UNIT – 5
Computer Network Security (ngmt)

★ Network Management System :–

→ It is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

→ Network management system components assist with –

1. Network device directory – It is used to identifying what devices are present on a network.

2. Network device monitoring – It is used to monitoring at the device level to determine the health of network components.

3. Network performance analysis – It is tracking performance indicators such as bandwidth utilisation, packet loss, latency, availability and up time of routers, switches and other simple network management protocol (SNMP) enabled devices.

4. Intelligent notifications – It is some configurable alerts that will respond to specific network scenarios by paging, e-mailing, calling or texting a network administrator.

★ SNMP Architecture :–

→ The fullform of SNMP is "Simple Network Management Protocol."

→ In 1988, the specification for SNMP was issued and rapidly became the dominant network management standard.

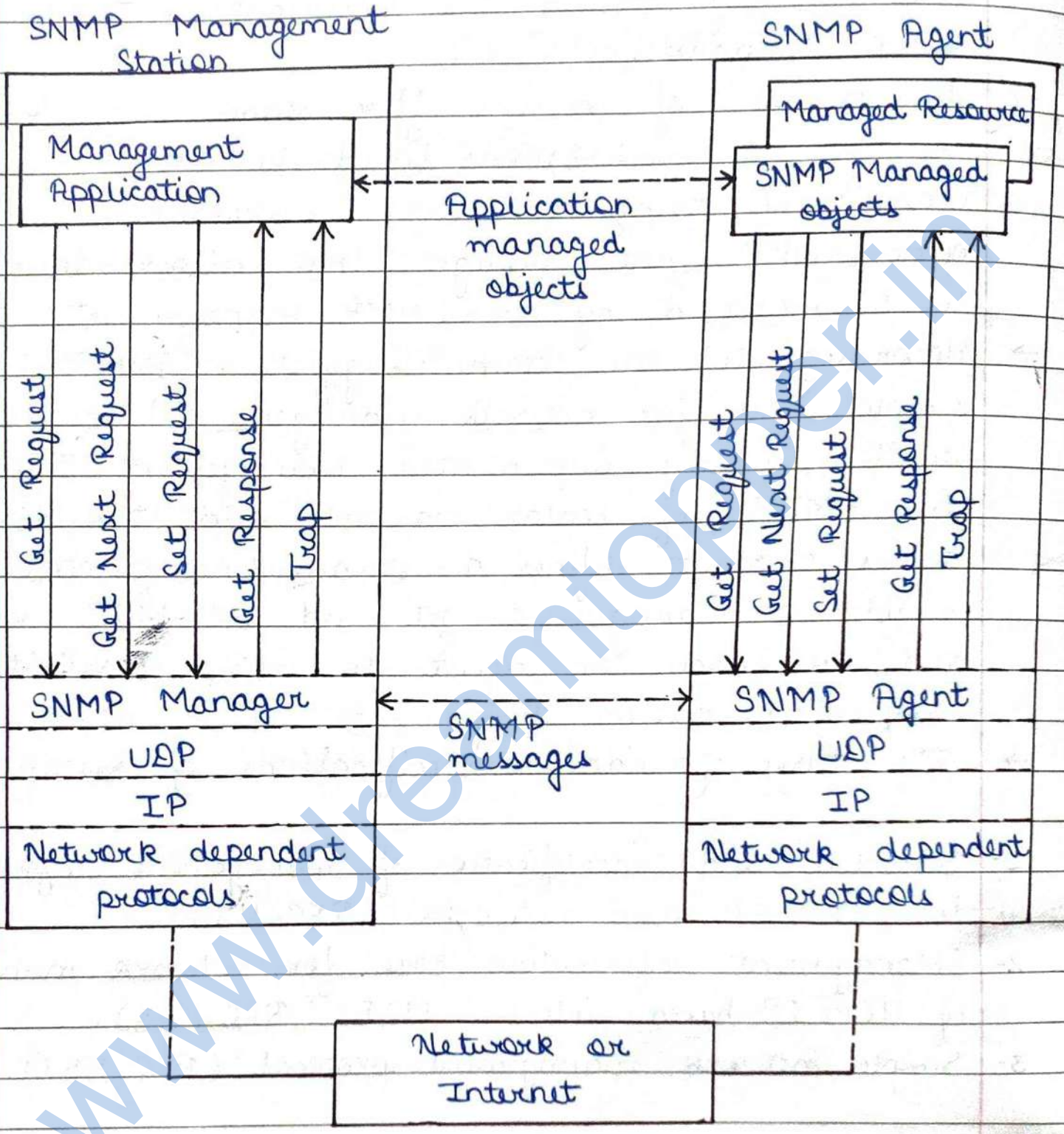
→ The number of vendors offer stand-alone network management workstations based on SNMP, most vendors of bridges, routers, workstations and PCs, offer SNMP agent packages that allow their products to be managed by an SNMP management station.

