Computer Networks
Prof: Sujoy Ghosh
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur
Lecture-25
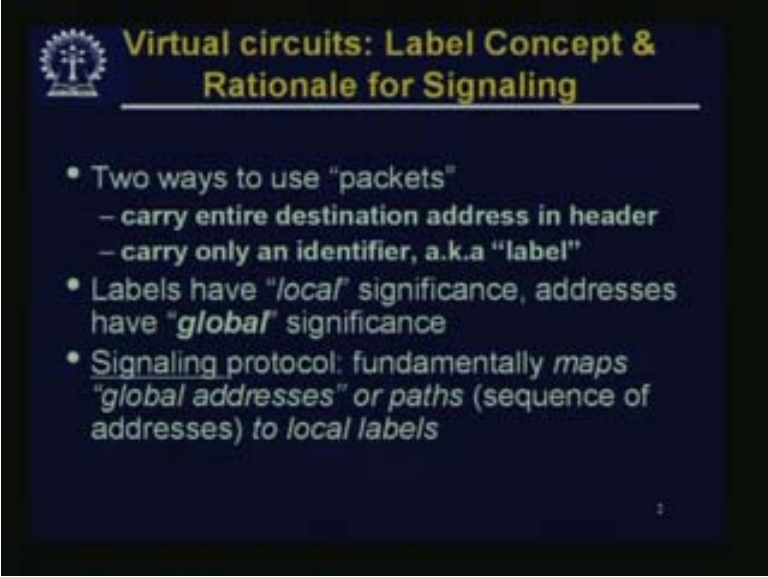**ATM Signaling, Routing and LAN Emulation**

We have looked at ATM technology in the box, in the sense that how it handles cells, how it makes cells. Today, in the first half of this lecture or first part of this lecture, we will discuss ATM signaling and routing. Since Ethernet networks and other kinds of networks are ubiquitous, everywhere, if ATM is used in a backbone, how they would interoperate between an IP network and an ATM network. We will talk about that in the second part of this lecture. So today we talk about ATM signaling, routing, and LAN emulations.

(Refer Slide Time: 01:23)

The first concept is that ATM uses virtual circuits; that means there are two ways to use packets: carry entire destination address in header, or carry only an identifier, also known as label. Labels have local significance, addresses have global significance. Signaling protocol fundamentally maps global addresses or paths or sequence of addresses to local labels. We will discuss this in much more detail when we discuss routing of IP packets, which we will take up after this lecture.

(Refer Slide Time: 01:31)

Usually when you have a packet switching network, then each packet is considered in one extreme, that is, in the IP end. Each packet is considered on its own. That means each packet must contain the destination address at the very least. It also contains the source address that is different; so it must contain the destination address, so that looking at each packet, an intermediate router would know where it should go. That is one end of the spectrum, whereas in the connection-oriented system we know that the physical connection is set up. In ATM we set virtual circuits or virtual paths. In virtual circuits or virtual paths, what happens is that these ATM cells are very small, only 53 bytes long.

Each of the cells will contain some local label; so a path is set up. Now setting up a path in ATM means that each of the intermediate switches would know that a flow of cells is going to go through them – from one source to some destination. They make provision to accommodate this flow; they make provision for the virtual circuit, and then, once they do that, they set up this virtual circuit in the starting phase. After that, each of the cells need not contain any specific identifier or specific address for the destination. It just needs a small address, which tells the intermediate switches which virtual circuit to use. It contains a virtual circuit identifier. Actually it is divided into two parts as we have seen in the cell header: we have the VPI part and the VCI part. Simply looking at that label, the intermediate switch would know which virtual circuit to use.

(Refer Slide Time: 04:44)
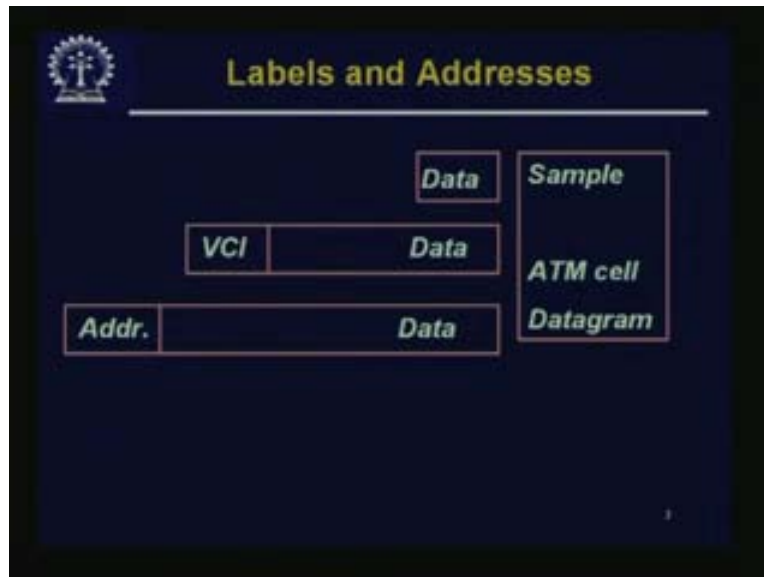
Before this virtual circuit, we see that we have the samples. Suppose we have the data in the ATM cell, the data would be preceded by simply the virtual circuit identifier and this might have two parts: VPI and VCI, whereas in a regular datagram the entire address may have to be there in each packet.

(Refer Slide Time: 05:11)
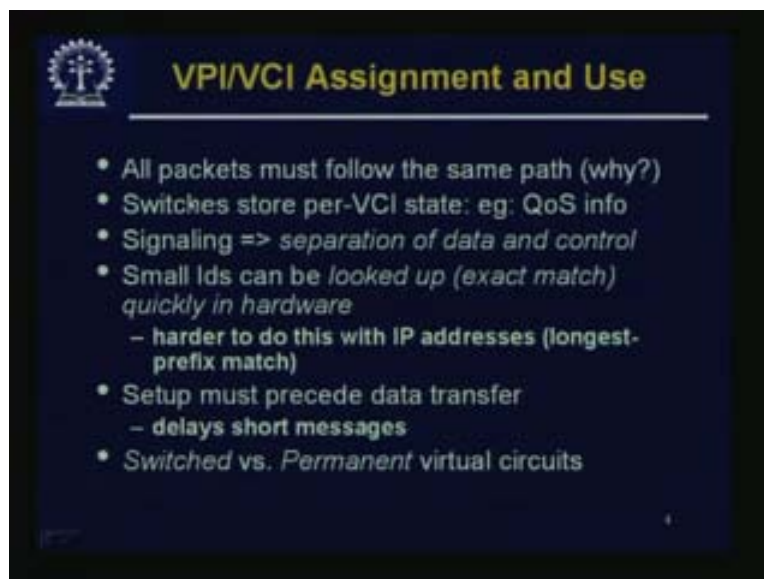
In VPI/VCI assignment used in this case, all packets must follow the same path unlike a datagram, because this virtual circuit is set up before any actual flow of packets begins. There is a time for the circuit set up and this circuit is not a physical circuit we have in a telephone network; but this is a virtual circuit, that means each of the intermediate nodes simply knows that

a flow is about to begin. So this has to be set up. Once this is set up, all packets would flow through the same path. Switches store per VCI state, e.g. QOS (quality of service) information about this particular VCI. Signaling implies separation of data and control. When we do ATM signaling, we are talking about setting up the entire path. We will come to that; small ids can be looked up exactly much quickly in hardware – that is one good thing. If you have a small VCI, which means, virtual circuit identifier, it can be looked up very quickly in a hardware – this is a bottle neck in a router. This can be handled very fast; it is harder to do this with IP address. That means this longest prefix match – we will come to that later on. The setup must precede data transfer. This is the other disadvantage of this – the VPI and VCI must be set up, which means it delays short messages. There are two types of virtual circuits: switched and permanent virtual circuits.

(Refer Slide Time: 06:58)
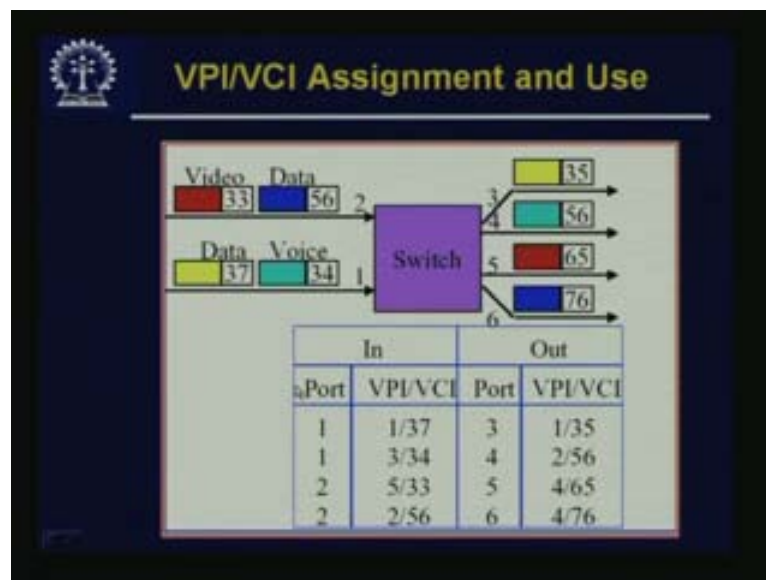
This is an example, the switch knows in the input ports say 1 and 2, 1/37. If these are the VPI or VCI identifiers, out will be through port 3, 1/35. Similarly port 1 for 34 will go to 4, 2/56 and so on. There is a table which simply quickly matches the VPI/VCI values and puts it on another VCI/VPI pair on the other side. This is how VPI/VCIs are assigned and used.

(Refer Slide Time: 07:44)
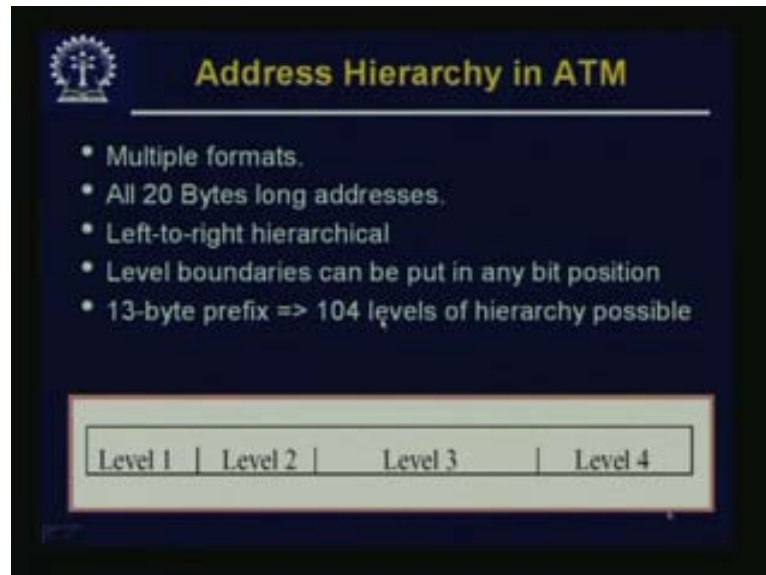
We now come to ATM addresses. This address is different from the VPI/VCI; that is, the virtual circuit identifier/virtual path identifier, which is simply local. But for setting up the path, initially you require an address, and you cannot do with a local address. You have to do with a globally consistent address. This global address of ATM is 20 bytes long. There is a 20-byte long ATM address, which you use for setting up a circuit. I mentioned previously that there are two types of circuits: switched virtual circuits and permanent virtual circuits. In permanent virtual circuits, a path is set up initially manually. The path remains a permanent virtual circuit.

Whenever there are two end points between which a lot of traffic will flow, you may skip this overhead of path set up and set up a permanent virtual circuit; this is like a leased line. Whenever there is something to go from this source to that destination, it will simply use the pre-existing permanent virtual circuit or otherwise, we may have a switched virtual circuit. That means this virtual circuit is set up on the fly, as the network is being used. In an ATM switch, hundreds of thousands or may be millions of virtual circuits may be set up or taken down every second. This is a very fast process. For setting up this virtual circuit, we require an ATM format and this is 20-byte long address. Unlike an IP address, which is only 4 bytes, this is 20 bytes. This is a very long address, left to right hierarchical. in this, there are level 1, level 2 level 3 and level 4. The first two levels have a 13-byte prefix, this are the levels of hierarchy. This part is usually used for the actual network addressing inside. Since it is such a long address, it can accommodate various schemes. ATM was conceived as a technology, which will subsume and absorb all pre-existing technologies.

(Refer Slide Time: 10:17)
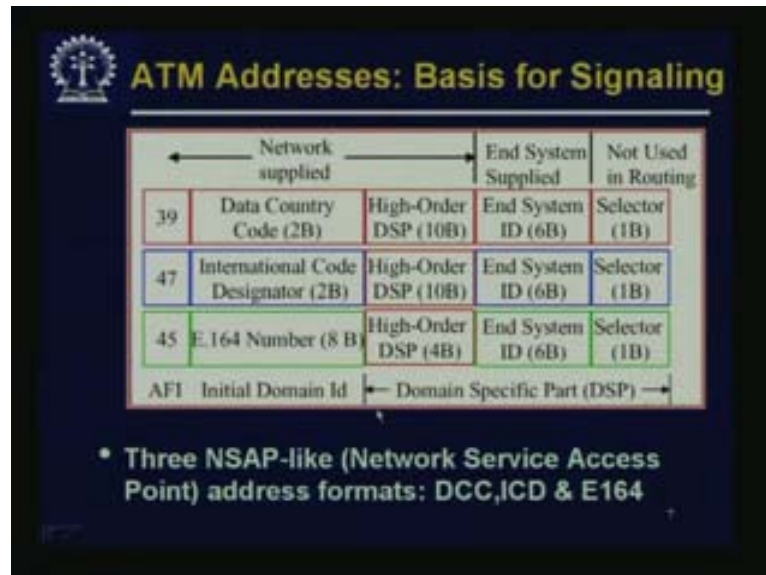
The people who designed ATM tried to accommodate different kinds of addressing schemes in one super addressing scheme, which they say is ATM addressing scheme. As you see here, there are different types of addresses possible. Since there are 20 bytes, it is possible to have more number of schemes. These are the schemes 1 byte + 2 byte 3 plus 10, 13 – this is supplied by the network. These 6 bytes are end-system supplied and not used in routing. This may be used inside the host; 1 byte for maybe de-multiplexing inside. These network supplied parts are 1 byte, which indicates the scheme. The three NSAP (network service access point address) formats are DCC, ICD, and E.164 or ICD number or DCC number. This is a data country code, which uses 2 bytes and 10 are used for the other part of the network.

