

**Computer Networks and Internet Protocol**  
**Prof. Sawmya Kanti Ghosh**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture - 10**  
**Application Layer - V ( SMTP, SNMP )**

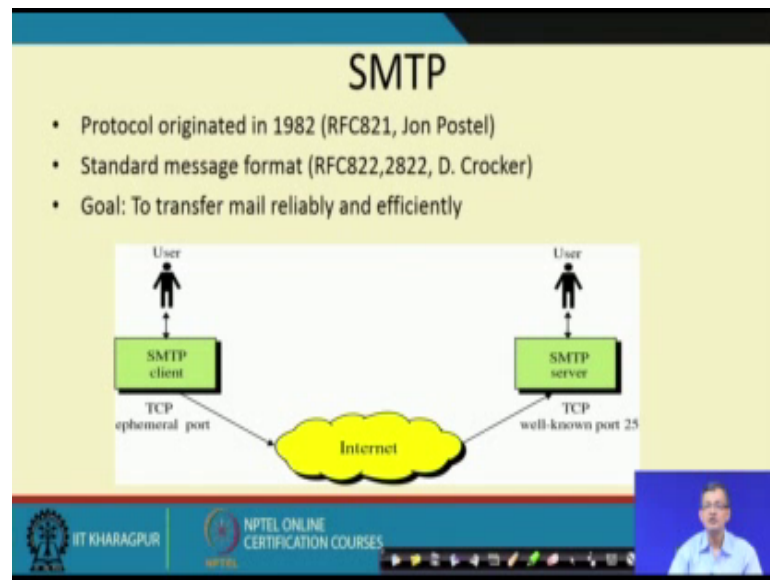
Hello. So, today we will discuss about two more protocol at the application layer, right SMTP and SNMP. So, we will take an overview of the this protocol. We have already discussed FTP, HTTP, Telnet and so and so forth on our client server base. So, this case is also. So, as any application layer protocol, they rely on underlining other layers like transport IP etcetera, right.

So, SMTP is for transferring mail from one to another. So, mail as we all know or realize is became a part and parcel of our life, right. Without mail it is not possible, it is something difficult to communicate also right. So, it is now became slowly becoming your official channel of communication and several places now official channel of communication. Another protocol is SNMP which is mainly for management purpose.

Now, you see if you look at the overall networking, even in a small or in organizational scale like say institute like IIT Kharagpur. There are several departments large department which has sub networks the institute has different sub networks and several routers etcetera. Even if we do not go outside the network itself, the internal dynamics of the network is extremely complicated, right. And to manage this we require something to some information to do that, right.

So, we can only it is not only when the failure is there signal is not there, but how to manage this all this underlining network. So, this is one of the protocol which is SNMP which gives that it helps us in collecting and acting on the information's from different network resources. So, we will have a brief overview of these 2 protocol and before we go to the other layer side.

(Refer Slide Time: 02:33)

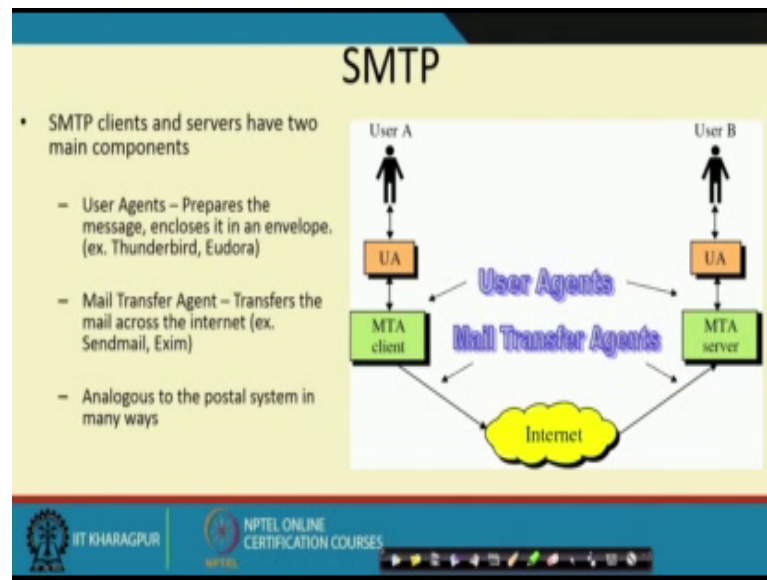


So, simple mail transfer protocol at it stands for is something like that, we have a main client at one end 2 mail client at one end. Popular SMTP server is works on it is TCP, on the basis of TCP and works on port 25, right. So, it is the port 25 where the SMTP server is active, right. Traditionally, traditionally means what we say, default port is port 25.

So, it was protocol was originated long back with RFC 821 in 1982, then we have 822 for message formatting goal to transfer mail reliably from one, thing one say one mail can a mail client to another mail client at the other end, right. Now whenever there is a client server protocol the server needs to listen at one port which is port 25 in this case. So, whatever mail you are coming received by your mail server like say we have a mail server is CAC mail server or cac dot iitkgp ac dot in or iitkgp ac dot in is the our generic mail server here institute mail server.

So, it receives at port 25, by default if not there are other changes in there. There can be other type of things also like what we say there can be mail gateway security type of things. Then we have some other configuration, but nevertheless the standard default mail gateway is a mail server port is the port 25. So, what is there the client over the network can the interact with the server at port 25, right.

(Refer Slide Time: 04:36)



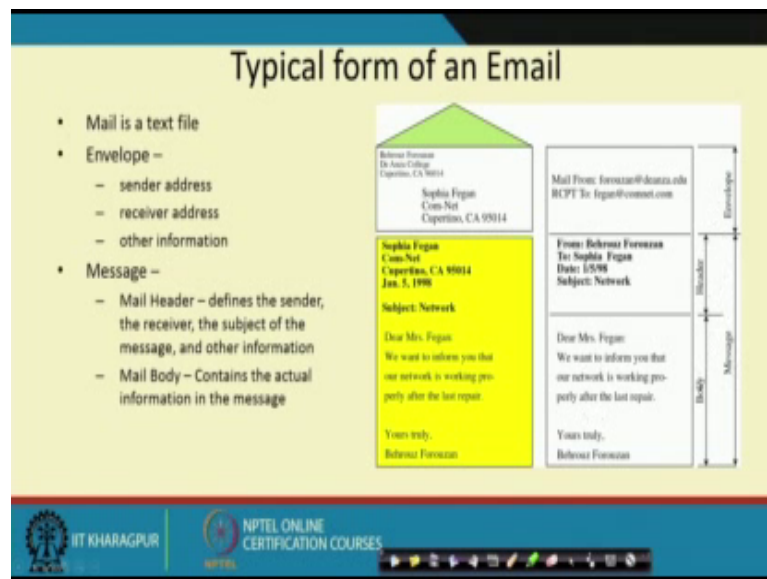
So, SMTP clients and servers have 2 major components. One is that user agent prepare the message encloses in envelope like some agents the popular agents initially your Thunderbird Eudora and you can have lot of other agents. There is a mail transfer agent transfer the mail across the internet right, and this is analogous to our postal system in many way. And there is a as MTA is the client. So, corresponding MTA server is there, and there is a user agent at the other end which reads the message, right. If it is a 2-way thing, then it can send and it access the server and so and so forth. The server things so, a SMTP demons would be running at the 2 end.