→ According to the name suggests, SNMP is a simple tool for network management. It defines a limited, easily implemented Management Information Base (MIB) of scalar variable and two dimensional tables and it defines a stream lined protocol to enable a manager to get and set MIB variables and to enable an agent to issue unsolicited notification called traps.

→ The three foundation specifications of SNMP are—

1- Structure and identification of management information for TCP/IP based networks (RFC 1155).
2- Management Information Base for network management of TCP/IP based internet MIB (RFC 1213).
3- Simple network management protocol (RFC 1157).

- SNMP Architecture Diagram —



SNMP Entity :- Each SNMP entity includes a single SNMP engine. An SNMP engine implements functions for sending and receiving messages, authenticating and encrypting / decrypting messages and controlling access to managed objects.

★ SNMPv1 Community Facility —

→ SNMP v1, as defined in RFC 1157, provides only a very basic or simple rudimentary security facility based on the concept of community. This facility gives a certain level of security but is open to various attacks.

→ The application involves a one to many relationship between a manager and a set of agents, the manager is able to get and set objects in the agents and is able to received traps from the agents.

→ Thus, from an operational or control point of view, the manager "manages" a number of agents.

→ We also need to be able to view SNMP, network management as a one to many relationship between an agent and a set of managers.

→ Each agent controls its own local MIB and must be able to control the use of that MIB by a number of managers.

→ There are three aspects of this control —

1. Authentication service
2. Access service
3. Proxy service

1- Authentication service in SNMPv1 community facility-

→ The purpose of the SNMPv1 authentication service is to assure the recipient that an SNMPv1 message is from the source that it claims to be from.

→ SNMPv1 only provides for a trivial scheme for authentication. Every message (get or put request) from a manager to an agent includes a community name, this name functions as a password, and the message is assumed to be authentic if the sender knows

the password.

→ The community name could be used to trigger an authentication procedure, with the name functioning simply as an initial password screening device. The authentication procedure could involve the use of encryption/decryption for more secure authentication functions. This is beyond the scope of RFC 1157.

2- Access policy in SNMP — By defining a community, an agent limits access to its MIB to selected set of managers. By the use of more than one community, the agent can provide different categories of MIB access to different managers. There are two aspects to this access control —

(a) SNMP MIB view — A subset of the objects within an MIB. Different MIB views may be defined for each community.

(b) SNMP access mode — An element of the set [READ-ONLY, READ-WRITE]. An access mode is defined for each community. The combination of an MIB views and access mode is referred to as an SNMP community profile. Thus a community profile consists of a defined subset of the MIB at the agent, plus an access mode for those objects. An SNMP community profile is referred to as an SNMP access policy.

3- Proxy service in SNMP — The community concept is also useful in supporting the proxy service.

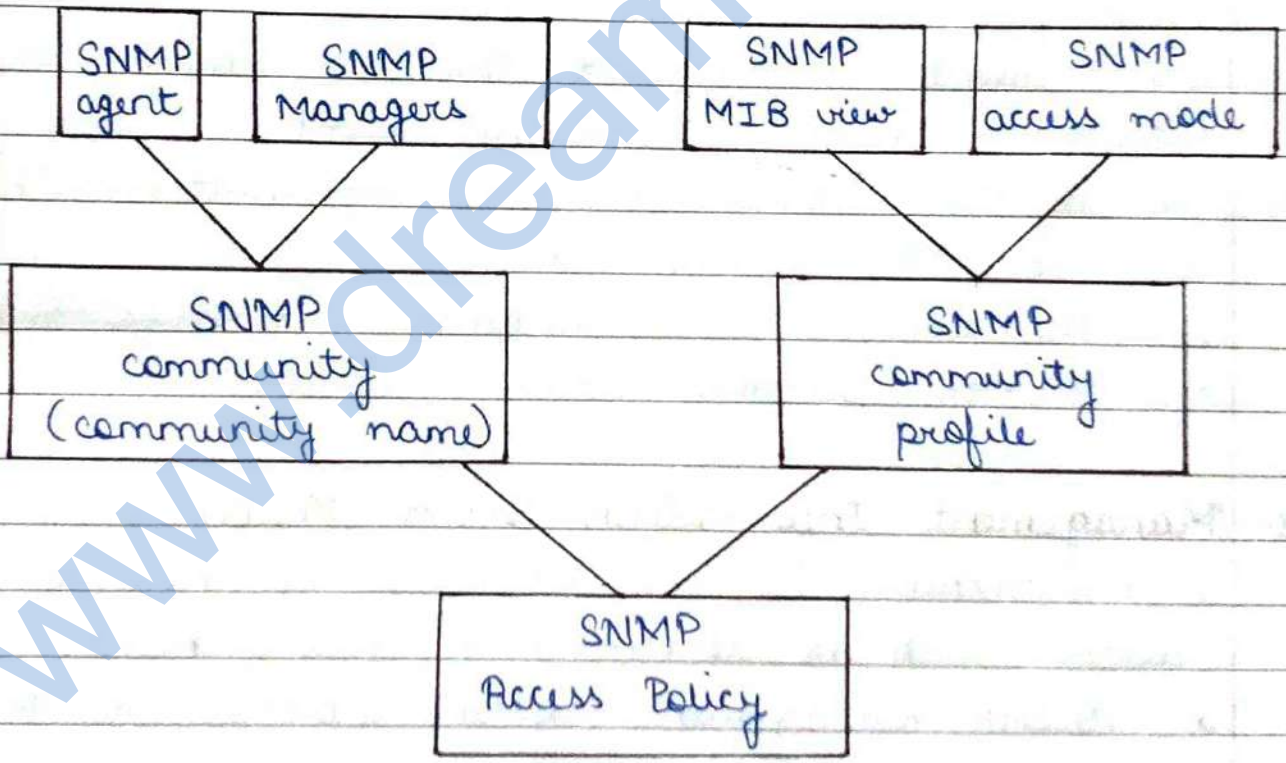
→ Proxy is an SNMP agent that acts on behalf of

