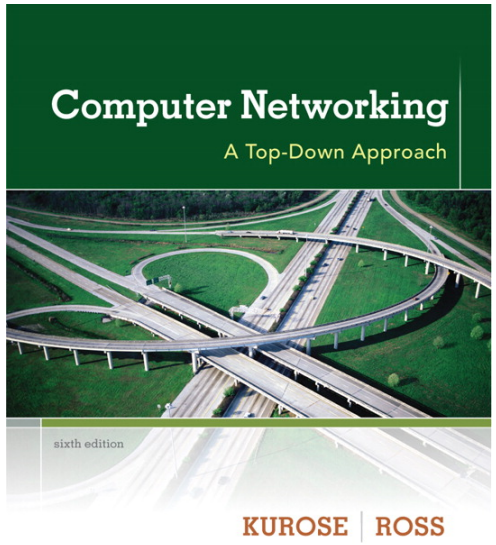
Chapter 9
Gestione della rete



Roberto Petroccia

petroccia@di.uniroma1.it

Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

Queste slide sono un adattamento delle slide fornite dal libro di testo e pertanto protette da copyright.

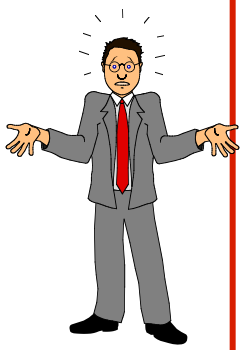
All material copyright 1996-2012 J.F Kurose and K.W. Ross, All Rights Reserved

Parte dell informazioni estratta da wikipedia ed altre fonti internet (tra cui slide Simon Pietro Romano – Reti Calcolatori II - Dipartimento diInformatica e Sistemistica dell'Università di Napoli)

Outline

- Introduzione alla gestione della rete
  - Motivazioni
  - Componenti principali
- Strumenti per i protocolli di gestione
  - **MIB: Management Information Base**
    - Base di dati di gestione
    - Standard per le informazioni gestite
  - **SMI: Structure of Management Information**
    - Linguaggio di definizione dei dati
  - SNMP: Simple Network Management Protocol
    - Protocollo di gestione della rete
  - RMON: Remote MONitoring
    - Protocollo che serve a monitorare il traffico di rete
  - Sicurezza ed amministrazione
- codifica dei nomi ASN.1

Cosa si intende per gestione della rete



"Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."

Gestione di sistemi autonomi ("reti"): dove abbiamo migliaia di componenti sia hardware che software che devo cooperare ed iteragire tra loro

Sono perciò sistemi complessi

Tipologia dei problemi affrontati

- **Monitorare**
  - Stato host
  - Traffico per utilizzo ottimale i risorse
  - SLA (Service Level Agreement)
- **Rilevare**
  - Guasti
  - Variazioni inaspettate di comportamento (tabelle di instradamento)
  - Intrusioni
- **Configurazione**
  - Necessità di raccogliere informazioni e intervenire su stato dispositivi e SW
- **Tracciare**
  - Necessità di raccogliere informazioni su traffico, connessioni ecc.
- **Controllo delle prestazioni**
- **Guasti**
- **Sicurezza**

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.

- Non è semplice gestire tutti i possibili dispositivi che possono essere installati all'interno di una rete.

- E' necessario una metodologia unica che consenta di accedere alle informazioni di configurazione e di performance in modo diretto.

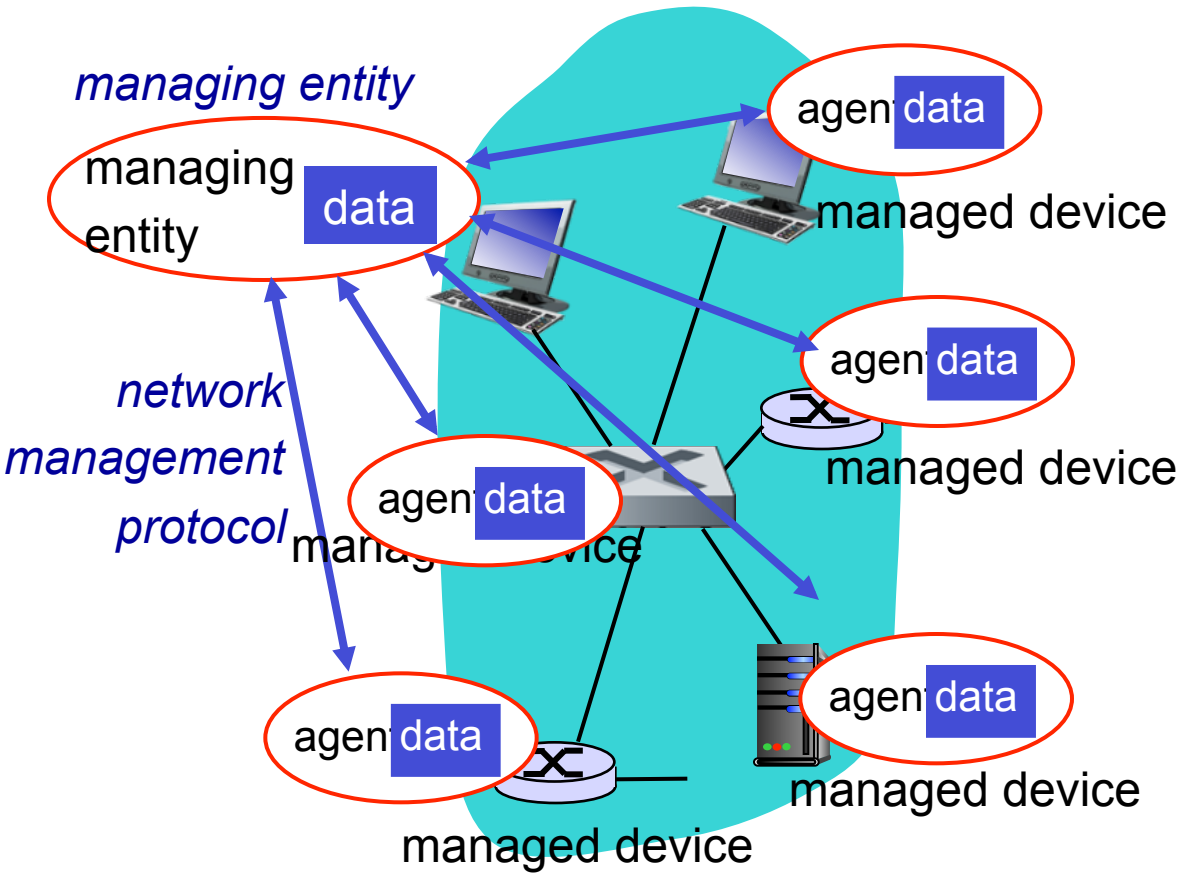
Approccio generale

Esistono diverse entità:

- **Network element**: dispositivi hardware (computer, router, ecc.) che vengono connessi alle reti.
- **Agent**
  - Elemento attivo (SW) presente su ogni dispositivo da controllare
  - E' in sostanza un server
  - Raccoglie informazioni di stato sul dispositivo
  - Offre un'interfaccia per agire in modalita' remota sul dispositivo
- **Manager**
  - Raccoglie informazioni/agisce sul dispositivo
  - Accede al dispositivo attraverso l'agente
  - Agisce da client verso l'agente di gestione
- **Protocollo tipo client/server tra manager e agent**

Infrastruttura per la gestione della rete

definitions:



managed devices contengono *managed objects* i cui dati sono organizzati in *Management Information Base (MIB)*

Network management standards

OSI CMIP

- Common Management Information Protocol
- designed 1980's: *the* unifying net management standard
- too slowly standardized

SNMP: Simple Network Management Protocol

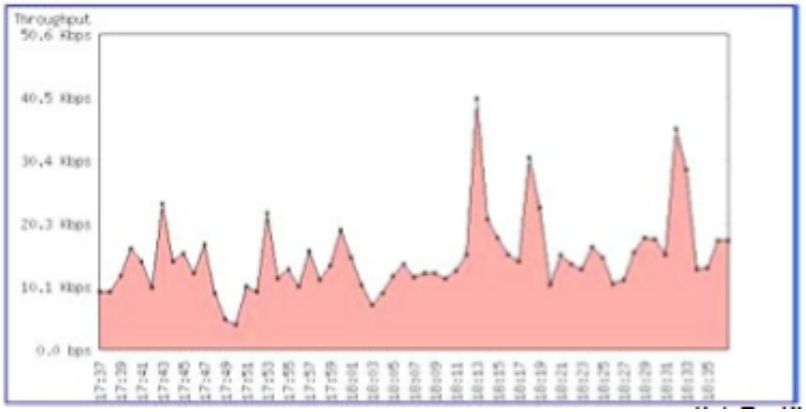
- Internet roots (SGMP)
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

SGMP: Simple Gateway Monitoring Protocol

SNMP e RMON

- **SNMP** (SimpleNetwork Management Protocol) è uno standard e un protocollo 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 overview: 4 key parts

- Management information base (MIB):
  - Collezione delle informazioni di rete da gestire
- Structure of Management Information (SMI):
  - Linguaggio per la definizione degli oggetti MIB
- SNMP protocol
  - Interazione manager<->managed object info, comandi
- Funzionalità di sicurezza ed amministrazione
  - Principali aggiunte in SNMPv3

Introduzione a SNMP 1/2

- Prima versione 1988, divenuto lo standard de facto per la gestione delle reti. E' il protocollo più popolare per la gestione delle reti. Siamo alla terza versione.
- Gli oggetti gestiti attraverso il protocollo SNMP debbono essere accessibili, in maniera da poterli interrogare e modificare.
- La struttura delle informazioni di gestione, descritta nell'RFC 1155.
- Ciascun elemento SNMP gestisce oggetti specifici a cui sono associate caratteristiche specifiche.
- Ciascuna coppia oggetto/caratteristica ha un proprio ObjectIdentifier (OId), consistente di numeri separati da punti.

