Unit: Network Security

B.Tech VIII

NETWORK AND SYSTEM SECURITY (CORE ELECTIVE - 5) (CS424)

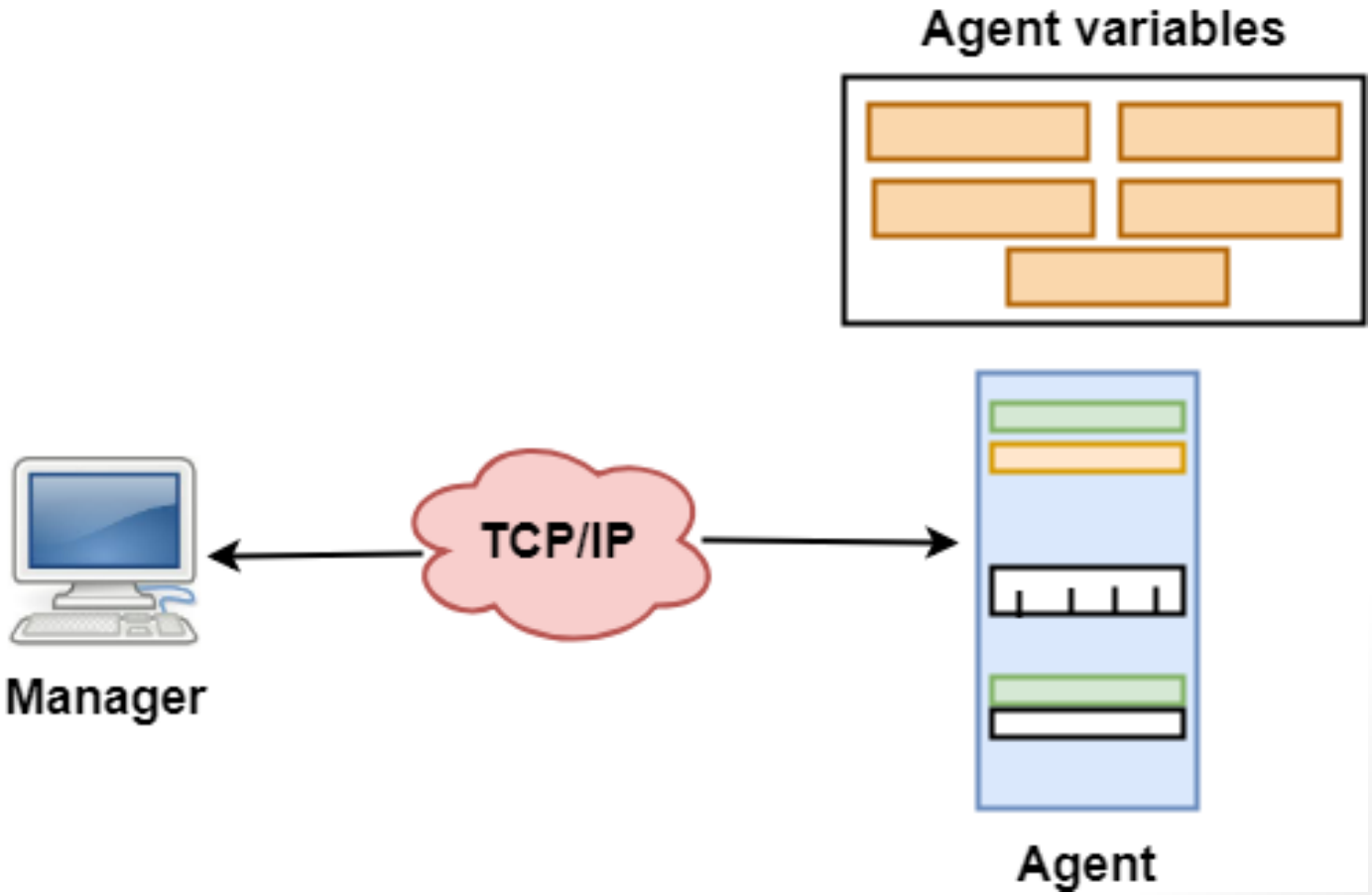
SNMP Protocol

SNMP Protocol

- SNMP stands for **Simple Network Management Protocol**.
- It is a framework used for managing devices on the internet.
- It is an application layer protocol that uses UDP port number 161/162.
- SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.
- A protocol can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.
- **Its purpose is to let network administrators remotely manage an Internet system.**

