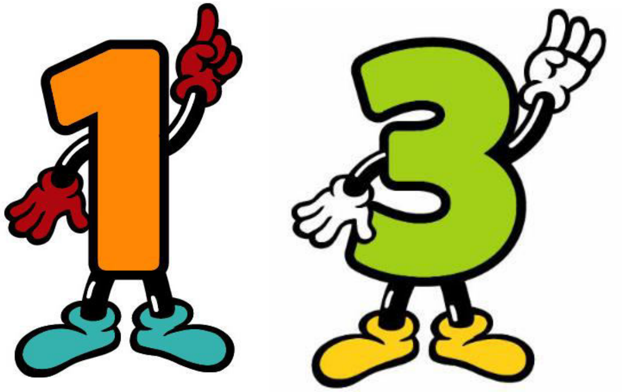


Network Management
(SNMP)

Networking Monitoring

Network Management

Network Management System (NMS)

Manager, Managed Device & Agent

Network Management Protocols

Simple Network Management Protocol (SNMP)

Management Information Base (MIB)

SNMP Commands

SNMP Versions

Make sure that the network is up and running.

So

Monitor it!

Waite a minute.
There is more!

No such thing as **100% uptime**

Only 45 minutes of downtime a month!

Planned maintenance

Baselining

What is normal for your network?

Load on links
Percent usage of resources
Dropped data
Reported errors or failures

Network Management

Process of operating/configuring, monitoring (situations in which computers violate policies) , debugging and controlling the network
to
Ensure it works as intended and provides value to its users (maximize its efficiency and productivity)

Network Management?

Know when to upgrade
e.g. Is your bandwidth usage too high? Is the equipment too old?

Keep an audit trace of changes
e.g. record all changes

Accounting
e.g. track usage of resources

Know when you have problems
e.g. Stay ahead of your users!

Small networks with only a few devices confined to a single location

Network engineers can individually inspect devices and check for anomalies

Large networks with a number of devices increases

Manual device monitoring becomes increasingly difficult

Manually monitoring several servers, routers and printers can be time consuming

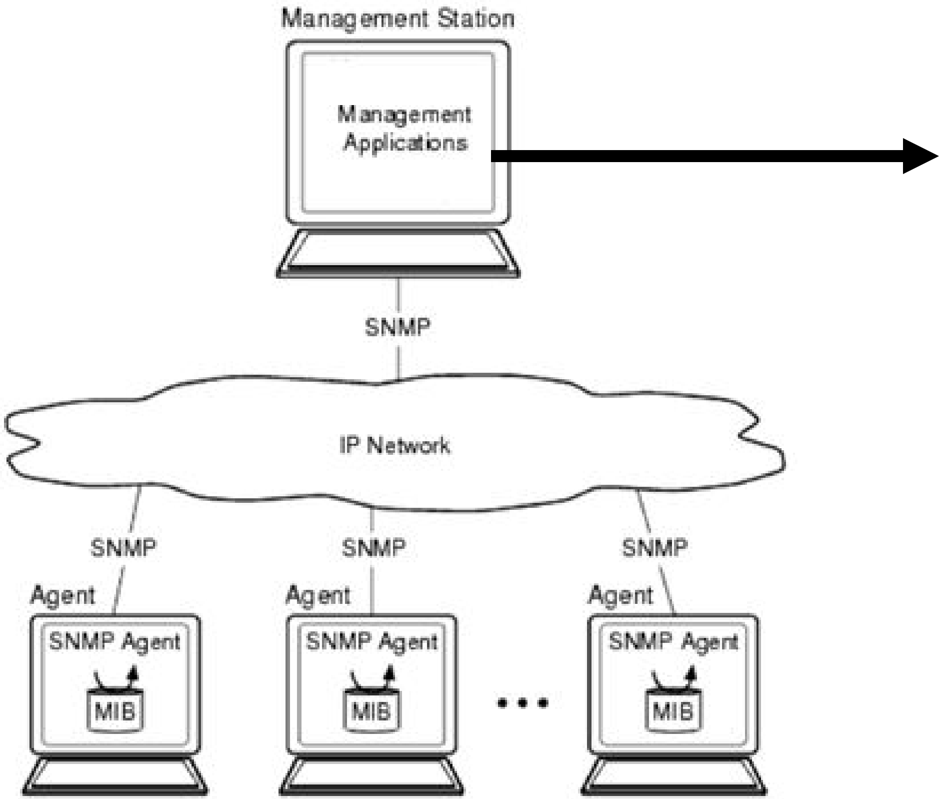
Only logical to automate this task by implementing a **Network Management System (NMS)**

Network Management System (NMS)

Application on a system that monitors and controls the **Managed Devices** through the agent using **SNMP commands**

Network management software uses SNMP to communicate with **Software Agents** on **Managed Devices**

Allow an IT professional to supervise the individual components of a network within a larger network management framework.