other devices. Typically, the other devices are foreign. In this sense, that they do not support TCP/IP and SNMP.

→ In some cases, the proxied system may support SNMP but the proxy is used to minimize the interaction between the proxied device and network management system.

→ For each device that the proxy system represents, it maintains an SNMP access policy. Thus the proxy knows which MIB objects can be used to manage the proxied system (the MIB view) and their access mode.

Diagram of SNMPv1 administrative concepts —



Key Elements of SNMP :-

1. Management Station
2. Management Agent
3. Management information base
4. Network management protocol

1- Management Station — It is typically a stand alone device, but may be a capability implemented on a shared device. It serves as a interface for the human network manager into the network management system. It is a set of management applications for data analysis, fault recovery and so on. It is an interface by which the network may monitor and control the network.

2. Management, Managers & Agents —

→ A management stations, called a manager. It is a host that runs the SNMP client program.

→ A managed station, called an agent. It is a router (or a host) that runs the SNMP server program.

→ Management is achieved through simple interaction between a manager and an agent.

→ The agents keeps performance information in a database. The manager has access to the values in the database. The manager can also make the router perform certain actions.

3- Management Information Based (MIB) — MIB is a hierarchical virtual database of network objects (devices such as routers, switches, hubs) describing a network management system (NMS). An MIB is used by SNMP and Remote Monitoring 1 (RMON1)

4- Network Management Protocol —

→ The management station and agents are linked by a network management protocol.

→ The protocol used for the management of TCP/IP

networks is the SNMP. It involves following key capabilities.

Get — Enables the management station to retrieve the value of objects at the agent.

Set — Enables the management station to set the value of objects at the agent.

Nolify — Enables an agent to notify the management station of significant events.

★ SNMPv3 :-

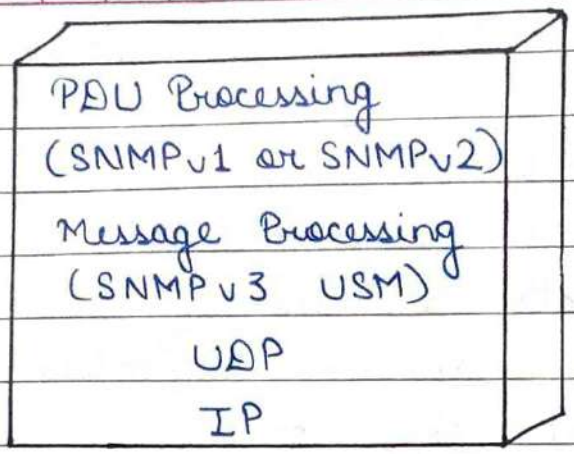
→ In 1998, the IETF, SNMPv3 working group produced a set of proposed internet standards, currently RFC, 2570 through 2576.

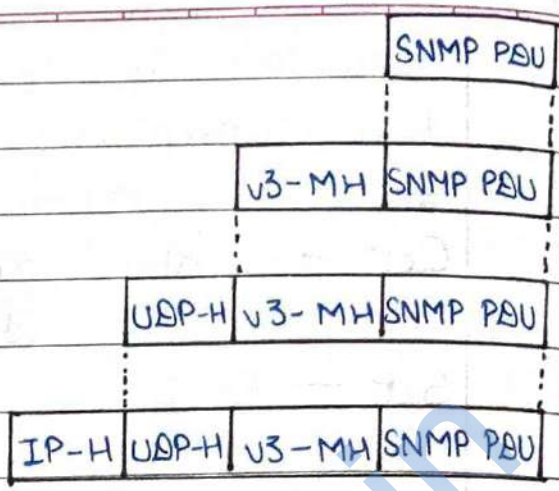
→ This documents set defines a framework for incorporating security features into an overall capabilities that includes either SNMPv1 or SNMPv2 functionality. In addition the documents define a specific set of security and access control.