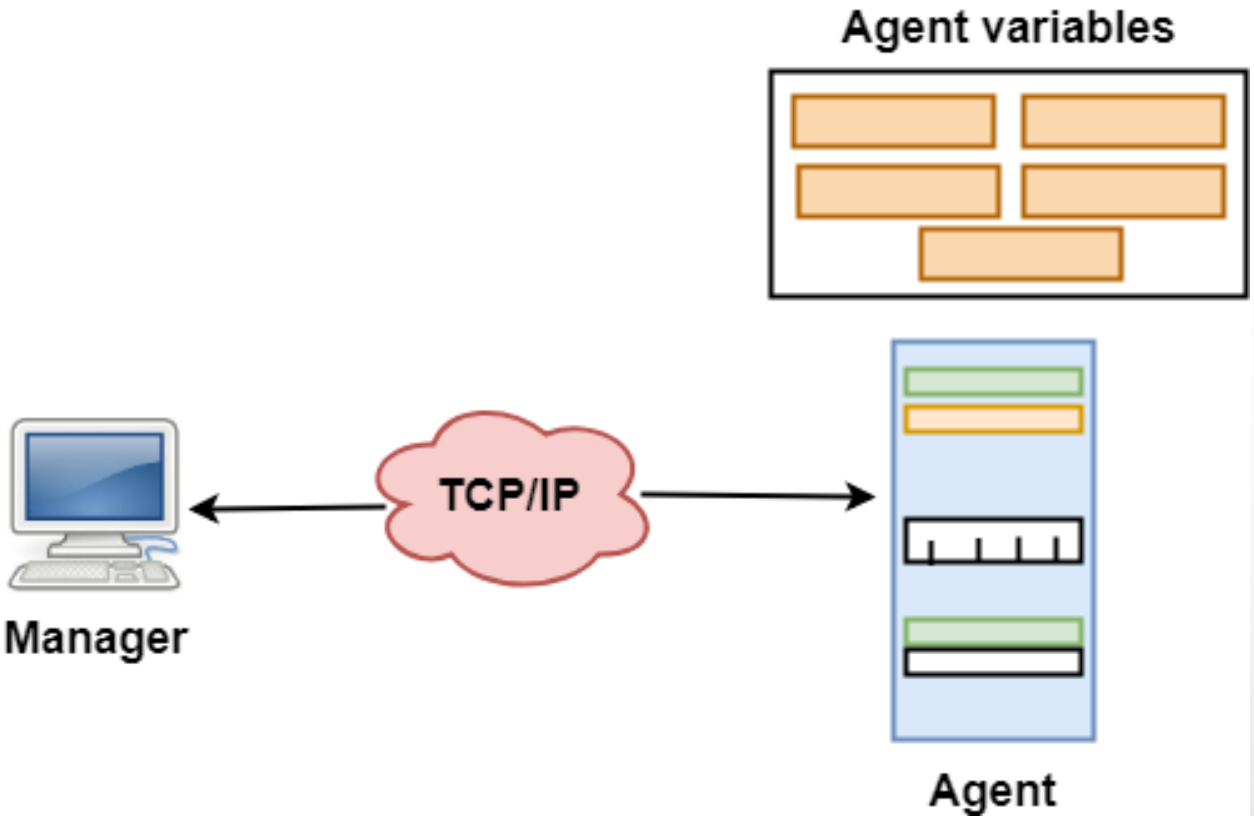
SNMP Components

- SNMP has two components
  - **Manager**
  - **Agent**



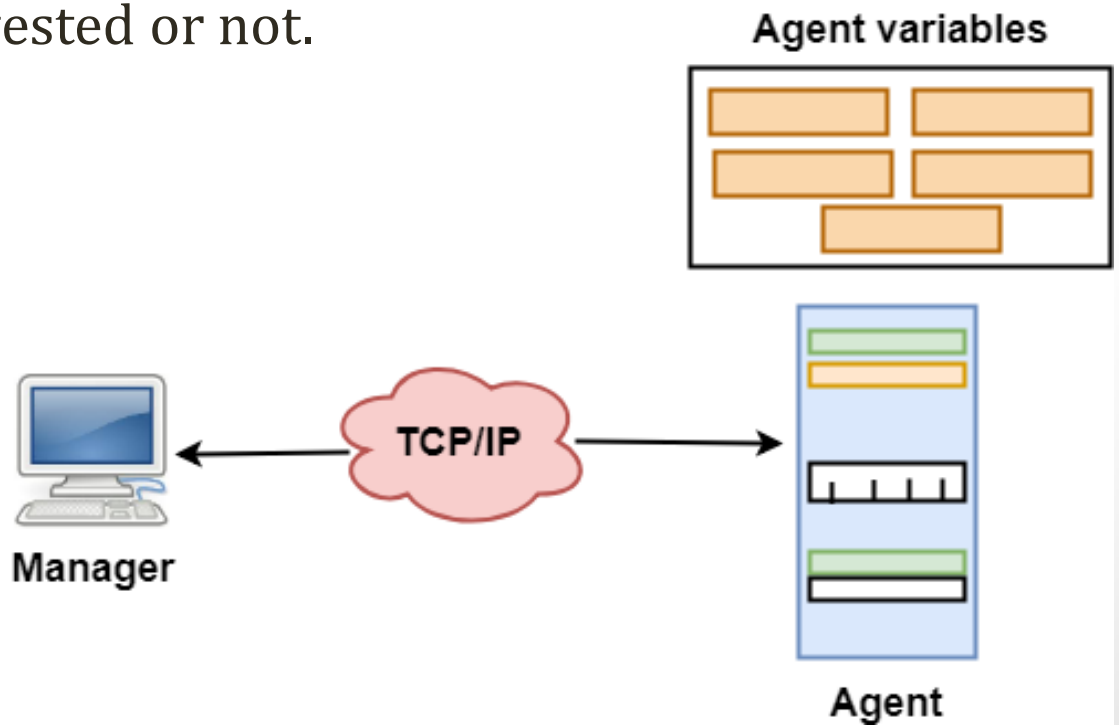
SNMP Components

- A **manager** is a host that runs the SNMP client program while the **agent** is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.