(Refer Slide Time: 11:57)
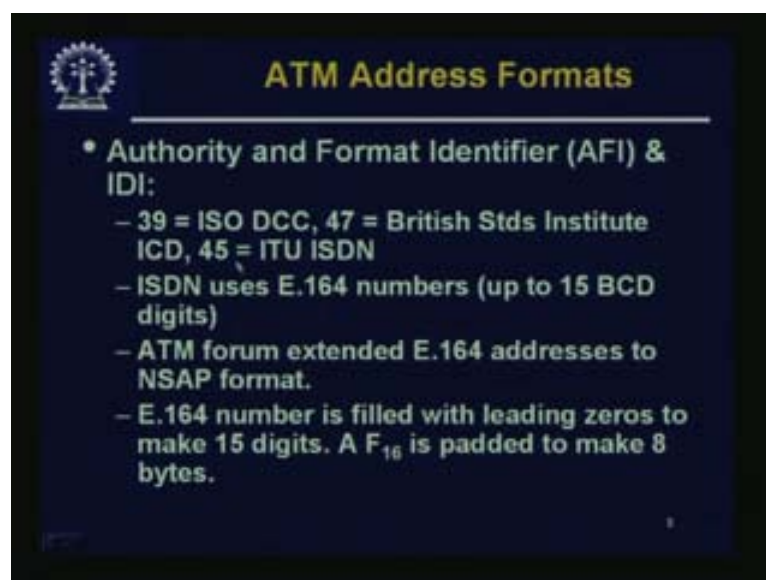
Actually here, authority and format identifier is the first thing. So 39 is ISO DCC; 47 is British Standards Institute ICD; and 45 is ITU ISDN, which means that this E.164 is actually an ISDN number. ISDN uses 15 characters, i.e. 15 binary coded decimals, that is, 7½ bytes. This entire ISDN number, which again can subsume telephone numbers, can be put over here. ISDN uses E.164 numbers. ATM forum extended E.164 addresses to NSAP format and E.164 number is filled with leading 0s to make 15 digits, that is, AF_{16} is padded to make 8 bytes instead of 7½ bytes. End system identifier is the other part. This is the end system identifier part, and these 6 bytes could be various things, specifically this 6 byte could be 48-bit IEEE MAC address.
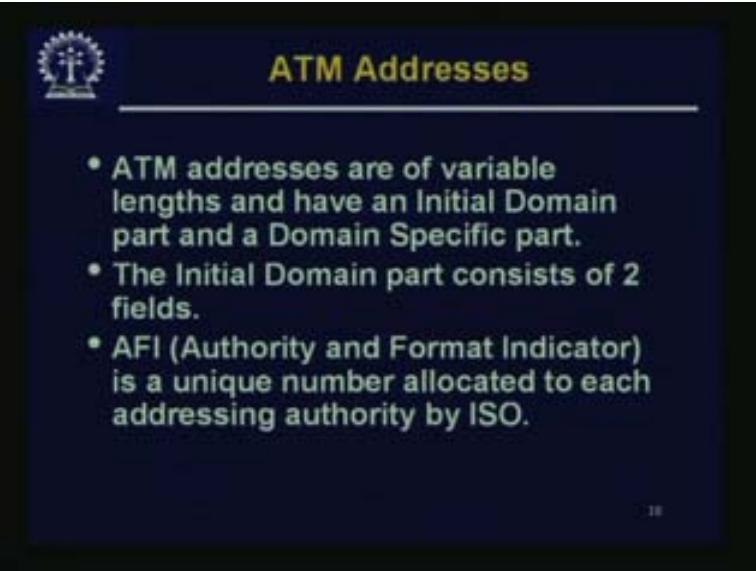
(Refer Slide Time: 13:08)
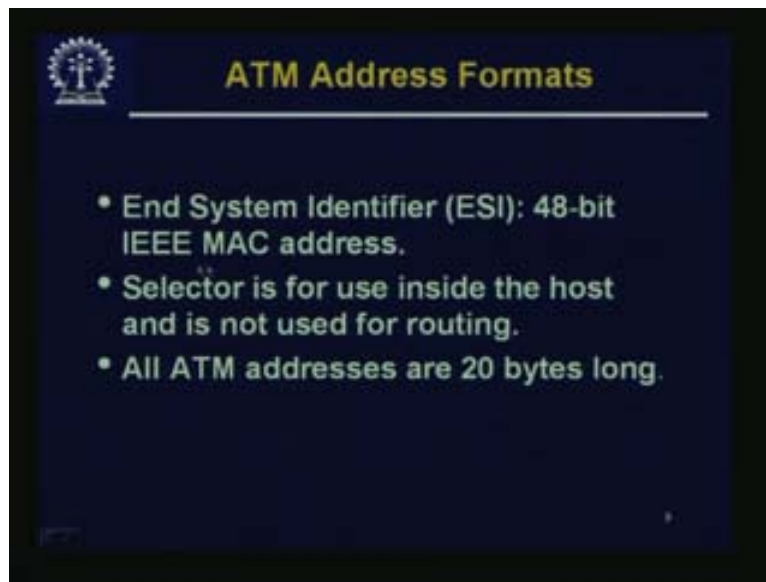
Remember the MAC address that we used in the data link layer is 6 bytes, supplied by IEEE. The entire 6 bytes can straightaway be incorporated in the low order bits of the address. Selector is for use inside the host; all ATM addresses are thus 20 bytes long. There are various ways you can route this ATM; given an ATM address there are various schemes possible.
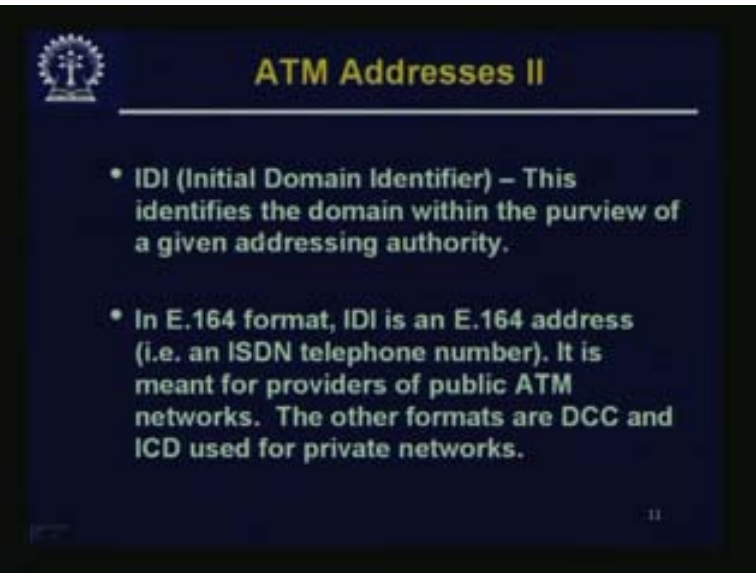
(Refer Slide Time: 13:43)

Since various schemes are possible, ATM addresses could be of variable lengths and have an initial domain part and a domain specific part. The initial domain part consists of two fields as we have already mentioned: AFI, that is, the authority and format indicator, and IDI, that is, initial domain identifier. This identifies the domain within the purview of a given addressing authority.
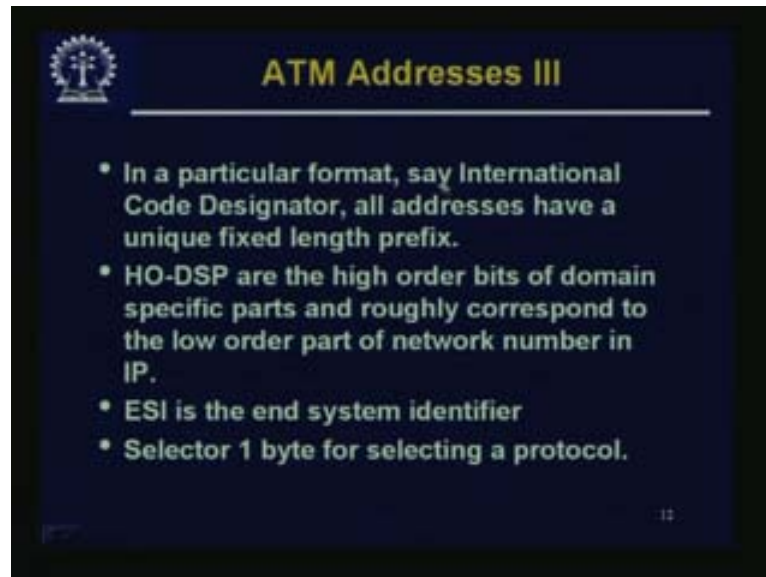
(Refer Slide Time: 14:04)

(Refer Slide Time: 14:16)

ATM Addresses III

- In a particular format, say International Code Designator, all addresses have a unique fixed length prefix.
- HO-DSP are the high order bits of domain specific parts and roughly correspond to the low order part of network number in IP.
- ESI is the end system identifier
- Selector 1 byte for selecting a protocol.

In a particular format, say ICD (international code designator), all addresses have a unique fixed length prefix. The high order DSP or the high order bits of domain specific parts roughly correspond to the low order part of network number in IP; ESI is the second. This particular scheme can subsume a lot of other schemes, which were possible. The reason for showing this in this fashion is that a similar thing was tried later on in IP version 6. We have a very large address field where a lot of previous schemes could be subsumed in this. One of the difficulties with this IP addressing scheme was that it was done in a very haphazard manner, unlike the telephone number.

For example, the telephone numbers are geographically distributed. That means, you put particular first few digits and that will immediately indicate which country and region you are calling. It is easy for the router to just look at the first few digits and send it to the trunk. But that is not possible in the IP version 4 which is used, because it has no geographic correlation. You have to take keep a very long table and look into the table. Once again when people developed this ATM addresses or the IP version 6, they tried to bring back some order into this addressing scheme.

(Refer Slide Time: 16:19)
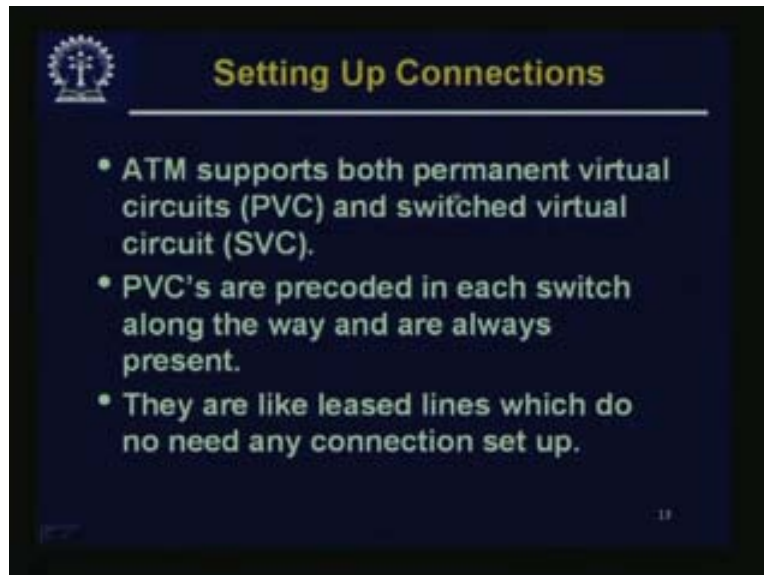
For setting up connections: IP ATM supports both permanent virtual circuits and switched virtual circuits. PVCs are pre-coded in each switch along the way and are always present. They are like leased lines, which do not need any connection setup.

(Refer Slide Time: 16:37)
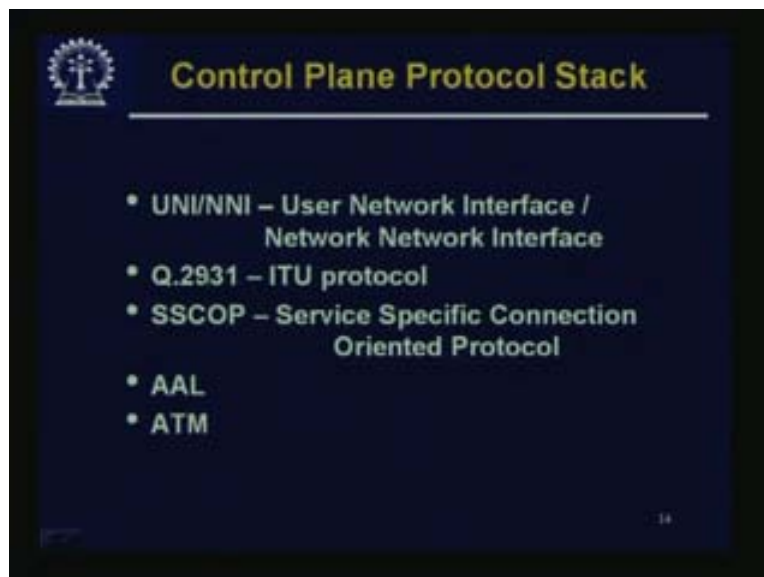
For connection setup there is a user network interface or UNI, and the network interface, which is the NNI. There is a part called Q.2931, which is an ITU protocol for setting up paths and this SSCOP means service specific connection oriented protocol. You have the AAL and ATM. These layers have already been talked about earlier.