→ It is important to realise that SNMPv3 is not a stand-alone replacement per SNMPv1 and/or SNMPv2. SNMPv3 defines a security capability to be used in conjunction with SNMPv2 (preferred) or SNMPv1.

→ In addition RFC 2571 describes an architecture within which all current and future version of SNMP fit.

→ RFC 2575 describes an access control facility, which is intended to operate independently of the core SNMPv3 capability.





here IP-H = IP header
UDP-H = UDP header
v3-MH = SNMPv3 message header
PDU = Protocol data unit

→ Information are exchanged between a management station and an agent in the form of SNMP message.

- SNMPv3 Terminology :-
Some SNMPv3 terms are introduced in RFC 2271. Some important SNMPv3 terms are as follows-

1- SNMP Engine ID — Unique and unambiguous identifier of an SNMP engine, as well as the SNMP entity that corresponding to that engine.

2- Context Engine ID — Uniquely identifies as SNMP entity that may realise an instance of a context with a particular context name.

3- Context Name — Identifies a particular context within an SNMP engine. It is passed as a parameter to the dispatcher and access control subsystem.

4- Scoped PDU — A block of data consisting of a context engine ID, a context name and an SNMP PDU. It is passed as a parameter to/from the security subsystem.

5- SNMP Message Processing Model — Unique identifier of a message processing model of the message processing subsystem. Possible values include SNMPv1, SNMPv2, SNMPv3.

6- SNMP Security Model — Unique identifier of a security subsystem. Possible values include SNMPv1, SNMPv2 and USM.

7- SNMP Security Level — A level of security at which SNMP messages can be sent or with which operations are being processed, expressed in terms of whether or not authentication and/or privacy are provided. The alternative values are no authpriv, authNoPriv and authpriv.

8- Principal — The entity on whose behalf services are provided or processing takes place. A principal can be an individual acting in a particular role, a set of individuals, with each acting in a particular role, an application or set of applications and combinations thereof.

9- Security Name — A human-readable string representing a principal. It is passed as a parameter in all of the SNMP primitives (dispatcher, message processing, security, access control).

★ VACM (View Based Access Control Model) :-

→ It is an SNMPv3 mechanism regulates access to MIB objects by providing a fine-grained access control mechanism associating users with MIB views.

→ The VACM facilities are essential in ensuring a completely secure agent.

→ There are five elements defined in VACM model -

(a) Groups
(b) Security level
(c) Contexts
(d) MIB views
(e) Access policy

→ VACM has two important characteristics -

1- VACM determines whether access to a managed object in a local MIB by a remote principal should be allowed.

2- VACM makes use of an MIB that -

(a) define the access control policy for this agent.
(b) makes it possible for remote configuration to be used.

- Motivation in VACM — The concept that make up VACM appear to result in a rather complex definition of access control. The motivations for introducing those concepts are to clarify the relationships involved in accessing management information and to minimize the storage and processing requirements at the agent.

★ SNMPv2 :-

→ The strength of SNMPv2 is its simplicity. SNMP provides a basic set of network management tools in a package that is easy to implement and easy to configure.

→ However, as users have come to reply its deficiencies have become all the apparent.

→ These defficiencies fall into three categories -

(1-) Lack of support for distributed network management.

(2-) Functional deficiencies

(3-) Security deficiencies

→ The first two categories of defficiencies are addressed in SNMPv2 which was issued in 1993, with a revised version issued in 1996 (currently RFCs 1901, 1904 through 1908, 2578 & 2579).

→ SNMPv2 quickly gained support and a number of vendors announced products within months of the issuance of the standard. The security defficiencies have been address in SNMPv3.

Q- Compare and contrast - SNMPv1 and SNMPv3

★ Comparision between SNMPv1 & SNMPv3 :-

	Basis of comparision	SNMPv1	SNMPv3
1-	Version	It was the Ist version of SNMP.	It is the newest version of SNMP.
2-	Goal	Open and standard protocol.	Uses SNMPv2 protocol operations.

3-	Support	Smaller RTUs commonly support SNMPv1.	Net guardian 832A is one RTU that supports SNMPv3.
4-	Security	No security from someone with access to the network.	Enhanced security
5-	Complexity	Performance and security limitations.	Focuses on improving the security aspect.
6-	Message format	Five messages - GetRequest, GetNextRequest, SetRequest, Trap, Response.	Implements SNMPv1 and SNMPv2 specifications along with proposed new features.