Digital Voice and Picture Communication

Prof. S. Sengupta

Department of Electronics and Communication Engineering

Indian Institute of Technology, Kharagpur

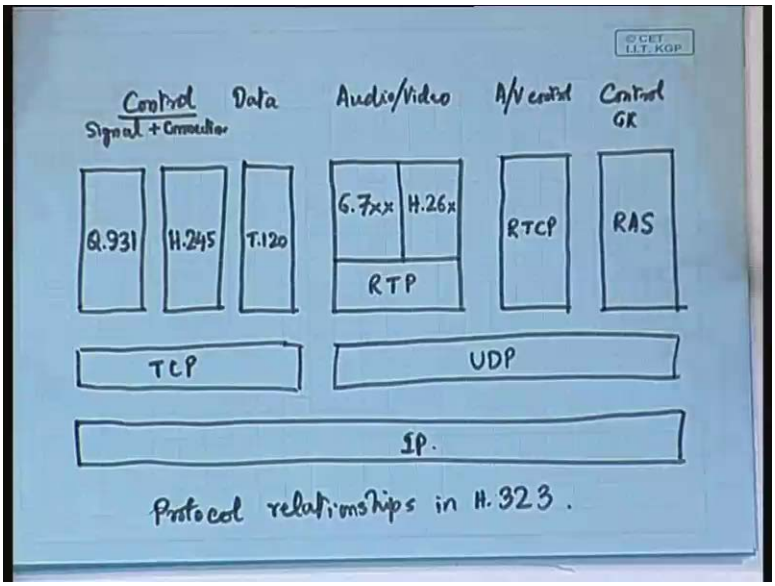
Lecture - 34

H dot 323 Call Controls and Enhancements

In continuation of the H dot 323 standard that we were talking about for the call signaling and we will be talking about the various issues of H dot 323 because not all the issues we could discuss in the last class. So essentially what we are going to do is that amongst all these issues we should take up the control or rather call control and enhancements because there are certain limitations that exists in the H dot 323 version 1 and we would like to see that how those limitations are overcome in the subsequent versions and then only the H dot 323 after avoiding those limitations H dot 323 could be made at par with the PSTN telephones in terms of popularity.

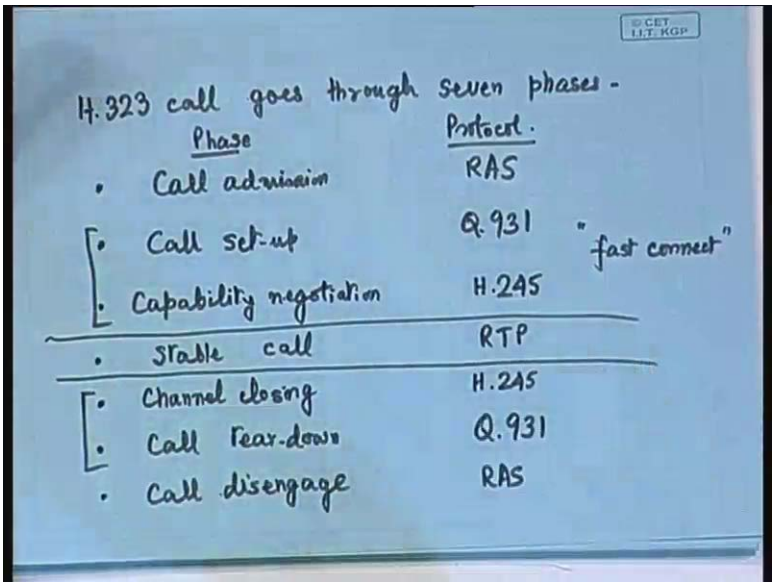
Thus, now regarding the call control, actually before going to that, let us just take a quick look at the aspects which we had seen in the last class.

(Refer Slide Time: 02:21)



Therefore, towards the end of the class we were discussing two aspects: one is the protocol relationship where you can see that essentially we try to separate the data and the signaling aspects. The signaling aspects are very important; as far as its sanctity is concerned it has to be a very reliable communication. So Q dot 931 which addresses the signaling H dot 245 which addresses the capability negotiation T dot 120 that takes care of the data integration all these things have to be send through the TCP/IP whereas the bit-stream which are generated from the codecs the audio and the video codecs they have to be transmitted over the RTP/UDP/IP protocol channel.

(Refer Slide Time: 03:21)



And we had essentially identified seven phases of the H dot 323's call starting from the call admission up to the call disengage. And this is the part (Refer Slide Time: 3:33) where the actual message transfer is going on means when the parties are actually in conversation is only this part. So there are certain things prior; the signaling that is prior and there are signaling that have to close down. So these are taken care by the different parts of the protocol: the RAS, the Q dot 931 all these things we mentioned.