Introduzione a SNMP 2/2

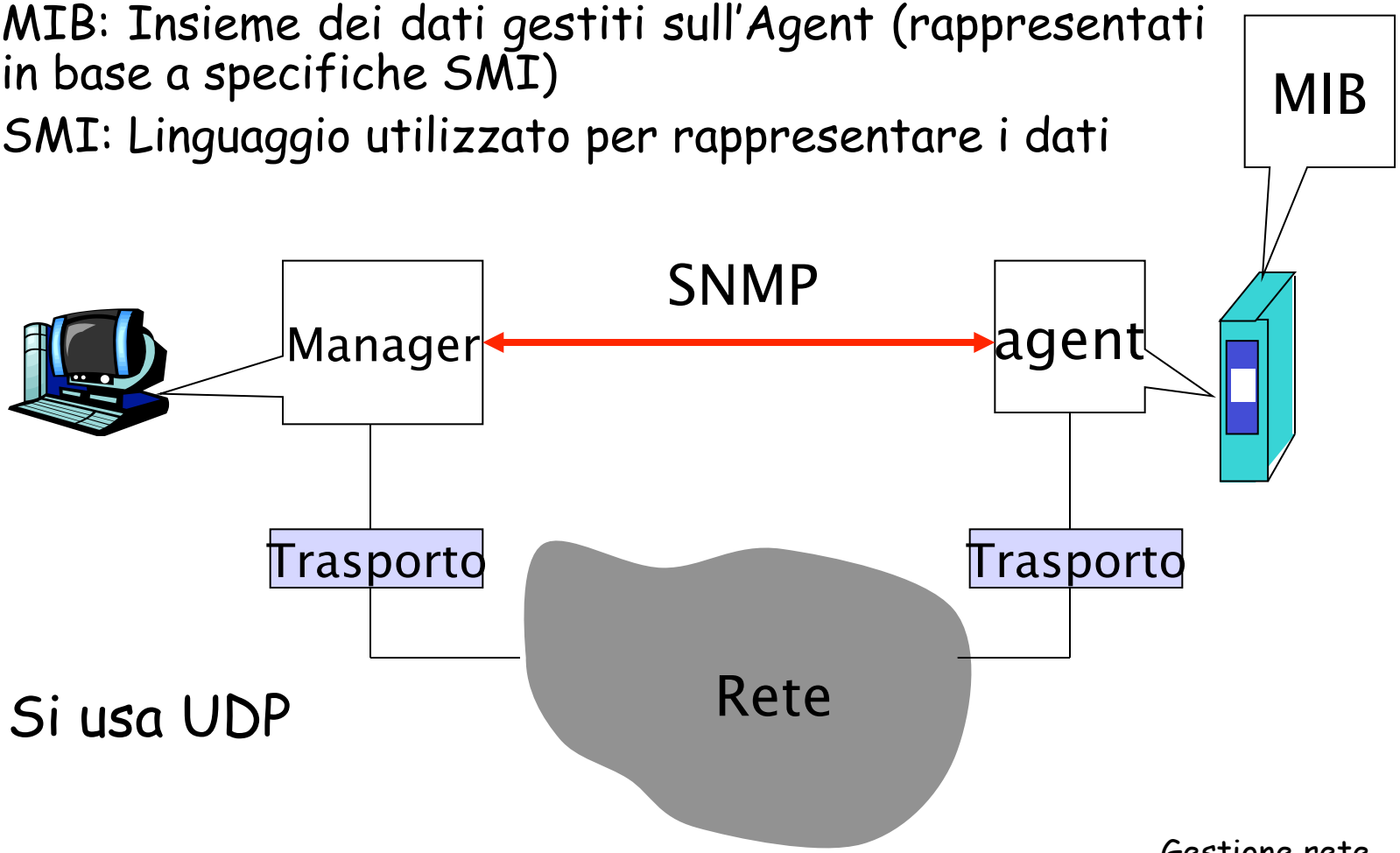
- Un Management Information Base consente di accedere in maniera efficiente alle informazioni che si desidera gestire.
- Il protocollo SNMP è basato sul modello Manager/Agent.
- Ci si riferisce al protocollo SNMP con il termine "semplice" in quanto il software da installare sull'Agent (nodo della rete da gestire) è minimo.
- La maggior parte delle capacità di elaborazione risiede, infatti, sulla Network Management Station (Manager).

Problemi

- Indipendenza dalla tecnologia
  - il protocollo agisce a livello applicativo
- Come definire i dati
  - Dispositivi assai diversi tra loro
  - Oggetti atomici, tabelle, strutture
  - Dati locali/globali
  - Dati statici/dinamici
- Codifica
- Accesso
  - Denominazione
- Protocollo di trasporto usato
  - UDP - semplice, inaffidabile
  - TCP - complesso, affidabile

Architettura SNMP

- SNMP: Protocollo modello client/server usato per accedere al MIB
- MIB: Insieme dei dati gestiti sull'Agent (rappresentati in base a specifiche SMI)
- SMI: Linguaggio utilizzato per rappresentare i dati



Si usa UDP

In SNMP abbiamo

- **Managed object**: un managed object consiste in una caratteristica o in una proprietà che deve essere gestita.

- **Management information base (MIB)**: un MIB consiste in un insieme di managed object che risiedono all'interno di un database (il MIB appunto).

- **Sintassi**: linguaggio usato per descrivere i managed object contenuti in un MIB mediante un formato indipendente dal computer. Sottoinsieme dello standard ISO ASN.1 (Abstract Syntax Notation)

- **Structure of management information (SMI)**: definisce le regole per descrivere le informazioni di gestione. E' definito attraverso l'ASN.1.

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. La codifica SMI è descritta nella specifica ISO detta Basic Encoding Rules (BER)
- Versioni SMI: SMIv1, SMIv2, SMIng (next generation)

SMI: linguaggio di specifica dei dati

- *Finalità:* esprimere una sintassi e semantica di gestione ben definita e senza ambiguità
- Tipi di dati fondamentali: semplici, tediosi
- OBJECT-TYPE

  Tipo di dati, stato, semantica dell'oggetto da gestire
- MODULE- IDENTITY

  raggruppamento di oggetti affini in un modulo MIB

Tipi di dati fondamentali

INTEGER

Integer32

Unsigned32

OCTET STRING

OBJECT IDENTIFIED

IPaddress

Counter32

Counter64

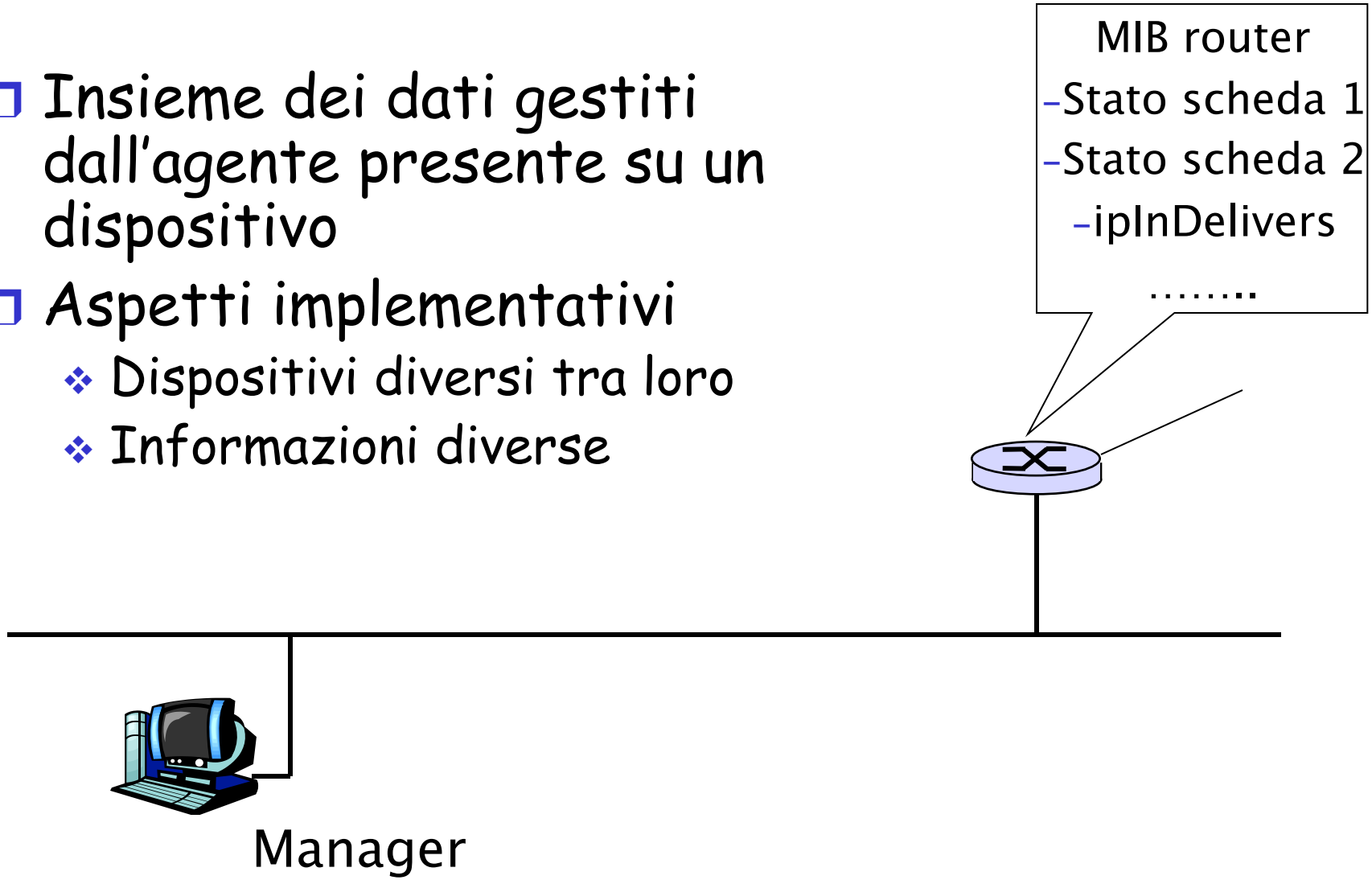
Gauge32

Time Ticks

Opaque

MIB (Management Information Base) 1/2

- Insieme dei dati gestiti dall'agente presente su un dispositivo
- Aspetti implementativi
  - Dispositivi diversi tra loro
  - Informazioni diverse



MIB (Management Information Base) 2/2

Modulo MIB specificato tramite SMI

MODULE-IDENTITY

(200 moduli MIB stndardizzati (IETF), molti altri con specifiche private dei produttori)

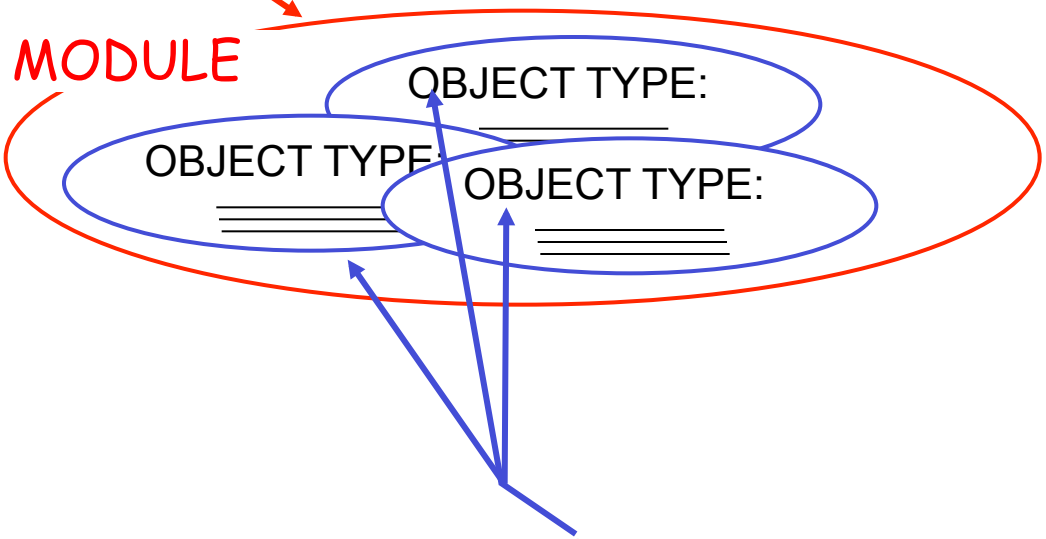
OBJECT-TYPE è un costrutto SMI di alto livello per specicare tipo di dati, stato e smeantica degli oggetti da gestire. Ha 4 campi:

SINTAX: tipo dell'oggetto

MAX-ACCESS: permessi di accesso (lettura/scrittura)

