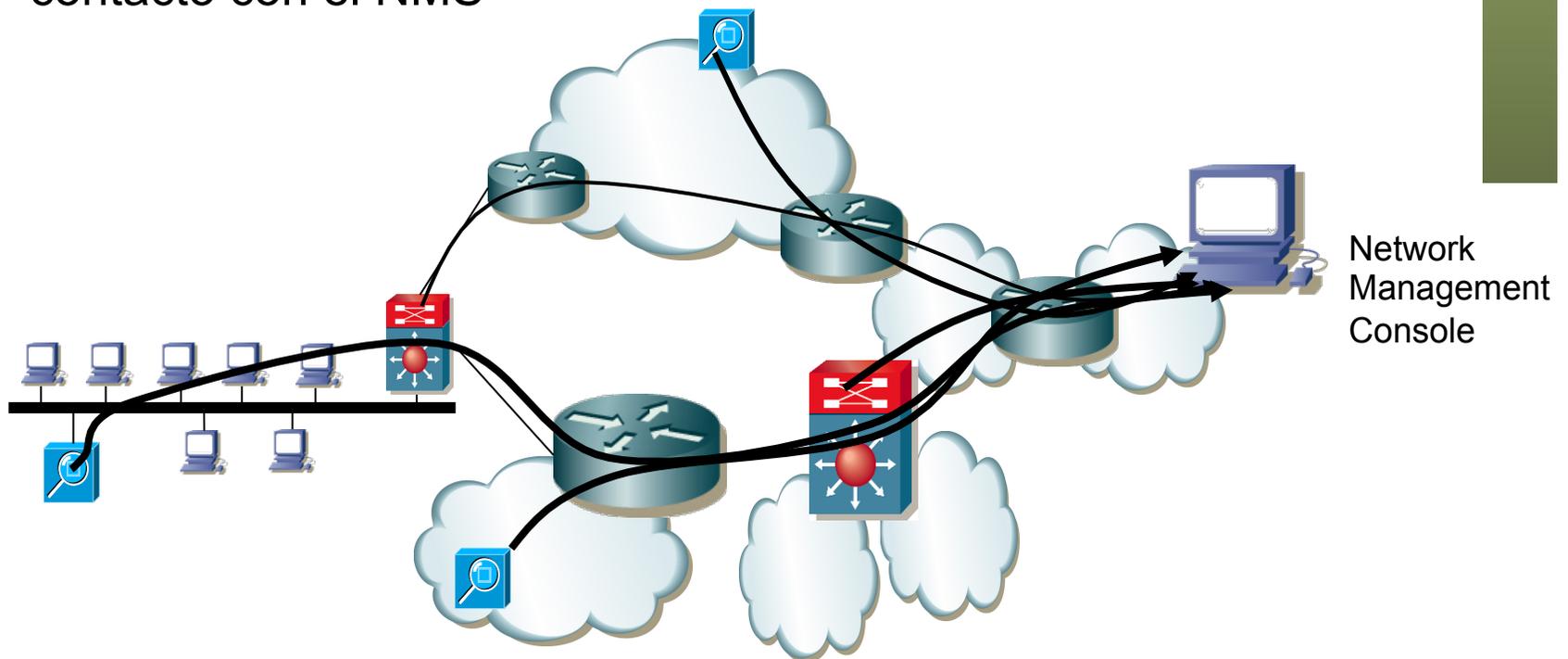
Sonda

- Puede ser un equipo específico
- O un módulo (hardware) en un conmutador (capa 2 ó 3)



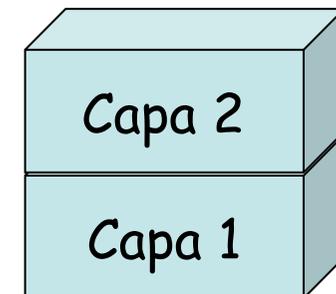
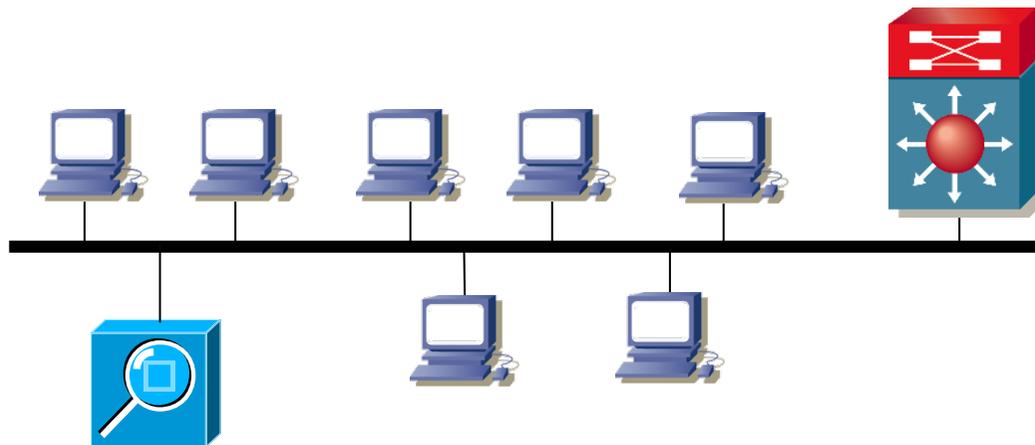
Monitorización remota