So, ideally what I can have? We can have 2 different mail servers things which can communicate these mails. And we have the other users which poke into this mail server and get the mails out of it, right So, I have individual mailboxes like here, we are having individual mailboxes in our say iitkgp mail server or cac server. And then we are connecting to the server either through some sort of a directly web link, or I am pulling that mail to some other client at the things. So, we will talk about it, right. So, these are the user agents a mail transfer agents. So, there is little bit problem in the arrow, it should have been here, and this should have pointed here, right.

So, SMTP also allows use of relays allowing other MTAs to relay the mail right. So, other than MTA acting as a server client, server and client it also allows MTA relay. So, getting a mail, it is relayed to the internet to the other mail and so on and so forth, right.

So, mail gateway are used to mail relay prepared by their protocol other than SMTP and convert it to the SMTP, right. So, this basically it relays from one server to another. So, the mail goes on different goes to this different relays and reach the things. So, there it acts as a mail we have that mail gateway, which allows that mail to go to the other end of the thing.

(Refer Slide Time: 06:58)



Now if you look at the typical format of email. So, mail is a mail is a text file envelope that is sender address receiver address and other information of the things. Message there is a email header defines the sender receiver and subject of the message and other information and mail body contains the actual information of the message, right.

So, this is the typical thing so, mail from something mailed to the address. And there are other details and then we have that actual context. So, we have the envelop this is the overall message which has a header part and a body part.

(Refer Slide Time: 07:38)

SMTP Keywords	
Keyword	Arguments
HELO	Sender's Host Domain Name
MAIL FROM:	Email Address of sender
RCPT TO:	Email of Intended recipient
DATA	Body of the message
QUIT	

And if you look at different SMTP keywords or if SMTP what we say that functional modules; one is HELO: sender's host domain name, right, MAIL FROM: email address of the sender, Received To: email of intended recipient, DATA: body of the message and QUIT or quitting this thing.

So, these are the standard keywords which are there in the mail under the SMTP. If you remember we were talking about that during our HTTP discussion or HTTP lecture, that we can use Telnet like Telnet www dot iitkgp dot ac dot in blank, 80 provided that is not knows any security barrier.

So, it will talk to that port 80 and then go on. You can set get post and type of comment. Here also if I know the mail server and if I that is allowed that I can connect like that. So, Telnet I can have say cac dot iit kgp ac dot in right. So, it will return me that after authentication I can use this all, right as a MAIL FROM, Received To, putting the data and type of things.

So, I can instead of having any separate front end module or agent I can communicate like this right. So, that is the possibility, that that is the beauty of this having interoperable services across the thing.

(Refer Slide Time: 09:17)

SMTP Keywords	
Keyword	Arguments
RSET	
VERFY	Name to be verified
NOOP	
TURN	
EXPN	Mailing list to expand
HELP	Command Name

There are a few more key words like reset or verify name to be verified NOOP, TURN, EXPN mailing list to be expanded help. So, these are extra key words not that what we say not. So, popular keywords, but these are the things which are also allowed in the SMTP.

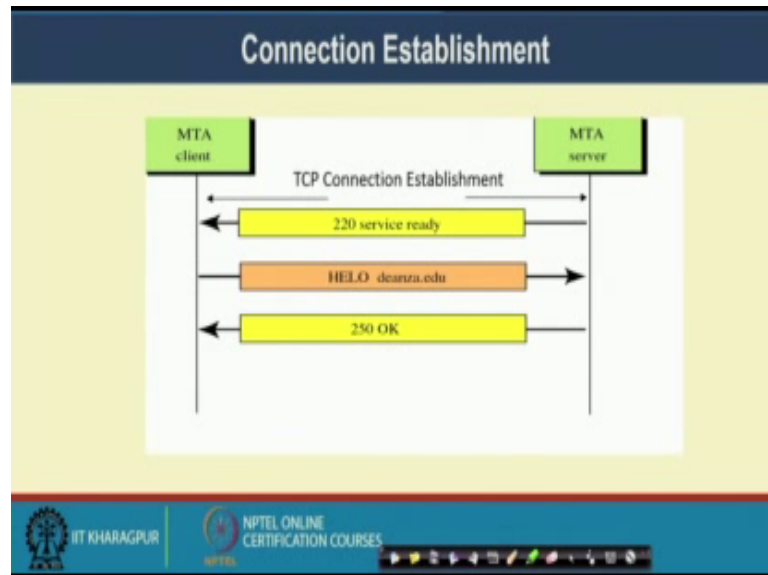
(Refer Slide Time: 09:38)

Status Codes
<ul style="list-style-type: none"><li>• The Server responds with a 3 digit code that may be followed by text info<ul style="list-style-type: none"><li>– 2## - Success</li><li>– 3## - Command can be accepted with more information</li><li>– 4## - Command was rejected, but error condition is temporary</li><li>– 5## - Command rejected, Bad User!</li></ul></li></ul>

There are some status code 2 hash hash is the success, then we have 3 hash hash - command can be accepted in more with more information. 4 hash hash is the command was rejected, but error condition is temporary right and 5-hash hash is the command

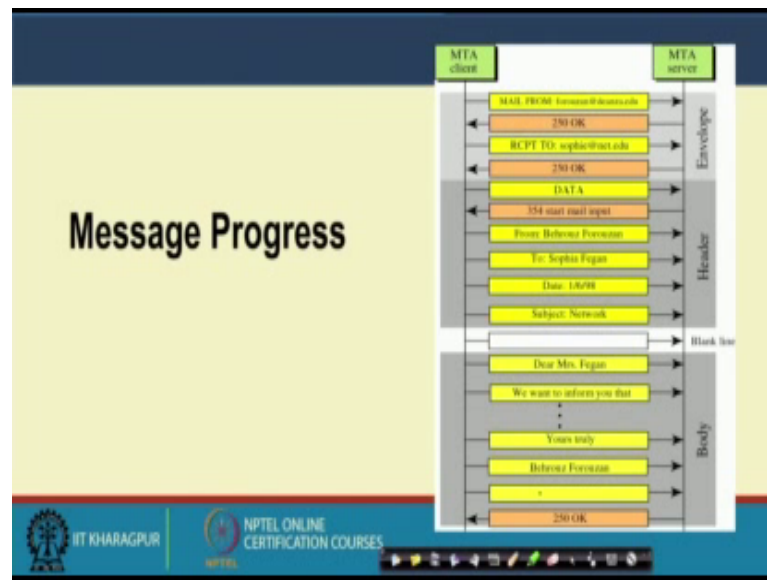
rejected bad user. So, there are different 3 digits code to handle that this SMTP communication.

(Refer Slide Time: 10:07)



Like here say, MTA this is TCP connection has been established, then the that 220 service ready that; that is, the 2 as we have seen 2 hash hash is the success thing, then HELO some message goes and then it says like this. So, initially the connection is established between the two the client and the server client request for the connection the connection establish the server respond with 220 a service ready. Then it sends a HELO message and then it responses that it is received and go so and so forth.