Performance

- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

Net Management

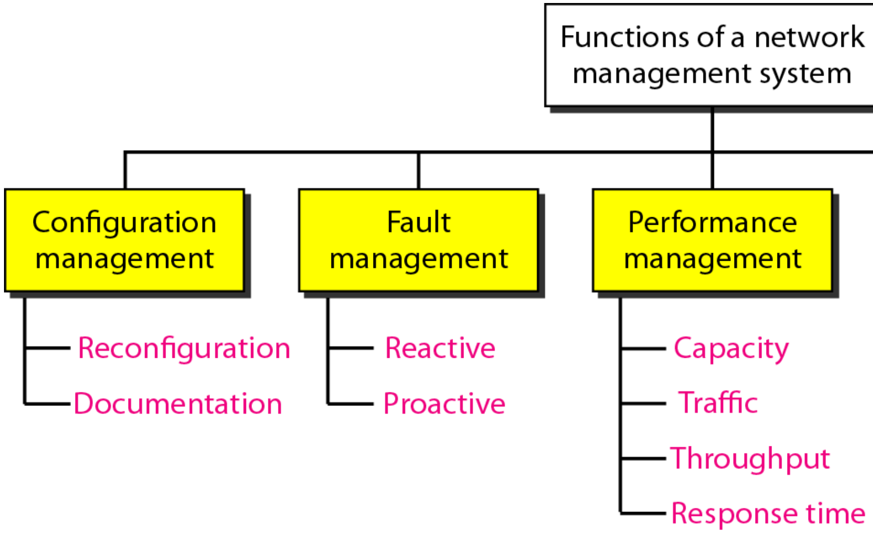
- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix

Change Management

- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle



Reconfiguration: H/W, S/W & User Reconfiguration

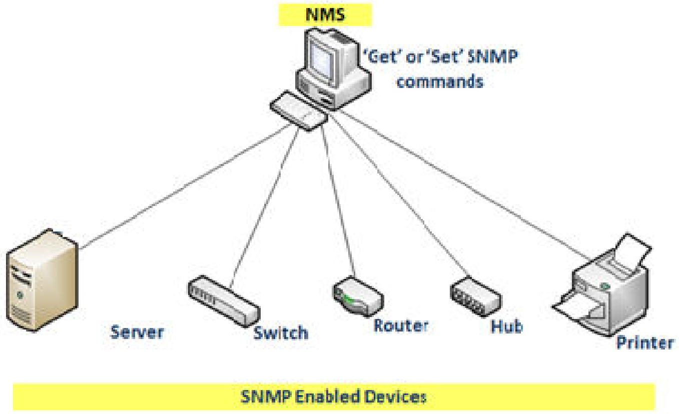
Documentation: Every change is documented for h/w (type, serial number, vendor), s/w (version, license agreement), and user accounts (privil eges)

Reactive: Handles short-term solutions to faults (Detecting → Isolating →Correcting →Recording faults)

Proactive: Tries to prevent faults from occurring

Manager

Software program running on a workstation or larger computer
Communicates with agent processes that run on each device being managed/monitored.



Manager polls the agents making requests for information
Agents respond when asked with the information requested.

Managed Device

Node in the network that requires some form of monitoring/management supports SNMP
e.g. routers, switches, firewall, hubs, printers, servers, wireless access points or workstations.

Agent

Software that is part of the monitored device.
An agent has access to the MIB (management information database) of the device
Allows NMS systems to read and write to the MIB.

Device being managed **maintains control and status information** that a manager can access.

