5 Network Management Security and Network Access Control

Syllabus

At the end of this unit, you should be able to understand and comprehend the following syllabus topics :

- Network Management Security - SNMPv3
- Network Access Control (NAC)
  - Principle elements of NAC
  - Principle NAC enforcement methods
  - How to implement NAC Solutions
  - Use cases for Network Access Control

5.1 Introduction to Networking Components

A computer network could be very simple to very complex depending upon where you are looking from and what you are looking at. For example, if you are on your phone, then all you need to do is to just connect it to a service provider, such as `Airtel` or Vodafone, and boom you are connected to the world. It is a simple and straightforward process without realising any complexities behind how you can make voice calls and consume internet data.

However, computer networking for offices, web servers, internet media streaming, etc. are quite complex and require fair amount of understanding to correctly establish and then operate with minimal downtime so as to serve the global consumers. Following are some of the common and major components that are often involved in setting up a computer network.

1. **Servers :** Servers are computers that hold shared files, programs, or any other computing resources. They run an operating system such as Windows or Linux Server or any other specially designed server software. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions.

   For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few.

   Sometimes it is also called host computer. Servers are powerful computers that store data or application and connect to resources that are shared by the user of a network.

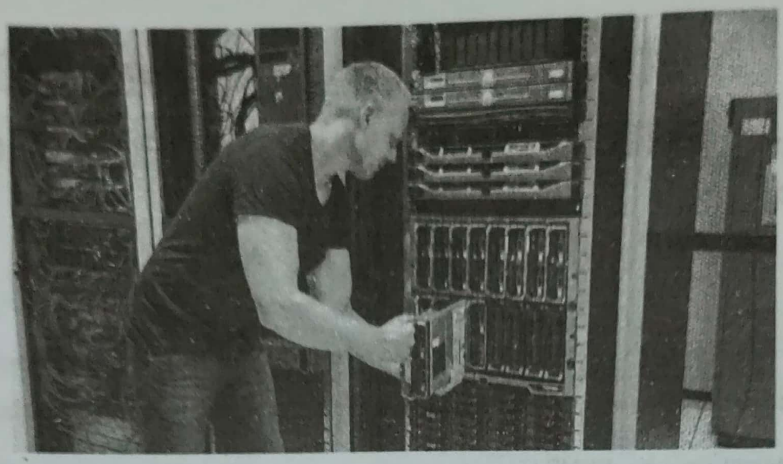

Fig. 5.1.1

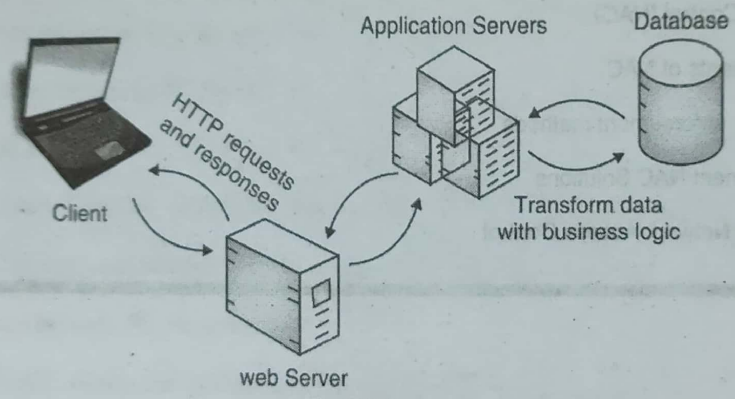

Fig. 5.1.2

2. **Clients :** Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive services from the servers.

   These days, it is typical for a client to be a personal computer that the users also use for their own non-network applications. A client could be a mobile phone, tablet, TV, laptop, desktop, Amazon Alexa, Google home, or any other device in any other form factor that can connect to a network and interact with the server providing the resources over the network.

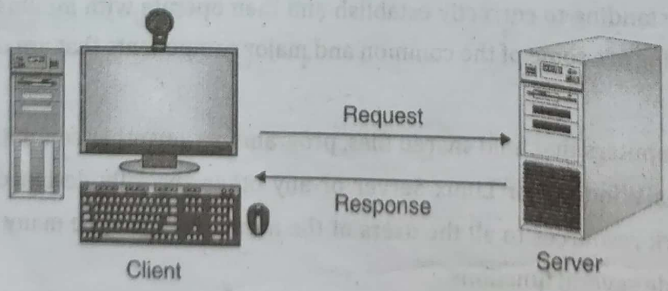

Fig. 5.1.3

3. **Transmission Media :** Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fibre cable. Transmission media are sometimes called transmission medium channels, links or lines.

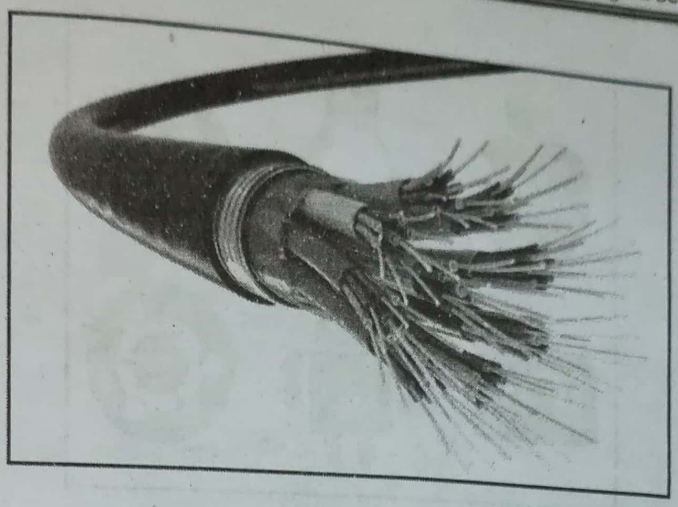

Fig. 5.1.4

4. **Shared data :** Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.

5. **Shared printers and other peripherals :** Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

6. **Network Interface Card (NIC) :** Each computer in a network has a special expansion card called a network interface card (NIC).

   The NIC prepares(formats) and sends data, receives data, and controls data flow between the computer and the network.

   On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.

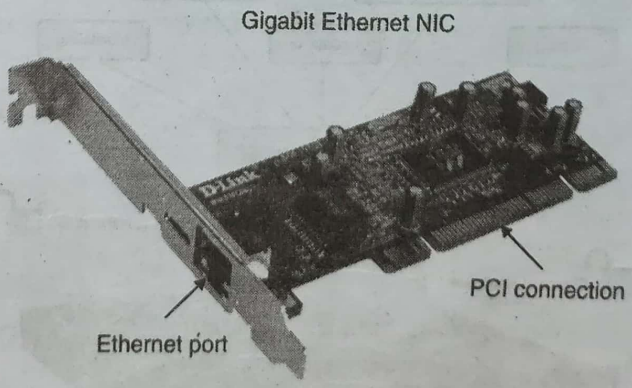

Fig. 5.1.5

7. **Local Operating System :** A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer.

   Some examples of local OS are Windows 10, Ubuntu, MacOS, Android, iOS, etc. Local OS contains drivers for network communication. You don't need to install any other software just for networking.

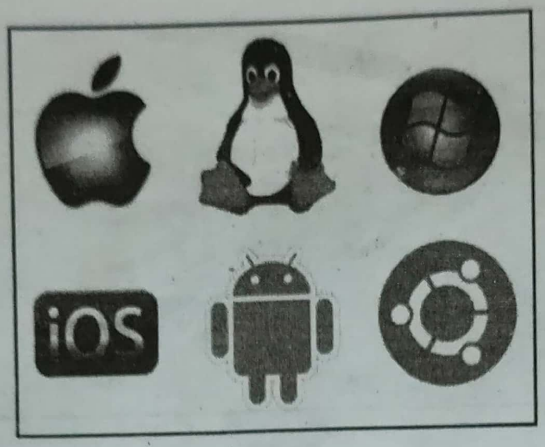

Fig. 5.1.6

8. **Network Operating System :** The network operating system runs on specialised networking devices, such as routers and switches, that help to establish and operate a computer network.