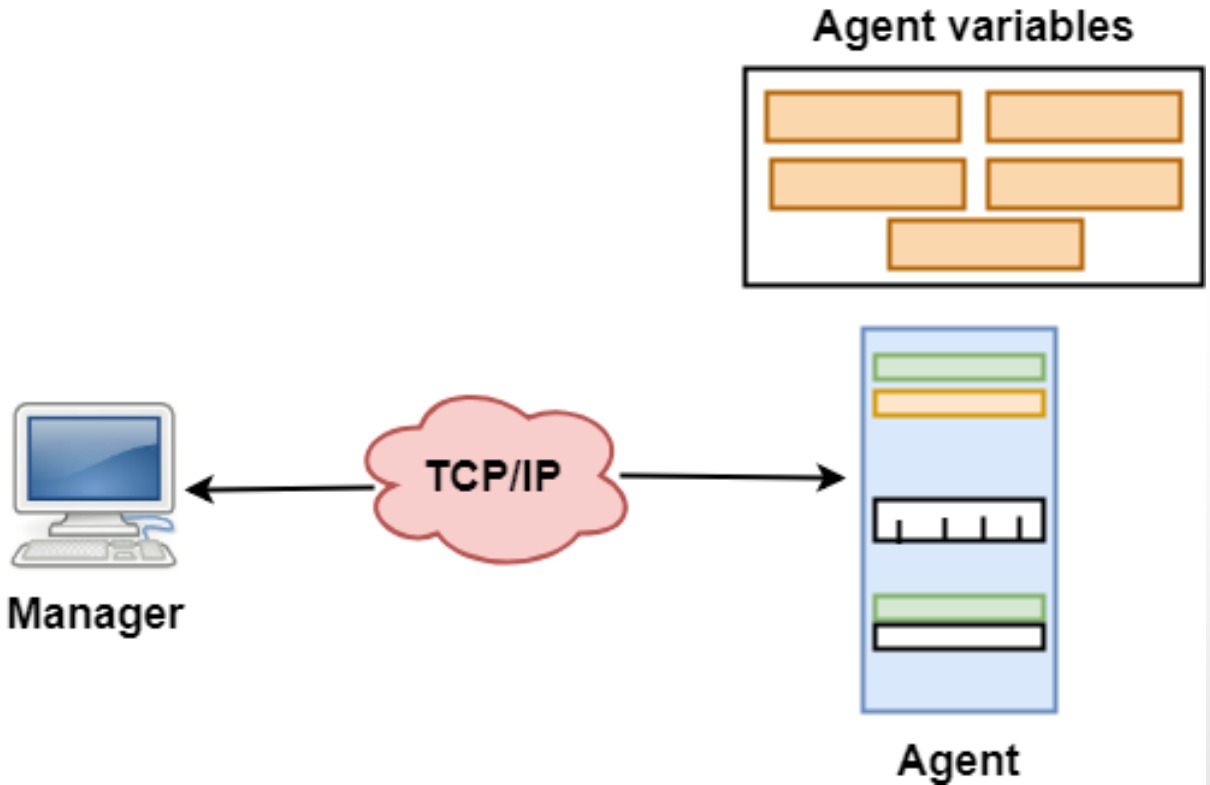
SNMP Components

- The **agent** is used **to keep the information in a database** while the **manager** is used **to access the values in the database**.
- For example, a **router** can store the variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.



SNMP Components

- Agents can also contribute to the management process.
- A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

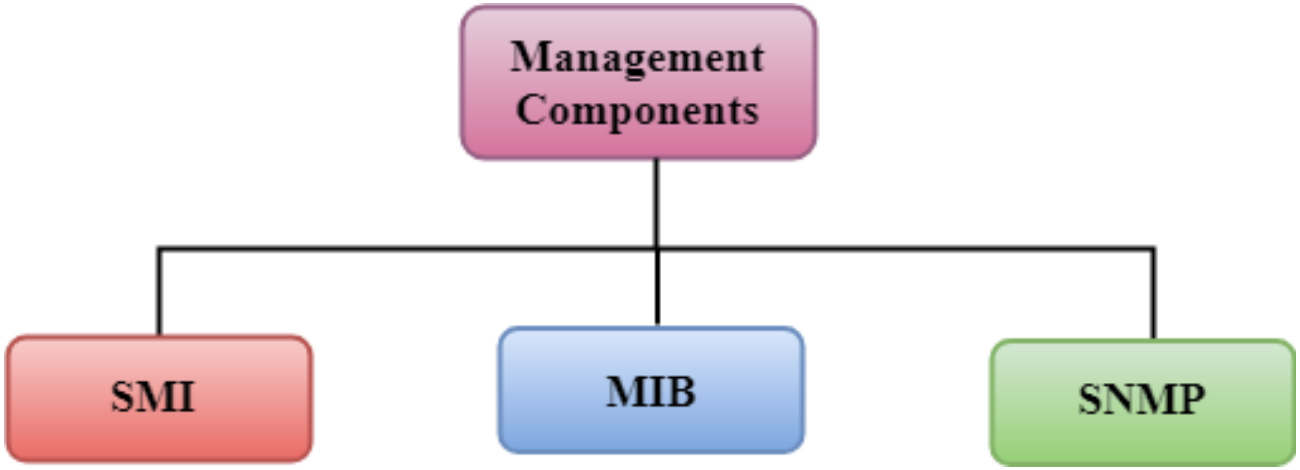


Management with SNMP

- A manager checks the agent by requesting the information that reflects the behaviour of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