(Refer Slide Time: 17:07)
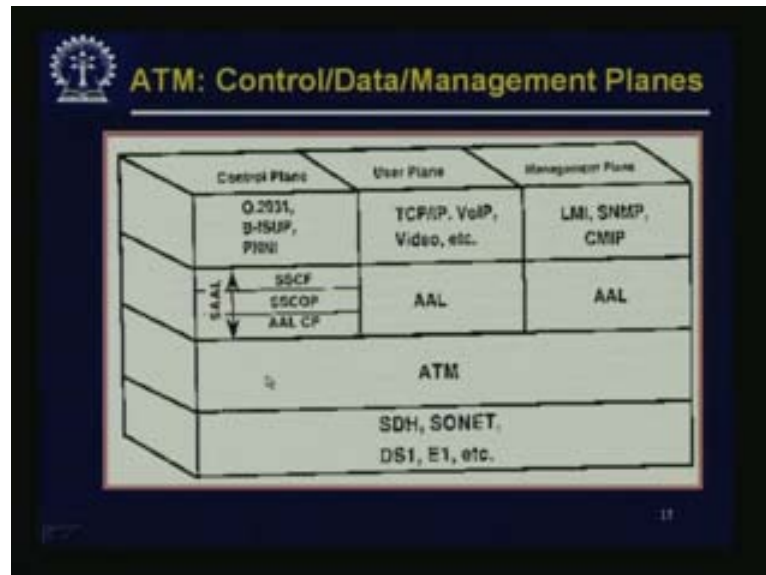
Unfortunately this whole scheme turned out to be quite a complex one. We will not go into all the details. We have already seen the ATM layer and the AAL layer, which is in the user plane. Today we are going to talk a little bit on this control plane, which has one service AAL and three parts: SSCF, SSCOP and AALCP or AAL common part. For setting up the circuits, etc., we have Q.2931, BISUP and PNNI or public network-to-network interface.

(Refer Slide Time: 17:50)
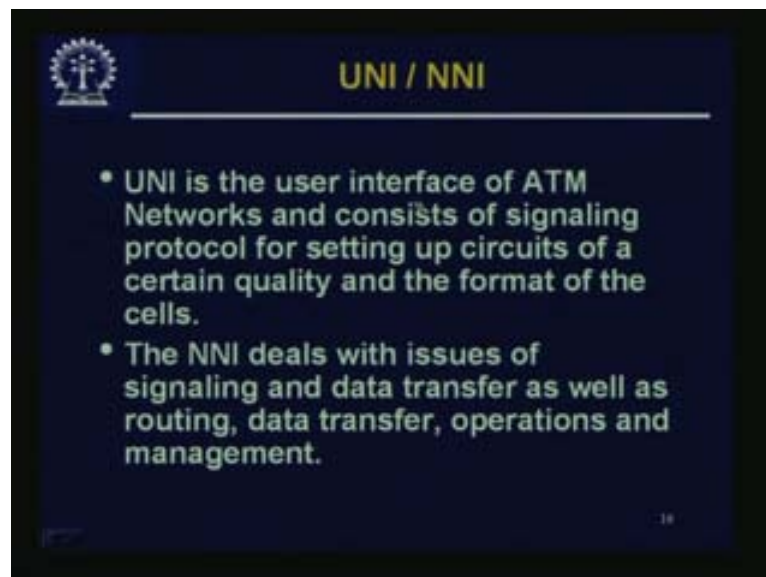
UNI is the user interface of the ATM networks and consists of signaling protocol for setting up circuits of a certain quality and the format of the cells. The NNI deals with the issue of signaling and data transfer as well as routing, data transfer, operations and management.

Remember there is also a slight difference between the cells which go through in the UNI part and this NNI part. In the NNI part, the GFC is dropped and we use the whole thing to accommodate more number of virtual circuits; but that is a small technical point.

(Refer Slide Time: 18:31)
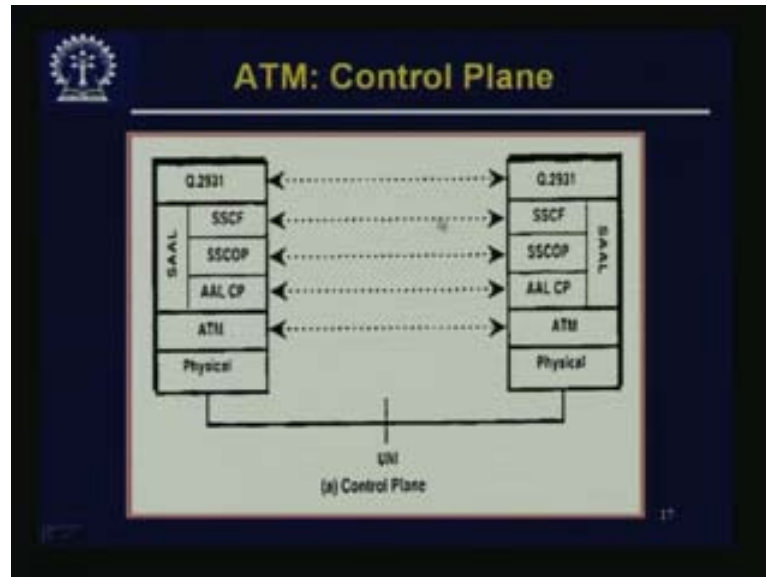
If you look at the control stack, that is, control plane stack, we have this Q.2931 sitting on this SSCF, this SAAL, that is, service ATM adaptation layer, which sits on the ATM layer, which again is on some physical layer, there is a virtual link between two ATMs, AALCPs and so on between a stack from the source to the destination or from one hop to the other.
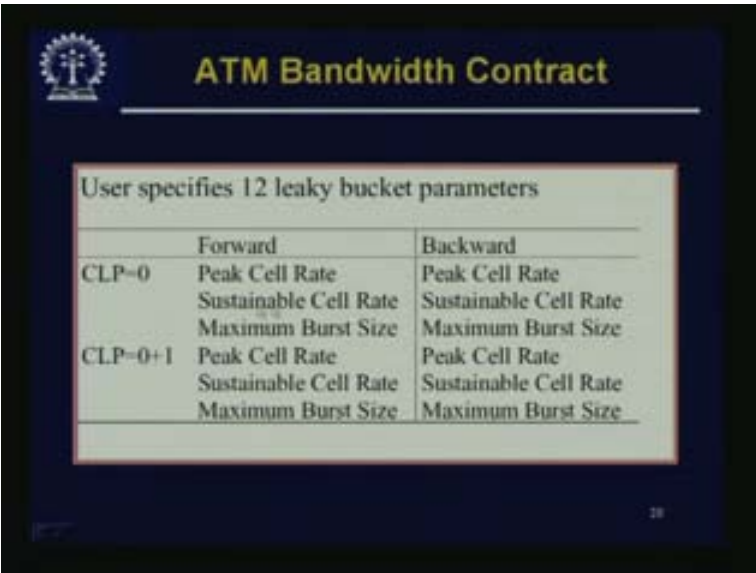
(Refer Slide Time: 19:02)

Let us see what Q.2931 is. We will not go into this, once again the protocol is quite complex. We will just touch upon some aspects of it. This is an ITU protocol for setting up a connection. First it sends a request in the Meta signaling channel 0 to negotiate a quality of service for a signaling channel. What is done is that, for setting up the circuit, you have to do some communication. This communication again will be through ATM. Actually for that, it will require some kind of virtual path and virtual circuit. ATM is quite strong on quality of service. There is a question of quality of service of the service channel also. Although the service channel would be used for a very short time, once the circuit is set up, that service channel may be released. There is a Meta signaling channel called 0, where you can negotiate the quality of service for the weak signal channel with the quality of service. Otherwise, there is a default which is VP0, VC5, which means, virtual path number 0. In virtual path number 0, which is a bundle of circuits, take the VC 5, which is a standard channel, where you put your request for signal, for setting up the path. Now if this is successful, then a new VC is assigned for connection setup requests and replies. Then you first make the request in this channel then a new VC would be assigned for this particular connection setup. Q.2931, if you remember, is at the top of the control plane protocol stack, which initiates at the setting up of the circuit and handles setting up of circuits.

(Refer Slide Time: 21:15)
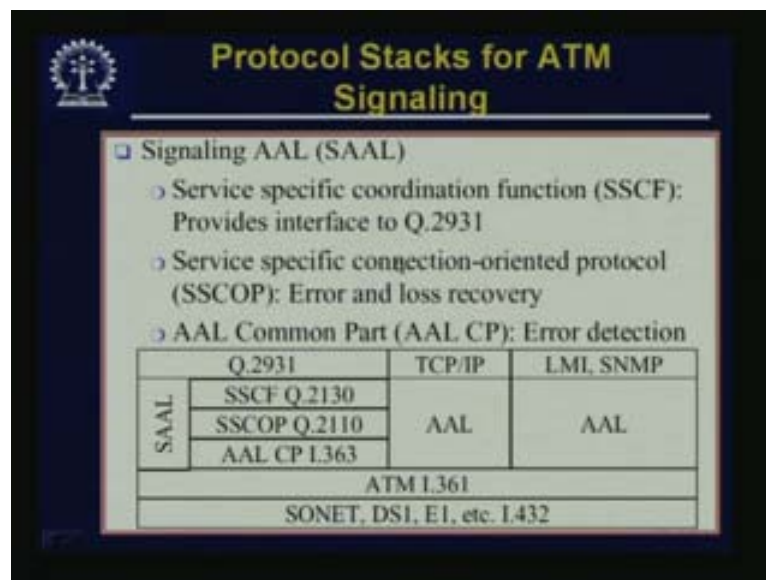
Below the Q.2931 we have the signaling AAL; that means, signaling ATM adaptation layer, which again contains three parts: service specific coordination function, which provides interface Q.2931; interface between Q.2931 and the ATM stack; service specific connection-oriented protocol, which is the SSCOP – this handles error, loss and recovery. All these are communications for setting up circuit for communication for the control purpose and the AAL common part, which handles error detection. This is roughly the stack.

(Refer Slide Time: 22:00)

There are various kinds of parameters in the forward direction and in the backward direction. There are various parameters that you can specify for the quality of service. With ATM, when it was introduced, a serious attempt to handle the issue of quality of service was made. It has now become so important that in the IP domain also, which is turning out to be the dominant technology, quality of service has become important. People have thought of various schemes for handling quality of service. Many of the schemes that people had already thought about with ATM have been adopted in various ways. We will talk in detail about quality of service later on.

Today, we will just touch upon it; there are various parameters like peak cell rate – that means the peak rate at which you will be pumping inside; sustainable cell rate; maximum burst size; etc. All these different parameters can be negotiated for one particular virtual circuit. When a path is set up along the way, each of the ATM switches on the way makes some provision for supporting that particular new virtual circuit with that kind of service. If it cannot handle that, may be some negotiation about it can be handled. Leaky bucket is some kind of congestion control algorithm. We will discuss it later.
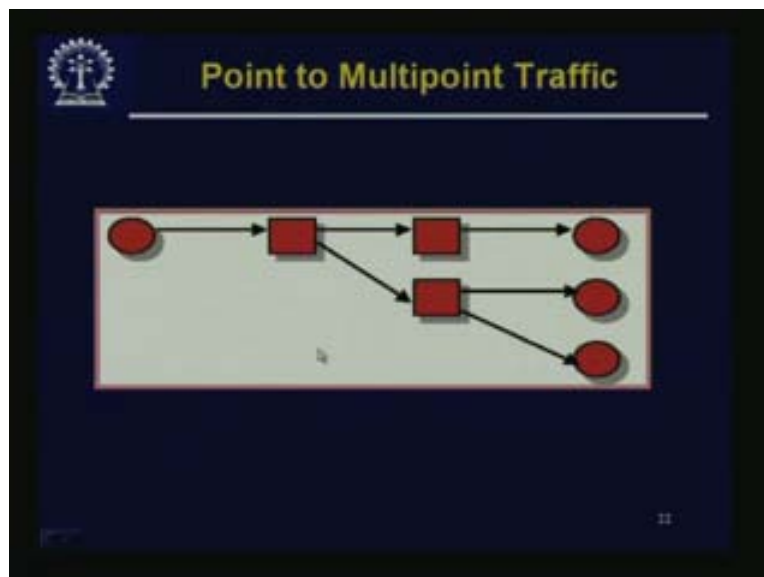
(Refer Slide Time: 24:00)
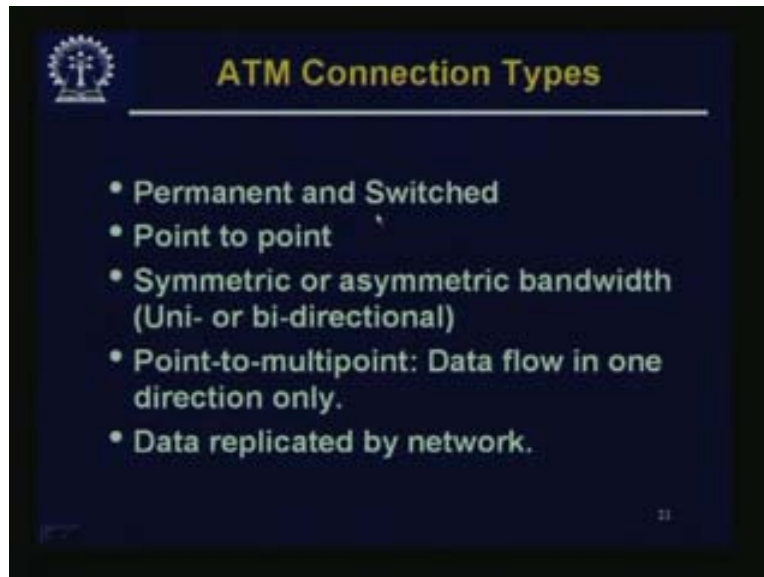
ATM connection types are of various types; the most pre-dominant ones are the switched virtual circuits, where you set up a path and take it down; or permanent virtual circuit, which is pre-coded. There are other connection types, e.g. simple point-to-point connection, symmetric or asymmetric bandwidth connection, point-to-multipoint connection, data flow in one direction only, or data is replicated by the network. So this is an example of a point-to-multipoint network.