- Los resultados del análisis hecho por la sonda deben ir al NMS
- Cuando el NMS está en un lugar y la sonda en otro segmento se habla de “monitorización remota”
- “Remonte MONitoring”
- Comunicación mediante SNMP
- La sonda almacena datos así que no es crítico que pierda contacto con el NMS



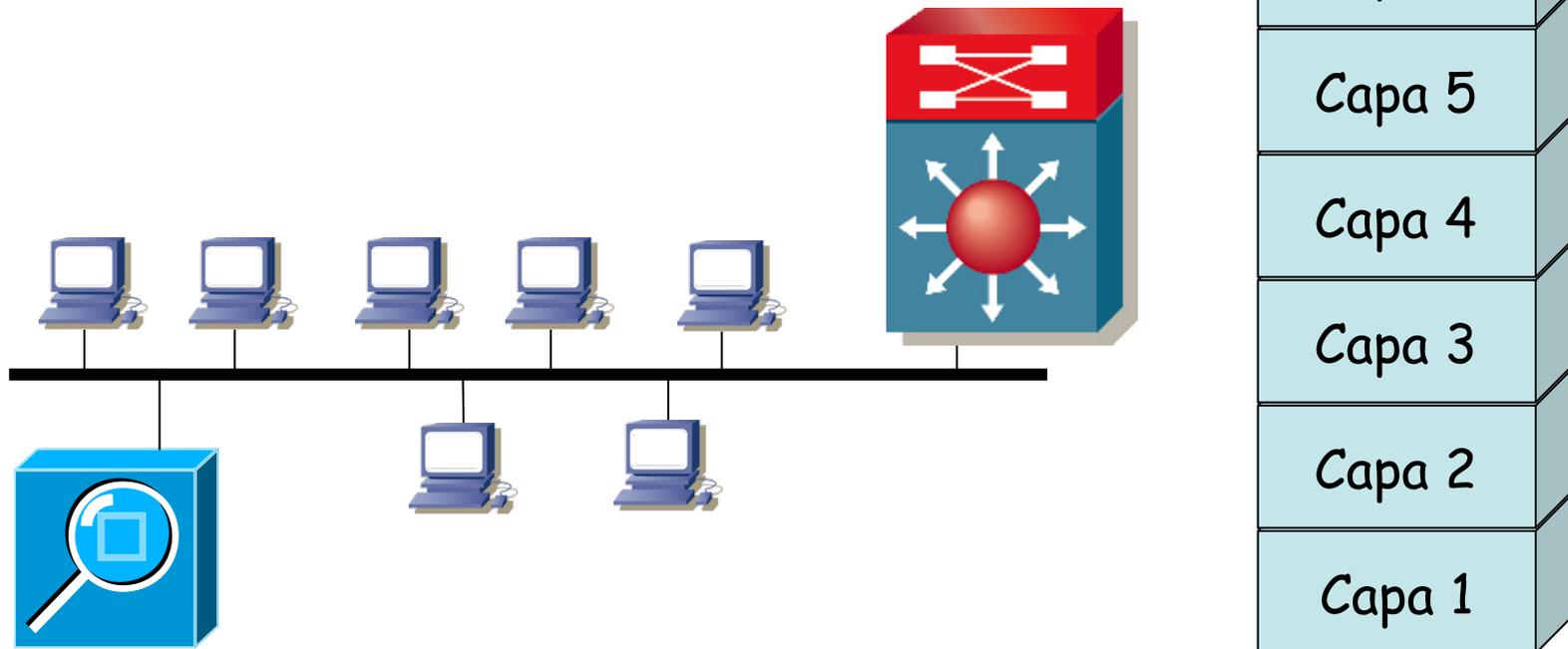
RMON

- RMON1 RFC original 1271 (año 1991) para LANs Ethernet (extendida para Token-Ring), hoy obsoleta
- Hoy en día RFC 2819
- 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 capa 2

