Università di Firenze
Dipartimento di **E**lettronica e **T**elecomunicazioni

La gestione di rete basata su SNMP

Ing. **Tommaso Pecorella**

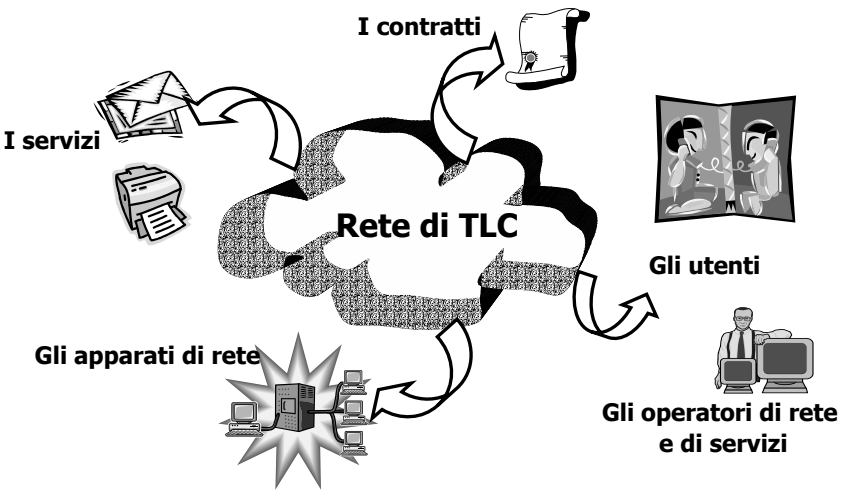
Ing. **Giada Mennuti**

{pecos,giada}@lenst.det.unifi.it

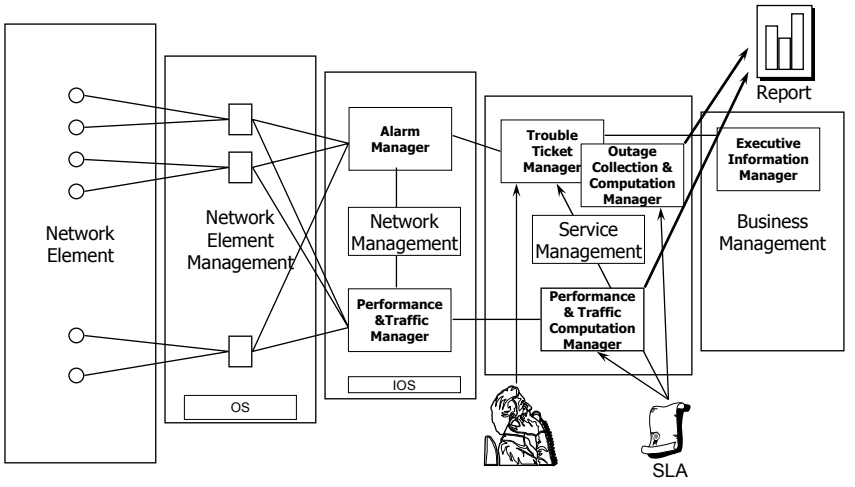
Sommario

1. **Chi gestisce cosa e come?**
2. **Aree funzionali del management OSI**
3. **Modello Manager/Agent/Managed object**
4. **Management Information Base**
5. **Simple Network Management Protocol**
6. **Utilizzo di SNMP per gestire una rete**

Da Che Parte Iniziare?



Un Possibile Approccio..

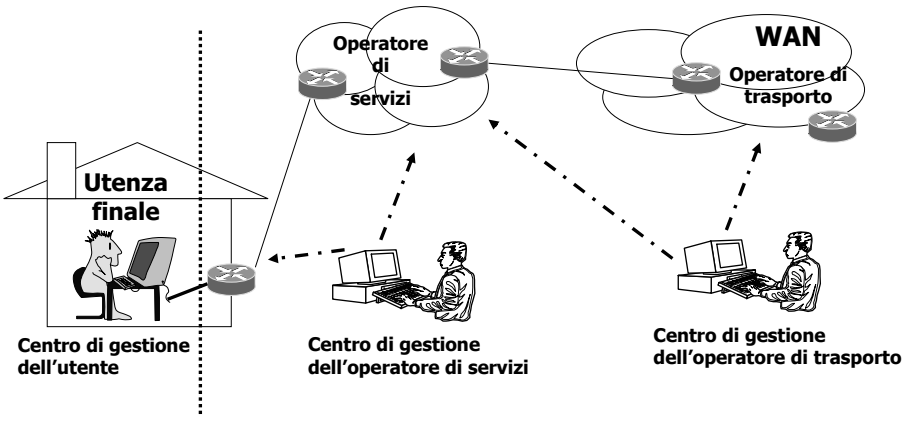


Rete: chi gestisce cosa?

Si possono avere vari livelli di gestione di rete :

- Gestione di rete di backbone (operatore di TLC)
  - **apparati Frame Relay, ATM, SDH, ottici: usano protocolli proprietari x trasporto info e gestione/segnalazione in WAN**
  - **IP e Gbit Ethernet sempre più usati, dunque gestione più "open source", soprattutto agli edge della rete di dorsale (MAN, accesso)**
- Gestione di rete locale (LAN system administrator)
  - **IP, Ethernet, WLAN**
  - **Linux sempre più usato x gestire rete & servizi**

Domini di competenza



Come gestire una rete?

Gestire un insieme complesso di risorse di rete significa:

- Far funzionare correttamente e in modo sicuro la rete
- Configurare opportunamente accessi e apparati
- Fare campagne di monitoraggio della funzionalità e delle prestazioni della rete
- Last but not least: soddisfare le richieste degli utenti (sia in WAN che in LAN !!)