(Refer Slide Time: 24:30)
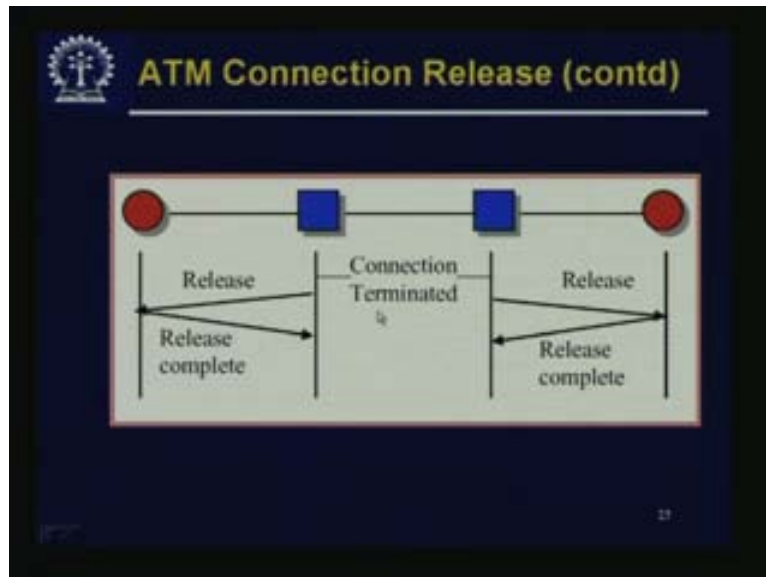
(Refer Slide Time: 24:36)
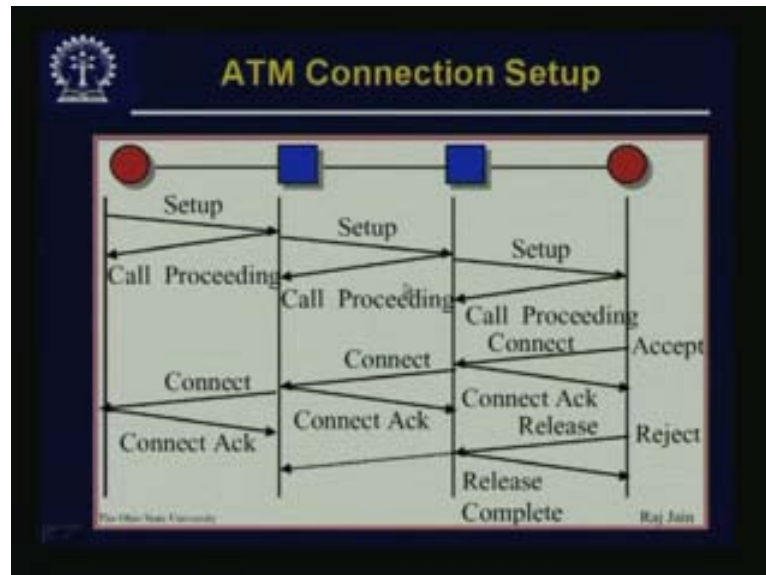
When you do an ATM connection setup, you set up signal and maybe this is the source and this is the destination. These are the intermediate switches. From the source, there is a set up signal, which goes through the intermediate switch, which sends back an acknowledgement saying that the call is proceeding and sends a set up signal to the next hop. The set up signal is then sent to the next hop and each of them immediately will send back an acknowledgement. When the call is accepted, a connect signal will start flowing in the other direction and when it reaches the source, a connect acknowledgement will flow and each of them will give this connect acknowledgement for this connect signal. The circuit has now been set up. Or alternatively, the destination may reject it; then it simply sends a region release kind of a signal.

(Refer Slide Time: 25:46)
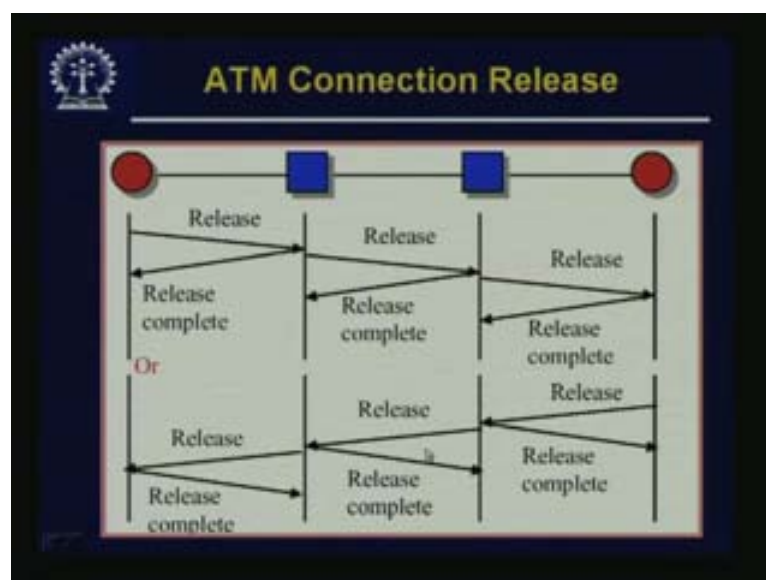
For circuit setting up and for taking down a circuit, the source will send a release; that means he has finished sending release and release complete will go on. Then finally the destination will send a release all the way back. A release could be initiated by the sender or the release could be initiated by the destination also. The connection gets terminated and release is completed.

(Refer Slide Time: 26:24)

(Refer Slide Time: 26:29)
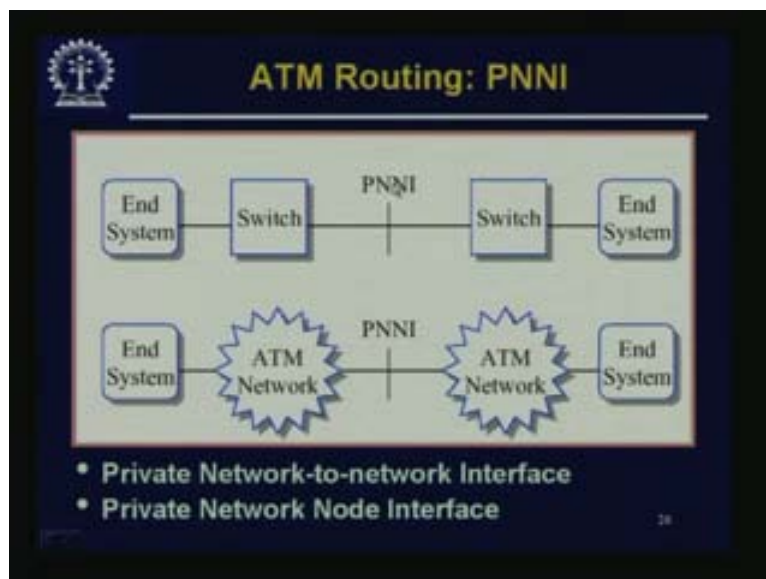
PNNI is the private network-to-network interface; that means between the end system and the switch, we have the UNI and we have the NNI. PNNI is a private network-to-network interface and this could be between two switches or two entire networks. PNNI uses link state routing protocol for ATM networks. We will look into the details of link state routing when we deal with

OSPF in the IP worlds.Since IP is the more prevalent technology, we will discuss it in detail when we do it here. Each node will periodically broadcast the state of the link to which it is connected to all parts of the network. This way all the switches get some global picture about the status of the various links, so that they can run some algorithm locally in a centralized fashion and find out all the possible paths. They use this for setting up the path later on.

(Refer Slide Time: 28:15)
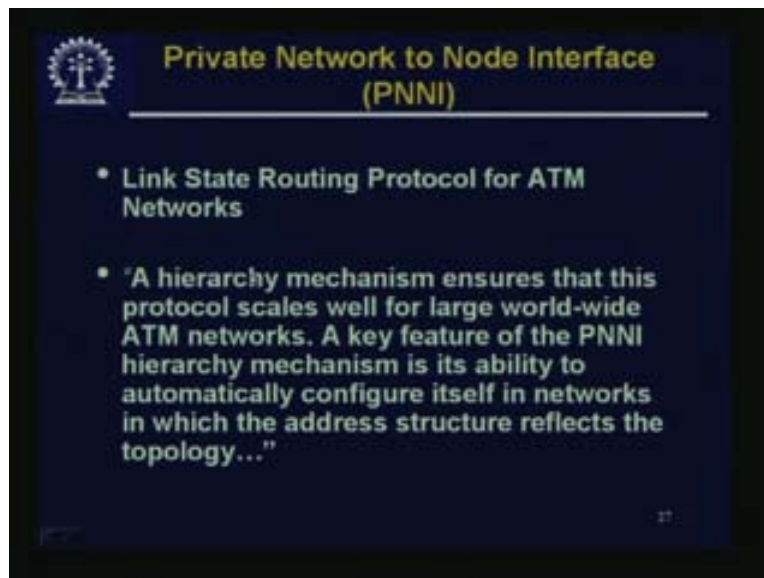
Actually the situation is a little more complex than what I have just said, because there is a hierarchy mechanism that ensures that this protocol scales well for large, worldwide ATM networks. A key feature of the PNNI hierarchy mechanism is its ability to automatically configure itself in networks in which the address structure reflects the topology. There are two things here: one is this hierarchy we are talking about, and the same kind of thing is used in OSPF in the IP domain. When we discuss OSPF, we will go into the details of this; but there is a hierarchy over there. Imagine what would happen if all were ATM switches, which they are not, but suppose they all were.

That was the vision; and if the ATM switches were communicating with everybody else with their link states, the database and everything would become huge. In order to scale to a very large network, it goes through in a hierarchical fashion, meaning you can have a hierarchy of networks and at each hierarchy, the peers run some kind of PNNI for routing within that level of hierarchy. And at a lower level, they will again run PNNI for that level and various hierarchy levels are possible. You have seen that the ATM address is given in such a way that we have only shown the broad boundaries but within those boundaries, it can be further divided into a number of hierarchies and again different designated authorities can break it up in a different way. All these flexibilities are possible; PNNI allows that in some plane, in some hierarchy, one kind of addressing scheme is used and in another, a different kind of addressing scheme is used.
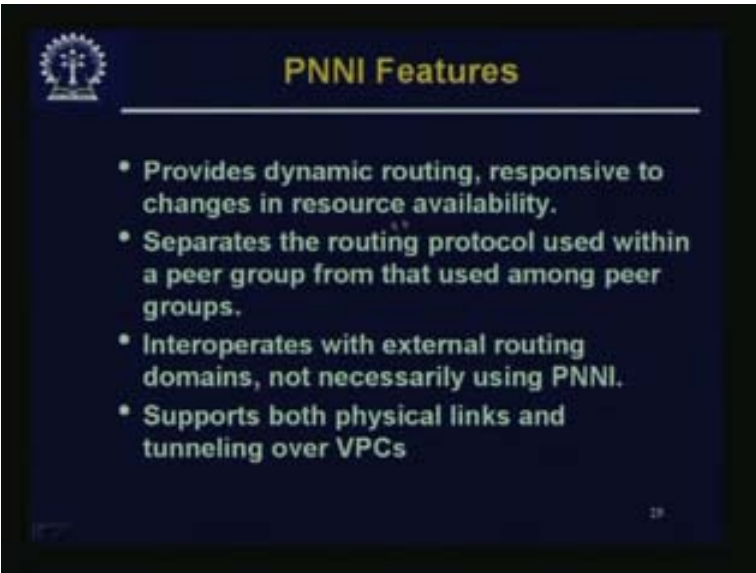
(Refer Slide Time: 30:18)
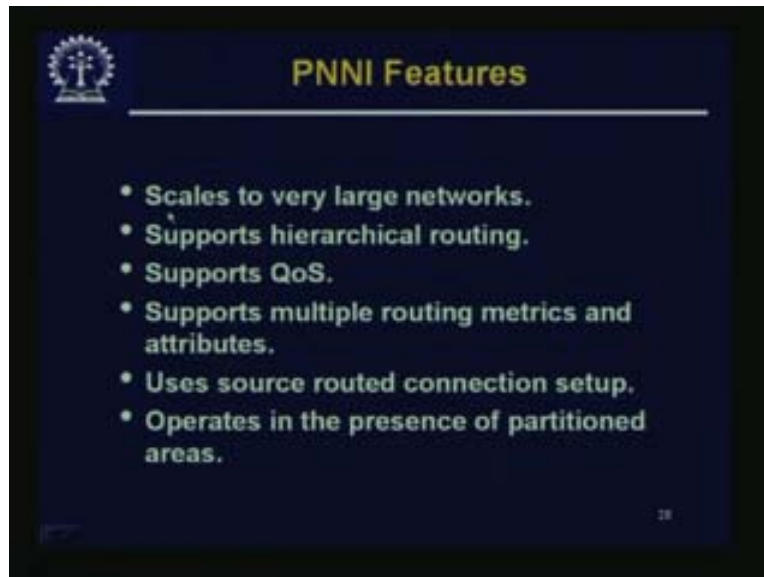
The substance is that it scales to very large networks, supports hierarchical routing, supports quality of service, supports multiple routing metrics and attributes, because when you broadcast the link state, i.e., the state of the link, you may also broadcast all different kinds of parameters about the links that can be handled in that link or how much can be handled by the switches, etc. can be propagated throughout the network. If you have a fair idea about what is possible and what is not possible, then you can plan your route in the source in a particular fashion. Use of source routed connection setup: since the source has the global picture, it will use that global picture to compute the route and set up the connection. Once it decides on the route, it used the Q.2931 to give all the connection setup. That set up request, acknowledgement and release etc. will be used. It operates in the presence of partitioned areas.