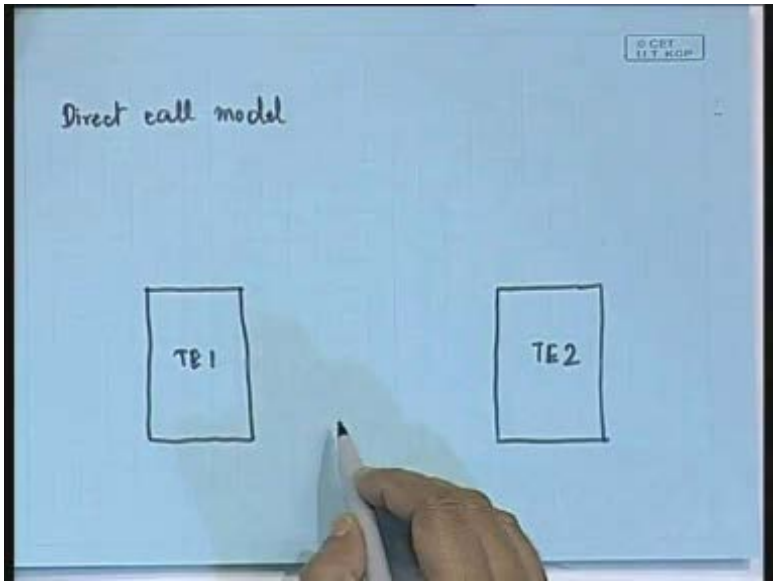
Now it appears that the protocol could be quite that it would involve some amount of time to go through these seven phases so the protocol would make the process slower. But there are some shortcuts which are available; one of which I was trying to mention in the last lecture is that that there is also a fast connect possibility where the call setup and the capability negotiation these two could be integrated.

In fact, capability negotiation part may be dispensed within a small scale version of the H dot 323 system and call admission well, call admission's basic purpose is that there are several things that goes with the call admission that it is another level of protocol that is being maintained and in fact as I was mentioning that in the beginning this call admission was not there so that the two

end points could communicate without going to the call admission process but really speaking the involvement of the gatekeepers makes that mandatory to have a RAS protocol for the call admission so that the call admissibility and its status monitoring that could be done by the gatekeeper.

Now, going by that actually there are two basic models that can be thought of for the call control; two fundamental call control models. One is what we are calling as the direct call model. in the case of direct call model we will take the endpoints. Let us say that this is terminal equipment number 1 and this is the terminal equipment number 2 and these two terminal equipment they want to have a communication.

(Refer Slide Time: 6:21)

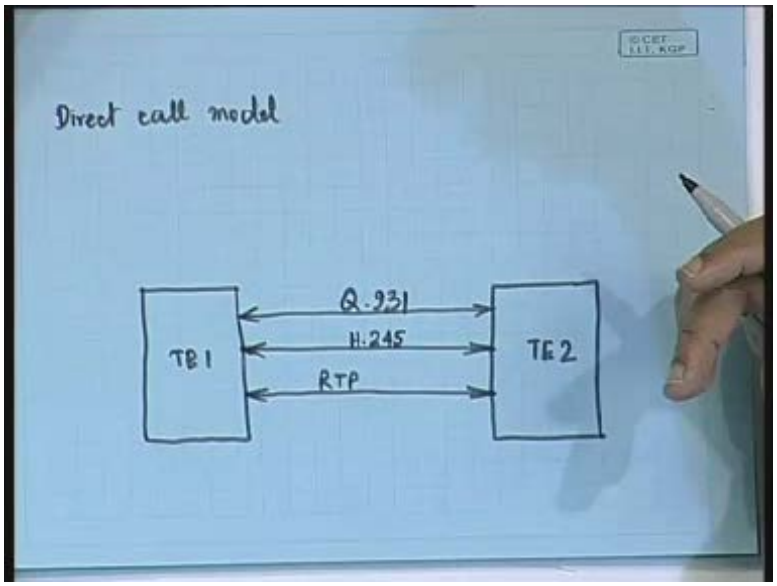


Now here there will be now obviously as far as the data part is concerned the RTP would be the protocol that would be followed in order to in order to exchange the voice packets between TE 1 and TE 2. But before that some signaling is really required signaling and negotiations.

Now, in the direct call model the signaling and the negotiations are done between the TE 1 and TE 2 without the involvement of the GK the gatekeeper. So what are these; like the Q dot 931

which is the signaling protocol that that is what we were discussing in the last class so Q dot 931 could be used directly over the communication channel that would be setup between the TE 1 and the TE 2 and the H dot 245 or rather to say it is a direct TE 1 to TE 2 or TE 2 to TE 1 back those communications would take place and this would go through the H dot 245 actually this is the capability negotiation.

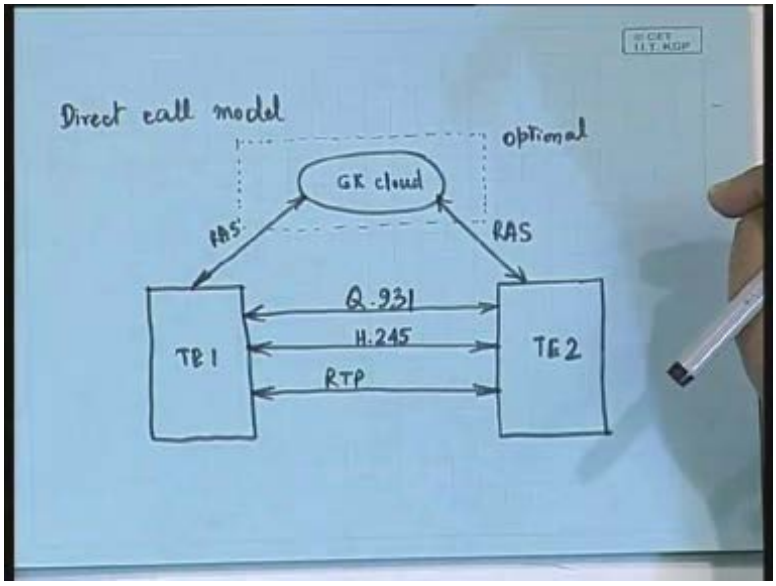
(Refer Slide Time: 7:46)



But mind you, we have not shown any RAS. Now RAS if the RAS is dispensed with in that case we do not have any problem. in fact the direct call model can work without the involvement of RAS or if you want to keep an RAS actually in that case if RAS is needed in that case the presence of GK is necessary because RAS is not something which you can have directly between TE 1 and TE 2 the RAS has to go through the gatekeeper. So here if we have a gatekeeper cloud (Refer Slide Time: 8:30) then we can have the gatekeeper to TE 1 communication through the RAS protocol. And likewise between TE 2 and RAS between TE 2 and the GK cloud it could be through the RAS. So this is the direct call model. And why we put it as dotted is that this block is an optional block. We may dispense with this if so needed. In fact that used to be the case in the initial PC centric proprietary VoIP applications. There, there was no concept of gatekeeper that

was introduced. But when people planned for having a commercialization and exercising control of the GK there this RAS is necessary.