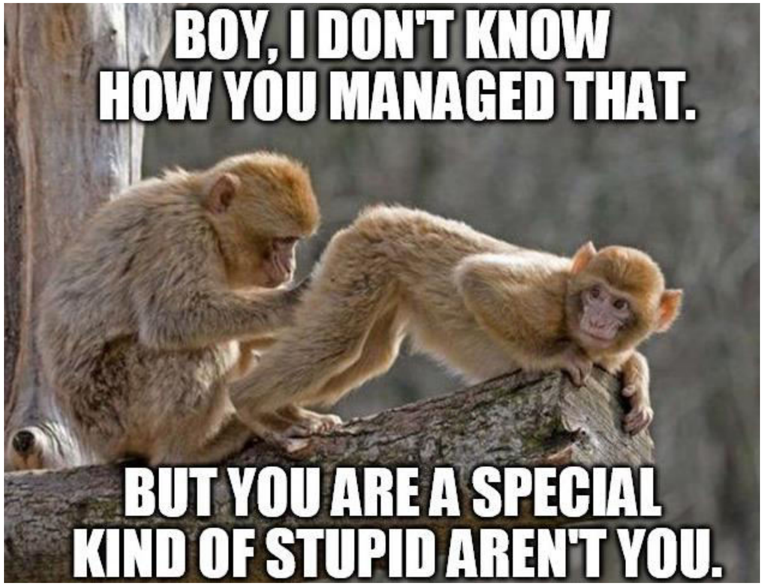
↓

Router

Keeps statistics on the status of its network interfaces, counts of incoming and outgoing packets, dropped datagrams, and error messages.

Modem

Keeps statistics about the number of bits (or characters) sent and received



Network Management Protocols

Simple protocol defines common data formats and parameters and allows for easy retrieval of information

Complex protocol adds some change capability and security

e.g. SNMP (Simple Network Management Protocol)

Advanced protocol remotely executes network management tasks

e.g. CMIS/CMIP (Common Management Information Services/Common Management Information Protocol)

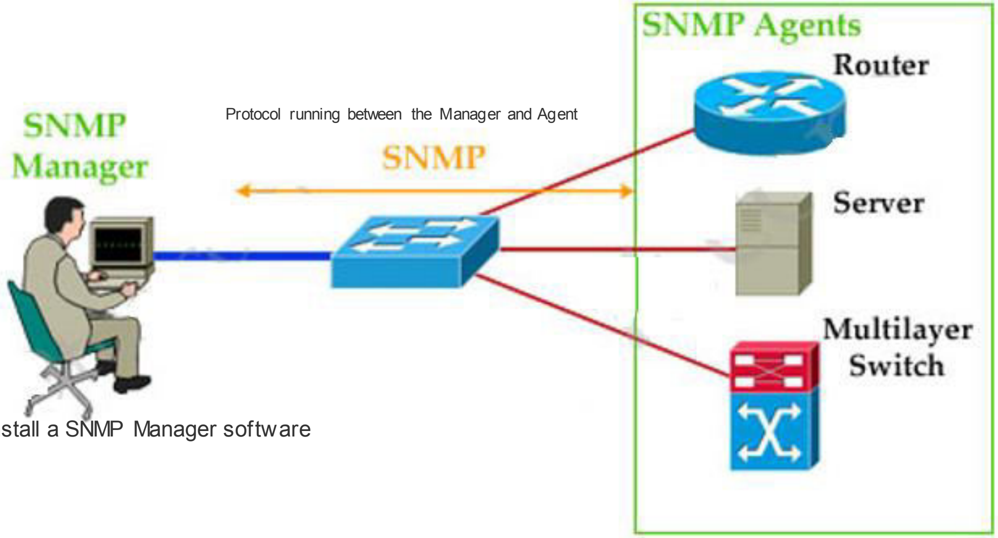
Network Management Protocols specify communication between