Some examples of network OS are Cisco `iOS`, Juniper's `Junos`, Onyx, Cumulus, etc.

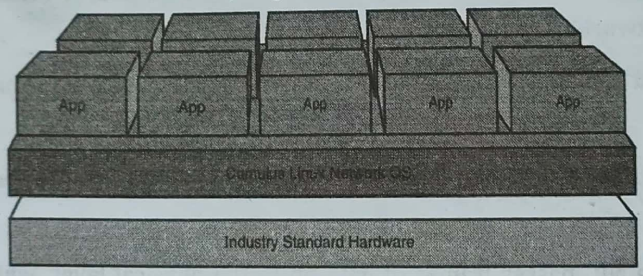

Fig. 5.1.7

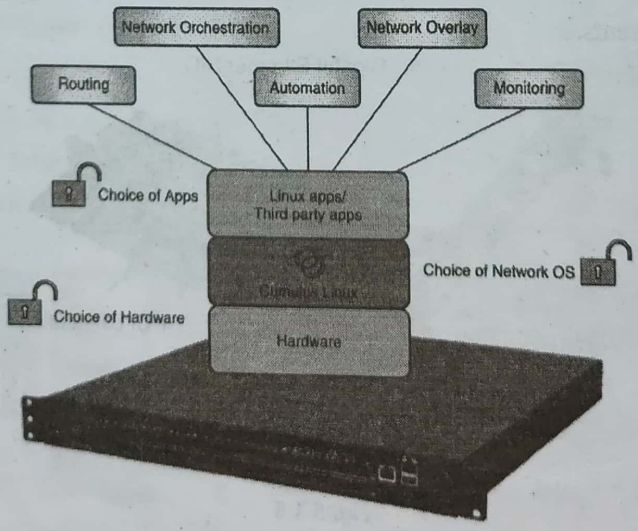

Fig. 5.1.8

9. **Hub :** Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer requests information from a network or a specific computer, it sends the request to the hub through a cable.

The hub will receive the request and transmit it to the entire network.

Each computer in the network should then figure out whether the broadcasted data is for them or not and respond appropriately.

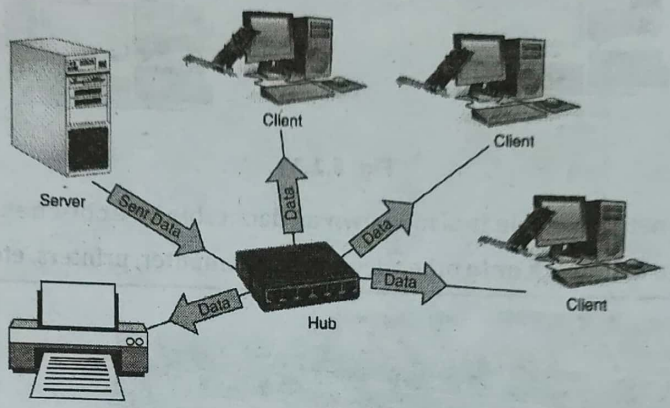

Fig. 5.1.9

10. **Switch :** Switch is similar to a hub but is built in with advanced features. It uses physical device addresses (called MAC address) in each incoming messages so that it can deliver the message to the right destination or port instead of just broadcasting the information to the entire network. Unlike a hub, switch doesn't broadcast the received message to entire network, rather before sending, it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network.

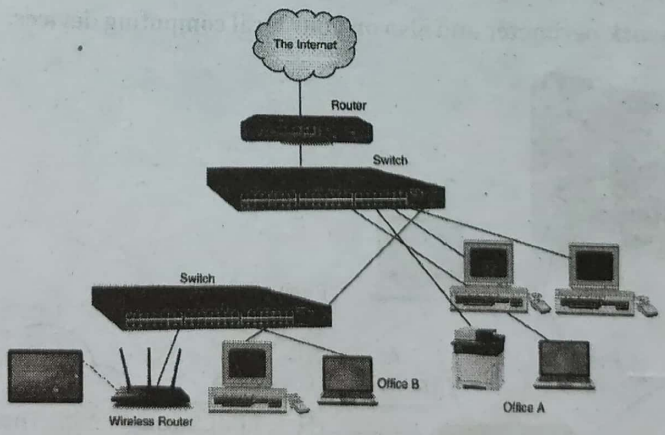

Fig. 5.1.10

11. **Router :** Routers is a networking device that is used to connect two different networks. For example, when you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router. In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks.

There are two types of Router - wired and wireless. The choice depends on your requirements.

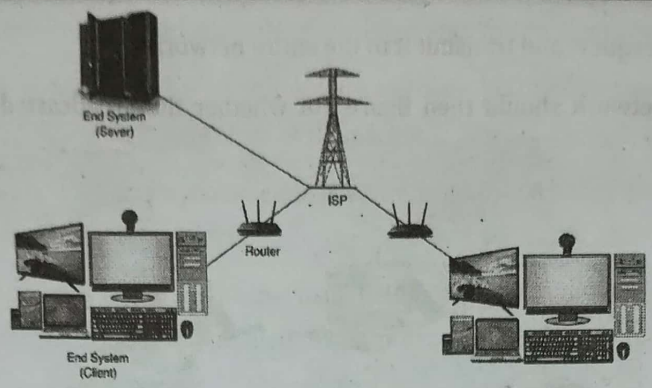

Fig. 5.1.11

12. **LAN Cable :** A local area network cable is also known as data cable or ethernet cable which is a wired cable used to connect a device to a network or to other devices like computer, printers, etc.

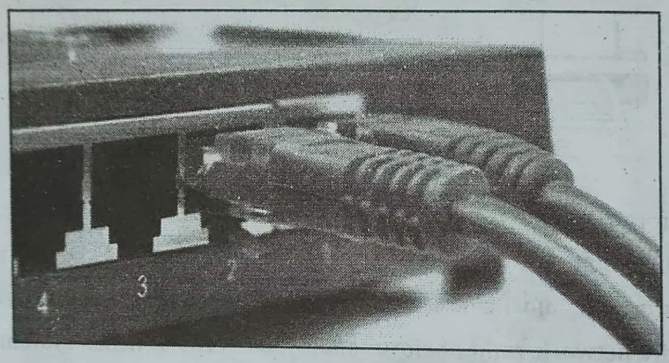

Fig. 5.1.12

13. **Firewall :** Firewall is used to protect your computing device from malicious or unwanted network traffic. It is usually configured at network perimeter and also on your local computing devices.

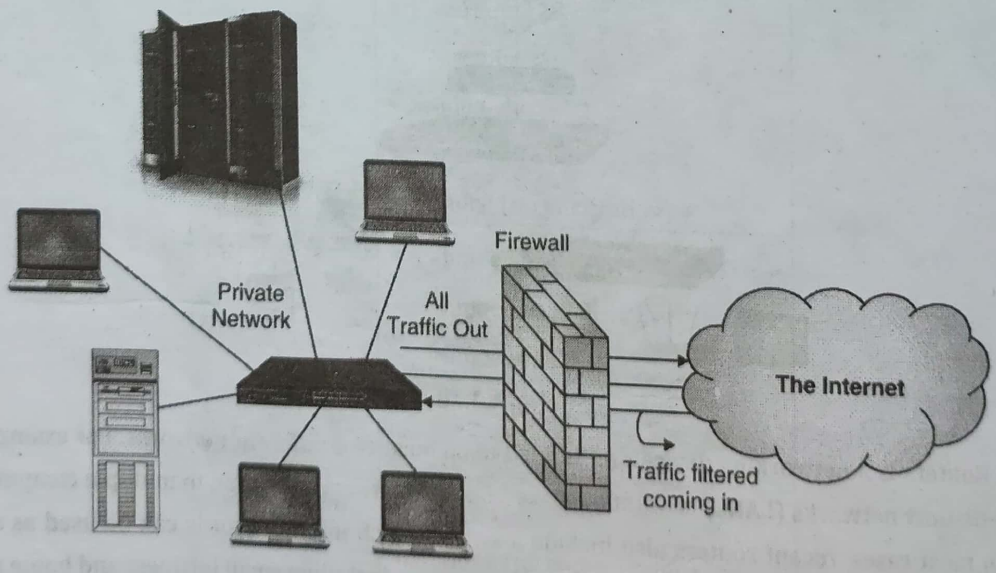

Fig. 5.1.13

5.2 Network Management Security - SNMPv3

Before you learn about SNMPv3, let's spend time and understand SNMP-based network management in brief.

