Computer Networks
Prof. S. Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture # 37
Network management

Good day, so today we will talk about network management. You know that as the network becomes very large we need support for managing these networks, we need support for keeping track of these networks and how these are done is what we are going to discuss. So the topic for today is network management.

(Refer Slide Time: 1:17- 1:40 min)

Network management is the process of controlling a complex data network to maximize its efficiency and productivity. The overall goal of network management is to help with the complexity of a data network and to ensure that data can go across it with maximum efficiency and transparency to the users.

(Refer Slide Time: 1:41- 2:54 min)

The ISO that is the International Organization for Standards in network management forum divided network management into five functional areas: Fault management, configuration management, security management, performance management, and accounting management. Out of these often you find that there are two systems which has deployed in large network. One is the Network Management System and another is the Enterprise Management System. Enterprise Management System usually takes care of the configurations of individual machines etc, and the Network Management does the fault management and performance management. These are two aspects which network management always has to take place and it can do some configuration management for some network devices also. So we will just quickly run through each one of these.

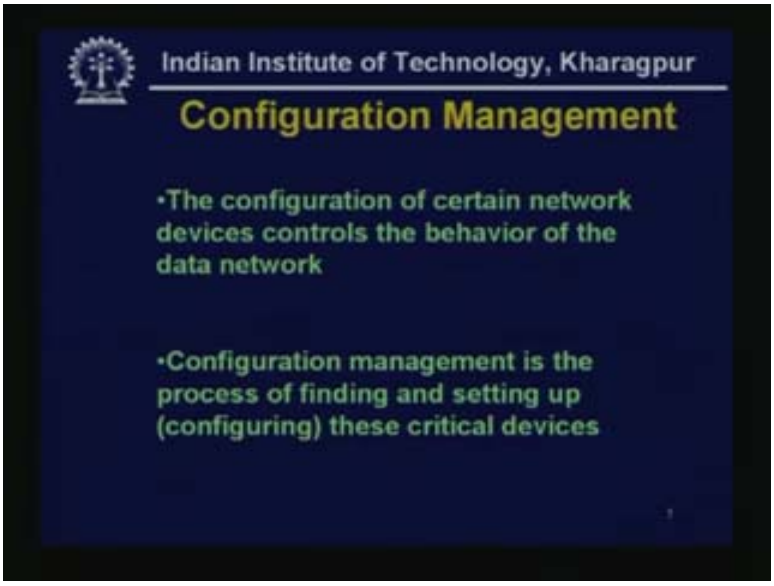
(Refer Slide Time: 2:56- 5:48 min)

Fault management is the process of locating problems or faults on the data networks. It involves the following steps: Discover the problem, isolate the problem, and fix the problem (if possible). Sometimes it is possible to fix the problem remotely and sometimes it is not possible. First of all discovering the problem is important because usually in a large network there are so many hundreds of components which have been deployed over a considerable area. You need to have a good support for discovering the fault. A fault in one part of a network can lead to impairment of services in another part of a network.

For example, suppose some switch has become faulty and it is generating a lot of spurious traffic, now the first thing is to locate where all these traffic is coming from, and then you have to isolate it, and then fix it. Sometimes you need to physically go there and fix it but sometimes you can do it remotely. But before you can fix it, you have to discover that there is a problem and this is where the problem lies, this is the central part of fault management.

Another thing to note is that, the network devices may come up first and be switched off. Therefore the topology of the entire network is not fixed, some of them may be off, some may be switched on but it is not working. So anyway the topology of the network is not fixed therefore for fault management, first you have to discover which are the areas or which are the elements that are currently on the network and are put on and are working correctly and then which others are not working. That is, they are switched off, or may be they are faulty etc. Continuously you have to be in a mode of discovering the topology of the network, as to find out which of these are switched on and which is doing what. Then we need to locate the faults as it occurs. This is fault management. Then you have configuration management.

(Refer Slide Time: 5:45- 6:02 min)



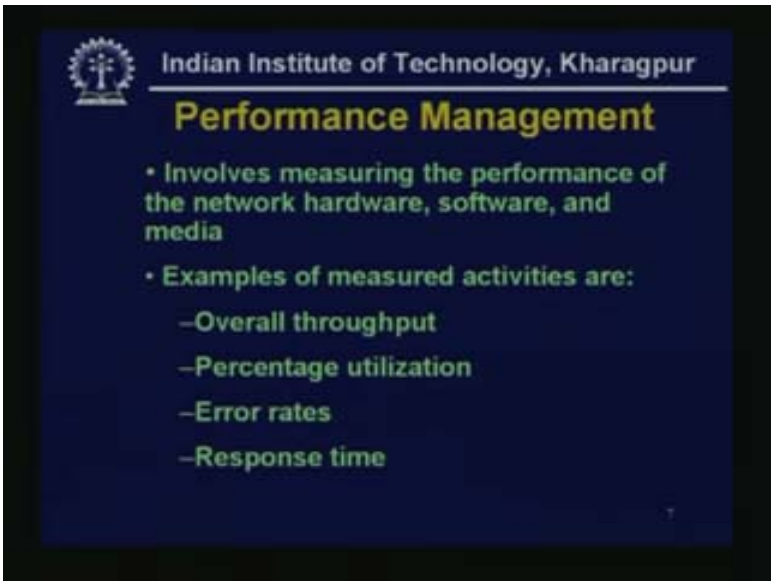
The configuration of certain data network devices controls the behavior of the data network. Configuration management is the process of finding and setting up that is (configuring) these critical devices.

(Refer Slide Time: 6:03- 6:36 min)

Security management: it is the process of controlling access to information on the data network. It provides a way to monitor access points, and records information on a periodic basis, and provides audit trails, and sounds alarms for security breaches. We will be talking more about security in the next lecture which is a very big topic by itself but

we will devote only one lecture to it. There we will talk little bit more about the security management and securities in network.

(Refer Slide Time: 6:39- 7:48 min)



Performance management: Involves measuring the performance of the network, hardware, software and media. Examples of measured activities are: Overall throughput percentage utilization, error rates, response time. Quite often a fault in a network does not always be faulty but there may be degradation in performance. For example, in one particular network node you may find that a lot of packets getting dropped. So you have to find out periodically that, who is doing what, and how, in a sense that at what percentage? How many packets it has handled? How many it has handled successfully? How many it has dropped and so on. And from such statistics you have to come to a conclusion about whether this is really malfunctioning or not. Error rates are important, response time, percentage and utilization. Once again there are ways to find out these things and we will talk about them.

(Refer Slide Time: 7:51- 8:11min)

Accounting Management: It involves tracking individual's utilization and grouping of network resources to ensure that users have sufficient resources. This involves granting or removing permission for access to the network etc so this is also important in many cases.

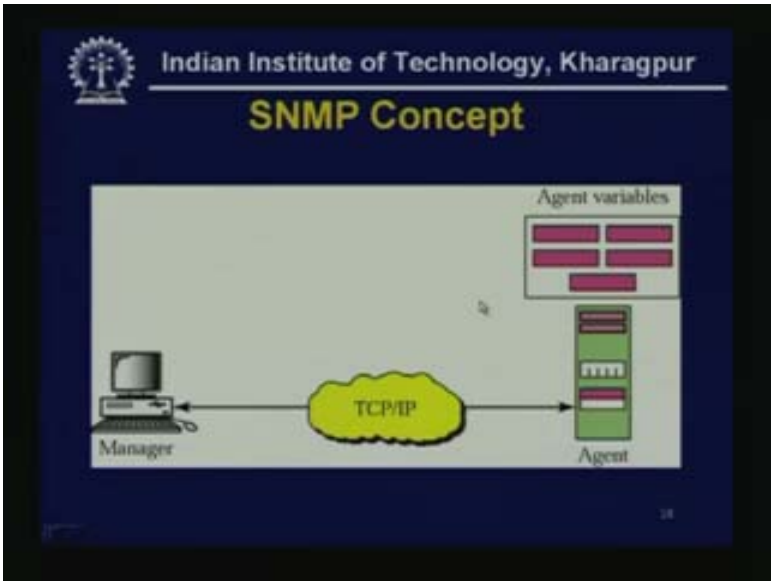
(Refer Slide Time: 8:13 - 10:50 min)

Now the protocol that is used for network management is known as SNMP Simple Network Management Protocol. Objectives are following: It is a framework for management devices in an internet using TCP/IP. It provides a set of fundamental operations for monitoring and maintaining an internet, and an application level protocol

allows it to monitor devices made by different manufacturers installed on different physical networks. In a particular network all the network devices will not come from the same vendor. You may have procured some of the devices at some point of time from some vendors and some other devices from some other vendor and all of them form a part of the same network. When you are talking about network management in that place, you have to talk about all these heterogeneous platforms. There has to be a standard protocol by which the network manager can talk to each of these devices.