⬇

Network management application running on the manager’s computer

+

Network management agent executing on a managed device

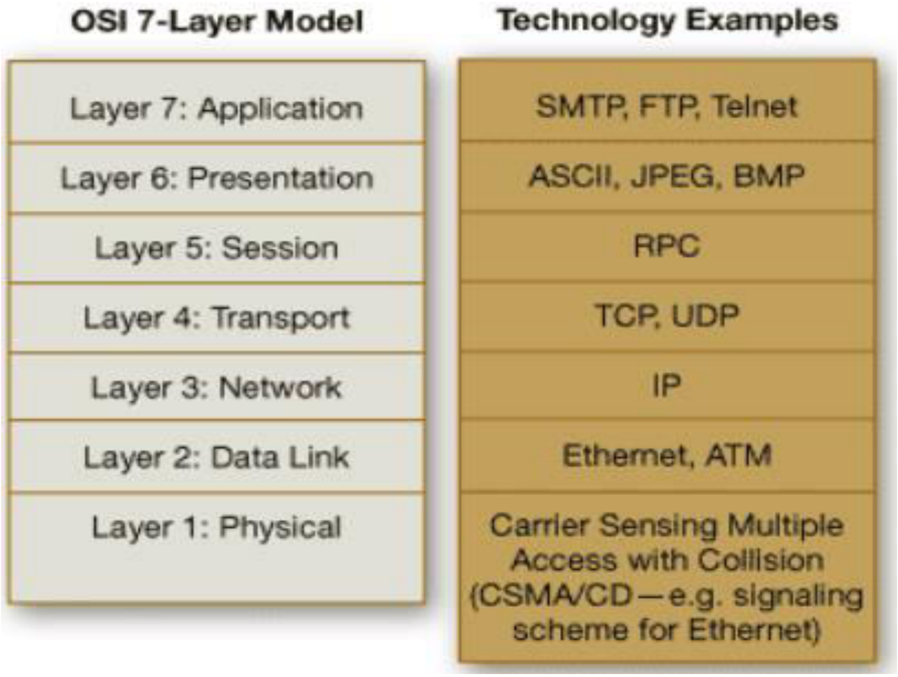


Protocol running between the Manager and Agent

Install a SNMP Manager software

Run SNMP Agent on all of them

Simply, manager and the managed system converse using Simple Network Management Protocol (SNMP).



OSI 7-Layer Model	Technology Examples
Layer 7: Application	SMTP, FTP, Telnet
Layer 6: Presentation	ASCII, JPEG, BMP
Layer 5: Session	RPC
Layer 4: Transport	TCP, UDP
Layer 3: Network	IP
Layer 2: Data Link	Ethernet, ATM
Layer 1: Physical	Carrier Sensing Multiple Access with Collision (CSMA/CD—e.g. signaling scheme for Ethernet)

Simple Network Management Protocol (SNMP)

Standard TCP/IP protocol for network management i.e. most commonly used protocol for managing network devices

Application layer protocol

Provides a message format for communication between managers and agents

Reads and changes the status (values) of objects (variables) in SNMP packets.

Current version *SNMPv3*.

I ♥ SNMP

Uses of SNMP

Monitoring traffic flowing through the device

Detecting and notifying faults encountered on network devices

Collecting device performance data over long periods and identifying trends

Remotely configuring network devices

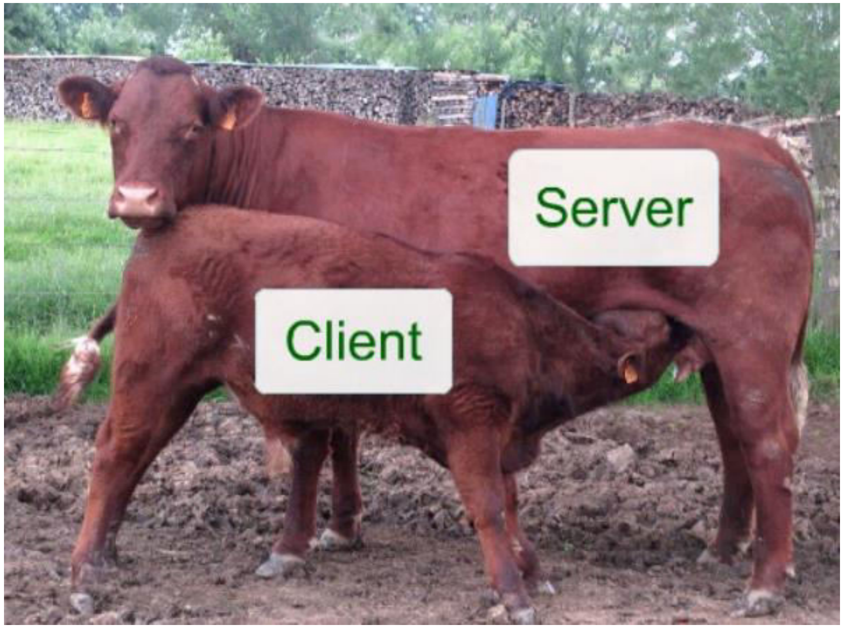
Remotely accessing and controlling network devices

Does not specify exactly which data can be accessed on which devices.

