



Network Management

– Course 1 –

Chapter 3: Remote Network Management Services (1/1) Introduction

Dr. Nadira Benlahrache

NTIC Faculty

email@univ-constantine2.dz



Network Management

– Course 1 –

Chapter 3: Remote Network Management Services (1/1) Introduction

Dr. Nadira Benlahrache

NTIC Faculty

email@univ-constantine2.dz

Concerned Students :

Faculty/Institute	Department	Level	Speciality
NTIC	TLSI	License 3	G.L.

Objectives:

- Overview of Remote Network Management Services
- Presentation of the Telnet service,
- Presentation of the SNMP service,

Introduction

A network management tool should include, according to the ISO (see chapter 1), five distinct functions:

- Configuration Management
- Security Management
- Anomaly management
- Performance Management
- Cost and accounting management.

Introduction

In this course, two services will be presented, their mission is to provide **management** and **remote configuration** of TCP/IP-based network equipment regardless of their level of heterogeneity, namely:

- **Telnet** service,
- **SNMP** service.

Problem statement

- Nowadays, networks can consist of hundreds or thousands of machines located in geographically distant places.
- It is difficult, if not impossible, for a manager to monitor, manage and maintain this type of network without appropriate tools.
- Network management software aims to be this type of tool.
- Unfortunately, due to the diversity of hardware, network operating systems and types of networks (IBM, Bull, H.P., Novell...), **there is no universal tool.**

Problem Statement

- Multiple network administration platforms will be required to manage different environments.
- Three main ideas emerge regarding administration needs:
 - **Prevention** is better than cure,
 - Manage the network as a whole and not as a collection of small networks,
 - **Administer** from any point on the network.

Problem Statement

One of the essential functionalities that a network administration software must provide is **Configuration Management**. This function actually consists of 2 parts:

- ① Remote **configuration** and **reconfiguration** of hardware: with a good tool that allows a network administrator to:
 - remotely configure newly installed hardware from their console,
 - reread these configurations and modify them if the chosen parameter values were not the most appropriate.
 - the same should be possible for **servers** and, if possible, for **workstations**.

Problem Statement

② Asset management:

① **Hardware asset management:** to automatically or manually:

- establish a database containing all the hardware on the network,
- easily determine from a console the hardware characteristics of a server or workstation; processor type, memory size, disk capacity, etc.

② **Software asset management:** some management software allows:

- scanning the disks of servers and workstations to discover the list of installed software and their versions,
- remotely installing software on workstations from one or more servers,
- automatically updating installed software,
- some software can limit the number of users working with an application, based on the number of declared licenses.

1. Telnet

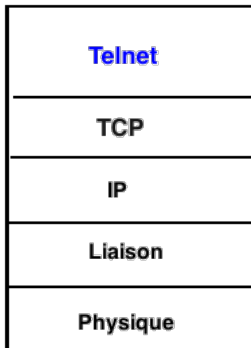
Telnet is the first historical remote administration protocol:

- It belongs to the **application** layer of the OSI model,
- Works in Client-Server mode,
- Created in **1969**, it is a very general and bidirectional (half-duplex) communication method.
- It is standardized by the IETF (RFC 15, 854, and 855).
- It was used to administer remote UNIX servers or network equipment.

1. Telnet

The clients usually connect to the TCP port **23** of the server protocol.

Figure: Position of Telnet



2: Operation

The main use of the **telnet** command is to connect to a **telnet server**,

- launch a daemon on the host machine called **telnetd**,
- request for an identifier and a password,
- provide a command line on the remote machine in exchange.

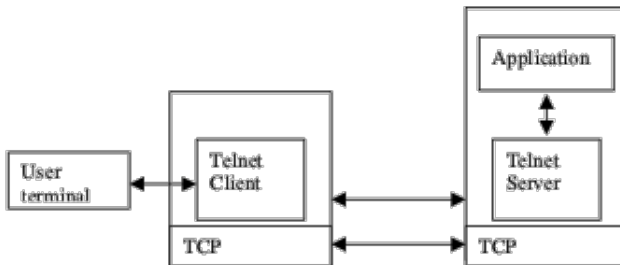
2: Operation

Here are the steps for how Telnet works:

- ➊ The client sends a connection request to a Telnet server using the default port 23.
- ➋ The Telnet server accepts the connection request and sends a welcome message to the client.
- ➌ The client provides its login credentials (username and password) to the Telnet server.
- ➍ The Telnet server checks the login credentials of the client.
- ➎ If the login credentials are valid, the Telnet server provides a command prompt to the client, otherwise the connection is refused.
- ➏ The client can then send commands and receive responses from the remote machine, as if physically connected to it.
- ➐ To exit the Telnet session, the client can simply type the "exit" or "logout" command.