Gestione di rete OSI e Internet

- **<u>Approccio ISO/OSI</u>:**
  - **definizione di 5 aree funzionali di gestione di rete,**
  - **Common Management Information Protocol (CMIP),**
  - **Gestione distribuita,**
  - **maggiore complessità sugli elementi di rete da gestire.**
- **<u>Approccio IETF</u>:**
  - **protocollo semplice di gestione (SNMP: 1988 primo draft, 1998 SNMPv3)**
  - **gestione centralizzata,**
  - **colloquio basato su UDP.**

Aree funzionali del MGMT OSI

1. **Fault: gestione dei guasti e degli allarmi**
2. **Configuration: gestione delle configurazioni**
3. **Accounting: gestione degli account e dei costi dei servizi**
4. **Performance: gestione delle prestazioni**
5. **Security: gestione della sicurezza e degli accessi**

1. Fault Management

- Riconoscere tempestivamente guasti sulla rete (apparati di rete, server, connessioni)
- Log dei guasti e degli allarmi, procedure aziendali dedicate
- Test diagnostici
- Rispettare le specifiche di contratto sul ripristino dei servizi (es. ripristino in 2 ore, in 8 ore o in un giorno!)
- Gestire il call center dedicato agli allarmi e dei guasti, interfacciarsi con il cliente
- Allarmi dovuti a guasti effettivi o a superamento di soglie prestazionali (es. banda non più garantita..)

2. Configuration Management

- raccolta e distribuzione di dati sullo stato delle risorse di rete
- inizializzazione e modifica delle configurazioni degli apparati
- Modifiche on-line o off-line della configurazione
- Variazione della configurazione per l'ottimizzazione delle prestazioni
- Configurazione di router, firewall, switch, provisioning delle connessioni fisiche

3. Accounting Management

- determinazione/modifica dei diritti e caratteristiche di accesso al servizio, in base al contratto stipulato
- billing dei servizi – addebitamento dei costi agli utenti finali
- definizione di limiti di utilizzo delle risorse da parte degli utenti
- calcolo di costi combinati per l'impiego di più risorse nell'ambito di un servizio – es. problema del roaming in reti cellulari e nelle reti wireless LAN di nuova generazione per l'accesso a Internet per utenti mobili

4. Performance Management

- Monitoraggio delle prestazioni della rete, in base alle specifiche contenute nel Service Level Agreement con il cliente
- Log delle prestazioni monitorate e report agli utenti finali
- Modifica dell'allocazione delle risorse della rete per soddisfare le richieste dei clienti
- Adozione di misure preventive per evitare situazioni di congestione o di disservizio

5. Security Management

- Analisi delle aree di rete a rischio (es. database con informazioni sensibili sui clienti)
- Adozione di piani per la sicurezza aziendale, sia fisica che di rete
- Controllo e logging degli accessi (passwords, diritti di accesso..)
- Test di vulnerabilità sulla rete e sugli ambienti fisici di accesso a server e database

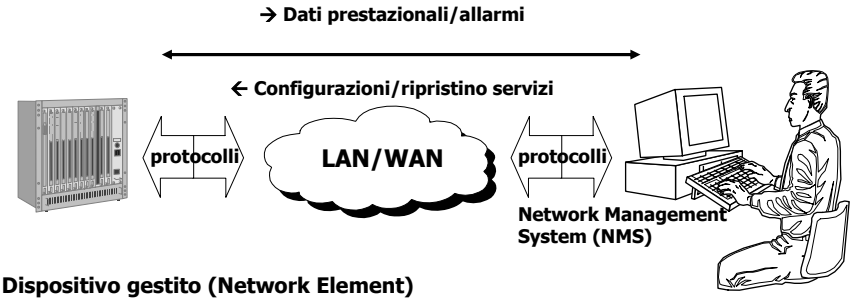
Componenti di un sistema di Gestione di Rete

I principali elementi di un sistema di gestione di rete sono:

- **Network Element da gestire**
- **Network Management System – stazione di gestione**
- **Protocollo di gestione**

Raccolta ed analisi di dati

Gli elementi di rete sono sistemi "attivi"
La piattaforma di gestione raccoglie i dati dall'elemento di rete
L'operatore di gestione visualizza i dati elaborati e li interpreta



Gestione in WAN e LAN

Network Element da gestire:

<u>WAN</u>: nodo Frame Relay o ATM, commutatore SDH, sistema optoelettronico per comunicazioni in fibra ottica, router IP di dorsale, collegamento punto-punto in fibra, ….

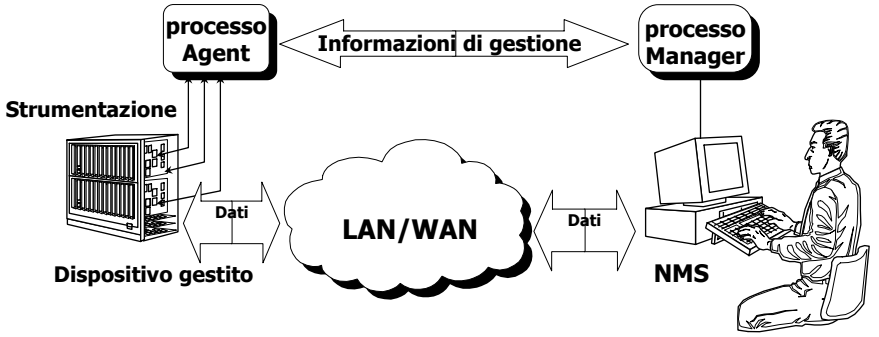
<u>LAN</u>: server di mail, Web, FTP, stampanti, switch, Access Point per WLAN, database, pc uffici, centraline telefoniche/VoIP