STATUS: indica se la definizione di un oggetto è valida, obsoleta o recuperabile

DESCRIPTION: descrizione testuale dell'oggetto



Oggetti specificati tramite SMI

Costrutto OBJECT-TYPE

SMI: esempio di oggetto e modulo MIB

OBJECT-TYPE: ipInDelivers

```
ipInDelivers OBJECT-TYPE
  SYNTAX        Counter32
  MAX-ACCESS    read-only
  STATUS    current
  DESCRIPTION
     "Il numero totale di
      datagrammi ricevuti e
      passati ai protocolli IP utente
      (compreso ICMP)"
::= { ip   9}
```

MODULE-IDENTITY: ipMIB

```
ipMIB MODULE-IDENTITY
  LAST-UPDATED "941101000Z"
  ORGANZATION "IETF SNMPv2
           Working Group"
  CONTACT-INFO
    " Keith McCloghrie
      ......"
  DESCRIPTION
    "Modulo MIB per la gestione delle
     implementazioni di IP e ICMP,
     escludendo la loro gestione dei
     cammini IP"
  REVISION "019331000Z"
 .........
::= {mib-2 48}
```

MIB: esempio di modulo UDP

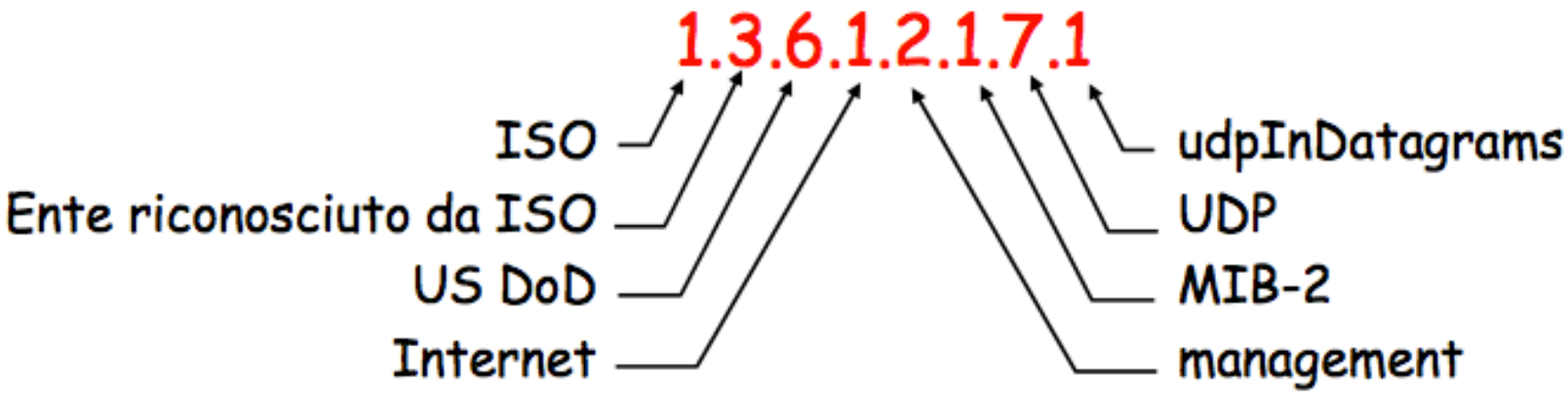
ID dell'oggetto	Nome	Tipo	Descrizione
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	Numero di datagrammi UDP recapitati
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	Numero di datagrammi UDP ricevuti per i quali non c'erano applicazioni alla porta di destinazione
1.3.6.1.2.1.7.3	UDPInErrors	Counter32	Numero di datagrammi UDP ricevuti, ma non recapitati (per motivi diversi dal precedente)
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	Numero di datagrammi UDP inviati dall'entità
1.3.6.1.2.1.7.5	UDPTable	SEQUENCE	Sequenza di oggetti UdpEntry, uno per ogni porta di applicazione, con l'indirizzo IP e il numero di porta dell'applicazione

Denominazione degli oggetti (ObjectId)

domanda: come chiamare un oggetto standard qualsiasi (protocollo, dato . . .) in una rete standard qualsiasi?

risposta: *albero di identificazione degli oggetti ISO:*

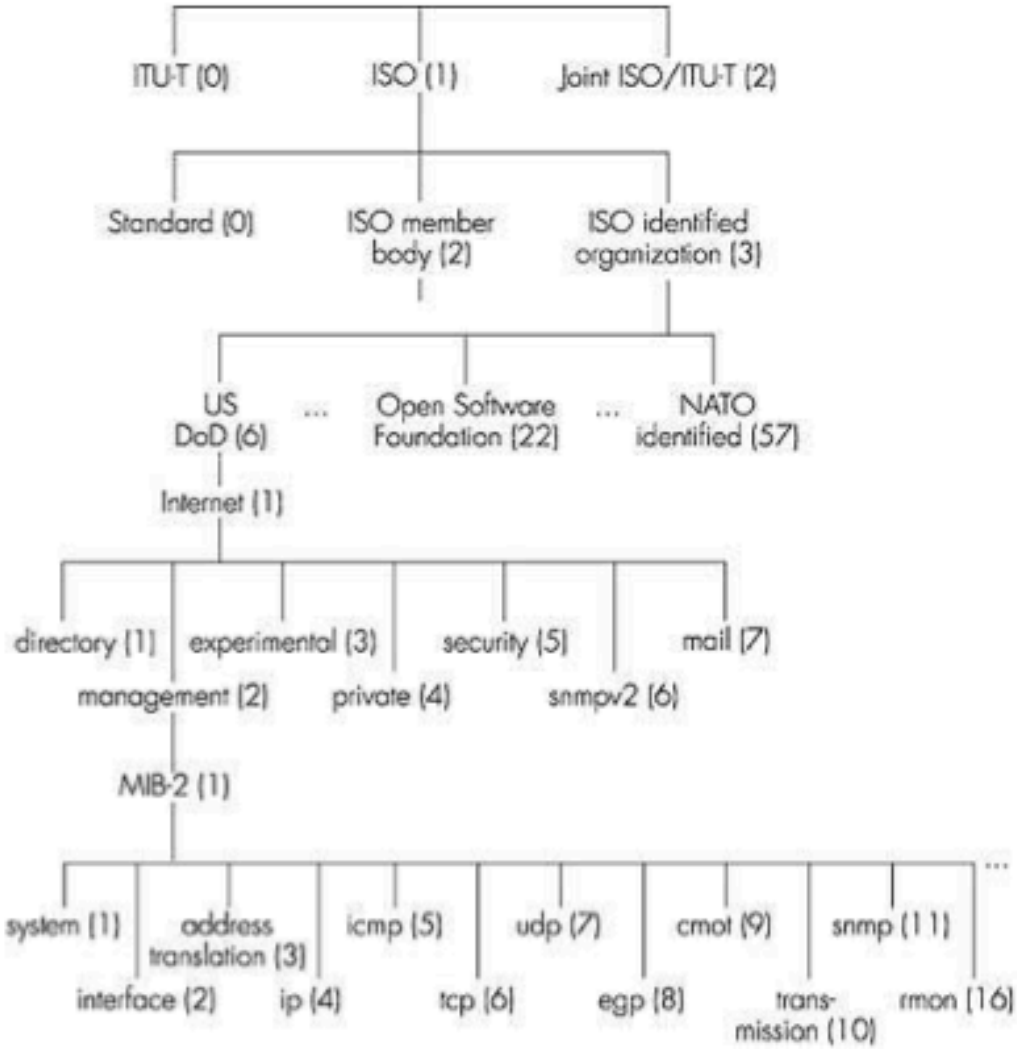
- denominazione gerarchica di tutti gli oggetti
- ogni ramo ha un nome e un numero



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.

Albero di identificazione degli oggetti OSI

Cfr. sito:
http://www.alvestrand.no/objectid/top.html

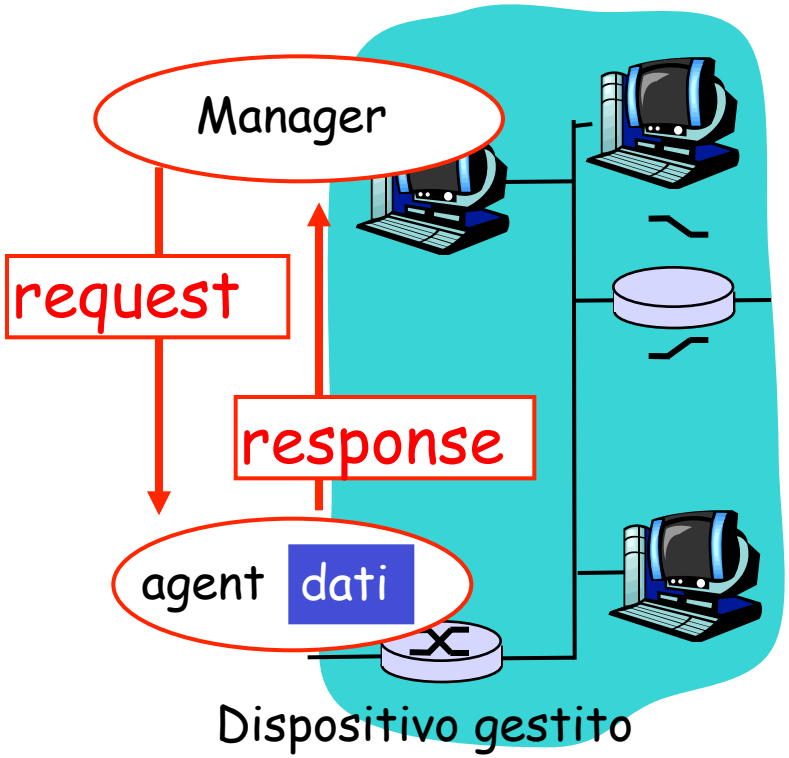


Protocollo SNMP

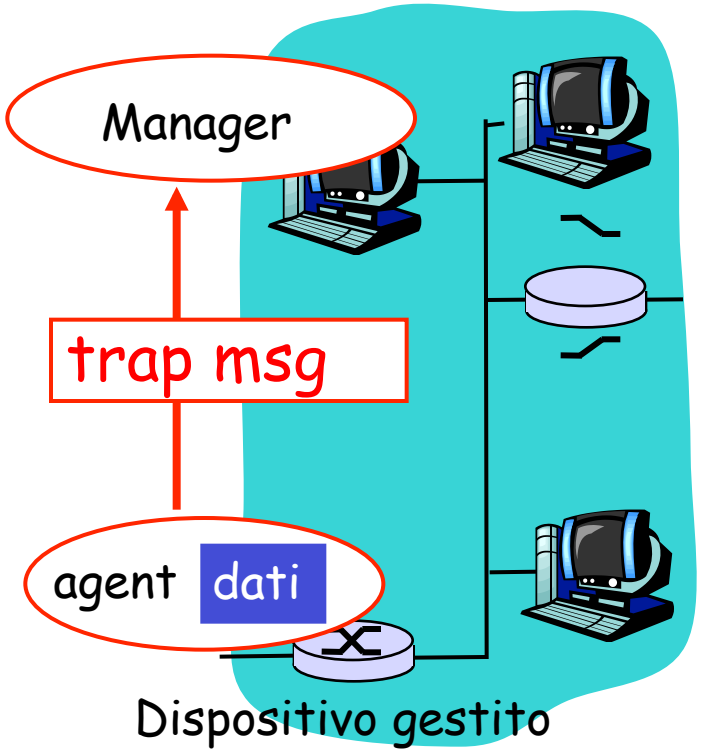
- Protocollo per il trasferimento e la manipolazione dei dati dei MIB
- Diverse versioni
  - Attuale: SNMPv3
- Protocollo a scambio di messaggi
  - Richiesta/modifica di variabili MIB
    - gestore -> agente
  - Tra manager
  - Da agente MIB a manager
    - Risposta a messaggi di richiesta/modifica
    - Trap - eventi eccezionali

