SNMP

Corso di Amministrazione di Reti
A.A.2002/2003

Materiale preparato utilizzando dove possibile materiale AIPA
http://www.aipa.it/attivita[2/formazione[6/corsi[2/materiali/Reti%20di%20Calcolatori/welcome.htm

Giorgio Calarco - DEIS

Argomenti

- Approcci ad hoc per la gestione delle reti
- SNMP – il Simple Network Management Protocol
- Struttura delle informazioni di gestione: cenni su SMIv1, SMIv2, SMIIng
- Il Management Information Base II
- Versioni del protocollo SNMP
- Cenni sulle Piattaforme di gestione
- Prodotti commerciali e open

Approcci ad hoc per la gestione delle reti

- Sono disponibili diversi tool e programmi che possono essere utilizzati per la gestione delle reti; ad esempio:
  - ping;
  - traceroute;
  - netstat;
  - whois;
  - telnet;
  - rlogin.
- Sfortunatamente tali approcci non consentono di gestire in maniera semplice tutti i possibili dispositivi che possono essere installati all'interno di una rete. Gli amministratori delle reti infatti necessitano di un protocollo unico che consenta di accedere alle informazioni di configurazione e di performance in modo diretto.

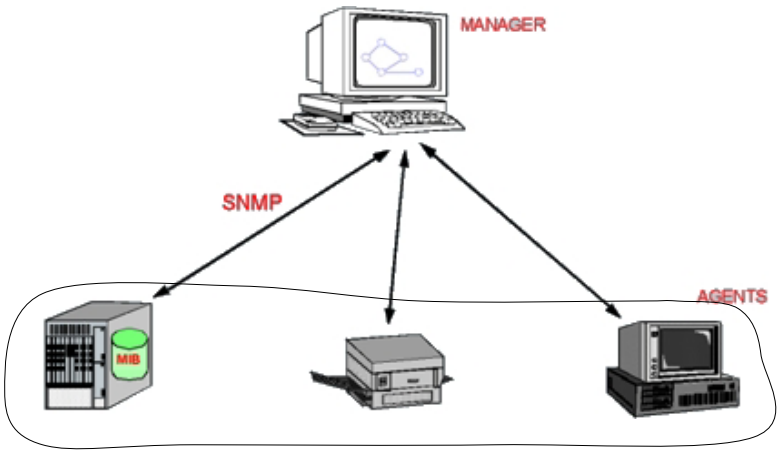
Introduzione a SNMP

- Sin dal suo sviluppo nel 1988, il protocollo SNMP (Simple Network Management Protocol) è divenuto lo ***standard de facto*** per la gestione delle reti. Poiché SNMP costituisce una semplice soluzione al problema del network management, molti produttori di hardware implementano il protocollo SNMP nei propri prodotti.
- Gli oggetti gestiti attraverso il protocollo SNMP debbono essere accessibili. L'accessibilità comporta che le informazioni di gestione vengano memorizzate da qualche parte, e che si possano interrogare e modificare. La struttura delle informazioni di gestione, descritta nell'**RFC 1155**, organizza le informazione ed assegna ad esse dei nomi in modo tale che si possa realizzare un accesso corretto a tali informazioni.
- Ciascun elemento SNMP gestisce oggetti specifisci a cui sono associate caratteristiche specifiche. Ciascuna coppia oggetto/caratteristica ha un proprio **Object Identifier** (OId), consistente di numeri separati da punti.
- Un Management Information Base consente di accedere in maniera efficiente alle informazioni che si desidera gestire.
- Il protocollo SNMP è basato sul **modello Manager/Agent**. Ci si riferisce al protocollo SNMP con il termine "semplice" in quanto il software da installare sull'Agent (nodo della rete da gestire) è minimo. La maggior parte delle capacità di elaborazione risiede, infatti, sulla Network Management Station (Manager).

Caratteristiche di SNMP

- Allo stato attuale il protocollo SNMP è il protocollo più popolare per la gestione delle reti. E' basato sulle seguenti entità:
  - **Network element**: dispositivi hardware (computer, router, ecc.) che vengono connessi alle reti.
  - **Agent**: sono moduli software che risiedono sui network element, il loro compito è quello di memorizzare informazioni.
  - Management information base (**MIB**): un MIB consiste in un insieme di managed object che risiedono all'interno di un database (il MIB appunto).
  - **Management protocol**: un management protocol viene utilizzato per scambiare informazioni tra agent e Manager. Il protocollo SNMP è lo standard de facto per la comunità Internet.
  - **Managed object**: un managed object consiste in una caratteristica o in una proprietà che deve essere gestita.
  - **Sintassi**: linguaggio usato per descrivere i managed object contenuti in un MIB mediante un formato indipendente dal computer. Si usa un sottoinsieme dello standard ISO ASN.1 (Abstract Syntax Notation) sia per definire il formato dei pacchetti scambiati dal protocollo di gestione che gli oggetti che debbono essere gestiti.
  - Structure of management information (**SMI**): definisce le regole per descrivere le informazioni di gestione. E' definito attraverso l'ASN.1.