5.2.1 What is SNMP?

In today's complex network of routers, switches, and servers, it can seem like a daunting task to manage all the devices on your network and make sure that they are not only up and running but also performing optimally. This is where the Simple Network Management Protocol (SNMP) can help. SNMP was introduced in 1988 to meet the growing need for a standard for managing Internet Protocol (IP) devices.

Definition : *SNMP provides a simple set of operations that allows you to manage network devices remotely.*

The core of SNMP is a simple set of operations (and the information these operations gather) that gives administrators the ability to change the state of some SNMP-based device. For example, you can use SNMP to shut down an interface on your router or check the speed at which your Ethernet interface is operating. SNMP can even monitor the temperature on your switch and warn you when it is too high.

5.2.2 How SNMP Works?

The Fig. 5.2.1 illustrates a very simplistic view of how SNMP works.

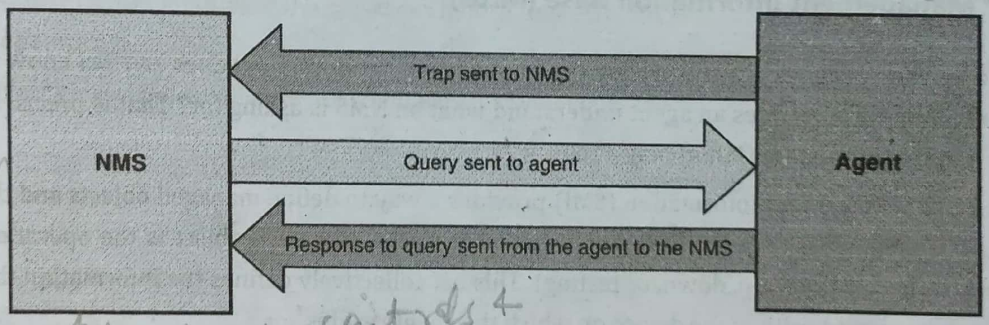

Fig. 5.2.1

At a high-level, there are two kind of entities involved in a SNMP managed network infrastructure - SNMP Managers and SNMP Agents .

Definition : *A SNMP manager is a server running some kind of software system that can handle management tasks for a network.*

- SNMP Managers are often referred to as Network Management Stations (NMSs).An NMS is responsible for polling and receiving traps from SNMP agents in the network. A poll, in the context of network management, is the act of querying an agent (router, switch,
- Unix server, etc.) for some piece of information. This information can be used later to determine if some sort of catastrophic event has occurred. A trap is a way for the agent to tell the NMS that something has happened. Traps are sent asynchronously by the agent on its own without queries from the NMS. The NMS is further responsible for performing an action based upon the information it receives from the agent.
- For example, when a router interface goes down, then it can send a trap to your NMS informing about the same. In turn, the NMS can take some corrective actions automatically to fix the problem or notify network administrators who could look into the situation further and take the required actions.

The second entity is the SNMP agent.

Definition : *SNMP agent is a piece of software that runs on the network devices you are managing.*

- It can be a separate program, or it can be incorporated into the operating system (for example, Cisco's IOS on a router, or the low-level operating system that controls a UPS). Today, most IP devices come with some kind of SNMP agent built-in. The fact that vendors are willing to implement agents in many of their products makes the system administrator's or network manager's job easier.
- The agent provides management information to the NMS by keeping track of various operational aspects of the device. For example, the agent on a router is able to keep track of the state of each of its interfaces - which ones are up, which ones are down, etc.
- The NMS can query the status of each interface and take appropriate action if any of them are down. When the agent notices that something bad has happened, it can send a trap to the NMS. This trap originates from the agent and is sent to the NMS, where it is handled appropriately. Some devices also send a corresponding "all clear" trap when there is a transition from a bad state to a good state.
- This can be useful in determining when a problem situation has been resolved. It is important to keep in mind that polls and traps can happen at the same time. There are no restrictions on when the NMS can query the agent or when the agent can send a trap.

5.2.3 SNMP Management Information Base (MIBs)

- There could be various types of network devices from various vendors. How does an NMS know what it can ask an agent for? Similarly, how does an agent understand what an NMS is asking for? That is precisely where SNMP Management Information Base (MIBs) play a role.
- The Structure of Management Information (SMI) provides a way to define managed objects and their behaviour. An agent has in its possession a list of the objects that it tracks. One such object is the operational status of a router interface (for example, up, down, or testing). This list collectively defines the information the NMS can use to determine the overall health of the device on which the agent resides.
- The Management Information Base (MIB) can be thought of as a database of managed objects that the agent tracks. Any sort of status or statistical information that can be accessed by the NMS is defined in a MIB. The SMI provides a way to define managed objects while the MIB is the definition (using the SMI syntax) of the objects themselves. Like a dictionary, which shows how to spell a word and then gives its meaning or definition, a MIB defines a textual name for a managed object and explains its meaning.
- An agent may implement many MIBs, but all agents implement a particular MIB called MIB-II (RFC 1213). This standard defines variables for things such as interface statistics (interface speeds, MTU, octets sent, octets received, etc.) as well as various other things pertaining to the system itself (system location, system contact, etc.). The main goal of MIB-II is to provide general TCP/IP management information. It does not cover every possible item a vendor may want to manage within its particular device. A vendor typically publishes its own MIBs corresponding to the network devices that it sells. For example, consider a vendor that is bringing a new router to market. The agent built into the router will respond to NMS requests (or send traps to the NMS) for the variables defined by the MIB-II standard. It probably also implements MIBs for the interface types it provides. In addition, the router may have some significant new features that are worth monitoring but are not covered by any standard MIB. So, the vendor defines its own MIB (sometimes referred to as a proprietary MIB) that implements managed objects for the status and statistical information of its new router.

- Note here that simply loading a new MIB into your NMS does not necessarily allow you to retrieve the data / values / objects, etc., defined within that MIB. You need to load only those MIBs supported by the agents from which you are requesting queries.
- The definition of managed objects can be broken down into three attributes as following.

1. Name : The name, or object identifier (OID), uniquely defines a managed object. Names commonly appear in two forms: numeric and "human readable". In either case, the names are long and inconvenient. In SNMP applications, a lot of work goes into helping you navigate through the namespace conveniently.
2. Type and syntax : A managed object's `datatype` is defined using a subset of Abstract Syntax Notation One (ASN.1). ASN.1 is a way of specifying how data is represented and transmitted between managers and agents, within the context of SNMP. The nice thing about ASN.1 is that the notation is machine independent. This means that a PC running Windows 10 can communicate with a Linux machine and not have to worry about things such as byte ordering.
3. Encoding : A single instance of a managed object is encoded into a string of octets using the Basic Encoding Rules (BER). BER defines how the objects are encoded and decoded so that they can be transmitted over a transport medium such as Ethernet.

- Managed objects are organised into a treelike hierarchy. This structure is the basis for SNMP's naming scheme. An object ID is made up of a series of integers based on the nodes in the tree, separated by dots (.). Although there is a human-readable form that is friendlier than a string of numbers, this form is nothing more than a series of names separated by dots, each representing a node of the tree. You can use the numbers themselves, or you can use a sequence of names that represent the numbers. The Fig. 5.2.2 shows the top few levels of this tree.