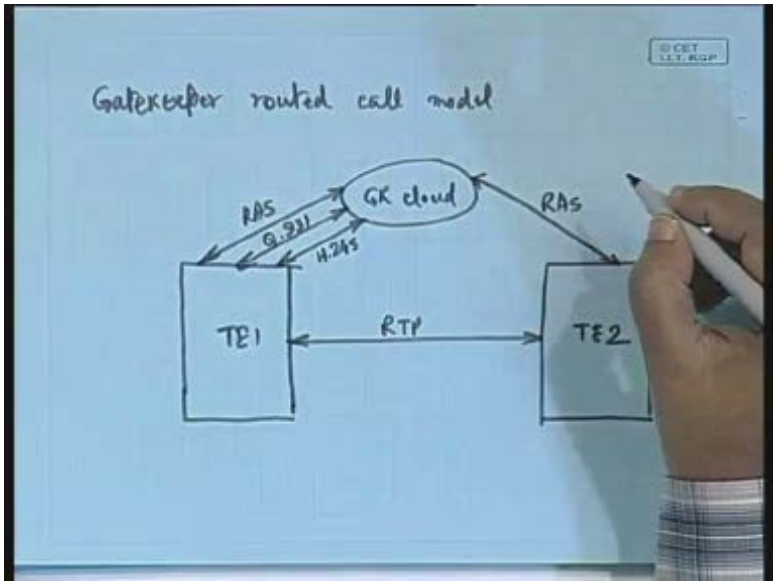
(Refer Slide Time: 9:31)



But in this case see that although it is only the RAS but the signaling still takes place between the TE 1 and TE 2 directly without the involvement of the GK cloud at least as far as the Q dot 931 and H dot 245 are concerned.

There is a second alternative model which we call as the gatekeeper routed call model. And in this model the entire signaling has to go through the GK cloud. So we have the TE 1 and the TE 2. Now TE 1 and TE 2 will only have the RTP between them but all the rest of the signals has to pass through the GK. So if we have the GK cloud here then essentially any communication with GK has to start with the RAS then the Q dot 931 and the H dot 245. Ultimately it is endpoint to endpoint but has to go through the GK cloud.

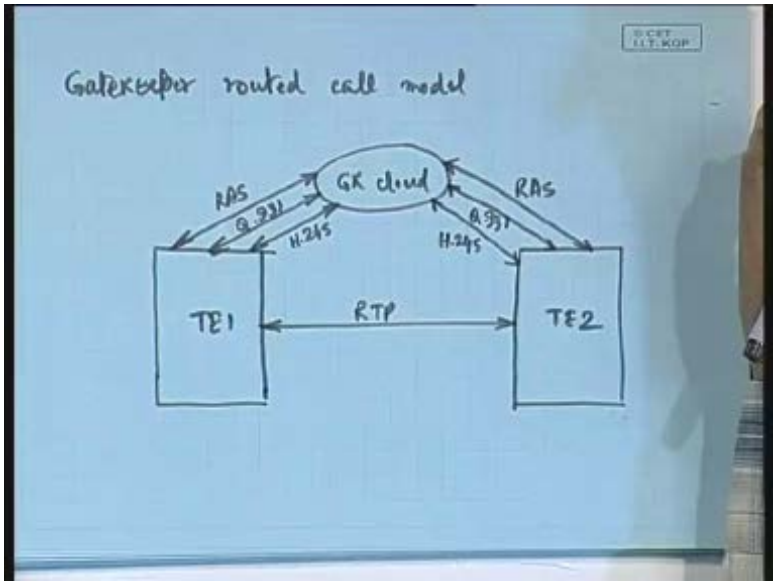
(Refer Slide Time: 11:11)



Likewise, even between TE 2 and GK cloud it is RAS. Why is it called as GK cloud anybody can just draw some light on that?

GK cloud because actually what happens is that typically it is an interconnection of several WANs that would exists we had shown in the last example we had shown only two LANs but it may go through multiple WANs and in that case there will be involvement of several GKs because every LAN whenever you are connecting from one LAN segment to the other every LAN is going to have the gatekeeper so it is gatekeeper to gatekeeper and again there may be involvement of more than two gatekeepers also. So, in effect it is a gatekeeper cloud. So the gatekeeper to which TE 1 is connected and the gatekeeper to which TE 2 is connected is not the same. But we are showing the block as a GK cloud and RAS we have to have Q dot 931 and this is the H dot 245 so this will be the gatekeeper routed control model.

(Refer Slide Time: 12:26)



The advantage that we get in this process is that in this case the gatekeeper has the control in the sense that since all the signaling is taken care by the gatekeeper and it is with the knowledge of the gatekeeper that is why the call monitoring and call billing everything can be done because everything is under the GK. And not only that; one aspect which I did not explicitly mention in the last class is about the security because although again not in the version one of H dot 323 but in subsequent versions it was felt that definitely the security is very important and especially when the call signaling takes place things like the authentication, the data integrity everything must be taken into consideration and that is why there is also a standard that has been developed by the ITUT for the security or for a secured communication of all these signaling because this is very important because this is where..... I mean, if you have any intrusion you can that can lead to lot of unauthorized communication or could lead to the data corruptions and all such things, any impersonation everything can happen.