Caratteristiche di SNMP



Struttura delle informazioni di gestione

- Lo **SMI** (Structure of Management Information) impone che tutti i managed object abbiano:
  - un nome;
  - una sintassi;
  - una codifica.
- Il *nome* corrisponde ad un Object Identifier (OId); la *sintassi* definisce il tipo di dato dell'oggetto (ad esempio, intero o reale). La *codifica* descrive come le informazioni associate al managed object sono formattate per poter essere trasmesse in rete.

SMIv1, SMIv2

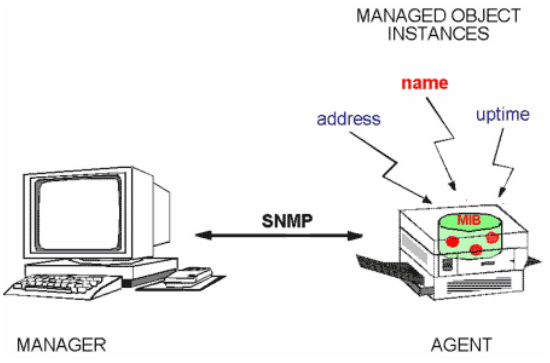
- Gli RFC 1155 e 2578 definiscono rispettivamente le versioni 1 e 2 dello SMI. Le informazioni di gestione associate ai managed object debbono essere rappresentate necessariamente mediante:
  - valori scalari;
  - tabelle (vettori bidimensionali di valori scalari).
- Si deve comunque notare che nel protocollo SNMP possono essere scambiati solamente valori scalari.
- I tipi di dato dello SMI sono suddivisi in 3 categorie:
  - Simple type;
  - Application-wide type;
  - Simply constructed type.
- ***Simple type:*** i Simple type includono 4 tipi di dato primitivi definiti in ASN.1:
  - Interi;
  - Sequenze di byte;
  - Object Identifier;
  - Sequenze di bit.

SMIng

- Il progetto SMI Next Generation (SMIng) ha lo scopo di migliorare alcune caratteristiche degli SMI precedenti. I principali problemi associati allo SMIv2 sono:
  - lo SMIv2 si basa sulla versione ASN.1 del 1988;
  - i tool per lo SMIv2 sono abbastanza complessi;
  - alcuni tipi di dato non sono presenti nello SMIv2 (ad esempio, gli interi a 64 bit);
  - nello SMIv2 non è stato definito un meccanismo per le estensioni;
  - nello SMIv2 sono comparse delle varianti non perfettamente compatibili.
- L'obiettivo principale dello SMIng è quello di individuare un linguaggio di definizione dei dati (Data Definition Language o DDL) che sia realmente indipendente dai protocolli.

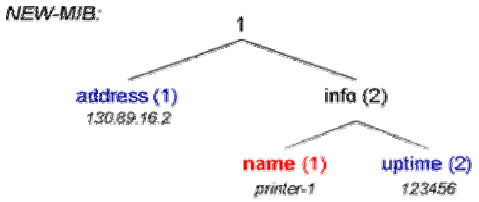
Management Information Base

- Un MIB (Management Information Base) può essere descritto come un albero n-ario la cui radice non ha nome. Le foglie dell'albero sono costituite da entità individuali. Gli Object Identifier (OId) consentono di individuare univocamente una entità all'interno dell'albero. Gli OId sono assimilabili a dei numeri telefonici strutturati in maniera gerarchica; ogni organizzazione possiede una propria sequenza di numeri.



Management Information Base

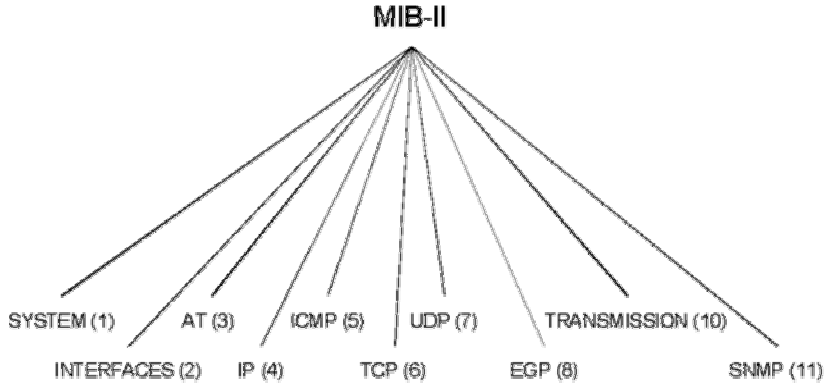
- Ad esempio, alla stampante in figura si può associare la seguente gerarchia:



Gli elementi di tale gerarchia possono essere individuati facilmente nel seguente modo:
• **address**
Object ID = 1.1 , Object Instance = 1.1.0 , Value of Instance = 130.89.16.2
• **info**
Object ID = 1.2
• **name**
Object ID = 1.2.1 , Object Instance = 1.2.1.0 , Value of Instance = printer-1
• **uptime**
Object ID = 1.2.2 , Object Instance = 1.2.2.0 , Value of Instance = 123456

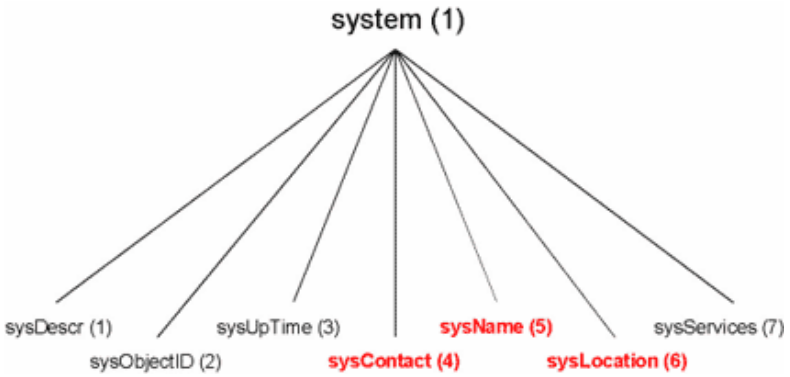
MIB II

- L'attuale MIB standard per Internet, MIB-II, è stato definito nell'RFC 1213 e contiene 171 oggetti. Tali oggetti sono stati raggruppati per protocollo (ad esempio TCP, IP, UDP, ecc) e per categoria (ad esempio System e Interfaces).



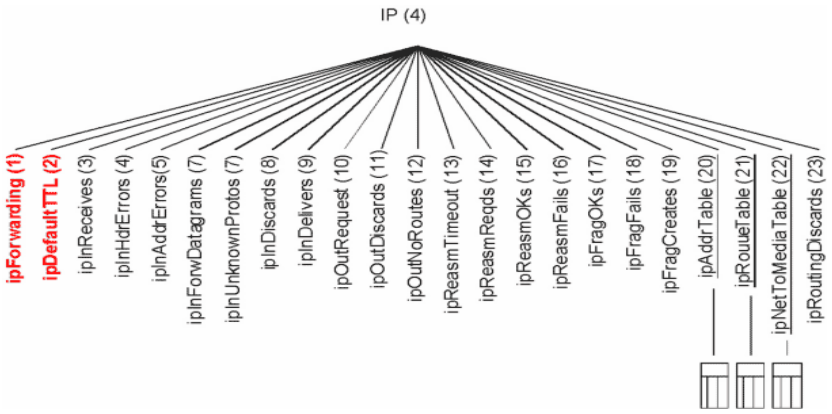
MIB II – system group

- Questo gruppo è fondamentale per tutti i dispositivi. Contiene informazioni relative al nome del sistema, il nome della persona da contattare in caso di necessità, la descrizione del sistema, ecc.
- La gerarchia MIB-II associata a tale gruppo è illustrata nella seguente figura.



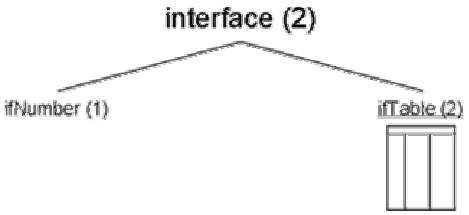
MIB II – Protocol Group

- In questo gruppo vengono definite le informazioni relative ai protocolli disponibili sui dispositivi che si desidera gestire.
- ***Internet Protocol Group:*** il sottoalbero relativo al protocollo IP contiene diverse informazioni necessarie per i dispositivi che utilizzano il protocollo IP: variabili di configurazione (ad esempio, TTL); contatori per gli errori; indirizzi IP e netmask per ciascuna interfaccia di rete; la tabella per il routing IP.



MIB II – Interface Group

Il sottoalbero relativo all'Interface group contiene una variabile scalare ed una tabella.

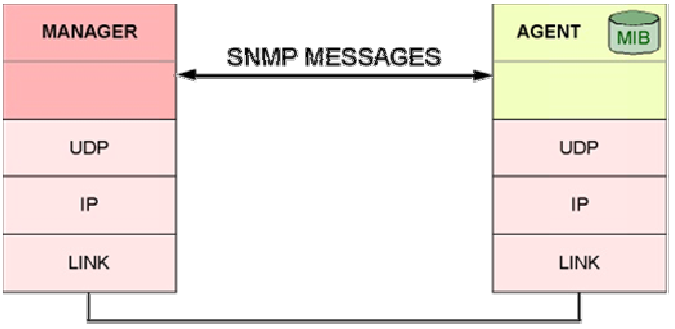


Il numero totale di interfacce di rete è indicato da IfNumber(1).