SNMP Model defines two entities, which works in a client-server mode

Client part is the **SNMP manager** in charge of the data collection and display

SNMP server is called a **SNMP agent** and is located on the device to monitor.



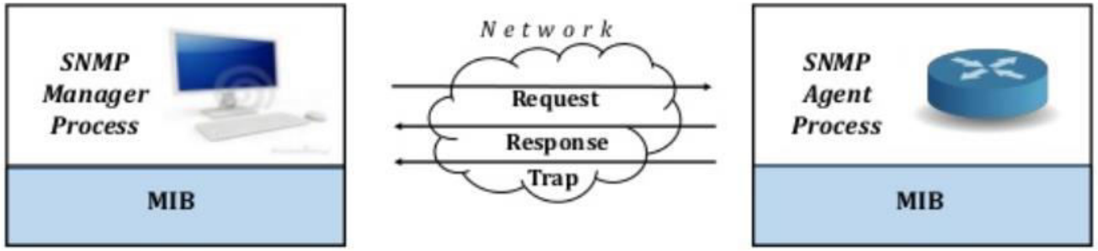
Components of SNMP

SNMP Managers: s/w that manages the n/w & queries managed device via polling

SNMP agents: small piece of code (SNMP s/w) on managed device which gathers/sends data about the device in response to a request from the manager

Management Information Bases (MIBs): collection of network information

SNMP protocol: manage network resources with a few commands.

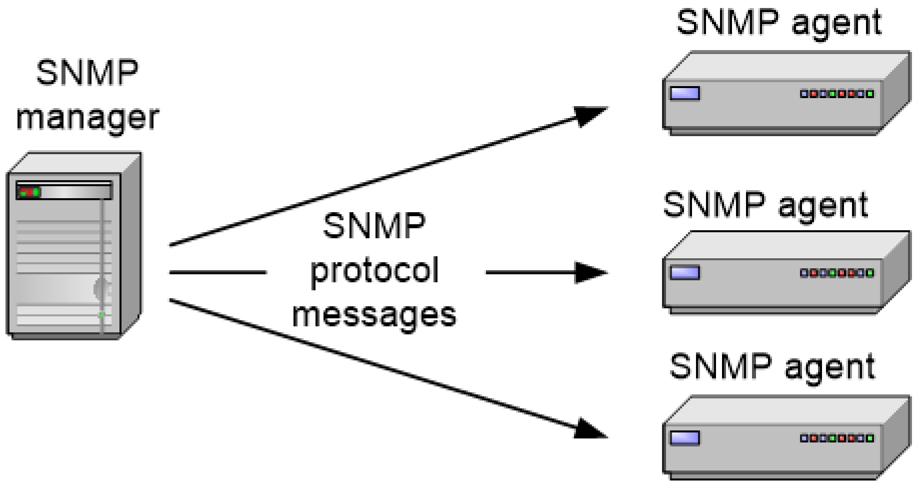


Management with SNMP is based on 3 basic ideas

A manager checks an agent by requesting information.

A manager forces an agent to perform a task by resetting values in the agent database **(MIB).**

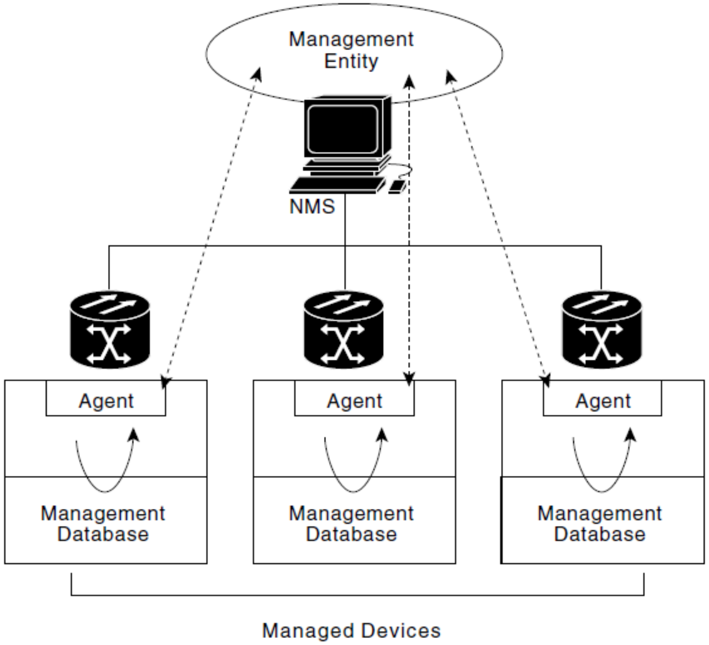
An agent contributes to the manager by warning for an unusual situation.