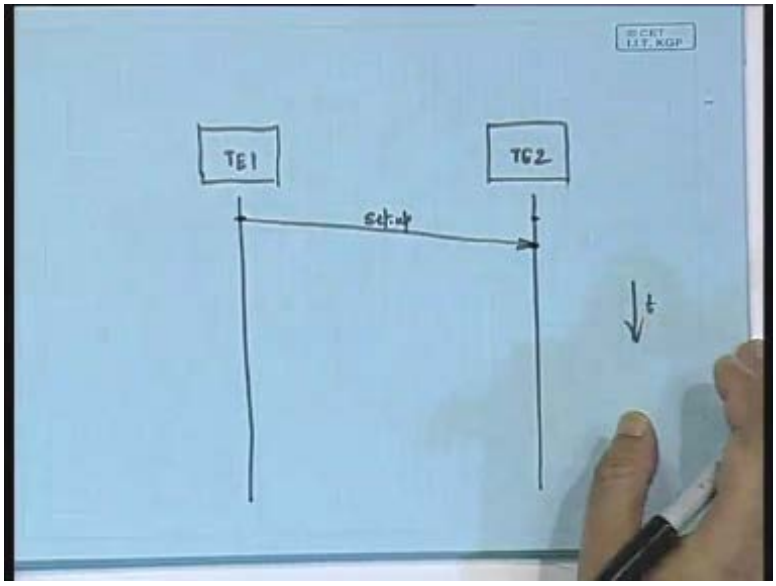
Now, before we go into the security aspects, a look at the call setup model that is going to be followed. So we know now that one simplest model is without the gatekeeper where the RAS is not needed. Even the gatekeeper also will not be needed at all and there essentially everything is,

the signaling is also between the TE 1 and TE 2. So, in that simplest model we can have the have an overview of the protocol of the signaling that has to take place.

So, if we have TE 1 over here and we have TE 2 over here, in order to show their protocol timings it is customarily shown like this that whatever is at the TE 1 end for that we draw a vertical line and whatever is at the TE 2 end we draw a vertical line below TE 2 and this will be the time access so this is the increasing direction of time (Refer Slide Time: 15:17) so that whatever TE 1 initiates at a particular time would be shown over here and if the TE 2 receives that signal instantly without any timing delay then it will be a perfectly horizontal line.

But if TE 2 has got some delay means the perfect horizontal line ends over here but actually there is a delay in the communication between the channels; supposing a delay of this much is there in that case the line that you are going to draw should be an inclined line. The line can never have an inclination like this because you cannot initiate something and then ahead of that it is received in the destination terminal that is not possible. So this is what we will be having for the setup. This signal is for the setup that TE 1 wants to set up a call like you can say the dialing. So let us look at it from the what do you say from the PSTN consideration itself that is how it takes place, you want to communicate so naturally what you want to do is to dial the number.

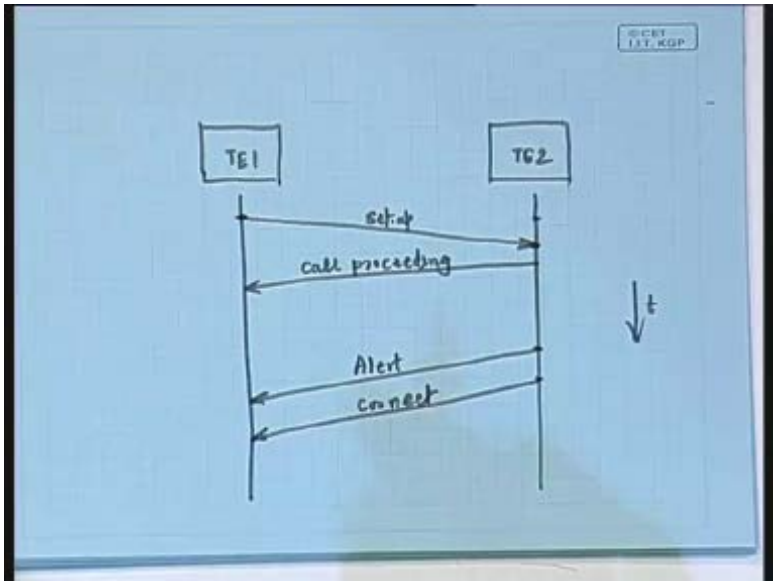
(Refer Slide Time: 16:48)



So the setup, there is no involvement of any gatekeeper. So the setup signal that would arrive over here and if the path is completed if this TE 2 telephone is active in that case it sends the call proceedings. So there is a call proceeding which means that it is an acknowledgement to the setup. But actually the TE 2 may take some time although a direct involvement of TE 1 and TE 2 would make the ringing almost immediately but let us say that in time the ringing is staring from here so this is where the TE 2 starts ringing and the very fact that TE 2 is ringing would be also received in TE 1. So this is called an alert because with this signal TE 1 gets prepared that now any time TE 2 can lift the telephone. Because you have, TE 1 is the source, TE 1 initiates the calls so TE 1 has already lifted the handset and TE 1 through this alert is actually listening to the ringing tone that is going on in the other end. TE 2's ringing tone TE 1's user is finding.

So now TE 1's user is getting alerted that anytime when TE 2 user lifts his/her handset then the call is going to commence. Only after that, only when the receiver at the TE 2 is lifted then the actual connect will be there so with that there is a connect signal. This is the simplest kind of a signaling protocol that would go on from the setup up to the connect.

