Monitorización de red

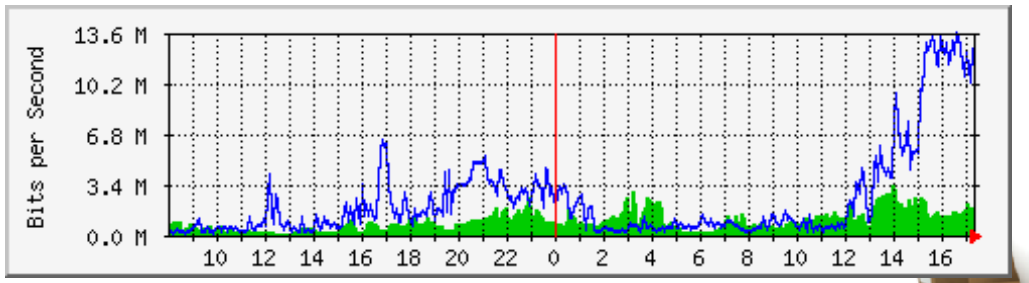
Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 4º

Ejemplo

¿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”



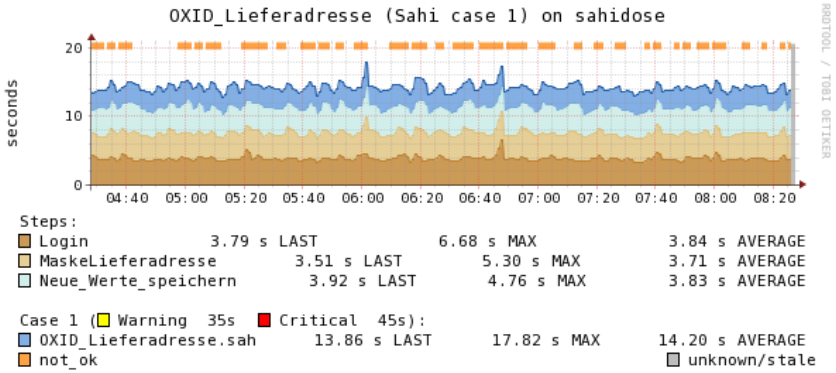
Medir

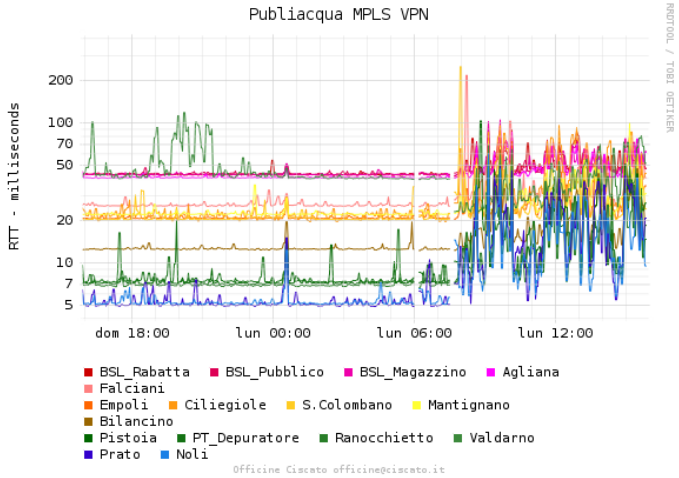
- Por un lado está la “captura” del tráfico
  - Hardware de propósito general o específico
  - Software comercial o gratuito

- Por otro lado el “análisis”
  - Software, de nuevo comercial o gratuito
  - Sobre hardware general o específico

Casos comunes: MRTG

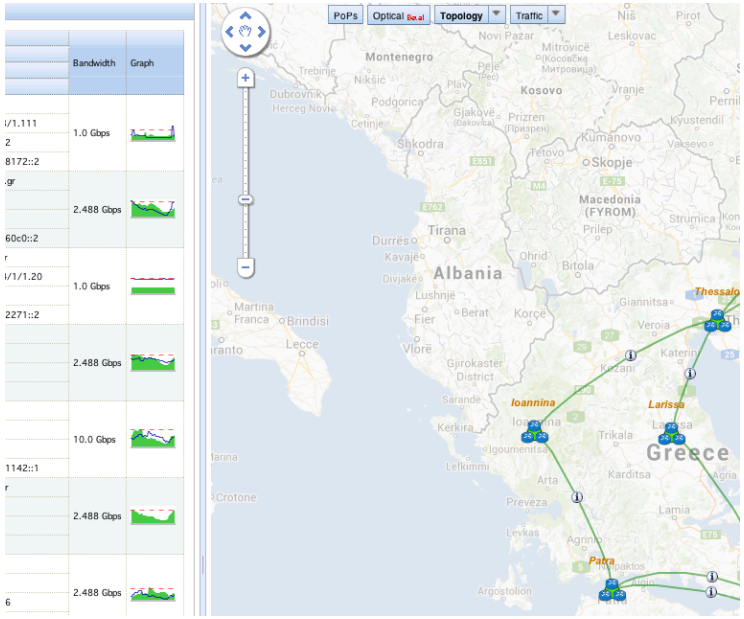
- Multi Router Traffic Grapher
- http://oss.oetiker.ch/mrtg
- Monitoriza variable SNMP
- Comúnmente es utilización de enlaces
- Crea páginas HTML con imágenes
- Consolida datos antiguos
- Free, GPL
- Puede emplear RRDtool
  - http://oss.oetiker.ch/rrdtool/
  - Mayor flexibilidad en las gráficas y mejor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