- Besides SNMP, Network Management is achieved through the use of the other two protocols:
  - **SMI (Structure of management information)**
  - **MIB(management information base)**

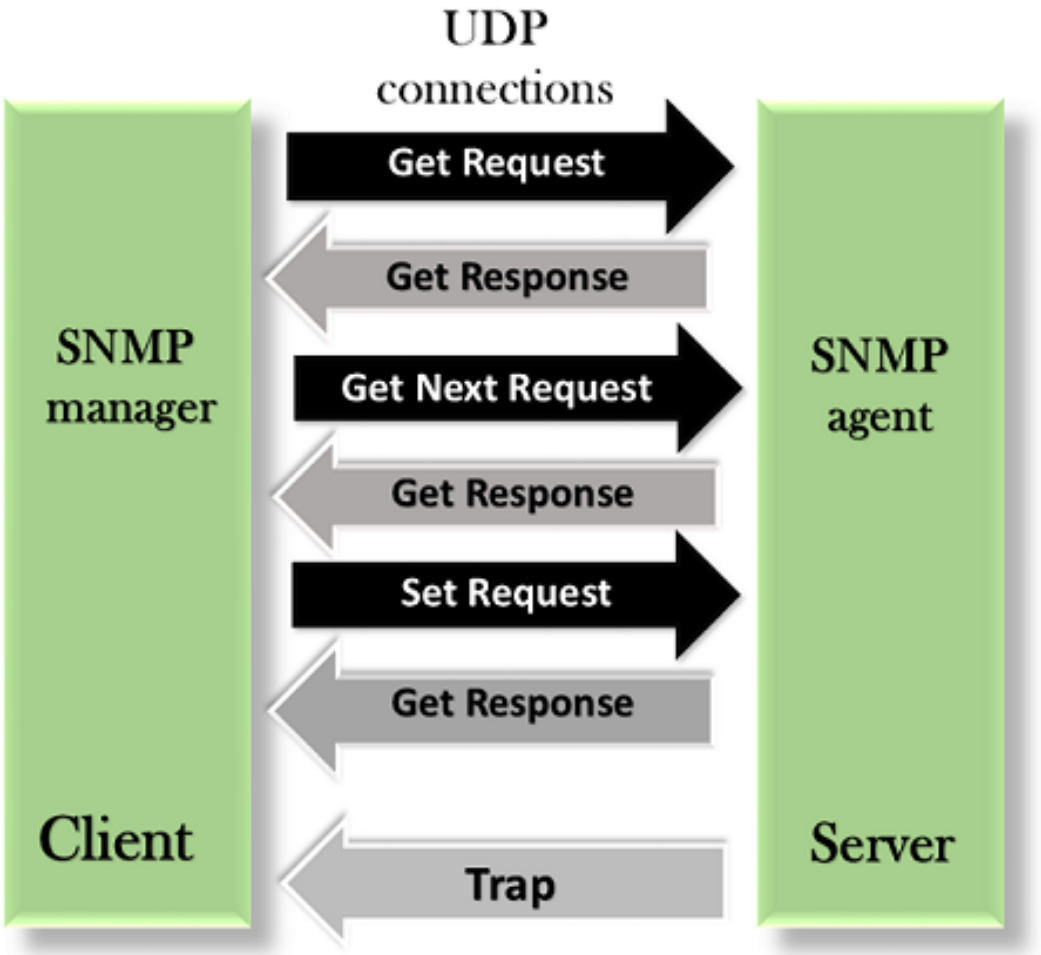


Management Components

- **SMI (Structure of management information)**
  - Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.
- **MIB(management information base)**
  - Each agent has its own MIB, which is a collection of all the objects that the manager can manage.
  - MIB is categorized into **eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp.**
  - These groups are under the mib object.