Paradigma Manager/Agent

Il colloquio tra NMS e Network Element si svolge tra:

- processo "*Agent*" sul network element
- processo "*Manager*" sul NMS

Manager ed Agent colloquiano usando un protocollo di gestione (SNMP)



Comunicazioni fra oggetti

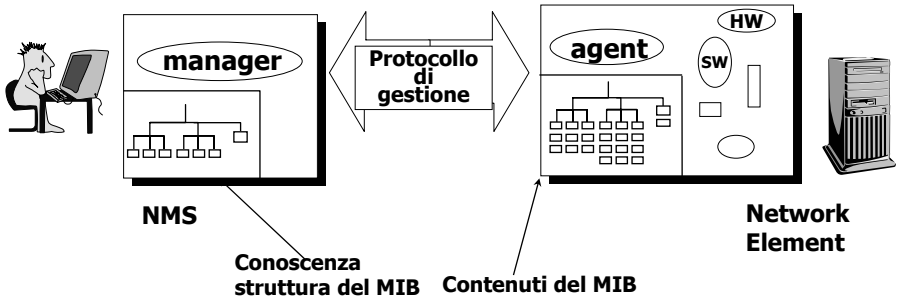
- **Manager ed Agent sono due processi software che implementano <u>oggetti</u> logici.**
- **Gli oggetti sono caratterizzati da:**
  - <u>uno stato</u> (funzionante, guasto)
  - <u>degli attributi</u> (caratteristiche relative all'oggetto gestito) – Management Information Base
  - <u>un protocollo</u> (utilizzato per scambiare messaggi con altri oggetti)

MANAGER / AGENT / MANAGED OBJECT

Il Management Information Base (MIB) è la rappresentazione logica degli oggetti gestiti:

- è organizzata come una "*directory*" con struttura ad albero
- le variabili del MIB rappresentano gli attributi degli oggetti, che ne determinano lo stato: es. max bit-rate di un interfaccia, numero di pacchetti in coda..

Il protocollo di gestione è uno strumento per effettuare interrogazioni "*query*" sul MIB

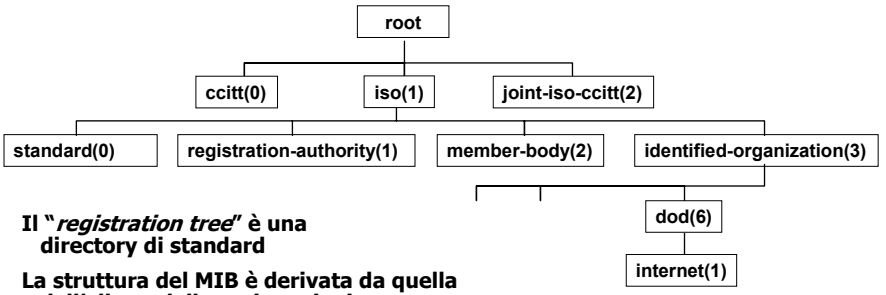


Management Information Base

MIB

- **organizzato ad albero**
- **E' contenuto nel processo Agent**
- **Contiene le variabili relative al network element gestito**
- **Il Manager conosce la struttura ad albero del MIB, e la "naviga" mediante i messaggi SNMP di request**
- **Il MIB deriva da una struttura logica ad albero più generale, l'albero delle registrazioni ISO**

Albero delle Registrazioni ISO



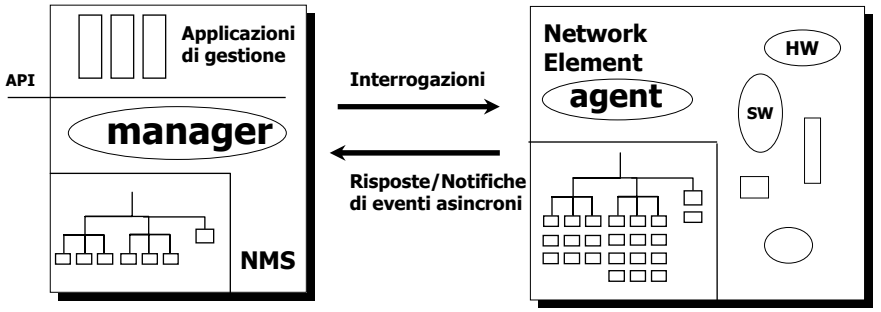
Il "*registration tree*" è una directory di standard

La struttura del MIB è derivata da quella dell'albero delle registrazioni

Un elemento dell'albero è identificato in modo univoco dal suo OBJECT IDENTIFIER: sequenza dei rami per raggiungerlo a partire dalla radice:

- internet OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 } sintassi SMI
  che in genere si indica con:
  - 1.3.6.1 formato numerico
  - iso.org.dod.1 formato simbolico