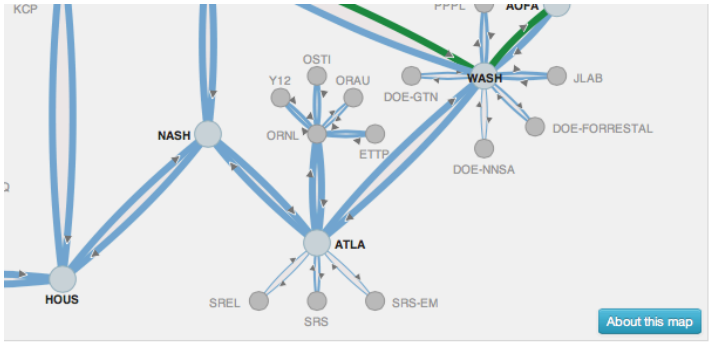


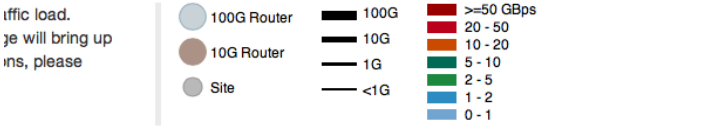


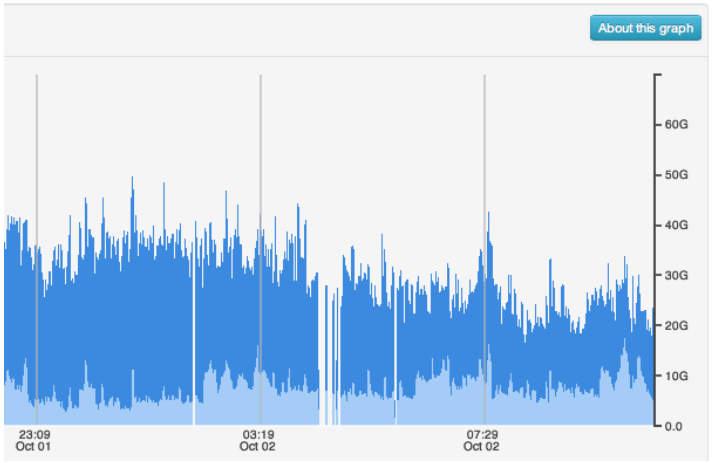
Otros ejemplos

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





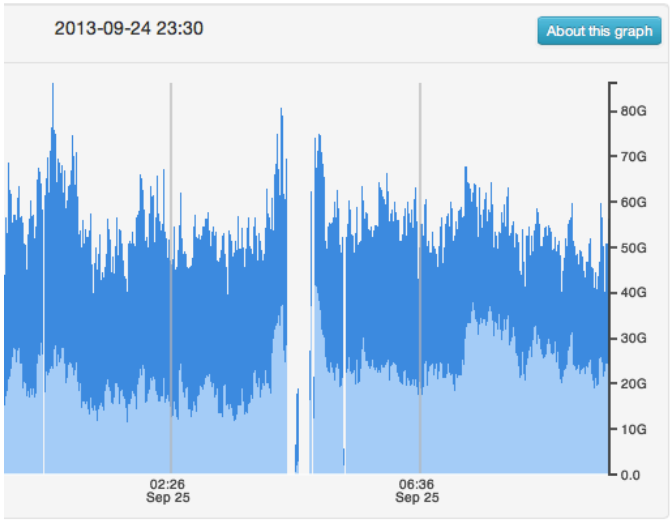




“Monitorización” de red

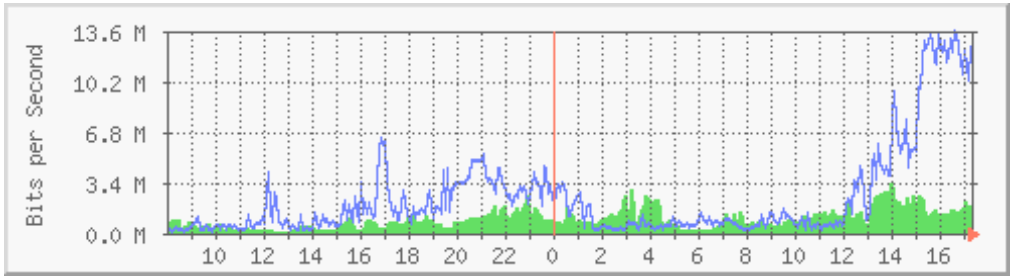
"Monitorización" de red

- 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…



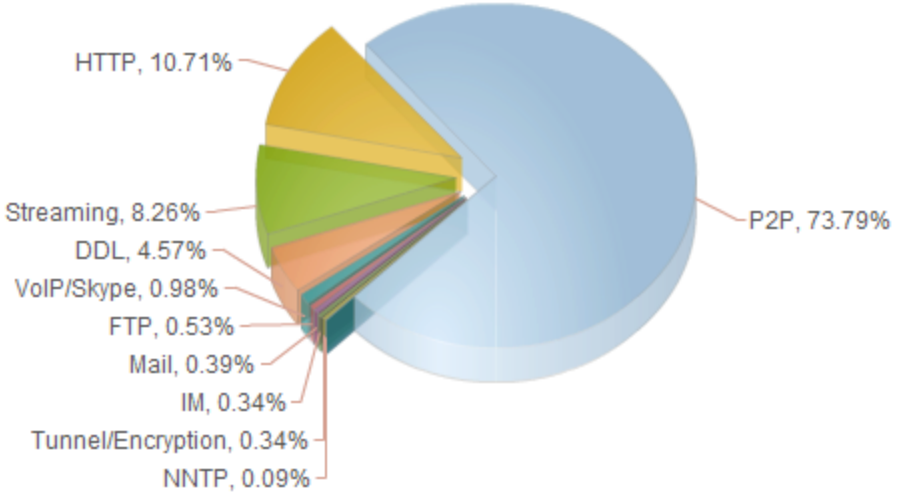
¿Para qué monitorizar?

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



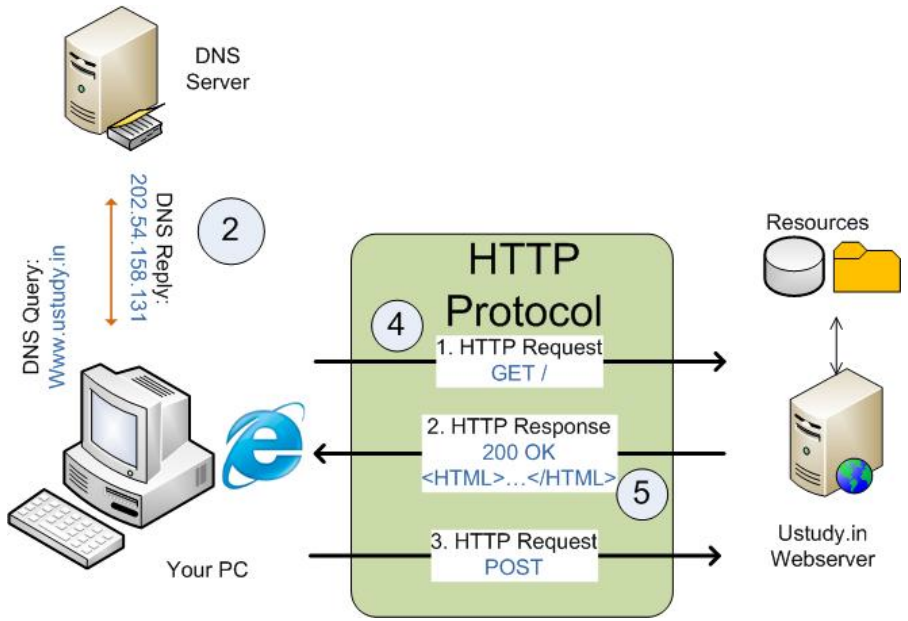
¿Para qué monitorizar?

- 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)
- (…)



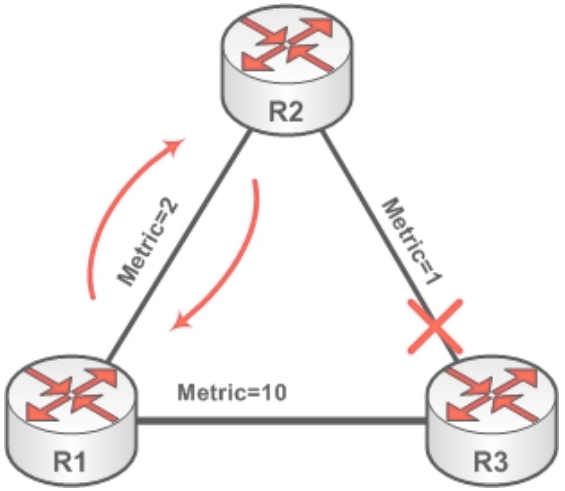
¿Para qué monitorizar?

- 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)

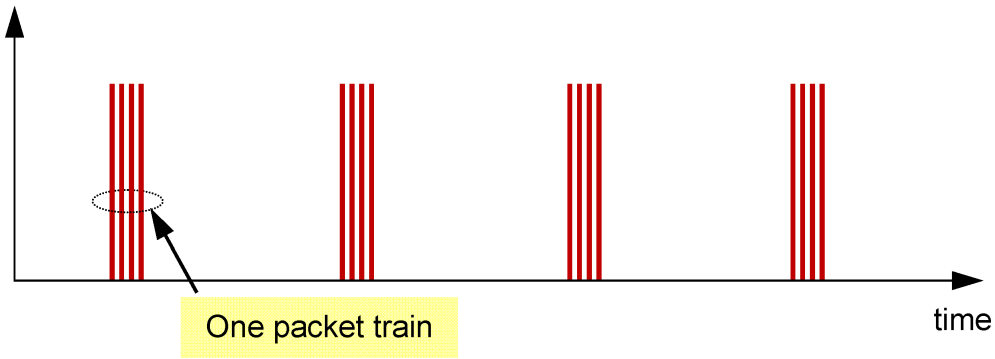
Medidas activas y pasivas

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)

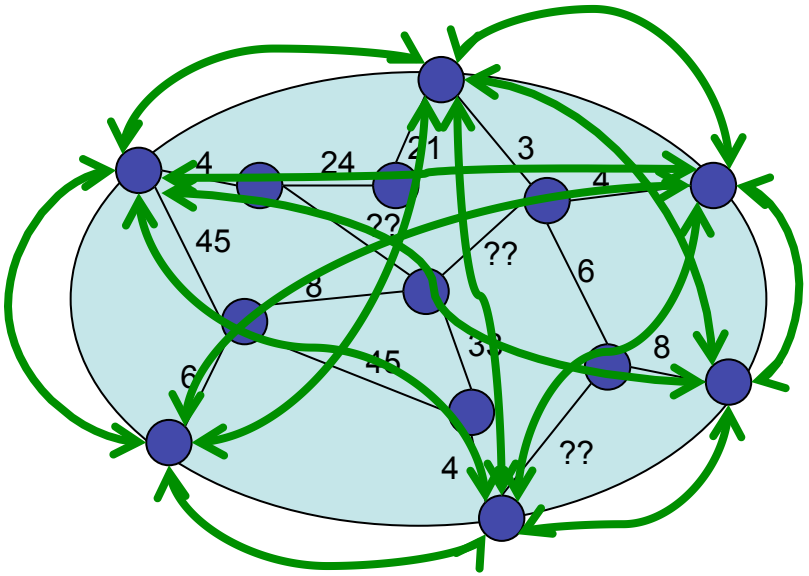


Limitaciones de SNMP

¿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? (...)

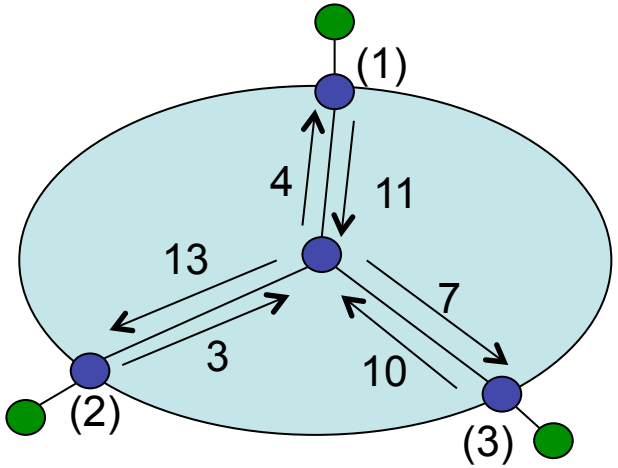
$$TM = \begin{pmatrix} 0 & I_{12} & I_{13} & I_{14} & I_{15} & I_{16} \\ I_{21} & 0 & I_{23} & I_{24} & I_{25} & I_{26} \\ I_{31} & I_{32} & 0 & I_{34} & I_{35} & I_{36} \\ I_{41} & I_{42} & I_{43} & 0 & I_{45} & I_{46} \\ I_{51} & I_{52} & I_{53} & I_{54} & 0 & I_{56} \\ I_{61} & I_{62} & I_{63} & I_{64}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