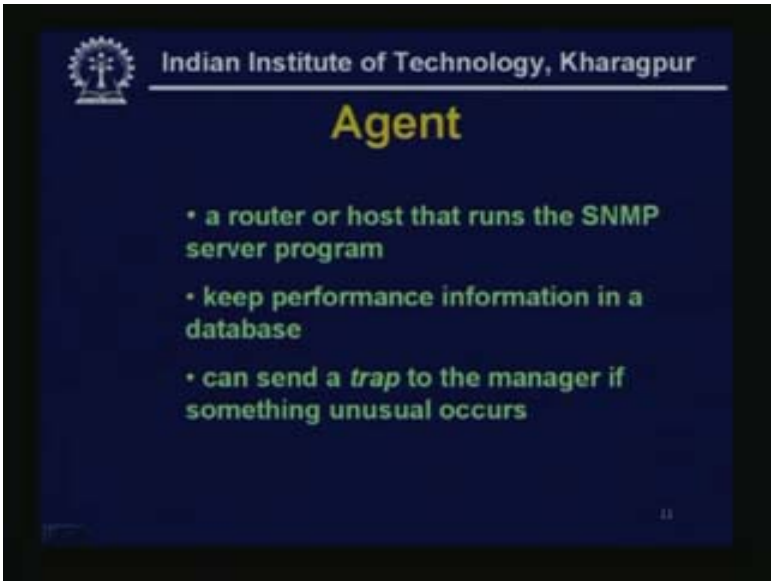
When you look at the network devices which are available in the market, you find that there are broadly two types of devices: managed device and unmanaged device. For example, for a switch there is a managed switch and an unmanaged switch. Obviously the switch which is unmanaged does not support this SNMP and do not have the so called management agent in it. In order to manage and get the information about it from a central place the devices have to be managed. Therefore at the very edge of the network for cost consideration you may put some unmanaged devices but then management of fault etc, for those devices have to be handled separately. You cannot monitor them centrally. For monitoring them centrally you need to have managed devices. Managed devices would contain some kind of software and some hardware support inside each of the device to talk to this network management station wherever it is broke. Usually this costs money but for a large network this is important.

(Refer Slide Time: 10:51 - 11:12 min)



This is a very simplified picture, we have the network manager here and through the TCP/IP protocol it talks to an agent. This agent resides in a managed device and these agents will have some agent variables which should be available to this manager for monitoring. That is the basic idea.

(Refer Slide Time: 11:14 - 11:48 min)

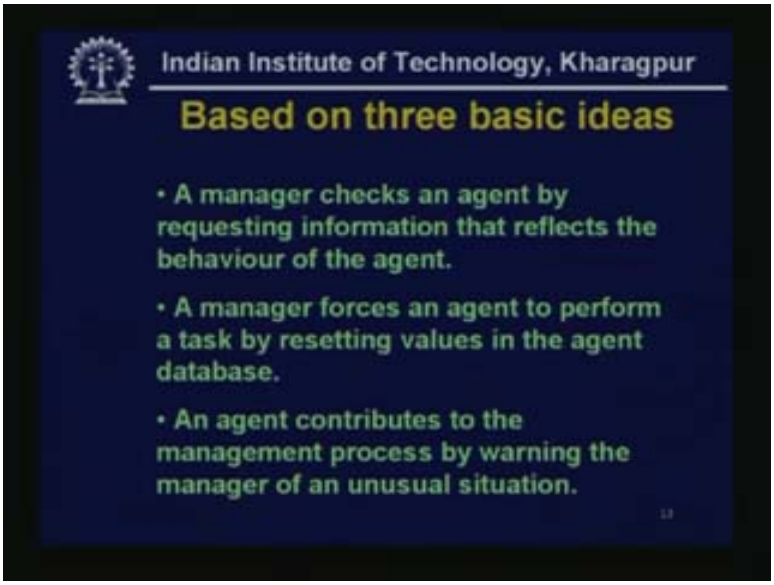


Agent: is a router or host that runs the SNMP server program. By the way, apart from managing network devices you can also have management agents in software etc to instrument it in some fashion. The agent keeps performance information in a database, can send a trap to the manager if something unusual occurs. So, trap is a sort of alert to the manager.

(Refer Slide Time: 11:50 - 11:56 min)

Manager is a host that runs the SNMP client program and has access to values in the agent's database.

(Refer Slide Time: 11:57 - 12:28 min)

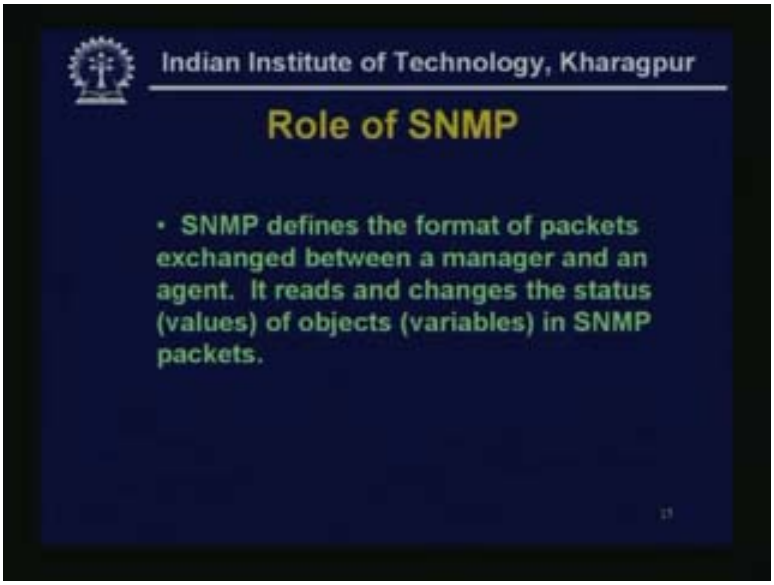


Based on three basic ideas, a manager checks an agent by requesting information that reflects the behavior of the agent. A manager forces an agent to perform a task by resetting values in the agent database. An agent contributes to the management process by warning the manager of an unusual situation. These are the three basic approaches and we have specific commands for doing all these.

(Refer Slide Time: 12:29 - 12:46 min)

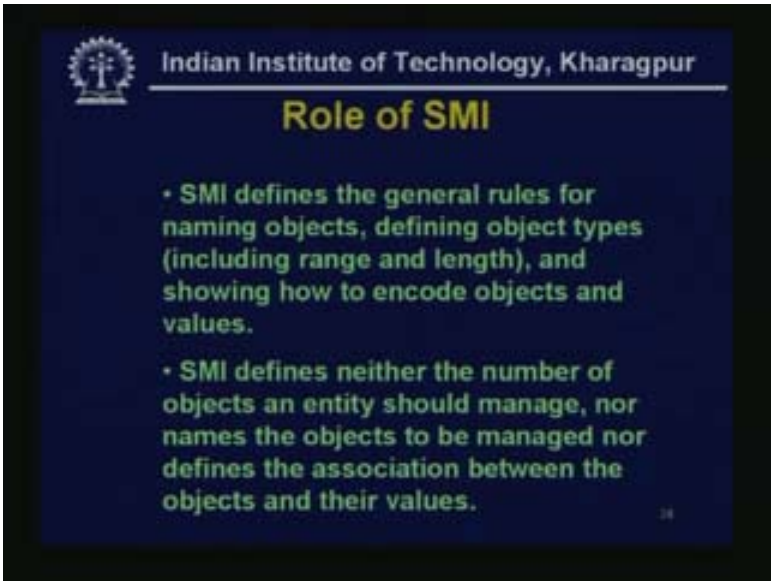
SNMP uses two other protocols: SMI: Structure of Management Information, and MIB: Management Information Base. So, one is used for naming objects and the other is the basic management information base accessed by the manager.

(Refer Slide Time: 12:47 - 12:57 min)



SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status that is the values of objects, variables in SNMP packets.

(Refer Slide Time: 12:58 - 13:52 min)



SMI defines the general rules for naming objects, defining object types including range and length and showing how to encode objects and values. SMI defines neither the number of objects an entity should manage nor the names the objects to be managed nor defines the association between the objects and their values. Instead, what SMI does is to have some scheme for giving names to the object. The names are not human friendly but they look as a series of integers, but there is a way of encoding the names of objects so

that we are very precise and distinct about what we are talking taking into consideration we can have a heterogeneous network.

(Refer Slide Time: 13:54 - 14:04 min)

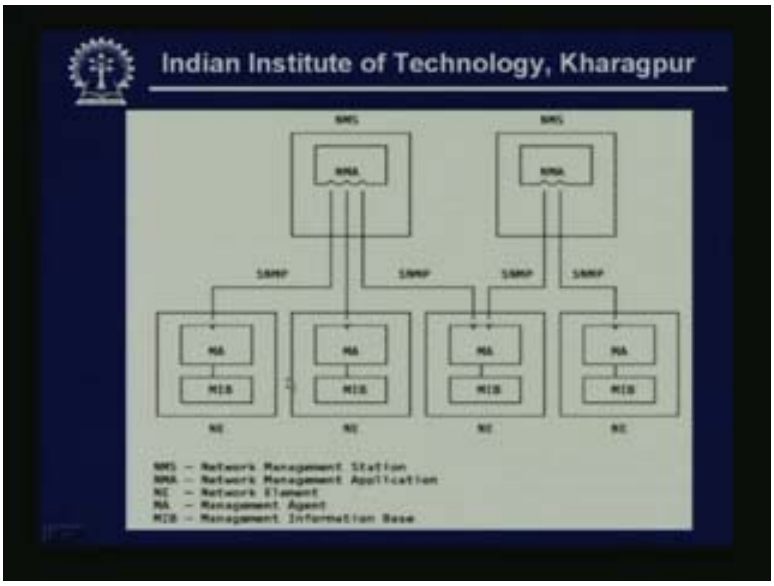
The role of MIB: MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.

