Introduzione al protocollo SNMP
Introduzione

SNMP (*Simple Network Management Protocol*) è un protocollo a livello di applicazione definito per introdurre una semplice architettura per la gestione di reti basate sulla suite di protocolli **TCP/IP**. Tale protocollo definisce le modalità di scambio di informazioni tra apparecchiature di rete, consentendo agli amministratori di tenere sotto controllo le performance della rete e di accorgersi in tempo reale del manifestarsi di malfunzionamenti.

Attualmente il protocollo presenta tre definizioni successive: dalla versione 1 alla versione 3 (SNMPv1, SNMPv2, SNMPv3). Le versioni più recenti introducono nel protocollo alcune nuove funzionalità e correzioni, soprattutto relativamente alla sicurezza.

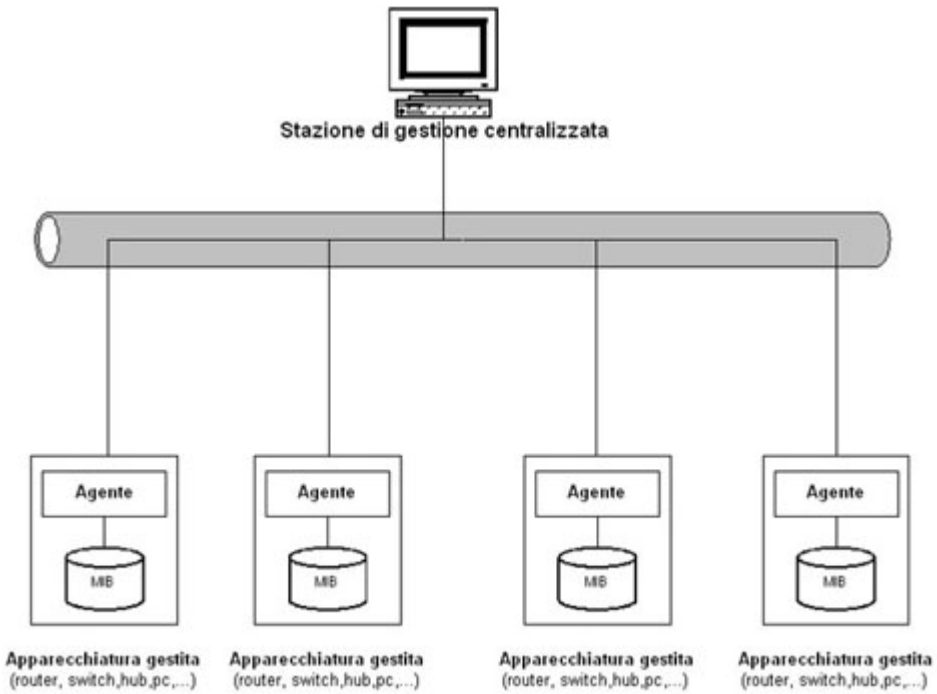
Il protocollo SNMP è attualmente quello più diffuso per la gestione delle reti di calcolatori ed è supportato da praticamente tutti i produttori di hardware ed apparecchiature di rete.

Nei paragrafi successivi si affronterà innanzitutto l'architettura prevista dalla versione 1 del protocollo.

Architettura

L'architettura di cui il protocollo SNMP fa parte, è detta *Internet Network Management Framework* (NMF).
L'architettura consente di gestire degli **elementi di rete** (che sono apparecchiature di rete come **router**, **switch**, **hub**, computer,...) usando degli **agenti**, cioè moduli software che risiedono sulle apparecchiature da gestire. Tali agenti comunicano con una **stazione di gestione centralizzata** (*Network Management Station*) che, interagendo con i primi, può leggere o scrivere informazioni e raccogliere eventuali segnalazioni di errore.
Le informazioni o caratteristiche che è possibile gestire per una particolare apparecchiatura, mediante il protocollo SNMP, sono dette ***Management Objects***. L'insieme di questi oggetti costituisce un'astrazione di database detta ***Management Information Base*** (**MIB**).

Uno schema logico di tale architettura è riportato di seguito.



SNMP definisce lo standard di comunicazione tra la stazione di management centralizzata e gli agenti, per il trasferimento delle informazioni da e verso le apparecchiature.

Le operazioni possibili sono:

- **Read**: è possibile leggere i valori mantenuti dalle apparecchiature gestite, per poterle monitorare;
- **Write**: è possibile scrivere variabili mantenute nella periferica per controllarne il funzionamento;
- **Traversal operations**: servono alla stazione di gestione centralizzata per capire quali sono le informazioni gestite dalla periferica;
- **Trap**: sono messaggi inviati in modo asincrono dalla periferica alla stazione di gestione centralizzata, per segnalare un malfunzionamento e quindi permettere all'operatore di accorgersene in tempo reale.