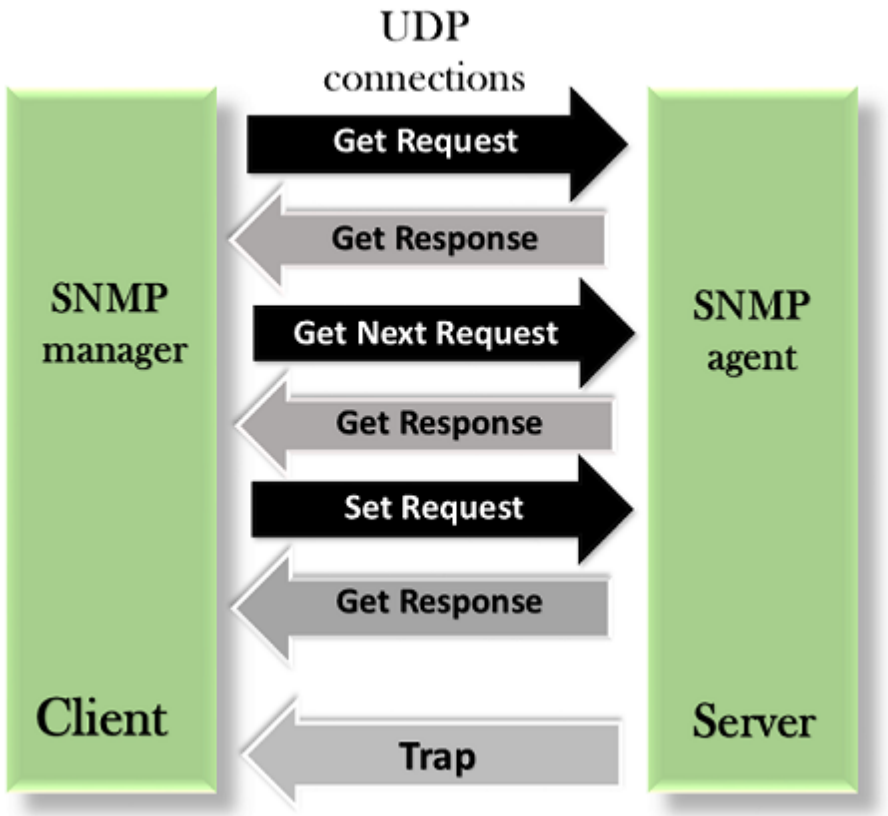
Management Components

- **SNMP(Simple Network Management Protocol)**
- SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.



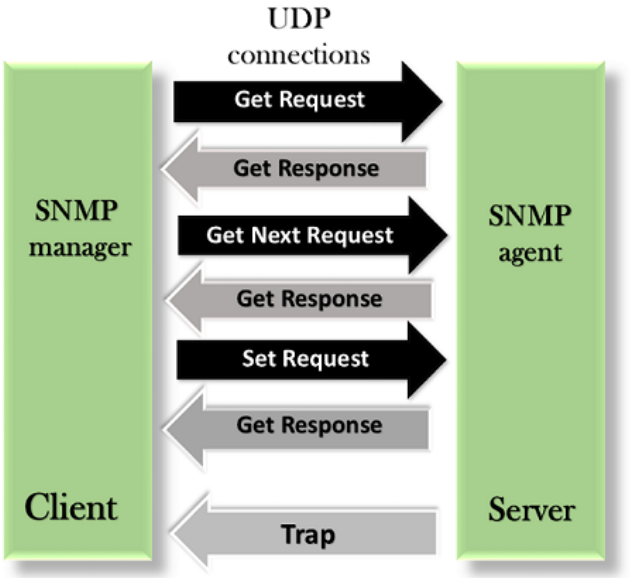
Management Components

- **SNMP(Simple Network Management Protocol)**
- **GetRequest:** sent from a manager (client) to the agent (server) to retrieve the value of a variable.