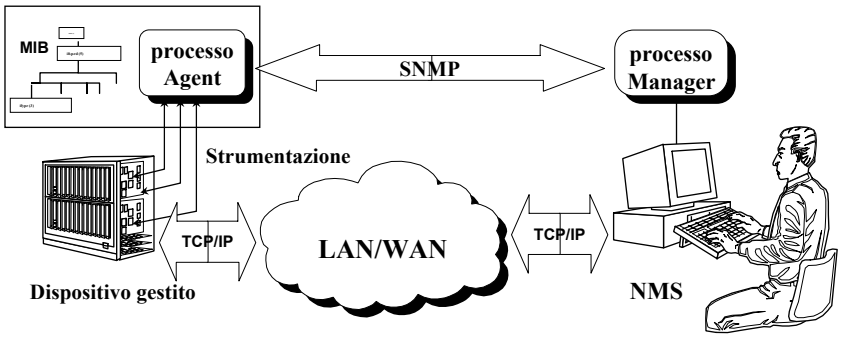
Comunicazione Manager/Agent



Gestione SNMP

Manager ed Agent colloquiano usando il protocollo SNMP
L'agente SNMP

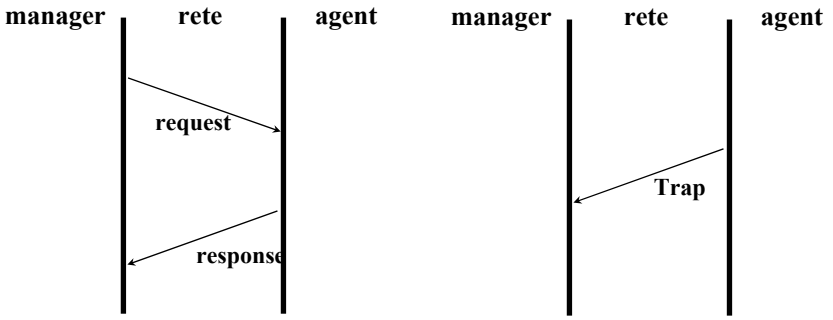
- controlla la strumentazione
- tiene aggiornato il MIB
- processa le query del manager
- notifica al manager eventi significativi (trap)



SNMP: messaggi

Due modi di scambiare informazioni:

- Polling effettuato periodicamente o meno dal manager sull'agent
- messaggi asincroni da agent a manager, a causa di guasti/allarmi



Variabili MIB

Cosa contengono i messaggi SNMP?

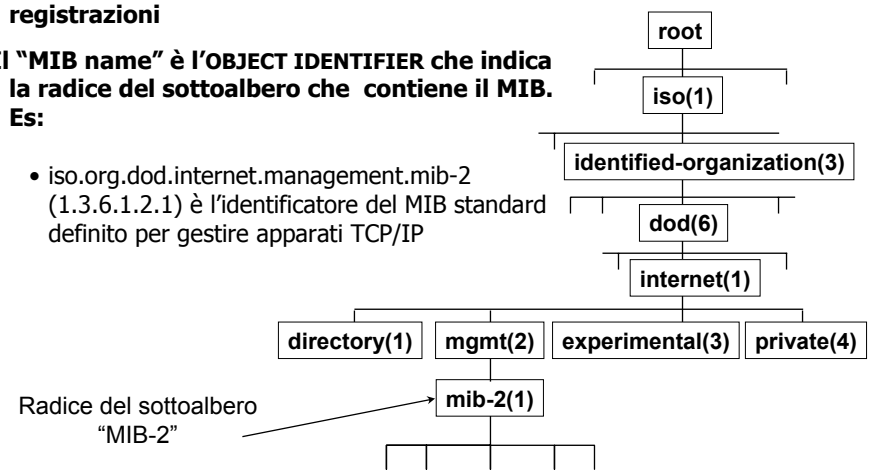
- **Vengono usati per fare query sul Management Information Base**
- **Il MIB è strutturato ad albero, in modo che Manager e Agent possono condividerne la conoscenza tramite convenzioni.**
- **I messaggi SNMP contengono variabili di stato del network element: banda utilizzata di un router, numero medio di pacchetti in coda su uno switch, etc**

MIB name

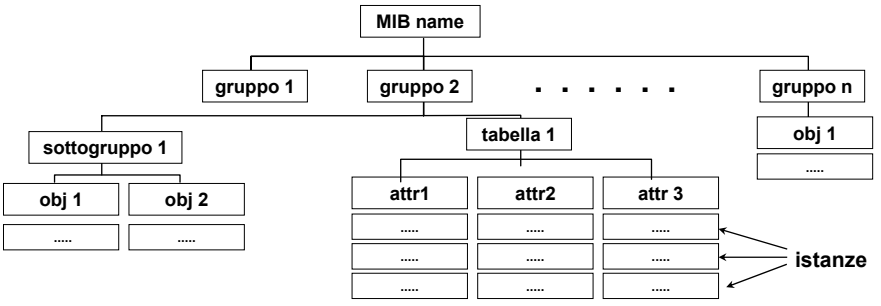
I MIB SNMP sono estensioni dell'albero delle registrazioni

Il "MIB name" è l'OBJECT IDENTIFIER che indica la radice del sottoalbero che contiene il MIB. Es:

- iso.org.dod.internet.management.mib-2 (1.3.6.1.2.1) è l'identificatore del MIB standard definito per gestire apparati TCP/IP



Struttura del MIB



I dati del MIB sono memorizzati nelle foglie dell'albero

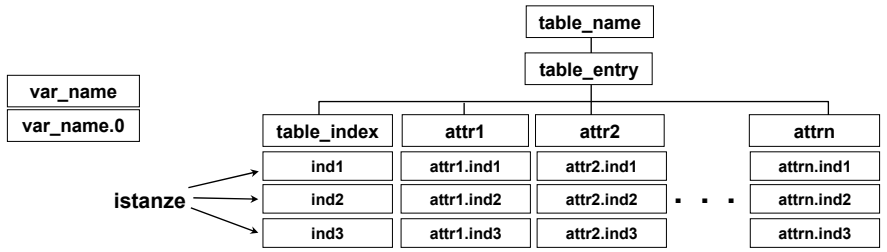
I nodi interni del MIB rappresentano raggruppamenti logici di oggetti (gruppi)

entità "multi-istanza" sono memorizzate sotto forma di tabelle

la struttura del MIB è statica

..... il contenuto è modificato dinamicamente

Variabili Scalari e Tabelle



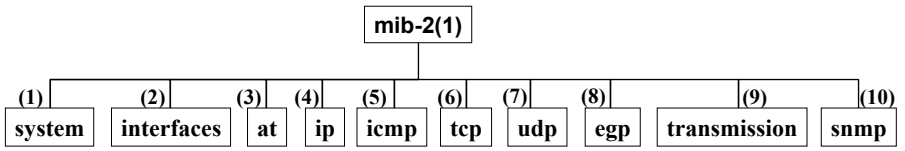
Variabili *scalari*

- hanno un solo valore possibile

Tabelle

- descrivono oggetti presenti in più instanze: interfacce, connessioni, etc.
- ogni colonna contiene tutti i valori di un attributo per le diverse istanze

