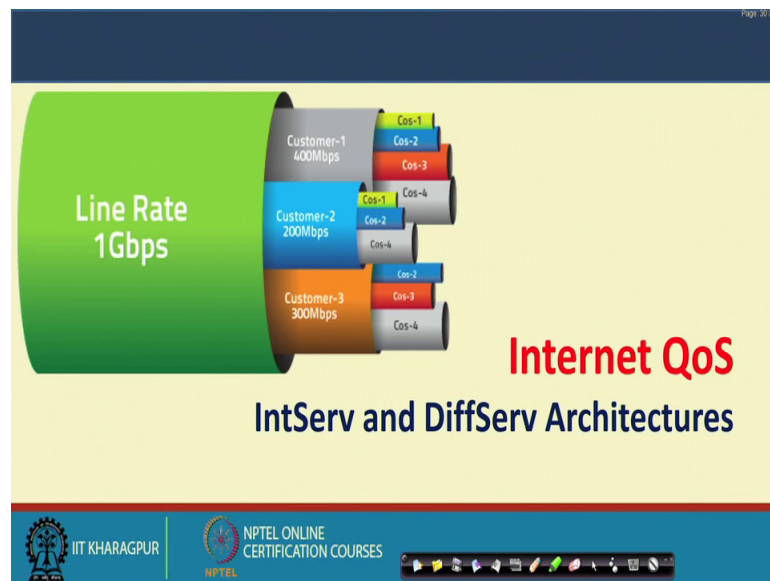


Computer Networks and Internet Protocol
Prof. Sandip Chakraborty
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 35
Internet QoS - V (Integrated and Differentiated Service Architecture)

Welcome back to the course on Computer Network and Internet Protocol.

(Refer Slide Time: 00:21)



So, today we are going to cover the last topic of Internet Quality of Service. So, we are going to talk about two specific quality of service architectures called integrated service architecture or IntServ architecture or that under differentiated service architecture or DiffServ architecture. So, in the beginning let me give you a brief idea about the differences between this IntServ and DiffServ architectures. So, we have two modes of services to provide quality of service over the internet.

So, the first mode of services, which we call as the guaranteed service, that is the integrated service architecture. So, the integrated service architecture what we try to do? We try to provide the kind of guaranteed service to the end users based on their service level agreement. So, what is mean by guaranteed service? Guaranteed service means if the service level agreement says that all of my packets should not get more delay than 10 millisecond. Then the network will ensure that all the packets of my which as coming

from my devices, they will get less than 30 millisecond of delay or the 10 milliseconds of delay that I have on my service level agreement.

So, that we call as a guaranteed service. Now, you see that for this kind of guaranteed service to or to support this kind of integrated service architecture, what you need to do? You need to ensure that every individual router in the network should take care of about your service level agreement. So, every individual router need to make an estimate whether it will be able to provide your service or they need to do a pre reservation of resources inside the routers, to ensure that that specific service level agreement is made.

Now to do that the routers need to coordinate with each other; because the packet is flowing to multiple routers whenever it is moving from one source to another destination and then individual routers need to coordinate with each other to reserve the resources for you such that it can guarantee the service that is promised to you. So, this particular architecture we call it as integrated service architecture. Now in this integrated service architecture the problem is that, this coordination among the routers. Now you think of the scale of the internet you have millions of routers and whenever you are transferring certain application then it need to pass a large number of routers there under the control of different service providers at different levels.

You have this star 0 ISP star, 1 ISP's the entire 2 ISP's the then the local ISP's. So, all these different service providers they need to coordinate with each other and the entire mechanism is very much complicated for this internet scale or internet level implementation. So, that is why we have a second class of quality of service, which does not give you guaranteed quality of service or which does not ensure that whatever the network service provider has promised to me in terms of service level agreement.

For a 100 percent times that will get executed, but what it tries to do? It tries its best to meet the service requirements. So, it is like that, if your network is too congested you cannot do anything in that case your packets will suffer, but if the network has a medium load, then it will provide you the required quality of service. Again the scenario come from the example of airport that security check scenario that if your airport is very much loaded to with the millions of passengers at the peak time then the security guards also cannot do anything.

So, what if you do you transfer some passengers from one queue to another queue it does not matter much. But whenever the load is high, but not very high during that time the security officials they tries to provide certain quality of service, if they finds out that will certain queue is growing longer, but in other queue there are remaining passengers.

So, they shift certain passengers, from one queue to another queue and it tries to provide you some level of quality of service based on the best that they can do. So, this kind of architecture we call it as a differentiated service architecture or DiffServ architecture. So, for internet scale implementation, DiffServ architecture is more suitable where you just try your best to provide the quality of service, but there is no guarantee that 100 percent of the time it will met the desired quality of service. So, we will look into this IntServ architecture and the DiffServ architecture in details.

(Refer Slide Time: 05:33)

Internet Service Architecture (ISA)

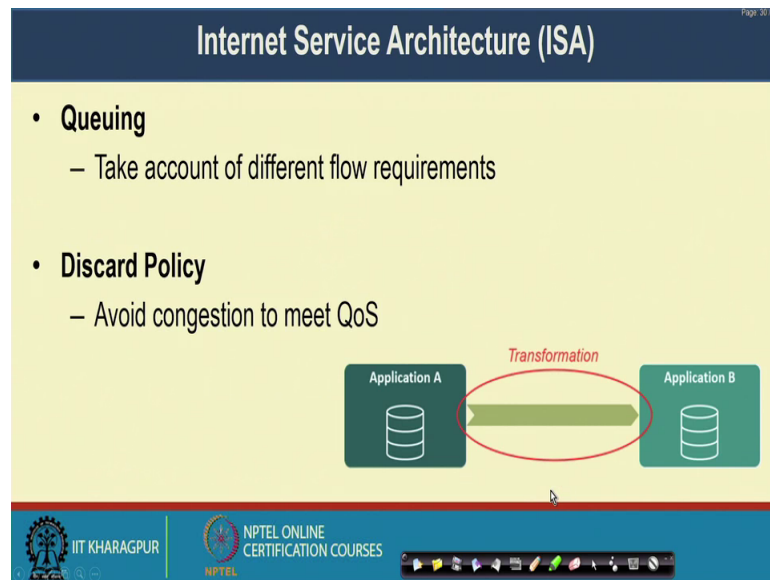
- Integrated Service (IntServ) QoS architecture over the Internet
- **Admission Control**
 - For QoS, reservation required for new flow
 - Resource Reservation Protocol (RSVP)
- **Routing Algorithm** - routing decision based on QoS parameters

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, first part of our journey with this integrated service architecture, to start with first let us look the service architecture principles in the internet, we call it the internet service architecture or ISA. So, this internet service architecture or ISA, it provides integrated service QoS architecture over the internet. So, it has few steps like the admission control. So, this admission control for quality of service you require reservation for the new flows, for that we run at something called the resource reservation protocol or RSVP, we will look into this RSVP in little more details. Then you have the routing control. So, you make the routing decision based on the quality of service parameters. So, you find out

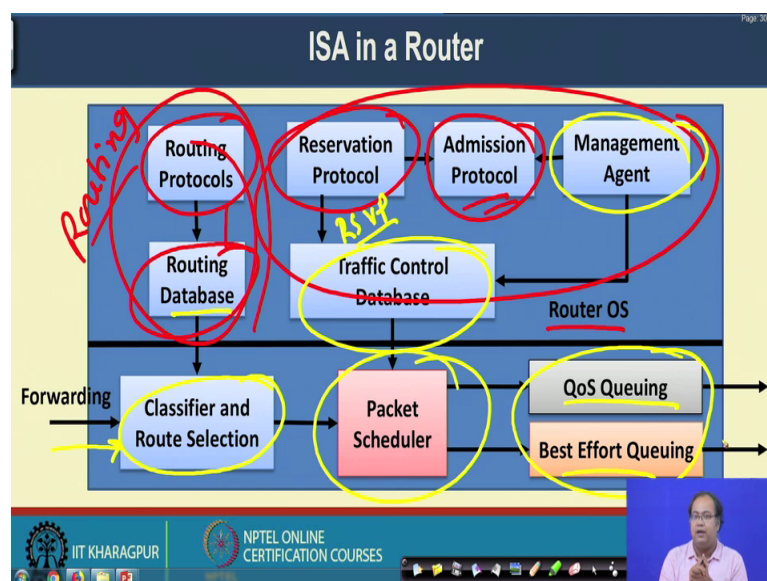
that whether a particular router is loaded if a particular router is loaded then you rather not route the packet to that router rather you route it to some alternate router. So, your routing algorithm is also depending on the depends on the quality of service parameters.