L'Interface group definisce le informazioni relative:
al tipo di tecnologia dell'interfaccia;
- alla stima della banda attuale espressa in bit/s;
- allo stato dell'interfaccia;
- a statistiche sul traffico in ingresso e in uscita;
- agli errori

Versioni del protocollo SNMP

- Il protocollo SNMP assume che i canali di comunicazione siano connectionless, quindi utilizza come protocollo di livello Transport il protocollo **UDP**. Di conseguenza, il protocollo SNMP non garantisce l'affidabilità dei pacchetti SNMP.

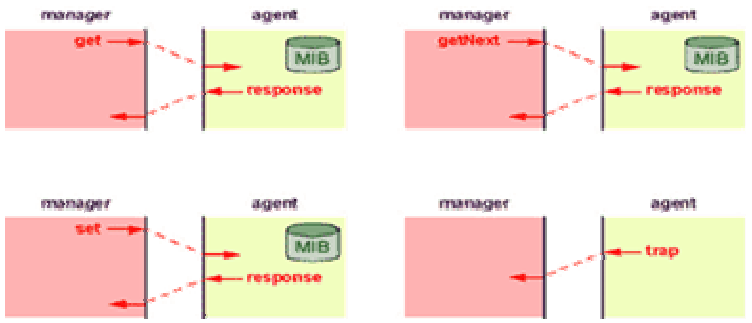


Versioni del protocollo SNMP

- Le caratteristiche principali del protocollo sono:
  - I moduli Agent sono in ascolto sulla porta UDP 161.
  - Le risposte sono inviate alla Network Management Station (Manager) utilizzando un numero di porta casuale.
  - La dimensione massima del pacchetto SNMP è limitata solamente dalla massima dimensione del payload UDP (65507 byte).
  - I messaggi di errore e le eccezioni (Trap) sono spediti dall'Agent al Manager in maniera asincrona utilizzando la porta UDP 162.

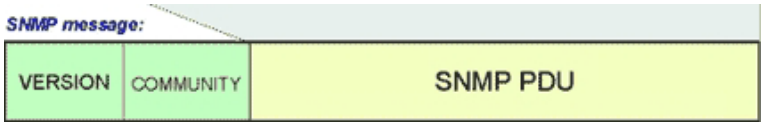
SNMPv1

- Le principali operazioni del protocollo SNMPv1 sono:
  - GET: utilizzata dal Manager per reperire un valore dal MIB dell'Agent.
  - GET-NEXT: utilizzata dal Manager per accedere ricorsivamente sul MIB.
  - SET: utilizzata dal Manager per impostare un valore sul MIB.
  - TRAP: utilizzata dall'Agent per inviare messaggi di errore al Manager.

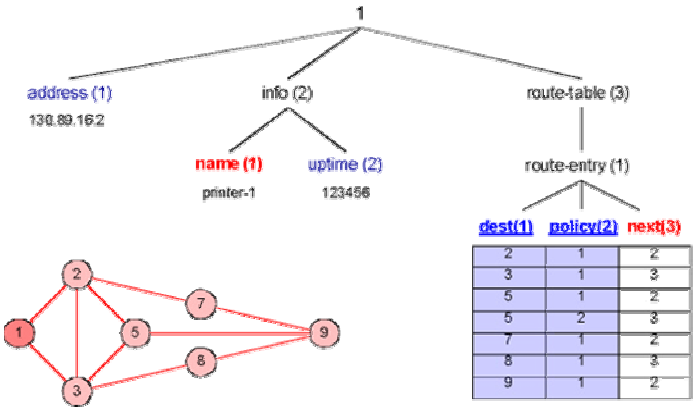


SNMPv1

- Il formato del pacchetto SNMP che consente la gestione di tali operazioni comprende:
  - Un numero di versione.
  - Una **Community** String utilizzata come password.
  - Uno o più payload di tipo SNMP.



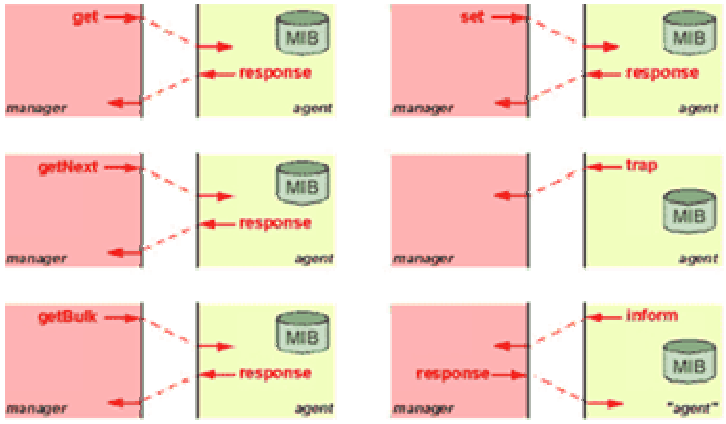
SNMPv1 – esempio di GET



get(1.1.0) -> response(1.1.0 => 130.89.16.2)
get(1.2.0) -> response(error-status = noSuchName)
get(1.1) -> response(error-status = noSuchName)
get(1.1.0; 1.2.2.0) -> response(1.1.0 => 130.89.16.2; 1.2.2.0 => 123456)
get(1.3.1.3.5.1) –> response(1.3.1.3.5.1 => 2)

SNMPv2

- Le principali limitazioni del protocollo SNMPv1: presenza di regole non documentate; codici di errori limitati; tipi di dato limitati; scarse prestazioni; dipendenza dal protocollo di trasporto; assenza di gerarchia nell'architettura Manager/Agent; scarsa sicurezza.