Il MIB-2



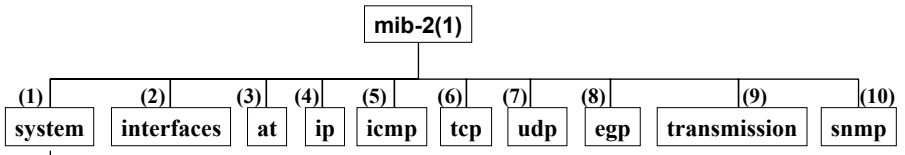
Il mib-2 è stato definito (RFC 1213) per facilitare l'integrazione nella gestione di apparati IP

10 gruppi inizialmente definiti per 171 "classi" di oggetti gestiti

Ogni agente deve obbligatoriamente implementare system, interfaces, IP, ICMP ed SNMP.

L'implementazione dei rimanenti gruppi è legata al tipo di dispositivo.

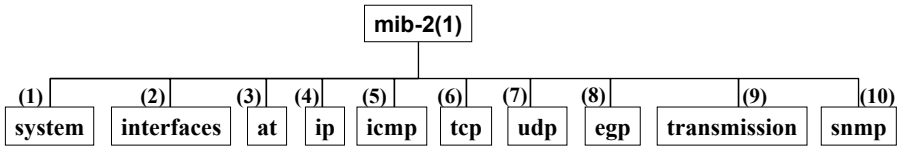
Il gruppo system (mib-2.1)



- sysDescr (1)
- sysObjectID (2)
- sysUpTime (3)
- sysContact (4)
- sysName (5)
- sysLocation (6)
- sysServices (7)

Contiene le informazioni principali che fanno riferimento all'intero sistema

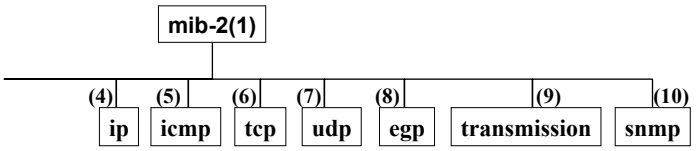
Il gruppo interfaces (mib-2.2)



- ifNumber
- ifTable
  - ifEntry
    - » ifIndex (1)
    - » ifDescr (2)
    - » ifType (3)
    - » **ifAdminStatus(7)**
    - » **ifOpStatus (8)**
    - » **ifLastChange (9)**
    - » **ifInOctets (10)**
    - » **ifInUcastPkts (11)**
    - » **ifInNUcastPkts (12)**
    - » **ifInDiscard (13)**
    - » **ifInErrors (14)**
    - » **ifInUnknwProt (15)**
    - » **ifOutOcts (16)**
    - » **ifOutUcastPkts (17)**
    - » **ifOutNUcastPkts (18)**
    - » **ifOutDiscards (19)**
    - » **ifOutErrors (20)**
    - » **ifOutQLen (21)**
    - » **ifSpecific (22)**

Contiene le informazioni principali sulle interfacce del sistema

Il gruppo IP (mib-2.4)



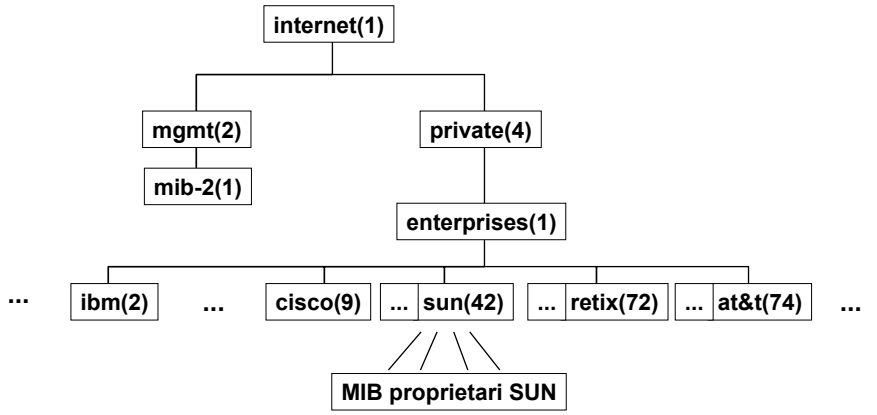
- ipForwarding (1)
- ipDefaultTTL(2)
- ipInReceives (3)

- ipInDiscards(8)
- ipInDelivers (9)
- ipOutRequests (10)
- ipOutDiscards(11)
- ipOutNoRoutes (12)
- ipReasmTimeout (13)
- ipReasmReqds (14)
- ipReasmOKs (15)

- ipReasmFails (16)
- ipFragOKs (17)
- ipFragFails (18)
- ipFragCreates (19)
- ipAddressTable (20)
- ipRouteTable (21)
- ipNetToMediaTable (22)
- ipRoutingDiscards (23)