Ejemplo: matriz de tráfico

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

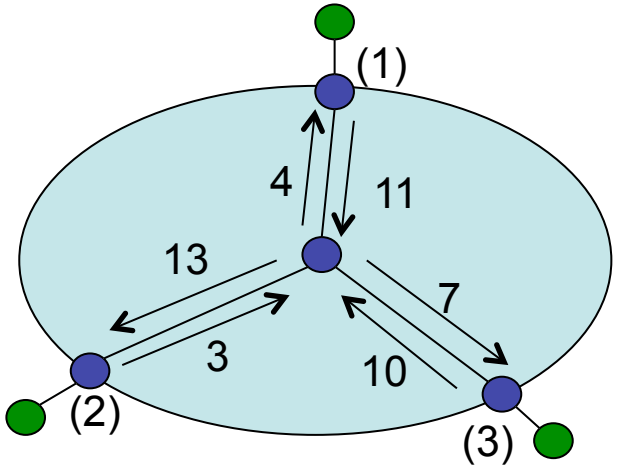
$$TM = \begin{pmatrix} 0 & I_{12} & I_{13} \\ I_{21} & 0 & I_{23} \\ I_{31} & I_{32} & 0 \end{pmatrix}$$

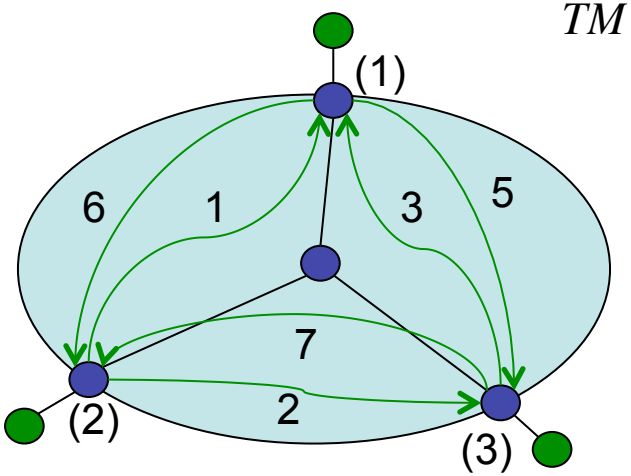


Ejemplo: matriz de tráfico

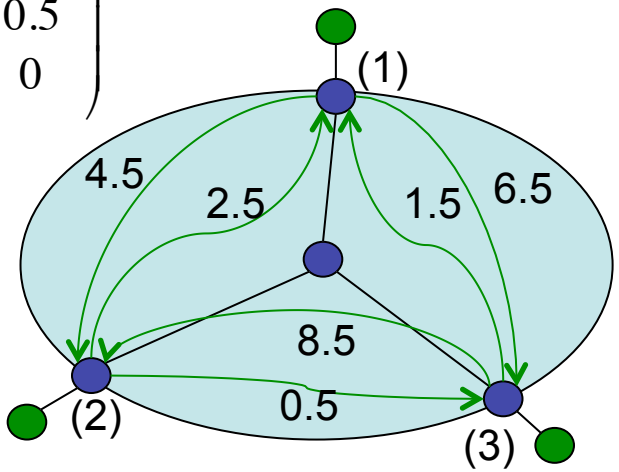
- Intensidad de tráfico para cada (origen, destino) frontera de la red
- Ejemplo:
  - Lo que sabemos con contadores
  - ¿Solución? (...)

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



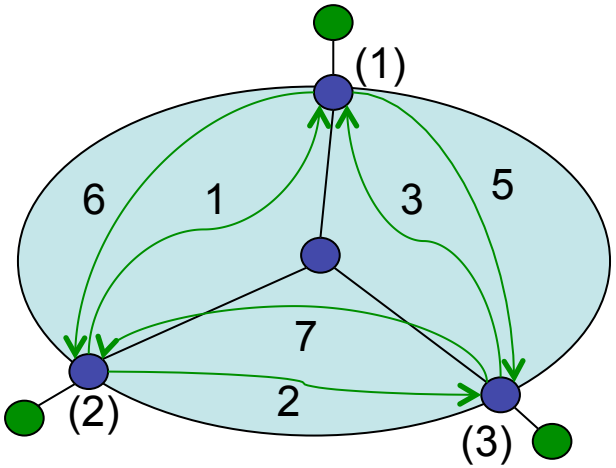


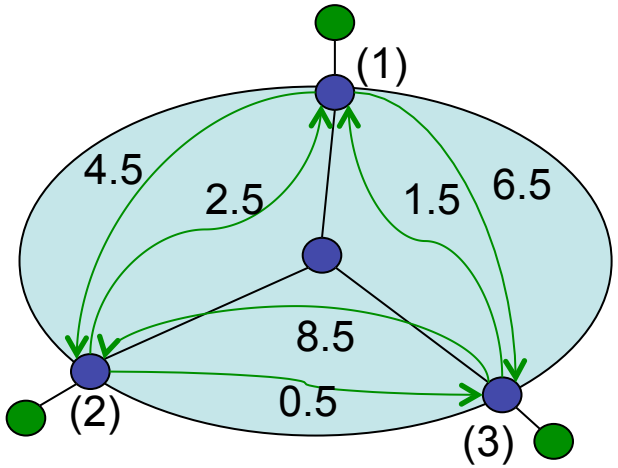
$$TM' = \begin{pmatrix} 0 & 4.5 & 6.5 \\ 4.5 & 0 & 0.5 \\ 6.5 & 8.5 & 0 \end{pmatrix}$$



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





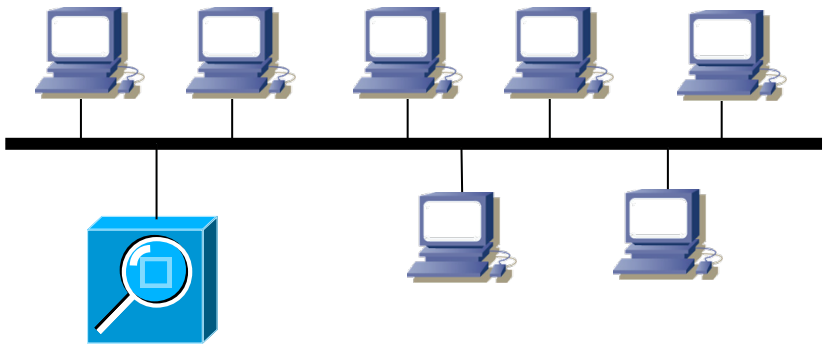
¿Nos vale con SNMP?

- 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

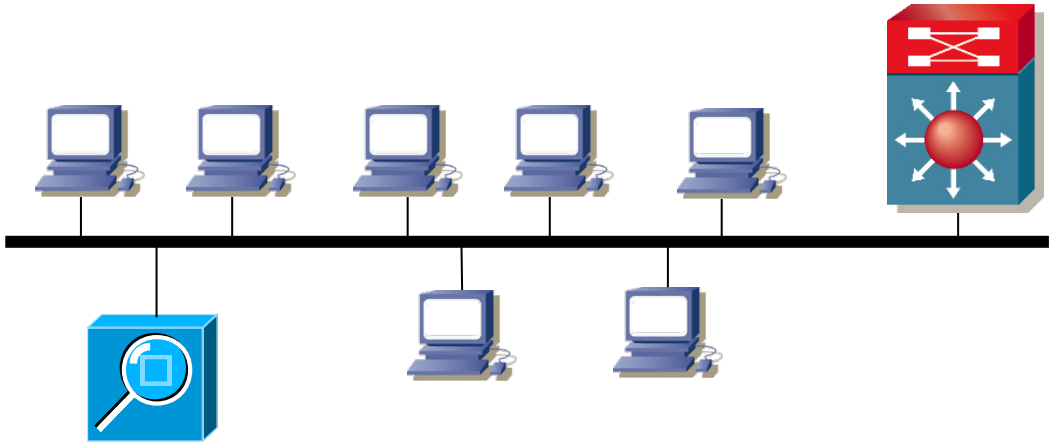
Sonda

- 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 haba de “sonda local” (“local probe”)
- Tradicionalmente los hemos llamado también “sniffers”