PNNI features provide dynamic routing; that means, the link states may change from time to time. Each of the switches are going to broadcast their link states; it is responsive to changes in resource availability; separates the routing protocol used within a peer group from that used among peer groups. Various hierarchies are possible: interoperates with external routing domains, which are not necessarily using PNNI and supports both physical links and tunneling over virtual circuits.
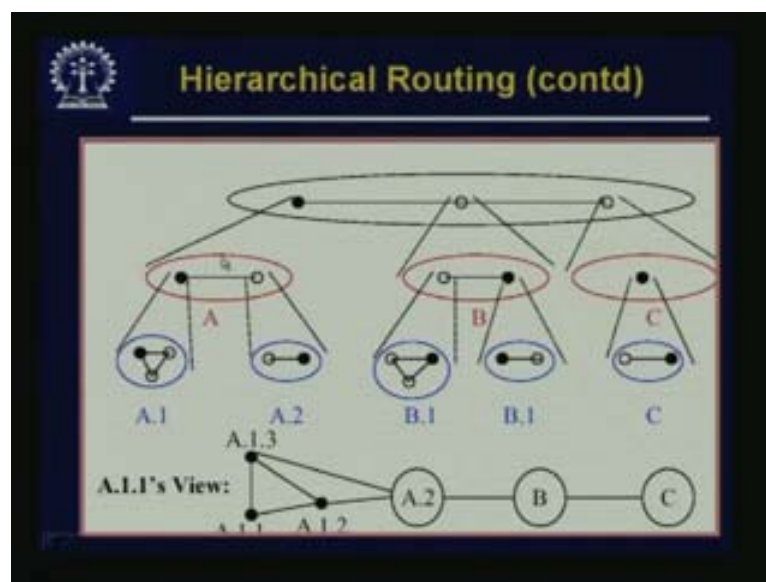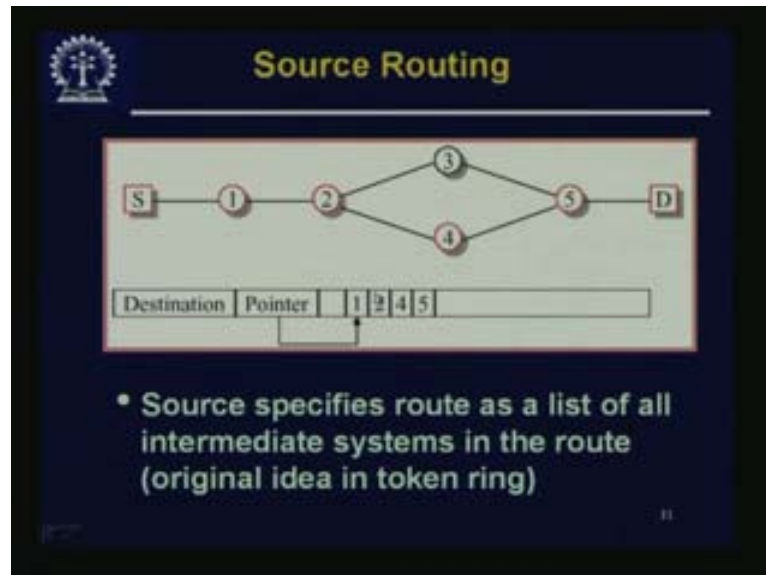
(Refer Slide Time: 31:37)

(Refer Slide Time: 32:17)

This is an example of hierarchy. This big network, which is again a network of networks, is represented by one node in the top level of the hierarchy. Similarly, you use PNNI to plan a route like this. Within the network you might have to again do a planning and each node may again be corresponding to another network at a lower level. At each higher level of the hierarchy, you can use PNNI to plan the route if there is A.1.1. Its view of A.1.1 is something below A.1.1, A.1.2, A.1.3 are explicit. These have abstracted notions of A.1.2 and then you come to B; these are B and C. Although when the call setup is passing through B, it may come all the way down and do the actual path setup. That is how the hierarchy works.

(Refer Slide Time: 33:45)

At any level of the hierarchy, A.1.1 will make a source route, which goes through A.1.2, then B and C. So the source specifies the route as a list of all intermediate systems in the route. This was the original idea also in the token ring.
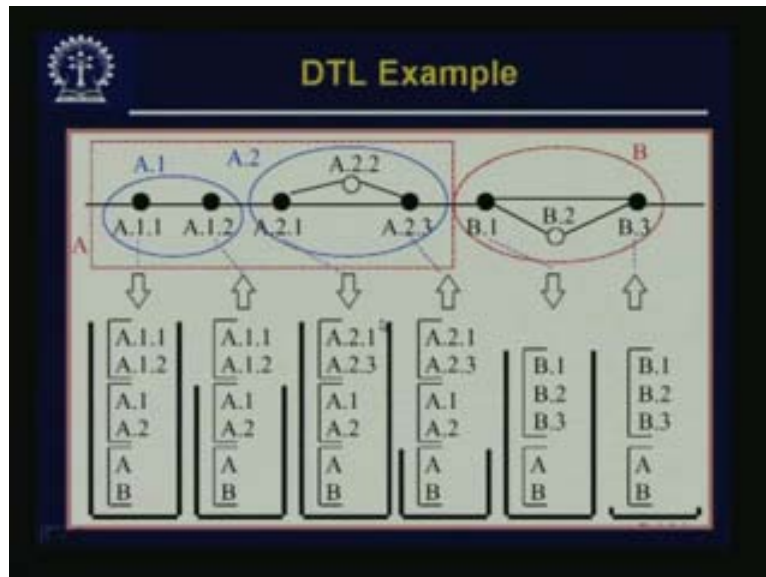
(Refer Slide Time: 34:11)

For this, it uses a designated transit list (DTL), which is in the form of a stack, as I will show you. Source route is across each level of hierarchy; there is an entry switch for each peer group; it specifies complete route through that group; and set of DTL manipulations is implemented as a stack.

(Refer Slide Time: 34:32)

A and B may be at the bottom of the stack; A.1 is at the top level of the hierarchy and this is how it is put in a stack and the path is completed.

(Refer Slide Time: 34:46)
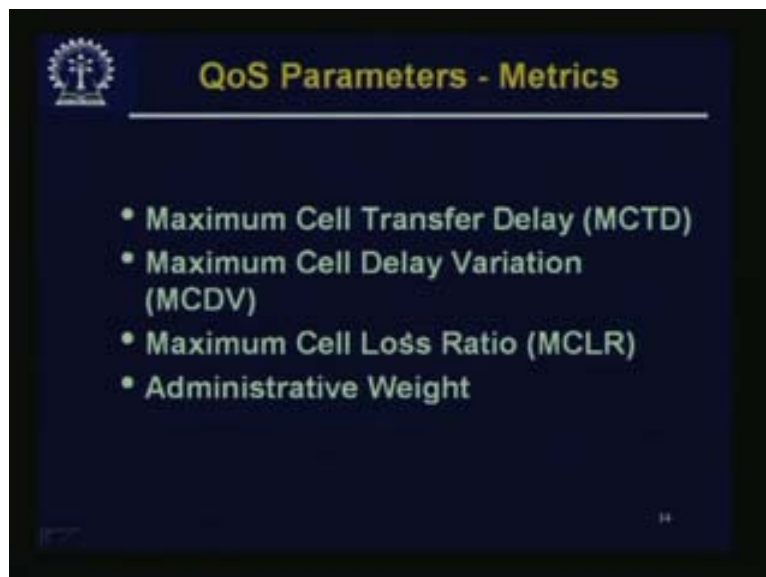
We now discuss the quality of service parameters. I will just mention some of the metrics, etc. We will not go again very deep into this because we do not have that much time. But it will give you some idea about what we mean when we say quality of service.

One such parameter metric is maximum cell transfer delay; that means, the delay from the beginning of the first bit of the first cell to the last bit of the cell. Others include maximum cell delay variation; the variation of this time; maximum cell loss ratio; whether the cells could be lost, and if so, what is the maximum cell loss ratio; administrative weight, etc.

(Refer Slide Time: 35:33)
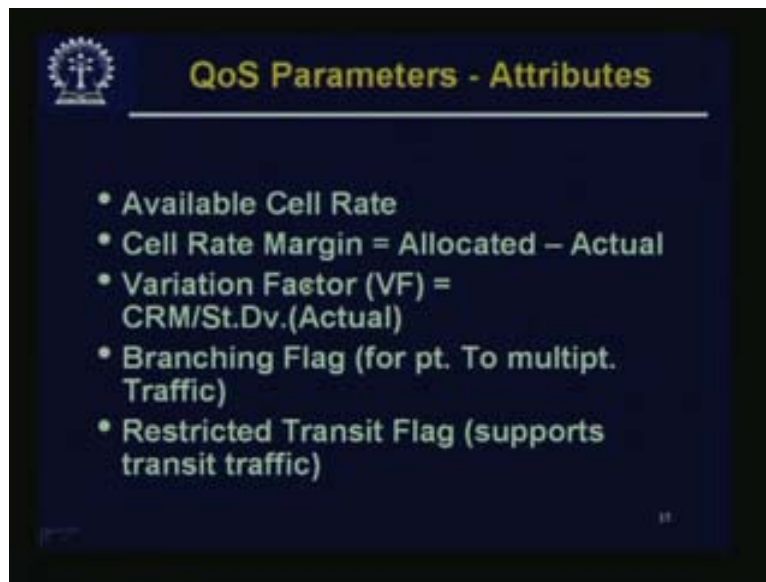
The attributes of the parameters are available cell rate or its capacity, whether it is available; cell rate margin is allocated minus actual; variation factor; branching flag; restricted transit flag. These are all different parameters and their attributes – QOS parameters and their attributes. One way this is handled is the generic call admission control, which happens when you are on the source side, i.e., when you are deciding on the route and you are doing a source routing, at that point whether you can admit a request, which has finally come from the user, from the UNI, etc.

(Refer Slide Time: 35:56)
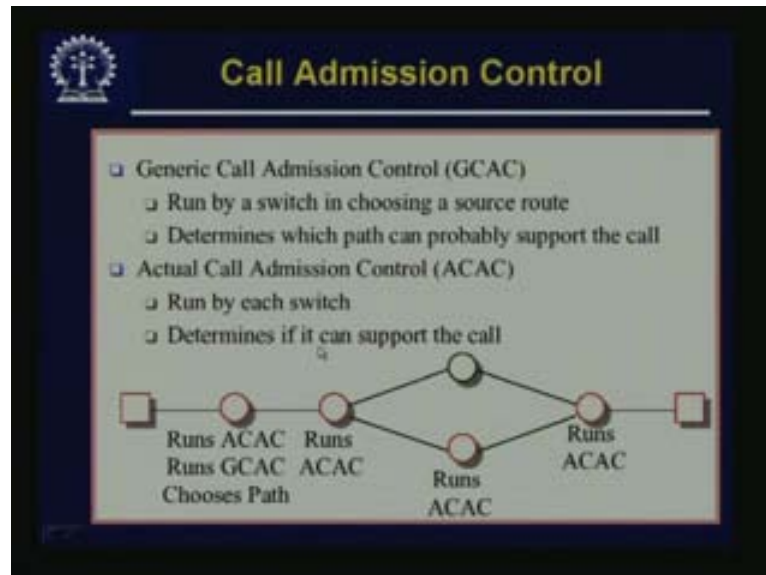
But at that particular point of time before making the request, there is an admission control, which is a generic cell admission control run by a switch for choosing a source route. It determines which path can probably support the call; that way it will try to route the call setup. Actual call admission control is run by each switch. In the beginning we will run a GCAC as well as ACAC and the intermediate switch simply runs an ACAC or the actual call admission control to check whether that request has come to this switch, whether it can handle this request or not; this is the protocol which is running.
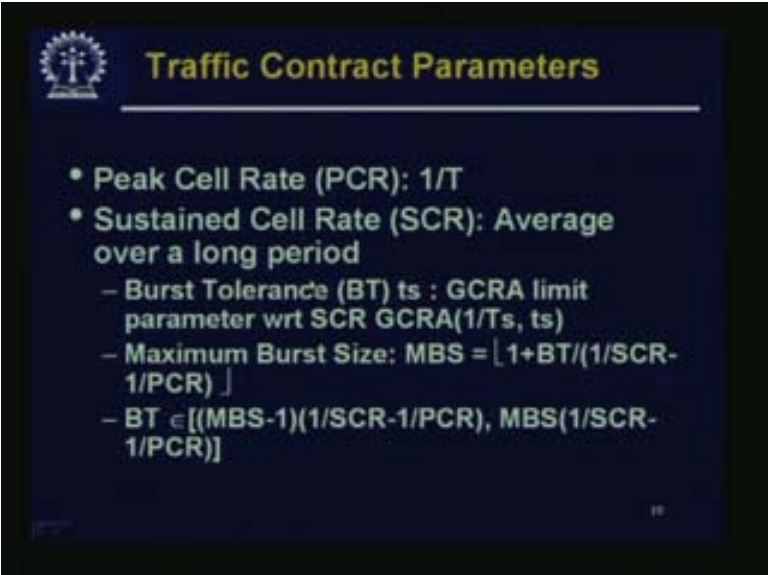
(Refer Slide Time: 37:28)
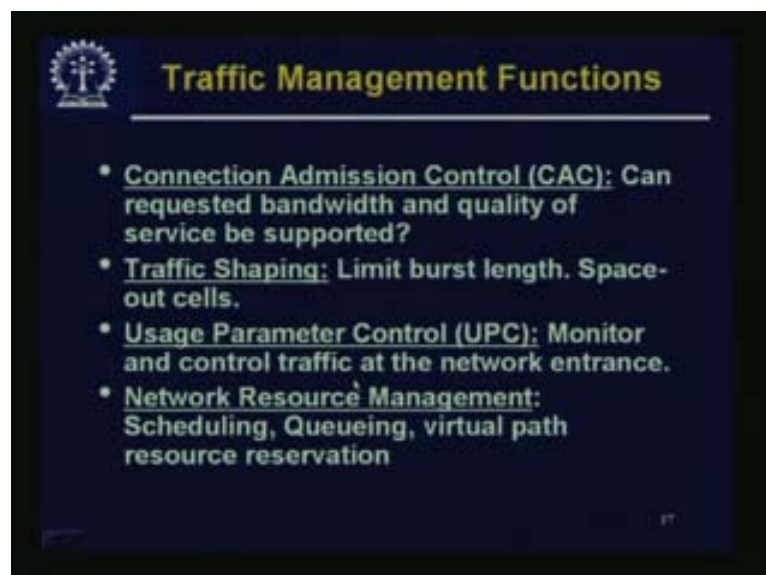
There are traffic management functions; the call admission control is a kind of traffic management. Traffic shaping means limit burst length, space out cells, etc. for getting a maximum throughput; usage parameter control is to monitor and control traffic at the network entrance of various traffic management systems. Both quality of service management and traffic management are possible in ATM, and there are extensive protocols for negotiating these various parameters and for setting it up.