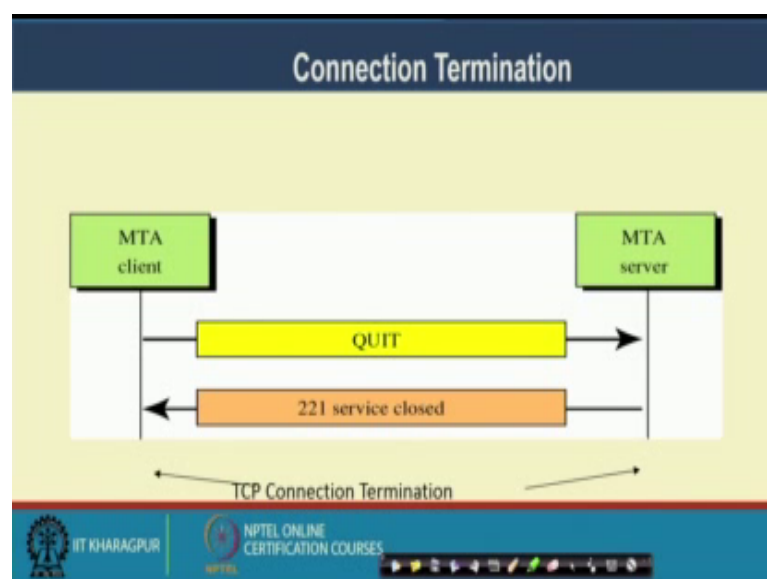
(Refer Slide Time: 10:46)



So, if you go on expanding things. So, it goes from mail form it responded with a OK message. It is received 2 for this OK message, then the data then start mail input and go on doing these other information. So, this is the envelope, this is the header with a blank line; you go on the body of the message right.

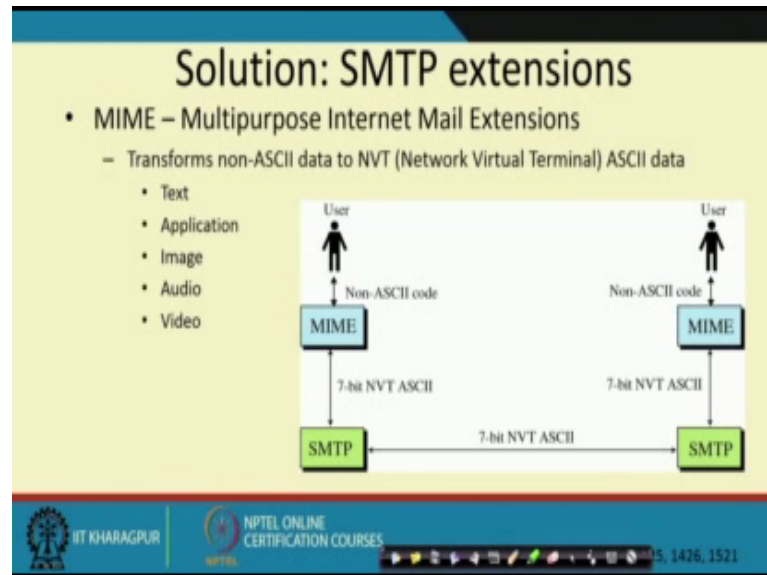
So, and then it continues once the body once it is terminated. It will come to that it says that 250 drive, that the mail has been pushed to the towards the mail gateway or the MTA.

(Refer Slide Time: 11:25)



So, connection termination is sending a QUIT a formal QUIT by the mail client, and then mail 220 one receive service close messages sent by the MTA.

(Refer Slide Time: 11:45)



So, one is now there are some problems of in our generic SMTP extends SMTP that it cannot handle all sort of data set. So, that is a SMTP extension what we say MIME multipurpose internet mail extension. So, transformed a Non-ASCII character to a NVT or Network Virtual Terminal ASCII character, right; so, otherwise it will not be able to communicate with the thing. So, we can now we have text, application, image, audio, video which can be pushed to this all MIME. So, what we do usually attach that things in some form of other with the mail.

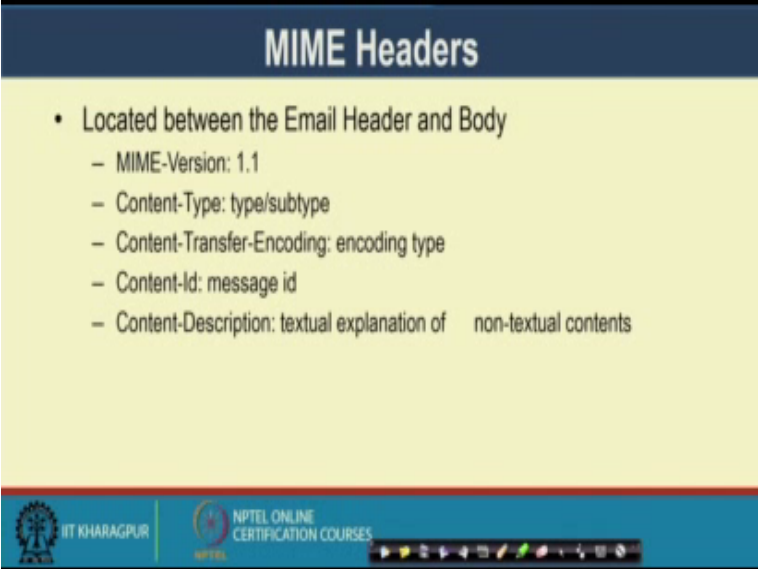
So, those are if there is a Non-ASCII character, there are there may be problem in transmission because those ASCII character etcetera may interact the thing, right. So, this MIME takes care of that. So, it converts it to a 7 bit NVT ASCII which the SMTP envelop takes as a payload, and the communication is between this SMPT server client at the 2 end. And the other end also I have the MIME which able to decode and for the user.

So, this multipurpose internet mail extension gives a way to communicate between the two with Non-ASCII type of character sets, right which comprises text, application, image, audio, video. There can be situation where some of the things are blocked like if you some of the mail server may not accept application or executable files. Some mail

servers may not accept video files, and that some there are may be restriction on the size of the thing.

So, those are what we say upper layer, yeah or application there are different restriction on the above SMTP write basic SMTP allows the communication between the 2 2 SMTP server client system.

(Refer Slide Time: 13:59)



The slide is titled "MIME Headers" in a dark blue header bar. The main content area is yellow and contains a bulleted list. The footer is blue and contains logos for IIT Kharagpur and NPTEL, along with a navigation bar.

- Located between the Email Header and Body
  - MIME-Version: 1.1
  - Content-Type: type/subtype
  - Content-Transfer-Encoding: encoding type
  - Content-Id: message id
  - Content-Description: textual explanation of non-textual contents

So, there are typical MIME headers located between the email header, and the body header like if you remember this was our email header, and the body header and it lies between these 2, and there is that comes with a MIME version; that is, type of a content type, contents transfer encoding type, content id and content description. So, these are the thing which the MIME header contains.