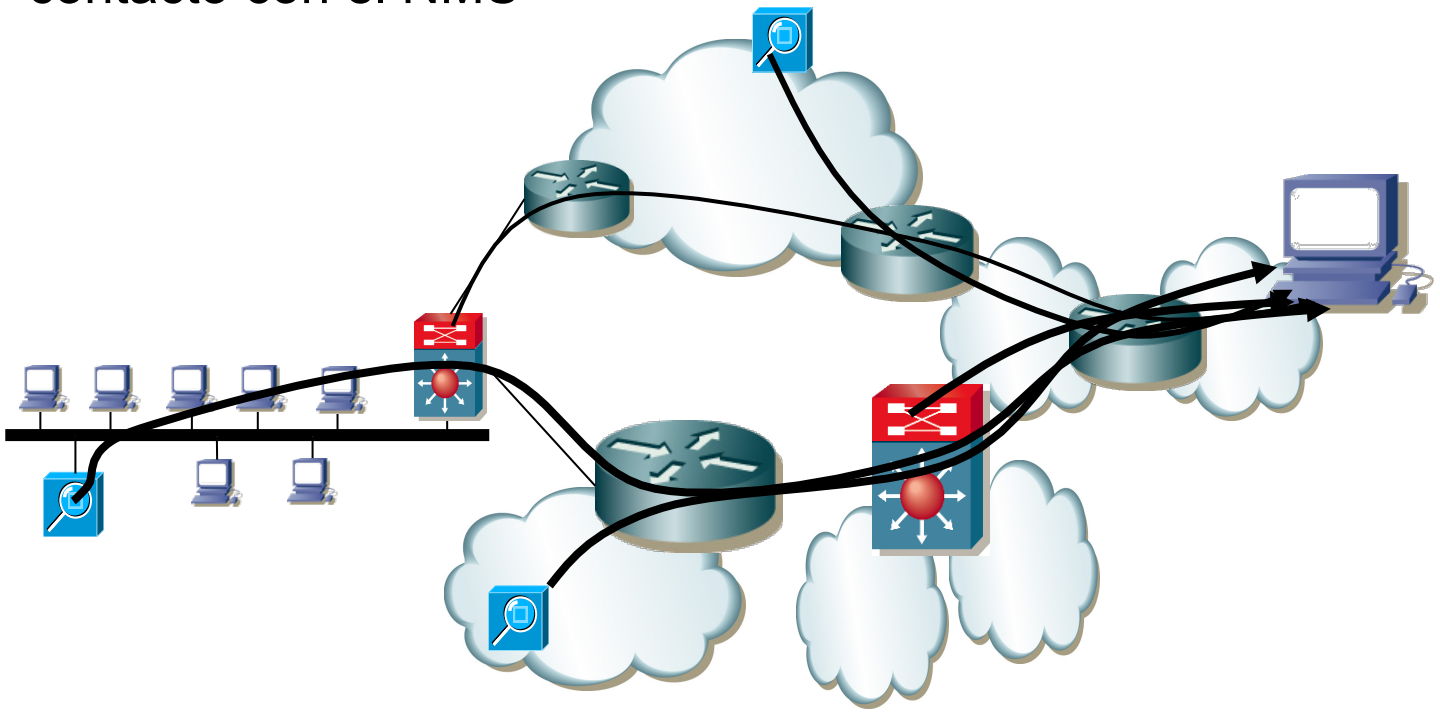
Sonda

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



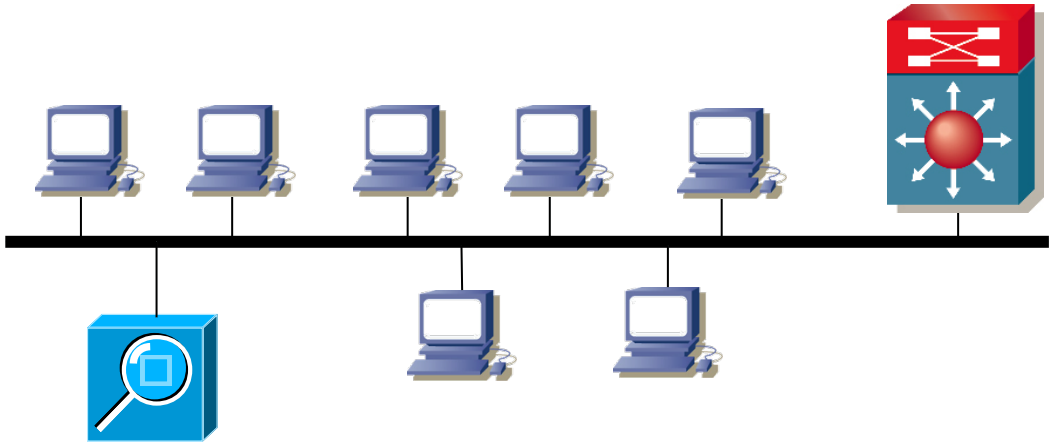
Monitorización remota

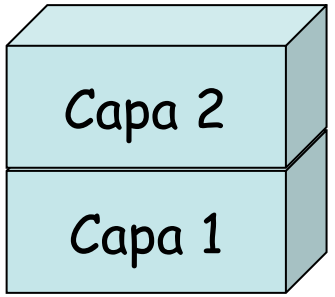
- Los resultados del análisis hecho por la sonda deben ir al NMS
- Cuando el NMS está en un lugar y la sonda en otro segmento se habla de “monitorización remota”
- “Remonte MONitoring”
- Comunicación mediante SNMP
- La sonda almacena datos así que no es crítico que pierda contacto con el NMS



RMON

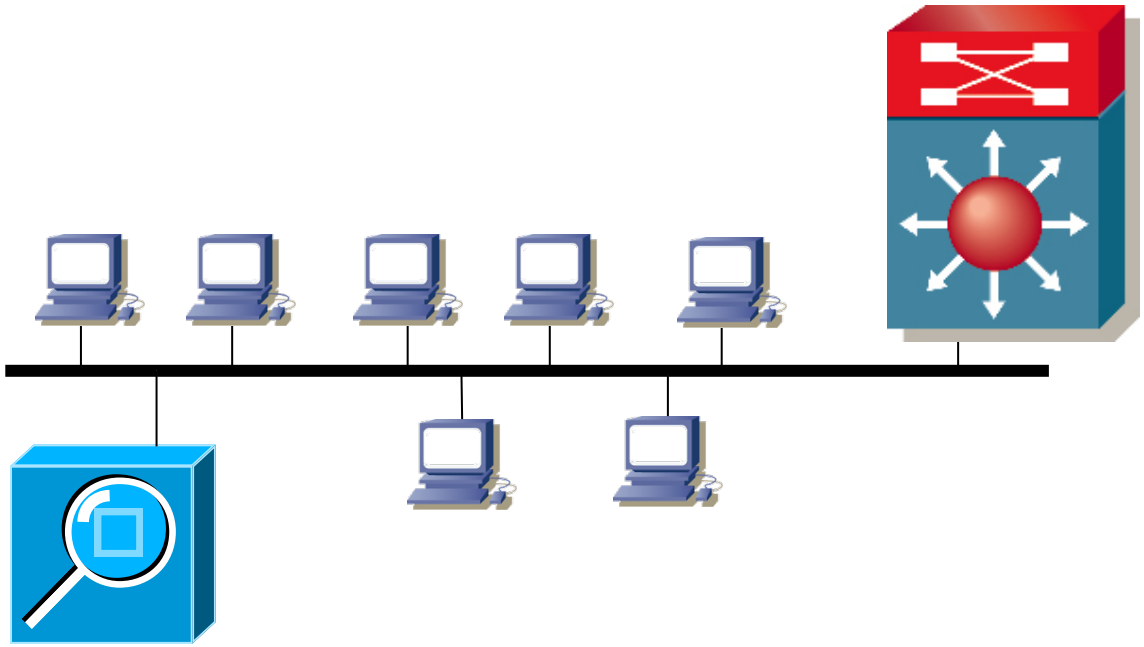
- RMON1 RFC original 1271 (año 1991) para LANs Ethernet (extendida para Token-Ring), hoy obsoleta
- Hoy en día RFC 2819
- Desarrollado para dar estadísticas de tráfico Ethernet y diagnóstico de fallos (número de paquetes, errores de CRC, colisiones...)
- Inicialmente en la época de hubs y modo promiscuo
- 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