(Refer Slide Time: 06:35)



Then have the different kind of queuing strategies that we have already discussed in the last lecture, which takes account of different flow requirements. And finally, you have described policy like the congestion avoidance algorithm to meet the quality of required quality of service like the random early detection algorithm that we have discussed earlier.

(Refer Slide Time: 06:55)



So, this is this entire ISA architecture of ISA architecture that runs inside a router. So, if you look into this ISA architecture you have these routing protocols, which are finding out the routing parts and then you have the routing database and that is the routing part which is running inside your router operating system, and then you have this quality of service associated protocol.

So, this quality of service associated protocols, it has this admission control part, it has this admission protocol it ensures that the packet, which we are going inside the network the mixed the required quality of service. Say for example, whenever you are admitting a new flow in the network, then you need to ensure that the new flow get service from the internet or that it gets the required service from the internet.

If you do not able to ensure that the required flow get the required services from the internet, then you simply drop that particular flow. So, this particular thing possibly you have observed when making a voice call, sometime you have heard that a nice voice from a lady that all lines are busy please dial after some time. So, it is just like the network is not allowing you to get admitted in the network because it does not have sufficient amount of resources. So, that is the purpose of this admission control protocol.

Now, this admission control protocol get input from the reservation protocol. So, the reservation protocol actually reserves the resources in individual routers, through the RSVP protocol that we will look after a couple of slides. So, this RSVP protocol or the

resource reservation protocol, it ensures that the resource are getting reserved in individual routers in the into end path.

So, if you are not able to reserve any further resource, then the admission control we will deny or entry to the network. Then you have a management agent which manages different functionalities of the quality of service like this traffic shaping, traffic policing and all these aspects and then you have a traffic control database. So, this traffic control database actually tells you that how your packets need to be treated by the network.

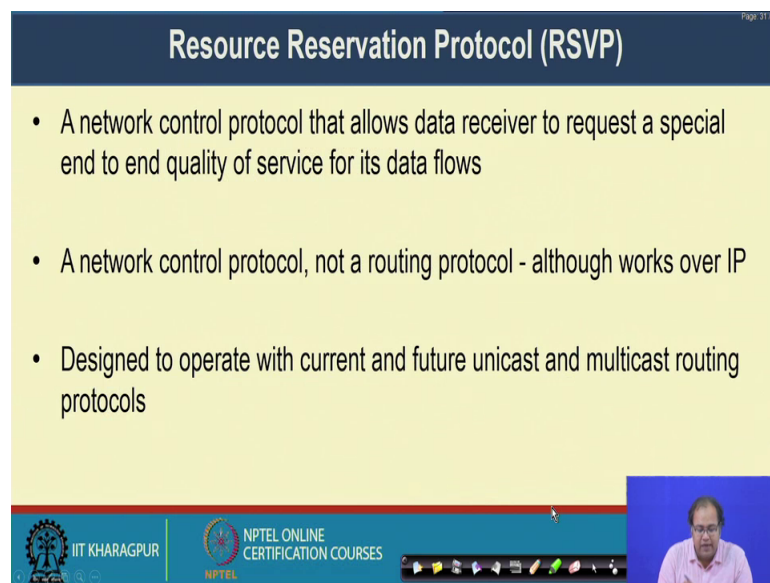
Now, let us come to the forwarding plane of the router. So, the forwarding plane whenever, you are getting a new packet then first you have this classified and the route selection. So, this classifier and the route selection mechanism it will classify your packets into one of the available traffic classes and then based on that it will select the route by looking into the routing database then comes your packet scheduler. So, this packet scheduler it will get input from this route information as well as from the traffic control database, that the how your packets need to be treated, and then it puts it in one of the queues.

So, either in the best effort queuing or you can have multiple queuing for the quality of service traffic. So, the queue is associated queuing then your scheduler is running which actually runs on this queues and transfer the packets based on one of the queuing policies. So, that it is the entire ISA implementation inside a router that, actually integrates the routing and quality of service together makes a integrated treatment over the packets which are coming from the end user applications.

(Refer Slide Time: 10:42)

Resource Reservation Protocol (RSVP)

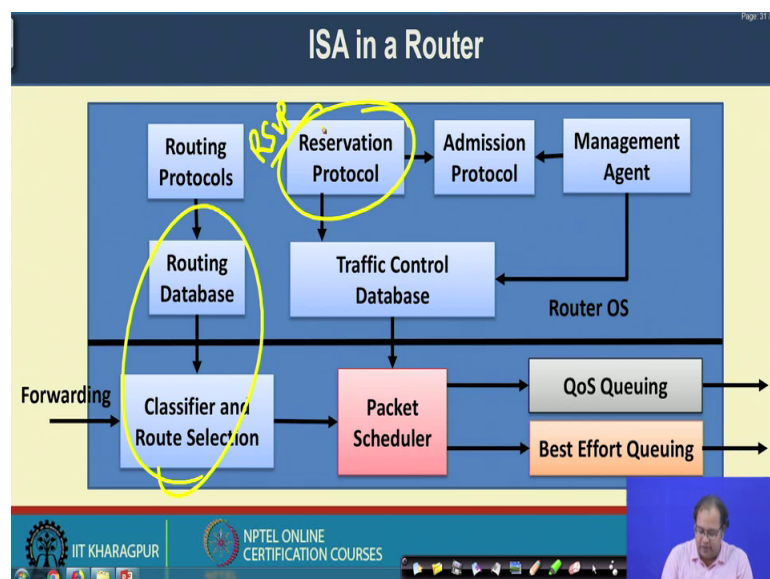
- A network control protocol that allows data receiver to request a special end to end quality of service for its data flows
- A network control protocol, not a routing protocol - although works over IP
- Designed to operate with current and future unicast and multicast routing protocols



The slide features a dark blue header with the title 'Resource Reservation Protocol (RSVP)'. Below the header, on a light yellow background, are three bullet points describing RSVP. At the bottom, there is a blue footer bar containing the IIT Kharagpur logo, the NPTEL logo, and the text 'NPTEL ONLINE CERTIFICATION COURSES'. A small video inset of a speaker is visible in the bottom right corner.

Now, let us first look into the resource reservation protocol. So, this resource reservation protocol or RSVP, is a network control protocol that allows data receiver to request a special end to end quality of service for its data flow. So, you require certain kind of special quality of service for your end to end flow, for that you apply this resource reservation protocol. Remember that RSVP is a network control protocol and it is not a routing protocol. It works with IP that is true, but it works in association with IP.

(Refer Slide Time: 11:17)



So, if you look into the earlier slide, we have the routing control protocol here, which takes care of your routing and then your reservation protocol the RSVP is running here, that takes care of this resource reservation and individual routers. So, it is not a routing protocol or a directive waste protocol which works in association with routing well.