MIB TREE DIAGRAM

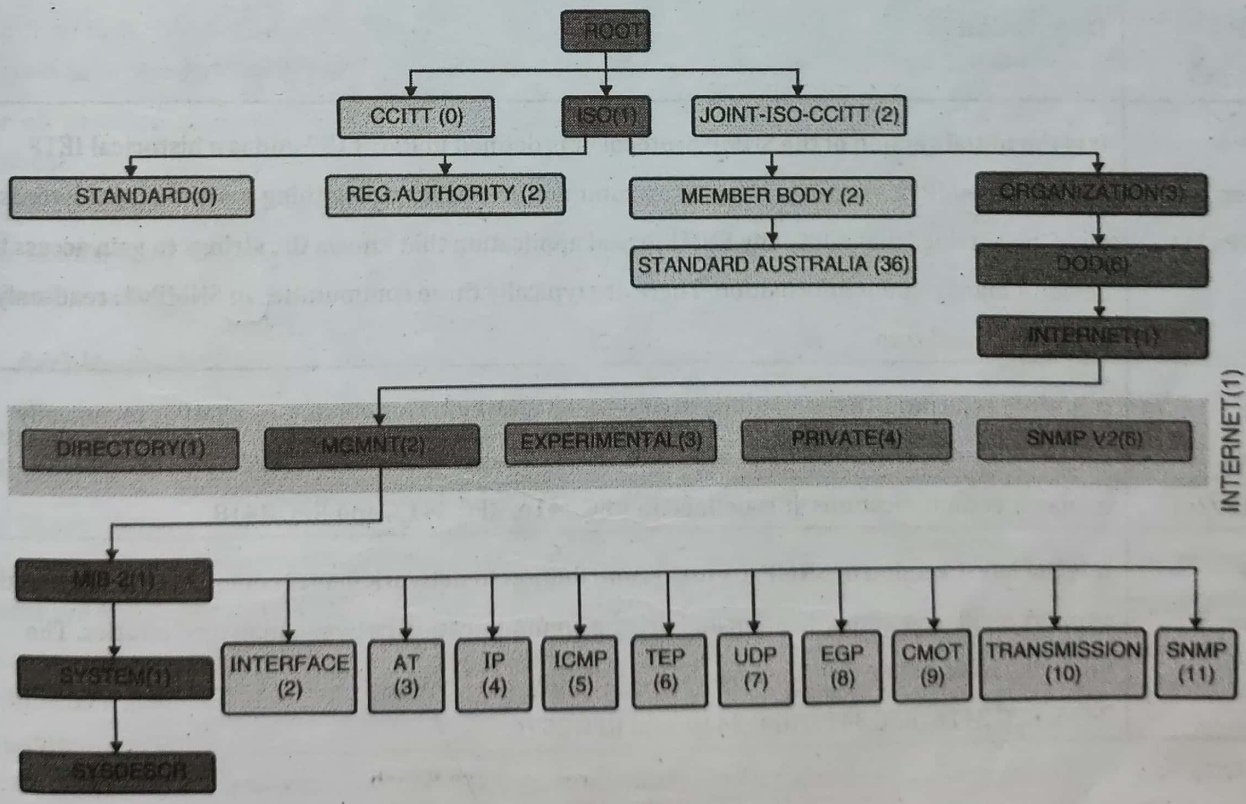

Fig. 5.2.2

- To provide an example from the Fig. 5.2.2, the OID of sysDescr is ".1.3.6.1.2.1.1.1", which can be found by following the path from ROOT to sysDescr as following.
  - ISO is .1
  - ORGANIZATION is .3
  - DOD is .6
  - INTERNET is .1
  - MGMT is .2
  - MIB-2 is .1
  - SYSTEM is .1
  - sysDescr is .1

Communication strings act as a form of authentication between the SNMP client & SNMP agent. It is like a user ID or password that allows access to the SNMP agent for eg, a router's, firewalls or other network device statistics

- In the object tree, the node at the top of the tree is called the root, anything with children is called a subtree, and anything without children is called a leaf node.

Polling is process of querying an SNMP-enabled device for information eg current state, configuration.

5.2.4 SNMP Versions

The Table 5.2.1 summarises the SNMP versions.

Table 5.2.1

SNMP Version	Description
SNMP version 1 (SNMPv1)	It is the initial version of the SNMP protocol. It is defined in RFC 1157 and is a historical IETF standard. SNMPv1's security is based on communities, which are nothing more than passwords: plain-text strings that allow any SNMP-based application that knows the strings to gain access to a device's management information. There are typically three communities in SNMPv1: read-only, read-write, and trap.
SNMP version 2 (SNMPv2c)	It is often referred to as community-string-based SNMPv2. This version of SNMP is technically called SNMPv2c. It includes improvements in the areas of performance, security and manager-to-manager communications. It is defined in RFC 3416, RFC 3417, and RFC 3418.
SNMP version 3 (SNMPv3)	It is the latest version of SNMP. Its main contribution to network management is security. It adds support for strong authentication and private communication between managed entities. The following RFCs define the standard: RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418, and RFC 2576.

RFC - request for comment by such as IETF, W3C

5.2.5 Comparison between SNMP Versions

The Table 5.2.2 provides a quick comparison between the SNMP versions focusing on security aspects.

Table 5.2.2

Comparison Attribute	SNMPv1	SNMPv2	SNMPv3
Used today	No	Yes, but less commonly	Yes, most commonly
Encryption (Privacy)	No	No	Yes
Authentication	No	No	Yes
Community Strings	Yes	Yes	No
Username	No	No	Yes

5.2.6 Security Enhancements in SNMPv3

- Now that you have covered basics of SNMP, let's learn about the security enhancements in SNMPv3.
- Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent.
- Any security-conscious network or system administrator knows that clear-text passwords provide no real security at all. It is trivial for someone to intercept the community string, and once she has it, she can use it to retrieve information from devices on your network, modify their configuration, and even shut them down.
- The Simple Network Management Protocol Version 3 (SNMPv3) addresses the security problems that have plagued both SNMPv1 and SNMPv2.
- For all practical purposes, security is the only issue SNMPv3 addresses; there are no other changes to the protocol.
- There are no new operations; SNMPv3 supports all the operations defined by versions 1 and 2. There are several new textual conventions, but these are really just more precise ways of interpreting the datatypes that were defined in earlier versions.

5.2.7 Architecture Change in SNMPv3 for Security

- Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, its developers have managed to make things look much different by introducing new textual conventions, concepts, and terminology.
- The most important change is that Version 3 abandons the notion of managers and agents. Both managers and agents are now called SNMP entities. Each entity consists of an SNMP engine and one or more SNMP applications.
- These new concepts are important because they define an architecture rather than simply a set of messages; the architecture helps to separate different pieces of the SNMP system in a way that makes a secure implementation possible.

RFC 3410 Request for comments

- The overall SNMPv3 architecture looks like the Fig. 5.2.3

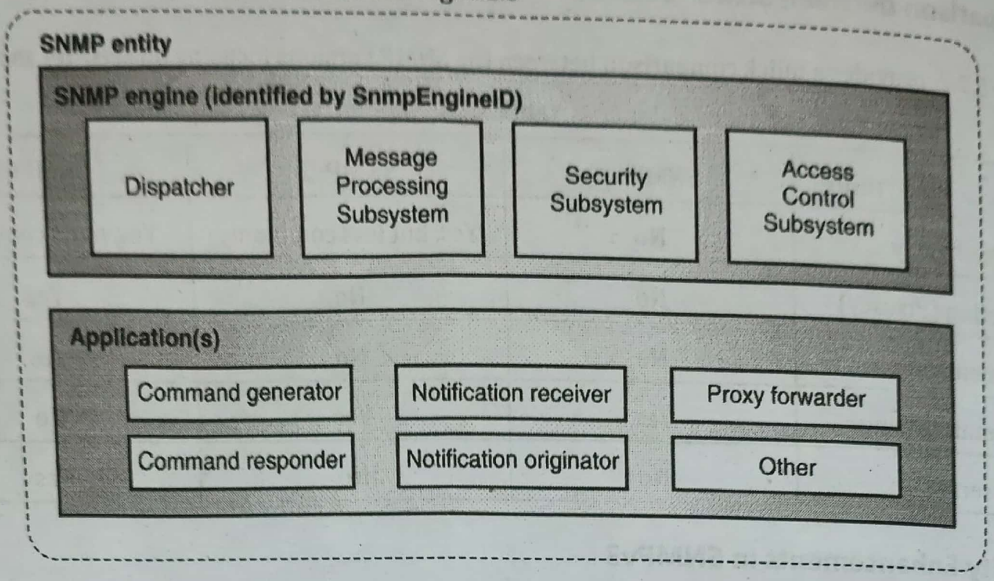

Fig. 5.2.3

- Let's learn about it in brief.