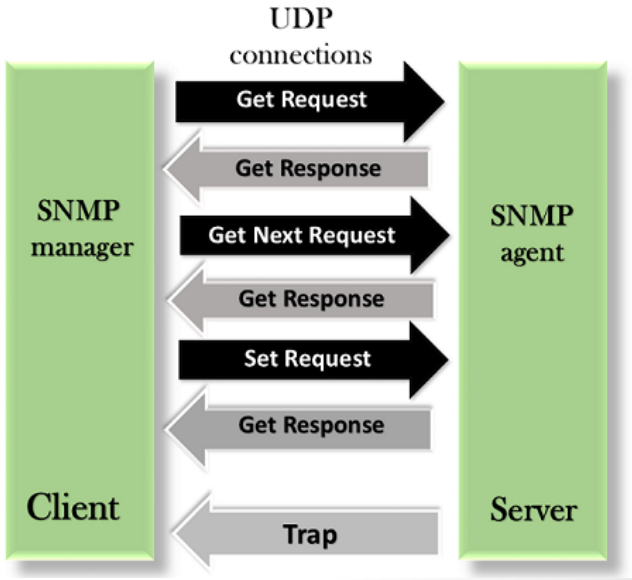
Management Components

- **SNMP(Simple Network Management Protocol)**
- **GetNextRequest:** sent from the manager to agent to retrieve the value of a variable.
- It is used to retrieve the values of the entries in a table.
- If the manager does not know the indexes of the entries, then it will not be able to retrieve the values. So it will continuously ask for the value of variable untill end of database.



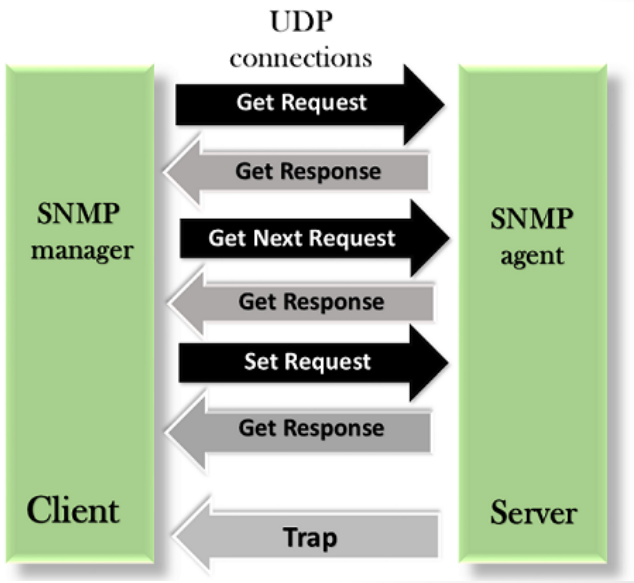
Management Components

- **SNMP(Simple Network Management Protocol)**
- **GetResponse:** The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message.
- This message contains the value of a variable requested by the manager.