(Refer Slide Time: 14:28)

**MIME Headers (cont'd)**

- **Content-Type** – Type of data used in the Body
  - Text: plain, unformatted text; HTML
  - Multipart: Body contains different data types
  - Message: Body contains a whole, part, or pointer to a message
  - Image: Message contains a static image (JPEG, GIF)
  - Video: Message contains an animated image (MPEG)
  - Audio: Message contains a basic sound sample (8kHz)
  - Application: Message is of data type not previously defined
- **Content-Transfer-Encoding** – How to encode the message
  - 7 bit – no encoding needed
  - 8 bit – Non-ASCII, short lines
  - Binary – Non-ASCII, unlimited length lines
  - Base64 – 6 bit blocks encoded into 8-bit ASCII
  - Quoted printable – send non-ASCII characters as 3 ASCII characters, =##, ## is the hex representation of the byte

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

And there are several other constant like what are the different type of things will be there takes, when takes, multi part message, image, video, audio, application. There can be different content transfer encoding how to encode the images 7 bit, 8 bit binary, base 64 quoted printable and so and so forth. So, what we see that MIME also has a rich set of a headers to handle different kind of data.

(Refer Slide Time: 15:02)

**MTAs and Mail Access Protocols**

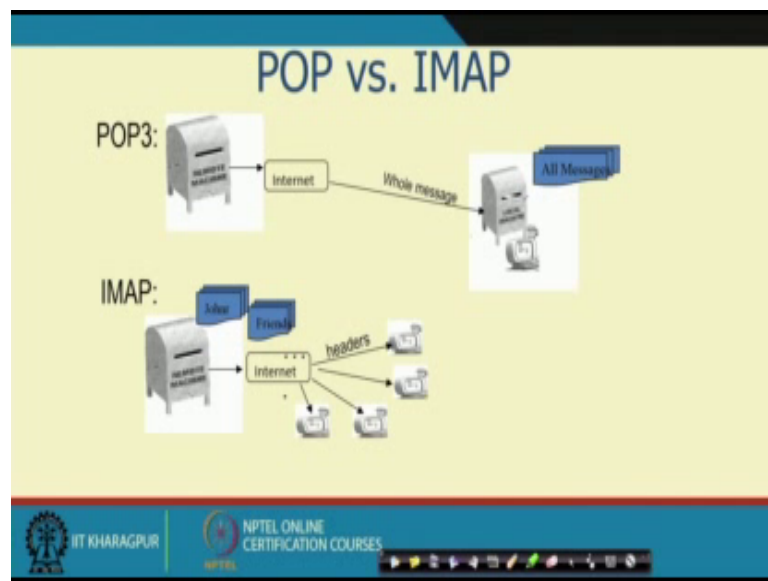
- The MTA delivers email to the user's mailbox
- Can be complex with numerous delivery methods, routers, and ACLs
- Exim, Postfix, Sendmail
- The Mail Access Protocols are used by the users to retrieve the email from the mailbox
  - POP3
  - IMAP4

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, MTA and mail access protocol, right. So, that is another thing, that if I have a mail server so, how I can access that mail? So, MTA delivers the email to the user's mailbox.

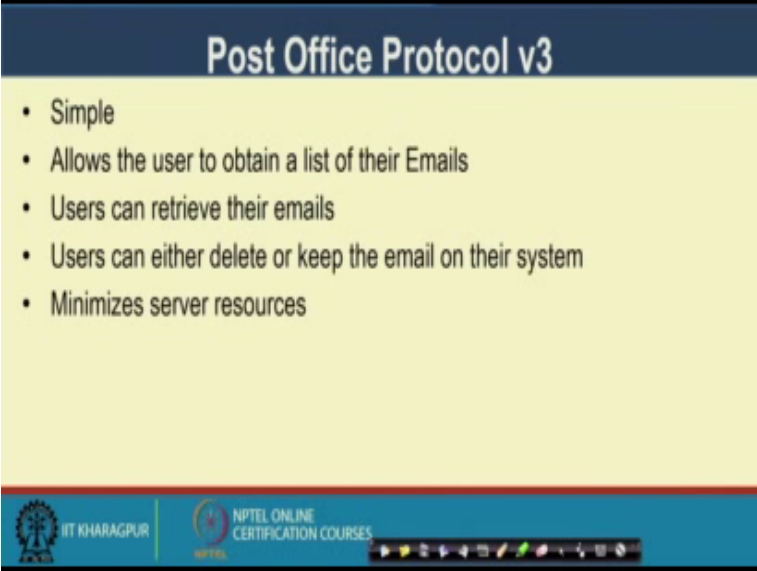
So, user's mailbox is lying in the mail server can be complex with numerous delivery models routers ACLs and type of things, right. So, there are Exim, Postfix, Sendmail and these are the different kind of what we say mail server or mail client which acts on the things. Now this mail access protocol can be used by the user to retrieve the email from the mailbox. So, two popular thing has POP3, and IMAP4. So, these are the 2 popular mail access protocols.

(Refer Slide Time: 15:48)



So, what it does? So, it is from the all messages are there in that mail server. So, that so this POP3, a POP3 actually pulls that message from the mail server or in some cases that is goes on in push pull form and to the to your that mail access what we are looking at that mail access protocols, right? Similarly, IMAP also acts in a similar fashion.

(Refer Slide Time: 16:24)



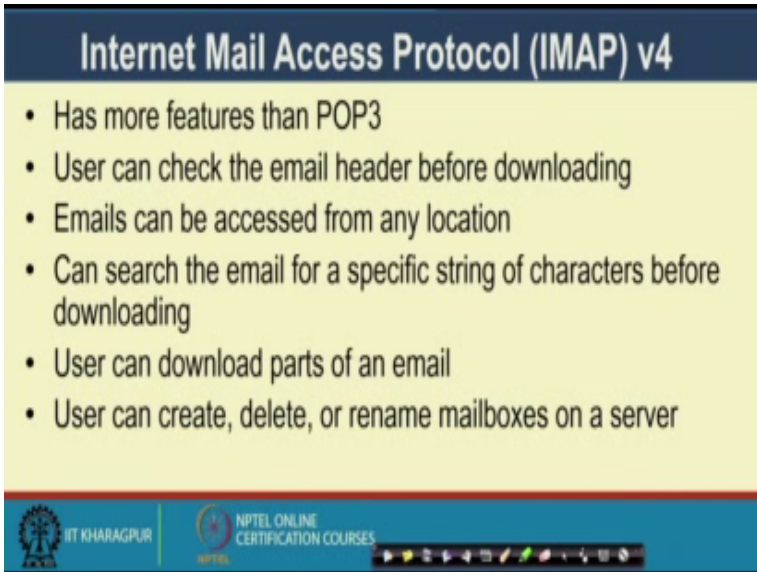
### Post Office Protocol v3

- Simple
- Allows the user to obtain a list of their Emails
- Users can retrieve their emails
- Users can either delete or keep the email on their system
- Minimizes server resources

The slide footer includes the IIT Kharagpur logo, the text 'IIT KHARAGPUR', the NPTEL logo, and the text 'NPTEL ONLINE CERTIFICATION COURSES'. A navigation bar with various icons is located at the bottom right.

But so, post office protocol or POP3 it is simple. Allow the user to obtain a list of their emails. Users can retrieve their mails. Users can either delete or keep mails in their systems and minimize the server resources. In other sense, this POP3 or even IMAP allows the user to manage each mail, right and can it is gives a frontend to the user to handle it is mail services, right.