5.2.8 The SNMPv3 Engine

The engine is composed of four pieces.

1. **Dispatcher :** The Dispatcher's job is to send and receive messages. It tries to determine the version of each received message (i.e., v1, v2, or v3) and, if the version is supported, hands the message off to the Message Processing Subsystem. The Dispatcher also sends SNMP messages to other entities.
2. **Message Processing Subsystem :** The Message Processing Subsystem prepares messages to be sent and extracts data from received messages. A Message Processing Subsystem can contain multiple message processing modules. For example, a subsystem can have modules for processing SNMPv1, SNMPv2, and SNMPv3 requests. It may also contain a module for other processing models that are yet to be defined.
3. **Security Subsystem :** The Security Subsystem provides authentication and privacy services. Authentication uses either community strings (SNMP v1 and v2) or SNMPv3 user-based authentication. User-based authentication uses the MD5 or SHA algorithms to authenticate users without sending a password in the clear. The privacy service uses the DES or AES algorithm to encrypt and decrypt SNMP messages.
4. **Access Control Subsystem :** The Access Control Subsystem is responsible for controlling access to MIB objects. You can control what objects a user can access as well what operations she is allowed to perform on those objects. For example, you might want to limit a user's read-write access to certain parts of the mib-2 tree while allowing read-only access to the entire tree.

→ This technology provides commercial grade security & the ease of administration, which includes authentication, authorization, access control & privacy.

5.2.9 SNMPv3 Applications

SNMP version 3 divides (organises) most of the SNMP operations into SNMP applications.

1. **Command generator :** It generates `get`, `getnext`, `getbulk`, and set requests and processes the responses. This application is implemented by an NMS, so that it can issue queries and set requests against entities on routers, switches, Unix hosts, etc.
2. **Command responder :** It responds to `get`, `getnext`, `getbulk`, and `set` requests. This application is implemented by an entity such as a Cisco router or Unix host. For versions 1 and 2, the command responder is implemented by the SNMP agent.
3. **Notification originator :** It generates SNMP traps and notifications. This application is implemented by an entity such as a router or Unix host. For versions 1 and 2, the notification originator is part of an SNMP agent.
4. **Notification receiver :** It receives traps and inform messages. This application is implemented by an NMS.
5. **Proxy forwarder :** It facilitates message passing between entities.

RFC 3411 allows additional applications to be defined over time. This ability to extend the SNMPv3 framework is a significant advantage over the older SNMP versions.

5.3 User-based Security Model (USM)

- User-based Security Model (USM) is used within the SNMP Architecture to provide security services for SNMP. The idea is that the traditional concept of a user (identified by a `userName`) is used to associate security information with SNMP operations. The implementation level details are specified in RFC 3414.

5.3.1 Common Terms Used by USM

Let's understand some basic terminologies used by USM.

Table 5.3.1

Term	Description
`snmpEngineID`	This is an unambiguous identifier for an SNMP engine as well as the SNMP entity that corresponds to the engine.
`snmpEngineBoots`	A count of the number of times an SNMP engine has rebooted.
`snmpEngineTime`	The number of seconds since the `snmpEngineBoots` counter was last incremented.

Term	Description
snmpSecurityLevel	• There are three security levels. • The first is no authentication or privacy (noAuthNoPriv). Note that if this mode is used, a securityName is still required. • The second is authentication and no privacy (authNoPriv). • The third and final one is authentication and privacy (authPriv). While you can have authentication without privacy, you cannot have privacy without authentication.
Authoritative SNMP engine	A nonauthoritative engine must discover the snmpEngineId of the authoritative engine with which it communicates. The rules for designating the authoritative engine are as following : • If the SNMP message requires a response (get, getnext, getbulk, set, or inform), the receiver of these messages is authoritative. If the message does not require a response (trap or report), the sender of the message is authoritative. • Generally, an SNMP agent is authoritative, and an NMS is non authoritative.

5.3.2 SNMPv3 Packet Format

An SNMPv3 message (packet) format has the following fields.

Table 5.3.2

Field	Description
msgVersion	The SNMP version of the message, set to 3
msgID	Used between a manager and agent to coordinate request and response messages.
msgMaxSize	Maximum message size supported by a sender of an SNMP message.
msgFlags	An 8-bit value that specifies whether a report PDU is to be generated, whether privacy is used, and whether authentication is used.
msgSecurityModel	Specifies which security model was used by the sender of the message. Current values are 1, 2, and 3 for SNMPv1, SNMPv2c, and SNMPv3, respectively.
msgSecurityParameters	Contains security-specific information
contextEngineID	Uniquely identifies an SNMP entity
contextName	Identifies a particular context within an SNMP engine
scopedPDU	A block of data made up of a contextEngineID, contextName, and SNMP PDU

Field	Description
msgSecurityParameters	The msgSecurityParameters in an SNMPv3 message are as follows: • msgAuthoritativeEngineID : The snmpEngineID of the authoritative engine. • msgAuthoritativeEngineBoots : The snmpEngineBoots of the authoritative engine. • msgAuthoritativeEngineTime : The snmpEngineTime of the authoritative engine. • msgUserName : The user who may be authenticating and encrypting the message. • msgAuthenticationParameters : This value is null if no authentication is used. Otherwise, the field contains the computer HMAC message digest for the message. Currently the RFC specifies that MD5 and SHA must be used. • msgPrivacyParameters : This value is null if no encryption is used. Otherwise, this field is used to form the initial value of the Cipher Block Chaining mode of the Data Encryption Standard (CBC-DES) or AES algorithm.

The Fig. 5.3.1 shows the entire SNMPv3 message.