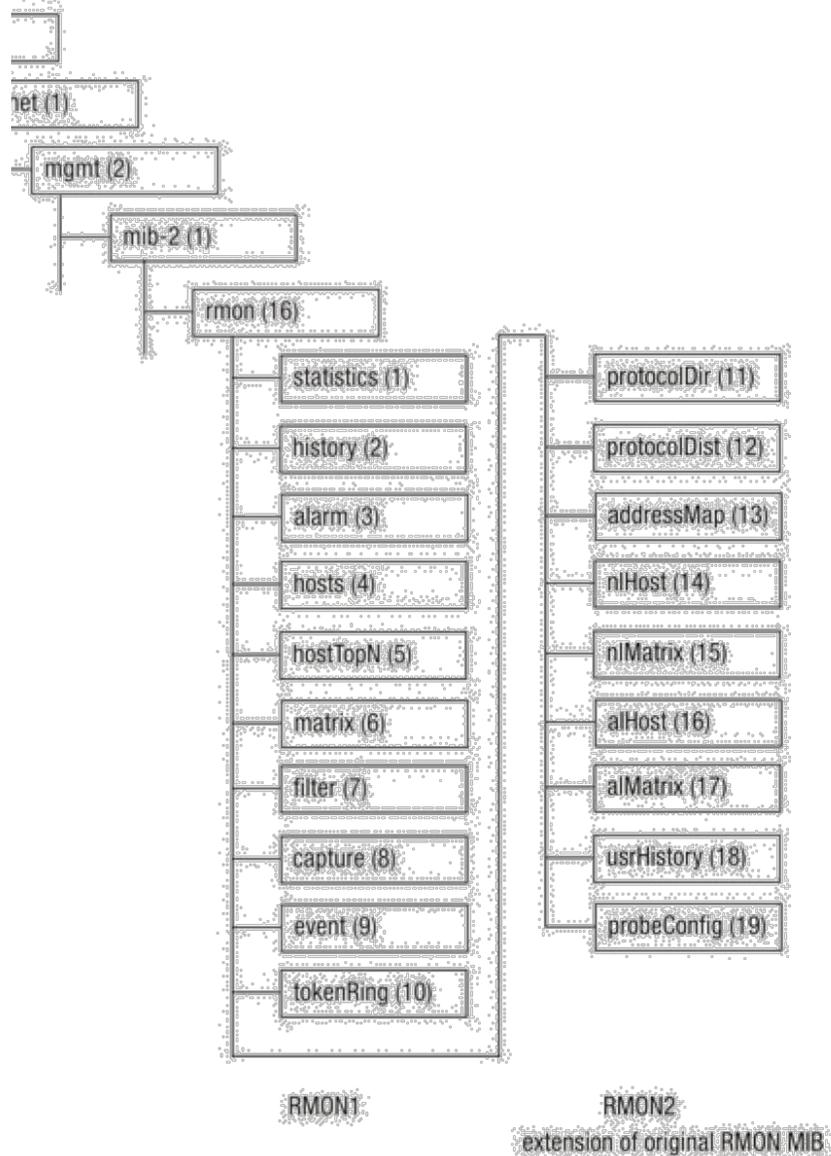


RMON2

- Año 1997 (RFC 2021)
- Hoy en día RFC 4502 “Remote Network Monitoring Management Information Base Version 2”
- Decodifica hasta capa de aplicación (sea la capa 7 OSI u otra cosa) frente a RMON1 que solo llega a capa 2
- Definido en base a SMIv2
- Define varios grupos, pero se pueden no implementar todos
- Obliga a implementar IF-MIB (RFC 2863)



MIB RMON

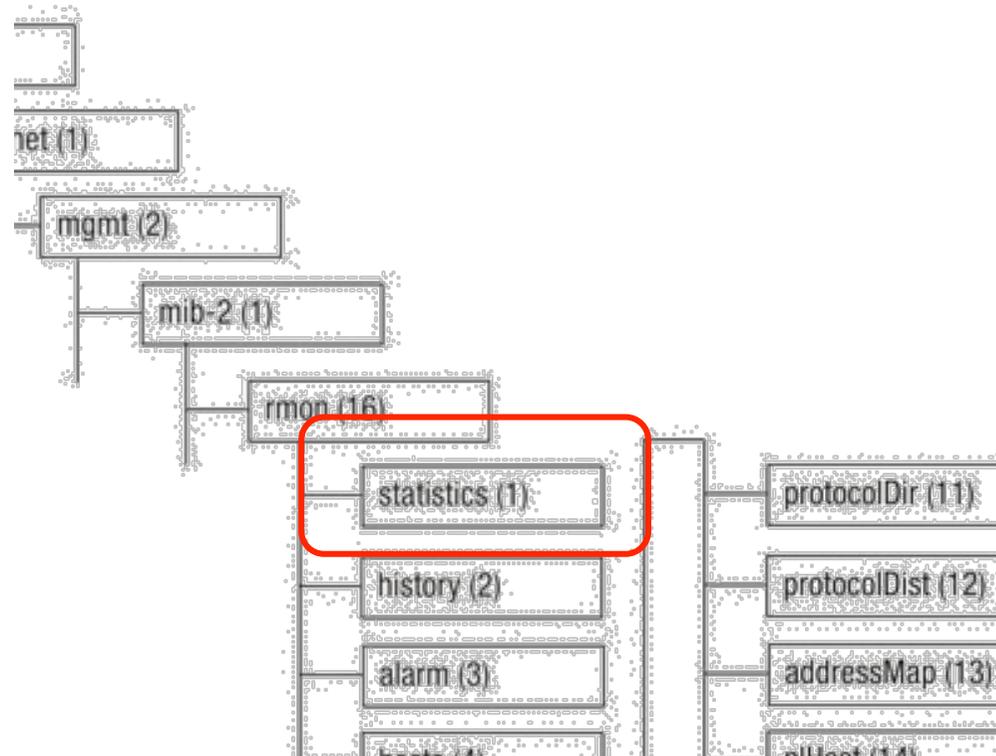


- La información se guarda mediante una MIB
- Es el grupo número 16 bajo mib2 (mib-2 16)
- 10 grupos en la MIB RMON1
- Otros 10 en la RMON2
- Tablas para indicar parámetros de control
- Y tablas donde se introducen los datos