(Refer Slide Time: 18:58)



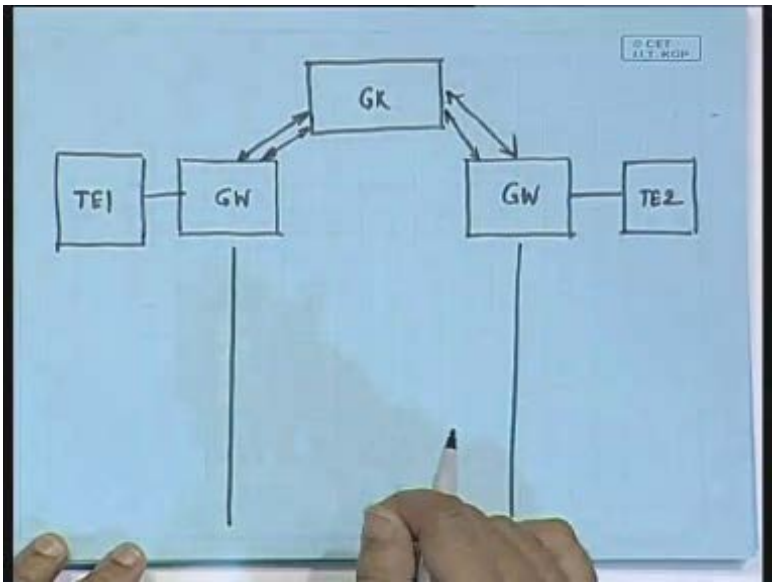
This looks pretty simple because this is a direct connection. This is what we are showing as the call setup with no gatekeeper. But when gatekeeper is involved the call setup proceed here will undergo some change why because there will be the gatekeeper which is interposed in between so there will not be any direct signaling that would go from TE 1 to TE 2 rather everything should go through the gatekeeper. Now let us see that how the involvement of gatekeeper changes.

We will show for one gatekeeper but when more than one gatekeeper is involved it is just a simple extension of what we are talking of.

Now here let us say again we have a terminal equipment here and we have another terminal equipment over here and then we have a gatekeeper, we have a gatekeeper. Now the terminal equipment actually in this case if it is between two LANs in that case one can have the gateways. So instead of the terminal equipment we can also have gateways over here. So this is gateway on this side, this is another gateway and the terminal equipment number 1 may be connected to this gateway and terminal equipment number 2 may be connected to another gateway. Then we could have the gatekeeper or the gatekeeper cloud coming in between. So there we have the RAS and

all the signaling protocols which would be over here. This (Refer Slide Time: 21:10) is through the gatekeeper whereas the RTP would go through the gateway. Anyway that is not very that is not what we are trying to emphasize upon here but let us see the kind of the signals that would be required.

(Refer Slide Time: 21:31)



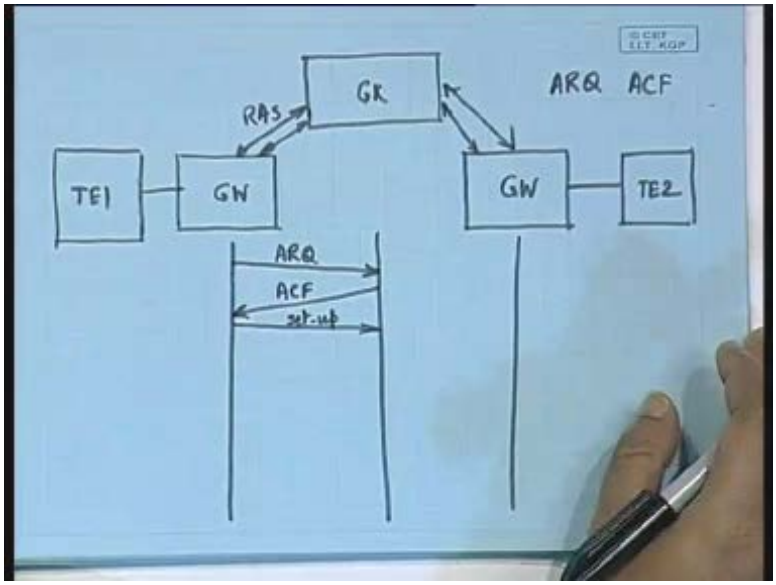
We start with the gateways and this is the GK the gatekeeper so gatekeeper timings also would be shown by this vertical line. This vertical line corresponds to GK (Refer Slide Time: 21:41) and these two vertical lines correspond to the gateway at this end and the other. And again let us assume that it is the terminal one that wants to initiate a call. So what now the terminal equipment 1 or this gateway has to do is that before the setup it has to ask for an admission request because there is a gatekeeper that is involved so RAS protocols are coming into place and because of RAS protocol you need to have the admission request; the short form of admission request is ARQ so I am writing this as the ARQ.

ARQ has to go from the gateway to the gatekeeper. This is the ARQ or the admission request. Now protocol-wise it is defined in the RAS protocol that ARQ has to be acknowledged if the

admission is granted so there should be a signal which is which we call as the ACF or Admission Confirmation. So the admission confirmation has to come.

In fact, it could be ARJ also the Admission Reject. If the admission is not there then it may also send an admission reject signal but let us say that admission is confirmed so this is ACF which goes back from the gatekeeper to the gateway. So now it is only after the admission that the gateway should initiate the setup. Now GK has already accepted this TE 1; GK has already registered so there is no problem in passing on this setup information to the destination GW in turn to the destination terminal.