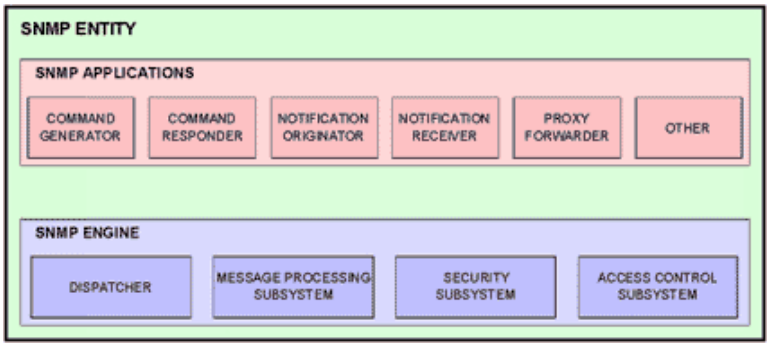


SNMPv3

- A partire dalla seconda metà del 1999 è disponibile una ulteriore versione del protocollo snmp. Poiché le differenze con le precedenti sono notevoli, ne vediamo le caratteristiche maggiormente innovative. Si tratta della terza versione del protocollo e nasce, in special modo, per sopperire alle mancanze dei suoi predecessori nell'ambito della sicurezza delle trasmissioni. Questo protocollo è stato pensato, inoltre, per essere scalabile, duraturo, per quanto riguarda la sua architettura, portabile, compatibile con le precedenti versioni (usa gli stessi MIB).
- Nonostante ciò, la versione 3 non ha, almeno per ora, trovato grosso spazio sul mercato, dove continua a farla da padrone la versione 1, forse anche perchè, nonostante fosse fra gli obiettivi di questa nuova versione, la maggiorazione del numero delle caratteristiche è andato a scapito della semplicità del protocollo.

SNMPv3

- La classica architettura di tipo Manager/Agent, nella v3, è stata sostituita da una più complessa composta da Motore ed Applicazioni. Infatti, un'entità Snmp v.3 è composta da:
  - **Snmp Engine** (Motore): contiene un Dispatcher (smistatore di messaggi), un sottosistema per elaborare i messaggi, uno per la sicurezza e uno per il controllo dell'accesso;
  - **Snmp Applications** (Applicazione): contiene un generatore di comandi, un ricettore di notifiche, un risponditore ai comandi e altre....

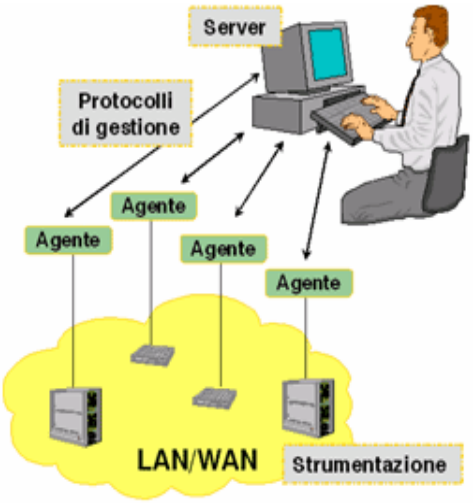


SNMPv3

- **Formato dei Messaggi:** Il formato dei messaggi di snmp versione 3 è sostanzialmente diverso da quello delle precedenti versioni. Infatti include anche alcuni parametri di sicurezza ed il controllo dell'accesso.
- **Sicurezza:** Tramite appropriate politiche di sicurezza, SNMPv3 consente di accettare messaggi solo nel caso in cui alcune domande ricevano una risposta affermativa o, comunque, valida come ad esempio:
  - Il messaggio è autentico?
  - Chi vuole eseguire una certa operazione? (Usa l'autenticazione con chiavi di crittografia pubbliche e private)
  - Quali oggetti sono coinvolti dall'operazione?
  - Quali diritti di accesso ha il richiedente sull'oggetto al quale vuole accedere?
- Queste politiche di sicurezza sono implementate tramite **crittografia**, funzioni di hash e altri strumenti che consentono l'autenticazione dei pacchetti (ad esempio contro un attacco di sniffing e ripetizione di pacchetto), delle password e, anche, delle PDU (anche queste ultime possono essere codificate).
- Tramite diversi livelli di sicurezza si può stabilire se consentire un accesso senza autenticazione (no pwd/no Priv), con autenticazione (Pwd/no Priv) o con autenticazione e codifica dei dati (pwd/Priv).