(Refer slide time: 14:06 - 14:30 min)

SNMP: A group was formed and their efforts were completed in early 1993. There are 12 documents describing SNMP version 2, there is an SNMP version 3 also. There are three

basic commands that are used with SNMP: get, set, get next. These are the basic operations then you can have a bulk, get, etc.

(Refer Slide Time : 14:31 - 15:35 min)



This is the general situation we have. Network management station: There may be more than one network management station. In a very critical network you may have two network management stations, etc. Therefore we have some network management station which runs some network management application, NMA. This software talks in SNMP which manage devices. These are network elements which are managed. This NMA Network Management Application uses the SNMP protocol to talk to the management agent which resides in every managed object. This managed object maintains the MIB Management Information Base and from this the information passes back and forth. Hence this is the general scheme.

(Refer Slide Time: 15:36 - 15:40 min)

There are two approaches for the management system to obtain information from SNMP: One is the traps and other is polling.

(Refer Slide Time: 15:41 - 16:14 min)

First let us talk about traps. Traps are basically the information which is being pushed from the managed device to the network management station. Traps are un-requested event reports that are sent to a management system by an SNMP agent process A. A trap will contain the network device name, time the event happened, and the type of event.

(Refer Slide Time: 16:15 - 16:51 min)

When a trappable event occurs, a trap message is generated by the agent and is send to a trap destination - a specific configured network address which is the network address for the management station. Many events can be configured to signal a trap like a network, cable fault, failing NIC, or hardware, a general protection fault, or a power supply failure. Although many events can be configured to signal a trap but there are pros and cons of what event is being configured a trap, there are trade offs.

(Refer Slide Time: 16:52 - 18:15 min)

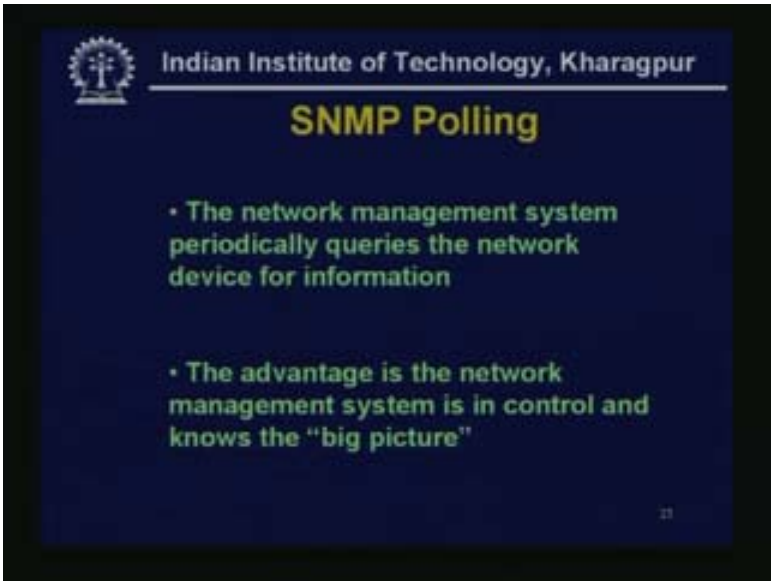
Traps can also be throttled. You can limit the number of traps sent per second from the agent, this is important. For example, a faulty node may keep on generating a very large

number of traps. So that it will overwhelm the network and it will not carry any extra information in helping to set right the fault. You may have to constrain the number of traps that can be generated per minute time or something. So traps have a priority associated with them. Critical, major, minor, warning, marginal, informational, normal, unknown etc. Actually it may not be a good idea to generate traps. For low clarity may be you should not be generating any trap at all because if you do that, remember that a network may consist something of the order of a few hundred or a few thousand network devices and if all of them generate routine reports and keep on sending traps then that may not be a very effective way of managing a network.

(Refer Slide Time: 18:16 - 18:43 min)

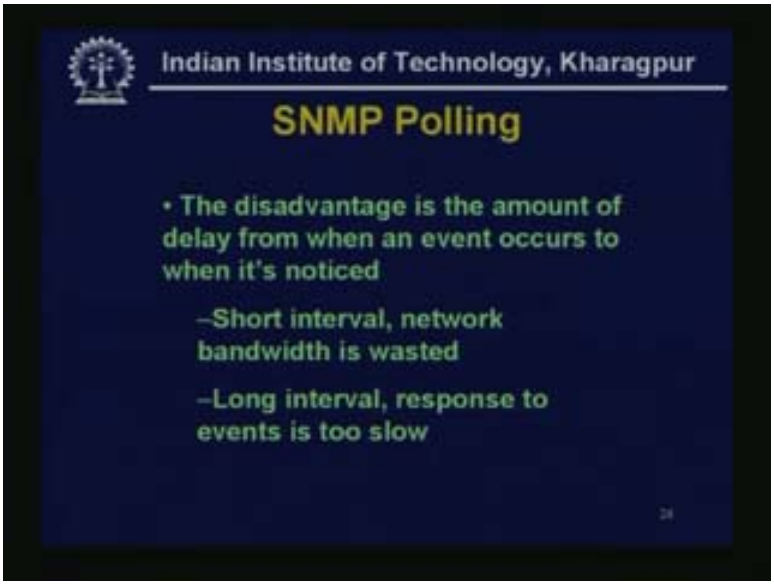
Resources are required on the network devices to generate a trap. When a lot of events occur the network bandwidth may be tied up with traps. So, thresholds can be used to help because the network device has a limited view. It is possible that the management system has already received the information and the trap is redundant. If something has happened somewhere else and somebody else has detected it and generated a trap then that is not generating any extra or relevant information.

(Refer Slide Time: 18:49 - 19:26 min)



The network management system periodically queries the network device for information. So this is the other mode which is SNMP polling. From time-to-time the network management agent will request for some information from the management agent and this might do in a round robin fashion, in a periodic fashion using some period which is configurable. The advantage is, the network management system is in control and knows the big picture. So this is the other way; one is trap, the other is polling.

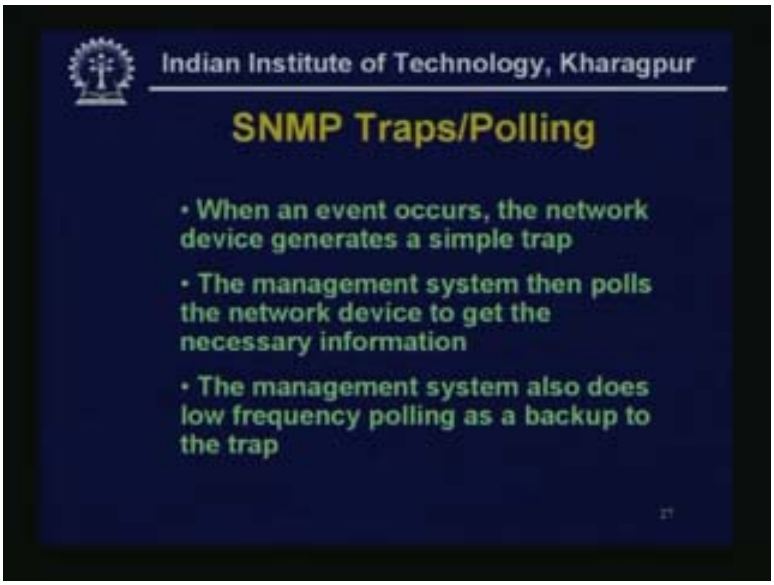
(Refer Slide Time: 19:27 - 20:25 min)



The disadvantage is the amount of delay from when an event occurs to when it is noticed. For short interval the network bandwidth is wasted and for long interval the response to

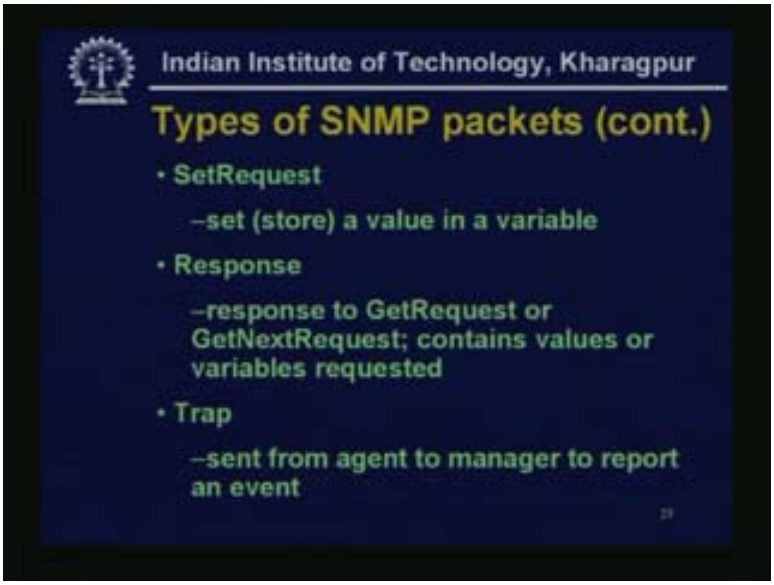
events is too slow. The point is that, if you are depending only on polling and if you are polling at a very low frequency then after your last poll immediately some fault may have occurred but you will discover that only when you poll next. So, in a long interval the response to events is quite slow. On the other hand if you poll very fast then most of the network bandwidth and network resources are used for this network management so that is not very efficient and bandwidth is wasted. So you have to come to some kind of trade-off between the two.