(Refer Slide Time: 23:52)



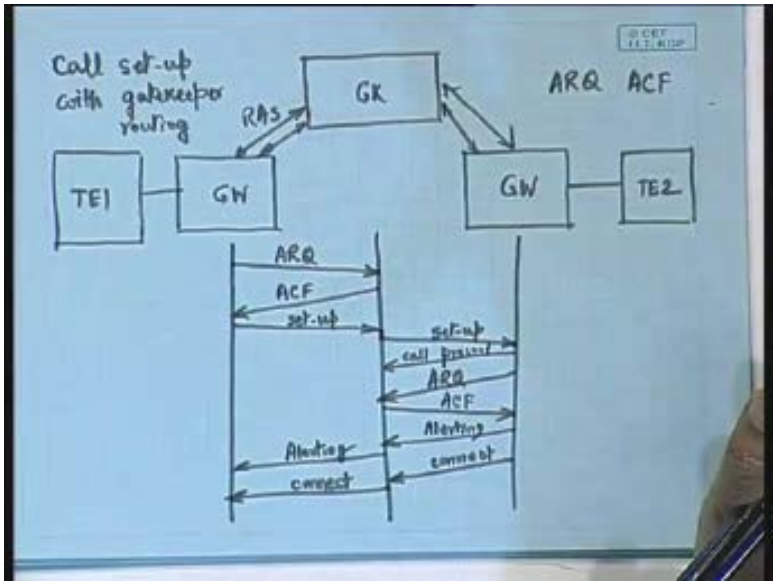
Now we can show it almost instantly but with a minor cosmetic delay we can show that the setup signal goes from the gatekeeper to the gateway. This is not a direct connection, this is through the gatekeeper. this gateway tells the gatekeeper, gatekeeper tells the next or the destination gateway and in between this much of delay whatever is there this is the delay by the gatekeeper; may be the gatekeeper software will have a little bit of delay which may be negligible kind of a delay but setup typically, this is where the setup signal will reach over here.

Now, when the loop close is detected then the setup would be responded by call proceed. This is where we will be having the call proceed as before.

Now what happens is that you should expect that the alerting should be there. But mind you that gatekeeper although has sent the setup signal, gatekeeper has not yet admitted this terminal equipment or this gateway so the admission would be necessary now. So what now when it sees that there is a call that is going to materialize this gateway has to seek the permission of the gatekeeper. so with the setup see This is with the loop closer this will take place so no problem but the gateway has to send an ARQ; the gateway has to send an admission request to the gatekeeper and in response to that there will be an admission confirmation.

Now this gateway, the destination is also registered. Now the source is registered, the destination is also registered so now the alerting or the ringing takes place. alerting will be done first to the GK, then the GK passes on this alerting to the source gateway; so this is alerting (Refer Slide Time: 26:21) and now when this gateway or this TE 2 is commencing the actual conversation or goes off to or you can starts the communication then this connect which is there the connect after so the connect will be routed through the gateway to the source. This is where the connect will be there. This is with the involvement of one gateway one gatekeeper so what you can see in this case is that basically the setup, call proceed, alerting, connect they remain almost the same but there is a there is an extra procedure which comes in and that is this ARQ/ACF kind of a handshaking which is needed both for the source end as well as for the destination end. Now this is the call setup with gatekeeper routed call signaling. So call setup with gatekeeper routing. this is the second model that we are talking of.

(Refer Slide Time: 27:51)



Of course we are showing only the signaling part. But mind you, again gateway to gateway communication that would take place directly over the RTP protocol. For that the GK is not coming into the picture. GK is only for the admissibility and signaling.

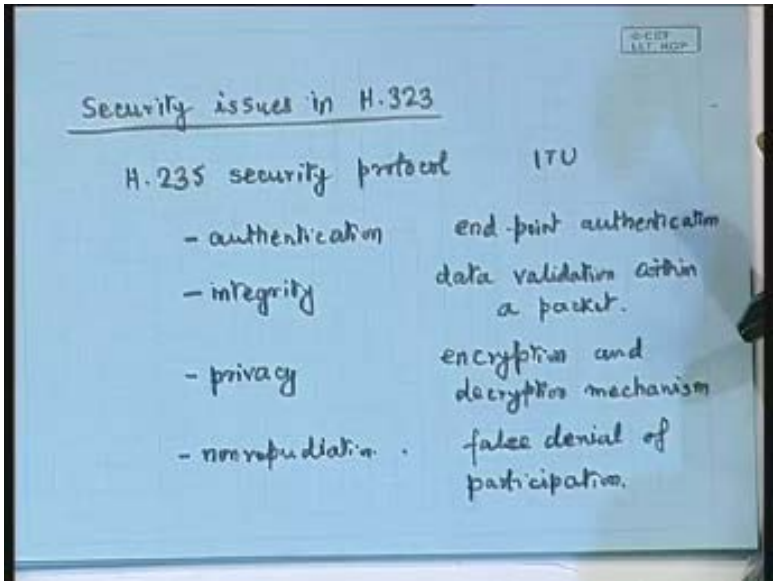
Now, also it is quite appropriate at this stage to talk about the security issues in H dot 323. In fact H dot 323 has got subset specifications which is referred to as the H dot 235 which is the security protocol. Again H dot 235 is the security protocol that is defined by the ITU. In fact you will find; from the name itself you will be able to make out that who are owning these standards because many-a-times the standards or the protocols they end with something PTCP/IP/RTP/UDP all these things are by the IETF Internet Engineering Task Forces whereas all these standards like G dot 729, G dot 728, H dot 261, H dot 263, 264 or yesterday what we learnt H dot 323 or the protocols like the H dot 320, 324 that is for the video conferencing. Everything is by the ITU and there are sometimes corresponding versions of protocols almost quite identical version of protocols where the names given by the IETF is different from that of the name that is given by the ITU.