(Refer Slide Time: 11:41)

Resource Reservation Protocol (RSVP)

- A network control protocol that allows data receiver to request a special end to end quality of service for its data flows
- A network control protocol, not a routing protocol - although works over IP
- Designed to operate with current and future unicast and multicast routing protocols



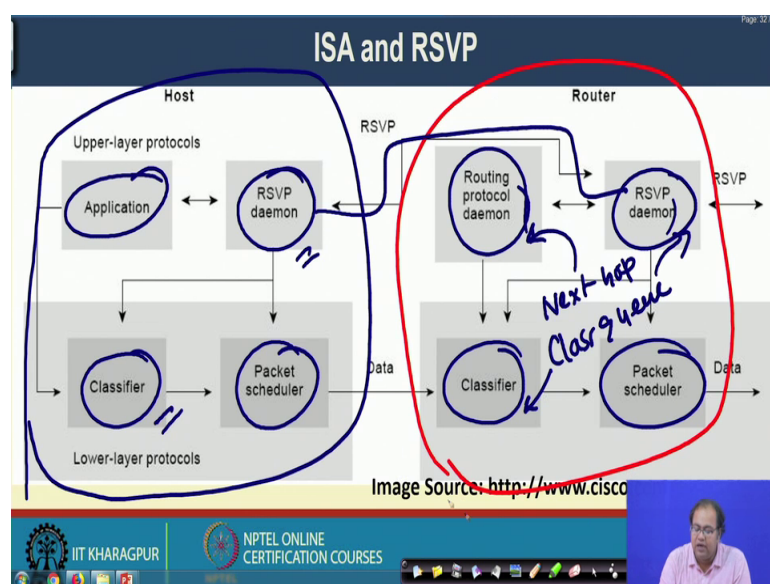
IIT KHARAGPUR

NPTEL ONLINE CERTIFICATION COURSES



So, it is designed to operate with current and future unicast and multicast routing protocols.

(Refer Slide Time: 11:49)



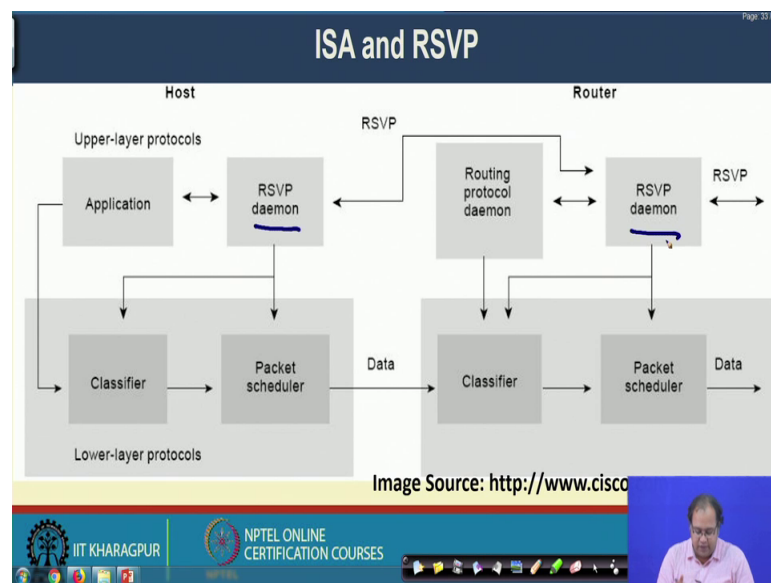
So, this is the architecture for integrated service architecture and RSVP together. So, we have just shown the instances of two different machines, the host machine and the router machine. So, the first one is so, this is at the host machine, the module which runs inside the host machine and these are the module which runs inside the router machine.

Now inside the host machine let us see the modules that we have. So, you have the applications which are running there, that application talks with the classifier, that classifiers your packet what type of quality of service classes that packets belongs to. And then you have a RSVP daemon that RSVP daemon actually runs in the host as well as in all the intermediate routers. So, this RSVP demons; so, you can see that these RSVP demons they talk with each other.

So, you have an arrow connecting the individual RSVP daemon. So, this RSVP daemon talk with each other and the reserve the resources for a particular flow inside, every routers the end to end path. So, it finds out whether it is able to resource the reserve or it will be able to reserve the resource for a particular flow. If it is able to reserve the resources, then it allows the flow through the admission control mechanism otherwise it simply drops that particular flow. Now you have that packet scheduler that works in cooperation with the classifier and the RSVP daemon, that talks about that what type of resources have been reserved for you, and accordingly the package scheduler schedule a packets into multiple queues.

Now again the similar thing happens here that you have the routing protocol daemon which is running inside the routers. So, this routing protocol daemon in association with RSVP daemon and the packet classifier, you decide the next stop which is coming from the routing part and your corresponding class queue, which is coming from this RSVP part RSVP under classifier part and in your packet scheduler will actually schedule your packet based on your next stop and class queue that is being determined. And then the packet will be sent to the next router, and in every router this particular thing will run. So, remember this important aspect of this RSVP daemon at both the host at all the intermediate router.

(Refer Slide Time: 14:15)



So, all the RSVP daemons and all the routers in the end to end path they need to coordinate with each other. And that is why the implementing in this integrated service architecture over the internet is a difficult thing, because you need a coordination among all the routers which is difficult to achieve for large scale internet. Well let us look into certain RSVP terminologies.

(Refer Slide Time: 14:39)

RSVP Terminologies

- Quality of Service is implemented for a particular data flow by a mechanism called "traffic control"
- **Packet Classifier:** Determines the QoS
- **Packet Scheduler:** Link layer dependent mechanism to determine which particular packets are forwarded
 - For each outgoing interface, the scheduler achieves the desired QoS.

So, quality of service is implemented for a particular data flow by a mechanism that we call as a traffic control and RSVP; we have the packet classifier that determines the

quality of service level, and the packet scheduler that link layer dependent mechanism to determine which particular packets are forwarded. Now for each outgoing interface the scheduler achieve the desired quality of service.

So, if you look into a router perspective you can have multiple outgoing interfaces, like eth 0 eth 1 eth 2 eth 3 and so, on. So, these are the different outgoing interfaces for a router, now for every individual outgoing interface I need to maintain these multiple queues. Because you remember that these queues are specific to outgoing interface. So, with this outgoing and interface possibly another router this is connected. So, that is why for every interface, you need to apply this queuing mechanism.

So, the routing algorithm will take tell you that in which outgoing interface the packet need to be forwarded to and then in that particular outgoing interface you would on the queuing mechanism to serve the packets to serve all the packets, which need to be forwarded to that particular interface.

(Refer Slide Time: 16:01)

The slide is titled "RSVP Reservation Procedure" in a dark blue header. The main content area is yellow and contains three bullet points. The first bullet point states: "During reservation setup, an RSVP QoS request is passed to two local decision modules: 1. Admission control 2. Policy control." The second bullet point states: "Admission Control: Determines whether the node has sufficient available resources to supply the requested resources." The third bullet point states: "Policy Control: Determines whether the user has administrative permission to make the reservation." The word "SLA" is handwritten in blue ink above the third bullet point. In the bottom right corner, there is a small video inset showing a man in a pink shirt. The bottom of the slide features a blue footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a navigation bar.

RSVP Reservation Procedure

- During reservation setup, an RSVP QoS request is passed to two local decision modules: 1. Admission control 2. Policy control.
- **Admission Control:** Determines whether the node has sufficient available resources to supply the requested resources.
- **Policy Control:** Determines whether the user has administrative permission to make the reservation.

SLA

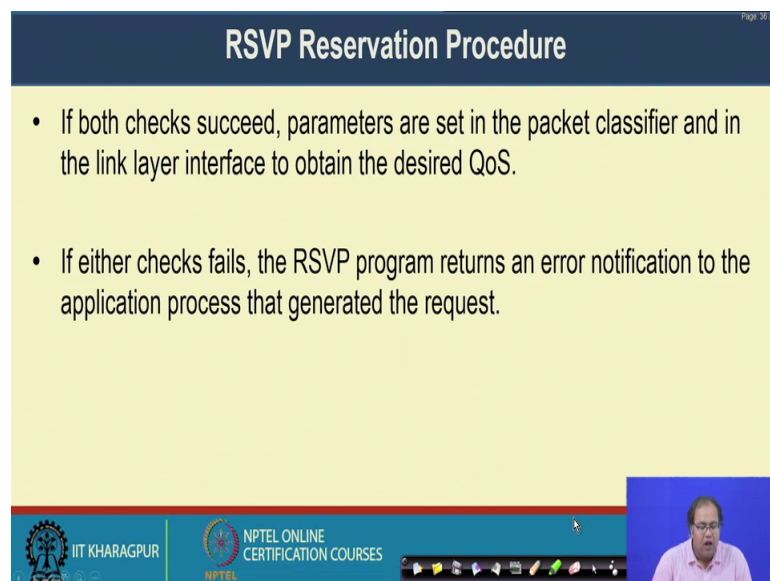
IIT KHARAGPUR NPTEL ONLINE CERTIFICATION COURSES

Now this is the reservation procedure for RSVP during the reservation setup, first we send. An RSVP QoS request which is passed to two local decision module the decision modules are the admission control module and the policy control module; now that admission control module it determines whether the node has sufficient available resources to supply for the requested resources.