2: Operation

Figure: Operating Model of Telnet



3: Roles and Objectives

- **Telnet** allows the development of a **standard interface**, called **NVT** (*Network Virtual Terminal*), providing a **standard communication basis**.
- **Telnet** consists of creating an abstraction of the terminal, allowing any host (client or server) to communicate with another host without knowing its characteristics (**overcome heterogeneity problem**).
- Telnet allows access to a **plain text** console on a remote computer.
- It is also defined to be used for terminal-to-terminal communication ("**link**") and process-to-process communication (**distributed computing**).

4: Some Telnet negotiation options

- DO → (sender wants receiver to enable option) WILL ← (receiver agrees to enable option)
- DO → (sender wants receiver to enable option) WON'T ← (receiver refuses to enable option)
- WILL → (sender wants to enable option) DO ← (receiver grants permission)
- WILL → (sender wants to enable option) DON'T ← (receiver refuses to grant permission)
- WON'T → (sender wants to disable option) DON'T ← (receiver responds with OK)
- DON'T → (sender wants receiver to disable option) WON'T ← (receiver responds with OK)

5: Standard Commands

The standard Telnet commands are as follows:

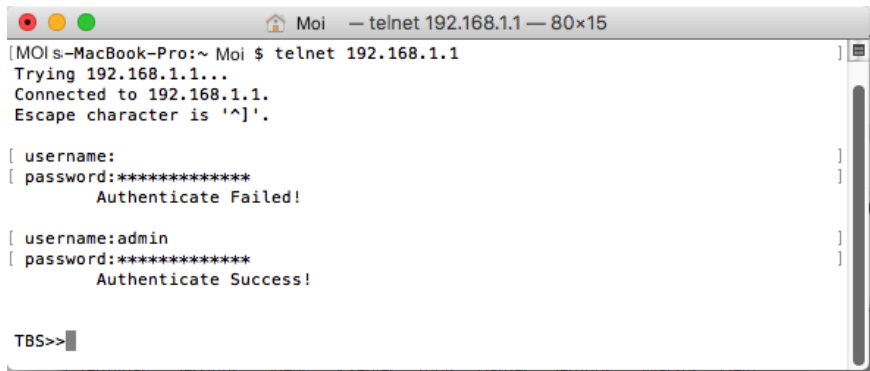
- **telnet**: Establishes a connection with the remote host
- **close**: Terminates the current connection
- **logout**: Terminates the Telnet session
- **quit**: Terminates both the connection and Telnet session
- **status**: Displays status information regarding the current Telnet session
- **mode**: Allows switching between line and character mode
- **?**: Provides help. Without an argument, it displays the help menu.

6: Telnet on Linux

- The server software is called "**telnetd**"
- The Telnet service consists of two packages:
 - ① The Telnet client **telnet-0.17-23.rpm**;
 - ② The Telnet server **telnet-server-0.17-23.rpm**
- By default, the Telnet service is disabled. To activate it, you need to edit the file **/etc/xinetd.d/telnet** and set **disable=no**.
- It can be started with the following parameters: **telnet [-d] [-a] [-n file] [-l user] host [port]**
 - **-d**: Starts debug mode.
 - **-a**: Enables automatic connection by transmitting the USER environment variable to the contacted host computer to simplify the connection process.
 - **-n**: Records trace information in the indicated file for later debugging.
 - **-l**: Connects as the user under the specified name.