(Refer Slide Time: 20:26 - 21:23 min)



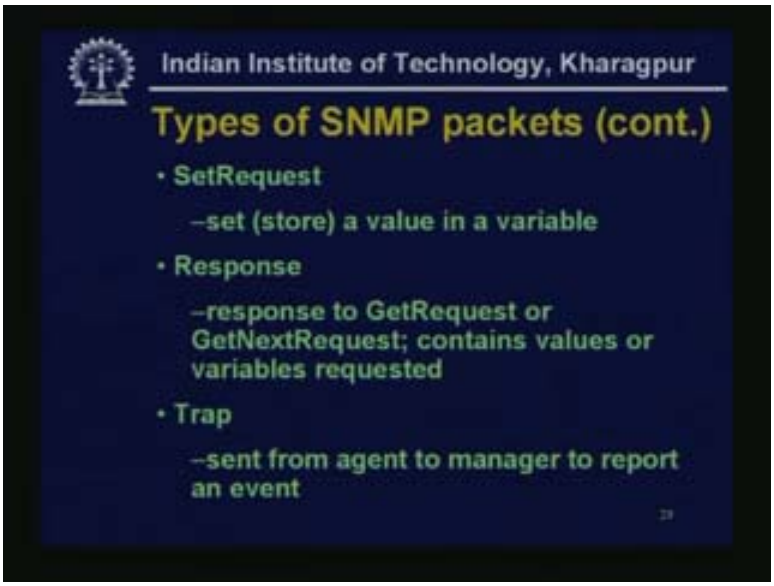
One good way to approach this is to use both traps and polling. When an event occurs the network device generates a simple trap. The management system then polls the network device to get the necessary information. The management system also does the low frequency polling as a backup to the trap. What might have happened is, you cannot depend purely on trap for one reason that is, the network device may have gone down in such a way that it is not even able to generate the trap. In that case the trap will never come, only thing is that, when the network management station polls that particular device it will fail to respond and that way it will find out that something is wrong. So you should use a mixture of trap and polling to do your management.

(Refer Slide Time: 21:24 - 21:26 min)



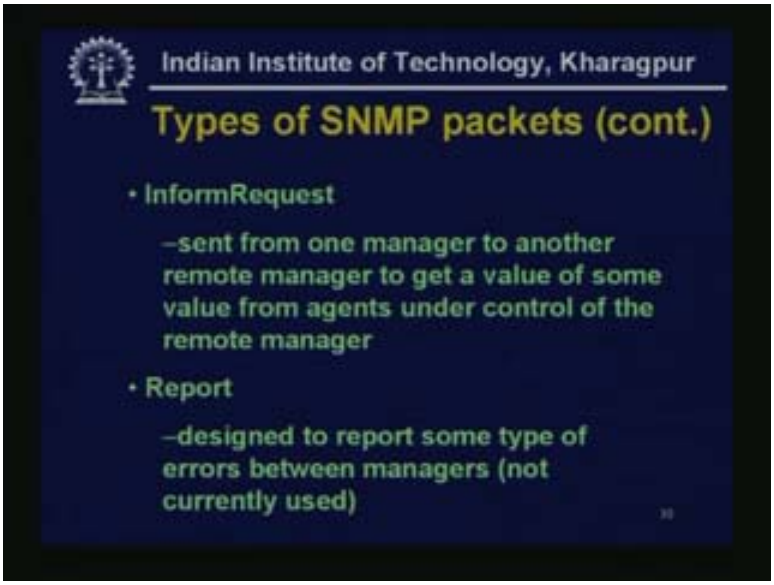
Let us quickly go through the types of SNMP packets: GetRequest - It retrieves the value of a variable or a set of variables; GetNextRequest – Is used to retrieve values of entries in a table; GetBulkRequest- Retrieves a large amount of data used instead of multiple get request and get next request so that in one go you can get a lot of information as far as bandwidth is concerned.

(Refer Slide Time: 21:57 - 2:11 min)



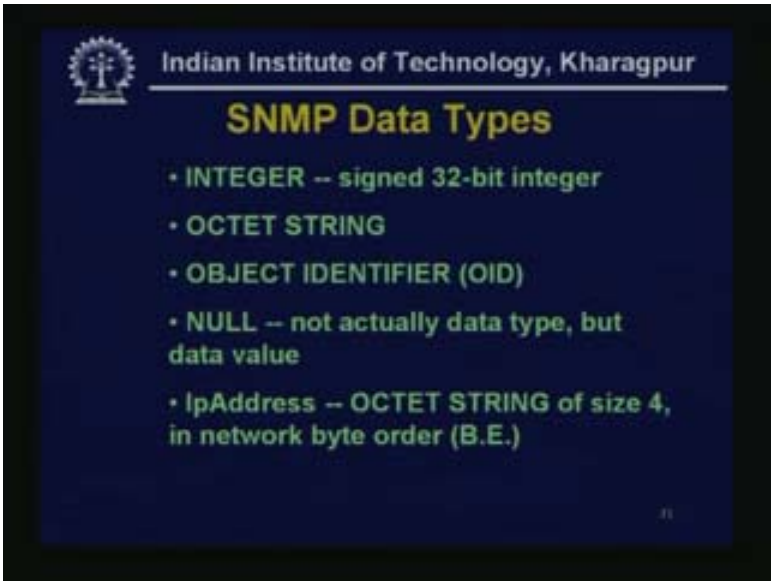
SetRequest - Set or store a value in a variable; Response – Response to get request or get next request contains values of variables requested; Trap - Sent from agent to manager to report an event.

(Refer Slide Time: 22:15 - 22:31 min)



Inform Request - Sent from one manager to another remote manager to get some value from agents under control of the remote manager; Report - designed to report some types of errors between managers but is not very widely used.

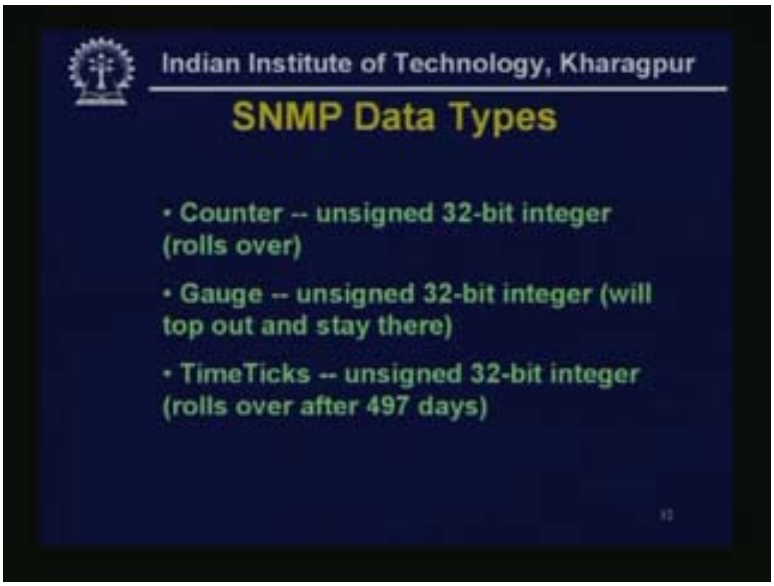
(Refer Slide Time: 22:32 - 24:01 min)



Now we come to the SNMP data types, These data types have to be, since network may contain devices from different vendors, each vendor of course will design his own agent so he has to agree to some kind of standard about what will be there. But at the same time we do not want to standardize things in such a way so that people cannot innovate and come up with new kinds of devices. What is defined are the different data types, different

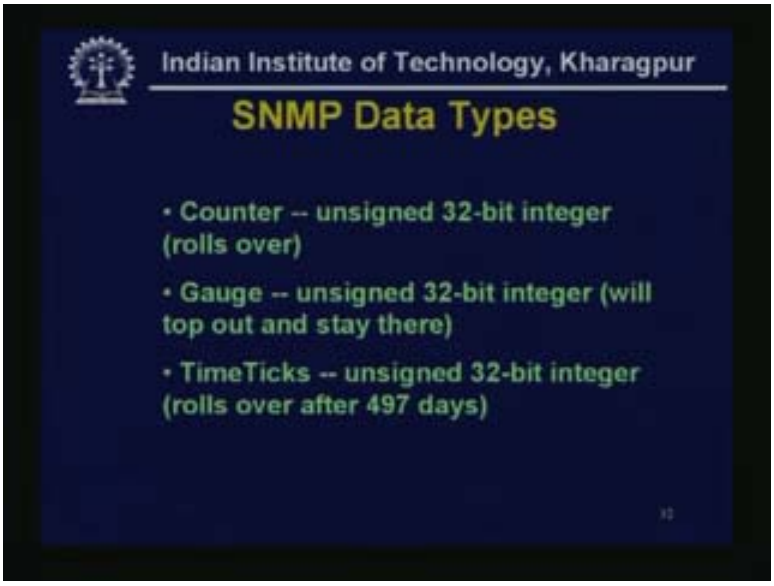
types of variables, one is the integer - it is a signed 32-bit integer, Octet string that is the byte string, Object identifier - is one of the most important data types and we will look into the detailed of object identifier when we talk about SMI; NULL: Is not actually a data type but a data value, IP address is a special data type, it is an octet string of size 4 bytes. We are using 4 byte of addresses in network byte order.