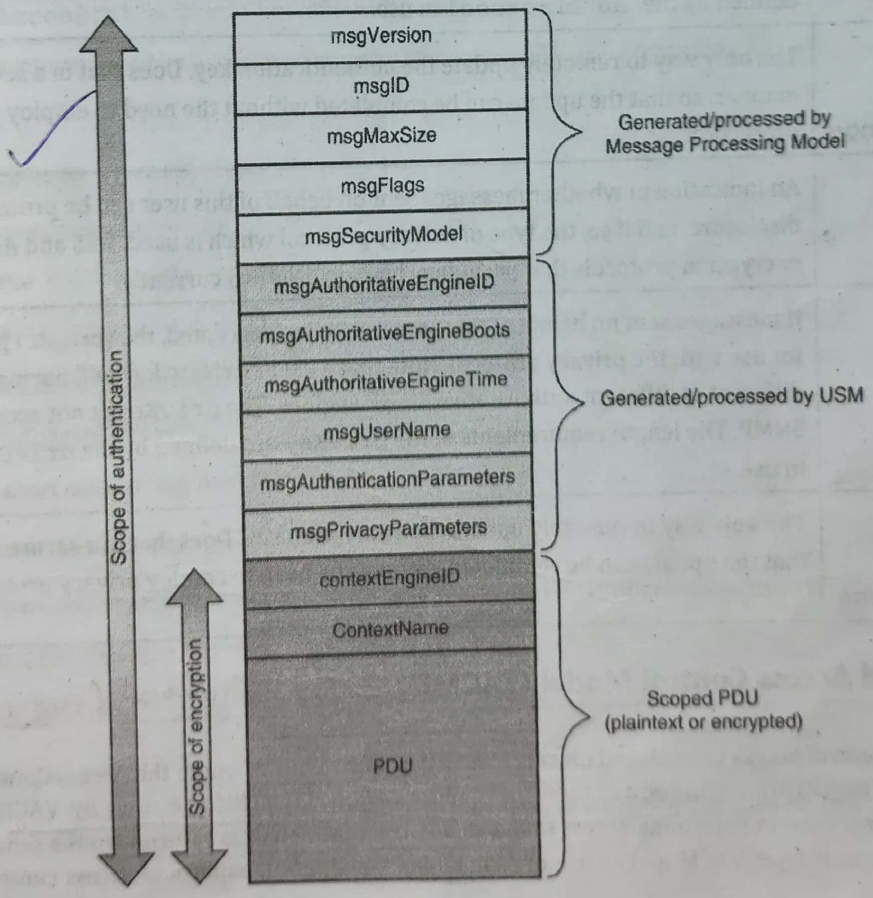

Fig. 5.3.1

5.3.3 SNMPv3 User Attributes

An SNMP engine that wishes to communicate with another SNMP engine must also have knowledge of a user known to that engine, including knowledge of the applicable attributes of that user. A user and its attributes are defined as following.

Table 5.3.3

Field	Description
`userName`	A string representing the name of the user.
`securityName`	A human-readable string representing the user in a format that is Security Model independent. There is a one-to-one relationship between `userName` and `securityName`.
`authProtocol`	An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol which is used (MD5 and SHA).
`authKey`	If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. Note that a user's authentication key will normally be different at different authoritative SNMP engines. The `authKey` is not accessible via SNMP. The length requirements of the authKey are defined by the `authProtocol` in use.
`authKeyChange` and `authOwnKeyChange`	The only way to remotely update the authentication key. Does that in a secure manner, so that the update can be completed without the need to employ privacy protection.
`privProtocol`	An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. DES and AES are the encryption protocols that provide privacy in SNMPv3 currently.
`privKey`	If messages sent on behalf of this user can be en/decrypted, the (private) privacy key for use with the privacy protocol. Note that a user's privacy key will normally be different at different authoritative SNMP engines. The `privKey` is not accessible via SNMP. The length requirements of the `privKey` are defined by the `privProtocol` in use.
`privKeyChange` and `privOwnKeyChange`	The only way to remotely update the encryption key. Does that in a secure manner, so that the update can be completed without the need to employ privacy protection.

5.4 View-based Access Control Model (VACM)

VACM is used to control access to managed objects in a MIB or MIBs. This is where the Access Control Subsystem comes into play. The `msgFlags`, `msgSecurityModel`, and `scopedPDU` fields are used by VACM for message access. Each parameter is used to determine access to managed objects. An error is returned to the sender if access is not allowed for the request type. VACM makes use of four tables for different aspects of access control. Let's learn about those tables.

Context Table

The vacmContextTable is a collection of managed objects that have access constraints which are associated with a context name. The vacmContextTable stores all available contexts. The table is indexed by a contextName, and each row in this table contains vacmContextName.

Security to Group Table

The vacmSecurityToGroupTable is used to store group information. A group is made up of zero or more securityModel and securityName combinations. This combination defines what managed objects can be accessed. The table itself is indexed by a securityModel and securityName. The table contains rows made up of the following columns.

1. **vacmSecurityModel** : The security model in use, e.g., USM
2. **vacmSecurityName** : In the case of the USM, securityName and userName are identical
3. **vacmGroupName** : A textual name for the group to which this table entry belongs

Access Table

The vacmAccessTable is used to store the access rights defined for groups. This table is indexed by a groupName, contextPrefix, securityModel, and securityLevel. Each row in this table contains the following.

1. **vacmGroupName** : A name of a group with access rights.
2. **vacmAccessContextMatch** : A simple form of wildcard matching. A value of exact dictates that the index contextName must exactly match the value in vacmAccessContextPrefix. If set to prefix, the index contextName can simply match the first few characters of the value in vacmAccessContextPrefix.
3. **vacmAccessContextPrefix** : An index contextName must match either exactly or partially the value of vacmAccessContextPrefix.
4. **vacmAccessSecurityModel** : The securityModel that must be used to gain access.
5. **vacmAccessSecurityLevel** : Defines the minimum securityLevel that must be used to gain access.
6. **vacmAccessReadViewName** : The authorised MIB viewName used for read access.
7. **vacmAccessWriteViewName** : The authorised MIB viewName used for write access.
8. **vacmAccessNotifyViewName** : The authorised MIB viewName used for notify access.

View Tree Family Table

The vacmViewTreeFamilyTable is used to store MIB views. A MIB view is defined as a family of view subtrees that pair an OID subtree value with a mask value. The mask indicates which sub identifiers of the associated subtree OID are significant to the MIB view's definition.

All the MIB views are stored in the vacmViewTreeFamilyTable. It is indexed by a `viewName` and an OID of a MIB `subtree`. The VACM MIB defines the `vacmViewSpinLock` advisory lock that is used to allow several SNMP engines to coordinate modifications to this table. Each row in the `vacmViewTreeFamilyTable` contains the following :

1. **`VacmViewTreeFamilyViewName`** : A textual name for the MIB view.
2. **`vacmViewTreeFamilySubtree`** : The OID `subtree` that, when combined with the mask, defines one or more MIB view subtrees.
3. **`vacmViewTreeFamilyMask`** : A bit mask that, in combination with the corresponding OID subtree, defines one or more MIB view subtrees.
4. **`vacmViewTreeFamilyType`** : Indicates whether the corresponding MIB view `subtrees` defined by the OID `subtree` and mask are included or excluded from the MIB view.

5.4.1 How VACM Works?

Based on the VACM tables, the logic access flow mechanism for VACM is as shown in Fig. 5.4.1.

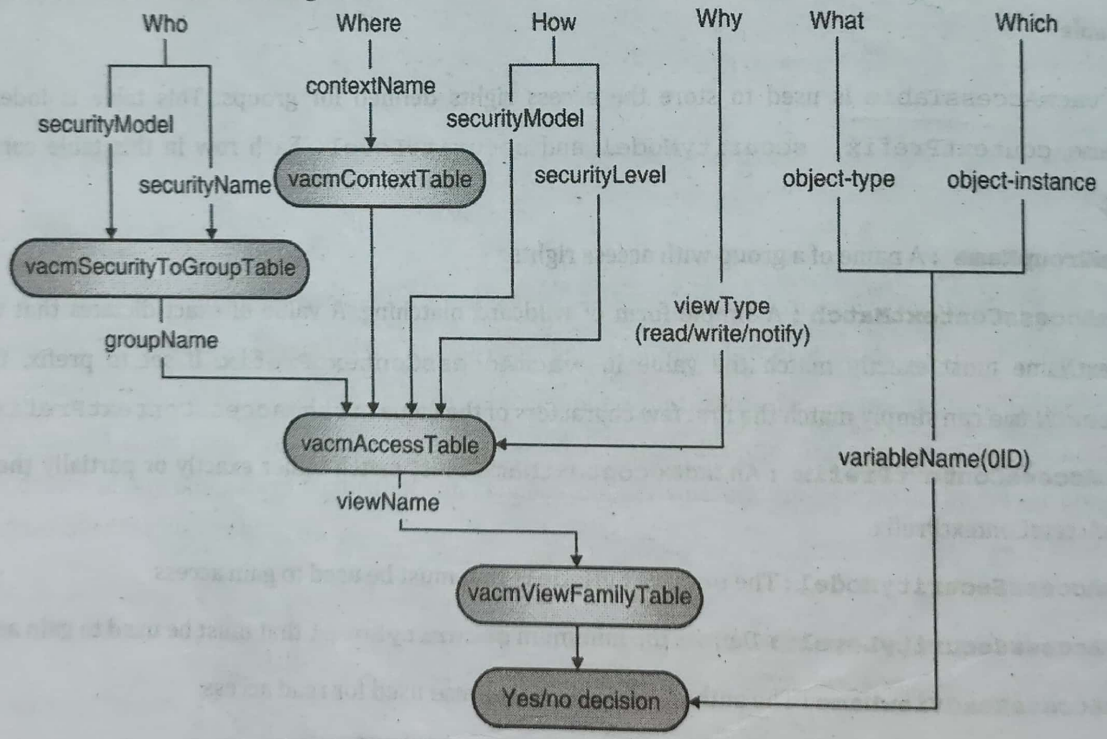

Fig. 5.4.1

SNMPv3 in Real World

Now, that you have the background in SNMPv3, let's outline the common configuration options you should expect when you have to configure an SNMPv3 device or network management platform.