MIB

Nel Management Information Base (MIB) sono descritte tutte le informazioni che è possibile gestire con il protocollo SNMP, per una certa periferica. Un MIB ha un'organizzazione ad albero dove i dati costituiscono le foglie. Ciascun oggetto all'interno del MIB viene identificato mediante un OID (Object IDentifier), costituito da numeri interi organizzati gerarchicamente (Es. 1.3.6.1.4.1.9.2.2.1.51).

La struttura attuale del MIB presenta tre ramificazioni principali definite da organismi di standardizzazione internazionali, rispettivamente CCITT (*Consultative Committee for International Telegraph and Telephone*), ISO (*International Organization for Standardization*) ed una congiunta ISO/CCITT.

La gerarchia del MIB è estensibile ed anche i produttori di hardware possono definire delle proprie ramificazioni per potere includere particolari caratteristiche dei loro prodotti.

SMI

La ***Structure of Management Information (SMI)*** definisce le strutture dati usate dal protocollo SNMP.
In particolare ne definisce il nome, che segue la struttura gerarchica descritta nel paragrafo precedente, la sintassi e la codifica.

La sintassi definisce il tipo di dati, che per SNMP è un sottoinsieme dell' ISO/OSI *Abstract Syntax Notation 1* (ASN.1).
Sono definiti tipi di dato primitivi e non primitivi.

I tipi primitivi sono:

- ***Integer***: valori interi positivi o negativi incluso lo zero;
- ***Octet String***: definisce insiemi ordinati di byte;
- ***Object Identifier***: definisce un valore unico secondo le specifiche ASN.1.
- **NULL**: definisce il tipo nullo.

Tra i tipi non primitivi abbiamo:

- **Indirizzi di rete**: rappresentano un indirizzo IP;
- ***Counter***: sono interi non negativi che possono solo essere incrementati fino ad un valore massimo, dopo il quale ritornano a zero;

- ***Gauge***: è un intero non negativo che può essere sia incrementato che decrementato;
- ***Time Tick***: rappresenta l'intervallo di tempo trascorso a partire da un certo evento;
- ***Opaque***: può contenere un qualsiasi valore, viene usato per passare informazioni che non seguono strettamente le definizioni dei tipi della SMI.

La codifica invece descrive come le informazioni associate agli oggetti sono formattate per essere trasmesse sulla rete. La codifica SMI è descritta nella specifica ISO detta *Basic Encoding Rules* (BER).

Versioni successive del protocollo

La prima versione del protocollo (SNMPv1) presentava alcuni problemi che sono stati in parte risolti con le versioni successive.
SNMPv1 non presentava alcuna implementazione di funzionalità orientate alla sicurezza e ciò ne limitava l'impiego in reti di grandi dimensioni, inoltre comportava un grosso sforzo di risorse in termini di CPU e banda per l'acquisizione di quantità elevate di informazioni, risultando problematico dal punto di vista delle performance.
SNMPv2 viene quindi introdotto per tentare di risolvere queste problematiche. Oltre ad introdurre nuovi tipi di dato alla SMI, aggiunge operazioni che permettono il reperimento di informazioni multiple con meno sforzo in termini di risorse impiegate e permette l'acquisizione delle informazioni a più livelli, decentralizzandola e quindi rendendola più efficiente. Migliora anche la gestione degli errori.
SNMPv2 è incompatibile con SNMPv1 e per questo motivo viene introdotto il Proxy Agent che ha il compito di supportare le entità che conoscono solo la vecchia versione del protocollo.

SNMPv2 però non risolve tutti i problemi di SNMPv1 e ne sono state implementate tra l'altro diverse versioni.
Viene quindi introdotta la versione 3 del protocollo (SNMPv3) per unificare le diverse implementazioni e risolvere i problemi delle precedenti. Viene adottata un'architettura modulare dove Manager ed Agenti sono genericamente detti entità SNMP, senza una netta distinzione tra loro. Queste entità SNMP hanno funzionalità di invio e ricezione di messaggi, oltre che di autenticazione, sicurezza e crittografia.
Ogni entità è costituita da moduli e, soprattutto, moduli di diverse versioni possono coesistere, risolvendo in maniera trasparente la coesistenza dei protocolli SNMPv1 e SNMPv2.
Il protocollo diventa naturalmente estendibile con l'aggiunta di nuovi moduli.

Conclusioni

Questa breve trattazione ha lo scopo di introdurre i sistemi di gestione delle reti di calcolatori, facendo vedere che esistono potenti strumenti per il monitoraggio della rete. È importante sottolineare che c'è la possibilità di essere allertati in maniera automatica ed in tempo reale del verificarsi di malfunzionamenti. SNMP è lo standard di fatto per quanto riguarda i sistemi di gestione delle reti ed è il protocollo più largamente diffuso in questo ambito.

I **riferimenti bibliografici** consentono di svolgere autonomamente ulteriori attività di approfondimento.