Cenni sulle piattaforme di gestione

- Il cuore di un sistema di gestione di rete è generalmente costituito da un potente *server* applicativo che raccoglie le informazioni rese disponibili dagli *agenti* di rete tramite i *protocolli di gestione*, ne offre una rappresentazione all'operatore umano ed esegue le applicazioni di controllo e monitoraggio sulla *strumentazione* di rete.



Cenni sulle piattaforme di gestione

- Una piattaforma di gestione sarà quindi in grado di supportare i protocolli di comunicazione tipici della gestione (**SNMP** e/o **CMIP**), fornire un accesso da parte degli applicativi alla rete di gestione tramite opportune API, realizzare funzioni di visualizzazione dello stato della rete e dei suoi elementi, ed interfacciarsi con vari tipi di database, contenenti la mappa della rete e dati di tipo statistico e amministrativo.

La differenza tra i protocolli di gestione fino ad ora analizzati in questo modulo, è evidenziata dall'immagine qui affianco, ove si vuole rappresentare in un modello stratificato, il modello di comunicazione delle piattaforme di gestione. Troviamo l'applicazione di gestione (*Applicazione di management*) al top della pila di elementi, mentre mano a mano che scendiamo si trovano protocolli che hanno sempre meno specializzazioni inerenti al nostro obiettivo.

Protocolli vs. Applicazione

- Abbiamo:
  - **SNMP** (specializzato alla gestione delle reti),
  - **UDP** (specializzato nel trasporto real-time/inaffidabile di pacchetti),
  - **IP** (specializzato nella consegna nel miglior modo di pacchetti)
- Il più basso livello, riguarda le specifiche costruttive della rete di trasporto (es. 802.3 oppure FDDI oppure Frame Relay oppure ATM ...).
- I protocolli di gestione forniscono accesso alla strumentazione, mentre le piattaforme di gestione raccolgono dati, presentano le informazioni, controllano i "network element" ed eseguono applicazioni di gestione.

Oggi

- Un primo aspetto da considerare nella strutturazione delle applicazioni di gestione è quale sia la *quota di interventi richiesta all'operatore umano* rispetto alle azioni portate a termine automaticamente dal software applicativo.

Attualmente si tende ancora a lasciare la parte maggiormente rilevante delle decisioni all'operatore umano a causa della capacità ancora scarsa di formalizzazione di molti processi gestionali, che fanno ancora ritenere più sicuro, anche se meno veloce ed efficiente, l'intervento umano su una buona quantità di decisioni critiche. In uno scenario di questo genere assume una importanza determinante la qualità della **rappresentazione grafica** dei dati

Domani ?

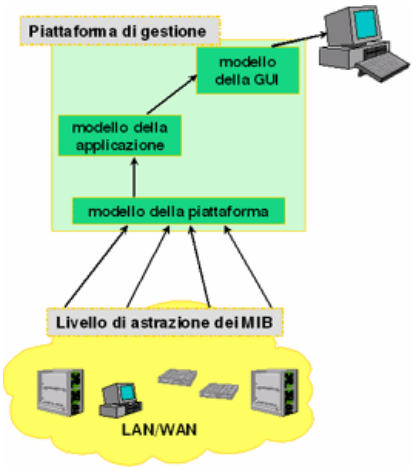
- In futuro si dovrà però abbandonare questa visione in favore di una maggiore delega del potere decisionale alle applicazioni, allo scopo di migliorare la scalabilità e le prestazioni dei sistemi di gestione e quindi, in ultima analisi, di diminuire i costi di esercizio. Si vuole evidenziare che questo passo richiede una sempre migliore comprensione e formalizzazione dei processi di gestione attualmente delegati agli operatori.

Data Management

- Un problema di grande rilievo nel progetto di una piattaforma di gestione riguarda i diversi modelli impiegabili per la modellizzazione delle informazioni. Infatti i **MIB** (**M**anagement **I**nformation **B**ase), rappresentano solo una delle viste possibili dello stato della rete, in particolare quella che è più vicina alle informazioni raccolte dalla strumentazione.
- I MIB sono un modello della strumentazione che rappresenta i dati raccolti ad un basso livello di astrazione. La piattaforma ha il compito di raccogliere i dati dei MIB secondo modelli più adatti alla manipolazione e successivamente anche il compito di fornire una più adeguata rappresentazione.