Grupos de la MIB RMON1

Statistics (rmon 1)

- Estadísticas para cada interfaz Ethernet de la sonda
- Tipos de paquetes, tamaños, errores, colisiones
- Tablas: etherStatsTable, etherStats2Table
- Lo del “2” en la tabla es que se añadió a RMON1 durante la especificación de RMON2



Grupos de la MIB RMON1

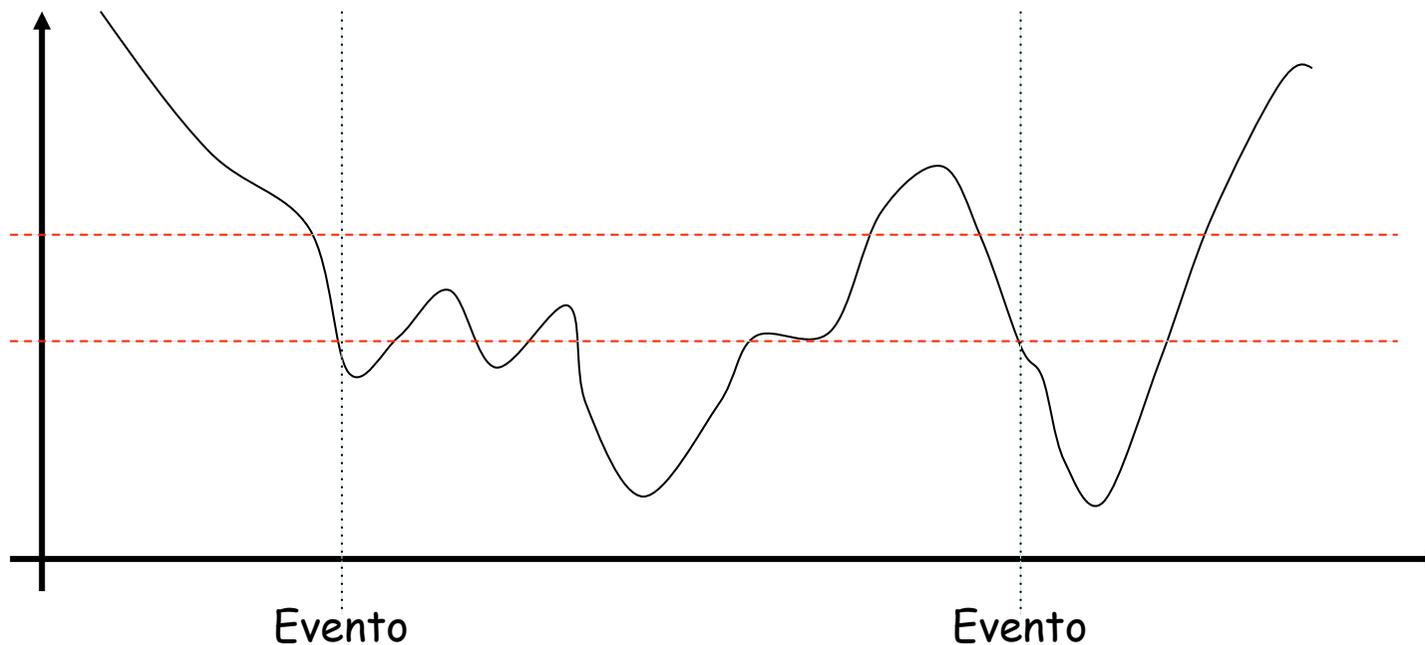
History (rmon 2)

- Permite almacenar un histórico
- Se especifica en tabla de control con qué periodicidad se recoge el dato
- Pueden ser bytes, paquetes, errores, colisiones, utilización...
- Tablas: historyControlTable, etherHistoryTable, historyControl2Table, etherHistory2Table

Grupos de la MIB RMON1

Alarm (rmon 3)