(Refer Slide Time: 38:07)
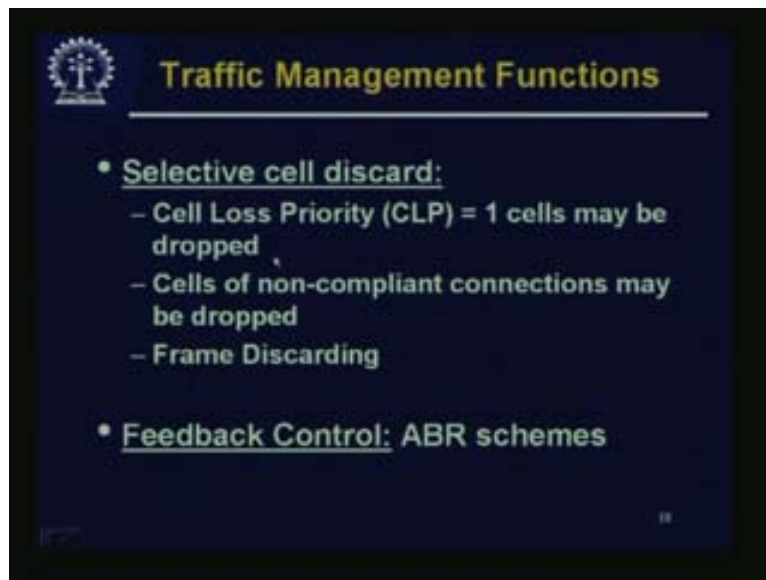
The functions of traffic management are as follows: there is selective cell discard with CLP or cell loss priority. If CLP is 1, the cells may be dropped if the situation warrants. It is something like an unspecified bit rate and it may have a very low priority. Cells from non-compliant connections may be dropped. There is also framing discarding. One example of feedback control is an ABR scheme.
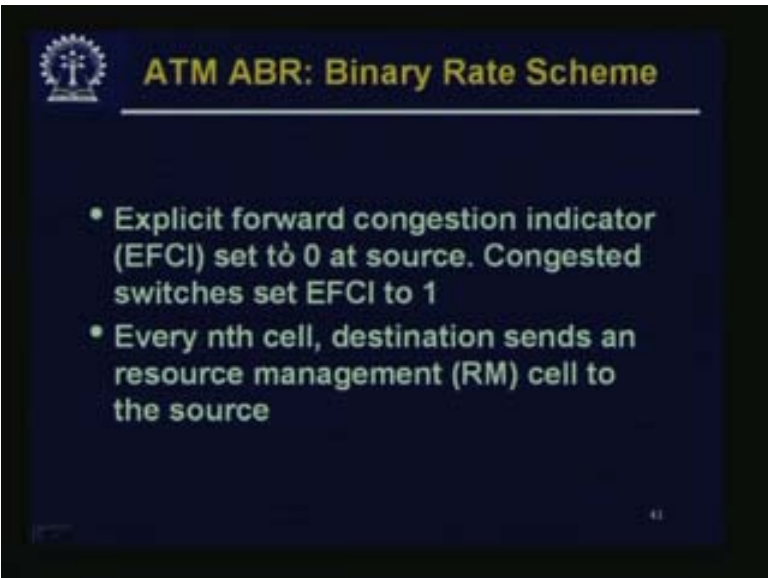
(Refer Slide Time: 38:40)

Traffic Contract Parameters

- Peak Cell Rate (PCR): 1/T
- Sustained Cell Rate (SCR): Average over a long period
  - Burst Tolerance (BT) ts : GCRA limit parameter wrt SCR GCRA(1/Ts, ts)
  - Maximum Burst Size: MBS = $\lfloor 1+BT/(1/SCR-1/PCR) \rfloor$
  - BT $\in$ [(MBS-1)(1/SCR-1/PCR), MBS(1/SCR-1/PCR)]

We will just quickly look at the peak cell rate. I am not going into the details of these: cell transfer delay, cell delay variation, cell delay variation tolerance, cell loss ratio, etc. are the parameters.
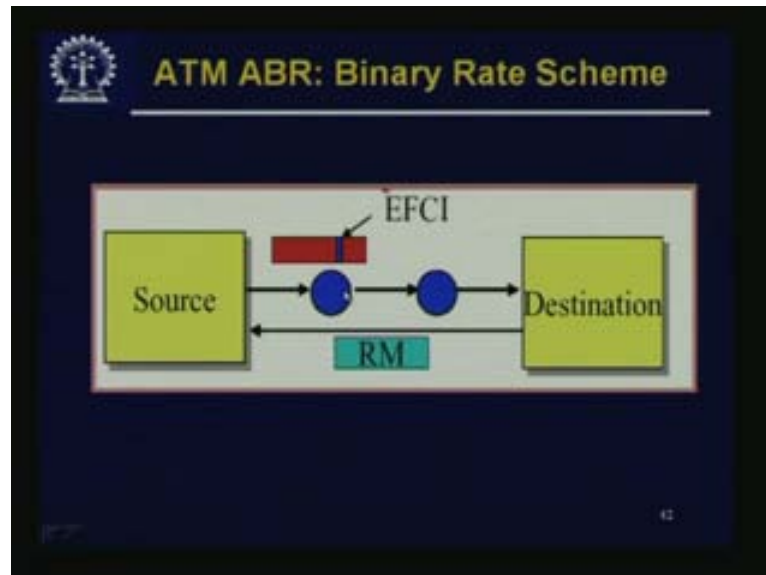
(Refer Slide Time: 38:47)

ATM ABR: Binary Rate Scheme

- Explicit forward congestion indicator (EFCI) set to 0 at source. Congested switches set EFCI to 1
- Every nth cell, destination sends an resource management (RM) cell to the source

Explicit forward congestion indicator: we will just have a quick look at this ABR system, which is a binary rate system, which sends an EFCI. This is explicit forward congestion indicator, which is set to 0 at source and congested switch is set to 1. Every nth cell destination sends a resource management cell to the source.

(Refer Slide Time: 39:22)

What happens is that somewhere in-between if an intermediate source, or EFCI, is congested, this may set it to 1 and then that information may flow back finally to the source and the source may try to restrict its requests.

(Refer Slide Time: 39:44)
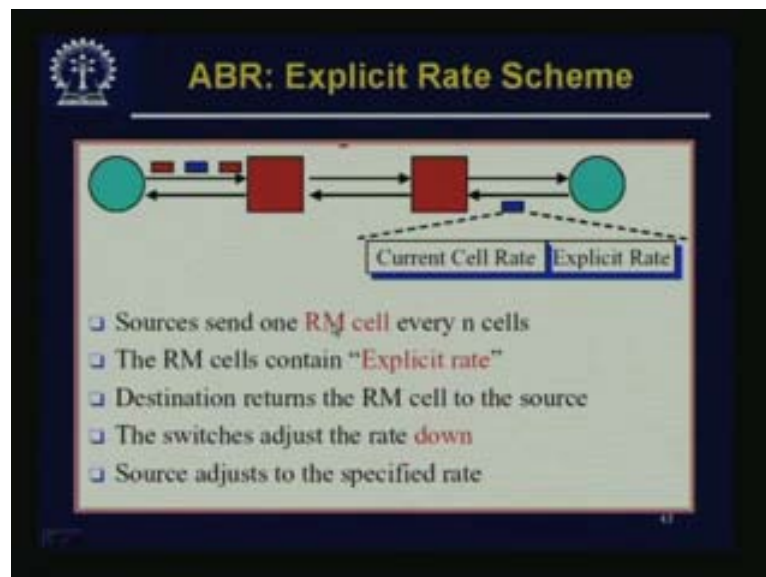
Sources send 1 RM cell every nth cells, the RM cells contain the explicit rate that has been asked for; the destination returns the RM cell to the source. The switches adjust the rate down; that means if it is congested, it may adjust the rate down and the source adjusts to the specified rate. Whatever rate comes through this, going up and coming down through this negotiation, is what the source finally has to accept.
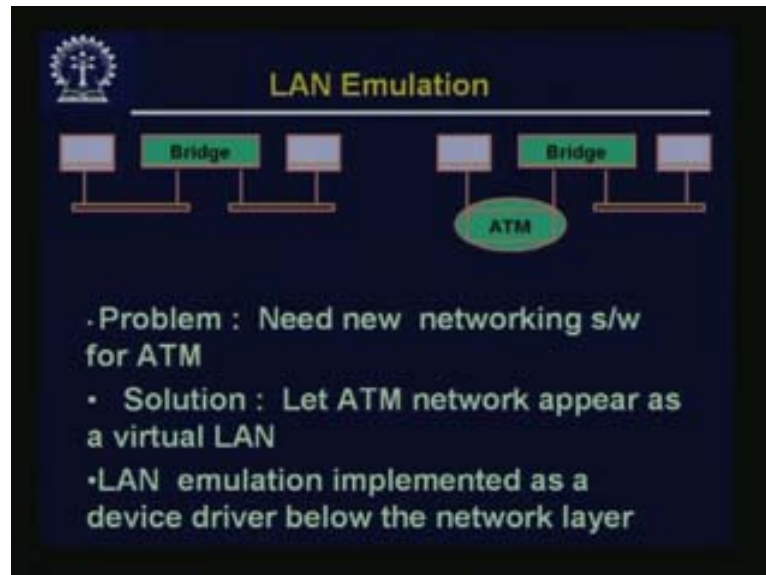
(Refer Slide Time: 40:17)

We will talk a little bit about LAN emulation, which is emulating a local area network when the backbone is of an ATM or when you use an ATM but still want to use the Ethernet and IP, specifically IP, in the nodes. And one very specific reason this is required is as follows. One of the reasons ATM was not successful in the LAN segment, although it was put as a LAN solution also in enterprise LAN solutions, was that there was hardly any software which was developed on ATM. Whereas a huge amount of software has been developed using IP and so much of software has been developed in IP, you cannot throw it up nor can you translate it to ATM software overnight; that is very difficult. People took a more pragmatic approach and thought the backbone network technology be that of ATM or have an ATM. Let us emulate the LAN so that your software IP based software can still run.

Problem: it needs new networking software for ATM solution. Let ATM network appear as a virtual LAN. How can an ATM network appear as a virtual LAN? LAN emulation is implemented as a device driver below the network layer. These are LAN emulation bridges actually; if there is an ATM, this will look like a LAN.

(Refer Slide Time: 41:39)

(Refer Slide Time: 42:03)
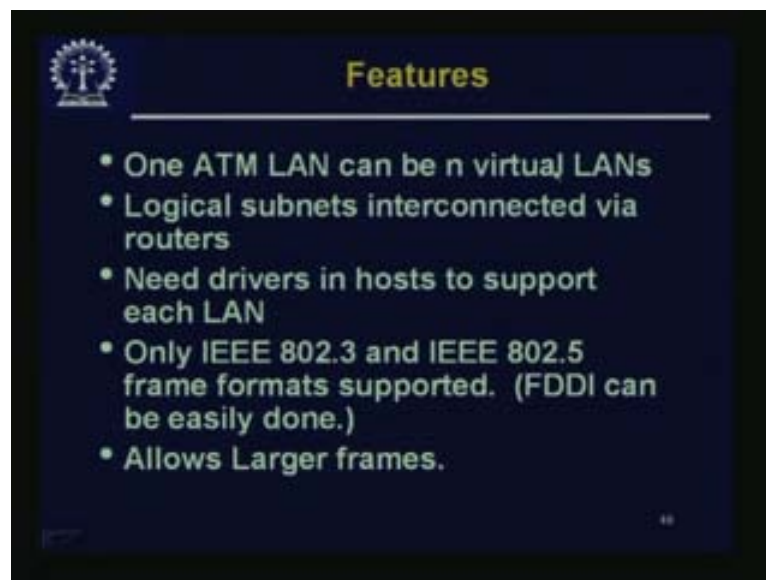
For this, 1 ATM LAN can be n virtual LANs. Many virtual LANs can be there in the same ATM LAN. Only one of them may be sufficient, this is a logical subnet interconnected via routers. This is the abstraction; this is the picture that we want to give to the world. It needs drivers in hosts to support each LAN; so in actual practice, only IEEE 802.3 and 802.5 were supported, although FDDI could also be done.

(Refer Slide Time: 42:42)
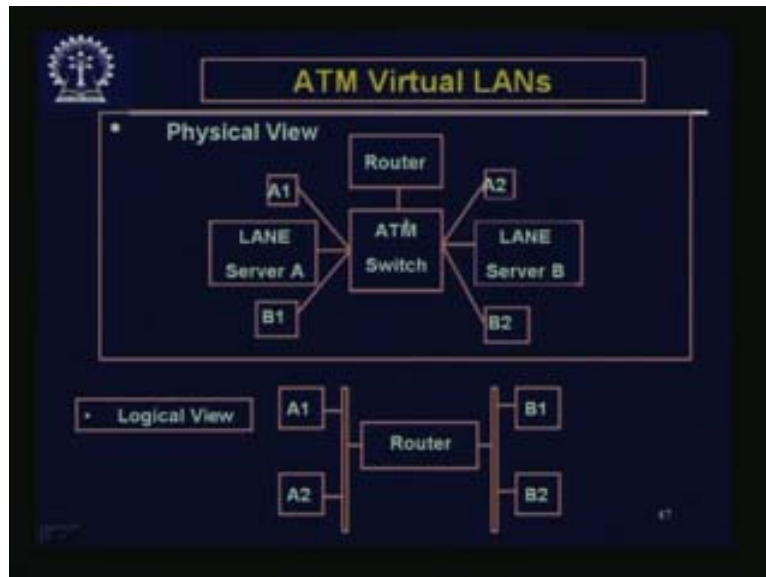
This is the picture: we have an ATM switch, we have some LANE servers, we have multiple LANs on this, we have a LANE server A and a LANE server B. The logical view would be as if a router is also connected to the ATM switch. The logical view looks like an IP network. We have A1, A2 connected via this network A and B1, B2 and there is a network B, which is connected. These two IP networks are connected via routers. This is the logical view, although the actual view is emulated here.