(Refer Slide Time: 24:00 - 25:02 min)



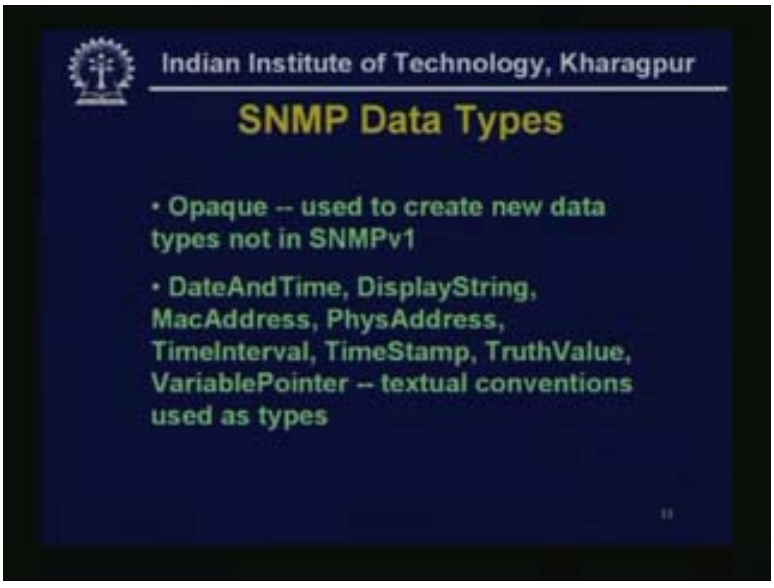
Then you have a counter: It is an unsigned 32-bit integer which rolls over. The 32-bit will count to about 4 trillion. After the end of the counter the value is rescheduled which means it will go back to zero and start counting from zero again. This counter is more important because that is what will give you the statistics about the network. For example, you want to know that in the last may be ten minutes or so how many packets this has been sent, and how many packets has been dropped, and how many packets has been successfully processed etc. So the management station may want to know such information. So these are the kind of statistics you collect. Therefore you need to have these counters for these different values. Now a counter is going to go back to zero after sometime so you need to take care of that.

(Refer Slide Time: 25:02 - 26:05 min)



If this going back to zero then after a poll, when you have got a value and when you see that the counter value is sufficiently high, you may like to set it to zero deliberately so that you get the right count next time. Gauge: unsigned 32-bit integer, once again it is the same as counter but it will top out and stay there. That means, it is going to top out and the next time you come it will not show a very low value but it will show a high value. And if you see that the gauge has topped out may be you can reset it after that but you get some estimate of what has happened rather than a rolled over value. Time ticks: Unsigned 32-bit integer so 32-bit integer rolls over after 497 days. But 497 days is very long in this network world.

(Refer Slide Time: 26:06 - 26:36 min)

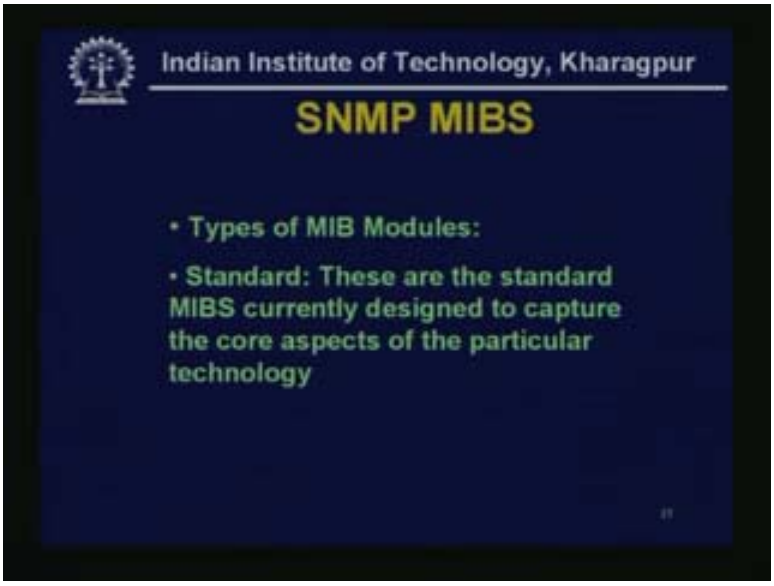


Opaque: Used to create new data type not in SNMPv1. And then there are some other data types for specific purpose like date and time, display string, MAC address, physical address, time interval, time stamp, truth value, variable pointer, textual conventions used as types. These are the different SNMP data types.

(Refer Slide Time: 26:37 - 27:43 min)

Let us just have a look at the SNMP MIBS. Management Information Base is a collection of related managed objects used to define what information you can get back from the network device. These are standard and enterprise specific MIBS. The point is that, some things may be standard, and there are some information about the device. For example, if we have a device designed by CISCO then that may have its own specialty which is not found in other vendors. Therefore that specialty will require some information which is specific to the particular vendor. Hence we have vendor specific information also, and we have general information also. There are standard and enterprise specific MIBS. And, if you later on mix up between the two, that means, something that is specific to vendor 1 and something specific to vendor 2 it will not work out and so these two need to be separated. So naming of objects is very important. Thus there is standard and enterprise specific MIBS.

(Refer Slide Time: 27:45 - 27:55 min)



Types of MIB modules: Standard: These are the standard MIBS currently designed to capture the core aspects of the particular technology.

(Refer Slide Time: 27:56 - 28:10 min)

Experimental: Temporary and if achieves standardization then it is placed in the standard module. Then Enterprise-specific: Vendor specific MIBS that provide additional management capabilities for those features that require it.

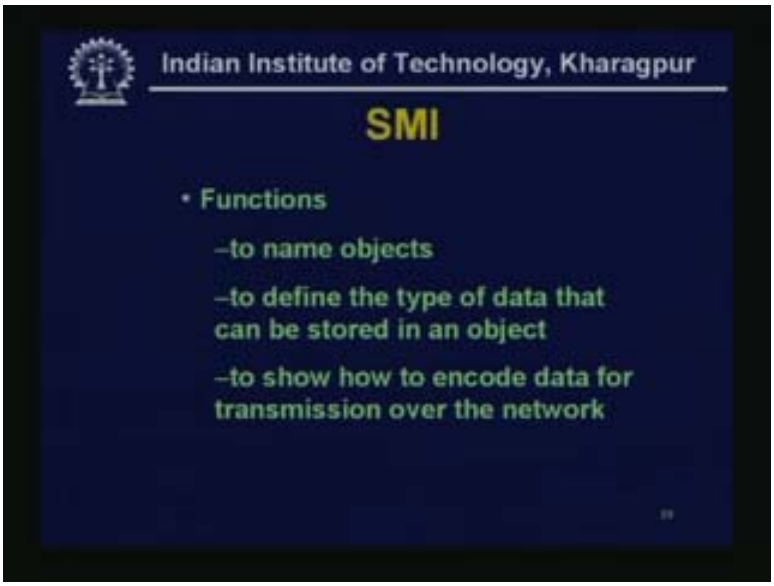
(Refer Slide Time: 28:11 - 28:56min)

If you are using the MIB you also require the MIB tools, you require a MIB compiler, you require a MIB browser, a MIB alias tool, a MIB query tool, etc. A MIB browser allows you to browse through the management information base in a particular device directly. And MIB alias is required because, as we see the naming is very complex. So once you have given a name you do not have to repeat that name in every query so you have an aliasing tool and a MIB query tool.

(Refer Slide Time: 28:57 - 29:10min)

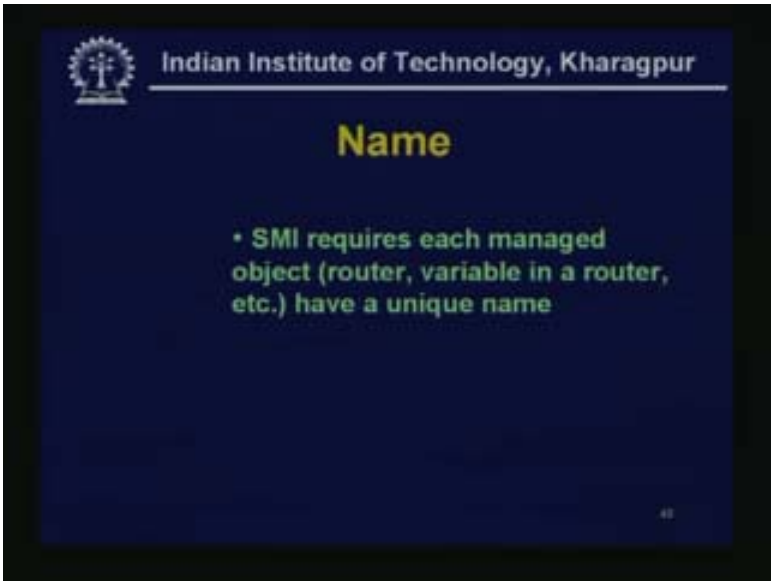
SMI: Structure and identification of management information. The SMI defines the rules for how managed objects are described and how management protocols may access these objects.

(Refer Slide Time: 29:11 - 29:24 min)



Functions: Are to name objects, to define the type of data that can be stored in an object, to show how to encode data for transmission over the network.

