SNS COLLEGE OF TECHNOLOGY
Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECT301- COMMUNICATION NETWORKS

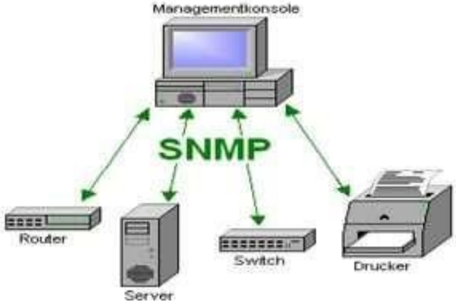
III YEAR/ V SEMESTER

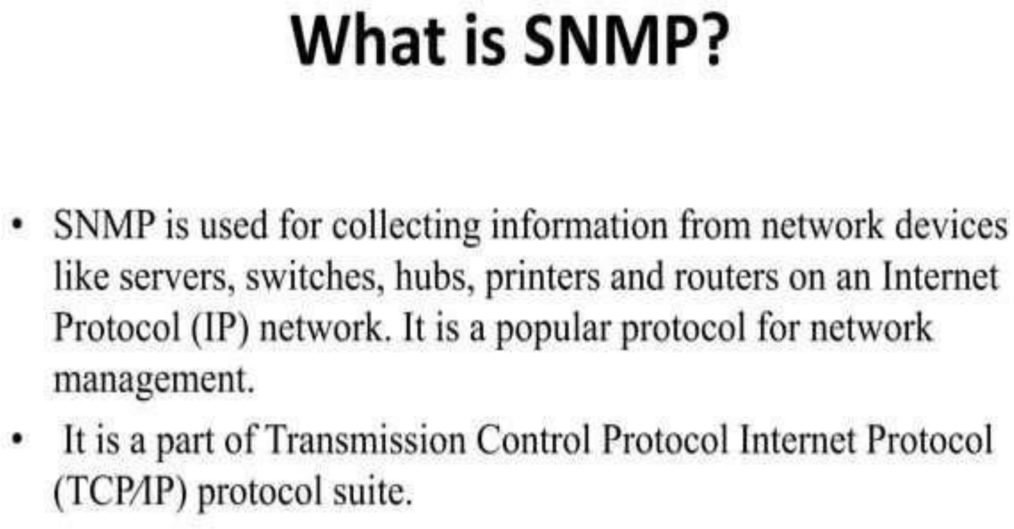
UNIT 3 TRANSPORT LAYER & APPLICATION LAYER

TOPIC – SNMP

Introduction

- The Simple Network Management Protocol (SNMP) is by far, the dominant protocol in network management.
- A key reason for its widespread acceptance, besides being the chief Internet standard for network management is its relative simplicity.

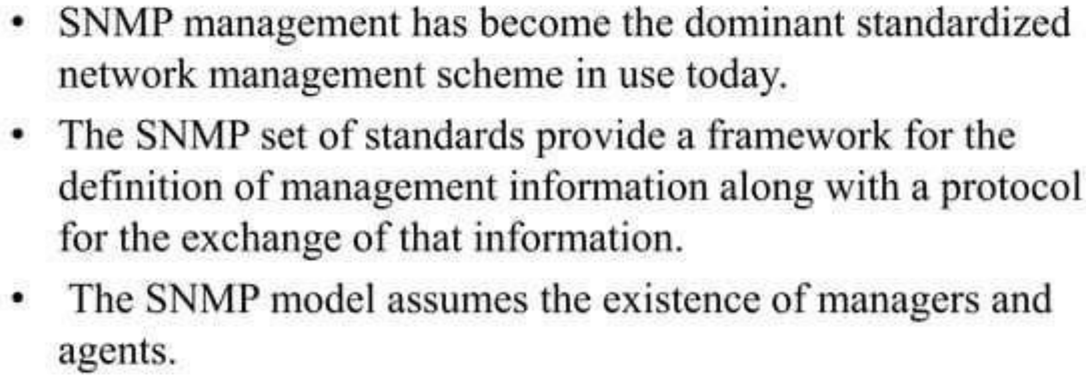




What is SNMP?