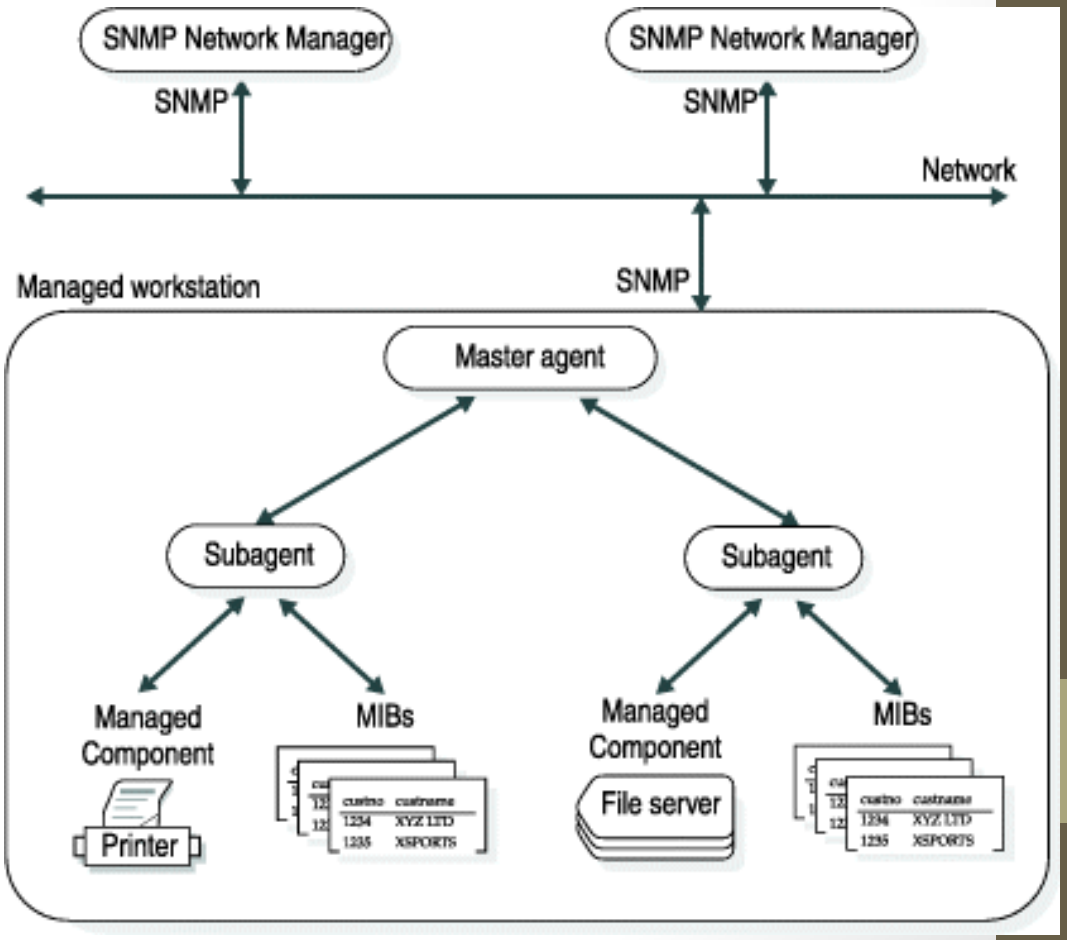
Management Components

- **SNMP(Simple Network Management Protocol)**
- **SetRequest:** sent from a manager to the agent to set a value in a variable.
- **Trap:** sent from an agent to the manager to report an event. For example, if the agent is rebooted, then it informs the manager as well as sends the time of rebooting.



SNMP Architecture

- SNMP architecture includes four layers.
  - Network Managers
  - Master agents
  - Subagents
  - Managed components



SNMP Architecture

- A network can have multiple SNMP Network Managers.
- Each workstation can have one master agent.
- The SNMP Network Managers and master agents use SNMP protocols to communicate with each other.
- Each managed component has a corresponding subagent and MIBs.

SNMP Architecture

- **SNMP network managers**
  - It is a program that asks for information from master agents and displays that information.
  - One can use SNMP Network Managers to select the items to monitor and the form in which to display the information.
- **Master agents**
  - It is program that provides the interface between an SNMP Network Manager and a subagent.
- **Subagents**
  - It is a program that provides information to a master agent.

SNMP Architecture

- **Managed components**
  - A managed component is hardware or software that provides a subagent.
  - For example, database servers, operating systems, routers, and printers can be managed components if they provide subagents.
- **Management Information Bases**
  - It is a group of tables that specify the information that a subagent provides to a master agent.