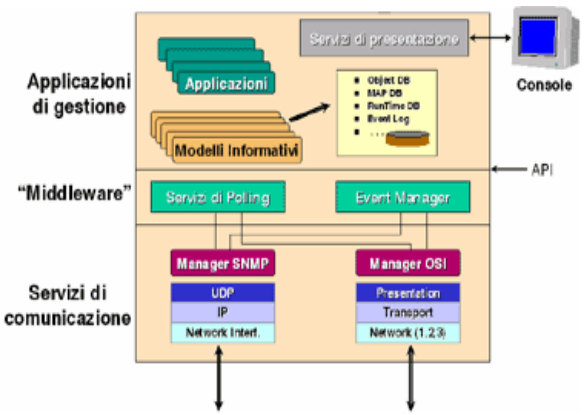
Data Management

- Una prima trasformazione di queste informazioni avviene quando queste vengono memorizzate all'interno della piattaforma per essere trattate dalle applicazioni, che non solo richiedono una diversa rappresentazione sintattica, ma spesso hanno anche bisogno di utilizzare un **livello di astrazione più elevato**. Problemi analoghi si hanno per la rappresentazione delle informazioni in forma grafica, e per l'accesso a sistemi di gestione di basi di dati impiegati per memorizzare l'enorme quantità di dati di gestione necessari in una rete.
- Sarà consuetudine per le applicazioni di gestione utilizzare **modelli specifici** diversi da quelli della piattaforma: ad es. le interfacce grafiche di rappresentazione (GUI) hanno bisogno di modelli finalizzati alla presentazione dei dati.



Architettura di una piattaforma di gestione

La figura rappresenta l'architettura di una generica piattaforma di gestione di rete. L'immagine illustra come sia possibile impiegare protocolli di gestione OSI o SNMP, con i rispettivi modelli informativi.

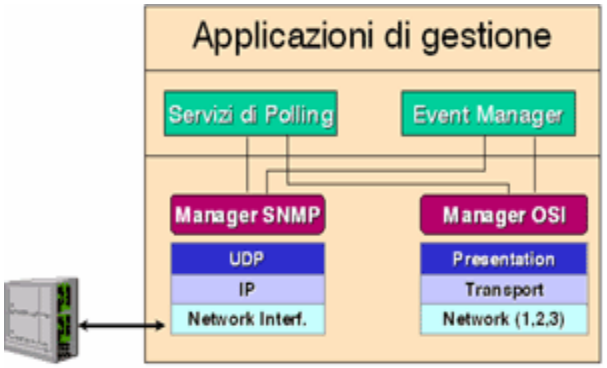


Applicazioni di gestione
Strato software in grado di astrarre i servizi offerti dagli specifici stack protocollari, utilizzando una interfaccia di programmazione (**API**) comune alle applicazioni di gestione ed ai servizi generici sviluppati sulla piattaforma.

Middleware
Fra questi servizi generici, i più importanti sono quelli di gestione del polling e degli eventi. In particolare quest'ultimo invia gli eventi ricevuti dalla rete a quelle applicazioni che hanno espresso un interesse per eventi di quel tipo.

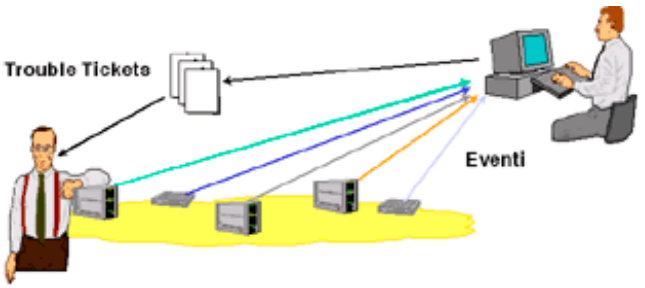
Architettura: Servizi di polling

- Lo scopo dei servizi di polling è quello di semplificare l'accesso agli agenti remoti da parte delle applicazioni di gestione.



Architettura: Event Manager

La raccolta degli eventi consente di avere informazioni tempestive sui cambiamenti nello stato della rete. Possono essere generati da agenti, da servizi di polling o da altre applicazioni. Gli eventi generati devono essere limitati in modo da non creare problemi prestazionali alla piattaforma di gestione. Vi è inoltre il problema della garanzia di ricezione di un evento da parte del manager, che non si può avere, ad esempio, se viene usato SNMP. Devono essere raccolti ed analizzati in modo da poter individuare correttamente la causa radice, ovvero il fenomeno avvenuto nella rete (guasto, riconfigurazione, sovraccarico o altro) che li ha generati.



Prodotti commerciali e opensource

- Il mercato oggi propone numerosi prodotti di System & Network Management. Tra le famiglie più complete troviamo:
  - **OpenView** di Hewlett Packard,
  - **Tivoli** di IBM,
  - **SMS** di Microsoft.
- Alternativa Open Source e Freeware
  - **MRTG** (**M**ulti **R**outer **T**raffic **G**rapher). Questa è attualmente utilizzata sia dal DEIS, sia dalla Facoltà di Ingegneria, sia dal CESIA (Centro Servizi Informatici d'Ateneo)
- Sono disponibili sulle principali piattaforme Unix e NT.
- La scelta non è ovviamente facile, poiché i criteri sono dipendenti dalle reali necessità dell'azienda. In genere, se c'è necessità di una gestione "trasversale" che interessi diverse aree, gli utenti più maturi scelgono una suite integrata piuttosto di un insieme di prodotti specializzati in diverse nicchie. Altre funzioni determinanti nella scelta del prodotto sono la capacità di gestire più piattaforme, la disponibilità di una interfaccia grafica versatile e, possibilmente, accessibile in remoto via Web.