(Refer Slide Time: 43:22)
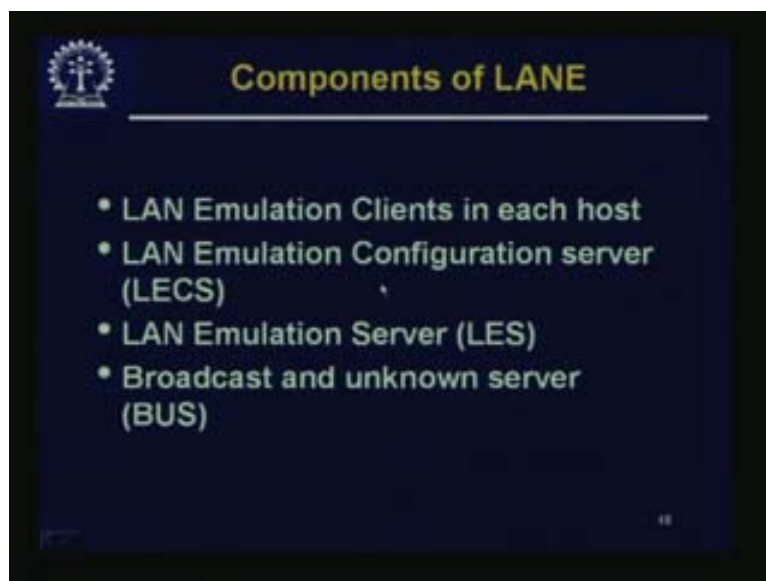
It requires several components; one component is that we require a LAN emulation client in each host. Each host must have LEC or LAN emulation client, which is small software, which can be

loaded in each host. LAN emulation configuration server or LECS will be in one central server, it will be taken as the LAN emulation configuration server. Whenever somebody wants to join the LAN or leave the LAN, the LAN emulation client will first ask for the parameters from the LECS. It has to know the address of the LECS and here is a LAN emulation server itself, the LES, and a broadcast and unknown server. If there is something, like the broadcasting in a network, which is done, we know that it is in a particular network for an ARP.
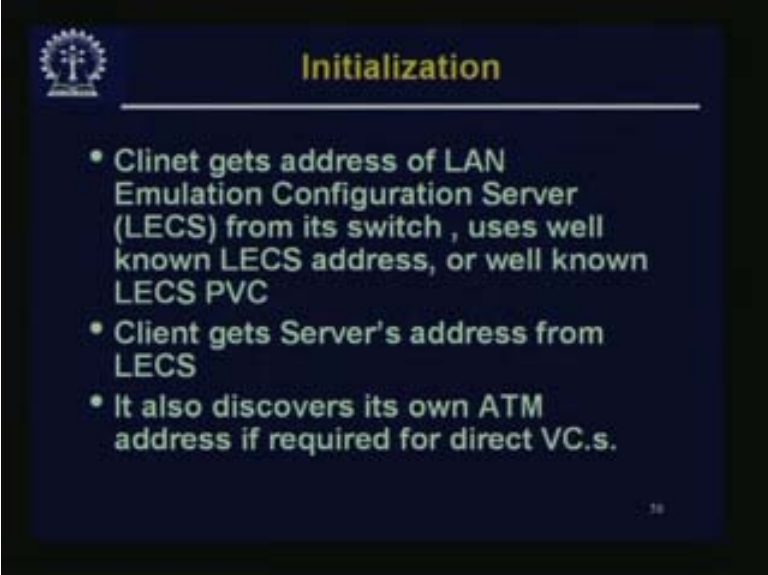
We want to do an address resolution protocol. What we do is that we broadcast a request, i.e., the IP address; what is the data link address? Remember that this ATM works on point to point, mostly, as a point-to-point connection. Although point-to-multipoint is possible, but it is not in both directions. Instead of trying to do the broadcast from the host itself, what it does is that if each host in this LAN emulation client has to broadcast anything, it will send it to another server called bus; there is a virtual connection between every host and the bus, and the bus will send the broadcast to each of the hosts. That way in an indirect fashion, the broadcast takes place. Similarly there is an unknown server; that means I do not know the address of the server like ARP. Once again, you send the request to this bus and the bus will find out and finally give you the address. These are the main components of LANE, namely LEC, LECS, LES and bus.

(Refer Slide Time: 46:00)
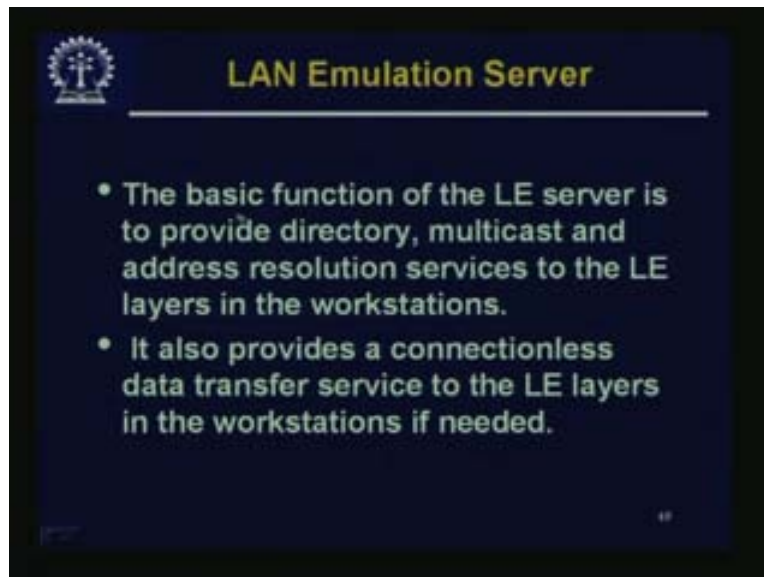
What does the LES do? The basic function of the LE server is to provide directory, multicast, and address resolution services to the LE layers in the work stations. That is what the LAN emulation server does. It also provides a connectionless data transfer service to the LE layers in the workstation if needed. The parameters for setting up a server, etc., will be known to the LECS, which will communicate to the LEC as the LEC joins the network.
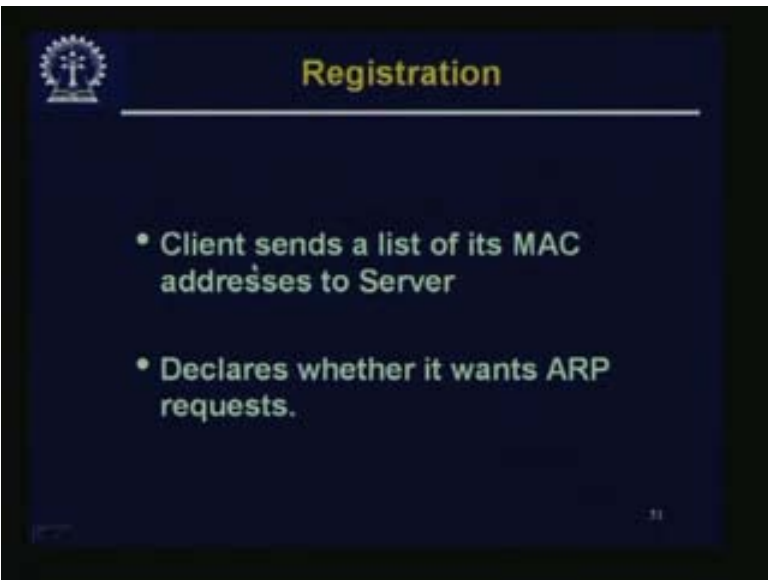
(Refer Slide Time: 46:52)

Initialization: The client gets the address of LECS from its switch, uses well-known LECS address, or well-known LECS PVC. There has to be particular PVC, which it starts using automatically. The client gets server's address from LECS. It also discovers its own ATM address if required for direct VCs. That means if it wants to do some direct communication between two nodes, it has to get the ATM address of the other side if it wants to set up a direct VC instead of going via the servers. In that case it will require its own ATM address also.

(Refer Slide Time: 47:45)

It does a registration; client sends a list of its MAC addresses to the server; declares whether it wants ARP requests. These have to be known to the server so that the server can give the service to the other nodes connected to that network. Client sends ARP request to server.

(Refer Slide Time: 48:01)
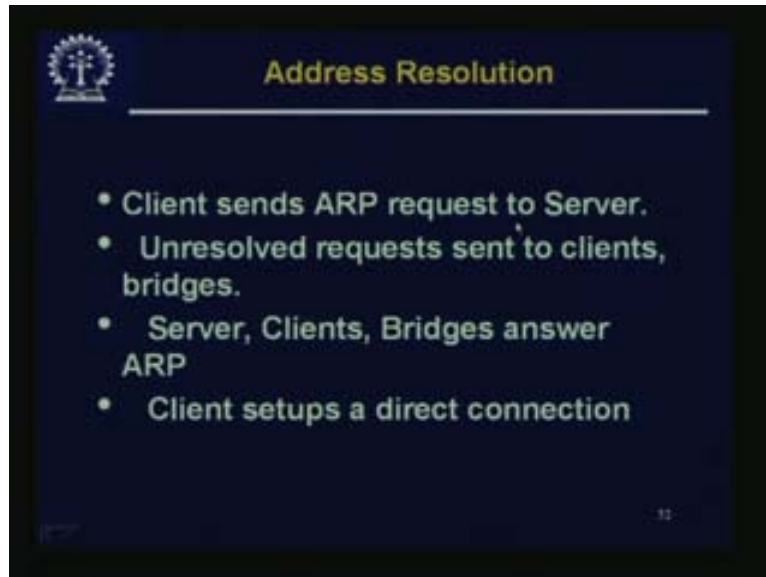
Address resolution: client sends ARP request to server; unresolved requests are sent to clients, bridges, servers and the ARP; client sets up a direct connection. This is how a connection is set up.
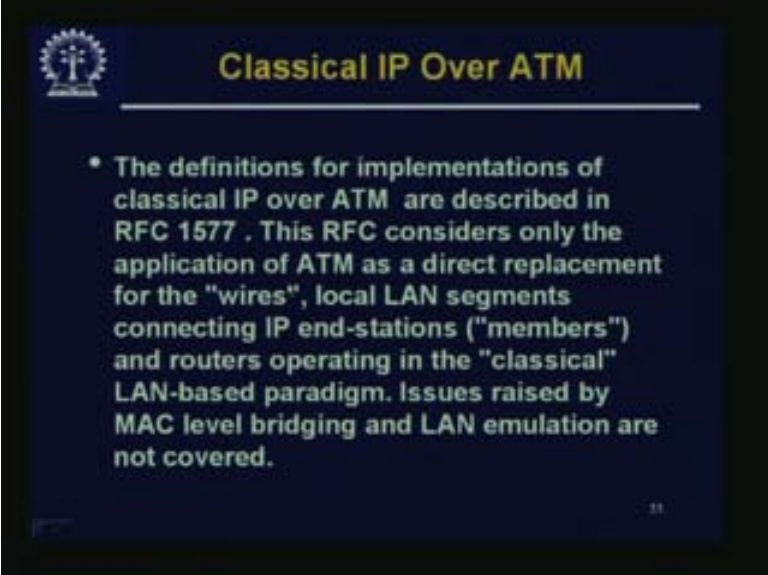
(Refer Slide Time: 48:20)
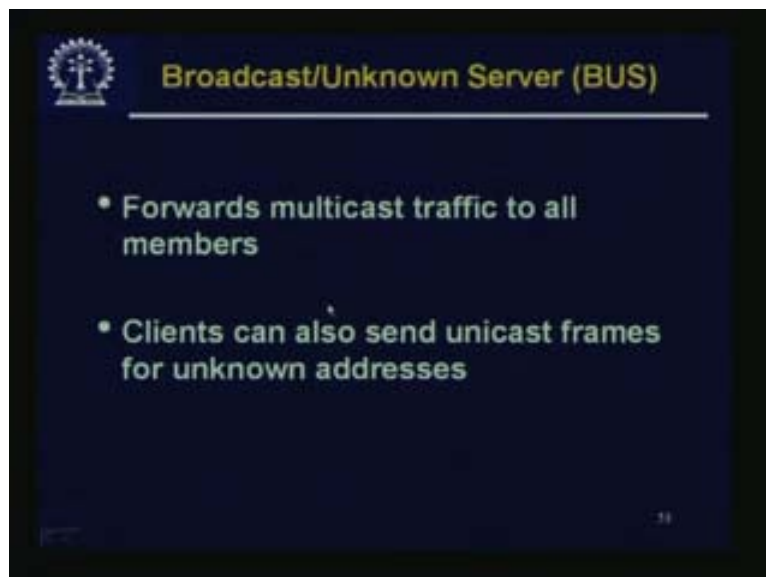
Broadcast to unknown server or bus: as I said, it forwards multicast traffic to all members. Clients can also send unicast frames for unknown addresses there. Suppose some address is not known, you send it to bus and then bus will try to find out.

(Refer Slide Time: 48:41)
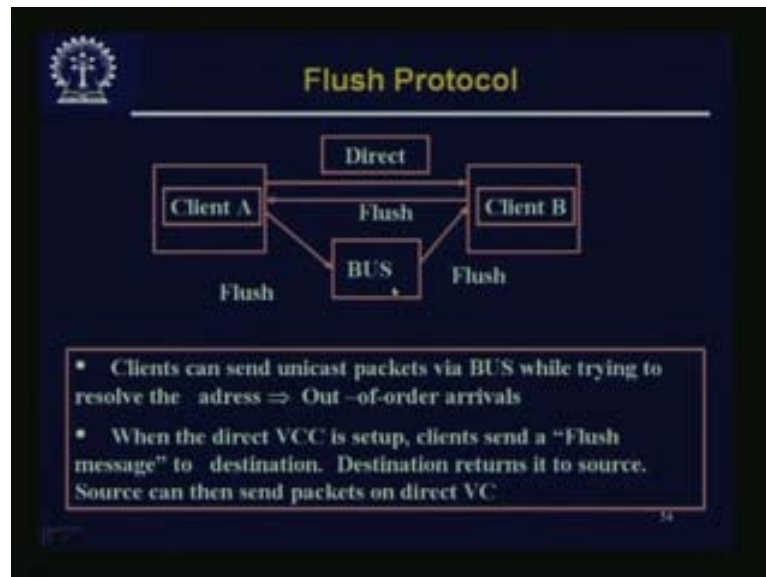
There is a flush protocol. That means clients can send unicast packets via bus while trying to resolve the address. What might happen is that client may try to get the address, then get some address, maybe send it directly. What might happen is that something which was not sent directly here, the packets may come out of order. Remember I mentioned that in ATM, one guarantee is that cells will not come out of order. Cells may get lost, but cells will not come out of order, unlike pure datagram services. But in this particular case this may happen because we are not talking about one particular VC. In one particular virtual circuit, the packets will indeed not go out of order but in this particular case, they might. When direct VCC is set up, client sends a flush message to the destination, destination returns it to source, can then send packets on VC. This is a flush message that this problem is solved.