Network devices make use of a data store called the **Management Information Base (MIB).**

All SNMP compliant devices contain an MIB that consists of information on valid attributes of a device.

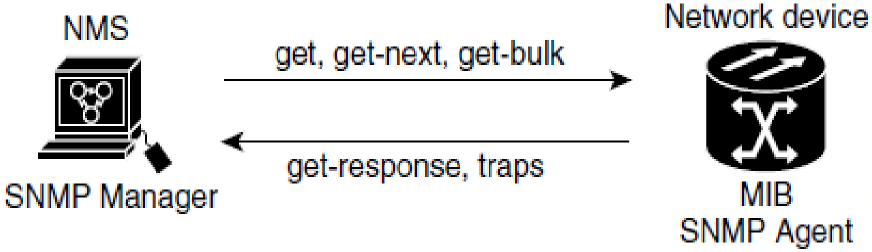
Some attributes in the MIB are fixed, while others are dynamic values calculated by the Network Management System



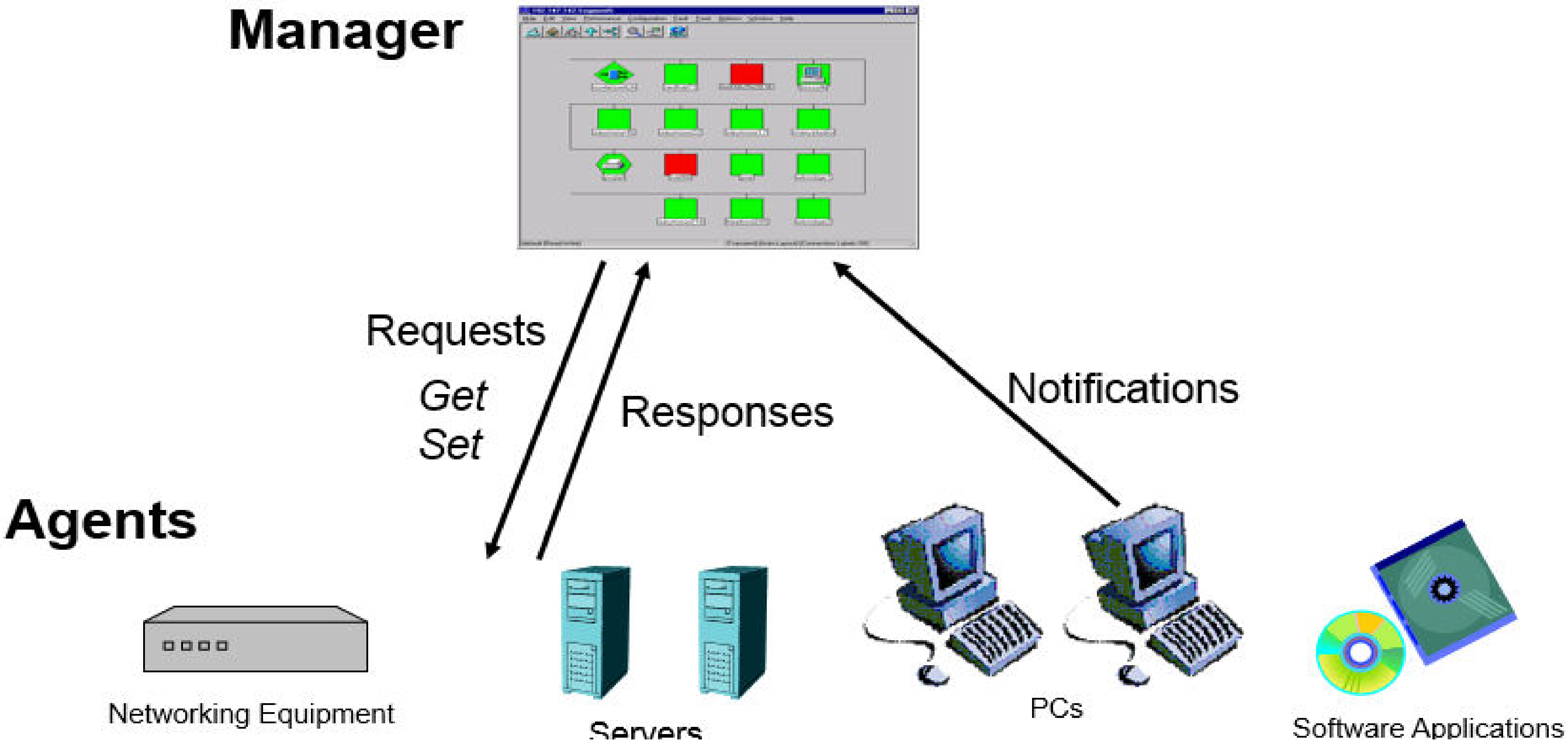
The "conversation" between the manager and the managed system is about the Management Information Base (MIB)