- Username : This is the textual description of the person responsible for the SNMP entity that is to be managed. It is also referred to as security name. This is very much like the username that you use for login into your email account.
- Security level : Some applications require you to explicitly set the security level and others determine it based on the combination of authentication and privacy protocol in use.
- The security level could be set to the following.
  - `noAuthNoPriv`: which is no authentication and no privacy
  - `authNoPriv`: which is authentication but no privacy
  - `authPriv`: which is authentication and privacy
- Note that you cannot have privacy without authentication, but you can have authentication without privacy. Also, note here that the means to achieve privacy is through encryption using DES or AES algorithms.
- Authentication protocol : The protocol used for authentication that is, to prove that you are who you say you are. Currently, MD5 and SHA1 are used.
- Authentication passphrase : The passphrase used in conjunction with the authentication protocol. It must be at least eight characters long. You may also see it referred to as a password.
- Privacy protocol : The protocol used for privacy, that is, to encrypt the data portion of the SNMP packet. Currently, DES and AES are used.
- Privacy passphrase : The passphrase used in conjunction with the privacy protocol. It must be at least eight characters long. You may also see it referred to as a password.
- At a high-level, you take the following three steps for `manging` your network devices using SNMPv3.
  1. Create a USM entry on a device with proper USM attributes: username, authentication protocol, etc.
  2. Configure the management station with the proper USM attributes for the managed device. Note that the username and passphrases created in step 1 will need to be entered manually in this step.
  3. Begin managing the device.

5.5 Network Access Control (NAC)

- As organisations shift their business models to keep up with the technologically evolving world, their networks continue to grow more complex with the influx of new devices.
- In turn, security teams struggle to maintain visibility across remote, in-office, and hybrid work environments, increasing the potential for cyber criminals to gain entry into organisation's networks without being detected.

- Typically, there are several devices (network resources) in an organisation's network (LAN).
- They range from desktops, laptops, switches, routers, servers, printers, IP-based CCTV cameras, Smart TVs, and what not. As a user, you may not have access to all the network resources.
- Network and security administrators ensure that there is enough protection in the network to restrict access to only authorised users and track any malicious attempts to access network resources in an unauthorised way.

✍ ***Definition :*** *Network access control is a centralised approach to secure network access to only authorised entities using security policies that are enforced across all devices and users.*

5.5.1 Principal Elements of NAC

At a high-level, there are three main elements of NAC.

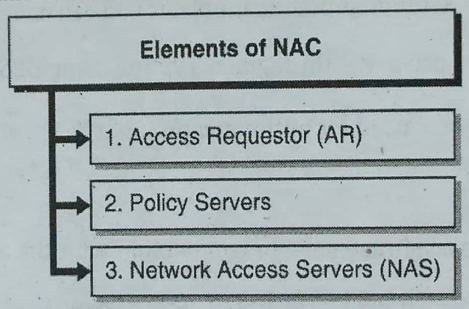

Fig. 5.5.1: Elements of NAC

1. **Access requestor (AR) :** The AR is the entity (device, user, process, etc.) that is attempting to access the network resource. It could be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices. ARs are also referred to as supplicants, or simply, clients.
2. **Policy Server :** Based on the AR's identity, authorisation level, attempted request, and an organisation's defined access policy, the policy server determines what access should be granted to AR.

   The policy server often relies on backend systems, including antivirus, patch management, or a user directory, to help determine the host's condition. An organisation defines various access policies to explicitly allow or deny such access.

   Note here that there are several commercial products in the market today that offer such policy servers for both on-premises computing as well as cloud computing. Cisco Identity Services Engine (ISE),The `Forescout Platform`, `Aruba ClearPass` Policy Manager, and `FortiNAC` are some of the most prevalent examples. These products provide very granular ways to define organisation policies and manage the entire IP infrastructure of the organisation.
3. **Network Access Server (NAS) :** The NAS functions as an access control point for users in remote locations connecting to an organisation's internal network. Typically, these act as VPN, and provide access to the organisation's internal network. These days, policy server solutions typically provide NAS function as well.

An enterprise network is a large-scale IT infrastructure that connects users, devices, and applications within an organisation,

The Fig. 5.5.2, illustrates the placement of these NAC elements. The goal is to provide reliable and secure digital services to employees, partners, customers and sometimes other things - They are made up of LANs & WANs