(Refer Slide Time: 29:25 - 29:52 min)



Name: SMI requires each managed object that is router, variable in a router, etc. which have a unique name. So router will have a name, a variable in a router will also have a

name, and a specific router coming from location should also have some way of describing that.

(Refer Slide Time: 29:53 - 32:24min)

The naming convention really starts from a high level and it uses the integer.representation. There is a name.notation. Actually ISO has defined a very global naming tree. It starts from ISO itself, and under ISO there are so many things and under each of these there are so many things.

For example, ISO.org.dod.internet.Management.MIB 2 and when I say this much, actually this ISO has got the number 1 and under ISO there are so many entities, one of them is called organization and this is an entity, a number 3 and there is a department of defense of US, that is an entity with a value 6. ISO is a European organization and all these are decided by ISO.

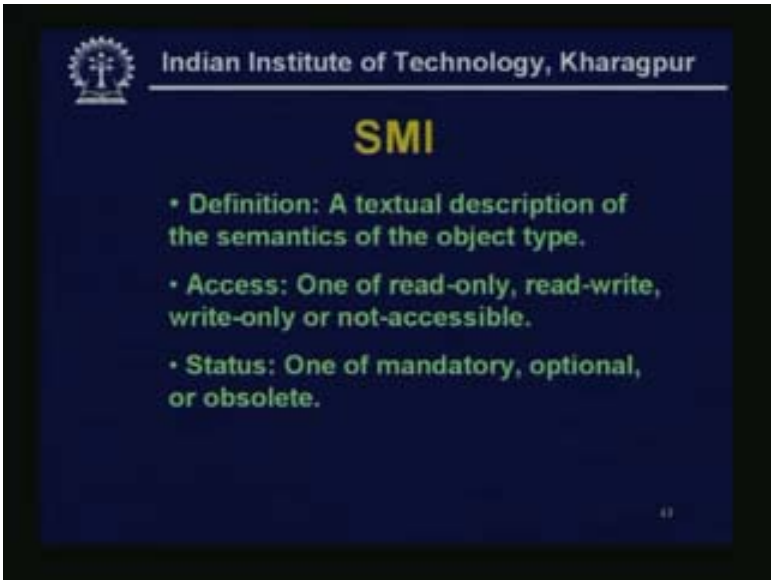
Therefore, the Department of Defense did not take a note of it. But when the internet started on the Department of Defense they saw that nobody has used anything of the naming convention and they decided to take one. And then management.2, then MIB is .2 and up to this much we have not even come anywhere close to the particular device that we are trying to manage.

All objects managed by SNMP are given an object identifier. The object identifier always starts with 1.3.6.1.2.1 because we are talking about network management, and in network management naturally it has to do with network, then may be it has to do with MIB.2 and then internet and since it is the internet it has to do with DODN and all the way up to ISO. So that 1.3.6.1.2.1 etc is always the prefix of any name and there are many other integers with many more DODs in them.

(Refer Slide Time: 32:25 - 32:52 min)

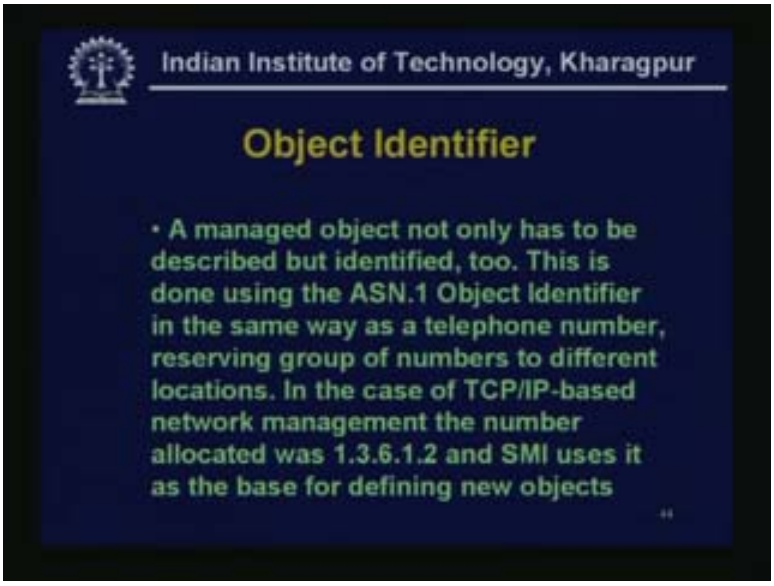
Apart from this an object in SMI has a textual name which is there in SMI termed as the object descriptor for the object type along with its corresponding object identifier which is defined. Syntax: the abstract syntax for the object type. It can be a choice of simple syntax that is integer, octet string, etc or application syntax.

(Refer Slide Time: 32:54 - 33:08 min)



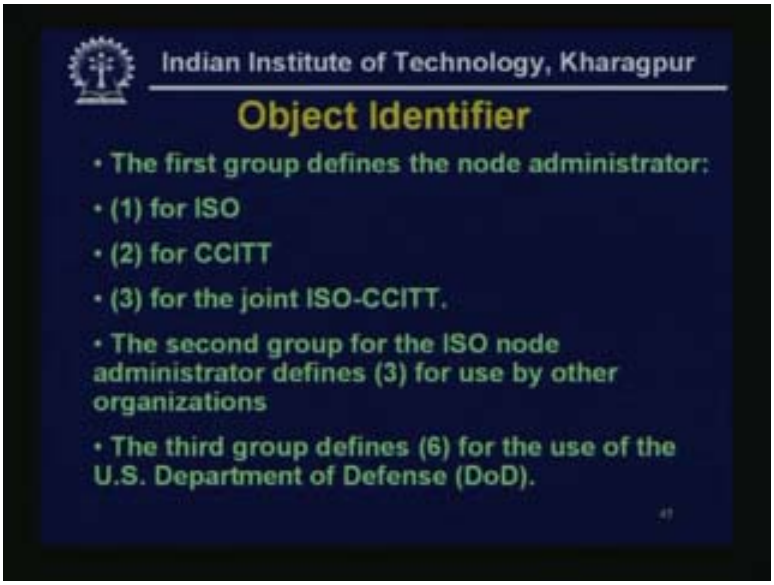
Definition is a textual description of the semantics of the object type. What type of object it is? Access: one of the read only, read write, write only, or not accessible kind of access is defined. And status: One of mandatory, optional, or obsolete.

(Refer Slide Time: 33:10 - 33:30 min)



This object identifier is also a part of that, it is like a telephone number and it always starts with 1.3.6.1.2 and SMI uses it as the base for defining new objects.

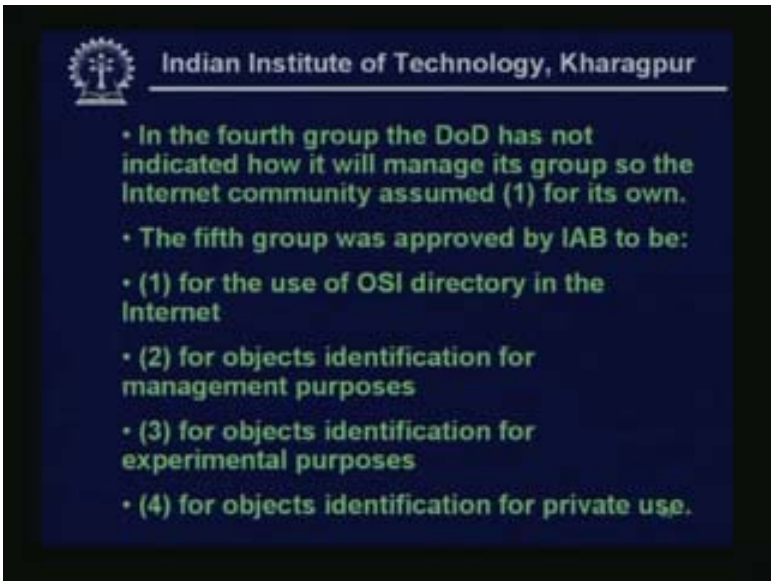
(Refer Slide Time: 33:31 - 34:25 min)



In the first group, ISO was 1, CCITT was 2, and for the joint ISO – CCITT there was a number 3. Since this is under ISO that is how the first one comes. The second group for the ISO Node administrator defines 3 for use by other organizations. So in 1.3 the 3 is the other organization. Actually there are a large number of things in that particular level, we are having a global naming tree for naming anything under the sun. So there is a thing

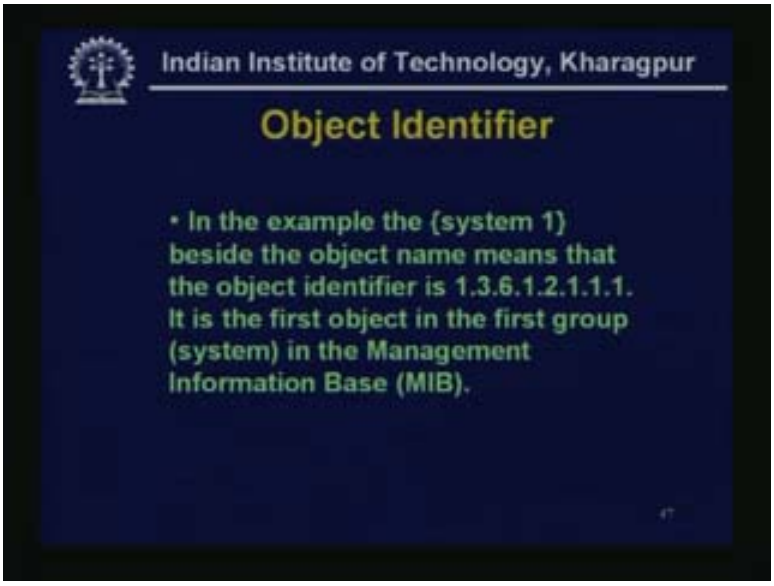
called other organization and that other organization is 3 and the third group defines 6 for the use of U.S. Department of Defense, so it is 1.3.6.