If you have sufficient amount of resources, then you allow the flow to enter in the network, otherwise you simply drop the flow. Then you have the policy control module this policy control module determines whether the user has administrative permission to make the reservation.

Now that is an important aspect in the internet scale, say for example, you have not made the specific service level agreement; in that case even if you are trying to send some voiceover IP packet, that voice over IP packets will be treated as a best effort packet not as an high priority packet. So, that is why you need to make at the corresponding service level agreement with the network service provider, before sending any quality of service associated packet. So, this policy control actually comes from the service level agreement, that talks about whether the user is actually have sufficient administrative privilege to mark its packet as a high priority packet or not.

(Refer Slide Time: 17:23)



RSVP Reservation Procedure

- If both checks succeed, parameters are set in the packet classifier and in the link layer interface to obtain the desired QoS.
- If either checks fails, the RSVP program returns an error notification to the application process that generated the request.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, if this both checks succeed then the parameters are set in the packet classifier, and in the link layer interface to obtain the desired level of quality of service. If either of the check fails like either your admission control check fails or the policy control check fails, then the RSVP program returns an error notification to the application process that generated the request that you are not allowed to send this packet over the internet with this quality of service which you are claiming.

(Refer Slide Time: 17:55)

RSVP Reservation Model

- An RSVP request consists of : flowspec together with a filterspec. This pair is called the "flow descriptor".
- The flowspec specifies a desired QoS.
- The filterspec together with the session specification defines the set of data packets.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, let us look into the reservation model in RSVP how RSVP does the reservation. So, a RSVP request it consists of two part; one thing we call as the flowspec and another thing we call as the filterspec. So, this pair is known as the flow descriptor. So, this flowspec it specifies the desired level of quality of service. So, what type of quality of service you are expecting from the end user?

And the filterspec together with the session specification defines the set of data packets like this filter spec actually talks about that what type of queuing mechanism you want to implement on your packet. Whether you want to go for priority queuing or a custom queuing or a weighted fair queuing or whatever other queuing mechanisms that we have to provide the internet quality of service.

(Refer Slide Time: 18:50)

RSVP Reservation Model

- The flowspec is used to set parameters in the packet scheduler, while the filterspec is used to set parameters in the packet classifier
- The flowspec in a reservation request will generally include a service class and two sets of numeric parameters:
 - Rspec - defines the desired QoS,
 - Tspec - describes the data flow.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, this flowspec it is used to set the parameters in the packet scheduler, while as the filterspec it is used to set the parameter in the packet classifier. So, based on the filterspec you actually filter out the packets that is why the name filterspec. So, it is put in the packet classifier to classify the packets, and then design that or put that packet associated with different type of queues that you have to provide quality of service.

And the flowspec it is used to set up parameters in the packet scheduler that, what would be the individual parameters to setting up the queues. Now this flowspec it is a reservation request it generally includes a service class and two sets of numeric parameter. So, one is called the Rspec another one is called the Tspec. So, this Rspec defines the desired quality of service and the Tspec defines the data flow that which particular packets of a flow you are going to consider.

(Refer Slide Time: 19:48)

flowspec Structure

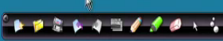
```
typedef struct flowspec {
    ULONG TokenRate;
    ULONG TokenBucketSize;
    ULONG PeakBandwidth;
    ULONG Latency;
    ULONG DelayVariation;
    SVCETYPE ServiceType;
    ULONG MaxSduSize;
    ULONG MinimumPolicedSize;
} FLOWSPEC, *PFLOWSPEC, *LPFLOWSPEC;
```



IIT KHARAGPUR



NPTEL ONLINE
CERTIFICATION COURSES



So, here is a flow spec structure. So, you can see that it contains multiple parameters like this token rate token bucket size the peak bandwidth latency.

(Refer Slide Time: 19:57)

flowspec Structure

```
typedef struct flowspec {
    ULONG TokenRate;
    ULONG TokenBucketSize;
    ULONG PeakBandwidth;
    ULONG Latency;
    ULONG DelayVariation;
    SVCETYPE ServiceType;
    ULONG MaxSduSize;
    ULONG MinimumPolicedSize
} FLOWSPEC, *PFLOWSPEC, *LPFI
```



IIT KHARAGPUR



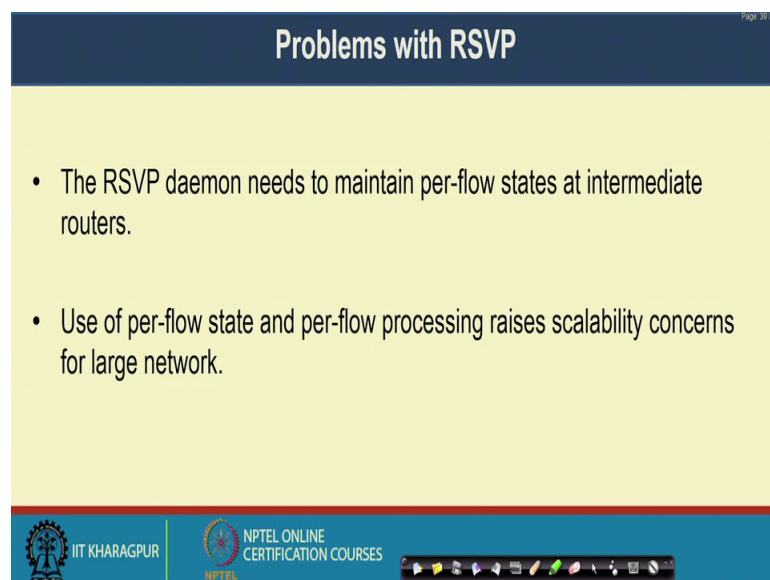
NPTEL ONLINE
CERTIFICATION COURSES

So, it is token rate token bucket size they are kind of are belongs to the Rspec that talks about the scheduler parameters whereas, the peak bandwidth latency delay variation, all these things they talk about flow specific parameters the maximum Sdu size minimum policy size.

So, they belong to the Tspec bit of this flow spec. So, this flow specifies all these numeric values, which actually determine your corresponding service level agreement. So, based on the flow spec you determined that what level of quality of service you want to provide to a particular user, then you control or you configure the intermediate routing queues based on these particular parameters.

Whereas, in case of filterspec you are actually marking the packet classifier or you are configuring the packet classifier, to say that well this particular user, may generate via traffic video on demand traffic and the best effort traffic as per it is a service level agreement that the traffic classifier needs to take care of.