- SNMP is used for collecting information from network devices like servers, switches, hubs, printers and routers on an Internet Protocol (IP) network. It is a popular protocol for network management.
- It is a part of Transmission Control Protocol Internet Protocol (TCP/IP) protocol suite.

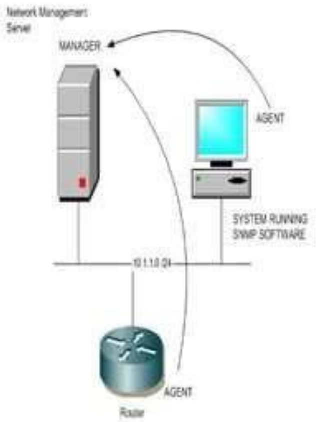
SNMP Management



- SNMP management has become the dominant standardized network management scheme in use today.
- The SNMP set of standards provide a framework for the definition of management information along with a protocol for the exchange of that information.
- The SNMP model assumes the existence of managers and agents.

How does SNMP work?

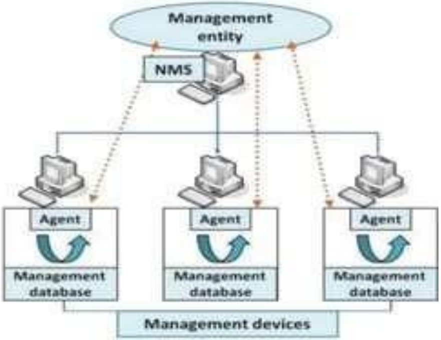
- The simple network management protocol (SNMP) use for monitoring of network-attached devices for any conditions that warrant administrative attention. For example all of the following devices can use SNMP for managing devices on IP networks:
- Network router
- Network switch
- Printer
- NAS server
- ADSL ISP router / modem
- Linux / UNIX / Windows servers



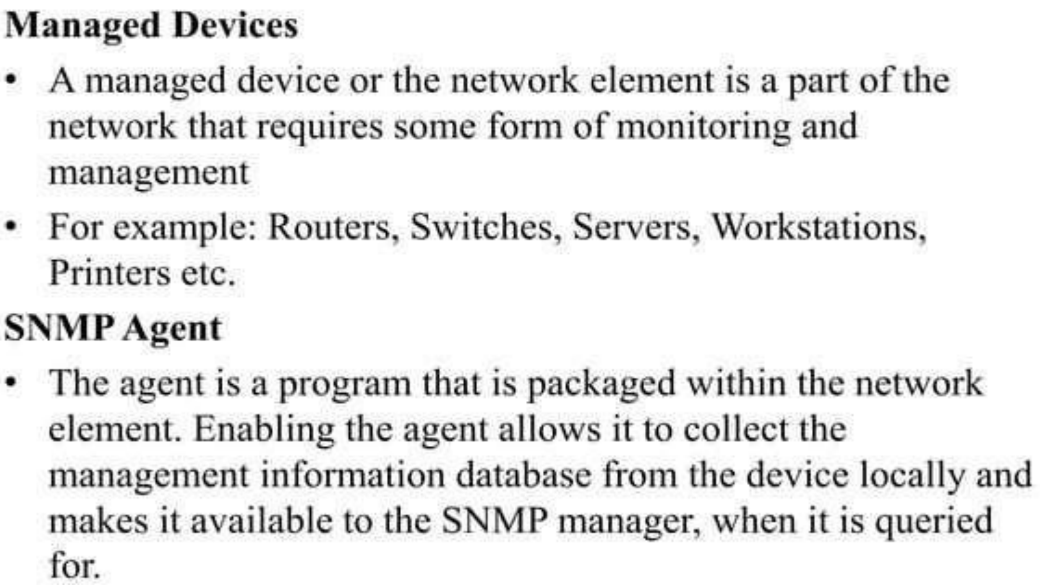
SNMP components

SNMP Manager

- A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.
- SNMP Manager's key functions
- Queries agents
- Gets responses from agents