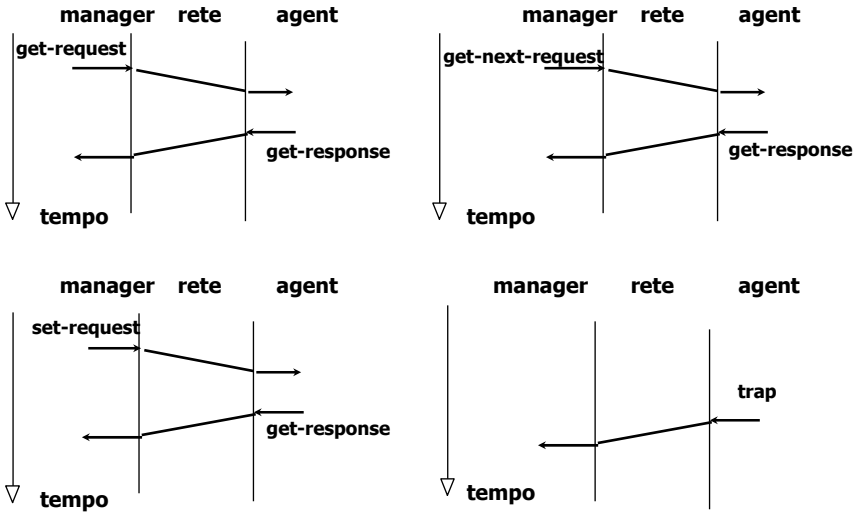
Contiene le informazioni principali sul livello IP

M I B privati (proprietari)

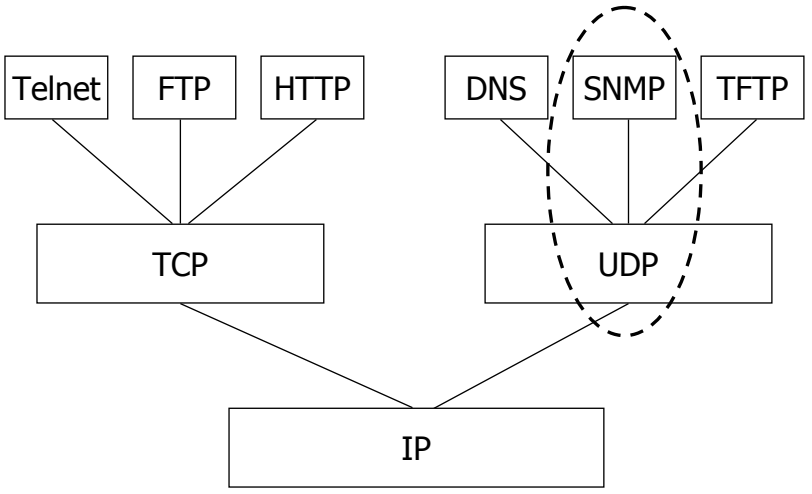


Permettono di descrivere aspetti specifici dei sistemi non descritti dal MIB-2

SNMP: primitive di comunicazione



SNMP e TCP/IP



SNMP: il protocollo

Simple Network Management Protocol
è il protocollo di gestione in ambito Internet

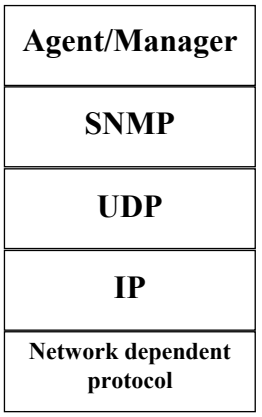
Protocollo semplice basato su domande/risposte

⇩

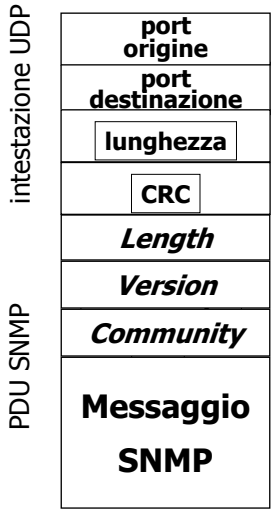
usa protocollo di trasporto semplice e non connesso

⇩

UDP



SNMP: formato dei messaggi

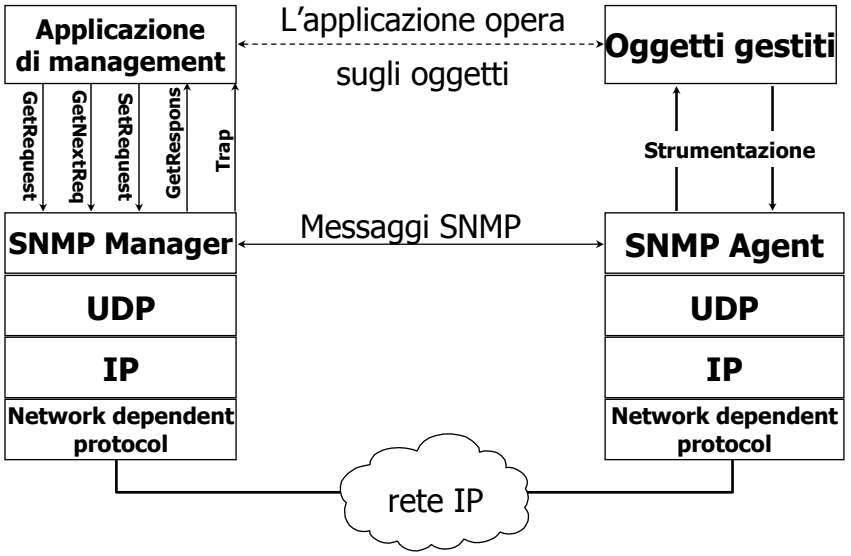


Sicurezza in SNMP:

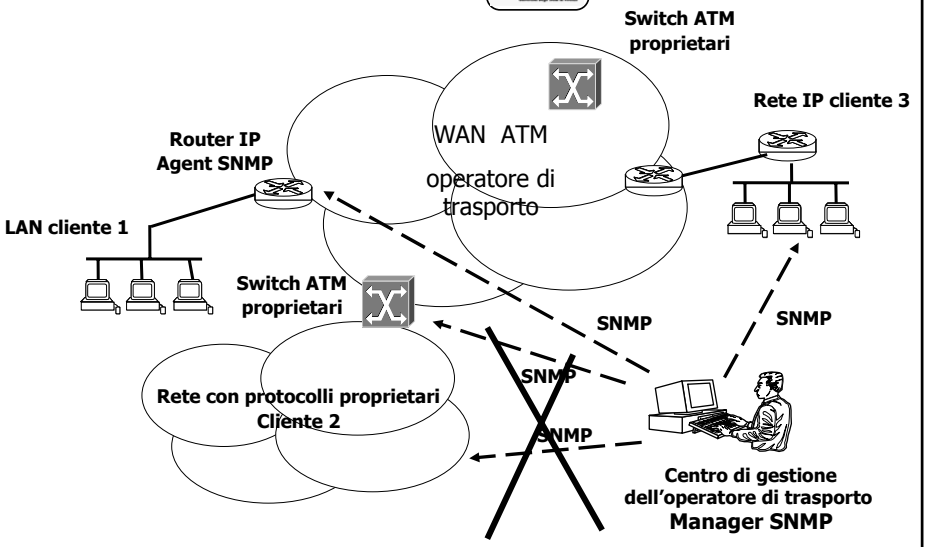
- **In ogni agent sono definite comunità di Manager , con diritti sulle variabili MIB:**
  - Read Only
  - Read Write
- **I manager inseriscono il "community name" in ogni messaggio inviato all'agente (get, get-next, set)**
- **La conoscenza della community name da parte del manager è considerata come autenticazione del manager da parte dell'agent**

Limitazione SNMPv1 e v2: community name in chiaro

Il ruolo di SNMP

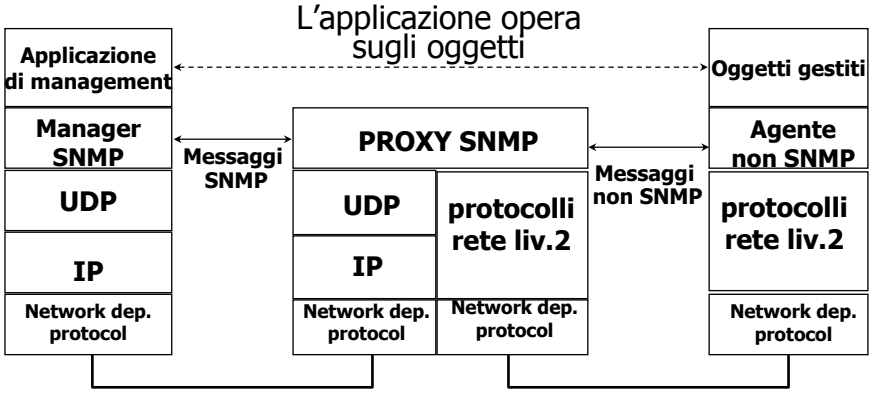


Reti eterogenee



Agenti Proxy

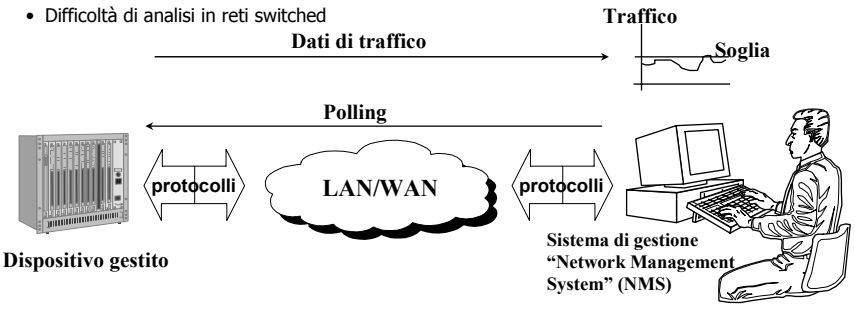
Fanno da traduttori fra processi SNMP/UDP/IP e processi con protocolli proprietari su apparati non-IP



Gestione di rete SNMP "tradizionale"

Continue interrogazioni degli agenti
Tutte le elaborazioni sono fatte sul NMS

- Eccessivo traffico di gestione sulla rete
- Eccessiva capacità elaborativa richiesta al manager
- Impossibilità di raccogliere tutte le informazioni necessarie
- Impossibilità di raccogliere dati relativi ad i segmenti di LAN
- Difficoltà di analisi in reti switched



Gestione con "Remote Network MONitoring"

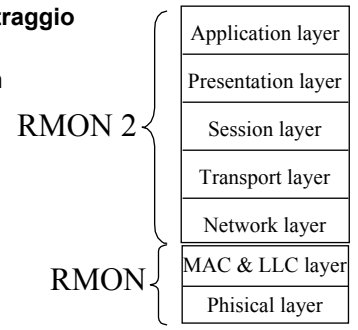
"Probe" remoti per Monitoring di segmenti di LAN

analisi continua del traffico
invio dei risultati al Manager solo in seguito a richiesta