Access via Telnet

Access from a terminal (Mac-OS) as an example:

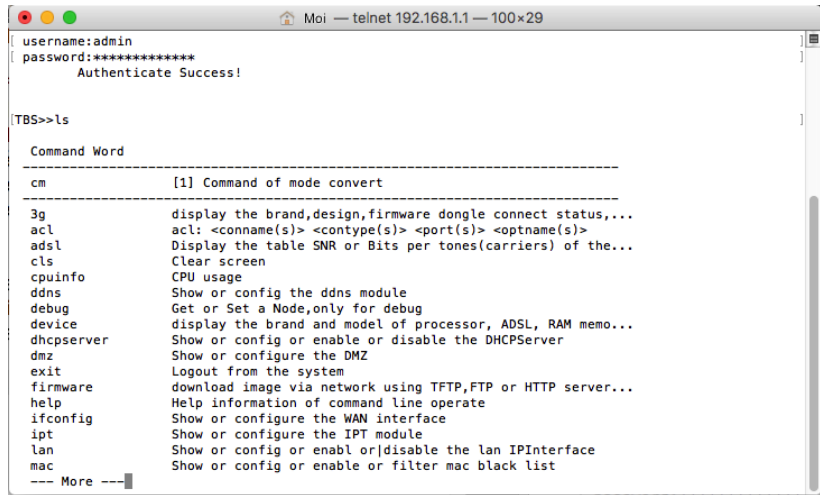


The screenshot shows a Mac OS terminal window titled "Moi — telnet 192.168.1.1 — 80x15". The terminal content is as follows:

```
[MOI:s-MacBook-Pro:~ Moi $ telnet 192.168.1.1  
Trying 192.168.1.1...  
Connected to 192.168.1.1.  
Escape character is '^]'.  
  
[ username: ]  
[ password:***** ]  
    Authenticate Failed!  
  
[ username:admin ]  
[ password:***** ]  
    Authenticate Success!  
  
TBS>> ]
```

Access via Telnet

Access from a terminal (Mac-OS) as an example:



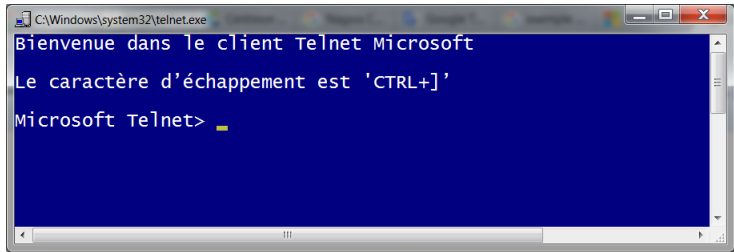
```
Moi — telnet 192.168.1.1 — 100x29
[ username:admin
[ password:*****
    Authenticate Success!

[TBS>>ls

Command Word
-----
cm                [1] Command of mode convert
-----
3g                display the brand,design,firmware dongle connect status,...
acl               acl: <conname(s)> <contype(s)> <port(s)> <optname(s)>
adsl              Display the table SNR or Bits per tones(carriers) of the...
cls               Clear screen
cpuinfo           CPU usage
ddns              Show or config the ddns module
debug             Get or Set a Node,only for debug
device            display the brand and model of processor, ADSL, RAM memo...
dhcpserver        Show or config or enable or disable the DHCPserver
dmz               Show or configure the DMZ
exit              Logout from the system
firmware          download image via network using TFTP,FTP or HTTP server...
help              Help information of command line operate
ifconfig           Show or configure the WAN interface
ipt               Show or configure the IPT module
lan               Show or config or enabl or|disable the lan IPInterface
mac               Show or config or enable or filter mac black list
--- More ---
```

7: Advantages and disadvantages

- + Allows executing keyboard-entered commands on a remote machine,
- + Simple to use,
- + Without any specific interface,
- - Transmission in clear text, security issue.



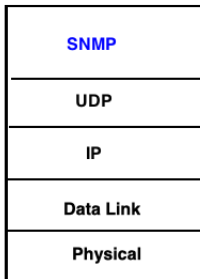
SNMP Protocol

SNMP (Simple Network Management Protocol) defined in RFC 1157, is a:

- Protocol and environment,
- Based on client/server architecture,
- Based on TCP/IP: usable for all networks,
- Common transaction interface for all devices,
- Use of MIB (Management Information Base): databases for equipment **variables**,
- Hundreds of implementations,
- see: www.net-snmp.org

SNMP Protocol

Position of the SNMP protocol in the protocol stack according to the TCP/IP model. It uses ports **161** and **162**:



SNMP and Protocols Stack

SNMP Protocol

SNMP is a protocol and an environment that enables the following functions:

- Configuration of equipment,
- Monitoring of network operations,
- Detection and prediction of errors,
- Notification of failures, etc.