SNMP components…

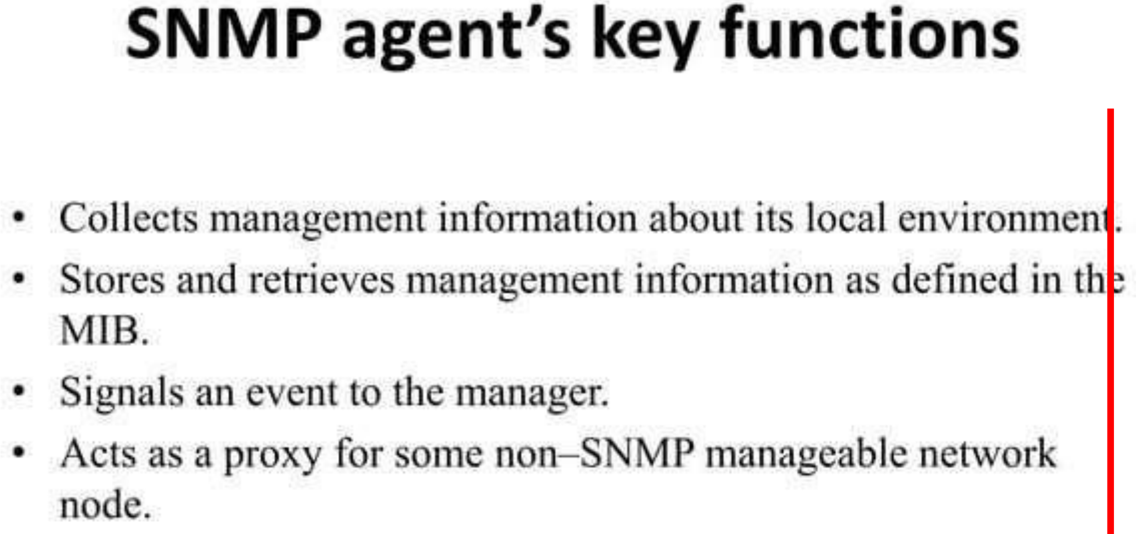


Managed Devices

- A managed device or the network element is a part of the network that requires some form of monitoring and management
- For example: Routers, Switches, Servers, Workstations, Printers etc.

SNMP Agent

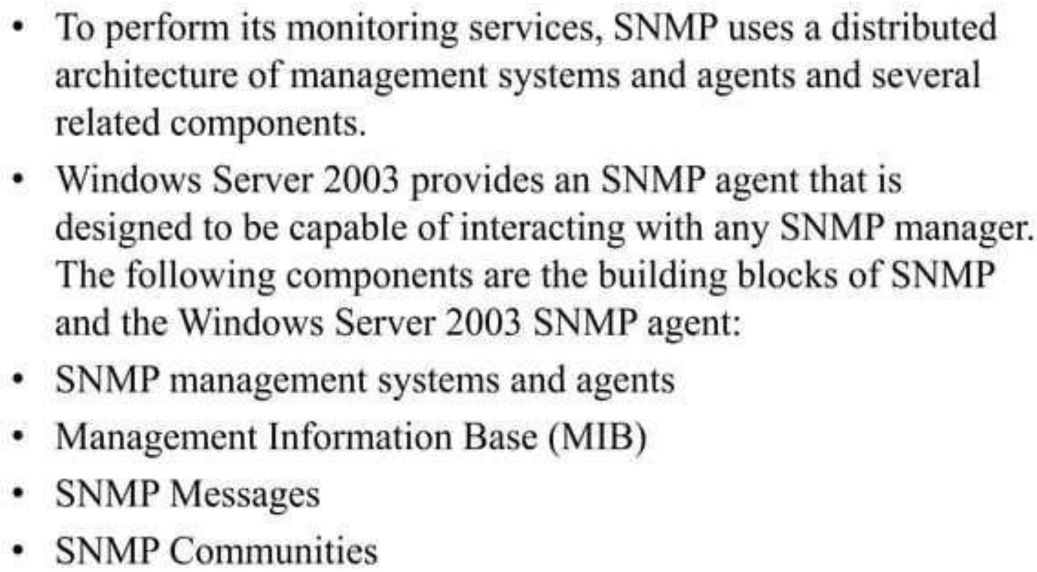
- The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for.