Uso del protocollo SNMP

Due modalità per trasportare le informazioni MIB:



Modalità richiesta/risposta

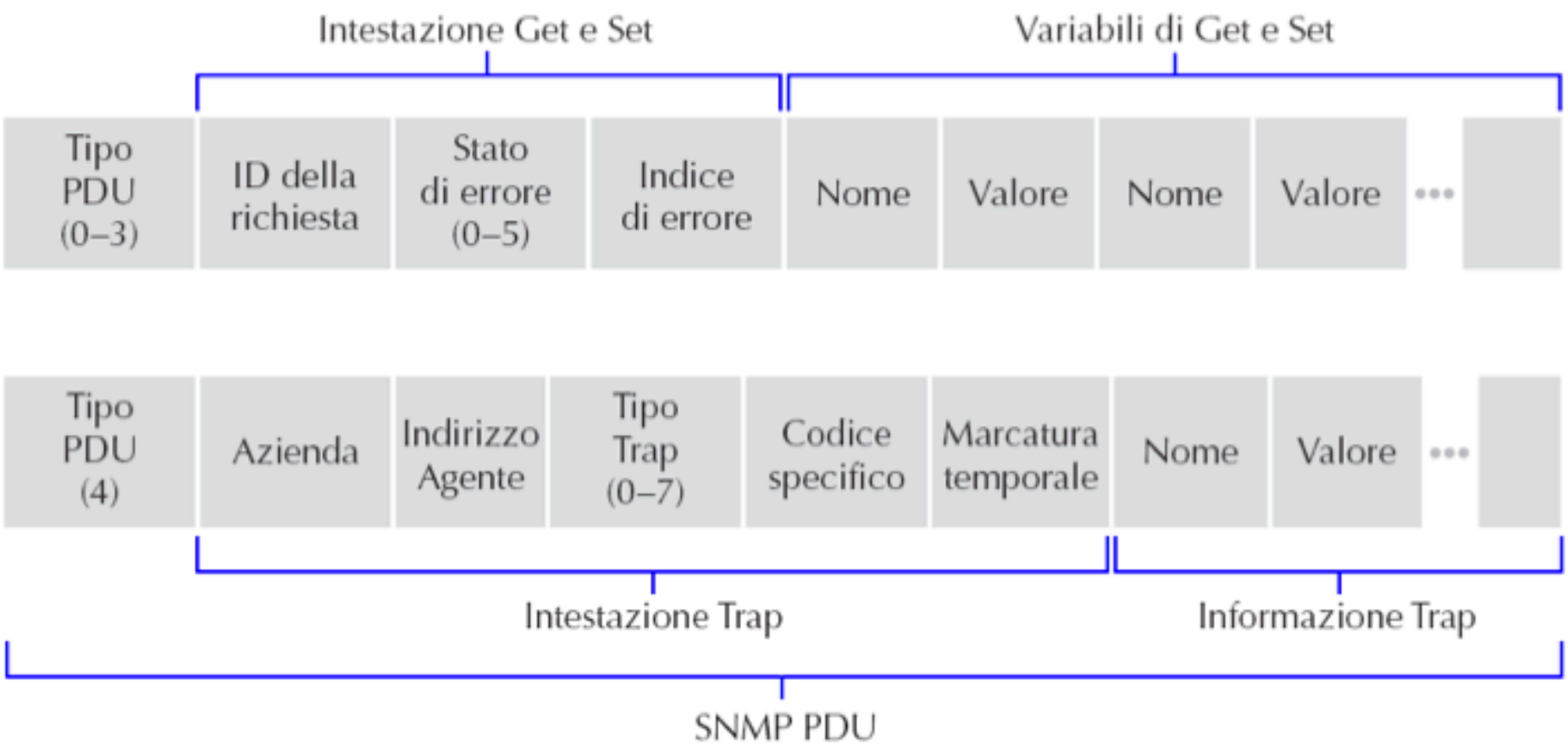


Modalità trap

SNMP: Tipi di messaggio

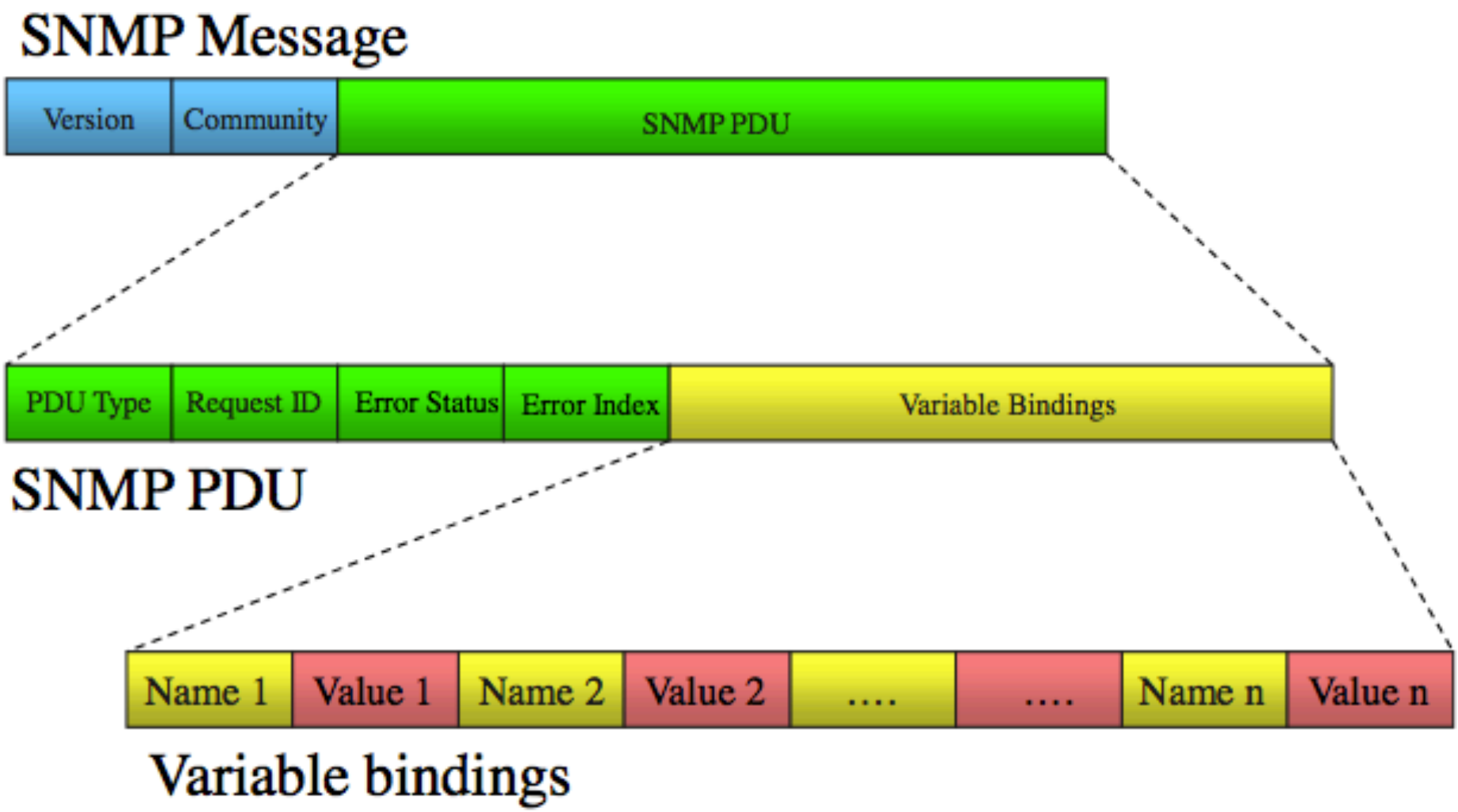
Tipo di messaggio	Funzione
GetRequest GetNextRequest GetBulkRequest	Dal manager all'agente per richiedere i valori di oggetti MIB (istanza, prossimo nella lista, blocco)
InformRequest	Da manger a manager: fornisce un valore MIB
SetRequest	Da manger a agent: imposta il valore MIB
Response	Da agente a manager: valore, risposta alla richiesta
Trap	Da agente a manager: informa il manager di un evento inatteso

SNMP: formati del PDU



PDU = Protocol Data Unit

Struttua dei messaggi



Campi messaggio 1/2

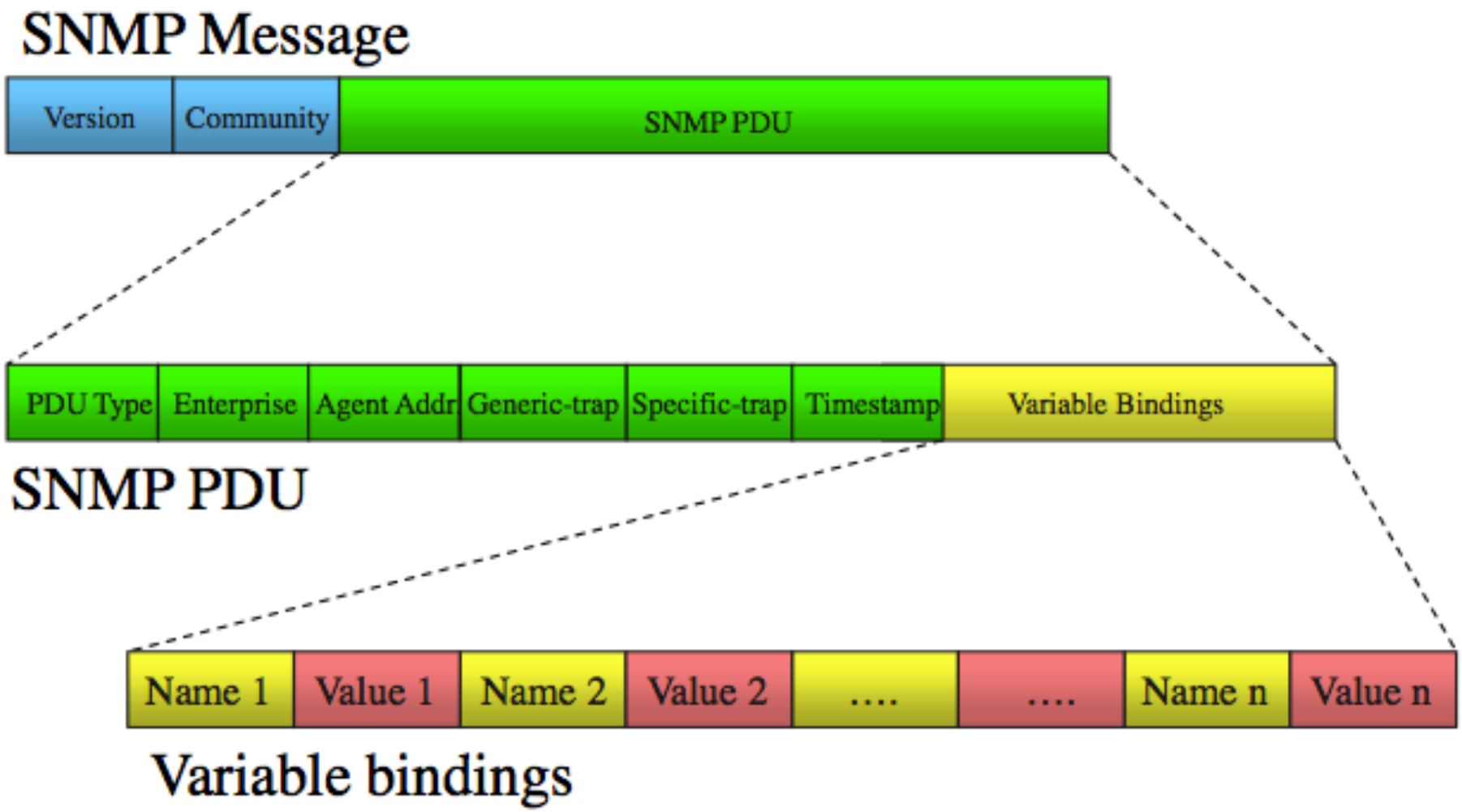
- **Version**: vale *1* per SNMPv1, 2 per SNMPv2, ecc..
- **Community**: "password" di autenticazione in chiaro
- **PDU Type**: non è un vero campo del messaggio, ma una "meta-informazione" di tipo ASN.1 del messaggio
  - cfr slide seguenti…
- **Request ID**: ID univoco per ogni richiesta; permette di appaiare le risposte (in caso di perdita di sequenza)
- **Error Status**: vale *0* nelle richieste, e nelle risposte fornisce un esito della richiesta:

noError (0)	noSuchName (2)	readOnly (4)
tooBig (1)	badValue (3)	genErr (5)