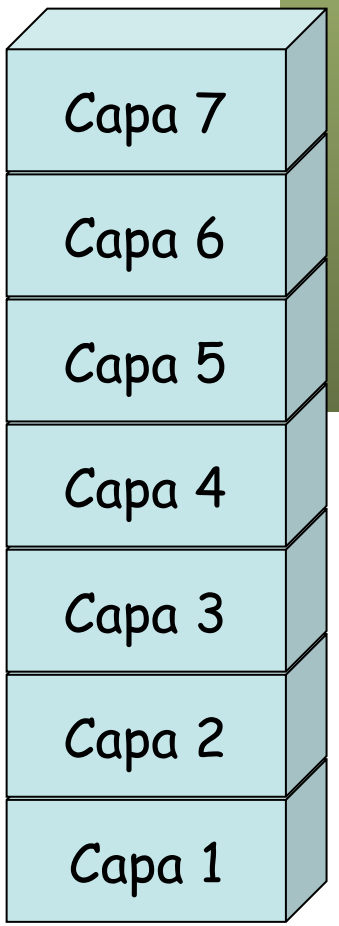




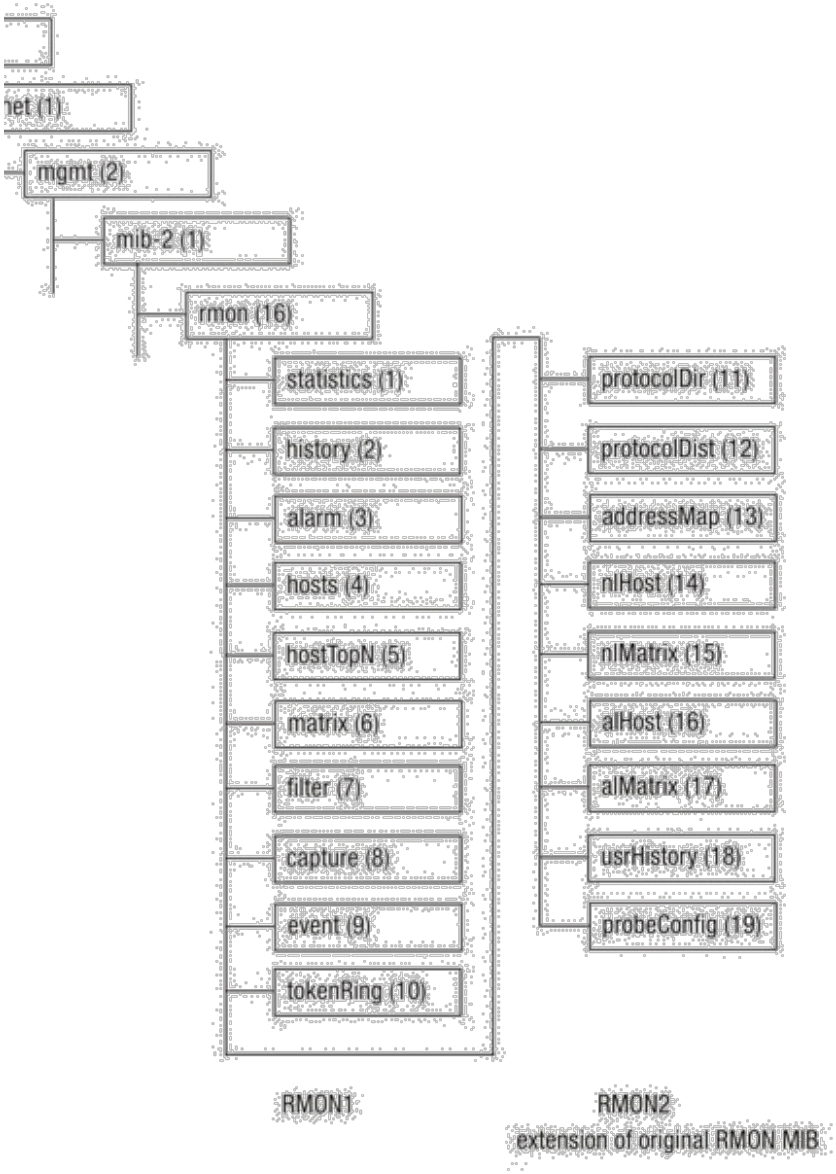
RMON2

- 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

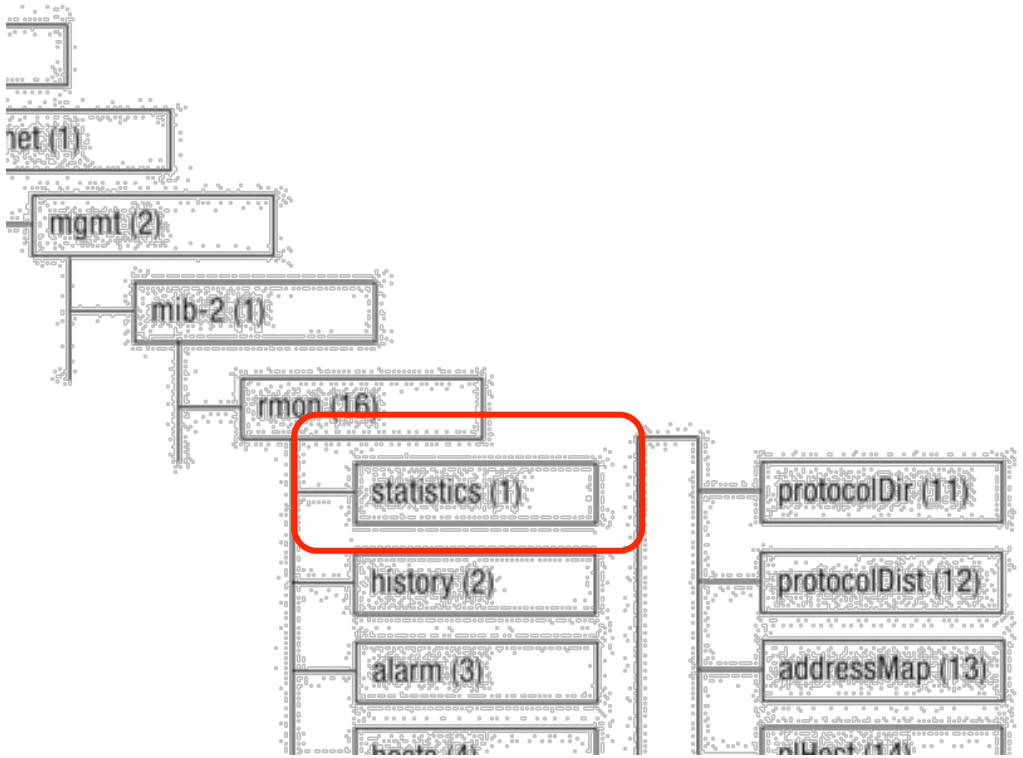


- La información se guarda mediante una MIB
- Es el grupo número 16 bajo mib2 (mib-2 16)
- 10 grupos en la MIB RMON1
- Otros 10 en la RMON2
- Tablas para indicar parámetros de control
- Y tablas donde se introducen los datos

Grupos de la MIB RMON1

Statistics (rmon 1)

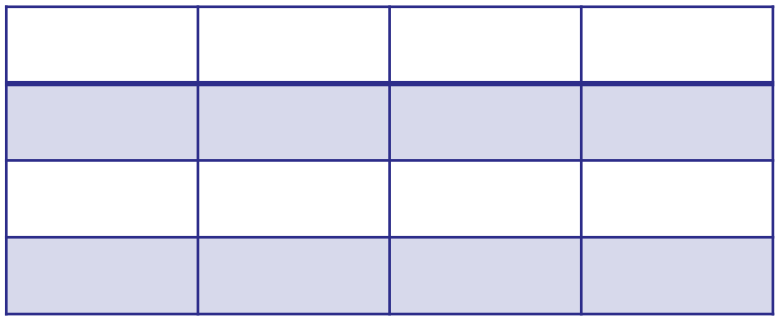
- Estadísticas para cada interfaz Ethernet de la sonda
- Tipos de paquetes, tamaños, errores, colisiones
- Tablas: etherStatsTable, etherStats2Table
- Lo del "2" en la tabla es que se añadió a RMON1 durante la especificación de RMON2



Grupos de la MIB RMON1

History (rmon 2)

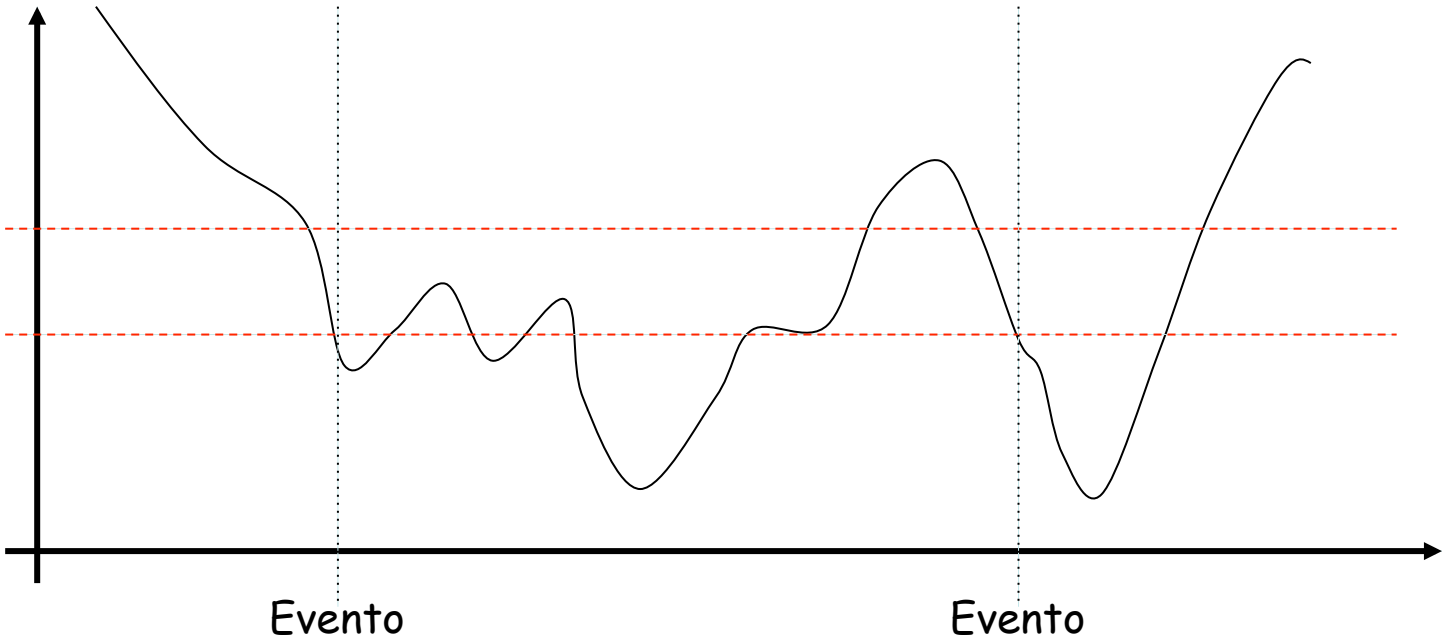
- Permite almacenar un histórico
- Se especifica en tabla de control con qué periodicidad se recoge el dato
- Pueden ser bytes, paquetes, errores, colisiones, utilización…
- Tablas: historyControlTable, etherHistoryTable, historyControl2Table, etherHistory2Table