SNMP agent’s key functions

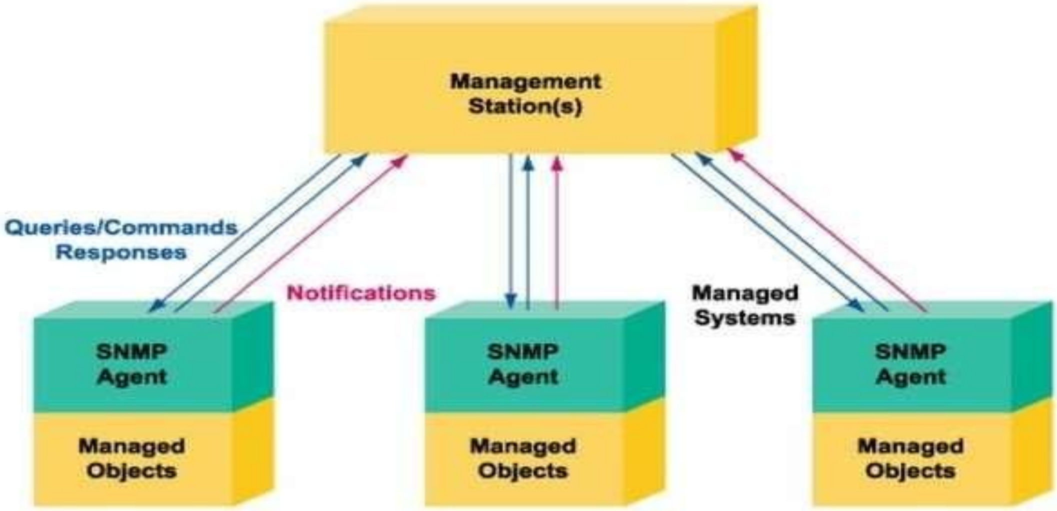
- Collects management information about its local environment.
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non–SNMP manageable network node.

