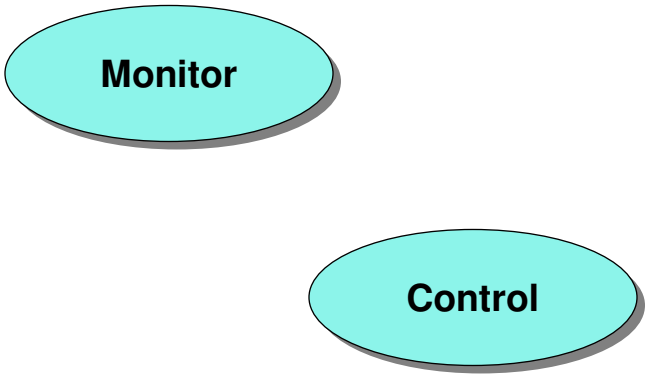
SNMP e RMON

Pietro Nicoletti
Studio Reti s.a.s
Mario Baldi
Politecnico di Torino

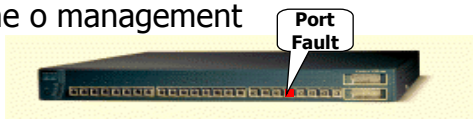
Nota di Copyright

Network Management

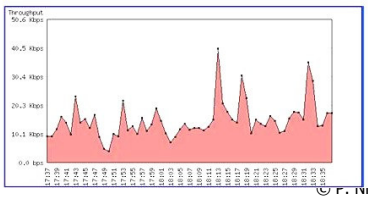


SNMP e RMON

- SNMP (Simple Network Management Protocol) è uno standard e un protocollo semplice che serve per comunicare informazioni di stato di un apparato di rete ad una stazione di gestione o management



- RMON (Remote MONitoring) è uno standard che serve a monitorare il traffico di rete, raccoglierne i dati necessari a disegnare il profilo di traffico e le sue caratteristiche, catturare i pacchetti

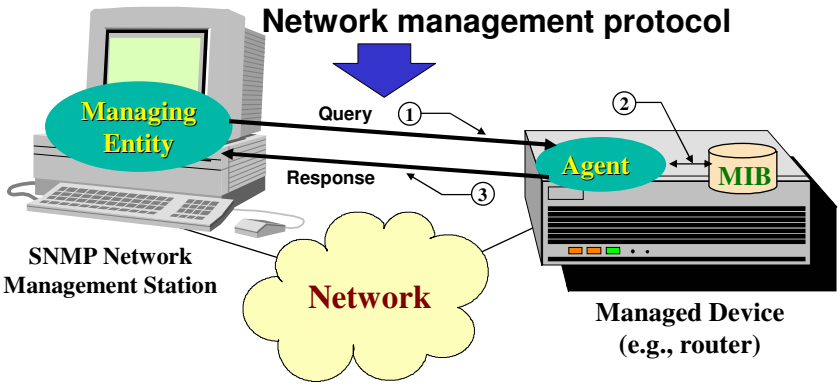


SNMP Network Management

- La gestione di rete basata su SNMP incorpora:
  - Management station
  - Agents
  - Management Information Base (MIB)
  - Network management protocol
    - Il protocollo utilizzato tra l'entità di gestione e l'apparato da gestire

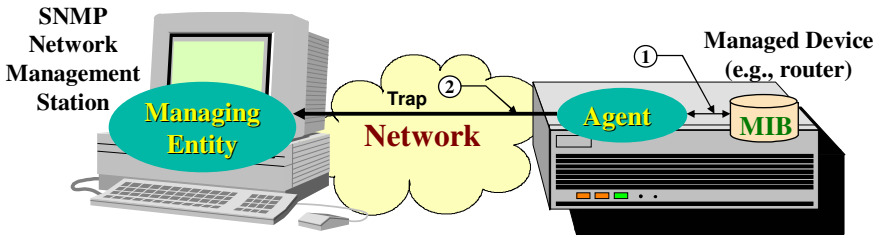
Architecture

- Client/server
- Query/Response
- Fetch/Store



SNMP

- Protocollo semplice di tipo Request-Response
- Paradigma di tipo Fetch-store
- SNMPv2: trap
  - Le notifiche sono inviate in modalità asincrona dal managed device