Grupos de la MIB RMON1

Alarm (rmon 3)

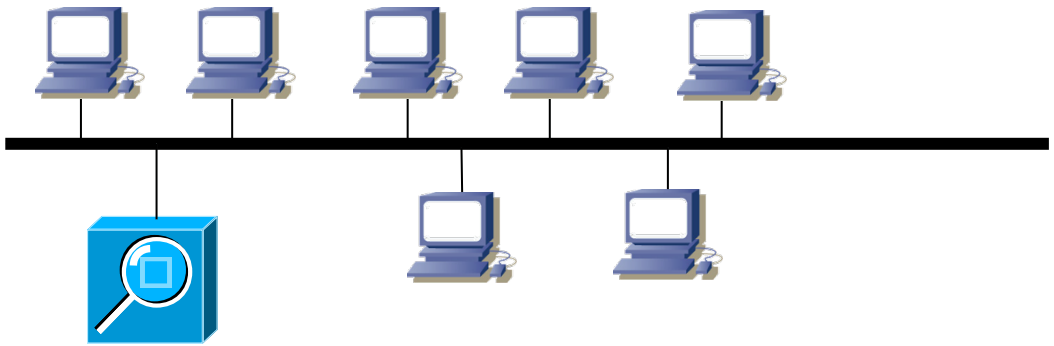
- Toma valores con periodicidad indicada y compara con unos umbrales
- Cuando se cruza el umbral se genera un "evento"
- Para no generar muchos eventos tiene que cruzar un segundo umbral antes de poder volver a cruzar el primero y generar de nuevo evento
- Tablas: alarmTable



Grupos de la MIB RMON1

Hosts (rmon 4)

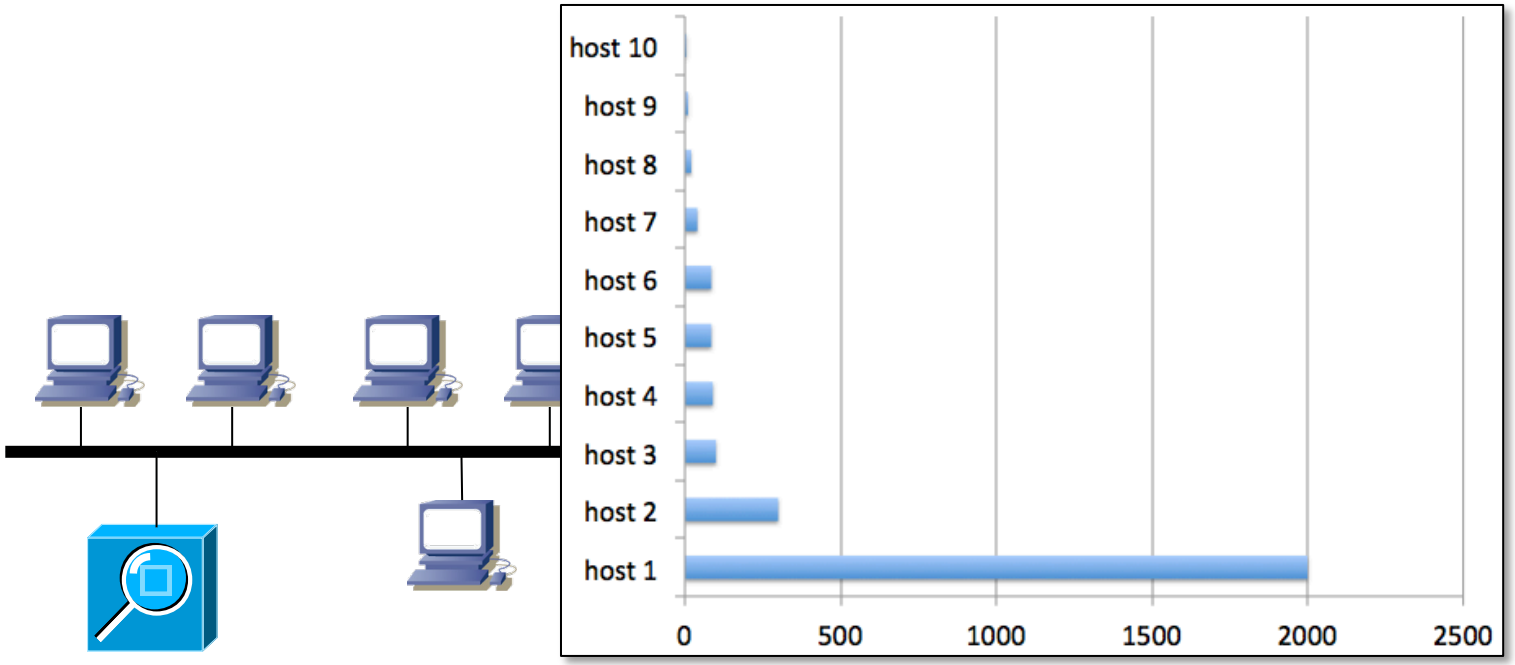
- Recopila una lista de hosts en base a las direcciones MAC en las tramas Ethernet
- Mantiene estadísticas sobre esos hosts
- Tablas: hostControlTable, hostTable, hostTimeTable, hostControl2Table



Grupos de la MIB RMON1

Hosts Top N (rmon 5)

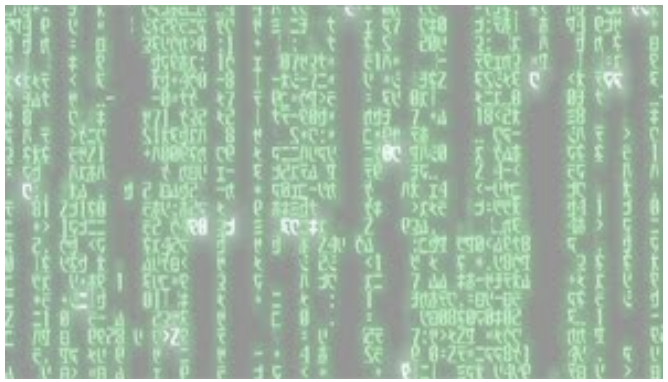
- Genera rankings de los N hosts que más acumulan de la variable especificada
- Por ejemplo podría ser de tramas enviadas
- Tablas: hostTopNControlTable

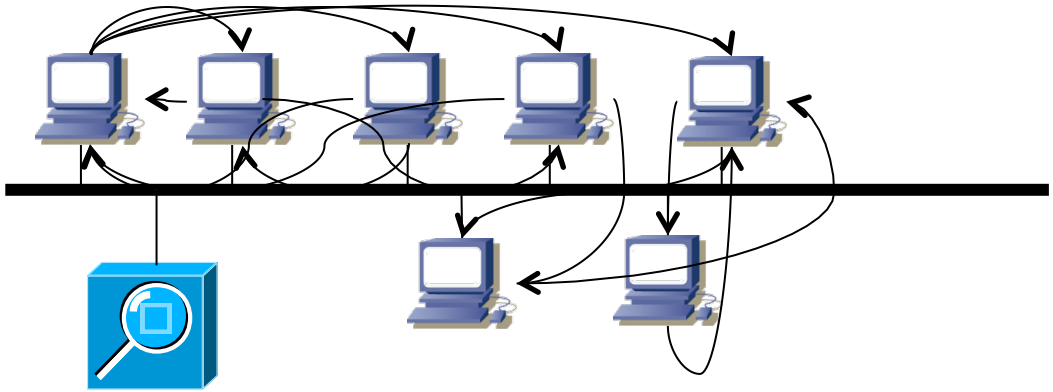


Grupos de la MIB RMON1

Matrix (rmon 6)