(Refer Slide Time: 34:26 - 34:45 min)



In the fourth group the DOD has not indicated how it will manage so internet is 1. The fifth group was approved by IAB to be 1 for the use of OSI directory, 2 for object identification for management purpose. So this is the one that we are interested in.

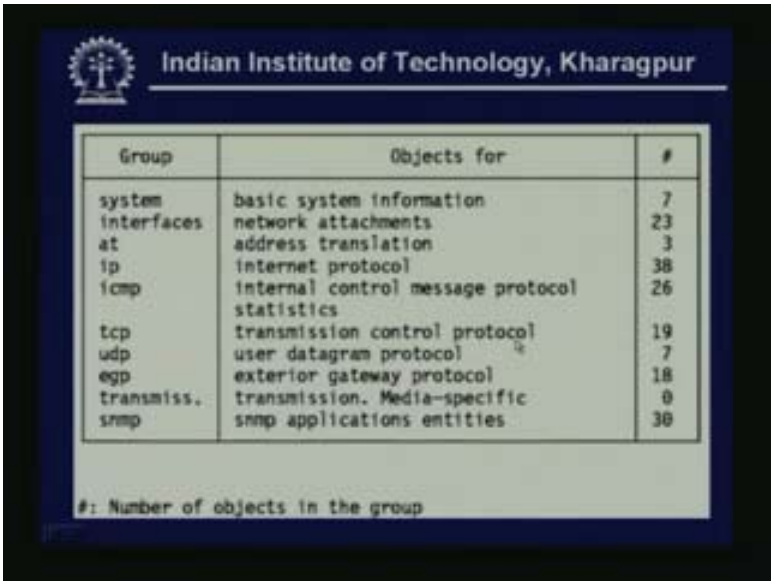
(Refer Slide Time: 34:46 - 36:22min)



Therefore we have 1.3.6.1.2.1.1.1 and since it is a global naming tree we have to come quite deep down to any particular level. Finally it is possible that not only you have some

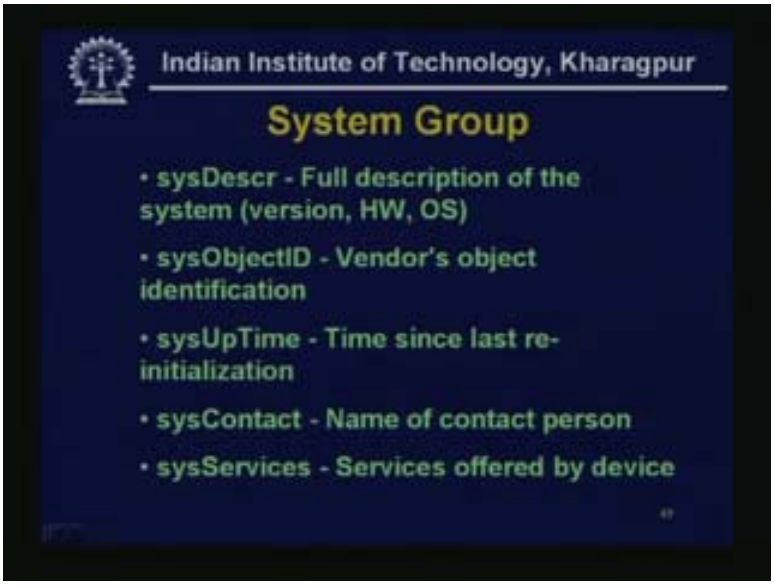
network devices etc somewhere down in the tree but you also have some sub trees for specific vendors. So this naming can go down that sub tree to talk about something specific to a particular vendor. Or even if we have come down to the tree somewhere and now you have got into a router, now in the router also we want to talk about interfaces and about other things so the tree also goes down from that point. So the point is, through this naming procedure we can exactly specify anything that is being talked about in this whole management scenario. Only trouble is, it is almost impossible for human beings to remember any of these names or any of these things. But the network management application makes this query to MIBS etc., so you are usually spared the trouble of looking into this. But if you look into this you will find such object identifiers in the MIB.

(Refer Slide Time: 36:23 - 36:53 min)



The MIB-2 group: This was divided into ten groups: One for system, one for interfaces, one for address translation, one for internet protocol and so on. And the number of objects in each of these groups is given over here.

(Refer Slide Time: 36:54 - 37:32 min)



We have a system group which has a system descriptor system, object ID system up time, system contact. The system up time is the time since last re initialization, and system object ID is vendor object identification and so on. This makes the scheme very general so that even devices from heterogeneous vendors can also be accommodated and you can talk about very standard things and that is why it was done this way.

(Refer Slide Time: 37:33 - 38:03min)

Now let us look at the network management platform. Historically, network management revolved around multiple systems each managing one specific set of components on the data network. Restrictions of money, physical space, and technical expertise led to the

desire to have the components managed by a single system that would show their inter connections on a network map.

(Refer Slide Time: 38:04 - 39:20 min)

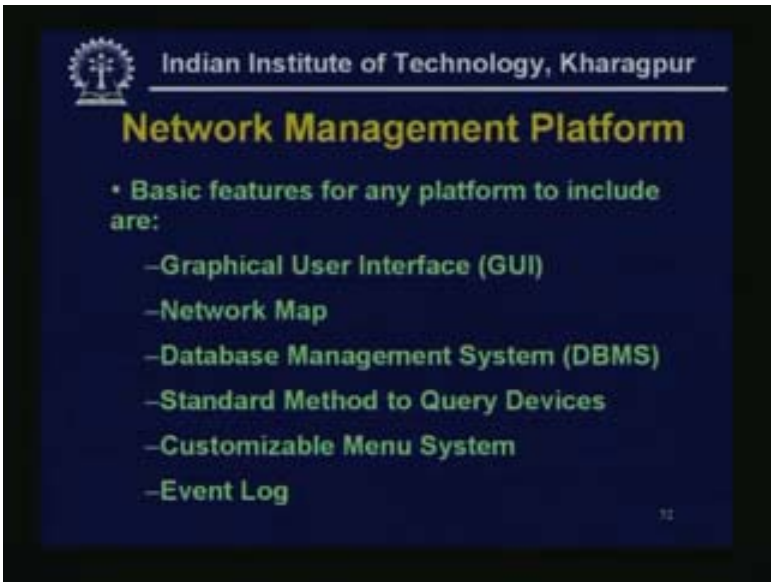
This is how a network management platform evolved. It is a software package that provides the basic functionality of network management for different network components. So, a network management platform has to be a general kind of software.

For example, on one side you have specific vendors for managing a specific set of devices, you may have some network management application etc which is there. Hence you have this particular application from this vendor for managing his devices, and then you have some other network management application for some other devices from some other vendor etc. But then finally you would like to sit in one place and have the big picture. So there has to be a platform which can couple with these different network management applications known as the network management platform, i.e. the general software which is running which can integrate all these different components.

(Refer Slide Time: 39:21 - 39:57 min)

The goal of the platform is to provide generic functionality for managing a variety of network devices. There are some functionality and some requirements for network management which is very general. Those are collected in the network management platform and if there are specific things you have to talk about for a particular type of device may be from that particular vendor then that is out of the platform although that software can integrate with this network management platform. That is the idea of having a network management platform.

(Refer Slide Time: 39:58 - 41:11min)



Basic features for any platform to include are Graphical User Interface GUI and network map. The first thing that a network management platform should do or is expected to do is to go on discovering the different network devices which are right now on, which are accessible etc, and those which are not accessible that means which were supposed to be previously there. And it would be nice if you can show it graphically on a screen like showing different colors for different types, and different icons for different types of nodes, and different colors showing whether it is working, not working, switched off etc, and if you can see that picture then you get the big picture in one go. Therefore this network map is important. A DBMS naturally wants to keep this management data and then query etc so it needs some DBMS. You need a standard method to query devices and a customizable menu system, event log, etc. These are the basic features for any platform.

(Refer Slide Time: 41:12 - 42:19 min)

Additional features for a platform using graphing tools which graphically shows with some kind of plots that how each device is performing. This should be able to show you the plot very easily. So this graphing tool is also an integral part. Then the application programming interface API is important because after you have finished talking about the generic network management aspects then you also have these special aspects for which the different vendors are going to give you special tools. These special tools now have to integrate with this network management platform. Therefore the API Application Programming Interface has to be very clearly defined. Finally it is the system security which is always present.

(Refer Slide Time: 42:16 - 42:33min)

Here are some examples of network management platforms: Sun's SunNet Manager, IBM Netview, HP's OpenView by the way is a very widely used network management platform in this category.