(Refer Slide Time: 21:15)



Problems with RSVP

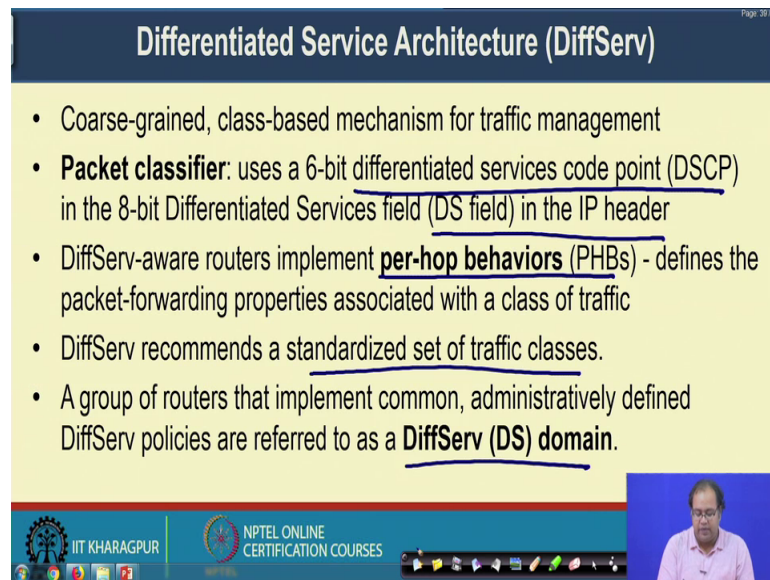
- The RSVP daemon needs to maintain per-flow states at intermediate routers.
- Use of per-flow state and per-flow processing raises scalability concerns for large network.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

So, the problems which are associated with RSVP there are major two problems that I have already pointed out that the RSVP daemon needs to maintain per-flow states at intermediate routers, because the RSVP daemon needs to maintain per-flow states at intermediate routers it is a heavy process.

So, use of this per-flow state and per-flow processing, it raises the scalability concerns over a large network. And that is why from the integrated service architecture we move towards the differentiated service architecture or DiffServ architecture.

(Refer Slide Time: 21:46)



Differentiated Service Architecture (DiffServ)

- Coarse-grained, class-based mechanism for traffic management
- **Packet classifier**: uses a 6-bit differentiated services code point (DSCP) in the 8-bit Differentiated Services field (DS field) in the IP header
- DiffServ-aware routers implement **per-hop behaviors (PHBs)** - defines the packet-forwarding properties associated with a class of traffic
- DiffServ recommends a **standardized set of traffic classes**.
- A group of routers that implement common, administratively defined DiffServ policies are referred to as a **DiffServ (DS) domain**.

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Page 30/30

So, this differentiated service architecture or the DiffServ architecture it is a coarse grained, class based mechanism for traffic management. It has a packet classifier which uses a six bit differentiated service coat point field or the DSCP field. So, this DSCP field which indicates that in which particular traffic class it belongs to. So, remember in case of your integrated service architecture, the black packet classifier or the classifier classes are not fixed or predetermined, it can be user based or it can vary from user to user and that is why we are using filterspec to inform the classifier that what different type of packet classes can belong to a particular user.

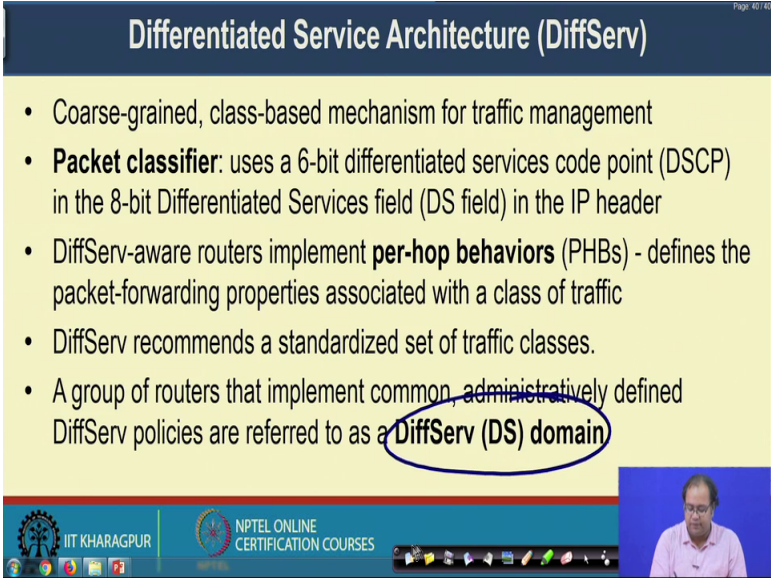
But in case of differentiated service architecture, we do not have that level of flexibility we do not have this kind of user specific quality of services that, rather network wide we have some fixed classes of services; and those fixed classes of services are determined by this DSCP field. So, DSCP field is included inside the eight bit differentiated service field the DS field inside the IP header.

So, in the IP header itself we will find out this DS field which contains the DSCP field and that DSCP field, determines the fixed traffic classes that the differentiated service architecture can support. So, that is the difference a major difference between the integrated service architecture and the differentiated service architecture and that is why this kind of filterspec model it is not required in case of DiffServ architecture.

Because your traffic classes are fixed and that is why your classifier has a fixed behaviour, rather than a user specific behaviour. In case of your integrated service architecture you had this user specific behaviour, and that is why you had the requirement of the filterspec to configure the traffic classifier. Now, DiffServ aware routers implement something called a per hop behaviour. So, this per hop behaviour defines the packet forwarding properties associated with that class of traffic.

So, how the packets will be forwarded for DiffServ aware routers; now DiffServ recommends standardised set of traffic classes that I have mentioned it has standardized and fixed set of traffic classes. Now, a group of routers that implement a common administratively defined DiffServ policies we are referred what DiffServ domain. So, we will implement differentiated service architecture over a DiffServ domain.

(Refer Slide Time: 24:19)



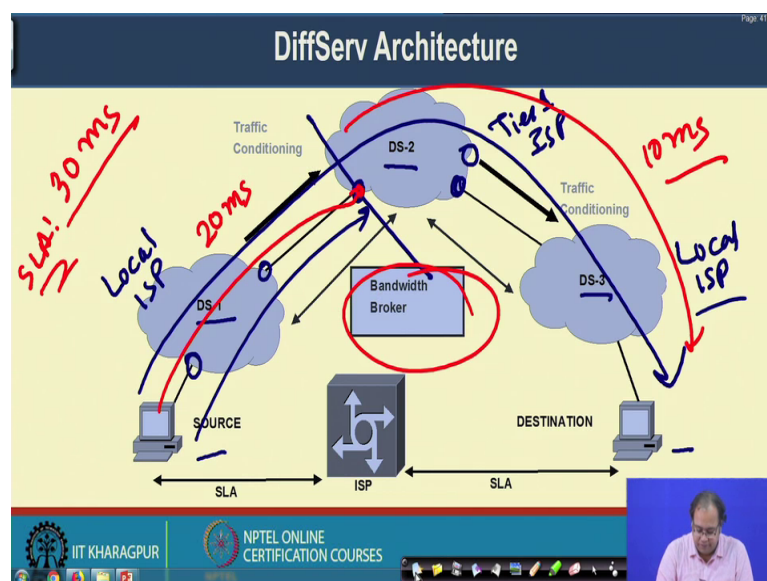
Differentiated Service Architecture (DiffServ)

- Coarse-grained, class-based mechanism for traffic management
- **Packet classifier**: uses a 6-bit differentiated services code point (DSCP) in the 8-bit Differentiated Services field (DS field) in the IP header
- DiffServ-aware routers implement **per-hop behaviors** (PHBs) - defines the packet-forwarding properties associated with a class of traffic
- DiffServ recommends a standardized set of traffic classes.
- A group of routers that implement common, administratively defined DiffServ policies are referred to as a **DiffServ (DS) domain**

The slide includes a footer with logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES, along with a video inset of a man in a pink shirt speaking.

Now, this is the architecture of DiffServ.

(Refer Slide Time: 24:21)



You have multiple DiffServ domains DiffServ 1, domain DiffServ domain 1 DiffServ domain 2 and DiffServ domain 3, now whenever you are transferring a packet from a source to a destination it need to go through these three DiffServ domains. Now when it needs to go through these three DiffServ domain, what we do that? We will look into these intermediate routers at the edge routers. So, the idea of this differentiated service architecture is something like this, that whenever you are entering a packet to one DiffServ domain, what you try to do you try to make an estimation about what is the end to end quality of service requirement, and how much quality of service it has already obtained.