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

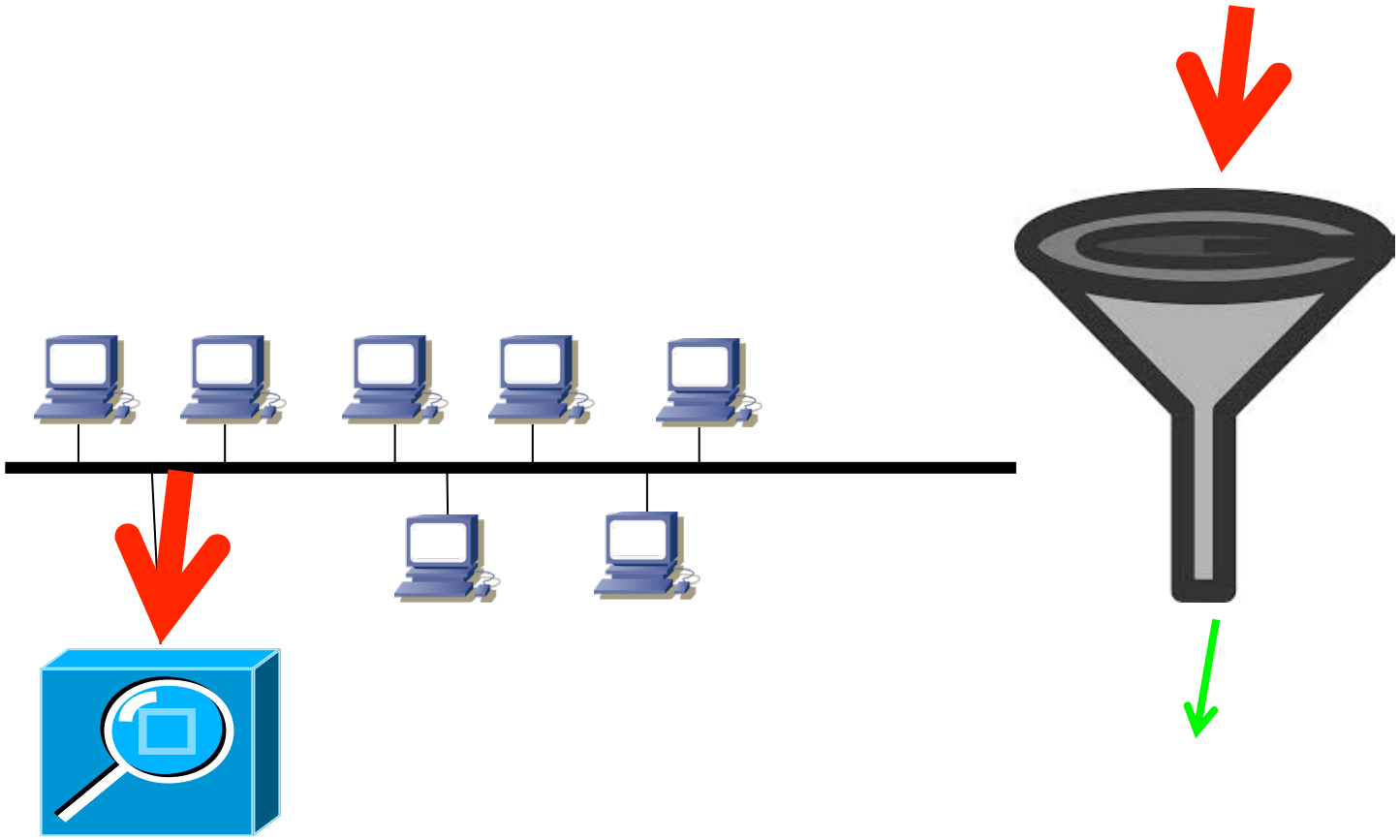




Grupos de la MIB RMON1

Filter (rmon 7)

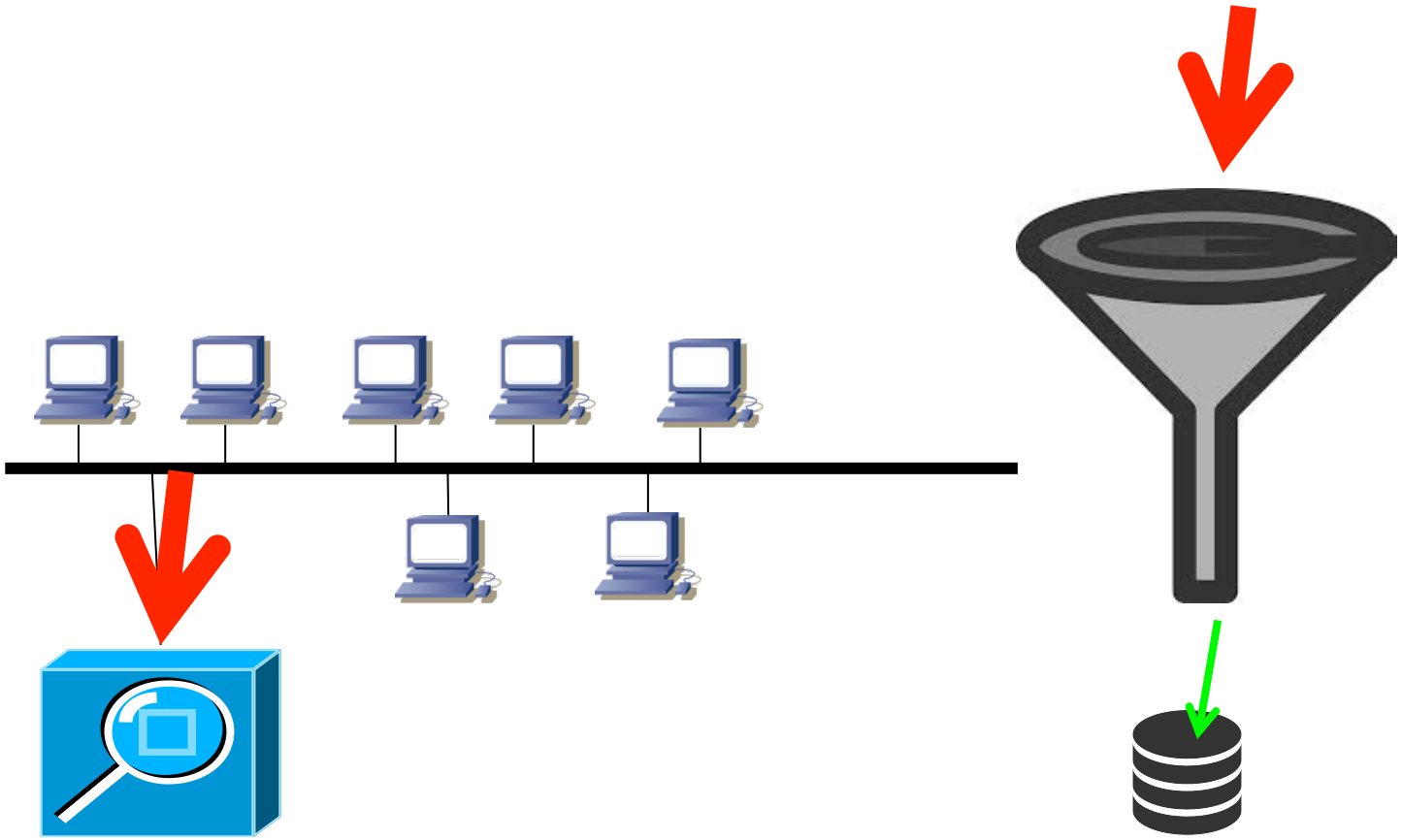
- Permite especificar filtros que se aplican a los paquetes
- De esta forma se limita lo que capturar o que puede generar eventos
- Tablas: filterTable, channelTable, filter2Table, channel2Table



Grupos de la MIB RMON1

Packet Capture (rmon 8)

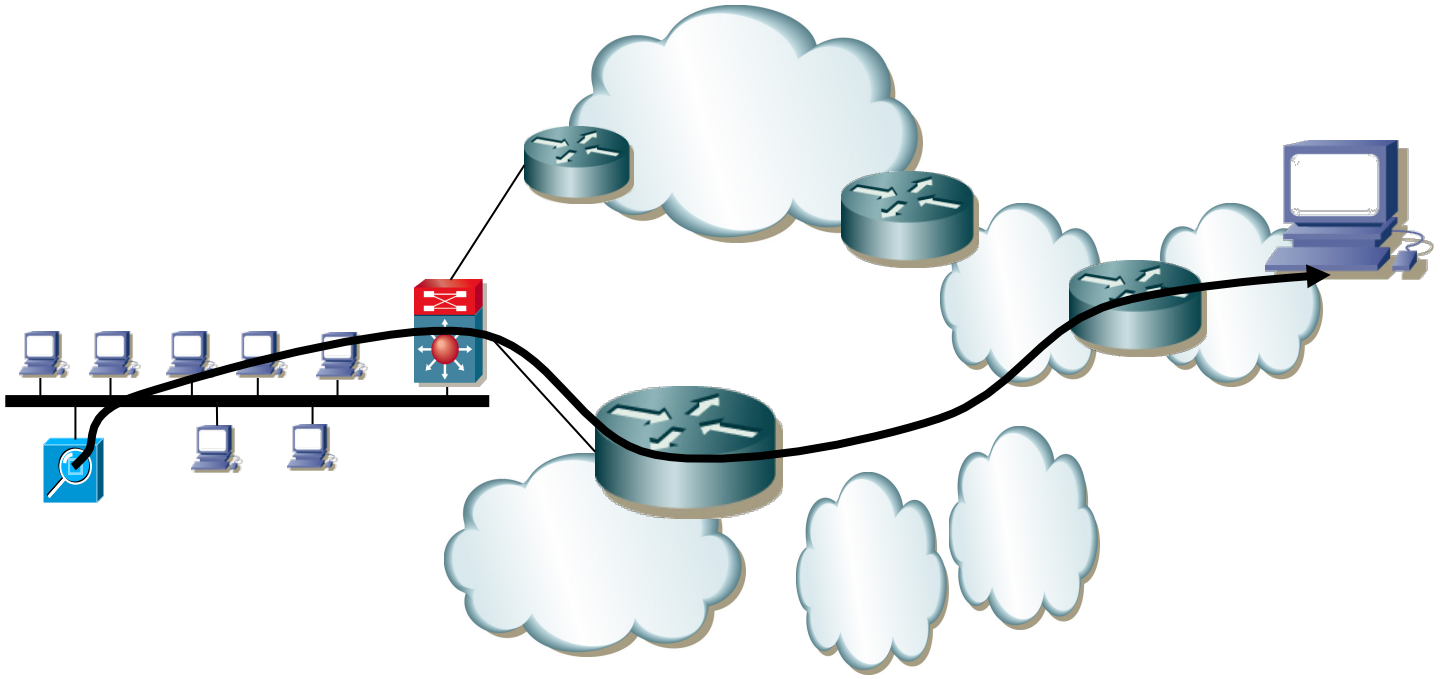
- Captura paquetes que pasan unos filtros
- Tablas: buffercontrolTable, captureBufferTable