(Refer Slide Time: 42:34 - 43:02 min)

If you remember, one diagram in which we showed two network management stations etc which has to do with the network management architecture and the network management platform can use various architectures to provide functionality. The three most common are: Centralized, Hierarchical and Distributed.

(Refer Slide Time: 43:04 - 44:22 min)

In the centralized architecture as the name suggest you have one central network management station or network management platform besides on a single computer system that is a centralized system. In that case that particular station becomes absolutely critical because in a large network network management software is used all the time. Hence, if you have them centrally it becomes a single point of failure. So what you may do is that, you may duplicate the same thing on another machine. If one of them fails, it will not want to have single point of failure in a network if you want to at least make the critical components of it; and network management is a critical component of a large network. So you may like to have a fall back mechanism where in the primary one fails the other one can immediately take over. Although we have put two network management stations this is a centralized architecture. Therefore for full redundancy the computer system is backed up by another system, can allow access and forward events to other consoles on network. So this is a centralized architecture.

(Refer Slide Time: 44:23 - 44:38 min)

This is used for all network alerts and events, all network information, access all management applications etc. Hence one central architecture is used.

(Refer Slide Time: 44:38 - 45:20min)

And the pros are the following: A single location to view events and alerts, a single place to access network management applications and information, security is easier to maintain. This is an advantage, so in one place you get all that you want to view and it is easier to make it secure, and a single place to access the NMI because using the NMI, set etc you can also do things to the network, and you do not want any unauthorized person to have access to the network management station.

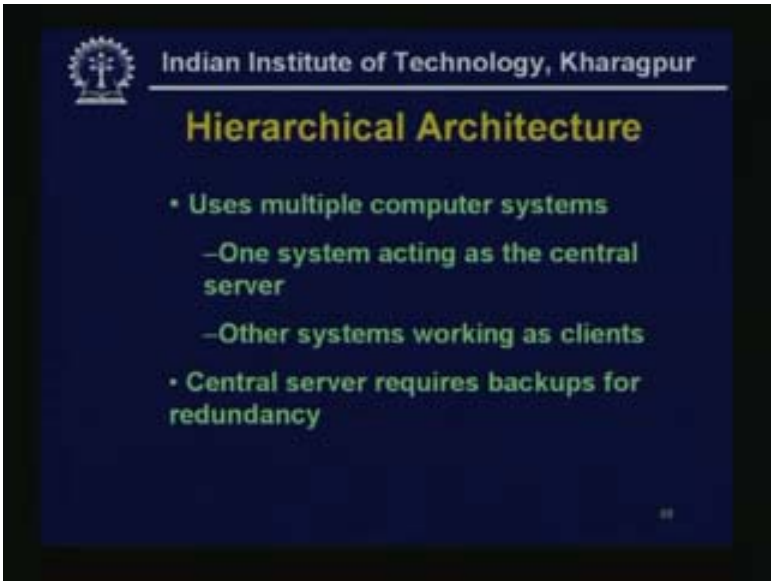
(Refer Slide Time: 45:21 - 47:08 min)

In the cons of the centralized architecture it has disadvantages. Single system is not redundant or fault tolerant, but you can make it somewhat fault tolerant by keeping another machine but if the connection to this room is somehow cut then the entire network becomes a black box. As network elements are added, may be it is difficult or expensive to scale the system to handle the load, having to query all devices from a single location.

As a matter of fact think of an enterprise of today. An enterprise of today that may be across various locations, it may be over a WAN, and many of these locations may be quite big hence a network that an enterprise may want to control centrally may become too big. So there is a question of whether a central server can scale it to that extent.

Actually there are problems, for example, if WAN bandwidth server or some part of it is out of WAN and WAN bandwidth is also a problem because if all the network management traffic is also coming over a WAN then that becomes quite an expensive scenario. But at the same time you have this advantage of this centralized architecture that in one place you can view all the things. These are the pros and cons, and so having to query all devices from a single location will not be good.

(Refer Slide Time: 47:09 - 49:14 min)



Therefore we go to the next step which is the hierarchical architecture. It uses multiple computer systems where one system acting as a central server and other systems working as clients. Central server requires backups for redundancy, this is the situation. Once again think of the same enterprise which is distributed geographically which may be five different locations and in each of these locations you have a big local area network to manage. So what you might do is, for each of these locations you may put its own management station who will manage the local network. You can even put a central server and all these management stations in different locations would be the client to the central server so only the important information or only the condensed and summarized information is coming to the central location via the WAN. Therefore, by this you conserve WAN bandwidth and at the same time you have a central location where you can get the entire picture and if you want you can talk to one of the clients and drill down and look at the specifics if there are problems somewhere, so this has all kinds of other advantages. For example, you can keep very good and expensive network experts in the central location as he can detect a problem over there and then over the network itself he can actually look into the issue and offer a genuine advice as to what needs to be done at that juncture. This is an advantage and this is a hierarchical architecture. The central server can also be backed up for redundancy.

(Refer Slide Time: 49:15 - 49:36 min)

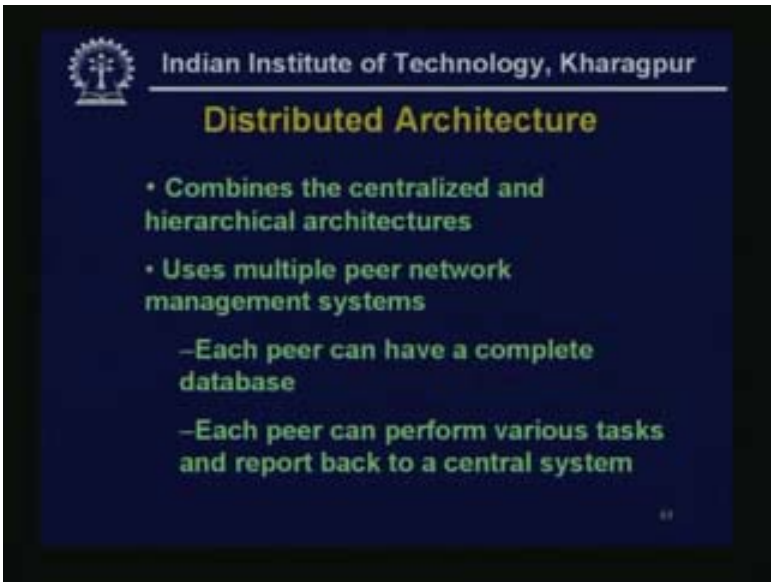
Key features: Not dependent on a single system. So, even if a single system or a single link is cut still some of the network is being managed. Distribution of network management tasks is distributed now. Network monitoring distributed throughout the network, and centralized information storage is also there. These are the advantages of hierarchical architecture.

(Refer Slide Time: 49:38 - 50:02 min)

Pros: Multiple systems to manage the network.

Cons, the disadvantages: Information gathering is more difficult and time consuming because it is coming through two layers. And the list of managed devices managed by each client needs to be predetermined and manually configured.

(Refer Slide Time: 50:03 - 50:56 min)



Then we have a distributed architecture. It combines the centralized and hierarchical architecture. It uses multiple peer network management systems. Each peer can have a complete database. Each peer can perform various tasks and report back to a central system. Previously there was only one station that was central and the others were in a sort of master-slave kind of situation but now there are all peers so each of them can keep an entire database if it wants to. Therefore each of them can work as a central management network station and they are distributed.

(Refer Slide Time: 50:57 - 51:18 min)

It contains advantages from central and hierarchical architectures, single location for all network information alerts and events, single location to access all management applications, not dependent on a single system, distribution of network management tasks, distribution of network monitoring throughout the network.

(Refer Slide Time: 51:19 - 52:03 min)

We already discussed about the network management platform. Now let us talk about specific network management applications. The goals of specific network management applications are to effectively manage a specific set of devices, avoid functionality overlap with the platform which means the network management platform, integrate with

a platform through the API and menu system, and reside on multiple platforms. These are the goals. So, applications do not share information because these two applications may have come from two different vendors.

(Refer Slide Time: 52:04 - 52:09 min)

Some examples are; Cisco works or 3com's Transcend etc.

(Refer Slide Time: 52:10 - 52:30 min)

Choosing a Network Management System: It is built from two major components: the platform and applications. A practical approach follows these steps: Perform device

inventory, prioritize the functional areas of network management, survey network management applications choose the network management platform.

(Refer Slide Time: 52:31 - 54:45 min)

We will just mention about another term which comes quite often. RMON: Remote Monitoring MIB. These have agents and probes. So this is actually used for monitoring MIB remotely and there are specific groups for this RMON, that is statistics group, history group, alarm group, host group, host top N, etc. These are standardized to operate on Ethernet segments so that apart from network management stations you can monitor it from other places also.

I think I am going to stop here, as you can see what I have tried is, to give you a broad overview of this network management system and as it is growing it.

Network management is something which in today's world you cannot do meaningful network management without machine support, i.e. you cannot do it manually and those days are actually gone. And in large network the number of events that are happening is really tremendous and it is not also possible to keep a log, the machine of course keeps a log and after a month or so the log has become so big, may be you have to delete it from your machine and then the log starts accumulating at a very high rate because the network traffic is flowing back and forth at a tremendous pace and you have to somehow keep track of those and at the same time keep a balance. That is a major part in designing a network management system, keep a balance among trap and polling, keep a balance about what information you will take and what information you will not take, keep a balance about how much you are going to manage.