(Refer Slide Time: 49:55)
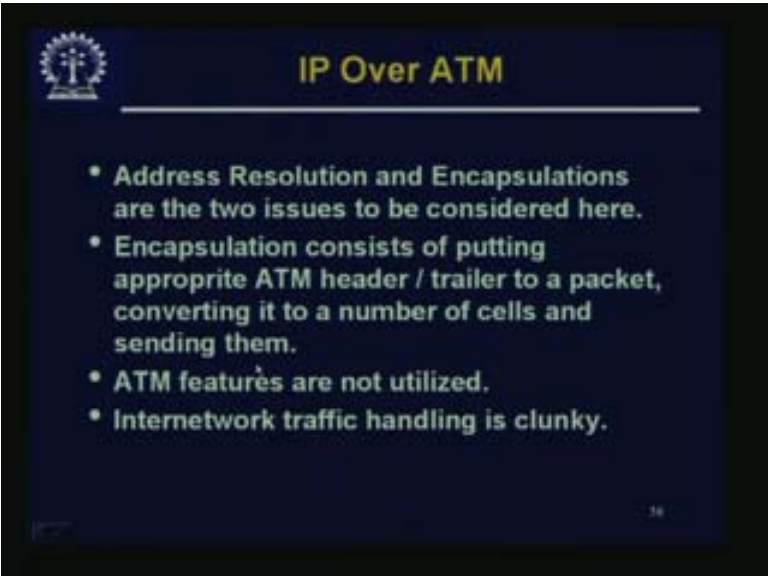
There is another approach to this, which does not use LAN but uses classical IP over ATM. What is classical IP of our ATM? The definitions for implementations of classical IP over ATM are described in RFC 1577. All the details are here; once again, we will just simply mention it very quickly. This RFC considers only the application of ATM as a direct replacement of the wires; local LAN segments connecting IP end stations which are the members; and routers operating in the classical LAN based paradigm; issues raised by MAC level bridging and LAN emulation are not covered.

(Refer Slide Time: 50:39)

If you want to look at classical IP over ATM, you have to do address resolution and encapsulation. These are the two issues to be considered here. Encapsulation consists of putting appropriate ATM header trailer to a packet, converting it to a number of cells and then sending them. This is encapsulation, which means that you have an ATM packet. This is classical IP running over ATM when you have a big packet. You know that cells have to break it up, and put a proper header on each one and then send them. ATM features are not utilized and inter network traffic handling is clunky.
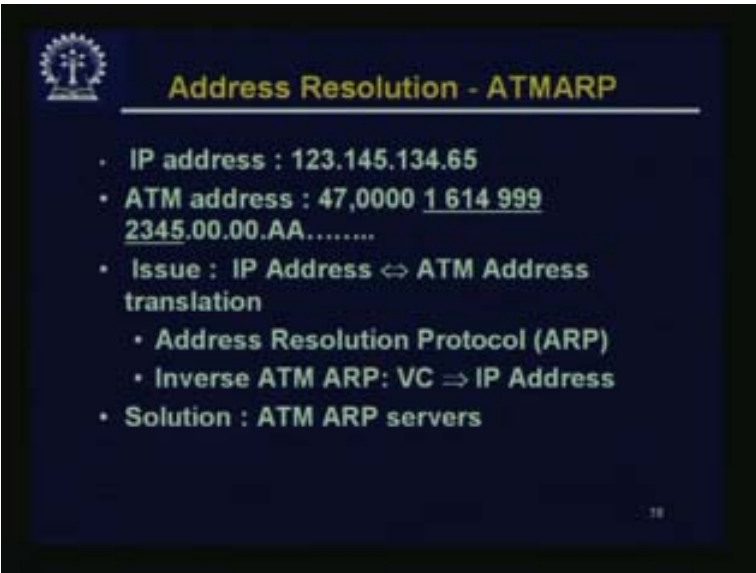
(Refer Slide Time: 51:21)
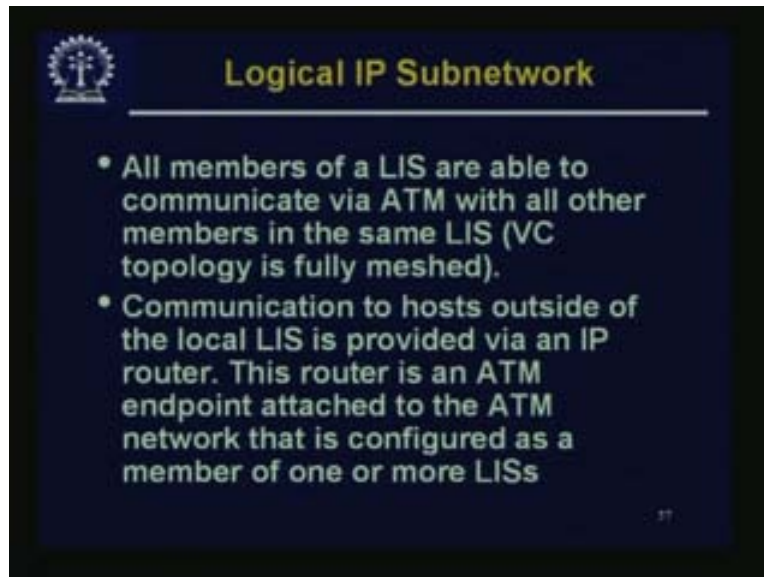
 Each of the IP sub-networks is a logical IP sub-network. All members of a logical IP sub-network are able to communicate via ATM with all other members in the same LIS, which means that if two nodes are in the same logical IP sub-network, i.e., same LIS, you would set up a VC on. There is a VC between every pair within or amongst all nodes in a particular logical IP sub-network. There is a VC mesh; everybody can communicate to everybody else. Communication to hosts outside the LIS, local LIS, is provided via an IP router. This router is an ATM endpoint attached to the ATM network that is configured as a member of one or more LIS.

(Refer Slide Time: 52:22)

Naturally, a router may be a member of more than one network. Similarly, the network is configured as a member of one or more LIS. You have to do an address resolution. The valid question is that, if the IP address is this, what is the ATM address? You have to do an ATM ARP: IP address to ATM address translation, address resolution protocol is used. Inverse ATM ARP means VC to IP address; solution: use ATM ARP servers. There are ATM ARP servers there.

(Refer Slide Time: 52:50)
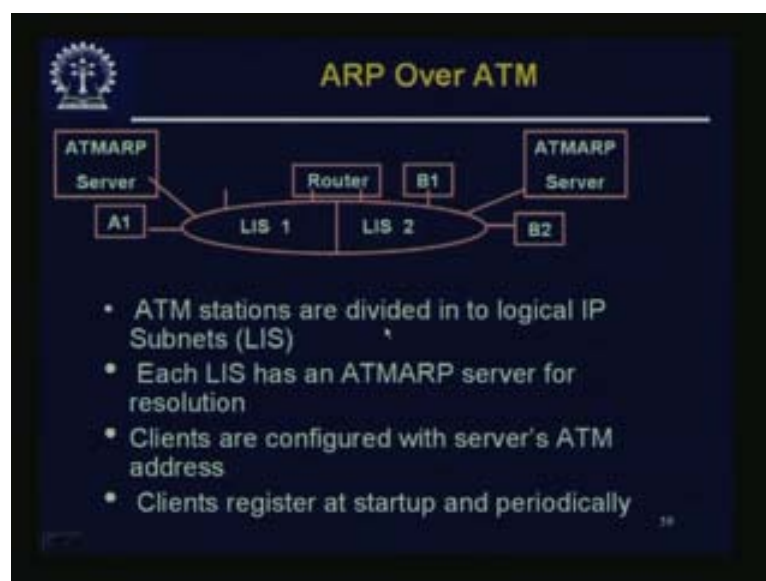
This is a diagram, suppose this is a logical IP sub-network number 1 and this is logical IP sub network number 2, each of them has its own ATM ARP server for doing ARP, that means, IP to

ATM address translation and vice versa. Nodes are connected; if A1 wants to communicate to B2, naturally at the top level, you give the IP address. Previously we were breaking it up into data link address. Finally what is the route to take if it is in some other list? If it is in the same list, you have a direct VC to it and you have a direct virtual circuit; you take that. Each LIS has an ATM ARP server for resolution; clients are configured with the server's ATM address and clients register at start up periodically.

(Refer Slide Time: 53:50)
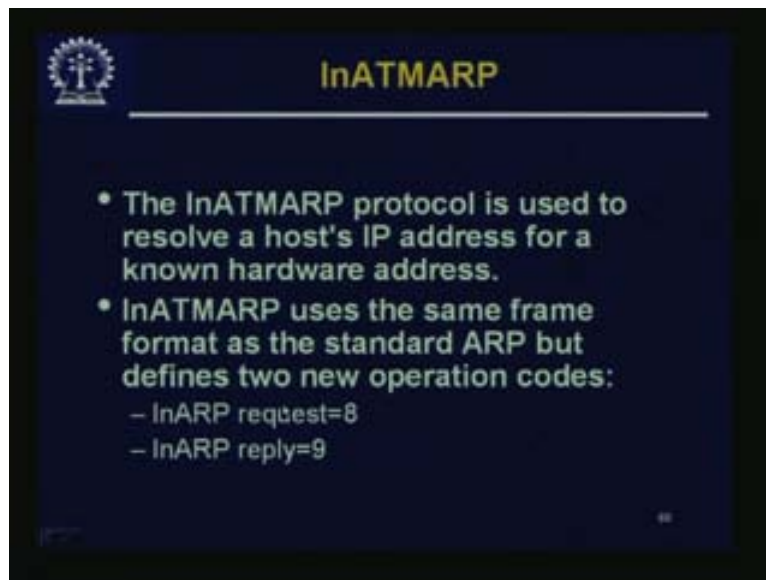
In ATM, ARP protocol is used to resolve a host IP address for a known hardware address. It is the inverse ATM ARP. As you can understand, this ATM is a rather complex technology and this is one of the reasons it was not so successful. As you will find later on, many of the ideas which were used in ATM, namely, about this quality of service, about setting up flows and setting up virtual circuits with VCI VPI labels, these ideas were later on adopted in IP and we will discuss it a lecture called MPLS, that is, multi protocol label switching, where the similar ideas have been used to give this kind of services later on. Also, ATM is used quite extensively in big backbone networks because of the various facilities. Although it has moved out of the LAN segment, these days the gigabit Ethernet has replaced it simply because of the host. Thank you.

Preview of the next lecture

(Refer Slide Time: 55:11)

So today we will start our discussion on routing. Actually we have already talked about routing a little bit in different context specifically in the context of ATM. How the ATM virtual path are set up. Today, we will talk about the major area. We will start our discussion on the major area of routing which is how and specially with reference to the TCP IP stack. That is how packets are routed in an IP network we will talk about.
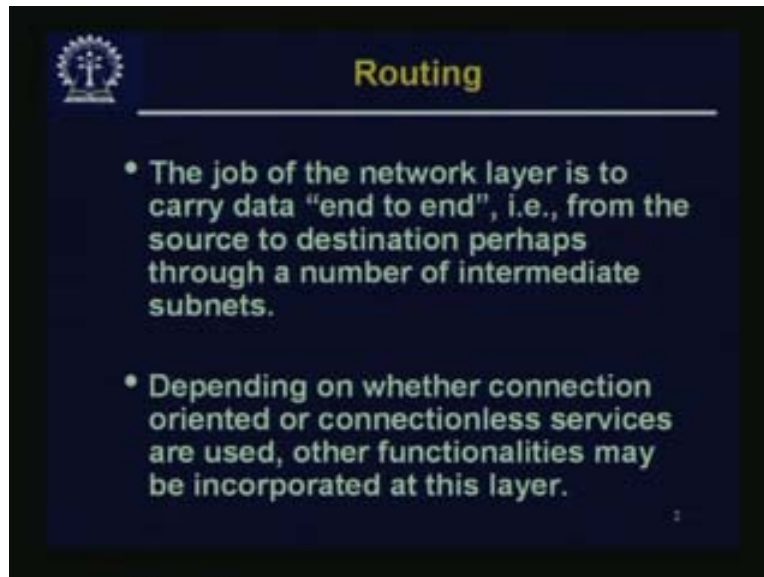
(Refer Slide Time: 55:54)

Today, we start the introduction and to routing, we will take up the discussion about different routing protocols in next set of lectures.

(Refer Slide Time: 56:09)

Let us just recollect what the job of the network layer or what is routing. This is to carry data end to end, i.e. from source to destination perhaps through a number of intermediate subnets depending on whether connection oriented or connectionless services are used. Other functionalities may be incorporated at this layer; we will talk about this later on. We are talking about IP routing of IP packets and how you can have a virtually connection oriented system on that. We will discuss it later on, the point is unlike data link layer remembering the next hop just the link which is immediately adjacent.

That has some advantages in the sense that whatever information you require about it are locally available here. Routing is the major problem; we are talking about routing over multiple networks and towards a very remote system. The packet might have to take many hops maybe 10, 20 even 30 hops to reach the end point and when you take naturally. Let say 20 hops, the area you are sort of serving becomes so large with so many machines connected to it. How to keep track and naturally switch so many machines with so many links is the problem. Some of the link may go down some of the machines, may come up and when I say machines it may refer to actual either PCs servers etc. They may also refer to the network boxes like other routers Calculate the check sum which is for your connection.

(Refer Slide Time: 58:03)
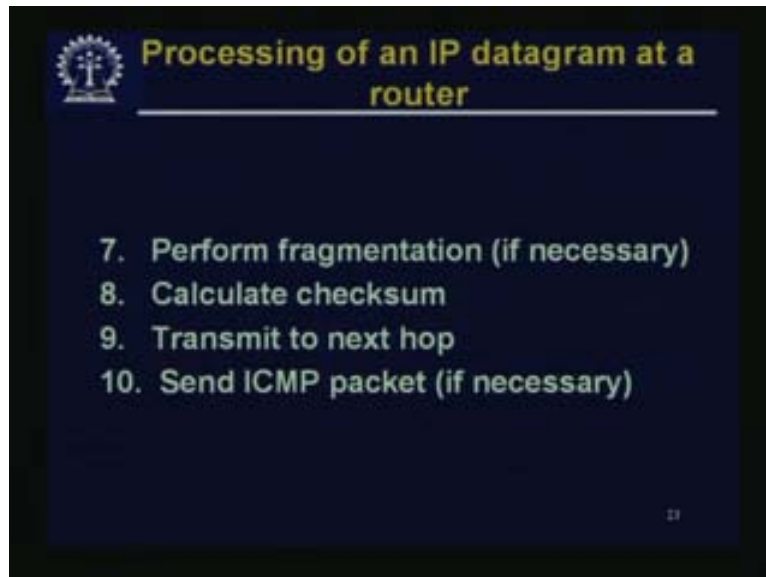
As we know can transmit to the next hop and send an ICMP packet if necessary. ICMP is for internet control message protocol if the routers may use ICMP packets for sort of talking to each other and sending various messages if necessary. We will see 1 example,.