That defines all the information that can be seen or changed by the manager

NMS uses SNMP commands to read data that is stored in the device's MIB.



SNMP in One Slide



Manager

Requests

Get

Set

Responses

Notifications

Agents

Networking Equipment

Servers

PCs

Software Applications

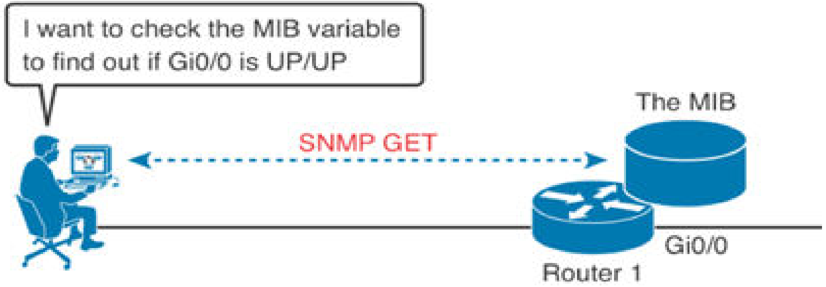
SNMP Commands (just some of them)

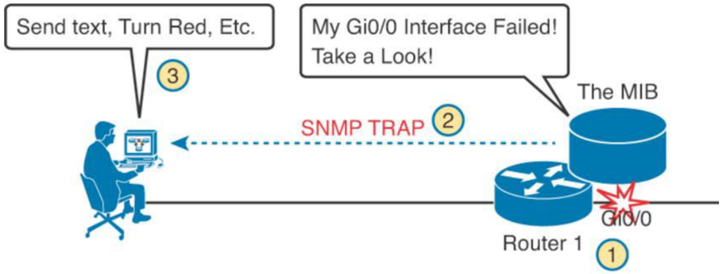
Get (manager -> agent): query/retrieve for one or more values

Set (manager -> agent) Set a value, or perform action in MIB

Trap (agent -> manager) Spontaneous notification from equipment e.g. line down

INFORM: Similar to the TRAP initiated by the Agent, includes confirmation from the SNMP manager on receiving the message.


I want to check the MIB variable to find out if Gi0/0 is UP/UP
SNMP GET
The MIB
Gi0/0
Router 1


Send text, Turn Red, Etc.
3
My Gi0/0 Interface Failed! Take a Look!
The MIB
SNMP TRAP
2
Gi0/0
Router 1
1

SNMP v1	SNMP v2c	SNMP v3
Easy to set up. Only requires a plain text community string to authenticate packets	Identical to version 1	Setup is more complex. Does not use community strings but users with authentication and encryption.
Packet Types: • Get-Request • Get-Next-Request • Set Request • Get Response	Packet Types: • Get-Request • Get-Bulk-Request • Get-Next-Request • Set Request • Inform-Response • SNMP v2 Trap	The basic functions of v3 are from v1 and v2. v3 has a new SNMP message format

That's all Folks!