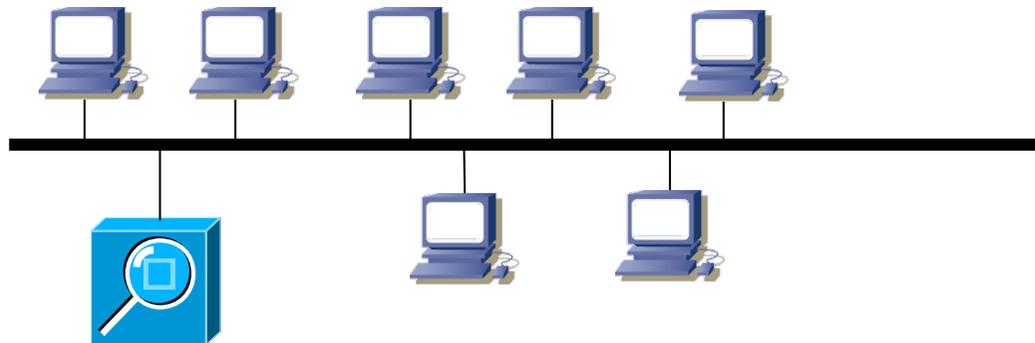
- Toma valores con periodicidad indicada y compara con unos umbrales
- Cuando se cruza el umbral se genera un “evento”
- Para no generar muchos eventos tiene que cruzar un segundo umbral antes de poder volver a cruzar el primero y generar de nuevo evento
- Tablas: alarmTable



Grupos de la MIB RMON1

Hosts (rmon 4)

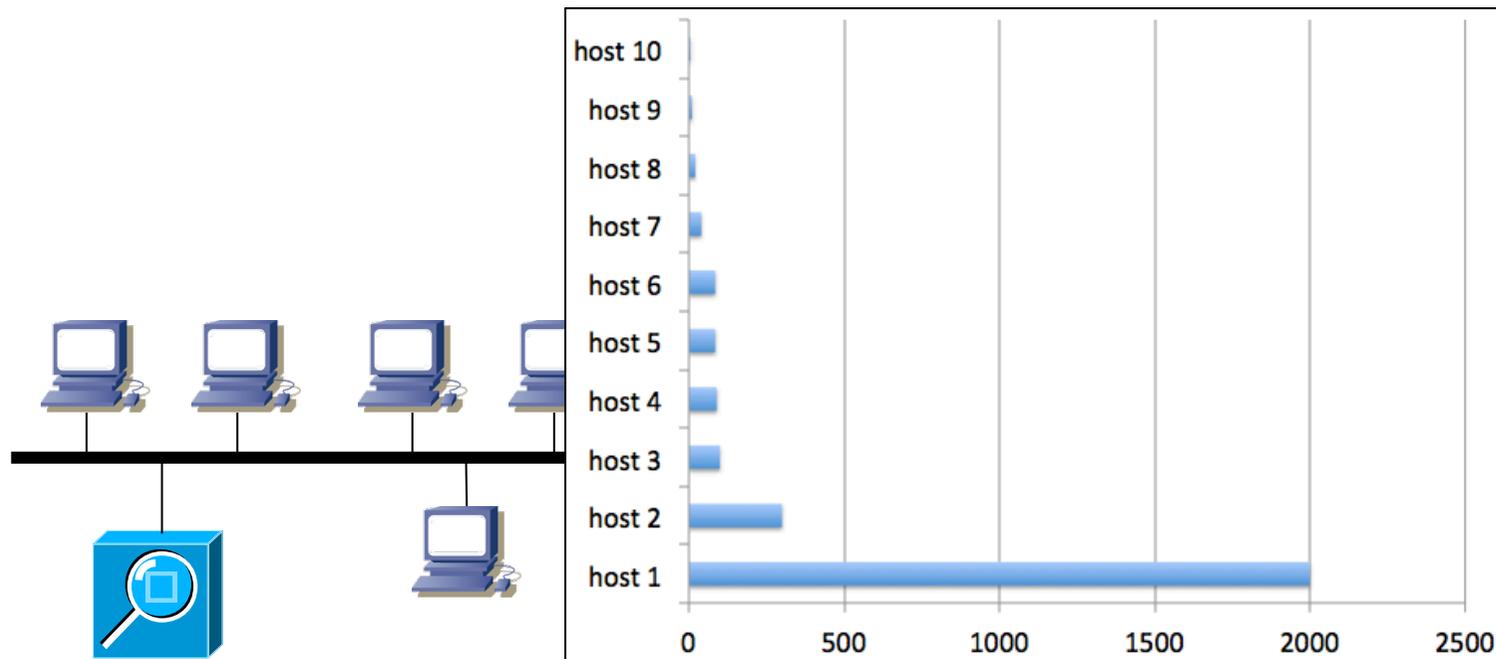
- Recopila una lista de hosts en base a las direcciones MAC en las tramas Ethernet
- Mantiene estadísticas sobre esos hosts
- Tablas: hostControlTable, hostTable, hostTimeTable, hostControl2Table



Grupos de la MIB RMON1

Hosts Top N (rmon 5)