Grupos de la MIB RMON1

Event (rmon 9)

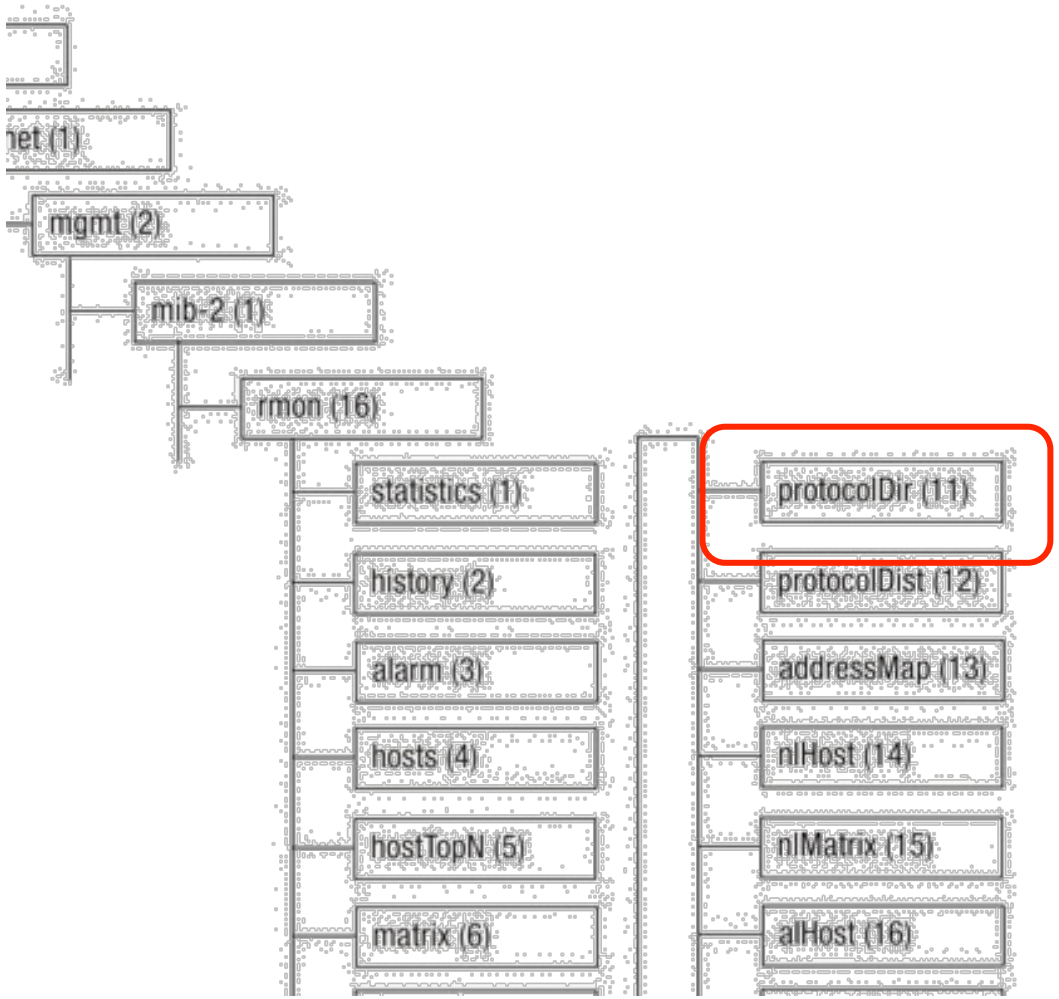
- Controla la generación y notificación de eventos
- Puede ser recoger un log o enviar una *trap* SNMP
- Tablas: eventTable, logTable



Grupos de la MIB RMON2

Protocol Directory (rmon 11)

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



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

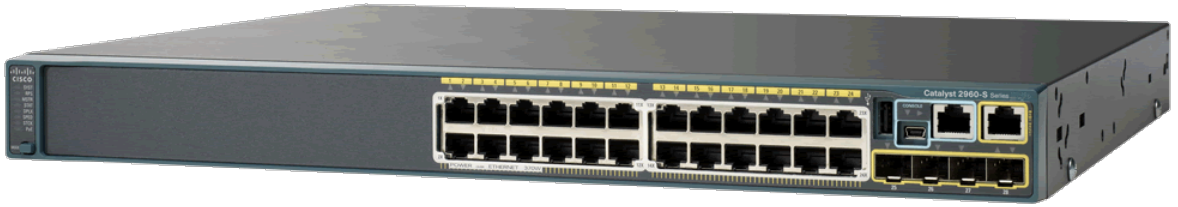
User History (usrHistory) (rmon 18)

- 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)

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).

RMON: Ejemplo (NAM-3)

Cisco Catalyst 6500 Series Network Analysis Module (NAM-3)

- El trabajo de monitorización es exigente
- Se puede llevar a cabo en módulos especializados

RMON: Ejemplo (NAM-3)

Feature	Description
NAM-3 architecture	• Two high-performance CPUs with hardware-based packet acceleration offering greater than 10 Gigabit Ethernet monitoring performance, 24 GB RAM, 600 GB SATA hard disk drive, mini SAS, and 10 Gigabit Ethernet external storage interface, and 1 Gigabit Ethernet management interface • 20 gigabit interface to backplane for Switched Port Analyzer (SPAN)/VLAN access control list (VACL) capture data sources, NetFlow, encapsulated remote SPAN (ERSPAN), and Cisco WAAS Flow Agent data sources
Supported platforms	• NAM-3 can be deployed in a slot in Cisco Catalyst 6500-E or Catalyst 6807 Switches with Supervisor Engine 2T (supported part numbers: VS-S2T-10G, VS-S2T-10G-XL) or Cisco Catalyst 6500-E Switches with Supervisor Engine 720 (supported part numbers: WS-SUP720-3B, WS-SUP720-3BXL, VS-S720-10G-3C, VS-S720-10G-3CXL) • Supported with Cisco IOS® Software 12.2(33)SXJ1(minimum) for Supervisor Engine 720 and Cisco IOS Software release 15.0(1)SY1 (minimum) for Supervisor Engine 2T
Supported topologies and data sources	• LAN: SPAN, RSPAN, ERSPAN, VACL-based captures, NetFlow (versions 5 and 9), and Cisco WAAS Flow Agent • WAN: NetFlow (versions 5 and 9) from local and remote devices, VACL-based captures for FlexWAN/Optical Service Module (OSM), and Shared Port Adapter (SPA) interfaces, and WAAS Flow Agent
Supported communication protocols	• HTTP and HTTPS with embedded web-based Cisco Prime NAM Software • Simple Network Management Protocol Version 1 (SNMPv1) and Version 2c, with standards-based applications
Cisco Prime Network Analysis Module Software	• Cisco Prime NAM Software 6.1 • Web-based: Requires Microsoft Internet Explorer 10 or later or Mozilla Firefox ESR 24 or later • Supports Secure Sockets Layer (SSL) security with up to 256-bit encryption • Role-based user authorization and authentication locally or using TACACS+ • Supported with Cisco IOS Software Release 12.2(33) SXJ1 (minimum). Refer to the Cisco Prime NAM 6.1 Release Notes for more details regarding supported system software.

RMON: Ejemplo (NAM-3)

Feature	Description
MIBs	The Cisco NAMs are standards compliant and support the following major MIB groups: • MIB-II (RFC 1213) - All groups except Exterior Gateway Protocol (EGP) and transmission • RMON (RFC 2819) - Alarm and Event groups only • RMON2 (RFC 2021) - trapDestTable only • Cisco Discovery Protocol • EntityMIB (RFC 2737)
Protocols	The Cisco Catalyst 6500 Series NAM-3 supports two protocol classification modes, DPI (NBAR2) and Classic. A list of the NBAR2 protocols supported in NAM 6.1 can be found at: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/pp710/nbar-prot-pack710.pdf. NBAR2 Protocol Packs for NAM can be found, when available, on the Cisco Prime NAM Software support site at: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/tsd-products-support-general-information.html. The DPI mode is the default mode. Cisco Prime NAM in Classic mode identifies hundreds of unique protocols (Layers 2 through 4) and automatically detects unknown protocols. It also supports URL-based application definition. Supported protocols include, but are not limited to: • TCP and User Datagram Protocol (UDP) over IP, including IPv6 • HTTP and HTTPS • Voice over IP (VoIP) including Skinny Client Control Protocol (SCCP), Real-Time Protocol/Real-Time Control Protocol (RTP/RTCP), Media Gateway Control Protocol (MGCP), and Session Initiation Protocol (SIP) • SIGTRAN protocols • Mobile IP protocols, including General Packet Radio Service (GPRS) Tunneling Protocol (GTP) • SAN protocols • Database protocols • Peer-to-peer protocols • Switch and router protocols • Cisco proprietary protocols • Unknown protocols by TCP/UDP ports and Remote Procedure Call (RPC) program numbers
Custom applications	Cisco Prime NAM supports custom applications. These applications can be defined on the basis of port, port range, server IP address, server IP address range, or HTTP URL.