SNMP Architecture

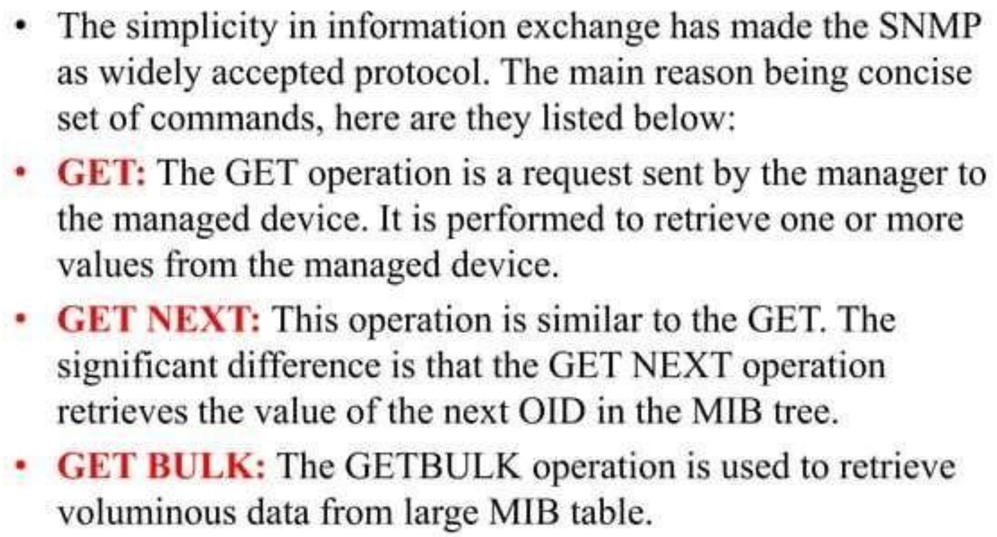


- To perform its monitoring services, SNMP uses a distributed architecture of management systems and agents and several related components.
- Windows Server 2003 provides an SNMP agent that is designed to be capable of interacting with any SNMP manager. The following components are the building blocks of SNMP and the Windows Server 2003 SNMP agent:
- SNMP management systems and agents
- Management Information Base (MIB)
- SNMP Messages
- SNMP Communities

SNMP Architecture...

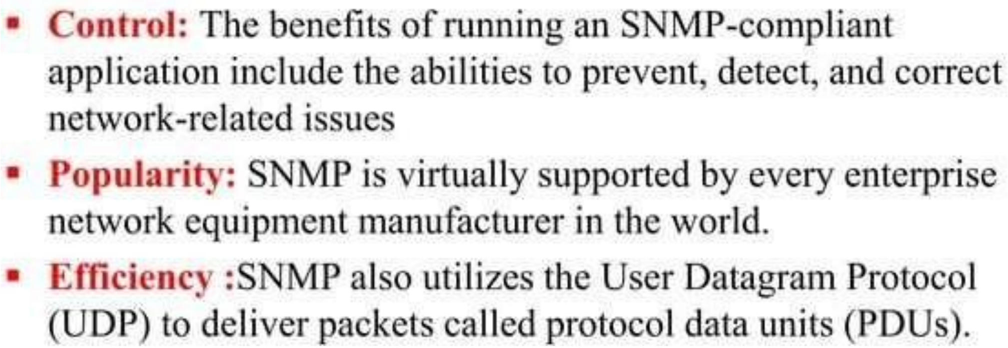


Basic commands of SNMP



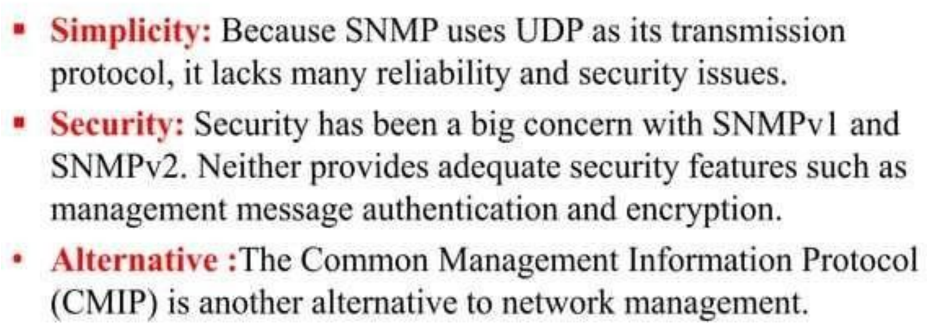
- The simplicity in information exchange has made the SNMP as widely accepted protocol. The main reason being concise set of commands, here are they listed below:
- **GET:** The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.
- **GET NEXT:** This operation is similar to the GET. The significant difference is that the GET NEXT operation retrieves the value of the next OID in the MIB tree.
- **GET BULK:** The GETBULK operation is used to retrieve voluminous data from large MIB table.

BENEFITS



- **Control:** The benefits of running an SNMP-compliant application include the abilities to prevent, detect, and correct network-related issues
- **Popularity:** SNMP is virtually supported by every enterprise network equipment manufacturer in the world.
- **Efficiency :**SNMP also utilizes the User Datagram Protocol (UDP) to deliver packets called protocol data units (PDUs).