SNMP Protocol

Three important elements in SNMP:

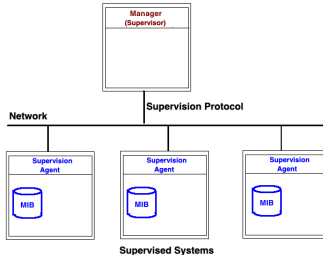
- A **database (MIB)** managed by each **SNMP agent** and possibly modifiable by a **SNMP manager**. (RFC 1156 and 1213 define MIB-1 (version 1) and then MIB-2).
- A **common structure** and system for representing objects in the MIB: SMI (Structure of Management Information, RFC 1155).
- A **protocol for exchange between manager and agent** (RFC 1157).

The SNMP protocol has evolved to incorporate aspects of confidentiality and authentication.

SNMP Protocol

A management software that uses the SNMP management protocol must have 2 types of modules:

- The **Agent** installed in the network components to be managed. The agent controls and provides information through a set of variables (MIB).
- The **Manager** installed in the Management Console, manages and controls through this base.



SNMP Protocol

Which components can be managed by SMNP?

- **Hardware:**

- ① Network hardware
 - Manageable hub stacks,
 - Switches, Bridges,
 - Routers.
- ② Servers,
- ③ Workstations,
- ④ Modems,
- ⑤ Printers...

- **Software:**

- Databases on servers
- Manageable applications (Backup, Antivirus, Printing...)

SNMP Operation

- The diagram below presents the operation of management software using SNMP (this standard is the most used).

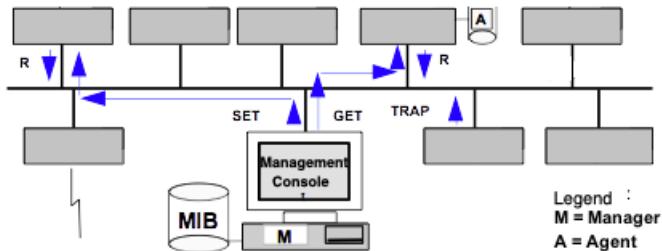
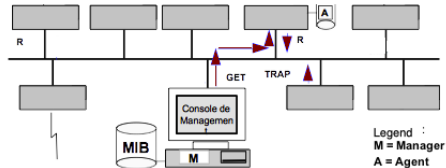


Figure: SNMP Query

SNMP Operation

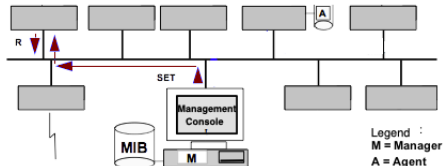
How is the dialogue between the Manager and the Agents done?

- When the Manager wants to know the value of a variable in a network component, it sends a **GET REQUEST** type request to the Agent of this component. The agent responds with a **GET RESPONSE**.
- If several values are requested from the agent in sequence (for example, reading in a table), the Manager can use a **GET NEXT REQUEST** request.
- **WALK** a subtree, on the other hand, **GET** a leaf node.



SNMP Operation

- If the Manager wants to modify the value of a variable in a component, it sends a **SET** type request to the Agent, followed by the name of the variable and the value to be modified.
- If an unforeseen event occurs in a manageable component of the network, the Agent sends a message (**Trap**) to the Manager. Depending on the severity of the incident, the message can be transformed into an **Alarm** which is displayed at the **Management Console** level.



Other SNMP commands

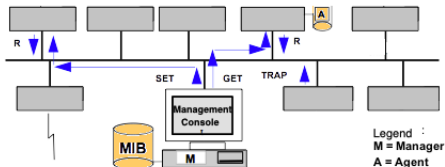
- **GET BULK:** Used to retrieve large amounts of data from a large MIB table.
- **INFORM:** This command is similar to the *TRAP* initiated by the agent, but *INFORM* includes a confirmation from the SNMP manager upon receiving the message.
- **RESPONSE:** This is the command used to retrieve the value(s) or signal of actions directed by the SNMP manager.
- **TABLE:** Retrieves the contents of an SNMP table and displays it in a tabular format.

Note: It is important to configure the use of these commands correctly to avoid any security or performance risks to the network.