Microsoft SMS

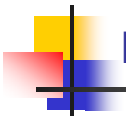
- debutto nel 1994
- framework di applicazioni e tecnologie progettate con l'intenzione di ridurre i costi di gestione del parco macchine aziendale. Col passare degli anni il prodotto ha fatto strada includendo funzioni di hardware e software inventory, software metering e deployment, nonché strumenti per il troubleshooting di postazioni remote.
- Le aree in cui il prodotto Microsoft davvero eccelle sono quelle della gestione delle informazioni di sistema e la reportistica. Grazie alla stretta integrazione con SQL server e Crystal Report (fornito insieme a SMS), i tool messi a disposizione dal software permettono all'utente di avere il pieno controllo sulle informazioni relative ai client.
- SMS dispone di un ottimo strumento per la *diagnosi in remoto* dei PC e per verificarne lo stato di salute.
- *Network Trace*, un utilissimo strumento in grado di supportare gli amministratori di rete in quanto è in grado di produrre uno schema grafico della rete includendo workstation, stampanti, router e tutti gli oggetti connessi

HP OpenView

- OpenView è un insieme di strumenti specializzati e in grado di interoperare e di coprire le seguenti aree di management: applicazioni e sistemi, rete, sicurezza, ambiente NT, desktop e software, storage e infine IT Service Level.
- Gli strumenti di OpenView utilizzano le tecnologie DCOM, ActiveX, ITIL (Information Technology Infrastructure Library) e Java.
- Nella piattaforma OpenView possono coesistere i tool di network management (Network Node Manager, NNM), system management (IT/Operations) e molti altri ancora, come ad esempio:
  - *Desktop Administrator* - per controllare l'assetto dei pc e ridurre i costi e le attività associate alle funzioni di amministrazione;
  - *IT Service Manager* - per controllare la qualità dei servizi mission-critical con l'automatizzazione dei processi di gestione;
  - *IT/Administration* - per fornire un'accurata visione e un pieno controllo dei sistemi gestiti attraverso l'inventario, la distribuzione del software e le configurazioni;
  - *ManageX* - per assicurare la disponibilità e prestazioni ottimali dei sistemi e delle applicazioni NT.

IBM Tivoli Enterprise

- Suite costituita da applicazioni specializzate che, estendendosi dall'S/390 fino al laptop, permettono di gestire i sistemi eterogenei e distribuiti come un'unica architettura integrata.
- Architettura comune, **T**ivoli **M**anagement **F**ramework (TMF), composta da oggetti conformi allo standard *OMG/CORBA*
- Spettro di azione particolarmente ampio:
  - Amministrazione - gestione del sofware (inventario,distribuzione) e delle configurazioni degli elementi della rete da una singola locazione centrale
  - Availability - piena disponibilità delle risorse di rete e delle applicazioni mission-critical. Tivoli NetView permette di esplorare le reti TCP/ IP, visualizzarne le topologie ed effettuare un monitoring proattivo delle risorse;
  - Sicurezza - protezione di applicazioni mission-critical, con il completo controllo della sicurezza cross-platform oltre alla gestione di utenti e gruppi.
  - Servizio - continuità del servizio, effettuando dalla console centrale il controllo dei processi, la pianificazione delle attività e il supporto alle decisioni.
  - Operation - grazie ai moduli ad hoc, è possibile automatizzare le funzioni amministrative di routine
  - Application - gestione dei database, del server Lotus Notes, di Microsoft Exchange, di IBM MQ Series, di SAP R/3 ecc.



MRTG

- Autore: Tobias Oetiker, nasce nel 1994, scritto in Perl e C
- Web site: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- Obiettivo iniziale:
  - a tool to monitor the traffic load on network-links.
  - generate HTML pages containing graphical images which provide a LIVE visual representation of this traffic.
- In realtà può essere utilizzato per monitorare qualunque network element dotato di un MIB, anche PC, server, stampanti, ecc.
- Si installa su **piattaforme**: Linux 1.2.x, 2.0.x, 2.2.x, 2.4.x (Intel,Alpha, Sparc,PowerPC,MIPS,S/390),SunOS 4.1.3,Solaris,AIX,HPUX,WindowsNT, 2000, XP,IRIX, BSD/OS,NetBSD,FreeBSD,OpenBSD,Digital Unix,SCO Open Server,Reliant UNIX,NeXTStep,OpenStep,Mac OS X
- Per vederlo in azione: http://mrtg.deis.unibo.it/ oppure http://www2.reti.unibo.it/Almanet_file/slide0002.htm