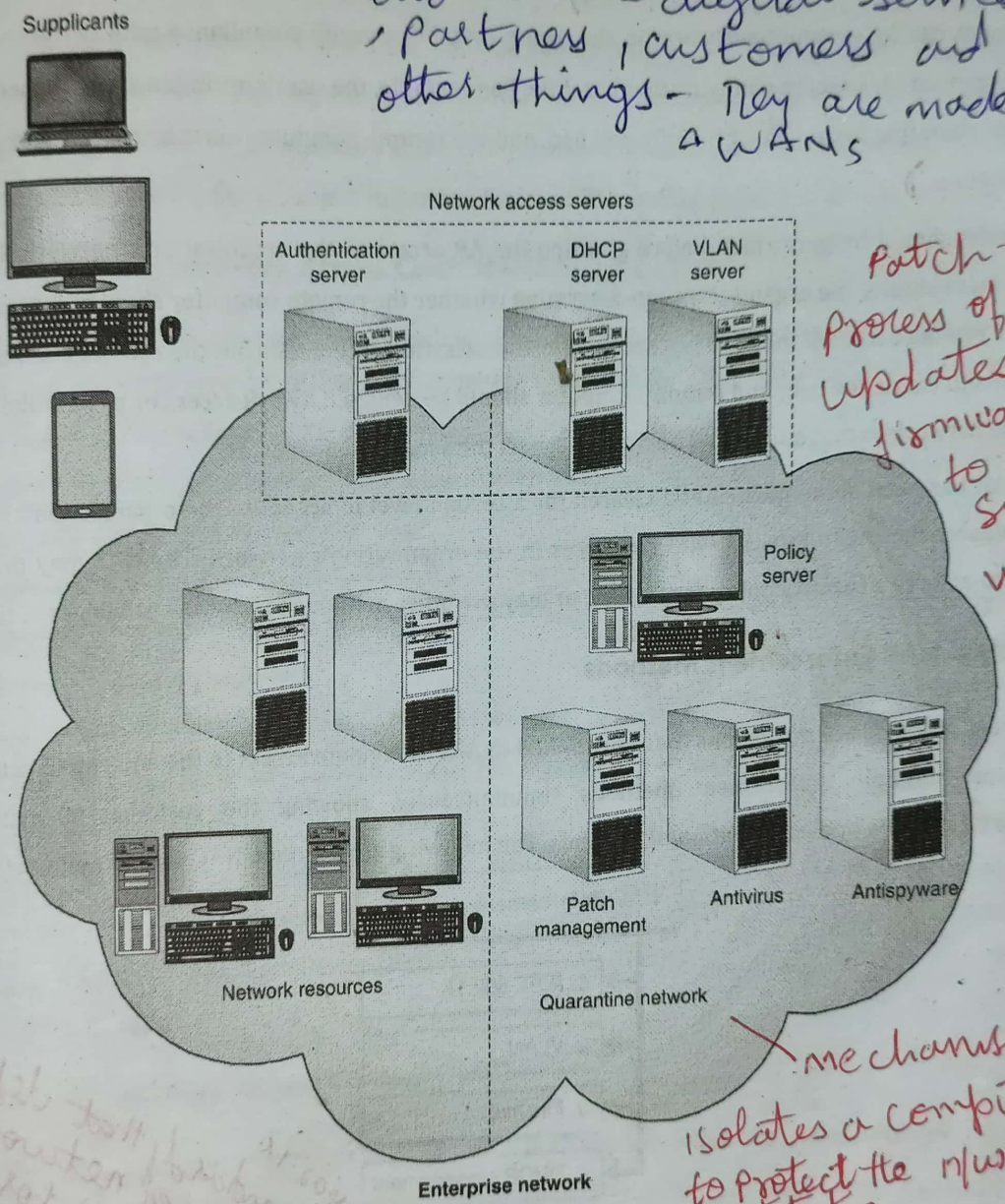

Fig. 5.5.2

Patch management is process of applying updates to software & firmware & devices to protect systems from vulnerabilities & ensure optimal performance

Mechanism that isolates a computer from a n/w to protect the n/w's integrity & the institution

- The first step is generally to authenticate the AR. Authentication typically involves some sort of secure protocol and the use of cryptographic keys. Authentication may be performed by the NAS, or the NAS may mediate the authentication process. In the latter case, authentication takes place between the supplicant and an authentication server that is part of the policy server or that is accessed by the policy server.
- The authentication process serves a number of purposes. It verifies a supplicant's claimed identity, which enables the policy server to determine what access privileges, if any, the AR may have. The authentication exchange may result in the establishment of session keys to enable future secure communication between the supplicant and resources on the organisation's network.

5.5.5 How to Implement NAC Solutions?

Implementing NAC solutions could vary from organisation to organisation depending upon the vendor's solution that is supposed to be implemented and the organisation policies. However, at a high-level, implementing NAC solutions generally involve the following steps.

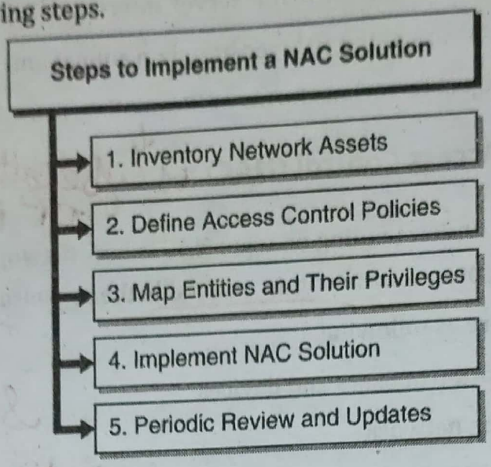

Fig. 5.5.4

1. **Inventory Network Assets :** Before you can successfully implement a NAC solution, you must perform an exhaustive survey of every endpoint inside your network and inventory them precisely. This includes every device, server, and piece of equipment that has to interface with digital resources. Without this information, your NAC system will struggle to protect the entire organisation. An attacker can find a network asset that is not in your protected resources list and could potentially get access to it. Once the attacker is already on the organisation's network, she can then make lateral movements and access other network resources. Quite a few NAC solutions provide a way to automatedly discover network endpoints and build inventory. This can speed-up the process and can ensure that you do not miss any network resources in your "to be protected" inventory list.
2. **Define Access Control Policies :** Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organisation or corporate policy to specific operational constraints (e.g., remote access). The set of rules, defined in the policies, governs all aspects of security-relevant system and system element behaviour. System elements include technology, machine, and human elements. Rules can be stated at very high levels (e.g., an organisational policy defines acceptable behaviour of employees in performing their mission/business functions) or at very low levels (e.g., an operating system policy that defines acceptable behaviour of executing processes and use of resources by those processes). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent. You should work with senior management to establish access control policies that your organisation would enforce for authorising access to network resources. The policy should also call out how the organisation would carry out audit for such access control attempts.
3. **Map Entities and Their Privileges :** The next step is to take the organisation defined policies and map it to the privileges that would be granted to entities in the organisation. For example, remote access might be allowed for a full time employee but may not be allowed for a contractor. In that case, you would assign remote access privilege to the full time employees but no remote access to contractors.

4. **Implement NAC Solution :** Based on the vendor that you have decided to go with, you should design and implement the NAC solution to enforce the organisation policies according to roles and privileges for various entities. The implemented NAC solution should control access to the entire network and should mediate all access attempts to unify access approval. It is important to ensure that the NAC solution itself is continuously patched and is kept updated as per the vendor's guidelines for it to continue working effectively.

5. **Periodic Review and Updates :** You should periodically review the performance of the implemented NAC solution and the effectiveness of the access policies. Following are some of the questions that you might want to ask when auditing.

- How many access attempts were blocked?
- Were they correct or incorrect?
- What exceptions were raised?
- Which organisation policy was most used?
- Which organisation policy was least used?
- What was the uptime of the NAC solution?
- Did user raise any support tickets for help?

Based on your findings, you should update the access policies and fine tune the implemented NAC solution.

Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

[A] Introduction to Networking Components

Q. 1 Describe a few networking components. **[6 Marks]**

[B] Network Management Security - SNMPv3

Q. 2 Write a short note on SNMP. **[4 Marks]**

Q. 3 How SNMP works? **[6 Marks]**

Q. 4 Explain SNMP Management Information Base (MIBs). **[6 Marks]**

Q. 5 What are the various SNMP versions? List their major attributes. **[4 Marks]**

Q. 6 Compare various SNMP versions. **[4 Marks]**

Q. 7 Describe the general security enhancements in SNMPv3. **[6 Marks]**

Q. 8 Explain the components of SNMPv3 Engine. **[6 Marks]**

Q. 9 Explain SNMPv3 Applications. **[6 Marks]**

Q. 10 Explain SNMPv3 architecture. **[6 Marks]**

Q. 11 How can you use `snmpSecurityLevel` to define the security requirements for SNMPv3? **[4 Marks]**

Q. 12 Explain `msgSecurityParameters` with respect to SNMPv3 packet. [6 Marks]

Q. 13 What are SNMPv3 user attributes? [6 Marks]

Q. 14 Write a short note on SNMPv3 View-based Access Control Model (VACM). [4 Marks]

Q. 15 You are a network security administrator. What would you do to use SNMPv3 to manage your network securely? [6 Marks]

[C] Network Access Control (NAC)

Q. 16 Write a short note on Network Access Control (NAC). [4 Marks]

Q. 17 Explain the various elements of Network Access Control (NAC) system. [6 Marks]

Q. 18 How do the various elements of Network Access Control (NAC) system work together? [6 Marks]

Q. 19 Explain a few Network Access Control (NAC)enforcement methods. [4 Marks]

Q. 20 List the various use-cases of Network Access Control (NAC). [4 Marks]

Q. 21 Describe the types of Network Access Control (NAC). [4 Marks]

Q. 22 How can you go about implementing a NAC solution? [6 Marks]

□□□

Chapter 5 ESE Questions

Q1 Explain principle elements of NAC. 5M

Q2 Explain the need of Network Access Control in Enterprise Network. Explain the major NAC enforcement methods 10M

Q3 Short note on use cases for NAC 5M

Q4 Explain different NAC enforcement methods 5M

Q5 What is Network access control? Discuss the elements in this context 10M

Q6 What is Network Management Security? Explain SNMP V3. 10M

Q7 Explain the implementation of NAC with one use case 10M

Q8 Explain how N/w mngt security is implemented 10M