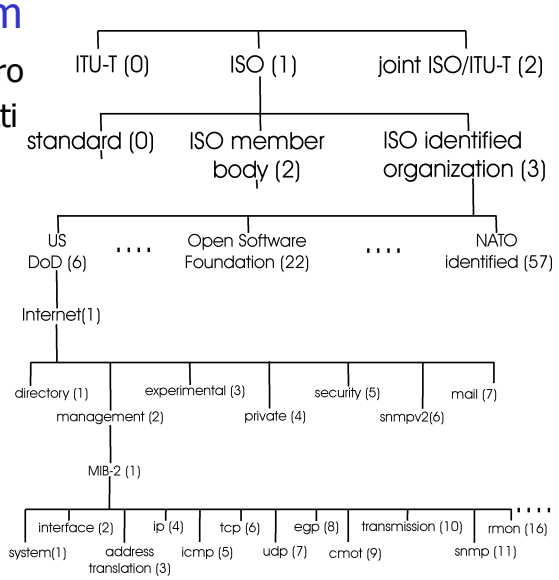
- SNMPv3 (1999): security
  - Importante dal momento che SNMP viene usato sempre più per controllare e monitorare la rete

Management Information Base (MIB)

- Variabile MIB: contiene delle informazioni specifiche dell'elemento di rete ed è divisa in gruppi denominati:
  - system, interfaces, at(address translation), ip, icmp, tcp, udp ecc
- Le informazioni contenute nella MIB possono essere interrogate e modificate dal network manager
- Mantenuta nel management agent
- Structure of Management Information (SMI)
  - Linguaggio che descrive gli oggetti MIB
    - Attributi e loro tipo
  - Basato on ASN.1
    - Abstract Syntax Notation 1
    - Standard ISO
- La definizione delle MIB non è contenuta in SNMP

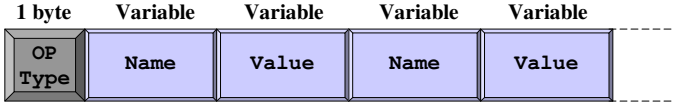
Naming System

- Struttura ad albero
- Standard a oggetti



Formato del messaggio SNMP

- OP Type
  - GetRequest (management entity → agent)
    - GetNextRequest, GetBulkRequest
  - SetRequest (management entity → agent)
  - Response (agent → management entity)
  - InformationRequest (management entities)
  - SNMPv2-Trap (agent → management entity)
- Name: 1.3.6.1.2.1.4…..
- Value: in accordo con la descrizione dell'oggetto SMI



SNMP Encapsulation

- UDP
  - Agent port 161
  - Management entity port 162: traps
- L'invio delle informazioni di management è particolarmente importante in momenti di grandi perdite di dati dovute a:
  - Congestione
  - Operazioni sbagliate

Remote Monitoring (RMON)

- Serve a controllare e misurare il traffico di rete
- Fa uso di un'estensione del MIB-2 denominata RMON MIB
- I probe Stand-Alone contengono l'agente RMON
- Presente tipicamente sugli Switch, ma non sempre in modo completo con tutti i 9 gruppi di funzioni
  - Spesso vengono implementati solo i primi 4 gruppi
- Configurabile remotamente via SNMP

I gruppi di RMON

- Statistics (gruppo 1):
  - Misura le statistiche di traffico della LAN come: utilization, bytes, packets, collisions, SMT frames, broadcasts, runts, jabbers, CRC errors
- History (gruppo 2):
  - Colleziona i campionamenti selezionati di statistiche presenti in memoria
- Alarm (gruppo 3):
  - Definisce le soglie per delle statistiche specifiche e invia una trap RMON SNMP alla stazione di gestione
- Hosts (gruppo 4):
  - Misura le statistiche specifiche degli host

I gruppi di RMON

- Hosts top N (gruppo 5):
  - Il probe osserva tutte le conversazioni e fornisce le informazioni riguardanti gli host ordinate per entità di traffico
- Traffic Matrix (gruppo 6):
  - Memorizza le statistiche per coppie di indirizzi (stazioni)
- Filter (gruppo 7):
  - Definisce dei filtri per pacchetti da utilizzare in cattura o per generare degli eventi
- Packet Capture (gruppo 8):
  - Funzione di cattura dei pacchetti
- Event Group (gruppo 9):
  - Controlla la generazione e la notifica degli eventi