Campi messaggio 2/2

- **Error Index**:
  - vale 0 nelle richieste
  - nelle risposte, è non-nullo in caso di errore, e dà l'indice della *prima variabile* che ha causato l'errore
- **Variable Bindings** (*varbinds*): lista di coppie nome/valore
  - Nelle GetRequest e GetNextRequest il valore è nullo.
    - è quindi possibile richiedere più variabili in contemporanea
    - viene eseguita la stessa operazione (get, get-next, set) su tutte le variabili
    - permette di limitare il numero di richieste da fare e gli scambi manager-agent
    - utilizzato molto per la scansione delle tabelle...

Struttura della Trap



Campi della trap

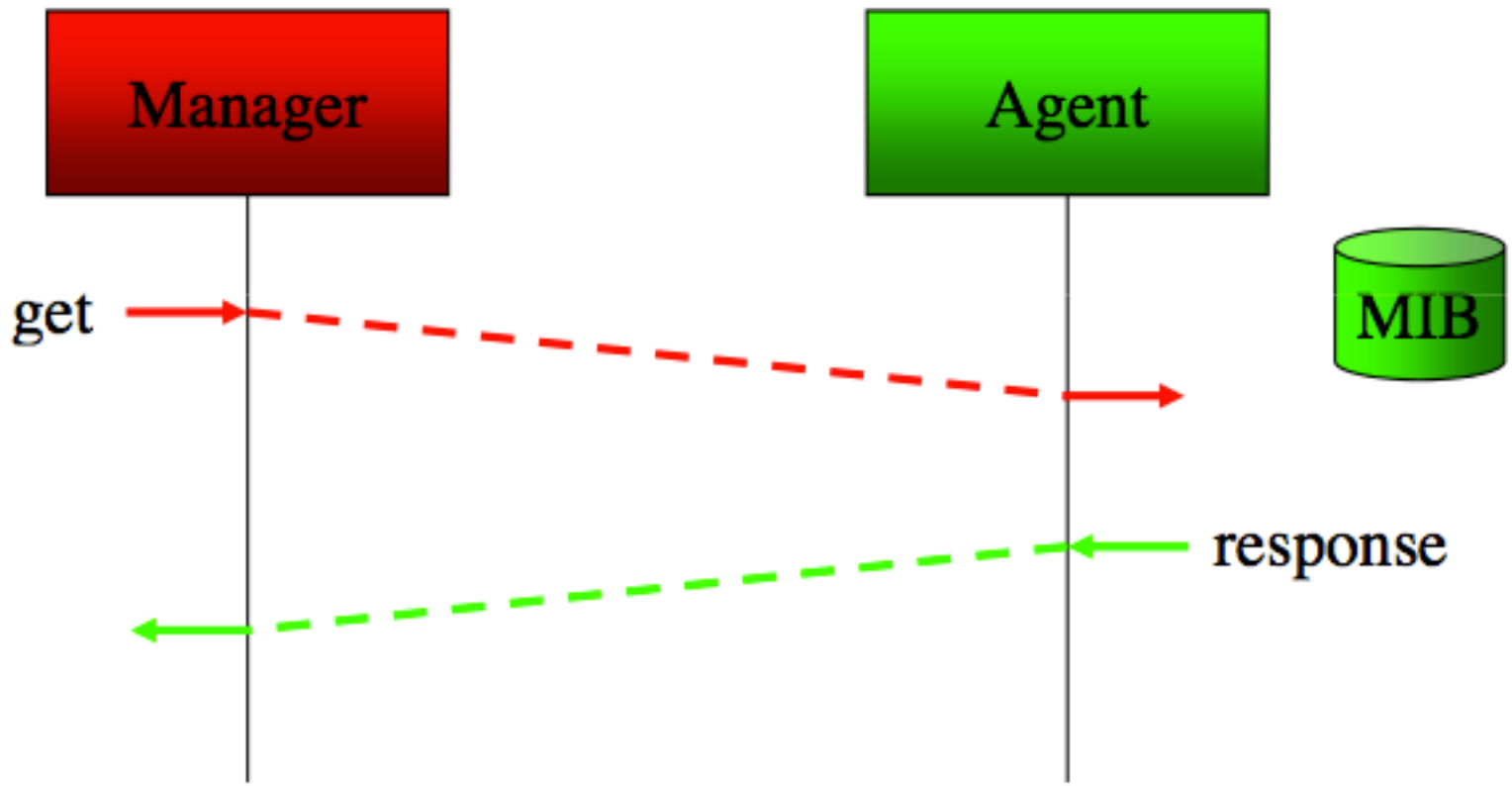
- **Enterprise**: basato sulla variabile sysObjectID
  - permette di individuare il tipo di apparato/sottosistema originario
- **Agent Address**: indirizzo IP dell'agent generatore
- **Generic Trap**: tipo di trap tra un insieme predefinito

coldStart (0)	linkDown (2)	authenticationFailure (4)
warmStart (1)	linkUp (3)	egpNeighborLoss (6)

enterpriseSpecific (6) [per le trap proprietarie – cfr campo successivo]

- **Specific Trap**: tipo di trap non standard
- **Timestamp**: indica il momento in cui è stata inviata la trap
- **Variable bindings**: come per le altre PDU

SNMP: GetRequest 1/2



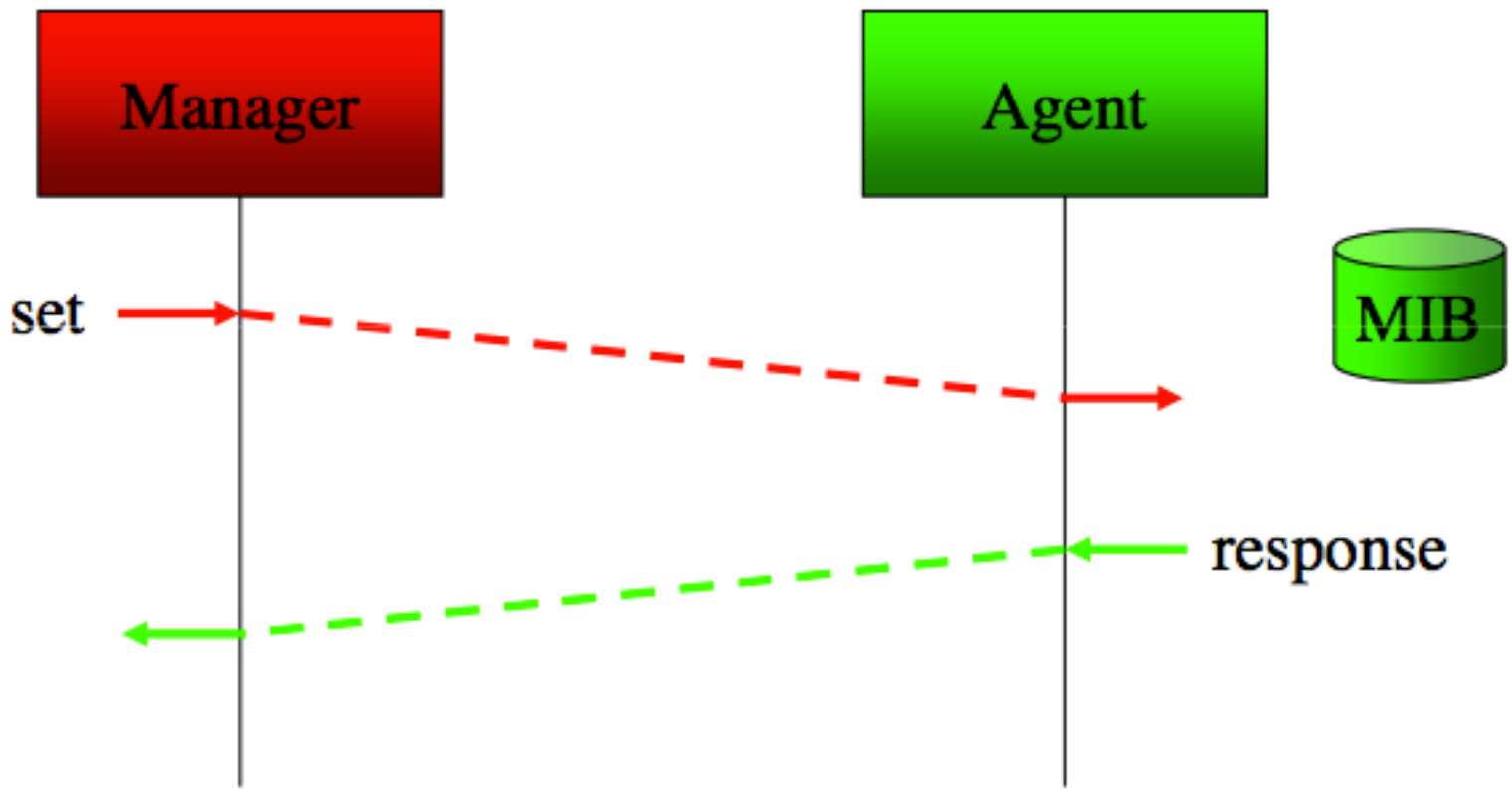
SNMP: GetRequest 2/2

Permette di richiedere il valore di una o più variabili di MIB. In questo caso i campi valore della porzione Variable Bindings sono vuote

Possibili errori:

- *noSuchName: l'oggetto non esiste o non è una foglia dell'albero*
- *tooBig: la risposta non sta nella PDU di risposta*
- *genErr: errore generico, tutti gli altri casi*