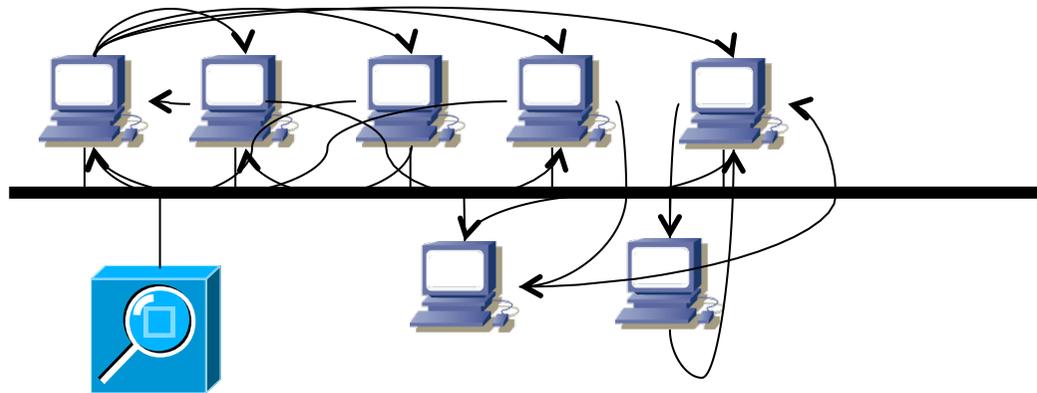
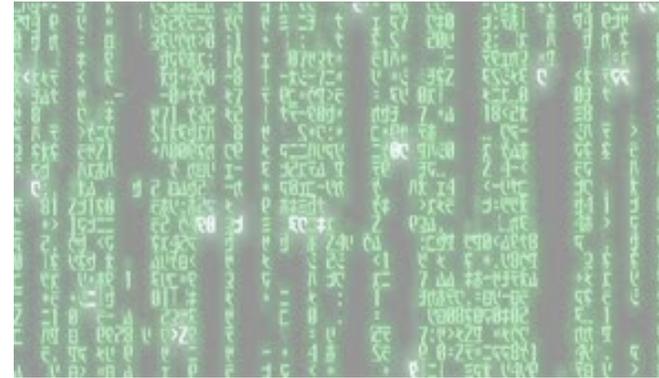
- Genera rankings de los N hosts que más acumulan de la variable especificada
- Por ejemplo podría ser de tramas enviadas
- Tablas: hostTopNControlTable



Grupos de la MIB RMON1

Matrix (rmon 6)

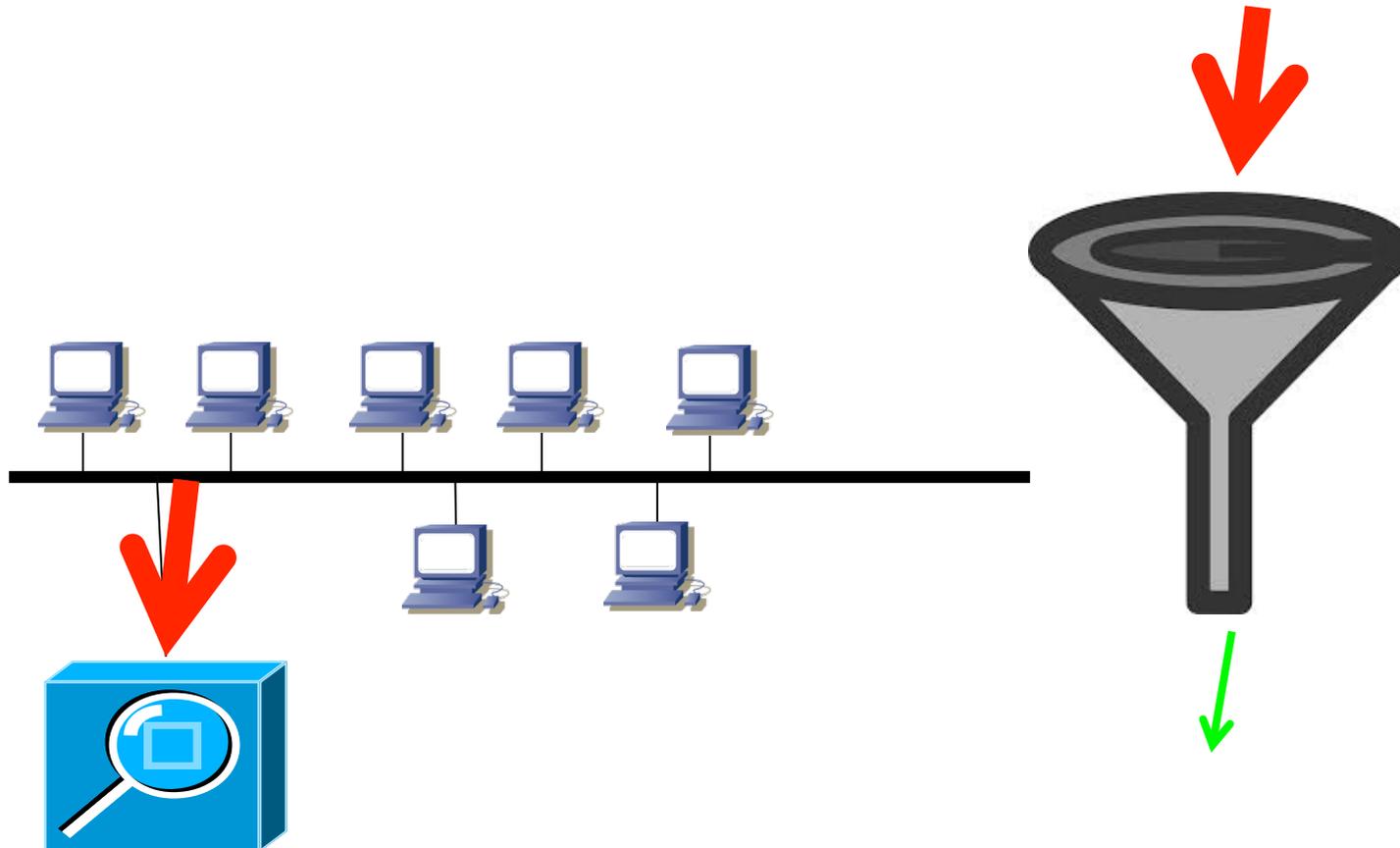
- Estadísticas de “conversaciones” entre hosts
- Una entrada por cada pareja origen-destino que detecta la sonda
- Tablas: matrixControlTable, matrixSDTable, matrixDSTable, matrixControl2Table