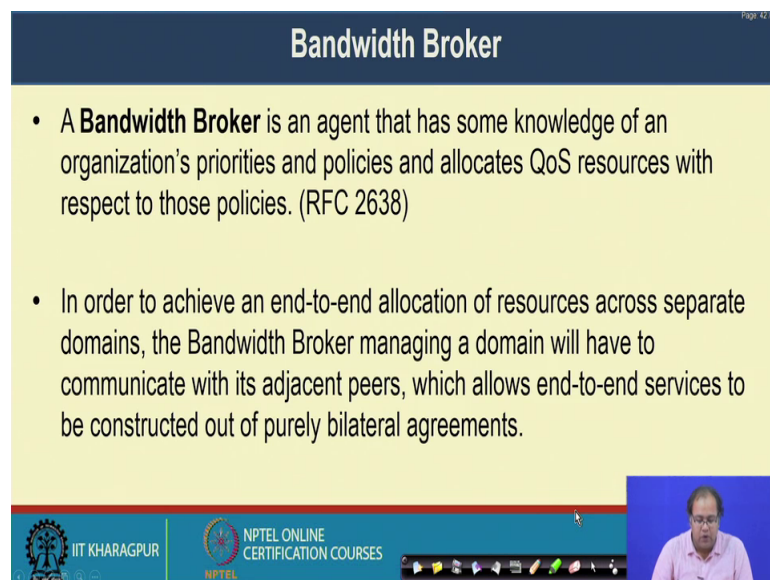
Now remember this individual DiffServ domains can be like different service providers, which are there in the internet. So, whenever. So, it may happen that this is a local ISP this is say a tier 1 ISP, and this is again a local ISP. Now, whenever the packet is going through this star 1 ISP, that this DiffServ domain actually looks into that what is my end to end service level agreement. And how much serviced a packet from these sources already received; say for at this point say my end to end delay need to be 30 millisecond, that is written inside.

The service level agreement and what we see here that when in the packet reaches here, it has already received 20 milliseconds of delay. From the source to da 1; that means, from this DS 2 to DS 3 and final destination you have to transfer the packet within 10

millisecond, to meet the required service level agreement. Now based on this differentiated service architecture actually takes the decision about how to treat the packet for this particular flow.

To do this it actually have a coordination among other DiffServ domain remember that unlike other integrated service architecture the things that, we have done we required a coordination among all the routers, here we do not required a coordination among all the routers we just required a coordination among all the DiffServ domains, and that is done by this bandwidth broker ok.

(Refer Slide Time: 26:54)



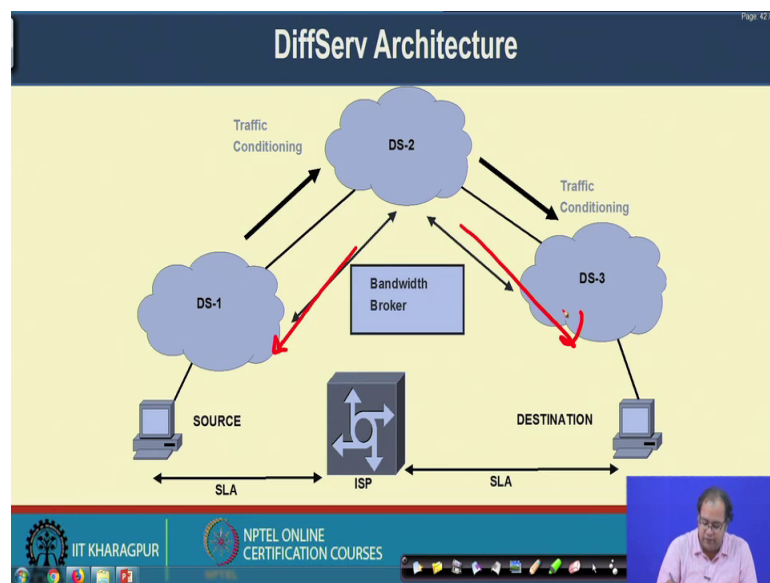
Bandwidth Broker

- A **Bandwidth Broker** is an agent that has some knowledge of an organization's priorities and policies and allocates QoS resources with respect to those policies. (RFC 2638)
- In order to achieve an end-to-end allocation of resources across separate domains, the Bandwidth Broker managing a domain will have to communicate with its adjacent peers, which allows end-to-end services to be constructed out of purely bilateral agreements.

The slide footer includes the IIT Kharagpur logo, NPTEL ONLINE CERTIFICATION COURSES text, and a video inset of a man in a pink shirt speaking.

So, the bandwidth broker is an agent that has some knowledge of an organizations priorities and policies, and allocates quality of service resources with respect to those policies as per the definition bandwidth broker given in RFC 2638. Now in order to achieve an end to end the allocation of resources across separate domains that indeed broker managing a domain we will have to communicate with its adjacent pairs.

(Refer Slide Time: 27:22)



So, here in the earlier picture this bandwidth broker running at the s two it need to communicate with the bandwidth broker DS 1 and bandwidth broker DS 3, to determine that what level of quality of service can be given to a particular flow.

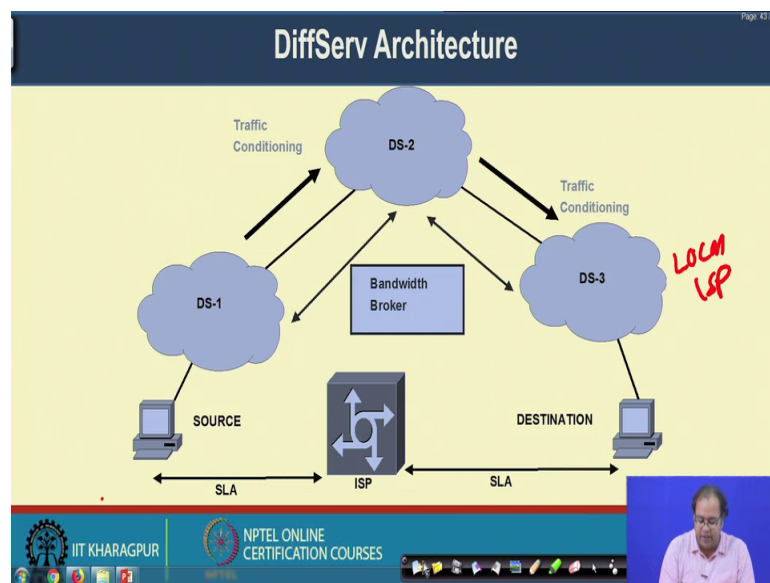
(Refer Slide Time: 27:37)

Bandwidth Broker

- A **Bandwidth Broker** is an agent that has some knowledge of an organization's priorities and policies and allocates QoS resources with respect to those policies. (RFC 2638)
- In order to achieve an end-to-end allocation of resources across separate domains, the Bandwidth Broker managing a domain will have to communicate with its adjacent peers, which allows end-to-end services to be constructed out of purely bilateral agreements.

Have to communicate with this the adjacent pairs, which allows end to end services to be constructed out of purely bilateral agreement. So, remember that it is a kind of pure bilateral agreement. So, you can and why we call it as a best effort service and not a guaranteed service, again coming back to the previous picture.

(Refer Slide Time: 27:57)



That it may happen that this particular service domain or this particular local ISP, it does not have a pairing relationship with this tier 1 ISP. So, it does not have any agreement with DS 2 in terms of this quality of service in that case, it will not be able to provide that end to end quality of service. So, now we are giving the flexibility at the ISP levels that individual ISPs can ensure the pairing with or quality of service associated pairing with the neighbours and can take the decision accordingly. So, that is the task of the bandwidth broker, these sets of this kind of pairing relationships.