So H dot 323 includes a separate security protocol subset and that subset is called as H dot 235 and this includes this H dot 235 security protocol includes four essential aspects. The first is what is called as the authentication. It is the user authentication that has to be done so essentially it is endpoint authentication. So the TE 1 and TE 2 that has to be authenticated that it is really registered to the network, they are valid users of the network they are paying for it or I mean, if it is a commercial network then they are paying for it or otherwise if it is a network that is there in some classified domain like say for example in defense or somewhere then also the validity should be there that it is a genuinely known user or approved users who are working.

Then the second security aspect is the integrity. Whatever data we send from the source to the destination, that has to be really validated. So there should be a data validation. because if you happen to an intruder and you corrupt the data there should be mechanism of detecting this; so data validation within a packet, so there should be some checks which should ensure that.

The third aspect is what is called as the privacy so that one cannot really look at the contents in an unauthorized way; like for any espionage or something that you would like to steal or you would like to snoop into others' private information, you want to know the credit card information when it is being transferred from one terminal to the other. So these are some of the things that should be prevented with the encryption and decryption mechanism. In fact it is there in the internet protocol and this protection should also be there in the VoIP because VoIP is also by no means has to be a secured communication because whatever you are speaking why should your privacy be affected, so encryption and decryption mechanism should be there.

(Refer Slide Time: 33:59)



Then the fourth aspect is prevention against what is called as the nonrepudiation. Nonrepudiation means that someone falsely denying that they participated in a conference. So it is false denial of participation. In fact, this could be there in situations like, say for example, there is some enquiry that whether a group of people they had a conference and then they plotted something plotted something mischievous and then if it is detected then it should not happen that after detection the denial..... that no no it is not we did it but there should be specific stamps which would show that yes these are the parties these are the TEs that were involved in the conferencing process.

Now all these security issues have to be built-in in no other place but the gatekeeper because all these protocols must reside in gatekeeper and that is why in the gatekeeper routed protocol it becomes absolutely essential that all these have to be all these signaling have to go through the gatekeeper.

Now the RAS, even the RAS channel that is used from the gateway to the gatekeeper that is also not a secured channel and that is why H dot 235 that has a gateway to check the authentication of the RAS message. Because before the RAS message is passed on; even the RAS message also has to be authenticated because it is not through the secured channel that goes on. So these are

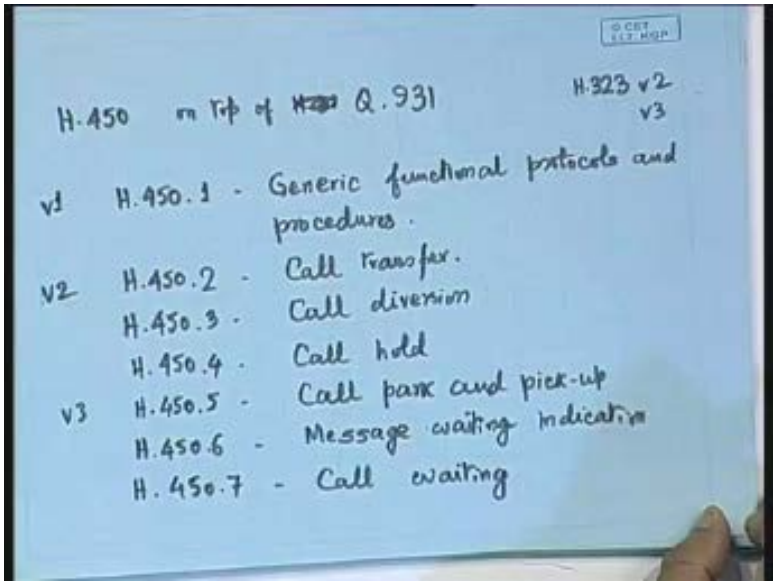
the security aspects which one should take into consideration and I should also talk about certain given..... all the good features of H dot 323.

The basic idea of H dot 323 should be to make it more and more popular and definitely its usage should be as much as that of the PSTN; eventually becoming more popular than PSTN because PSTN happens to be the circuit switched network and should be much costlier as we were mentioning in the earlier class.

Now the PSTN over the years has gone through several kinds of enhancements. Now you know that in the normal telephones you are getting..... I mean, with exchange provided services you are getting the caller identification; you know who is calling, you can have a call transfer facility, you can have a call divert facility that if you are not on this telephone and if you are somewhere else you can just divert your call to that particular number, so all these are some of the enhancement features that is already available in the PSTN. And the similar features should also be applicable or should also exist with the H dot 323 or in the VoIP domain.