MIB Database

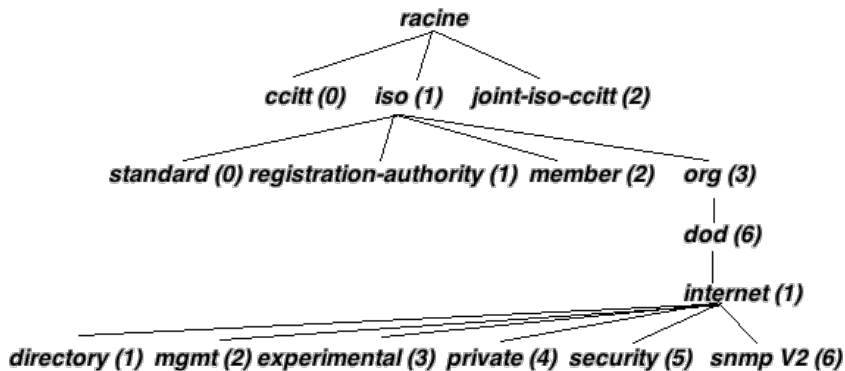
The **names of variables** and their **definitions** are stored in a global database called **MIB** (*Management Information Base*) located in the **Management Console**. The MIB is a database managed by an SNMP agent that contains the managed objects. It can be divided into two main parts:

- The **Generic MIBs** that contain general variables that can be found on all manageable components.
- The **Proprietary or Private MIBs** that contain variables specific to particular hardware from different manufacturers.



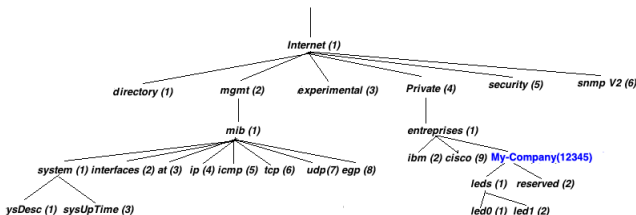
MIB Structure

MIB tree:



MIB Structure

- The OID for **internet** is **1.3.6.1**,
- Under **internet**, there are several branches corresponding to companies or organizations,
- Each company can create its own branches with its own specific objects,
- For example, the **dod** branch corresponds to the US government organization Department of Defense, and contains several sub-branches for its specific objects.



MIB Structure

- Each node in the MIB tree has a **symbolic name**.
- Each object can be identified either symbolically or using its **OID**.
- For example, the object **sysDescr** has a symbolic name of **iso.org.dod.internet.mgmt.mib.system.sysDescr.0**.
Its OID, following SMI rules, is **1.3.6.1.2.1.1.1.0**.
- It is worth noting that it is the **OID** that is transmitted in an SNMP request, not the symbolic name of the object.

MIB Structure

- If the agent needs to manage its own objects, they are part of the private MIB. These objects are placed in the branch:
iso.org.dod.internet.private.enterprises.company_name.
- In this way, the SNMP agent's MIB is extended. The identifier number of the company or institution is normally assigned by the **IANA** (Internet Assigned Numbers Authority).
- Let's assume that the number assigned to **My-Company** is **12345**.
- The object **led0** has the symbolic name:
iso.org.dod.internet.private.enterprises.My-Company.leds.led0.0.
- Its OID, following SMI rules, is:
1.3.6.1.4.1.12345.1.1.0.
- Note that the sub-tree **1.3.6.1** is the most important.

SNMP Versions

In 1993, new RFCs (RFC 1441 to 1452) were added to revise **SNMPv1** and define **SNMPv2c** (classic). SNMPv2c was updated in 1996 (RFC 1901 to 1908) to become SNMPv2. The main differences between SNMPv1 and SNMPv2 are:

- New SNMP **queries** defined.
- Two **new branches in the MIB**: snmpV2 and snmpV2-M2M (Manager to Manager).
- **Security flaws fixed**: no clear text community on the network. Use of encryption and authentication procedures for SNMP queries.
- Mechanisms for **remote configuration**.

SNMP Versions

- Since the **SNMPv3** version (RFC 2571 to 2575) appeared,
- It provides secure access to devices by authenticating and encrypting data packets on the network. The security functions provided in SNMPv3 are:
 - **Message integrity**: ensures that a packet has not been tampered with during transit.
 - **Authentication**: determines that the message comes from a valid source.
 - **Encryption**: scrambles the content of a packet to prevent it from being learned by an unauthorized source.