(Refer Slide Time: 16:58)



### Internet Mail Access Protocol (IMAP) v4

- Has more features than POP3
- User can check the email header before downloading
- Emails can be accessed from any location
- Can search the email for a specific string of characters before downloading
- User can download parts of an email
- User can create, delete, or rename mailboxes on a server

The slide footer includes the IIT Kharagpur logo, the text 'IIT KHARAGPUR', the NPTEL logo, and the text 'NPTEL ONLINE CERTIFICATION COURSES'. A navigation bar with various icons is located at the bottom right.

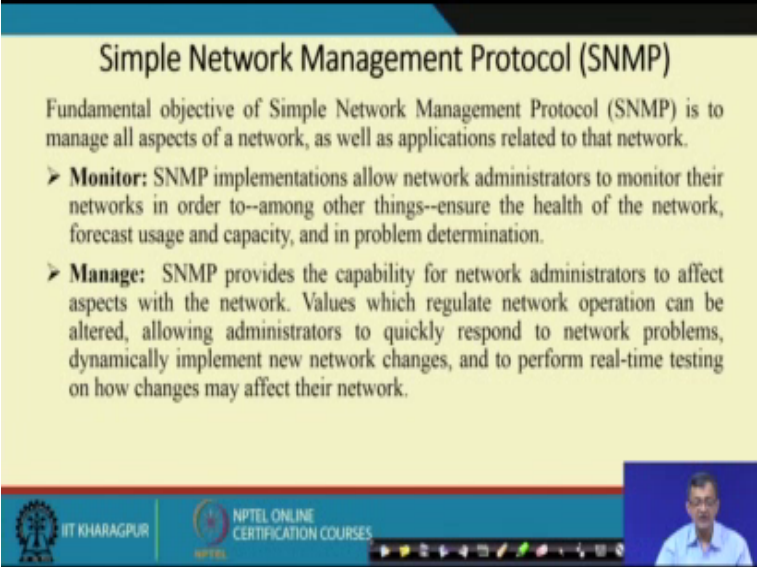
So, on the other hand, IMAP v4 is the basic philosophy is same. So, it has more features than POP3. User can check email header before downloading, right. So, in case of

IMAP4 the user can check the header before downloading, and then take a call with that to download or not. Email can be accessed from any location can search email for a specific string of characters before downloading, right.

So, it can be it can search the email for a specific string of characters before downloading that; that means, it keeps more manageability or control to the user to handle his mailbox in other sense. User can download part of an email; user can create delete rename mailboxes of a server. So, it is a in the mail server in it is own mailbox, it gives at lot of flexibility in handling that a mailbox. So, that is the part of this in case of a IMAP or IMAP version 4.

So, with this we have we see a broad overview of these mail how SMTP works. Now let us have another protocol that SNMP or Simple Network Management Protocol.

(Refer Slide Time: 18:22)



**Simple Network Management Protocol (SNMP)**

Fundamental objective of Simple Network Management Protocol (SNMP) is to manage all aspects of a network, as well as applications related to that network.

- **Monitor:** SNMP implementations allow network administrators to monitor their networks in order to--among other things--ensure the health of the network, forecast usage and capacity, and in problem determination.
- **Manage:** SNMP provides the capability for network administrators to affect aspects with the network. Values which regulate network operation can be altered, allowing administrators to quickly respond to network problems, dynamically implement new network changes, and to perform real-time testing on how changes may affect their network.

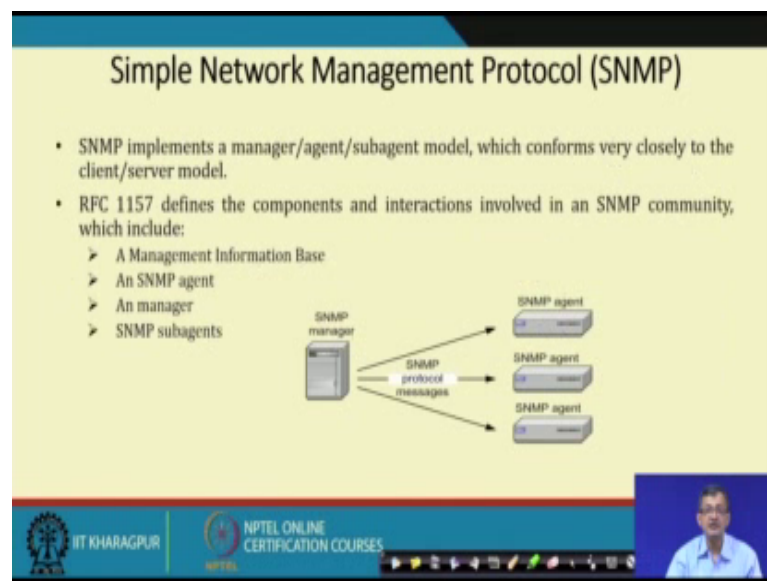
IT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So SNMP, so fundamental objective or basic objective of SNMP is to manage all aspects of network as well as application related to the network. So; that means, it is a more of a protocol which allows manageability of the network. Rather than other protocols what we have seen, it is the major purpose is transferring data etcetera from one part to another, right. Anyway in case of SNMP it is primarily to manage the network. And specially the network as it expands the overall management becomes a major issue, not only from the failure, but to give a better bandwidth service and so on so forth.

So, two major functionalities of SNMP one is monitor, SNMP implements implementation allow network administrators to monitor their networks in order to ensure the health of the network, right. So, there are other things, but it to ensure the health of the network, forecast uses and capacity and in problem determinations. So, this is one of the thing so, that is a monitoring of the network.

The other part is SNMP provides the capability of the network administrator to affect aspects with the network. Values which regulate network operation can be altered allowing administrator to quickly respond to network problems dynamically etcetera. So, one is monitoring; so, what is during that it is getting regular information about the thing. Another is based on that information the network manager or the administrator can take a call on the things; that means, it can manage the things like implement new network changes, improve real time testing and how it is getting affected and type of things it can do on the network.

(Refer Slide Time: 20:20)

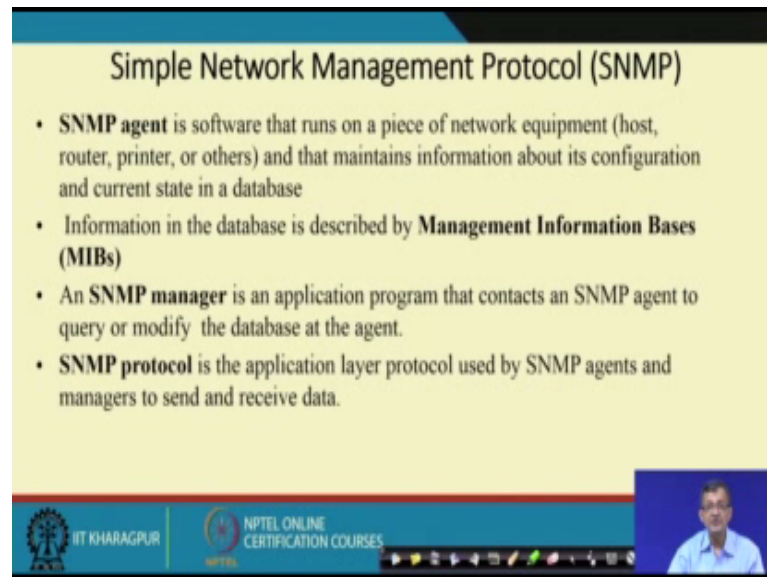


So, as it requires there should be some agents or what we say SNMP agents who will be reporting the status of the network or information about the network. So, SNMP implements a manager client sub agent model which conforms very closely to the client server model, right.