Grupos de la MIB RMON1

Filter (rmon 7)

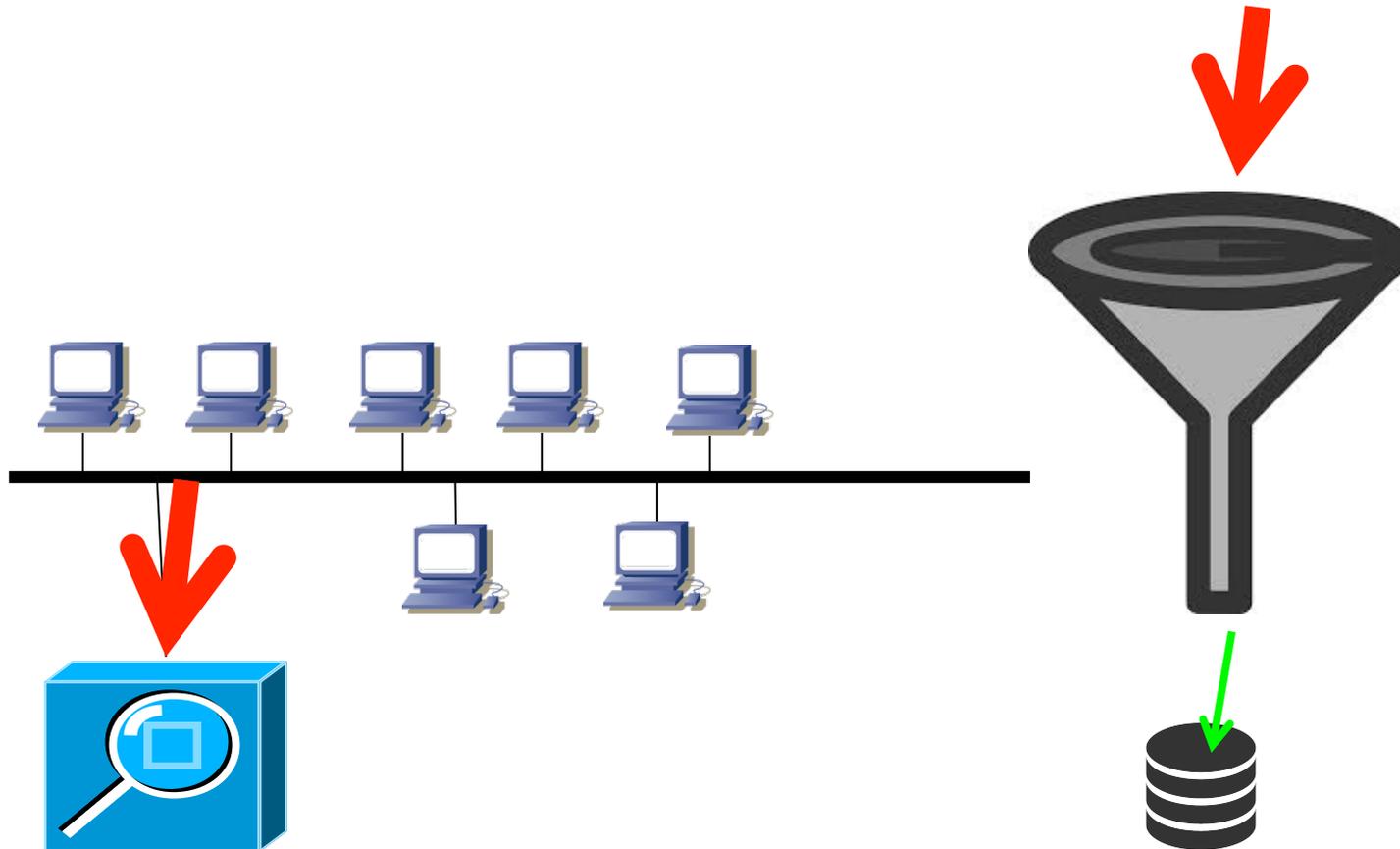
- Permite especificar filtros que se aplican a los paquetes
- De esta forma se limita lo que capturar o que puede generar eventos
- Tablas: filterTable, channelTable, filter2Table, channel2Table