SNMP: SetRequest 1/2



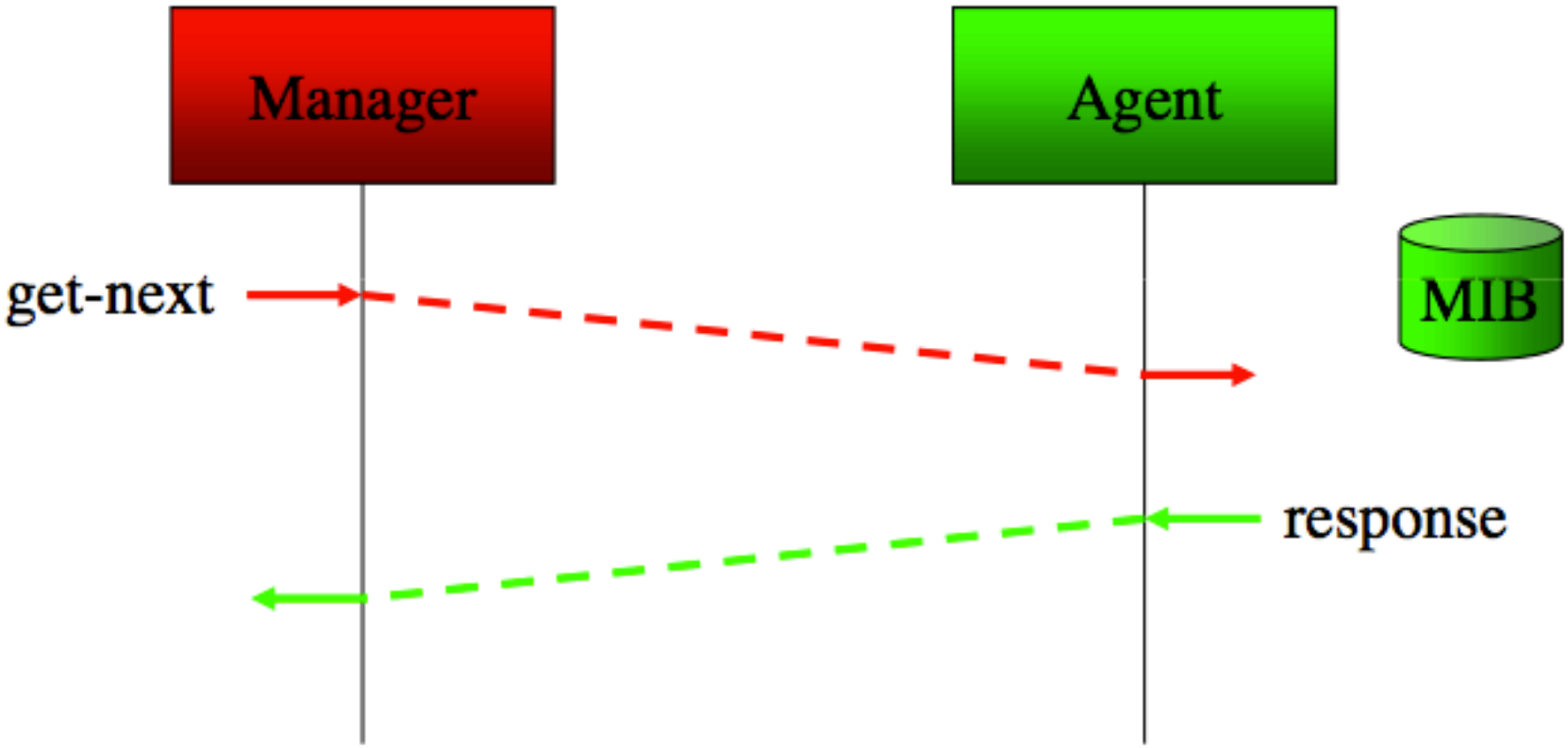
SNMP: SetRequest 2/2

Permette di assegnare un valore a istanze di variabili già esistenti o comandare azioni. In questo caso i campi valore della porzione Variable Bindings contengono I valori da settare per ogni variabile.

Possibili errori:

- *noSuchName: l'oggetto non esiste o non è una foglia dell'albero*
- *badValue: valore fornito inadeguato per il tipo*
- *tooBig: la risposta non sta nella PDU di risposta*
- *genErr: errore generico, tutti gli altri casi*

SNMP: GetNextRequest 1/2



SNMP: GetRequest 2/2

Restituisce il nome ed il valore della successiva istanza di una variabile MIB.

È usata per accedere alla struttura della MIB, e per navigare tabelle

Possibili errori:

- *noSuchName: l'oggetto non esiste o non è una foglia dell'albero*
- *tooBig: la risposta non sta nella PDU di risposta*
- *genErr: errore generico, tutti gli altri casi*

SNMP trap 1/2

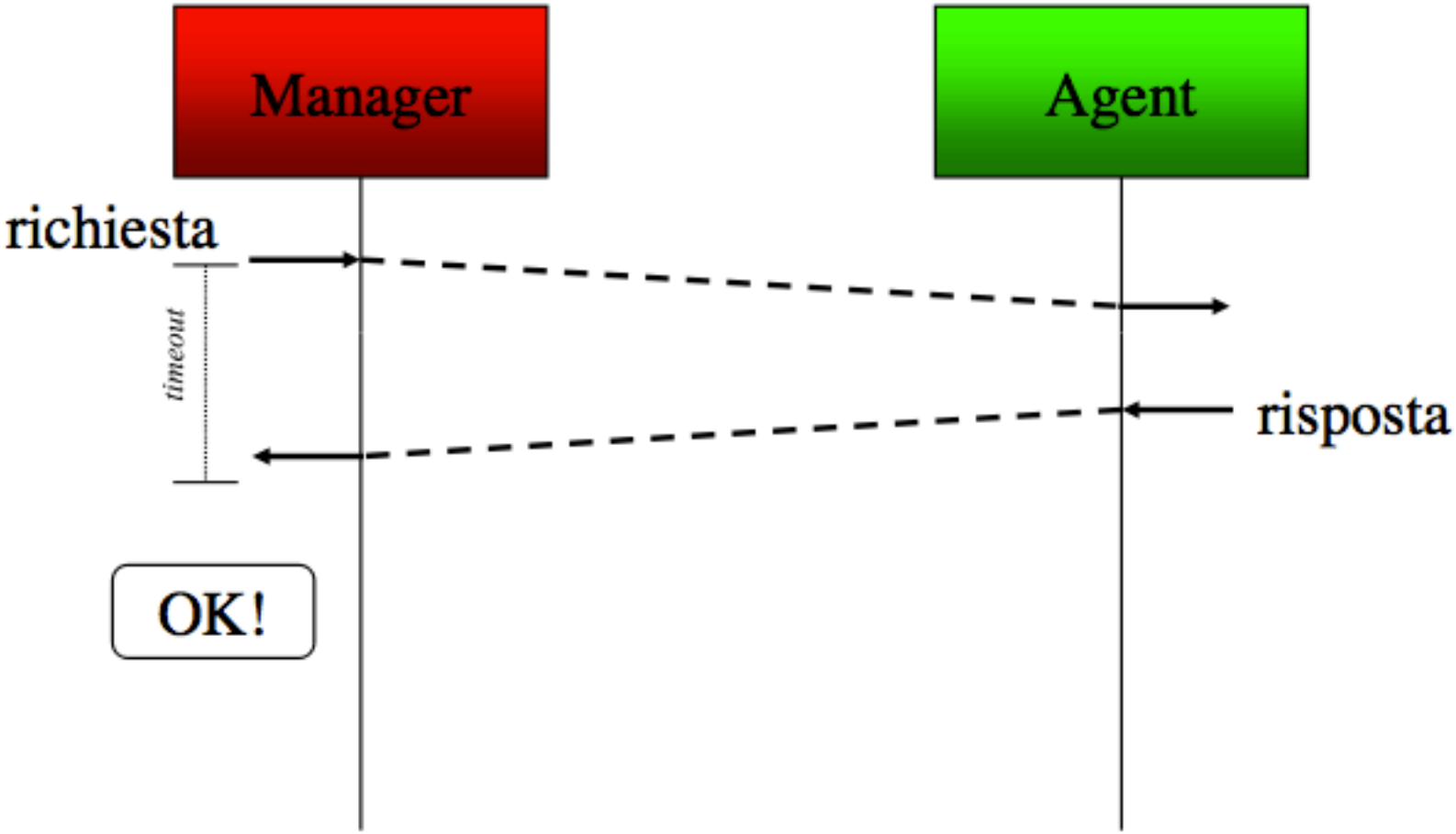
SNMP trap 2/2

- Segnala un evento
- La ricezione di una trap non è confermata (unreliable)
- Gli Agent possono essere configurati in modo da:
  - non emettere traps
  - emettere traps solo verso manager specifici

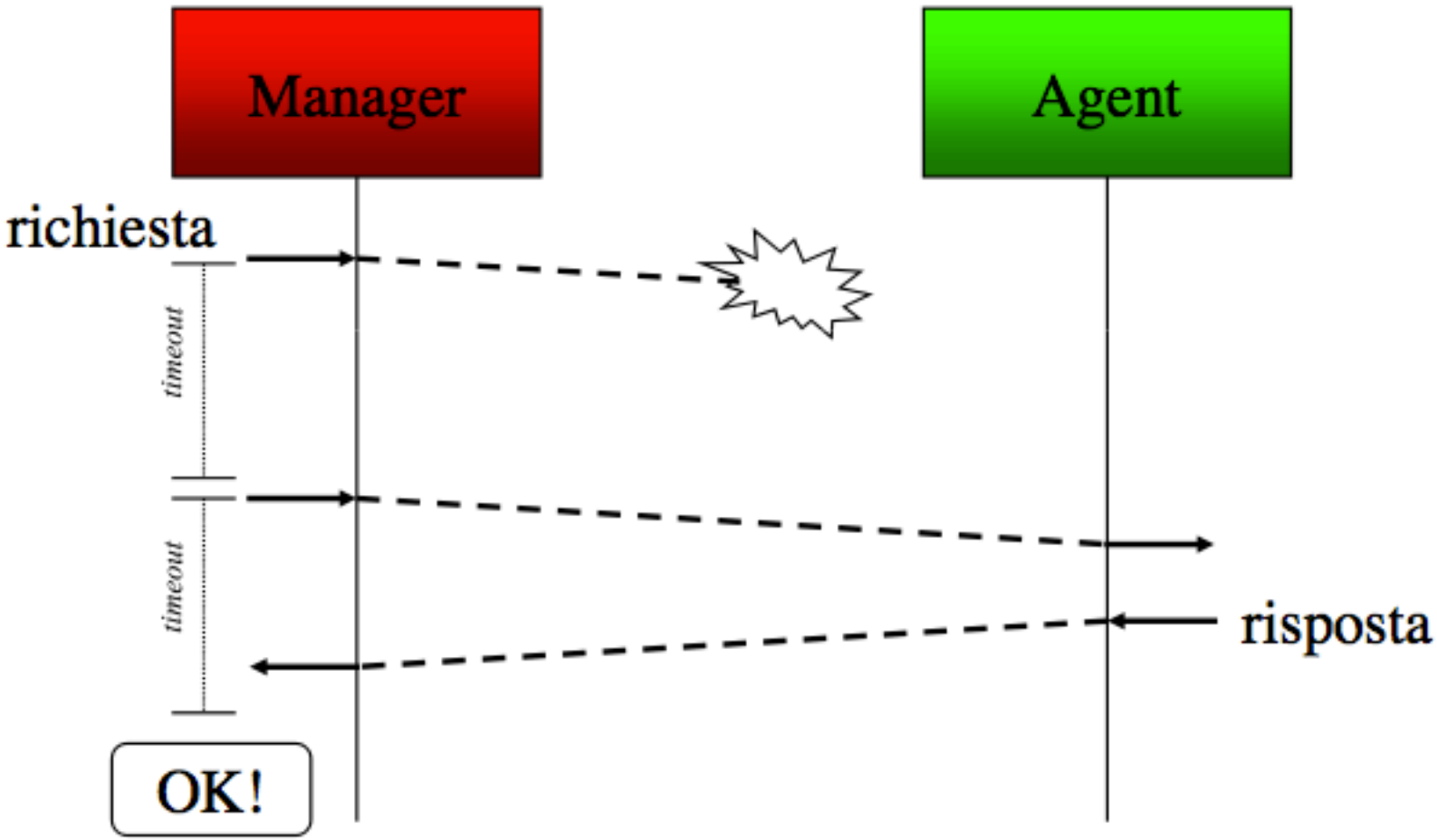
SNMP: uso di UDP

- Per la natura delle comunicazioni ("botta e riposta") - quindi senza scambio di grosse quantità di dati - UDP è preferibile:
  - Più legggero
  - Più robusto in consizioni critiche
  - Nel caso una richiesta vada persa potrebbe non aver senso rimandarla
  - Porta 161 per richieste e 162 per messaggi Trap
- UDP è *connectionless e unreliable (non affidabile):*
  - *l'invio di un messaggio non significa la garanzia della sua consegna*
  - *fatta una richiesta SNMP, la risposta arriva in maniera asincrona, senza garanzia*
- *Vanno messi in piedi meccanismi di timeout e di retry per simulare una interazione affidabile (quello che fa TCP)*