So, it is sort of a agent based things. So, RFC 1157 defines the component and interaction involved in a SNMP community which include management information base

or a MIB SNMP agent a SNMP manager, and there are SNMP subagent. So, this constitutes or defined based these are the things which are required for this operation of the SNMP.

(Refer Slide Time: 21:12)



### Simple Network Management Protocol (SNMP)

- **SNMP agent** is software that runs on a piece of network equipment (host, router, printer, or others) and that maintains information about its configuration and current state in a database
- Information in the database is described by **Management Information Bases (MIBs)**
- An **SNMP manager** is an application program that contacts an SNMP agent to query or modify the database at the agent.
- **SNMP protocol** is the application layer protocol used by SNMP agents and managers to send and receive data.

And SNMP agent is a software that runs on a piece of network equipment. It can be host router printer and others, and maintains the information about the configuration or current state of the database.

So, in other sense wherever this network connectivity is there, if we need to be managed like specially intermediate things like router etcetera. This SNMP agents runs on a on that particular equipment. So, it is a software which runs on either in the host, network printer, in a router and or any network type of devices. And that maintains information about the configuration and current state of the database, right.

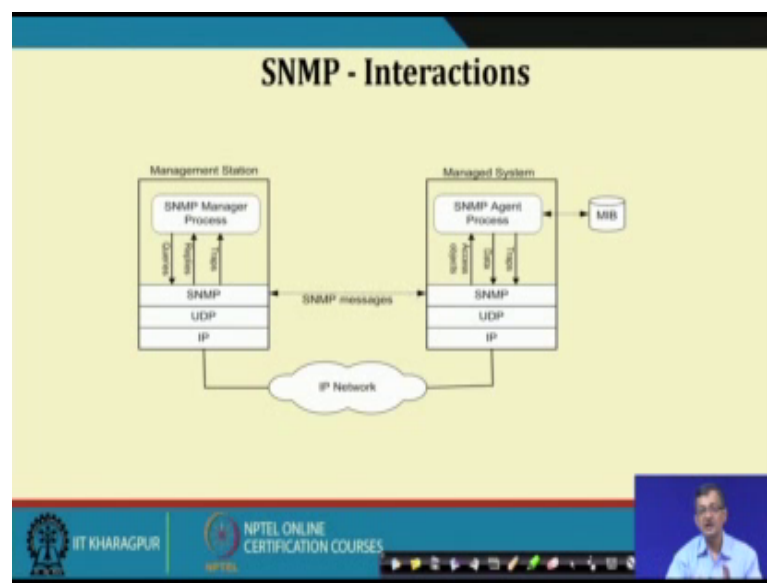
So, information in the database is described in management information base or MIBs right. So, it has a particular structure by which these management information bases are maintained. So, SNMP manager is an application program that connects to the SNMP and to query or modify the database in the agent.

So, the manager connects to the SNMP agent to either query the agent formed data or update the database or modify the database. SNMP protocol is the application layer protocol used by SNMP agents and manager to send the send and receive data, right. So,

it is a application layer protocol used by the SNMP agents and manager to send and receive data is the SNMP protocol basic protocol.

So, what we have? We have agent which is collecting data, we have a management information base to have the database. We have a SNMP manager. There is the application program that contacts the SNMP agents to query and modify the database. And we have a SNMP protocol is the application layer protocol that is SNMP agents and manager sends and received data.

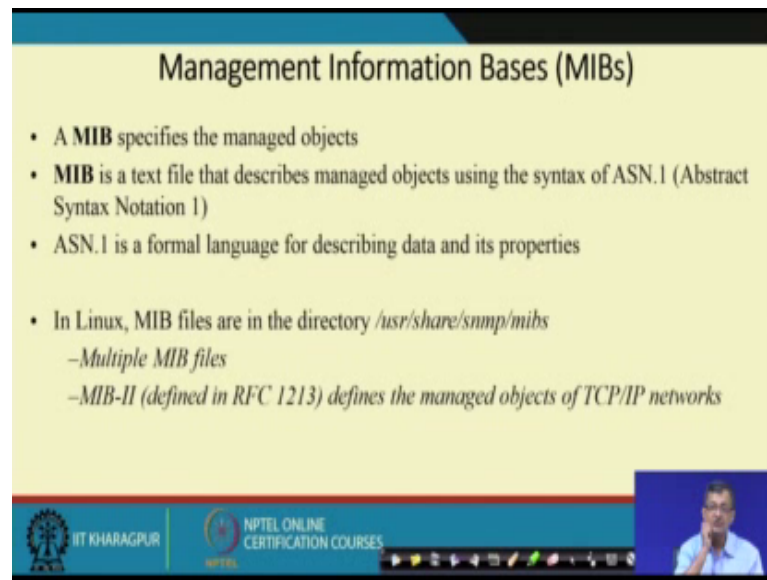
(Refer Slide Time: 23:01)



The management station; so, if we look at that particular configuration so, we have this management station, where SNMP manager process is running SNMP this protocol is running it runs. SNMP incidentally runs on primarily on UDP. We have on the line IP, then the IP network and the data things are there. So, if there is a query, it goes through and access these agents. So, from the manager, the query goes to the agent the data or traps comes to the things. This SNMP agent as we are discussing it has a MIB or management information base, right.

So, it contains the database address. So, the manager this agent is in some networked devices. So, these SNMP messages are communicated between these two, in between these two SNMP of the manager and SNMP of the agent.

(Refer Slide Time: 24:05)



**Management Information Bases (MIBs)**

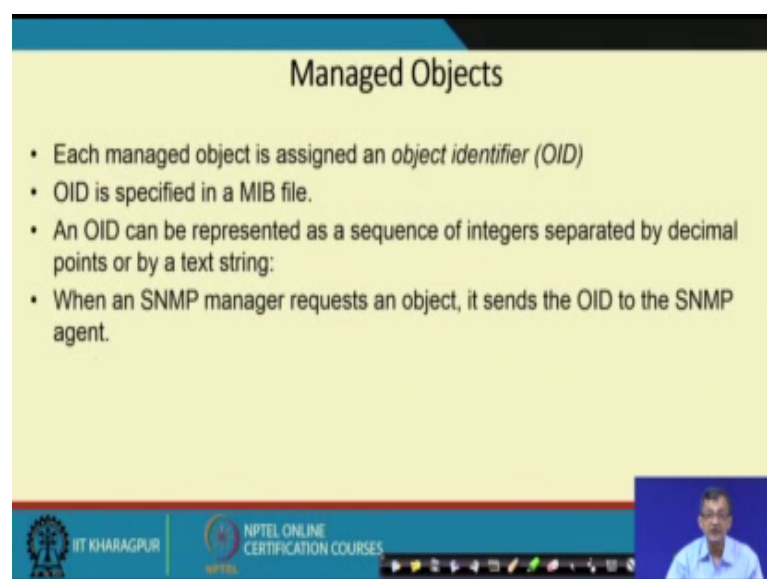
- A **MIB** specifies the managed objects
- **MIB** is a text file that describes managed objects using the syntax of ASN.1 (Abstract Syntax Notation 1)
- ASN.1 is a formal language for describing data and its properties
- In Linux, MIB files are in the directory `/usr/share/snmp/mibs`
  - Multiple MIB files
  - MIB-II (defined in RFC 1213) defines the managed objects of TCP/IP networks

The slide footer includes the IIT Kharagpur logo, the text 'IIT KHARAGPUR', the NPTEL logo, and the text 'NPTEL ONLINE CERTIFICATION COURSES'. A small video inset in the bottom right corner shows a man speaking.