Grupos de la MIB RMON1

Packet Capture (rmon 8)

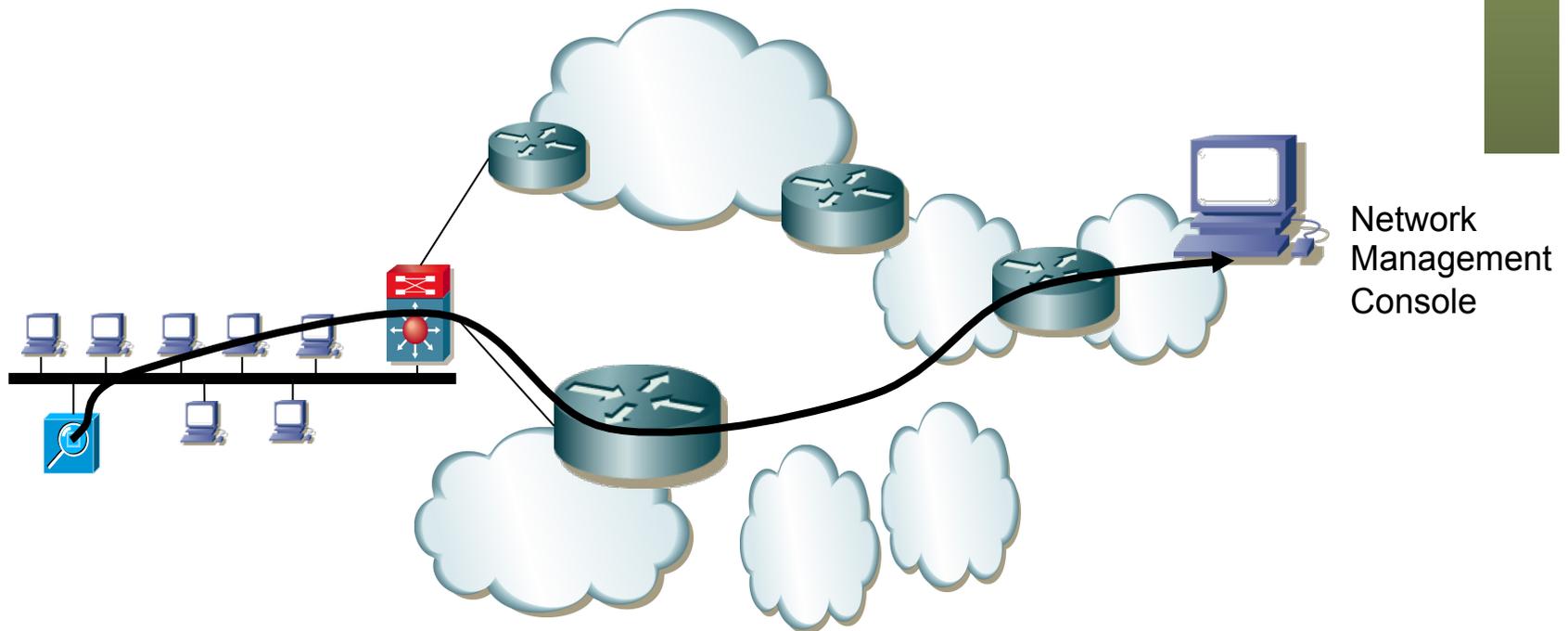
- Captura paquetes que pasan unos filtros
- Tablas: buffercontrolTable, captureBufferTable



Grupos de la MIB RMON1

Event (rmon 9)

- Controla la generación y notificación de eventos
- Puede ser recoger un log o enviar una *trap* SNMP
- Tablas: eventTable, logTable



Grupos de la MIB RMON2

Protocol Directory (rmon 11)

- Inventario de protocolos que la sonda puede monitorizar
- Se pueden añadir, borrar y configurar

Protocol Distribution (rmon 12)

- Tráfico de los distintos protocolos (paquetes y bytes)

Address Map (rmon 13)

- Asociaciones de dirección de red y dirección MAC

Network-layer Host (nlHost) (rmon 14)

- Contadores de tráfico por cada dirección de red detectada

Network-layer Matrix (nlMatrix) (rmon 15)

- Conversaciones entre pares de hosts a nivel de red
- Incluye el cálculo del top N

Application-layer Host/Matrix (alHost y alMatrix) (rmon 16 y rmon 17)

- Análogos pero a nivel de aplicación

User History (usrHistory) (rmon 18)

- Combina las funcionalidades de los grupos *history* y *alarm* de la MIB RMON1
- Es decir, muestrea periódicamente y puede enviar eventos o guardar log

Probe Configuration y RMON conformance (rmon 19 y rmon20)