LIMITATIONS

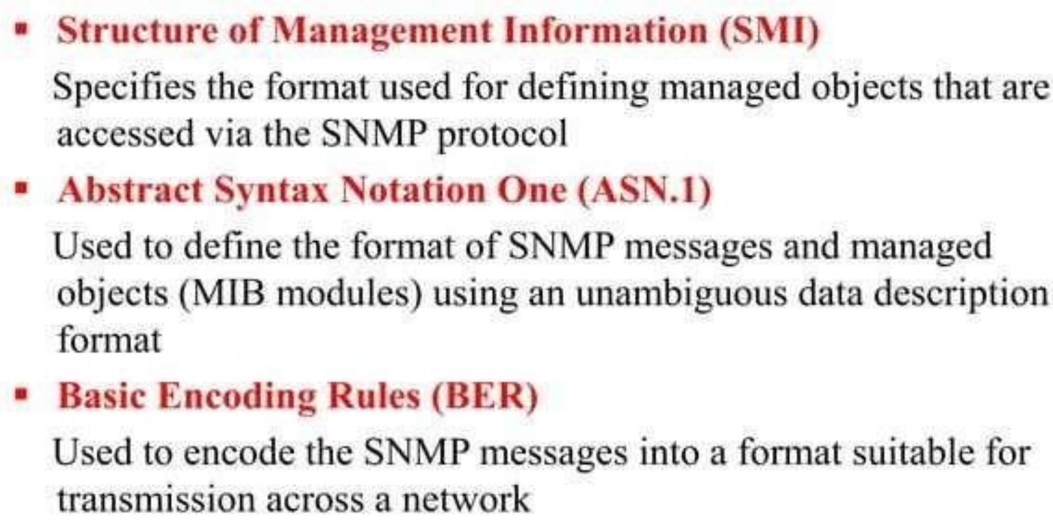


- **Simplicity:** Because SNMP uses UDP as its transmission protocol, it lacks many reliability and security issues.
- **Security:** Security has been a big concern with SNMPv1 and SNMPv2. Neither provides adequate security features such as management message authentication and encryption.
- **Alternative :**The Common Management Information Protocol (CMIP) is another alternative to network management.

SNMP SECURITY

- Lacks authentication. Vulnerable to the variety of security threats.
- Vulnerable to masquerading, modification of information, time modifications, message sequencing and disclosures.
- Message sequence and timing modifications occurs when an entity who is unauthorized reorders, delays, or copies and later replays a message generated by an authorized entity.

Languages of SNMP



- **Structure of Management Information (SMI)**

  Specifies the format used for defining managed objects that are accessed via the SNMP protocol

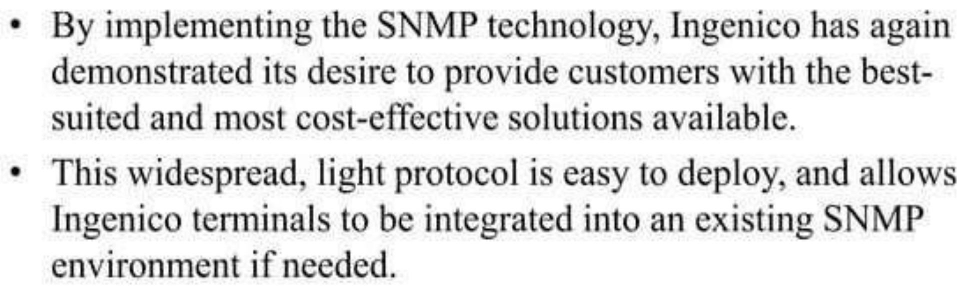
- **Abstract Syntax Notation One (ASN.1)**

  Used to define the format of SNMP messages and managed objects (MIB modules) using an unambiguous data description format

- **Basic Encoding Rules (BER)**

  Used to encode the SNMP messages into a format suitable for transmission across a network

CONCLUSION



- By implementing the SNMP technology, Ingenico has again demonstrated its desire to provide customers with the best-suited and most cost-effective solutions available.
- This widespread, light protocol is easy to deploy, and allows Ingenico terminals to be integrated into an existing SNMP environment if needed.

THANK YOU