So, what is this MIB? It specifically specifies the management object. MIB is a text file. That describes named objects using a syntax which is described in abstract syntax notation 1, right. So, ASN.1 is a formal language for describing the data and its properties.

So, it is a standard formula standard way of representation. In Linux, MIB files are in the directory that particular directory. And MIB 2 defined in RFC 1213 defines the managed objects of the TCP/IP network. So, these are the data base of the data which are contained in the things.

(Refer Slide Time: 24:45)



**Managed Objects**

- Each managed object is assigned an *object identifier (OID)*
- OID is specified in a MIB file.
- An OID can be represented as a sequence of integers separated by decimal points or by a text string:
- When an SNMP manager requests an object, it sends the OID to the SNMP agent.

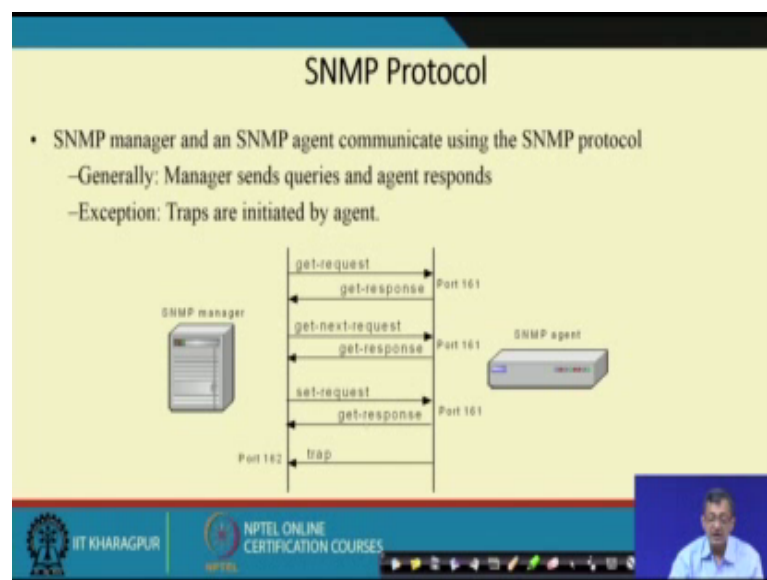
The slide footer includes the IIT Kharagpur logo, the text 'IIT KHARAGPUR', the NPTEL logo, and the text 'NPTEL ONLINE CERTIFICATION COURSES'. A small video inset in the bottom right corner shows a man speaking.

So, which object to be managed? Managed objects each managed object is assigned a object identifier, or OID, OID is a specified in a MIB file. So, what is the object identifier is specified in a object identifier. So, the OID can be represented as a sequence of integers separated by 2 decimal point or a and by a text string, right.

So, it is a sequence of in integer which is separated by decimal points and by a text string. So, recently here the example was not there. But if you check in any standard book or thing; so, you see that how it is represented. When SNMP manager requests for the object you send the OID or object identifier to the SNMP agent, right.

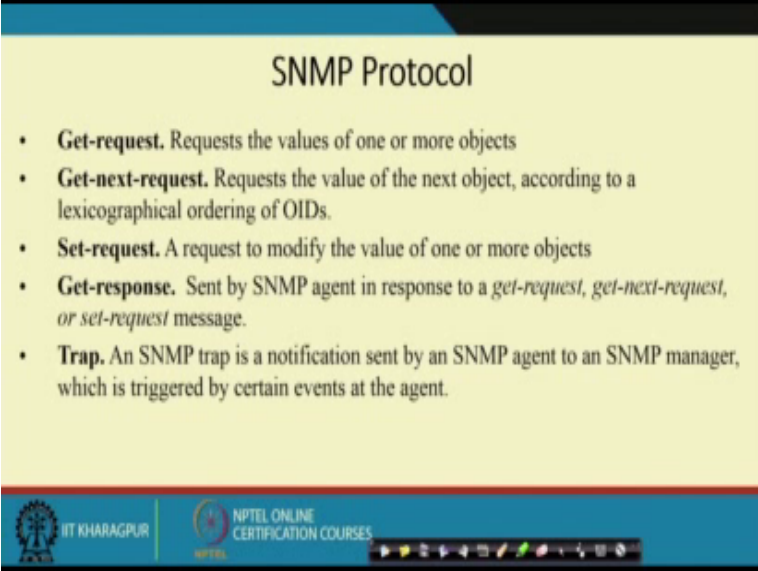
So, in that way, it can find out that only for a particular data or information if it is manager is seeking for some manageability issues it can it can hook into like this.

(Refer Slide Time: 25:51)



So, if we look at the SNMP protocol down the line. So, SNMP manager and SNMP agents communicate by a SNMP protocol. Generally, manager sends queries and agents and agent responses. So, manager sends query agent responses. Exception traps are initiated by agents. So, there if there are external situation the traps are initiated by the agents which are pushed to the manager. So, one side manager or other agent so it get requests get response. If this is at port 161 get next requests and next responds and it goes on like this. So, it said request and response, and if there is a trap without any request it can send the trap message to the SNMP manager.

(Refer Slide Time: 26:38)

A presentation slide titled "SNMP Protocol" with a yellow background and a blue header. It lists five types of SNMP messages: Get-request, Get-next-request, Set-request, Get-response, and Trap. Each item is preceded by a bullet point. The slide also features logos for IIT Kharagpur and NPTEL Online Certification Courses at the bottom.

### SNMP Protocol

- **Get-request.** Requests the values of one or more objects
- **Get-next-request.** Requests the value of the next object, according to a lexicographical ordering of OIDs.
- **Set-request.** A request to modify the value of one or more objects
- **Get-response.** Sent by SNMP agent in response to a *get-request*, *get-next-request*, or *set-request* message.
- **Trap.** An SNMP trap is a notification sent by an SNMP agent to an SNMP manager, which is triggered by certain events at the agent.

IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES

So, in case of a SNMP protocol, it has a get request the value for one or more object, gets next request the value from next object according to the lexicographical order of OID. So, a OID has a chronological lexicographical order. And it requests for that set requests a request to modify the value of one or more object that is a set request.

So, you want it wants to set the request, Get-respond- sent by SNMP agent in response to the Get-request, Get-next-request or Set-request message, right.