N.B: the only stable and widely used version is SNMPv1 (despite its flaws!). However, SNMPv3 is increasingly being adopted as it is considered the safest and most reliable version. SNMPv2c is still used but is considered less secure than SNMPv3 due to its lack of advanced security features.

SNMP under Linux

- Firstly, navigate to the SNMP configuration directory and create a blank configuration file:

```
cd /etc/snmp vim snmpd.conf
```

- Then, enter the community string that is accessible in read-only mode:

```
rocommunity mycommunity
```

- We increase security by adding the authorized source to query:

```
rocommunity mycommunity 192.168.1.1
```

- We can add a community string that is accessible in read-write mode using: **rwcommunity**
- Thus, the IP address 192.168.1.1 will be authorized to query (which is the supervision server).

SNMP on Linux

- Enabling an **SNMP** configuration allows you to retrieve various information (CPU, RAM, interface usage, etc.).
- It is then possible to restart the SNMP service:

`/etc/init.d/snmpd restart`

- To test an SNMP configuration, you can use the `snmpget` or `snmpwalk` command:

`snmpget -v version -c community ip address oid`

or

`snmpwalk -v version -c community name ip device OID`

SNMP on Linux

- **version:** V1, V2c or V3 (it is recommended to use v2c or V3)
- **community name:** name of the community declared in the **device** to access information,
- **device IP:** IP address or hostname of the equipment to be tested,
- **OID:** manufacturer identifier used to obtain information about the equipment.

Here is an example of using **snmpwalk**:

```
snmpget -v 2c -c public 192.168.1.13 1.3.6.1.2.1.2.2.1.10.1
```

Advantages of SNMP

SNMP has many advantages as a network management tool:

- Network management is performed from a **central machine** (preferable for security).
- Security has increased over its different versions, to meet most of the imposed constraints.
- It ensures that requests are **properly delivered** and **correctly interpreted**.
- The **use of a tree structure** for variable management allows for continuous evolution of functional capabilities accessible through this protocol.
- **Diversity management**: the use of a **standard interface** for all hardware allows for the same control of all network equipment (practical in the case of a highly diversified IT park).

Advantages and Disadvantages of SNMP

In summary, we can retain:

- Centralized access,
- Security,
- Reliability,
- Scalability,
- Diversity management,
- – Poor communication standard interface that provides little information for management.

Advantages and Disadvantages of SNMP

These points summarize the advantages and disadvantages of SNMP.

- It is important to note that, although it is a useful tool for network management, it may be insufficient in some cases.
- For example, if you need more advanced and fine-grained management of your network equipment, or if you need to perform more complex tasks, you may need to consider other network management tools.

Conclusion

The aim of this course was to present:

- Network administration services, particularly those related to the configuration of hardware and software.
- The Telnet protocol (service) for standard administration, its role, functioning, and configuration under Linux, as well as its advantages and disadvantages.
- The network management protocol SNMP. Its mechanism of operation and the database used. Its use under Linux, its advantages and disadvantages.

References

- 'TELNET under Single-Connection TCP Specification', Darryl E. Rubin, 1976, PN edition.
- 'Telnet 31 Success Secrets - 31 Most Asked Questions On Telnet - What You Need To Know', Earl Fleming, 2013, Earl Fleming.
- 'Essential SNMP, 2nd Edition', Douglas Mauro Kevin Schmidt, 2009, ©O'Reilly Media, Inc.
- 'SNMP MIB Handbook Paperback', Larry Walsh , 2008, Wyndham Press, ISBN-10: 0981492207.
- 'SNMP Simple Network Management Protocol Amazing Projects from Scratch' Gerard Blokdyk , 2017, CreateSpace Independent Publishing Platform, ISBN-10: 1978043929.
- 'Administration de réseaux informatiques : protocole SNMP', Olivier WILLM, ©Techniques de l'Ingénieur, online (PDF).

Some useful links

- <http://www.mayan.cn/IA/15/8-TELNET-20150414.pdf>
- <http://abcdrfc.free.fr/rfc-vf/pdf/rfc854.pdf>
- <http://files.mbouabid.webnode.fr/200000109-ee0e8ef080/service-Telnet.pdf>
- Site officiel: www.net-snmp.org
- <https://www.manageengine.com/network-monitoring/what-is-snmp.html>