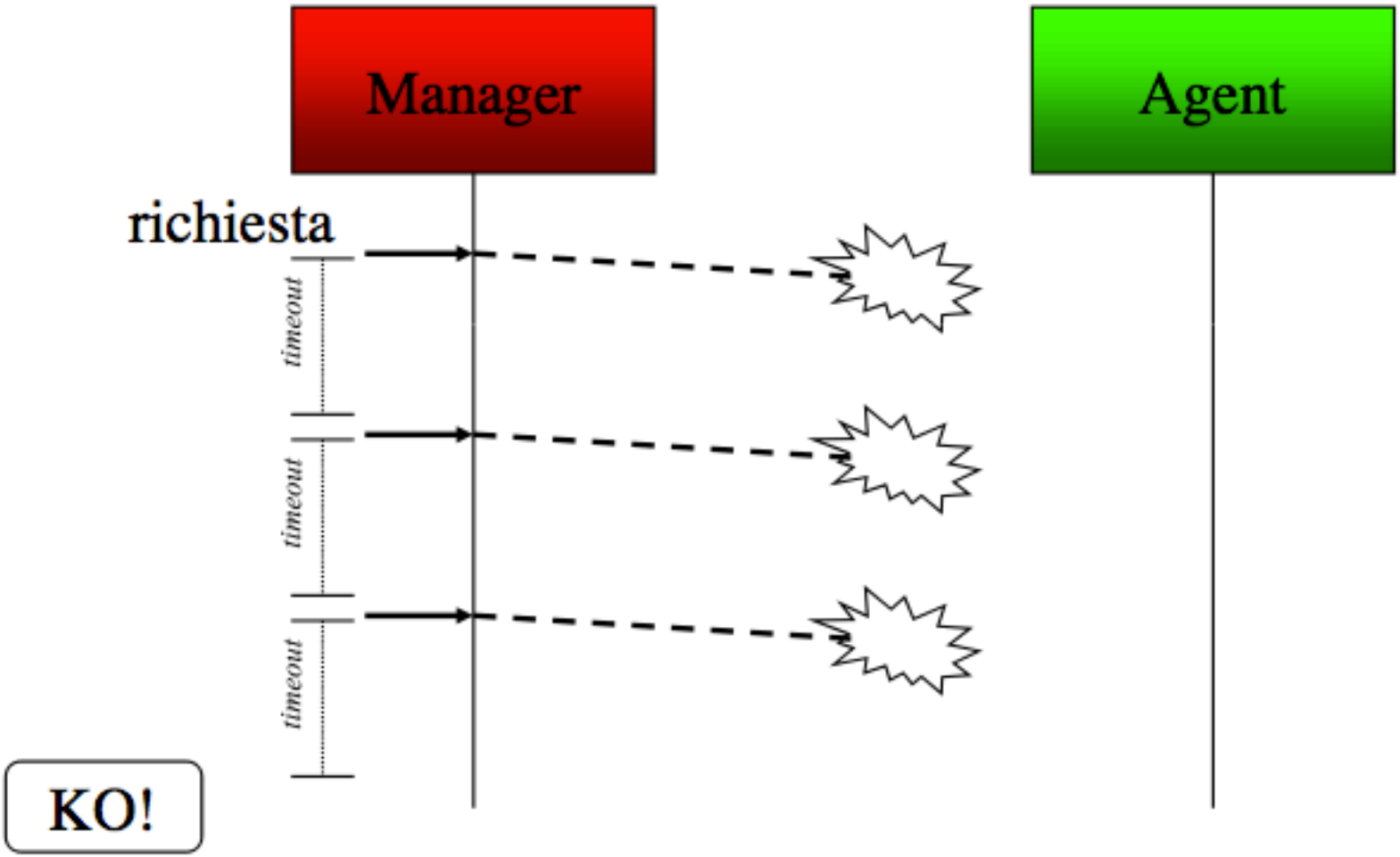
SNMP: Possibile scenario 1



SNMP: Possibile scenario 2



SNMP: Possibile scenario 3



SNMP: parametri di gestione

- Timeout: tempo trascorso prima di ritentare
  - non deve essere troppo lungo, per consentire un rinvio rapido in caso di non risposta, né troppo corto per evitare rinvii inutili
- Retry count: numero di tentativi prima di dichiarare fallita la connessione
  - non deve essere troppo basso, per dare un minimo di affidabilità, né troppo alto, per non sovraccaricare la rete di richieste

SNMPv1: Sicurezza 1/2

- La gestione della sicurezza da parte del protocollo SNMPv1 è estremamente elementare.
- Approcci più adeguati sono definiti per le versioni successive: SNMPv2 e SNMPv3 (molto meglio)
- Il concetto fondamentale è quello di *community, a cui sono associati dei diritti di accesso READ- ONLY o READ-WRITE*
- La gestione delle *community non viene specificata dagli standard ed è quindi lasciata all'implementazione. Lo standard specifica solo che la community è una stringa che va trasmessa con il messaggio SNMP*
- *La community viaggia in chiaro sulla rete*

SNMPv1: Sicurezza 2/2

Per limitare i rischi, alcune misure:

- utilizzare password non banali, e cambiare spesso
- configurare l'Agent ad inviare le trap di authentication Failure
- configurare la rete (con filtri o firewalls) per impedire il traffico SNMP al di fuori dai percorsi Manager-Agent

Nella realtà, gli apparati forniscono anche meccanismi di ACL (Access Control List), dove vanno inseriti gli indirizzi dei manager di fiducia

Maggiori dettagli "Community" SNMP

- In SNMPv1 e SNMPv2 la sicurezza veniva gestita tramite gruppi di amministrazione conosciuti come comunità.
- SNMPv3 utilizza invece per la sicurezza autenticazione con nome utente e password, insieme ad una chiave di crittografia.
- L'insieme degli apparati di rete gestiti da SNMP appartengono ad una comunità (community).
- La comunità rappresenta un identificativo che permette di garantire la sicurezza delle interrogazioni SNMP.
- Un agent SNMP risponde solo alla richieste di informazioni effettuate da una Management Station appartenente alla stessa comunità. Il valore del campo community viaggia in chiaro sulla rete.

Maggiori dettagli "Community" SNMP

- Un dispositivo può appartenere a più comunità contemporaneamente.
- I nomi di comunità sono formati da 32 caratteri e sono di tipo case sensitive.
- Esistono tre tipi di comunità:
  - monitor: permette di lavorare in sola lettura;
  - control: permette tramite gli agent SNMP di effettuare delle operazioni in lettura/scrittura sul dispositivo – richiede controllo di sicurezza;
  - trap: permette ad un agent di inviare un messaggio trap SNMP alla management station secondo la propria configurazione.

SNMPv3: sicurezza e amministrazione

cifratura: messaggio SNMP criptato con DES

autenticazione: usa Message Authentication Code (MAC). Calcola la funzione hash sul messaggio (m) con chiave segreta condivisa (k)

protezione dagli attacchi di replica: usa i nonce

controllo dell'accesso:

- L'entità SNMP conserva il database dei diritti e delle politiche di accesso per vari utenti
- Il database stesso è accessibile come oggetto gestito!

Remote Monitoring (RMON)

- Serve a controllare e misurare il traffico di rete. Fa uso di un'estensione del MIB-2 denominata RMONMIB. Contiene 9 gruppi di funzioni
- 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 1/2

- 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 statistichepresenti 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 2/2

- 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

Perché occore una codificare per i dati

- Vogliamo far comunicare dispositivi e sistemi diversi.

D: una copia perfetta dei dati da memoria a memoria può risolvere "il problema della comunicazione"?

R: non sempre!

```
struct {
   char code;
    int x;
    } test;
test.x = 259;
test.code='a'
```

test.code	a
test.x	00000001
	00000011

Formato host 1

test.code	a
test.x	00000011
	00000001

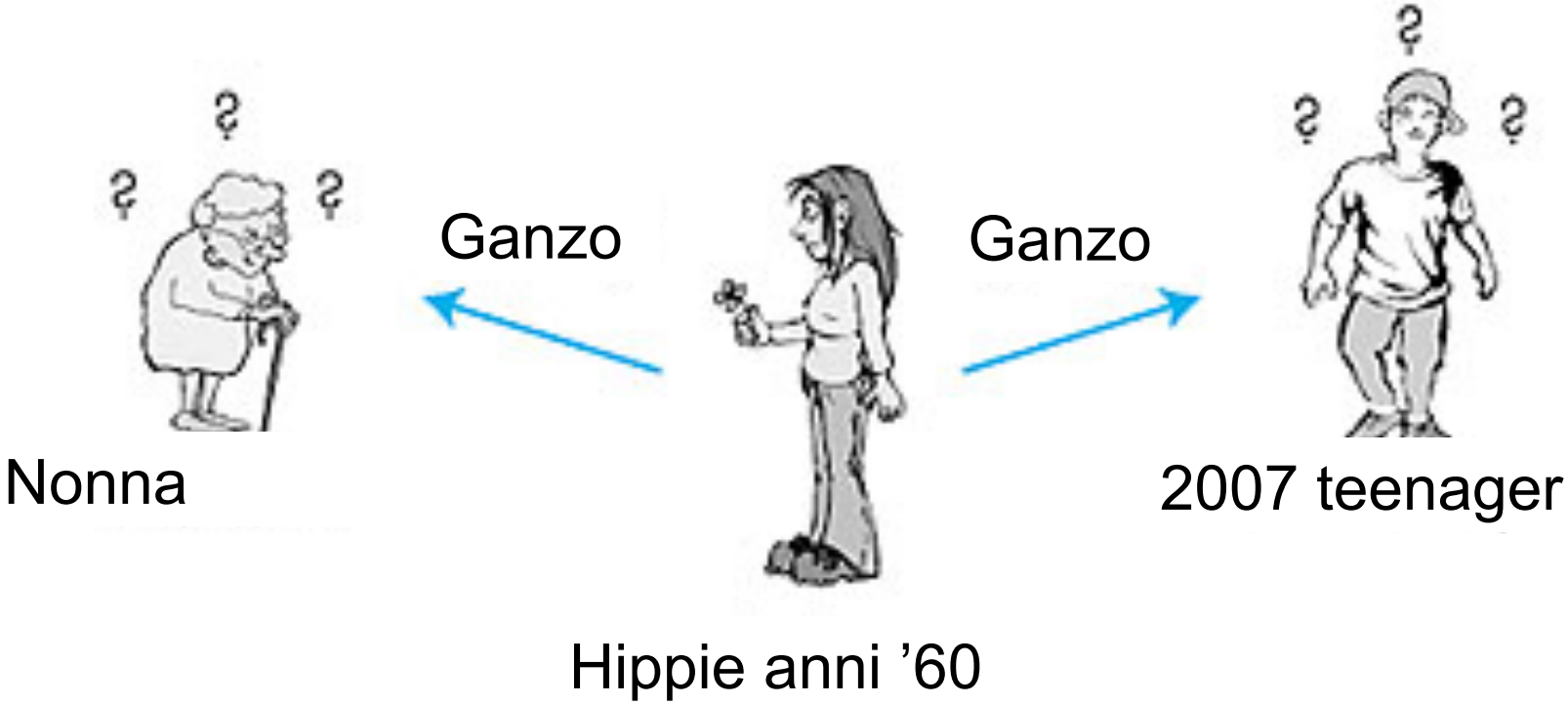
Formato host 2

Host1 ed host2 memorizzano i dati con ordinamenti diversi:

byte più significativo che precede il secondo (host1): big-endian

byte più significativo che segue il secondo (host2): little-endian

Stesso problema nella vita reale



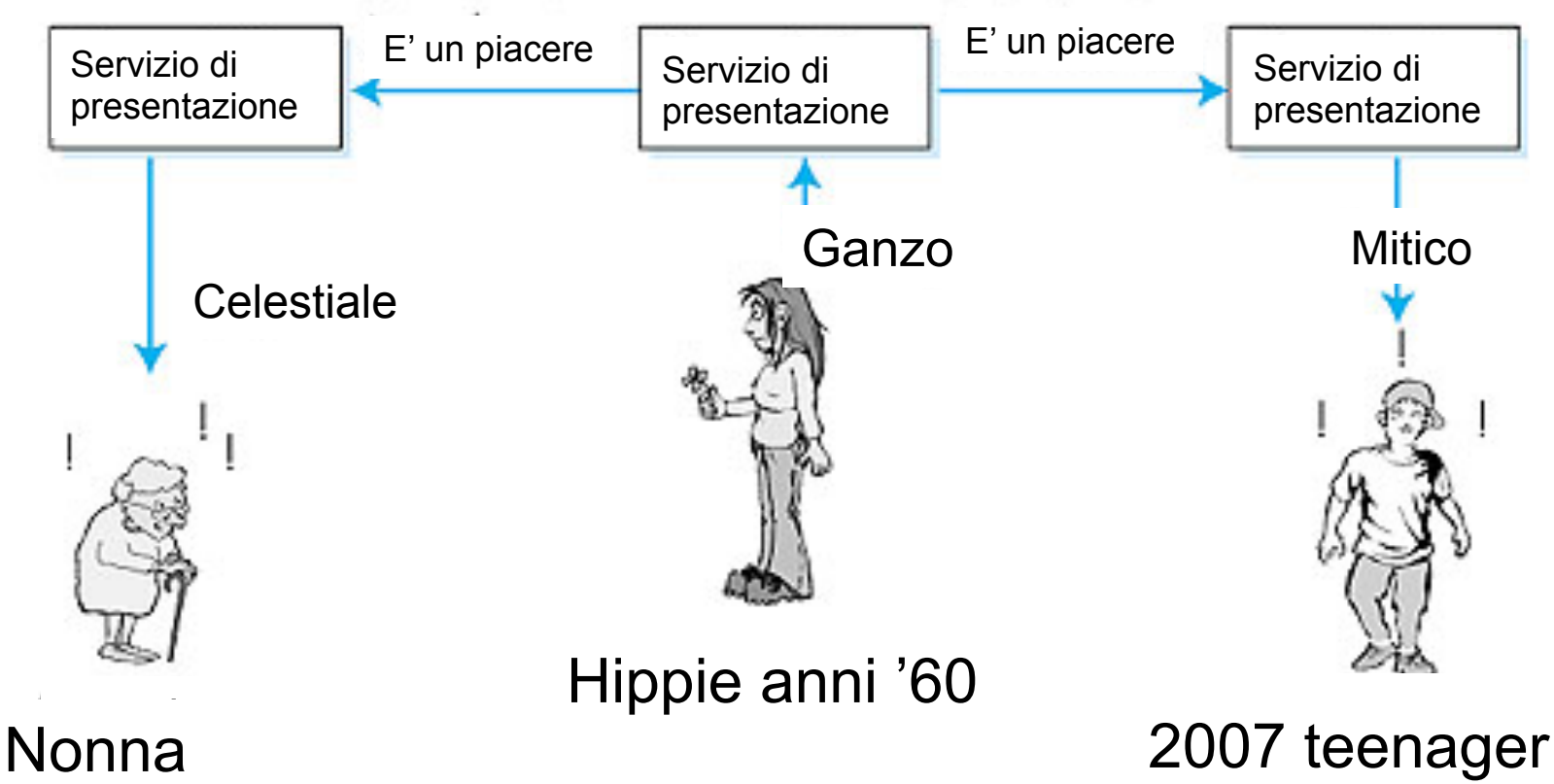
Possibili soluzioni

Il mittente impara il formato del destinatario. Il mittente traduce il formato in quello del destinatario. Il mittente trasmette.

Il mittente trasmette. Il destinatario impara il formato del mittente. Il destinatario traduce nel suo formato.

Il mittente traduce in un formato indipendente dall'host e trasmette. Il destinatario traduce nel suo formato. (Soluzione utilizzata)

Soluzione al problema della presentazione



Codifica dei nomi ASN.1:

Abstract Syntax Notation One

Standard ISO X.680

Largamente utilizzato in Internet

Tipi di dati definiti, costruttori di oggetti

come SMI

BER: Basic Encoding Rules (regole base per la codifica)

- specifica come trasmettere gli oggetti di dati definiti secondo ASN.1
- ogni oggetto trasmesso ha una codifica TLV (Tipo, Lunghezza, Valore)

Codifica TLV

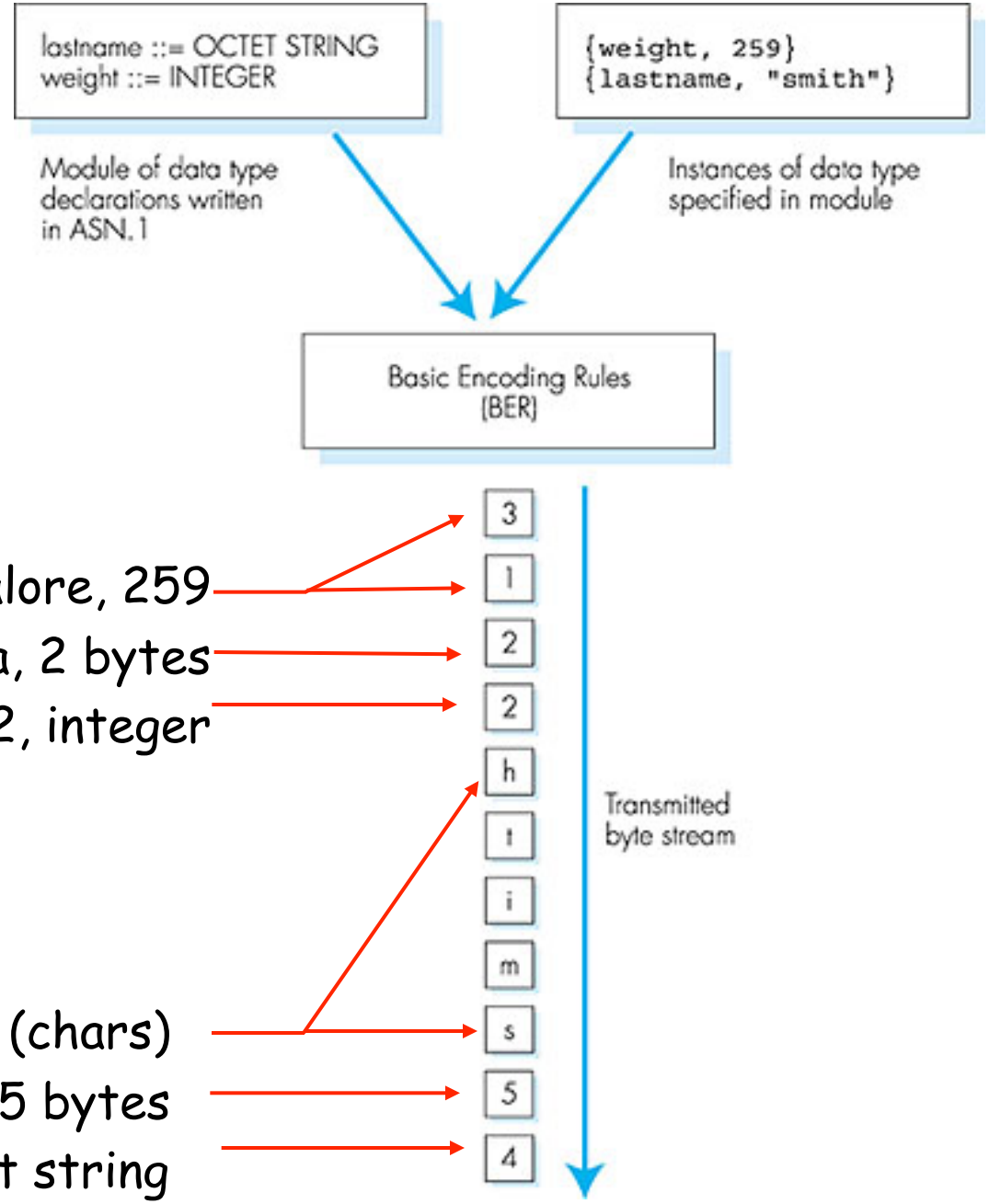
Idea: i dati trasmessi sono auto-identificati

- T: Tipo di dati, uno dei tipi definiti da ASN.1
- L: Lunghezza dei dati in byte
- V: Valore dei dati, codificati secondo lo standard ASN.1

Etichetta	Tipo
1	Boolean
2	Integer
3	Bitstring
4	Octet string
5	Null
6	Object Identifier
9	Real

Esempio Codifica TLV

Trasmsettiamo stringa "smith" seguita dal valore 259



Valore, 259

Lunghezza, 2 bytes

Tipo=2, integer

Valore, 5 octets (chars)

Lunghezza, 5 bytes

Tipo=4, octet string

Network management: summary

- Gestione della rete
  - estremamente importante: 80% del "costo" della rete
  - ASN.1 per la codifica dei dati
  - SNMP protocolo usato per scambio di informazioni
- Gestione della rete: più arte che scienza
  - Cosa va misurato/monitorato
  - Come reagire in caso di guasti?
  - Come mettere in relazione e filtrare segnali di allarme e malfunzionamenti?

Prodotti commerciali e opensource

Il mercato oggi propone numerosi prodotti di System & Network Management. Tra le famiglie più complete troviamo:

1. **OpenView** di HewlettPackard,
2. **Tivoli** di IBM,
3. **SMS** di Microsoft.

Alternativa OpenSource e Freeware: **MRTG** (Multi Router Traffic Grapher).

Attualmente utilizzata da diverse Università e centri di ricerca. Sono disponibili sulle principali piattaforme Unix e NT.

La scelta non è ovviamente facile, poiché i criteri sono dipendenti dalle reali necessità dell'azienda

Domande?