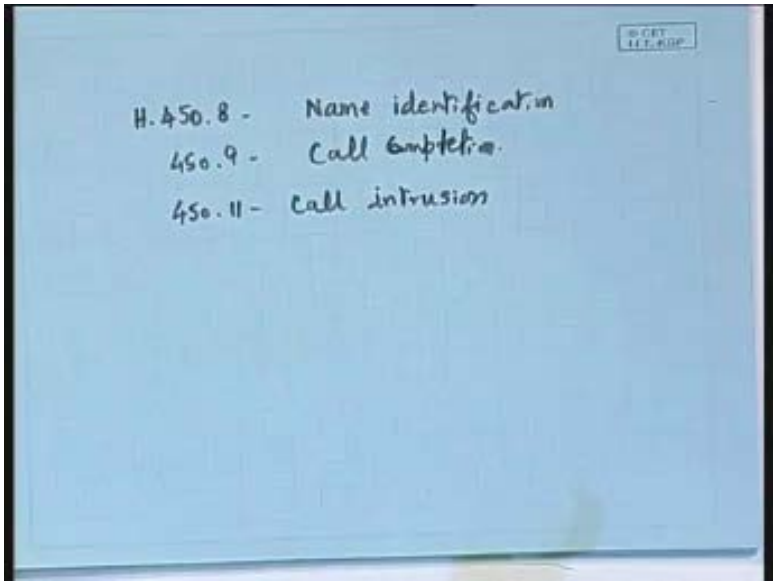
Now H dot 323 per say did not have any of these extension features, any of these enhancement features in what is called as the H dot 323 V 1 H dot 323 V 1. It is only some generic functional protocols and procedures between end-to-end. Because you see that for the terminals there should be some end-to-end signaling that we are talking of and these end-to-end signals functioning that should be defined and in fact all these generic functionals as well as the subsequent enhancements or enhanced capabilities instead of building them in the H dot 323, instead of incorporating H dot 323 into it what they did is to have another protocol called as H dot 450 which would reside on top of the H dot 323. So there should be another protocol called as H dot 450 which should sit on top of the H dot 323, so this is on top of H dot 323; or rather H dot 450 is a part of..... I mean, I should not say on top of H dot 323 but since it is all signaling enhancement so I should say that H dot 450 should be on top of Q dot 931 because Q dot 931 is the signaling protocol that is there in the H dot 323. So with the incorporation of H dot 450 on top of Q dot 931we can now go in for enhanced versions of H dot 323 and in fact we can go in for the version 2, version 3, version 4 and so on.

(Refer Slide Time: 41:52)



Now H dot 450 has got different sections into H. The H dot 450.1 that refers to the generic functional protocols and procedures, then H dot 450.2 this refers to the call transfer, then 450.3 that is call diversion which essentially refers to the call forwarding, then H dot 450.4 that refers to the call holding call hold and then H dot 450.5 that is called park and pickup and then H dot 450.6 that is a message waiting indication, 450.7 that is call waiting. Then actually this is supported in version 1. Version 1 only supports this, version 2 onwards supports this and I think this call park and pickup onwards these are things which are supported in version 3 and from the version 4 onwards we have some more enhancement capabilities; that is in 450.8 we have the name identification, 450.9 addresses the call completion call completion, 450.11 that refers to call intrusion and so on. These are just some of the enhancements that I just refer to; you do not have to remember everything; the whole idea is that just to tell you that there are certain capabilities, there are lot of enhancement capabilities which are there in H dot 450 which sits on top of Q dot 931 in order to have some enhanced facilities. It means whatever facilities are there in the PSTN phones should also exist with the VoIPs that is what was thought of.

(Refer Slide Time: 42:39)



Now, basically the inclusion of H dot 450 which was done at a later date not in the initial phase of the H dot 323 but it was added later on, a problem that was realized is that with these enhancement facilities is it that you are going to change all the terminal equipment; because the terminal equipment have been already there and users have spent money to buy those terminal equipment.

Now, if you give the enhanced facilities and say that no now have to change your terminal equipment, everything cannot be done; or writing a new standard and then changing the terminal equipment that is not something which is desirable or feasible always. So at least some of these facilities may not be things like the name identification and intrusion information where specifically then the handset has to contain those capabilities it must be having an LCD display, it must be having some particular form of messaging those things will be there. But at least many of these things like the call transfer, call diversion all these things should be possible with the gatekeeper. So there are many non H dot 450 enhancements which could be built into the gatekeeper software. That is why so that is what made the enhancements possible may be in a bit of cheaper way.

The enhancements are definitely making the VoIP a very popular thing. But I think what needs to be done is that is it as powerful as that of PSTN. Even if we include all these enhanced capabilities is not that the VoIP as of present has got lot of limitations. It is, mostly because, especially when I was talking to you about the third phase that means to say that where the carrier great telephony has to work with the VoIP there you would realize a major shortcoming and the primary shortcoming that you will come across is with the number of lines that can be catered for.

Now, today in exchanges, I mean, whenever you are having the circuit switch exchange there you can have a large number of lines, may be tens of thousands of lines which are catered for by the exchanges. But here it is only a few thousand or a fraction of few thousands which would be possible with the VoIP with H dot 323 as of present because one major shortcoming of H dot 323 is that, if you look at the block diagram, I think you would realize one major difficulty that we are putting excessive stress on the gateway because it is not..... I think yesterday we were having some discussions on this that it is not the simple gateway which we are using for just the IP interface from one LAN to the other that if the then only the protocol aspect is say taken care.

But in this case the gateway has to be an enhanced gateway because the gateway also has to work with the interworking; gateway also has to facilitate the interworking with the PSTN that is why lot of demands are put on to the gateway and the gateway is quite complicated; if you are realizing it by hardware it would involve large amount of hardware, also there will be considerable amount of software in the form of the implementation of the protocols which will be there. Therefore, doing everything in one box is indeed a problem that is going to be there with the gateways so there are some methodologies there are some schemes which should take care of this and make the H dot 323, its capabilities better.

And in fact this is what we will be seeing in the next class that how those efforts were taking place. In fact, we will come first to the structure of the gateway. We have been talking about the gateway but never seen the internal structure of it. We will see the structure of the gateway and then we ourselves we will realize the complication and then there must be some form of an

architectural change so that the gateways could be decentralized because at the moment there is too much of centralization with the gateways. So any form of a decentralized gateway should help in the scalability. We will talk about that in the next lecture, thank you.