So, what we have? One is that requesting the thing. One is one other type of thing is the setting the request that is request to modify some one or more of the object, and it gets a response of the thing. Trap is a SNMP trap is a notification sent by the SNMP agent without any query from the SNMP manager to a SNMP manager which triggered by certain events at the agent. So, agent may have some certain events which it wants to inform immediately to the manager. So, this trap messages are for that.

(Refer Slide Time: 27:48)

### SNMP Versions

- Three versions are in use today:
  - SNMPv1 (1990)
  - SNMPv2c (1996)
    - Adds "GetBulk" function and some new types
    - Adds RMON (remote monitoring) capability
  - SNMPv3 (2002)
    - SNMPv3 started from SNMPv1 (and not SNMPv2c)
    - Addresses security
- All versions are active
- Many SNMP agents and managers support all three versions of the protocol.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, SNMP versions; so, the typically there are 3 versions which are in active using SNMP version; one that is in 1990 it came up, version 2 c which is 1996 and version 3 2002. So, these are the things, and in version 2, there is it attempts to version 3 attempts to address the security issues. So many SNMP agents and managers supports all 3 versions of the protocol. So, there are SNMP agents and manager which supports all these parts, all these 3 versions of the protocol.

(Refer Slide Time: 28:33)

### Format of SNMP Packets

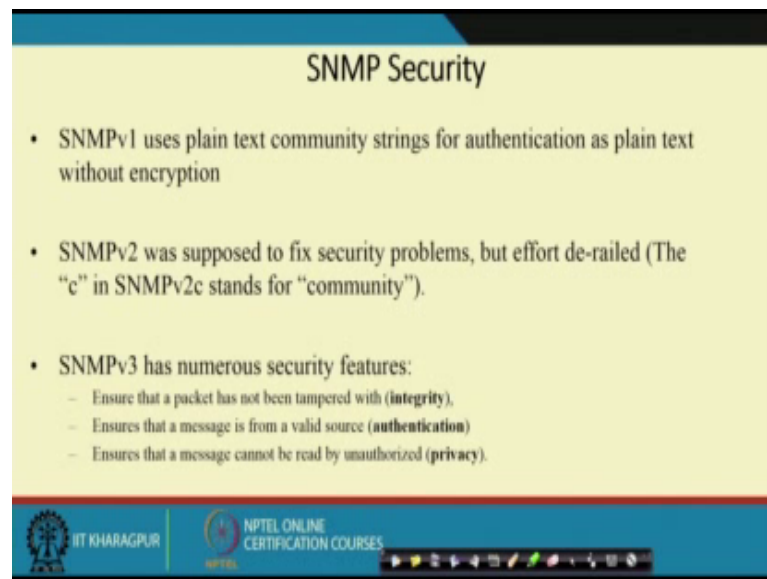
- SNMPv1 Get/Set messages:

Version	Community	SNMP PDU	
		PDU Type	Request ID
		Error Status	Error Index
		Object 1, Value 1	
		Object 2, Value 2	
		...	

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, this is a typical format of SNMP packet which SNMP 1 Get Set messages, clear text string that is used as a password. PDUs type for SNMP 132 bit and for SNMP it is 64 bit. Unique ID that matches the request with the replies, right otherwise who as is the request response. So, we need to have some unique id to identify that which with whose response it is.

(Refer Slide Time: 29:10)

A presentation slide titled "SNMP Security" with a yellow background and a blue header. It contains three bullet points: 1. "SNMPv1 uses plain text community strings for authentication as plain text without encryption". 2. "SNMPv2 was supposed to fix security problems, but effort de-railed (The 'c' in SNMPv2c stands for 'community')". 3. "SNMPv3 has numerous security features:" followed by three sub-bullets: "Ensure that a packet has not been tampered with (integrity)", "Ensures that a message is from a valid source (authentication)", and "Ensures that a message cannot be read by unauthorized (privacy)". The slide footer includes the IIT Kharagpur logo, the NPTEL logo, and the text "NPTEL ONLINE CERTIFICATION COURSES".

**SNMP Security**

- SNMPv1 uses plain text community strings for authentication as plain text without encryption
- SNMPv2 was supposed to fix security problems, but effort de-railed (The "c" in SNMPv2c stands for "community").
- SNMPv3 has numerous security features:
  - Ensure that a packet has not been tampered with (**integrity**),
  - Ensures that a message is from a valid source (**authentication**)
  - Ensures that a message cannot be read by unauthorized (**privacy**).

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Finally, we have a issue of SNMP security, as this it carries information about the different network devices and accumulate. So, security becomes a major challenge. So, SNMP version 1, uses plain text community string for authentications as print text without encryption in case of SNMPv1. SNMPv2 was supposed to fix security problems, but effort, but could not the c is the SNMP stands for community type of issues. Finally, SNMP version 3 has numerous security features. Like it ensures that the packet has not been tampered with there is an integrity issue; ensures data is valid so that the authentication.

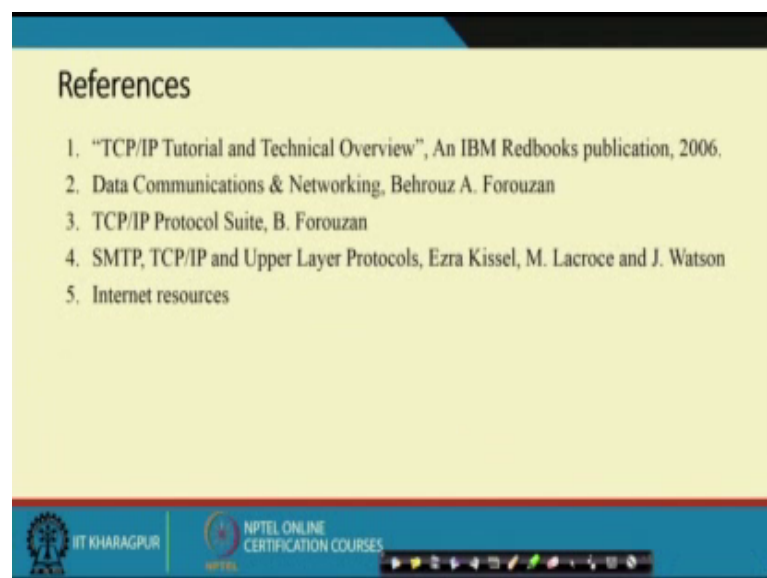
And ensures that the message cannot be read by unauthorized some agent or person or whatever, that is the privacy or confidentiality is maintained. So, what we see that all these integrity authentication privacy or confidence if there are CIA property sometimes, you say are tried to has been tried to a has been attempted in a SNMP version 3.

So, in this particular discussion what we try to impress upon or what our objective is to so discuss about one two again popular protocol. One SMTP that is the mail protocol

which we experienced in day out., SNMP as such we do not experience directly, but virtually the management of the network keeps this whole thing running, right.

So, it is the overall management of the network which makes these things running. And for that this SNMP with SNMP these agents and the these managers they take care of this overall management and take corrective actions to make the keep the health condition of the network in a appropriate state. We have referred some of the references we I have mentioned and though it is there can be other several internet resources.

(Refer Slide Time: 31:29)



So, let us stop at this stage today. And we will discuss about other layers and applications in the subsequent lectures.

Thank you.