(Refer Slide Time: 28:43)

SLA and TCA

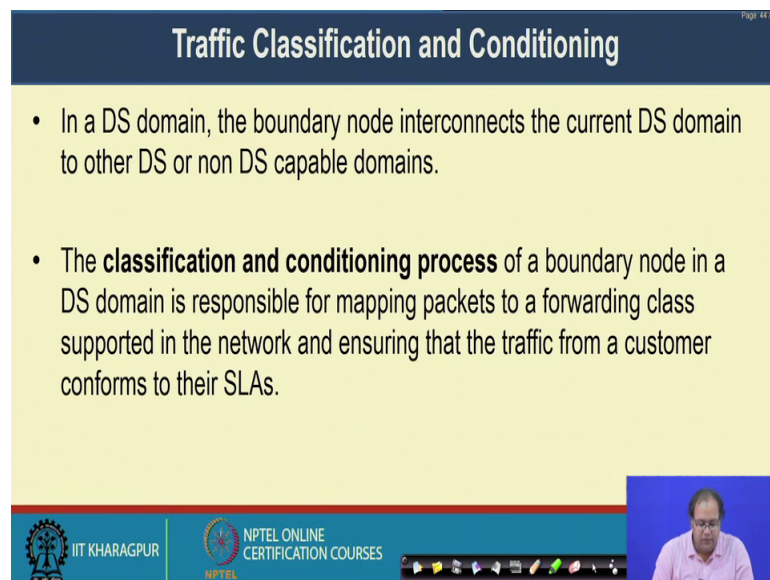
- **Service Level Agreement (SLA):** A set of parameters and their values which together define the service offered to a traffic stream by a differentiated service (DS) domain.
- **Traffic Conditioning Agreement (TCA):** A set of parameters and their values which together specify a set of classifier rules and traffic profile.

The slide footer includes IIT KHARAGPUR, NPTEL ONLINE CERTIFICATION COURSES, and a small video feed of a presenter.

So, the service level agreement; so, we have two type of agreement in DiffServ architecture, one is called a service level agreement which is a set of parameters and their values which together define the service order to a traffic stream by a DS domain. And the traffic conditioning agreement is a set up parameters and their values which together specify a set of classifier rules and traffic profile. So, this traffic condition agreement actually is an agreement which says. So, that see I have this fixed set of classes and your packet will belong to one of these fixed set of classes.

So, tell me that in which fixed set of classes you want to purchase. So, if you say that I want to purchase class 1 you have to pay more money, if you say that I want to passes class to service you have to pay little less money and so, on. So, that we call as the traffic conditioning agreement and the service conditioning agreement or the service level agreement is that well I am purchasing that class one my traffic is in class 1. But in class one traffic you should give little more priority to my traffic, because I am going to use a via services. So, it is just like multi class of via services one is ensuring a perfect QoS here is another one is ensuring some compromised QoS.

(Refer Slide Time: 29:54)



The slide is titled "Traffic Classification and Conditioning" in a dark blue header. The main content area is yellow and contains two bullet points. The first bullet point states: "In a DS domain, the boundary node interconnects the current DS domain to other DS or non DS capable domains." The second bullet point states: "The **classification and conditioning process** of a boundary node in a DS domain is responsible for mapping packets to a forwarding class supported in the network and ensuring that the traffic from a customer conforms to their SLAs." In the bottom right corner, there is a small video inset showing a man in a pink shirt. The bottom of the slide features a blue footer with the IIT Kharagpur logo, the text "NPTEL ONLINE CERTIFICATION COURSES", and a row of navigation icons.

Traffic Classification and Conditioning

- In a DS domain, the boundary node interconnects the current DS domain to other DS or non DS capable domains.
- The **classification and conditioning process** of a boundary node in a DS domain is responsible for mapping packets to a forwarding class supported in the network and ensuring that the traffic from a customer conforms to their SLAs.

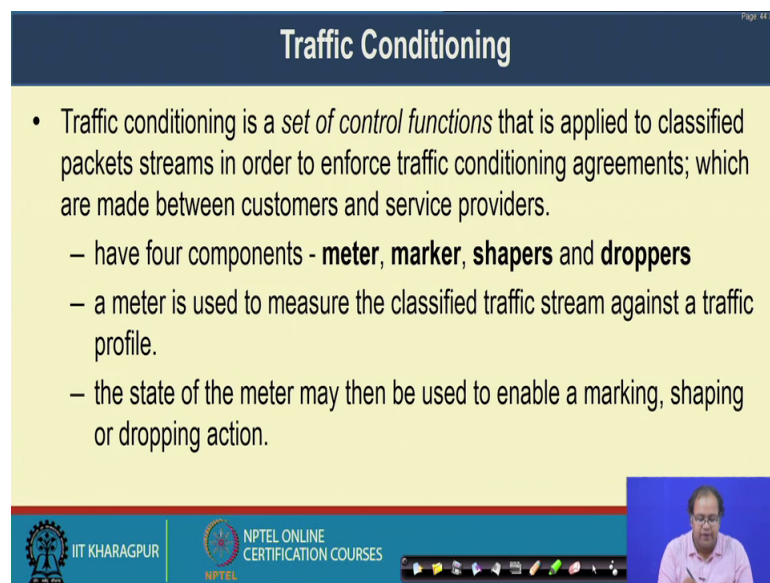
IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now in a DS domain the boundary nodes or the border nodes, they interconnects the current DS domain to other DS remain or non capability DS domain, we call them as the boundary nodes or the edge nodes. The classification and conditioning process of a

boundary node in a DS domain it is responsible for mapping packets to a forwarding class.

Supported in a network and ensuring that the traffic from a customer confirms to get service level agreement. So, that are done by the classification and the conditioning process, which is running in a boundary node.

(Refer Slide Time: 30:28)



Traffic Conditioning

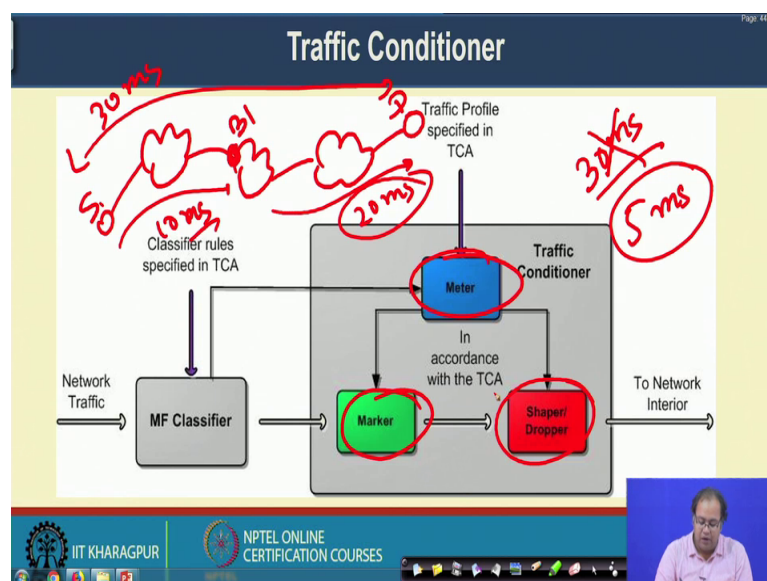
- Traffic conditioning is a *set of control functions* that is applied to classified packets streams in order to enforce traffic conditioning agreements; which are made between customers and service providers.
 - have four components - **meter**, **marker**, **shapers** and **droppers**
 - a meter is used to measure the classified traffic stream against a traffic profile.
 - the state of the meter may then be used to enable a marking, shaping or dropping action.

The slide footer includes the IIT KHARAGPUR logo, NPTEL ONLINE CERTIFICATION COURSES text, and a small video inset of a man speaking.

Now, the traffic conditioning it is a set of control functions, that is applied to a classified packets stream in order to enforce traffic conditioning agreements like, how your packet need to be treated which are made between the customers and the service provider. So, it has four components meter marker shaper dropper now a meter is used to measure the classified traffic stream again the traffic profile, that you need, a meter is basically used to estimate that how much quality of service you have already got and what is the level of quality of service that you have to give to whenever you are going to the next DS domain.

And the state of the meter may then be used to enable a marking; that means, classifying your packet in one of the service classes shaping or dropping the action.

(Refer Slide Time: 31:15)



So, here is the idea. So, you have a classifier from that classifier it is coming to the marker, now the marker make an estimate say your packet is from the source it is going to one DS domain then another DS domain then the third DS domain and finally, the destination. Now when the packet is reaching to say this boundary node say B 1, it runs its meter this meter module to find out that if you have a end to end 30 millisecond of delay requirement, what is the amount delay the packet has already achieved say at the packet has already achieved, 10 millisecond delay.