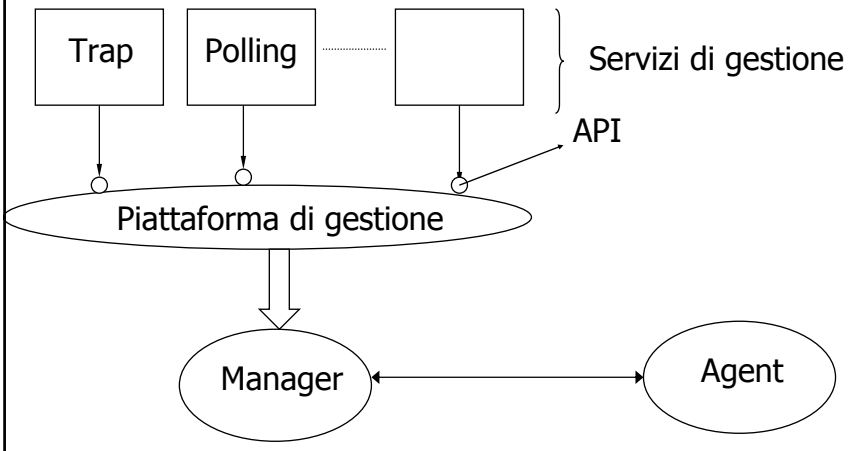
- Riduzione del traffico
- Semplicità di gestione
- Maggiore controllo sugli apparati
- Riduzione dei costi di gestione
- Utilizzabile anche in ambito LAN-internetworking

RMON ed RMON 2

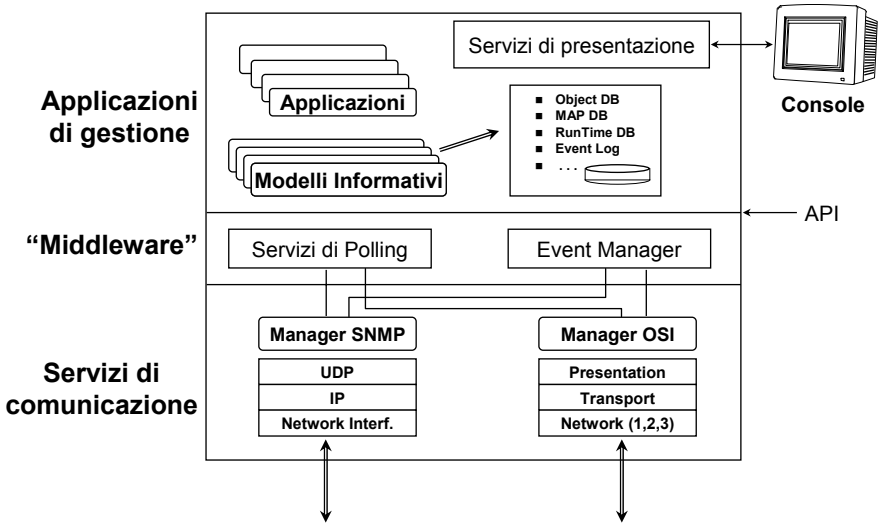
- **RMON permette di analizzare i primi due livelli della pila OSI**
- **RMON 2 è un'ulteriore estensione (RFC 2021)**
  - **Analisi dei livelli più alti (sino al livello applicativo)**
  - **Miglioramento delle capacità di filtraggio dei pacchetti**
  - **Miglioramento delle funzionalità in ambiente Multi-Manager**
  - **Miglioramento delle capacità di elaborazione locale dei dati sull'agente**



Piattaforme di gestione



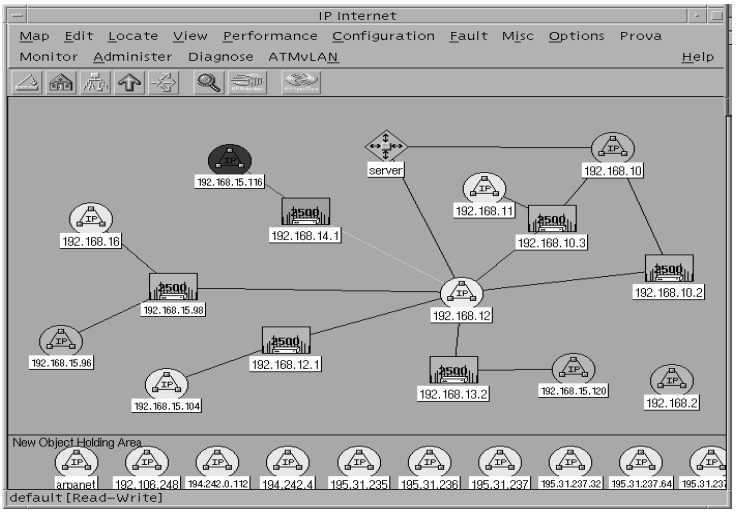
Architettura funzionale delle piattaforme di Mgmt



Strumenti per la gestione

- **Strumenti Generici:**
  - **MIB Browser**
  - **Strumenti per la gestione della topologia della rete (PING, Discovery)**
  - **Strumenti di ausilio alla gestione di workflow**
- **Strumenti Specifici:**
  - **Non sono forniti dalla piattaforma di gestione, e dipendono dal tipo di apparato da gestire e dal suo costruttore.**

Discovery



Gestione attiva e passiva

Il monitoraggio/gestione di un network element può avvenire in modo:

- **<u>attivo</u>: si immette traffico nella rete per eseguire la misura**
  - Es: query SNMP, ping, traceroute,
  - Vantaggi: metodo più semplice e flessibile
  - Limiti: si "rubano" risorse di rete al traffico utile
- **<u>passivo</u>: si osserva il traffico che attraversa un network element e si traggono statistiche e valutazioni (cattura dati, analisi e monitor)**
  - Es: RMON, batch di dati elaborati a posteriori
  - Vantaggi: non interferisce con il funzionamento della rete dati
  - Limiti: richiede grosse moli di dati da elaborare per ogni nodo