Now it needs to find out that well the packet has already achieved 10 milliseconds of delay. So, I have to transfer the packet within 20 millisecond. Now let us look into this packet status in compared to other packets which are already in my interface queue, if you can find out that well the other packets need to be transferred we did not say average delay of 30 millisecond, but this packet need to be translated within 20 millisecond then we increase the priority of that packet.

But if you see that the other packets need to be transferred in 5 millisecond and this packet need to be transferred into 30 millisecond then you reduce its priority. So, that way the priority is dynamically assigned, by the marker and that priority assignment is done by this marker module. And accordingly you include the traffic shaper a dropper which we will shape your traffic or drop your traffic or apply certain kind of scheduling policy to ensure the quality of service requirements.

(Refer Slide Time: 32:53)

The slide is titled "Classification and Marking - Per Hop Behaviors (PHB)". It lists four types of PHBs:

- **Default PHB** - for best-effort services
- **Expedited Forwarding (EF) PHB** - dedicated to low-loss, low-latency traffic
- **Assured Forwarding (AF) PHB** - gives assurance of delivery under prescribed conditions (different queuing behaviors)
- **Class Selector PHBs** - which maintain backward compatibility with the IP Precedence field.

Handwritten red notes on the slide include:

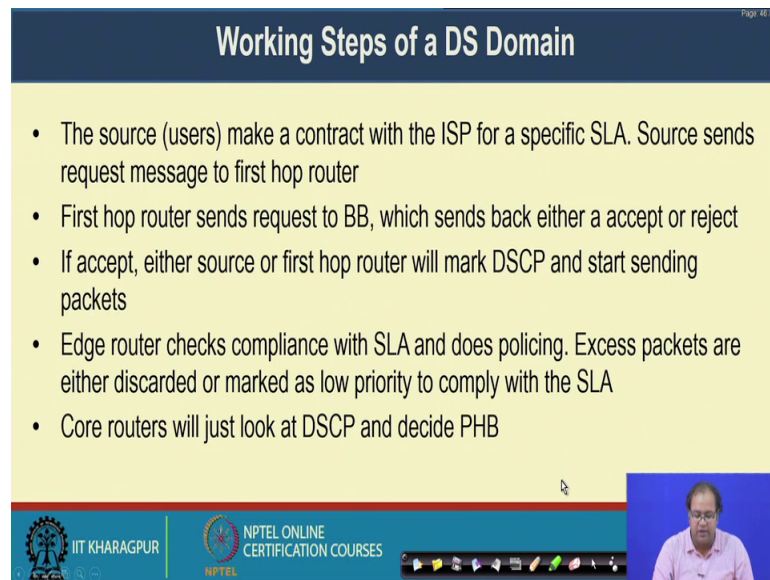
- Arrows pointing to "Default PHB" and "Expedited Forwarding (EF) PHB" with the text "Priority queue".
- An arrow pointing to "Assured Forwarding (AF) PHB" with the text "Custom queue".
- An arrow pointing to "Class Selector PHBs" with the text "WFB" (likely referring to Weighted Fair Queuing).

The slide footer includes the IIT Kharagpur logo, the text "NPTEL ONLINE CERTIFICATION COURSES", and a small video inset of a speaker.

So, this classification and marking there the per hop behaviours; so, we have four different type of per hop behaviours, the default per hop is to provide best effort service by expedited forwarding or EF PHB to which is to give priority, to the low loss low latency traffic. Assured forwarding per hop behaviour it gives assuring to delivery under prescribed condition like you require some fixed amount of bandwidth for that particular application, then you go for assured forwarding which can be implemented with the help of a custom queuing.

The expedited forwarding on the other hand can be implemented inside the priority queuing. So, you can apply a priority queue for this, and the custom queue for this. And you can have certain class based selector per hop behaviour which maintains backward compatibility with the IP precedence field. So, something like you can use weighted fair queuing to ensure the fairness.

(Refer Slide Time: 33:53)



Working Steps of a DS Domain

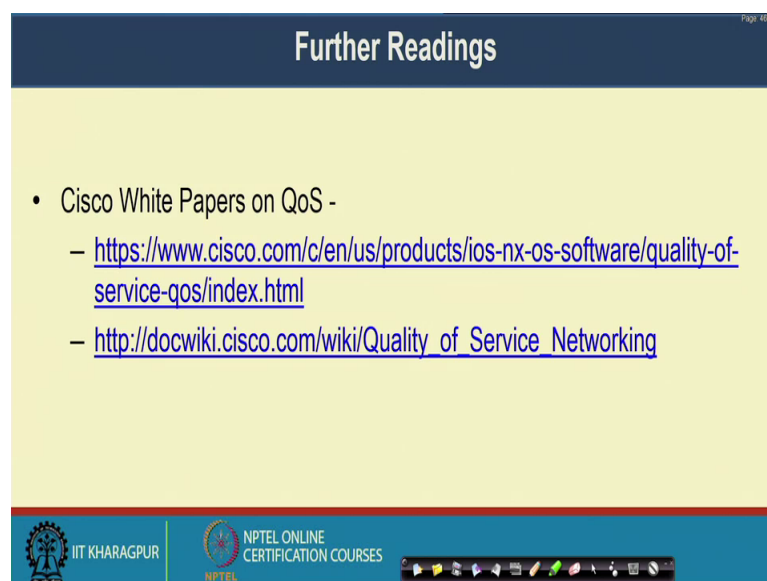
- The source (users) make a contract with the ISP for a specific SLA. Source sends request message to first hop router
- First hop router sends request to BB, which sends back either a accept or reject
- If accept, either source or first hop router will mark DSCP and start sending packets
- Edge router checks compliance with SLA and does policing. Excess packets are either discarded or marked as low priority to comply with the SLA
- Core routers will just look at DSCP and decide PHB

The slide includes logos for IIT KHARAGPUR and NPTEL ONLINE CERTIFICATION COURSES at the bottom. A small video inset in the bottom right corner shows a man speaking.

These are the working steps of a DS domain the source or the users it make a contact with contract with the ISP for a specific service level agreement. The source sends a request message to the first hop router, then the first hop router sends the request to the bandwidth broker, which send backs either accept or reject based on whether the bandwidth can be whether the SLA can be ensured, in delivering the packet. If it is accepted then either the source or the fist hop router will mark the DSCP field, and start sending the packet.

And edge router stay at every DS domain they check compliance with the SLA and does the policing. The excess packets are either discarded or marked as low priority to comply with a SLA because the excess packets are marked as low parity that is why you say it is not a guaranteed QoS that are a expected QoS or the best effort QoS. Now the core router it will just look at to the DSCP and decides the corresponding part of behaviour.

(Refer Slide Time: 34:48)



The slide is titled "Further Readings" in a dark blue header. The main content area is light yellow and contains a bulleted list of two links. The footer is dark blue and includes the IIT Kharagpur logo, the NPTEL Online Certification Courses logo, and a navigation bar with various icons.

Further Readings

- Cisco White Papers on QoS -
 - <https://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-service-qos/index.html>
 - http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

IIT KHARAGPUR | NPTEL ONLINE CERTIFICATION COURSES

Now, here are certain links that you can look further to understand in details the differentiated service and the integrated service architecture. So, these two topics are little advanced topic which are not there in your reference book that we have mentioned earlier so, that is why you have given two links. So, you can browse to these two links to find out the details. So, this is all about the quality of service in the internet, and I hope that by this time you have a nice idea about what quality of service means and how to apply quality of service over a internet.

And you can go through this Cisco documentation that I have shared to understand more about this quality of service and how different types of quality of service are actually implemented in set Cisco routers indeed the process; is a bit complex and there are multiple modules each work all together to support this. So, I try to give you a very brief overview or a, but self view of this entire quality of service to give you an understanding about this topic.

Thank you all for attending this class.